Research Article

Cross-Domain Authentication Technology of UAV Based on Alliance Chain

Tao Xia, Jun He, and Haifeng Liu

National University of Defense Technology, Wuhan, Hubei, China

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

Received 16 June 2022; Revised 5 August 2022; Accepted 10 August 2022; Published 21 September 2022

Academic Editor: Lalit Garg

Copyright © 2022 Tao Xia et al. 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.

As the application scope of UAV expands, the demand for the cross-domain mission execution capability of UAV is increasing, which also puts forward higher requirements for the cross-domain certification capability of UAV. This paper proposes and verifies a cross-domain authentication scheme based on alliance chain technology. The experimental results show that compared with the original scheme, it greatly improves the efficiency of cross-domain authentication while solving the problem of trust between control stations.

1. Introduction

As technology advances, drones can carry a variety of sensors that collaborate to complete related tasks [1, 2]. Various applications [3] and the ability to work efficiently have increased the demand for the ability of drones to work across domains. In order to achieve the trust between the control stations and ensure the efficient cross-domain authentication of the UAV, this paper designs a cross-domain authentication scheme based on the alliance chain technology.

1.1. Related Work

With the development of science and technology, more demands are raised for the ability of UAV to perform missions across domains. In order to ensure the capability of cross-field work, the design of cross-field certification mechanism with high certification efficiency and high-security guarantee has become the focus of UAV safety technology research.

At present, there are three main cross-domain authentication technologies used for drones, as shown in Table 1.

Literature [4] uses hash and other algorithms to realize the identity information protection of cross-domain authentication UAV, and literature [5] uses the Dijkstra algorithm to improve the transmission efficiency between the registration domain and the receiving domain. However, both have two problems. One is the low authentication efficiency because the communication between the distant two-side domain control stations needs to pass through the relay station, and it is extended and easy for interference. Second, the success rate of certification cannot be guaranteed. When the registration domain control station is invaded or damaged or the communication between the control stations is strongly disturbed, the relevant legal UAV will fail temporarily or even permanently certification.

Long-term authorization of cross-domain authentication means that one CA stores the standardized information provided by the other CA as login information for a long time. In this case, there are often overdue information caused by delayed update problems [6]. This method cannot quickly reach a consensus between control stations and meet the requirements of low latency and high credibility between UAV control stations, so it is not suitable for cross-domain authentication.

Blockchain technology is a new application mode of computer technology such as consensus mechanism, distributed data storage, and encryption algorithm. It has the characteristics of decentralization, tamper-proof, anti-forgery prevention and high reliability and can be divided
1.2. Motivations. Due to the wireless communication between drones and control stations, there are urgent security challenges in the cross-domain process. Specifically, UAV communication networks are vulnerable to man-in-the-middle attacks, replay attacks, and other attack methods [11]. Therefore, a secure cross-domain authentication scheme is needed that enables the registered and authorized UAVs to safely communicate with the control stations in the nonregistered domain, thereby protecting their privacy and security. In particular, the identity of the communicating party can be verified by mutual authentication between the UAV and the control station before exchanging secret and sensitive information on the insecure communication channel. Several important factors need to be considered in designing cross-domain identity authentication schemes. First, the proposed scheme should be robust to different types of attacks, including middleman attacks, replay attacks, and eavesdropping attacks. In addition, due to the limited resources available for drones, expensive authentication (such as digital certificates) is necessary. Finally, it is necessary to achieve mutual trust between the different control stations to facilitate the information transmission between the control stations. Drones have limited energy resources [12], so need lightweight authentication solutions. Therefore, the method of carrying alliance chain certificate at the authentication node is not applicable for drones, such as literature [7–9]. Traditional cross-domain authentication schemes represented by the literature [4] do not solve the problem of mutual trust between control stations, and they are also not applicable to the cross-domain certification of UAV. Blockchain technology can create a trust environment [13] and effectively address trust issues in the cross-domain process. Combining the two methods is a good choice. Alliance chain technology is used between the control stations to achieve mutual trust, and the traditional methods of authentication between the UAV and the control stations can achieve the trust between the control stations, and there is no need to store the expensive data such as digital certificates on the UAV.

1.3. Contributions. In order to achieve the trust between the control stations and ensure the efficient cross-domain authentication of the UAV, this paper designs a cross-domain authentication scheme based on the alliance chain technology. The main work is as follows:

(1) A cross-domain authentication scheme for UAV is designed based on alliance chain technology. The scheme adopts alliance chain technology between control stations to achieve mutual trust environment and the identity authentication of secret information between drones and control stations.

(2) Security analysis was performed based on the Dolev–Yao threat model to demonstrate the security of this cross-domain authentication scheme.

(3) In order to prove the high authentication efficiency of this scheme, the cross-domain authentication scheme proposed by literature [4] is compared through simulation experiments, and the authentication efficiency of the proposed authentication scheme is improved compared with the UAV cross-domain authentication scheme represented by literature [4].
2. Design of the UAV Cross-Domain Authentication Scheme Based on Alliance Chain

Drawing on the cross-domain authentication method of the Internet of Things, compared with the forwarding and authentication of the UAV authentication information in the authentication process, the secret information such as identification information can be directly distributed in the initialization stage. This can both reduce one round of communication and improve the robustness of the scheme. Based on this idea, this paper designs a cross-domain UAV authentication scheme based on the alliance chain technology. The cross-domain authentication scheme based on alliance chain technology designed in this paper can complete the transmission and endorsement of identity authentication information in the initialization stage, reduce the number of communication rounds, and improve the cross-domain authentication efficiency of UAV on the premise of ensuring the security of cross-domain authentication.

2.1. Parameter Representation. In this paper, the parameters and their corresponding meanings are shown in Table 2.

2.2. Initialization. The initialization stage of this scheme mainly includes the initialization of the alliance chain between the control stations and the UAV.

2.2.1. Alliance Chain Initialization. After the CA authentication of each control station, the nodes peer0.org1, peer0.org2, peer0.org3, and peer0.org4 corresponding to the UAV control stations in different domains add the same channels corresponding to the control station requiring cross-domain authentication, such as peer0.org1 and peer0.org2 accession channel channel1 and peer0.org2 and peer0.org4 accession channel channel2. This paper illustrates the examples of peer0.org1 and channel channel1 added by peer0.org3 in Figure 1. Call the official supplied Smart contract in the channel, and the corresponding chain code is packaged and installed.

2.2.2. Initialization of the UAV Identity Information. The initialization of UAV identity information in this scheme is divided into two parts: the upper link of identity authentication and related information in the registration domain.

Identity authentication in the registration domain selects the identity authentication scheme based on the ECC algorithm. `reg station` selects \( G = (x, y) \) as the basis of the \( E \). Generate the random numbers \( \text{rand}_0, \text{rand}_1, \text{rand}_2, \ldots, \text{rand}_n \in [1, n - 1] \) as the private key, and calculate \( P_0 = (x_0, y_0) = [d_0](x, y), P_1 = (x_1, y_1) = [d_1](x, y) \cdots \) as the corresponding public key.

Subsequently, `reg station` generates six random numbers \( \text{RAND}_0 \) for each pair of public-private key as its \( \text{in} \) in the key table, selects \([P_0, d_0]\) as the public-private key of `reg station`, selects the public-private key in the remaining public-private key pairs, and passes the parameters \( \{\text{RAND}, n, E, G, H, (.), P_0, \text{pku}, \text{sku}\} \) to the `reg station` and other UAVs into the network authentication and two-way identity authentication and obtain generation.

The upper chain of the relevant information is mainly implemented by using the way of calling the chain code, and the `reg station` in the corresponding channel call chaincode will give \( ID_n, \text{pku} \) to the `in`. The specific steps are shown in Figure 1.

The reg station creates the proposal as a transaction and signs the signed proposal generation.

The signed proposal is sent to the peer0.org1 node for endorsement processing, which returns the proposal response message after successfully successful chain code call transaction.

Create a signed transaction `signedTX` based on the message returned by the peer0.org1 node.

Transaction information is sent to the order node for network sorting and broadcasting to all the peer nodes of the channel (such as the peer0.org1 and peer0.org3 nodes listed in this article) for confirmation.

2.3. Cross-Domain Authentication. The main steps of the cross-domain authentication process are shown in Figure 2.

UAV transfers to `acc station` \( \{T_u, ID_n\} \).

`acc station` verifies the parameter \( T_u \), if \( T_c - T_u < \Delta t \) and then queries the information according to the \( \text{in} \) in \( ID_n \) corresponding chain code on the alliance chain in.

If `acc station` successfully obtains \( \text{pku} || ID_n \) from the chain code, and if it is the same, the authentication is successful.

`acc station` generates \( ID_{n+1} \) and updates the chain code on the corresponding channel by using \( \text{pku} || ID_{n+1} \), then \( ID_{n+1} \) calculation is

\[
ID_{n+1} = \text{in} \cdot \text{dH}(ID_n, IV),
\]

`acc station` uses \( \text{pku} \) building secure communication channels with UAV.

After the UAV has successfully communicated with the `acc station`, the UAV updates the local machine \( ID_n \) to generate \( ID_{n+1} \) in the same calculation way.

3. Safety Analysis

Data transmitted over wireless channels is vulnerable to theft [14, 15], so UAV communication networks using wireless communications face serious security threats. The Dolev–Yao model [16] is an analytical model widely recognized by the industry, and this chapter will demonstrate the security for cross-domain authentication schemes based on this model (because the security of alliance chain technology has been widely recognized by the industry, and this default control stations are in a secure communication environment).

3.1. Antireplay Attack Analysis. The current time stamp is enclosed in the message structure transmitted between the
The control station and the UAV can test the time stamp, that is, whether the inequality $T_c - T_u < \Delta t$ is satisfied. Because the attacker consumes more time to forward the message, they can judge whether a replay attack.

3.2. Antimiddleman Attack. During the authentication process, after each verification process, it needs to be updated, namely, $ID_{n+1} = \text{in}dH(\text{ID}_n, IV)$. Therefore, in the case of intermediate interception, the same can only complete a single authentication and cannot be used for the second authentication and can guarantee the security of the channel.

3.3. Forward Safety and Backward Safety of $ID_n$. The identity information $ID_n$ of this scheme has forward security and backward security, $ID_{n+1} = \text{in}dH(\text{ID}_n, IV)$. The unidirectional of SM3 algorithm ensures that the attacker cannot infer $ID_n$ through $ID_{n+1}$ in polynomial time. Since IV is a parameter that the attacker cannot obtain, the attacker can also not get $ID_{n+1}$ through $ID_n$.

4. Experimental Design and Analysis

After the initialization of UAV, acc station, and reg station, the alliance chain-based cross-domain authentication scheme and the traditional temporary cross-domain authentication scheme were conducted, respectively.

4.1. Experimental Environment. The experimental environment is mainly divided into UAV environment and acc station environment and communication environment. The UAV is configured as Intel (R) Core (TM) i7-7700HQ CPU @ 2.80 GHz with 3 GB memory, Linux version 4.15.0-171-generic operating system with the /light control module and communication module. Among them, the flight control system module adopts the four-rotor UAV simulation model built based on the gazebo platform, and the communication module is built based on the PyCharm.
2021.1.1 x64 platform, using the python 3.9 interpreter. The acc station is specifically configured as Intel (R) Core (TM) i7-7700HQ CPU @ 2.80 GHz 2.81 GHz, 4 GB of memory, Linux version 5.13.0–35-generic operating system, internal alliance chain peer0.org1, and the communication module. Alliance chain peer0.org1 is implemented in hyperledger fabric 2.2 version, and the communication module is built based on the PyCharm 2021.1.1 x64 platform, using the python3.9 interpreter. Since the mainstream communication chip adopts 2.4 GHz band [17], the communication environment adopts 2.4 GHz band communication, which is realized through the socket () function used in the UAV communication module such as DJI tello.

The comparison scheme of simulation experiments is the temporary cross-domain authentication scheme used in literature [4]. Since the relevant experiments were not conducted in the original literature, the comparison scheme is run in the experimental environment of this paper. The steps are shown in Figure 3.

4.2. Experimental Content and Results. The initialization of the drone and the alliance chain needs to be completed first before conducting all the tests. The standby screenshot of the UAV completed after initialization is shown in Figure 4. The screenshot of the alliance chain after its initialization is shown in Figure 5.

4.2.1. Certification Time Test Comparison. The operation UAV communication module initiates cross-domain identity authentication to the acc station. After the authentication reception, the operation screenshot after the UAV model receives the take-off command, as shown in Figure 6:

The two schemes are run ten times each, and the output time of the UAV communication module is recorded. The results are shown in Figure 7.
The main difference between the scheme and the document [4] process is that the scheme does not require data transmission between control stations. Since reg station uploads and endorses the UAV information in the process of building the chain code between reg station and acc station, acc station can query the UAV information on the chain code.

Figure 5: Alliance chain peer0.org2 initialization screenshot.

Figure 6: Screenshot of the drone’s operation.

Figure 7: Certification time comparison.
locally. In contrast, the scheme adopted by document [4] needs to transmit information to reg station to judge the process. The information transmission mode between the control stations is also wifi communication. In the case of relay without using the satellite system, the wireless signal transmission in the atmosphere can be negligible, but the signal decoding and coding process of the control station consumes more time. If the control station environment is more complex or remote, we need to borrow the satellite system for relay transmission, transmission distance, and satellite signal processing between the control station data transmission time cost which will be greatly increased; in this case, using the scheme proposed in this paper, the certification efficiency will be far more than expected in this paper.

4.2.2. Communication Overhead Comparison. This paper mainly compares the traffic in the cross-domain authentication stage after the initialization of the UAV and other equipment. To ensure the validity of experimental comparison, IDn of both experiments uses the same string, time stamp length T, IDn length ID, control station return command c, and reg station return to acc station result r, and the results are shown in Table 3.

| Communication between the two sides | Our scheme | Controlled experiment |
|-----------------------------------|------------|-----------------------|
| UAV and acc station               | T + ID + c | T + ID + c            |
| Acc station and reg station       | 0          | ID + r                |
| Total communication volume        | T + ID + c | T + ID + 2 + c + r    |

It can be seen from the table that the scheme communication overhead adopted in this paper can reduce the communication overhead between control stations, and the IDn can still be verified when the acc station and reg station are interrupted to complete cross-domain authentication.

5. Conclusion

In this paper, we propose a UAV cross-domain authentication scheme based on alliance chain technology. Under the premise of completing the security analysis of the scheme, the simulation experiments prove that the scheme has the advantages of small communication cost and high authentication efficiency, which meets the expectations of the cross-domain authentication scheme. However, due to the small number of UAVs, the large-scale UAV communication network cannot be simulated, and the complex network electromagnetic environment cannot be simulated due to the limitations of computer simulation experiments. The later work is mainly to study the multithreaded processing process of multiple drones for cross-domain authentication, and the simulation aspects of the complex environment is based on the artificial intelligence technology.

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 conflicts of interest.

Authors’ Contributions

Tao Xia and Jun He contributed equally to this work.

References

[1] Yu-J. Chen and Li-C. Wang, “Privacy protection for internet of drones: a network coding approach,” IEEE Internet of Things Journal, vol. 6, no. 2, 2019.
[2] S. Aggarwal and N. Kumar, “Path planning techniques for unmanned aerial vehicles: a review, solutions, and challenges,” Computer Communications, vol. 149, no. C, 2020.
[3] S. H. Sa and P. Corke, “Outdoor flight testing of a pole inspection uav incorporating highspeed vision,” in Field and Service Robotics, pp. 107–121, Springer, 2015.
[4] Yu Pan, Research and Implementation of Uav Communication Security Technology, Xidian University, China, 2018.
[5] W. Jiang, Research on Cross-Domain Authentication and Path Selection Scheme in Wireless Networks, Lanzhou University of Technology, China, 2011.
[6] W. Xin, X. Wang, Z. Yu, S. Guo, and X. Qiu, “Cross-domain authentication of the Internet of Things based on the alliance chain,” Journal of Software, vol. 32, no. 08, pp. 2613–2628, 2021.
[7] Z. Zhou, L. Li, and Z. Li, “Efficient cross-domain authentication scheme based on blockchain technology,” Computer Applications, vol. 38, no. 2, pp. 316–320, 2018.
[8] X. Ma, W. Ma, and X. Liu, “Cross-domain authentication scheme based on blockchain technology,” Journal of Electronics, vol. 46, no. 11, pp. 2571–2579, 2018.
[9] Z. Guan, Y. Chen, D. Li, W. Liu, and D. Yu, “A blockchain-based cross-domain authentication scheme for the Internet of Vehicles,” Cyberspace Security, vol. 11, no. 09, pp. 62–69, 2020.
[10] H. Thomas and P. Alex, “Verifiable anonymous identities and access control in permissioned blockchains,” 2016, https://arxiv.org/abs/1903.04584.
[11] M. Wazid, A. K. Das, and J.-H. Lee, “Authentication protocols for the internet of drones: taxonomy, analysis and future directions,” Journal of Ambient Intelligence and Humanized Computing, vol. 987, p. 234, 2018 (prepublish).
[12] N. Mahdi, A. Haleh, and S. K. Hafizul, “A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance,” Journal of Systems Architecture, pp. 12–34, 2020, (prepublish).
[13] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of Things,” IEEE Access, vol. 4, 2016.
[14] A. T. Fadi, E. Y. Kirsal, E. Enver, X. Nguyen Huan, 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, p. 374, 2017.
[15] Y. Kirsal 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.

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

[17] Z. Yan, *Research on Anti-deception and Communication Encryption Technology of Quadrotor UAV*, University of Electronic Science and Technology, China, 2017.