IoD 환경에서의 인증 프로토콜 보안 취약점 분석 및 대응 방안

최지혜, 김채언, 박영호
경북대학교
jihye@knu.ac.kr, chaeon@knu.ac.kr, parkyh@knu.ac.kr

Cryptanalysis and countermeasures of authentication and key agreement scheme in Internet of Drones

Choi Ji Hye, Kim Chae Eon, Park Young Ho
Kyungpook National Univ.

요 약

최근 정보 통신 기술의 발전 및 드론 기술의 발전으로 인해 Internet of Drones(IoD)에 관한 관심이 점차 증가하고 있다. 하지만, IoD 환경에서의 통신은 공개된 무선 채널을 통해 데이터 교환이 이루어지기 때문에 다양한 보안 위협에 노출될 가능성이 존재한다. 이에 대응하기 위하여 2023년, Hussain 등은 IoD 환경에서의 안전한 상호 인증을 위한 프로토콜을 제안하였다. 그러나, Hussain 등이 제안한 프로토콜은 위장 공격 및 드론 캡처 공격에 취약함을 보였다. 본 논문에서는 Hussain 등이 제안한 프로토콜을 보안 분석하고 취약점에 보완할 수 있는 대응 방안을 제시하고자 한다.

Ⅰ. 서 론

Internet of Drones (IoD)는 드론의 높은 기동성을 이용하여 인간에게 편의를 제공할 수 있기 때문에, 최근 많은 주목을 받고 있는 산업 중 하나이다[1]. 드론은 인간이 하기 힘든 일을 대체할 수 있고 산업 모니터링, 농업, 배송 서비스 등 다양한 분야에서 활용될 수 있다[2]. IoD 환경에서 드론은 일반적으로 control server (CS)와 통신하며 데이터를 교환하고, 사용자에게 편리한 서비스를 제공한다[3]. 하지만, IoD 환경에서의 통신은 공개된 무선 채널을 통해 이루어지기 때문에 중간자, 위장, 재전송 공격 등 다양한 보안 공격에 취약할 수 있다[4]. 따라서, 사용자와 드론 간의 안전한 상호 인증 프로토콜이 필수적이다.

2023년, Hussain 등은 IoD 환경에서 드론과 사용자 간의 상호 인증 프로토콜을 제안하였다[5]. 하지만, Hussain 등이 제안한 방식은 위장 공격에 취약하며 상호 인증을 제대로 보장하지 못하는 문제점이 있다. 본 논문에서는 Hussain 등이 제안한 인증 프로토콜을 살펴보고, 보안 분석을 통해 해당 취약점 및 대응 방안에 대해 논의하고자 한다.

Ⅱ. 본론

2.1 Hussain 등이 제안한 인증 프로토콜

Hussain 등이 제안한 인증 및 키 합의 방식은 사용자 등록, 드론 등록과 인증 및 키 합의 단계로 구성된다. 먼저, 사용자 U_i와 드론 D_j는 CS를 통해 등록 단계를 거친 후, 각각의 비밀 키인 ρ_i와 ρ_j를 CS와 공유하게 된다.

사용자 등록 단계의 경우, 사용자가 자신의 아이디 ID_i와 패스워드 PWD_i를 선택한 뒤 CS에게 전송하면 CS가 마스터 키 MSK를 이용하여 사용자의 비밀 키 ρ_i 및 임시 아이디 TID_i를 계산하여 다시 사용자에게 보내준다. 사용자는 이를 자신의 아이디와 패스워드로 암호화하여 저장하게 된다.

드론 등록 단계의 경우, 드론이 자신의 아이디 ID_{D_j}를 선택한 후 CS로부터 비밀 키 ρ_j를 받고 이를 자신의 메모리에 저장하는 과정이다.

이후의 인증 및 키 합의 단계에서 사용자와 드론은 세션 키 합의를 위한 임의의 난수 R_2와 R_3을 생성한 후, 등록 단계에서 공유한 비밀 키 값으로 암호화하여 전송하고, 이 임의의 난수 값을 이용하여 세션 키를 계산한다. Hussain 등이 제안한 프로토콜의 자세한 과정은 다음 그림 1-3과 같다.

2.1.1 Hussain 등의 드론 등록 단계

다음 그림 1은 Hussain 등이 제안한 프로토콜의 드론 등록 단계이다.

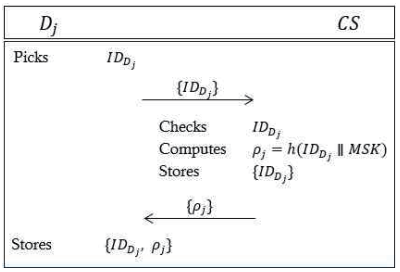

그림 1. 드론 등록 단계.

2.1.2 Hussain 등의 사용자 등록 단계

다음 그림 2는 Hussain 등이 제안한 프로토콜의 사용자 등록 단계이다.

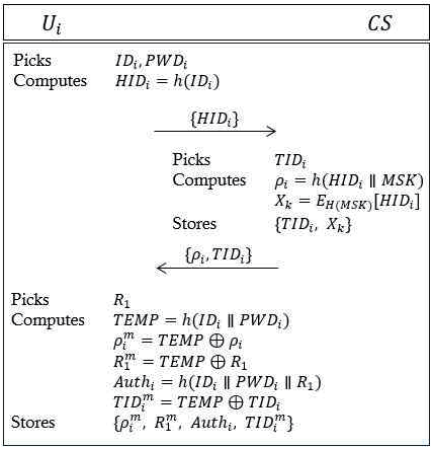

그림 2. 사용자 등록 단계.

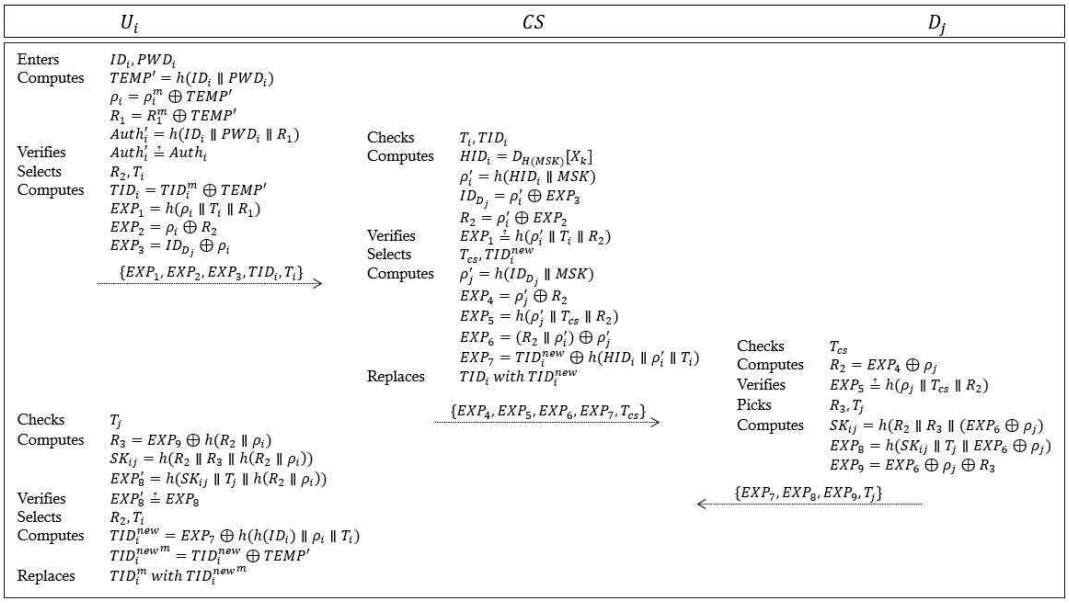

그림 3. 인증 및 키 합의 단계.

2.1.3 Hussain 등의 인증 단계

다음 그림 3은 Hussain 등이 제안한 프로토콜의 인증 및 키 합의 단계이다.

2.2 보안 취약점

본 논문에서는 비정형 보안 분석을 통해 Hussain 등이 제안한 인증 프로토콜이 위장 공격 및 드론 캡처 공격에 취약함을 다음과 같이 증명한다.

2.2.1 위장 공격

공격자는 power analysis 공격을 통해 탈취한 사용자의 스마트 디바이스로부터 $\{\rho_i^m, R_1^m, Auth_i, TID_i^m\}$을 얻을 수 있다. 또한 공격자는 공개 채널로 전송되는 TID_i를 탈취할 수 있다. 이를 통해 $TEMP = TID_i^m \oplus TID_i$를 계산하고 $\rho_i = \rho_i^m \oplus TEMP$를 얻을 수 있다. 공격자가 사용자의 비밀 키인 ρ_i를 알게 될 경우, 메시지 $\{EXP_1, EXP_2, EXP_3, TID_i, T_i\}$를 생성할 수 있기 때문에 위장 공격을 시도할 수 있고 결과적으로 드론과 세션 키를 합의할 수 있다.

2.2.2 드론 캡처 공격

공격자가 드론 D_j를 캡처하여 드론에 저장된 비밀 키 ρ_j를 얻어낼 경우, 공개 채널을 통해 전송되는 메시지들을 이용하여 $R_2 = EXP_4 \oplus \rho_j$, $R_3 = EXP_9 \oplus EXP_6 \oplus \rho_j$를 계산할 수 있다. 따라서, 공격자는 최종적으로 세션 키 $SK_{ij} = h(R_2 \| R_3 \| EXP_6 \oplus \rho_j)$를 얻을 수 있다.

2.3 대응 방안

위장 공격의 경우, 사용자 등록 과정에서 R_1, ρ_i, TID_i를 모두 같은 $TEMP$를 이용하여 마스킹하는 것이 문제점이 된다. 따라서, $\{R_1^m = R_1 \oplus TEMP,\ \rho_i^m = \rho_i \oplus h(TEMP \| R_1),\ TID_i\}$와 같이 다른 값으로 마스킹하여 저장하면 사용자의 비밀 키인 ρ_i가 유출되는 것을 막을 수 있다. 드론 캡처 공격의 경우, physical unclonable function(PUF)를 이용할 수 있다. PUF의 challenge-response 값의 유일성을 활용하여 드론의 비밀 키인 ρ_j를 response 값으로 마스킹하여 저장하면, 드론 캡처 공격을 방지할 수 있다.

Ⅲ. 결론

본 논문에서는 Hussain 등이 제안한 IoD 환경에서의 사용자 및 드론 간의 인증 프로토콜을 보안 분석하여 위장 공격과 드론 캡처 공격에 취약함을 확인하였다. 이러한 보안 취약점은 실제 IoD 환경에서 사용자와 드론 간의 안전한 통신을 저해하고 시스템 전체의 신뢰성을 위협할 수 있다. 따라서, 본 논문은 위 취약점을 보완하기 위한 각각의 대응 방안을 제시하였다. 본 논문에서 제시한 대응 방안을 통해 IoD 환경에서 사용자 및 드론 간의 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., Das, A. K., Park, Y. "SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments," IEEE Transactions on Vehicular Technology, pp. 10374-10388, Jul. 2022.

[2] Yu, S., Das, A. K., Park, Y. "RLBA-UAV: A Robust and Lightweight Blockchain-Based Authentication and Key Agreement Scheme for PUF-Enabled UAVs," IEEE Transactions on Intelligent Transportation Systems, pp. 21697-21708, Oct. 2024.

[3] 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. 2034-2058, Feb. 2023.

[4] Zhang, Z., Hsu, C., Au, M. H., Harn, L., Cui, J., Xia, Z., and Zhao, Z. "PRLAP-IoD: A PUF-based robust and lightweight authentication protocol for Internet of Drones," Computer Networks, pp. 110118-110129, Jan. 2024.

[5] Sharma, M., Narwal, B., Anand, R., Mohapatra, A. K., and Yadav, R. "PSECAS: A physical unclonable function based secure authentication scheme for Internet of Drones," Computer and Electrical Engineering, pp. 108662-108678, May. 2023.