JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 8, pp. 1509-1517, Aug. 2022

Check for updates

IoV환경의 V2V 통신을 위한 경량 상호인증 프로토콜의 취약점 분석

박 현 욱[1] · 최 윤 성[2*]
[1]인제대학교 컴퓨터공학부 학사과정
[2*]인제대학교 AI융합대학 조교수

Security Analysis of a Lightweight Mutual Authentication Protocol for V2V Communication in IoV

Hyun-Wook Park[1] · Youn-Sung Choi[2*]

[1]Undergraduate Course, Department of Computer Science, Inje University, Gimhae-si 50834, Korea
[2*]Assistant Professor, AI Convergence College, Inje University, Gimhae-si 50834, Korea

[요 약]

현재의 도로교통은 주차, 환경, 안전 등의 많은 문제점을 마주하고 있다. 이것을 해결하기 위해 제안된 것이 스마트 이동수단이며, 이를 실현하는데 있어 중요한 시스템인 IoV(Internet of Vehicle)는 인터넷 통신이 가능한 자동차로 네트워크, 모바일기기, 다른 자동차 등의 외부 기기와 연결이 가능하다. 이러한 IoV 연구의 주요 과제는 안전한 인증과 통신 방법을 개발하는 것이다. 이에 Vasudev 등은 비밀 키를 이용하여 사용자가 서버에 안전하게 인증할 수 있는 경량 상호 인증 프로토콜을 설계하였다. 본 논문에서는 Vasudev 등의 프로토콜의 동작과정을 분석하여, 오프라인 ID, PW 추측 공격, 재전송 공격, 내부자의 사용자 위장, 완전 순방향 비밀성 미충족, 비트수 불일치의 보안 취약점이 있다는 것을 밝혀냈다.

[Abstract]

Current road traffic faces many problems such as parking, environment, and safety. To solve this problem, a smart transportation means is proposed, and the Internet of Vehicle (IoV), an important system for realizing this, is a vehicle capable of Internet communication and can be connected to external devices such as networks, mobile devices, and other vehicles. The main task of these IoV research is to develop secure authentication and communication methods. Accordingly, Vasudev et al. designed a lightweight mutual authentication protocol that allows users to securely authenticate to a server using a secret key. In this paper, we analyzed the protocol of Vasudev et al. and found several security weakness, offline ID, PW guessing attack, replay attack, user impersonation of insider, lack of perfect forward secrecy, and bit mismatch.

색인어 : 취약점 분석, 상호 인증 프로토콜, 차량 인터넷, 자동차 네트워크

Keyword : Weakness Analysis, Mutual Authentication Protocol, Internet of Vehicles, Vehicular Ad-hoc Network

http://dx.doi.org/10.9728/dcs.2022.23.8.1509

Received 21 June 2022; **Revised** 26 July 2022
Accepted 23 August 2022

***Corresponding Author; Youn-Sung Choi**

Tel: +82-055-320-3206
E-mail: cys2020@inje.ac.kr

Ⅰ. 서 론

오늘날 스마트 이동수단은 스마트 도시의 실현에 있어서 필수적인 요소이다. 도시 이동수단은 주차문제, 교통문제, 안전 문제, 환경 문제 등을 마주하게 된다. 지능적 교통 시스템(ITS)은 효율적이고 접근성이 좋으며 안전한 스마트 메커니즘을 제공함으로써 위의 문제를 해결할 수 있게 한다[1-5]. 스마트 이동수단을 가능하게 하는 가장 중요한 것은 Internet of Vehicle(IoV)이다 [6]. IoV는 인터넷 통신이 가능한 자동차로, 네트워크, 다른 개체(인프라, 도로 주변장치, 모바일 기기 등), 앱, 서비스 등의 외부 기기와 연결이 가능하다. IoV의 매력적인 점은 V2X라는 통신 요소인데, 'X'는 자동차, 인프라, 도로주변기기(RSU), 보행자, 센서, 모바일/휴대용 기기 등과 같은 모든 개체가 될 수 있고 [7] 차대차(V2V), 차대 인프라(V2I), 차대주변기기(V2R), 차대보행자(V2P), 차대센서(V2S), 그리고 차대모바일기기(V2M) 통신를 포함하고 있다.

인증 보안과 통신 보안을 보장하는 것이 IoV의 주된 연구 과제이다. 다양한 연구의 결과들 중 IoV시나리오에서 인증/통신과정[8]-[10]과 경량급[11]-[14]의 중요성에 대해 연구하였다는 것을 알 수 있었다. 경량급은 실행/계산 시간이 적음을 의미한다. 즉, 인증/통신과정에서 시간이 많이 걸리지 않는 구조를 경량이라 하며 이것이 프로토콜 설계의 주된 기준이 된다. 그러므로 사용자 인증/통신을 보장하는 경량급 보안 프로토콜을 설계하는 것이 필요하다. Vasudev 등은 기존의 인증 프로토콜에서 발생하는 취약점을 해결하면서도 비밀키를 이용하여 등록된 사용자를 클라우드 서버에 안전하게 인증할 수 있는 구조의 경량 상호 인증 프로토콜을 설계하였고 계산량을 줄이는 효과가 큰 것으로 분석하였다[15].

본 논문에서는 Vasudev 등이 제안한 프로토콜을 분석하고 그 과정에서 오프라인 패스워드 추측공격, 내부자 공격, 재전송 공격에 취약하고 완전 순방향 비밀성을 만족시키지 않으며 동작과정에서 비트수가 불일치 할 수 있다는 것을 발견했다.

본 논문의 구성은 먼저 2장에서 Vasudev 등이 제안한 프로토콜을 이해하기 위해 필요한 관련 연구들에 대해 설명하고 3장에서 Vasudev 등이 제안한 프로토콜의 등록 및 인증 과정을 분석하고 4장에서 Vasudev 등의 프로토콜에 대한 취약점 분석을 통해 밝혀진 문제점에 대해 설명한다. 마지막 5장에서 본 논문의 결론으로 논문을 마무리한다.

Ⅱ. 관련 연구

IoV의 정상적인 동작은 개체들 사이에서의 안전한 메시지 교환에 의존한다. IoV는 승객/운전자의 안전, 발전된 네비게이션, 안전하지 못한 응용프로그램 등의 응용 프로그램에 해결책을 제공한다는 것을 스스로 증명해야 한다. IoV를 기반 연구들은 RSU 또는 AP(Access Points), WiFi 등을 통한 연결이 가능함을 보이는데 성과를 거두었다 [16]-[19].

2-1 이전의 IoV 연구

현존하는 IoV 연구들은 서로 다른 컨셉을 기반으로 한다. Vasudev 등은 몇몇 연구들을 검토해 보았고 다음과 같다. 몇몇 연구들은 도로교통정보기구 [20], 최적화된 데이터 전송 [21], 저비용 네비게이션 시스템 또는 GPS 관련 [22], 교통흐름 예측과 충돌관리 [23] 등의 분야에서 이루어 졌다. 2017년에 Chen 등 [24]은 안전운전 향상을 위한 딥 러닝을 설계하였다. IoV에서 후방 충돌 회피 시스템의 의사결정을 위해 CPGN(GA 최적화 신경망 기반 충돌 예측 모델) 이라는 이름의 확률론적 모델이 제안되었다. 하지만 보안성을 측정하지 않았다. Liu 등 [25]은 자동차와 RSU들 사이에서의 안전한 통신을 위한 설계를 제안하였다. 처음에는 새로운 CLSS(certificateless short signature scheme, 인증서 없는 짧은 서명 스킴)를 설계하고 삭제 가능성이 있는지 랜덤 오라클에서 검사하였다. 효율적이고 익명인 빠른 상호 인증 스킴은 CLSS와 지역 관리 전략을 통합하여 설계되었다. 다른 스킴들과 비교하였을 때 주요 장점은 자동차와 RSU들 사이 상호작용의 고효율성이다. 그러나 계산 비용이 너무 많이 드는 것으로 측정되었다.

2-2 인증기반 VANET 또는 IoV 연구

2012년에 Mun 등 [26]은 Wu 등의 강화된 익명 인증 체계 [27]에 한계가 있음을 확인하였다. Mun 등은 이러한 약점을 극복하고 성능을 향상시키기 위해 타원 곡선 기반 Diffie-Hellman (ECDH)을 이용한 향상된 체계를 제안하였다. 이 스킴의 주요 장점은 MITM 공격에 안전함과 상호 인증의 보장이다. 2014년에는, Zhao 등[28]이 [26]의 한계를 확인하고 글로벌 모빌리티 네트워크에 서비스를 로밍하여 효율적인 인증 스킴으로 향상시켰다. 이 스킴의 주요 장점에는 익명성, 로컬 비밀번호 확인, 다양한 공격들에 대한 방어 등이 있다. Zhao 등은 이 스킴이 전력이 낮고 자원이 한정된 모바일 기기에 적합하며 그러므로 실제로 사용 가능하다고 주장한다. 그러나, 이 스킴은 계산 비용이 많이 들었다. 2017년에 Mohit 등 [29]은 사용자와 자동차들에게 교통 정보를 교환할 수 있도록 하는 WSN(Wireless Sensor Network, 무선 센서 네트워크) 기반의 보안 자동차 통신 스킴을 설계했다. 이 스킴은 효율적이고 스마트카드 도난 공격을 포함한 모든 공격에 안전하면서도 계산 비용이 적다. 이 스킴은 낮은 통신 비용이 드는 SHA-1 (160비트)을 사용하지만 충돌 공격에 취약하다. Ying 등[30]은 스마트카드(ASC) 기반의 익명 경량급 인증 스킴을 제안했다. 이 스킴은 저렴한 암호화 작업으로 사용자(차량)의 정당성과 데이터 메시지의 유효성을 입증할 수 있다. 그들은 통신과 계산 비용 측면에서 50% 이상의 비용을 절약할 수 있다고 주장했다. 최근에는 Chen 등[31]이 Ying 등의 결점을 찾아내었고 이를 개선한 IoV 보안 인증 프로토콜을 설계하였다. 하지만 Chen 등의 스킴 또한 데이터 처

리이 느리다는 단점이 있었다. Vasudev 등 기존의 IoV 인증 프로토콜에서 발생하던 취약점 문제를 해결하면서도 계산량을 줄인 경량 상호 인증 프로토콜을 설계하였다. Vasudev 등이 주장한 것처럼, Vasudev 등이 제안한 인증 프로토콜은 사용되는 계산량 측면에서는 우수하지만, 본 논문에서 분석한 것처럼 프로토콜 동작과정에서 발생하는 취약점이 존재하고 있었다.

Ⅲ. Vasudev 등의 프로토콜의 동작과정 분석

Vasudev 등은 호스트 인증이 가능하면서 자동차와 자동차 서버(VS)사이의 보안 키 발행 또한 가능한 보안 프로토콜을 설계하였다. 인증 프로세스는 호스트의 적합성을 인증하게 해주고 비밀 키를 사용해 앞으로의 의사소통에 생길 요청을 암호화한다. 표 1에서 의사소통 프로세스에 쓰이는 기호들을 정리하였다.

3-1 시스템 모델

등록과정이 끝나고 나면 RA(Registration Authority)는 TA(Trusted Authority)에 몇몇 파라미터를 즉시 전송한다. 이 방식은 RA가 인증 프로세스에 항상 참여하지 않아도 돼 RA의 오버헤드를 방지 할 수 있다는 이점을 가진다. 전송된 파라미터들은 의사소통 중 진실성 확인에 쓰인다. 또, 몇몇 파라미터들은 자동차 내(OBU)의 스마트카드에 저장되고 인증 과정에서 그 값들을 불러오게 된다. 제안된 프로토콜의 네트워크 모델은 그림 1에 있다.

오직 RA만이 등록과정에 참여하고 그 후 RA가 TA에 등록된 값들을 전송한다. 또, 의사소통 과정에서 자동차가 VS에 데이터를 요구할 때 마다 TA와 의사소통하고 진실성을 증명해야 한다. 성공적으로 인증이 되면 자동차는 VS에 필요한 요청을 할 수 있다. 그림 1에서 모든 의사소통은 양방향으로 이루어진다. 그러므로 자동차와 RA, 자동차와 TA, RA와 TA, TA와 VS를 양방향 화살표로 나타내었다. 여기서 고려되는 보안상의 중요점은 RA, TA, VS가 신뢰되는 개체로, 손상될 수 없다는 점이다. 이 시스템 모델은 아래의 설명을 기초로 두었다.

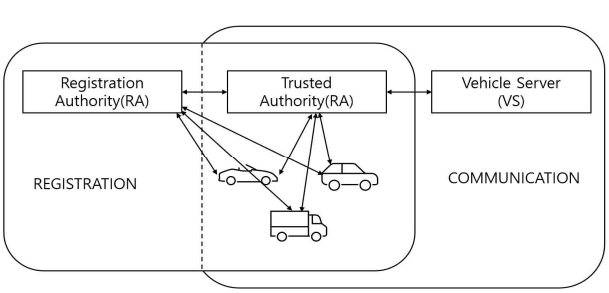

그림 1. 네트워크 모델
Fig. 1. Network Model

표 1. 제안된 프로토콜에서 쓰이는 용어 설명
Table 1. Symbols used in protocol

Notation	Description
UID_i	Identification Number of the i^{th} host
PW_i	Password of UID_i
CID	Identification Number of TA
SID_k	Identification Number of the k^{th} VS
$h(\bullet)$	One way cryptographic hash
Nu_i	Nonce generated by UID_i
Ns_k	Nonce generated by SID_k
K_s	Secret Key shared between VS and TA
$\|$	Concatenation operation
$\oplus$	XOR operation

① 등록된 자동차만 IoV 통신 시나리오에 참여할 수 있다.
② TA, RA, VS는 신뢰되는 개체이다.
③ 인증된/정당한 사용자는 신뢰하지 않는 사람과 절대로 패스워드를 공유하지 않는다.

3-2 적대적 모델

IoVs 통신은 무선 채널에서 수행되며, 여러 적대적 행위들이 이러한 통신을 수행하는 올바른 작업들에 악영향을 끼칠 수 있다. 공격자는 다양한 능력을 가지고 있을 수 있는데, 각각의 능력들은 서로 다른 스킬 세트, 별칭, 구조를 가진 공격자로 간주될 수 있다. 공격자($\dot{A}$)는 강력한 공격 능력을 가지고 있는데, 악의적 전송 반복을 통한 트래픽 혼잡 야기, 메시지 요청 수정, 다른 사용자로 위장, 메시지 가로채기, 순수 텍스트/메시지 수정 등 시스템의 기능에 악영향을 끼친다. 일반적으로, ($\dot{A}$)는 다른 종류의 작업들을 수행할 수 있다. 제안된 프로토콜에서 모든 파라미터들이 안전하지 않은 채널을 지나갈 때 ($\dot{A}$)는 데이터/메시지를 쉽게 공격할 수 있고 반복, 수정, 위장 등의 강한 악의적 적대 행위를 수행할 수 있다. ($\dot{A}$)가 아래와 같은 능력을 가지고 있다고 정의하였다.

① 모든 메시지들은 안전하지 않은 채널을 통과하므로, ($\dot{A}$)는 공격이 가능한 모든 것을 시도할 수 있다.
② ($\dot{A}$)는 사용자 ID, PW, 임의의 값과 같은 핵심 인증요소를 소지하고 있다면 시스템 전체를 공격할 수 있고 개체들 사이의 통신 지연을 발생시킬 수 있다.

③ $(\dot{A})$는 개체들 사이의 통신에 위장공격을 할 수 있으므로 신뢰받는 개인과 프로시드로 위장할 수 있다.

④ $(\dot{A})$는 스마트카드를 훔칠 수 있다. 내장된 파라미터들로 스마트카드 도난 행위를 할 수 있다. 공격자는 값을 가져가 다른 값들을 계산하는 데에 사용할 수 있다.

⑤ $(\dot{A})$는 오프라인 패스워드 추측 공격을 통해 패스워드를 추측할 수 있다.

⑥ $(\dot{A})$는 서로 다른 세션들로부터 메시지를 가로채어 추적할 수 없는 공격을 할 수 있다

⑦ $(\dot{A})$는 중간자 공격을 할 수 있다. 여기서 $(\dot{A})$는 서로 직접적으로 통신한다고 믿는 두 개체 사이에서 비밀리에 통신을 중재/수정할 수 있다.

⑧ $(\dot{A})$는 한 번에 한 개의 값만을 추측할 수 있다. 한 개의 값을 추측함으로써, $(\dot{A})$는 계산에 필요한 다른 파라미터들을 얻을 수 있다. 하지만, 다항 시간에서 하나 이상의 값은 추측될 수 없다.

3-3 등록단계

제안된 프로토콜은 등록 단계로 시작한다. VS에게 정보를 요청하기 위해 자동차는 RA에 등록하는 과정을 가진다. RA는 호스트 사용자의 신분을 확인하고 인증과 통신에 쓸 파라미터들을 저장한 스마트카드를 발급한다. 아래는 등록과정에 대한 설명이고 그림 2에 나타내었다.

① 사용자 / 운전자 / 호스트는 사용자 아이디와 패스워드 $< UID_i, PW_i >$를 랜덤 값 RU_i 와 함께 선택한다. H_i 가 은폐된 사용자 ID와 사용자의 패스워드를 $HUID_i = h(UID_i \| RU_i)$, $HPW_i = h(PW_i \| RU_i)$ 로 계산하고 보안 채널을 통해 RA로 전송한다. 보안 채널을 통해서 전송되기 때문에 데이터의 비밀성과 무결성을 보장할 수 있다.

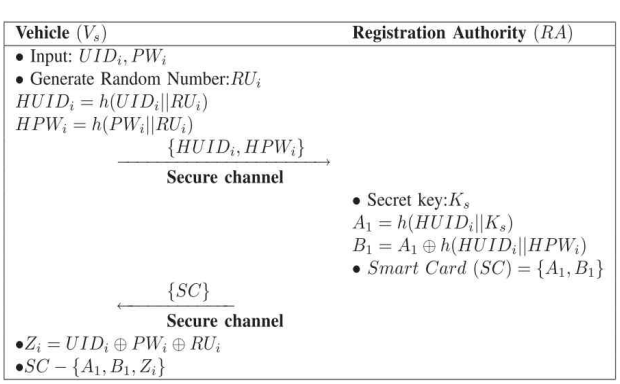

그림 2. 등록 단계
Fig. 2. Registration phase

② RA는 모든 호스트 기기들의 두 파라미터 A_1, B_1을 계산한다. $A_1 = h(HUID_i \| K_s)$로 계산되며 K_s는 TA와 VS에 의해 공유되는 비밀 키이다. $B_1 = A_1 \oplus h(HUID_i \| HPW_i)$로 계산한다. RA는 파라미터 A_1 과 B_1을 스마트카드에 저장하고 TA에 전송한 다. TA는 스마트카드를 보안 채널을 통해 H_i에 전송한다.

③ 스마트카드를 전송받은 뒤, H_i는 또 하나의 파라미터 $Z_i = UID_i \oplus PW_i \oplus RU_i$를 계산한다. H_i는 Z_i와 스마트카드값들을 앞으로의 통신을 위해 저장한다.

3-4 로그인, 인증, 통신 단계

등록 단계가 완료되고 나면 H_i는 VS에 정보를 요청하기 위해 로그인 후 TA에 자신을 인증해야 한다. TA는 RA에게 받은 사용자 정보를 인증 단계에서 사용할 수 있다. 인증 단계는 H_i의 타당성을 증명하고 제 3자 기기의 악의적 위장 행위를 방지할 수 있다. 인증 단계는 또한 VS에 보낸 요청의 응답을 받아올 때 올바른 서버임을 확인하기 위해 한 번 더 수행된다. 로그인, 인증, 통신 단계는 아래에 설명, 그림 3 에서 나타내었다.

① 사용자는 사용자 ID와 비밀번호로 로그인한다. UID_i와 PW_i를 확인할 때 쓰이는 B_1을 계산한다. 자동차(V_s)는 랜덤수 N_u와 타임스탬프 T_u을 생성한다. V_s는 인증에 쓰이는 세 개의 파라미터 Msg_1, X_1, Y_1을 계산한다. 그리고 Msg_1, Y_1, X_1을 각각 $Msg_1 = h(A_1 \| T_u \| HPW_i \| N_u)$, $Y_1 = h(B_1 \| HPW_i)$, $X_1 = N_u \oplus Y_1$로 계산한다. 그 후 $\{Msg_1, X_1, T_u, SID\}$ 가 TA로 메시지 형태로 보안이 없는 채널을 통해 전송된다.

② TA는 $Y_1 = h(B_1 \| HPW_i)$, $N_u^* = X_1 \oplus Y_1$을 계산한다. $Msg_1 = h(A_1 \| T_u \| HPW_i \| N_u^*)$를 계산하고 계산된 Msg_1이 채널로 전송되어 온 것과 같은지 확인한다. 이것은 수신한 메시지의 무결성을 확인하는데 쓰인다. TA는 $HCID$를 $HCID = h(HUID_i \| CID \| SID)$로 계산한다. Msg_2, X_2를 각각 $Msg_2 = h(HCID \| K_s \| T_c \| N_u)$, $X_2 = N_u \oplus h(K_s)$ 로 각각 계산한다. T_c는 TA가 생성한 타임스탬프이다. 마지막으로, $\{Msg_2, X_2, T_c, HCID\}$를 VS로 전송한다.

③ VS는 먼저 $N_u^* = X_2 \oplus h(K_s)$를 계산하고 $Msg_2 =$

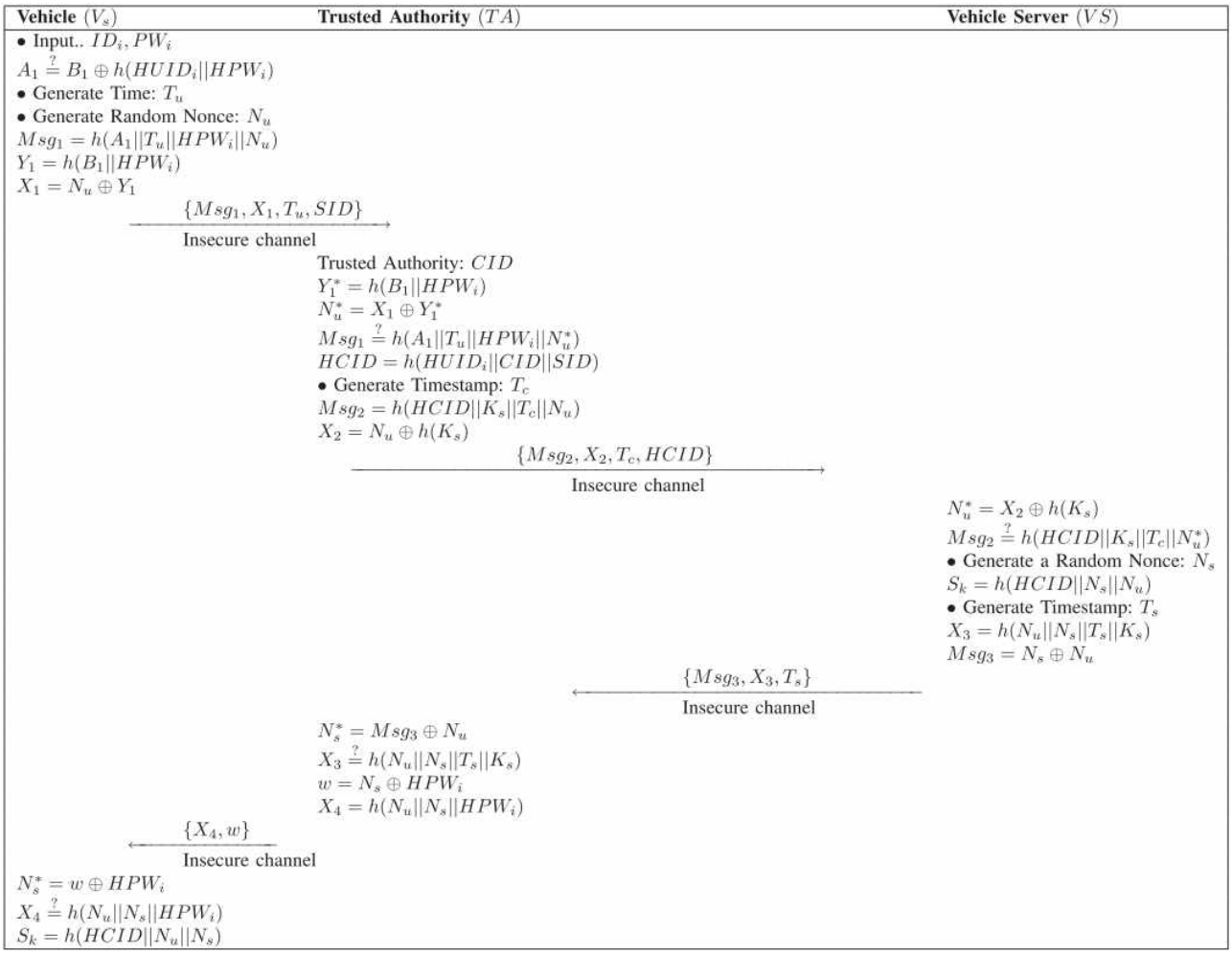

그림 3. 인증단계
Fig. 3. Authentication phase

$h(HCID||K_s||T_c||N_u^*)$를 확인한다. VS는 랜덤 값 N_s, 타임스탬프 T_s 를 생성한다. VS는 H_i와 공유해 비밀 키 $Sk = h(HCID||N_s||N_u)$를 생성한다. VS는 또한 $X_3 = h(N_u||N_s||T_s||K_s), Msg_3 = N_s \oplus N_u$를 계산한다. Msg_3, X_3, T_s 를 TA에 전송한다.

④ TA는 $N_s^* = Msg_3 \oplus N_u$를 계산하여 $X_3 = h(N_u||N_s^*||T_s||K_s)$가 맞는지 확인한다. TA는 $w = N_s \oplus HPW_i$, $X_4 = h(N_u||N_s||HPW_i)$를 계산, $\{X_4, w\}$를 VS에 전송한다.

⑤ V_s는 $N_s^* = w \oplus HWP_i$를 계산하여 $X_4 = h(N_u||N_s^*||HPW_i)$를 확인하고 비밀 키 $Sk = h(HCID||N_s||N_u)$를 계산한다.

⑥ 비밀 키는 앞으로의 V2V통신에 쓰인다. VS는 이 통신 후에 호스트의 신분과 Sk 를 저장한다. 자동차 V_a가 또 다른 자동차 V_b와 통신을 요구할 때, V_a는 V_a의 키로 메시지를 암호화한다. V_b가 메시지를 받으면 V_a의 신분을 VS에게 전송한다. VS는 V_b 와 V_a의 타당성을 확인한다(전송된 신분을 이용하여). 만약 이것이 성공적이면 VS는 V_a의 키를 보안채널을 통해 V_b로 보낸다.

Ⅳ. Vasudev 등의 프로로콜 취약점 분석

본 논문에서는 Vasudev 등의 프로로콜의 동작 과정을 분석하였다. Vasudev 등은 자신들의 프로토콜이 안전하다고 하지만 분석결과 오프라인 ID,PW 추측 공격, 내부자의 사용자 위장 공격, 완전 순방향 비밀성 결여, 재전송 공격, 비트수 불일치 등의 보안 취약점이 있음을 확인하였다. 아래에 각 취약점에 대한 설명을 하고 그림으로 나타내었다.

4-1 Offline ID, PW Guessing Attack

Vasudev 등의 논문에서 그들은 자신들의 프로토콜이 ID, PW 추측 공격에 안전하다고 하지만 스마트카드를 도난당할 경우 오프라인 ID, PW 추측 공격에 취약함을 확인했다.

공격자가 어떠한 방법으로 사용자의 스마트카드 값을 알 수 있다고 가정하면 공격자가 가질 수 있는 값은 A_1, B_1, Z_1 이다. 이 값들을 이용하면 등록단계에서 다음 식과 같이 랜덤 값 RU_i를 추측할 수 있다.

$$Z_i = UID_i \oplus PW_i \oplus RU_i \quad (1)$$
$$RU_i = UID_i \oplus PW_i \oplus Z_i$$

공격자는 스마트카드 값 Z_i를 알고 있기 때문에 등록과정의 계산에서 RU_i를 쉽게 유추할 수 있다. 인증단계에서 RU_i를 이용해 다음 수식을 도출해 낼 수 있다.

$$HUID_i = h(UID_i || (UID_i \oplus PW_i \oplus Z_i))$$
$$HPW_i = h(PW_i || (UID_i \oplus PW_i \oplus Z_i))$$

$$B_1 = A_1 \oplus h(HUID_i || HPW_i) \quad (2)$$

$$B_1 = A_1 \oplus h(h(UID_i || (UID_i \oplus PW_i \oplus Z_i)) || h(PW_i || (UID_i \oplus PW_i \oplus Z_i))$$

등록과정에서 공격자는 사용자 ID, PW를 랜덤 값 RU_i와 함께 암호화한 값인 $HUID_i$, HPW_i 의 계산과정을 모두 자신이 알고 있는 값으로 바꿀 수 있고 이것을 B_1 계산식에 대입하면 공격자는 사용자의 ID, PW를 제외한 모든 값들을 자신이 아는 값으로 수식을 바꿀 수 있다. 따라서 Vasudev 등의 프로토콜은 오프라인 ID, PW 추측 공격에 안전하지 않다. 그러므로 Vasudev 등이 제안한 프로토콜에서는 공격자가 사용자의 스마트카드를 획득하게 되면, 사용자의 ID뿐만 아니라 PW를 분석을 통해 알아낼 수 있다는 위협이 존재하고 있다.

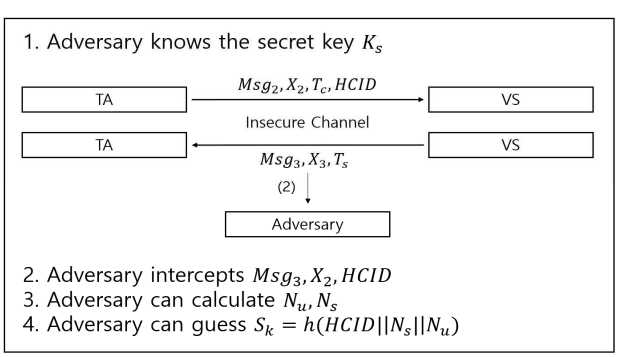

그림 4. Vasudev's Scheme의 완전 순방향 비밀성 미충족
Fig. 4. No perfect forward secrecy in Vasudev's Scheme

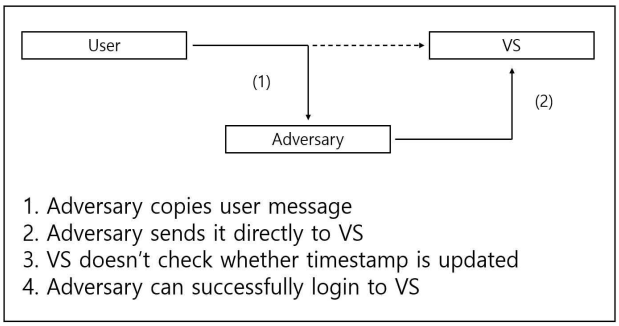

그림 5. Vasudev's Scheme의 재전송 공격
Fig. 5. Replay Attack in Vaudev's Scheme

4-2 Lack of Perfect Forward Secrecy

완전 순방향 비밀성은 서버의 long-term key(비밀 키 등)가 노출되더라도 그 후 통신에서 발생하는 세션 키는 노출되지 않아야 한다는 성질이다. Vasudev 등의 프로토콜에서 그들은 세션 키의 보안이 안전하다고 하지만 서버의 비밀 키가 노출될 경우 세션 키를 쉽게 추측할 수 있기 때문에 완전 순방향 비밀성을 만족하지 못하는 것으로 확인했다.

등록 단계에서 TA는 비밀 키 K_s를 발행한다. 인증단계의 모든 통신은 안전하지 않은 채널을 통과하기 때문에 공격자는 사용자와 서버 사이에서 주고받는 모든 값을 가로챌 수 있다. 공격자는 비밀 키 K_s를 이미 알고 있다고 가정하자. 공격자는 TA에서 V_s로의 통신에서 $HCID$와 X_2를, V_s 에서 TA로의 통신에서 Msg_3을 가로챈다. 그러고 나서 공격자는 $X_2 = N_u \oplus h(K_s)$에서 N_u를, $Msg_3 = N_s \oplus N_u$에서 N_s를 알아낼 수 있다. 최종적으로 세션 키 $S_k = h(HCID || N_s || N_u)$에서 공격자는 $HCID, N_u, N_s$ 모두를 알고 있으므로 쉽게 세션 키 S_k를 계산할 수 있다. 따라서 Vasudev 등의 스킴은 완전 순방향 비밀성을 만족하지 못한다. 그래서 Vasudev 등의 제안한 프로토콜에서는 서버에 저장되어 있는 비밀키 등을 포함한 long-term key가 노출되게 되면, 이전에 사용되었던 모든 세션키를 공격자가 알아낼 수 있는 문제가 존재하게 된다.

4-3 Replay Attack

재전송 공격이란 공격자가 사용자가 서버에 전송하는 데이터를 가로채 그대로 다시 서버에 재전송하여 올바른 사용자로 인증을 받는 공격이다. Vasudev 등의 프로토콜에서 사용자는 VS에 자신을 인증하기 위해 A_1, T_u, HPW_i, N_u를 해쉬함수로 암호화 하여 Msg_1로 전송하고 T_u, X_1 또한 전송한다. 전송된 값을 받은 중재자 TA는 T_u, X_1과 등록과정에서 RA로부터 전송받은 사용자 데이터를 계산해 Msg_1을 만들고 이것이 사용자로부터 받은 값과 같은지 확인하여 같다면

올바른 사용자로 인식하게 된다. 이 과정에서 공격자가 $\{Msg_1, X_1, T_u, SID\}$를 가로채어 서버에 재전송하면 TA는 타임스탬프 값인 T_u가 최신으로 갱신된 값인지 확인하는 절차를 거치지 않기 때문에 전송받은 T_u와 이것으로 계산한 Msg_1이 같다면 무조건 올바른 사용자로 인식할 수 밖에 없다. 따라서 Vasudev 등이 제안한 프로토콜에서는 공격자가 이전에 사용된 메시지를 이용하여 정상적인 사용자로 인증을 받을 수 있는 위험이 존재하므로 타임스탬프 점검을 추가할 필요가 있다.

4-4 Insider Attack - User Impersonation

내부자 공격이란 시스템 안의 권한을 가진 내부자가 권한을 악용해 적대적 행위를 하는 것을 말한다. Vasudev 등의 프로토콜에서 등록 기관인 RA의 내부자가 사용자 정보를 수집해 사용자로 위장할 수 있음을 확인하였다.

먼저 RA내부자는 사용자 V_s로부터 $HUID_i, HPW_i$를 받아오고 이 값들로 스마트 카드 파라미터 A_1, B_1을 계산할 수 있다. 또 인증단계에서 랜덤 값 N_u와 타임스탬프 T_u를 같은 비트 수의 랜덤한 값으로 생성한다. 내부자는 최종적으로 $Msg_1 = h(A_1 \| \ T_u \| HPW_i \| N_u)$, $X_1 = N_u + Y_1$, $Y_1 = h(B_1, HPW_i)$를 계산하고 TA에 이를 전송한다.

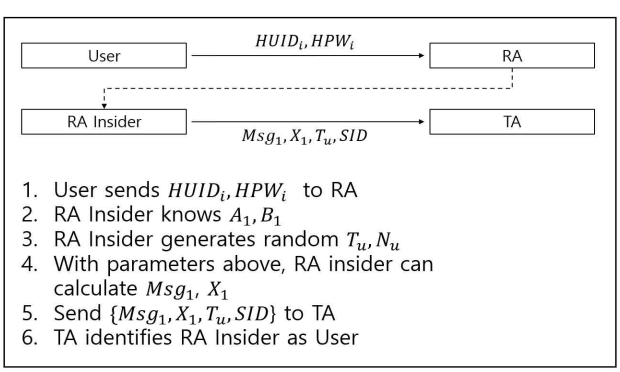

그림 6. Vasudev's Scheme의 내부자 공격
Fig. 6. Insider Attack in Vasudev's Scheme

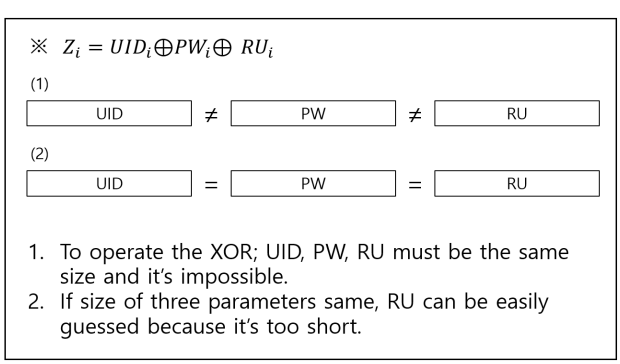

그림 7. Vasudev's Scheme의 비트 오류
Fig. 7. Bit Mismatch in Vasudev's Scheme

내부자는 인증에 필요한 값들을 모두 전송하였으므로 TA와 VS는 올바른 사용자로 인식하고 성공적으로 인증을 완료한다. 내부자는 사용자의 ID, PW를 몰라도 그 사용자로 인증을 할 수 있게 되는 것이다. 따라서 Vasudev 등의 프로토콜은 내부자의 사용자 위장 공격에 안전하지 못하다. Vasudev 등의 프로토콜에서 내부자의 의한 사용자 위장 공격이 가능하다는 위험이 존재하므로, 사용자 측면에서 프로토콜의 신뢰할 수 없는 문제가 발생하게 된다.

4-5 Bit Mismatch

Vasudev 등의 논문에서는 계산과정에서 XOR 연산을 자주 사용되는 것을 볼 수 있다. XOR 연산은 좌항과 우항의 비트 수가 일치하여야 한다. 하지만 Vasudev 등의 프로토콜의 XOR 연산에서 비트수가 일치하지 않을 수밖에 없는 경우가 있음을 확인하였다.

등록단계에서 스마트카드 값 Z_i를 계산하는 과정 $Z_i = UID_i \oplus PW_i \oplus RU_i$ 에서 사용자의 ID, PW와 랜덤 값 RU_i 세 파라미터를 한 번에 XOR 연산하는데 기본적으로 ID, PW가 비트 수가 일치할 수 없을뿐더러 RU_i와도 비트 수가 일치하기가 어렵다. 또 세 값의 비트 수가 일치한다고 가정하면 RU_i의 크기가 너무 작아 쉽게 추측될 수 있고 이는 보안상의 큰 취약점이 될 수 있다. Vasudev 등이 제안한 프로토콜에서 발생한 비트 불일치 오류는 프로토콜의 동작과 정상의 오류를 발생시킬 수 있어 성능적 측면에서 위험이 존재하고 있으며, 비트 불일치 오류를 수정하기 위해 RU_i의 크기를 작게 설정하면 안전성 측면에서 문제가 발생한다.

V. 결 론

Vasudev 등은 IoV에서 V2V 통신 경량급 상호 인증 프로토콜을 제안하였고 보안 분석에서 몇몇 공격에 안전하다고 하였다. Vasudev 등이 제안한 방식은 인증 프로토콜의 경량화에는 성과가 있었으나, 본 논문에서는 Vasudev 등의 프로토콜을 분석한 결과 오프라인 ID, PW 공격, 재전송 공격, 내부자의 사용자 위장 공격, 완전 순방향 비밀성 미충족, 비트 수 불일치의 취약점이 있음을 발견하였다. 본 논문을 통해 분석된 취약점을 해결하면서도 경량화된 상호 인증 프로토콜을 설계하는데 도움이 될 것으로 판단된다.

참고문헌

[1] S. I. Hwang, and J. W. Shim, "Semantic Network Analysis of 'Smart City' in Newspaper Articles - From 2016 to 2019 -," *Journal of Digital Contents Society,* Vol. 21, No. 5, pp.

941-950, May 2020.
https://doi.org/10.9728/dcs.2020.21.5.941

[2] H. J. Kim, T. S. Shon, “A Study on Cyber Security Threat Intelligence(CTI) Utilization for Smart City Security,” *Journal of Digital Contents Society*, Vol. 20, No. 6, pp. 1173-1180, Jun. 2019.
https://doi.org/10.9728/dcs.2019.20.6.1173

[3] H. S. Park et al. “Research Trend Analysis on Smart City based on Structural Topic Modeling(STM)”,*Journal of Digital Contents Society,* Vol. 20, No. 9, pp. 1839-1846, Sep. 2019. https://doi.org/10.9728/dcs.2019.20.9.1839

[4] D. J. Kim, “Implementation of Parking Management System using Cloud based License Plate Recognition Service”, Journal of Digital Contents Society, Vol. 19, No. 1, pp. 173-179, 2018. https://doi.org/10.9728/DCS.2018.19.1.173

[5] S. K. Park et al. “A study on the factors influencing the intention to adopt network streaming connection system characteristics in a smart city environment –focusing on IT industry workers,” *Journal of Digital Contents Society*, Vol. 21, No. 6, pp. 1131-1141, Jun. 2020.
https://doi.org/10.9728/dcs.2020.21.6.1131

[6] X. Wang et al., “A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of Vehicles,” *IEEE Commun. Mag.*, Vol. 56, No. 9, pp. 19–25, Sep. 2018.

[7] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, “V2X access technologies: Regulation, research, and remaining challenges,” *IEEE Commun. Surv. Tut.*, vol. 20, no. 3, pp. 1858–1877, Jul.–Sep. 2018.
https://doi.org/10.1109/comst.2018.2808444

[8] H. Vasudev and D. Das, An efficient authentication and secure vehicle-to-vehicle communications in an IoV, in *Proc. IEEE 89th Veh. Technol. Conf.*, pp. 1–5, Apr. 2019.

[9] T. Qiu, X. Liu, K. Li, Q. Hu, A.K. Sangaiah, and N. Chen, “Community-aware data propagation with small world feature for Internet of Vehicles,” *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 86–91, Jan. 2018.

[10] H. Vasudev and D. Das, A lightweight authentication protocol for V2V communication in VANETs, in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov.*, pp. 1237–1242, Oct. 2018.

[11] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, “2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET,” *IEEE Trans. Veh. Technol.*, Vol. 65, No. 2, pp. 896–911, Feb. 2016.
https://doi.org/10.1109/TVT.2015.2402166

[12] H. Vasudev and D. Das, Secure lightweight data transmission scheme for vehicular Ad hoc networks, in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst.*, pp. 1–6. 2018.

[13] S. Jiang, X. Zhu, and L. Wang, “An efficient anonymous batch authentication scheme based on HMAC for VANETs,” *IEEE Trans. Intell. Transp. Syst.*, Vol. 17, No. 8, pp. 2193–2204, 2016.
https://doi.org/10.1109/TITS.2016.2517603

[14] H. Vasudev and D. Das, A lightweight authentication and communication protocol in vehicular cloud computing, in *Proc. Int. Conf. Inf. Netw.*, pp. 72–77, 2019.

[15] H. Vasudev et al., "A lightweight mutual authentication protocol for V2V communication in internet of vehicles," *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 6, pp. 6709-6717, June, 2020.
https://doi.org/10.1109/tvt.2020.2986585

[16] J. Ott and D. Kutscher, “A disconnection-tolerant transport for drive-thru internet environments,” in *Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc.*, vol. 3, pp. 1849–1862, Mar. 2005.

[17] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine, and J. Zahorjan, “Interactive WiFi connectivity for moving vehicles,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 4, pp. 427–438, Aug. 2008.
https://doi.org/10.1145/1402946.1403006

[18] A. U. Joshi, and P. Kulkarni, “Vehicular WiFi access and rate adaptation,” in *Proc. SIGCOMM*, pp. 423–424, 2010.

[19] F. Xu et al., “Utilizing shared vehicle trajectories for data forwarding in vehicular networks,” in *Proc. IEEE INFOCOM*, pp. 441–445, Apr. 2011.

[20] J. Ahn, Y. Wang, B. Yu, F. Bai, and B. Krishnamachari, “RISA: Distributed road information sharing architecture,” in *Proc. IEEE INFOCOM*, pp. 1494–1502, Mar. 2012.

[21] C. T. Calafate et al., “An efficient and robust content delivery solution for IEEE 802.11 p vehicular environ ments,” *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 753–762, 2012. https://doi.org/10.1016/j.jnca.2011.11.008

[22] Z. Wu, M. Yao, H. Ma, and W. Jia, “Improving accuracy of the vehicle attitude estimation for low-cost INS/GPS integration aided by the GPS-measured course angle,” *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 553–564, Jun. 2013. https://doi.org/10.1109/TITS.2012.2224343

[23] A. Abadi, T. Rajabioun, and P. A. Ioannou, “Traffic flow prediction for road transportation networks with limited traffic data,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 653–662, Apr. 2015.
https://doi.org/10.1109/TITS.2014.2337238

[24] C. Chen, H. Xiang, T. Qiu, C. Wang, Y. Zhou, and V. Chang, “A rear-end collision prediction scheme based on deep learning in the Internet of Vehicles,” *J. Parallel Distrib. Comput.*, vol. 117, pp. 192–204, 2018. https://doi.org/10.1016/j.jpdc.2017.08.014

[25] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, An efficient anonymous authentication scheme for Internet of Vehicles, in *Proc. IEEE Int. Conf. Commun.*, pp. 1–6, May 2018.

[26] H. Mun, K. Han, Y. S. Lee, C. Y. Yeun, and H. H. Choi, “Enhanced secure anonymous authentication scheme for roaming service in global mobility networks,” *Math. Comput. Modelling*, vol. 55, no. 1–2, pp. 214–222, 2018.

[27] C. C.Wu,W. B. Lee, andW. J. Tsaur, “A secure authentica tion scheme with anonymity for wireless communications,” *IEEE Commun. Lett.*, vol. 12, no. 10, pp. 722–723, Oct. 2008. https://doi.org/10.1109/LCOMM.2008.080283

[28] D. Zhao, H. Peng, L. Li, and Y. Yang, “A secure and effective anonymous authentication scheme for roaming service in global mobility networks,” *Wireless Personal Commun.*, vol. 78, no. 1, pp. 247–269, 2014.

[29] M. Prerna, A. Ruhul, and G. P. Biswas, “Design of authentication protocol for wireless sensor network-based smart vehicular system,” *Veh. Commun.*, vol. 9, pp. 64–71, Jul. 2017.

[30] X. Li et al., “A robust ECC based provable secure authentication protocol with privacy protection for indu strial Internet of Things,” *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018. https://doi.org/10.1109/tii.2017.2773666

[31] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, “Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks,” *Multimedia Syst.*, vol. 21, no. 1, pp. 49–60, 2015.

박현욱(Hyun-Wook Park)

2018년 3월～현 재 : 인제대학교 컴퓨터공학부 학사과정

※관심분야 : 정보보호, 취약점 분석, 인증 프로토콜

최윤성(Youn-Sung Choi)

2006년 2월 : 성균관대 정보통신공학부 (공학학사)
2007년 8월 : 성균관대학교 전자전기 컴퓨터공학부 (공학석사)
2015년 8월 : 성균관대학교 전자전기 컴퓨터공학부 (공학박사)
2016년 3월～2020년 2월 : 호원대학교 사이버보안학과 조교수
2020년 3월～현 재 : 인제대학교 AI 융합대학 (산업보안전공) 조교수

※관심분야 : 정보보호, 디지털포렌식, 산업보안