# Cryptanalysis and Countermeasures of the Recent Authentication and Key Agreement Scheme for Internet of Drones

Sungjin Yu, Keonwoo Kim, Kim Taesung, Boheung Chung, and Yousung Kang
*Cryptography & Authentication Base Technology Research Section*
*Electronics and Telecommunications Research Institute (ETRI)*
Daejeon, South Korea 305-700
E-mail: sj.yu@etri.re.kr

***Abstract*—With the advances in 5G communication and mobile device, internet of drones (IoD) has emerged as a fascinating new concept in the realm of smart cities, and has garnered significant interest from both scientific and industrial communities. However, IoD are fragile to variety of security attacks because an adversary can reuse, delete, insert, intercept or block the transmitted messages over an open channel. Therefore, it is imperative to have robust and efficient authentication and key agreement (AKA) schemes for IoD in order to to fulfill the necessary security requirements. Recently, Nikooghadm et al. designed a secure and lightweight AKA scheme for internet of drones (IoD) in IoT environments. However, we prove that their scheme is not resilient to various security threats and does not provide the necessary security properties. Thus, we propose the essential security requirements and guidelines to enhance the security flaws of Nikooghadm et al.'s scheme.**

***Index Terms*—Cryptanalysis, countermeasure, security protocol, internet of drones (IoD)**

## I. Introduction

With the advancements in "5G communication" and "smart device" technologies, internet of things (IoT) has been able to connect objects and share large amounts of real-time data through resource-constrained devices. As a result, IoT has become a convenient and useful tool for providing service such as healthcare, internet of drones (IoD), and smart grid [1]–[3]. The emergence of IoT has provided a new paradigm for improving the efficiency of managing resources and assets, optimizing urban services, and enhancing the quality of citizens' lifes. Despite the numerous benefits of IoT, there are still various challenges and difficulties that need to be addressed. One such issue is the fact that communication between the user and the service provider in IoT environments occurs over a public channel without any encryption method. If an adversary gains access to sensitive data belonging to legitimate users, they could potentially carry out cyber security threats. These cyber security threats could result in an adversary introducing fake data into the system of legitimate users, leading to serious criminal purposes. Besides cyber security threats, physical security threats could also affect IoT devices since they are often deployed in unmonitored environments. Moreover, since IoT devices are limited with regard to computing power and resource [4], public key cryptography (PKC), which requires high computation overhead, is not a suitable solution. Therefore, it is crucial to have robust and lightweight authentication and key agreement (AKA) schemes to provide effective services for the next-generation IoT [5], [6].

This work was supported by Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korea government (MSIT). (No. 2022-0-01019, Development of eSIM security platform technology for edge devices to expand the eSIM ecosystem)

In 2021, Nikooghadm et al. [7] introduced a "provably secure and lightweight AKA protocol for IoD-based smart city surveillance". According to Nikooghadm et al., their scheme claimed that potential security threats where thwarted and that all necessary security features were guaranteed. However, we discover that Nikooghadm et al.'s scheme was vulnerable to possible security threats, such as drone physical capture and imperonsation attacks, and lacked essential security properties such as session key security and authentication. Furthermore, their scheme was not ideal for resource-constrained IoD, as it relied on PKC, which required a high-level performance.

Hence, we present the crucial security requirements and guidelines to augment the security issues of Nikooghadm et al.'s scheme [7].

### A. Adversary Model

We present the attack assumptions that encompass the widely-used "Dolev-Yao (DY)" model [8], in order to scrutinize the security of existing AKA scheme. The adversary's abilities are outlined as follows:

- "Based on DY model [8], a malicious attacker ($MA$) can block, inject, eavesdrop, reuse, modify, and resend the transmitted messages over an open channel".
- "$MA$ is capable of stealing a mobile devicec from its legitimate user and subsequently extracting the confidential credentials stored in its memory through the utilize of power-analysis attacks [9]. Furthermore, $MA$ has the ability to physical capture certain IoD that may be situated in insecure and unattended environments. One captured, $MA$ can extract the secret parameters stored within those certain IoD".

- "After getting the secret parameters of a mobile device or a captuped drone, $MA$ may attempt potential security attacks, including the "off-line password guessing", "replay", "MITM" attacks [10]".

### B. Organization

The remainder of the article is organized as follows. Section II reviews the Nikooghadm et al.'s scheme [7] and then Sections III demonstrates the security flaws of Nikooghadm et al.'s scheme. In Section IV, we present the necessary security requirements and guidelines to enhance the security flaws of Nikooghadm et al.'s scheme. Finally, we summarize the conclusions and future works in Section V.

## II. Review of Nikooghadm et al.'s Scheme

This section provides an overview of Nikooghadm et al.'s scheme for the IoD. Their scheme consists of three processes: "system setup, registration, and authentication". Table I succinctly summarizes all the notations employed in Nikooghadm et al.'s scheme.

TABLE I: Notations for Nikooghadm et al.'s Scheme

| Notation | Description |
|---|---|
| $U_i$ | User |
| $D_j$ | Drone |
| $CS$ | Control serve r |
| $ID_i$ | $U_i$'s identity |
| $ID_j$ | $D_j$'s identity |
| $P$ | Based point of $E_p(a, b)$ |
| $s$ | A secret key of $CS$ |
| $SK$ | Common session key |
| $a_j, d_i, q_i, z_i, g_j$ | Random number from $Z_p$ |
| $T_i$ | Timestamp |
| $\Delta T$ | Threshold value for the timestamp |
| $h(\cdot)$ | Hash function |
| $\oplus$ | Bitwise XOR operation |
| $\|\|$ | Concatenation operation |

### A. System Setup Process

The system setup process is identical to the system configuration process highlighted in the scheme of Nikooghadm et al.

### B. Drone Registration Process

$D_j$ is required to register within $CS$ in order to provide valuable services. We introduce the drone registration process of Nikooghadm et al.'s scheme.

**DRP-1:** "$D_j$ selects a unique identity $ID_j$ and then sends it to $CS$ over a secure channel".

**DRP-2:** "$CS$ checks the validation of $ID_j$ by comparing it with stored identities in the database. If $ID_j$ is matched with the existing identity, $CS$ will ask $D_j$ to select another unique $ID_j$. Otherwise, $CS$ chooses a random number $a_j \in Z_p$ and calculates $PID_j = h(a_j||ID_j)$ and $key_j = h(ID_j||s||a_j)$. Then, $CS$ stores $\{ID_j, PID_j, key_j\}$ in the database and transmits $\{ID_j, PID_j, key_j, h(\cdot)\}$ to the $D_j$ over a secure channel".

**DRP-3:** "After receiving the messages from the $CS$, $D_j$ stores $\{ID_j, PID_j, key_j, h(\cdot)\}$ in the memory".

### C. User Registration Process

To access drone application services, it is necessary for $U_i$ to complete registration with $CS$.

**URP-1:** "$U_i$ chooses a unique identity $ID_i$ and password $PW_i$. After that, a mobile device ($MD_i$) of $U_i$ selects a random number $d_i \in Z_p$ and calculates $ppw_i = h(h(ID_i||d_i) \oplus h(PW_i||d_i))$. $MD_i$ transmits $\{ID_i, ppw_i\}$ to the $CS$ over a secure channel".

**URP-2:** "$CS$ chooses a two random numbers $f_i, q_i \in Z_p$ and computes $FID_i = h(ID_i||f_i)$, $K_i = h(FID_i||s||q_i)$, $A_i = h(FID_i||ppw_i||f_i||K_i)$, $A_i = h(FID_i||ppw_i||f_i||K_i)$, and $B_i = h(A_i||FID_i)$. Finally, $CS$ stores $\{ID_i, FID_i, K_i\}$ in the database and transmits $\{f_i, K_i, B_i, h(\cdot)\}$ to the $U_i$ over a secure channel".

**URP-3:** "Upon getting the messages, $U_i$ stores $\{d_i, f_i, K_i, B_i, h(\cdot)\}$ in the $MD_i$".

### D. Authentication and Key Agreement Process

$U_i$ and $D_j$ mutually authenticate ony another by $CS$, subsequently established a shared sesssion key $SK$. All messages are tnramistted over a public channel. We are

In this process, $U_i$ and $D_j$ are mutually authenticated each other with the aid of $CS$ and then established a common session key $SK$. All messages are exchanged over a public channel.

**AKP-1:** "$U_i$ first enter an identity $ID_i$ and password $PW_i$ into the $MD_i$. After that, $MD_i$ computes $ppw_i^* = h(h(PW_i||d_i) \oplus h(ID_i||d_i))$, $FID_i^* = h(ID_i||f_i)$, $A_i^* = h(FID_i^*||ppw_i^*||f_i||K_i)$, and $B_i^* = h(A_i^*||FID_i^*)$. Then, $MD_i$ checks whether $B_i^* \stackrel{?}{=} B_i$. If the condition is not valid, $MD_i$ aborts this process; otherwise, the next process is executed".

**AKP-2:** "$MD_i$ chooses a random number $z_i \in Z_p$ and timestamp $T_1$. Then, $MD_i$ computes $A1_i = h(T_1||FID_i||K_i)$ and transmits $\{z_iP, A1_i, FID_i, PID_j, T_1\}$ to the $CS$ over a public channel".

**AKP-3:** "$CS$ verifies whether $|T_2 - T_1| \leq \Delta T$. If the condition is equal, $CS$ retrieves the tuple $\{ID_i, FID_i, K_i\}$ from the database and calculates $A1_i^{'} h(T_1||FID_i||K_i)$ and checks whether $A1_i^{'} \stackrel{?}{=} A1_i$. If it is not valid, $CS$ terminates the current session; otherwise, $CS$ is authenticated. $CS$ computes $K_{ij} = K_i \oplus key_j$ and $A3_i = h(PID_j||key_j||ID_j||K_i)$. Finally, $CS$ transmits $\{A3_i, T_2, z_iP, PID_j, K_{ij}, FID_i\}$ to the $D_j$".

**AKP-4:** "$D_j$ first checks the freshness of the messages by checking whether $|T_3 - T_2 \leq \Delta$. If it is valid, $D_j$ computes $K_i = K_{ij} \oplus key_j$ and $A3_j = h(PID_j||key_j)||ID_j||K_i$. It further verifies whether $A3_j^* \stackrel{?}{=} A3_j$. If it is correct, $D_j$ chooses a random number $g_j \in Z_p$ and computes $sk_j = h(ID_j||g_jz_iP||K_i||FID_i)$ and

$Auth_j = h(sk_j||FID_i||T_3||K_i)$. Finally, $D_j$ sends $\{g_jP, Auth_j, T_3\}$ to the $U_i$ over a public channel".

**AKP-5:** "$MD_i$ verifies whether the freshness of the $|T_4 - T_3| \leq \Delta_T$. If it is equal, $U_i$ computes a session key $sk_i = h(ID_j||z_i g_j P||K_i||FID_i)$ and $Auth_j^* = h(sk_i||FID_i||T_3||K_i)$. Finally, $U_i$ verifies whether $Auth_j^* \stackrel{?}{=} Auth_j$. If the condition is valid, $U_i$ authenticates $D_j$, successfully".

## III. Security Flaws of Nikooghadm et al.'s scheme

This section discusses the security vulnerabilities of Nikooghadm et al.'s scheme [7]. According to Nikooghadm et al., their scheme could effectively prevent potential security attacks while also providing necessary security requirements. However, we demonstrated that their scheme is susceptible to "drone physical capture" and "impersonation" attacks. Additionally, it fails to provide important security properties such as "session key security" and "mutual authentication".

### A. Session Key Security

Nikooghadm et al. [7] claimed that their scheme ensures a session key security between $MU_i$ and $D_j$ successfully. However, Nikooghadm et al.'s scheme [7] cannot resist session key disclosure attacks as follows because their scheme was designed that all participants publicly know the $D_j$'s identity.

- **Step 1:** "According to Section I-A, $MA$ can steal a mobile device and extract secret parameters stored in its memory, and eavesdrop the transmitted messages via a public channel. Thus, $MA$ can calculate $key_j = K_{ij} \oplus K_i$".
- **Step 2:** "$MA$ selects a new random number $z_{MA}$ and computes $z_{MA}P$. Then, $MA$ selects a timestamp $T_{MA1}$, generates a $A1_{MA} = h(T_{MA1}||FID_i||K_i)$, and sends $\{T_{MA1}, z_{MA}P, A1_{MA}, FID_i, PID_j\}$ to the $CS$ through an insecure channel".
- **Step 3:** "Upon getting the messages, $CS$ selects a timestamp $T_2$ and computes $A1'_{MA} = h(T_{MA1}||FID_i||K_i)$ and verifies whether $A1'_{MA} \stackrel{?}{=} A1_{MA}$. If it is correct, $CS$ computes $K_{MAj} = K_i \oplus key_j$, and $A3_{MA} = h(PID_j||key_j||ID_j||K_i)$, and also sends $\{A3_{MA}, T_2, z_{MA}P, PID_i, K_{MAj}, FID_i\}$ to the $D_j$".
- **Step 4:** "After obtaining the messages, $D_j$ selects a timestamp $T_3$ and computes $K_i = K_{MAj} \oplus key_j$ and $A3_{MA} = h(PID_j||key_j||ID_j||K_i)$. If the condition $(A3'_{MA} \stackrel{?}{=} A3_{MA})$ is valid, $D_j$ selects a random number $g_j$ and computes $sk_j = h(ID_j||g_j z_{MA}P||K_i||FID_i)$ and $Auth_j = h(sk_j||FID_i||T_3||K_i)$. Finally, $D_j$ sends $\{g_jP, T_3, Auth_j\}$ to the $MA$ through an insecure channel".
- **Step 5:** "Upon getting the messages, $MA$ computes $SK_{MA} = h(ID_j||z_{MA}g_jP||K_i||FID_i)$ and establishes a $SK$ between $MA$ and $D_j$. Thus, Nikooghadm et al.'s scheme cannot resist session key disclosure attacks because $MA$ establishes a session key with $D_j$ successfully".

On the other hand, if Nikooghadm et al.'s scheme [7] was designed that all participants cannot know $D_j$'s real identity, their scheme cannot establish the correct session key $sk_i = h(ID_j||z_i g_j P||K_i||FID_i)$ between $MU_i$ and $D_j$ successfully because all participants know only a $D_j$'s pseudo-identity $PID_j$. Consequently, Nikooghadm et al.'s scheme [7] does not ensure session key security or agreement due to these two cases.

### B. Mutual Authentication

Nikooghadm et al.'s scheme [7] claimed that their scheme ensures secure mutual authentication among $MU_i$, $CS$, and $D_j$. Unfortunately, we point out that their scheme cannot provide secure mutual authentication. Based on Section I-A, $MA$ is able to calculate $key_j = K_{ij} \oplus K_i$ and generate a authentication request message $A1_i = h(T_1||FID_i||K_i)$ successfully. Thus, Nikooghadm et al.'s scheme [7] cannot achieve secure mutual authentication because $MA$ can calculate an authentication message of the legitimate $MU_i$.

### C. Impersonation Attacks

Section I-A presents how $MA$ can obtain the secret credentials of mobile device and the exchanged messages through a public channel. After getting these the secret parameters, $MA$ generates a random number $z_{MA}$ and timestamp $T_{MA1}$. Then, $MA$ computes $z_{MA}P$ and $A1_{MA} = h(T_{MA1}||FID_i||K_i)$ and sends $\{T_{MA1}, z_{MA}P, A1_{MA}, FID_i, PID_j\}$ to the $CS$. Thus, Nikooghadm et al.'s scheme [7] is insecure to impersonation attacks because $MA$ can calculate the authentication request and response message, and the session key successfully.

### D. Drone Physical Capture Attacks

According to Section I-A, when $D_j$ is physically captured by $MA$, $MA$ is able to extract all secret credentials $\{ID_j, PID_j, key_j, h()\}$ in the memory. Moreover, $MA$ can replay, eavesdrop, insert, delete, and modify the exchanged messages over insecure channels. After that, $MA$ computes $K_i = K_{ij} \oplus key_j$ and generates a new random number $g_{MA}$ and a timestamp $T_{MA3}$. Then, $MA$ computes a session key $sk_{MA} = h(ID_j||g_{MA}z_iP||K_i||FID_i)$ and authentication message $Auth_{MA} = h(sk_{MA}||FID_i||T_{MA3}||K_i)$.Thus, Nikooghadm et al.'s scheme [7] cannot prevent drone physical capture attacks because $MA$ can impersonate as a legitimate drone and calculate a session key successfully.

## IV. Security Requirements and Guidelines

In Nikooghadm et al.'s scheme, the main security problems are that $MA$ can steal a mobile device of $U_i$ or capture the drones, and then $MA$ may attempt various security attacks. According to Section III, Nikooghadm et al.'s scheme [7] is vulnerable to various security attacks such as "MITM", "impersonation", and "session key disclosure" attacks and does not provide "secure mutual authentication". Thus, we propose some security requirements and guidelines to enhance the security shortcomings of Nikooghadm et al.'s scheme [7].

- **Guideline 1:** "During the AKA process, all parties should securely encrypt and send the sensitive information by utilizing a symmetric key since $MA$ can alter, delete, forge, inject, eavesdrop, block, and reuse the transmitted messages over an insecure channel".

- **Guideline 2:** "As shown in Section III, $MA$ can impersonate as a legitimate user successfully. Thus, Nikooghadm et al.'s scheme should store the masked secret credentials with random nonce, password, and biometric by using hash and XOR functions to improve the security level".
- **Guideline 3:** "In Nikooghadm et al.'s scheme, drones should utilize physical unclonable functions (PUF) to resist physical security attacks. PUF-based AKA schemes are resilient against physical capture and power-analysis attacks because $MA$ cannot access the PUF's secret value".
- **Guideline 4:** "Nikooghadm et al.'s scheme may cause serious security issues in the future since the exchanged message is not dynamic in each session. Hence, Nikooghadm et al.'s scheme [7] should periodically change the secret credentials to improve the security level".

It is worth noting that we do not claim that the security guidelines presented by us as a full-proof solution to the pointed out flaws of Nikooghadm et al.'s scheme. However, it will definitely increase the complexity of $MA$.

Nikooghadm et al.'s scheme [7] would have worked tirelessly to create a cryptographic protocol for useful service in IoT environments. Unfortunately, Nikooghadm et al.'s scheme would not have viewed their scheme from the point of view that we have analyzed and proven. Thus, these security guidelines will lead to the generating of more secure and effective authentication and key agreement protocols in IoT environments.

## V. Conclusions

In this paper, we proved that Nikooghadm et al.'s scheme is not resilient to potential security threats, including impersonation, session key disclosure, and MITM attacks and also do not provide secure mutual authentication. After obtaining the secret credentials stored in the mobile device or the drone, a malicious adversary calculates a common session key and then impersonates the legitimate entity. Thus, we suggest the necessary security requirements and guidelines to enhance the security flaws of Nikooghadm et al.'s scheme. Consequently, we can enhance the pointed out security issues not only in Nikooghadm et al.'s scheme, but we believe that these will be also helpful in future authentication and key agreement schemes for next-generation IoD.

## References


[1] S. Yu, A. K. Das, Y. Park, and P. Lorenz, "SLAP-IoD: Secure and Lightweight Authentication Protocol Using Physical Unclonable Functions for Internet of Drones in Smart City Environments". *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10374-10388, 2022.

[2] S. Balaji, K. Nathani, and R. Santhakumar, "IoT Technology, Applications and Challenges: A Contemporary Survey". *Wireless Personal Communications*, vol. 108, pp. 363-388, 2019.

[3] S. Yu, J. Lee, A. K. Sutrala, A. K. Das, and Y. Park, "LAKA-UAV: Lightweight Authentication and Key Agreemeht Scheme for Cloud-Assisted Unmanned Aerial Vehicle Using Blockchain in Flying Ad-Hoc Networks". *Computer Networks*, vol. 224, pp. 1-15, 2023.

[4] Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure Smart Health with Privacy-aware Aggregate Authentication and Access Control in Internet of Things". *Journal of Network and Computer Applications*, vol. 123, pp. 89-100, 2018.

[5] S. Yu, K. Park, and Y. Park, "A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environments". *Sensors*, vol. 19, no. 16, pp. 1-20, 2019.

[6] K. Park, S. Noh, H. Lee, A. K. Das, M. Kim, Y. Park, and M. Wazid, "LAKS-NVT: Provably Secure and Lightweight Authentication and Key Agreement Scheme Without Verification Table in Medical Internet of Things". *IEEE Access*, vol. 8, pp. 119387-119404, 2020.

[7] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A Provably Secure and Lightweight Authentication Scheme for Internet of Drones for Smart City Surveillance". *Journal of Systems Architecture*, vol. 115, pp. 1-16, 2021.

[8] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, pp. 198-208, 1983.

[9] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis, in Advances in Cryptology (CRYPTO)," Springer, 1999, pp. 388-397.

[10] S. Yu, N. Jho, and Y. Park, "Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes". *IEEE Access*, vol. 9, pp. 126186-126197, 2021.