情報保護學會論文誌
第20卷 第4號, 2010. 8

차량 밀집환경에서 안전하고 효율적인 V2V 메시지 인증기법*

정 석 재,† 유 영 준, 백 정 하, 이 동 훈‡
고려대학교 정보경영공학전문대학원

Secure and Efficient V2V Message Authentication Scheme in Dense Vehicular Communication Networks*

Seock Jae Jung,† Young Jun Yoo, Jung Ha Paik, Dong Hoon Lee‡
Graduate School for Information Management and Security, Korea University

요 약

지능형 차량 네트워크(VANET)환경에서 메시지 인증은 필수적인 보안요소이다. 메시지 인증이 안전하게 이루어지기 위해서는 무결성, 가용성 및 프라이버시 보호기능을 갖추어야 하고, 다양한 환경에서의 효율성을 갖추는 것도 매우 중요하다. RAISE 스킴은 일반적으로 효율성을 보장하기 어려운 차량이 많이 밀집된 환경에서 효율적으로 메시지 인증을 하기 위해서 제안되었다[1]. 하지만 RAISE에서도 통신하는 차량이 많아질수록 전송되는 메시지의 크기가 차량 수에 비례하여 커지게 되어 오버헤드가 발생하므로 이를 줄일 필요성이 존재하고, 특정 공격에 취약한 약점도 가지고 있다. 따라서 본 논문에서는 차량 밀집환경에서 RSU(Road Side Unit)가 Bloom Filter를 통해 주변 차량들의 메시지를 적은 통신량으로 한번에 처리하고 전송할 수 있도록 하는 방법과 재생공격을 막는 타임스탬프의 사용을 통해 기존의 기법보다 더욱 안전하고 효율적인 스킴을 제안한다. 또한, 제안하는 스킴에 핸드오버 기능을 지원하여 차량이 다른 지역으로 이동하는 경우 불필요한 키교환을 하지 않도록 인증과정을 간소화시킨다. 그리고 오류가 일어날 확률을 시뮬레이션 하고 통신량 계산 등의 분석을 통해 안전성과 효율성을 검증한다.

ABSTRACT

Message authentication is an essential security element in vehicular ad-hoc network(VANET). For a secure message authentication, integrity, availability, privacy preserving skill, and also efficiency in various environment should be provided. RAISE scheme has been proposed to provide efficient message authentication in the environment crowded with lots of vehicles and generally considered to be hard to provide efficiency[1]. However, as the number of vehicles communicating in the area increases, the overhead is also incurred in proportion to the number of vehicles so that it still needs to be reduced, and the scheme is vulnerable to some attacks. In this paper, to make up for the vulnerabilities in dense vehicular communication network, we propose a more secure and efficient scheme using a process that RSU(Road Side Unit) transmits the messages of neighbor vehicles at once with Bloom Filter, and timestamp to protect against replay attack. Moreover, by adding a handover function to the scheme, we simplify the authentication process as omitting the unnecessary key-exchange process when a vehicle moves to other area. And we confirm the safety and efficiency of the scheme by simulating the false positive probability and calculating the traffic.

Keywords: VANET, V2V, Authentication, Bloom Filter, k-anonymity

* 접수일(2010년 3월 23일), 수정일(2010년 6월 28일), 게재확정일(2010년 7월 2일)
* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(정보통신)의 일환으로 수행하였음. [KI002113, Car-헬스케어 보안 기술개발]
† 주저자, sjjung10341@hanmail.net
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

최근 인터넷과 무선통신기술의 급속한 발달로 인해 지능형 차량네트워크(VANET, Vehicular Ad Hoc Network)는 산업과 학계 모두에서 점점 큰 주목을 받고 있다. VANET은 MANET(Mobile Ad Hoc Network)의 한 종류로 차량과 차량 간의 통신(V2V, Vehicle to Vehicle), 차량과 인프라스트럭처간의 통신(V2I, Vehicle to Infrastructure)을 통하여 지역정보를 수집, 전송하여 도로상의 안전 및 운행의 효율성 등 다양한 기능을 제공한다.

VANET은 주로 도로상에 위치한 RSU(Road Side Unit)와 차량에 탑재 된 OBU(On Board Unit)의 통신으로 이루어지며 각각의 차량은 자신의 속도, 위치, 가속정보 등의 교통관련 정보를 전송하여 사고나 기타 긴급상황에 따른 안전한 차량 운전을 제공하거나 교통정체 등의 상황에 대한 사전 반응을 할 수 있도록 한다. 뿐만 아니라 각 차량에서의 주변지역 정보의 획득이나 콘텐츠의 자유로운 업/다운로드 등의 다양한 기능도 제공한다. 이러한 VANET의 다양한 장점들을 활용하기 위해서는 메시지 및 사용자 인증, 프라이버시 등 보안관련 문제가 가장 중요한 사항중 하나이며, 이와 관련된 많은 연구가 전 세계적으로 진행되어왔다. 미국에서는 IEEE 802.11p/P1609(WAVE)에서 차량 통신용 키 관리를 위한 익명성 지원 비대칭 암호 기술을 연구하고 있고[2], 유럽에서도 NoW, SEVECOM등의 프로젝트를 통해서 차량 통신 보안에 대해서 연구 개발을 추진하고 있다[3][4]. 그 결과 VANET환경에서의 인증 및 프라이버시 보호를 위해서 최근에 많은 연구들이 이루어졌다. Lin 등은 그룹서명을 통해 프라이버시를 보호하는 방법을 제안하였고[5], Raya 등은 [6]에서 긴 길이의 익명키쌍을 사용하는 방법을 제안하였다. 또 Zhang 등은 [7]에서 ID기반의 일괄검증기법을 통해 프라이버시를 보호하는 방법을 제안하였다.

하지만 위의 연구들은 차량들이 밀집된 지역에서의 효율성을 보장하지 못한다. 각 차량은 모든 메시지에 서명과 인증서를 부착하여 보내게 되는데 이로 인해 패킷 길이가 너무 커지게 되고, 따라서 차량들이 많이 밀집한 대도시 지역에서는 큰 오버헤드가 발생할 수 있다. 한 노드의 전송범위가 400m내외정도인 것을 감안하여 최대 300개의 노드와도 통신을 할 수 있는 상황을 생각하면 통신량 및 계산량을 줄이는 일은 매우 중요한 일이다[8]. Zhang등은 RSU의 역할을 통해 이를 간소화 시켜주고, HMAC 및 k-anonymity를 사용해 이러한 환경에서 효율적으로 메시지 인증을 할 수 있는 RAISE를 제안하였다[1].

하지만 RAISE도 마찬가지로 차량들이 보내는 메시지가 많아지면 통신량이 늘어나고 재생공격에 취약한 점 등의 단점이 있다. 특히 RAISE에 사용되는 인증 메시지는 차량의 수에 비례하여 그 크기가 증가하기 때문에 차량 밀집 지역을 위한 기법이지만 효율이 매우 떨어진다고 할 수 있다. 본 논문에서는 이 RAISE의 단점을 보완하기 위하여 Bloom Filter를 사용하여 통신량을 줄이고, 타임스탬프를 사용하여 재생공격에 안전하도록 설계한 메시지 인증 기법을 제안한다. 특히, 제안하는 기법은 차량의 밀도와 각 차량이 전송하는 메시지의 수와 관계없이 일정한 크기의 인증 메시지를 생성하여 매우 효율적인 인증 환경을 구성 할 수 있다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 RAISE와 Bloom Filter, k-anonymity등의 기본 개념에 대해서 기술하고, 3장에서는 본 논문의 시스템 모델 및 보안 요구사항과 제안하는 기법에 대하여 설명한다. 4장에서는 제안하는 기법을 안전성과 효율성 측면에서 분석하고, 마지막으로 5장에서는 본 논문의 결론을 내린다.

II. 관련 연구

2.1 RAISE

RAISE는 기존의 PKI기반의 메시지 인증기법을 사용했을 때 출퇴근시간의 대도시 등과 같은 차량이 밀집된 상황에서 발생하는 오버헤드 문제를 해결하기 위하여 개발되었다. RSU는 차량들이 보낸 메시지를 통합하여 수신차량에게 보내고 수신차량은 자신이 받은 메시지가 RSU가 보낸 정보에 들어있는지 확인 작업만을 수행함으로써 기존의 방법보다 효율적인 메시지 인증을 가능하게 한다.

2.1.1 RAISE 기법

RAISE는 차량들 간의 메시지 인증을 위해 아래와 같은 절차를 진행한다.

1) 대칭키 설립

Diffie-Hellman 키 교환 프로토콜을 통해 차량과 RSU 사이에 키를 공유한다[9].

2) 해쉬통합 (Hash Aggregation)

i번째 메시지 송신차량은 공유한 키로 메시지에 대한 HMAC값을 계산하여 송신할 메시지에 대하여 다음과 같은 값을 RSU와 주변의 차량에게 전송한다.

$$ID_i \| M_i \| HMAC_{K_i}(ID_i \| M_i)$$

RSU는 정해진 임계치 시간마다 주기적으로 여러 차량에게서 받은 HMAC값을 다음과 같은 방법으로 통합하여 다시 주변의 차량에게 전송한다.

먼저 받은 ID값이 ID-Key 테이블에 있는지 확인한다. 그리고 공유한 키를 이용해 HMAC값이 정당한 값인지 확인한다. ID나 HMAC이 정당하지 않으면 해당 메시지는 버린다. RSU는 임계치 시간 안에 수신한 모든 ID, M쌍을 각각 해쉬하여 통합하고, 이것을 자신의 개인키로 서명하여 주변의 차량들에게 다음과 같이 전송한다. 여기에서 $HAggt = H(ID_1 \| M_1) \| \cdots \| H(ID_n \| M_n)$ 이다.

$$HAggt \| (HAggt)_{K_{RSU}}$$

3) 검증

메시지 수신차량은 메시지 송신차량에게서 받은 $ID_i \| M_i \| HMAC_{K_i}(ID_i \| M_i)$값과 RSU에게서 받은 $HAggt \| (HAggt)_{K_{RSU}}$값 중에서 먼저 $HAggt$의 서명값을 RSU의 공개키로 검증하고, 수신한 메시지 M_i의 해쉬값이 RSU에게서 받은 $HAggt$에 있는지를 확인하여 메시지를 검증한다.

4) k-anonymity

k개의 차량은 똑같은 PID(Pseudo-ID)를 사용한다. 따라서 공격자는 k개의 차량 중에서 특정 차량을 구분할 수 없지만 RSU는 각 차량과 키를 공유하고 있기 때문에 가지고 있는 키로 차례로 계산해 봄으로써 적합한 키를 사용했는지 확인할 수 있고, 따라서 송신자를 인증할 수 있다.

2.1.2 RAISE 기법의 문제점

RAISE는 각 차량 메시지의 HMAC값을 사용해 오버헤드를 줄이고 k-anonymity를 통해 익명성을 제공하지만, 동시에 다음과 같은 문제점을 가지고 있다.

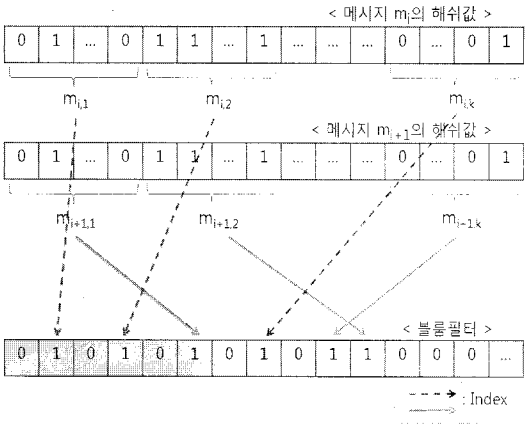
- RAISE는 차량이 집중된 곳에서 사용되는 기법이고, 송신되는 메시지의 개수는 차량의 수에 비례하여 많아지기 때문에 전송되는 메시지의 밀도가 높아지게 되며, 결론적으로 RSU가 각각의 차량에게 보내는 $HAggt$값이 매우 커지게 되어 비효율적이다.
- 공격자가 이 전에 사용되었던 값을 다시 사용했을 때 발생하는 재생공격에 취약하다. 공격자가 RSU의 $HAggt$과 다른 차량의 메시지 $ID_i \| M_i \| HMAC(ID_i \| M_i)$을 가로채 일정시간이 지난 후 다시 보내게 되면 수신차량은 유효한 메시지로 간주하고 해당 행동을 다시 취할 수 있다.

2.2 Bloom Filter

Bloom Filter[10]는 어떤 원소가 어떤 집합에 속해있는지를 확인하는데 쓰이는 확률적인 자료구조이다. 많은 양의 데이터를 입력하여도 자료구조의 크기가 늘어나지 않게 유지할 수 있으며, 데이터의 포함여부를 매우 빠르게 확인할 수 있다. 하지만, False positive가 존재하여 어떤 값이 실제로는 집합에 속해있지 않지만 자료에 속해 있다고 잘못 판단하는 경우도 발생한다.

Bloom Filter는 *Insert*와 *Check*, 두 가지 함수로 구성된다. 먼저 *Insert*는 원소를 Bloom Filter에 삽입하는 함수이다. 입력값으로 Bloom Filter와 n개의 메시지를 받아 각 메시지에 대한 k개의 해쉬값을 계산하고, 각 해쉬값의 위치에 있는 Bloom Filter의 값을 1로 바꾸어 출력한다. 이렇게 n개의 메시지에 입력된 Bloom Filter 가 존재하면, 어떤 원소가 Bloom Filter에 들어있는지를 검증하기 위한 *Check*함수를 사용할 수 있다. *Check*는 입력값으로 Bloom Filter와 하나의 메시지를 받아 해당 메시지에 대한 k개의 해쉬값을 계산하고, 그 위치에 있는 Bloom Filter 중 하나라도 0이 있는 것이 있으면 False를, 그렇지 않으면 True를 출력한다.

또한 Bloom Filter는 Union(∪)과 Intersection(∩)속성을 지원하는 특성을 가지고 있다. Union은 Bloom Filter의 합집합을 말하는 것으로써 만약 두 개 이상의 Bloom Filter의 크기가 같다면 Bitwise-OR 연산을 통하여 양쪽의 Bloom Filter에 속한 원소들의 값 모두를 하나의 Bloom Filter로 표현할 수 있다. 그리고 Intersection은 Bloom Filter의 교집합을 말하는 것으로써 두 개 이상의 Bloom Filter의 크기가 같다면 Bitwise-AND 연산



〔그림 1〕 제안하는 기법의 Bloom Filter

을 통하여 양쪽의 Bloom Filter 모두에 들어있는 값들만을 하나의 Bloom Filter로 추출해낼 수 있다.

일반적으로 Bloom Filter는 서로 다른 여러 개의 해쉬함수를 사용하지만, 본 논문에서 제안하는 Bloom Filter는 한 개의 SHA-1 함수를 k개의 조각으로 분할하여 사용한다. 이는 *Insert*와 과정에 사용되는 해쉬함수의 수를 줄여 효율성을 높이기 위한 것으로 160bits 출력을 가지는 SHA-1을 적절히 나누면 충분한 신뢰성을 가지는 Bloom Filter를 구성할 수 있고, 이에 대한 분석은 4장에서 다루기로 한다.

2.3 k-anonymity

k-anonymity는 하나의 신뢰된 기관과 k개의 노드가 통신할 때 각 노드는 똑같은 ID를 사용하여 서로간의 익명성을 보장하면서 신뢰된 기관은 각각의 노드를 구분할 수 있는 기법이다.

최초 신뢰된 기관과 k개의 노드는 키교환을 한다. 그리고 k개의 각 노드는 k-1개의 다른 노드와 똑같은 PID를 자신의 ID로 사용한다. 따라서 공격자는 k개의 노드 중에서 특정 노드를 구분할 수 없어 각 노드의 프라이버시가 보장된다. 하지만 신뢰기관은 각 노드와 키를 공유하고 있기 때문에 추 후 각 노드가 보낸 메시지를 자신이 가지고 있는 키로 차례로 복호화 해봄으로써 해당 메시지를 적합한 키로 암호화했는지 확인할 수 있고, 키에 대한 정보로 인해 송신자를 인증할 수 있다〔11〕.

III. 제안하는 기법

3.1 시스템 모델 및 가정

VANET의 기반구조(Infrastructure)는 크게 두 개의 계층으로 이루어져 있다. 상위계층은 AS(Application Server)와 RSU(Road Side Units)와의 통신을 말하고, 하위계층은 RSU와 각 차량 간의 통신을 말한다. AS는 안전한 채널을 통해 RSU와 연결될 수 있고, RSU는 AS가 하위계층에 정보를 전달할 수 있는 통로역할을 한다. 이 논문에서 제안하는 기법은 RSU는 항상 신뢰받는다는 가정을 두고 있다. 많은 V2V 또는 V2I 인증 기법에서 RSU는 항상 안전한 환경이라고 가정한다〔1〕〔12〕〔13〕. 따라서, RSU와 AS와의 통신구간은 안전하고 공격자는 RSU를 위장하거나 획득(compromise)하기 힘들다.

3.2 보안 요구사항

공격자는 도청, 메시지 변조/삭제 등의 악의적인 공격 및 차량의 위치나 신분의 노출 등 프라이버시 침해에 관한 위협을 할 수 있다. 이러한 공격에 안전하기 위해 다음과 같은 요구사항들을 만족해야 한다〔14〕〔15〕.

- 인증(Authentication)

메시지의 송신자가 정당한지를 확인할 수 있는 인증기능을 갖추어야 한다. 공격자는 정당한 메시지를 위조하거나 기존의 메시지를 사용하여 정당한 메시지를 생성하거나 그대로 재사용(Replay Attack) 할 수 없어야 한다.

- 메시지 무결성(Message Integrity)

송신자가 보낸 메시지가 전송 중에 부당하게 변조되지 않았음을 보장해야 한다.

- 가용성(Availability)

사용자가 데이터를 필요로 할 때 항상 원하는 객체 또는 자원을 접근하고 사용할 수 있는 것을 보장해야 한다. 이를 위해서는 통신상의 오버헤드를 줄이고 빠른 계산이 보장되어야 한다.

- 익명성 및 비연결성
  (Anonymity and Unlinkability)

사용자의 신분을 노출하지 않게 하기 위해서 ID를 숨기는 익명성이 제공되어야 하고 임의의 두 개의 메시지가 같은 사용자로부터 보내진 것이라는 것을 확인할 수 없도록 하는 비연결성 기능도 제공되어야 한다.

3.3 용어 정리

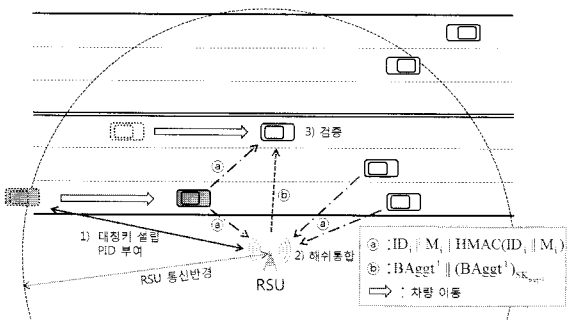
본 논문에서 사용되는 용어는 〔표1〕과 같다.

〔표 1〕 용어 정리

표 기	정 의
RSU^j	j번째 영역의 RSU
SV_i^j	j번째 영역에서 메시지를 송신하는 i번째 차량
RV_i^j	j번째 영역에서 메시지를 수신하는 i번째 차량
$K_{A,B}$	RSU A와 차량 B간에 교환한 대칭키
ΠD_i	i 번째 PID (Pseudo-ID)
$HMAC_{K_{A,B}}(C)$	C의 HMAC을 $K_{A,B}$로 계산한 값
$Cert_A$	A의 인증서
$(A)_{SK_B}$	A를 B의 개인키로 서명한 값
$bAggt$	각 메시지의 해쉬값을 삽입한 Bloom Filter 값
$BAggt$	T(타임스탬프)$\|\|bAggt$
$Enc_{K_B}(A)$	A를 B의 공개키로 암호화한 값
K_{RSU^j}	RSU^j의 공개키

3.4 제안하는 기법

제안하는 기법은 RSU와 각 차량이 대칭키를 교환한 후, 각 차량의 메시지를 RSU가 통합하여 해쉬통합값을 Bloom Filter로 처리하고 각 차량이 이를 받아 수신한 메시지를 검증할 수 있게 한다. 또, 타임스탬프를 사용하여 재생공격을 방지한다. 제안하는 기법의 해쉬통합 및 검증과정은 〔그림 2〕와 같다.



〔그림 2〕 제안하는 기법의 해쉬통합 및 검증

1) 대칭키 설립

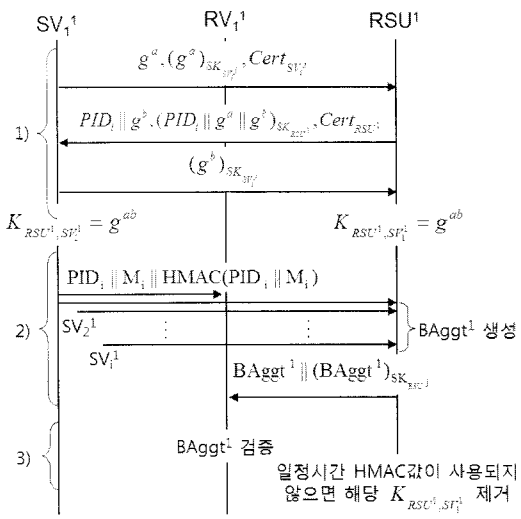
j번째 영역에서의 i번째 차량 V_i^j가 자신의 통신반경 안에서 RSU^j를 감지하면 둘 사이에 공유할 대칭키 K_{RSU^j,V_i^j}를 교환한다. 이 과정은 〔그림 3〕과 같이 기존의 공개키 기반의 Diffie-Hellman 키 교환 프로토콜을 적용함으로써 이루어지며 k-anonymity를 적용시켜 RSU는 k개의 차량에게 똑같은 PID를 할당하여 ID-Key 테이블에 저장한다. 그리고 해당 key는 일정 시간동안 HMAC에서 사용되지 않으면 테이블에서 사라진다.

이 때, 사용된 PID는 k개의 차량이 똑같이 사용하는 ID이고, RSU는 어떤 메시지를 받았을 때 자신이 가지고 있는 ID-Key 테이블의 모든 키로 차례로 복호화 해봄으로써 메시지 송신차량이 자신의 ID-Key 테이블에 있는 key값을 사용했는지 알 수 있다. 따라서 k개의 차량은 똑같은 PID를 사용하여 임의의 공격자는 k개의 차량을 구별할 수 없지만 RSU는 각 차량의 ID가 아닌 고유 key를 통하여 차량의 신원을 확인할 수 있다.

2) 해쉬통합 (Hash Aggregation)

메시지 송신차량 SV_i^j는 RSU^j와 공유한 대칭키 K_{RSU^j,SV_i^j}로 메시지 인증코드($HMAC$)를 생성하여 RSU^j 및 주변의 다른 차량에게 다음과 같은 값을 전송 한다.

$$PID_i \| M_i \| HMAC_{K_{RSU^j,SV_i^j}}(PID_i \| M_i)$$



〔그림 3〕 해쉬통합 및 검증 프로토콜

ID	Key	Cert	Time Stamp
PID_1	K_1	$Cert_1$	T_1
PID_1	K_2	$Cert_2$	T_2
PID_1	K_3	$Cert_3$	T_3
⋮	⋮	⋮	⋮
PID_1	K_k	$Cert_k$	T_k

〔그림 4〕 ID-Key 테이블

이를 받은 RSU^j는 다음과 같은 과정을 통해서 해쉬통합을 하고 다시 주변의 차량에게 전송한다.

먼저 RSU^j는 받은 $PID_i \| M_i \| HMAC_{K_{RSU^j,SV_i^1}}(PID_i \| M_i)$ 값을 최초 키 교환을 통해 만들어진 자신의 ID-Key 테이블의 모든 K_i값으로 차례로 풀어보아 유효한 K_i로 생성된 메시지인지 검증을 한다. 만약 자신이 가지고 있는 key목록 중에 $HMAC$과 맞는 값이 존재하지 않으면 해당 메시지는 버린다.

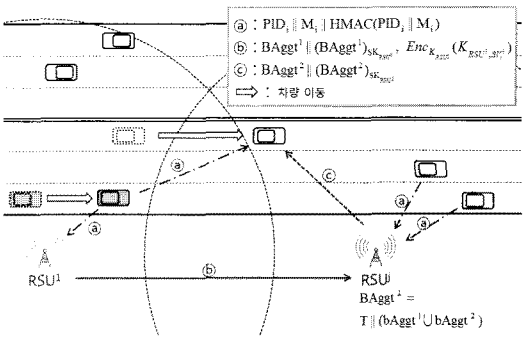
정해진 임계치의 시간까지 받은 모든 M_i값을 해쉬하여 Bloom Filter에 삽입한 값을 $bAggt$라고 한다. 그리고 현재의 시간정보인 타임스탬프값 T에 $bAggt$를 붙인 값을 $BAggt$라고 칭한다. 즉, $BAggt = T \| bAggt$이며, 이 값은 주기적으로 새로 생성하기 때문에 이전 통신에서의 주변차량 정보가 누적되지 않고 메시지 송신 시점의 송신차량 주변차량들의 정보가 전송되게 된다. 그리고 이 $BAggt$값에 RSU의 개인키로 서명한 값을 붙여 다음과 같은 값을 각 수신차량 RV_i^j에게 송신하고, 이후에도 같은 방법으로 임계치 시간만큼의 메시지들에 대한 $BAggt$값을 주기적으로 전송을 한다.

$$BAggt \| (BAggt)_{SK_{RSU^j}}$$

여기에서 타임스탬프를 붙이는 이유는 위에서 설명한 것처럼 RAISE에서는 공격자에 의해 재생공격이 가능한데 여기에 타임스탬프를 사용하면 이 공격을 방지할 수 있기 때문이다. 송신차량이 T값과 Bloom Filter를 붙여서 메시지를 송신하면 이 메시지를 받은 수신 차량은 T를 확인하여 주어진 임계치의 시간보다 크게 되면 메시지를 버리고, 임계치보다 크지 않은 경우에만 유효한 메시지로 간주한다.

3) 검증

RSU에게서 $BAggt \| (BAggt)_{SK_{RSU^j}}$값을, 메시지 송신 차량에게서 $PID_i \| M_i \| HMAC_{K_{RSU^j,SV_i^1}}(PID_i \| M_i)$값을 받은 메시지 수신 차량은 먼저 $BAggt$의 서명값을 RSU의 공개키로 검증한다. 서명값이 유효하면 $BAggt$의 타임스탬프 값이 주어진 임계치를 벗어나는지를 확인하여 발생 가능한 재생공격을 막는다. 그리고 메시지 송신 차량에게서 받은 $PID_i \| M_i \| HMAC_{K_{RSU^j,SV_i^1}}(PID_i \| M_i)$값에서 M_i의 해쉬값을 계산하여 이 값이 RSU에게서 받은 $BAggt$에 포함되는지 확인하는 방법으로 메시지를 검증할 수 있다.

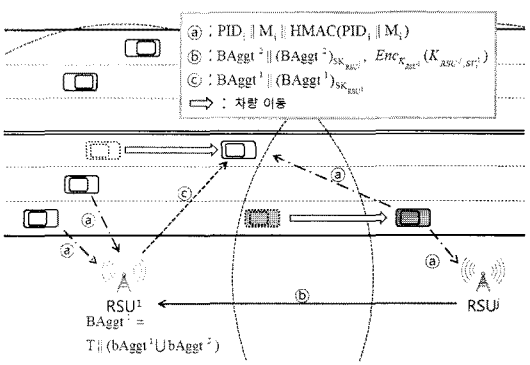


〔그림 5〕 차량의 이동 - 메시지 수신차량의 도메인이동

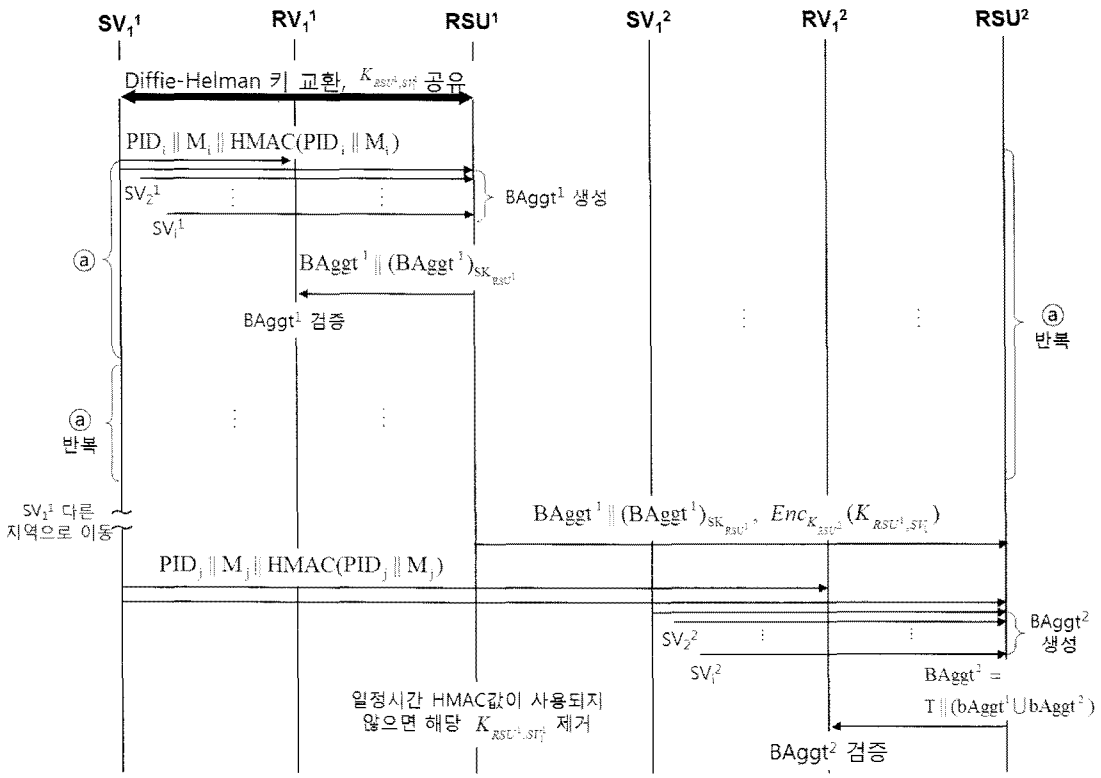
4) 핸드오버

차량이 한 RSU의 범위에서 다음 RSU로 이동하는 경우에는 핸드오버과정을 통하여 인증과정을 간소화 시킨다. RSU^1은 주위의 RSU^j에게 만들어진 $BAggt$값과 함께 자신이 가지고 있는 RSU^1과 핸드오버 차량 SV_i^1의 key정보 K_{RSU^1,SV_i^1}을 각 RSU^j의 공개키로 암호화 하여 보낸다. 이 때 보내어지는 값은 다음과 같다.

$$BAggt \| (BAggt)_{SK_{RSU^1}},\ Enc_{K_{RSU^j}}(K_{RSU^1,SV_i^1})$$



〔그림 6〕 차량의 이동 - 메시지 송신차량의 도메인이동



〔그림 7〕 제안하는 기법의 프로토콜

이를 수신한 RSU^j는 자신의 Bloom Filter 값 $BAggt^2$에 새로 받은 $BAggt^1$값을 Bitwise-OR 연산하여 두 가지 정보를 모두 포함하도록 한다. 즉, $BAggt^2 = T\|(bAggt^1 \cup bAggt^2)$이다. RSU^j는 이렇게 생성된 $BAggt^2$값을 임계치 시간이 지나면 버리고 자신의 통신반경에서 새로 생성된 $BAggt$값을 마찬가지 방법으로 주위의 RSU들에게 전송한다. 이 때 사용되는 $BAggt^1$과 $BAggt^2$값은 주기적으로 새로 생성되는 값이기 때문에 이를 $Union$한 $BAggt^2$값속의 각 차량정보는 계속해서 누적되지 않는다.

이러한 과정을 통해 차량이 한 RSU의 통신반경에서 다른 RSU의 통신반경으로 이동하는 경우에도 간단하게 메시지 인증이 가능하다. 메시지 수신 차량이 RSU의 통신범위에 들어오고, 메시지 송신 차량은 들어오지 않은 경우 메시지 수신차량은 수신한 메시지가 정당한 값인지 알 수 있다(〔그림 5〕). 마찬가지로 메시지 수신 차량은 RSU의 통신범위에 들어있고, 메시지 송신 차량은 RSU의 통신범위에서 빠져나갔을 때에도 메시지 송신차량의 정보를 수신 차량이 확인할 수 있도록 RSU^j가 주변 RSU에게 $BAggt$값을 보낸다(〔그림 6〕).

또한 RSU^j는 자신의 개인키로 RSU^1에게서 받은 $Enc_{K_{RSU^j}}(K_{RSU^1,SV_i^1})$값을 복호화 하고, 여기에서 얻은 K_{RSU^1,SV_i^1}값을 자신의 ID-Key 테이블에 추가한다. 이를 통해 추 후 해당 키를 가진 차량이 자신의 도메인에 들어왔을 때 별도의 키교환 없이 차량의 키를 가질 수 있게 된다. 각 차량이 새로운 RSU^j로의 이동시 RSU^j는 한번의 복호화 과정만으로 주위의 RSU에게서 키정보를 받아 사용할 수 있고, 각 차량도 최초의 키교환을 제외하면 이후 새로운 지역으로 이동하더라도 별도의 계산과정 없이 여러 RSU와 키를 공유할 수 있다. 그리고 이 key는 일정 시간동안 사용되지 않으면 ID-Key 테이블 목록에서 자동으로 제거되고, 이로 인해 이전 영역에서 차량이 빠져나간 것을 확인할 수 있다.

제안하는 기법의 전체적인 프로토콜은 〔그림 7〕과 같다.

IV. 안전성 및 효율성 분석

4.1 안전성

4.1.1 보안 요구사항

1) 인증

메시지 송신 차량에 대한 인증을 위하여 *RSU*가 가지고 있는 ID-Key 테이블만 안전하게 보호된다면 메시지에 해당하는 키를 통해 사용자 인증이 가능하다. 그리고 차량의 핸드오버 시 *RSU*의 공개키로 암호화하여 보내진 K_{RSU^j,SV_i}를 통하여 새로운 지역으로 이동한 차량에 대한 인증이 가능하다. 또한 이러한 과정에 사용되는 인증 메시지는 *RSU*가 검증한 후 타임스탬프를 붙여 송신차량들에게 보낸다. 따라서 공격자가 재생공격을 위해 특정 메시지를 보관하고 일정 시간 뒤에 사용하더라도 타임스탬프 값이 특정 임계치를 넘어가면 무효한 메시지로 간주함으로 인해 재생공격을 막을 수 있다.

2) 메시지 무결성

메시지 송신차량이 각 수신차량과 *RSU*에게 보내는 메시지는 $PID_i \| M_i \| HMAC_{K_{RSU^j,SV_i}}(PID_i \| M_i)$이다. 최초 설립한 메시지 송신차량과 *RSU*간의 대칭키 K_{RSU^j,SV_i}가 노출되지 않는다면 *HMAC*의 안전성에 의해 메시지는 변조될 수 없다. *RSU*가 메시지 검증을 위해 각 차량들에게 보내는 $BAggt \| (BAggt)_{SK_{RSU}}$의 값도 *RSU*의 개인키로 서명하기 때문에 *RSU*의 개인키가 노출되지 않는 이상 변조될 수 없다. 차량의 다음 지역으로의 이동에 따른 핸드오버 시에도 수신 *RSU*의 공개키로 K_{RSU^j,SV_i}을 암호화 하여 보내기 때문에 메시지 검증을 위해 필요한 대칭키를 안전하게 이동시킬 수 있다.

3) 가용성

기존의 기법에서 메시지의 개수에 비례하여 크기가 늘어났던 해쉬통합 값이 제안하는 기법에서는 하나의 Bloom Filter값으로 표현됨으로 인해 통신량이 줄어들었다. 그리고 차량이 다른 지역으로 이동할 경우에는 새로이 키교환을 할 필요가 없다. 이로 인해 사용자가 자원에 접근하는데 있어서 가용성이 늘어났다.

4) 익명성 및 비연결성

k-anonymity 개념을 적용하여 k개의 차량은 똑같은 ID를 사용하므로 임의의 공격자가 특정 차량에 대한 구분을 할 수 없고, 익명성 및 비연결성을 보장한다. 따라서 각 차량에 대한 프라이버시를 향상시킬 수 있다.

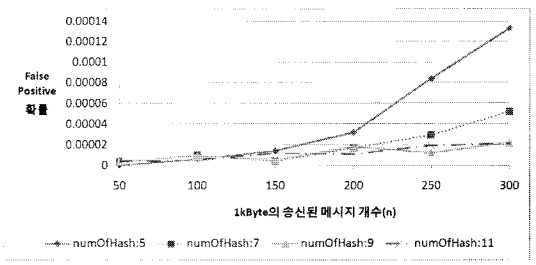
4.1.2 False Positive

제안된 기법은 Bloom Filter를 사용했기 때문에 전송되는 패킷의 크기가 줄어들지만 False Positive가 발생할 가능성이 있다. 다시 말해, 정당한 절차를 거쳐 *RSU*로부터 인증 받지 않은 메시지 M_i가 Bloom Filter에 포함되어 있다고 판정될 수 있는 확률이 존재한다. 따라서 False Positive의 확률은 제안하는 기법의 안전성에 영향을 준다. Bloom Filter에서 발생할 수 있는 False Positive의 확률은 다음과 같다 [16].

$$P = (1-(1-\frac{1}{m})^{kn})^k \approx (1-e^{-kn/m})^k$$

- P : False Positive 확률
- k : 해쉬 함수의 개수
- m : Bloom Filter의 크기
- n : 메시지의 개수

본 논문에서는 k개의 해쉬 대신에 계산량을 줄이기 위하여 하나의 해쉬를 k개의 조각으로 나누었다. 밀집된 차량들이 주기적으로 항상 전송해야 하는 Bloom Filter 값은 크기가 커지면 오버헤드로 인해 많은 문제점이 생길 수밖에 없다. 따라서 Bloom Filter의 크기는 일정크기 미만으로 지정 해주어야 하고, 이 Bloom Filter의 위치값을 나타내게 되는 해쉬값의 크기는 Bloom Filter의 크기를 *B*라고 할 때 $\log_2 B$미만이어야 한다. 차량 밀집환경에서 매번 1KByte를 초과하는 패킷을 보내는 것은 부담이 되



[그림 8] 메시지 수(n)에 따른 False Positive 확률

므로 $\log_2|1KByte|$, 즉 13bit 미만의 해쉬값들을 사용해야 한다. 일반적으로 해쉬값은 160bit 이상의 값을 가지기 때문에 본 논문의 환경에서는 하나의 해쉬값을 여러개로 나누어 사용하였고, 여러 개의 해쉬값을 사용한 것과 같은 효과를 얻을 수 있다.

이를 표현하기 위해 Java를 이용하여 차량이 밀집된 상태의 환경을 구성하고 Bloom Filter 및 인증과정을 구현하여 시뮬레이션 하였다. [그림 8]은 Java를 통하여 구현된 환경에서 1 Kbytes의 *BAggt*메시지를 보내고 이를 검증할 때 메시지 개수와 해쉬의 개수에 따른 False Positive 발생 확률의 시뮬레이션 결과이다. 구현에 사용된 해쉬함수는 SHA1이다. 결과를 보면 통신범위 내에 300대 가량의 많은 수의 차량이 밀집해있을 경우에도 False Positive의 확률이 0.01% 미만으로 나타나는 것을 확인할 수 있다. 특히, 사용되는 해쉬함수 조각의 수가 7개 이상일 때 False Positive는 0.006% 이하로 나타난다. 따라서 해쉬함수의 수를 충분히 유지하여 인증기법을 구성한다면 안전한 인증환경을 구성할 수 있다.

4.2 효율성

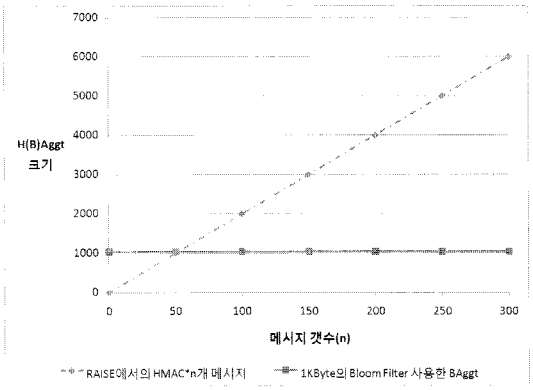
4.2.1 통신량

RAISE와 제안된 기법에서 각 차량이 RSU와 다른 차량에게 전송하는 메시지 $\Pi D_i \| M_i \| HMAC_{K_{RSU}}(\Pi D_i \| M_i)$의 크기는 같다. 두 기법간의 다른 점은 RSU가 전송하는 *HAggt*와 *BAggt*의 차이이다. RAISE에서는 전송되는 패킷의 크기가 n의 개수에 비례하기 때문에 RSU가 보내는 *HAggt*는 $H \times n$이다. 하지만 제안된 기법에서는 Bloom Filter에 타임스탬프를 붙인 값이기 때문에 일정하며 [그림 9]와 같이 송신되는 메시지의 개수가 많아져도 그 크기가 크지 않다.

4.2.2 계산량

RAISE는 기존의 PKI기반의 프로토콜과 비교했을 때 수신차량 주위의 모든 차량에게서 받은 인증서를 검증해야 하는 것을 하나의 *HAggt*로 줄여 많은 계산량을 감소시켰다.

RAISE와 제안된 기법의 계산량을 비교해 보면 각 차량들의 Diffie-Hellman 키교환의 계산량의 합을 *D*, 해쉬 계산을 한번 할 때의 계산량을 *H*, 각 차량이



[그림 9] 차량밀도에 따른 *HAggt*, *BAggt*의 크기

[표 2] RAISE와 제안된 기법의 계산량

	RAISE	제안된 기법
키교환 회수 (RSU-V)	$D \times r$ *	D **
해쉬통합 (RSU)	$H \times n$, *HAggt*의 서명 계산	$H \times n$, *BAggt*의 서명 계산
검증 (V)	*HAggt*의 서명 검증, *H*	*BAggt*의 서명 검증, *H*

* : 매 *RSU*와 통신하는 각 차량들과의 키 교환
** : 초기 키 교환 한번, 이후 *RSU*를 통한 키 이동

이동할 때 거치는 *RSU*의 개수를 r, 그리고 *RSU*의 통신범위 내의 모든 차량이 전송하는 메시지의 개수를 n이라고 할 때 [표 2]와 같다.

결과를 보면 먼저 키 교환 단계에서 RAISE는 최초 각 차량이 *RSU*와 키교환을 한 후 다른 지역으로 이동 할 때마다 새로운 *RSU*와 매번 다시 키교환을 해야 한다. *RSU*입장에서는 키교환시마다 상위 계층의 AS를 통해 각 차량의 *Cert*를 확인해야 하고, 차량입장에서도 별도의 계산이 필요하지만, 제안된 기법에서는 최초의 키교환 이후에는 *RSU*끼리 키정보를 주고받기 때문에 *RSU*는 한번의 복호화과정만으로 키정보를 받을 수 있고, 차량은 최초 키교환 시의 한번의 계산량만이 필요하다.

*RSU*의 해쉬통합 단계에서는 n개 각각의 메시지에 대하여 해쉬계산을 한 후 모두 붙이는 RAISE와 n개의 메시지에 대한 해쉬값을 Bloom Filter에 삽입하는 제안된 기법이 *HAggt*와 *BAggt*의 형식만 다를 뿐 같은 계산량을 필요로 한다. 메시지 수신차량이 수신한 메시지를 검증하는 단계에서도 서명값을 계산할 때와 마찬가지로 같은 계산량이 필요하다.

V. 결 론

본 논문에서는 차량이 밀집되고 통신량이 많은 VANET 환경에서 RSU가 차량들의 통신을 도와 효율적이면서도 안전하게 메시지 인증을 할 수 있는 방법을 제안하였다. 기존의 방법들은 이러한 특정한 상황을 간과하거나 효율적이지 못한 방법을 사용함으로써 오버헤드나 기타 공격이 발생할 수 있었다. 본 논문에서는 Bloom Filter를 사용하여 기존의 방법보다 통신량 및 계산량을 줄였고, 타임스탬프를 사용하여 기존에 발생 가능했던 재생공격을 막았으며, 차량이 다른 지역으로 이동시 불필요한 키교환 과정을 생략함으로써 인증과정을 간소화시켰다. 그 결과 효율성을 높이면서도 메시지 무결성, 사용자 인증, 익명성 등 기본적인 보안 요구사항을 만족하였다. 또 세부적인 계산과 구현을 통하여 안전성과 효율성을 보였다. 향후에는 본 논문에서 제안한 차량 밀집환경에서의 스킴과 일반적인 환경에서의 다른 스킴과의 연계과정을 위한 연구를 진행할 예정이다.

참고문헌

[1] C. Zhang, X. Ling, and P-H. Ho, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks," in Proc. IEEE ICC 2008, Beijing, China, pp. 1451-1457, May. 2008.

[2] IEEE1609.2. IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages, Jul. 2006.

[3] M. Gerlach, A. Festag, T. Leinmuller, G. Goldacker, and C. Harsch, "Security Architecture for Vehicular Communication," 5th International Workshop on Intelligent Transportation (WIT), Hamburg, Germany, Mar. 2005.

[4] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya. "Architecture for Secure and Private Vehicular Communications," In ITST'07, Sophia Antipolis, France, pp. 1-6, Jun. 2007.

[5] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications," IEEE Transaction on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[6] M. Raya and J. P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, vol. 15, no. 1, pp. 39-68, Jan. 2007.

[7] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks," in Proc. IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, Arizona, pp. 246-250 , May. 2008.

[8] DSRC: Dedicated short range communications.http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[9] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

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

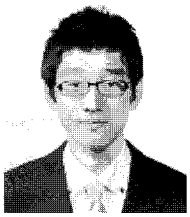
[11] L. Sweeney, "K-ANONYMITY: A Model for Protecting Privacy," International Journal on Uncertainty, uzziness, and Knowledge-based Systems, vol. 10, no. 5, pp. 557-570, Oct. 2002.

[12] Y. Xi, K. Sha, W. Shi, and L. Schwiebert, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," in Autonomous Decentralized Systems, ISADS, pp. 344-351, Mar. 2007.

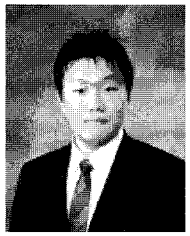
[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in Proc. IEEE International Conference on Computer Communications (INFOCOM'08),

Phoenix, Arizona, Apr. 2008.
[14] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks", in Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, Sep. 2005.
[15] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," IEEE Network, vol. 15, no. 6, pp. 30-39, Nov. 2001.
[16] L. Fan, P Cao, J. Almeida, and A. Z. Broder, "Summary Cache : A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Transactions on Networking, vol. 8, no. 3, pp. 281-293, Jun. 2000.

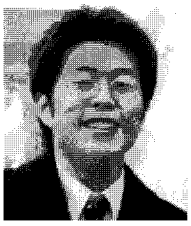
〈著者紹介〉



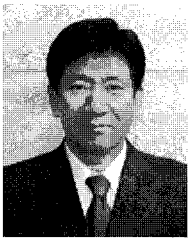
정 석 재 (Seock Jae Jung) 학생회원
2009년 2월: 서울시립대학교 수학과 졸업
2009년 3월 ~ 현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 암호프로토콜, VANET, 스마트폰 보안, 클라우드 컴퓨팅, PET 기술



유 영 준 (Young Jun Yoo) 학생회원
2008년 2월: 숭실대학교 수학과 졸업
2010년 3월: 고려대학교 정보경영공학전문대학원 석사
〈관심분야〉 암호프로토콜, VANET, 네트워크 코딩, 응용암호



백 정 하 (Jung Ha Paik) 학생회원
2006년 2월: 고려대학교 수학과 졸업
2006년 3월 ~ 2008년 2월: 고려대학교 정보경영공학전문대학원 석사
2008년 3월 ~ 현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 암호프로토콜, VANET, 스마트폰 보안, 클라우드 컴퓨팅, 애드 혹 네트워킹



이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월 ~ 1997년 2월: 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월: 고려대학교 전산학과 부교수
2001년 3월 ~ 현재 : 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술