안전한 IoD 환경을 위한 키 합의 프로토콜의 보안 분석 및 개선방안

이상준, 김채언, 손승환, 박영호

경북대학교

gumoning9010@knu.ac.kr, chaeon@knu.ac.kr, sonshawn@knu.ac.kr, parkyh@knu.ac.kr

Security Analysis and Improvements of Key Agreement Protocol for Securing IoD Environment

Lee Sang Jun, Kim Chae Eon, Son Seung Hwan, Park Young Ho

Kyungpook National Univ.

요 약

최근, 다양한 작업에서 드론에 대한 수요 증가로 인해, 드론 인터넷(Internet of Drones, IoD)은 학계와 산업에서 여러 가지 이점을 제공함으로써 많은 주목을 받고 있다. IoD 환경은 사물인터넷과 비행 애드혹 네트워크 인프라의 잠재력을 통합함으로써 교통 및 환경 모니터링, 재난 상황 관리와 군사 작전 수행과 같은 다양한 서비스를 제공한다. 그러나 IoD 환경에서의 통신은 민감한 정보들이 불안전한 공개 채널을 통해 교환되기 때문에 잠재적인 보안 위협에 취약하다. 또한, 계산 능력과 자원 용량이 제한적인 드론과의 통신에서 높은 계산 및 통신 오버헤드를 요구하는 기존의 공개 키 기반의 암호화 방식을 적용하는 것은 실용적이지 않다. 최근, Alzahrani 는 IoD 환경 보안을 위한 안전한 키 합의 프로토콜을 제안하였다. 그러나, Alzahrani 의 프로토콜이 타원 곡선 암호 방식으로 인한 높은 계산 오버헤드를 가지며, 공개 채널 메시지 도청을 통한 가장 공격과 세션 키 유출 공격에 취약하다는 사실을 발견하였다. 따라서, 본 논문에서는 Alzahrani 가 제안한 프로토콜의 보안 분석을 통해 좀 더 안전하고 경량화할 방안을 제안한다.

Ⅰ. 서 론

드론 인터넷(IoD)은 일반적으로 드론이라고 불리는 무인 항공기(UAV)가 관리되는 공역 내에서 상호작용할 수 있도록 설계된 혁신적인 네트워크 아키텍처이다 [1]. 최근 몇 년간 IoD는 도시 관리부터 군사 작전에 이르기까지 다양한 잠재적 응용 분야로 인해 학계와 산업계에서 많은 관심을 받고 있다. IoD 환경에서 드론은 필요에 따라 다양한 비행 영역에 배치되어 순찰 및 환경 데이터 감지와 같은 다양한 작업을 수행하고 실시간으로 데이터를 수집한다. 이 데이터는 중앙 통제 기관인 지상 관제소로 전달되어 처리되거나 원격 사용자에게 제공된다. IoD는 신속한 배치, 높은 이동성, 유연성, 쉬운 재배치 가능성, 실시간 모니터링과 같은 여러 장점을 제공하여 스마트 농업, 수색 및 구조, 감시 시스템과 같은 광범위한 분야에 적용이 가능하다. 이처럼 IoD는 수많은 이점을 제공하지만, 해결해야 할 몇 가지 과제가 존재한다. 특히 개방된 무선 통신 환경과 드론의 배터리 기반 특성은 중대한 보안 및 개인 정보 보호 문제를 야기한다 [2]. 무선 채널은 본질적으로 신뢰성이 떨어져서 보안 문제에 취약하며, 드론의 높은 이동성은 이러한 문제를 더욱 복잡하게 만든다. 데이터의 높은 민감성과 전송 매체의 접근성은 신원 및 위치 정보 유출, 물리적 탈취를 통한 비밀 정보 추출, 오프라인 비밀번호 추측 공격 등 다양한 보안 공격의 위험을 증가시킨다 [3]. 이러한 문제를 해결하기 위해 Alzahrani 는 IoD 환경 보안을 위한 안전한 키 합의 프로토콜을 제안하였다 [4]. 하지만, Alzahrani 가 제안한 프로토콜은 공개 채널 메시지 도청을 통한 가장 공격과 세션 키 유출 공격을 방어할 수 없다. 또한, 드론은 계산 능력 및 에너지 소비 측면에서 제약이 있는 경량 장치이므로, 높은 계산 복잡성을 요구하는 보안 솔루션은 비효율적일 수 있다 [5]. 본 논문에서는 보안 분석을 통해 Alzahrani 가 제안한 프로토콜을 경량화하고 보안 문제를 개선할 방안을 제안한다.

Ⅱ. 본론

2.1 시스템 모델

Alzahrani 가 제안한 시스템 모델은 그림 1과 같이 드론, 모바일 장치, 지상 관제소의 세 가지 참여자로 구성된다.

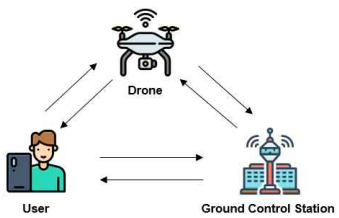

그림 1. 시스템 모델.

- 지상 관제소 (Ground Control Station, GCS) : GCS는 충분한 처리 및 저장 능력을 갖춘 신뢰할 수 있는 제3자이다. IoD 환경에서 GCS는 시스템 관리자 역할을 한다. 또한, GCS는 모바일 장치와 드론의 등록을 위해 비밀 키를 생성하여 전달한다.
- 모바일 장치 (Mobile Device) : 사용자는 IoD 서비스를 제공받기 위해 모바일 장치를 사용하여 드론과 통신한다. 모바일 장치는 먼저 GCS에 등록되며, 상호 인증 및 합법적인 서비스를 위해 신원, 비밀번호 및 다른 민감한 정보를 저장한다.
- 드론 (Drone) : 드론은 시스템 모델의 핵심적인 개체이며, 전술적 작업을 위해 배치될 수 있다. 드론은 먼저 GCS에 등록된 후, 수많은 작업을 위해 IoD 환경에 배치된다.

2.2 등록 단계

Alzahrani 가 제안한 프로토콜의 등록 단계는 그림 2, 그림 3과 같다.

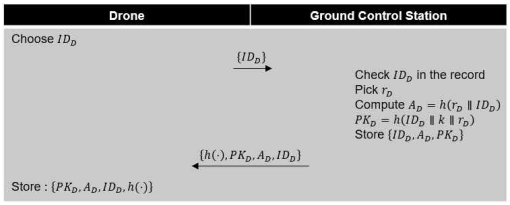

그림 2. 드론 등록 단계.

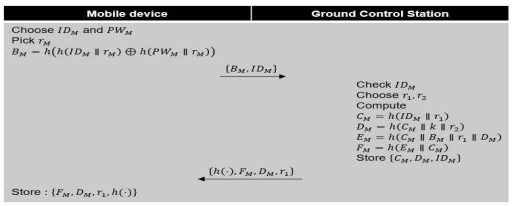

그림 3. 모바일 장치 등록 단계.

2.3 키 합의 단계

Alzahrani 가 제안한 프로토콜의 키 합의 단계는 그림 4와 같다.

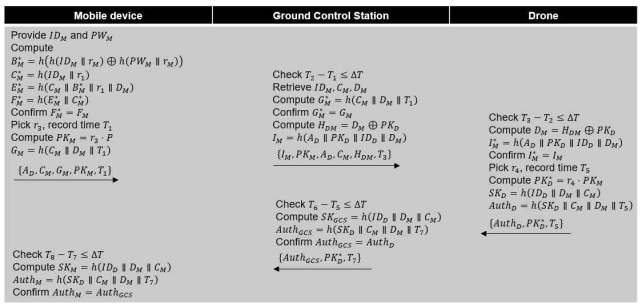

그림 4. 키 합의 단계.

2.4 보안 분석

본 논문에서는 보안 분석을 통해 Alzahrani 가 제안한 프로토콜이 공격자가 공개 채널 상의 메시지를 도청하는 것만으로 사용자 가장 공격, 드론 가장 공격, 세션 키 유출 공격과 같은 치명적인 보안 공격을 허용할 수 있다는 사실을 입증하였다.

2.4.1 드론 가장 공격

공격자는 공개 채널 메시지를 도청하여 $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$ 을 얻을 수 있다. 얻은 값들과 드론의 공개키를 XOR 연산하여 D_M을 계산할 수 있다. 계산한 D_M과 얻은 C_M을 사용하여 세션 키와 $Auth_D$를 계산할 수 있다. 마지막으로, 공격자는 랜덤 난수를 선택하여 PK_{AD}^*를 계산하면 드론이 GCS에게 보내는 메시지를 전부 계산할 수 있기 때문에 드론 가장 공격이 성립한다.

2.4.2 사용자 가장 공격

공격자는 공개 채널 메시지를 도청하여 $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$ 을 얻을 수 있다. 얻은 값들과 드론의 공개키를 XOR 연산하여 D_M을 계산할 수 있다. 얻은 C_M과 계산한 D_M을 사용하여 GM을 계산할 수 있다. 그리고 랜덤 난수를 선택하여 PK_{AM}을 만들 수 있다. 계산한 D_M, 얻은 C_M을 사용해서 세션 키를 계산하여 $Auth_{GCS}$를 계산할 수 있다. 따라서, 공격자는 사용자가 보내는 인증 요청 메시지와 받는 응답 메시지를 전부 계산할 수 있기 때문에 사용자 가장 공격이 성립한다.

2.4.3 세션키 유출 공격

공격자는 공개 채널 메시지를 도청하여 $\{I_M, PK_M, A_D, C_M, H_{DM}, T_3\}$ 을 얻을 수 있다. 얻은 값들과 드론의 공개키를 XOR 연산하여 D_M을 계산할 수 있다. 계산한 D_M과 얻은 C_M을 사용하여 세션 키를 계산할 수 있기 때문에 세션 키 유출 공격이 성립한다.

2.5 개선방안

Alzahrani 가 제안한 프로토콜은 공개 채널 메시지 도청으로 인한 사용자 가장 공격, 드론 가장 공격, 세션 키 노출 공격이 성립한다. 이러한 보안 취약점이 발생하는 이유는 세션 키를 계산하는데 필요한 비밀값들을 암호화하지 않고 공개 채널 메시지에 그대로 넣어서 통신하기 때문이다. 본 논문에서는 등록 단계에서 민감한 정보들을 한 번 더 암호화하여 저장하고 랜덤 난수와 비밀 키들을 사용하여 세션 키의 보안성을 개선하고, XOR 연산과 해시 함수만을 사용함으로써 좀 더 경량화하는 방안을 제안한다.

Ⅲ. 결론

본 논문에서는 Alzahrani 가 제안한 IoD 환경 보안을 위한 키 합의 프로토콜의 보안을 분석하여 취약점을 발견하였다. 보안 분석을 통해 Alzahrani 가 제안한 프로토콜이 공개 채널 메시지 도청 공격을 통한 드론 가장 공격, 사용자 가장 공격과 세션 키 유출 공격을 방어할 수 없음을 입증하였다. 이러한 공격을 방어하기 위해 등록 단계를 강화하고 랜덤 난수와 비밀 키들을 활용하여 XOR 연산과 해시 함수만을 사용함으로써 IoD 환경에 적합한 개선방안을 제안했다. 향후 본 논문에서는 제안한 개선방안을 실제로 적용하여 IoD 환경에서의 더 경량화되고 보안이 강화된 키 합의 프로토콜을 설계할 예정이다.

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] Gharibi, M., Boutaba, R., and Waslander, S. L. “Internet of drones,” IEEE Access, pp. 1148-1162, Mar. 2016.

[2] 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, Jul. 2022.

[3] Choi, J., Son, S., Kwon, D., and Park, Y. “A PUF-Based Secure Authentication and Key Agreement Scheme for the Internet of Drones,” Sensors, p. 982, Feb. 2025.

[4] Alzahrani, A. A. “VSKAP-IoD: A Verifiably Secure Key Agreement Protocol for Securing IoD Environment,” IEEE Access, pp. 58039-58056, Apr. 2024.

[5] Yu, S., Lee, J., Sutrala, A. K., Das, A. K., and Park, Y. “LAKA-UAV: Lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks,” Computer networks, p. 224, Apr. 2023.