공학석사 학위논문

VANET에서 멀티-홉 통신에 적합한 인증된 키 일치 프로토콜

2009년 8월

부경대학교 대학원

정 보 보 호 학 협 동 과 정

고 인 제

공학석사 학위논문

VANET에서 멀티-홉 통신에 적합한 인증된 키 일치 프로토콜

지도교수 이 경 현

이 논문을 공학석사 학위논문으로 제출함.

2009년 8월

부경대학교 대 학 원

정 보 보 호 학 협 동 과 정

고 인 제

고인제의 공학석사 학위논문을 인준함.

2009년 8월 26일

주　심　이학박사　조 성 진　(인)

위　원　공학박사　김 창 수　(인)

위　원　이학박사　이 경 현　(인)

<차 례>

<표 차례>

<그림 차례>

An Authenticated Key Agreement Protocol
suitable for Multi-hop Communication in VANET

In Je Ko

Interdisciplinary Program of Information Security
The Graduate School
Pukyong National University

Abstract

VANET (Vehicular ad hoc network) is a next-generation industry that combines vehicle and IT, and provides optimal driving environment by enhancing convenience and safety of drivers through mutual reaction of automotive sensors and electronic devices in an intelligent and organic manner. Subsequently, the potential drivers under the VANET environment is regarded to request intimate communication service among vehicles, as well as purchasing and sharing various multimedia contents. In addition, the acceleration of vehicles in road conditions such as expressways will eventuate in extending the distance among vehicles on road. The drivers in such circumstances are expected to frequently ask for not only single-hop communication, but also multi-hop communication service among the vehicles. According to such a tendency, Li et al. proposed an authenticated key agreement protocol considering the multi-hop communication environment among vehicles that utilize one-way hash chain and non-interactive public key protocol

scheme. However, the previously proposed protocol has group key's backward security of group key problems and compromised RSU problems due to the unique feature of one-way hash chain. Therefore, this thesis is aimed at deducing the security vulnerabilities of the existing protocol, and apply complements to propose an authenticated key agreement protocol suitable for multi-hop communication environments in VANET.

Ⅰ. 서 론

1. 연구 배경

VANET(Vehicular ad hoc network)은 고도화된 자동차 산업과 함께 첨단 IT기술과 차량통신이 융합한 네트워크 통신으로, 지능형 차량과 함께 신 융합 개념의 유비쿼터스 환경에서 새로운 블루오션으로 주목받고 있다.

최근 자동차의 성능 및 기술이 발전되면서 다양한 기술의 접목으로, 운전자의 편의성과 안전성, 엔터테인먼트의 서비스 지원여부가 이슈화 되었다. 또한, 첨단 IT기술이 접목된 보다 나은 서비스의 요구가 급증하면서 다양한 응용분야에서의 개발이 요구 될 뿐만 아니라, 보안적 측면 역시 중요한 블루칩으로 떠오르면서 향후 지속적인 연구 및 개발이 요구되고 있다.

VANET의 통신환경에서 전자통신의 비약적인 성장의 결과로 무선통신 및 위성위치확인시스템(GPS) 기술을 활용한 텔레매틱스(Telematics)[1]는 차량 정보 관리, 원격/헬프 서비스의 제공 등 실제 적용되어 산업의 전 분야의 효율성이 극대화되면서 고도성장의 기반이 되고 있다. 또한 위치 기반 서비스(Location Based Service)[2]의 이용이 확대되면서 실시간 교통정보나 위치추적을 통한 길안내와 같은 서비스가 실제 생활에서 필수적인 요소로 자리 잡고 있다.

이러한 고도의 성장과 함께 친환경 교통시스템 구축의 필요성을 느끼게 되면서 지능형 교통 시스템(Intelligent Transportation System)[3-6]은 세계 각 국 뿐만 아니라 국내에서도 활발한 연구와 더불어 실제 교통시스템에 적용하고 있으며, 새로운 부가가치를 얻을 수 있을 뿐만 아니라 잠재시

장이 매우 클 것으로 기대되고 있다 [1].

이러한 고부가가치의 첨단 IT 신기술을 기반으로 최근 진행 중인 스마트 하이웨이[7]는 친환경적이고 쾌적한 도로환경으로 차량의 이동성, 편의성, 안전성을 목표로 개발 중인 차세대 도로이다. 향후, 이러한 도로환경 조성으로 무인운전주행이 가능해지고, 이동속도의 증가로 주요 거점 도시들의 산업의 경제적 파급효과가 기대된다.

스마트 하이웨이와 같은 쾌적한 도로환경에서 차량의 진행속도가 최대시속 160km/h로 고속화되면서 다수의 차량 또는 원거리의 차량과 통신하기 위해 단일-홉에서 멀티-홉 통신으로 변화하는 추세를 보이고 있으며, 이에 따라 자동차의 센서 및 전자장치가 지능적·유기적으로 상호작용하여 운전자의 안전 및 편의성을 고려한 최적의 운전환경을 제공한다.

이와 함께 지능형 교통시스템[3-6]은 전자통신의 첨단기술을 교통에 실제 적용하여 운전자의 안전성과 편의성을 높이고 있다. 또한, 위치 기반 서비스를 활용한 차량 내에서 내비게이션, PDA 등 모바일 기기들의 활용도가 높아지면서 모바일 단말기들을 이용한 주변지역 및 지리정보 검색, 멀티미디어 다운로드 등 다양한 컨텐츠의 서비스 이용이 확대되고 있다.

이렇듯, 첨단화 교통시스템과 지능형 차량의 발전과 함께 새로운 브랜드 가치로서 도약한 교통 환경은 차량의 증가 및 고속화 추세에 대응하여 실제 교통 환경에 적합한 다양한 형태의 디지털 기반시설과 융합함으로서 최적의 환경을 제공한다 [8].

결과적으로 운전자들의 차량간 교통정보 메시지 전송뿐만 아니라, 다양한 멀티미디어 컨텐츠 구매·공유 및 차량간 기밀통신 서비스가 급증할 것으로 사료되며 이후 차량간 유용한 정보 및 데이터의 교환 또는 공유를 위한 그룹통신의 이용이 확대될 것으로 기대되면서 VANET의 보안적인 측면[9,10]에서 안전한 차량간 통신을 보호하기 위한 보안통신의 중요성이 확

대되고 있다.

2. 연구 범위 및 목표

최근 연구되고 있는 멀티-홉 기반 커뮤니티 네트워크에서는 이러한 변화의 필요성을 강조하고 있으며, 이로 인해 상호간 인증 및 기밀통신을 위한 세션키 교환은 매우 중요한 이슈가 되고 있다 [11]. 상기 언급한 상황을 고려한 인증 및 안전한 통신을 위한 기반 기술로, 2008년에 Li외 저자들은 일방향 해쉬 체인과 신원기반 키 일치 기법[12]을 이용하여 차량간 멀티-홉 통신환경을 고려한 인증된 키 일치 프로토콜[8]을 제안하였다.

그러나, Li 등 저자들이 제안한 프로토콜은 일방향 해쉬 체인의 고유한 특성만을 사용하여 두 가지의 보안 취약성을 가지게 되었다. 즉, 특정 시간 이후에 진입한 차량이 신뢰기관으로부터 수신한 그룹키를 악용하여 이전에 그룹키를 계산할 수 있는 문제점과 RSU(Road Side Unit)가 손상되었을 경우에 시스템 전체가 붕괴될 수 있는 보안 취약성을 가진다. 따라서 본 논문에서는 변형된 일방향 해쉬 체인을 이용하여 기 제안된 키 일치 프로토콜[8]의 보안 취약성을 해결한 VANET에서 멀티-홉 통신에 적합한 인증된 키 일치 프로토콜을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 제안 시스템의 설계를 위한 기반기술인 신원기반 키 일치기법과 일방향 해쉬 체인을 소개한 후, 기 제안된 VANET에서 인증된 키 일치 프로토콜을 소개한다. 3장에서는 제안 시스템의 배경 기술로 차량 네트워크 및 무선통신 기술과 하드웨어를 소개하고 제안 프로토콜에서의 요구사항 및 구성요소의 소개한다. 4장에서는 기 제안된 프로토콜의 보안적 문제점을 해결함과 동시에 VANET에서 멀

티-홉 통신에 적합한 새로운 인증된 키 일치 프로토콜을 제안한 후, 안전성 및 보안 요구사항을 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

본 장에서는 제안하는 프로토콜 설계에 필요한 기반기술로 신원기반 키 일치 기법과 일방향 해쉬 체인을 소개하며, Li 등이 제안한 VANET에서 인증된 키 일치 프로토콜과 보안 취약성을 도출한다.

1. 신원기반 키 일치 기법

Maurer and Yacobi의 신원기반 키 일치기법[12]은 아래 그림 1과 같이 신뢰기관에 사전에 등록한 사용자의 신원정보 (ID, Identity)와 신뢰기관의 비밀키를 이용하여 사용자의 신원정보에 대응하는 비밀키를 생성하여 분배하는 방법으로서 기법의 안전성은 소인수 분해 문제의 어려움에 기반하고 있다.

<그림 1> 신원기반 키 일치 기법

가. 설정 단계

최초 시스템 설정단계에서 신뢰기관은 공통의 원시원소가 존재하기 위해 각 $(p_j-1)/2$가 홀수이며 각 $(p_j-1)/2$들이 서로소 관계인 소수 p_1, p_2, p_3,

p_4를 선택하고, $N = p_1 \cdot p_2 \cdot p_3 \cdot p_4$을 계산한다. 이후, 신뢰기관은 각 사용자들에게 개인키를 할당하기 위해 비밀키 $mk \in Z^*_{\phi(N)}$을 선택한다. 여기서, ϕ는 오일러 함수이다.

신뢰기관의 비밀키 및 시스템변수는 다음과 같다.

⑴ 신뢰기관의 비밀키 : p_1, p_2, p_3, p_4 그리고 비밀키 mk

⑵ 신뢰기관의 공개키 : N, g.

신뢰기관은 자신의 비밀키를 이용하여 사용자 U_i에 대한 비밀키 s_i를 아래와 같이 생성한 후, 사용자 U_i에게 안전한 채널을 통하여 전송한다.

$$s_i = mk \cdot \log_g(ID_i^2) (\mathrm{mod}\, \phi(N))$$

여기서, g는 $GF(p_j)$의 원시원소이다$(1 \le j \le 4)$.

나. 세션키 생성 단계

임의의 사용자 U_i와 U_j의 공통키 K_{ij} 설정은 다음과 같다.

$$K_{ij} \equiv ((ID_j)^2)^{s_i} \equiv (g^{vs_j})^{s_i} \equiv (g^{vs_i})^{s_j} \equiv ((ID_i)^2)^{s_j} (\mathrm{mod}\, N)$$

여기서, $v \equiv (mk)^{-1} (\mathrm{mod}\, \phi(N))$이다.

따라서, 각 사용자들은 자신의 비밀키와 상대방의 신원정보를 공통키를 생성하기 때문에, 상호간 통신 없이 공통의 세션키를 생성할 수 있다.

2. 일방향 해쉬 체인

일방향 해쉬 체인은 중요한 암호학적 기반기술[13]로서, 임의의 x_n을 시작 값으로 n번의 해쉬 함수를 반복적으로 사용하여 생성되는 연속되는 값 $(x_n, \cdots, x_0)$들의 집합으로 나타낸다. 시작 값을 제외한 모든 해쉬 값들을 SHA-1과 같은 암호학적 해쉬 함수 $h: \{0,1\}^* \rightarrow \{0,1\}^l$를 이용하여 나타내면 다음과 같다.

$$x_i = h(x_{i+1}),\ (0 \leq i \leq n-1)$$

그리고, 마지막 값인 $x_0 = h^n(x_n)$은 일방향 해쉬 체인의 루트(Root)라고 정의된다. 그림 2는 크기가 n인 일방향 해쉬 체인을 나타낸다.

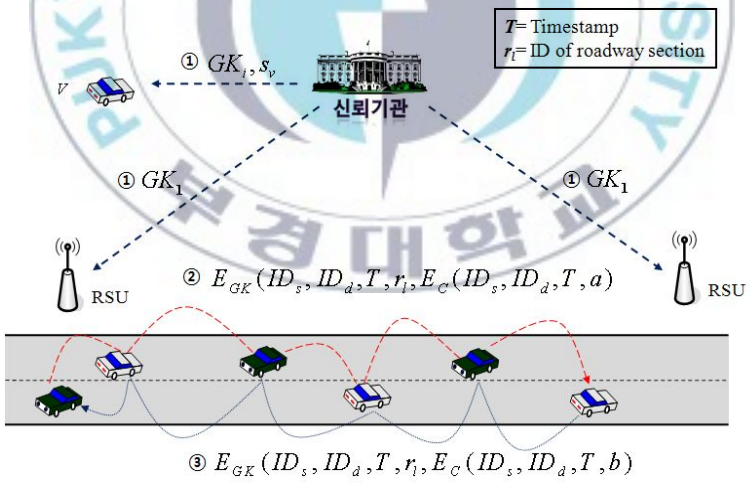
<그림 2> 일방향 해쉬 체인

일반적으로, 일방향 해쉬 체인은 x_n에서 x_0로 생성되지만, 역방향인 x_0에서부터 x_n으로 사용되어진다.

본 논문에는 일방향 해쉬 체인 기법을 이용하여 효율적인 그룹키 갱신 절차를 수행한다.

3. VANET에서 인증된 키 일치 프로토콜

VANET에서 운전자의 프라이버시 보호 및 차량간 안전한 데이터 공유 서비스 등을 위하여, 차량간 메시지 전송과정에서 기밀성과 무결성은 필수 부가결한 요소가 되었다. 이로 인하여, 최근에 Li 등은 이러한 보안 요구사항을 충족시키기 위하여 신원기반 키 일치 기법[12]을 이용하여 차량간 인증된 키 일치 프로토콜을 제안하였다[8]. 제안 프로토콜에서는 외부 공격자의 악의적인 도청을 방지하기 위하여, 일방향 해쉬 체인을 이용하여 각 차량에게 그룹키를 할당하고 RSU를 이용하여 주기적으로 그룹키를 갱신하였다. 다음 그림 3은 Li 등이 제안한 VANET에서 인증된 키 일치 프로토콜 과정을 보여주고 있으며 자세한 절차는 다음과 같다.



<그림 3> VANET에서 인증된 키 일치 프로토콜

- 설정단계에서 신뢰기관은 일방향 해쉬 체인을 이용하여 그룹키 목록

$(GK_1, GK_2, \cdots, GK_t)$을 생성 한다 (여기서, $GK_1 = h(sk), GK_i = h(GK_{i-1})$이며, sk는 신뢰기관의 비밀키임).

- 등록단계에서 신뢰기관은 정당한 차량들에게 현재 사용하고 있는 그룹키 GK_i를 발급하고, 모든 RSU에게는 GK_1을 발급한다. 또한, [8]의 개인키 설정 알고리즘을 이용하여 차량의 신원정보에 대한 개인키 VK를 각 차량에게 발급한다.

이후, 차량 s와 d간의 세션키 $K_{s,d}$를 생성하기 위한 프로토콜의 절차는 다음과 같다.

1) s는 태그 (tag) 및 비밀값 a와 최대 차량간 홉 수 hop를 선택하고, 신원기반 키 일치 기법을 이용하여 차량 d의 신원정보 ID_d 대한 공통키 C를 생성한다.
2) 공통키 C를 이용하여 a를 암호화 한 후, 구간 그룹키 GK_i를 이용하여 다음과 같이 메시지를 생성하여 브로드캐스트 형태로 전송한다.

$$GK_i \oplus (tag, ID_s, ID_d, hop, T, r_l, C \oplus (ID_s, ID_d, T, r_l, a))$$

여기서, T는 타임스탬프이고, r_l은 도로 구간명이다.

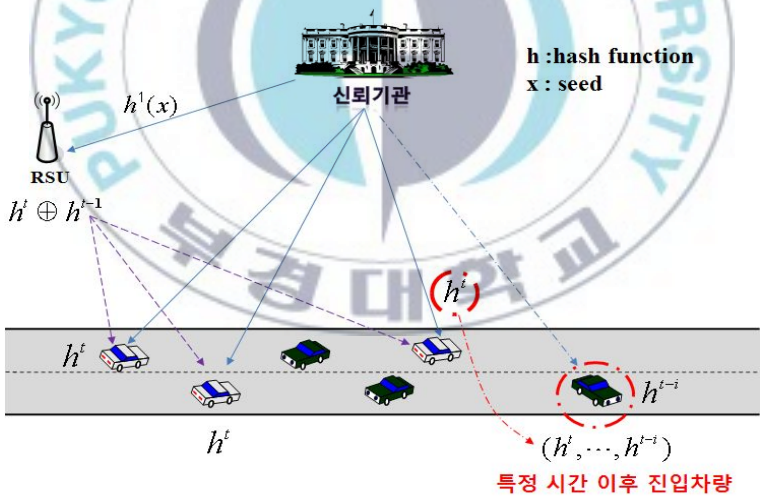
3) 메시지를 수신한 인증된 차량들은 그룹키를 이용하여 메시지를 복호화 한 후, hop이 1 이상이면 1을 감소시키고 그룹키로 재암호화하여 전송한다. 만약, hop이 0이면 수신된 메시지를 제거한다.
4) 메시지를 수신한 d는 ID_s를 이용하여 공통키 C를 생성하여 메시지의 무결성을 검증한다.
5) 무결성 검증을 통과하면, d는 비밀값 b를 생성하여 동일한 방법으로

s에게 b를 전송한다. 이후, s와 d는 i번째-세션키 $K_{s,d} = H(a||b||i)$를 설정한다.

6) 또한, RSU는 주기적으로 새로운 구간 그룹키 GK_{i+1}를 사용 중인 그룹키 GK_i로 암호화하여 브로드캐스트 형태로 전송한다. 메시지를 수신한 차량들은 GK_i을 이용하여 새로운 그룹키 GK_{i+1}를 생성한다.

$$\text{RSU} \rightarrow * : GK_i \oplus GK_{i+1}$$

하지만, 일방향 해쉬 체인의 특성으로 인하여 [8]에서 제안된 프로토콜은 다음의 그림 4와 같이 보안 취약성들을 가진다.



<그림 4> 프로토콜의 보안 취약성

[보안 취약성 1] 일방향 해쉬 체인 값들을 그룹키로 사용하기 때문에, 특정 시간 이후에 진입한 차량의 그룹키 GK_i로부터 이전에 사용한 그룹키 목록 $(GK_{i+1}, \cdots, GK_t)$를 계산할 수 있다. 즉, 새로 진입한 차량은 이

전에 사용된 그룹키들을 추출할 수 있다.

[보안 취약성 2] RSU를 통한 주기적인 그룹키 갱신을 위하여 신뢰기관은 RSU에게 해쉬 체인의 루트 값을 전송한다. 하지만, 일반적으로 RSU는 높은 안전성을 제공하지 못하기 때문에, RSU가 손상되었을 경우에 시스템 전체가 붕괴될 수 있다.

따라서, 본 논문에서는 기 제안된 차량간 인증된 키 일치 프로토콜[8]의 효율성을 유지하면서, 위와 같은 보안 취약성들을 해결한 새로운 키 일치 프로토콜을 설계한다.

Ⅲ. 시스템 모델

본 장에서는 제안 프로토콜의 기반이 되는 시스템 모델을 위한 네트워크 모델과 보안 요구사항을 알아보고, 제안 시스템 모델의 각 요소 및 가정 사항을 소개한다.

1. 네트워크 모델

VANET에서는 차량 네트워크 측면과 차량 하드웨어 측면으로 분류되며, 차량 외부망 네트워크는 크게 V2V와 V2I로 구분한다.

V2V(Vehicle-to-Vehicle)[3]은 차량간 무선통신에 의한 자율적인 형태의 차량 통신망 기술을 뜻하며, 차량 충돌 경고나 차량간 그룹 통신을 지원한다.

V2I(Vehicle-to-Infrastructure)[3]는 차량과 노변기지국간 통신에 의한 차량 통신 인프라 기술로 정의되며, 교통 및 안전정보 또는 엔터테인먼트 다운로드 등 여러 가지 기능을 지원한다.

무선 통신 기술에서는 IEEE 802.11p/P1609 WAVE[14-17]과 DSRC (Dedicated Short Range Communication)[18,19,20]가 주로 이용되며 IEEE 802.11p/P1609 WAVE의 경우 고속으로 주행하는 차량의 안전 정보 및 상업적 서비스를 제공하기 위해 미국에서 개발 및 표준화 구축이 진행 중인 차량 네트워크에서 핵심 무선전송 기술이다. 또한, DSRC의 경우는 5.9 GHz 주파수 대역의 무선 주파수 대역을 사용하며, RSU와의 근거리 통신에서 이용되어 전자 톨게이트 시스템에서 주로 적용되며, 수동형 DSRC와 능동형 DSRC로 형태로서 지능형 교통 시스템[3-6]을 지원하는

통신 기술이다.

차량 하드웨어에서는 차량에 탑재되는 차량용 단말기로서 OBU(On Board Unit)[20]가 있으며 RSU와의 통신 및 차량 간 통신과정에서 실제 멀티미디어 컨텐츠 및 교통정보를 저장 및 전송하는 역할을 담당한다.

2. 시스템 요구사항

시스템의 보안 요구사항은 다음과 같다.

- **차량 신뢰성 인증**

차량은 독립된 하나의 객체로서, 신뢰기관의 인증과정을 통해 신뢰된 차량으로 인증됨으로 메시지의 송·수신과정이 명확해야 한다.

- **메시지 인증 및 무결성**

통신과정에서 교류되는 모든 메시지 및 컨텐츠 등의 무결성이 보장되어야 하며, 악의적 행위 및 잘못된 정보제공의 결과로 발생되는 피해에 대한 명확한 책임규명을 전제로 발신지의 신원확인의 보장을 위한 메시지 인증이 필요하다.

- **메시지 기밀성**

차량간 통신상에 메시지 정보의 비밀유지가 이루어져야하며, 특정시간

이후 진입차량이 신뢰기관으로부터 발급받은 자신의 신원정보와 개인키 및 후 키를 악용하여 이전에 사용된 후 키 추출과 같은 기민행위와 악의적인 공격자의 불법 감청 및 도청 공격의 시도에 대해 정보의 누출되더라도 유용한 정보획득이 불가능함으로서 메시지에 대해 신뢰되지 않은 객체로부터 안전해야한다.

- **멀티-홉 통신에서의 상호인증**

차량간 통신에서는 차량의 안전과 관련된 정보교환 및 교차로의 진입과정, 차량 주변의 실시간 교통상황과 같은 정보와 멀티미디어 컨텐츠와 같은 엔터테인먼트 관련 고용량의 데이터를 공유하기 위해 단일-홉을 포함한 멀티-홉 차량과의 상호 인증된 통신이 요구된다.

- **인증된 동적 세션키 생성**

차량간 안전한 통신을 하기 위한 과정으로 차량간 키 교환이 요구되며, 상호간 키 교환과정에서 보다 높은 안전성을 보장하기 위한 인증된 동적 세션키 생성 및 교환이 요구된다.

3. 제안 시스템 모델 및 표기법

제안 시스템은 그림 5와 같이 신뢰기관, RSU 및 OBU로 구성되며, 각 객체들의 기능 및 역할은 다음과 같다.

<그림 5> 시스템 모델

- 신뢰기관 (Trusted Authority)

신뢰기관은 키 발행기관 및 인증기관의 역할을 담당하는 유일한 신뢰된 개체로서, 차량과 RSU 구성상에 안전한 통신을 위한 비밀키와 공개키를 발행하고 그룹키를 할당하여 안전한 시스템 구축을 제공한다.

- RSU (Road Side Unit)

RSU는 신뢰기관과 차량 사이의 가교역할을 하는 기반시설로서, 송·수신범위가 넓고 송·수신 강도가 일반 차량보다 강하여 신뢰기관으로부터 전송받은 메시지 및 인터넷을 통한 컨텐츠 다운로드, 엔터테인먼

트 서비스, 교통정보제공, 주변 지리 등의 위치서비스를 차량에게 제공한다. 또한, 주기적 그룹키 갱신을 통한 악의적 공격자의 불법행위로부터 차량의 안전을 보장해준다.

- OBU (On board Unit)

차량은 OBU(On Board Unit)을 장착한 지능형 차량으로 신뢰기관으로부터 차량의 독립된 ID를 부여받고, 공개키와 개인키를 할당받아 다른 객체로부터 통신 및 인증과정에서 정당한 차량으로 활용하게 된다. 또한, 차량 네트워크에서 무선통신을 이용하여 RSU로부터 다양한 컨텐츠 및 정보를 제공받고, 차량간 단일-홉 또는 멀티-홉 간 세션키를 통한 인증함으로서 정당한 차량과 안전한 통신이 가능하다.

제안 시스템은 아래와 같은 사항을 가정한다.

- 신뢰기관(TA)는 완전한 신뢰를 전제로 하는 기관으로 다른 객체들의 신원정보를 포함한 모든 정보를 보유하고 있으며, 차량과 RSU와 함께 시스템을 구성하는 것을 가정한다.
- RSU는 VANET환경을 구축하는 도로주변에 위치한 인프라 시설로서, 무선통신 및 라디오주파수를 통한 교통과 관련 정보를 브로드캐스트 형태로 전송한다.
- VANET의 통신 수단은 무선통신 채널로 사용하며 IEEE 802.11p와 같은 기술을 기반으로 운영 제공한다.
- 각 OBU들은 DSRC의 특성의 의하여 0.3초마다 교통정보와 같은 안전 관련 메시지를 브로드캐스트 형태로 전송한다.

- 신뢰기관은 RSU 및 OBU들이 악의적인 공격자에 의해 손상되는지 실시간 감시한다.

제안 프로토콜의 표기법은 다음과 같다.

<표 1> 표기법

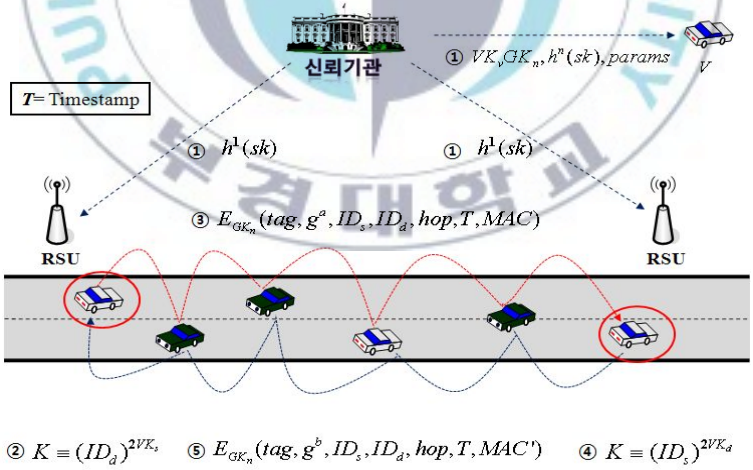
표 기	의 미
$params$	시스템 변수
g	Z_p^*의 생성자
ID_v	차량 v의 신원정보
VK_i	ID_i에 대한 비밀키
GK_i	특정 구간의 그룹키
sk, sk'	신뢰기관의 비밀키
$h(), f()$	암호학적 일방향 해쉬 알고리즘
$MAC_K()$	K에 대한 메시지 인증 코드
$E_K()$	대칭키 암호화 알고리즘

Ⅳ. 제안 프로토콜의 설계 및 분석

본 장에서는 VANET에서 상호인증 및 무결성을 제공하는 멀티-홉 통신에 적합한 인증된 키 일치 프로토콜을 제안한 후, 보안 요구사항을 분석한다.

1. 제안 프로토콜의 설계

제안 프로토콜은 다음 그림 6과 같이 설정, 그룹키 설정, 등록, 차량간 인증된 키 교환, 그룹키 갱신 단계로 구성되며 각 단계의 자세한 절차는 다음과 같다.



<그림 6> 제안 프로토콜

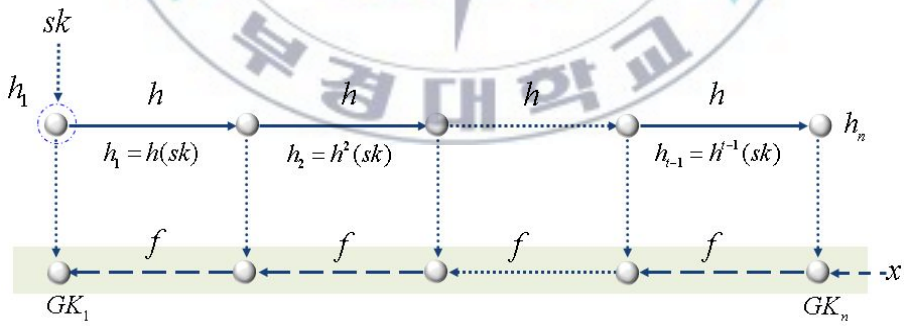
[설정] 신뢰기관은 임의의 비밀키 (sk, sk')를 선택하고, Diffie-Hellman

키 분배 기법[21]과 신원기반 키 일치 기법[12]을 이용하여 시스템 변수 $params$를 다음과 같이 설정한다.

$$params = (N, p, q, g)$$

여기서, 각 p_i는 임의의 4개의 소수들에 대하여 공통의 원시원소가 존재하기 위해 $(p_i - 1)/2$가 홀수이며 각 $(p_i - 1)/2$들이 서로소 관계인 소수들을 선택하고 $N = p_1 \cdot p_2 \cdot p_3 \cdot p_4$을 계산한다. q는 $GF(p_i)$ $(i = 1, 2, 3, 4)$의 원시원소이며 g는 Z_p^*의 생성자 (Generator)이다.

[그룹키 설정] 신뢰기관은 임의의 x를 선택하여, 비밀키 sk와 암호학적 해쉬 함수를 이용하여 아래 그림 7과 같이 그룹키 목록 $(GK_t, GK_{t-1}, \cdots, GK_1)$을 생성한다.



<그림 7> 그룹키 생성

$$\begin{cases} GK_t &= f(x, h^t(sk)) \\ GK_{t-1} &= f(GK_t, h^{t-1}(sk)) \\ \quad\vdots & \\ GK_1 &= f(GK_2, h(sk)) \end{cases}$$

$H=(h_1,h_2,\cdots,h_n)$는 일방향 해쉬 체인이며, H의 값들을 salt로 이용하여 그룹키 목록을 생성한다. 또한, GK_n이 그룹키의 시작 값이고, GK_1이 그룹키의 루트 값이다.

[등록] 신뢰기관은 신뢰된 차량 v에 대하여 차량의 신원정보 ID_v를 이용하여 차량의 비밀키 VK_v를 다음과 같이 생성한다.

$$VK_v = sk' \bullet \log_q(ID_v^2) \pmod{\phi(N)}$$

여기서, $\phi()$는 오일러 함수이다.

또한, 등록시점에서 사용하는 그룹키 GK_i 및 그룹키 갱신에 필요한 정보 $h^i(sk)$를 차량의 비밀키 및 시스템 변수와 함께 안전한 채널을 통하여 v에게 전송한다.

$$\text{신뢰기관} \Rightarrow v : VK_v, GK_i, h^i(sk), params$$

더불어, 신뢰기관은 주기적으로 효율적인 그룹키 갱신을 위하여 모든 RSU에게 $h(sk)$를 안전한 채널을 통하여 전송한다.

$$\text{신뢰기관} \Rightarrow \text{RSU} : h(sk)$$

[차량간 인증된 키 교환] 차량 s와 d의 안전한 통신을 위한 세션키 $K_{s,d}$를 생성하기 위하여, s는 임의의 tag와 a를 선택하고 $g^a \pmod p$를 계산한다.

이후, MAC 키로 사용할 $K \equiv (ID_d)^{2\,VK_s} \pmod N$를 계산하고, 구간 그룹키 GK_i를 이용하여 아래와 같이 메시지를 암호화 한다.

$$E_{GK_i}(tag, g^a, ID_s, ID_d, hop, T, MAC)$$

여기서, $MAC = MAC_K(g^a, ID_s, ID_d, T)$, T는 타임스템프(Timestamp)이다.

s는 암호화한 메시지를 브로트캐스트 형태로 전송한다. 메시지를 수신한 정당한 차량들은 GK_i를 이용하여 메시지를 복호화한 후 hop이 1 이상이면 1을 감소시키고 GK_i로 암호화하여 재전송한다. 만약, hop이 0이면 수신된 메시지를 제거한다.

d는 수신된 메시지를 복호화 한 후, MAC 키 $K \equiv (ID_s)^{2\,VK_d} \pmod N$를 생성하여 MAC 값을 검증한다. 검증을 통과하면, d는 난수 b를 생성하여 동일한 방법으로 s에게 g^b를 전송한다.

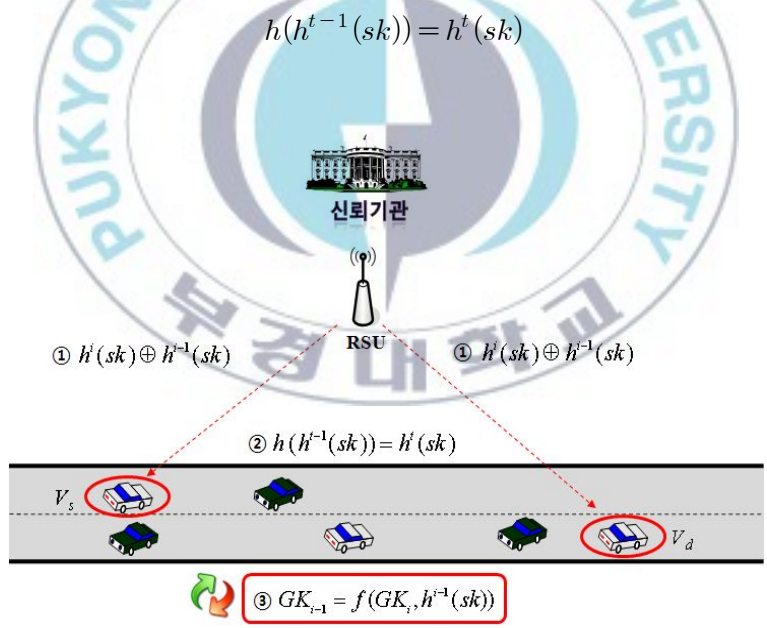
마지막으로, s는 g^b와 a를 이용하여 $g^{ab} \pmod p$를 계산하고, d는 g^a와 b를 이용하여 $g^{ab} \pmod p$를 계산한다. 이후, s와 d의 l번째-세션키는 $K_{s,d} = h(g^{ab} \| l)$로 설정한다.

[그룹키 갱신] 다음 그림 8은 제안 프로토콜에서 그룹키 갱신과정을 보

여주고 있으며, 자세한 절차는 다음과 같다. RSU는 주기적으로 기존 그룹키 GK_i를 GK_{i-1}로 갱신하기 위하여, 아래와 같이 메시지를 생성하여 브로트캐스트 형태로 전송한다.

$$\text{RSU} \rightarrow * : h^i(sk) \oplus h^{i-1}(sk)$$

이후, 정당한 차량들은 $h^i(sk)$을 이용하여 수신된 메시지에서 $h^{i-1}(sk)$를 추출하고, 일방향 해쉬 체인의 특성을 이용하여 수신된 $h^{i-1}(sk)$의 인증을 다음과 같이 수행한다.



<그림 8> 제안 프로토콜 그룹키 갱신

만약, 위의 식을 만족하면, 각 차량들은 새로운 그룹키 GK_{i-1}를 아래와 같이 설정한다.

$$GK_{i-1} = f(GK_i, h^{i-1}(sk))$$

2. 보안 요구사항 분석

- **차량 신뢰성 인증**

등록과정에서 신뢰기관으로부터 각 차량들은 자신의 신원정보에 관한 개인키 및 그룹키를 발급받기 때문에, 발급받은 키를 통해 정당한 차량으로서 그룹 통신 및 다양한 멀티미디어 컨텐츠의 활용이 가능해진다.

- **메시지 인증 및 무결성**

통신과정에서 전송되는 모든 메시지에 대해 차량 통신하기 위한 암호화과정에서 자신의 신원정보를 포함하여 발송하기 때문에, 이후 수신차량의 경우 정보제공자의 신원의 확인이 가능하여 책임규명의 부분의 보장이 가능하며 메시지 인증코드의 사용으로 메시지의 인증 및 무결성을 보장한다.

- **메시지 기밀성**

특정시간 이후 진입차량이 신뢰기관으로부터 발급받은 개인키 및 그룹키를 악용하여 이전에 사용된 그룹키 추출과 같은 기민행위와 악의적인 공격자의 불법 감청 및 도청 공격의 방지와 일방향 해쉬 체인과 차

량간 통신상의 기밀성을 유지하기 위하여 변형된 일방향 해쉬 체인을 사용하고 RSU의 주기적인 그룹키 갱신을 통해 차량간 통신상의 데이터 정보누출에 대한 안전성을 제공한다.

- **멀티-홉 차량간 상호인증**

차량간 상호인증을 위한 과정에서 최초 신원기반 키 일치기법을 사용하여 상호통신 없이 공통키를 생성하게 되고, MAC을 이용한 메시지 무결성 검증 후, 인증된 동적 세션키를 생성함으로서 멀티-홉 차량간 안전한 상호인증을 제공하게 된다.

3. 제안 프로토콜의 안전성 분석

[보안 취약성 1] 이전 사용된 그룹키 추출 문제

본 논문에서 제안한 프로토콜은 기존의 일방향 해쉬체인을 변형하여 보완한 형태의 구조로 그룹키 설정과정에서 정당한 차량들이 구간 그룹키 GK_i와 $h^i(sk)$를 획득하더라도 해쉬 알고리즘의 일방향성으로 인하여 GK_{i+1}을 계산할 수 없다. 따라서 새로 진입한 차량을 통한 이전 그룹키들의 추출이 불가능하다.

[보안 취약성 2] RSU의 손상경우 시스템 전체의 붕괴 위험성

제안 프로토콜에서는 Li 등이 제안한 프로토콜[8]과는 달리 RSU에게 자신의 비밀키를 제외한 정보가 제공되지 않기 때문에 이를 이용한 각 차량들이 그룹키를 갱신 및 차량의 비밀키$(h(sk),\cdots,h^t(sk))$를 획득하더라도 임의의 그룹키 GK_i를 계산할 수 없다. 그로인하여, RSU가 악의적인 공격자에 의하여 손상되더라도 시스템에 영향을 주지 않는다.

4. 제안 프로토콜의 효율성 분석

기 제안된 Li 등의 프로토콜[8]과 제안 프로토콜의 연산량 비교 결과는 다음의 표 2 와 같다.

<표 2> 제안 프로토콜과 Li 등의 프로토콜의 연산량 비교

	Li 등의 프로토콜[8]	제안 프로토콜
차량 s	$1T_{\exp}+2T_{AES}$	$2T_{\exp}+1T_{MAC}+1T_{AES}$
차량 i	$1T_{AES}$	$1T_{AES}$
차량 d	$1T_{\exp}+2T_{AES}$	$2T_{\exp}+1T_{MAC}+1T_{AES}$

- $T_{\exp}$: 모듈러 지수승 (Modular Exponentiation) 연산시간
- T_{AES} : 블록 암호 알고리즘 (AES, Advanced Encryption Standard) 연산시간
- T_{MAC} : 메시지 인증 코드 (MAC, Message Authentication Code) 연산시간

제안 프로토콜은 차량 간 상호통신에서 시스템의 안전성을 강화하기 위하여 암호학적 기법 적용하였기 때문에, 제안 프로토콜의 연산량은 기 제안된 프로토콜[8] 보다 다소 증가하였다. 하지만, 지수승 연산 및 MAC 연산은 충분한 컴퓨팅 파워를 가진 차량에서는 고려하지 않아도 되는 연산이므로, 제안 프로토콜은 기 제안된 프로토콜과 유사한 효율성을 가진다.

Ⅵ. 결 론

VANET은 고도로 성장한 자동차산업과 정보통신 및 첨단 IT기술과 함께 새로운 블루오션으로 각광받고 있으며, 국내를 포함한 세계전역에서 차세대 유비쿼터스 산업을 주도할 신 융합 기술개발이 활발히 진행되는 추세이다. 또한 차량과 IT기술의 결합으로 지능형 차량으로 발전되면서 이를 지원하는 기술 및 인프라 시설도 최적의 교통 환경을 제공하고 있다.

특히 운전자 편의성 추구 및 안전성 강화를 위한 다양한 서비스가 제공되면서 멀티-홉 차량간 통신의 요구가 점차 확대될 것으로 예상되며, 이러한 차량간 통신과정에서 교환 및 공유되는 교통정보, 멀티미디어 컨텐츠 데이터 및 메시지의 보호를 위한 상호인증 및 기밀통신을 위한 세션키 교환은 중요한 이슈로 부각되고 있다. 이러한 상황을 고려하여 Li 등은 일방향 해쉬 체인과 신원기반 키 일치 기법을 이용한 차량간 인증된 키 일치 기법을 소개하였다.

본 논문에서는 Li 등이 제안한 VANET에서 차량간 인증된 키 일치 프로토콜[8]의 보안적 취약성을 제시하고, 이를 해결하기 위한 새로운 인증된 키 일치 프로토콜을 제안하였다. 제안 프로토콜은 VANET에서 멀티-홉 통신에 적합한 인증된 키 일치 프로토콜로서, 차량간 키 교환 단계에서 Diffie-Hellman 키 교환 기법[21]과 MAC을 이용하여 2번의 암호화를 요구했던 프로토콜[8]보다 다소 적은 계산량을 요구한다. 결론적으로, 제안 프로토콜은 기 제안된 효율적인 키 일치 프로토콜[8]의 보안적 취약성을 해결하면서 유사한 효율성을 제공한다.

참 고 문 헌

[1] 박종흥, 이상락, 김은혜, “물류 산업의 텔레매틱스 기술 적용 방안 및 서비스 동향,” 전자통신 동향 분석 23권 4호, pp. 147-155, 2008.

[2] B. Sadoun and O. Al-Bayari “Location based services using geographical information systems,” Computer Communications, pp. 3154 - 3160, 2007.

[3] 오현서, 박종현, “차량통신 네트워크 기술동향,” 전자통신 동향 분석 23권 5호, pp. 49-55, 2008.

[4] J. Miller, “Vehicle-to-Vehicle-to-Infrastructure Intelligent Transportation System Architecture,” Intelligent Vehicles Symposium (IVS), pp. 715-720, 2008.

[5] L. Qi, “Research on Intelligent Transportation System Technologies and Applications,” Power Electronics and Intelligent Transportation System (PEITS), pp. 529-531, 2008.

[6] P. Mirchandani and F. Wang “RHODES to Intelligent Transportation Systems,” IEEE Intelligent Systems, Vol. 20, No. 1, pp. 10-15, 2005.

[7] Smart Highway, http://www.smarthighway.or.kr/.

[8] C. 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, No. 12, pp. 2803-2814, 2008.

[9] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular

Communications - Assumptions, Requirements, and Principles," Embedded Security in Cars (ESCAR), 2006.

[10] M. Raya and J.-P. Hubaux "The security of vehicular ad hoc networks," Security of Ad Hoc and Sensor Networks (SASN), pp. 11-21, 2005.

[11] 노효선, 정수환, "유비쿼터스 네트워크 환경에서 커뮤니티 멤버간 인증 및 세션키 교환 기법," 전자공학회 논문지 제 46권 TC편 제 2호, pp. 213-220, 2009.

[12] U. M. Maurer and Y. Yacobi "A non-interactive public-key distribution system," Designs, Codes and Cryptography, Vol. 9, Issue 3, pp. 305-316, 1996.

[13] C.-C. Lee, L.-H. Li, and M.-S. Hwang, "A remote user authentication scheme using hash function," ACM Operating Systems Review, 36(4), pp. 23-29, 2002.

[14] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," Vehicular Technology Conference (VTC), pp. 2036-2040, 2008.

[15] S. Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard," Vehicular Technology Conference (VTC), pp. 2199-2203, 2007.

[16] S.-Y. Wang, H.-L. Chao, K.-C. Liu, and T.-W. He, C.-C. Lin, C.-L. Chou, "Evaluating and improving the TCP/UDP performances of IEEE 802.11(p)/1609 networks," IEEE Symposium on Computers and Communications (ISCC), pp. 163-168, 2008.

[17] IEEE P1609.2 Version 1 - Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Massages. In development, 2006.

[18] C. Tchepnda, H. Moustafa, H. Labiod, and G. Bourdon, “Prioritizing and Enhancing Vehicular Networks Authentication Process Using DSRC Channels Diversity,” Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 429-434, 2008.

[19] D. Jiang, V. Taliwal, A. Meier, W.-L. Holfelder, and D. AG, “Design of 5.9GHz DSRC-based Vehicular Safety Communication,” In Magazine of IEEE Wireless Communications IVC Specials, pp. 36-43, 2006.

[20] W.-Y. Shieh, W.-H. Lee, S.-L. Tung, B.-S. Jeng, and C.-H. Liu, “Analysis of the Optimum Configuration of Roadside Units and Onboard Units in Dedicated Short-Range Communication Systems,” IEEE Transactions on Intelligent Transportation Systems, 7(4) pp. 565-571, 2006.

[21] W. Diffie and M.E. Hellman “New Directions in Cryptography,” IEEE Transactions on Information Theory, Vol. IT-22, pp. 644-654, 1976.