Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 12 pp. 7292-7301, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.12.7292
ISSN 1975-4701 / eISSN 2288-4688

VANET 환경에서 차대번호를 활용한 V2I기반의 통신 프로토콜 설계

이주관[1*], 박병일[1], 박재표[2], 전문석[1]
[1]숭실대학교 컴퓨터학과, [2]숭실대학교 정보과학대학원

Design of V2I Based Vehicle Identification number In a VANET Environment

Joo-Kwan Lee[1*], Byeong-Il Park[1], Jae-Pyo Park[2], Mun-Seok Jun[1]
[1]**Department of Computer Science, SoongSil University**
[2]**Graduate School of Information Science, SoongSil University**

요 약 IT 정보통신 기술의 발달로 인하여 차량통신분야쪽에서 정보, 전자, 통신기술이 융합된 지능형 교통 시스템의 연구가 활발히 진행되고 있다. VANET환경에서는 주로 차량과 차량간의 통신, 차량과 기반 시설간의 통신을 하고 있으며 교통의 편의성 및 안전성을 제공하고 있다. 효율적인 지능형 차량통신을 구축하기 위해서는 보안 기술이 정립되어야 하고, 정적인 네트워크 환경과는 달리 동적인 고속의 이동성을 가지는 VANET환경에서는 차량 통신간의 무선 보안 위협과 많은 취약점이 존재한다. 그러므로 본 논문에서는 VANET 환경에서 차량의 차대번호를 사용하여 이를 신원기반 암호기술로 암호화 하여 안전한 메시지 통신 프로토콜을 설계한다. 제안하는 프토로콜은 차량의 차대번호와 RSU의 일련번호를 활용하여 차량을 등록하고, 신원기반 암호화 방식의 안전한 통신 프로토코을 설계한다. 성능 평가부분에서는 기존의 VPKI 기술과 비교하여 속도적인 측면에서 약 44%의 감소하였으며, 안전성에서는 인증, 메시기 기밀성 및 프라이버시 위협등을 분석하였다.

Abstract With the development of IT Info-Communications technology, the vehicle with a combination of wireless-communication technology has resulted in significant research into the convergence of the component of existing traffic with information, electronics and communication technology. Intelligent Vehicle Communication is a Machine-to-Machine (M2M) concept of the Vehicle-to-Vehicle. The Vehicle-to-Infrastructure communication consists of safety and the ease of transportation. Security technologies must precede the effective Intelligent Vehicle Communication Structure, unlike the existing internet environment, where high-speed vehicle communication is with the security threats of a wireless communication environment and can receive unusual vehicle messages. In this paper, the Vehicle Identification number between the V2I and the secure message communication protocol was proposed using hash functions and a time stamp, and the validity of the vehicle was assessed. The proposed system was the performance evaluation section compared to the conventional technique at a rate VPKI aspect showed an approximate 44% reduction. The safety, including authentication, confidentiality, and privacy threats, were analyzed.

Key Words : Vehicular Adhoc Network(VANET), Authentication

1. 서론

오늘날 IT 정보통신 기술의 발달로 사람과 사람 사이의 통신뿐만 아니라, 최근에는 사람과 사물, 사물과 사물 간의 통신으로 그 영역이 확대 되고 있다. 이는 M2M(Machine to Machine)의 개념으로 차량 통신에서는 차량과 무선통신기술이 접목된 텔레메틱스 또는 ITS(Intelligent Transportation System) 기술의 연구가

*Corresponding Author : Joo-Kwan Lee(SoongSil Univ.)
Tel: +82-10-6431-1018 email: khjljk@nate.com
Received August 8, 2014 Revised December 2, 2014 Accepted December 11, 2014

활발히 진행되고 있다. 국내에서는 차량통신에 관한 연구를 꾸준히 하고 있으며 정보통신기술, 토목기술, 차세대 자동차 기술을 상호기술을 융합한 지능형 고속도로 사업(스마트하이웨이 사업)이 수행중이다[2,6]. 이러한 차량 통신을 위해서는 VANET(Vehicular Adhoc Network) 기술이 필수적이다. VANET은 무선 환경에서 제한적인 대역폭을 사용하므로 많은 제약 요인과 특수성이 고려되어야 한다[1]. VANET환경은 무선통신을 사용함으로써 기존의 보안위협을 계승 및 다양한 공격에 노출될수 있다[3].

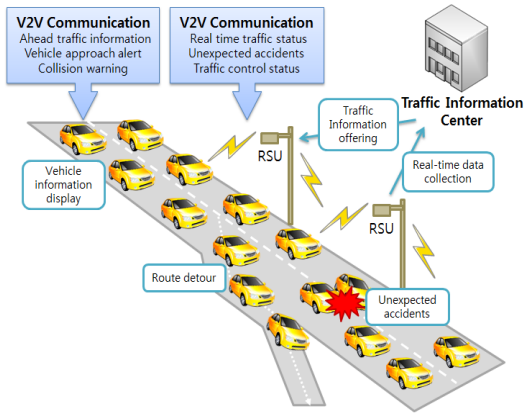
그러므로 본 논문에서는 V2I 기반의 통신 프로토콜에 관하여 연구하고 메시지 정보의 프라이버시를 보호하고 차량과 기반 시설간의 안전한 메시지 전송을 위한 프로토콜을 제안한다.

2. 관련연구

2.1 VANET(Vehicular Ad-hoc Network)

2.1.1 VANET 정의

VANET은 IEEE 802.11 기반의 무선 네트워크 기술로 모바일, 센서, Ad-hoc 네트워크 등과 같은 다양한 정보통신 기술이 융합된 기술이다. 기존 VANET은 위치 탐색이나 경로 설정 등과 같은 단순한 기능 제공 중심이었으나, 최근에는 돌발 상황 알림, 도로 교통 정보 제공 기능과 다양한 서비스가 증가하고 있다. 또한 지능형 통신체계와 기존의 교통정보 알림시스템과 차세대 자동차기술을 융합한 시스템을 연구하고 있다.



[Fig. 1] VANET of wireless Environment

이에 VANET 환경에서 ITS 서비스를 제공하기 위해 효과적이고 적절한 통신 시스템에 요구되고 있으며, 차량 특성에 알맞은 무선 전송 기술이 사용되어야 한다[7,16].

VANET은 이동하는 차량 내에 설치되어 동작하는 통신 모듈인 OBU(On Board Unit)와 도로변에 설치되어 주행 중인 차량이 네트워크 액세스 노드를 이용해 통신 서비스를 이용할 수 있는 기반 시설인 RSU(Road Side Unit)로 구성되어 있다.

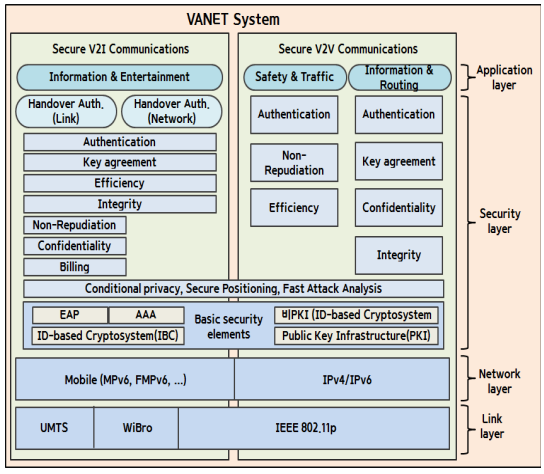
VANET의 메시지 통신방법에서는 Vehicle to Vehicle(V2V)와 Vehicle to Infrastructure(V2I)으로 구분된다[4].

2.1.2 VANET 보안 요구사항

VANET의 V2I, V2V 통신에서 차량 네트워크의 각각 응용서비스 및 네트워크 유형에 따른 보안 요구사항은 다음 Fig. 2와 같이 구분한다[11,12,17].

(1) 차량 및 RSU 인증

VANET에서 통신 개체(OBU, RSU)는 자신의 ID가 정당한 소유자를 인증해야 하고 이를 개체 인증(Entity Authentication)이라 한다. 따라서, 통신 개체는 유일한 ID를 가져야 한다. 즉, 특정 그룹의 차량 간 통신을 수행할 때 그룹의 구성원인 각 차량은 자신이 현재 그룹의 구성원인 것을 증명하여야 한다.



[Fig. 2] Vehicle network security architecture

(2) 메시지 무결성 및 기밀성

V2V 또는 V2I 통신 간에 송수신 되는 메시지는 위·변조되지 않고 안전하게 전송되어야 한다. 또한 비인가 된 사용자의 접근이 보호되어야 한다. 그리고 통신 개체 간 송수신되는 메시지는 공격자에 의한 기밀성이 보호되어야 한다.

(3) 프라이버시 보호

운전자는 자신의 차량에 대한 정보(운전자 식별 정보, 주행 정보 및 위치 정보)를 다른 차량으로부터 보호할 수 있어야 한다. 또한, 주행 안전과 관련해 차량 간의 메시지 통신 프로토콜에 대한 신뢰가 형성되어야 하며 차량을 추적할 수 있는 프라이버시에 대한 보호 방안이 제공되어야 한다.

(4) 부인 봉쇄

메시지를 송신한 개체는 메시지를 전송 받은 사실을 부인 할 수 없어야 하는데 VANET환경에서는 디지털 서명을 활용하기 때문에 부인 봉쇄 기능이 제공한다.

(5) 가용성

각각의 노드는 메시지를 송신할 수 있게 활성화되어야 하고, 전송되는 메시지 는 수신 노드에 적절한 시간 안에 도착해야 한다.

2.2 VANET 환경의 인증기술

2.2.1 TPD(Tamper-Proof Device)

차량 네트워크에 존재하는 각 차량은 TPD라는 정보 변경이 불가능한 고유의 전자번호가 존재하고 있다. 차량 사용자의 비밀정보가 저장되고 있으며 인증기능을 수행한다.

2.2.2 디지털 서명(Digital Signature)

메시지에 대한 인증 및 사용자의 부인 방지 기능을 제공하는 기술로써 사용자의 서명된 Signature가 포함되고 있다. 수신자는 송신자의 공개키를 사용하여 서명된 값을 검증 후 정당한 메시지임을 확인한다.

2.2.3 VPKI(Vehicular PKI)

IEEE 1609.2 표준에서는 PKI기반 VANET 보안 구조를 표준화에 명시되어 있다.16]. VPKI는 인터넷 기반의 PKI(Public Key Infrastructure)를 차량에 적용한 기술로, 제공받는 인증서가 포함된다. 차량은 공인 기관으로부터 부여받은 인증서를 기반으로 V2V, V2I 통신에서 사용되고 있다. 그러나 PKI 구조에서는 차량들이 고속으로 이동하기 때문에 차량 긴급 메시지, 교통 상황 메시지 등의 신속한 반응을 요구하는 서비스에서는 차량의 인증서 유효 검증을 위한 절차로 메시지 송신 시간의 지연으로 인해 차량들이 신속하게 대응하기 어렵다.

2.2.4 익명 키(Anonymous Keys)

VANET 환경에서 네트워크를 사용하는 차량들의 프라이버시를 보호하기 위한 목적으로, 익명 키(Anonymous Key)를 통하여 개인 정보 유출에 관한 목적이 있다.

2.2.5 신원기반 암호방식

고속으로 이동하는 차량으로부터 메시지를 신속하게 전송하기 위해 연구하는 서비스이다. 이 방식은 공개키 암호 시스템의 공개된 값을 사용하여 사용자의 신원를 식별하는 방법으로 사용한다. 신원 방식 암호화 방식의 특징으로는 기존 PKI기반 방식의 상대방 인증을 위한 절차가 없다. 따라서 기반구조를 사용하지 않는 Ad-hoc 네트워크와 같은 환경에 적용하여 사용이 가능하다[10][14].

신원기반 암호방식의 수학적 구조는 bilinear map 함수를 사용하며, 이 함수는 다음과 같은 공식으로 나타낸다.

$$Pair(a \cdot X, b \cdot Y) = Pair(b \cdot X, a \cdot Y)$$

식에서 사용된 연산자는 타원 곡선상의 점들의 곱을 나타내고 있다. 식을 살펴보면 $\cdot$의 연산은 X와 $a \cdot X$를 알고 a를 찾는 역산은 불가능 하다는 특징을 갖는다. 이 방식을 적용한 키 관리 서버는 난수로부터 s와 P를 생성한다. P와 $s \cdot P$ 값은 모든 사용자에게 공지되며, 사용자 x의 개인키인 $s \cdot ID_x$를 계산하여 사용자에게 전달 후 Bob은 임의의 난수 r을 정하고 아래와 같은 식을 활용하여 대칭키를 생성한다.

$$k = Pair(r \cdot ID_{Alice}, s \cdot P)$$

여기서 사용되는 값 $s \cdot P$는 키 서버가 공지한 값이며, $r \cdot ID_{Alice}$는 연산을 수행한 값으로 공개된 값을 사용한다. Bob은 메시지 m에 대하여 생성된 키 k로 암호화한다.

수신자 Alice에게는 암호문 $E_k[m]$과 $r \cdot P$를 전송 후 아래와 같이 수신자의 복호키를 다음과 같이 생성한다.

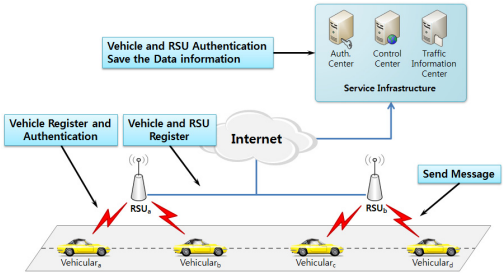
$$k = Pair(s \cdot ID_{Alice}, r \cdot P)$$

생성되는 복호용 키는 $s \cdot ID_{Alice}$ Alice의 개인키 값이 되며, $r \cdot P$는 Bob이 Alice에게 송신한 값이다. 개인키 값은 Alice만이 알고 있는 값으로 암호문의 복호는 Alice만이 가능하다.

3. V2I기반의 차량인증 및 메시지 프로토콜 설계

3.1 제안 프로토콜 개요

본 논문에서 제안하는 시스템의 전체 구성도는 Fig. 3과 같다. V2I 구간에서 차량(Vehicular) A에서 수집한 정보는 RSU를 통해 서비스 인프라의 인증서버에서 인증 및 등록 후 차량(Vehicular) B로 교통 정보(현재 교통 상황, 안전 메시지 등)를 전송하는 메시지 전송 프로토콜을 제안한다.



[Fig. 3] Proposed System Entire Configuration

제안하는 프로토콜은 신원 기반 암호기술을 활용 후 V2I 기반 차량 인증 및 등록 프로토콜, 메시지 전송 프로토콜을 설계한다. 제안 방식은 다음과 같은 조건을 만족한다.

1. Authentication Server는 Road SIde Unit(RSU)의 Serial Number(S/N)를 등록하고 DB에 저장한다.
2. Authentication Server는 Vehicular의 차대번호를 Database에 저장하고 있다.
3. Vehicular, RSU, Authentication Server는 V2I 통신으로 신원기반 암호기술을 활용하여 메시지 암·복호화가 가능하다.

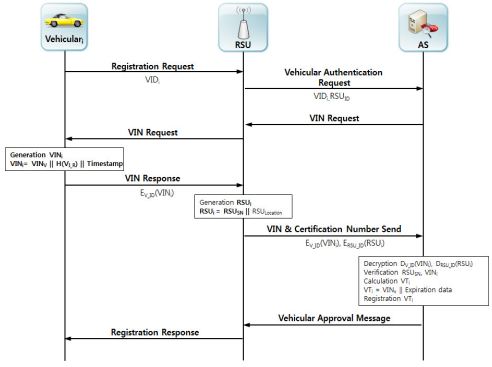
다음 Table 1은 차량 인증 및 등록 프로토콜, 메시지 전송 프로토콜에서 쓰이는 약어 표기법이다.

[Table 1] Abbreviation notation

Notation	Description
VID	Vehicle number
RSU_{ID}	RSU of ID
RSU_{SN}	RSU of Serial Number
$RSU_{Location}$	RSU of Location Value
VIN	Vehicle identification number
$H()$	hash function
V_R	Vehicular generation random Number
VT_i	Validity period the vehicle has been authenticated

3.2 제안시스템 V2I 기반 메시지 전송 기법

차량과 RSU는 차대 번호와 RSU의 Serial Number를 Authentication Server에 송신하고 Authentication Server는 수신 받은 차대 번호와 Serial Number를 검증하여 Database에 등록 후 승인 완료 메시지를 송신한다. 차량 등록 및 인증 프로토콜은 다음 Fig. 4과 같다.



[Fig. 4] Vehicle registration and Authentication Protocol

① Vehicular는 RSU에 차량번호 VID_i를 송신하여 등록을 요청한다.

② RSU는 Authentication Server에 수신 받은 차량번호 VID_i와 RSU_{ID}를 Authentication Server에 송

신하여 등록을 요청한다.

③ Authentication Server는 RSU를 통해 Vehicular에게 차대번호를 요청한다.

④ Vehicular는 아래 식과 같이 VIN_i을 생성한다.

$$VIN_i = VIN_v \| H(V_{i-R}) \| TIMESTAMP$$

차대번호 VIN_v 과 Vehicular가 생성한 난수 R을 해쉬함수를 통해 나온 값 $H(V_{i-R})$, 타임스탬프($TIMESTAMP$) 값을 연접하여 생성한 VIN_i을 차량번호를 신원기반 암호기법을 활용하여 $E_{v-id}(VIN_i)$을 RSU에게 송신한다.

⑤ RSU도 RSU_i를 생성한다. 생성 값은 아래 식과 같다.

$$RSU_i = RSU_{SN} \| RSU_{Location}$$

RSU_{SN}과 RSU의 위치 값 $RSU_{Location}$을 연접하여 생성한 RSU_i를 RSU의 ID를 신원기반 암호기법을 활용하여 $RSU_{RSU-ID}(RSU_i)$와 Vehicular에게 송신 받은 $E_{v-id}(VIN_i)$값을 같이 Authentication Server로 송신한다.

⑥ Authentication Server는 송신 받은 $RSU_{RSU-ID}(RSU_i)$, $E_{v-id}(VIN_i)$값을 복호화하고 RSU_{sn}, VIN_v을 검증한다. 이후 VT_i값을 계산하여 Database Server에 값을 저장하고 등록한다. VT_i의 값은 아래 식과 같다.

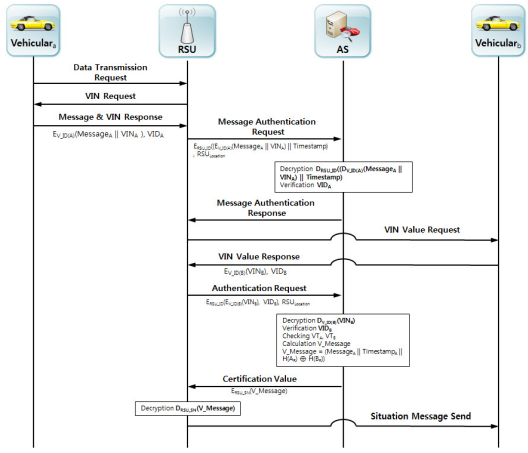
$$VT_i = VIN_v \| Expiration\ Data$$

차대번호 VIN_v와 유효기간 정보를 생성 후 연접하여 DataBase Server에 등록한다.

⑦ Authentication Server는 RSU에게 차량 승인 메시지를 송신하고, RSU는 Vehicular에게 등록 메시지를 송신한다.

3.2.2 메시지 전송 프로토콜

RSU는 Vehicular A에서 수신 받은 메시지를 Authentication Server에 전송하고 차대번호를 검증 및 인증한다. 이후 Vehicular B는 수신 받은 메시지를 전송하기 위해 Vehicular B의 차대번호를 Authentication Server에 송신하고 검증완료 후 Vehicular B에게 메시지를 송신한다. 메시지 전송 프로토콜은 다음 Fig. 5과 같다.



[Fig. 5] Message transmission Protocol

① Vehicular A는 RSU_i에게 데이터 전송을 요청한다.

② RSU_i는 Vehicular A에게 차대번호를 요청하고 Vehicular A는 차대번호 $VIN_A, Message_A$를 암호화 하여 Authentication Server에게 전송한다.

$$E_{V-ID}(Message_A \| VIN_A), VID_A$$

차량번호 VID_A를 활용하여 Vehicular A가 수집한 정보와 차대번호를 연접 후, 암호화하여 VID_A값을 송신한다.

③ RSU_i는 수신 받은 값의 VID_A를 확인하고 아래와 같은 식을 생성하여 Authentication Server에게 전송한다.

$$E_{RSU-ID}(E_{V-ID}(Message_A \| VIN_A), Time\ Stamp), RSU_{Location}$$

수신 받은 값과 Time stamp 값을 RSU_{ID}로 신원기반 암호기술을 활용하여 암호화하고 $RSU_{Location}$을 추가하여 Authentication Server에게 전송한다.

④ Authentication Server는 수신 받은 $D_{RSU-ID}(D_{V-ID}(Message_A \| VIN_A), Time\ Stamp), RSU_{Location}$ 값을 복호화 하여 Vehicular 차대번호 VID_A을 검증하여 RSU_i에게 인증완료 메시지를 전송한다.

⑤ 인증완료 메시지를 수신 받은 RSU_i는 Vehicular B에게 차대번호 VIN 값을 요청한다.

⑥ Vehicular B는 VIN 값을 RSU_i에게 전송한다. 식은 아래와 같다.

$$E_{V-ID}(VIN_B), VID_B$$

Vehicular B의 차대번호 VIN_B를 신원기반 암호 방식으로 암호화하여 차량번호 VID_B를 RSU_i에게 전송한다.

⑦ RSU_i는 Vehicular A와 같이 수신 받은 값의 차대번호 VID_B를 확인하고 아래와 같은 식을 생성하여 Authentication Server에게 전송한다.

$$E_{RSU-ID}(E_{V-ID}(Message_B \| VIN_B), TimeStamp), RSU_{Location}$$

수신 받은 값과 Time stamp 값을 RSU_{ID}로 신원기반 암호기술을 활용하여 암호화하고 RSU의 위치 $RSU_{Location}$을 추가하여 Authentication Server에게 전송한다.

⑧ Authentication Server는 VID_B를 확인하고 $D_{RSU-ID}(D_{V-ID}(Message_B \| VIN_B), TimeStamp), RSU_{Location}$ 값을 복호화 하여 차대번호 VID_B을 검증하고 등록된 VT_A, VT_B값을 검증한다. 이후 $V-Message$을 계산하여 생성한다. 식은 아래와 같다.

$$V-Message = (Message_A \| TimeStamp_A \| H(A_R) \oplus H(B_R))$$

Vehicular A에게 송신받은 $Message_A$, 타임스탬프 값 $TimeStamp$와 차량을 인증할 때 생성된 $H(A_R), H(B_R)$을 Xor한 값을 연접하여 RSU의 Serial Number를 이용하여 신원기반 암호기술을 활용한 값 $E_{RSU-SN}(V-Message)$을 RSU_i에게 송신한다.

⑨ 수신 받은 RSU_i는 $D_{RSU-SN}(V-Message)$을 복호화 하여 Vehicular B에게 메시지를 송신한다.

4. 구현 및 비교분석

4.1 구현 환경

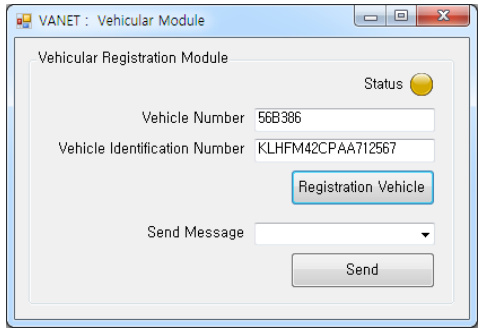
본 논문에서 제안하는 프로토콜의 구현 환경은 다음 Table 2과 같다.

[Table 2] System Development Tool

Division		Description
Operating System		Windows 7 (64bit)
Hardware	CPU	Intel(R) Core(TM) i7-2600 CPU @ 3.40Ghz
	RAM	8.00 GB
Development Tool	Development Tools	qt3 platform and g++ compiler g++ with 4.4.5 Microsoft Visual Studio 2013
	Simulation Tools	NCTUns with Fedora 11

4.2 구현 결과

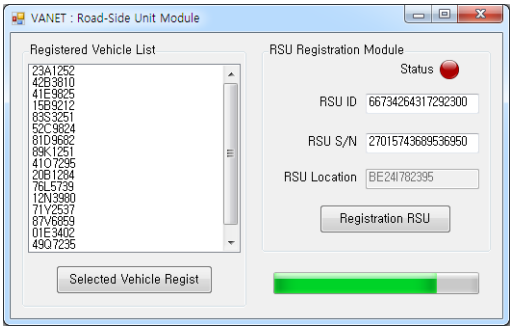
본 논문에서 제안한 V2I 기반 메시지 전송 시스템은 차량 등록 모듈, RSU 관리 모듈 그리고 Authentication Server 모듈을 사용하여 Vehicular와 RSU간 통신구간, RSU와 Authentication Server간 통신구간으로 진행한다. Vehicular에서 메시지 전송을 위한 차량 등록 및 인증 요청 화면은 다음 Fig. 6과 같다. 차량은 Authentication Server에 인증을 수행하기 위해 RSU에게 차량 번호와 차대 번호를 전송한다.



[Fig. 6] Vehicle registration Module

RSU는 차량의 인증 요청을 수신하고, Vehicular의 식별번호와 RSU의 ID와 RSU S/N, RSU Location 정보를 활용하여 식별값을 생성 후 요청작성을 수행한다.

사용하여 식별번호를 생성하고, 인증서버에 차량과 RSU의 인증을 요청한다. RSU 관리 모듈은 다음의 Fig. 7와 같다.

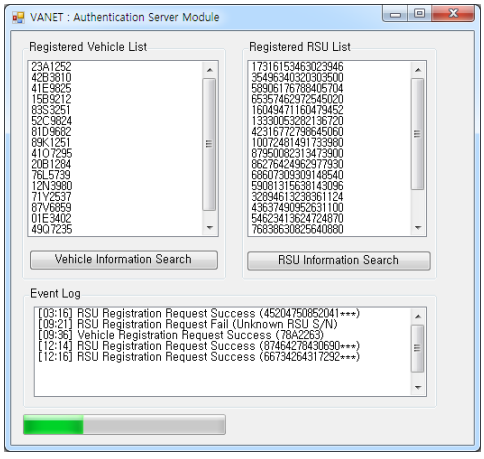


[Fig. 7] RSU Management Module

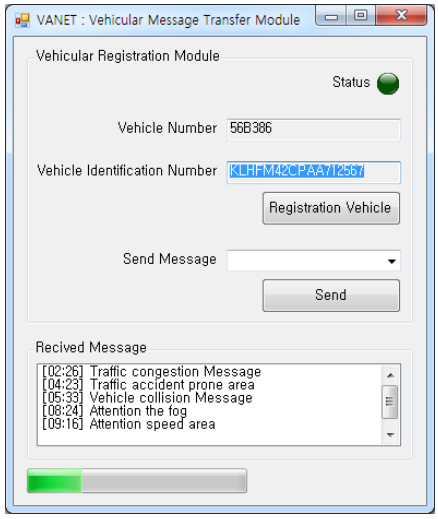
RSU 관리 모듈은 이전 단계에서 등록을 요청한 차량 관리 및 Authentication Server에서 식별값등을 Location 정보를 통해 RSU를 등록하는 모듈이다. 차량과 RSU의 인증 메시지를 RSU 등록 메뉴를 통해 Authentication Server에 요청하게 된다. 하단 Progress Bar는 통신 진행 상태를 나타낸다.

차량과 RSU의 식별 메시지를 수신 받은 Authentication Server는 복호화를 수행하여 검증한 후 RSU로 식별값을 전송한다.

Fig. 8은 Authentication Server 모듈 조작 화면을 나타낸다. 좌측 공간은 차량 인증정보를 등록하고, 우측 공간에는 RSU 인증정보를 등록 후 상세정보를 파악하고 차량 정보, RSU 정보를 확인할 수 있다.



[Fig. 8] Authentication Server Module



[Fig. 9] Vehicle Message Transmission Module

위의 Fig. 9는 차량 메시지 전송 모듈로, Vehicular는 차량 번호와 차대 번호 그리고 Vehicular가 생성한 랜덤 값을 사용하여 RSU를 통해 Authentication Server에 인증한 후 메시지를 송수신 한다.

4.3 기존 시스템과의 비교 분석

4.3.1 효율성 분석

본 절에서는 제안 시스템을 구현하여 VANET 환경의 통신 시스템과 효율성에 관하여 비교분석하였다. 차량 등록 및 인증 효율성 비교분석에서는 제안 프로토콜과 기존 차량통신 인증 기술의 효율성 분석 결과, 대략 2.3배의 성능 차이가 난다.

[Table 3] Vehicle Authentication and registration Efficient Comparison

Division	PKI Based Technique(VPKI)	Proposed Protocol
1 Time	23.24	10.1
5 Times	111.84	49.5
10 Times	217.92	97.8
50 Times	1078.72	489.2
100 Times	2117.92	967.3

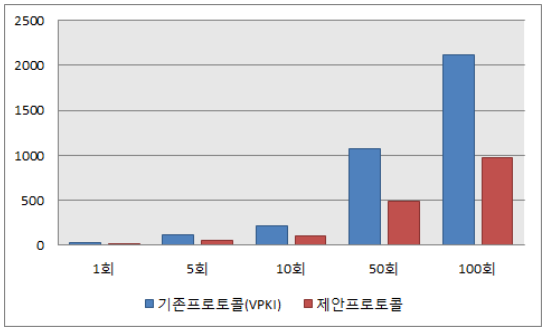
Table 3은 RSU를 경유하여 다른차량에서 메시지를 전송하는 속도에 대한 수치를 나타낸 표이다.

[Table 4] Message transmission Efficient comparison

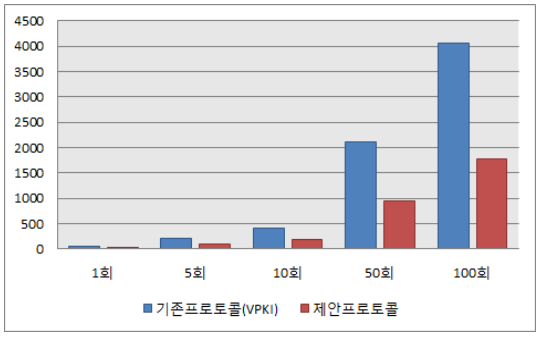
Division	PKI Based Technique (VPKI)	Proposed Protocol
1 Time	43.32	19.3
5 Times	213.4	95.8
10 Times	418.8	188.8
50 Times	2117.8	947.5
100 Times	4048.6	1782.1

VT_i 생성 및 RSU의 S/N 검증, 차량의 VID_i를 검증 단계의 시간이 증가한다. 그러나 앞서 등록 및 인증 절차에서 인증 수행 후 차대번호 및 RSU 인증 단계에서는 시간이 감소한다.

제안 프로토콜은 VPKI 방식에 비해 전체 송수신 소요시간이 대략 44% 감소하였다. PKI(Private Key 2048)보다 신원기반 암호기술(Private Key 388)을 활용함으로써 소요시간 감소 및 인증 효율성이 증가한다. Fig. 10, Fig. 11은 효율성 비교분석을 그래프로 표현하였다.



[Fig. 10] Authentication technologies based VPKI with Proposed Protocol of Authentication Efficient Comparison Graph



[Fig. 11] Authentication technologies based VPKI with Proposed Protocol of Message Transmission Efficient Comparison Graph

키 길이가 짧으므로 전수조사 공격에서는 위험하지만 공개된 차량 번호, RSU ID와 비공개된 차대번호, RSU S/N을 활용하여 통신함으로써 안전한 통신을 설계하였다.

4.3.2 안전성 분석

본 절에서는 기존 VANET 통신 암호기술과 제안 프로토콜의 안전성을 분석한다. VANET 통신의 기존 통신 프로토콜과 제안한 프로토콜의 안전성은 아래 Table 5와 같다.

• 차량 및 RSU인증에 대한 공격

- 공격자가 ID를 도용하여 다른 차량에 거짓 정보를 전송하는 위장 공격과, 다수의 ID를 가지고 네트워크 환경을 공격하는 Sybil 공격, 서비스 인프라에 대한 공격에 의해 보안 위협이 발생할 수 있다. 그러나 제안 프로토콜에서는 Authentication Server가 Vehicular 고유 정보인 차대번호(VIN)를 차대번호와 RSU의 SN을 등록함으로서 비인가된 접근이 불가능하다.

[Table 5] Comparative analyzes of safety

Division	The existing VANET Communication	PKI based Technique	Proposed Protocol
Attack on the RSU authentication and vehicles	Possible	ImPossible	ImPossible
Attack on integrity of the message	Possible	Possible	ImPossible
Attack on confidential	Possible	ImPossible	ImPossible
attack againtst on non-repudiation	Possible	ImPossible	ImPossible
Attack on availability	Possible	Possible	ImPossible

• 메시지 무결성에 대한 공격

- Vehicular, RSU에서 송신하는 메시지 정보는 VANET 환경의 무선통신기술을 사용하여 전송되기 때문에 기존 무선통신환경의 보안위협을 계승한다. 대표적으로 라우팅 메시지의 위/변조 공격, 차량 비밀 정보 위/변조 공격 등이 있다. 제안하는 프로토콜에서 차량번호, RSU의 ID, 차대번호, Serial Number를 활용하여

$E_{v-id}(VIN_i)$, $RSU_{RSU-ID}(RSU_i)$ 메시지를 전송함으로서 메시지의 무결성이 안전하다.

• 기밀성에 대한 공격

- 차량의 OBU 또는 RSU에서 무선통신을 활용하여 소프트웨어 업데이트에 의한 데이터 송수신과정에서 기밀성에 대한 위협을 받을 수 있다. 그러나 제안하는 프로토콜은 신원기반 암호기술을 활용하여 안전하게 메시지를 전송하므로 데이터 기밀성의 보호가 가능하다.

• 부인봉쇄에 대한 공격

- V2I기반에서 공격자에 의한 부인봉쇄에 관한 취약점이 있다. 그러나 제안 프로토콜에서는 차대번호(VIN_i), RSU S/N(RSU_{SN}), 해쉬값($H(N_R)$)을 검증함으로서 부인봉쇄가 가능하다.

• 가용성에 대한 공격

- 기본 V2I 기반에서는 비인가된 접근 경로를 통하여 DDoS공격에 대한 공격이 노출될 수 있다. 제안 프로토콜에서는 V2I 기반으로 프로토콜을 설계하였고, VT_i를 생성하여 검증함으로써 가용성에 대한 공격에 대한 피해를 최소화 한다.

5. 결론

본 논문에서는 VANET환경에서 차대번호를 활용하여 V2I 구간에서 차량, RSU 인증 및 등록을 제안하였다. 또한 인증 프로토콜에서 해쉬 함수와 타임스탬프를 활용하여 V2I 기반의 통신 프로토콜을 설계 및 구현하였다.

기존 VANET환경에서는 비인가된 접근, 메시지 기밀성 및 무결성, 프라이버시 위협과 다수의 ID, 익명의 ID를 통한 DDOS공격등이 있다. 제안하는 프로토콜은 신원기반 암호기술을 활용하여 차량의 기밀정보인 차대 번호와 RSU의 일련번호를 전송하여 인증서버에 등록 후 안전한 통신 프로토콜을 설계하였다. 제안한 프로토콜과 기존 프로토콜의 효율성 및 안전성을 비교하였을 때, 기존 차량통신 기술(VPKI) 보다 인증 속도가 44%감소함으로써 효율성 및 안전성이 향상되었다.

향후에는 본 논문에서 제안한 V2I 기반의 통신 프로토콜 뿐아니라, V2X기반의 효율성 있고 안전한 통신 프로토콜에 대한 연구가 필요하다.

References

[1] Young-ho Park. “Vehicle Registration Protocol for Secure Communication in VANET Environment”. KSIIS Vol 15 No. 4. 2010.

[2] Sang Woo Lee. “Vehicle Communication Security Technology Trens, vol.1556. 2012.

[3] Won-Woo Lim. “Reduced RSU-dependency Authentication Protocol to Enhance Vehicle Privacy in VANET”. Kiisc Vol21 No.6. 2011.

[4] Soo Hwan Jung. “Vehucle Network Security Issue and Technology Trends”. kmms Vo.l12 No.4. 2008.

[5] Soo Hwan Jung. “A Study on Security Framework and Protocol for VANET”. NRF. 2010.

[6] Tae Wook Hwang. “IT Convergenc based V2X Vehicle Communication Technology Trends”. Journal of Communications & Radio Spectrum , 2012.

[7] TTAS.KO-06.0025_R1. “Standard of DSRC Radio Communication between Road-side Equipment and On-board Equipment in 5.8 GHz band”. TTA. 2006.

[8] TTAK.KO-06.0193. “Vehicle-to-Vehicle Communication System Stage2: Architecture”. TTA, . 2008.

[9] TTAK.KO-12.0208. “Security Requirements for Vehicle-to-Vehicle Communication”. TTA. 2012.

[10] Marc Joye, “ID-based Secret-Key Cryptography”, 1998.

[11] N Bißmeyer. “Security Requirements of Vehicle Security Architecture”. PRESERVE project. 2011.

[12] P.Padadimitratos. “Secure Vehicular Communication Systems: Design and Archiectrue”. IEEE Communications Magazine Volume 46 Issue 11. 2008.
DOI: http://dx.doi.org/10.1109/MCOM.2008.4689252

[13] S.Y. Wang and Y.W. Li, "Evaluations of Intelligent Traffic Signal Control Algoritms under Realistic Landmark-based Traffic Patterns over the NCTUns Network Simulator," IEEE ITSC. 2012.
DOI: http://dx.doi.org/10.1109/ITSC.2012.6338620

[14] Xiaoting Sun. “Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme". ICC '07. IEEE International Conference on Communications.
DOI: http://dx.doi.org/10.1109/ICC.2007.258

이 주 관(Joo-Kwan Lee) **[정회원]**

- 2008년 2월 : 상명대학교 소프트웨어공학과 (공학사)
- 2010년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2010년 3월 : 숭실대학교 컴퓨터학과 박사과정

<관심분야>
정보보호, 인증 시스템, VANET

박 병 일(Byeong-Il Park) **[정회원]**

- 2011년 8월 : 평생교육원 컴퓨터공학과 (공학사)
- 2013년 9월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2014년 10월 ~ 현재 : K sign 주임연구원

<관심분야>
네트워크 보안, PKI전자서명인증, VANET

박 재 표(Jae-Pyo Park) **[정회원]**

- 1996년 2월 : 숭실대학교 컴퓨터학부 (공학사)
- 1998년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2008년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어 기술 연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
컴퓨터 통신, 네트워크 보안, 암호학

전 문 석(Moon-Seog Jun) **[정회원]**

- 1989년 2월 : University of Maryland Computer Science 박사
- 1989년 9월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<관심분야>
정보보호, 네트워크 보안, 인증 시스템, 암호학