JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 10 : 2309~2315, Oct. 2013

차량 네트워크에서 강한 익명성이 지원되는 인증 프로토콜을 위한 확률론적 접근방식

김태연[1] · 안도식[2] · 조기환[2*]

A Probabilistic Approach for Robust Anonymous Authentication Protocol in VANETs

Tae-yeon Kim[1] · Do-sik An[2] · Gi-hwan Cho[2*]

[1] Department of Computer Science & Information Communication, Seonam University, Namwon 590-711, Republic of Korea
[2] Division of Computer Science & Engineering(CAIIT), Chonbuk National University, Jeonju 561-756, Republic of Korea

요 약

차량애드혹네트워크(VANET: Vehicular Ad-hoc Network)는 차량 간 통신을 통하여 운전자의 안전을 향상시키는 응용으로 많은 관심을 받고 있다. 이러한 VANET의 활성화를 위해서는 프라이버시가 보장되는 상호 인증이 보장되어야 한다. 기존 연구에서는 그룹 기반 인증 프로토콜들이 제안되었다. 그러나 키 그룹의 반복사용으로 인한 ID노출과 RSU(Road side Unit)의 DoS의 공격 위험에 대한 문제가 고려되지 않았다. 본 논문에서는 강한 익명성이 지원되는 인증 프로토콜을 위한 확률론적 접근방식을 제안한다. VANET 환경에서 제안된 구조를 몇 가지의 조건 하에서 성능을 평가하여 제안한 구조가 프라이버시를 향상시키는데 더 효율적인 방식임을 밝힌다.

ABSTRACT

VANET(Vehicular Ad-hoc Network) is getting attention as an application to improve driver safety through inter-vehicle communication. For activation of VANET, privacy-preserving mutual authentication has to be guaranteed. In previous works, authors proposed various group-based authentication protocols. However, risks on ID exposure due to repeated use of group key and RSU(Road Side Unit) DoS attack were not considered. In this paper, we propose a probabilistic approach for robust anonymous authentication protocol. We evaluated our proposed method in a sets of criteria in VANET and verified it is an efficient solution for enhancing privacy.

키워드 : 차량통신, 인증 프로토콜, 익명성, 확률론적 접근

Key word : Vehicular ad-hoc network, Authentication Protocol, Anonymous, Probabilistic approach

접수일자 : 2013. 06. 20 심사완료일자 : 2013. 07. 15 게재확정일자 : 2013. 07. 31

*** Corresponding Author** Gi-hwan Cho(E-mail:ghcho@jbnu.ac.kr, Tel:+82-63-270-3437)
Division of Computer Science & Engineering(CAIIT), Chonbuk National University, Jeonju 561-756, Republic of Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.10.2309 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

무선 통신 기술이 빠르게 진전되고 광범위하게 적용됨에 따라 VANET는 교통 시스템에서 도로의 효율성과 운전자의 안전성을 향상시키는 응용으로 많은 관심을 받고 있다. 일반적으로 VANET은 유선 인터넷에 연결된 특정 지역의 도로 관리국(RA: Road Authority)과 중계기(RSU: Road-Side Unit), 차량(OBU: On-Board Unit) 등의 노드들로 구성된다. 차량은 도로 상황에 관련된 데이터를 수집하여 전파하거나 주행 시 비상사태 등에 관련된 정보를 송수신하는데, 대부분의 통신은 차량 간(V2V) 또는 차량과 RSU(V2I) 간에 이루어진다. 따라서 노드 간에 교환되는 메시지는 긴급성과 정확성이 요구되고 있지만 무선 환경으로 인해 다양한 보안 위협에 노출되고 있다.

VANET 환경에서 발생할 수 있는 보안 위협들로는 사용자의 가장, 메시지의 불법접근과 수정, 송수신 거부, 네트워크의 장애 유도, 사용자의 프라이버시 침해 등이 있다. 특히 메시지 내에 실제 ID를 사용하는 경우 적대자(adversary)는 차량의 ID를 쉽게 알 수 있다[1-2]. 따라서 메시지의 프라이버시를 보장하기 위해서는 익명성이 지원되는 상호인증뿐만 아니라 분쟁이 발생한 경우 신뢰기관을 통해 해당 노드의 ID를 추적할 수 있어야 한다.

지금까지 발표된 대부분의 구조들은 익명성이 지원되는 인증을 위해 공개키 방식을 사용하고 있다. 하지만 인증을 받기 위해 사용되고 있는 인증서는 차량의 실제 ID를 확인할 수 있어 사용자의 프라이버시를 보장할 수 없다. 이러한 문제를 해결하기 위해 몇몇 연구가들은 차량의 ID를 감추거나 가명을 사용하는 방식들을 제안하였다. 또한 동일한 가명을 반복적으로 사용하는 경우에 차량의 위치를 쉽게 추적할 수 있기 때문에 가명을 수시로 변경하는 방식도 제안되었다[3-4]. 하지만 이러한 구조들은 네트워크에 연결된 중간 노드들(인증서버, RSUs)을 전적으로 신뢰한다는 가정 하에서 제안되었다.

일반적으로 인증을 처리하는 과정에서 높은 익명성의 수준을 지원하기 위해서는 낮은 수준을 지원할 때보다 더 많은 자원사용(통신비용과 계산비용)을 필요로 한다. 최근에 Xi[5] 등은 익명성 수준과 자원사용을 절충할 수 있는 적응적 그룹 기반 익명성 인증 프로토콜을 제안하였다. 그들의 구조에서 익명성 수준과 자원사용 비용은 키 그룹의 크기(k)에 따라 좌우된다. 사용자가 인증을 처리하는 과정에서 k를 크게 설정하면 프라이버시 수준은 높아지지만 중간 노드인 RSU와 차량에서의 계산비용이 증가하고, 반대로 k를 작게 설정하면 프라이버시 수준은 낮아지지만 계산비용이 줄어든다. 하지만 그들의 구조에서 야기될 수 있는 몇 가지 문제점이 있다. 첫째, 특정 차량이 정해진 시간에 동일한 장소를 통과하는 경우에, 해당 차량은 특정 키 그룹을 반복해서 사용하기 때문에 차량의 실제 ID가 노출될 확률은 $1/k$보다 높아진다. 게다가 RSU가 ID를 알아내기 위해 프로빙을 실시하고 사용자가 확률적 검증을 수행하는 경우는 ID가 노출될 확률은 더 높아진다. 두 번째는 적대가가 고의적으로 k를 크게 설정하여 RSU의 과부하를 받게 하는 DoS 공격을 시도하는 문제이다. 따라서 본 논문에서는 익명성 수준은 높이면서 자원사용을 최소화하고, RSU의 장애를 유발시키려는 DoS 공격을 줄일 수 있는 강한 익명성 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보고, 3장에서는 제안된 구조에 대한 프로토콜을 기술한다. 4장에서는 성능 및 보안 분석을 설명하고, 5장에서는 본 논문의 결론과 향후 연구 방향을 기술한다.

Ⅱ. 관련연구

VANETs 환경에서 공개키를 사용하여 익명성이 제공되는 사용자 인증을 수행하는 연구들을 살펴보면 다음과 같다.

Lu 등은 보안상 중간노드인 RSU는 보안상 안전하다는 가정 하에서 그룹 서명 프로토콜을 사용하여 OBU들에게 일시적인 익명성이 지원되는 인증서를 발급하는 ECPP를 제안하였다[3]. 하지만 인접한 RSU들이 서로 공모하여 차량을 추적할 수 있다. 그리고 인증서를 발급받을 때마다 동일한 가명을 사용하기 때문에 차량의 프라이버시가 보장되지 못한다.

Mishra 등은 안전하고 효율적인 메시지 인증을 통해 차량의 프라이버시가 보장되는 프로토콜을 제안하였다[6]. 이 구조는 통신비용과 계산비용을 줄일 수 있는 방식이지만 중간노드인 RSU를 전적으로 신뢰한다는 가

정을 두고 있다.

Tan은 ID-기반 그룹 서명을 통해 차량의 프라이버시를 보장하는 상호 인증 프로토콜을 제안하였다[4]. 이 구조에서 RSU들의 서로 공모한다고 하더라도 이동 차량의 위치를 추적하기 어렵다. 하지만 인증을 처리하는 과정에서 이동 차량이 동일한 가명을 사용하기 때문에 적대자에게 ID의 노출이 가능하다.

Hu 등은 RSU들의 공모나 내부 공격을 예방하고, 악의 있는 적대자가 차량을 추적하기 어렵게 하기 위해 Weil Pairing의 구조와 그룹 기반 (t, n) 한계점 서명을 기반으로 한 새로운 익명성 프로토콜(ATCS)을 제안하였다[7]. 하지만 이 구조를 구현하기 위해서는 인증 처리를 수행하는데 필요한 충분한 차량들(t)이 근거리에 존재하여야 한다. 근거리에 있는 차량들이 고의적으로 인증 처리에 협력을 하지 않는다거나 실제로 필요한 차량들(t)이 존재하지 않으면 인증 처리가 불가능한 구조이다.

Ma 등은 차량의 프라이버시를 위해 통신을 할 때마다 가명을 리필해 주는 2가지 방식을 제안하였다[8]. 이 구조에서 모든 차량은 1개의 인증서를 관리하고, 가명이 필요한 경우에 자신의 개인키를 사용하여 도로 관리국(RA)에 메시지를 보내고 가명들을 수신하는 구조이다. 따라서 RSU가 직접 인증을 수행하지 않지만 가명을 생성해 주는 곳이 RSU가 아닌 도로 관리국 RA이기 때문에 RA의 자원사용 부담이 있는 단점이 있다. 그리고 차량들은 해당 지역을 벗어나면 RA로부터 새로운 가명을 받아야 하기 때문에 RA가 이동 차량을 추적할 수 있다.

Ⅲ. 제안된 인증 프로토콜 구조

3.1. VANET구조

VANET에서 차량들은 WDSRC(Wireless Dedicated Short Range Communications)를 통해 다른 차량 또는 도로에 설치된 RSU와 통신을 한다. 차량이나 RSU는 송·수신한 메시지의 타당성을 입증하기 위해서는 디지털 서명을 사용해야 한다. 이를 위해서는 각 노드는 인증기관(Certificate Authority : CA)이 발부한 인증서를 관리해야 한다.

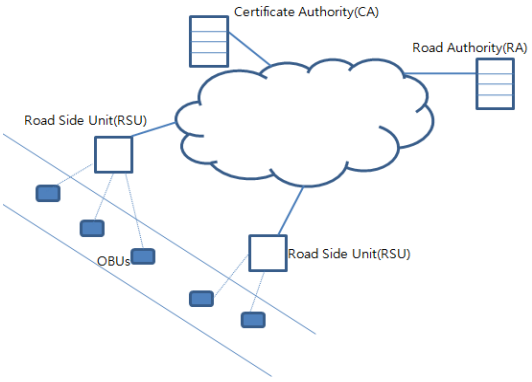

그림 1. VANET의 구조
Fig. 1 Structure of VANET

본 논문에서 제안한 프로토콜이 수행될 환경인 VANET의 구조는 그림 1과 같이 인증서를 발부하는 노드(CA)와 모든 차량들을 관리하는 노드(RA), 중간 노드들(RSUs), 차량들(OBUs)로 구성된다. 기존의 구조와는 달리 제안된 구조에서는 모든 차량들은 CA에 의해서 생성된 k개의 인증서를 관리한다. 하지만 CA는 어떤 인증서가 어떤 차량에 분배할 것인지에 대해서는 관여하지 않는다. 차량들에게 인증서들은 분배하는 기관은 RA이며, 실제 인증 처리는 노드 RSU에게 위임한다. 따라서 CA는 인증서를 생성하거나 갱신, 민원이 발생한 경우의 분쟁 처리, 과부하에 따른 문제 등을 처리하는 일들을 수행한다. RA는 차량들의 리스트와 인증서들의 리스트, 폐기·갱신된 인증서들의 리스트를 관리하고, 인증처리에 필요한 자료를 분배하는 역할을 한다.

3.2. 키 관리와 상호 인증

키 관리에 있어서 잠재적인 차량의 수와 실제 등록된 차량의 수, 한 차량이 관리해야 하는 키 쌍이 각각 N과 n, k라고 가정한 경우에 RA와 RSU는 $kN(= n + a)$개의 키 쌍과 그 인덱스를 관리한다. 여기에서 a는 아직 등록하지 않은 차량의 수를 나타내며, k개의 키 간에는 서로 연관성이 없다. 모든 키 쌍은 여러 개의 키 그룹으로 나뉘어서 관리된다. 그룹 조직을 융통성이고 효율적으로 관리하기 위해 모든 멤버들은 인덱스로 순서화된 완전 이진 트리로 구성된다. 여기에서 잎 노드는 공개키이고, 내부 노드는 각 서브그룹을 구분하는 서브그룹 ID이다.

각 키 그룹의 크기(*Sg*)는 멤버의 수로 최소(min)에서 최대(max)로 가정한 경우에 1/2(*N*/min+*n*/max)를 만족해야 하고, 각 그룹은 버전으로 구분된다.

RA가 등록된 차량에 *k*개의 키 쌍을 분배하는 과정은 일정한 규칙에 의해서 이루어지는 것이 아니라 랜덤하게 분배한다. 다시 말해서, 각 차량이 관리하고 있는 *k*개의 키 쌍 중에서 몇 개가 같은 그룹에 중복되거나 각각 서로 다른 그룹에 속할 수 있다. 각 사용자는 자신이 속해 있는 노드의 상위 레벨의 서브그룹 ID와 버전을 관리해야 한다. 그리고 키 분배는 RA에 의해서 이루어지기 때문에 CA나 RSU는 현재 어떤 노드의 키 쌍이 실제 사용 중인 것인지 더미로 사용 중인지를 알지 못한다. 또한 제안된 구조에서는 차량의 등록이나 취소, 할당된 키 쌍들을 갱신하기 위한 동적인 키 관리를 지원한다. 이전에 사용하던 키를 더 이상 사용할 수 없도록 하거나 갱신을 하고자 하는 경우에는 해당 노드의 키 쌍들을 다른 키로 변경하고, 그 그룹의 버전을 변경한 다음에 해당 그룹의 멤버들에게만 분배한다.

본 논문에서 제안한 인증 프로토콜은 입증 가능한 공통 비밀 인코딩(verifiable common secret encoding)을 기반으로 하기 때문에 사용자가 익명성 인증을 받기 위해서는 자신이 관리하고 있는 키 그룹 중 특정 그룹 버전의 서브그룹 ID와 버전을 RSU에게 전송하면 된다. 일반적으로 더 강한 익명성이 보장되는 인증을 받기 위해 더 상위 레벨의 그룹 ID를 전송하면 더 많은 계산비용을 감수해야 한다. 하지만 제안된 구조에서는 더 낮은 레벨의 서브그룹 ID를 사용하여도 같은 수준의 익명성을 보장할 수 있는 효과를 얻을 수 있다.

3.3. 제안된 프로토콜

익명성이 보장되는 그룹 기반 인증을 위한 프로토콜은 그림 2와 같다. 그룹 기반 인증 프로토콜은 인증 요청자가 자신의 ID를 노출하지 않은 채 그룹 내의 한 멤버라는 사실만을 알리고, 요청 메시지를 받은 RA는 요청자의 실제 ID를 모르는 채 그룹 내의 정당한 멤버임을 확인하는 과정이다.

인증 처리 과정은 다음과 같다.

(1) RSU는 자신의 ID와 공개 키, 현재 시간을 인증기관의 개인키(Cert)로 암호화하여 방송한다.

(2) OBU는 수신한 메시지를 인증기관의 공개키로 복호화하여 RSU의 ID와 공개키를 알아낸다. 그리고 자신이 생성한 세션키와 자신이 속해있는 그룹들 중의 어느 한 그룹의 ID(GID), 그룹 버전(VG), 서브그룹 ID(SubID), 현재시간(T2), 부가적인 정보(auth_self)를 전송한다. auth_self는 AS에게 전송하는 메시지로서 노드 RSU가 과부하 유도나 침입이 예상되는 경우에 CA에게 전송하도록 하여 자신의 정당성을 인정받기 위함이다.

(3) RSU가 OBU로부터 받은 메시지를 보고 과부하를 유도하거나 침입이 예상되는 경우에 요청하는 단계이다.

(4) CA가 해당 차량에 대한 개인 인증을 수행하고 그 결과를 별도로 관리하여 추후에 과금 여부의 자료로 사용할 수 있다. 정상적인 요구인 경우는 true로, 비정상적긴 경우는 false로 해서 전송한다. 특별한 경우에만 단계 3과 4를 수행한다.

(5) RSU는 랜덤 값 x를 생성해서 해당 서브그룹 멤버들의 공개키로 암호화 한 다음에 OBU에게 전송한다.

(6) OBU는 자신의 개인키를 사용하여 값 x′를 생성한다. 그리고 새로 생성된 x′를 나머지 멤버들의 공개키로 암호화하여 Pub1(x′), Pub2(x′), ..., Pubm(x′)를 생성한 다음 수신한 내용과 비교한다. 만일 서로 일치하면 RSU에게 응답을 보내고 그렇지 않으면 무시한다.

(1) RSU → OBUs: $Cert(ID^{RSU}, Pub^{RSU}, T_1)$

(2) OBU → RSU: $[SK, GID, V_G, SubID, T_2, auth\_self]Pub^{RSU}$

auth_self : $[OBU, GID, V_G, , SubID, [T_2, RSU]Pri^{OBU}]Pub^{CA}$

(3) RSU → CA: $[OBU, V_G, T_2, auth\_self]Pub^{CA}$

(4) CA → RSU: $[true/false, OBU, T_3, [OBU, T_3]Pri^{CA}]Pub^{RSU}$

(5) RSU → OBU: $[Pub_{SubID}(x), T_4, GID, V_G, [T_4]Pri^{RSU}]SK$

(6) OBU → RSU: $[x, Req, T_5]SK$

그림 2. 제안된 프로토콜
Fig. 2 Proposed protocol

Ⅳ. 성능과 보안 분석

이 장에서는 Rivest[9]에 의해서 제안된 구조(Rivest)와 Xi[5]에 의해서 제안된 구조(Xi), 본 논문에서 제안된 구조(Proposed)에 대해 차량의 계산비용과 보안성 측면에서 비교분석한다. 본 시뮬레이션을 위한 네트워크 모델을 다음과 같다.

(1) 공개키 암호화는 때문에 OBU내의 인베디드 프로세서로 Intel SA-1110을 사용하고, RSU에는 Pentium-M 1.7Ghz를 사용한다.
(2) 각 차량에 한 대의 RSU를 설치하고, 수신 감도와 전송력은 -77dBm와 17dBm으로 설정한다.
(3) RSU의 서비스 영역권 내에 동시에 존재하는 차량의 수는 차량간의 물리적 공간을 감안하여 10대로 제한한다.
(4) 인증 요구 단말이 사용하는 공통 비밀 슬롯을 20으로 한다.

4.1. 성능분석

Xi와 Proposed에서는 확률론적 인증 개념을 사용하기 때문에 계산비용은 Rivest의 서명 방식에 비해 훨씬 적게 들지만 Proposed는 Xi보다는 다소 처리 비용이 더 든다. 다시 말해서, Xi와 Proposed가 Rivest보다 계산비용이 적게 드는 것은 공통 비밀 슬롯을 모두 검증하지 않기 때문이며, Proposed와 Xi의 차이는 키 검색 시간에 기인된다.

그림 3은 검증 비율에 따라 계산비용을 나타낸 것이다. 검증 비율이 변함에 따라 Rivest은 계산비용에 영향을 주지 않지만 Xi과 Proposed는 그 수준이 감소할수록 처리 시간이 줄어든다. 그리고 Xi 구조와 Proposed 구조에서의 차이는 RSU에서 키를 검색하는데 필요한 계산비용 때문이다. 따라서 강한 익명성을 필요하지 않는 환경에서는 처리시간을 상당히 단축시킬 수 있게 된다.

4.2. 보안성 분석

공개키를 기반으로 하는 구조에서 차량의 프라이버시를 강화하기 위해서는 공통 비밀 슬롯의 수를 늘리거나 사용자가 관리하는 인증서의 수를 늘리는 방법이 있을 수 있다. 전자처럼 슬롯의 개수를 늘리면 키 관리 비용에는 영향을 미치지 않지만 계산비용이 상대적으로 증가한다. 반면에 차량이 관리하는 인증서의 수를 늘리는 경우에 키 관리비용을 제외하면 계산비용은 증가하지 않는다.

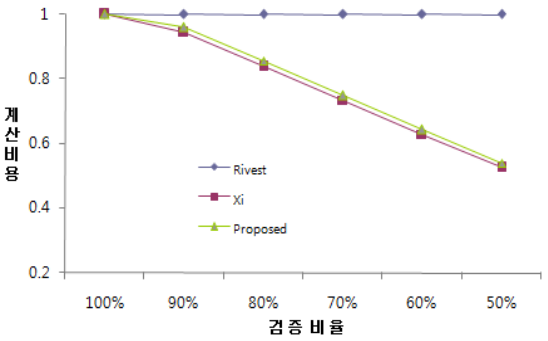

그림 3. 검증 비율과 계산비용
Fig. 3 Verification rate and the computational cost

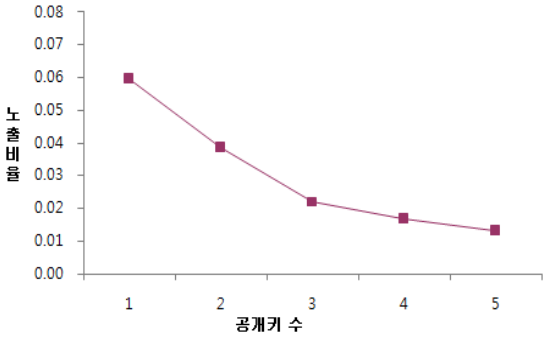

그림 4. 공개키의 수와 노출 비율
Fig. 4 Number of public key and expose ratio

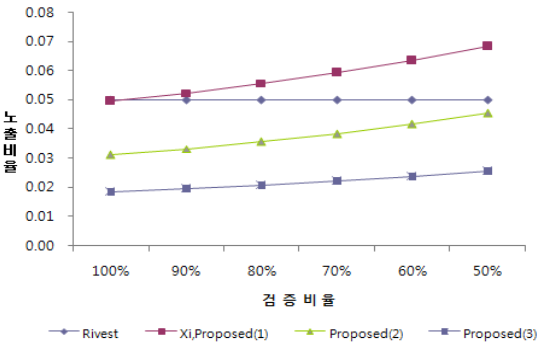

그림 5. 검증비율과 노출비율
Fig. 5 Verification rate and expose ratio

그림 4는 검증 정도를 70%로 했을 경우에 사용자가 관리하는 키의 수에 따라 차량의 ID가 노출될 확률을 나타낸 것이다. 인증서의 수가 증가할수록 차량의 ID가 노출될 확률이 낮아짐을 알 수 있다.

그림 5는 Rivest의 구조와 Xi 구조, Proposed 구조에서 인증서의 수를 1개와 2개, 3개로 했을 경우 ID가 노출될 확률을 나타낸 것이다. Rivest의 구조는 확률론적 익명성 개념을 사용하지 않기 때문에 노출 확률이 일정하지만 Xi의 구조와 제안된 구조는 검증 정도에 따라 노출 확률이 증가함을 나타낸다. 하지만 Proposed 구조에서의 계산비용이 추가로 들지 않고 더 높은 사용자 프라이버시가 보장됨을 알 수 있다.

따라서 사용자가 더 빠른 응답 또는 프라이버시 조건이 매우 중요하지 않는 경우에 익명성 조건을 낮추면 되고, 사용자가 프라이버시 요구조건을 강화하고자 하는 경우는 약간의 통신 대역폭을 늘려줌으로써 더 강한 익명성을 보장받을 수 있다.

Ⅴ. 결 론

본 논문은 시스템의 성능과 차량의 프라이버시 수준을 적절하게 조절할 수 있는 강한 익명성이 지원되는 인증 프로토콜을 위한 확률론적 접근방식을 제안한다. 시뮬레이션을 통해 성능 측면과 사용자의 프라이버시 보장 측면을 비교분석하였다. 각 노드로 하여금 k개의 인증서를 관리하도록 함으로써 계산 비용은 줄이고 보안 강도는 높이는 효과를 얻을 수 있지만, 키 관리를 하는데 추가 비용이 소요된다. 특히, 특정 차량이 정해진 시간에 동일한 장소를 통과하는 경우에 사용자의 프라이버시 보장의 강도가 더 높다는 것이 확인되었다. 그리고 네트워크의 장애를 유발시키려는 DoS 공격이 예상되는 경우에 더 강한 인증을 실시할 수 있는 메커니즘을 추가하였다. 향후 필요한 연구과제는 실제 VANET환경에서 제안된 기술을 구현하는 것이다.

REFERENCES

[1] Y. Hao, T. Han, and Y. Cheng, “A cooperative message authentication protocol in VANETs,” in *Proceeding of GLOBECOM*, Anaheim, CA, pp. 5562-5566, 2012.

[2] J. Chen and J. Wu, “Cooperative anonymity authentication in vehicular networks,” in *Proceeding of IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, Macau, pp. 1018-1023, 2009.

[3] R. Lu et al, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proceeding of INFOCOM*, Phoenix, AZ, pp. 1903-1911, 2008.

[4] Z. Tan, “A privacy-preserving mutual authentication protocol for vehicle Ad Hoc networks,” *Journal of Convergence Information Technology*, vol. 5, no. 7, pp. 180-186, Sep. 2010.

[5] Y. Xi et al, “Probabilistic adaptive anonymous authentication in vehicular networks,” *Journal of Computer Science and Technology*, vol. 23, no. 6, pp. 916-928, Nov. 2008.

[6] B. Mishra, S. K. Panigrahy, D. Jena, and S. K. Jena, “A secure and efficient message authentication protocol for VANETs with privacy preservation,” in *Proceeding of World Congress on Information and communication Technologies*, Mumbai, pp. 880-885, 2011.

[7] W. Hu, K. Xue, P. Hong, and C. Wu, “ATCS: A novel anonymous and traceable communication scheme for vehicular Ad Hoc networks,” *International Journal of Network Security*, vol. 13, no. 2, pp. 71-78, Sep. 2011.

[8] Z. Ma, F. Kargl, and M. Weber, “Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications,” in *Proceeding of IEEE 68th Conference on Vehicular Technology Conference*, Calgary, BC, pp. 1-5, 2008.

[9] R. L. Rivest, A. Shamir, and A. Tauman, “How to leak a secret,” *Lecture notes in Computer Science*, pp. 552-565, 2001.

김태연(Tae-Yeon Kim)

1986년 전남대학교 계산통계학과 학사
1988년 전남대학교 전산통계학과 석사
1996년 전남대학교 전산통계학과 박사
1996년 3월 ~ 현재 서남대학교 컴퓨터정보통신학과 조교수
※관심분야 : 네트워크 보안, 이동 컴퓨팅, 네트워크 관리, 센서 네트워크

안도식(Do-Sik An)

2008년 전북대학교 전자정보공학부 학사
2010년 전북대학교 전자정보공학부 석사
2010년 9월 ~ 현재 전북대학교 전자정보공학부 박사과정
※관심분야 : 차량이동통신, 네트워크보안, 대용량데이터전송, 센서 네트워크

조기환(Gi-Hwang Cho)

1985년 전남대학교 계산통계학과 학사
1987년 서울대학교 계산통계학과 석사
1996년 Newcastle대학교 전산학과 박사
1987년 9월 ~ 1997년 8월 한국전자통신연구원 선임연구원
1997년 9월 ~ 1999년 2월 목포대학교 컴퓨터과학과 전임강사
1999년 3월 ~ 현재 전북대학교 컴퓨터공학부 교수
※관심분야 : 이동컴퓨팅, 컴퓨터통신, 분산처리시스템, 무선보안, 무선네트워크