VANET에서 ECDH 기반 그룹키를 이용한 그룹간 인증 설계

(A Design of Group Authentication by using ECDH based Group Key on VANET)

이 병 관*, 정 용 식, 정 은 희*****

(Byung Kwan Lee, Yong Sik Jung, and Eun Hee Jeong)

요 약 본 논문에서는 안전한 V2V 통신과 V2I 통신을 보장하는 ECDH(Elliptic Curve Diffie Hellman) 기반 그룹키를 제안하였다. 본 논문에서 제안하는 ECDH기반 그룹키는 AAA 서버를 사용하지 않고 차량과 차량사이의 그룹키인 VGK(Vehicular Group Key), 차량 그룹 사이의 그룹키인 GGK(Globak Group Key), 그리고 차량과 RSU사이의 그룹키인 VRGK(Vehicular and RSU Group Key)를 ECDH 알고리즘을 이용하여 생성한다. 차량과 RSU 사이의 그룹키인 VRGK는 현재 RSU에서 다음 RSU에게로 RGK(RSU Group Key)로 암호화하여 안전한 채널을 통하여 전달하기 때문에 완벽한 순방향 기밀(Perfect Forward Secrecy) 보안 서비스가 제공된다. 또한, 메시지를 전송한 차량이 해당 그룹의 구성원인지를 그룹키 이용하여 확인함으로써 Sybil공격을 탐지할 수 있다. 그리고 그룹간의 안전한 통신으로 불필요한 네트워크 트래픽이 발생하지 않으므로 메시지 전송 시간 및 서버의 오버헤드를 줄일 수 있다.

핵심주제어 : 차량 애드 혹 네트워크, 차량간 통신, 그룹 키, 그룹 통신, 인증, 타원곡선

Abstract This paper proposes a group key design based on ECDH(Elliptic Curve Diffie Hellman) which guarantees secure V2V and V2I communication. The group key based on ECDH generates the VGK(Vehicular Group key) which is a group key between vehicles, the GGK(Global Group Key) which is a group key between vehicle groups, and the VRGK(Vehicular and RSU Group key) which is a group key between vehicle and RSUs with ECDH algorithm without an AAA server being used. As the VRGK encrypted with RGK(RSU Group Key) is transferred from the current RSU to the next RSU through a secure channel, a perfect forward secret security is provided. In addition, a Sybil attack is detected by checking whether the vehicular that transferred a message is a member of the group with a group key. And the transmission time of messages and the overhead of a server can be reduced because an unnecessary network traffic doesn't happen by means of the secure communication between groups.

Key Words : VANET, V2V, V2I, Group Key, Group Communication, Authentication, ECDH, VGK, GGK, VRGK

* 관동대학교 컴퓨터학과, 제1저자
** 관동대학교 의료경영학과, 제2저자
*** 강원대학교 지역경제학과, 교신저자
(jeongeh@kangwon.ac.kr)

1. 서 론

VANET(Vehicular Ad-hoc NETwork)은 차량간의 통신인 V2V(Vehicle To Vehicle)와 차량과 RSU (Road Side Unit)들 사이의 통신인 V2I(Vehicle To Infrastructure)을 제공하는 MANET (Mobile Ad-hoc NETwork)의 한 형태이다[1]. V2V와 V2I 통신은 모든 도로 여행에서 안전, 효율, 안락함을 향상시키고, 상업적인 정보나 혹은 인터넷 접속과 같은 다른 부가가치 서비스들을 제공하기 때문에 이 네트워크들은 미래 ITS(Intelligent Transportation System)를 위하여 가장 전망이 좋은 해법이라 할 수 있다.

하지만, VANET은 기본적으로 기존의 네트워크 기반의 무선 환경을 바탕으로 하고 있기에, 기존의 무선 네트워크 환경이 가지고 있는 보안상의 취약점을 그대로 승계하고 있다[2]. 더욱이, VANET에서는 차량간 교환되는 메시지가 사용자의 안전과 직결되는 내용을 포함하고 있기 때문에 높은 신뢰성이 보장되어야 하는데, 악의적인 코드에 의해 수정되어 응용프로그램들이 전파 방해 공격, 위조 공격, 위장 공격, 트래픽 위·변조 공격 등을 일으킬 수 있다. 따라서 빠른 이동성을 가진 차량으로 구성된 VANET에서는 차량 사이의 안전한 통신과 키 교환을 위한 효율적인 암호 기법이 필요하다.

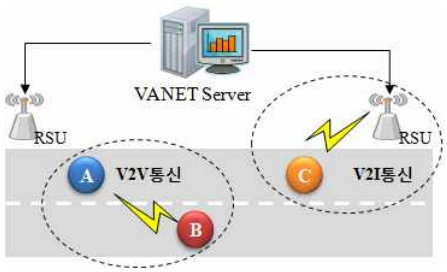
본 논문에서는 ECDH 기반 V2V 그룹키와 V2I 그룹키를 설계하여 차량간 데이터 전달 및 인증, 또는 개별적으로 안전한 그룹 통신 제공하고, 교통과 관련된 정보에 대한 안전한 통신을 제공하고자 한다.

본 논문의 구성은 2장에서 VANET에서 발생하는 보안 취약점을 살펴보고, 3장에서는 본 논문에서 제안하는 각 그룹의 ECDH 그룹키 생성과정을 설명한다. 그리고 본 논문에서 제안하는 ECDH 그룹키의 안전성 분석 결과를 4장에서 설명하고, 5장에서 결론을 맺는다.

2. 관련연구

2.1 VANET

VANET은 차량간의 통신인 V2V와 차량과 도로변 RSU와의 통신인 V2I로 구분할 수 있다. VANET 서버는 RSU를 유·무선 인터넷으로 관리하고, 도로변의 RSU들은 또한 유·무선 인터넷으로 서로 정보를 주고받는다. 그리고 이러한 모든 정보를 관리하는 VANET 서버로 구성된다. <그림 1>은 일반적인 VANET 시스템의 구성을 설명한 것이다.



<그림 1> VANET 시스템

<표 1>은 VANET에서 발생하는 보안 취약성들을 설명한 것이다[4][5][6].

<표 1> VANET 보안 취약성

공격 종류	설명
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
Jamming Attack	일반적인 네트워크상에서의 DoS와 같은 공격방법으로, 일정 네트워크 영역 내에서 다른 자동차의 통신에 장애를 초래하는 신호를 발생시켜 네트워크 통신을 마비시키는 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 상태 정보로 변경하여 다른 자동차로 하여금 잘못된 자동차 인식을 하도록 하는 공격
On-board Tampering	속도, 위치, 자동차 전장 부분의 상태, 각종 센싱 정보등과 같은 자동차 내부의 정보에 대해 위 변조 공격을 함으로써 속도나 위치 등의 센서 정보를 악의적으로 수정하여 부정확한 정보를 제공 하는 것.

이러한 공격들은 다른 차량에서 보내는 메시지의 정확성을 판단할 수 있거나, 차량의 고유 ID를 확인할 수 있으면 해결가능하다. 본 논문에서는 그룹키를 생성하여 차량간의 메시지 무결성을 검증함으로써 이러한 공격을 방지하거나 탐지하고자 한다.

3. ECDH 기반 그룹키 설계

본 논문에서는 차량들의 그룹을 설정하는 방법을 제안하고, 그룹의 인증키인 그룹키를 설계하여 차량간의 안전한 메시지 통신 제공 및 적절한 통신 트래픽을 유지하고, <표 1>에서 설명한 VANET의 보안 취약점을 해결하고자 한다.

본 논문에서 설계하는 VANET 시스템은 가정은 다음과 같다.

첫째, 모든 차량들은 (공개키, 비밀키)를 갖고 있다.

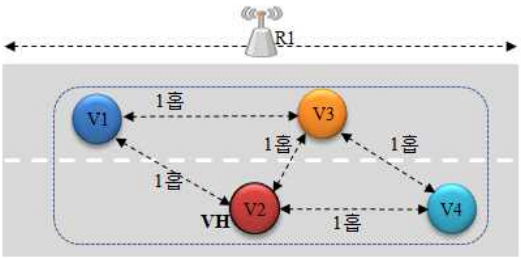
둘째, 모든 차량들은 EC-DH 기반 공개키 교환을 한다.

셋째, RSU는 도로 구간별로 그룹화 되어 있고, (그룹 공개키, 그룹 비밀키)를 가지며 서로 안전한 채널을 통해 메시지를 교환한다.

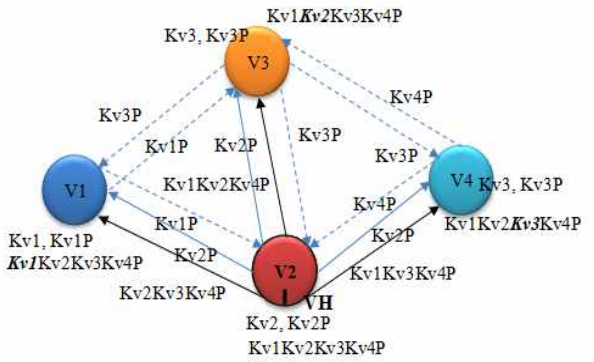
3.1 V2V통신 그룹키 설계

3.1.1 그룹 설정 및 그룹키 생성

차량 그룹을 설정하고 그룹키인 VGK(Vehicular Group Key)를 생성하는 절차는 다음과 같으며, <그림 2>는 차량그룹 생성과정과 VGK 생성과정을 설명한 것이다.



(a) 그룹생성



(b) VGK($K_{v1}K_{v2}K_{v3}K_{v4}P$) 생성

<그림 2> 그룹 생성과정과 VGK 생성과정

[1 단계] 같은 방향으로 이동하는 차량들 중에 1홉의 거리에 있는 차량들을 선택한다.

[2 단계] 선택된 차량들의 가장 중앙에 위치하고 그룹내의 모든 차량들과 1홉의 거리에 있는 차량을 그룹의 헤더로 선정한다.

[3 단계] 그룹 헤더 차량 x(VH_x)는 차량 x의 ID (v_x), 차량 x가 위치한 도로 번호(r_x), (속도($Speed_x$), 위치(GPS_x), 그리고 이웃 노드들의 리스트($NList_x$)를 포함하고 있는 요청메시지인 ReqMsg을 생성한다. 그리고 자신의 비밀키($SK_{VHx}=K_{v2}$)로 서명하여 자신의 공개키($PK_{VHx}=K_{v2}P$)와 그룹 내의 차량 목록을 1홉의 거리에 있는 이웃 차량들에게 이 메시지를 브로드캐스트 한다.

$$\text{ReqMsg}(v_x, r_x, Speed_x, GPS_x, NList_x),\ \text{Sign}(\text{ReqMsg}, SK_{VHx}), PK_{VHx}$$

[4 단계] 이 메시지를 전송받는 이웃 차량들은 메시지의 $NList_x$의 순서에 따라 자신의 공개키를 전달한다. 예를 들어 차량 v_1은 자신의 공개키인 $K_{v1}P$을 1홉 거리내의 이웃 차량에게 브로드캐스트 하고, 차량 v_2는 자신의 공개키를 $K_{v2}P$을 1홉 거리내의 이웃 차량에게 브로드캐스트 한다. 그 결과 그룹 헤더인 차량 x는 이웃 차량과는 1홉 거리이므로 모든 이웃 차량의 공개키를 전달받는다.

[5 단계] 그룹 헤더 차량 $x(=v_2)$라 할 때, 해당 차량의 공개키만을 제거한 모든 차량의 공개키를 해당

차량에게 유니캐스트 한다. 즉, 그룹 내의 차량이 v_1, v_2, v_3, v_4이고, 그룹 헤더 차량이 v_2이라면, 차량 v_2는 차량 v_1에게 그룹내의 차량들의 공개키들의 곱셈연산 결과인 $K_{v2}K_{v3}K_{v4}P$를 유니캐스트 한다.

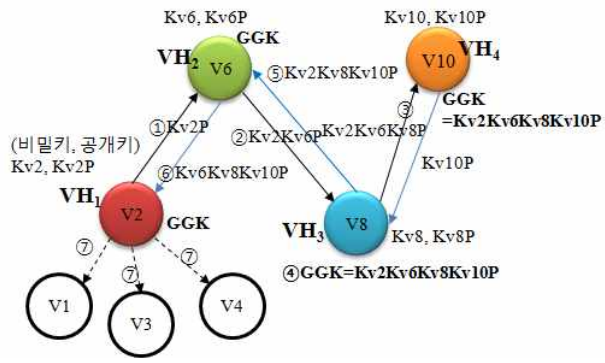
[6 단계] 차량 v_1는 그룹 헤더 차량인 $x(=v_2)$로부터 받은 그룹 차량들의 공개키 곱셈 연산 결과인 $K_{v2}K_{v3}K_{v4}P$에 자신의 비밀키인 K_{v1}를 곱셈연산하여 차량 그룹키인 VGK= $K_{v1}K_{v2}K_{v3}K_{v4}P$ 를 계산한다.

[7 단계] 차량 v_3은 그룹 헤더 차량인 $x(=v_2)$로부터 받은 그룹 차량들의 공개키 곱셈 연산 결과인 $K_{v1}K_{v2}K_{v4}P$에 자신의 비밀키인 K_{v3}를 곱셈연산하여 차량 그룹키인 VGK= $K_{v1}K_{v2}K_{v3}K_{v4}P$를 계산한다. 차량 v_4도 같은 방법으로 차량 그룹키인 VGK= $K_{v1}K_{v2}K_{v3}K_{v4}P$를 계산하므로, 모든 차량들은 같은 그룹키를 계산하게 된다.

3.1.2 그룹간의 그룹키 생성

VANET 시스템에서는 같은 그룹 내의 차량들만 메시지 송수신이 발생하는 것이 아니라 다른 그룹에 메시지를 전달해야하는 경우가 발생한다. 본 논문에서는 이러한 경우 그룹의 헤더가 다른 그룹 내의 차량들의 메시지를 전송해야 하므로 멀티 홉 브로드캐스팅 하도록 설계한다. 그리고 이때 두 그룹이 사용하는 그룹키인 GGK(Global Group Key)를 생성한다.

<그림 3>은 GGK 생성에 대한 흐름을 설명한 것이고, GGK 생성 절차는 다음과 같다.



<그림 3> GGK 생성 과정

[1 단계] 4개의 그룹이 있다고 할 때, $VH_1(=v_2)$는 이웃 그룹 헤더인 $VH_2(=v_6)$에 공개키 $K_{v2}P$를 전달한다.

[2 단계] $VH_2(=v_6)$는 $VH_1(=v_2)$의 공개키에 자신의 비밀키를 곱셈 연산하여 $K_{v2}K_{v6}P$를 생성하고 $VH_3(=v_8)$에 전송한다. $VH_2(=v_6)$가 전송한 $K_{v2}K_{v6}P$를 전달받은 $VH_3(=v_8)$도 자신의 비밀키를 곱셈 연산하여 $K_{v2}K_{v6}K_{v8}P$를 생성하고, 그 결과를 마지막 그룹 헤더인 $VH_4(=v_{10})$에 전송한다.

[3 단계] $VH_3(=v_8)$의 곱셈 결과값을 전달받은 마지막 그룹 헤더인 $VH_4(=v_{10})$는 자신의 비밀키 K_{v10}를 곱셈 연산하여 $K_{v2}K_{v6}K_{v8}K_{v10}P$인 GGK를 생성한다. 그리고 자신의 공개키 $K_{v10}P$를 이웃 그룹 헤더인 $VH_3(=v_8)$에게 전달한다.

[4 단계] $VH_3(=v_8)$은 $K_{v2}K_{v6}K_{v8}P$에 $VH_4(=v_{10})$의 공개키 $K_{v10}P$를 곱셈 연산하여 GGK인 $K_{v2}K_{v6}K_{v8}K_{v10}P$를 생성한다. 그리고 $VH_2(=v_6)$에 $K_{v2}K_{v8}K_{v10}P$를 전달한다.

[5 단계] $VH_2(=v_6)$는 자신의 비밀키인 K_{v6}를 곱셈 연산하여 GGK인 $K_{v2}K_{v6}K_{v8}K_{v10}P$를 생성한다. 그리고 $VH_1(=v_2)$에 $K_{v6}K_{v8}K_{v10}P$를 전달한다.

[6 단계] $VH_1(=v_2)$는 $K_{v6}K_{v8}K_{v10}P$에 자신의 비밀키인 K_{v2}를 곱하여 GGK인 $K_{v2}K_{v6}K_{v8}K_{v10}P$ 를 생성한다. 그 결과 모든 그룹의 헤더는 동일한 GGK를 갖는다.

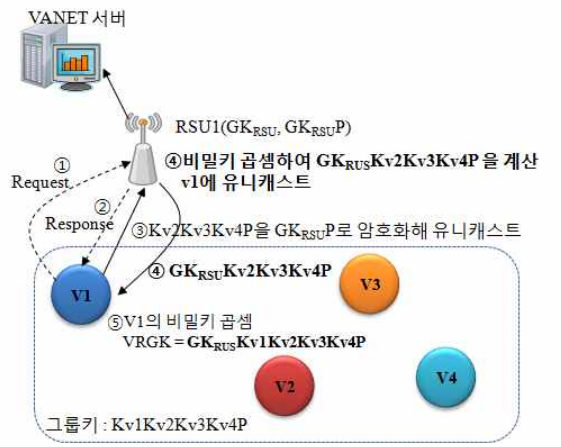
[7 단계] 끝으로, 각 그룹헤더는 그룹헤더가 속해 있는 그룹의 그룹키로 $K_{v2}K_{v6}K_{v8}K_{v10}P$ 를 암호화하여 그룹 구성원들에게 GGK를 배포한다.

3.2 V2I 통신 그룹키 설계

V2I 통신은 차량과 도로변의 RSU 장치와의 통신을 말한다. 본 논문에서는 RSU가 도로 상황이나 위급상황을 도로 위의 차량들에게 전달해야 할 경우에는 인증없이 메시지를 전달한다. 하지만, 차량이 RSU에 요청한 정보를 전달받을 경우에는 차량과 RSU사이에 인증이 필요할뿐만 아니라 메시지를 암호화하여 전송함으로써 메시지의 기밀성을 유지해야 한다.

<그림 4>는 안전한 V2I 통신을 위한 차량과 RSU 사이의 그룹키 생성과정을 설명한 것이다. 그리고

RSU와 차량 사이의 그룹키인 VRGK(Vehicular and RSU Group Key) 생성 절차는 다음과 같다.



<그림 4> VRGK 생성 과정

[1 단계] 차량 v_1은 RSU_1에 요청 메시지 ReqMsg와 ReqMsg를 차량 v_1의 비밀키로 서명하여 보낸다.

ReqMsg(v_1,r_1,$Speed_{v1}$,GPS_{v1}, ETime),
Sign(ReqMsg, K_{v1}) $K_{v1}P$

여기서 r_1는 도로번호, $Speed_{v1}$는 차량 v_1의 속도, GPS_{v1}는 차량 v_1의 위치, ETime은 메시지의 유효기간, $K_{v1}P$는 차량 v_1의 공개키를 말한다.

[2 단계] RSU_1는 차량 v_1의 ReqMsg에 대한 응답 메시지 RespMsg를 보낸다.

RespMsg(v_1, r_1, ETime $GK_{RSU}P$),
Sign(RespMsg, GK_{RSU}),$Cert_{RSU1}$

[3 단계] 차량 v_1은 차량 그룹키인 VGK= $K_{v1}K_{v2}K_{v3}K_{v4}P$ 에서 자신의 비밀키를 제외한 $K_{v2}K_{v3}K_{v4}P$을 RSU_1의 그룹 공개키 $GK_{RSU}P$로 암호화하여 긴밀하게 유니캐스트한다.

[4 단계] RSU_1는 그룹 비밀키를 복호화하고, 그 결과에 RSU_1의 그룹 비밀키를 곱셈 연산한다. 그리고 곱셈결과인 $GK_{RSU}K_{v2}K_{v3}K_{v4}P$ 를 차량 v_1에 유니캐스트한다.

[5 단계] 차량 v_1는 자신의 비밀키를 곱셈 연산하여 차량 v_1와 RSU_1사이의 그룹키 VRGK인 $GK_{RSU}K_{v2}K_{v3}K_{v4}P$ 를 생성한다.

4. 안전성 분석

본 논문에서 설계한 ECDH기반 그룹키로 VANET 시스템에서 안전한 V2V 통신과 V2I통신을 제공한다.

4.1 기존 방식과 비교

기존 방식인 PKI, IEEE 802.11i에서는 이동 중인 차량이 안전한 VANET 서비스를 이용하기 위해서는 지능형 차량과 모든 RSU 사에에는 연속적인 세션키 교환이 이루어져야 하므로, V2I간의 세션키 교환이 빈번하게 발생한다. 따라서, 차량이 모든 RSU와 세션키를 교환하기에는 많은 오버헤드가 발생한다.

제안기법은 차량과 RSU간에 VRGK인 세션키인 그룹키를 생성하고, RSU가 이 그룹키를 차량이 이동하는 방향과 속도를 고려하여 해당 RSU에 안전하게 전달하므로 차량 이동시 추가적으로 차량과 RSU 사이의 새로운 그룹키(=세션키) 생성 없이 사용할 수 있다. 따라서 RSU 개수만큼 세션키를 생성하는 기존 방식과는 달리 제안한 V2I 그룹키 기법은 RSU 그룹 수만큼만 그룹키를 생성하므로 키 생성 횟수를 줄였다.

또한 그룹키는 AAA 서버와 CA 서버를 사용하지 않고 V2I 간의 그룹키를 생성함으로써 그룹키 생성시에 발생하는 서버의 오버헤드를 줄일 수 있다.

<표 2> V2I 키 교환 기법 비교[7][8]

	IEEE 802.11i	PKI	제안기법
키 생성	차량과 RSU 이동	차량과 RSU 이동	차량과 RSU 이동
키 주체	AAA서버	차량,CA서버	차량,RSU
키 교환 대상	차량과 RSU 사이	차량과 RSU 사이	차량과 RSU 사이
차량 키 생성개수	1	1	1
교환 메시지 수	4	2	2

4.2 안전성 평가

본 논문에서 제안하는 ECDH 기반 그룹키 생성 기법은 비밀키가 노출이 되어도 ECDH 알고리즘을 사용하므로 완벽한 순방향 기밀 보안 서비스를 제공한다. 또한, 그룹키인 VGK, GGK, VRGK으로 차량이 각 그룹의 구성원인지를 확인하여 Sybil 공격을 탐지할 수 있고, 그룹키인 VGK, GGK, VRGK으로 메시지를 암호화하여 전송함으로써 악의적인 공격자에 의한 메시지·변조 공격으로부터 안전한 통신을 지원 할 수 있다.

본 논문에서는 RSU가 차량과 RSU 사이의 그룹키인 VRGK를 다른 RSU에 전달할 때, RGK으로 암호화하여 안전하게 전달할 수 있으며, RSU는 VGRK로 이동한 차량에 대해 사전에 등록된 차량인지를 확인할 수 있다. 따라서 악의적인 공격자가 RSU를 통해 불법적으로 네트워크에 접속을 시도 할 경우, RSU는 차량에 대해 사전에 등록된 차량인지를 확인함으로써 악의적인 공격자의 접근을 차단 할 수 있다.

5. 결 론

본 논문에서는 안전한 V2V 통신과 V2I 통신을 보장하기 위는 ECDH 기반 그룹키를 제안하였다.

첫째, 차량 그룹 내의 안전한 통신을 보장하기 위한 방법으로 같은 방향으로 이동하는 차량간의 그룹을 설정하고, 그 그룹의 구성원들의 ECDH 기반 그룹키인 VGK를 설계하였다.

둘째, 차량 그룹간의 안전한 메시지 통신을 위한 차량 그룹간 ECDH 기반 그룹키를 GGK를 설계하였다.

셋째, 차량과 RSU 사이에 안전한 메시지 통신을 위한 ECDH 기반 그룹키인 VRGK를 설계하였다. 이때, VRGK는 AAA 서버나 CA 서버를 사용하지 않고 차량과 RSU 사이의 그룹키인 VRGK를 생성한다.

그 결과, VRGK의 생성 횟수를 줄여 VANET 서버와 무분별한 통신 트래픽 발생을 방지하여 서버의 오버헤드를 줄일 수 있었으며, 각 그룹의 그룹키로 차량이나 RSU의 신분을 확인함으로써 Sybil 공격이나 메시지 위·변조 공격을 탐지할 수 있다.

참 고 문 헌

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

[2] 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

[3] P. Celka, N. J. Bershad, and J. M. Vesin, "Stochastic gradient identification of polynomial Wiener systems: Analysis and applicaion," IEEE Transactions on Signal Processing, vol. 49, issue 4, pp.301-313, 2001.

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

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

[6] 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.

[7] IEEE Computer Society, "IEEE Standard for Information technology - Telecommuni -cations and information exchange between systems- Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifications," 2007.07

[8] S. Boeyen Entrust, T. Howes Netscape, P. Richard Xcert "Internet X.509 Public Key Infrastructure Operational Protocols- DAPv2," RFC 2559, IETF PKIX Working Group, April. 1999

이 병 관 (Byung Kwan Lee)

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

정 용 식 (Yong Sik Jung)

- 종신회원
- 대구대학교 산업공학과 공학사
- 건국대학교 산업공학과 공학석사
- 일본 오사카부립대학 경영공학과 공학박사
- 미국 캘리포니아 주립대학 경영정보학과 방문교수
- 캐나다 알버타 주립대학 의과대학 보건의료센터 방문교수
- 관동대학교 의료경영학과 교수
- 관심분야 : 의료정보시스템, U-Healthcare 서비스

정 은 희 (Eun Hee Jeong)

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