ISSN 2234-4438
중소기업융합학회 논문지 제6권 제3호 pp. 57-64, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.3.057

고속도로에서 차량네트워크(VANET)의 효율적인 인증 보안 매커니즘

김갑인, 김영찬, 이종근*
창원대학교 컴퓨터공학과

An Efficiency Authentication Security Mechanism of VANET in Highway

Gab-In Kim, Yong-Cahn Kim, Jong-Kun Lee*
Dept. of Computer Engineering, Changwon National University

요 약 차량네트워크에서 정보의 전달은 열려진 통신 환경에서 배분되어지는 환경이기 때문에, 차량네트워크에서의 정보 보안 문제는 가장 중요한 문제 중 하나가 된다. 차량네트워크의 효율적인 통신체계 구축을 위해서는 각 도로통신장치와 차량단말장치에서 수집되어지는 정보의 특성과 모든 주변 환경과의 정확한 정보 소통이 요구되어진다. 본 논문에서는 고속도로 환경에서 차량 네트워크에서 도로통신장치와 차량단말장치 간의 정보 통신을 신원 기반의 기존 정보를 활용하여 차량의 인증을 위한 보안 매커니즘을 제안하며 기존의 제안된 알고리즘과 성능을 비교 분석함으로 그 효율성을 검증한다.

키워드 : 신원기반 인증, 도로통신장치, 차량단발장치, 차량네트워크, 차량 인증

Abstract Since the information transmitted in VANET is distributed in an open access environment, the security problem is one of the most critical issue in VANET. For the communicate efficiently in VANET, each RSU(Roadside Unit) or OBU(On-Board Units) need certain features that will help them to gather information, to inform their neighbors and to make decisions by considering all of the collected information. In this paper, we propose a novel authentication scheme guaranteeing secure RSUs to OBUs of VANET in highway used the ID-based authentication scheme. We show a usefulness and effectiveness of proposed authentication scheme after compared with previous works.

Key Words : ID-based authentication, OBU, RSU, VANET, vehicle authentication

1. 서론

차량네트워크(VANET: Vehicular Ad-Hoc Network)는 도로 교통량의 관리 및 안전관리를 위한 무선 통신 기반의 정보시스템 네트워크이다. 차량네트워크에서는 각 차량들이 통신 노드가 되어 주요 지역에 설치 된 도로통신장치(RSU : Road-side unit)과 차량 간 통신 그리고 차량과 차량 간의 통신을 포함한다. 특히 차량네트워크에는 차량단말장치(OBU : On-board unit)에 의하여 제공되어지는 현재 차량의 위치, 현재 시간, 스피드 등의 각종 교통 관련 정보, RSU에 의한 교통의 특이 사항과 사고 여부 및 사고 예방을 위한 제반 정보들이 유통된다. 이러한 정보의 제공 수집 및 공유는 지역의 교통 상황과 혼잡 여부 및 사고예방 조치나 혼잡한 교통량 해소와 대체 도로의 권고 등을 통하여 각 종 도로의 교통 상황을 원활하게 제어하는 역할을 차량네트워크가 담당하고 있다[1-12]. 그러나 차량네트워크에서는 고속으로 진행되고 있는 차량의 속도 관계와 무선 환경에서 발생 되어지는 제반 정보들을 소통하고 수집 가능한 네트워크의 성

Received 2016-09-02 Revised 2016-09-08 Accepted 2016-09-09 Published 2016-09-30
*Corresponding author : Jong-Kun Lee (jklee@changwon.ac.kr)

능과 이러한 환경에서 발생 가능한 각종 보안문제에 대처 할 수 있는 시스템 구축이 요구된다[1,19]. 또한 상호 정보 소통 중에 발생 가능한 사용자의 개인 정보 노출도 문제가 되고 있다. 이를 방지하기 위하여 발생될 수 있는 빈번한 차량 인증은 통신량의 증대를 유발시키어 보안의 능력을 오히려 감소케 할 수 있다. 따라서 차량 간의 통신과 차량과 관련 시스템과의 통신을 가능한 최적화하며 OBU와 RSU의 정보 통신에서 사용자에 대한 정확한 인증 검증이 주요 관건이라 하겠다. 이러한 인증 문제에 대하여 공개키·개인키를 이용한 인증 기법 등 많은 기법들이 제안되었다[1-14,20,21]. 제안된 기법들의 특징은 통신에 적용되는 각각의 키는 매우 짧은 기간을 두고 송수신되므로 통신량이 과대하게 발생 될 수 있으나 공개키와 비밀 키를 통하여 OBU에 대한 인증이 검증되어져 이력관리와 효율성 그리고 연결성의 효과가 있도록 제안되었다. 이러한 기법들은 OBU가 여러 개의 키를 소유하여 각종 보안 공격에 대처가 가능하나 운영에서 많은 투자비용을 요구하게 되고 특히, OBU의 해지 경우에도 키를 사용하여야만 해지가 가능한 한계성을 가지게 된다. 본 연구에서는 기존에 이미 등록되어진 신원정보를 활용하는 인증 매커니즘의 단순화를 통하여 발생 할 수 있는 인증 절차를 제안한다. 즉 새로운 정보가 아닌 차량정보 등의 신원기반 정보를 활용하여 많은 데이터의 통신 교환을 배제하면서 효율적으로 인증이 가능한 인증 매커니즘에 대하여 제안하고 기존의 방식들과 비교 검토하여 그 효율성을 검증한다.

본 연구의 구성은 2장에서 관련연구에 대하여 정리하고 3장에서 제안하는 모델을 통한 OBU2I, OBU2OBU와 RSU2RSU의 매커니즘을 모델링한다. 4장에서 제안한 모델의 보안성과 성능을 평가하고 5장에서 결론과 앞으로의 연구에 대하여 정리한다.

2. 관련 연구

차량네트워크에서의 인증에 관하여 그룹 키를 이용한 연구도 활발한데 Raya et al.는 다양한 공개키와 개인키 조합을 활용한 인증기법을 제안하였다[9-16]. Lu et al.은 차량네트워크를 위한 임시적 공개키를 이용한 ECPP 차량인증 프로토콜을 제안하였다[11]. 그러나 ECPP 프로토콜은 송수신 정보의 인증과 정확성 확인을 위하여 높은 사양의 시스템 구축과 경제성을 요구하는 한계점을 가지고 있다. 한편 Zhang et al. 은 해쉬 함수를(HMAC) 이용한 인증 프로토콜을 제안하였고, Chang et al.은 V2I 통신을 위하여 단순한 인증시스템을 기반으로 한 PPSA 시스템을 제안하였다[9,12]. Kim 은 인증 검증을 위하여 Petri net을 이용하여 검증하였다[15,16]. 위와 같은 기반 자료들을 통하여 차량네트워크에서의 인증 프로토콜은 경제성과 신속성을 갖는 인증 매커니즘을 요구하고 있으며 이러한 연구가 지속적으로 이루어지고 있다[9-16]. 본 연구에서는 이러한 관점에서 기존의 OBU의 신원기반 정보를 활용하여 인증을 위하여 많은 교환 통신을 최소화하면서 효율적으로 인증이 가능한 매커니즘에 대하여 제안한다.

3. 보안 매커니즘(VASM : Vehicular Authentication Security Mechanism)

3.1 제안 모델

본 연구에서는 VANET에서 발생하는 차량에 대한 인증처리에 초점을 맞추고 있다. 즉 *OBU*와 *RSU* 간에 발생 되는 정보의 교환과 수집을 통하여 차량에 대한 인증을 확실히 함으로 발생 가능한 사고 예방은 물론, 사고 후 발생 되어질 수 있는 각종 책임 문제 등에 대한 자료로 활용 될 수 있기 때문이다.

특히 *OBU*와 *OBU*간 통신에서 서로 다른 ID를 가져야하며 송수신하는 *OBU*는 위변조가 불가능 하여야 한다. *OBU*와 *RSU*간 통신 메시지는 인가되지 아니한 *OBU*나 *RSU*에 대하여 기밀성이 보장되어야 한다. 아울러 *OBU*와 *RSU*간 통신을 수행하기 위해서 각 *OBU*의 보안 인증 방법에는 정보 보안 요구 사항인 데이터 무결성, 사생활 보호, 기밀성, 부인 봉쇄, 가용성 등이 함께 보장 되어야 한다. 일반적인 차량네트워크에서의 그룹 관리에 대하여서는 인증센터 (CA: Certificate Authority)가 있어서 *RSU*와 각종 *OBU*에 대한 인증을 주도적으로 관리하도록 구성되었다[3,6,14]. 이러한 문제는 *OBU*2*OBU*, *OBU*2*RSU*, *RSU*2*RSU*간의 많은 통신량의 증가를 요구하며 또한 *OBU*의 운행 속도가 빠름에 따른 교신과 수집에 대한 통신 네트워크의 질적인 향상 문제를 야기하고 있다. 따라서 본 연구에서는 고속도로에서의 VANET 상황으로 한정하고 고속도로 진입 요금소(첫

번째 *RSU*)가 CA의 기능을 함께 이수하여 진입 *OBU*에 대하여 등록 검증하고 검증된 자료들을 통하여 *RSU*에서 *OBU*의 그룹관리를 한다면 빈번하게 발생 가능한 통신량을 효율적으로 제어가 가능하며 또한 정확한 인증을 통한 정보의 활용은 교통제어와 각종 교통사고 등 도로상황 관리에 적절하게 사용 될 것으로 기대된다(Fig. 1)[15,16].

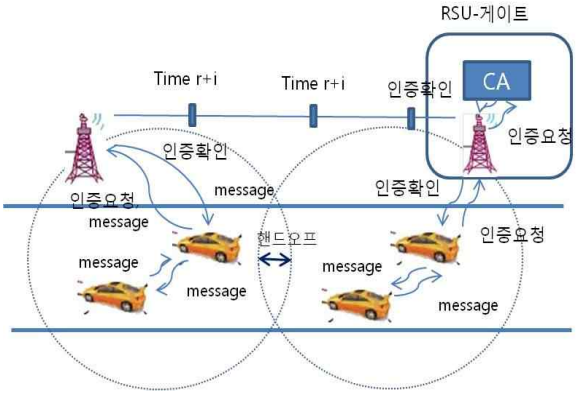


Fig. 1. The Illustration of proposed VANET architecture

본 연구에는 3단계의 제안으로 구성하는데 중 *RSU*2*OBU* 인증 문제, *OBU*2*OBU* 인증 문제 그리고 *RSU*2*RSU* 의 3가지 매커니즘을 제안한다. 본 연구의 모델링 환경은 신규로 필요한 RSU들을 신설하는 것 보다 기 도로에 설치되어있는 무인 속도 감지기나 정보 수집기 등에 *RSU*의 기능을 첨가함으로 새로운 장비의 설치 없이 *RSU*를 통한 *OBU*2*I* 통신을 가능하게 하고자 한다. 한편, 본 연구에서 제안하는 차량 인증 보안 매커니즘에는 *OBU*2*I* 통신에서 RSU가 자신의 그룹 내에 들어오는 *OBU*의 등록인증과정과 인증 받은 *OBU*의 *RSU* 그룹 내에서 주기적인 인증 과정을 함께 포함하고 있다. *OBU*의 주기적인 재 인증 처리가 필요한 이유는 처음 인증 받은 *OBU*의 상태가 제반 보안공격에 의하여 필요한 정보들이 노출 될 수도 있으므로, 일정한 시간 주기별로 계속적인 인증을 통하여 이러한 보안위협에 대비하고자 한 것이다. 본 논문에서 사용되어지는 기본적인 용어는 Table 1에 정리하였다[16].

Table 1. Notations

Parameter	Notations
E	Encryption
D	Decryption
k-pru	security key
k-pub	Public key
VIDi	Id of OBUi
HC	Hipass card number
t	TimeStamp
r	random number of OBU
i	Periodic time
Bf	Bloom filter
H	hash function

3.2 *OBU*2*I* 알고리즘

*OBU*가 요금소를 통과하면서 *OBU*는 *RSU*에게 하이패스 카드(통행카드 번호)를 *RSU*에게 보내어 등록을 검증하고 RSU 고유번호를 통하여 승인 완료 메시지를 *OBU*에 송신함으로 초기등록을 마감한다. *RSU*의 관리 그룹 영역으로 *OBU*가 접근하면 해당 *RSU*에게 *OBU*는 자신의 *UnitNumber*(*VID*, *HC*)를 전송하고, RSU는 *OBU*에게서 받은 *UnitNumber*를 처음 *RSU*에 포함 된 CA에서 해당 *OBU*를 확인 검증하고 정확한 VID와 HC일 경우 진입시간 TimeStamp t 와 일정 시간 간격을 표시하는 난수 r을 생성시켜 *RSU*의 비밀 키로 *OBU*의 VID와 HC와 함께 암호화하여 *OBU*에게 전달한다. 또한 지속적인 인증을 위하여 일정 시간 i 마다 *OBU*에 대한 인증을 계속적으로 검증하여 최초 인증을 유지하도록 한다. *RSU*2*I* 인증 프로세스는 다음과 같다(Fig. 2, 3):

3.2.1 초기 인증 : 등록인증

(1) 키 교환프로토콜을 이용하여 *OBU*와 *RSU*는 대칭키를 공유한다.

(2) *OBU*은 *RSU*에 해당 *OBU*번호 VID_i와 하이패스카드 번호(혹은 고속도로통행카드번호) HC_i를 송신하여 등록을 요청한다.

(3) *RSU*는 수신 받은 *OBU*번호 VID_i와 하이패스 카드 번호 HC_i를 검증한다.

(4) 등록 요청 *OBU*은 다음과 같이 *OBU*번호 VIN_i를 생성한다.

$$VIN_i = VID_i \| H(r) \| TimeStamp \qquad (1)$$

OBU번호 VIN_i와 난수 R을 해쉬 함수로 얻은 값 $H(r)$, $TimeStamp$ t를 연접하여 생성한 VIN_i를 신원기반 암호기법으로 얻은 Ev-id (VIN_i)를 RSU에 송신한다.

(5) RSU도 RSU_i를 생성한다. 생성 값은 다음과 같다.

$$RSU_i = RSU_{SN} \parallel RSU_{LOCATION} \quad (2)$$

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

(6) RSU는 생성한 $RSU_{RSU-ID}(RSU_i)$와 $E_{v-id}(VIN_i)$값을 복호화하고 VT_i값을 계산하여 등록한다.

$$VT_i = VIN_v \parallel \text{Exp}iration\ Data \quad (3)$$

OBU번호 VIN_i와 검증간격기간 r을 생성 후 등록한다. RSU는 OBU에게 등록 메시지를 송신한다.

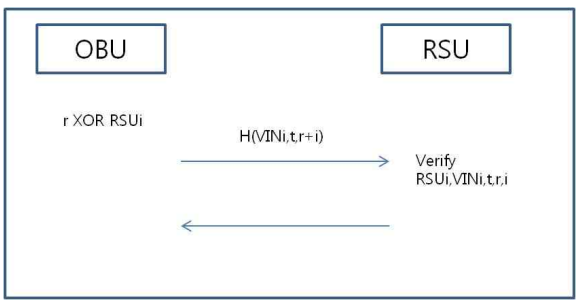


Fig. 2. The first authentication process

3.2.2 주기적 인증

(1) 일정한 시간 후 OBU는 다시 자신의 $UnitNumber$와 초기 시작 $TimeStamp$ t와 각 RSU 에서 임의 시간 간격 i 와 확률변수 r에 의한 $r+i$를 OBU의 비밀 키로 암호화 시킨 후 RSU에게 보낸다.

(2) RSU는 OBU의 VIN을 확인하고 OBU의 해당 비밀 키를 활용해 t와 $r+i$ 및 VID를 복호화 하여 OBU의 $TimeStamp$ t와 $r+i$의 값을 검증하여 올바른 값이 확인되면 OBU는 외부 공격으로부터 안전하게 운행되고 있음을 알 수 있다.

(3) OBU가 RSU의 그룹을 벗어 나갈 때까지 위의 스텝 2과정을 반복한다.

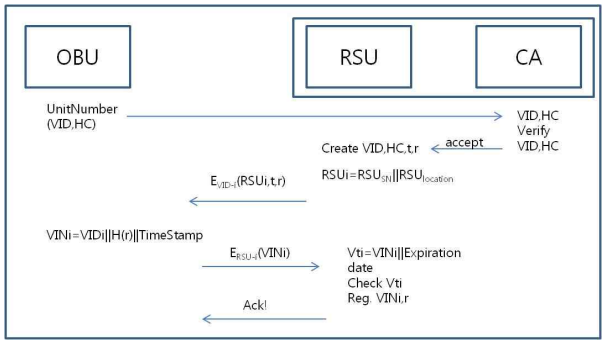


Fig. 3. The periodic authentication process.

3.3 OBU2OBU 알고리즘

RSU는 OBU_A 에서 수신 받은 메시지를 RSU에 전송하고 OBU번호를 검증한다. 이후 OBU_A는 수신 받은 메시지를 전송하기 위하여 OBU_B의 OBU 번호를 RSU_i에 송신하고 검증 완료 후 OBU_A에게 송신한다. 인증 프로세스는 다음과 같다(Fig. 4):

1) OBU_A는 RSU_i에게 자료 전송을 요청

2) RSU_i는 OBU_A에게 OBU-ID를 요청하고 OBU_A는 OBU-ID VIN_A, $Message_A$를 암호화하여 RSU_i에게 송신한다.

$$Ev\text{-}ID(Message_A \parallel VIN_A),\ VIN_A \quad (4)$$

OBU-ID VID_A을 활용하여 OBU_A가 수집한 정보와 OBU-ID를 연접한 후 암호화하여 Ev-ID를 송신한다.

3) RSU_i는 수신한 Ev-ID을 확인하고 다음의 식을 생성하여 검증한다.

$$E_{RSU-ID}(Ev\text{-}ID(Message_A \| VIN_A),\ TimpStamp),\ RSU_{LOCATION} \quad (5)$$

RSU는 EV-ID를 RSU-ID로 신원기반 암호기술로 암호화를 하고 $RSU_{Location}$을 추가하여 검증한다.

4) RSU의 검증 부문은 수신 받은 $D_{RSU-ID}(D_{V-ID}(Message_A||VIN_A), TimeStamp), RSU_{Location}$ 값을 복호화하여 OBU-ID VID_A을 검증하고 인증 완료 시킨다.
5) RSU_i는 OBU_B에게 OBU-ID VIN값을 요청한다.
6) OBU_B는 VIN값을 RSU_i에 전송한다.

$$E_{V-ID}(VIN_B),\ VID_B \tag{6}$$

OBU_B의 OBU-ID VIN_B를 신원기반 암호방식으로 암호화하여 OBU-ID VID_B를 RUS_i에 전송한다.
7) RUS_i는 OBU_A와 같이 송신 받은 OBU-ID VIN_B를 확인하고 아래의 식을 생성하고 검증한다.

$$E_{RSU-ID}(E_{V-ID}(Message_B \parallel VIN_B), TimeStamp),\ RSU_{Location} \tag{7}$$

수신 받은 값과 $TimeStamp$ 값을 RSU_{ID}로 신원기반 암호기술을 이용하여 암호화하고 $RSU_{Location}$인 RSU의 위치 ID를 추가하여 검증한다.
8) 검증부문은 VID_B를 확인하고 값을 복호화하여 OBU-ID VID_B를 검증하고 등록 된 VT_A, VT_B 값을 검증한다. 해쉬 함수를 이용하여 V-$Message$를 계산하여 생성한다.

$$V\text{-}Message = (Message_A||TimeStamp_A||H(A_r) \oplus H(B_r)) \tag{8}$$

OBU_A에게로부터 송신 받은 $Message_A$ 와 $TimeStamp$와 OBU를 인증 할 때 생성된 $H(A_r)$, $H(B_r)$을 논리 합한 값을 연접하여 RSU의 ID를 이용하여 신원기반 암호기술을 활용한 값 $R_{RSU-SV}(V\text{-}Message)$을 생성한다.
9) $D_{RSU-SV}(V\text{-}Message)$을 복호화하여 OBU_B에게 메시지를 송신한다.

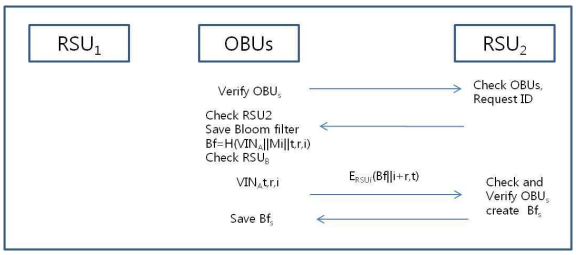


Fig. 4. OBU2OBU authentication process

3.4 $RSU2RSU$ 알고리즘

RSU에서 새로운 다른 RSU의 관리 범주로 진입하는 OBU의 경우 새로운 RSU는 진입 OBU의 메시지를 자신의 볼륨필터[17]에 저장한 후 OBU의 키 값을 이전의 RSU의 공개키로 암호화하여 등록함으로 새로운 RSU에 가입하게 됨을 고지한다[9]. 새 RSU는 이전 RSU의 공개키로 암호화 되어진 OBU의 메시지를 받게 된다. 이 때 새 RSU는 새로운 RSU의 공개키를 새로운 OBU에게 보내어 새로운 OBU가 새 RSU공개키로 자신의 정보를 암호화하며 이후의 OBU 인증은 $OBU2I$ 알고리즘을 사용하면 된다(Fig. 5,6).

3.4.1 수신 OBU의 새 RSU로 이동

새로운 RSU ID를 수신하게 된 OBU는 기존의 RSU 도메인에서 다른 도메인의 RSU로 관리와 인증 절차가 이동하게 되며 기존에 인증되어진 RSU로부터 블룸 필터를 제공 받는 것과 동시에 기존의 RSU의 키 값이 공개키 값으로 암호화되어 제공 받게 된다[18].

$$Bf = H(VIN_r||M_i||t,r,i) \tag{9}$$

이를 전송받은 새로운 도메인의 RSU는 OBU의 키 값을 추출하기 위해 자신의 키 값을 사용하며 동시에 블룸 필터에 포함시키기 위해 블품 필터에 배타적논리합(XOR)연산을 시행한다.

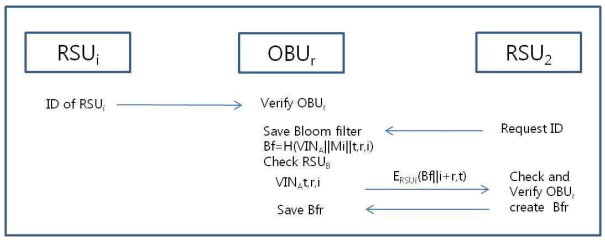


Fig. 5. RSU2RSU(received) authentication process

3.4.2 송신 *OBU*의 새 *RSU*로 이동

주기적 인증을 원하는 *OBU*의 위치가 새로운 *RSU*의 서비스 범위 안으로 이동되었을 경우 새로운 도메인의 *RSU*는 *OBU*의 키 값을 변경 전RSU의 공개키로 암호화하여 관리영역의 변경 여부를 확인하게 된다. 이를 전송받은 *RSU*는 *OBU*의 키 값을 추출하기 위해 변경되기 전 *RSU*의 도메인을 이용하여 *OBU*의 개인키를 활용하여 키 값을 추출함과 동시에 블룸필터에 배타적논리합 연산을 통하여 새로운 키 값을 블룸 필터에 저장 갱신시키게 된다.

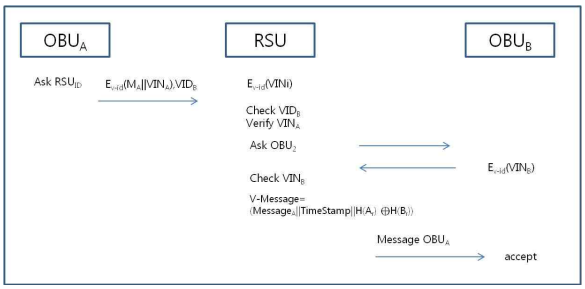


Fig. 6. RSU2RSU(send) authentication process

4. 제안 기법의 효율성 분석

4.1 효율성 분석

제안한 알고리즘의 경우 이미 등록 되어진 *OBU*의 기존 데이타 즉 *ID*와 하이패스 카드를 사용하며 또한 *CA*는 고속도로 진입 시 한번만 활용하므로 해쉬 함수의 발생 빈도를 최소화 할 수 있는 장점이 있다.

성능분석을 위한 지표로 *OBU* 등록 프로세스와 주기적 인증 프로세스 그리고 *OBU*2*OBU*, *OBU*2*I*의 인증과정에서 발생되어지는 암호화, 복호화를 위한 확률변수의 수, 해쉬 함수의 발생 건 수와 또 XOR 함수 계산의 발생 수를 기준으로 비교하였다. 등록 과정과 주기적 인증 프로세스를 기존의 PPAS와 Ashritha와 비교하면 Table 2와 같다[9,15]. PPAS는 등록과정에서 해쉬 함수를 3번 생성하였으며 주기적 검증 과정에서는 9번의 해쉬 함수와 2번의 확률 변수를 생성하과 XOR 산술은 2번 시행한다. Ashritha의 기법에서는 검증 과정에서 3번의 해쉬 함수를 만들어 내고 각 2번씩의 확률변수와 XOR산술을 시행한다. 본 연구에서 제안하는 매커니즘의 경우 2번의 해쉬 함수와 확률변수를 생성하고 1번의 XOR산술을 시행하여 XOR산술에서 유리하며 해쉬 함수의 생성에서도 2번으로 효율적임을 보인다. 기 제안 된 기법들의 환경은 *CA*를 중앙에 배치하고 모든 *RSA*와 *OBU*에 대하여 통합 관리함으로 인증에 필요한 모든 정보의 소통이 *CA*를 거쳐야하므로 해쉬 함수의 발생 빈도가 높다고 하겠다. 그러나 제안한 매커니즘의 경우 이미 등록되어진 차량의 제반정보를 하이패스 카드가 요금소를 통과하면서 확인되고 검증되어 인증을 위한 해쉬 함수의 발생 빈도를 최소화 할 수 있는 장점이 있다 하겠다.

Table 2. Computation overhead

	registration	authentication
PPAS[9]	n(3Ch)	9Ch+2Cr+2CXOR
Ashritha[15]		3Ch+2Cr+2CXOR
Prposed Mechanism		2Ch+2Cr+CXOR

Ch: cost of hash function, CXOR: Cost of executing XOR, Cr:Cost of random number, n:number of OBUs in the VANET[9]

4.2 보안 분석

본 논문에서는 *OBU*와 *RSU*간의 통신에서 *OBU*의 ID 정보를 기반으로 사전 교환 되어진 공개키와 비밀 키를 가지고 난수 값 그리고 타임스탬프등과 같은 여러 인자들을 이용하여 *OBU*와 *RSU*간의 인증을 시행함으로 연계성을 가지지 않는 새로운 인증이 필요시 마다 새롭게 인증하도록 제안 되였다.

키를 재사용하는 문제에 대하여서는 *OBU*나 *RSU*가 인증 절차에서 *TimeStamp*를 데이타와 함께 전송하게 된다. 따라서 인증 요청 데이타가 주어진 시간 간격을 만족하는 경우에만 지속적인 인증처리가 가능하게 된다.

거짓 데이타를 전송하는 위장공격이나 Sybil공격 등에 의한 보안취약점에 대하여서는 첫 번째 RSU에 포함되어있는 *CA*가 *OBU* 번호, 하이패스카드와 타임스탬프 t를 확인하고 또한 일정 시간 r+i마다 검증하므로 *OBU* 및 *RSU*인증에 의한 위협이 불가능하다.

메시지 무결성에 대한 공격에 대하여는 *OBU*가 관할 *RSU* 지역을 벗어나 새로운 *RSU*지역으로 진입 할 경우 *RSU*간의 인증을 통하여 *OBU*와의 송수신을 통하여 *RSU*와 *OBU*의 인증을 시행하므로 메시지 무결성을 유지 할 수 있다. 특히 일정 시간마다 주기적인 인증을 시행하므로 인증의 유지를 위한 과정이 주기적으로 시행되어 정보의 유효성을 유지한다고 하겠다. 또한 제안 매커니즘에서는 이미 등록 인증처리에서 하이패스 카드에 의한 동일 *ID*를 가지고 있으며 이를 이용하여 각 *OBU*의 볼륨필터에 기억하여 이와 비교하여 인증을 하므로 또한

일정한 시간마다 인증을 시행함으로 가용성이 있다.

5. 결론

본 논문에서 제안한 OBU2I 통신에서의 OBU 인증 보안 매커니즘으로 RSU2OBU, OBU2OBU와 RSU2RSU의 3단계 인증 매커니즘을 제안하였다. 인증 처리를 위하여 해쉬 함수와 확률변수를 사용하였다. 제안 매커니즘의 효율성에 대하여 기존의 연구들과 비교 분석하여 확률변수의 생성과 해쉬 함수의 빈도 발생을 각각 2회로 효율화 하였고 XOR 산술의 경우도 1회로 기존의 제안 기법들 보다 단순화 할 수 있어 경제적이라고 이야기 있다. 제안 매커니즘의 보안 분석에 있어서는 키 재사용문제, 가용성과 비밀성 또한 위장공격 등에 대하여서도 등록인증과 주기적 인증을 통하여 보안을 안정화 할 수 있는 특성을 갖는다고 하겠다.

앞으로의 관심 연구는 제안 매커니즘에 대한 모델링 분석과 성능분석을 더욱 다양한 함수를 이용하여 수치화 하여 검증 할 필요가 있으며 보안 분석에 대하여는 필요한 항목별로 비교 분석이 요구된다.

ACKNOWLEDGEMENTS

본 논문은 “2015-2016년도 창원대학교 자율연구과제 연구비” 지원을 받아 수행된 것임.

REFERENCES

[1] C. Zhang, X. Lin, R. Lu, P. H. Ho and X. Shen, “An Efficient Message Authentication Scheme for Vehicular Communications,” *IEEE Transactions on Vehicular Technology*, Vol 57, No. 6, pp. 3357-3368, Nov. 2008.

[2] S. Biswas, R. Tatchikou and F. Dion, “Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,” *IEEE Communication Magazine*, Vol. 44, Issue 1, pp. 74-82, Jan. 2006.

[3] X. Sun, X. Lin and P. H. Ho, “Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme,” *Proceedings of the 2007 IEEE International Conference on Communications*, pp. 1539-1545, 2007.

[4] C. T. Li, M. S. Hwang and Y. P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,” *Computer communications*, Vol. 31, Issue 12, pp. 2803-281, Jul. 2008.

[5] M. H. Eiza and Q. Ni, “A Reachability-Based Routing Scheme for Vehicular Ad Hoc Networks”, *Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 1578-1584, 2012.

[6] S. Biswas, J. Misic and V. Misic, “ID-based safety Message Authentication for Security and Trust in Vehicular Networks,” *Proceedings of the 2011 31st International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 323-331, 2011.

[7] S. Biswas and J. Misic, “Proxy Signature-based RSU Message Broadcasting in VANET,” *Proceedings of the 2010 25th Biennial Symposium on Communications (QBSC)*, pp. 5-9, 2010.

[8] A. Hesham, A. A. Hanid and M. A. El-Nasr, “A Dynamic Key Distribution Protocol for PKI-based VANETs,” *Proceedings of the 2011 IFIP Ahmed Hesham; Ayman Abdel-Hamid; Mohamad Abou El-Nasr Wireless Days (WD)*, pp. 1-3, 2011.

[9] M. C. Chuang and J. F Lee, “PPAS: A Privacy Preservation Authentication Scheme for Vehicle-to-Infrastructure Communication Networks,” *Proceedings of the 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1509-1512, 2011.

[10] M. Raya and J. P. Hubaux, “Securing Vehicular Ad Hoc Networks,” *Journal of Computer Security-Special Issue on Security of Ad-hoc and Sensor Networks*, Vol. 15, No. 1, pp. 39-68, Jan. 2007.

[11] R. Lu, X. Lin, H. Zhu, P. H. Ho and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,” *Proceedings of the 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies INFOCOM 2008*, pp. 1229-1237, 2008.

[12] C. Zhang, X. Lin, R. Lu and P. H. Hp, “RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehiclular Communiction Networks,” *Proceedings of the IEEE International Conference on Communications*

2008(ICC '08), pp. 1451-1457, 2008.

[13] M. Ashritha and CS. Sridhar, "RSU Based Efficient Vehicle Authentication Mechanism for VANETs," *Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1-5, 2015.

[14] A. Shamir, "Identity Based cryptosystems and signature schemes," *Advances in Cryptology*, Vol. 196, pp. 47-53, Nov. 2000.

[15] Y. Chan Kim and J. Kun Lee, "A Secure Analysis of Vehicular Authentication Security Scheme of RSUs in VANET," *Journal of Computer Virology and Hacking Techniques*, Vol. 12, No. 3, pp. 145-150, Aug. 2016.

[16] Y. Chan Kim, Y. Jin Song, J. Kun Lee, "Vechicular Authentication Security Mechanism Modeling using Pwtei Net," *Indian Journal of Science and Technique*, Vol. 8, No. S7, pp. 443-337, Apr. 2015.

[17] B. Bloom, "Space/Time Trade-offs in Hash Coding with Allowable Errors," *Communications of ACM*, Vol. 13, No. 7, pp. 422-426, Jul, 1970.

[18] S. J. Jung, Y. J. Yoo, J. H. Paik and D. Hoon Lee, "Secure and Efficient V2V message Authentication Scheme in Dense Vehicular Communication Networks," *Journal of Korea Institute of Information Security and Cryptology*, Vol. 20, No. 4, pp. 41-52, Aug. 2010.

[19] Y. S. Jeong and S. H. Lee, "A User Privacy Protection Scheme based on Password through User Information Virtuality in Cloud Computing", *Journal of Convergence Society for SMB*, Vol. 1, No. 1, pp. 29-37, Nov. 2011.

[20] S. G. Yeo and K. H. Lee, "Smart Phone and Vehicle Authentication Scheme with M2M Device," *Journal of the Korea Convergence Society*, Vol. 2, No. 4, pp. 1-7, Dec. 2011.

[21] S. H. Kim and K. Ho Lee, "User Authentication Risk and Countermeasure in Intelligent Vehicles," *Journal of the Korea Convergence Society*, Vol. 3, No. 1, pp. 7-11, Mar. 2012.

저 자 소 개

김 갑 인(Gab-In Kime) [정회원]

- 1988년 3월 : 창원대학교 전자계산학과 학사
- 2005년 2월 : 창원대학교 산업대학원 컴퓨터공학과 수료
- 2012년 3월 ~ 현재 : (주)맥스 연구개발부 재직 중

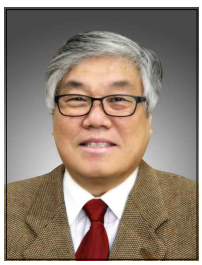
<관심분야> : 기업정보시스템, 차량용 네트워크

김 영 찬(Young-Chan Kim) [정회원]

- 1998년 2월 : 대구대학교 제어계측공학과 학사
- 2011년 2월 : 창원대학교 산업대학원 컴퓨터공과 석사
- 2016년 2월 : 창원대학교 대학원 컴퓨터공학과 박사
- 2016년 9월 ~ 현재 : ㈜사람과기술 대표이사

<관심분야> : 스케쥴링 성능분석, 패트리 넷 모델링, 정보보안

이 종 근(Jong-Kun Lee) [정회원]



- 1974년 2월 : 숭실대학교 전자계산학과 학사
- 1978년 8월 : 고려대학교 경영대학원 경영학과 석사
- 1986년 8월 : 숭실대학교 대학원 컴퓨터공학과 석사
- 2002년 3월 : 에꼴 쌍뜨랄 빠리 컴퓨터공학 박사
- 1983년 9월 ~ 현재 : 창원대학교 컴퓨터공학과 교수

<관심분야> : 스케쥴링 성능분석, 패트리 넷 모델링, 정보보안