지능형 차량 이동네트워크 환경에서 차량과 통신설비간의 효율적인 인증프로토콜

An Efficient Authentication Protocol between Vehicle and Communication Infrastructure for Intelligent Vehicular Networks

황 병 희*, 김 범 한*, 이 동 훈*
(Byung-Hee Hwang, Bum Han Kim, Dong Hoon Lee)

Abstract : Vehicular Ad hoc Networks have attracted extensive attentions in recent years for their promises in improving safety and enabling other value-added services. Security and privacy are two integrated issues in the deployment of vehicular networks. Privacy-preserving authentication is a key technique in addressing these two issues. We propose a hash chain based authentication protocol that preserves the user privacy . We show that the our scheme can efficiently authenticate users. Name of Our protocol is

Keywords: VANET, Authentication

I. 서론

안전한 차량 운전과 교통 정체를 줄이기 위한 방법으로 VANET(Vehicle Ad-hoc Network)에 대한 관심이 증가 되고 있다. VANET은 MANET의 하나로써 차량과 차량(V2V : Vehicle to Vehicle), 차량과 인프라스트럭쳐 사이의 통신 (V2I : Vehicle to Infrastructure) 을 통하여 지역 정보 수집과 분배, 데이터 이동, 정보 분배 등을 목적으로 한다, VANET은 주로 OBU(On-Board Units)과 RSU(Road-Side Units)을 포함한다. OBU는 차량에 설치 돼서 차량에게 무선 통신 능력을 제공하고, RSU는 도로상에 분포되어서 그들의 범위내의 차량에게 무선 서비스를 제공한다.

V2I 통신 환경에서 차량은 OBU를 이용하여 RSU를 통하여 인프라스트럭쳐와 통신을 한다. 이러한 환경에서 차량과 인프라스트럭쳐 사이에 안전한 무선 통신을 하기 위해서는 신원 확인을 위한 인증이 필요하다. 또한 통신 메시지의 보호를 위하여 데이터 암호화가 필요하다. 마지막으로 차량의 프라이버시 보호를 위하여 차량의 위치와 아이디가 다른 차량이나 인프라스트럭쳐 내부에 알려져서는 안 된다. 즉, 익명성과 비연결성을 만족시켜야 한다. 하지만 사고나 범죄와 같은 일이 벌어졌을 경우 수사기관은 인프라스트럭쳐 내부 데이터의 도움을 받아 차량을 추적 할 수 있는 추적가능성이 필요하다. 마지막으로 차량의 이동속도가 빠르고 무선 통신 환경이므로 통신량과 연산량을 줄이는 것 또한 중요하다.

차량과 인프라스트럭쳐 사이의 인증 프로토콜에 중 익명성을 보장하는 프로토콜은 크게 두 가지로 나눌 수 있다. 하나는 공개키를 사용하는 방법으로 대표적인 프로토콜로 Sha 등이 제안한 그룹 기반 인증 프로토콜이 있다. 다른 하나는 랜덤키 이용하는 방법으로 Xi등이 제안한 대칭 랜덤 키 셋을 사용한 인증프로토콜이다. 그룹 기반 인증 프로토콜은 공개키 기반이기 때문에 연산 오버헤드가 크고, 대칭 랜덤 키 셋을 사용한 인증프로토콜은 OBU와 RSU가 인증 시 소유한 랜덤 키 셋 중 공유된 것을 이용한다. 이 방법은 키 저장을 위하여 많은 메모리를 요구하고 추적성을 제공하지 않는다. 또한 키가 폐기 되었을 경우 키를 따로 관리해야 하고, 일정 시간이 지난 후에는 키를 재분배해야 하는 문제도 존재한다.

이 논문에서 우리는 이러한 각 프로토콜의 단점을 보완하면서 인증프로토콜에 필요한 보안요구사항을 만족 시키는 지능형 차량 이동네트워크 환경에서 차량과 통신설비간의 효율적인 인증프로토콜을 제안한다. 제안하는 프로토콜은 해쉬함수를 사용하여 효율성을 높이면서도 차량의 익명성을 보장한다. 또한 타임 메모리 트레이드 오프를 이용하여 메모리 사용을 줄였다.

2장에서는 보안요구사항에 대하여 서술하고, 3장에서는 시스템 모델에 대하여 서술한다. 4장에서는 제안하는 프로토콜에 대하여 설명하고 5장에서는 제안하는 프로토콜의 안전성을 분석한다. 마지막으로 6장에서는 결론을 내린다.

II. 보안요구사항

1. 가용성

가용성은 특정 공격에 의해서 네트워크가 마비되지 말아야 한다는 것을 의미한다. 이는 도스 공격이나 전파방해와 같은 공격은 메시지를 손실 시키거나 네트워크를 마비 시킬 수 있다. 따라서 네트워크는 이러한 공격에 강해야 한다.

2. 기밀성

도청을 통하여 차량의 아이디와 같은 차량에 관련된 정보를 얻을 수 있다. 무선 환경에서의 도청은 유선 환경에서보다 쉬우므로 기밀성을 유지하여야 한다.

3. 비연결성

비연결성은 이웃 차량이나 베이스스테이션이 특정한 메시지로부터 특정 차량의 이동경로를 파악할 수 없어야 한다는 것을 의미한다. 비연결성은 사용자의 위치에 대한 프라이버

* 책임저자(Corresponding Author)
황병희 : 고려대학교 정보경영공학전문대학원
(lovessyar@korea.ac.kr)
"본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (IITA-2008-(C1090-0801-0025))

시를 제공하기 위한 성질이다.

4. 인증

프로토콜에서 각 객체는 적법한 메시지에 대해서만 응답해야 하므로 메시지를 보내는 주체에 대한 인증이 요구된다.

5. 익명성

익명성은 이웃 차량이나 RSU 가 특정 메시지로부터 메시지 근원 차량의 아이디 정보를 알 수 없어야 한다는 것을 의미한다. 사용자의 아이디 노출에 대한 프라이버시를 제공하기 위한 성질이다.

6. 추적성

추적성은 특정 차량에 대해서 사고나 범죄가 발생했을 경우에만 수사기관에서는 메시지의 근원을 추적할 수 있어야 하며, 차량의 아이디를 알 수 있어야 한다.

III. 시스템 모델

1. 인가 서버(Authorization Server)

신뢰 기관에서 관리하는 서버로서 RSU를 관리하고 차량 등록 및 인증 서버를 이용하여 차량의 통신 인가를 한다. RSU, 차량 등록 및 인증 서버와 유선으로 연결되어 있고 각각 대칭키를 공유하고 있다.

2. RSU(RoadSide Unit)

차량의 통신을 돕기 위한 통신 설비로 도로에 일정한 간격으로 고정되어 있다. 인가 서버와 유선으로 연결되고 대칭키를 공유하고 있다.

3. 차량

OBU을 이용하여 무선통신을 하고 안전한 저장장치(tamper-proof device)을 가지고 있다.

4. 차량 등록 및 인증 서버

차량이 판매되면 차량에 고유한 아이디와 마스터 키를 부여하고 차량 내부의 안전한 저장장치에 이를 저장한다. 인가 서버와 유선으로 연결되어 있고 대칭키를 공유한다.

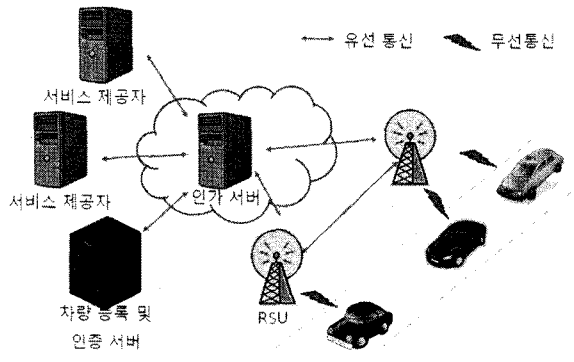

그림 1 시스템 모델.

Fig. 1. System Model.

5. 서비스 제공자 서버

인증된 차량에게 도로정보나 교통 정보 같은 콘텐츠를 제공하는 서버이다.

IV. 제안하는 프로토콜

본 절에서는 프로토콜을 표기하는데 사용할 표기 법을 정의하고, 지능형 차량 이동네트워크 환경에서 차량과 통신설비간의 효율적인 인증프로토콜을 제안한다. 제안하는 프로토콜은 차량과 RSU사이에 상호 인증을 지원하고 차량의 프라이버시를 보호하는데 목적이 있다.

1. 표기법

VID: 차량 등록 시 차량 등록 기관에서 발급하는 차량의 고유한 아이디

$E_K(M)$: 키를 K로 사용하는 대칭키 암호화 함수

$D_K(M)$: 키를 K로 사용하는 대칭키 복호화 함수

KEK : 키 암호화용 키, 차량과 RSU 사이에 공유된 세션 키를 설립하기 위해 사용됨.

MK: 차량과 키 분배센터 사이에 공유된 마스터 키

RID(j): j번째 Road-Side Unit의 아이디

PID: 차량의 가상 아이디,

$G(\bullet)$: 충돌방지 일방향 해쉬함수(H와는 다른 해쉬함수)

$H(\bullet)$: 충돌방지 일방향 해쉬함수

$H^t(M)$: 메시지 M을 해쉬함수 H로 t번 해쉬한 값,

T: 타임 스템프

2. 차량등록 단계

차량이 출고되면 차량은 차량 등록 및 인증 서버에 등록한다. 차량이 등록하게 되면 차량 등록 및 인증 서버는 차량에게 아이디 VID와 마스터 키 MS, 키 사용 횟수 t를 차량의 안전한 저장장치에 저장한다. 아이디와 마스터 키를 입력 받은 차량은 마스터 키를 t번 해쉬하여 저장한다.

3. 익명의 차량인증 단계

차량이 도로를 이용하면서 도로에 설치된 RSU와 인증을 하여 서비스 제공자 서버로부터 콘테츠를 제공 받아서 이용하는 단계이다.

Step 1 : 차량은 RSU에게 PID와 $E_{KEK}(PID,T)$을 전송한다. PID는 $G(G(H^t(MS))||t)$이고 KEK는 $G(H^t(MS))$이다. 차량은 t를 t-1로 대체한다.

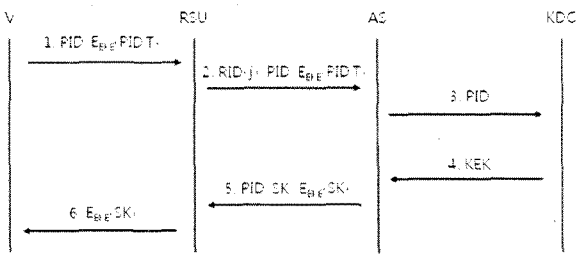

그림 2 익명의 차량인증 단계.

Fig. 2. Pseudonym Vehicles Authentication Phrase.

Step 2 : 차량 V에게 메시지를 받은 RSU는 자신의 아이디 RID(j)와 차량에게 받은 메시지 PID와 $E_{KEK}(PID,T)$를 인가 서버에게 전달한다.

Step 3 : RSU에게 RID(j), PID, $E_{KEK}(PID,T)$를 전달 받은 인가서버는 저장 받은 내용을 저장하고 PID를 차량 등록 및 인증 서버에게 전달한다.

Step 4 : 인가 서버에게 PID를 전달받은 차량 등록 및 인가서버는 PID가 등록된 차량의 것인지 확인하고, 등록된 차량의 것이라면 KEK를 인가 서버에게 전송하고 자신의 데이터베이스에 저장되어 있는 PID와 KEK를 각각 $G(G(H^{t-1}(MS))\|t-1)$이고 KEK는 $G(H^{t-1}(MS))$로 대체한다.

Step 5 : 차량 등록 및 인증 서버에게 KEK를 전달받은 인가서버는 KEK를 이용하여 $D_{KEK}(E_{KEK}(PID,T))$를 계산하여서 PID가 존재 하는지 확인한다. 존재한다면 랜덤하게 SK를 선택하고, $E_{KEK}(SK)$를 계산한다. 그리고 RSU에게 PID, SK, $E_{KEK}(SK)$를 전송한다.

Step 6 : 인가 서버에게 PID, SK, $E_{KEK}(SK)$를 전송 받은 RSU는 PID, SK를 저장하고 차량에게 $E_{KEK}(SK)$를 전송한다.

Step 7 : RSU에게 $E_{KEK}(SK)$를 전달받은 차량은 KEK를 이용하여 $D_{KEK}(E_{KEK}(SK))$를 계산한다. 차량은 SK를 알게 된다. 차량과 RSU 사이에 세션키 SK가 공유 되었으므로 공유된 키를 이용하여 데이터를 암호화하여 전송한다.

4. 추적 단계

교통 사고가 발생하거나 차량을 이용한 범죄가 발생한 경우 차량의 경로 추적이나 위치 추적이 필요하다. 이러한 경우 수사기관은 인가 서버와 차량 등록 및 인증 서버의 도움을 받아서 추적이 가능하다. 먼저 수사기관이 추적하고자 하는 차량의 VID를 알고 잇는 경우 차량 등록 및 인가 서버에게 요청하여 VID가 사용한 PID를 획득한다. 그 후 인가서버에게 획득한 PID들이 이용한 RSU의 정보를 확인하면 VID의 이동 경로를 파악할 수 있다.

V. 제안하는 프로토콜의 안전성 분석

1. 가용성

해쉬함수를 사용하여 PID 와 KEK 를 만들기 때문에 PID와 KEK 를 생성하는데 걸리는 시간이 매우 짧다. 또한 암호화 방식도 대칭키 암호화 방식만 사용하므로 암복호화에 걸리는 시간이 매우 짧다. 따라서 인증에 소요되는 전체 시간이 짧아서 효율적이다. 따라서 제안하는 프로토콜은 가용성이 뛰어나다.

2. 기밀성

메시지를 도청하더라도 공격자가 얻을 수 있는 정보는 차량의 가상아이디인 PID 뿐이다. 하지만 PID 는 매번 인증 시마다 변경되기 때문에 차량에 대하여 정보를 제공하지 않는다. PID 를 제외한 모든 정보는 대칭키 암호화 방식을 통하여 암호화되어 전달된다, 안전한 대칭키 암호를 사용하기 때문에 키를 모르고서는 내용을 알 수가 없다. 따라서 제안하는 프로토콜은 기밀성을 만족한다.

3. 비연결성

차량은 인증을 할 경우 PID 만을 자신의 식별자로 사용 한다. 하지만 PID 는 매번 인증 시마다 변경되기 때문에 각 인증 사이의 관계를 다른 차량이나 RSU 가 알 수 없다. 따라서 제안하는 프로토콜은 비연결성을 만족 시킨다.

4. 인증

각 차량은 PID 를 이용하여 자신을 나타내고 차량 등록 및 인증 서버와 차량의 동기화에 의하여 KEK 를 알 수 있다. 만약 거짓으로 PID 를 만든다면 PID 가 데이터 베이스에 있을 확률이 적고, 있다 하더라도 KEK 까지 일치할 수는 없다. 따라서 제안하는 프로토콜은 인증을 만족한다.

5. 익명성

제안하는 프로토콜은 VID 의 노출 없이 PID 만을 사용하여 통신한다. 그러므로 통신내용을 통하여 VID 를 알아 낼 수 없다. 따라서 제안하는 프로토콜은 익명성을 보장한다.

6. 추적성

제안하는 프로토콜은 사고가 발생한 경우 인가 서버와 차량 등록 및 인증 서버가 정보를 공유하면 차량의 이동 경로를 파악할 수 있다. 따라서 제안하는 프로토콜은 추적성을 만족 시킨다.

VI. 결론

우리는 지능형 차량 이동네트워크 환경에서 차량과 통신 설비간의 효율적인 인증 프로토콜을 제안하였다. 제안하는 프로토콜은 가용성, 기밀성, 비연결성, 인증, 추적성을 만족 시킨다. 따라서 제안하는 프로토콜은 지능형 차량 이동네트워크 환경에 사용하기에 적합한 프로토콜이다.

참고문헌

[1] B. Parno, A. Aziz and J-P. Hubaux, "Efficient Secure Aggregation in VANETs", *VANET*, September, 2006.

[2] C. Meadows, "A formal framework and evaluation method for network denial of service", *In 12th IEEE Computer Security Foundations Workshop*, p.4-13, June, 1999.

[3] D. Otway and O. Rees, "Efficient and timely mutual authentication", *ACM Operating Systems Review*, January, 1987.

[4] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks", *In Proc, of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, Sept, 2005.

[5] K. Sha, Y. Xi, W. Shi, L. Schwiebert and T. Zhang, "Adaptive Privacy-Preserving Authentication in Vehicular Networks", *In Proc. of the International Workshop on Vehicle Communication and Applications*, Oct, 2006.

[6] M. Raya and J-P. Hubaux, "Security Aspects of Inter-vehicle Communications", *STRC*, May, 2005.

[7] M. Mauve, J. Widmer and H. Hartenstein, "A Survey on Posi-

tion-Based Routing in Mobile Ad Hoc Networks", *IEEE Network*, 2001.

[8] P. Syverson, "A taxonomy of replay attacks", *In 7th IEEE Computer Security Foundations Workshop*, p.187-191, June, 1994.

[9] T. Aura and P. Nikander, "StateLess connections", *Information and Computer Secrity, First International Conference*, p.87-97, 1997.

[10] T. Mak, K. Laberteaux and R.Sengupta, "A multi-channel vanet providing concurrent safety and commercial services", in *in Proc. of the 2nd ACM international workshop on Vehicular ad hocnetworks*, Sept, 2005. [6]

[11] J. Choi, M. Jakobsson and S. Wetzel, "Balancing auditability and privacy in vehicular networks", *In Proceedings of the 1st ACM international workshop on Quality of Service and Security in Wireless and Mobile Networks*, Oct, 2005.

[12] W. Mao and C. Boyd, "On the use of encryption in cryptographic protocols" *Codes and Ciphers - Cryptography and Coding IV*, p.251-262, 1995.

[13] Y. Xi, K. Sha, W. Shi and L. Schwiebert, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks", *Autonomous Decentralized Systems, ISADS'07*, March, 2007.