Design of emergency UAV network identity authentication protocol based on Beidou

Donghao Zhao*, *Yu* Lu, *Xiaoguang* Liu, *Wenxin* Qiao, *Zhiwei* Li, and *Yicen* Liu

Army Engineering University(Shijiazhuang Campus), Shijiazhuang,050003, China

Abstract. In view of the bad environment and intermittent communication of UAV network, based on the short message communication function of Beidou satellite navigation system, which can provide all-weather and no blind area communication service, a UAV network identity authentication protocol under emergency state when conventional means cannot communicate is designed.

1 One time password technology

One time password authentication is a dynamic password authentication method based on pseudo-random sequence. Compared with the authentication method based on public key infrastructure, it does not need the participation of the third-party CA, and has lower cost; compared with the authentication method based on static password, it has higher security; compared with the authentication method based on biometrics, it does not need the support of complex devices, so it is easier to implement. Generally speaking, the authentication method based on one-time password not only ensures certain security, but also does not need the support of CA. It has the advantages of small calculation and low energy consumption. It is also the authentication method adopted in this protocol.

One time password authentication is usually divided into four ways: one-time password based on password sequence, one-time password based on time synchronization, one-time dynamic password based on event synchronization and one-time dynamic password based on challenge / response. The four kinds of one-time password forms are specific compared as follow.

We compare these authentication methods in terms of traffic, security, complexity, computation and hardware support. The results are shown in Table 1.

Through the comparative analysis of the above four one-time passwords, it can be seen that the authentication mechanism based on time synchronization has the advantages of small traffic volume, high security and small amount of user calculation. Moreover, the Beidou satellite navigation system terminal carried by UAV can effectively solve the problem of time synchronization. Generally speaking, compared with the other three authentication mechanisms, it has obvious advantages, and It is a feasible choice for UAV network emergency communication protocol.

* Corresponding author: zhaodonghao1@sina.com

Table 1. Comparison of one time passwords.

Type	Traffic	Security	system complexity	client computing	special hardware support
Password sequence	large	low	complex	large	not required
Event synchronization	large	low	complex	small	required
Challenge / response	large	high	simple	large	either will do
Time synchronization	small	high	complex	small	required

2 Protocol description

The identity authentication protocol is divided into initialization process and authentication process. The symbols and meanings involved in the protocol are shown in table 2.

Table 2. Symbols and meanings involved in the agreement.

symbol	meaning
UAV	Certification initiator UAV node
GCS	Certification responder ground control station
ID_i	Identification
PW_i	Login password
$IMEI_i$	Terminal hardware identification code
$Seed_i$	Unique seed for each device
T	Timestamp value
P	The basis of UAV authentication S legal identity
SHA()	Hash function SH1-1 encryption
‖	Connector
⊕	XOR operator
Reg	Registration request
Log	Landing request

2.1 Initialization process

The initialization process mainly includes the establishment of the connection and the data exchange between the two sides of the communication.

In the data exchange stage, the initiator and the responder provide their own identification to each other, complete the exchange of seed and serial number to complete the registration. The specific exchange process is as follows:

(1) UAV→GCS: The initiator UAV inputs ID and PW and sends registration request, encrypted ID, paired ID, IMEI and seed to GCS of responder, that is, sending reg, SHA（ID）, P=SHA(ID+PW), SHA(IMEI) and SHA（Seed）;

(2) GCS→UAV: The responder GCS verifies whether it is a registered user. If it exists, it will send a message to the user that the user name already exists and fails to register; if not, it will bind the ID with IMEI, PW and seed and store it in the database, and send the registration success information to the initiator UAV.

The initialization process is shown in Figure 1.

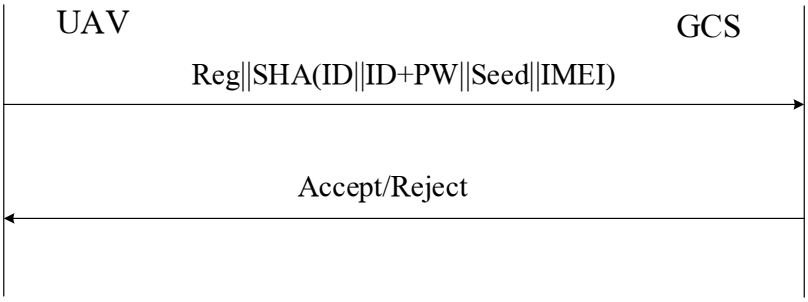

Fig. 1. Initialization process.

2.2 Identity authentication stage

In the authentication stage, the mutual authentication of both parties is completed. In the process of authentication, both sides verify the operation result of irreversible hash function to realize the authentication of one-time password. The specific authentication process is as follows.

(1) UAV→GCS: Log, $SHA（ID）$

The initiator UAV inputs the ID and PW, sends the login request Log and $SHA（ID）$;

(2) GCS→UAV: $(T \oplus P)||SHA(R \oplus IMEI \oplus Seed)/Reject$

The GCS of the responder verifies whether it is registered according to the user name $SHA（ID）$ saved in the database. If there is no relevant user in the database, it refuses to authenticate and disconnects the conversation with the initiator UAV. If the relevant user is queried, the time stamp T is obtained from BDS, and the information after T, seed and IMEI calculation $(T \oplus P)||SHA(T \oplus IMEI \oplus Seed)$ is sent to the initiator UAV;

(3) UAV→GCS: $SHA(PW||T'||IMEI||Seed)/Reject$

After receiving the message, the initiator UAV extracts the $T \oplus P$ and $SHA(R \oplus IMEI \oplus Seed)$ by string operation. The calculation results are as follows:

Make $PS=P \oplus T$, $Q=SHA(T \oplus IMEI \oplus Seed)$

$P'=SHA(ID+PW)$

$T'=P' \oplus PS$

$Q'=SHA(R' \oplus IMEI \oplus Seed)$

(4) GCS→UAV: $T \oplus P$ Accept/Reject

The responder GCS finds the corresponding PW, IMEI, and Seed by querying the ID. if it does not exist, the GCS refuses to authenticate. If it does, it hashes PW, T, IMEI and Seed, and make $R'=SHA(PW||T||IMEI||Seed)$. If $R=R'$, the initiator UAV is authenticated by the responder's GCS, otherwise, the initiator's UAV is refused to log in.

At this point, the mutual authentication between the initiator UAV and the responder GCS is completed, and the certification process is shown in Figure 2.

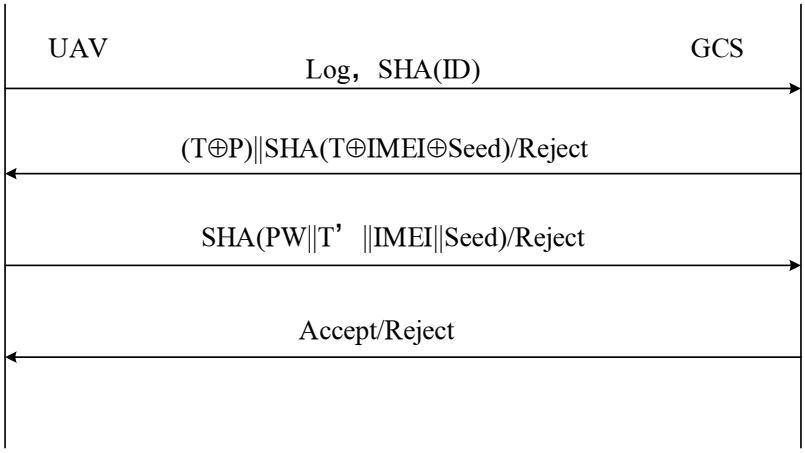

Fig. 2. Certification process.

3 Performance analysis

3.1 Safety analysis

(1) Analysis of anti replay attack characteristics

Since the one-time password is generated by adding the time stamp value into the seed saved by itself, the hash algorithm is used to generate the password, and the time of each authentication is different, so the password calculated is also different, which can effectively prevent replay attacks.

(2) Analysis of anti decimal attack characteristics

In this protocol, the password information of the previous authentication will not be saved, and the password of the later authentication has no connection with the previous password, which fundamentally prevents the decimal attack.

(3) Analysis of anti counterfeiting attack characteristics

Different from the traditional one-way authentication, in this protocol, both sides of the communication will compare the one-time password received and the password calculated by themselves. If any error is found, the communication will be stopped immediately, realizing the two-way authentication, which can effectively prevent the counterfeiting attack.

(4) Analysis of message tamper resistance

This protocol uses hash function to calculate the one-time password. The security features of hash function can make the communication parties judge the integrity of the message, and can effectively prevent message tampering.

(5) Analysis of anti man in the middle attack

The information exchange in this protocol is carried out in the "Beidou" short message channel, and the information is encrypted by hash function. Due to the high security of the short message channel itself and the unidirectionality of the hash function, even if the information in the channel is intercepted, the effective information cannot be calculated and obtained.

In terms of meeting security requirements and resisting common attacks, the protocol is compared with other protocols, and the results are shown in table 3. Where Y means that the attack can be resisted or the requirement can be met, and N means that it can not be resisted or not satisfied. Common security requirements and attack types are as follows:

A1: complete two-way certification;
A2: forward safety;
A3: resist replay attack;
A4: resistance to decimal attack;
A5: resistance to denial of service attacks;
A6: resistance to the attack of middlemen;
A7: resist parallel session attack;
A8: eavesdropping attack.

Table 3. Safety comparison.

	A1	**A2**	**A3**	**A4**	**A5**	**A6**	**A7**	**A8**
literature [1]	Y	Y	Y	Y	N	Y	N	Y
literature [2]	Y	Y	Y	Y	Y	Y	Y	N
literature [3]	N	Y	Y	Y	Y	N	Y	Y
literature [4]	Y	Y	Y	Y	N	Y	Y	Y
This Agreement	Y	Y	Y	Y	Y	Y	Y	Y

This protocol not only achieves the security goal of the traditional one-time password authentication protocol, but also enhances the security performance of the protocol and the resistance to eavesdropping and man in the middle attacks combined with the "Beidou" short message channel. From the above analysis and the data in the table, we can see that this protocol can resist common security attacks and has certain advantages in security performance.

3.2 Performance analysis

According to the theory of computational complexity, the performance of user mutual authentication protocol depends on the number of sessions, traffic, computation and storage.

Table 4 shows the performance comparison with several protocols proposed at present. L represents the output of hash function, the random number generated by using pseudo-random function and the length of challenge value, P represents pseudo-random number operation, H represents hash operation, Pk represents asymmetric encryption and decryption operation, and Se represents symmetric encryption and decryption operation.

Table 4. Performance analysis.

	Number of sessions	**traffic**	**computation**	**storage**
literature [1]	4	2L	2Pk+P	6L
literature [2]	6	4L	4H+2P	4L
literature [3]	5	6L	2Pk+3P	8L
literature [4]	16	2L	2Se+2P	4L
This Agreement	4	2L	3H	2L

According to the analysis results in table 4, compared with the asymmetric operation required in reference [1], the protocol proposed in this paper only needs hash operation, which greatly reduces the terminal's requirements for computing capacity and also reduces power consumption. The protocol proposed in reference [2] is also superior in all aspects, but there are still security risks due to the lack of encryption of authentication information;

the protocol in reference [3] is also asymmetric encryption, and does not occupy any advantages in all aspects, especially the communication volume is three times of the protocol, and it is not suitable for short message channel with shortage of bandwidth resources; because the protocol in reference [4] is based on the aid of authentication Because of the three-party authentication of the certificate server, it has a greater disadvantage in the number of sessions compared with other protocols. Although this protocol uses physical means to keep the session secret, the increase of the number of sessions will inevitably increase the probability of leakage.

In a word, compared with other traditional authentication protocols using one-time password, this protocol has certain advantages in terms of traffic and computation, which can reduce the use of channel bandwidth resources of precious short message as far as possible; at the same time, since the frequency of sending messages in the channel is 1s / time, in order to shorten the authentication time as much as possible. We use the time-based dynamic one-time password authentication, and complete the two-way authentication with the least number of interactions.

4 Conclusion

Aiming at the problem of emergency authentication when the ordinary wireless channel can not communicate, combined with the Beidou satellite navigation system independently developed in China. This paper proposed an emergency authentication protocol for UAV network based on "Beidou", which uses the unique short message channel of Beidou satellite navigation system for message interaction, so that any terminal carrying BDS can be at any time and any place.The unidirectionality of hash function and the reliability of short message channel ensure the security of authentication. The performance analysis shows that the protocol has certain advantages in the similar lightweight protocols.

This work was supported by the National Natural Science Foundation of China under Grants 62071483.The authors would like to thank the editor and anonymous experts for the instructive comments, and we appreciate your warm work earnestly.

References

1. Wang Qin, Beijing Jiaotong Univercity,Research on Identity Authentication Protocol in Mobile Commerce Based on OTP (2010).
2. Gong Long-yan,Pan Jing-xin,Liu Bei-bei,et al,Journal of Computer and System Sciences, A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords,**79**, 122-130,(2013).
3. Yun-Seok L,Eun K,Min-Soo J,Proceedings of the 3rd International Conference on Computer Science and Information Technology,A NFC based Authentication Method for Defense of the Man in the Middle Attack, 10-13,(2013).
4. Xu Wei,Wang Xue-ming, Communications Technology, A Novel Lightweight Identity Authentication Protocol in NFC Application,**49**,1529-1534,(2016).
5. Xie Jun,Chang Jin, Spacecraft Engineering, Innovation achievements and prospects of Beidou-2 satellite system,**26**,1-8,(2017)
6. Zhong Cheng,Li Xing-hua,Song Yuan-yuan, Chinese Journal of Computers, A Lightweight Anonymous Authentication Protocol Based on Shared Key in Wireless Networks,**41**,191-205,(2018)

7. Chuang Y H, Lo N W, Yang C Y, et al., Sensors, A Lightweight Continuous Authentication Protocol for the Internet of Things,**18**,1104,(2018)
8. Shen J, Chang S, Shen J, et al, Future Generation Computer Systems, A lightweight multi-layer authentication protocol for wireless body area networks,78,(2016)