A lightweight identity authentication scheme for UAV and road base stations

Yinyin Li
International Joint Research Laboratory for Cooperative Vehicular Networks of Henan, Kaifeng
Henan University
Kaifeng, Henan
104753190645@henu.edu.cn

Xiaoyu Du†
School of Computer and Information Engineering
Henan University
Kaifeng, Henan
dxy@henu.edu.cn

Sufang Zhou
Institute of Data and Knowledge Engineering
Henan University
Kaifeng, Henan
zsf@henu.edu.cn

ABSTRACT

At present, unmanned aerial vehicles (UAVs) have been widely used in civilian fields (such as smart cities). However, the external environment of the UAV network is complex and computing resources are limited, so it is vulnerable to serious security threats, such as replay attacks, forgery attacks, man-in-the-middle attacks. Seriously, it will cause great damage to the work of the UAV in smart cities. Aiming at the problem of transmission instruction data leakage caused by malicious UAV in communication between road base stations and UAVs, this paper proposes a lightweight identity authentication scheme based on elliptic curve cryptography (ECC). The purpose is to ensure the identity authentication of the UAV and the road base station, to ensure that the mission instructions received by the UAV are authentic and reliable, and to ensure the privacy of the UAV's identity information. The algorithm mainly includes the system initialization phase, initializing the UAV and road base station, and the identity authentication phase. Compared with the traditional identity authentication method, this method has the characteristics of low computational cost, short key and high security, and is more suitable for UAV communication.

CCS CONCEPTS

•Security and privacy~Security services~Authentication •Security and privacy~Network security~Mobile and wireless security

KEYWORDS

Elliptic curve cryptography (ECC); Identity authentication; UAV and road base stations;

CIAT 2020, December 4–6, 2020, Guangzhou, China

ACM ISBN 978-1-4503-8782-8/20/10…$15.00
https://doi.org/10.1145/3444370.3444547

1 Introduction

With the development of aviation technology and smart cities, unmanned aerial vehicle (UAV) are becoming more and more popular. Since the 2008 Wenchuan earthquake in Sichuan, the use of UAV has begun to rise in China. As of 2019, the market size of UAV had reached 21 billion yuan [1]. At present, the UAV are widely used in distribution, aerial photography, surveillance, tracking, agriculture, surveying, rescue and personal hobbies. Compared with a single flight system, the UAV group can meet different operational requirements, and each UAV in the network can perform different tasks. Since UAVs usually carry secret data and tasks, and may even threaten national security, identity authentication must be performed when new UAV join the network or when they communicate with road base stations to prevent malicious nodes or attackers. UAVs are gradually playing an important role in smart cities. For example, the UAV can achieve target detection, precise positioning, and data collection in urban environments. During the 2019-nCoV epidemic, the UAV has achieved unmanned material distribution and residents' social distance monitoring, helping to better slow the spread of 2019-nCoV. When the UAV perform tasks, they are vulnerable to attacks such as interference, eavesdropping, deception, and hijacking [2] due to the particularity of their networks, so the network security of UAVs is becoming more and more important in the current stage of social development.

The UAV network is a typical Ad Hoc network, which has the characteristics of rapid changes in the network topology, so the reliability and safety of network communication are more demanding. The security of UAV communication is first to pass secure identity authentication to ensure the correctness of the identity during the communication process and maintain the integrity of the data. Due to the limited battery resources of UAVs, safety and energy efficiency are also one of the issues that cannot be ignored. In order to save resources, the certification should be completed as soon as possible to perform the task [3], so the design of the UAV certification scheme must be lightweight of.

The design of this scheme is mainly based on the smart city scene in Figure 1. In the identity authentication process of the

UAV and the road base station, step ① represents that the UAV sends an authentication request to the road base station. Step ② represents the road base station to apply to the trusted center TA to verify the identity of the UAV. Step ③ It means that the TA feeds back the identity information of the UAV, and the road base station checks it. Step ④ It means that the road base station sends an instruction message to the UAV after the check is successful.

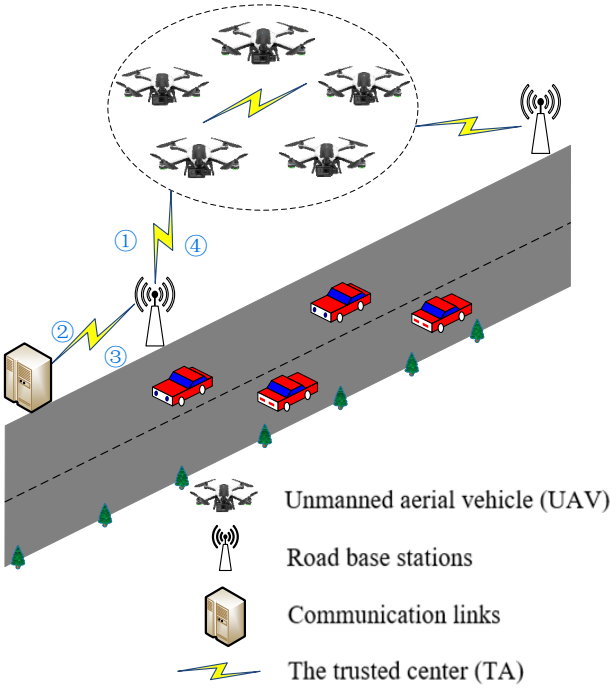

Figure 1: Identity authentication of UAV and road base stations in smart city scenarios

This article first introduces the safety issues that may be encountered in the communication process of UAVs, especially UAVs and road base stations. Since the road base station is the center of direct mission instructions to UAVs, once the road base stations communicate with UAVs Destroying directly causes the UAV to communicate with the attacker, causing the data carried by the UAV to be snooped, and severely causing the UAV to accept dangerous mission instructions, causing the UAV to destroy it, and seriously threatening people The safety of life, so its communication security is particularly important. It mainly proposes a lightweight identity authentication scheme based on elliptic curve algorithm to ensure the safety and data integrity of the communication between UAV and road base station. The main contributions of this article are as follows:

1) A lightweight elliptic curve algorithm for UAV and pavement base station safety certification scheme (UASECC) is proposed. Compared with the currently more popular RSA algorithm, its authentication efficiency is higher, the overhead is smaller, and it is more suitable for internet of drone (IOD).

2) By designing the UAV's anonymous identity, the UAV can protect its true identity from leaking when communicating with any node, and ensure the security of the UAV's identity information.

3) When the UAV and the road base station perform identity authentication, it mainly depends on the trusted center (TA) to determine the identity information of both parties (It is assumed that TA is the most secure and reliable).

2 Related Work

In the internet of drone (IOD) environment, the UAV is vulnerable to various attacks. In the process of performing tasks in the air, the road base station has the most contact with the UAV. The road base station communicates with the UAV to obtain real-time road information (such as traffic conditions and weather conditions) collected by the UAV, and issue new mission instructions to the UAV at any time. However, when UAV and road base stations send collected real-time road information, they can easily be intercepted by malicious users. And when the drone receives instructions from the road base station, it is easy to be tampered with by malicious users. Therefore, the UAV network is very vulnerable.

At present, there is relatively little research on the safety of UAVs, and the current mainstream solutions also draw on the idea of Ad Hoc security networking. In 2016, Gharibi et al. [4] pointed out that various threats must be prevented. Among the most prominent threats are the authentication of UAVs and other components outside the IOD system, the interference of broadcast information, the blockage of airspace and the hacking of UAVs. Lamport [5] introduced the concept of password-based remote authentication. Inspired by this pioneering work, many researchers have put forward their innovative suggestions for designing more secure authentication protocols in various environments. Watro [6] proposed a user authentication protocol based on the RSA algorithm, using the Diffie-Hellman key exchange algorithm to calculate the encryption key, but the protocol is easily affected by sensor nodes, so the protocol is easy to be disguised as the user of the sensor attack. However, Tseng [7] and others further pointed out that the Watro method is easy to leak passwords. In order to prevent users from changing passwords at will, Tseng et al. proposed an enhanced user authentication method to deal with various attacks and reduce password disclosure vulnerabilities.

Most of the methods to solve the UAV identity authentication problem need to consume a lot of computing resources, which reduces the quality and efficiency of communication, and is not suitable for the highly dynamic UAV network. The traditional password protection method uses modular exponentiation. In order to reduce the amount of calculation, the elliptic curve encryption algorithm is regarded as the best choice because of its faster calculation speed for the same data. Therefore, this paper proposes an identity authentication method based on the elliptic curve encryption algorithm. By anonymizing the UAV's identity, it ensures that the UAV will not leak its identity information during communication at any time, and avoid data leakage. The

method proposed in the article must meet the following requirements:

1) Lightweight computing. Due to the hardware limitations of the UAV, it is not allowed to conduct too much data analysis and processing. Therefore, a lightweight elliptic curve is the best choice.

2) Reliable identity authentication. This method requires a third-party trusted center to perform identity authentication more reliably.

3 Identity Authentication Phase

This chapter is divided into three stages according to the designed scheme: system initialization stage, initializing UAV and road base station, and identity authentication stage. The symbol definition of the design is as follows:

Number	Notations	Definition
1	p, q	two large prime numbers.
2	E	an elliptic curve defined by the equation $y^2=x^3+ax+b \bmod p$, where $a, b \in F_p$
3	G	an additive group with the order q, where G consists of all points on the elliptic curve E.
4	P	a generator of the group G
5	s	the private key of the system
6	P_{pub}	the public key of the system
7	P_R	the public key of the road base station
8	H	a secure function
9	ID	the identity of the UAV
10	AID	the anonymous identity of the UAV
11	U_i	the public key of the UAV
12	$\|\|$	the message concatenation operation.

3.1 System Initialization

In the system initialization phase, the Trusted Center (TA) generates system parameters (a finite field and its defined elliptic curve), and the information is loaded on the UAV system by the TA, and then broadcast to the UAV network.

1) The trusted center (TA) chooses two large prime numbers p, q and an elliptic curve E: $y^2=x^3+ax+b \bmod p$, where $a, b \in F_p$. An additive group G of order q formed by all points on the elliptic curve E, TA selects a generator P of order q in G, P is composed of all points on the elliptic curve E and infinite points.

2) TA chooses a random number s, where $s \in Z_q^*$ and calculates the public key of the system as $P_{pub}=s \cdot P$. Only TA knows s and can be used to extract part of the key (and the traceable master key).

3) TA chooses a safe hash function $H \{0,1\}^* \rightarrow Z_q^*$.

4) TA assigns a real identity ID and certificate Cert to each UAV, and pre-installs the message page $mes=\{ID_i, Cert_i, s\}(i=1,2,3)$ into each UAV.

5) The TA sends the system parameters $parmas=\{p,q,a,b,P,F_p,P_{pub},H\}$ to road base stations and UAVs.

3.2 Initialize UAVs and Road Base Stations

In the phase of initializing the identity information of the UAV and the road base station, when a new UAV needs to be added to the current network, the UAV will send its real ID to the TA. TA verifies whether it is legal. If it is not, the joining fails. If it is legal, TA generates an anonymous identity and security certificate for the UAV based on the elliptic curve mechanism.

1) TA generates a set of random numbers $m_i \in Z_q^*$, and calculates the corresponding point position $Pm_i=m_i \cdot P$ through the elliptic curve; TA generates its corresponding anonymous identity $AID_i=H(ID_i \| Pm_i \| T_i)$ for the UAV (where D is the current timestamp), so the real UAV The identity ID is hidden in AID_i.

2) The UAV chooses a random number x as its private key, and calculates the UAV's public key $U_i=x \cdot P$.

3) M_i is the road surface information collected by the UAV. The UAV encodes $\{AID_i, M_i, U_i, Cert_i\}$ to a point O on the elliptic curve and generates a random number r to calculate $C1=O+rP_{pub}$ and $C2=rP$.

4) The road base station generates its unique identity RID_i, and selects a random number w to calculate the public key $P_R=w \cdot P$ of the road base station. Code $\{RID_i, P_R\}$ to a point J on the elliptic curve, and select a random number n to calculate $C3=J+nP_{pub}$ and $C4=nP$.

3.3 Identity Authentication

At this stage, the trusted center mainly relies on the assessment of the safety of UAVs and road base stations. Based on the difficulty of ECDLP, the safety certification of UAVs and road base stations is achieved through a third-party secure trusted center.

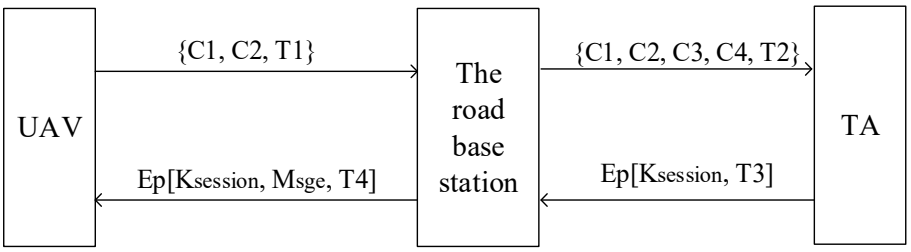

Figure 2: Detailed process description diagram of identity authentication for UAV and road base station

Figure 2 is a detailed process description diagram of the identity authentication of the UAV and the road base station. he UAV and the road base station use the trusted center TA to determine each other's identity information, thereby ensuring the reliability of identity authentication.

The road base station sends page $\{RID_i, P_R, M_{sge}, T_i\}$ to the UAV for identity authentication. The UAV verifies the identity information of the road base station. After the identity authentication is successful, the UAV receives the task instruction message M_{sge} sent by the road base station and executes it. UAVs and road base stations perform identity authentication based on elliptic curves. The identity authentication process is as follows:

1) The UAV initiates an authentication request with the corresponding road base station and sends $\{C1,C2,T1\}$ to the road base station.

2) After the road base station receives the authentication message sent by the UAV, it verifies whether the time stamp T1 is within the acceptable delay range ($T-T_i<\Delta T$, T is the time when the message is received, T_i is the current timestamp, and ΔT is the corresponding maximum transmission delay in the UAV scenario).

If it is within the acceptable time delay range, according to formula (1), the coordinate information of point O is obtained, and point O is decoded to obtain the encrypted content.

$$O=C1-wC2=O+rP_{pub}-r(\mathrm{s}\cdot P) \tag{1}$$

The road base station sends the received UAV information and its own identity information $\{C1, C2, C3, C4, T_2\}$ to the trusted center TA.

In the same way, we get formula (2):

$$J=C3-sC4=J+nP_{pub}-n(\mathrm{s}\cdot \mathrm{P}) \tag{2}$$

3) TA first verifies whether the timestamp T2 meets the minimum delay requirement, after receiving the message packet sent by the road base station. After meeting the requirements, TA verifies formula (1) and formula (2). After the verification is successful, a successfully verified session key $K_{session}$ is generated, and $Ep[K_{session}, T3]$ is sent to the road base station.

4) After receiving the TA message, the road base station decrypts the data packet with its own private key to verify whether the time stamp T3 meets the minimum delay requirement. If the requirements are met, complete the certification of the UAV on the road base station, and save the corresponding session key $K_{session}$ of the UAV, AID_i of the UAV, and the certificate Cert of the UAV.

5) After the UAV receives the data packet from the road base station, it decrypts it with its own private key to verify whether the timestamp T4 meets the minimum delay requirement. If it meets the requirements, complete the identity authentication of the UAV and the road base station. Finally, the UAV executes the message instruction.

4 Security and Assessment

Because the UAV network is highly dynamic, it requires lower CPU overhead and takes up less bandwidth and storage space. Compared with the RSA algorithm, the elliptic curve encryption algorithm has a shorter key generation time, which is more in line with the needs of the UAV network. By encrypting the 128bit data for 30 times, the average processing time ratio of ECC and RSA is about 1: 163; And a shorter key can achieve the same encryption security, so the elliptic curve encryption algorithm is the best choice in the UAV communication network. The elliptic curve encryption algorithm mainly relies on the difficulty of the discrete logarithm problem. Selecting a secure elliptic curve can ensure the security of data encryption.

- Unforgeability: When the UAV communicates with the road base station, the messages sent by the UAV are only C1 and C2, so third-party malicious attackers cannot forge communication information by cracking their private keys.
- Replay attack: Since the timestamp T is included in the information during each communication, the validator can detect the replay attack when the time is not fresh.
- Traceability: Since the real identity of the UAV is in the anonymous identity $AID_i = H(ID_i \| Pm_i \| T_i)$, the TA can extract the real identity of the UAV from the anonymous identity of the UAV through the key.

- Resilient to Message Modification Attack: Because the road base station relies on elliptic curve encryption when launching mission commands to the UAV, the difficult attacker based on ECDLP cannot crack the communication packet and modify the mission command in a short time.
- Man-in-the-middle attack: After receiving the message from the UAV, the ground base station will first verify the message $C1 - wC2 = O + rP_{pub} - r(\mathrm{s}\cdot P) = O$, and then decode the point O to obtain the encrypted content. By verifying the correctness of the UAV's identity, it is ensured that the message is not subject to man-in-the-middle attacks.

5 Conclusion

With the development of society and the advancement of science and technology, the development and use potential of UAVs have brought more and more convenience to people's lives, so they are used more and more widely. Today, UAVs also play an indispensable role in smart transportation. Therefore, the security risks in the UAV network are gradually exposed one by one. Identity authentication can ensure that the UAV will not receive mission instructions from malicious users and perform illegal missions when communicating. This paper mainly studies the identity authentication of UAV and road base station, the purpose is to ensure that the mission instructions issued by the road base station received by the UAV are true and credible. Due to the particularity of the UAV network, a lightweight elliptic curve encryption algorithm was selected and compared with the traditional public key encryption algorithm RSA. For the same size of encrypted information, the elliptic curve encryption algorithm authentication time can be shortened to one hundred and sixty-thirds of RSA, which can realize efficient authentication and achieve higher security.

ACKNOWLEDGMENTS

This work was supported by National Natual Science Foundation of China (61701170), Science and technology development plan of Henan Province (202102210327).

REFERENCES

[1] Prospective Industry Research Institute UAV Research Group, "Analysis of the Development Status and Prospects of my country's UAV Industry," Dual-use Technologies and Products, pp. 10-19, 07 2020.
[2] HAYAT S, YANMAZ E and MUZAFFAR R, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," IEEE Communications Surveys & Tutorials, pp. 2624-2661, 2016.
[3] D. A. K. ,. K. N. ,. e. a. Jangirala S, ". TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment[J].2019:1-1.," IEEE Transactions on Vehicular Technology, pp. 1-1, 2019.
[4] R. B. a. S. L. W. M. Gharibi, "Internet of Drones," IEEE Access, pp. 1148-1162, 2016.
[5] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, pp. 770-772, 1981.
[6] D. K. S. C. C. G. C. L. P. .. K. a. P. .. T. R. Watro, "Securing sensor networks with public key technology," Proceedings of the 2nd ACM Workshop On Security Of Adhoc and Sensor Networks, pp. 59-64, 2004.
[7] R.-H. J. a. W. Y. H.-R. Tseng, "An improved dynamic user authentication scheme for wireless sensor networks," in IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference, pp. 986-990, 2007.