J Korea Industr Inf Syst Res Volume 18 Number 4
http://dx.doi.org/10.9723/jksiis.2013.18.4.043

차량간 인증 기반 메시지 집계 프로토콜 관리시스템 설계†

(A Design of Protocol Management System for Aggregating Messages based on Certification between Vehicles)

이 병 관*, 정 은 희**
(ByungKwan Lee and EunHee Jeong)

요 약 본 논문에서는 차량 간의 메시지 전송 시에 차량 메시지를 인증함으로서 Sybil 공격에 의해 메시지가 위·변조되는 것을 막고, 동시에 전송 시에 빈번하게 발생하는 중복되는 차량 메시지를 집계하여 효율적인 통신을 제공하는 차량간 인증 기반 메시지 집계 프로토콜 관리시스템 설계를 제안한다. 이를 위하여 제안 시스템은 첫째, 세션 키 기반 로컬인증서인 SKLC(Session Key based Local Certificate)를 설계하고, 둘째, 중복되는 차량 메시지를 집계하는 MAP(Message Aggregation Protocol) 설계를 제안한다. 따라서 제안 시스템은 차량의 인증서를 확인할 때, 해시 함수 연산으로 메시지 무결성을 검증하여 신뢰성이 높은 정보를 안전하게 제공할 뿐만 아니라, 연산 처리 시간을 줄여 통신 효율도 향상시킨다.

핵심주제어 : VANET, 세션키 기반 로컬 인증서, 시빌 공격, 메시지 집계, 무결성

Abstract This paper proposes the design of protocol management system for aggregationg messages based on certification between vehicles which not only prevents the messages between vehicles from being forged and altered by Sybil attack by authenticating the them, and but also provides the efficient communication by aggregating the redundant vehicle messages which frequently happens when communicating. For this, the proposed system proposes the SKLC(Session Key Local Certificate) design which is a local certificate based on a session key, and the MAP(Message Aggregation Protocol) design which aggregates the redundant vehicle messages. Therefore, when the proposed system checks the certificate of vehicle, it provides the reliable information securely by verifying the integrity of vehicle with a hash function operation, and improves communication efficiency by reducing the processing time.

Key Words : VANET, SKLC, MAP, Sybil Attack, Message Aggregation, Integrity

1. 서 론

최근 국내외적으로 차량에 IT기술을 적용하는 ITS(Intelligent Transportation System) 연구가 활발하게 이루어지고 있다. 여기에 ITS의 핵심 기술인 VANET(Vehicular Ad-hoc Network)은 MANET (Mobile Ad-hoc Network)의 확장 개념으로 차량 간

† 본 논문은 중소기업청에서 지원하는 2012년 산학연공동기술개발사업(No. C0034249)의 연구수행으로 인한 결과물임을 밝힙니다.
* 관동대학교 컴퓨터학과, 제1저자
** 강원대학교 지역경제학과, 교신저자(jeongeh@kangwon.ac.kr)

출동 방지 및 교통량 통제 등의 여러 가지 방법을 제시하고 있다[1][2].

즉, VANET은 지능형 차량을 이용한 V2V(Vehicular-to-Vehicular), V2I(Vehicular-to -Infrastructure)간의 무선 통신을 지원함으로써 사회적으로 문제가 되고 있는 심각한 교통 체증 문제 해결과 사고 사전 예방 등 다양한 서비스 제공을 기본 목표로 하고 있다. 하지만, VANET은 기본적으로 네트워크 기반의 무선 환경을 바탕으로 하고 있기 때문에, 기존의 무선 네트워크 환경이 가지고 있는 보안상의 취약점을 그대로 승계하고 있다[3].

더욱이, VANET에서는 악의적인 코드에 의해 수정된 응용프로그램들이 전파 방해 공격, 위조 공격, 위장 공격, 트래픽 위·변조 공격 등으로 차량 간 교환되는 메시지가 사용자의 안전에 직접적인 위협을 가하기 때문에 VANET은 높은 신뢰성이 보장되어야 한다[4].

따라서 VANET에는 안전 운행과 관련된 메시지의 내용이 공격자들에 의해서 위·변조되어 전파되면 고의적인 사고가 유발될 수 있으므로 적절한 보안 메커니즘뿐만 아니라, 차량 간 전송되는 빈번한 메시지에 비정상적이거나 중복되는 교통정보가 포함되어 있어 VANET의 통신 효율이 저하되므로 이 통신 오버헤드를 줄일 수 있는 메커니즘도 필요하다.

본 논문에서는 차량 간의 메시지 전송 시에 차량 메시지를 인증함으로써 Sybil 공격에 의해 메시지가 위·변조되는 것을 막고, 동시에 메시지 전송 시에 빈번하게 발생하는 중복되는 차량 메시지를 집계하여 효율적인 통신을 제공하는 차량간 인증 기반 메시지 집계 프로토콜 관리시스템을 제안한다. 이를 위하여 첫째, 세션 키 기반 로컬 인증서인 SKLC(Session Key based Local Certificate)를 설계하고, 둘째, 전송 시에 빈번하게 발생하는 중복되는 차량 메시지를 집계하여 안전하고 효율적인 통신을 제공하는 MAP (Message Aggregation Protocol)을 설계한다.

본 논문의 구성은 2장에서 VANET에서 발생할 수 있는 공격들과 VANET 프로토콜의 기본 개념들을 살펴보고, 3장에서는 본 논문에서 제안하는 SKLC 생성 과정과 SKLC를 이용한 메시지 인증과 메시지 집계하는 MAP을 설명한다. 그리고 4장에서는 본 논문에서 제안하는 SKLC와 MAP의 검증과정과 시스템의 안전성에 대한 분석 결과를 설명하고, 5장에서 결론을 맺는다.

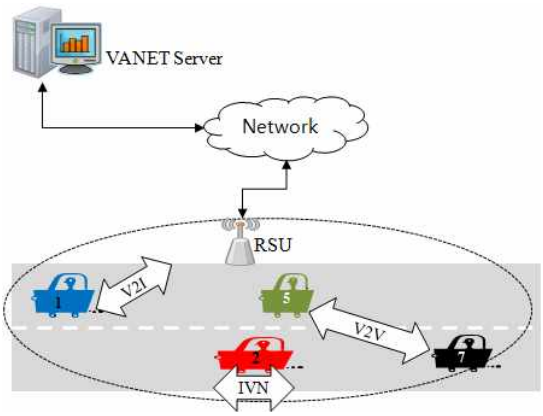
2. 관련연구

2.1 VANET

VANET은 그림 1에서 설명하고 있는 것처럼 차량 내·외부망으로 구분할 수 있는데, 차량 내부망은 일반적으로 IVN(In-Vehicle Network)라고 부르며, 차량 외부망은 차량 간 통신망(V2V)과 차량과 인프라 통신망(V2I)으로 분류된다.

IVN은 차량의 보디나 섀시 부분을 연결하고 제어하는 CAN, 차량의 오디오, 앰프, CDP 등 멀티미디어 기기 접속을 위한 MOST, 그리고 브레이크나 조향장치를 연결하고 제어하는 X-by- Wire(Flexray)가 있다[5, 6].

V2V는 차량 간 통신을 기반으로 통신망을 구성하고 정보를 전달하는 인프라 도움 없이 구성될 수 있는 차량통신망을 형성하여 차량 추돌경고 서비스와 그룹통신을 제공한다. V2I는 차량과 유무선 통신 인프라 망이 접속되어 단말과 서버 간에 통신을 지원할 수 있는 통신망을 제공함으로써 IP 기반의 교통정보 및 안전 지원, 다운로드 서비스를 제공할 수가 있다[6, 7].



<Fig 1> VANET 시스템

하지만 VANET은 다음과 같은 공격에 취약하다[4,8,9,10,11].

- Sybil Attack : 단일 공격자가 네트워크 상에서 복수 개의 환영(illusion) 노드들로 나타나서 혼란을 가중시키는 공격.
- Sending False Information : 거짓 정보를 발생하는 공격 자동차에 의해 일정 네트워크 영역 내에서 다른 자동차들을 거짓 정보로 오염시키는 공격.

- In-transit Traffic Tampering : 고속 주행 중 메시지를 전달하는 과정에서 공격 자동차에 의한 메시지 삭제 및 변조를 통해 자동차 통신을 방해하는 공격.
- Node Impersonation Attack : 이웃 자동차의 정보를 자신의 상태정보로 변경하여 다른 자동차로 하여금 잘못된 자동차 인식을 하도록 하는 공격.

이러한 공격들은 다른 차량에서 보내는 메시지의 정확성을 판단할 수 있거나, 차량의 고유 ID를 확인할 수 있으면 해결가능하다. 본 논문에서는 차량의 신분을 확인할 수 있는 SKLC를 설계하여 이러한 공격들을 탐지하거나 방지하고자 한다.

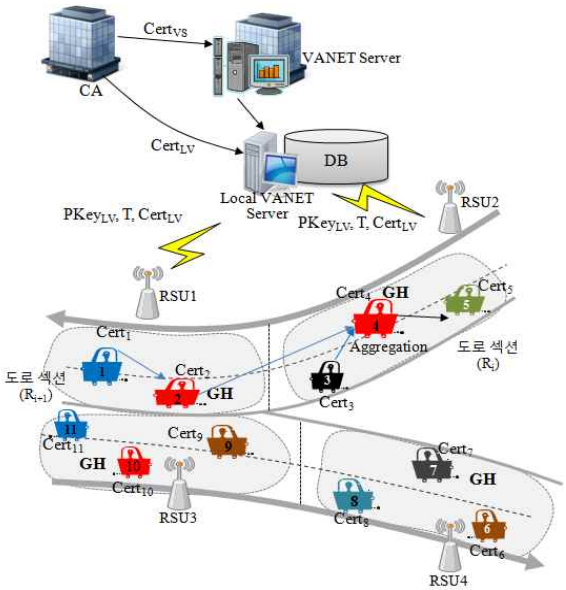
2.2 VANET 프로토콜

VANET의 보안과 프라이버시 요구사항 모두를 만족시키는 암호학 기반 프로토콜은 메시지 송신자의 익명성을 보장할 수 있는 그룹서명과 은익서명을 이용하고 있다[12]. 예를 들어, X. Lin 등에 의해 제안된 GSIS(Group Signature and Identity-based Signature) 프로토콜은 그룹 서명에 기반을 둔 암호학 기반 프로토콜의 대표적인 예이다[13]. GSIS는 인증서를 전송하지 않아도 된다는 장점을 지니고 있지만, 송신차량이 폐지 목록에 포함되어 있는지 확인하기 위한 방대한 연산이 요구된다. 그룹화 기반의 프로토콜은 차량들을 그룹으로 묶어 각 차량의 정확한 ID와 위치를 숨기는 것으로 C. Zhang 등은 k개의 차량이 그룹을 이루고 모두 동일한 ID를 사용하는 기법을 제안하였다[14].

본 논문에서는 암호학기반과 그룹화 기반을 접목한 차량간 인증기반 메시지 집계 프로토콜 관리시스템을 설계하여, 메시지를 전송한 실제 차량의 ID를 알 수는 없지만, 차량이 속한 그룹을 확인하여 차량 신분 확인 및 메시지 무결성을 검증함으로써 VANET의 보안을 강화시키고 네트워크 효율성을 향상시키고자 한다.

3. 차량간 인증기반 메시지 집계 프로토콜 관리 시스템 설계

본 논문에서 제안하는 차량간 인증기반 메시지 집계 프로토콜 시스템은 VANET 서버, 로컬 VANET 서버, 차량, RSU(Road Side Unit)으로 구성되며, 그림 2는 제안하는 시스템의 전체적인 구성요소와 흐름을 설명한 것이다. 여기서 VANET 서버는 로컬 VANET 서버와 RSU를 유·무선 네트워크를 이용하여 전체적으로 관리하고, 로컬 VANET 서버는 그 지역 내의 차량과 EC-DH 알고리즘[13]을 이용하여 세션키를 생성하여, 세션키를 이용한 로컬 인증서인 SKLC를 생성하고, SKLC로 차량의 신분을 인증하는 역할을 한다.



<Fig 2> 차량간 인증 기반 메시지 집계 프로토콜 관리 시스템의 구성 요소

표 1은 논문에서 사용하는 약어들을 설명한 것이다.

<Table 1> 약어 설명

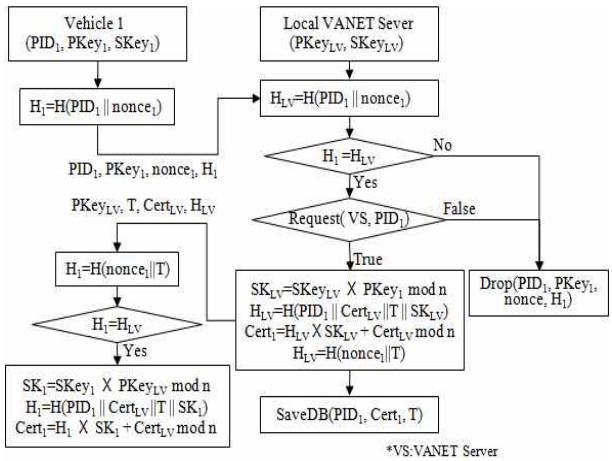
약어	설명
SKLC	세션키기반 로컬 인증서
H	해시함수
GH	그룹헤더(Group Header)
$SKey_{LV}$	로컬 VANET 서버의 비밀키
$PKey_{LV}$	로컬 VANET 서버의 공개키
$Cert_{LV}$	로컬 VANET 서버의 인증서
SK_{LV}	로컬 VANET 서버의 세션키
H_{LV}	로컬 VANET 서버가 계산한 해시값
ID_1	차량 1의 ID
PID_1	차량 1의 익명 ID
$SKey_1$	차량 1의 비밀키
$PKey_1$	차량 1의 공개키
SK_1	차량 1의 세션키(Session Key)
H_1	차량 1이 계산한 해시 결과값
$Cert_1$	차량 1의 로컬 인증서

약어	설명
T	인증서 유효기간
‖	연결기호(Concatenate)
mod	modular 연산 기호
TrafficMsg	교통정보메시지
ArgMsg	집계된 메시지

3.1 SKLC 설계

모든 차량들이 VANET 시스템을 사용하기 위해서는 차량 정보가 사전에 VANET 서버에 등록되어 있어야 한다. 본 논문에서는 차량이 사전에 VANET 서버에 차량 ID, PID(Pseudonym ID), 차량에 대한 기본적인 정보들이 등록되어 있고, VANET 서버, 로컬 VANET 서버 그리고 차량은 ECC 알고리즘[16]을 이용해 차량의 비밀키와 공개키를 생성한다고 가정한다.

SKLC(Session Key based Local Certificate)는 각 차량의 PID, 비밀키, 공개키, 인증서 유효날짜 T, 그리고 로컬 VANET 서버의 인증서를 이용하여 생성한다. 그림 3은 SKLC 생성 흐름도를 설명한 것이며, SKLC 단계별 생성과정은 다음과 같다[17].



<Fig 3> SKLC 생성 흐름도

[1 단계] 차량 1은 VANET 서버에 등록한 PID_1, $PKey_1$, $nonce_1$, PID_1와 $nonce_1$를 해시한 값 H_1을 로컬 VANET 서버에 전송한다.

$$H_1 = H(PID_1 \| nonce_1)$$

[2 단계] 로컬 VANET 서버는 차량 1로부터 전달받은 PID_1, $nonce_1$를 해시한 값인 H_{LV}와 전달받은 H_1을 비교하여 무결성을 확인한다. 그 결과가 참이면, 로컬 VANET 서버는 차량1의 PID_1를 VANET 서버에 확인을 요청한다. 만약 차량 A의 PID_1가 VANET 서버에 존재한다면 다음 단계를 실행하고, 그렇지 않다면 "접속 거부" 메시지를 차량 1에게 전달하고 로컬 인증서 생성 작업을 강제 종료한다.

[3 단계] 로컬 VANET 서버는 차량 1의 공개키 $PKey_1$와 로컬 VANET 서버의 비밀키 $SKey_{LV}$를 곱셈 연산을 하여 차량 1과 로컬 VANET 서버의 공유 비밀키인 세션 키 SK_{LV}를 생성한다. 그리고 인증서 유효 날짜인 T, 로컬 VANET 서버의 인증서인 $Cert_{LV}$, 차량 1의 PID_1, 세션 키인 SK_{LV}를 연접하여 해시함수로 해시한다. 로컬 VANET 서버는 그 해시값을 세션 키인 SK_{LV}로 곱셈 연산을 하고, 로컬 VANET 서버의 인증서의 지문과 덧셈 연산을 하여 차량 1의 로컬 인증서인 $Cert_1$를 생성하여 로컬 VANET 서버의 DB에 (PID_1, $Cert_1$, T)를 저장한다.

$$SK_{LV} = SKey_{LV} \times PKey_1 \bmod n$$
$$H_{LV} = H(PID_1 \| Cert_{LV} \| T \| SK_{LV})$$
$$Cert_1 = H_{LV} \times SK_{LV} + Cert_{LV} \bmod n$$

[4 단계] 로컬 VANET 서버는 차량로부터 전달받은 $nonce_1$과 인증서 유효기간 T를 연접하여 해시함수로 해시한 값인 H_{LV}와, 공개키 $PKey_{LV}$, 인증서 유효기간 T, 로컬 VANET 서버 인증서 $Cert_{LV}$를 차량 1에게 전송한다.

$$H_{LV} = H(nonce_1 \| T)$$

[5 단계] 차량 1은 $nonce_1$과 로컬 VANET 서버로부터 전달받은 인증서 유효기간 T를 연접하여 해시함수로 해시한 값 H_1과 로컬 VANET 서버로부터 전달받은 해시 값 H_{LV}를 비교하여 무결성을 확인한다. 그 결과가 참이면, 차량 1은 로컬 VANET 서버의 공개키와 차

량 1의 비밀키를 곱셈 연산하여 공유 비밀키인 세션 키 SK_1을 생성한다.

$$H_1 = H(nonce_1 \| T)$$
$$SK_1 = SKey_1 \times PKey_{LV} \bmod n$$

[6 단계] 차량 1은 4단계에서 로컬 VANET 서버로부터 수신한 T, $Cert_{LV}$와 5단계에서 차량 1이 계산한 세션 키인 SK_1를 연접하여 해시함수로 해시한다.

$$H_1 = H(PID_1 \| Cert_{LV} \| T \| SK_1)$$

[7 단계] 차량 1은 5단계의 세션 키와 6단계의 해시값, 그리고 로컬 VANET 서버 인증서의 지문을 이용하여 세션 키 기반 로컬 인증서인 $Cert_1$을 생성한다. 이때 이용된 값과 계산 방식은 3단계와 같으므로, 차량 1의 세션키 기반 로컬 인증서는 3단계에서 계산된 인증서와 동일한 값을 갖게 된다.

$$Cert_1 = H_1 \times SK_1 + Cert_{LV} \bmod n$$

3.2 MAP 설계

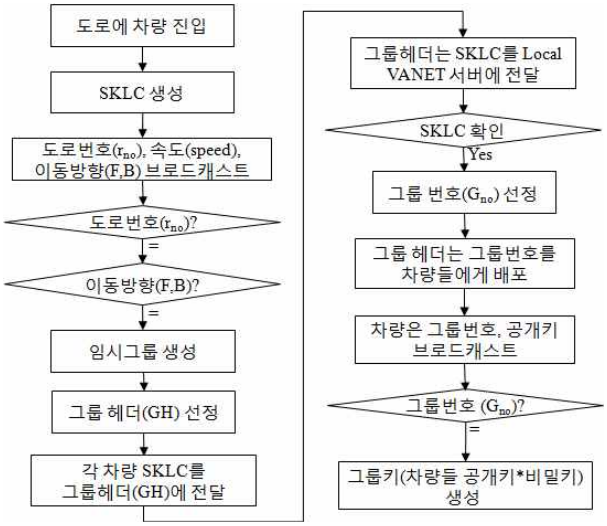
VANET 시스템에서 모든 차량들이 이웃하는 차량들에게 메시지를 전송한다면, VANET 시스템 네트워크의 오버헤드가 발생하므로 VANET 시스템의 통신 효율이 감소할 것이다.

본 논문에서는 VANET 시스템 내의 차량들을 그룹으로 묶은 후 그룹 헤더를 선정하고, 그룹 헤더가 메시지를 집계한 후, 이웃하는 그룹 헤더에게 메시지를 전달하도록 함으로써 VANET 시스템의 통신 효율을 증가시키고자 한다.

3.2.1 그룹 설정

본 논문에서는 차량의 이동 방향과 도로 섹션 번호가 같은 차량들로 그룹을 묶고, 해당 그룹 내의 차량 중에서 그룹 헤더를 선정하도록 설계한다. 그룹 헤더는 그룹 내의 메시지를 집계하거나, 다른 그룹 헤더가 전달한 메시지를 그룹 내의 차량들에게 브로드캐스트하는 역할을 담당한다.

차량 그룹 설정, 그룹 헤더를 선정하고 그룹키를 생성하는 과정은 그림 4와 같으며, 그 단계 절차는 다음과 같다.



<Fig 4> 그룹, 그룹키 생성 흐름도

[1 단계] 차량이 도로에 진입을 하면, 차량은 자신의 위치와 속도, 이동방향을 주변 차량에 브로드캐스트 한다.

[2 단계] 새롭게 진입한 차량들은 서로의 이동방향과 속도, 도로 번호를 확인한 후, 임시 그룹으로 분류한다.

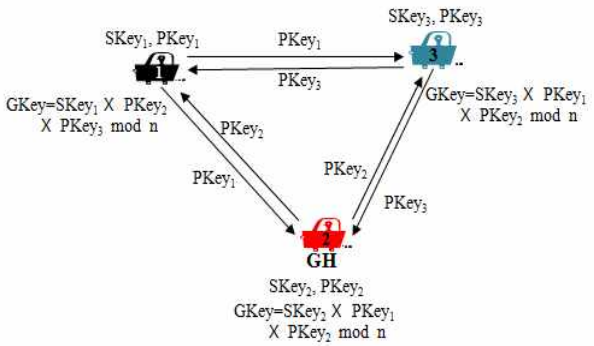
[3 단계] 임시 그룹 내의 모든 차량들과 1홉 단위로 브로드캐스트 하는 곳에 위치하고 있는 차량을 그룹헤더로 선정한다.

[4 단계] 그룹헤더는 임시 그룹 내의 모든 차량으로부터 받은 SKLC들을 로컬 VANET 서버에 확인을 요청한다.

[5 단계] 로컬 VANET 서버는 SKLC를 확인한 후, 그룹 번호를 부여하면, 그룹 헤더는 그룹 내의 모든 차량들에게 그룹번호를 브로드캐스트 한다.

[6 단계] 그룹 내의 모든 차량들은 공개키, 그룹번호를 브로드캐스트하면, 차량들은 그룹번호를 확인하고, 그룹 내의 모든 차량들의 공개키와 자신의 비밀키로 그룹키를 생성한다.

예를 들어, SKLC로 서로의 신분을 로컬 VANET 서버에 이미 확인한 차량 1, 차량 2, 차량 3이 같은 차량 그룹이고, 이 차량 그룹의 그룹헤더가 2인 경우에 그룹키는 그림 5와 같이 생성된다[3].



<FIg 5> 그룹키 생성의 예

3.2.2 MAP 설계

VANET 시스템에서 모든 차량들이 이웃하는 차량에게 일관성이 없는 비정상적인 데이터 전송을 막고, 중복되는 데이터를 없애고, 또한 해시함수를 이용한 메시지 무결성을 검증하는 MAP(Message Aggregation Protocol)를 설계한다. 이때, 차량이 전송하는 모든 메시지는 해당 그룹 내의 그룹키로 서명하여 그룹헤더에 메시지를 전송하고, 그룹 헤더는 차량들이 전송한 메시지의 무결성을 검증하도록 설계한다. 그리고 집계된 메시지를 이웃 차량 그룹 헤더에 전달함으로써 빈번한 교통정보 메시지 전달로 인한 VANET 네트워크 오버헤드를 줄여 통신 효율과 신뢰성을 향상시키고자 한다.

메시지 집계 과정은 다음과 같으며, 그림 6에서 그룹헤더가 모든 차량으로부터 전송된 교통정보메시지의 무결성을 검증하고 메시지의 중복성을 제거한 후에 저장하는 집계 메시지(AgrMsg)의 구조와 안전하게 메시지를 집계하는 과정을 설명하고 있다.

[1 단계] 그룹 내의 모든 차량들은 교통정보메시지(TrafficMsg)를 그룹헤더에 전달한다.

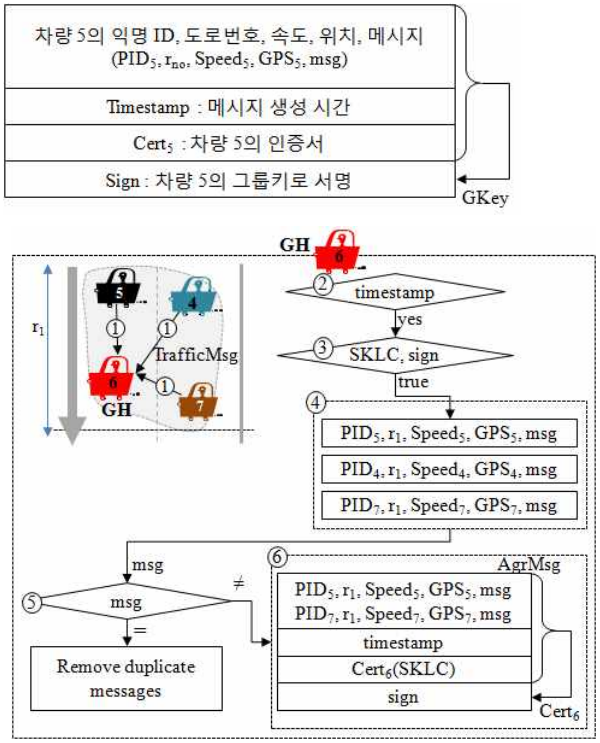
[2 단계] 그룹헤더는 TrafficMsg의 timestamp로 메시지 유효기간을 확인한다.

[3 단계] 그룹헤더는 메시지 보낸 차량의 SKLC로 차량의 신분을 확인하고, sign을 이용하여 집계된 메시지의 무결성과 그룹 구성원임을 확인한다.

[4 단계] 그룹헤더는 3단계의 결과가 True인 것만을 수집한다.

[5 단계] 그룹 헤더는 수집된 메시지의 내용을 비교하여 중복된 데이터를 삭제한다.

[6 단계] 그룹헤더는 중복성이 제거된 메시지를 집계 메시지에 추가하고, 집계 메시지 생성시간, 그룹헤더의 인증서, 서명을 추가한 AgrMsg를 다른 그룹의 헤더에게 전달한다.



<Fig 6> MAP 흐름도

4. 분 석

4.1 SKLC 검증

그림 7은 SKLC 검증 절차를 설명한 것이고, 검증 단계는 다음과 같다.

[1 단계] 차량 1은 차량 2에게 메시지를 전달하기 전에 차량 1의 익명 ID인 PID_1와 로컬 인증서 $Cert_1$을 전송한다.

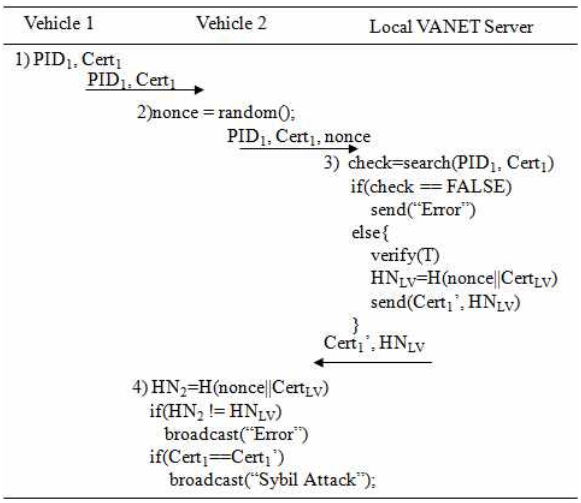
[2 단계] 차량 2는 랜덤한 수 nonce를 생성하고, 차량 1에게서 전달받은 PID_1와 nonce를 로컬 VANET 서버에 전송한다.

[3 단계] 로컬 VANET 서버는 PID_1를 로컬 VANET 서버의 DB에서 확인한다.

[4 단계] 로컬 VANET 서버는 차량 1의 PID_1가 확인되면, 로컬 VANET 서버의 DB에서 PID_1의

로컬 인증서를 검색하고, 유효기간(T)을 확인한다. 그리고 차량 2에게서 수신된 nonce와 로컬 VANET 서버의 인증서를 해시한 값 HN_{LV}과, 차량 1의 로컬 인증서 $Cert_1'$를 차량 2에게 전달한다. 만약, PID_1가 VANET 서버에 존재하지 않으면, 등록되지 않는 차량으로 경고메시지를 VANET 시스템 내의 모든 차량에 브로드캐스팅 한다.

[5 단계] 차량 2가 nonce와 로컬 VANET 서버의 인증서를 해시한 값인 HN_2와 수신된 HN_{LV}와 일치하는지 검사한다. 이때, 일치하지 않으면, 차량 2가 의뢰한 로컬 VANET 서버가 아닌 것으로 간주하고, 에러 메시지를 출력한다.



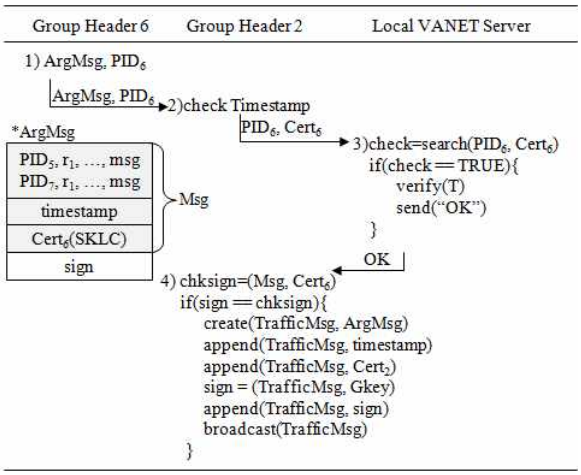
<Fig 7> SKLC 검증 절차

[6 단계] 4단계의 검사 결과가 참이면, 차량 1이 전송한 $Cert_1$과 로컬 VANET 서버가 전송한 로컬 인증서인 $Cert_1'$를 비교한다. 이 두 개의 로컬 인증서가 일치하지 않으면, 차량 A는 Sybil 공격으로 검출된다.

4.2 MAP 검증

본 논문에서는 그룹헤더에 의해서 생성된 집계 메시지를 다른 그룹 헤더에게 전달함으로써 빈번한 교통정보 메시지 교환으로 인한 네트워크 오버헤드를 줄이고, 그룹헤더에 의해 전달된 집계 메시지의 무결성을 검증함으로써 VANET의 신뢰성을 향상시키고자 한다.

그룹헤더 6이 다른 그룹의 그룹헤더인 2에게 집계된 메시지인 ArgMsg를 전달하였다고 가정할 때, 집계된 메시지의 무결성 검증 절차는 다음과 같으며, 그 과정을 그림 8에서 설명하고 있다.



<FIg 8> 메시지 무결성 검증 절차

[1 단계] AgrMsg를 전달받은 그룹헤더 2는 메시지의 timestamp를 이용하여 유효한 시간이내의 메시지인지를 확인한다.

[2 단계] 그룹헤더 2는 로컬 VANET 서버에 그룹헤더 6의 인증서인 $Cert_6$의 유효성 확인을 요청한다.

[3 단계] 로컬 VANET 서버의 확인 결과 그룹헤더 6의 신분이 확인되면, 그룹헤더 2는 $Cert_6$으로 ArgMsg에 대한 서명을 생성한 후, ArgMsg의 서명(sign)과 확인한다.

[4 단계] 3 단계의 결과가 일치하면, 그룹헤더 2는 집계된 메시지를 그룹키인 $GKey$로 서명하여 그룹 내의 차량에게 브로드캐스트 한다.

4.3 안전성 평가

본 논문에서 제안하는 SKLC는 차량의 ID가 아닌 익명 ID를 사용하므로, VANET 시스템의 RSU와 V2V 통신하는 다른 차량들은 차량의 실제 ID를 알 수 없다. 차량이 로컬 VANET 서버에 다른 차량의 신분을 요청할 때, 익명 ID와 EC-DH으로 계산된 세션키로 생성된 로컬 인증서를 이용하므로, 차량의 비밀키를 소유하고 있지 않으면 인증서를 생성할 수 없

으며, 익명 ID와 인증서로는 차량 ID를 추적할 수 없으므로 차량의 프라이버시를 제공한다.

또한, 제안하는 시스템의 그룹키는 차량이 각 그룹의 구성원인지를 확인하여 Sybil 공격을 탐지할 수 있을 뿐만 아니라, 그룹키로 메시지를 암호화하여 전송함으로써 Sending False Information, In-transit Traffic Tampering, Node Impersonation Attack과 같은 거짓 정보 전송 또는 메시지 위·변조 공격으로부터 안전한 통신을 지원 할 수 있다.

제안하는 시스템에서 생성되는 TrafficMsg와 AgrMsg에는 각각 타임스탬프가 포함되어 있다. 따라서 메시지에 포함된 타임스탬프가 임계시간 범위를 벗어나면 삭제하도록 설계하였다. 따라서 VANET 통신에서 차량이 브로드캐스트 하는 모든 메시지에 메시지 발생 시간이 포함되어 있으므로 임계시간 이내에 메시지가 수신된 메시지 이외의 메시지는 재생공격으로 간주하여 메시지를 버리므로 재생공격을 방지할 수 있다.

5. 결 론

VANET 환경의 서비스는 실시간 교통 정보의 수집과 제공을 통해 차량 간의 정보 전송, 추돌 방지, 응급상황 경고, 도로 상태 경고 등 운전자의 안전과 밀접한 서비스를 지원한다.

본 논문에서는 조건부 익명성을 제공하는 차량간 인증기반 메시지 집계 프로토콜 관리 시스템을 설계하여 다음과 같은 VANET 시스템의 효율성을 제공하였다.

첫째, 차량 간의 신분을 확인하기 위한 세션 키 기반 로컬 인증서인 SKLC를 생성하였다.

둘째, SKLC로 차량 간의 신분을 확인함으로써 ID를 도용하는 Sybil 공격을 쉽게 검출할 수 있다.

셋째, 익명 ID를 사용하므로 차량의 프라이버시를 보호할 수 있다.

넷째, 차량의 인증서를 확인할 때, 해시함수를 이용한 간단한 연산으로 차량 신분 확인을 위한 연산 처리 시간을 줄였다.

다섯째, 빈번하게 발생하는 중복 메시지를 집계하여 전달함으로써 VANET 시스템의 통신 효율성을 향상시켰다.

여섯째, 메시지 무결성 검증으로 운전자는 신뢰성이 높은 정보로 안전하게 운행 할 수 있으며, 교통사고의 감소 효과를 기대할 수 있다

References

[1] P. Caballero-Gil, “Security Issues in Vehicular Ad Hoc Network,” Mobile Ad-Hoc Networks : Applications, pp.67-88, 2011.

[2] 홍원기, 변정식, “네트워크 단절 개선을 위한 적응적 전달자 노드 검색 기법,” 한국산업정보학회논문지 제14권 제3호, pp.50-57, 2009.

[3] Meng-Yen Hsieh, Hua-i Lin, Chin-Feng Lai and Kuan-Ching Li, “Secure protocol for data propagation and group communication in vehicular networks,” Journal on Wireless Communication and Networking, pp.1-16, 2011.

[4] 이병관, 정용식, 정은희, “VANET에서 ECHD 기반 그룹키를 이용한 그룹간 인증 설계”, 한국산업정보학회논문지, 제17권 제7호, pp.51-57, 2012.

[5] 이소연, “차내망 인터페이스,” TTA 저널, No.117, 2008년 5월.

[6] 오현서, 박종현, “차량 통신 네트워크 기술 동향,” 전자통신동향분석, 제23권 제5호, pp.49 -55, 2008년 10월.

[7] 오현서, 조한벽, 최혜옥, "차량통신기술동향," 연구진흥원 주간기술동향포커스, 2007년 9월호.

[8] 강상우, 박세진 “TPM의 Authenticated Boot를 활용한 VANET의 보안 향상 기법 설계,” 한국컴퓨터종합학술대회 논문집, Vol.36, No.1(D), pp.216-222, 2009.

[9] Douceur, J. “The Sybil Attack. In: First International Workshop on Peer-to-Peer Systems,” March 2002, pp. 251 - 260 (2002)

[10] Maxim Raya, Panos Papadimitrators, and Jean-Pierre Hubaux, "Securing Vehicular Communications," In Magazine of IEEE Wireless Communications - IVC Specials, EPFL, pp.8-15 Oct. 2006.

[11] 박영호, 나진한 문상재, “VANET 상에서의 차량간 통신을 위한 인증 프로토콜,” 한국산업정보학회논문지 제14권 제2호, pp.81-85, 2009.

[12] 김인환, 최형기, 김정윤, “프라이버시를 보호하며

안전하고 효율적인 차량간 통신 프로토콜," 정보과학회논문지 : 정보통신 제 37편 제6호, pp.420-430, 2010.
[13] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS : A Secure and Privacy-Preserving Protocol for Vehicular Communications," IEEE Transaction Vehicular Technology, vol.56, no.6, pp.3442-3456, 2007.
[14] C. Zhang, R. Lu, P.-H. Ho, and A. Chen, "A Location Privacy Preserving Authentication Scheme in Vehicular Networks," Proc. of IEEE WCNC 2008, pp.2543-2548, 2008.
[15] Elaine Barker, Don Johnson, and Miles Smid, "Recommenation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography(Revised),", NIST Special Publication 800-56A, March, 2007. (http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007. pdf)
[16] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol.48, pp.203-209, 1987.
[17] ByungKwan Lee, EunHee Jeong, Ina Jung, "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET," International Journal of Security and Its Applications Vol. 7, No. 3, pp. 1-10, May, 2013.

이 병 관 (ByungKwan LEE)

- 정회원
- 부산대학교 기계공학과 공학학사
- 중앙대학교 전자계산공학과 공학석사
- 중앙대학교 전자계산공학과 공학박사
- 관동대학교 공과대학 컴퓨터학과 교수
- 관심분야 : 네트워크 보안

정 은 희 (EunHee Jeong)

- 정회원
- 강릉대학교 통계학과 이학사
- 관동대학교 전자계산공학과 공학석사
- 관동대학교 전자계산공학과 공학박사
- 강원대학교 인문사회과학대학 지역경제학과 부교수
- 관심분야 : 네트워크 보안, 인터넷보안, 전자상거래 보안

논 문 접 수 일 : 2013년 07월 03일
1차수정완료일 : 2013년 07월 22일
게 재 확 정 일 : 2013년 07월 31일