Research on encryption, authentication and key update mechanism for CCSDS-TC protocol

Chen Hong*
School of Big Data, Chongqing Vocational College of Transportation, Chongqing, 402247, China

*Corresponding author e-mail: chen_honghit@163.com,

Abstract. In view of the shortcomings of the CCSDS-TC protocol key update mechanism, this paper proposes a satellite-ground key update scheme suitable for space communication. This article analyzes the encryption and authentication methods of the CCSDS-TC protocol, builds a satellite communication protocol simulation platform on OPNET, and implements the proposed satellite-ground key update scheme, encryption and authentication methods. The simulation test of the dynamic update of satellite-ground key and the simulation results of data security transmission denote that the proposed satellite-ground key update scheme in this paper has good security, scalability and low resource consumption, and can provide a secret key parameter which reveals important practical value.

1. Introduction

The various international space missions have widely adopted standards developed by the Consultative Committee for Space Data Systems (CCSDS) such as TC [1], TM and AOS. Considering the security threats faced by space missions, CCSDS released the Space Data Link Security (SDLS) protocol [2] in 2015 to provide security protection for communication data. However, CCSDS does not design a reasonable key management mechanism to realize the dynamic update of the key between the ground control center (GCC) and communication satellites which will cause great security risks.

Because Certificate Authority (CA) has three forms of existence in the space network topology, existing spatial key management algorithms can be divided into three categories, namely centralized control key management algorithms [3]-[5], distributed key management algorithm [6] and hierarchical group key management algorithm [7] [8]. The centralized control key management algorithm has the security problem of single point of failure. The disadvantage of distributed management algorithm is usually that the number of communication rounds is relatively large which is not suitable for spatial communication scenarios with large link delay and high bit error rate. The hierarchical group key management algorithm compromises these two schemes to avoid the single point of failure and reduce the communication calculation overhead. But it is suitable for scenarios where multi-level access control needs to be set. Therefore, this paper will focus on the security issues of CCSDS-TC protocol and proposes a satellite-ground key update scheme that conforms to the characteristics of the space information network. The proposed key update scheme will be applied to CCSDS-TC protocol to support and guarantee confidentiality, authentication and integrity of space communication.
2. Research on CCSDS-TC Protocol Security Mechanism

2.1. Analysis of encryption technology
The symmetric encryption algorithm used in the CCSDS-TC protocol is Advanced Encryption Standard (AES) [9]. The AES algorithm engraft substitution-permutation network (SPN) structure. Operations of each round consists of S-box substitution, row shifting, column mixing and round key addition. The encryption process of AES is illustrated in Figure 1 taking AES-128 as an example.

![AES encryption process](image)

**Figure 1.** AES encryption process

2.2. Analysis of message authentication mechanism
The typical message authentication mechanism adopted by the CCSDS-TC protocol is HMAC. HMAC is a technology that uses a one-way hash function to construct message authentication code (MAC) to confirm integrity and perform authentication. The construction method of HMAC is shown in formula (1) where \(ipad\) is a bit sequence formed by the cyclical bit sequence 00110110 and \(opad\) is formed by the cyclical bit sequence 01011100 whose length reach the group length of adopted one-way hash function.

\[
HMAC = hash((key \oplus ipad) \| hash((key \oplus opad) \oplus message))
\] (1)

The input of HMAC includes a message with arbitrary length and a shared key between the sender and the receiver. It can output fixed-length data called the MAC. CCSDS recommends the utilization of one-way hash function including SHA-224, SHA-256, SHA-384 and SHA-512.

2.3. Design of the satellite-ground key update mechanism
The satellite-ground key is an important communication parameter shared between the ground control center and communication satellite. The initial key \(IniKey\) will be pre-burned into the storage of satellite \(M_i\) \((i = 1, 2, ..., n)\). Let \(NewKey\) be the satellite-ground key to be updated whose binary sequence length is \(N\). The process of generating, distributing and updating of the satellite-ground key will adhere to the following steps.

Step1: Construct a bilinear map. GCC selects a safe large prime number \(q\) firstly, then selects a hypersingular elliptic curve \(E(F_p)\) defined on the finite field \(F_p = \{0,1,2, ..., p-1\}\) and \((G_1, +)\) is the \(q\)-
order cyclic group on $E(F_p)$ where $P$ is the generator of $G_1$. Finally, the multiplicative cyclic group $(G_2, \cdot )$ on the finite field is selected whose order is also $q$ to construct a bilinear map $e: G_1 \times G_1 \rightarrow G_2$.

Step2: Generate the public and private key pair of the system. GCC calculates the system public key $Q_{GCC}$ from formula (2) where $r$ is a random number in $Z_q^*$. Then GCC selects one-way hash functions $H_1: \{0, 1\}^* \rightarrow Z_q^*$ and $H_2: \{0, 1\}^* \rightarrow G_1$, and discloses parameter information $(q, G_1, G_2, e, P, Q_{GCC}, H_1, H_2)$.

$$Q_{GCC} = rP$$ (2)

Step3: Generate public-private key pairs for satellite nodes. The public-private key pair $<Q_i, S_i>$ of each satellite node can be calculated by GCC through formula (3) where $d_i$ expresses identity information of satellite node $M_i$.

$$\begin{cases} 
Q_i = H_1(d_i) \\
S_i = rQ_i 
\end{cases}$$ (3)

Step4: The form of the generating matrix of the LDPC code $C$ is displayed in formula (4) where $I$ is the $k$-th order identity matrix.

$$G = \left[ P \mid I_{k \times k} \right]$$ (4)

Step5: Calculate the satellite-ground key share. GCC calculates the satellite-ground key share of $n$ satellite nodes by formula (5) where $D$ is formed by connecting $NewKey$ and $k-1$ different $N$-dimensional column vectors.

$$T = (t_1, t_2, \cdots, t_{n-1}) = D \cdot G$$ (5)

Step6: Identity authentication of satellite-ground key shares. GCC randomly selects $P_i \in G_1$ and the integer $k$ in $Z_q^*$, and computes the signature information $\sigma_i = <\alpha_i, \beta_i > \in Z_q^* \times G_1$ by formula (6) where $y_i$ delivers the satellite-ground key share in ciphertext.

$$\begin{cases} 
b_i = e(P_i, P)^k \\
\alpha_i = H_1(y_i, b_i) \\
\beta_i = \alpha_i S_i + kP_i 
\end{cases}$$ (6)

Step7: Verify signature information. After receiving the signature data of satellite-ground key share $t_i$ sent by GCC, the satellite node $M_i$ calculates $b_i$ by formula (7) firstly and then calculates $H_i(y_i, b_i)$. If and only if $\alpha_i$ and $H_i(y_i, b_i)$ are equal, the signature verification can be passed, otherwise GCC needs to be notified to send the relevant data again.

$$b_i = e(\beta_i, P) e(Q_i, -Q_{GCC})^{\alpha_i}$$ (7)
Step8: Calculate the updated satellite-ground key. After the satellite $M_i$ exchanges the satellite-ground key share information with the participants in the qualified subset, it decrypts the satellite-ground key shares $t_j$ sent by other participants and then calculates the final updated satellite-ground key according to formula (8).

$$NewKey = \sum_{j=1}^{\mu} c_i t_j$$  \hspace{1cm} (8)

3. Results

3.1. The establishment of simulation model
The overall network model of the CCSDS-TC protocol security mechanism constructed in this paper is demonstrated in Figure 2 in the light of OPNET's modeling mechanism where ground node represents the ground control center node.

![Figure 2. Overall network model of CCSDS-TC protocol security mechanism](image)

This paper implements the CCSDS-TC protocol using the SDLS protocol on the OPNET platform. The format of its transmission frame is shown in Figure 3. The optional security guide is generally filled with the calculated message authentication code.

![Figure 3 Format of CCSDS-TC transmission frame with SDLS protocol](image)

3.2. Simulation analysis of the proposed ground-satellite key update scheme
In the OPNET simulation test, the hexadecimal 128-bit satellite-ground key regenerated by GCC is 52584cd3bb7157d126742c532b1f48be. The satellite-ground key shares of each satellite obtained through the raised scheme are cleared in Table 1. The hexadecimal representation of the satellite-ground key reconstructed by each satellite is the same as generated key by GCC.
Table 1. The satellite-ground key shares generated by GCC

| Number of satellite-ground key share | Data of satellite-ground key share (Hex) |
|-------------------------------------|----------------------------------------|
| $t_1$                               | 57671017070e5d515e632a82bba1a9d        |
| $t_2$                               | c3a79e8dc0517c2e946133a7a5a2a935        |
| $t_3$                               | 22a86a00612603bc4e66e5b82dd6984        |
| $t_4$                               | 279736c4dd59093c3471e369bd6a3a7        |
| $t_5$                               | 91f8d25c7eb202b6db2151ff48be6be18b    |
| $t_6$                               | 00000000000000000000000000000000      |
| $t_7$                               | 9074b11e6986d151977951d30b2073e9       |
| $t_8$                               | c713a1096e888c00c91a7b51b08e6974       |
| $t_9$                               | 70f0263da57546d61a2c9eb60c4213a        |
| $t_{10}$                             | c3a79e8dc0517c2e946133a7a5a2a935       |

It can be drawn from Table 1 that the proposed scheme can be executed correctly and the satellite-ground key is stored discretely to ensure the security of the satellite-ground key transmission in the space link.

### 3.3. Simulation analysis of encryption and authentication mechanism of CCSDS-TC protocol

The simulation results of AES encryption method to achieve safety remote control in CCSDS-TC protocol are shown in Figure 4. The communication key $52584cd3bb7157d126742c532bf48be$ between GCC and satellite is dynamically updated by the scheme in this paper. The simulation result of message authentication mechanism adopted by CCSDS-TC protocol is declared in Figure 5. The shared satellite-ground key guarantees the integrity of the remote control message.

#### AES encryption service of CCSDS-TC protocol (GCC)

Key(Hex): $52584cd3bb7157d126742c532bf48be$
Plaintext: How the lossless data compression was integrated into the CCSDS-based on-board data systems was studied.
Ciphertext(Hex): $8c9536f774170f301f2c219e4899f44d7e1da81e993d1ed94ad3a97e4b3e7ee9d8e6f7757010f7bda03b6f4fected3e5d0ff2186294e60db97c820715af6f22ad036c26fae4e423a1d38aab898e4ce60729da317d2f0ce2151bf03b0d8ae45d60b9d34dd1da$

#### AES decryption service of CCSDS-TC protocol (Satellite $M_3$)

Key(Hex): $52584cd3bb7157d126742c532bf48be$
Received ciphertext(Hex): $8c9536f774170f301f2c219e4899f44d7e1da81e993d1ed94ad3a97e4b3e7ee9d8e6f7757010f7bda03b6f4fected3e5d0ff2186294e60db97c820715af6f22ad036c26fae4e423a1d38aab898e4ce60729da317d2f0ce2151bf03b0d8ae45d60b9d34dd1da$
Recovered plaintext: How the lossless data compression was integrated into the CCSDS-based on-board data systems was studied.

#### HMAC authentication service of CCSDS-TC protocol (GCC)

Key(Hex): $52584cd3bb7157d126742c532bf48be$
Sent Message: How the lossless data compression was integrated into the CCSDS-based on-board data systems was studied.
MAC(Hex): $8f2404b3b93f7d1979eeb7d761ca4a7d32886b7b0c736ee6e33671e02268398c$

#### HMAC verification service of CCSDS-TC protocol (Satellite $M_4$)

Key(Hex): $52584cd3bb7157d126742c532bf48be$
MAC(Hex): $8f2404b3b93f7d1979eeb7d761ca4a7d32886b7b0c736ee6e33671e02268398c$
Received Message: How the lossless data compression was integrated into the CCSDS-based on-board data systems was studied.

Figure 4 Simulation result of AES encryption mechanism in CCSDS-TC protocol

Figure 5 Simulation result of message authentication mechanism in CCSDS-TC protocol
It can be concluded from the test results of Figure 4 and Figure 5 that the key update scheme proposed in this paper has important application value and can ensure the security of space remote control data.

4. Conclusion
This paper concentrates on that the SDLS protocol lacks a perfect key update mechanism for satellite-ground key. Firstly, this paper proposes an identity-based key update mechanism and decentralizes the transmission of satellite-ground key. Then the encryption, authentication and proposed key update method of CCSDS-TC protocol are designed and implemented on OPNET network simulation platform. Finally, the proposed satellite-ground key update method was simulated and analyzed. The simulation results indicate that the proposed satellite-ground key update scheme has low storage communication overhead and can provide an important key management mechanism for the CCSDS-TC protocol security technology.

References
[1] CCSDS. CCSDS 232.0-B-3 TC Space Data Link Protocol [S]. Washington, DC, USA: CCSDS Secretariat, National Aeronautics and Space Administration, 2015.
[2] CCSDS. CCSDS 355.0-B-1 Space Data Link Security Protocol [S]. Washington, DC, USA: CCSDS Secretariat, National Aeronautics and Space Administration, 2015.
[3] Karati A, Islam S H, Biswas G P, et al. Provably Secure Identity-Based Signcryption Scheme for Crowdsourced Industrial Internet of Things Environments [J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.
[4] Yang Y, Huang J, Chen J, et al. INAKA: Improved Authenticated Key Agreement Protocol Based on Newhope [J]. IEEE Access, 2020, PP (99): 1-1.
[5] Zhou J, Sun L Y, Song J D. Efficient Group Key Management for Non-reliable Link Networks [J]. Wireless Personal Communications, 2018, 98 (2): 1955-1973.
[6] Fakhrey H, Johnston M, Angelini F, et al. The Optimum Design of Location-Dependent Key Management Protocol for Multiple Sink WSN Using a Random Selected Cell Reporter [J]. IEEE Sensors Journal, 2018, 18(24): 10163-10173.
[7] Daghighi B, Kiah M L M, Iqbal S, et al. Host mobility key management in dynamic secure group communication [J]. Wireless Networks, 2018, 24(8): 3009-3027.
[8] Athmani S, Bilami A, Boubiche D E. EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for Heterogeneous WSNs [J]. Future Generation Computer Systems-the International Journal of Escience, 2019, 92: 789-799.
[9] Wegener F, Meyer L D, Moradi A. Spin Me Right Round Rotational Symmetry for FPGA-Specific AES: Extended Version [J]. Journal of Cryptology, 2020(3).