Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7537764, 10 pages
https://doi.org/10.1155/2022/7537764

Research Article

An Identity Authentication Scheme Based on SM2 Algorithm in UAV Communication Network

Tao Xia and Jun He

National University of Defense Technology, Wuhan, Hubei, China

Correspondence should be addressed to Tao Xia; xiatao17@nudt.edu.cn

Received 28 June 2022; Revised 12 August 2022; Accepted 25 August 2022; Published 15 September 2022

Academic Editor: Kuruva Lakshmanna

Copyright © 2022 Tao Xia and Jun He. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the advancement of technology, the collaborative networking of multiple UAVs has become a mainstream trend. Due to the characteristics of UAV communication networks, there are many security issues with their communication networks. At present, the UAV communication network needs a secure and efficient authentication scheme. In this paper, we optimise an UAV authentication scheme based on the SM2 algorithm, design a two-way authentication mechanism to improve the security of the authentication scheme, and adopt the method of preshared secret information instead of digital signatures to improve the efficiency of authentication. Subsequently, the safety proof was based on the Dolev-Yao model. Finally, simulation experiments demonstrate that the scheme is more efficient in authentication compared to other similar authentication schemes and meets expectations.

1. Introduction

The use of drones in medical, disaster relief, and surveillance applications is already attracting attention [1, 2]. As the volume of tasks increases, single drones can no longer meet the demand and the trend is for multiple aircraft to work together. UAV clustering technology has now attracted a great deal of attention, [3–5] and many countries have made significant breakthroughs in this area. The United States has built inexpensive drone colonies by developing projects such as locusts and elves. In 2017, China demonstrated more than 100 fixed-wing drones in clusters, and tried and successfully demonstrated projects such as intensive launch and group operations. The communication network composed of UAV cluster network has the characteristics of openness, resulting in UAV communication is more vulnerable to illegal eavesdropping, identity counterfeiting, message replay, and other attacks. These problems pose a serious threat to the security of communications networks. The identity authentication scheme in the UAV communication network refers to the authentication between the UAV to enter the network and the already network access node, which is the main means to deal with security threats.

1.1. Related Work. In recent years, the identity authentication scheme in UAV communication network security has attracted wide attention. The authentication schemes can be divided into those supported by the control station and those not supported by the control station. The literature [6] demonstrates that authentication schemes supported by control stations consume fewer resources than those not supported by control stations. The PKI- (Public Key Infrastructure-) based certification scheme is mainly adopted in the certification scheme supported by the control station. Such schemes generally require the verification of digital certificates, while the computational cost is large, which is not suitable for UAV communication networks with limited resources. Therefore, Chen et al. [7] proposed a certification scheme that could avoid the time cost consumed by public key certificate systems and improve the efficiency of authentication. However, the scheme needs to use TPM (trusted platform module) for proof, and the hardware requirements

are too high. Srinivas et al. [8] uses a method that preshares data such as the user's biometric information from the initialization phase to the ground control station, but the authentication efficiency of this scheme is low due to the use of a certificate mechanism. Mahdi et al. [9] uses secret messages instead of digital certificates to improve authentication efficiency, but uses an ECC algorithm with a longer key length than the SM2 algorithm [10]. Rui [10] designs an authentication scheme for UAV communication networks based on the SM2 algorithm, but ignores two-way authentication and the authentication efficiency needs to be improved. Two-way authentication can therefore be added to authentication using secret information for security and can be made more efficient by completing some of the calculations in the key negotiation protocol during the initialization phase.

1.2. Motivations. Information transmitted over wireless channels is vulnerable to theft[11, 12], and drones usually use wireless transmission of information [13]. Altawy and Youssef [14] detail the security threats to UAV communication networks. A secure authentication scheme enables legitimate entities in a communications network to communicate securely and efficiently, thereby protecting the information of legitimate entities and effectively addressing the security threats faced by UAV communications networks such as[15–17]. In particular, mutual authentication between the drone and the control station verifies the legal identity of both parties before exchanging secret and sensitive information on an insecure communication channel. Several important factors need to be considered in order to ensure the advanced nature of the scheme. First, the scheme should be robust to different types of attacks, including counterfeit attacks and man-in-the-middle attacks. Moreover, according to Jan et al. [16], and Pan [18], the authentication scheme should have higher authentication efficiency and lower communication overhead. The identity authentication scheme should be more efficient than other similar identity authentication schemes.

1.3. Contributions. In order to address the security threats faced by UAV communication networks, this paper designs an authentication scheme. The main contributions are as follows:

(1) Analysis of security threats to UAV communication networks based on Dolev-Yao model. A two-way authentication mechanism suitable for the wireless communication environment is adopted in the authentication scheme

(2) A two-way authentication mechanism suitable for the wireless communication environment is adopted in the authentication scheme. Using preshared secret information instead of digital signature reduces the communication overhead and improves the authentication efficiency

(3) Using preshared secret information instead of digital signature reduces the communication overhead and improves the authentication efficiency

(4) The calculation of random numbers and elliptic curve points is completed in the initialization stage, shortening the authentication time

2. Threat Model and Attacker Definition

This chapter will define the attacker facing the UAV communication networks based on the Dolev-Yao threat model [19].

2.1. Threat Model Profile. The Dolev-Yao model, proposed by Dolev and Yao [19] in the 20th century, has been widely used and become a standard for wireless network security protocols. The model assumes that the attacker has the ability to control the entire communication network, and assumes that the cryptosystem is perfect. It is very suitable for attacker definition for low secure wireless networks such as UAV communication networks. The model's assumptions about the attacker's capabilities are shown in Table 1.

2.2. Determination of the Attacker. Combined with Dolev-Yao model, the main attacks on the UAV network are mainly impersonation attacks, replay attacks, eavesdropping attacks, and man-in-the-middle attacks.

2.2.1. Impersonation Attack. Impersonation attack refers to the fact that an attacker has intercepted legitimate user identity information to fake a legitimate user by using the identity information to enter the network. One is an attacker intercepting the authentication message of the drone, and the fake drone node requests the authentication from the control station or other drones in the network. Second, the attacker establishes a communication channel by sending a forged message to a node, which in turn negotiates a session key with that node.

2.2.2. Eavesdropping Attack. An eavesdropping attack refers to an attacker stealing information transmitted by a drone node or a control station. The threat model assumes that the attacker has access to all information transmitted in the drone network. Therefore, an attacker can obtain confidential information transmitted in the UAV communication network through an eavesdropping attack.

2.2.3. Replay Attack. A replay attack is when an attacker sends a packet already sent for the purpose of illegal authentication. An attacker can eavesdrop and intercept an authentication message from the drone or control station and reissue the message to the corresponding node for authentication.

2.2.4. Man-in-the-Middle Attack. Man-in-the-Middle Attack (MITM) is an "indirect" way of intrusion attack, where the attacker puts himself between the two nodes of the communication network through various technical means, and then the attacker is called the "middleman". Malicious UAV nodes in the UAV communication network forge the authentication message between the legal UAV nodes through this means, and eavesdrop on the communication between the two parties.

Table 1: The Dolev-Yao model attacker capability assumptions.

The ability of the attacker to have a capability	Capabilities not by the attacker
Obtain any through-communication network information	Do not have the ability to guess the random numbers in a large enough space
Having a legal identity in the communication network may impersonate other subjects to initiate communication with any subject	Without the correct key (or private key), an attacker cannot achieve a plaintext-to-ciphertext or ciphertext-to-plaintext conversion
Become the recipient of the information sent from any subject	You cannot solve a private part, for example, a private key that matches a given public key
Send messages posing as any subject to any other subject	An attacker cannot gain access to private areas such as the offline storage of individuals in the communication network.

3. Design of Identity Authentication Scheme Based on SM2 Algorithm in UAV Communication Network

The identity authentication scheme based on SM2 algorithm (SM2-efficiency) negotiation key using the official key negotiation algorithm of SM2 algorithm based on preshared secret information.

3.1. Parameter Representation. Relevant parameters are shown in the following (Table 2):

3.2. Initialization Phase of the Certification Scheme. The initialization phase, as shown in Figure 1, mainly completes the following steps.

Step 1. S generates an elliptic curve $E(F_a)$ on F_a (based on the SM2 algorithm). *g*, *n*, *a*, and *b* are the relevant parameters of the elliptic curve.

Step 2. S uses the key generation function to generate its own public-private key pair, where the private key is d_S and the public key is P_S.

Calculated Z_S according to

$$Z_S = SM3(ENTL_S||ID_S||a||b||X_G||Y_G||x_s||y_s). \quad (1)$$

Where $ENTL_S$ represents the two-byte length of the ID_S, and ‖ represents the string splicing operation.

Step 3. S generates a public-private key pair, identification ID_u, and one-time random number for *U*, where the private key is d_U and the public key is P_U.

calculated Z_U according to

$$Z_U = SM3(ENTL_U||ID_U||a||b||X_G||Y_G||x_U||y_U). \quad (2)$$

Step 4. S transmits $\{E(F_a), G, n, P_U, ID_u, d_U, ID_S, P_S, Z_U, Z_S\}$ to *U* via a secure messaging channel.

Both *S* and *U* will store the parameters required for the authentication phase.

Step 5. U and *S* generate r_U and r_S based on the SM3 algorithm, which belong to $[1, n-1]$. And the R_U and the R_S are calculated separately.

3.3. UAV and Control Station Certification Phase. The specific process of the UAV and control station certification stage is shown in Figure 2.

Step 1. U sends R_U and ID_u to *S*.

Step 2. The ID_u is verified and if a legitimate and unauthenticated ID_u exists, the verification passes. Subsequently, following Equation (3) to calculate $\bar{x_2}$

$$\bar{x_2} = 2^{\omega} + (x_2 \& (2^{\omega} - 1)), \quad (3)$$

following Equation (4) to calculate t_S

$$t_S = (d_S + \bar{x_2} \bullet r_S) \bmod n, \quad (4)$$

S1 was subsequently calculated using the elliptical curve point R_U. The calculation is calculated as

$$S1 = [h \bullet t_S](P_U + [\bar{x_1}]R_U) = (x_S, y_S). \quad (5)$$

Check S1 (If S1 is not infinitely far, the validation succeeds) and calculate the session key K_S according to

$$K_S = KDF(x_s||y_s||Z_U||Z_S, klen)(klen = 128bit). \quad (6)$$

If the session key K_S is being successfully obtained, then *S* sends the identity identification ID_s of the elliptic curve points R_S and *S* to the UAV node *U*.

Step 3. U receives and validates the information to generate the session key. *U* first tests the ID_s and passes. If there are legitimate and unauthenticated identification ID_s in the database, then validation passes.

U Extract the domain element x_1 by R_U, computes $\bar{x_1}$. It is calculated as

$$\bar{x_1} = 2^{\omega} + (x_1 \& (2^{\omega} - 1)). \quad (7)$$

Calculate t_U as

$$t_U = (d_U + \bar{x_1} \bullet r_U) \bmod n. \quad (8)$$

U tests the R_S of the elliptic curve points coming from *S*. U1 is calculated as

$$U1 = [h \bullet t_U](P_S + [\bar{x_2}]R_S) = (x_u, y_u). \quad (9)$$

Table 2: Certification scheme parameter table.

Order number	Main parameter	Illustration
1	S	UAV control station
2	U	Legal drones to be certified
3	$E(F_a)$	An elliptic curve over a finite domain F_a
4	$G = (x_G, y_G)$	Base point of the elliptic curve $E(F_a)$
5	n, a, b	Order and formula parameters of the elliptic curves
6	SM3()	SM3 password miscellaneous algorithm
7	d_S, d_U	Private keys for the control station and the drone
8	$P_U = [d_U]G$	Public key of the UAV to be certified
9	$P_S = [d_S]G$	Public key of the UAV control station
10	$Z_U\ Z_S$	Summary value of UAV and control station
11	ID_U, ID_S	Identifiability signs of drones and control stations
12	r_U, r_S	Random numbers generated by drones, control stations
13	$R_U = [r_U]G = (x_1, y_1)$	Elliptical curve points generated by the UAV
14	$R_S = [r_S]G = (x_2, y_2)$	The elliptical curve points generated by the control station
15	KDF()	Key derived functions
16	$ENTL_S$	The two-byte length of the ID_S
17	||	Represents a string splicing operation

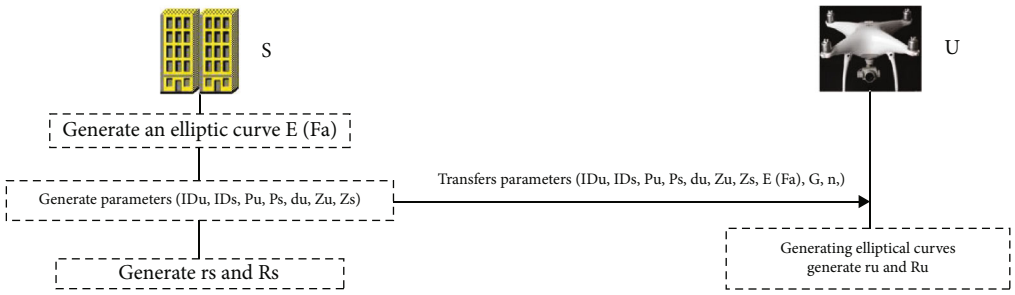

Figure 1: Schematic representation of the initial phase.

If U1 is not an infinity point, calculate KU according to

$$K_U = KDF(x_u||y_u||Z_U||Z_S, klen)(klen = 128bit). \quad (10)$$

Successfully obtained the session key K_U.

3.4. The Certification Phase between UAV R and UAV A. The certification process between the two drones is based on the establishment of safe communication channels between the two drones and the control station. The two drones are recorded as UAV R and UAV A, respectively, and the authentication steps are as follows:

Step 1. Drone R initiates a certification request. UAV R generates r_R, and $r_R \in [1, n-1]$. Subsequently, the discriminable identity ID_R was generated, calculating R_R based on r_R, and R_R was needed to satisfy $R_R = [r_R]G = (x_R, y_R)$. R sends the above parameters to the control station S via the encrypted channel.

Step 2. The control station S starts the authentication process. First, the control station S sends the received R_R and the summary value Z_R of R to the UAV A. Subsequently, the control station sends the summary information value of the UAV A, Z_A, to the UAV R.

Step 3. The UAV A generates the parameters and sends the authentication information. The UAV A generates r_A, and $r_A \in [1, n-1]$. The R_A is calculated from the r_A, and the R_A needs to satisfy the $R_A = [r_A]G = (x_A, y_A)$. The UAV A sends the parameters to the UAV R.

Step 4. UAV A calculates $\bar{x_A}$, from x_A in R_A according to

$$\bar{x_A} = 2^{\omega} + (x_A \& (2^{\omega} - 1)). \quad (11)$$

Then t_A was calculate as

$$t_A = (d_A + \bar{x_A} \bullet r_A) \bmod n. \quad (12)$$

$(x_{AK}, y_{AK}) = [h \bullet t_A](P_R + [\bar{x_R}]R_R)$ was calculated using parameters such as R_R. Convert x_{RK}, y_{RK} to bit string,

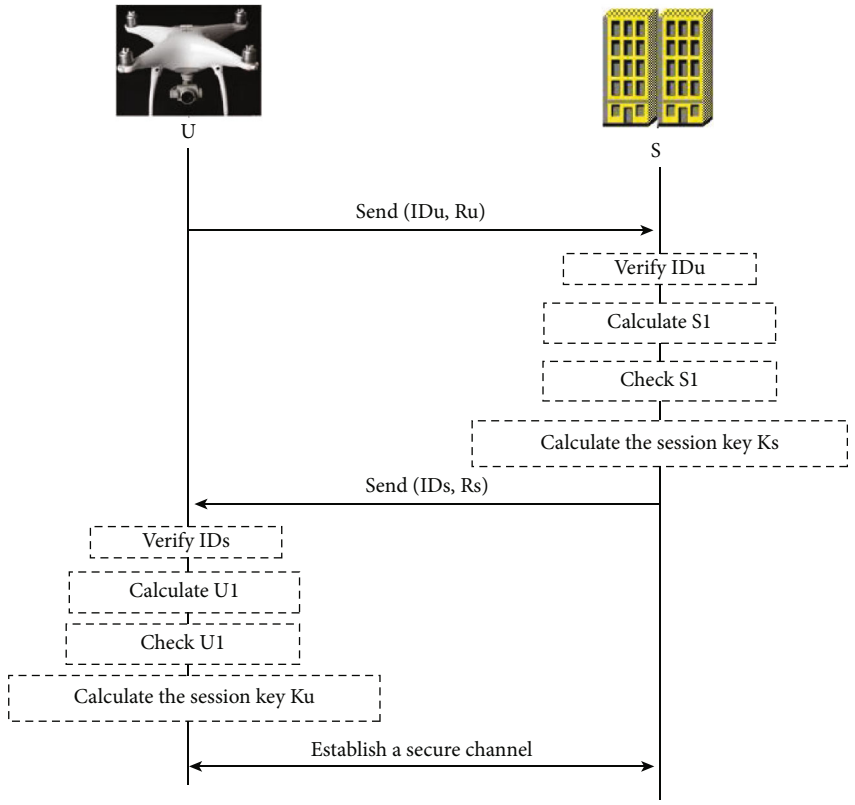

Figure 2: Schematic diagram of the certification phase.

```
Time_2 =get_cpu_time() #The start point of the authentication time is calculated
client. send(message(IDu,Ru)) #The start point of the authentication time is calculated
IDs,Rs = client. recv(1024)#The UAV receives the IDs and Rs sent by the control station
res = check(IDu) #The drone verifies the IDs
res, content = sm2_uav.negotiation(Rs, PS, IDS, option, Ru, Ru)#Key negotiation
if not res:
        print('error:', content)
        return
        if option:#Generates the negotiation key, the KU
        Ru, KU, SU, U2 = content
        else:
        Ru, KU = content
        SU = None
encData=client. recv(1024)#The drone receives the ciphertext
decData = SM4. decryptSM4(KU, encData)#The drone receives the ciphertext
Time_2 =get_cpu_time() #Calculate the cutoff point of the authentication time
print('Certification time consuming:%. 2f ms' % ((Time_2 - Time_1) * 1000))#Time used to output authentication
Command_send(decData)#The drone sends the decrypted commands to the UAV model operation in the Gazebo simulation
environment
```

Algorithm 1: Core algorithm of the UAV side.

calculate $K_A = KDF(x_{AK}||y_{AK}||Z_R||Z_A, klen)$. Get the negotiated session key K_A.

Step 5. R generates the session key after receiving the message. The UAV R calculates the $\bar{x_R}$ by Formula (13). Calculate the t_R by Formula (14).

$$\bar{x_R} = 2^{\omega} + (x_R \& (2^{\omega} - 1)), \tag{13}$$

$$t_R = (d_R + \bar{x_R} \bullet r_R) \bmod n. \tag{14}$$

Using parameters such as R_A to calculate $(x_{RK}, y_{RK}) = [h \bullet t_R](P_A + [\bar{x_A}]R_A)$, convert the x_{AK} and y_{AK} to a bit-string. Finally K_R is calculated following as

$$K_R = KDF(x_{RK}||y_{RK}||Z_R||Z_A, klen). \tag{15}$$

```
IDu,Ru = clientSocket. recv(1024)#The control station receives the IDu and Ru
res = check(IDu) #The control station checks the IDu
res, content = sm2_station.negotiation(Ru, PU, IDU, option, Rs, Rs)#Key negotiation
if not res:
        print('error:', content)
        return
if option:#Generates the negotiation key, the KS
        KS, SS = content
else:
        KS = content
clientSocket. send(message(IDs,Rs)#Send the IDs and Rs to the drone
encData = SM4. encryptSM4(KS, command)#The control station encrypts the instructions using a KS key
clientSocket. send(encData)#Send the text to the drone
```

Algorithm 2: Core algorithm of the control station end.

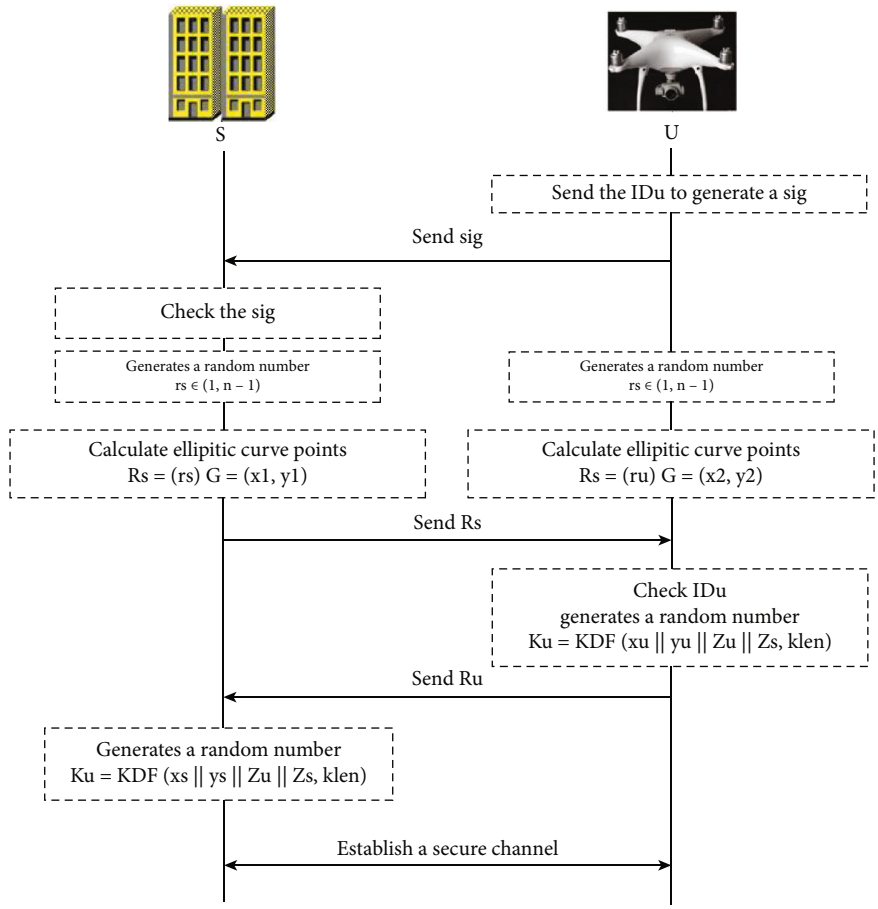

Figure 3: Schematic diagram of the SM2-normal scheme certification process.

3.5. Key Update Phase. To update the key, proceed as follows:

Step 1. The control station generates the public and private keys and sends them to the drone. The control station generates r in $[1, n-1]$ as the private key of the drone and computes the public key R and digest Z_{new} of the drone.

S generates random numbers $r \in [1, n-1]$, and calculate the elliptical curve points $R = [r]G = (x, y)$. The control station S takes the generated random number r as the new private key d_U of U, and R as the new public key P_U. The control station sends the P_U, identification ID_U and summary Z_U to the U.

Step 2. Update the key after the drone has verified that the data is legitimate. After the drone receives the information, verify that the Z_U is the same as that stored by itself. If the same, update your own public and private key and

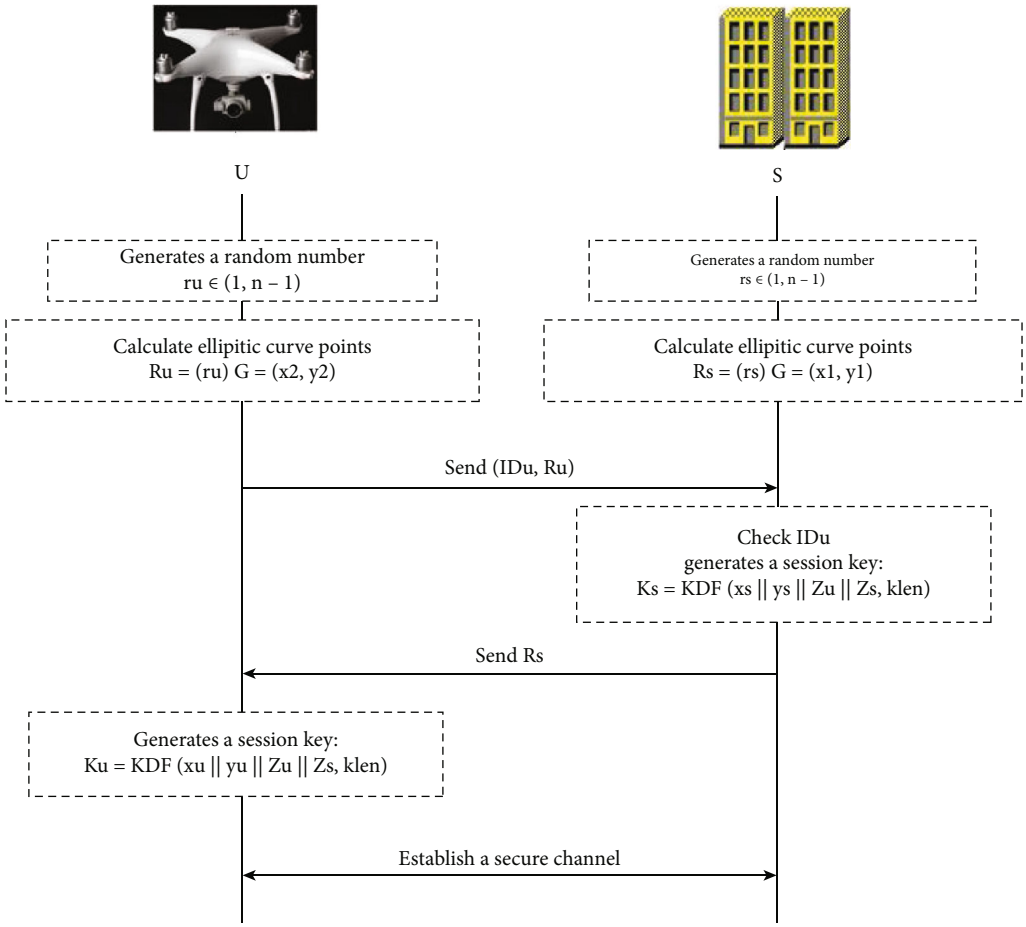

Figure 4: Schematic diagram of the literature [10] protocol certification process.

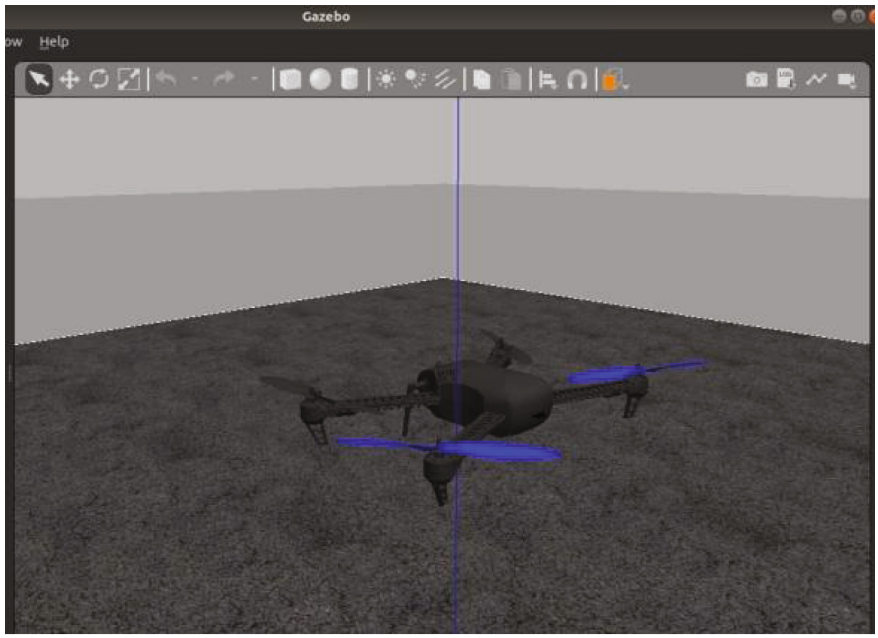

Figure 5: UAV model flight diagram.

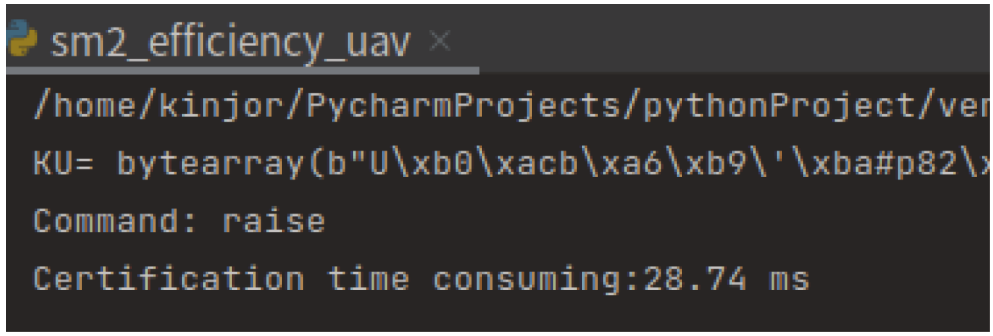

Figure 6: Output a screenshot of the authentication time.

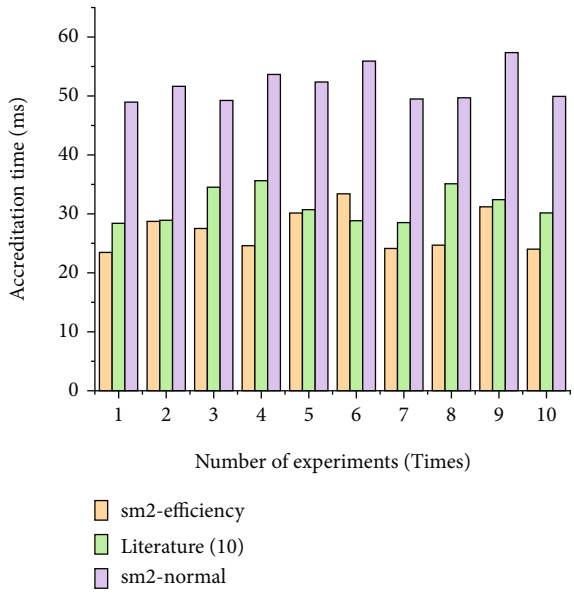

Figure 7: Histogram of the length of authentication.

digest. If they are the same, the drone updates its own public and private keys and digests. If they are not identical, the drone drops the packet.

3.6. Correct Analysis. It needs to be proved that the session key generated by the key parties through the KDF () function is equal.

Take the authentication key negotiation process of the UAV U and the control station S as an example. That needs to be proved

$$K_S = KDF(x_s||y_s||Z_U||Z_S, klen) = K_U = KDF(x_u||y_u||Z_U||Z_S, klen). \tag{16}$$

Inside:

$$\begin{aligned} S1 &= [h \bullet t_S](P_U + [\bar{x}_1]R_U) = (x_S, y_S), \\ U1 &= [h \bullet t_U](P_S + [\bar{x}_2]R_S) = (x_u, y_u). \end{aligned} \tag{17}$$

Based on the description of the SM2 key negotiation algorithm

$$(x_S, y_S) = (x_u, y_u). \tag{18}$$

The input of the key-derived function KDF () is the same in both formulas, and the verified output of the session key K_U and K_S is the same.

4. Safety Analysis

This chapter conducts a security analysis against the attacker definition described in Chapter 2.

4.1. The Ability to Withstand Impersonation Attacks

4.1.1. Attack Situation 1. In the authentication phase between the UAV and the control station, the attacker obtains a session key by analysing the information transmitted by the communication network and impersonates the control station or the UAV to communicate.

Defense analysis: If the attacker generates the correct session key, it needs to obtain the input value of the function KDF (), while the KDF () input values include Z_U and Z_S in which

$$\begin{aligned} Z_U &= SM3(ENTL_U||ID_U||a||b||X_G||Y_G||x_u||y_u), \\ Z_S &= SM3(ENTL_S||ID_S||a||b||X_G||Y_G||x_s||y_s). \end{aligned} \tag{19}$$

The attacker has no access to parameters such as a, b in the communication network to generate the correct digest values, so attack situation 1 is not valid.

4.1.2. Attack Situation 2. In the drone-to-drone authentication phase, the attacker obtains a session key by analysing the information transmitted by the communication network and impersonates the drone to communicate with the other party.

Defense analysis: Because the attacker cannot obtain the session key during the authentication phase between the UAV and the control station, the attacker cannot obtain the content of the communication between the UAV and the control station. Therefore, according to the threat model, an attacker cannot obtain parameters such as Z_R and Z_A transmitted in an encrypted channel. Therefore attack situation 2 is not valid.

4.1.3. Attack Scenario 3. The attacker communicates with the ground control station disguised as a drone during the key update process.

Defense analysis: According to the threat model, the attacker does not have the ability to break the encryption algorithm without the key being known; therefore the attacker cannot obtain the key parameters. Attack situation 3 is not valid.

4.2. Ability to Withstand Eavesdropping Attacks

4.2.1. Attack Situation 4. The attacker obtains the plaintext by analysing the information passed in the drone's communication network.

Defense analysis: Attack scenarios 1 and 2 have proved that the attacker cannot derive the key from the eavesdropping information. So the attack case 4 is not true.

4.2.2. Attack Situation 5. Attackers execute other types of attacks by analysing the information passed through the drone's communication network.

Defense analysis: Attack scenario 5 has proved that the attacker cannot obtain the clear text. So the attack scenario 5 is not valid.

4.3. Ability to Withstand Man-in-the-Middle Attacks

4.3.1. Attack Situation 6. During the authentication process, the attacker obtains the same session identity through the conversation key as the attacker.

Defense analysis: An attacker tampers with and replaces some interactive information in the authentication process with his own information through a middleman attack in the following situations:

(1) Attack scenario 6-1. The attacker attempts to send $\{R\_U, \mathrm{ID}_u\}$ to the UAV during the authentication process with the control station, or $\{R_S, \mathrm{ID}_S\}$ to the UAV as the control station. The correct session key is generated after the success.

Defense analysis: If an attacker wants to send $\{R\_U, \mathrm{ID}_u\}$ or $\{R_S, \mathrm{ID}_S\}$, he needs to obtain an unauthenticated and legally identifiable identification, and the attacker does not have the ability to guess the random numbers safely stored by the drone or the control station. Therefore, the attack case, 6-1 does not hold.

(2) Attack scenario 6-2. An attacker attempts to initiate a middleman attack in the process of mutual authentication between the drones or during the key update phase.

Defense analysis: According to the threat model, an attacker cannot achieve plaintext-to-ciphertext or ciphertext-to-plaintext conversion without knowing the key, so attack scenario 6-2 is not valid.

4.4. Ability to Withstand Replay Attacks

4.4.1. Attack Situation 7. During the authentication stage, the attacker replayed the obtained information and successfully executed the authentication protocol with the legal entity in the UAV communication network, and obtained the same session key.

Defense analysis: It has been demonstrated in the defense analysis of impersonation attacks that the attacker does not have access to key parameters. However, if the attacker replayed the stored historical messages, this could be divided into two cases as follows.

Attack scenario 7-1: The attacker replays the $\{R_U, \mathrm{ID}_u\}$ sent by the UAV node to the control station.

Defense analysis: If the control station compares the ID*u* , you can know that the UAV node has been verified, and the message received is a replay message, not through the verification. Therefore, the attack case, 7-1 does not hold.

Attack scenario 7-2: The attacker replays the $\{R_S, \mathrm{ID}_S\}$ sent by the control station to the UAV.

Defense analysis: the control station comparesID_S, you can know that this ID is illegal and does not pass the verification. Therefore, the attack case, 6-2 does not hold.

5. Simulation and Experimental Testing

To verify the improved performance of the SM2-efficiency scheme over the SM2-normal scheme (the traditional authentication scheme based on the SM2 algorithm) and the literature [10] scheme, this chapter designs simulation experiments to test the time required to complete the identity authentication of the three authentication schemes.

5.1. Experimental Environment. The experimental environment is mainly divided into two parts: control station terminal and UAV terminal. The control station end is configured with Intel(R)Core$(\mathrm{TM})i7-7700\mathrm{HQ}$ CPU@2.80 GHz 2.81 GHz, 16GB RAM. The UAV side is configured with Intel$(R$ $)$Core$(TM)i7-7700\mathrm{HQ}$ CPU@2.80 GHz 2.81 GHz, 8GB RAM. Uses the 2.4 GHz channel commonly used by drones [20] for communication. The main algorithms are written in python language, and the core algorithms of control station end and UAV end are as follows:

The comparison schemes are the SM2-normal scheme and the literature [10] scheme, where the authentication process of the SM2-normal scheme is shown in Figure 3.

The flow of the scheme in the literature [10] is shown in Figure 4.

5.2. Experiment Content and Results. The UAV node and ground control station procedures of the ten SM2-efficiency schemes, the SM2-normal schemes, and the literature [10] schemes are performed, respectively. A screenshot of the instructions received by the UAV model during operation is shown in Figure 5.

A screenshot of the output authentication time of a certain UAV is shown in Figure 6:

The authentication time of the UAV terminal output of each authentication scheme is recorded and drawn into a bar chart, and the results are shown in Figure 7.

As can be seen from the figure, the SM2-efficiency certification scheme designed in this paper requires the least certification time. After statistics, the average authentication time of the SM2-efficiency scheme is 27.27 ms, 31.33 ms for

the literature [10] scheme, and 51.84 ms for the SM2-normal scheme. Therefore, the SM2-efficiency certification scheme is about 15% higher relative to the literature [10], and 90% higher relative to the SM2-normal scheme.

6. Conclusion

With the diversification and complexity of UAV execution tasks, multi-UAV network collaboration has become an irreversible trend. Communication network security is an important basis of the UAV network, and one of the effective means to ensure that the UAV communication network is protected from security threats is to design an efficient and secure authentication scheme. In this paper, the idea of preshared secret information is used to optimise the authentication scheme for UAVs. The security analysis based on Dolev-Yao model has proved the security of the authentication scheme. Finally, the experimental simulation results show that this scheme is significantly more efficient than other authentication schemes. Future related studies can focus on the optimization of the SM2 algorithm structure as well as the standardization of the UAV certification process. Applying AI to identity authentication is also an important future research direction.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no competing interest.

Authors' Contributions

Tao Xia and Jun He are the co-first authors since they contributed to the manuscript equally.

References

[1] S. Ullah, K.-I. Kim, K. H. Kim et al., "UAV-enabled healthcare architecture: issues and challenges," *Future Generation Computer Systems*, vol. 97, pp. 425–432, 2019.

[2] H. Morohosi, "Network-based multiple UAVs search planning for disaster relief," *Journal of the Operations Research Society of China*, vol. 8, no. 4, pp. 669–679, 2020.

[3] L. Hu, Y. Tian, J. Yang, T. Taleb, L. Xiang, and Y. Hao, "Ready player one: UAV-clustering-based multi-task offloading for vehicular VR/AR gaming," *IEEE Network*, vol. 33, no. 3, pp. 42–48, 2019.

[4] Z. Jiaxian, *Research on Topology Reconfiguration and Key Technologies of UAV Cluster Network*, Xi'an University of Technology, 2022.

[5] X. Na, "Research on multi-UAV game decision making and cooperative communication method," Tianjin University, 2020.

[6] H. Zhu, Z. Yeping, P. Yu, Z. Zhiyi, H. Wu, and Z. Haiqiang, "Key management and authentication protocol for UAV networks," *Engineering Science and Technology*, vol. 51, no. 3, pp. 158–166, 2019.

[7] L. Chen, S. Qian, M. Lim, and S. Wang, "An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems," *China communications*, vol. 15, no. 5, pp. 61–76, 2018.

[8] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.

[9] N. Mahdi, A. Haleh, I. S. K. Hafizul, and M. M. Farhadi, "A provably secure and lightweight authentication scheme for Internet of drones for smart city surveillance," *Journal of Systems Architecture*, vol. 115, article 101955, 2021.

[10] R. Guo, *Design of Lightweight UAV Network Authentication Key Negotiation Protocol Based on National Secret Algorithm*, Xidian University, 2021.

[11] Y. K. Ever, "Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks," *IEEE Systems Journal*, vol. 13, no. 1, pp. 456–467, 2019.

[12] A. T. Fadi, E. Y. Kirsal, E. Enver, H. X. Nguyen, and D. D. Bakkiam, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, pp. 24617–24631, 2017.

[13] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of drones applications," *Computer Communications*, vol. 155, pp. 143–149, 2020.

[14] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, pp. 1–25, 2016.

[15] T. Muhammad, Z. A. Hussain, A. Musheer, B. Abdullah, and A. Hosam, "LAKE-IoD: lightweight authenticated key exchange protocol for the Internet of drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.

[16] S. U. Jan, I. A. Abbasi, and F. Algarni, "A mutual authentication and cross verification protocol for securing Internet-of-drones (IoD)," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 5845–5869, 2022.

[17] J. Won, S.-H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," in *Proceedings of the 10th ACM symposium on information, computer and communications security*, 2015.

[18] P. Yu, *Research and Realization of UAV Communication Security Support Technology*, Xidian University, 2018.

[19] D. Dolev and A. C.-C. Yao, "On the security of public key protocols," *IEEE Trans. Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[20] Y. Zijun, *Research on Anti-Spoofing and Communication Encryption Technology of Quadrotor UAV*, University of Electronic Science and Technology, 2017.