Controllable and Anonymous Authentication Scheme for Space Networks

Zhi-Yan Hu[1], Xue-Hui Du[2], Li-Feng Cao[3]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing Zhengzhou, China*
[2]*State Key Laboratory of Mathematical Engineering and Advanced Computing Zhengzhou, China*
[3]*State Key Laboratory of Mathematical Engineering and Advanced Computing Zhengzhou, China*
[1]*huzhiyan1234@126.com,* [2] *dxh37139@sina.com,* [3]*caolf302@sina.com*

Abstract: This paper analyzed the existing anonymous authentication schemes which have the weakness of high calculation and communication cost and weak security. So we designed a secure and efficient anonymous authentication scheme to meet the need of the space network, which has the characteristic of resource limited, high exposure and intermittent connectivity. At first we proposed a signature algorithm based on certificateless public key cryptosystem and one-off public key, and then presented an anonymous authentication scheme according to the proposed signature algorithm, it needs two message interaction to complete the mutual authentication and key agreement. When the user has the illegal behavior, the service provider can reveal the illegal user's real identity through cooperation with the trusted center. Compared with the similar literature, the proposed scheme achieves high security with low computation and communication cost. (Abstract)

1. Introduction

The space network structures with double plane of heaven and earth, which is based on the ground network and expanding with space-based network. The network consists of space-based backbone network, space-based access network, ground-based node network [1], so it has characteristics of heterogeneity, intermittent connectivity and high exposure. Compared with the traditional network, the space network is more easily attacked by eavesdropping, tampering and replay attack. The deployment of access authentication and privacy protection for the security of the space network is essential [2]. The space network of highly exposure makes it necessary for user real identity authentication when it needs to use the space network service. At the same time, network authentication needs to achieve anonymity and traceability in order to prevent the disclosure of privacy. What's more, it is necessary to reduce the computational overhead of the user and service provider for the resource limited space networks [2]. Last but not the least, the need to reduce the message length and minimize the number of interactions should also be considered for the characteristics of intermittent connectivity.

Scholars at home and abroad have done a lot of research on anonymous authentication in the wireless networks. Liu et al. [3] proposed an anonymous authentication scheme using certificateless public key cryptosystem to achieve mutual authentication using MAC, and it used bilinear pairing to build the user index to achieve the connection between user identity and the index. Shim[4] presented a signature algorithm for vehicular sensor networks based on bilinear pairings, and a mutual authentication scheme was presented based on the algorithm, but it still required a large amount of calculation and had the key escrow problem. Hsieh et al. [5] proposed an anonymous protocol using self-certified public key technology and bilinear pairing for mobile user, the user and the service provider needed three message interaction to realize authentication and key agreement, but a lot of calculation was required. Amin et al. [6] pointed out the shortage of Hsieh's protocol that cannot resist the server spoofing attack and unable to hide the true identity of the user, but Amin's scheme needed a trusted third party in the authentication process. He et al. [7] used self-certified public key mechanism to realize the anonymity of user authentication, and mutual authentication was achieved by verifying the non-forged messages, but the scheme did not achieve malicious user identity tracking and recovery, and the three information interaction increased the communication pressure. Zhou et al.[8] proposed a controllable roaming authentication protocol for heterogeneous wireless network which achieved anonymity, authentication and user tracking using one-off public key and signature algorithm, but using bilinear to track the true identity of the user required a large amount of computational overhead. Wan et al.[9] proposed an anonymous authenticated key agreement protocol based on trusted computing, the user

constructed dynamic identity using random number to realize the anonymity and untraceability every time, but it is essential to use smart card and biometric information to design the protocol. Zhou et al. [10] designed an anonymous authentication scheme that a server needs 1 rounds of message exchange to authenticate the user's real identity, the scheme can track the true identity of the illegal user with the help of home server, but there are complex certificate storage and calculation pressure using mobile trusted module technology to verify the trusted terminal.

Aimed at the problems of the existing anonymous authentication scheme, this paper proposes a secure and efficient anonymous authentication scheme which is suitable for the space network. It uses the certificateless public key cryptosystem to overcome the key escrow problem, and designs a one-off public key signature algorithm to realize efficient authentication, uses pseudonyms to achieve anonymous authentication, and tracks the true identity of the illegal user through the interaction with the trusted center.

2. Preliminaries

2.1 Bilinear Maps

Let l be a security parameter, q is a prime number of $l-bit$, G_1 represents a cyclic additive group of order q , G_T represents a cyclic multiplicative group of the same order, P is a generator of G_1 , Q is a generator of G_1 , we call map $e: G_1 \times G_1 \to G_T$ a bilinear map if the following properties are satisfied:

(1) Bilinearity: for all $a,b \in Z_q^*$, such that $e(aP,bQ) = e(P,Q)^{ab}$;

(2) Non-degeneracy: exist $P,Q \in G_1$, such that $e(P,Q) \neq 1$;

(3) Computability: $\forall P,Q \in G_1$, it's efficient to compute $e(P,Q)$.

2.2 System Model

In space networks, the system model is composed of space-based access network, space-based backbone networks, ground-based node network and base station (BS). As shown in Figure 1. The base station completes the work of system setup and key generation. Ground nodes makes an anonymous access request to the space-based network nodes when it's in the space-based network node's coverage range. Then ground nodes and space-based network nodes can communicate safely with each other after mutual authentication and key establishment.

3. One Signature Algorithm Based on Certificateless Cryptosystem and One-Off Public Key

3.1 Algorithm Design

Our algorithm contains 5 polynomial time algorithms including system setup, partial private key generation, user key generation, sign and verification.

3.1.1 System Setup

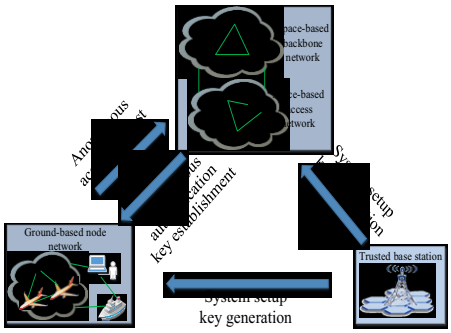

Figure 1. Anonymous authentication model for space networks

The trusted center KGC generates cyclic additive group G_1 and cyclic multiplicative group using security parameter k , and bilinear mapping $e: G_1 \times G_1 \to G_2$. It chooses $\lambda \in Z_q^*$ randomly as the master key and the generator $P \in G_1$, computes $P_{pub} = \lambda P$ .The KGC selects two secure hash functions $H_0: \{0,1\}^* \to Z_q^*, H_1: \{0,1\}^* \to Z_q^*$. In the end, the KGC makes system parameters set $paras = (G_1, G_2, e, P, P_{pub}, H_0, H_1)$ public and keeps the master key λ secret.

3.1.2 Partial Private Key Generation

The user A has the real identity of RID_A , A randomly selects $x_A \in Z_q^*$ and computes $R_1 = x_A P$, and transmits RID_A and R_1 to KGC through secure channel. Then it chooses $y_A \in Z_q^*$ randomly and computes $R_2 = y_A P$ and $R_A = R_1 + R_2$. The pseudonym is $PID = RID \oplus H_0(\lambda R_A, T_{ID})$ while T_{ID} represents valid period of the pseudonym. The KGC builds the connection between PID and RID , and then computes the partial private key $D_A = y_A + \lambda PID$. In the end, the KGC transmits (R_A, D_A, PID) to the user A through the secure channel.

3.1.3 User Key Generation

The user A generates the whole private key (x_A, D_A) when it received the massage transmitted from the KGC. And then A check the equation $(x_A + D_A)P = R_A + P_{pub} \cdot PID$ to verify the correctness of the private key. After verification user A randomly chooses $z \in Z_q^*$ and sets $P_1 = z(x_A + D_A)P$, $P_2 = zR_A$ and $P_3 = z \cdot PID \cdot P$. User A transmits (P_1, P_2, P_3) to other side B.

3.1.4 Sign

The user A randomly picks $a \in Z_q^*$ and computes $N = aP$, $h = H_1(N, M)$, $S = h(x_A + D_A)z + a \cdot h$, $M \in \{0,1\}^*$ represents the message. The user A transmits $\sigma = (N, S)$ and M to the other side B.

3.1.5 Verification

B checks the equation $e(P_1, P) = e(P_2, P)e(P_3, P_{pub})$ to verify the validity of one-off public key, as a result of

$$e(P_1, P) = e(z(x_A + D_A)P, P) = e(z(x_A P + y_A P + PID \cdot P_{pub}), P)$$
$$= e(zR_A + z \cdot PID \cdot P_{pub}, P) = e(P_2, P)e(P_3, P_{pub})$$

The user A is a legal user verified buy the trusted center who has the system master key after the verification. And then it computes $h = H_1(N, M)$ and verifies the validity of signature through $S \cdot P = h(N + P_1)$, if the equation holds, outputs true, otherwise false.

3.2 Security Analysis

3.2.1 Anonymity

At first, the public key and signature contain user's pseudonym other than the real identity of user at the interactive process of algorithm to ensure the anonymity of the algorithm. Secondly, in the process of the one-off public key, the user uses random selection of data to build the public key, so the attacker cannot connect the public key with the user. The algorithm achieves complete anonymity.

3.2.2 Traceability of Anonymous User

Assuming that the user is compromised by the adversary into a malicious user, the other party B can communicate with the trusted center KGC to achieve the tracking of malicious users A. B transmits the pseudonym of user A PID to the KGC, KGC can recover the real identity of malicious through $RID = PID \oplus H_0(\lambda R_A, T_{ID})$. The algorithm can achieve efficient revocation of the real identity of malicious users.

3.2.3 Key Escrow

The algorithm is based on certificateless public key cryptosystem, the user's full private key consists of (x_A, D_A), x_A is generated by the user, D_A is generated by the KGC. KGC gets x_A through $R_1 = x_A P$ is equivalent of solving discrete logarithm problem on elliptic curve group, so the KGC cannot get the full private key of user achieving the security of no key escrow.

3.2.4 Unforgeability

At first, the legal user can not forge the public key and signature. After the public key verification, the public key is proved to contain the system master key. After the signature verification, it is proved that the signature contains the system master key, so the signature is legal and cannot be forged. Secondly, the one-off public key cannot be forged. The signature cannot pass the verification if P_1 is forged, it cannot pass the public key verification if P_2, P_3 are forged.

The illegal user can not forge the public key and signature. The illegal user randomly picks $b \in Z_q^*$, sets $P_1^{'} = bP_1$, $P_2^{'} = bP_2$, $P_3^{'} = bP_3$. Obviously it can pass the public key verification, but it cannot get legal private key (x_A, D_A) to compute the signature. As a result of getting $(x_A + D_A)$ through $P_1^{'} = bz(x_A + D_A)P$ as well as getting a through $N = aP$ is equivalent of solving discrete logarithm problem on elliptic curve group. The illegal user can not compute valid signature. Furthermore, the illegal user randomly chooses $a, b \in Z_q^*$ and sets $P_1^{'} = aP_{pub} + bP$, $P_2^{'} = bP$, $P_3^{'} = aP_3$, obviously it can pass the public key verification, but it cannot construct valid signature through the forged private key. We can draw the conclusion that whether legal users or illegal users can not forge valid public key and signature.

4. Authentication scheme for the space network

4.1 Certificateless Anonymous Authentication Scheme

We propose an anonymous authentication scheme for space networks based on certificateless cryptosystem and one-off public key, as shown in Figure 2. The trusted base station completes system initialization and key generation in advance, then the user completes mutual anonymous authentication process with the access service satellite.

4.1.1 System Setup

The base station BS (the trusted center) generates system parameters according to Section 3.1, defines 4 hash functions $H_0:\{0,1\}^*\times G_1\to Z_q^*$, $H_1:\{0,1\}^*\to Z_q^*$, $H_2:Z_q^*\to Z_q^*$, $H_3:G_1\to\{0,1\}^*$, and publish system parameter set $paras=(G_1,G_2,e,P,P_{pub},H_0,H_1,H_2,H_3)$, keeps system master key λ secret.

4.1.2 Key Generation

The user A in space networks communicates with the trusted base station BS according to partial private key generation and user key generation algorithm descripted in section 3.1 , and verify the full private key (x_A,D_A) of the user A, which $D_A=y_A+\lambda PID$, $PID=RID\oplus H_0(\lambda R_A,T_{ID})$. The BS saves (R_A,PID) . The access service satellite randomly picks $v\in Z_q^*$ as the private key and sets $P_{AS}=vP$ as the public key.

4.1.3 Access Authentication

The first step, the user A in the space network randomly picks $z\in Z_q^*$, and computes the one-off public key $P_A=(P_1,P_2,P_3)$ which $P_1=z(x_A+D_A)P$, $P_2=zR_A$ and $P_3=z\cdot PID\cdot P$. Then A gets the current timestamp T_A , and randomly chooses $a\in Z_q^*$, computes $L_0=H_2(a)$, $k=H_3(aP_{AS})$, $\omega=k\oplus L_0$, $N=aP$, $h=H_1(N,T_A,L_0)$ and $S=ah+z(x_A+D_A)h$. The user A sends the signature $\sigma=(N,S)$, ω , T_A and P_A to AS.

The second step, the AS verifies the validity of timestamp when it receives the message. If the timestamp is fresh, then AS verifies the validity of the public key according to section 3.1. After verification the AS computes $k=H_3(vN)$, and gets $L_0=k\oplus\omega$. Then the AS computes $h=H_1(N,T_A,L_0)$ and verifies the validity of the signature through $S\cdot P=h(N+P_1)$. And then the AS creates the repeated authentication list $L_{RA}=\{PID,L_i,Num,T_{die}\}$ which $L_i=H_2(L_{i-1})$ and Num represents authentication times, T_{die} represents expiration time. In the end, the AS randomly picks $b\in Z_q^*$ and computes $M=bP$, the session key is $K_{AS-A}=bN=abP$. After that AS gets current timestamp T_{AS} , uses symmetric encryption algorithm to compute $EM=E_k(P_A,M,T_{AS})$, and sends T_{AS} and EM to the user A.

The third step, the user A verifies the freshness of the timestamp. After verification it decrypts the message EM using k . By comparing T_{AS} to prevent the message from being tampered, by comparing P_A to verify the identity of AS. After that the session key is $K_{A-AS}=aM=abP$.

4.2 Repeated Authentication and Key Update

When the same user makes the access request to the same access service satellite, they realize fast and efficient authentication and update the session key according to the following steps.

The first step, the user A in the space network randomly picks $a'\in Z_q^*$, computes $N=a'P$, $L_i=H_2(L_{i-1})$, $k=H_3(aP_{AS})$ and $\omega=k\oplus L_i$, and then sends $E_k(\omega,PID_i,T_A)$ to the AS.

The second step, the AS computes $k=H_3(vN)$ when it receives the message, and decrypts the message to verify the freshness of the timestamp. If the timestamp is invalid, rejects, otherwise it can get $L_i=k\oplus\omega$, and uses PID_i and L_i to check the repeated authentication list L_{RA} whether exists the corresponding item, if there is one item in the list, the AS checks the T_{die} . If all these verification pass, the user A passes the authentication. The AS updates the list $L_{RA}=\{PID,L_i,Num,T_{die}\}$. And then AS randomly chooses $b\in Z_q^*$, computes $M=b'P$, so it can get the session key $K_{AS-A}=b'N=a'b'P$. In the end, the AS gets the current timestamp T_{AS} and uses symmetric encryption algorithm to compute $EM=E_k(P_A,M,T_{AS})$, sends T_{AS} and EM to the user A.

The third step, the user A verifies the freshness of the timestamp at first. After that it decrypts the message EM using k . By comparing T_{AS} and P_A to verify the AS. If it passes, updates the session key $K_{A-AS}=a'M=a'b'P$.

4.3 Security Analysis

4.3.1 Traceability of Malicious User

In the process of access authentication, the access service satellite can recover the real identity of the malicious user through the communication with the trusted base station when it finds the malicious behavior of the user, so our scheme realizes the traceability of the malicious user. The AS sends the identity PID to the BS, the BS can get the real identity through $RID=PID\oplus H_0(\lambda R_A,T_{ID})$.

4.3.2 Anonymity

In the entire process of authentication, the user's pseudonym is transmitted other than the real identity, so our scheme realizes user identity privacy protection.

4.3.3 Mutual Authentication

In the first access authentication process, the AS can verify the user A through the one-off public key verification and signature verification to avoid forgery attack. The user A decrypts the message $EM = E_k(P_A, M, T_{AS})$, and verifies the AS through comparing T_{AS} and P_A as a result of only legal AS can decrypts the message through computing $k = H_3(vN)$. In the process of repeated access authentication, only the legal user A can compute $L_i = H_2(L_{i-1})$ through L_{i-1} that can pass the repeated authentication list.

4.3.4 Session Key Security

In this scheme, the intermediate parameters have strong timeliness and the session key is independent and unique which determined by both sides of communication using random number, the attacker cannot obtain session key information from the previous message, so our scheme achieves forward security, known session key security and key control security, and this scheme realizes no key escrow based on certificateless cryptosystem.

5. Performance Comparison

This paper compares the first authentication scheme, the repeated authentication scheme and some existing authentication schemes in authentication efficiency (as shown in Table 1) and security (as shown in Table 2). Compared with [5] [6], our scheme has lower computational overhead, the interaction time is less, and the communication cost is relatively lower. In terms of security, the [5] scheme cannot resist identity guessing attack, and a trusted center is not able to achieve recovery of the real identity of the user in the two schemes. Compared with the literature [7], although our authentication scheme has more multiplication in group, there is no exponentiation operation, so the total computational cost is relatively low, and the message interaction time is less leading to low communication overhead. In terms of security, our scheme realizes traceability. There is a large number of hash operations in the [8], and the scheme needs to consume 2n bilinear pairing operation to realize the recovery of the malicious user in the worst case (n is the number of registered users in the trusted center). Although our scheme's computational overhead is relatively large in the first authentication, there is no need to construct one-off public key and signature algorithm in the repeated authentication, and requires only one hash operation in the realization of a malicious user identity tracking which greatly reduces the computational overhead, and computational overhead of user is less than the server. All these properties meet the characteristics of resource limited for the space network. In terms of communication cost, our scheme only needs two interactive messages, and the message length is short which suitable for the characteristics of intermittent connectivity. In terms of security, our scheme achieves user anonymity, key escrow security and mutual authentication which can protect the communication security in the space network of highly exposure.

Table1. Efficiency comparison of authentication scheme

Operation	Literature [5]		Literature [6]		Literature [7]		Literature [8]		Our scheme-1		Our scheme -2	
	User	*Server*	*user*	*server*	*user*	*server*	*user*	*server*	*user*	*server*	*user*	*server*
Scalar Multiplication in group(M)	7	5	4	7	2	2	6	5	6	5	3	3
Scalar addition in group (A)	1	1	4	4	1	0	0	1	0	1	0	0
Map-to-point(P)	1	1	2	0	0	0	0	0	0	0	0	0
Hash(H)	7	2	9	8	8	5	5	5	3	3	2	1
Bilinear pairing (BP)	0	2	0	2	0	1	1	4	0	3	0	0
exponentiation (E)	0	2	0	0	2	4	0	0	0	0	0	0
Signature length	-		-		-		Z_q^*		$G_1 \times Z_q^*$		-	
Interaction times	3		4		3		2		2		2	
User identity recovery	×		×		×		2BP		1H		1H	

Table2. Security comparison of authentication schemes

Scheme	Anonymity	Traceability	Mutual authentication	No key escrow	Session key security
Literature [5]	N	N	Y	Y	Y
Literature [6]	Y	N	Y	Y	Y
Literature [7]	Y	N	Y	Y	Y
Literature [8]	Y	Y	Y	Y	Y
Our scheme	Y	Y	Y	Y	Y

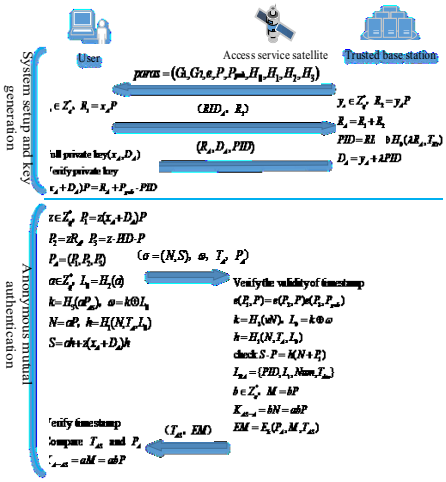

Figure 2. Anonymous authentication scheme

6. Conclusion

Most of the existing anonymous authentication schemes are aimed at heterogeneous wireless networks and vehicular ad hoc networks which cannot meet the requirements of high security and low power consumption. In this paper, we design a one-off public key and signature algorithm based on certificateless cryptography, and propose an efficient secure anonymous authentication scheme according to the proposed algorithm. It needs two message interaction between the user and the access satellite and one signature algorithm to complete the first authentication, and uses repeated authentication list to achieve efficiently repeated authentication. What's more, our scheme can realize anonymity revocation of malicious user through interaction with the trusted center. Comparative results show that our scheme achieves high efficiency while ensuring anonymity, mutual authentication, no key escrow, traceability and session key security which is more suitable for deployment in highly exposed and resource limited space networks.

Acknowledgment

This paper is supported by the National Key Research and Development Program of China (No.2016YFB0501900), the National Programs for High Technology Research and Development of China (No.2015AA016006) and the National Natural Science Foundation of China (No.61502531).

References

[1] FH Li, LH Yin, W Wu, LJ Zhang, and GZ Shi, "Research Status and Development Trends of Security Assurance for Space-ground Integration Information Network," Journal on Communications, vol. 37, Nov. 2016, pp. 156-168, doi:10.11959/j.issn.1000-436x.2016229.

[2] C Lin, Y Dong, and Z Shan, "Research on Space Internetworking Service Based on DTN," Journal of Computer Research & Development, vol. 51, May. 2014, pp. 931-943, doi: 10.7544/issn1000-1239.2014.20130769

[3] J Liu, Z Zhang, R Sun, and K S Kwak, "An Efficient Certificateless Remote Anonymous Authentication Scheme for Wireless Body Area Networks," Proc. EEE International Conference on Communications (ICC 12), IEEE Press, 2012, pp. 3404-3408, doi: 10.1109/ICC.2012.6363786.

[4] K A Shim, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks;" IEEE Transactions on Vehicular Technology, vol. 61, May. 2012, pp. 1874-1883, doi: 10.1109/TVT.2012.2186992.

[5] W B Hsieh and J S. Leu, "An Anonymous Mobile User Authentication Protocol Using Self-certified Public Keys Based on Multi-server Architectures," The Journal of Supercomputing, vol. 70, Oct. 2014, pp. 133-148, doi: 10.1007/s11227-014-1135-8.

[6] R Amin and G P Biswas, "Design and Analysis of Bilinear Pairing Based Mutual Authentication and Key Agreement Protocol Usable in Multi-server Environment," Wireless Personal Communications, vol. 84, May. 2015, pp. 439-462, doi: 10.1007/s11277-015-2616-7.

[7] D He, S Zeadally, N Kumar, and W Wu, "Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures," IEEE Transactions on Information Forensics & Security, vol. 11, Sep. 2016, pp. 2052-2064, doi:10.1109/TIFS.2016.2573746.

[8] YW Zhou, B Yang, and WZ Zhang, "Controllable and Anonymous Roaming Protocol for Heterogeneous Wireless Network," Chinese

Journal of Electronics, vol. 44, May. 2016, pp. 1117-1123, doi: 10.3969/j.issn.0372-2112.2016.05.015.

[9] T Wan, ZX Liu, and J F Ma, "Authentication and Key Agreement Protocol for Multi-Server Architecture," Journal of Computer Research and Development, vol. 53, Nov. 2016, pp. 2446-2453, doi: 10.7544/issn1000-1239.2016.20150107.

[10] YW Zhou, B Yang, and WZ Zhang, "Secure and Efficient Roaming Authentication Protocol with Controllable Anonymity for Heterogeneous Wireless Network," Journal of Software, vol. 27, Feb. 2016, pp. 451−465, doi:10.13328/j.cnki.jos.004840.