EURASIP Journal on Wireless Communications and Networking

RESEARCH

Open Access

ToAM: a task-oriented authentication model for UAVs based on blockchain

Aiguo Chen[1,2], Kun Peng[1,2], Zexin Sha[1,2], Xincen Zhou[1,2], Zhen Yang[3] and Guoming Lu[1,2*]

*Correspondence:
lugm@uestc.edu.cn
[1] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
Full list of author information is available at the end of the article

Abstract
The pervasive cooperation of a group of UAVs has attracted increasing attention due to the reduced cost and widespread availability. When working in an untrusted or adversarial environment, the mutual authentication of UAVs in the cooperative process is imperative. However, there are some major challenges, including changes in the network environment before and during task performing, and the weak connection network state faced by UAVs. Therefore, a novel task-oriented authentication model for UAVs based on blockchain (ToAM) is proposed, which divides UAVs authentication into group building authentication and intra-group authentication with a two-stage authentication framework. And two lightweight authentication protocols are presented, respectively, corresponding to two stages. Finally, analyses demonstrate that our model realizes secure and lightweight authentication function for the whole process of UAVs requisition and task performing.

Keywords: Authentication, Blockchain, Unmanned aerial vehicles, Smart contract

1 Introduction

Unmanned aerial vehicles (UAVs), also known as drones, are one type of aircraft which operate without a human pilot on board [1]. With the development of artificial intelligence and other technologies, like distributed machine learning and UAV-based edge computing [2, 3], a group of UAVs can cooperatively accomplish more complex tasks, such as search and rescue, fire-fighting, reconnaissance, and surveillance [4, 5]. Typically, the UAV group works in a task-oriented way. This means that multiple UAVs will be requisitioned to build a group and accomplish the task cooperatively when a task comes [6, 7]. During the group building and task performing progress, UAVs will have a lot of interaction with each other; the authentications between UAVs are particularly important when they work in an untrusted or adversarial environment.

However, UAVs in a group will face different network environments in the group building and task performing process. Because, network-connected UAVs have a two-layer network architecture, including a ground infrastructure network and a UAV ad hoc network [8]. In the UAV group building process, these UAVs are able to communicate efficiently with each other and ground station using UAV-to-infrastructure communication. And in the process of task performing, UAVs in the group have to fly to a given location, where UAVs can communicate efficiently with each other using UAV-to-UAV communication in an ad hoc network. But, the connection between UAVs and the ground infrastructure network becomes unreliable, which is called a weak connection state in this paper. These changes of network connection state bring great technical challenges to the design of authentication model for UAVs.

Currently, there have been some studies related to UAV authentication, which is considered to be a major challenge in the area of securing UAV group applications in the future. Existing authentication models for UAVs mainly focus on how to enhance security and reduce computing costs. Consequently, certificates and asymmetric cryptography methods have been widely used [9]. However, the computing cost is too huge. To deal with the resource limitation of UAVs, various lightweight schemes have been proposed [10, 11]. In addition, the blockchain technique, due to its decentralization and information disclosure, was proposed as a decentralized and distributed approach to guarantee security requirements and motivate the development of the IoT [12–14]. It keeps emerging to benefit from more reliable and lightweight authentication, and stores the identity information of the device securely in the block to facilitate the query during authentication to solve the problem of single-point failure caused by storage identity information in a centralized server [15–20]. In [15], it skillfully transforms the computation needed for authentication into blockchain data retrieval, which reduces the computation cost of device authentication to the domain server.

However, existing solutions are not able to solve the authentication problem of UAVs caused by the weak connection state during the task. In the above schemes, the identity information of UAVs is usually stored in the ground facilities. A UAV needs to get this identity information to complete authentication progress. However, in the weak connection state, UAV-to-infrastructure communication will become unreliable. As a result, the UAV cannot obtain identity information. Meanwhile, UAVs can only communicate with each other by using UAV-to-UAV communication in the ad hoc network, which means UAVs have to complete the identity authentication process in this ad hoc network. Hence, all the computing pressure is on the UAV group. But due to the limited hardware, a UAV cannot support a large number of calculations. Therefore, it brings great challenges to the authentication scheme design.

To adapt to the dynamic network environments and weak connection state faced by UAVs, a task-oriented authentication model based on blockchain is proposed in this paper. It divides UAVs authentication into group building authentication and intra-group authentication with a two-stage authentication framework. While group building, we present a lightweight and cross-domain authentication protocol based on the blockchain, which supports the requisition of cross-domain UAVs and building task groups securely. Then while the task performing, a pre-shared key authentication protocol with a chord ring is used, which realizes efficient and secure authentication in the UAV group under a weak network connection state.

The rest of the paper is organized as follows. Section 2 reviews the existing related works about the application of blockchain and authentication mechanisms of UAV. Section 3 gives the overview and design details of our proposed solution. Section 4 discusses the security performance and evaluation of our authentication mechanism. Finally, Sect. 5 concludes the paper.

2 Related works

Traditionally, there have been some researches on UAVs authentication. In [21], Sun et al. proposed an efficient and energy-saving distributed network architecture based on clustering stratification, and designed a double-authentication watermarking strategy to solve the information security problem of unmanned aerial vehicle ad hoc network communication. To achieve higher efficiency, a provably secure aggregate authentication scheme for UAVs cluster networks is proposed in [22], which secure that all kinds of data from different UAVs can be checked by batch instead of "one-by-one."

The above authentication mechanisms for UAVs mainly solve the security of communication data, and the key point of these innovations lies in the security and resource limitation, which is also the focus of existing UAV identity authentication researches. In [23], a traceable and privacy-preserving authentication scheme based on ECC for UAVs was proposed, and compared with the traditional signature mechanism, the application of ECC technology makes the authentication process more lightweight [24]. In [25], a framework called SENTINEL (Secure and Efficient authentication for unmanned aerial vehicles) under the Internet of Drones infrastructure is proposed. By using the flight session key during task performing progress, SENTINEL minimizes the computational and traffic overheads caused by certificate exchanges and asymmetric cryptography computations that are typically required for authentication protocols. However, SENTINEL uses a session key based on symmetric cryptography, and stores the secret key information in a central database, which reduces the security of the system.

To solve the contradiction between security and performance, in [15], it skillfully transforms the computation needed for authentication into blockchain data retrieval, which reduces the computation cost of device authentication to the domain server. In [26], Bera et al. proposed a novel access control scheme for unauthorized UAV detection and mitigation in an Internet of Drones (IOD) environment, called ACSUD-IOD, also with the help of the blockchain-based solution incorporated in ACSUD-IOD, the transactional data having both the normal secure data from a drone (UAV) to the Ground Station Server and the abnormal (suspected) data. And it is more effective and robust as compared to existing schemes. The latest research shows that blockchain can be used to improve security and reduce the complexity of authentication [13]. Meanwhile, blockchain-based authentication can effectively solve the problem of efficient authentication when requisitioning UAVs across domains.

However, existing UAV authentication mechanisms do not consider the changes in the network environment before and during the task performing. All of these schemes save the identity information of UAVs in ground facilities, which cannot solve the problem caused by the weak connection in the process of task performing. To solve the authentication in the cooperative accomplish task of UAV group. In this paper, we creatively propose a dynamic and task-oriented authentication model based on blockchain.

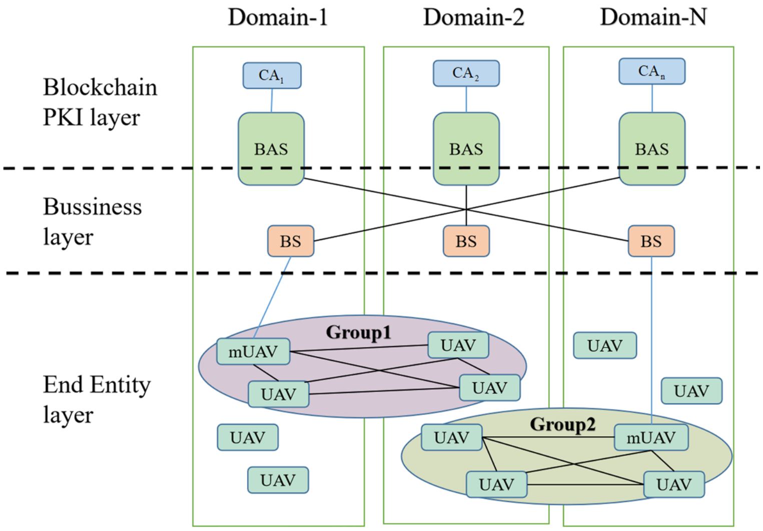


Fig. 1 ToAM system model. The ToAM system model includes three layers and several domains. UAV in different domains can dynamically build a drone group with the help of BS

3 Methods

3.1 System model

In our task-oriented authentication model, all entities serve as nodes in a blockchain in the ground infrastructure network environment, and the entire system is structured into three layers and multiple domains. The system model is shown in Fig. 1.

In the Blockchain PKI layer, there is a CA (Certificate Authority) to manage the identity information of the nodes in each domain. These top-level CAs jointly maintain a blockchain network for publishing, storing, and maintaining identity information.

The business processing layer contains BAS (Blockchain Authentication Server) and BS (Business Server).

- BAS: As an entity in the blockchain network, it plays the role of the master node. It can store the certificate information published by CA in the blockchain network or assist UAVs in querying the certificate information of other entities. It can be understood as a blockchain agent of UAV.
- BS: As an entity in the blockchain network, it is responsible for publishing task information to UAV and can maintain task information in the blockchain.

Both of them have the blockchain network accessing function. Together with the nodes in other domains, they build a blockchain network for publishing and storing information such as identities and tasks.

In the End Entity layer, there are multiple UAVs in each domain. When a UAV accepts a task, it will automatically be organized and scheduled according to the task requirement and cooperate with others to complete the task.

When BS publishes a task, it will filter out a UAV as a master UAV (mUAV) in the domain where the task is initiated. The principle of mUAV screening is based on the roles of different UAVs and the adaptability of their computing power. To avoid the problem of single-point failure of mUAV in the process of task performing, one or multiple standby ones can be selected simultaneously.

Then, the mUAV will work as the founder of a task-oriented UAV Group. It communicates with the alternative UAVs to build the group, completes the identity authentication, and generates and distributes a new identity for each UAV in the group and the pre-shared key of this group.

Before the UAVs of this group perform a task, they will transform from ground infrastructure network to ad hoc wireless network, which will cause a weak connection state. Therefore, this pre-shared key is used to authenticate with each other for the group of UAVs. Compared with the authentication based on blockchain in the process of group building, this constitutes the two-stage authentication framework proposed in this paper. The details are described from Sects. 3.3 to 3.6.

3.2 Presumption and definition

Mainly focusing on the progress of authentication of UAVs, we put forward the following presumptions to reduce the interference caused by unrelated factors and build the basic functions that UAVs must have.

(1) All UAVs have been registered with CA in the domain and have been registered in the blockchain network.
(2) The UAV that accepts the task will strictly implement the task requirements and will not generate false task intelligence.
(3) Physical attacks are not considered, and UAVs use TPM (trusted platform module) to ensure that important local data will not be violently read by attackers.

The symbols used in this paper are defined in Table 1.

We use GrpID to identify the existence of a UAV group, which is public to the outside world to make others perceive the existence of UAV groups. In each group, a pre-shared key SK is generated by its mUAV. When a UAV is authenticated and joined the group, mUAV will send the SK to it. Only these certified UAVs can use this SK to communicate with each

Table 1 Definition of symbols

Symbols	Definition
GrpID	The group ID of a UAV group
ID_x	The dynamic identity of UAV x
Ticket	Task tickets issued by mUAV for other UAVs
P_a, P_b	UAV a\b's public key
S_a, S_b	UAV a\b's private key
SK	Pre-shared key in a group
$E_K(\cdot)$	Encryption using a key K
$H(\cdot)$	Hash function
$Sign(\cdot)$	Signature
TS	Time stamp
$E(\cdot)$	Using secret channel to communicate with smart contract

other in the group. The pre-shared key SK in the group will ensure the security of the communication process and the legitimacy of the UAV identity. Meanwhile, each UAV obtains a specific ID_x to distinguish from each other.

$\mathrm{E}_{\mathrm{K}}(\cdot)$ represents an encryption operation. For symmetric encryption, the Advanced Encryption Standard (AES) algorithm is used. For asymmetric encryption, elliptic curve cryptography (ECC) is used, which is more suitable for constrained environments.

In addition, since the hash function and signature function involve the operation of blockchain smart contracts, it is necessary to use the blockchain signature function ECDHE and the blockchain standard hash function Keccak3. The cross-domain authentication mechanism exploits ECDHE, which is based on the elliptic curve discrete logarithm problem (ECDLP). ECDLP has been proved unsolvable by the polynomial-time algorithm now. In addition, all the information required for identity authentication, such as the public key of UAV, is stored on the blockchain, which connects all domains and provides a tamper-resistant record service. Besides, the privacy security of UAV's identity and data integrity of transactions and messages is more dependent on the hash function. The Keccak3 hash function has been used in this paper, which has never been compromised yet.

3.3 Blockchain-based authentication for group building

When a task comes, the system will select the most reliable UAV as the mUAV node. Then, the mUAV that receives the task from BS will start to build a task-oriented group and ensure the security of joining UAVs through security authentication protocols based on blockchain. We assumed that the mUAV here is honest and reliable. The specific process is shown in Fig. 2.

The protocol steps are as follows:

Step (0): When mUAV receives a task, it generates a pre-shared key SK for this group, and Tickets for each UAV selected as follows:

$$\mathrm{Ticket}\_to\_A = \{GrpID|ID_A|\mathrm{sign}(GrpID, ID_A)\}$$

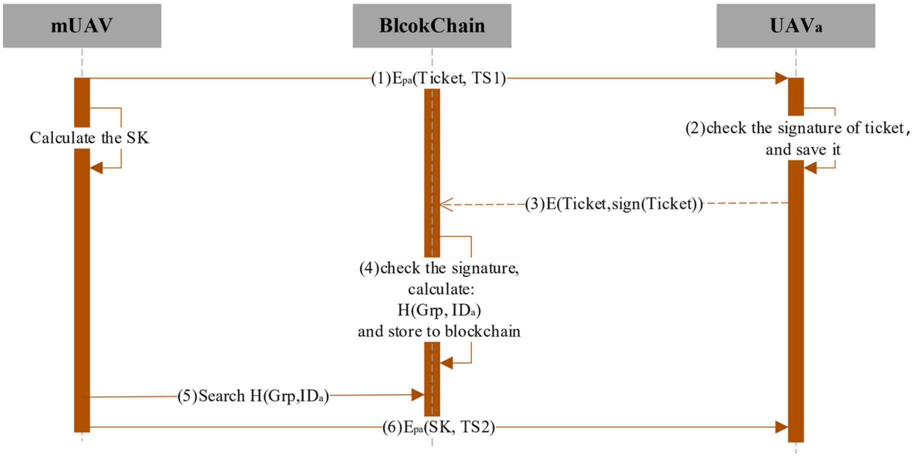


Fig. 2 Blockchain-based authentication for group building. This figure shows the process of authentication for group building and initialization

where *GrpID* represents the unique identifier of the UAV group built by mUAV, which is public. ID_A is a private identification generated by mUAV for UAV_A. *Sign(GrpID,*ID_A*)* is a signature, which is signed by mUAV's private key.

Step (1): After finding the public key of UAV_a through the blockchain, mUAV uses this public key to encrypt and sends {Ticket, TS1} to UAV_a.

$$\mathrm{mUAV} \xrightarrow{E_{\mathrm{pa}}\{\mathrm{Ticket}, TS1\}} UAV_a.$$

Step (2): After UAV_a decrypts the message with its private key, it judges the time stamp TS1, then obtains the public key of mUAV through the blockchain, checks the signature in the ticket, and after confirming the authenticity of the ticket, saves GrpID and ID_a.

Steps (3)–(4): UAV_a calls the smart contract, uploads {ticket, sign(ticket)}, then the smart contract uses the UAV_a's public key to verify the signature, and then uses the mUAV's public key to verify the signature in the ticket. After confirming their correctness, the smart contract writes H(GrpID, ID_a) into the blockchain.

Step (5): mUAV calls the smart contract to search the existence of H(GrpID, ID_a).

Step (6): If the search result in step 5 is existing, mUAV will send encrypted messages including the pre-shared key SK and a time stamp TS2 to UAV_a using the public key of UAV_a.

$$\mathrm{mUAV} \xrightarrow{E_{pa}\{SK, TS2\}} UAV_a.$$

After that, UAV_a decrypts and checks the time stamp TS2 to obtain the pre-shared key SK. So far UAV_a has successfully joined the group. At this time, all UAVs confirm to join the group will have the same GrpID and their confidential IDs, as shown in Fig. 3.

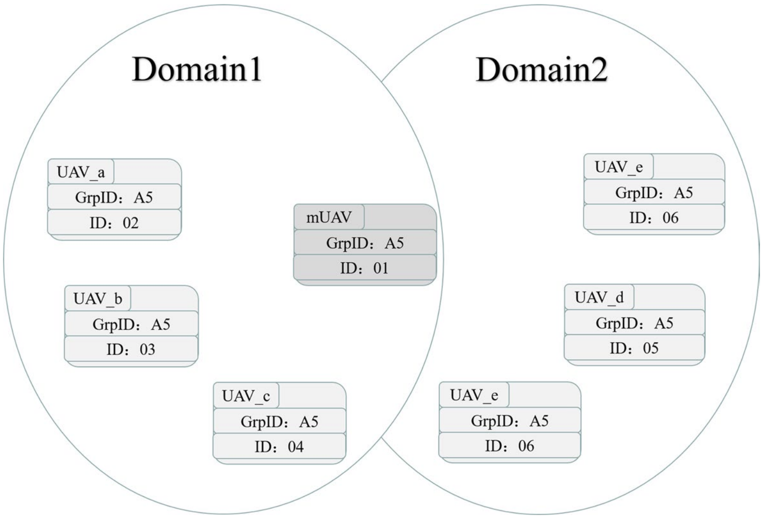


Fig. 3 An instance of a group containing UAVs from two domains. This figure shows how UAVs in different domains build groups

3.4 Identity information intra-group management method

During the task performing in the UAV group, it will inevitably encounter extreme conditions such as an unstable or unavailable network. In this weak connection state, it is important to ensure the reliability and efficiency of identity authentication in the group. In this section, an identity information intra-group authentication method based on Chord protocol is proposed. The Chord is a protocol and algorithm for a peer-to-peer distributed hash table, which is one of the first, simplest, and most popular distributed protocols and can be used as a backbone of the discovery and control services of an IoT system [27, 28]. Based on DHT and consistent hash, we have realized offline storage and fast access of UAV identity information.

3.4.1 Redundant storage of identity information

Distributed storage can ensure the lightweight of the UAV, and a consistent hash algorithm can ensure the efficiency of resource location. We use the Keccak3 as the hash function.

The ID of identity information and the UAV's address are mapped to the ring by SHA-1, and authentication information is stored in both two successor nodes in a clockwise direction. As shown in Fig. 4, the O59 resource is stored on the N1 and N8 nodes, and the O4 resource is stored on the N8 and N17 nodes. The O19 and O25 resources are stored on the N34 and N52 nodes.

From Fig. 4, it can be seen that when a new UAV node adds to the group, data migration will only occur between three UAVs according to the clockwise storage rule. For example, when a new UAV node N23 is added to the group, only O19 and O10 resources need to be migrated from N52 and N34 to N23.

3.4.2 Rapid location of identity information

To improve the efficiency of identity information access, each node can quickly access resources by maintaining a Finger table. The i-th item of the table is the resource which hash value is this UAV node plus $2^{(i-1)}$ and it's location. As shown in Fig. 5, take a hash space of 2^6 as an example.

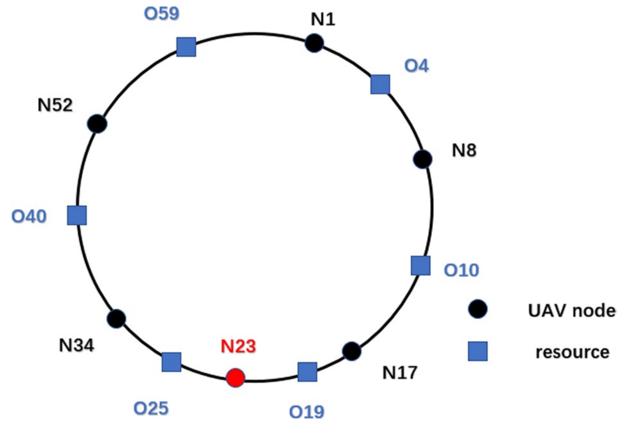
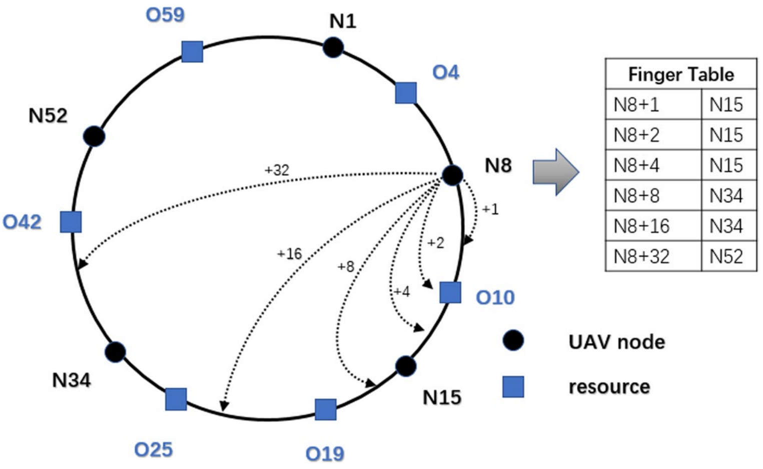


Fig. 4 Chord ring of identity information. We store the identity information in a chord ring



Finger Table	
N8+1	N15
N8+2	N15
N8+4	N15
N8+8	N34
N8+16	N34
N8+32	N52

Fig. 5 Rapid resource location with Finger table. Rapid resource location can be seen in this figure

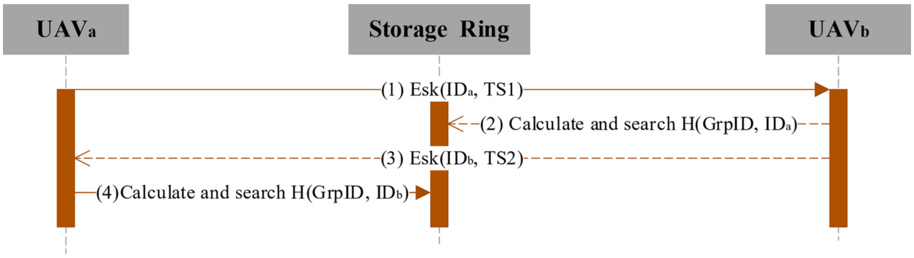

UAVa
Storage Ring
UAVb
(1) Esk(IDa, TS1)
(2) Calculate and search H(GrpID, IDa)
(3) Esk(IDb, TS2)
(4)Calculate and search H(GrpID, IDb)

Fig. 6 Intra-group authentication. This figure shows the authentication protocol of UAVs within a group

When a UAV node access a resource, it first judges whether its successor node holds the resource. If not, search from the last item in the Finger table. When found the hash value of the UAV node is less than the resource node, jump to the UAV node for a new search.

For example, the UAV (N8) needs to access the O42 resource. First, look up the own node (N8) and successor node (N15). They do not hold the resource, so the UAV(N8) reverse lookup Finger table. The N34 is the first UAV node with a hash value less than the resource. So, it jumps to the N34 node for a new search. The successor node of the N34 node is N52, which meets the condition of $42 \in (34{,}52]$, so the O42 resource is located in the N52 UAV nodes. When an uncontrollable factor causes the N52 UAV node to lose connection, the next UAV node N1 can be queried sequentially to read the redundant resources.

3.5 Intra-group authentication

In the process of task performing, UAVs will cooperate to accomplish the task. The authentication process of UAV within a group is shown in Fig. 6:

The protocol steps are as follows:

Step (1): UAV_a encrypts its ID_a and time stamp TS1 through the pre-shared key *SK* and sends it to UAV_b.

$$\mathrm{UAV}_a \xrightarrow{E_{\mathrm{sk}}\{\mathrm{ID}_a, TS1\}} \mathrm{UAV}_b.$$

Step (2): UAV_b decrypts the message and verifies the time stamp TS1, calculates Hash (GrpID, ID_a), and then uses the chord ring to compare and confirmed the existence of UAV_a.

Step (3): After UAV_b successfully confirmed the existence of UAV_a, it encrypts {ID_b, TS2} and sends it to UAV_a.

$$\mathrm{UAV}_b \xrightarrow{E_{\mathrm{sk}}\{\mathrm{ID}_b, \mathrm{TS2}\}} \mathrm{UAV}_a.$$

Step (4): After UAV_a decrypts the message, it verifies the time stamp TS2 and calculates Hash(GrpID, ID_b), then searches in chord ring and verifies the results.

If the result of the verification is correct, then enter the communication phase. UAV_a and UAV_b save each other's ID to the local cache, which is convenient for quick verification next time.

This authentication protocol has strong robustness. By using the chord ring, we can store the UAV information in the UAV group in a distributed way, avoiding the single-point failure problem.

4 Results and discussion

In this section, the authentication model will be analyzed from security and performance aspects.

4.1 Security analysis

Our task-oriented authentication model for UAVs integrates blockchain technology to improve flexibility and security. In addition, the chord ring method is proposed to maintain identity information, which is used to support that the model can work in a weak connection state. The detailed security assessment is given below.

When a task is initiated, a task-oriented trusted UAV group is built. The authentication between the UAV and the mUAV is executed by calling the blockchain smart contract. The smart contract automatically confirms the authenticity of the identity and writes the confirmation result into the block. All network nodes can confirm whether the identity authentication is successful by querying the blockchain. On the one hand, the blockchain has played the role of a certification authority, completing trusted and secure identity authentication in a decentralized way. On the other hand, all IDs of UAVs are stored in the form of hash values on the blockchain, and UAVs also use the ID assigned by the mUAV to authenticate and communicate with each other in the UAV group. If the attacker reads the authentication information stored on the chain by special means, but it can only get the group ID and the hash value of UAVs. Finally, each group only performs a task once. When the task is over, the group is automatically dissolved. All authenticated devices, tickets, tokens, and other identity authentication certificates will all expire. This achieves forward secrecy.

When the UAV group performs its task, all UAVs communicate in the trusted group, and the communications are kept secret by the pre-shared key generated when the group building. In intra-group authentication, the identity authentication data is stored in the UAV group by chord ring. It relies on the correctness of subsequent nodes to ensure the correctness of the ring. To avoid the single-point failure, each UAV contains a successor node list, and if a successor node fails, it will try other successor nodes in the list in turn. It can be promised that the time to find a successor is O(log N) in a network with the failure node of 1/2.

ToAM also has other security guarantees. On the one hand, all authentication messages are bound with a time stamp to prevent replay attacks. On the other hand, all authentications information and related authentications operations are stored in the security hardware module (TPM), ensuring that even if the UAV crashes or is captured, it will not affect the identity and communication security of other UAVs.

4.2 Performance analysis

In this subsection, we analyze our ToAM in terms of computation and communication costs by comparing it with a decentralized multi-domain authentication method and a UAV authentication method, namely BASA [9] and SENTINEL [25]. We calculate the computation and communication costs within one whole task, which includes both cross-domain authentication for group building and intra-group authentication.

4.2.1 Computation overhead

About computation overhead, it will be evaluated through theoretical analysis on most time-consuming operations. This means that complex operations are considered and simple ones are ignored. The simple operations, such as hash operation, integer addition, and multiplication cost little time in our computation cost, so they are not considered here. The symbols are listed as follows:

- C_s, the cost of performing a symmetric operation (encryption or decryption with a symmetric key).
- C_{sig}, the cost for performing an asymmetric private operation (plaintext decryption or signature using a private key).
- C_{ver}, the cost for performing an asymmetric public operation (plaintext encryption or signature verification using a public key).
- *CECDH*, the cost of executing an elliptic curve Diffie–Hellman (ECDH) operation.
- *N*, the number of UAVs joining in the task.

Table 2 Computation overhead

Protocol		UAV	mUAV	Server
ToAM	Group building	$2*C_s + C_{ver} + C_{sign}$	$(C_s + C_{sign}) * N$	$(C_s + CECDH + C_{ver} * 2) * N$
	Intra-group authentication	$2 * C_s * N$		\
BASA		$(2 * C_s + C_{ver} + C_{sign}) * N$		$(2 * C_s + C_{ver} + C_{sign}) * N$
SENTINEL	Mutual authentication and key agreement	$C_s + 2 * C_{ver} * N$		$2 *(C_s + C_{sign} + C_{ver}) * N$
	UAVs authentication	$C_s * N$		$C_s * N$

If ToAM and BASA use the same encryption algorithms and parameters, the computation overhead is compared as Table 2.

As Table 2 shows, compared with BASA and SENTINEL, ToAM has less average computation cost and higher verification efficiency, which helps to solve the problem of resource limitations. In addition, more computation cost is on the server, which is helpful to the computation limitation of UAV and mUAV.

4.2.2 Communication overhead

Because the length of the information about the task will change with the task, we only count the length of authentication-related messages. First, the mUAV calls the smart contract about 8 bytes and accepts UAV public key about 654 bytes. When a UAV group is built, the mUAV will send a message to each UAV, including the ticket with related signatures and a time stamp. Then, the UAV sends a signature with a private key and ticket to the blockchain. After that, the mUAV calls the smart contract to check whether the authentication is successful, which is about 4 + 20 bytes. Finally, the mUAV sends a 16-byte key and a 4-byte time stamp to the UAV, which are encrypted with the UAV's public key.

When the group is built, UAVs in the group need to perform mutual authentication first in the cooperative process of task execution. The initiator UAV first sends its 128-byte ID to prove its identity, then the receiver calculates and searches 20-byte hash value in the chord ring. If there are N UAVs in a group, $\mathrm{Log}_2 N + 1$ communications are required for identity verification. It's $\left(\mathrm{Log}_2 N + 1\right) * 16$ bytes in total.

Assuming there are N UAVs in a group, the number of all communication bytes is as Table 3.

As Table 3 shows, communication cost in group building is 886 bytes, when ToAM uses 128-byte long object_ID. Secondly, with the chord ring, the communication cost is reduced from $N \cdot 20 + 128$ to $20(\mathrm{Log2}(N) + 1) + 128$ in intra-group authentication. At the same time, the chord ring also avoids failure of identity authentication by weak connection or single point of failure.

To evaluate the communication efficiency of ToAM, we compare communication costs with our system and BASA and SENTINEL in the same environment. Assuming that the UAVs in the group are certified once in pairs and the number of them ranges from 0 to 50, we checked the cost of all UAV communication in the group. The result is as shown in Fig. 7, which shows communication efficiency of ToAM is higher than the other two

Table 3 Communication overhead

Phase	Information category	Length (bytes)
Group building	mUAV calls the smart contract and queries the UAV's public key	128 + 654
	Send the ticket and time stamp to UAV	28 + 4
	Send the ticket and related signatures to BS	28 + 20
	mUAV calls the smart contract and queries the related information	128 + 20
	Send the pre-shared key and time stamp to UAV	20 + 4
Intra-group authentication	The initiator UAV sends its ID	128
	The receiver searches the hash value in the chord ring	20·(Log2(N) + 1)

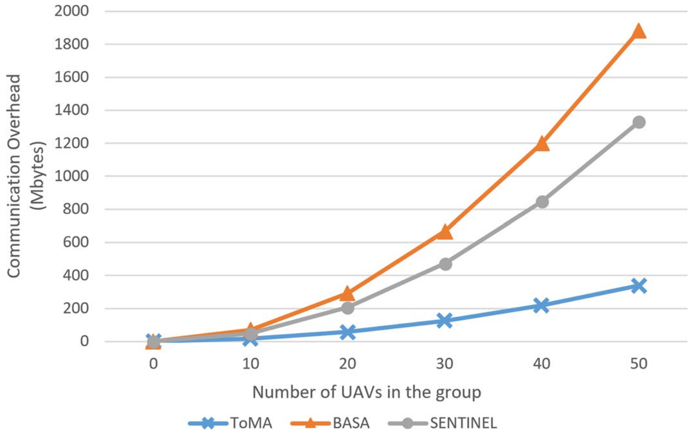


Fig. 7 Communication overhead. This figure shows the comparison of communication overheads under different scale nodes

methods. It is noted that since the main group building process is local, the communication cost of the intra-group authentication is less.

From the security analysis in Sect. 4.1, we can see that our ToAM integrates blockchain technology to improve flexibility and security. All authentication information is stored in the blockchain in the form of hash values, which ensures the security of the group building and intra-group authentication. To ensure the feasibility of working in a weak connection state, we use a chord ring. From the performance evaluation in Sect. 4.2, most of the computation cost of ToAM is in the group building, and the computation cost in the intra-group authentication is less. The average cost of both computation and communication is less than BASA and SENTINEL.

5 Conclusion

In the cooperative task performing scenario of the UAV group, they are faced with the transformation from ground infrastructure network to ad hoc wireless network, and the communication between these two networks is unstable or unavailable during the task performing, which brings great challenges to the authentication of UAVs. To this end, a task-oriented authentication model (ToAM) for UAVs based on blockchain is proposed in this paper, which adapts to the dynamic and complex network environments of the UAV group and supports the whole process authentication of UAV scheduling and tasks performing. In ToAM, a two-stage authentication framework is presented, which divides UAVs authentication into group building authentication and intra-group authentication. Then, two lightweight authentication protocols are presented, respectively, corresponding to these two stages. Analyses demonstrate that our model offered a lightweight and secure authentication for task-oriented UAV groups. In the future, we will pay more attention to the hierarchical blockchain method and study the lightweight blockchain method suitable for intra-group authentication.

Abbreviations

ToAM: Task-oriented authentication model; UAV: Unmanned aerial vehicle; mUAV: Master UAV; CA: Certificate authority; BAS: Blockchain authentication server; BS: Business server; TPM: Trusted platform module; GrpID: The group ID; ECDHE: Elliptic curve Diffie–Hellman ephemeral; ECDLP: Elliptic curve discrete logarithm problem; BASA: Blockchain-assisted secure device authentication.

Acknowledgements

We are thankful to the members of our research team Sijie Zhang, Guanju Li, Deying Liu, Yutong Long, and Xinyi Wen, who greatly assisted the research.

Authors' contributions

A.C., K.P., and Z.S. designed the model and conceived the experiments. Z.S. and Z.Y. performed the analysis. K.P., Z.S., and X.Z. analyzed the data and wrote this paper. G.L. and A.C. helped supervise the project. All authors read and approved the final manuscript.

Funding

This work was supported by the National Key R&D Program of China (No. 2018YFC0807500), by the National Natural Science Foundation of China (No. U19A2059), and by the Ministry of Science and Technology of Sichuan Province Program (Nos. 2019YFG0507, 2021YFG0018, 20ZDYF0343).

Availability of data and material

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China. [2]Trusted Cloud Computing and Big Data Key Laboratory of Sichuan Province, Chengdu 611731, China. [3]Information Center of China North Industries Group, Beijing 100089, China.

Received: 8 October 2020 Accepted: 2 August 2021
Published online: 14 August 2021

References

1. H. Hlavacs, Cooperative enhancement of position accuracy of unmanned aerial vehicles, in *International Conference on Advances in Mobile Computing and Multimedia* (2013), p. 326–334
2. W.Y.B. Lim, J. Huang, Z. Xiong, J. Kang, D. Niyato, X.S. Hua, C. Leung, C. Miao, Towards federated learning in UAV-enabledinternet of vehicles: a multi-dimensional contract-matching approach. Electr. Eng. Syst. Sci. arXiv:2004.03877 (2020)
3. J.S. Ng, W.Y.B. Lim, H.N. Dai, Z. Xiong, J. Huang, D. Niyato, X.S. Hua, C. Leung, C. Miao, Joint auction-coalition formation framework for communication-efficient federated learning in UAV-enabled internet of vehicles. IEEE Trans. Intell. Transp. Syst. **22**, 2326–2344 (2020). https://doi.org/10.1109/TITS.2020.3041345
4. M.S. Sharawi, D.N. Aloi, O.A. Rawashdeh, Design and implementation of embedded printed antenna arrays in small UAV wing structures. IEEE Trans. Antennas Propag. **58**(8), 2531–2538 (2010)
5. Z. Cai, Z. Duan, W. Li, Exploiting multi-dimensional task diversity in distributed auctions for mobile crowdsensing. IEEE Trans. Mob. Comput. **20**, 2576–25971 (2020). https://doi.org/10.1109/TMC.2020.2987881
6. C. Kennedy, J.I. Rogers, Virtuous drones? Int. J. Hum. Rights. **19**(2), 211–227 (2015)
7. M. Bae, H. Kim, Authentication and delegation for operating a multi-drone system. Sensors. **19**(9), 2066–2084 (2019)
8. I. Jawhar, N. Mohamed, J. Al-Jaroodi, D.P. Agrawal, S. Zhang, Communication and networking of UAV-based systems: classification and associated architectures. J. Netw. Comput. Appl. **84**, 93–108 (2017)
9. J.S. Lee, C.C. Chang, P.Y. Chang, C.C. Chang, Anonymous authentication scheme for wireless communications. Int. J. Mob. Commun. **5**(5), 590–601 (2007)
10. M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, M. Guizani, Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J. Sel. Areas Commun. **38**(5), 942–954 (2020)
11. M.L. Santos, J.C. Carneiro, A.M.R. Franco, F.A. Teixeira, L.B. Oliveira, FLAT: federated lightweight authentication for the Internet of Things. Ad Hoc Netw. **107**(1), 22–53 (2020)
12. S. Zhu, W. Li, H. Li, L. Tian, G. Luo, Z. Cai, Coin hopping attack in blockchain-based IoT. IEEE Internet Things J. **6**(3), 4614–4626 (2019)
13. S. Zhu, Z. Cai, H. Hu, Y. Li, W. Li, zkCrowd: a hybrid blockchain-based crowdsourcing platform. IEEE Trans. Industr. Inf. **16**(6), 4196–4205 (2020)
14. S. Khan, W.-K. Lee, S.O. Hwang, A Echain, A lightweight blockchain for IoT applications. IEEE Consumer Electron. Mag. https://doi.org/10.1109/MCE.2021.3060373 (2021)
15. W. Wang, N. Hu, X. Liu, BlockCAM: a blockchain-based cross-domain authentication model. in *2018 IEEE Third International Conference on Data Science in Cyberspace* (2018), p. 896–901
16. J. Xu, X. Meng, W. Liang, H. Zhou, K.-C. Li, A secure mutual authentication scheme of blockchain-based in WBANs. China Commun. **17**(9), 34–49 (2020)

17. A. Gibson, G. Thamilarasu, Protect your pacemaker: blockchain based authentication and consented authorization for implanted medical devices. Procedia Comput. Sci. **171**, 847–856 (2020)
18. C. Zhang, L. Zhu, C. Xu, BPAF: blockchain-enabled reliable and privacy-preserving authentication for Fog-Based IoT devices. IEEE Consumer Electron. Mag. (2021). https://doi.org/10.1109/MCE.2021.3061808
19. Z. Cui, F. Xue, S. Zhang, X. Cai, J. Chen, A hybrid blockchain-based identity authentication scheme for Multi-WSN. IEEE Trans. Serv. Comput. **13**(2), 241–251 (2020)
20. S. Dong, H. Yang, J. Yuan, L. Jiao, A. Yu, J. Zhang, Blockchain-based cross-domain authentication strategy for trusted access to mobile devices in the IoT. in *2020 International Wireless Communications and Mobile Computing (IWCMC)* (2020), p. 1610–1612
21. J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, L. Chen, A data authentication scheme for UAV ad hoc network communication. J. Supercomput. **76**, 4041–4056 (2020)
22. W. Hong, L. Jianhua, L. Chengzhe, W. Zhe, A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks. Peer-to-Peer Netw. Appl. **13**(2), 53–63 (2019)
23. C. Chen, Y. Deng, W. Weng, C. Chen, Y. Chiu, C. Wu, A traceable and privacy-preserving authentication for UAV communication control system. Electronics **9**(1), 62 (2020)
24. G. Sarath, D.C. Jinwala, S. Patel, A survey on elliptic curve digital signature algorithm and its variants. Int. J. Commun. Syst. **27**(8), 121–136 (2014)
25. G. Cho, J. Cho, S. Hyun, H. Kim, SENTINEL: a secure and efficient authentication framework for unmanned aerial vehicles. Appl. Sci. **10**, 31–49 (2020)
26. B. Bera, A.K. Das, A.K. Sutrala, Private blockchain-base access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment. Comput. Commun. **166**(3), 91–109 (2021)
27. I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, H. Balakrishnan, Chord: a scalable peer-to-peer lookup protocol for Internet applications. in *Proceedings of the ACM SIGCOMM '01* (2001), p. 149–160
28. P. Karrupusamy, Advanced metering infrastructure with secure chord lookup protocol for IoT Systems. J. Electric. Eng. Autom. **2**(3), 112–117 (2021)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.