Journal of the Korean Society of Marine Engineering, Vol. 41, No. 9 pp. 890~895, 2017
J. Korean Soc. of Marine Engineering (JKOSME)
https://doi.org/10.5916/jkosme.2017.41.9.890

ISSN 2234-7925 (Print)
ISSN 2234-8352 (Online)
Original Paper

기지국 기반 그룹키를 통한 안전한 통신에 관한 연구

조민재† · 김용건[1] · 김창돈[2] · 민병인[3] · 김진섭[4]

(Received November 3, 2017 ; Revised November 13, 2017 ; Accepted November 19, 2017)

Research on secure communication through RSU-based group key

Min-Jae Jo† · Yong-Geon Kim[1] · Chang-Don Kim[2] · Byoung-In Min[3] · Jin-Seob Kim[4]

요약: 최근 안전한 도로시스템과 교통량의 효율성을 위한 지능형 교통 체계(ITS, Intelligent Transportation Systems)와 관련된 많은 연구들이 진행되고 있으며, 국내에서는 스마트하이웨이와 차세대 지능형 교통 체계(C-ITS, Cooperative ITS) 등의 연구가 진행되어 지고 있다. 차세대 지능형 교통 체계(C-ITS)는 차량 간 통신인 V2V(Vehicle to Vehicle), 차량과 기지국 간의 통신인 V2I(Vehicle to Infrastructure) 커뮤니케이션을 사용하여 도로 환경의 안전에 초점을 맞춘다. V2V와 V2I 통신을 이용하여 도로를 주행하는 차량으로부터 여러 가지 정보를 수집하거나 사용자에게 도로의 소통 상황이나 사고 상황, 돌발 상황 등 도로 정보를 제공하여 사고와 지체가 없는 안정된 도로 주행 환경을 제공하고자 한다. 차량 간 및 차량과 기지국간 통신에서 안정된 도로 주행 환경을 제공하기 위해서는 사용자에게 전달되는 안전 메시지가 보호되어 통신되어야 한다. 특히, 사용자 안전과 밀접한 메시지들은 다른 사용자들에게 노출되거나 변조되지 않아야 하며 악의적인 목적을 가진 공격자로부터 메시지를 보호하여야 한다. 본 논문에서는 이러한 안전 메시지들을 보호하기 위한 통신 방안에 대한 연구를 정리하여 기지국(RSU, Road Side Unit)이 그룹의 리더가 되어 그룹 키를 배포, 생성, 관리를 통해 안전한 차량 네트워크 방식을 제안한다.

주제어: WAVE 통신, V2I, 그룹 키 통신, 안전한 차량 네트워크

Abstract: Recently, many studies related to the intelligent transportation systems (ITS) have been conducted for safer road systems and higher traffic efficiency. In Korea, studies such as the smart highway and cooperative intelligent transportation system (C-ITS, Cooperative ITS) are in progress. The C-ITS focuses on the safety of the road environment using vehicle-to-vehicle (V2V) communication, which is communication between vehicles and vehicle-to-infrastructure (V2I) communication, which is communication between a vehicle anda road side unit (RSU). Both forms of communication collect information from vehicles driven on the road or provide users with road information such as traffic situations, accidents, and unexpected situations to provide a stable road driving environment without accidents or delays. To do so, the messages must be protected and communicated in close relation to user safety. In particular, messages that are closely related to user safety should not be exposed or tampered with by other users, and the messages should be protected from malicious intruders. Therefore, in this paper, we summarized research on a secure vehicular network communication and proposed a group key communication based on an RSU.

Keywords: WAVE communication, V2I, Group key communication, Secure vehicular network

1. 서 론

최근 도로 교통 흐름의 효율성과 안전을 강화하기 위한 지능형 교통 체계(ITS, Intelligent Transportation Systems)에 대한 연구가 활발히 진행 되고 있으며, 차량 간 통신인 V2V(Vehicle to vehicle), 차량과 기지국 간 통신인 V2I(Vehicle to Infrastructure)인 V2X(Vehicle to everything) 통신기술을 이용한 도로 환경의 안정성을 중점으로 둔 C-ITS(Cooperative ITS)에 대한 연구도 활발히 진행 되고 있

† Corresponding Author (ORCID: http://orcid.org/0000-0002-4433-2539): R&D Center, eSSys Corp., 55, Gaetbeol-ro, Yeonsu-gu, Incheon, 21999, Korea, E-mail: eklim@essys.co.kr, Tel: 032-215-0850
1 R&D Center, eSSys Corp., E-mail: ygkim@essys.co.kr, Tel: 032-215-0846
2 R&D Center, eSSys Corp., E-mail: cdkim@essys.co.kr, Tel: 032-215-0847
3 R&D Center, eSSys Corp., E-mail: minbi@essys.co.kr, Tel: 032-215-0848
4 R&D Center, eSSys Corp., E-mail: hsjinseob@essys.co.kr, Tel: 032-215-0854

Table 1: Comparison between Raya and Hubaux and Extended Raya and Hubaux

	Raya and Hubaux	Extended Raya and Hubaux
Initial key transmission	$L \rightarrow * : H_A, \{SK\}_{PukA}, H_B, \{SK\}_{PukB}, H_C, \{SK\}_{PukC}, Sig_{PkL}[whole\,msg]$	$L \rightarrow * : H_A, \{SK\}_{PukA}, H_B, \{SK\}_{PukB}, H_C, \{SK\}_{PukC}, Sig_{PkL}[whole\,msg]$
Message transmission	$L \rightarrow * : M, HMAC_K(M)$	$L \rightarrow * : E_{SK}[M], Sig_{PKL}[HMAC_{SK}(M)]$
Add Vehicle	$L \rightarrow V : \{K\}_{PukV}, Sig_{PkL}[\{K\}_{PukV}]$	$L \rightarrow V : \{SK\}_{PukV}, Sig_{PkL}[\{SK\}_{PukV}]$

다. 국내에서는 스마트하이웨이, 차세대 지능형 교통 체계(C-ITS) 및 스마트 자율협력주행 도로시스템 개발 등의 연구가 진행되고 있다. 이러한 연구는 사용자가 빠르고 안전하게 주행하면서 필요한 정보를 받을 수 있게 하며 사고와 지체가 없는 안정된 도로를 목표로 하고 있다.

V2X통신 기술을 통해 도로 상황 정보, 날씨 정보, 주변 위치 정보뿐만 아니라 응급 상황, 돌발 상황 등 안전 관련 서비스, 차선 변경 도움, 교차로 조정, 비상 상황 알림과 같은 서비스를 제공하며, 도로에 주행하는 차량들의 여러 가지 정보들을 수집한다. 도로상에서 생성되는 정보들(돌발 상황 검지정보, 공사정보, 교통정보 등)을 효율적으로 차량에게 전달하는데 사용되며 교통 혼잡 및 사고를 개선하고자 한다.

이러한 사용자 안전과 밀접한 관련이 있는 서비스들은 안전한 통신을 토대로 서비스가 제공되어야 한다. 안전과 관련된 메시지들이 악의적인 목적을 가진 공격자들에게 노출되거나 변조되지 않아야 한다. 메시지 변조나 위조, 가로채기 등으로 인한 메시지 노출로 인하여 사용자의 안전 서비스가 방해받지 않아야 한다. 그렇기에 이러한 서비스들은 안정된 네트워크상에서 보호되어야 한다. 차량 네트워크상에서 안전한 통신을 위한 방안에 대한 연구들을 정리하여 소개한다.

본 논문에서는 차량 네트워크에서 안전한 통신을 위한 방안으로 그룹 키 방식에 대해 살펴보며, 그룹 내 차량이 리더가 되는 방식과 기지국이 리더가 되어 그룹 키를 관리하는 방안을 비교하며 기지국 기반의 그룹 키를 통해 안전한 차량 네트워크를 구성하는 방식에 대해 설명한다. 기지국이 그룹의 리더가 되어 그룹 키를 생성, 배포, 관리 및 차량에 대한 인증하는 방식에 대해 제안하고자 한다.

2. 관련 연구

Raya and Hubaux**[1][2]**는 GKMP(Group Key Management Protocol)로부터 안전한 차량 네트워크를 위한 간단한 안전한 차량 그룹을 제안하였다. 도로를 셀(cells)로 나누고 이 셀을 그룹으로 정의하였고, 셀의 중앙에 가까이에 위치한 차량을 그룹의 리더로 지정하였다. 인증된 공개키를 주기적으로 브로드캐스트하고 그룹의 리더는 그룹 키를 생성하여 그룹 멤버에게 분배하는 역할을 한다. 메시지 전송 시에는 암호화를 하지 않고 HMAC(Hash-based Message Authentication Code)을 이용한 메시지 무결성만 지원한다. 하지만 위와 같은 방식은 부인방지를 막을 수 없어서 생명과 연관된 안전 메시지 전송에서는 사용할 수 없다는 단점이 있다.

Extended Raya and Hubaux**[3]**는 기존 Raya and Hubaux의 통신 방식이 인증만을 지원하고 기밀성과 부인방지를 하지 못한다는 단점이 있어 이를 개선한 방식을 제안하였다. 안전한 그룹 통신을 위해서 메시지 전송 시 메시지를 공유된 그룹 키로 암호화하고, 메시지 무결성을 위해 HMAC을 사용하였다. 부인방지를 막기 위한 방법으로 보내는 차량의 비밀키를 이용하여 시그니처를 생성하고 전송하도록 하였다.

Table 1는 Raya and Hubaux 방식과 확장된 Raya and Hubaux 방식을 비교하였다. Raya and Hubaux 방식과 확장한 방식은 구조상에는 크게 다르지 않다. 두 방식 모두 그룹 내 차량이 리더가 되어 그룹 키를 다루는 방식이다. 하지만 기존 방식은 메시지 전송 시 암호화하지 않은 것과 부인방지를 하지 못하는 문제가 있어 확장한 방식에서 메시지 전송 시 암호화하고 부인방지를 지원하였다.

하지만, Raya and Hubaux 방식과 이를 확장한 방식은 그룹의 리더를 차량이 맡아 그룹 키를 생성, 관리, 배포를 담당한다. 그렇기에 그룹에서 리더를 맡은 차량이 오버헤드가 발생하게 되는 단점이 있다.

Robust and Scalable Protocol**[4]**은 그룹의 리더를 차량이 아닌 기지국을 이용한 안전한 자동차 네트워크를 위한 인증 프로토콜을 제안하였다. 인증 프로토콜은 signcrpytion과 group signature으로 나누어진다. signcrpytion은 차량에서 기지국으로부터 비밀 멤버 키를 받기 위해 사용되며, group signature은 차량 간 통신에 사용된다. 승인된 차량은 익명으로 메시지를 브로드캐스트(broadcast) 할 수 있다. 그룹 관리자인 TM(Tracing Manager)을 제외하곤 누가 메시지를 보냈는지 알 수 없다. 다만, TM은 잘못된 차량이 안전 메시지를 브로드캐스트 했을 때, 해당 차량을 찾아내어 보낸 메시지를 무시 할 수 있다.

ACPN**[5]**은 차량 에드혹 네트워크(VANET, Vehicular Ad-hoc NETworks)에서의 조건부적인 프라이버시 보호와 부인방지를 위한 인증 프레임워크를 제안하였다. 인증을 위해 IBC(ID-based Cryptography)을 사용하고, 프라이버스 보호와 부인방지를 위해 랜덤기반 메커니즘(pseudonym-based mechanism)을 사용한 방식을 제안하였다.

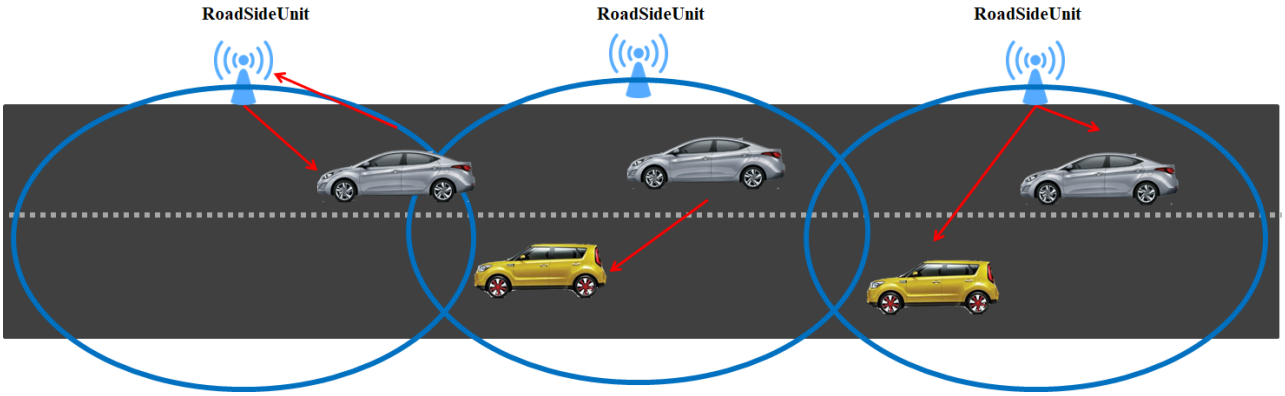

Figure 1: The Overview of our proposed System

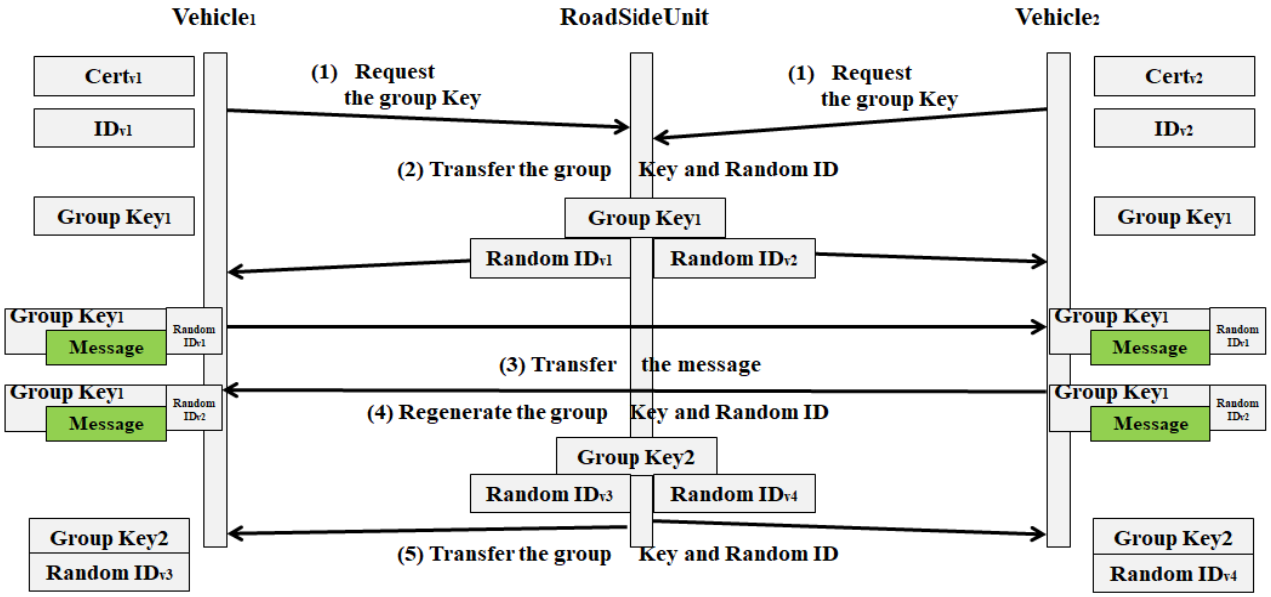

Figure 2: The Communication process of our proposed System

최근 C-ITS 등 차량 간 통신 및 차량과 기지국 간의 통신은 미국 표준인 IEEE WAVE**[6]** 통신을 주로 사용하고 있다. WAVE 통신에서 차량 간 및 차량과 기지국 간 통신에서 메시지 암호화와 인증 등의 기능을 제공하기 위해 IEEE 1609.2**[7]** 표준을 제정하였다. 암호화 알고리즘은 대칭키 기반의 AES-CCM(Advanced Encryption Standard - Counter with CBC-MAC)을 이용하고, 인증 등 메시지 무결성 지원을 위해서는 비대칭키 기반의 ECC(Elliptic Curve Cryptography) 알고리즘을 이용한다. 또한 PKI(Public Key Infrastructure)기반의 인증서를 사용하여 차량 및 메시지 인증 및 암호화를 지원한다. 또한 북미에서는 차량 간 및 차량과 기지국간 통신을 위한 메시지 보안 솔루션으로 SCMS(Security Credential Management System)**[8][9]** 프로젝트를 진행하고 있다. SCMS도 PKI기반의 방식을 사용하여 암호화 및 인증서 관리를 지원한다. SCMS에 의해 발행된 인증서를 통해 안전한 통신과 차량의 프라이버시 등을 보호할 수 있다.

3.제안하는 방식

자동차 네트워크에서 안전한 통신을 위해서 네트워크 그룹 내 차량을 리더로 선출하는 방식과 기지국을 이용하여 관리하는 방식에 대해 알아보았다. 먼저, 그룹 내 차량을 리더로 선출하는 방식은 리더 차량이 그룹 키를 생성, 배포, 관리를 하기에 그룹의 리더 차량이 오버헤드가 발생하게 되는 문제점이 있다. 이러한 단점을 극복하기 위해서 그룹의 리더가 차량이 아닌 기지국이 그룹 키를 생성하고 관리, 배포하는 방식이어야 한다. 따라서 본 논문에서는 기지국 기반의 그룹 키를 통한 안전한 차량 네트워크 시스템을 제안한다. **Figure 1**은 도로에서 기지국의 범위와 차량과 기지국간, 차량 간 그룹 내 통신 등 제안하는 방식의 구조이며, 제안하는 방식의 요약된 통신 절차는 **Figure 2**에 표현하였다. 각 절차는 크게 차량의 그룹 키 요청과 발급(1,2), 그룹 내 통신(3), 그룹 키 재생성 및 발급(4,5)으로 나눌 수 있다.

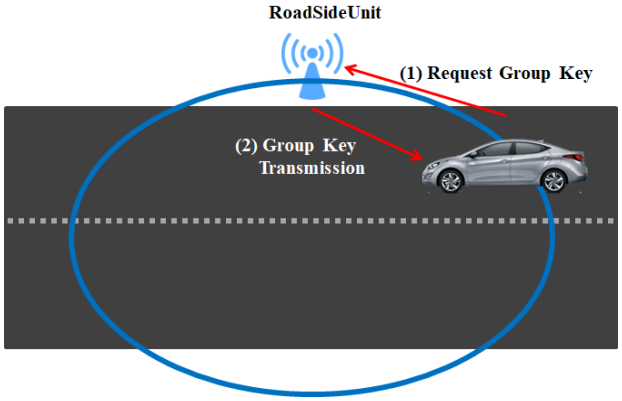

Figure 3: Initial phase of Secure communication

먼저, 초기 단계로 **Figure 3**와 같이 차량이 그룹에 들어왔을 때, 차량은 먼저 그룹 키 발급을 요청한다. 그룹 키를 발급 받기 위해서 차량을 인증 받아야한다. 인증을 위해 차량의 인증서와 차량 ID를 전송한다. **식 (1)**은 차량이 기지국에 그룹 키 발급을 요청하는 것이다.

$$V \rightarrow R: E_{PubR}[Cert_v, ID_V], Sig_{PkV}[Cert_v, ID_V] \quad (1)$$

여기서 V는 차량이며, R는 기지국으로 $V \rightarrow R$는 차량이 기지국에 $Cert_V$와 ID_V를 암호화와 시그니처를 생성하여 전송한다. $Cert_V$는 차량의 인증서이며, ID_V는 차량의 ID이다. E는 암호화 함수이며 Pub_R은 기지국의 공개키로 암호화(E_{Pub_R})는 기지국의 공개키를 가지고 암호화하는 것이다. 시그니처(Sig)는 차량의 비밀키(Pk_V)로 생성하여 부인방지를 지원한다.

기지국은 차량으로부터 받은 차량 인증서를 인증기관을 통해 인증서의 유효성을 검증한다. 차량이 검증된 이후 기지국은 차량에 따라 랜덤 ID를 생성한다. 생성된 랜덤 ID와 차량 정보는 기지국이 암호화하여 저장해 둔다. 기지국은 사고 발생 시 사고 조사를 위해 차량 ID, 인증서, 랜덤 ID를 저장하며 일정 시간이 지난 후에는 정보를 삭제한다. **식 (2)**는 기지국이 차량에게 그룹 키($GroupKey$)와 랜덤 ID (rID_V)을 전송하는 것이다. 기지국은 랜덤 ID와 그룹 키를 차량의 공개키(Pub_V)로 암호화하고 기지국의 비밀키(Pk_R)로 시그니처를 생성하여 전송한다.

$$R \rightarrow V: E_{PubV}[Group\,Key, rID_V], \; Sig_{PkR}[Group\,Key, rID_V] \quad (2)$$

기지국은 차량 인증서, 차량ID와 매칭 하여 랜덤 ID를 생성하고 저장한다. 랜덤 ID는 각 차량에게 익명성을 제공하기 위해서이며, 차량ID와 매칭 하여 관리하는 이유는 추후 사고 발생 시 추적을 위함이다. 이를 통해 익명성과 사고 추적을 가능 하게 한다.

두 번째 단계로 **Figure 4**과 같이 그룹 내 통신 단계이다. 기지국 반경 내에 있는 차량 간의 통신은 그룹 키를 사용하여 메시지를 전송할 수 있다. **식 (3)**은 차량(V)이 그룹 내의 차량이나 기지국(*)에게 메시지를 전송하는 것이다. 차량은 기지국으로부터 받은 그룹 키($GroupKey$)를 통해 그룹에 메시지(Msg)를 전송한다. 전송하고자 하는 메시지는 그룹 키로 암호화하고 인증과 무결성을 위해서 HMAC과 기지국으로부터 받은 랜덤 ID 사용한다.

$$V \rightarrow *: E_{GroupKey}[Msg], \; Sig_{rID_V}\{HMAC_{GroupKey}[Msg]\} \quad (3)$$

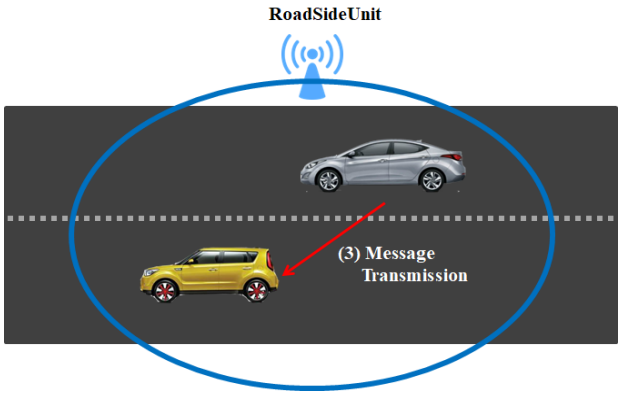

Figure 4: The Vehicle encrypts and transmits the message with the group key

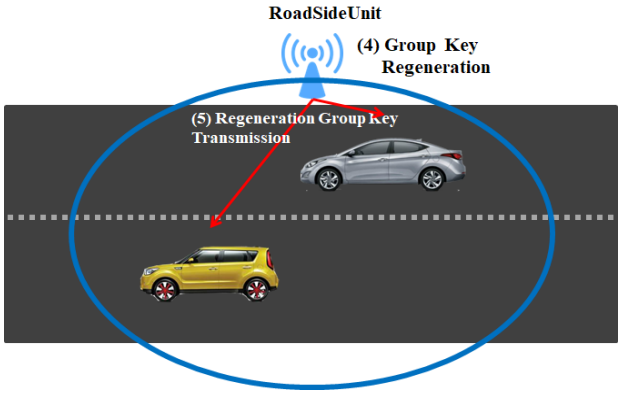

Figure 5: RSU regenerates the group key and transmits it to the vehicles

마지막 절차는 그룹 키 재생성과 발급으로 **Figure 5**과 같이 기지국은 주기적으로 그룹 키를 재 생성한다. 그룹 키는 주기적으로 생성하지만 변조된 메시지 등 공격이 의심되면 즉각 그룹 키를 재 생성한다. 하지만, 본 논문에서는 그룹 키 생성 알고리즘과 관련된 부분은 다루지 않는다.

식 (4)는 재 생성된 그룹 키를 그룹의 차량에게 전송하는 것이며 **식 (2)**와 비슷하다. 재 생성된 그룹 키($GroupKey$)만 각 차량의 공개키(Pub_V)로 암호화하여 전송한다.

$$R \rightarrow V_*: E_{PubV_*}[Group\,Key], \; Sig_{PkR}[Group\,Key] \quad (4)$$

Table 2: Comparison between Our Proposed System and Extend Raya and Hubaux

	Our proposed System	Extended Raya and Hubaux
Initial key transmission	$R \rightarrow V$: $E_{PubV}[Group\,Key, rID_V]$, $Sig_{PkR}[Group\,Key, rID_V]$	$L \rightarrow *$: $H_A, \{SK\}_{PukA}$, $H_B, \{SK\}_{PukB}$, $H_C, \{SK\}_{PukC}$, $Sig_{PkL}[whole\,msg]$
Message transmission	$V \rightarrow *$: $E_{GroupKey}[Msg]$, $Sig_{rID_V}\{HMAC_{GroupKey}[Msg]\}$	$L \rightarrow *$: $E_{SK}[M], Sig_{PKL}[HMAC_{SK}(M)]$
Add Vehicle	$R \rightarrow V$: $E_{PubV}[Group\,Key, rID_V]$, $Sig_{PkR}[Group\,Key, rID_V]$	$L \rightarrow V$: $\{SK\}_{PukV}, Sig_{PkL}[\{SK\}_{PukV}]$
Regeneration key transmission	$R \rightarrow V_*$: $E_{PubV_*}[Group\,Key]$, $Sig_{PkR}[Group\,Key]$	-

기지국은 **Figure 6**과 같이 차량이 전송한 메시지를 수신하며 메시지 검증을 한다. 검증을 통해 차량이 변조된 메시지 등 공격이 의심되는 메시지가 포함되어 있다면, 즉각 그룹 키를 재생성하고 해당 차량을 제외한 차량에게 다시 그룹 키를 전송한다.

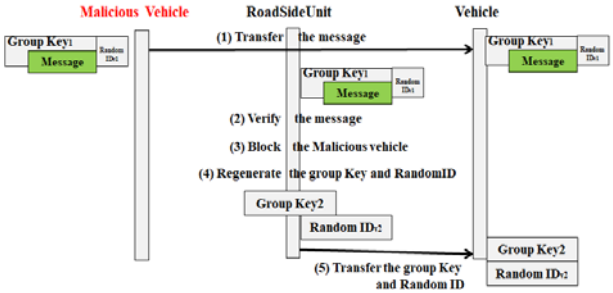

Figure 6: The communication process for block the malicious vehicle

4. 비교

제안하는 방식은 기지국이 리더가 되어 그룹 키를 관리하며 기존의 방식들 중 Extended Raya and Hubax는 차량이 그룹 내 리더가 되어 그룹 키를 관리하는 방식이다. 이 두 가지 방식에서 키 전송과 메시지 전송 등의 방식에 대해 비교하여 **Table 2**에 정리하였다. 그룹에서 그룹 키 전송은 제안하는 방식은 먼저 차량이 기지국에게 자신의 인증서와 차량 ID를 전송한다. Extended Raya and Hubax 방식은 인증서를 전송하며, 두 방식 모두 차량을 인지 후 차량에게 그룹 키를 전송한다. 하지만 제안하는 방식은 랜덤 ID를 부여하여 차량의 익명성을 제공하고 있다. 차량이 그룹 내에서 메시지 전송은 제안하는 방식과 기존 방식 모두 동일하다. 그룹 키로 암호화하고 무결성 및 메시지 인증을 위해 HMAC을 사용하여 시그니처를 생성하여 전송한다. 새로운 차량이 그룹에 진입한 경우에는 그룹 키 전송과 동일한 방식으로 진행되며 제안하는 방식은 랜덤ID를 부여하여 그룹키과 같이 전송해준다. 제안하는 방식은 그룹 키과 랜덤 ID를 재생성하여 그룹 내의 차량에게 다시 전송한다. 기존 방식 또한 그룹 키 재생성을 하여 사용하고 있지만 따로 언급하지 않았다.

Table 3은 기존 방식들과 제안하는 방식을 비교하였다. Raya and Hubaux은 메시지 전송 시 부인 방지와 기밀성을 지원하지 못하였고, 이를 확장한 버전은 부인방지와 기밀성을 지원하였지만 차량의 오버헤드가 발생하는 단점이 있다. Robust and Scalable Protocol는 익명 기반의 그룹 시그니처를 사용하여 부인방지와 기밀성, 익명성을 지원하고 Tracing Manager가 차량을 관리하는 방식을 제안하였다. 하지만 Tracing Manager라는 별도의 관리자가 있어야하는 단점이 있으며, 그룹의 인증서를 받아 그룹의 공개키와 비밀키를 사용하는 방식으로 PKI를 기반으로 한다. PKI를 이용하기에 연산하는 속도와 통신 처리 속도가 증가하게 된다.

본 논문의 제안 방식은 그룹 키를 통해 암호화하며 메시지를 전송하고 랜덤 ID를 발급하고 지속적으로 랜덤 ID를 바꾸면서 차량 추적을 불가능하게 하여 차량의 프라이버시를 보호하였다. 또한 랜덤 ID을 이용하여 시그니처를 생성하여 부인방지를 가능하게 하였고 기지국에서 그룹키를 생성, 관리, 차량 인증을 하였다. 그렇기에 차량의 오버헤드가 발생하지 않고 PKI기반으로 암호화를 하는 방식보다 연산 속도 및 통신 속도가 증가하는 장점이 있다. 별도의 관리자 없이 기지국이 역할을 수행 할 수 있다는 장점이 있다.

5. 결론 및 향후 연구방향

본 논문에서는 차량 네트워크 환경에서 차량 간 및 차량과 기지국 간 통신에서 안전한 통신을 위한 방안에 대해서 살펴보았다. 안전 관련 메시지에 초점을 맞추어 메시지 유출 및 변조가 되지 않도록 하는 방식을 제안하였다. 기존의 차량이 리더가 되는 방식이 아닌 기지국이 그룹의 리더가 되어 그룹 키를 생성, 관리, 배포를 담당하고 차량 인증을 진행하였다. 이러한 방식은 리더로써 차량의 오버헤드를 줄일 수 있다는 장점이 있다.

Table 3: Comparison With Our Proposed System

	Anonymity	Pros Cons	Key Management	Pros Cons
Our Proposed System	Random ID	• guarantee vehicle own's anonymity • other vehicle can't trace vehicles	RoadSideUnit	• vehicle's overhead decreases • key generation time decreases than PKI • don't need the additional manager
		• stores vehicle's information, so when Vehicle leave the group, RSE delete the vehicle information		• may increase attack the RSU
Raya and Hubaux	not support		Vehicle	• don't need the RSU
				• vehicle's overhead increases • key generation time increases than RSU based
Extended Raya and Hubaux	not support		Vehicle	• don't need the RSU
				• vehicle's overhead increases • key generation time increases than RSU based
Robust and Scalable Protocol	Group ID	• guarantee vehicle own's anonymity • other vehicle can't trace vehicles	Tracing Manager	• decreases vehicle's overhead
		• stores vehicle's information • need the group certification		• only tracing manager manages the group • need the additional manager

본 논문은 기지국이 그룹의 리더가 되어 그룹 키를 관리하는 방식으로 차량의 오버헤드는 줄일 수 있는 장점이 있다. 하지만 악의적인 목적을 가진 공격자가 기지국을 공격하여 문제가 발생 했을 때에 대해서는 아직 다루지 않고 있다. 향후에는 기지국에 대한 보안 및 그룹 키 관리로 인해 발생할 수 있는 오버헤드를 줄일 수 있는 방안에 대해서 연구하고자 한다. 또한 실제 테스트 사이트 기지국에 적용하여 기지국 기반 그룹 키 방식에 대한 데이터를 검증하고자 한다.

후 기

본 연구는 국토교통부 교통물류연구개발사업의 연구비 지원(17TLRP-B101446-03)에 의해 수행되었습니다.

References

[1] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks," Proceedings of SASN' 05, pp. 11-21, 2005.

[2] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[3] N. W. Wang, Y. M. Huang, and W. M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," Computer Communications, vol. 31, no. 12, pp. 2827-2837, 2008.

[4] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 4, pp. 1606-1617, 2010.

[5] J. Li, H. Lu, and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938-948, 2015.

[6] IEEE 802.11p-2013: IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metroploitan area networks - Specific requirements - Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Wireless Access in Vehicular Environments, July, 2010.

[7] IEEE 1609.2-2016: IEEE Standard for Wireless Access in Vehicular Environments(WAVE) - Security Services for Applications and Management Messages, January, 2016.

[8] https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf, Accessed October 31, 2017.

[9] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," Vehicular Networking Conference (VNC), 2013 IEEE. pp. 1-8, 2013.