An Efficient Certificateless Identity Authentication Scheme for Low Earth Orbit Satellite Networks Postprint

Authors: Zhang Yi, Wu Qi, Zhou Shuangshuang, Jia Mengchao

Date: 2022-05-18T16:08:25Z

Abstract

To address the issues of high latency in existing low-orbit satellite network authentication schemes that utilize centralized authentication methods and significant computational overhead arising from complex bilinear mappings, we introduce a certificateless authentication model and propose an efficient certificateless authentication scheme built upon the Gayathri scheme. This scheme integrates the user' s public key with their real identity, thereby eliminating third-party involvement in the authentication process and reducing authentication latency. Authentication messages are constructed using only a few point multiplication and point addition operations on elliptic curves, avoiding bilinear mappings and thus lowering computational overhead. The security of the scheme is proven under the random oracle model based on the elliptic curve discrete logarithm problem assumption. Finally, experimental simulations demonstrate that compared with existing low-orbit satellite identity authentication schemes, the proposed scheme achieves lower authentication latency, computational overhead, and communication overhead.

Full Text

Preamble

Vol. 39 No. 10
Application Research of Computers
ChinaXiv Cooperative Journal

Efficient Certificateless Authentication Scheme for LEO Satellite Networks

Zhang Yi, Wu Qi†, Zhou Shuangshuang, Jia Mengzhao
(School of Communication & Information Engineering, Chongqing University of

Posts and Telecommunications, Chongqing 400065, China)

Abstract: Existing authentication schemes for low earth orbit (LEO) satellite networks suffer from high latency due to centralized authentication and high computational overhead from complex bilinear mapping operations. To address these issues, this paper introduces a certificateless authentication model and proposes an efficient certificateless authentication scheme based on Gayathri' s scheme. The scheme unifies the user' s public key with their real identity, eliminating the need for third-party participation in the authentication process and reducing authentication delay. By constructing authentication messages using only a small number of point multiplication and point addition operations on elliptic curves, the scheme avoids bilinear mapping and reduces computational overhead. Security is proven under the random oracle model based on the elliptic curve discrete logarithm problem assumption. Finally, experimental simulations demonstrate that compared with existing LEO satellite identity authentication schemes, the proposed scheme achieves lower authentication delay, computational overhead, and communication overhead.

Key words: LEO satellite network; identity authentication; certificateless; random oracle model

0 Introduction

With socio-economic development, traditional terrestrial networks can no longer meet communication demands in special regions such as oceans, deserts, and mountainous areas. Satellite networks, characterized by wide coverage, long communication distances, and independence from geographical constraints, can effectively compensate for the limitations of ground-based networks. Among these, low earth orbit (LEO) satellite networks offer advantages including low latency, low communication power consumption, and high mobility [1], playing an increasingly important role in satellite networks.

LEO satellite networks feature exposed nodes, open channels, limited resources, highly dynamic network topology, and massive numbers of user terminals, making user access vulnerable to spoofing, malicious interception, and information theft. Consequently, secure access authentication for LEO satellite networks has become a focal point of concern. Unlike terrestrial networks, satellite network nodes have constrained resources and computing capabilities that cannot support complex computations or high communication overhead. Moreover, compared with medium and high earth orbit satellites, LEO satellite systems impose stricter requirements on transmission delay, real-time performance, and packet loss, necessitating low authentication latency. Additionally, frequent LEO satellite link handovers mean excessive authentication delays may cause connections to be interrupted before new satellite links are established, degrading communication quality. Therefore, authentication scheme design should

minimize computational overhead, authentication delay, and communication costs while ensuring security.

1 Preliminaries

1.1 Hard Problems

Elliptic Curve Discrete Logarithm Problem (ECDLP). Let be a generator of a cyclic group G of large prime order ; for any probabilistic polynomial-time algorithm , the probability of successfully solving the ECDLP problem is negligible, where the probability is taken over random selection from and the randomness of algorithm .

1.2 Certificateless Authentication Scheme Flow

A certificateless authentication scheme consists of five phases: Setup, Set-secret-key, Set-private-key, Sign, and Verify.

Setup: Executed by the KGC, taking a security parameter k as input to generate the system master key s and public parameters $params$.

Set-secret-key: Executed by user terminal devices, taking device identity as input to generate secret value x and public parameter X.

Set-private-key: Executed by the KGC, taking device identity and public parameter X as input to generate the user' s partial private key d.

Sign: Executed by any legitimate device, taking message m and the device' s private key pair to generate signature σ for the message.

Verify: Executed by any legitimate device, taking message m and signature σ as input and outputting a verification result (true/false).

1.3 Review of Gayathri et al. Scheme

Let signer V and verifier R be the main entities in the certificateless authentication scheme. According to Gayathri et al.' s scheme, V' s public-private key pair is . The public key consists of a partial public key generated by the PKG and a self-generated partial public key . Similarly, the private key comprises a partial private key generated by the PKG and a self-generated partial private key .

Sign Phase: V selects random numbers , then computes partial keys , obtains current timestamp , and generates signature before sending authentication request to verifier R.

Here, denotes a hash digest; denotes the x and y coordinates of a point on the elliptic curve; P, P_{pub}, and q represent the elliptic curve generator, system public key, and large prime number, respectively.

Verify Phase: Upon receiving V' s authentication request, R verifies whether Equation (1) holds. If it holds, authentication succeeds; otherwise, it fails.

1.4 Security Defects of Gayathri et al. Scheme

According to [9], certificateless cryptosystems face Type I adversaries capable of replacing legitimate users' public keys but without knowledge of the system master key. When obtains V' s public key , it forges a public key to replace , generating a forged signature . The specific interaction with R is as follows:

Sign: After obtaining V' s public key and identity identifier through a public channel:

Obtain current timestamp , select random number , forge public key as , and replace V' s public key. Where , then generate signature and finally send authentication request .

Verify: After receiving V' s authentication request, R:

a) Computes:

b) Verifies whether Equation (2) holds. If it holds, authentication succeeds; otherwise, it fails.

Since adversary forged V' s signature satisfies Equation (1), it can pass R' s verification. Therefore, has the capability to impersonate legitimate users, and Gayathri et al.' s scheme fails to achieve the claimed unforgeability against Type I adversaries. The proof is as follows:

2 Proposed Scheme

2.1 System Model

The system model of the scheme is shown in Figure 1. The main entities in LEO network authentication are briefly described below:

a) **KGC:** The manager of all entity information. It publishes public system parameters and is responsible for device information registration, generating public-private key pairs for legitimate devices.

b) **LEO Satellite:** Satellite network nodes, typically at altitudes of 500-2000km with propagation delays of approximately 20-40ms, primarily responsible for user access and data transmission. In this scheme, satellites possess certain computing capabilities and can verify user legitimacy.

c) **User Terminal:** Mainly includes mobile phones, vehicles, aircraft, and other ground terminals that require services from the LEO satellite network.

2.2 Scheme Flow

The proposed scheme consists of four phases: system initialization, secret value generation, partial private key generation, and mutual authentication. Symbols and their meanings are shown in Table 1.

2.2.1 System Initialization Phase

This phase is executed by the KGC. The KGC selects a cyclic group of order q (where $q > 2^k$, k is the security parameter), and P is a generator of . Define:

as the length of user identity identifier ID. Then the KGC randomly selects the system master key and computes the system public key . Finally, it publishes the public parameters .

2.2.2 Secret Value Generation Phase

This phase is executed separately by user terminals and satellites. Let user terminal device be U, which randomly selects secret value and computes . Then it sends to the KGC through a secure channel. Let satellite device be S, which randomly selects secret value and computes . Then it sends to the KGC through a secure channel.

2.2.3 Partial Key Generation Phase

This phase is executed by the KGC, user terminals, and satellites. Upon receiving user terminal device identity identifier and public parameter , the KGC randomly selects and computes . Then it returns to the device through a secure channel. After receiving the key from the KGC, the user terminal verifies whether holds to judge the legitimacy of the KGC-generated key. If verification fails, it reapplies to the KGC for a key. Otherwise, key generation succeeds. Finally, the user terminal U' s public key is and private key is . Similarly, the satellite' s public key is and private key is .

2.2.4 Mutual Authentication Phase

The mutual authentication process between user U (with identity identifier) and satellite S (with identity identifier) is as follows:

User U randomly selects , then generates signature and sends authentication request to satellite S.

Upon receiving the authentication request from user U, satellite S obtains current timestamp and checks whether . If not, the message is considered stale and authentication fails. Otherwise:

If satellite S successfully verifies user U's identity legitimacy, it randomly selects , then generates signature and returns authentication response .

After receiving the authentication response from satellite S, user U obtains current timestamp and checks whether . If not, the message is considered stale and authentication fails. Otherwise:

If both user U and satellite S successfully complete the above steps, mutual authentication is considered successful.

3 Security Analysis

3.1 Correctness Proof

The correctness analysis of signature verification in the authentication request phase is as follows: If the user' s signature is legitimate, the signature must satisfy the equation . From the user secret value generation phase and partial key generation phase, we know the user key satisfies the equation . Therefore, satellite can compute and verify using public parameters , , and :

a)
b)

Further, satellite can perform the following calculation:

During signature generation, the user' s signature satisfies the equation . Substituting the previous step yields:

3.2 Formal Security Proof

Theorem 1. Assume adversary can successfully forge a signature with non-negligible advantage within polynomial time. Then challenger can solve the ECDLP problem with probability , where represents the number of partial key generation queries, represents the number of secret value queries, and represents the number of signature queries.

Proof. Suppose adversary can forge a valid signature for target user with advantage in this scheme. Then for a given , challenger ' s goal is to compute .

The interaction between challenger and adversary proceeds as follows:

Initialization Phase: First runs the Setup algorithm to build the system, setting . Hash tables are populated with . Then public system parameters are published. Tables are established and maintained with contents , public key table with contents , and secret value table with contents . All tables are initially empty.

Oracle Query Phase: This phase involves the following oracle interactions between and :

Query: When inputs for inquiry. If exists in the corresponding tuple , return to ; otherwise, randomly select and return to , then save .

Query: When inputs for inquiry. If exists in the corresponding tuple , return to ; otherwise, randomly select and return to . Finally, save .

Partial Key Generation Query: When inputs for inquiry, first check if holds. If true, terminates the simulation. Otherwise, check if exists in the corresponding tuple . If it exists, return to ; otherwise, randomly select and return to . Finally, save .

Secret Value Query: When inputs for inquiry, first check if holds. If true, terminates the simulation. Otherwise, check if exists in the corresponding tuple . If it exists, return to ; otherwise, randomly select and return to , then save .

Public Key Generation Query: When inputs for inquiry, if exists in the corresponding tuple , return to ; otherwise, randomly select and query to obtain , then return to and add respectively.

Public Key Replacement: can choose a new public key to replace any legitimate user public key and save it to .

Signature Query: When makes inquiry with , first check if holds. If true, terminates the simulation. Otherwise, randomly select , then obtain through respectively. Since are randomly selected each time, each generated signature is random, and therefore signatures are not linkable.

Forward Security: Forward security ensures that authentication messages before and after user terminal compromise do not affect each other. In this scheme, even when user terminal is compromised, previously established session key information is not leaked because the session key is generated based on the Diffie-Hellman Key Exchange (DHKE) protocol and does not depend on the user terminal' s private key. Therefore, the proposed authentication scheme provides forward security.

a) **Anti-Replay Attack:** During authentication, both satellite and user terminal judge message freshness based on current timestamps. If the delay exceeds the system' s maximum tolerable threshold, the message is discarded, thereby preventing adversary replay attacks.

b) **Resistance to Man-in-the-Middle or Impersonation Attacks:** Attackers cannot forge user terminal signatures from intercepted authentication messages because the security foundation of authentication message construction is based on the hardness of the elliptic curve discrete logarithm problem.

Key Escrow Resilience: In the proposed scheme, user terminals and satellites' private keys include the partial private key computed by the KGC and the randomly selected by user terminals and satellites. Therefore, a malicious KGC cannot generate valid signatures without knowing . Thus, the proposed scheme is not affected by the key escrow problem.

Forgery: Finally, forges a signature for . If Equation (3) holds, succeeds in forgery, where is part of .

According to the Forking Lemma [15], can successfully forge another signature satisfying Equation (4) in polynomial time in the same manner but with different

.

Therefore, from Equations (3) and (4):

Probability Analysis: Let be the maximum number of partial key generation queries, the numb

The signature phase does not terminate (is not selected).

does not make partial key generation queries or secret value queries for the target identity ( ).

is a valid signature about .

Thus, the advantage can be expressed as . Therefore, the simulation does not terminate with probability .

Theorem 2. Assume adversary can successfully forge a signature with non-negligible advantage within polynomial time. Then challenger can solve the ECDLP problem with probability , where represents the number of public key generation queries, the number of secret value queries, and the number of signature queries.

Proof. The proof process is similar to Theorem 1.

3.3 Security Formal Analysis

Signature Unlinkability: In this scheme, user terminals and satellites randomly select each time, making each signature generation independent and thus providing signature unlinkability.

Forward Security: Forward security ensures that authentication messages before and after user terminal compromise do not affect each other. In this scheme, even when user terminal is compromised, previously established session key information is not leaked because the session key is generated based on the Diffie-Hellman Key Exchange (DHKE) protocol and does not depend on the user terminal' s private key. Therefore, the proposed authentication scheme provides forward security.

Anti-Replay Attack: During authentication, both satellite and user terminal judge message freshness based on current timestamps. If the delay exceeds the system' s maximum tolerable threshold, the message is discarded, thereby preventing adversary replay attacks.

Resistance to Man-in-the-Middle or Impersonation Attacks: Attackers cannot forge user terminal signatures from intercepted authentication messages because the security foundation of authentication message construction is based on the hardness of the elliptic curve discrete logarithm problem.

Key Escrow Resilience: In the proposed scheme, user terminals and satellites' private keys include the partial private key computed by the KGC and the randomly selected by user terminals and satellites. Therefore, a malicious KGC

cannot generate valid signatures without knowing . Thus, the proposed scheme is not affected by the key escrow problem.

4 Experimental Simulation

Computational overhead, authentication delay, and communication overhead are the most intuitive metrics for evaluating identity authentication schemes. This section compares the proposed scheme with recently published, highly secure access authentication schemes from three perspectives: computational overhead, authentication delay, and communication overhead. The selected comparison schemes are: the three-factor elliptic curve authentication scheme proposed in [7], the bilinear pairing-based authentication scheme proposed in [8], and the bilinear pairing-based certificateless authentication scheme proposed in [11].

4.1 Experimental Environment

The experimental environment uses Ubuntu 18.04.6 64-bit operating system running on a VMware virtual machine with 4GB RAM. The hardware environment is Intel i5-10210U 1.60GHz. The proposed authentication scheme is implemented on the Charm-crypto library with operations based on the underlying PCB library. Randomly simulating 100 runs of different cryptographic operations yields the results shown in Table 2.

Table 2. Running time of different operations (ms) - Bilinear pairing operation: - Elliptic curve point multiplication: - Elliptic curve point addition:

4.2 Computational Overhead and Authentication Delay Analysis

When comparing schemes, we primarily consider computational overhead from , , and operations, while ignoring ordinary hash operations and arithmetic operations due to their minimal time cost. For generality, we assume one-way transmission delay between user terminal and satellite and between satellite and NCC are both 20ms. As shown in Table 3, the proposed scheme does not involve computationally expensive operations. The signing and verification phases require only a small number of and operations, with total computational overhead of approximately 4.2ms. Compared with bilinear pairing-based schemes [8] (approximately 24.1ms) and scheme [11] (approximately 10ms), the proposed scheme demonstrates significant advantages in computational overhead. Compared with the non-bilinear pairing scheme [7] (which requires more operations, approximately 6.2ms), scheme [7] has higher computational overhead and additionally requires more interaction rounds. Therefore, the proposed scheme has the lowest computational overhead and is more efficient.

Authentication delay includes both computational overhead during identity authentication and propagation delay during message exchanges. As shown in Figure 2, due to using a small number of low-complexity elliptic curve point mul-

tiplication and point addition operations to construct signatures, the proposed scheme has minimal computational overhead. Moreover, based on the certificateless authentication model, it eliminates third-party participation in authentication, reducing the number of interactions and propagation delay. Therefore, the proposed scheme' s authentication delay is significantly lower than other schemes.

Table 3. Comparison of authentication costs | Scheme | Computational Overhead | |—-|————| | [7] | | | [8] | | | [11] | | | Ours | |

4.3 Communication Overhead Analysis

For convenient comparison, we assume device identity identifier length bytes, timestamp length 4 bytes, message length 20 bytes, and elements in positive integer domain occupy 20 bytes. Elements in cyclic groups G and G_1 occupy 20 bytes and 64 bytes respectively, so element lengths in G and G_1 are 40 bytes and 128 bytes respectively. Table 4 compares communication costs among different authentication schemes, showing that the proposed scheme has lower communication costs than other schemes.

Table 4. Comparison of communication costs | Scheme | Communication Length (Bytes) | |—-|————| | [7] | | | [8] | | | [11] | | | Ours | |

5 Conclusion

This paper proposes an efficient certificateless identity authentication scheme for LEO satellite networks. The scheme eliminates third-party participation during user authentication, reducing authentication delay, and avoids bilinear mapping in the authentication process, resulting in low computational overhead while maintaining high security. The scheme provides signature unlinkability, forward security, anti-replay attack resistance, resistance to man-in-the-middle or impersonation attacks, and key escrow resilience. However, there remains room for optimization in computational overhead, as both user terminals and satellites require certain computing capabilities. Future research will focus on constructing LEO satellite network identity authentication schemes with even lower computational complexity while maintaining high security strength.

References

[1] Yang Xin, Sun Zhili, Liu Huafeng, et al. Technology of new generation LEO satellite network and terrestrial MANET integration [J]. ZTE TECHNOLOGY JOURNAL, 2016, 22(4): 58-63.

[2] Cruickshank H S. A security system for satellite networks [C]// Fifth International Conference on Satellite Systems for Mobile Communications and Navigation, London: IET Press, 1996: 187-190.

[3] Zhang Yuanyuan, Chen Jianhua, Huang Baojun. An improved authentication scheme for mobile satellite communication systems [J]. International Journal of Satellite Communications and Networking, 2015, 33(2): 135-146.

[4] Saroj T, Gaba G S. A Lightweight Authentication Protocol based on ECC for Satellite Communication [J]. Pertanika Journal of Science & Technology, 2017, 25(4): 1317-1330.

[5] Zhu Hui, Chen Siyu, LI Fenghua, et al. User random access authentication protocol for low earth orbit satellite networks [J]. Journal of Tsinghua University (Science and Technology), 2019, 59(1): 1-8.

[6] Qi Mingping, Chen Jianhua, Chen Yitao. A secure authentication with key agreement scheme using ECC for satellite communication systems [J]. International Journal of Satellite Communications and Networking, 2019, 37(3): 234-244.

[7] Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications [J]. Computer Communications, 2019, 147: 85-97.

[8] Zhao Guofeng, Zhou Wentao, Xu chuan et al. A Secure identity authentication scheme for space-ground integrated network based on bilinear pairing [J]. Netinfo Security, 2020, 20(12): 33-39.

[9] Al-Riyami S S, Paterson K G. Certificateless public key cryptography [C]// International conference on the theory and application of cryptology and information security. Berlin: Springer Press, 2003: 452-473.

[10] Liu Yuchen, Zhang Aixin, Li Jianhua, et al. An anonymous distributed key management system based on CL-PKC for space information network [C]// 2016 IEEE international conference on communications (ICC). Kuala Lumpur: IEEE Press, 2016: 1-7.

[11] Wu Zhijun, Yang Yiming. BD-D1Sec: Protocol of security authentication for BeiDou D1 civil navigation message based on certificateless signature [J]. Computers & Security, 2021, 105: 102251.

[12] Zhou Yanwei, Yang Bo, Wang Qinglong. Secure certificateless signcryption scheme without bilinear pairing [J]. Journal of Software, 2017, 28(10): 2757-2768.

[13] Yang Xiaodong, Liu Rui, Chen Guilan, et al. Security analysis of a certificateless signcryption mechanism without bilinear mapping [C]// 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2020, 1: 2431-2434.

[14] Tedeschi P, Sciancalepore S, Eliyan A, et al. LiKe: Lightweight certificateless key agreement for secure IoT communications [J]. IEEE Internet of Things Journal, 2019, 7(1): 621-638.

[15] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures [J]. Journal of cryptology, 2000, 13(3): 361-396.

[16] Gayathri N B, Thumbur G, Reddy P V, et al. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks [J]. IEEE Access, 2018: 31808-31819.

[17] Xu Guangquan, Zhou Wenjuan. A Security-Enhanced Certificateless Aggregate Signature Authentication Protocol for InVANETs, in IEEE Network [J]. 2020, 34(2): 22-29.

Note: Figure translations are in progress. See original paper for figures.