A Secure and Anonymous Authentication Protocol for Internet of Drones Environment

1st Sangjun Lee
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
gumoning9010@knu.ac.kr

2nd Taehun Kim
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
kimth028@knu.ac.kr

3rd Deokkyu Kwon
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
kdk145@knu.ac.kr

4nd Youngho Park
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, South Korea
parkyh@knu.ac.kr

***Abstract*—Internet of Drones (IoD) provides diverse services such as logistics delivery, traffic control, and military operations. However, due to the transmission of sensitive data over open wireless channel in IoD environments, these services are vulnerable to various security attacks. The physical capture of drones or malicious data tampering can lead to confidential information leakage and severe casualties. Therefore, a secure authentication protocol is essential for IoD environments. In 2024, Algarni et al. proposed a secure and lightweight authentication protocol for securing IoD environment. However, we demonstrate through informal security analysis that Algarni et al.'s protocol is vulnerable to session key disclosure attacks and drone and mobile device impersonation attacks by eavesdropping messages on public channel. Furthermore, it does not provide drone anonymity and untraceability. Therefore, we propose a secure authentication protocol that efficiently improves Algarni et al.'s scheme.**

***Index Terms*—Internet of Drones, impersonation attack, session key disclosure attack, wireless channel, authentication protocol.**

I. Introduction

The rapid advancement of drone technology have driven significant attention to the Internet of Drones (IoD) in academia and industry. The IoD architecture interconnects numerous drones via internet networks to perform cooperative data collection and transmission within controlled airspaces [1]. In IoD environments, drone performs various tasks such as logistics delivery, disaster response, traffic monitoring, and border surveillance [2]. During the execution of these tasks, drones collect a multitude of data, including sensitive information [3]. However, due to their dependence on open wireless channel and vulnerability to physical attacks, IoD environments are susceptible to various security threats such as eavesdropping, data tampering, and hijacking [4]. Therefore, a secure authentication protocol is essential in the IoD environment.

In 2024, Algarni et al. [5] proposed a secure and lightweight authentication protocol to address these challenges in IoD environments. Algarni et al. claimed that their proposed protocol ensures secure information communication in IoD environments by guaranteeing the confidentiality of session key. However, through an informal security analysis, we demonstrate that Algarni et al.'s protocol cannot prevent session key disclosure, drone and mobile device impersonation attacks by eavesdropping messages on wireless channel. Furthermore, we show that their protocol does not provide drone anonymity and untraceability. Therefore, we propose a secure and anonymous authentication protocol for IoD environments.

This research was supported by the Regional Innovation System & Education(RISE) Glocal 30 program through the Daegu RISE Center, funded by the Ministry of Education(MOE) and the Daegu, Republic of Korea.(2025-RISE-03-001)

II. Preliminaries

A. System Model

As illustrated in Fig. 1, the system model designed for IoD environments consists of four principal entities: a drone, a mobile device, a ground station server, and a trusted third-party server.

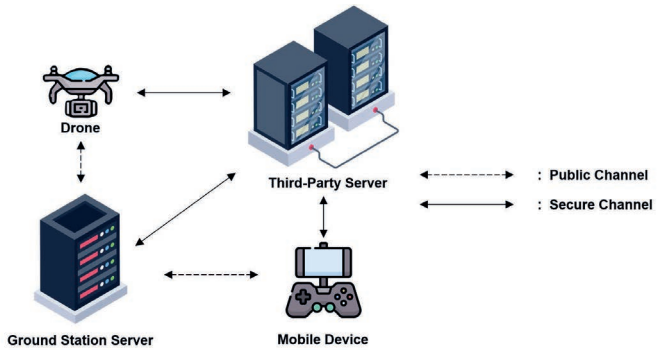

Fig. 1. IoD system model.

- Trusted third-party server (TTPS): TTPS is a fully trusted entity, and all network entities are registered with TTPS. TTPS manages the network and stores the secret credentials of ground station server, mobile device, and drone.
- Ground station server (GSS): GSS functions as an intermediary between a mobile device and a drone. GSS facilitates secure communication between a mobile device and a drone after verifying their legitimacy.
- Mobile device (MD): MD is a hand-held device used for exchanging messages with the GSS. With the assistance of the GSS, it performs mutual authentication with a drone, and subsequently communicates with the drone using a secret session key.
- Drone (D): With the assistance of the GSS, drone performs mutual authentication with a mobile device, and subsequently communicates with the mobile device using a secret session key. The drone collects information using its equipped sensors and transmits it to the mobile device.

B. Threat Model

To assess the security of the proposed protocol, we adopt the Dolev-Yao (DY) model as the threat model [6]. Under the assumptions, capabilities of the adversary are outlined below:

- The adversary can inject, modify, delete, or eavesdrop on messages exchanged over an open wireless channel [7].
- The adversary can compromise a legitimate mobile device and extract secret credentials stored in its memory by conducting a power analysis attack [8].
- The adversary can physically capture a drone and extract secret credentials in its memory [9].

III. Review of Algarni et al.'s protocol

We review Algarni et al.'s protocol comprising four phases : ground station server registration, mobile device registration, drone registration, and mutual authentication phases.

A. Registration Phase

Fig. 2, Fig.3 and Fig.4 illustrates the ground station server, mobile device and drone registration phase of Algarni et al.'s protocol.

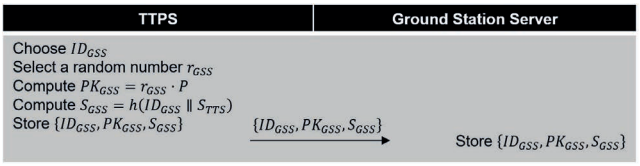

Fig. 2. Ground server station registration phase of Algarni et al.

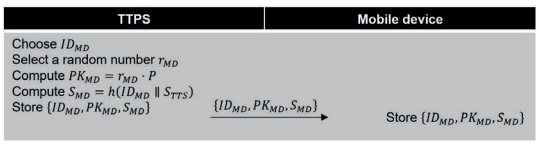

Fig. 3. Mobile device registration phase of Algarni et al.

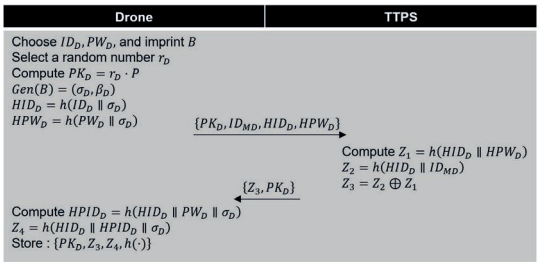

Fig. 4. Drone registration phase of Algarni et al.

B. Mutual Authentication Phase

Fig. 5 illustrates the mutual authentication phase of Algarni et al.'s protocol.

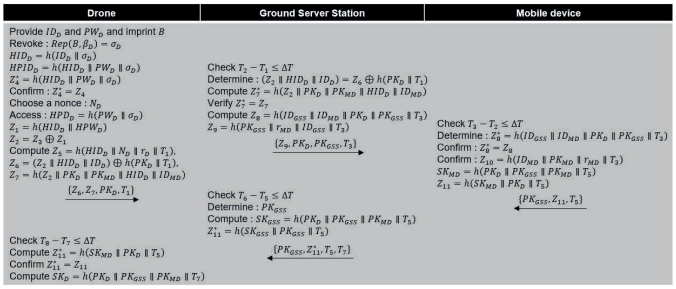

Fig. 5. Mutual authentication phase of Algarni et al.

IV. Cryptanalysis of Algarni et al.'s protocol

We demonstrate the security vulnerabilities in the protocol of Algarni et al. Their protocol is not resilient to session key disclosure attacks and drone and mobile device impersonation attacks by eavesdropping messages on wireless channel.

A. Session key disclosure attack

- **Step 1:** A malicious adversary can eavesdrop on the wireless channel messages $\{Z_9, PK_D, PK_{GSS}, T_3\}$ and $\{PK_{GSS}, Z_{11}, T_5\}$ to obtain $\{PK_D, PK_{GSS}, T_5\}$.
- **Step 2:** In Algarni et al.'s protocol, the mobile device's public key PK_{MD} is a public value, so the malicious adversary can use the intercepted $\{PK_D, PK_{GSS}, T_5\}$ with PK_{MD} to compute the session key $SK = h(PK_D \| PK_{GSS} \| PK_{MD} \| T_5)$.

Therefore, Algarni et al.'s protocol cannot prevent session key disclosure attacks.

B. Mobile device impersonation attack

A malicious adversary must be able to compute $Z_{11} = h(SK_{MD} \| PK_D \| T_5)$ in order to impersonate a legitimate mobile device.

- **Step 1:** By eavesdropping on the wireless channel messages $\{Z_9, PK_D, PK_{GSS}, T_3\}$ and $\{PK_{GSS}, Z_{11}, T_5\}$, a malicious adversary can obtain the values required to compute the session key $SK_{MD} = h(PK_D \| PK_{GSS} \| PK_{MD} \| T_5)$.

- **Step 2:** The malicious adversary can use the computed SK_{MD} with the intercepted PK_D and T_5 from the wireless channel messages to calculate $Z_{11} = h(SK_{MD} \parallel PK_D \parallel T_5)$.

Therefore, Algarni et al.'s protocol is vulnerable to mobile device impersonation attacks.

C. Drone impersonation attack

A malicious adversary must be able to compute $Z_6 = (Z_2 \parallel HID_D \parallel ID_D) \oplus h(PK_D \parallel T_1), Z_7 = h(Z_2 \parallel PK_D \parallel PK_{MD} \parallel HID_D \parallel ID_{MD})$ and $Z_{11} = h(SK_{MD} \parallel PK_D \parallel T_5)$ in order to impersonate a legitimate drone.

- **Step 1:** By eavesdropping on the wireless channel message $\{Z_6, Z_7, PK_D, T_1\}$, a malicious adversary can obtain PK_D and T_1, and then compute $h(PK_D \parallel T_1)$ to reveal Z_2, HID_D, and the drone's identity ID_D.
- **Step 2:** Using these values with other values obtained from wireless channel messages, the malicious adversary can compute Z_7.
- **Step 3:** By eavesdropping on the wireless channel messages $\{Z_9, PK_D, PK_{GSS}, T_3\}$ and $\{PK_{GSS}, Z_{11}, T_5\}$, the malicious adversary can obtain the values required to compute the session key $SK_{MD} = h(PK_D \parallel PK_{GSS} \parallel PK_{MD} \parallel T_5)$, which enables the malicious adversary to compute Z_{11}.

Therefore, Algarni et al.'s protocol is vulnerable to drone impersonation attacks. Moreover, their protocol does not provide drone's anonymity due to the exposure of drone's identity.

V. Proposed Protocol

The proposed protocol consists of the following phases: mobile device registration, drone registration, ground station server registration, and mutual authentication phases.

A. Registration Phase

The proposed mobile device, drone and ground station server registration phase in this paper is presented in Fig. 6, Fig. 7 and Fig. 8.

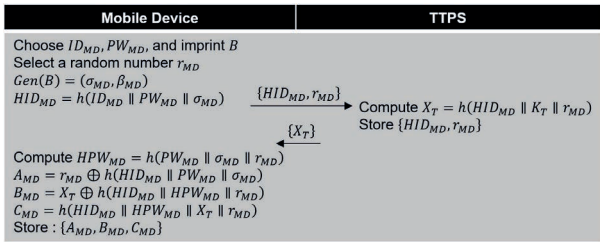

Fig. 6. Proposed mobile device registration phase.

B. Mutual Authentication Phase

The proposed mutual authentication phase in this paper is presented in Fig. 9.

VI. Informal Security Analysis

We perform an informal security analysis to evaluate the security of the proposed protocol.

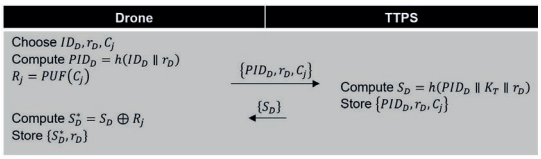

Fig. 7. Proposed drone registration phase.

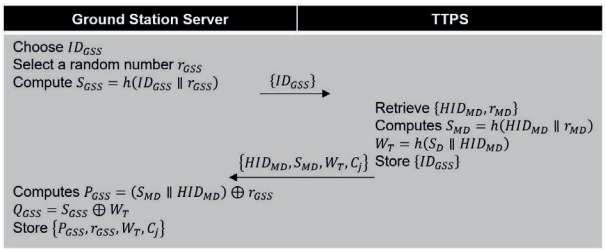

Fig. 8. Proposed ground server station registration phase.

A. Session key disclosure attack

A malicious adversary must know R_{MD}, R_{GSS}, and R_D to calculate the session key. However, the malicious adversary cannot compute the session key since these random nonces are masked with mobile user's secret key S_{MD} and drone's PUF parameter R_j. Therefore, the proposed protocol can prevent session key disclosure attack.

B. Mobile device impersonation attack

A malicious adversary must compute authentication request message $\{HID_{MD}, M_1, V_1, T_1\}$ and response message $\{M_4, V_4, T_4\}$ in order to impersonate a legitimate mobile device. However, the malicious adversary cannot generate valid request and response message since it is impossible to calculate $HID_{MD} = h(ID_{MD} \parallel PW_{MD} \parallel \sigma_D)$ and R_{MD}. Therefore, the proposed protocol is resilient to mobile device impersonation attack.

C. Drone impersonation attack

A malicious adversary must compute response message $\{HID_{MD}, C_j, S_{GSS}, M_2, V_2, T_2\}$ and authentication request message $\{M_3, V_3, T_3\}$ in order to impersonate a legitimate drone. However, the malicious adversary cannot generate valid request and response message since it is impossible to calculate $Q_{GSS} = S_{GSS} \oplus W_T$ and $W_T = h(S_D \parallel HID_{MD})$. Therefore, the proposed protocol is resilient to drone impersonation attack.

D. Physical drone capture attack

A malicious adversary can physically capture a drone and extract secret credentials $\{S_D^*, r_D\}$ from its memory. To compute the session key, the malicious adversary must know R_{MD}, R_{GSS}, and R_D. However, these random nonces are masked by the drone's secret key S_D which is encrypted using its PUF response value R_j. Therefore, the proposed protocol can prevent physical drone capture attack.

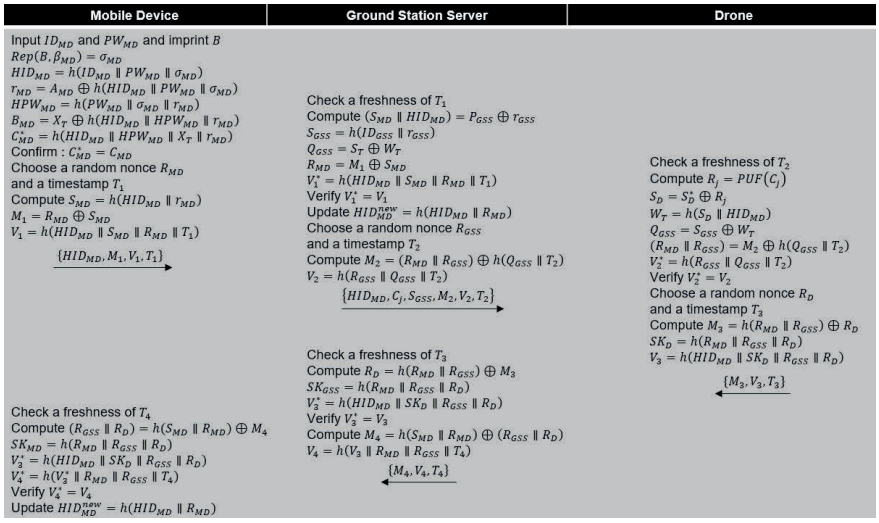

Fig. 9. Proposed mutual authentication phase.

E. Replay and MITM attack

In the proposed protocol, all messages are hashed with timestamps T_1, T_2, T_3, and T_4. So each network entity can check the timestamps to verify the freshness of messages. Furthermore, all messages include verification values V_1, V_2, V_3, and V_4. So each network entity can verify the validity of messages. Therefore, the proposed protocol can prevent replay and MITM attacks.

F. Anonymity and Untraceability

A malicious adversary can eavesdrop on all public channel messages and attempt to compromise and track the mobile user's identity. However, the mobile user's identity is masked in $HID_{MD} = h(ID_{MD} \parallel PW_{MD} \parallel \sigma_D)$ using a hash function with the mobile user's password and biometric data. Furthermore, the GSS updates HID_{MD} to HID_{MD}^{new} by hashing it with a random nonce R_{MD}. Therefore, the proposed protocol provides anonymity and untraceability.

VII. Conclusions

In this paper, we analyzed Algarni et al.'s protocol and identified security vulnerabilities. Through informal security analysis, we demonstrate that Algarni et al.'s protocol is vulnerable to session key disclosure attacks and drone and mobile device impersonation attacks, and it does not provide drone anonymity and untraceability. To mitigate these security weaknesses, we propose a secure authentication protocol for the IoD environment. We demonstrated that the proposed protocol can prevent various security attacks and provide anonymity and untraceability. In future work, we plan to enhance the security of the proposed protocol using well-known formal analysis such as Automated Verification of Internet Security Protocols and Applications (AVISPA) simulation and Real-or-Random (RoR) model.

References

[1] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of Internet of Drones (IoD): A review," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25532–25546, Nov. 2021.

[2] Y. Park, D. Ryu, D. Kwon, and Y. Park, "Provably secure mutual authentication and key agreement scheme using PUF in Internet of Drones deployments," *Sensors*, vol. 23, no. 4, p. 2034, Feb. 2023.

[3] S. Son, D. Kwon, S. Lee, Y. Jeon, A. K. Das, and Y. Park, "Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF," *IEEE Access*, vol. 11, pp. 60240–60253, Jun. 2023.

[4] S. Yu, A. K. Das, and Y. Park, "RLBA-UAV: A robust and lightweight blockchain-based authentication and key agreement scheme for PUF enabled UAVs," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 12, pp. 21697–21708, Dec. 2024.

[5] F. Algarni, S.U. Jan, PSLAPS-IoD: "A Provable Secure and Lightweight Authentication Protocol for Securing Internet-of-Drones (IoD) Environment," *IEEE Access*, vol. 12, pp. 45948-45960, Mar. 2024

[6] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–207, Mar. 1983.

[7] M. Wazid, J. Singh, C. Pandey, R. S. Sherratt, A. K. Das, D. Giri, and Y. Park, "Explainable deep Learning-Enabled malware attack detection for IoT-Enabled intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 26, no. 5, pp. 7231-7244, May. 2025.

[8] D. Kwon, S. Son, M. Kim, J. Lee, A. Kumar Das, and Y. Park, "A secure self-certified broadcast authentication protocol for intelligent transportation systems in uav-assisted mobile edge computing environments," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 11, pp. 19004–19017, Nov. 2024.

[9] J. Choi, S. Son, D. Kwon, and Y. Park, "A PUF-Based Secure Authentication and Key Agreement Scheme for the Internet of Drones," *Sensors*, vol. 25, no. 3, p. 982, Feb. 2025.