논문 20-45-06-01 The Journal of Korean Institute of Communications and Information Sciences '20-06 Vol.45 No.06
https://doi.org/10.7840/kics.2020.45.6.941

VANET을 위한 프라이버시가 제공된 인증 프로토콜

김 현 성◆°

Privacy Preserving Authentication Protocol Over VANET

Hyunsung Kim◆°

요 약

차량애드혹망 (Vehicular adhoc network, VANET) 보안 및 프라이버시를 위한 다양한 연구들이 진행되었다. 현재 관련 연구들에는 여전히 통신과 연산의 오버헤드 및 보안과 프라이버시 문제 등 해결해야 할 이슈들이 많다. 본 논문에서는 Ying과 Nayak이 제안한 차량애드혹망을 위한 인증 프로토콜이 서비스 거부 공격에 취약하고 익명성을 제공하지 못하는 문제가 있음을 보인다. 또한, Ying과 Nayak의 인증 프로토콜에 존재하는 문제들을 해결하기 위한 차량애드혹망을 위한 프라이버시가 제공된 인증 프로토콜을 제안한다. 본 논문에서 제안한 인증 프로토콜은 서버의 사용자 검증 테이블을 제거함으로서 높은 수준의 프라이버시와 보안을 동시에 제공한다. 상호 인증을 검증하기 위해서 정형화된 보안 검증 도구인 ProVerif를 활용한다. 특히, 본 논문에서 제안한 프로토콜은 오프라인 패스워드 추측 공격, 스마트 카드 분실 공격, 가장공격 등과 같이 공격들을 저항 할 수 있고 익명성과 비연결성을 제공한다.

키워드 : 인증프로토콜, 프라이버시, 익명성, 비연결성, 서비스거부공격
Key Words : authentication protocol, privacy, anonymity, unlinkability, denial of service attack

ABSTRACT

Various studies have been conducted for VANET (Vehicular adhoc network) security and privacy. There are still many issues to be solved in the previous researches, such as the overhead of communication and computation, and security and privacy issues. In this paper, we withdraw two weaknesses in Ying and Nayak's authentication protocol over VANET, which are weaknesses focused on the denial of service attack and the anonymity exposure attack. In addition, we propose a privacy preserving authentication protocol for VANET to solve the problems in Ying and Nayak's authentication protocol. The proposed protocol provides a high level of privacy and security at the same time by removing the usage of verifier table in the trusted server. To validate mutual authentication, we use a formal validation tool ProVerif. In particular, the proposed protocol can resist attacks such as offline password guessing attacks, smart card loss attacks and impersonation attacks, and provide anonymity and unlinkability.

Ⅰ. 서 론

차량애드혹망 (Vehicular adhoc network, VANET)은 운전자와 승객들을 위해 도로안전, 교통 관리, 인포테인먼트 보급에 중요한 역할을 수행할 기대되는 유망한 기술이다[1-3]. 차량애드혹망은 주로 차량내 장착 장치

※ 본 연구는 중소벤처기업부에서 지원하는 2019년도 산학연 Collabo R&D사업 (S2754028)의 연구 수행과 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(NRF-2017R1D1A1B04032598)으로 수행되었습니다.
◆° First and Corresponding Author : Kyungil University, School of Computer Science, kim@kiu.ac.kr, 정교수, 정회원
논문번호 : KICS201004-081-A-RU, Received April 7, 2020; Revised April 23, 2020; Accepted April 24, 2020

(On board unit, OBU)와 도로변 장치 (Road side unit, RSU)로 구성된다. 차량내 장착 장치는 차량 내에 설치되고 도로변 장치는 차량의 기지국 역할을 수행한다.

차량애드혹망의 상용화에 있어서 보안 및 프라이버시 기술에 대한 확신은 아주 중요한 이슈이다[4-7]. 특히, 인증 프로토콜은 보안과 프라이버시를 제공하고 데이터의 안전성 제공을 위한 기본 기법이다[8-12]. 사용자의 식별자(Identifier) 같은 민감한 정보는 불법적인 추적과 사용자 프로파일링과 같은 공격으로부터 보호되어야 한다. Liu등은 차량애드혹망을 위한 조건 프라이버시 (Conditional privacy)를 제공하는 프로토콜을 제안하였다[8]. 이 프로토콜은 단기 익명성 키와 인증서를 사용함으로서 저장 공간의 효율성을 제시하였다. 하지만 단기 익명성 키를 생성하는데 요구되는 연산 오버헤드의 문제점이 존재한다. Lin등은 각 메시지에 메시지 인증 코드 (Message authentication code)를 사용함으로서 통신과 연산 오버헤드를 줄일 수 있는 시간 효율적인 차량 통신 기법을 제안하였다[9]. 하지만 이 기법은 수신자가 복호된 정보를 확인하기까지 긴 대기 시간이 필요한 문제가 있다. Zhang등은 Blind 서명에 기반한 인증 기법을 제안하였다[10]. 이 기법 역시 높은 통신 오버헤드를 가진다. Paruchuri등은 차량애드혹망 상의 메시지 인증을 위해 스마트 카드 사용을 최초로 도입했다[11]. 스마트 카드는 차량내 장착 장치의 식별자, 공개키, 개인키들 및 인증서와 같은 정보를 저장한다. 하지만, 이 기법은 훔친 스마트 카드 공격 (Stolen smart card attack)에 취약한 문제가 있다. 이러한 문제를 해결하기 위해서 Ying과 Nayak은 스마트 카드 기반의 새로운 인증 프로토콜을 제안하였다[12]. Ying과 Nayak 프로토콜은 패스워드 추측 공격과 훔친 스마트 카드 공격에 안전하기 위해서 사용자의 식별자와 패스워드를 스마트 카드에 저장한다. 또한 동적 식별자를 사용함으로서 익명성 또한 제공하고자 하였다.

본 논문에서는 Ying과 Nayak의 인증 프로토콜에 존재하는 두 가지 보안 문제를 도출한다. Ying과 Nayak 프로토콜은 서비스 거부 공격에 취약하고 익명성을 제공하지 못함을 보인다. 특히, 이러한 문제를 해결하기 위한 사용자 검증 테이블을 사용하지 않는 새로운 프라이버시가 제공된 인증 프로토콜을 제안한다. 정형화된 보안 검증을 위해 ProVerif에 기반한 실험 결과를 제시한다[13]. 특히, 보안 분석 결과에서 제안한 프로토콜이 스마트 카드 분실 공격, 오프라인 패스워드 추측 공격 뿐 만 아니라 다양한 보안 공격에 안전하고 익명성 및 비추적성을 제공함을 보인다.

본 논문의 구성은 다음과 같다. 2장에서는 차량애드혹망 환경과 Ying과 Nayak 인증 프로토콜을 살펴본다. 3장에서는 Ying과 Nayak의 인증 프로토콜에 대한 문제점을 분석한다. 4장에서는 프라이버시가 제공된 인증 프로토콜을 제안하고 5장에서는 ProVerif를 통한 보안 검증 결과를 보인다. 6장에서는 제안한 프로토콜에 대한 보안 및 성능 분석을 제시한다. 마지막으로 7장에서는 결론을 제시한다.

Ⅱ. 차량애드혹망과 Ying과 Nayak 인증 프로토콜

본 장에서는 Ying과 Nayak이 제안한 차량애드혹망을 위한 인증 프로토콜에 대한 개요를 제시한다[12]. 이를 위해 먼저 차량애드혹망 환경에 대해 알아보고 Ying과 Nayak 인증 프로토콜에 대해 구체적으로 살펴본다.

2.1 차량애드혹망

차량애드혹망 통신 환경은 신뢰 기관 (Trusted authority, TA)과 도로변 장치, 그리고 차량내 장착 장치로 구성된다[19]. TA는 도로변 장치와 차량내 장착 장치의 등록을 책임지는 역할을 하고 충분한 계산 능력과 저장 용량을 가진다고 가정한다. 도로변 장치는 유선 또는 무선 네트워크 연결을 통해 TA와 통신할 수 있다고 가정한다. 차량내 장착 장치와 도로변 장치 간의 통신 뿐 만 아니라 차량의 차량내 장착 장치 간 통신은 IEEE 802.11p 표준을 준수한다고 가정한다. 또한 다음과 같은 추가적인 가정을 고려한다.

- TA는 차량애드혹망을 구성하는 모든 통신 참여자들이 완전히 신뢰한다. 또한, TA는 모든 도로변 장치의 식별자와 위치 정보를 알고 있다.
- 도로변 장치는 공격자에 의해 침해당할 수 있고 다른 도로변 장치와 공모 공격을 수행할 수도 있다. 하지만, TA는 높은 수준의 보안을 제공할 수 있도록 도로변 장치들에 대해 검증할 수 있다. 도로변 장치가 공격자에게 침해당하더라도 TA는 이를 탐지하고 복구할 수 있다[4].

2.2 Ying과 Nayak 인증 프로토콜

Ying과 Nayak이 제안한 인증 프로토콜은 등록 단계와 인증 단계 그리고 데이터 전송 단계로 구성된다[12]. 등록 단계는 차량이 차량애드혹망에 참가하기 전에 인증을 위한 스마트 카드 발급을 목적으로 한다. 인증 단계는 인증 참여자의 적법성 검증을 수행한다. 데이터 전송 단계는 3장에서 활용되지 않으므로 이 장에서는 생략한다. 본 논문에서는 표 1에서 제시한 기호들을 사용한다.

표 1. 기호 정의
Table 1. Notations.

Notation	Meaning
p	A prime number in a finite cyclic group G
ID_{Vi}	Vehicle V_i's identity
PW_i	V_i's password
$PVID_{Vi}$	V_i's pseudonym
A_i	V_i's parameter generated by TA
$\triangle T$	Time threshold
ID_{Ri}	RSU R_i's identity
x	Secret parameter generated by TA
y	TA's public key corresponding with x
u	Random number generated by smart card
v	Random number generated by TA
$DIDV_i$	Dynamic login identity of V_i
$DIDR_i$	Dynamic login identity of R_i
CV_i	V_i's authenticator for $DIDV_i$
K_{mast}	Temporary key generated by TA
C_3	Authenticator for V_i's keys and certification
$<PK_{Vi}, SK_{Vi}>$	V_i's anonymous private and public keys
$Cert_{Vi}$	V_i's corresponding anonymous certificate
$Seed_{Vi}$	V_i's seed
H_i	One way hash functions
$E_K()$	Symmetric key encryption with the key K
$\|\|$	Concatenation operation
$\oplus$	XOR operation

2.2.1 등록 단계

TA는 소수 p의 유한 곱셈 순환군 $G=<g>$를 선택한다. 또한, 임의의 비트 입력을 l_i 비트로 출력 ($\{0, 1\}^*$->$\{0, 1\}^{l_i}$)하는 해시함수 H_i (i=0, 1, 2, 3)를 정의한다. TA는 개인키 x와 공개키 $y=g^x \bmod p$를 계산한다. 차량애드혹망 통신을 위해 사용자 V_i는 TA에 등록되어야 한다. TA에 등록하기 위하여 V_i는 차량의 식별자 ID_{Vi}와 $H_0(PW_i)$를 제출하고 TA는 다음 연산을 수행한다.

- 시점 T_{reg}에 등록 요청을 받으면 TA는 ID_{Vi}와 T_{reg}를 저장하고, $PVID_{Vi}=H_0(ID_{Vi})$와 $A_i=H_0(H_0(PW_i)||PVID_{Vi})$ 그리고 $N_i=H_0(PW_i)\oplus H_0(x||PVID_{Vi}||T_{reg})$를 계산한다.
- TA는 $<A_i, N_i, g, p, y, H_0, H_1, H_2, H_3>$가 저장된 스마트 카드를 발급하고 이를 V_i에게 보낸다.

2.2.2 인증 단계

V_i의 운전자는 차량 단말기에 스마트 카드를 넣고 ID_{Vi}^*와 PW_i^*를 입력한다. 그림 1은 사용자 인증 단계의 요약을 보여준다. 구체적인 사용자 인증은 다음과 같다.

단계1: 스마트 카드는 V_i의 비밀번호와 식별자를 검증하고 V_i의 동적 로그인 식별자 $DIDV_i$를 생성한다. 자세한 내용은 다음과 같다.

- $ID_{Vi}^?=ID_{Vi}^*$와 $PW_i^?=PW_i^*$를 검증하기 위해서 $A_i^*=H_0(H_0(PW_i^*)||H_0(ID_{Vi}^*))$를 계산하고 이 값이 스마트 카드에 저장된 A_i와 동일한 지 확인한다. 만약 두 값이 일치하지 않으면, 스마트 카드는 이 단계를 끝낸다. 보안 강화를 위해서 스마트 카드는 인증 실패 임계값을 설정할 수 있다. 임계값을 넘어서는 경우 사용자 인증 시도 시 스마트 카드는 네트워크 관리 기관에 이 사실을 통보하고, 재설정 요청이 전송될 때까지 해당 계정을 중단시킨다.
- $k=H_0(x||PVID_{Vi}||T_{reg})=N_i\oplus H_0(PW_i^*)$를 계산한다.
- 난수 u를 생성하고 $C_1=g^u \bmod p$, $Y_1=y^u \bmod p$를 계산한다.
- V_i의 동적 로그인 식별자 $DIDV_i=H_0(ID_{Vi}^*)\oplus H_0(C_1||Y_1)$를 계산한다.
- $CV_i=H_0(Y_1||DIDV_i||k)$를 계산한다.
- $<C_1, DIDV_i, CV_i, T_{Vi}>$를 도로변 장치 R_i에게 보낸다.

단계2: T시간에 로그인 메시지를 받으면 R_i는 다음을 수행한다.

- $(T-T_{Vi})\le\triangle T$를 확인하고 조건이 만족하지 않으면 중단한다.
- R_i의 동적 식별자 $DIDR_i=DIDV_i\oplus ID_{Ri}$를 계산한다.
- $<C_1, DIDR_i, CV_i, T_{Ri}>$를 TA에게 보낸다.

단계3: T_1 시간에 메시지를 받으면, TA는 V_i의 합법성을 확인해야 하고 차량의 공개키와 개인키 쌍과 이를 위한 인증서를 생성한다. 상세한 내용은 다음과 같다.

- $(T_1-T_{Ri})\le\triangle T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $Y_1=(C_1)^x=y^u \bmod p$를 계산한다.
- $DIDV_i^*=PVID_{Vi}\oplus H_0(C_1||Y_1)$를 계산한다.
- $ID_{Ri}^*=DIDV_i^*\oplus DIDR_i^*$를 계산하고 ID_{Ri}^*가 TA에 저장된 ID_{Ri}와 같은지 검사함으로써 식별자의 적법성을 검증한다.
- $k=H_0(x||PVID_{Vi}||T_{reg})$를 계산한다.
- $H_0(Y_1||DIDV_i^*||k)$를 계산하고 계산한 값이 CV_i와 같은지 확인하고 같지 않으면 메시지를 거부한다. 그 후, TA는 차량의 익명 공개키와 개인키 한 쌍과 이를 위한 인증서를 포함하는 암호화 된 메시지를 전송한다. TA는 다음을 수행한다.
- $K_{mast}=(C_1)^v \bmod p$, $K_s=(C_1)^x \bmod p$, $C_2=g^v \bmod p$를 계산한다.
- $C_3=H_1(K_s||A||C_2)$를 계산한다.
- V_i의 공개키와 개인키 쌍 $<PK_{Vi}, SK_{Vi}>$와 V_i의 익

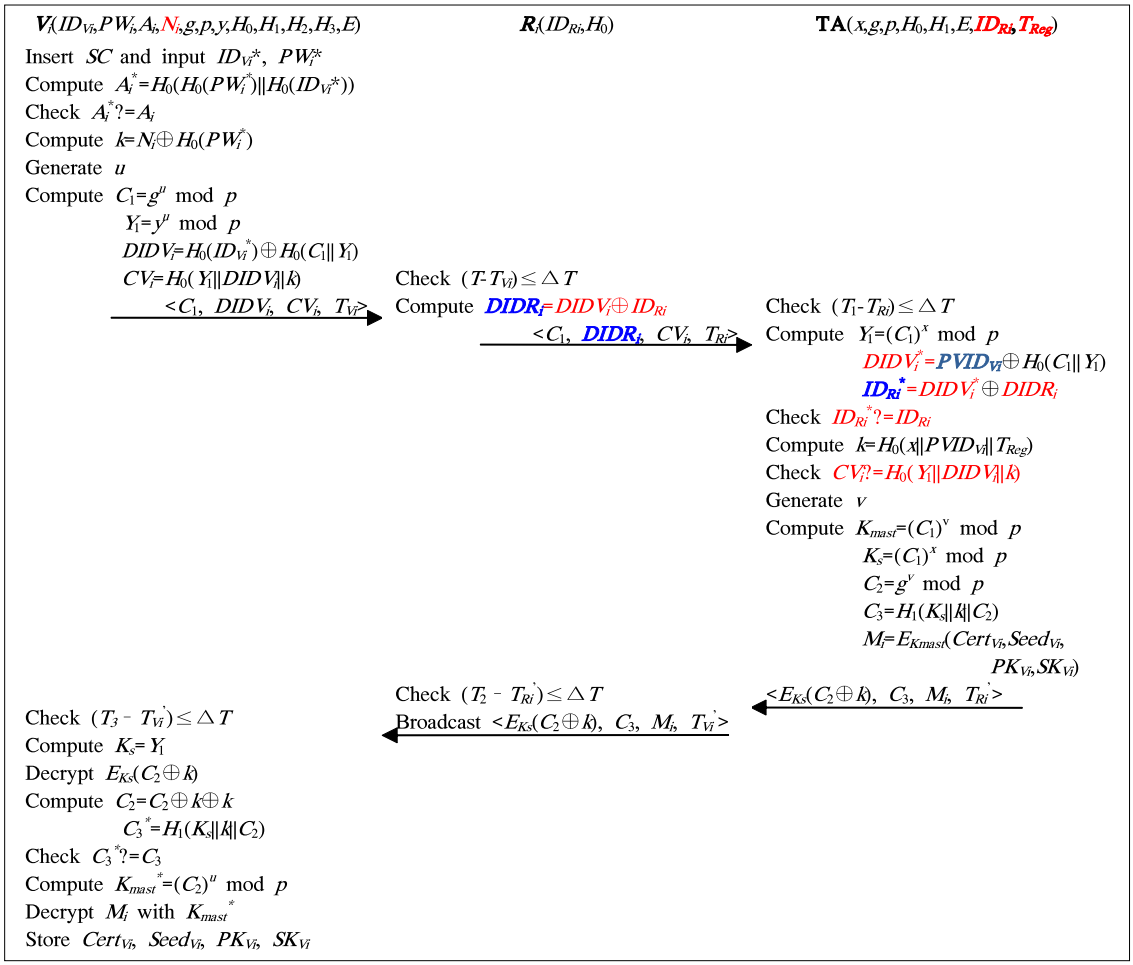

그림 1. Ying과 Nayak 인증 프로토콜의 인증 단계
Fig. 1. Authentication phase in Ying and Nayak's authentication protocol.

명 인증서 $Cert_{Vi}$그리고 V_i의 초기 값인 $Seed_{Vi}$를 이용하여 $M_i = E_{Kmast}(Cert_{Vi}, Seed_{Vi}, PK_{Vi}, SK_{Vi})$를 계산한다.

- $<E_{Ks}(C_2 \oplus k), C_3, M_i, T_{Ri}'>$를 R_i에게 보낸다.

단계4: T_2 시간에 메시지를 받으면, R_i는 다음을 수행한다.

- $(T_2 - T_{Ri}') \leq \Delta T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $<E_{Ks}(C_2 \oplus k), C_3, M_i, T_{Vi}'>$를 브로드캐스트(Broadcast)한다.

단계5: T_3에 메시지를 받으면, V_i는 메시지를 복호하고 공개키와 개인키 및 인증서를 얻는다. 다음과 같은 연산이 수행된다.

- $(T_3 - T_{Vi}') \leq \Delta T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $K_s = Y_1$를 계산하고 $E_{Ks}(C_2 \oplus k)$를 복호하고 $C_2 = C_2 \oplus k$를 도출한다.
- $C_3^* = H_1(K_s || k || C_2)$를 계산하고 이 값이 수신한 C_3와 같은지 확인한다. 두 값이 다르면 메시지는 거부된다.
- $K_{mast}^* = (C_2)^u \bmod p$를 계산한다.
- K_{mast}^*를 사용해 M_i를 복호하고 $Cert_{Vi}$, $Seed_{Vi}$, PK_{Vi}, SK_{Vi}를 저장한다.

Ⅲ. Ying과 Nayak 인증 프로토콜 취약점 분석

본 장에서는 2장에서 살펴본 Ying과 Nayak 인증 프로토콜에 대한 보안 취약성을 서비스 거부 공격

(Denial of service, DoS)과 익명성 노출 공격의 가능성 관점에서 분석한다. 이는 그림 1에 빨간색으로 표시된 값들에 대한 구성과 $N_i=H_0(PW_i)\oplus H_0(x\|PVID_{Vi}\|T_{reg})$의 초기값 설정으로 인한 문제이다. 구체적인 내용은 각 문제점에서 상세히 살펴본다.

3.1 서비스 거부 공격

Ying과 Nayak 인증 프로토콜 인증 단계의 단계2에서 R_i는 메시지 $<C_1, DIDR_i, CV_i, T_{Ri}>$를 TA에게 보낸다. TA는 받은 정보들을 통해 V_i의 적법성을 확인한 후 적법하면 차량을 위해 공개키와 개인키 쌍을 생성하고 이를 위한 인증서를 발급한다. V_i의 적법성 검증과정에서 TA는 $DIDV_i^*=PVID_{Vi}\oplus H_0(C_1\|Y_1)$ 연산을 수행한다. 하지만 TA가 $DIDV_i^*$를 계산하기 위해서는 그림 1의 바다색으로 표시된 $PVID_{Vi}$를 알아야 한다. TA가 $PVID_{Vi}$를 알기 위해서는 V_i나 R_i를 통해 관련된 값을 받거나 직접적인 계산을 수행해야 한다. 그러나 단계 2의 메시지인 $<C_1, DIDR_i, CV_i, T_{Ri}>$를 통해서 TA가 $PVID_{Vi}$를 찾을 수 있는 방법이 Ying과 Nayak 인증 프로토콜에는 제시되지 못하고 있다. 유일한 방법은 등록단계에서 저장된 차량의 식별자 ID_{Vi}와 T_{reg}를 통해 계산하는 것이다. 즉, TA가 적법한 $PVID_{Vi}$를 계산하기 위해 사용자 검증 테이블에 저장된 모든 값을 후보로 $DIDV_i^*$를 계산하고 이 값이 수신한 $DIDV_i$와 일치하는 ID_{Vi}를 찾아야만 한다.

Ying과 Nayak 인증 프로토콜의 문제는 서비스를 사용하는 모든 사용자가 TA를 통해 인증단계를 수행해야 하고 이러한 이유로 다양한 R_i들로부터의 메시지는 TA에게 병목현상 문제를 발생시킨다. 즉, 각각의 인증 요청에 따른 시스템에 등록된 전체 차량의 수만큼 매번 해시 연산을 수행해야하고 그 결과에 따른 추가적인 검증이 필요하다는 것이다. 이러한 과정에서 서비스 거부 공격이 발생할 수 있다.

3.2 익명성 노출 공격

Ying과 Nayak은 그들의 인증 프로토콜이 익명성을 제공할 수 있다고 주장하였다. 하지만, Ying과 Nayak 인증 프로토콜의 등록 단계에서 V_i로부터 등록 요청을 받은 TA는 차량의 식별자 ID_{Vi}와 T_{reg}를 시스템에 저장한다. 다양한 보안 관련 기법에서 시스템 침입을 통한 훔친 검증자 공격이 가능함을 보였다. 이를 통하여 본 논문에서도 공격자가 훔친 검증자 공격과 이전 세션의 메시지 도청을 통해 차량애드혹망 참여자 간 주고받은 메시지를 획득할 수 있다고 가정한다.

즉, 익명성 공격을 위해 공격자는 TA 시스템에 저장된 차량의 식별자 ID_{Vi}와 T_{reg} 테이블을 획득하고, 이전 세션의 메시지인 $<C_1, DIDV_i, CV_i, T_{Vi}>$와 $<C_1, DIDR_i, CV_i, T_{Ri}>$ 및 $<E_{Ks}(C_2\oplus k), C_3, M_i, T_{Ri}>$를 도청 공격을 통해 획득한다. 이렇게 수집된 메시지로부터 익명성 노출 공격을 수행하기 위해서 공격자는 TA로부터 획득한 사용자 검증 테이블을 통하여 ID_{Vi} 대입 공격을 통해 $DIDV_i^*$(그림 1에서 파란색으로 표시된 부분)를 계산한다. 계산된 값이 첫 번째 메시지에 포함된 $DIDV_i$와 같은 값이면 공격은 성공이다. 즉, 이러한 공격을 통해 공격자는 어떤 V_i가 현재 통신 중인지 확인할 수 있고 세션간 연계를 확인할 수 있다.

Ⅳ. 프라이버시가 제공된 인증 프로토콜

본 장에서는 Ying과 Nayak 인증 프로토콜의 문제점을 해결하기 위한 차량애드혹망 상의 새로운 프라이버시가 제공된 인증 프로토콜을 제안한다. 특히, 본 논문에서 제안한 프로토콜은 보안 및 프라이버시 강화를 위해 TA에 사용자 검증 테이블을 사용하지 않는다. 본 논문에서 제안한 프로토콜은 등록 단계와 인증 단계 그리고 데이터 전송 단계로 구성된다. 각 단계의 구체적인 내용은 다음과 같다.

4.1 등록 단계

TA는 소수 p의 유한 곱셈 순환군을 $G=<g>$를 선택한다. 또한, 임의의 비트의 입력을 l_i 비트로 출력 ($\{0, 1\}^*$->$\{0, 1\}^{l_i}$)하는 해시함수 H_i (i=0, 1, 2, 3)를 정의한다. TA는 개인키 x와 공개키 $y=g^x \bmod p$를 계산한다. 차량애드혹망 통신을 위해 사용자 V_i는 TA에 등록되어야 한다. TA에 등록하기 위하여 V_i는 차량의 식별자 ID_{Vi}와 $H_0(PW_i)$를 제출하고 TA는 다음 연산을 수행한다.

- 시점 T_{reg}에 등록 요청을 받으면 TA는 $PVID_{Vi}=H_0(ID_{Vi})$와 $A_i=H_0(H_0(PW_i)\|\| PVID_{Vi})$ 그리고 $N_i=H_0(PW_i)\oplus H_0(x\|\| PVID_{Vi})$를 계산한다.
- TA는 $<A_i, N_i, g, p, y, H_0, H_1, H_2, H_3>$가 저장된 스마트 카드를 발급하고 이를 V_i에게 보낸다.

4.2 인증 단계

V_i의 운전자는 차량 단말기에 스마트 카드를 넣고 ID_{Vi}^*와 PW_i^*를 입력한다. 그림 2는 사용자 인증 단계의 요약을 보여준다. 구체적인 사용자 인증은 다음과 같다.

단계1: 스마트 카드는 V_i의 비밀번호와 식별자를 검증하고 V_i의 동적 로그인 식별자 $DIDV_i$를 생성한다.

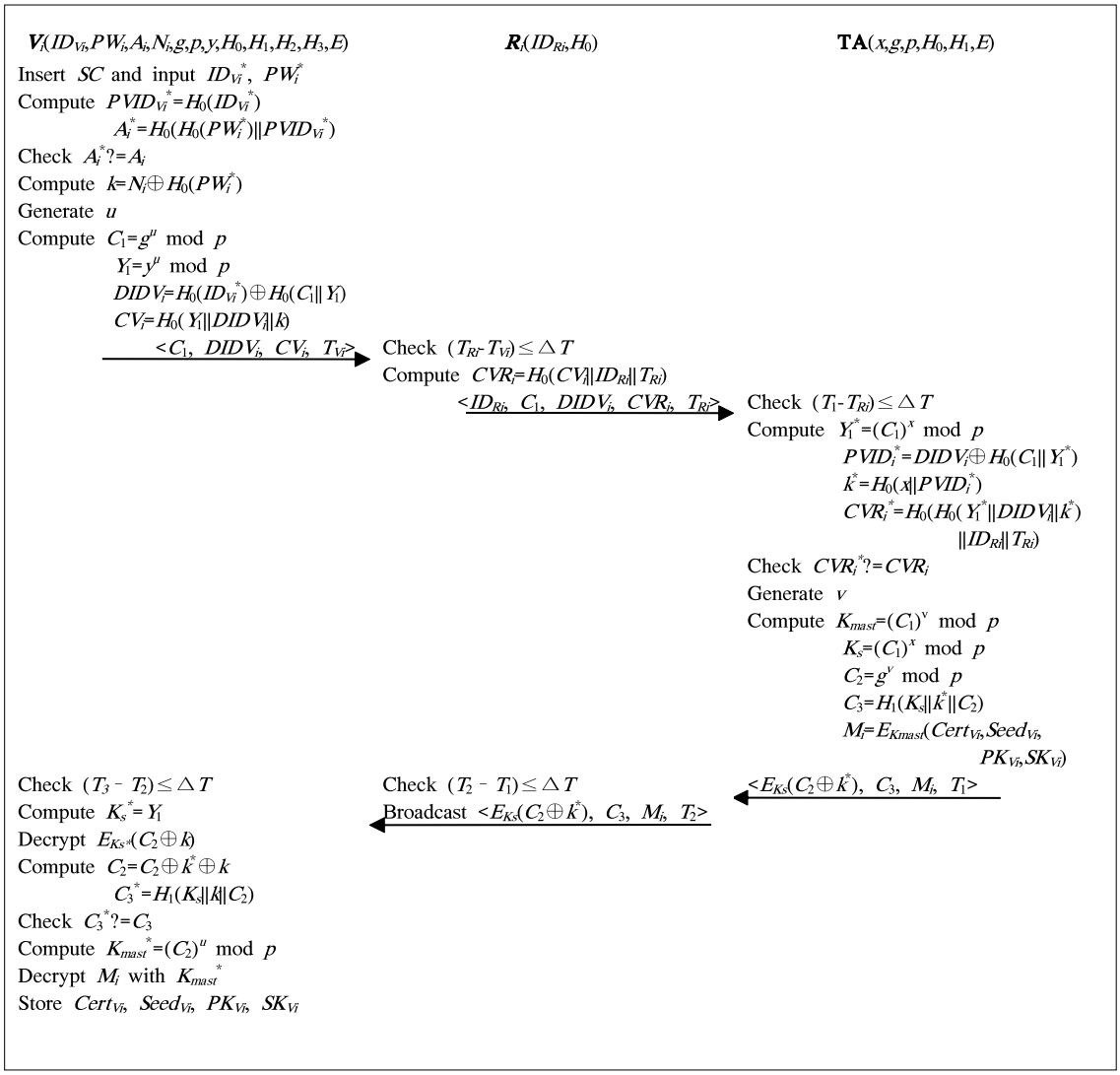

그림 2. 프라이버시가 제공된 인증 프로토콜의 인증 단계
Fig. 2. Authentication phase in privacy preserving authentication protocol.

자세한 내용은 다음과 같다.

- $ID_{Vi} ? = ID_{Vi}^*$와 $PW_i ? = PW_i^*$를 검증하기 위해서 $PVID_{Vi}^* = H_0(ID_{Vi}^*)$와 $A_i^* = H_0(H_0(PW_i^*) \| PVID_{Vi}^*)$를 계산하고 이 값이 스마트 카드에 저장된 A_i와 동일한 지 확인한다. 만약 두 값이 일치하지 않으면, 스마트 카드는 이 단계를 끝낸다. 보안 강화를 위해서 스마트 카드는 인증 실패 임계값을 설정할 수 있다. 임계값을 넘어서는 경우 사용자 인증 시도 시 스마트 카드는 네트워크 관리 기관에 이 사실을 통보하고, 재설정 요청이 전송될 때까지 해당 계정을 중단시킨다.
- $k = N_i \oplus H_0(PW_i^*)$를 계산한다.
- 난수 u를 생성하고 $C_1 = g^u \bmod p$과 $Y_1 = y^u \bmod p$을 계산한다.
- V_i의 동적 로그인 식별자 $DIDV_i = H_0(ID_{Vi}^*) \oplus H_0(C_1 \| Y_1)$를 계산한다.
- $CV_i = H_0(Y_1 \| DIDV_i \| k)$를 계산한다.
- $<C_1, DIDV_i, CV_i, T_{Vi}>$를 도로변 장치 R_i에게 보낸다.

단계2: T_{Ri}시간에 로그인 메시지를 받으면 R_i는 다음을 수행한다.

- $(T_{Ri} - T_{Vi}) \le \Delta T$를 확인하고 조건이 만족하지 않으면 중단한다.

- $CVR_i=H_0(CV_i||ID_{Ri}||T_{Ri})$를 계산한다.
- $<ID_{Ri}, C_1, DIDV_i, CVR_i, T_{Ri}>$를 TA에게 보낸다.

단계3: T_1 시간에 메시지를 받으면, TA는 V_i의 합법성을 확인하고 차량의 공개키와 개인키 쌍과 이를 위한 인증서를 생성한다. 상세한 내용은 다음과 같다.

- $(T_1-T_{Ri})\leq\triangle T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $Y_1^*=(C_1)^x=y^\mu \bmod p$를 계산한다.
- $PVID_{Vi}^*=DIDV_i\oplus H_0(C_1||Y_1^*)$를 계산한다.
- $k^*=H_0(x||PVID_{Vi}^*)$를 계산한다.
- $CVR_i^*=H_0(H_0(Y_1^*||DIDV_i||k^*)||ID_{Ri}||T_{Ri})$를 계산하고 이 값이 CVR_i와 동일한지 확인한다. 두 값이 다르다면 메시지는 거부된다.

  그 후, TA는 차량의 익명 공개키와 개인키 한 쌍과 이를 위한 인증서를 포함하는 암호화 된 메시지를 전송한다. TA는 다음을 수행한다.
- 난수 v를 생성하고 $K_{mast}=(C_1)^v \bmod p$, $K_s=(C_1)^x \bmod p$, $C_2=g^v \bmod p$를 계산한다.
- $C_3=H_1(K_s||k^*||C_2)$를 계산한다.
- V_i의 공개키와 개인키 쌍 $<PK_{Vi}, SK_{Vi}>$와 V_i의 익명 인증서 $Cert_{Vi}$그리고 V_i의 초기 값인 $Seed_{Vi}$를 이용하여 $M_i=E_{Kmast}(Cert_{Vi}, Seed_{Vi}, PK_{Vi}, SK_{Vi})$를 계산한다.
- $<E_{Ks}(C_2\oplus k^*), C_3, M_i, T_1>$를 R_i에게 보낸다.

단계4: T_2시간에 메시지를 받으면, R_i는 다음을 수행한다.

- $(T_2-T_1)\leq\triangle T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $<E_{Ks}(C_2\oplus k^*), C_3, M_i, T_2>$를 브로드캐스트한다.

단계5: T_3에 메시지를 받으면, V_i는 메시지를 복호하고 공개키와 개인키 및 인증서를 얻는다. 다음과 같은 연산이 수행된다.

- $(T_3-T_2)\leq\triangle T$를 확인하고 조건이 만족하지 않으면 중단한다.
- $K_s^*=Y_1$를 계산하고 $E_{Ks*}(C_2\oplus k^*)$를 복호하고 $C_2=C_2\oplus k^*\oplus k$를 도출한다.
- $C_3^*=H_1(K_s^*||k||C_2)$를 계산하고 이 값이 수신한 C_3와 같은지 확인한다. 두 값이 다르면 메시지는 거부된다.
- $K_{mast}^*=(C_2)^u \bmod p$를 계산한다.
- K_{mast}^*를 사용해 M_i를 복호하고 $Cert_{Vi}$, $Seed_{Vi}$, PK_{Vi}, SK_{Vi}를 저장한다.

4.3 데이터 전송 단계

V_i가 $Cert_{Vi}$, $Seed_{Vi}$, PK_{Vi}, SK_{Vi}를 획득한 후, 기법[14]에 기초한 메시지 인증을 위한 해시 체인을 이용한다. 각 차량은 상위 레벨과 하위 레벨의 해시 체인을 위해 해시 함수 H_2와 H_3을 사용한다. 상위 레벨의 해시 체인 수명은 n_H 간격($I_1, I_2, ..., I_{nH}$) 으로 나뉜다. 각 시간 간격 $I_t(1\leq t\leq n_H)$은 n_{nL}간격으로 다시 세분화되고 $I_{t,1}, I_{t,2}, ..., I_{t,nL}$로 표시된다. 상위 레벨의 해시 체인 $K_1, K_2, ..., K_{nH}$는 $Seed_{Vi}$를 초기 값($K_{nH} = Seed_{Vi}$)으로 활용하고 $t<j$ 조건을 만족하는 $K_t=H_2^{j-t}(K_j)$로 초기화 된다. 동시에 H_3와 K_{t+1}을 사용하는 각 시간 간격 I_t에 대한 하위 레벨 해시 체인은 $K_{t,nL}=H_3(K_{t+1})$, $K_{t,j}=H_3(K_{t,j+1})$로 계산된다. 메시지 인증 방법에 대한 자세한 내용은 논문[14]에서 확인할 수 있다.

Ⅴ. 보안 검증

제안한 인증 프로토콜에 대한 보안 검증을 위해서 Dolev-Yao 공격 모델[15]에 기반한 자동화된 암호학적 기법 정형화 검증 도구인 ProVerif를 활용한다[13]. ProVerif를 통해서 인증 프로토콜의 상호 인증과 보안성을 효율적으로 검증할 수 있다.

제안한 인증 프로토콜의 ProVerif 자료는 https://github.com/hs-kim-andre/kim-kiu.ac.kr/blob/master/privacy.pv에서 확인할 수 있다. 그림 3은 ProVerif 버전 1.96을 활용한 제안한 인증 프로토콜의 검증 결과이다. V_i와 TA 간 상호 인증이 성공적으로 달성하였음을 확인할 수 있다.

제안한 프라이버시가 제공된 인증 프로토콜의 ProVerif 보안 검증을 위하여 다음 단계를 진행하였다. 먼저, 공개 통신 채널을 위하여 ch1과 ch2를 정의하였다. ch1은 V_i와 R_i간 통신에 활용되고 ch2는 R_i와 TA간 통신에 활용된다. $K_{mast}=(C_1)^v \bmod p=(g^u)^v \bmod p=(C_2)^u$

ProVerif text output:

```
Completing equations...
Completing equations...
-- Query inj-event(VTend(t)) ==> inj-event(VTbegin(t))
Completing...
200 rules inserted. The rule base contains 186 rules. 24 rules in the queue.
Starting query inj-event(VTend(t)) ==> inj-event(VTbegin(t))
RESULT inj-event(VTend(t)) ==> inj-event(VTbegin(t)) is true.
-- Query inj-event(TVend(t_61)) ==> inj-event(TVbegin(t_61))
Completing...
200 rules inserted. The rule base contains 179 rules. 26 rules in the queue.
Starting query inj-event(TVend(t_61)) ==> inj-event(TVbegin(t_61))
RESULT inj-event(TVend(t_61)) ==> inj-event(TVbegin(t_61)) is true.
-- Query not attacker(svalueA[]); not attacker(svalueB[])
Completing...
200 rules inserted. The rule base contains 188 rules. 22 rules in the queue.
Starting query not attacker(svalueA[])
RESULT not attacker(svalueA[]) is true.
Starting query not attacker(svalueB[])
RESULT not attacker(svalueB[]) is true.
```

그림 3. ProVerif 검증 결과
Fig. 3. ProVerif validation results.

표 2. 프라이버시와 보안 비교
Table 2. Privacy and security comparisons.

Feature / Protocol	P1	P2	S1	S2	S3	S4	S5	S6
Ying-Nayak	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

P1:익명성, P2:비추적성, S1:스마트 카드 분실 공격, S2:암호 추측 공격, S3:재전송 공격, S4:가장 공격, S5:서비스 거부 공격, S6:훔친 검증자 공격

mod $p=(g^{v})^{u}$ mod p의 안전성을 검증하기 위하여 svalueA와 svalueB가 사용되었다. 또한 제안한 인증 프로토콜의 상호 인증을 검증하기 위하여 4개의 이벤트 TVbegin(entity), VTbegin(entity), TVend(entity), VTend(entity)가 선언되었다. 즉, 본 논문에서 제안한 인증 프로토콜은 V_i와 TA간의 상호 인증을 제공하기 위한 목적이 있으므로 이를 위한 인증 단계에 대한 논증을 진행하였다. 마지막으로 전체 인증 프로세스에 대한 모델을 제시하였다.

Ⅵ. 프라이버시/보안/성능 분석

본 장에서는 제안한 인증 프로토콜에 대한 프라이버시 및 보안 분석을 제시한다. 특히, Ying과 Nayak 인증 프로토콜의 문제점은 그림 1의 빨간색으로 표시된 부분으로 인한 문제를 그림 2의 새로운 프로토콜 설계로 해결하였다. 또한, TA에 사용자 검증 테이블을 사용하지 않는다. 표 2는 프라이버시 및 보안 분석 결과를 Ying과 Nayak 인증 프로토콜과의 비교를 보여준다. 또한, 성능 분석을 위해 연산과 통신 오버헤드 분석을 제시한다.

6.1 프라이버시 분석

[P1]익명성: 익명성에 대한 공격을 위해 공격자가 한 세션의 메시지들 $<C_1, DIDV_i, CV_i, T_{Vi}>$과 $<ID_{Ri}, C_1, DIDV_i, CVR_i, T_{Ri}>$ 그리고 $<E_{Ks}(C_2 \oplus k^{*}), C_3, M_i, T_1>$를 도청할 수 있다고 가정한다. 이러한 메시지를 통해서 사용자의 ID_{Vi}를 확인할 수 있는지 확인을 통해서 익명성 제공에 대한 여부를 확인할 수 있다. 제안한 인증 프로토콜에서 ID_{Vi}와 연계된 값은 $DIDV_i$이다. 즉 공격자가 $DIDV_i = H_0(ID_{Vi}) \oplus H_0(C_1 \| Y_i)$로부터 ID_{Vi}를 유도하기 위해서는 C_1을 이용해 Y_i을 계산할 수 있어야 한다. 이는 C_1에서 u를 계산하거나 y에서 x를 계산하는 어려운 문제인 타원곡선이산대수의 어려움과 동일한 문제이다. 특히, 본 논문에서 제안한 프로토콜은 TA에 사용자 검증 테이블을 저장하지 않기 때문에 Ying과 Nayak 프로토콜의 문제점인 프라이버시 문제를 해결할 수 있다. 이를 통해 제안한 인증 프로토콜은 사용자의 익명성을 효율적으로 제공한다.

[P2]비추적성: 비추적성을 위한 공격의 가정도 익명성과 동일하다. 즉 공격자가 한 세션의 메시지들 $<C_1, DIDV_i, CV_i, T_{Vi}>$과 $<ID_{Ri}, C_1, DIDV_i, CVR_i, T_{Ri}>$ 그리고 $<E_{Ks}(C_2 \oplus k^{*}), C_3, M_i, T_1>$를 도청할 수 있다. 이러한 메시지를 통해 임의의 다른 두 세션 간 연계를 확인할 수 있다면 비추적성에 대한 공격은 성공할 수 있다. 즉, 비추적성을 제공하기 위해서는 한 세션에서 사용하는 변수들의 값이 다른 세션에서 사용되는 값과 달라야 한다. 본 논문에서 이용한 메시지들의 모든 변수들은 세션 의존적인 난수나 시간 값을 포함하고 있다. 이를 통해서 세션간의 연계에 대한 추측을 효율적으로 보호할 수 있어서 비추적성을 제공한다.

6.2 보안 분석

[S1]스마트 카드 분실 공격: 효율적인 공격을 위해 공격자가 차량의 스마트 카드를 훔칠 수 있고, 부채널 공격과 메모리 공격을 통해 스마트 카드에 저장된 $\{A_i, N_i, g, p, y, H_0, H_1, H_2, H_3\}$를 추출할 수 있다고 가정한다. 제안한 인증 프로토콜은 공격자가 스마트 카드에 저장된 정보를 획득 할 수 있는 방법이 있다고 하더라도, 이들 정보는 인증 단계에서 활용될 수 있다. 인증 단계에서 활용되기 위해서는 단계1에서 수행하는 스마트 카드 소유자 인증을 통과할 수 있어야 한다. 특히, 소유자 인증을 통과하기 위해서 공격자는 ID_{Vi}와 PW_i 두 값을 한꺼번에 추측할 수 있어야 하고 아직까지 효율적인 결정적 다항시간 알고리즘이 존재하지 않는다. 즉, 제안한 인증 프로토콜은 스마트 카드 분실 공격에 안전하다.

[S2]패스워드 추측 공격: 패스워드 추측 공격은 패스워드 기반 보안 시스템에서 아주 중요한 문제이다. 공격자는 차량의 스마트 카드와 저장된 정보 $\{A_i, N_i, g, p, y, H_0, H_1, H_2, H_3\}$를 획득할 수 있다고 가정한다. 성공적인 공격을 위해서 공격자는 ID_{Vi}와 PW_i 두 값을 동시에 정확하게 추측할 수 있어야 한다. 하지만 한꺼번에 두 매개변수를 정확히 추측하는 것은 불가능하다. 따라서 제안한 인증 프로토콜은 패스워드 추측 공격에 안전하다.

[S3]재전송 공격: 공격자는 임의의 T_j시점 세션 메시지들 $<C_1, DIDV_i, CV_i, T_{Vi}>$과 $<ID_{Ri}, C_1, DIDV_i, CVR_i, T_{Ri}>$ 그리고 $<E_{Ks}(C_2 \oplus k^{*}), C_3, M_i, T_1>$를 도청

할 수 있다고 가정한다. 이들 메시지 중 임의의 메시지를 이후의 시점에 재전송함으로서 임의의 차량애드혹망 참가자로 가장하고자 한다. 하지만 모든 메시지는 시스템에 동기화 된 시간을 활용하고 T_j시점에 재전송된 메시지는 $(T_j - T_j) \leq \triangle T$ 검증으로 인해 성공할 수 없다. 즉, 제안한 인증 프로토콜은 재전송 공격에 안전하다.

[S4]가장 공격: 가장 공격을 위해서 공격자는 효율적으로 적법한 메시지를 구성할 수 있어야 한다. V_i를 가장하기 위해서는 적법한 $DIDV_i$와 CV_i를 통해서 $<C_1, DIDV_i, CV_i, T_{Vi}>$을 생성할 수 있어야 한다. 하지만 적법한 $DIDV_i$와 CV_i를 계산하기 위해서 공격자는 ID_{Vi}와 k를 각각 알아야 하고, 이는 이전 공격에서 명시한 대로 이를 위한 효율적인 결정적 다항시간 알고리즘이 존재하지 않는다.

[S5]서비스 거부 공격: 효율적인 공격을 위해 공격자가 차량의 스마트 카드와 저장된 정보 $\{A_i, N_i, g, p, y, H_0, H_1, H_2, H_3\}$를 획득할 수 있고 이전 세션의 메시지들 $<C_1, DIDV_i, CV_i, T_{Vi}>$과 $<ID_{Ri}, C_1, DIDV_i, CVR_i, T_{Ri}>$ 그리고 $<E_{Ks}(C_2 \oplus k^*), C_3, M_i, T_1>$를 도청할 수 있다고 가정한다. 하지만 제안한 인증 프로토콜에서는 공격자가 획득한 정보를 통해서 서비스 거부 공격이 수행될 수 있을 정도로 임의의 차량애드혹망 참여자에게 연산의 오버헤드를 제시할 수 있는 방법이 존재하지 않는다. 즉, 제안한 인증 프로토콜은 어떠한 네트워크 참여자도 특정 연산에 대한 네트워크 참여자 전체의 수에 해당하는 연산을 수행하지 않기 때문에 서비스 거부 공격에 안전하다.

[S6]훔친 검증자 공격: 제안한 인증 프로토콜은 TA가 따로 사용자의 정보를 저장하기 위한 검증자 테이블을 사용하지 않는다. 그러므로 제안한 인증 프로토콜은 훔친 검증자 공격에 안전하다.

표 3. 성능 비교
Table 3. Performance comparisons.

Feature / Protocol	Communication cost	Computation cost
Ying-Nayak	3,840 bits	$7t_e+10t_h+4t_{e/d}$
Proposed	3,968 bits	$6t_e+10t_h+4t_{e/d}$

6.3 성능 분석

인증 프로토콜의 효율성 분석을 위해 등록 단계와 비밀번호 변경 단계는 배제하고 인증 단계의 연산과 통신의 오버헤드만을 고려한다. 이러한 이유는 등록 단계와 비밀번호 변경 단계는 일반적으로 자주 사용하는 연산이 아니기 때문이다. 분석의 효율성을 위해서 식별자, 패스워드, 난수, 시간 값, 암호와 복호의 출력 그리고 해시함수의 출력을 128비트로 가정하고, p와 y 그리고 g는 1,024비트로 가정한다. 지수 연산, 해시 연산, 서명 연산, 암호/복호 계산 그리고 XOR연산을 위한 시간적 복잡도를 위해 기호 t_e, t_h, t_s, $t_{e/d}$ 그리고 t_x로 정의하면 시간 복잡도의 크기는 $t_s > t_e > t_h \geq t_{e/d} >> t_x$ 로 정의된다. 효율적인 분석을 위해 상대적으로 가장 작은 값인 t_x는 고려에서 제외한다. 본 논문에서 제안한 프로토콜의 효율성 분석을 위해서 Ying과 Nayak 인증 프로토콜과의 비교를 표 3과 같이 제시한다.

Ⅶ. 결 론

본 논문에서는 차량애드혹망에서 프라이버시와 보안을 제공할 수 있는 인증 프로토콜을 제안하였다. 효율적인 인증 프로토콜을 제안하기 위해서 Ying과 Nayak 인증 프로토콜에 대한 보안 및 프라이버시 분석을 제시하였고 이러한 문제를 해결하기 위한 새로운 프라이버시가 제공된 인증 프로토콜을 제안하였다. 본 논문에서 제안한 인증 프로토콜은 통신에서 128비트의 추가적인 오버헤드가 존재하지만, 연산 측면에서 보다 효율성이 있고, 보안과 프라이버시 측면에서 더 안전성을 제시함을 분석에서 확인할 수 있었다.

References

[1] P. K. Singh, S. K. Nandi, and S. Nandi. “A tutorial survey on vehicular communication state of the art, and future research directions,” *Veh. Commun.*, vol. 18, no. 100164, 2019.

[2] M. S. Talib, A. Hassan, B. Hussin, A. A. Mohammed, A. A. Hassan, and A. A. Mutlag, “Vehicular ad hoc network for intelligent transport system: A review,” *Int. J. Eng. & Technol.*, vol. 7, pp. 350-353, 2018.

[3] M. A. Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, “Systematic literature review on Internet-of-Vehicles communication security,” *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 12, 2018. https://doi.org/10.1177/1550147718815054.

[4] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and

M. S. Obaidat, "A systemetic review on security issues in vehicular ad hoc network," *Secur. and Privacy*, vol. 1, no. 5, 2018. https://doi.org/10.1002/spy2.39.

[5] S. Hamdan, A. Hudaib, and A. Awajan, "Detecting Sybil attacks in vehicular ad hoc networks," *Int. J. Parallel, Emergent and Distrib. Syst.*, pp. 1-11, 2019. https://doi.org/10.1080/17445760.2019.1617865.

[6] R. Kaur, T. P. Singh, and V. Khajuria, "Security issues in vehicular Ad-Hoc network (VANET)," in *Proc. 2018 2nd Int. Conf. Trends in Electron. and Info.*, pp. 884-889, Tirunelveli, India, 2018.

[7] H. Kim, "Security and privacy measures on data mining for internet of things," *Int. J. Appl. Eng. Res.*, vol. 13, no. 14, pp. 11648-11652, 2018.

[8] R. X. Liu, X. D. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, pp. 1229-1237, AZ, USA, 2008.

[9] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 12, pp. 4987-4988, 2008.

[10] C. Zhang, R. Liu, P.-H. Ho, and A. Chen, "A location privacy preserving authentication scheme in vehicular networks," in *Proc. Wireless Commun. and Netw. Conf. 2008*, pp. 2543-2548, NV, USA, 2008.

[11] V. Paruchuri and A. Durresi, "PAAVE: Protocol for anonymous authentication in vehicular networks using smart cards," in *Proc. IEEE GLOBECOM 2010*, pp. 1-5, FL, USA, 2010.

[12] B. Ying and A. Nayak, "Efficient authentication protocol for secure vehicular communications," in *Proc. 2014 IEEE 79th Veh. Technol. Conf.*, Seoul, South Korea, 2014.

[13] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in *Proc. 14th IEEE Workshop on Comput. Secur. Foundations*, pp. 82-96, Novia Scotia, Canada, 2001.

[14] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETS," *J. Netw. and Comput. Appl.*, vol. 36, pp. 1352-1364, 2013.

[15] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Info. Theory*, vol. IT-29, no. 2, pp. 198-208, 1983.

김 현 성 (Hyunsung Kim)

2002년 2월 : 경북대학교 컴퓨터공학과 공학박사

2002년 3월~현재 : 경일대학교 컴퓨터사이언스학부 정교수

2015년 12월~현재 : 말라위대학교 수학과 방문교수

2008년 12월~2010년 2월 : 더블린시립대학교 방문교수

<관심분야> 인지무선네트워크 보안, 네트워크 보안, 암호 프로토콜, 암호구현, 정보보호

[ORCID:0000-0002-78147454]