UAV 기반 IoV 환경에서 인증 및 키 합의 방식의 보안 취약점 분석 및 대응 방안

최지혜, 오지현, 손승환, 김명현, 박영호
경북대학교

jihye@knu.ac.kr, j2hnoh@knu.ac.kr, sonshwan@knu.ac.kr, kimmyeong123@knu.ac.kr, parkyh@knu.ac.kr

Cryptanalysis and countermeasures of authentication and key agreement scheme in UAV-assisted Internet of Vehicles

Choi Ji Hye, Oh Ji Hyeon, Son Seung Hwan, Kim Myeong Hyun, Park Young Ho
Kyungpook National Univ.

요 약

2024년 Miao 등은 IoV 환경에서의 차량, UAV 및 RSU 간의 상호 인증 프로토콜을 제안하였다. 그러나 Miao 등이 제안한 프로토콜은 중간자 공격 및 known session specific temporary information 공격에 취약할 뿐만 아니라 상호 인증을 보장하지 못함으로써 IoV 환경에서의 안전한 통신이 불가능하다. 본 논문에서는 비정형 분석을 통해 Miao 등의 프로토콜을 분석하고 안전한 상호 인증을 위한 대응 방안을 제시한다.

Ⅰ. 서 론

정보통신기술의 발전에 따라 IoV(Internet of Vehicles)에 대한 관심이 증가하고 있다[1]. IoV 환경은 RSU(Road Side Unit)를 활용하여 실시간으로 변화하는 교통 상황을 효율적으로 관리한다[2]. 그러나 RSU의 고정된 위치로 인한 물리적인 통신 한계가 존재한다. 이러한 문제점을 개선하기 위해 제시되는 해결책 중 하나가 UAV(Unmanned Aerial Vehicle)이며, UAV는 공중에서 자유롭게 이동함으로써 RSU의 위치적 한계를 보완할 수 있다[2, 3]. 그러나 최근에 이루어지고 있는 UAV를 이용한 연구는 통신 연결 및 궤적 최적화에 집중되어 있으며, UAV와 차량 간의 안전한 상호 인증 프로토콜에 대한 연구는 부족한 실정이다. IoV 환경에서 UAV와 차량은 공개된 무선 채널을 통해 정보를 교환하기 때문에 다양한 보안 공격에 취약할 수 있다[4, 5]. 따라서 안전한 통신을 위한 상호 인증 프로토콜을 구축하는 것이 중요하다. 이와 관련하여 2024년, Miao 등은 IoV 환경에서 차량, RSU 및 UAV 간의 타원곡선 암호를 이용한 인증 프로토콜을 제안하였다[6].

본 논문에서는 Miao 등이 제안한 프로토콜을 비정형 분석을 통해 중간자 공격, known session specific temporary information 공격에 취약함을 보이고 이를 안전하게 보완하기 위한 대응 방안을 제시한다.

Ⅱ. Miao 등이 제안한 인증 및 키 합의 방식

Miao 등이 제안한 인증 및 키 합의 방식은 차량 등록, UAV 등록 및 RSU 등록 단계와 인증 단계로 구성된다. 각 개체는 모두 TA(Trusted Authority)를 통해 등록 단계를 거친다. 본 논문에서 사용되는 매개 변수는 다음 표 1과 같다.

표 1. 매개변수

기호	의미
TA	Trusted Authority
H	해시 함수
RSU	Road Side Unit
V	차량
UAV	Unmanned Aerial Vehicle
RID_j	RSU의 Identity
$\oplus$	XOR 연산
T_i	Timestamp
s	TA의 마스터 키
$\|$	Concatenation 연산
TID_i	차량의 Temporary Identity
SK	세션 키

2.1 Miao 등의 차량 등록 단계

다음 그림 1은 Miao 등이 제안한 인증 프로토콜의 차량 등록 단계이다.

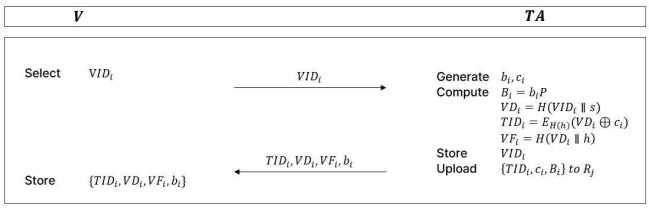

그림 1. 차량 등록 단계.

2.2 Miao 등의 UAV 등록 단계

다음 그림 2는 Miao 등이 제안한 인증 프로토콜의 UAV 등록 단계이다.

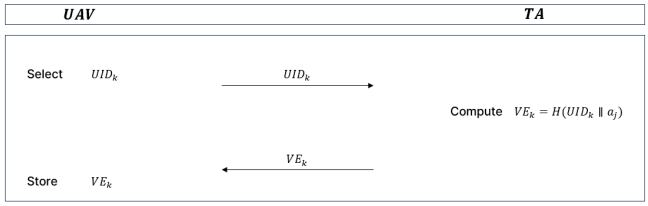

그림 2. UAV 등록 단계.

2.3 Miao 등의 RSU 등록 단계

다음 그림 3은 Miao 등이 제안한 인증 프로토콜의 RSU 등록 단계이다.

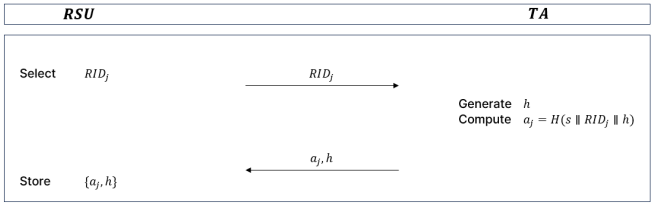

그림 3. RSU 등록 단계.

2,4 Miao 등의 인증 단계

다음 그림 4는 Miao 등이 제안한 인증 프로토콜의 인증 단계이다.

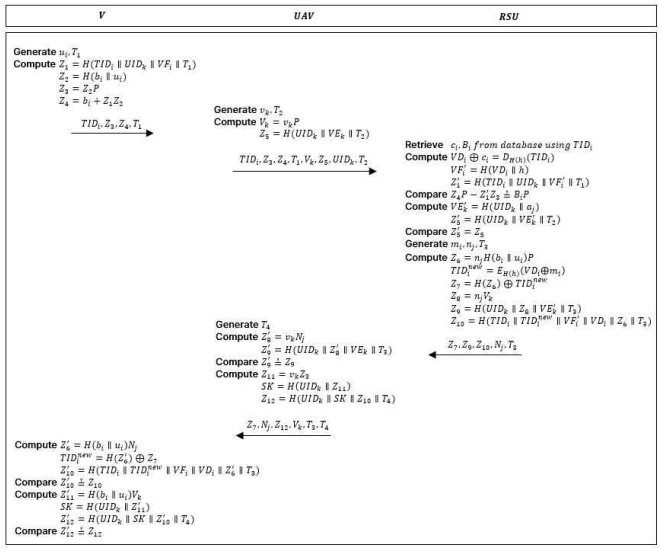

그림 4. 인증 단계.

Ⅲ. Miao 등이 제안한 프로토콜의 보안 취약점 및 대응 방안

본 논문에서는 비정형 보안 분석을 통해 Miao 등이 제안한 인증 프로토콜의 안전성을 분석하여 중간자 공격 및 known session specific temporary information 공격에 취약하고 차량, UAV 및 RSU 간의 상호 인증을 보장하지 않음을 증명한다. Miao 등이 제안한 프로토콜의 취약점 및 대응 방안은 다음과 같다.

3.1 취약점

3.1.1 중간자 공격

공격자는 자신의 임의의 난수인 r_a을 생성하고 $Z_a = r_a P$를 계산하여 UAV에게 $\{TID_i, Z_a, Z_4, T_1\}$을 전달한다. 그리고 UAV가 RSU에게 보내는 메시지 $\{TID_i, Z_a, Z_4, T_1, V_k, Z_5, UID_k, T_2\}$를 탈취한 뒤 RSU 에게 $\{TID_i, Z_3, Z_4, T_1, V_k, Z_5, UID_k, T_2\}$을 보낸다. RSU는 받은 Z_3,Z_4을 이용해 차량을 인증하고 Z_5를 이용해 UAV를 인증한다. 그 후 공격자는 UAV가 차량에게 보내는 메시지로부터 탈취한 뒤, 임의의 난수인 r_a를 이용해 $SK_a = H(UID_k \| r_a Z_3)$, $Z_{12a} = H(UID_k \| SK_a \| Z_{10} \| T_4)$를 계산하여 $\{Z_7, N_j, Z_{12a}, Z_a, T_3, T_4\}$를 차량에게 보낸다. 차량과 UAV는 각각 자신의 임의의 난수와 공격자의 임의의 난수 r_a가 곱해진 Z_{11}을 계산하게 되고 공격자와 같은 세션 키를 공유하게 된다.

3.1.2 known session specific temporary information 공격

공격자가 UAV가 생성하는 임의의 난수인 v_k를 알아낼 경우, 공개 채널로 전송되는 Z_3 값과 함께 $Z_{11} = v_k Z_3$을 계산할 수 있다. 그 후 공개 채널로 전송되는 UID_k 값을 통해 세션 키인 $SK = H(UID_k \| Z_{11})$을 얻어낼 수 있다.

3.2 대응 방안

Miao 등이 제안한 인증 프로토콜은 중간자 공격 및 known session specific temporary information 공격에 취약하며 UAV와 차량 간의 상호 인증을 보장하지 않는다. 타원곡선 암호 기반의 대칭 키 $Z_{11} = H(b_i \| u_i) v_k P$ 가 세션 키 생성에 이용되며, 공격자가 개체로부터 생성된 임의의 난수 값을 알거나 Z_{11} 값을 조작할 경우, 세션 키를 계산해낼 수 있다. 이 점을 보완하는 방법은 UAV와 차량 간의 사전 공유 키를 만들고 이것을 암호화 및 세션 키 합의에 이용하는 것이다. 등록 단계에서 TA가 차량과 UAV 만의 비밀 공유 키를 배분할 경우, 공격자가 중간자 공격을 시도하거나 세션 키 계산에 이용되는 임의의 난수를 알아도 사전 공유 키 값을 알지 못하면 메시지 복호화 및 세션 키 계산이 불가능하다.

Ⅳ. 결론

본 논문에서는 Miao 등이 제안한 IoV 환경에서의 차량, UAV 및 RSU 간의 인증 프로토콜이 중간자 공격과 known session specific temporary 공격에 취약함을 보임으로써 상호 인증이 제대로 이루어지지 않음을 증명하였다. 또한 위 취약점을 보완하기 위하여 차량과 UAV 간의 사전에 합의된 공유 키를 이용해 암호화 및 세션 키 합의 대응 방안을 제시하였다. 본 논문에서 제시한 대응 방안을 통해 IoV 환경에서 차량과 UAV 간의 안전한 상호 인증과 세션 키의 안전성을 보장하는 프로토콜을 제안할 수 있다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

[1] Yu, S., Lee, J., Park, K., Das, A. K., and Park, Y. “IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment,” IEEE access, pp. 167875-167886, Sep. 2020.

[2] Son, S., Kwon, D., Lee, S., Jeon, Y., Das, A. K., and Park, Y. “Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF,” IEEE Access, pp. 60240-60253, Jun. 2023.

[3] Sedjelmaci, H., Messous, M. A., Senouci, S. M., and Brahmi, I. H. “Toward a lightweight and efficient UAV aided VANET,” Transactions on Emerging Telecommunications Technologies, e3520, Aug. 2019.

[4] Kim, M., Lee, J., Oh, J., Park, K., Park, Y., and Park, K. “Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers,” Applied Energy, pp. 119445-119453, Sep. 2022.

[5] Park, Y., Ryu, D., Kwon, D., and Park, Y. “Provably secure mutual authentication and key agreement scheme using PUF in internet of drones deployments,” Sensors, pp. 2034-2048, Feb. 2023.

[6] Miao, J., Wang, Z., Ning, X., Shankar, A., Maple, C., and Rodrigues, J. J. “A UAV-Assisted Authentication Protocol for Internet of Vehicles,” IEEE Transactions on Intelligent Transportation Systems, Mar. 2024.