IoD 환경에서의 PUF 기반 경량 인증 프로토콜에 관한 취약점 분석 및 대응방안 연구

김채언, 최지혜, 권덕규, 박영호

경북대학교

chaeon@knu.ac.kr, jihye@knu.ac.kr, kdk145@knu.ac.kr, parkyh@knu.ac.kr

A Study on Security Analysis and Countermeasures for a PUF-based Lightweight Authentication Protocol in IoD Environments

Kim Chae Eon, Choi Ji Hye, Kwon Deok Kyu, Park Young Ho

Kyungpook National Univ.

요 약

최근 주목받고 있는 IoD (Internet of Drones) 환경에서는 드론이 다양한 분야에서 정보를 수집하고 처리하는 데 활용되고 있다. 그러나 드론은 물리적 공격에 쉽게 노출될 수 있으며, 제한된 자원과 실시간 통신 요구로 인해 보안 설계에 제약이 따른다. 이러한 문제를 해결하기 위해 2024년 Zhang 등은 PUF(Physical Unclonable Function)를 활용한 경량 인증 프로토콜을 제안하였으나, 다양한 보안 위협에 취약함을 확인하였다. 본 논문에서는 보안 분석을 통해 Zhang 등이 제안한 프로토콜의 보안 취약점을 증명하고 이를 개선할 대응방안을 제시하였다.

Ⅰ. 서 론

최근 드론 기술이 발전함에 따라, IoD (Internet of Drones) 환경이 학계와 산업계에서 주목받고 있다. 드론의 센서 및 통신 모듈을 통해 수집한 데이터를 바탕으로, 구조, 물류, 군사 정찰, 교통 감시 등 다양한 분야에서 활용되고 있다[1]. 그러나 드론은 무인 환경에서 운용되며, 데이터를 무선으로 전송하기 때문에 물리적 공격[2]뿐만 아니라 공개 채널을 통한 통신 메시지 변조 및 재전송 등의 다양한 보안 공격에 쉽게 노출될 수 있다[3]. 이러한 문제를 해결하기 위해 상호 인증을 포함한 안전한 인증 및 키 합의 프로토콜이 필요하다. 또한 드론은 배터리 용량, 메모리, 계산 능력 등 자원이 제한적인 장치이기 때문에 프로토콜의 경량성과 효율성도 중요하게 고려되어야 한다. 최근 Zhang 등[4]은 IoD 환경을 고려하여 PUF (Physical Unclonable Function)[5] 기반의 경량 인증 프로토콜을 제안하였으나, 해당 프로토콜은 내부자 공격, 재전송 공격, 임시 비밀 유출 등에 취약함을 발견하였다. 본 논문은 Zhang 등이 제안한 프로토콜의 보안성을 분석하고 안전한 인증을 위한 대응방안을 제시한다.

Ⅱ. 본론

2.1 시스템 모델

Zhang 등이 제안한 시스템 모델은 그림 1과 같다. 드론-게이트웨이-서버 3계층 프레임으로 구성되며, 서버, 게이트웨이, 사용자, 드론 4가지로 구성된다. 게이트웨이는 드론과 서버 간 통신 연결 역할을 수행하며, 사용자의 모바일 기기는 게이트웨이 역할로서 사용될 수 있다.

2.2 Zhang 등이 제안한 프로토콜

2024년 Zhang 등은 IoD 환경을 위한 PUF 기반 경량 인증 프로토콜을 제안하였다. 제안한 방식은 서버의 사전 배포 단계, 사용자와 드론의 등록 단계, 인증 단계로 구성되며 수행절차는 다음과 같다.

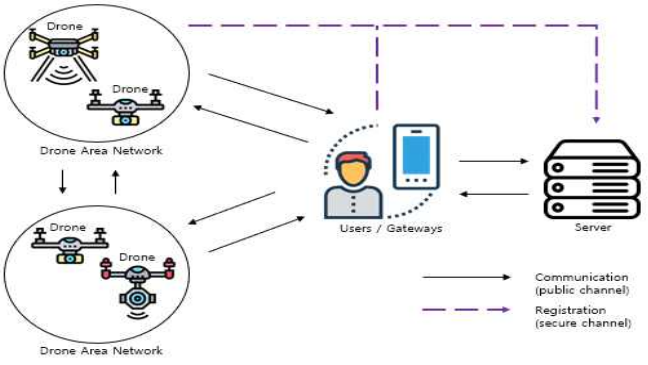

그림 1. Zhang 등이 제안한 시스템 모델.

2.2.1 사전 배포 단계

서버는 마스터 키 X_{ser}를 가지고, 게이트웨이의 아이디 GID_i, 해시함수 $h(\cdot)$를 생성해 각 게이트웨이에 저장한다.

2.2.2 등록 단계

(1) 드론 등록 단계

- 1단계: 드론은 랜덤값 r_b를 생성하고 자신의 아이디 DID_j로 가명 값 $HDID_j = h(DID_j \| \mathrm{r_b})$를 계산하여 서버로 등록을 요청한다.
- 2단계: 서버는 챌린지 값 $C_j = h(HDID_j \| X_{ser})$을 계산하고 드론과 통신할 게이트웨이의 GID_i를 선택하여 드론에 전송한다.
- 3단계: 받은 C_j로 PUF 응답 R_j, 비밀값 $B_j = h(C_j \| R_j \| GID_i)$를 계산하고 드론은 메모리에 $\{B_j, HDID_j, GID_i\}$를 저장한다.
- 4단계: 이후 서버는 드론이 보낸 R_j와 $HDID_j, C_j$ 정보를 보관한다.

(2) 사용자 등록 단계

- 1단계: 사용자는 자신의 아이디 ID_i, 비밀번호 PW_i를 입력하고 생성한 랜덤값 r_a으로 $HID_i = h(ID_i \| r_a)$, $HPW_i = h(PW_i \| r_a)$을

계산하고 이를 서버에 전송한다.

- 2단계: 서버는 $K_{GS}^{i}=h(HID_i \| X_{ser})$, $W_i=K_{GS}^{i} \oplus HPW_i$, $A=(C_j \| HID_i) \oplus HDID_j \oplus HPW_i$를 계산하고 $\{HID_i, K_{GS}^{i}\}$ 저장 후, 사용자에게 $COUNTER=0$ 값과 $\{W_i, A_1, HDID_j\}$를 전송한다.
- 3단계: 사용자는 전송받은 값과 HID_i, $A_2=h(ID_i \| PW_i) \oplus r_a$, $A_3=h(ID_i \| HPW_i)$값을 계산하여 함께 모바일 기기에 저장한다.

2.2.3 인증 단계

Zhang 등이 제안한 사용자 로그인 및 드론-게이트웨이 인증 단계는 아래 그림 2와 같다.

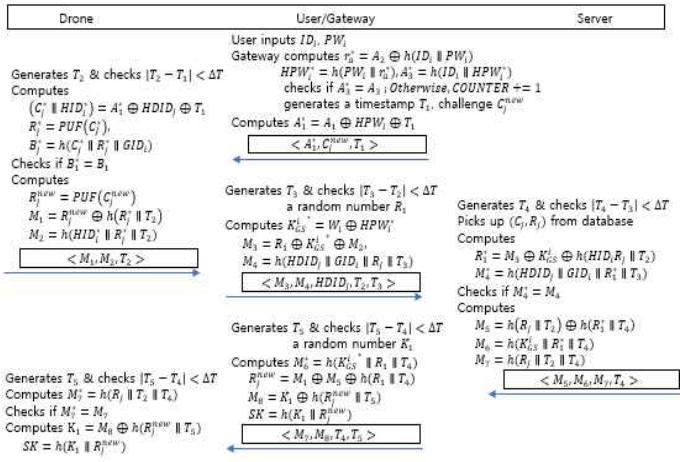

그림 2. 로그인 및 드론-게이트웨이 인증 단계.

2.3 Zhang 등이 제안한 프로토콜의 취약점

2.3.1 내부자 공격

공격자가 합법적인 사용자로 참여하여, 다른 사용자 및 드론 간의 세션 키를 유추할 수 있다. 공격자가 $C_j^{new}=C_j$로 합법적인 메시지를 보내면 $R_j^{new}=R_j$가 되어, $R_j^{new}=M_1 \oplus M_5 \oplus h(R_1 \| T_4)$를 계산하여 R_j값을 얻어낼 수 있다. 이후, 동일한 드론에서 R_j값은 동일하게 사용되므로, 다른 사용자 간의 인증 메시지로부터 M_1, M_8, T_2, T_5를 획득하고 $R_j^{new}=M_1 \oplus h(R_j \| T_2)$, $K_1=M_8 \oplus h(R_j^{new} \| T_5)$를 계산한다. 따라서, 공격자가 세션 키 $SK=h(K_1 \| R_j^{new})$를 알아낼 수 있게 된다.

2.3.2 재전송 공격

공격자는 이전에 합법적으로 송수신된 메시지를 재전송함으로써, 드론에 DoS (Denial of Service) 공격을 시도할 수 있다. 공격자는 공개 채널로부터 $A_1^*, HDID_j, T_1$를 획득하고, $A_1^*=(C_j \| HID_i) \oplus HDID_j \oplus T_1$을 계산하여 $(C_j \| HID_i)$를 구해낼 수 있으므로, 기존 메시지를 재구성할 수 있다. 따라서, 공격자는 새로운 C_j^{new}와 T_1을 생성하여 인증 요청 메시지를 위조할 수 있으며, 이로 인해 드론의 제한된 메모리, 전력 등이 소모되어 시스템에 부하를 초래할 수 있다. 위와 같이 Zhang 등이 제안한 인증 프로토콜은 재전송 공격에 취약하다.

2.3.3 임시 비밀 누출 공격

인증 과정에서 합의되는 세션 키는 임시 비밀 랜덤값이 유출되어도 보호되어야 한다[6]. 그러나 Zhang 등의 프로토콜에서는 랜덤값 R_1이 누출될 경우 공격자는 공개 메시지로부터 $K_{GS}^{i}=M_2 \oplus \mathrm{M}_3 \oplus \mathrm{R}_1$와 $R_j^{new}=M_1 \oplus M_5 \oplus h(R_1 \| T_4)$를 계산해낼 수 있으며, 이를 이용해 세션 키 $SK=h(K_1 \| R_j^{new})$를 알아낼 수 있게 된다.

2.4 대응방안

Zhang 등이 제안한 인증 프로토콜의 취약점을 보완하기 위해 다음과 같은 개선 방안을 제안한다. 첫째, 사전 공유키의 유출에 대비하여 타원곡선 암호와 같은 경량 공개키 기반 암호 기법을 도입할 수 있다. 둘째, 고정된 PUF 챌린지-응답 값으로 인해 발생하는 내부자 공격과 재전송 공격에 대응하기 위해, 매 세션마다 PUF 응답 및 공개 파라미터를 동적으로 갱신해야 한다. 셋째, Zhang 등의 프로토콜은 세션 키를 랜덤값만으로 구성하므로 임시 비밀 누출 공격에 취약하다. 따라서 세션 키 생성 시, 장기 비밀키를 함께 활용하여 세션 키의 보안성을 강화할 필요가 있다.

Ⅲ. 결론

본 논문에서는 Zhang 등이 제안한 PUF 기반 경량 인증 프로토콜이 내부자 공격, 재전송 공격, 임시 비밀 누출 공격에 취약하고 세션 키의 안전성을 보장하지 못함을 보였다. 이와 같은 취약점을 보완하기 위하여 경량 공개키 암호화 방식 및 매 세션마다 공개키 파라미터 등을 갱신하는 등의 대응 방안을 제시한다. 본 논문에서 제시한 대응 방안을 통해 안전한 상호 인증과 세션 키 보안을 제공하는 경량 인증 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] Abualigah, L., Diabat, A., Sumari, P., and Gandomi, A. H. “Applications, deployments, and integration of internet of drones (iod): a review,” IEEE Sensors Journal, pp. 25532-25546, Nov. 2021.

[2] Choi, J., Son, S., Kwon, D., & Park, Y. “A PUF-Based Secure Authentication and Key Agreement Scheme for the Internet of Drones,” Sensors, Feb. 2025.

[3] Yu, S., Das, A. K., Park, Y., and Lorenz, P. “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, Oct. 2022.

[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, Jan. 2024.

[5] Barbareschi, M., Bagnasco, P., and Mazzeo, A. "Authenticating IoT devices with physically unclonable functions models," Proc. Int. Conf. P2P Parallel Grid Cloud Internet Comput., pp. 563 - 567, 04-06 Nov. 2015.

[6] Kwon, D. K., Yu, S. J., Lee, J. Y., Son, S. H., and Park, Y. H. “WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks,” Sensors, Jan. 2021.