Security and Safety, Vol. 3, 2023030 (2024)
https://doi.org/10.1051/sands/2023030
sands.edpsciences.org

Security and Privacy for Space-Air-Ground Integrated Networks

Research Article OPEN ACCESS

Information Network

Enabling Space-Air integration: A Satellite-UAV networking authentication scheme

Sheng Li*, Jin Cao*, Xiaoping Shi, and Hui Li

The State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710126, China

Received: 30 June 2023 / Revised: 17 August 2023 / Accepted: 22 September 2023 / Published online: 31 January 2024

Abstract One of the goals of sixth-generation mobile networks (6G) is to achieve a larger network coverage area. Satellite networks enable global coverage and aerial nodes such as Unmanned Aerial Vehicle (UAV) can serve as a supplement to ground networks in remote environments. Therefore, 6G networks are gradually evolving towards Space-Air-Ground integrated networks. The combination of UAV networks and satellite networks is a research hotspot in the field of Space-Air integrated networks. However, the combination of UAV networks and satellite networks currently faces many challenges in terms of security. The characteristics of large propagation delay and unstable communication links in satellite networks make them vulnerable to various attacks, including eavesdropping, tampering, and impersonation. Meanwhile, existing research on UAV networks mainly focuses on UAV-Ground networking authentication mechanisms, which are not suitable for resource-constrained nodes in the Space-Air integration scenario. Therefore, based on elliptic curve public key cryptography and Chebyshev polynomial, we propose a secure networking authentication scheme for satellite nodes and UAV nodes in the Space-Air integration scenario. The security analysis indicates that our scheme possesses security attributes such as mutual authentication, key agreement, identity anonymity, unlinkability, perfect forward-backward security, and resistance against various protocol attacks, among other security properties. Performance analysis also indicates certain advantages of our scheme over existing schemes in terms of signaling, bandwidth, and computational overhead.

Keywords Space-Air-Ground integrated networks, Chebyshev polynomial, Elliptic curve public key cryptography system, UAV, Satellite, Networking authentication

Citation Li S, Cao J, Shi X and Li H. Enabling Space-Air integration: A Satellite-UAV networking authentication scheme. Security and Safety 2024; **3**: 2023030. https://doi.org/10.1051/sands/2023030

1 Introduction

With the gradual commercialization of the fifth-generation mobile networks (5G), the academic community has begun researching the sixth-generation mobile networks (6G). Due to limitations in the coverage of ground information networks, they struggle to meet the wireless access demands in various scenarios, especially in areas such as mountains, oceans, and deserts where infrastructure development is lacking. In comparison, SATellite (SAT) networks possess extensive coverage and can compensate for the shortcomings of ground networks [1–3]. Additionally, aerial nodes such as Unmanned Aerial Vehicles

[*] Corresponding authors (email: sli_01@stu.xidian.edu.cn (Sheng Li); caoj897@gmail.com (Jin Cao))

(UAVs) and airships can provide instant network access services for devices that are distant from terrestrial information networks [4–6]. Therefore, 6G networks are gradually evolving towards the direction of Space-Air-Ground integrated networks [6, 7].

UAVs possess characteristics such as maneuverability, rapid mobility, and cost-effectiveness, making them valuable in various military and civilian applications. Clustering multiple UAVs allows them to overcome individual resource limitations, thereby expanding their utilization across different domains. For example, they are widely used in tasks such as exploring dangerous areas and efficiently collecting various types of data. UAVs have become widely used and important aerial nodes. In the UAV-Ground network architecture, UAVs require stable communication and data links to receive commands, transmit data, and maintain contact with the ground control station. However, in certain special scenarios such as ocean shipping, remote area exploration, and disaster-stricken emergency rescue, UAVs may face issues with weak or unavailable communication signals, limiting their operational range and capabilities. Satellite networks have features such as global signal coverage, high flexibility, and high resilience. Combining them with UAV networks can expand the coverage range of UAV networks and enhance the robustness of UAV networks.

The combination of UAV networks and satellite networks currently faces many challenges in terms of security. Satellite networks have characteristics such as highly heterogeneous network structures, significant propagation delays, and unstable communication links, which make them vulnerable to malicious attacks such as message eavesdropping and tampering, impersonation attacks, and unauthorized access [4–6, 8–11]. On the other hand, current research on networking authentication for UAV networks mostly focuses on the networking authentication mechanism between UAVs and ground networks. Moreover, many of these existing schemes suffer from the issue of high signaling overhead between nodes. These schemes are difficult to fully adapt to the Space-Air integrated scenario. Therefore, the secure networking between satellites and UAVs has become a research hotspot.

Considering the characteristics of high latency between nodes, complex network topology, and limited node resources in the Space-Air integrated networks, we propose a secure networking authentication scheme for satellite nodes and UAV nodes in the Space-Air integration scenario, based on elliptic curve public key cryptography and Chebyshev polynomial. It mainly consists of two stages, SAT-HAP networking authentication stage and the SAT-UAV networking authentication stage, which respectively achieve networking authentication between SAT nodes and high altitude platform (HAP) nodes, as well as networking authentication between SAT nodes and UAV nodes assisted by HAP nodes. The contributions of this scheme are as follows:

(1) First, we propose a certificateless networking authentication protocol for satellite nodes and HAP nodes based on elliptic curve cryptography and Chebyshev polynomials. Our protocol enables efficient mutual authentication between SAT and HAP, and secure session key agreement between SAT and HAP based on the Chebyshev polynomial, thereby establishing a secure communication link between SAT and HAP.

(2) Next, we propose a certificateless networking authentication protocol for satellite nodes and UAV nodes based on elliptic curve cryptography and Chebyshev polynomials. In this protocol, efficient mutual authentication and session key agreement are achieved between SAT and UAV, as well as between UAV and HAP. Considering the scenario of the UAV group, in this protocol, the HAP acts as the group leader to aggregate the signaling of the UAVs. Through hierarchical management of UAV-HAP-SAT, it reduces signaling overhead and avoids massive authentication signaling conflicts, making it suitable for the Space-Air integration scenario.

(3) Through informal security analysis and formal security simulation using Scyther, the results indicate that our proposed scheme can achieve mutual authentication, node identity anonymity, key agreement, unlinkability, perfect forward-backward security, resistance against replay attacks, resistance against man-in-the-middle attacks, resistance against impersonation attacks, and other security properties. When compared with existing related schemes, our proposed scheme demonstrates superior security performance. Furthermore, by comparing our scheme with existing schemes in terms of signaling, bandwidth, and computational overhead, the comparative results indicate that our scheme exhibits good performance advantages.

The remaining parts of this article are organized as follows. Section 2 reviews the relevant literature in recent years. Section 3 introduces the Chebyshev polynomial. Section 4 presents the system model, threat model, and requirements. Section 5 introduces the networking authentication scheme proposed by us for UAVs and satellites. In Section 6, we analyze the security of the scheme through informal security analysis and formal security simulation. In Section 7, we analyze the performance of the scheme from three aspects: signaling, bandwidth, and computational overhead. Finally, we present future prospects in Section 8 and conclude in Section 9.

2 Related work

In this section, we will introduce some related research works on node authentication in Space-Air integrated networks.

Semal *et al.* [12] proposed a secure group authentication protocol for UAVs based on certificateless cryptography. The protocol can achieve secure key provisions for group members and avoid certificate management and key escrow problems. However, it consumes high computational cost due to the use of bilinear pairing operations. Srinivas *et al.* [13] proposed a lightweight authentication scheme based on temporal credentials, named TCALAS, to achieve mutual authentication and key agreement among the UAV, ground station, and users. In addition, it can ensure the anonymity of the user. However, Ali *et al.* [14] pointed out that the scheme does not have extendibility and cannot resist the tracking attack. They proposed another improved protocol, named iTCALAS. Alladi *et al.* [15] proposed two lightweight authentication protocols based on Physical Unclonable Functions (PUF) for UAVs, named SecAuthUAV, including an authentication protocol between the UAV and ground station and another authentication protocol between UAVs. However, they cannot ensure forward/backward security on the session key. Alladi *et al.* [16] also presented another authentication protocol based on PUF in tri-layered Software-Defined UAV networks, named PARTH. The protocol can achieve authentication among the mini drones, the leader drones, and the ground station. However, the protocol consumes high communication overhead due to multi-round interactions. Lei *et al.* [17] proposed an optimized lightweight authentication protocol based on the Chinese remainder theorem to achieve mutual authentication among sensor, UAV, access point, and server. The protocol can resist general attacks and ensure forward/backward security. In order to reduce the computational load of resource-constrained nodes, the protocol offloaded the complex computational processes to resource-rich server nodes. In order to resist location forgery attacks on UAVs, Melo *et al.* [18] proposed a secure identity and location validation scheme based on the signature technology and the rationality detection mechanism of UAV swarm movement. By combining two mechanisms, the protocol can detect intruders who cannot follow the expected trajectory and improve the accuracy of detection of malicious drones.

There are also some other schemes based on blockchain technology to solve high authentication latency for UAVs [19, 20]. However, some problems such as block mining, data anchoring, and fast real-time synchronization of authentication transactions all add to the overall overhead and development difficulty.

These schemes only achieve networking authentication for the communication between the UAV and the ground nodes (such as sensors, ground station, access point, server, *et al.*). There are few networking authentication schemes involving the UAV and the space nodes. In addition, most of the above authentication schemes have the problems of frequent interactions between nodes and lead to high signaling overhead. However, there is naturally higher time latency in Space-Air integrated networks than that in UAV networks due to the propagation distance. Therefore, the number of interactions is a key factor that affects the performance of the authentication scheme.

3 Background knowledge

3.1 Extended Chebyshev polynomials

Chebyshev polynomials, also known as Chebyshev chaotic mapping, are a sequence of polynomials defined recursively. In this article, we utilize the extended Chebyshev polynomials [21], which is defined as follows:

Let's set $n \in Z^*, x \in Z_q^*$, q is a large prime number, the cosine definition of the nth-order extended Chebyshev polynomials is:

$$T_n(x) = \cos(n \cdot \arccos(x))(\text{mod} q). \tag{1}$$

The recursive formula is as follows:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \, (\mathrm{mod} q), \tag{2}$$

where $T_0(x) = 1, T_1(x) = x$.

Next, we will introduce the commutative property and the challenging problems associated with the extended Chebyshev polynomials that we will be using in our article.

(1) The extended Chebyshev polynomials satisfy the commutative property, as follows:

$$T_m \left(T_n(x)\right) = T_n \left(T_m(x)\right). \tag{3}$$

(2) The challenging problems related to extended Chebyshev polynomials [22–26] are as follows:

(a) Chebyshev polynomials based discrete logarithm problem: The value of the Chebyshev polynomial as $y = T_n(x) \bmod q$, given the knowledge of y, x, and the large prime number q, it is impossible to solve for n in linear time.

(b) Chebyshev polynomials based computational Diffie-Hellman problem: If x, $T_m(x) \bmod q$, and $T_n(x) \bmod q$ are known, it is not possible to compute $T_m(T_n(x)) \bmod q$ or $T_n(T_m(x)) \bmod q$ in linear time.

Note: For simplicity, we will abbreviate $T_m(x) \bmod q$ as $T_m(x)$ in the remaining part of the article.

4 System model, threat model, and requirements

4.1 System model

The standalone operational capability of resource-constrained UAVs is relatively low. Therefore, in order to fully leverage the advantages of easy deployment and strong maneuverability of UAVs, they are often deployed in a cluster work mode in practical operations, thereby enhancing the processing capability of the UAV system. Additionally, in certain special scenarios such as ocean shipping, remote area exploration, and emergency rescue, the ground network architecture faces challenges in providing network access for UAVs. Therefore, as shown in Figure 1, we propose a Satellite-UAV networking architecture for the Space-Air integrated networks. In this architecture, UAVs establish secure links with SATellite (SAT) nodes with the help of High Altitude Platform (HAP) nodes, thereby enhancing the system's coverage range, service capability, and resilience against damage.

(1) UAV Nodes: UAV nodes are terminal devices with limited computing and storage capabilities that perform various tasks in the airspace, such as data collection, monitoring, and image capture. In this architecture, a certain number of UAV nodes can form a homogeneous or heterogeneous UAV cluster network based on the tasks.

(2) HAP Nodes: High-altitude platform nodes, such as airplanes, airships, and balloons, are devices that possess strong computational and storage capabilities, as well as extended endurance.

(3) SAT Nodes: In this model, satellite nodes primarily refer to satellites in Low Earth orbit (LEO) satellite networks. LEO satellite networks operate at a close distance to the Earth's surface and have short orbital periods.

(4) Registration Center (RC): In our system model, the RC is responsible for the registration of SAT nodes, HAP nodes, and UAV nodes. It maintains the public and private key information of the system and all nodes.

(5) Ground Station (GS): Ground station is used for communication between the ground and satellites.

(6) Terrestrial Control Center (TCC): The TCC is responsible for controlling and managing the satellite network.

(7) Base Station (BS): In this model, the base station primarily serves the purpose of forwarding information between the TCC and RC.

4.2 Threat model

In this paper, we employ the Dolev-Yao model [27] to analyze the security of the proposed protocol. The Dolev-Yao model assumes an open network channel, where adversaries have the ability to eavesdrop, modify, and intercept messages. Within this model, adversaries are capable of executing various protocol attacks, including impersonation attacks, replay attacks, and man-in-the-middle attacks, and so on.

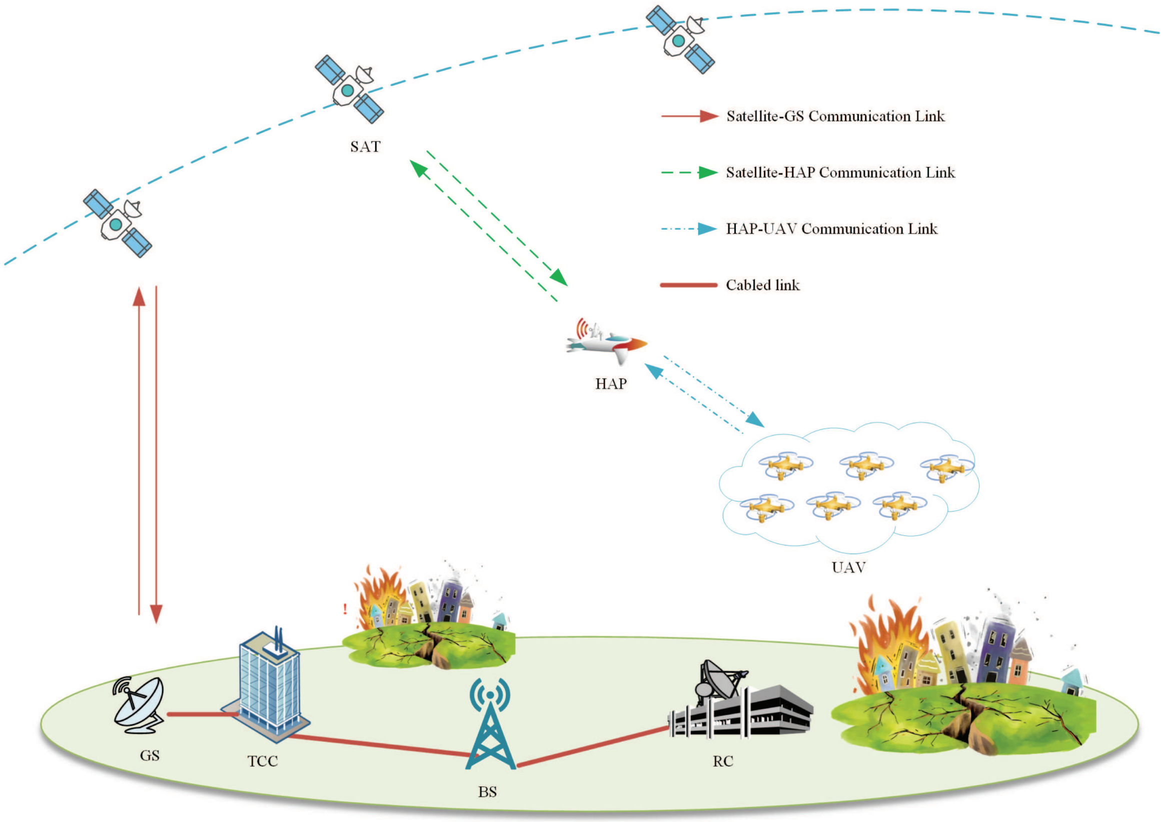

SAT
Satellite-GS Communication Link
Satellite-HAP Communication Link
HAP-UAV Communication Link
Cabled link
HAP
UAV
GS
TCC
BS
RC

Figure 1. System model

4.3 Security requirements

Considering that there is no secure communication link between SAT nodes, HAP nodes, and UAV nodes, the satellite-UAV networking architecture needs to fulfill the following security requirements to ensure the secure transmission of data over the air interface:

(1) Mutual authentication: Mutual identity authentication is required among the participating UAV nodes, satellite nodes, and HAP nodes to ensure that the nodes involved in forming the satellite-UAV network are legitimate.
(2) Session key agreement: After completing mutual authentication, the nodes need to engage in session key agreement to ensure communication security.
(3) Perfect forward/backward secrecy: Attackers are unable to deduce previous or subsequent session keys even if the long-term secrets used in session key exchange are compromised.
(4) Anonymity and unlinkability: It is necessary to ensure the confidentiality of node identities during the communication process, preventing attackers from linking the same entity's identity across different communication sessions.
(5) Resistance to various protocol attacks: The system should be capable of defending against replay attacks, reducing the risk of adversaries capturing and replaying expired messages. It should provide protection against man-in-the-middle attacks, preventing attackers from intercepting and tampering with legitimate messages. Additionally, it should offer resistance to impersonation attacks, ensuring that the identities of legitimate entities cannot be forged.

4.4 Performance requirements

We should consider the specific characteristics of the nodes and scenarios, as well as the corresponding performance requirements, as follows:

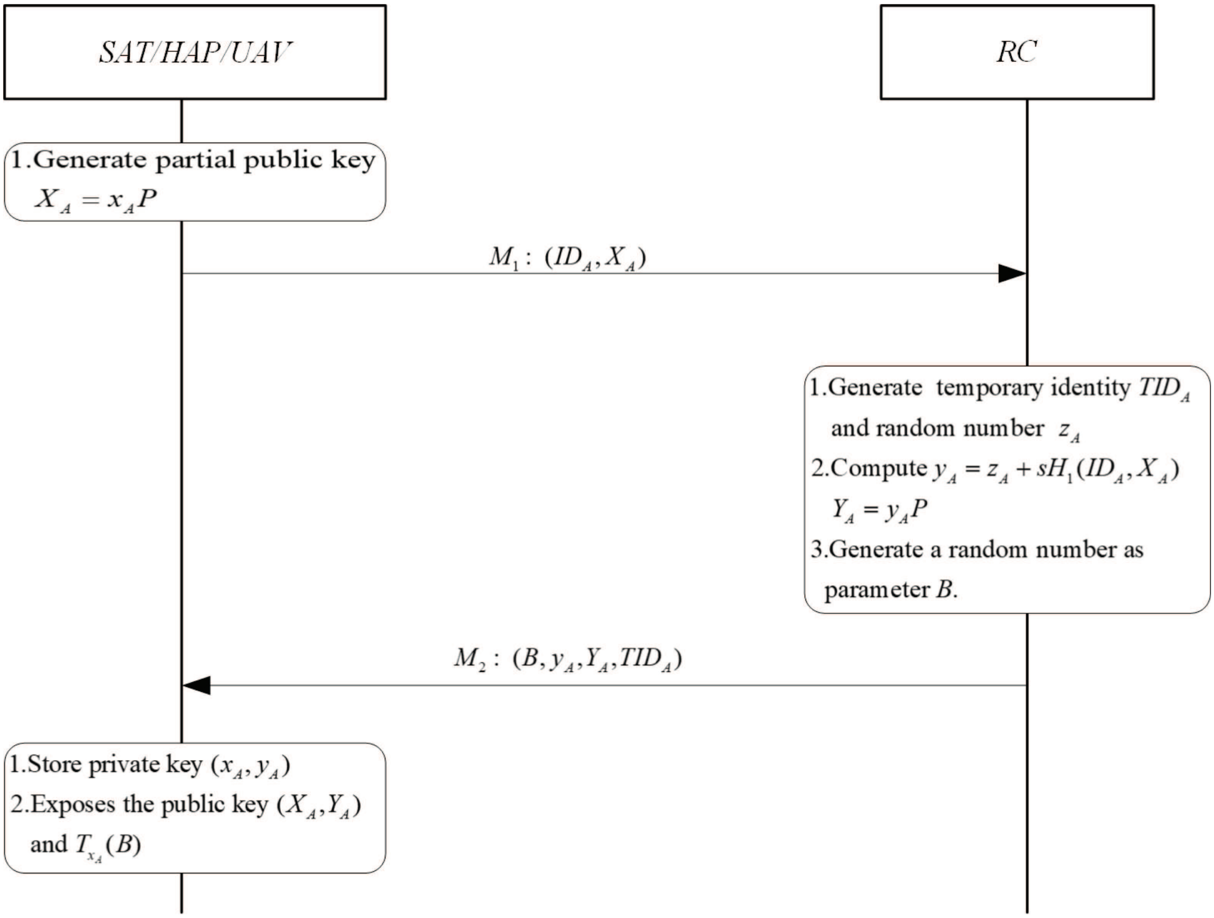

SAT/HAP/UAV
RC
1.Generate partial public key
$X_A = x_A P$
$M_1: (ID_A, X_A)$
1.Generate temporary identity TID_A
and random number z_A
2.Compute $y_A = z_A + sH_1(ID_A, X_A)$
$Y_A = y_A P$
3.Generate a random number as
parameter B.
$M_2: (B, y_A, Y_A, TID_A)$
1.Store private key (x_A, y_A)
2.Exposes the public key (X_A, Y_A)
and $T_{x_A}(B)$

Figure 2. Registration process

(1) Limited resources in nodes: The computing resources of the nodes are limited, thus requiring the design of lightweight secure networking protocols to reduce authentication overhead.
(2) High propagation delay: Due to the long distance between UAV and SAT nodes, there is a significant propagation delay. Therefore, it is important to minimize the signaling interactions in the networking authentication protocol.

5 Proposed scheme

This section presents the proposed secure networking authentication scheme for SAT nodes and UAV nodes in the Space-Air integration scenario. The scheme is divided into three stages, including the node registration stage, SAT-HAP networking authentication stage, SAT-UAV networking authentication stage.

5.1 Node registration stage

Nodes (including SAT nodes, HAP nodes, UAV nodes) need to complete the registration process at the RC initially. The specific registration process is illustrated in Figure 2.

(1) First, the RC selects a large prime number q. Then, an elliptic curve $E_p(a, b)$ and a series of points on the curve are chosen to form a cyclic group G of order q. Let P be a generator of this group. RC selects a random number $s \in \mathbb{Z}_q^*$ as its private key and then computes the public key is:

$$PK = sP \bmod q. \tag{4}$$

Then, RC selects a hash function H. Lastly, the parameters $\{q, G, P, PK, H\}$ are publicly disclosed to the entire system.

(2) The node A (SAT node, UAV node, and HAP node) generates a random number x_A and computes a partial public key as follows:

$$X_A = x_A P \bmod q. \tag{5}$$

The node then sends a registration request message (ID_A, X_A) to the RC.

(3) Once RC receives the request, it generates a random number $\mathrm{TID_A}$ as the temporary identity for node A. It then generates another random number z_A and computes a partial private key for node A as follows:

$$y_{\mathrm{A}} = z_A + sH(\mathrm{ID}_A, X_A) \bmod q. \tag{6}$$

Furthermore, the RC generates a partial public key for the node:

$$Y_{\mathrm{A}} = y_A P \bmod q. \tag{7}$$

RC stores $(\mathrm{ID}_A, \mathrm{TID}_A, y_A, X_A, Y_A)$, and sends $(B, y_A, Y_A, \mathrm{TID}_A)$ to node A in a secure environment, where B is a random number generated by the RC for the subsequent networking authentication process.

(4) Once node A receives the response, it securely stores the private key pair (x_A, y_A). Subsequently, the node A publicly exposes the public key pair (X_A, Y_A) and $T_{x_A}(B)$.

5.2 SAT-HAP networking authentication stage

In our architecture, the HAP nodes serve as devices with strong computing and storage capabilities, as well as a longer endurance compared to UAV nodes. HAP, capable of stable hovering at a specified position, is utilized in our scheme to assist in the authentication between UAV nodes and satellite nodes. To accomplish this, the HAP node needs to establish a secure connection with the satellite. In this section, we will introduce how to achieve mutual authentication between the HAP node and the SAT node. The specific process of authentication is depicted in Figure 3.

(1) First, HAP obtains the current timestamp t_{h1}. Subsequently, HAP selects a random number r_1 and compute $T_{r_1}(m)$, where $m = H(\mathrm{TID_{SAT}})$. Then, HAP computes the digital signature Jsat:

$$c = H(t_{h1}, T_{x_{\mathrm{HAP}}}(B), T_{r_1}(m)), \tag{8}$$

$$Jsat = x_{\mathrm{HAP}}(X_{\mathrm{SAT}} + Y_{\mathrm{SAT}} + cP) \bmod q. \tag{9}$$

Finally, the message $(\mathrm{TID_{HAP}}, Jsat, T_{r_1}(m), t_{h_1})$ is sent to the SAT node.

(2) After receiving the message, SAT first checks the freshness of the message using the timestamp t_{h1}. Then, SAT calculates $Jsat'$ to verify the authenticity of the HAP signature:

$$c' = H\left(t_{h_1}, T_{x_{\mathrm{HAP}}}(B), T_{r_1}(m)\right), \tag{10}$$

$$Jsat' = \left(x_{\mathrm{SAT}} + y_{\mathrm{SAT}} + c'\right) X_{\mathrm{HAP}} \bmod q. \tag{11}$$

If $Jsat = Jsat'$, SAT considers the signature verification to be successful. Then, SAT derives the temporary session key TSK_{HS} based on the Chebyshev polynomials using the following equation:

$$\mathrm{TSK}_{HS} = T_{x_{\mathrm{SAT}}}\left(T_{x_{\mathrm{HAP}}}(B)\right) \bmod q. \tag{12}$$

SAT obtains the current timestamp t_{s1}, selects a random number r_2 and compute $T_{r_2}(m)$, and calculates the authentication response value Rsat:

$$Rsat = H\left(\mathrm{TSK_{HS}}, \mathrm{TID_{SAT}}, t_{s1}, t_{h1}, T_{r_2}(m)\right) \tag{13}$$

Finally, SAT sends $(\mathrm{TID_{SAT}}, Rsat, t_{s1}, T_{r_2}(m))$ as the authentication response message to HAP and computes session key $\mathrm{SK_{HS}} = T_{r2}(T_{r1}(m)) \bmod q$.

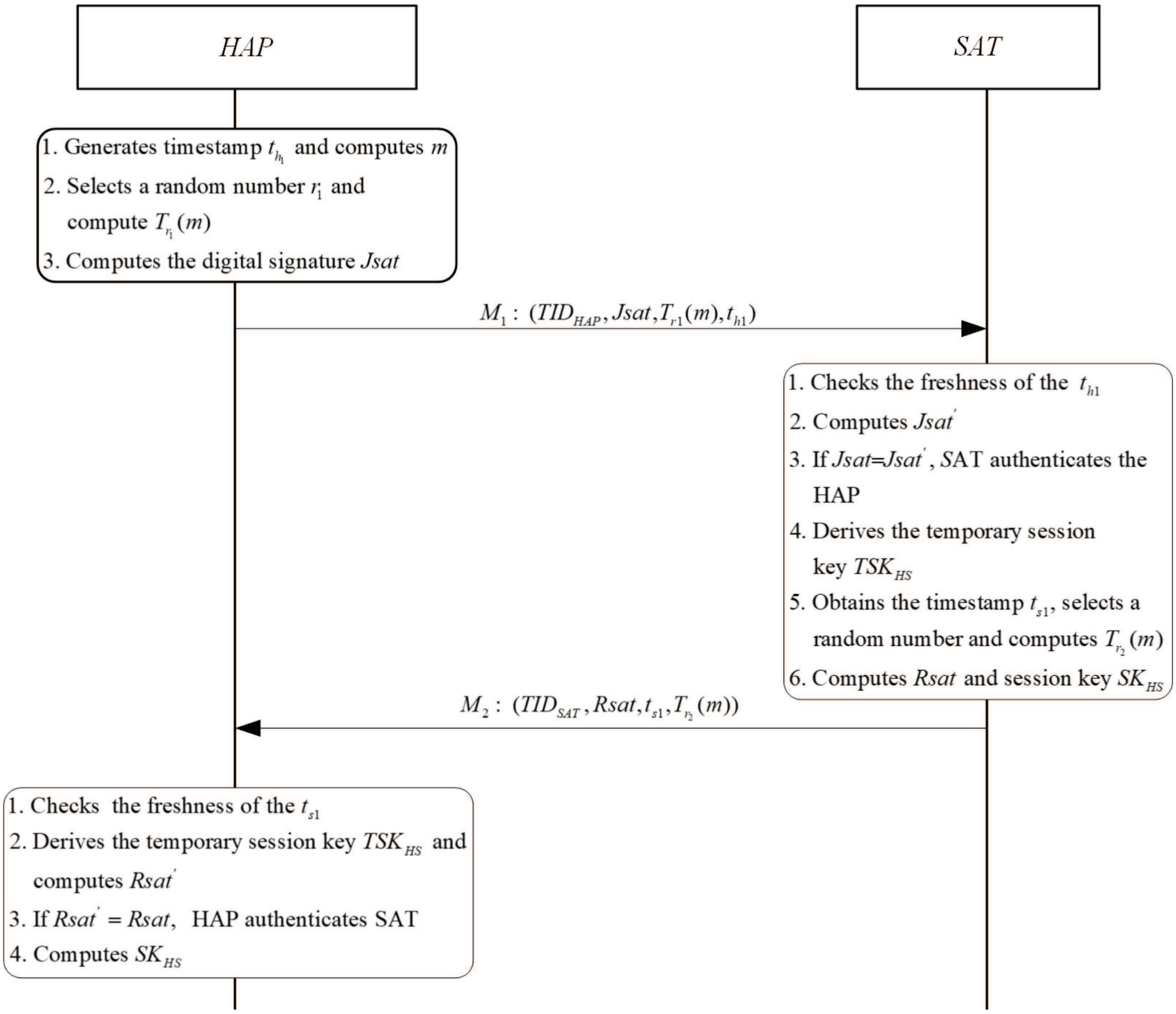

HAP
SAT
1. Generates timestamp t_{h_1} and computes m
2. Selects a random number r_1 and compute $T_{r_1}(m)$
3. Computes the digital signature $Jsat$
$M_1 : (TID_{HAP}, Jsat, T_{r1}(m), t_{h1})$
1. Checks the freshness of the t_{h1}
2. Computes $Jsat'$
3. If $Jsat=Jsat'$, SAT authenticates the HAP
4. Derives the temporary session key TSK_{HS}
5. Obtains the timestamp t_{s1}, selects a random number and computes $T_{r_2}(m)$
6. Computes $Rsat$ and session key SK_{HS}
$M_2 : (TID_{SAT}, Rsat, t_{s1}, T_{r_2}(m))$
1. Checks the freshness of the t_{s1}
2. Derives the temporary session key TSK_{HS} and computes $Rsat'$
3. If $Rsat' = Rsat$, HAP authenticates SAT
4. Computes SK_{HS}

Figure 3. Satellite-HAP networking authentication process

(3) After receiving the message, HAP first checks the freshness of the message using the timestamp t_{s1}. Then HAP generates a temporary session key $\mathrm{TSK}_{\mathrm{HS}}$ by the following equation:

$$\mathrm{TSK}_{\mathrm{HS}} = T_{x_{\mathrm{HAP}}}\left(T_{x_{\mathrm{SAT}}}(B)\right) \bmod q. \tag{14}$$

Then, HAP computes $Rsat'$ using the temporary session key $\mathrm{TSK}_{\mathrm{HS}}$. If $Rsat = Rsat'$, it implies that identity authentication is considered successful. Finally, HAP computes $\mathrm{SK}_{\mathrm{HS}} = T_{r_2}\left(T_{r_1}(m)\right) \bmod q$.

5.3 SAT-UAV networking authentication stage

After mutual authentication between the HAP and SAT, this section presents a security networking and authentication mechanism for UAV group and satellite networks assisted by the HAP in the Space-Air integration scenario. Firstly, UAV nodes autonomously initiate authentication requests to the HAP. Subsequently, the HAP aggregates and forwards these requests to a SAT node. Finally, these UAV nodes accomplish mutual identity authentication and session key agreement with both the HAP node and SAT node. Specific authentication steps can be found in the flowchart shown in Figure 4.

(1) First, UAV_i obtains the current timestamp t_{ui}. Subsequently, UAV_i selects a random number r_i and compute $T_{r_i}(m)$, where $m = H(\mathrm{TID}_{\mathrm{SAT}})$. Then $\mathrm{UAV_i}$ computes the signatures $J\mathrm{hap}_i$ and $J\mathrm{sat}_i$ to

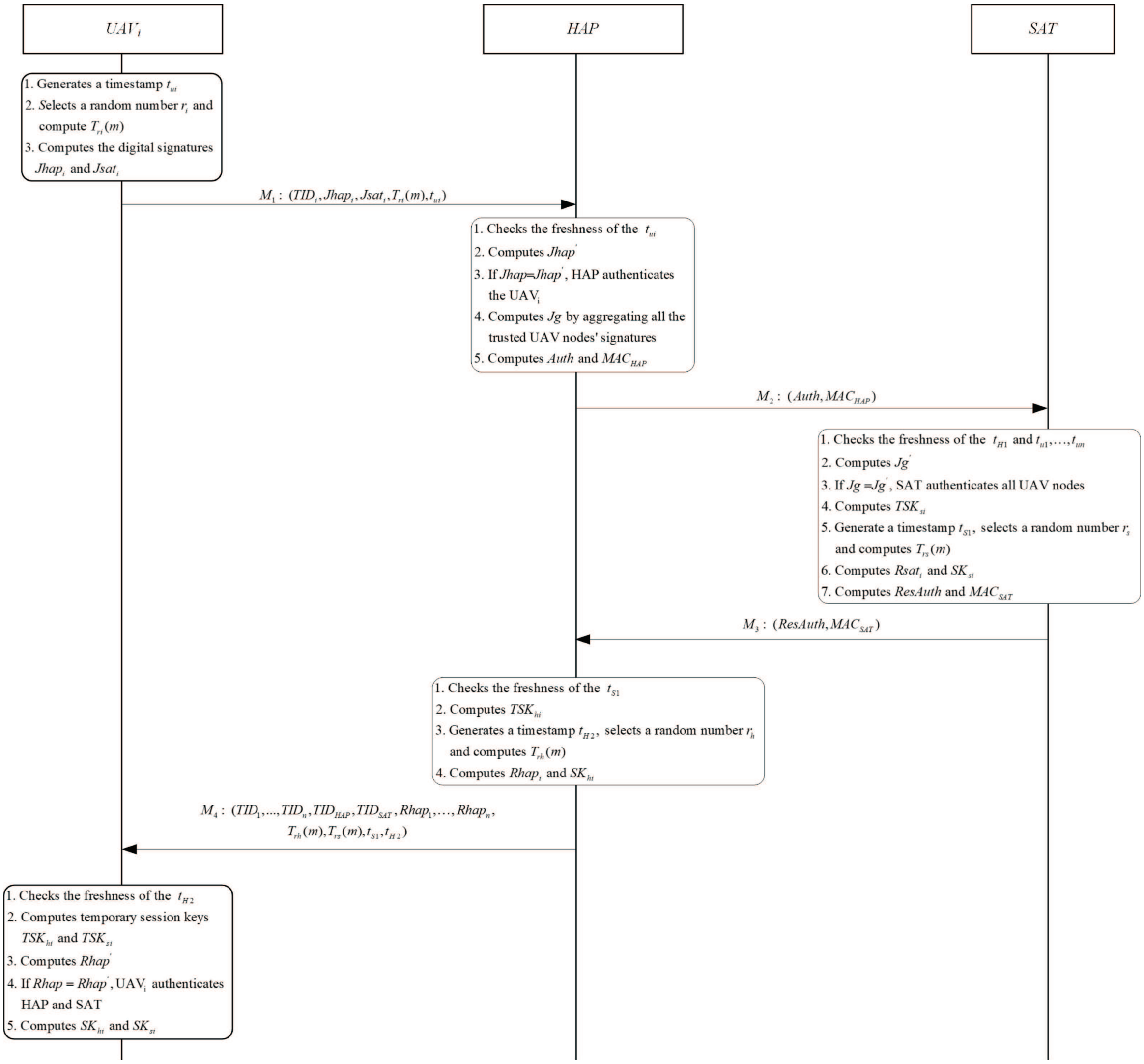

UAV_i
HAP
SAT
1. Generates a timestamp t_{ui}
2. Selects a random number r_i and compute $T_{ri}(m)$
3. Computes the digital signatures $Jhap_i$ and $Jsat_i$
M_1: $(TID_i, Jhap_i, Jsat_i, T_{ri}(m), t_{ui})$
1. Checks the freshness of the t_{ui}
2. Computes $Jhap'$
3. If $Jhap$=$Jhap'$, HAP authenticates the UAV_i
4. Computes Jg by aggregating all the trusted UAV nodes' signatures
5. Computes $Auth$ and MAC_{HAP}
M_2: $(Auth, MAC_{HAP})$
1. Checks the freshness of the t_{H1} and $t_{u1},\ldots,t_{un}$
2. Computes Jg'
3. If Jg =Jg', SAT authenticates all UAV nodes
4. Computes TSK_{si}
5. Generate a timestamp t_{S1}, selects a random number r_s and computes $T_{rs}(m)$
6. Computes $Rsat_i$ and SK_{si}
7. Computes $ResAuth$ and MAC_{SAT}
M_3: $(ResAuth, MAC_{SAT})$
1. Checks the freshness of the t_{S1}
2. Computes TSK_{hi}
3. Generates a timestamp t_{H2}, selects a random number r_h and computes $T_{rh}(m)$
4. Computes $Rhap_i$ and SK_{hi}
M_4: $(TID_1,...,TID_n, TID_{HAP}, TID_{SAT}, Rhap_1,\ldots,Rhap_n, T_{rh}(m), T_{rs}(m), t_{S1}, t_{H2})$
1. Checks the freshness of the t_{H2}
2. Computes temporary session keys TSK_{hi} and TSK_{si}
3. Computes $Rhap'$
4. If $Rhap = Rhap'$, UAV_i authenticates HAP and SAT
5. Computes SK_{hi} and SK_{si}

Figure 4. Satellite-UAV networking authentication process

be used for HAP and SAT.

$$c_i = H(t_{ui}, T_{x_i}(B), T_{r_i}(m)), \tag{15}$$

$$J\text{hap}_i = x_i(X_{\text{HAP}} + Y_{\text{HAP}} + c_i P) \bmod q, \tag{16}$$

$$J\text{sat}_i = x_i(X_{\text{SAT}} + Y_{\text{SAT}} + c_i P) \bmod q. \tag{17}$$

Finally, the message $(\text{TID}_i, J\text{hap}_i, J\text{sat}_i, T_{r_i}(m), t_{ui})$ is sent to the HAP node.

(2) After receiving the message, HAP first checks the freshness of the message using the timestamp t_{ui}. Then, HAP calculates $J\text{hap}_i'$ to verify the signature:

$$c_i' = H\left(t_{ui}, T_{x_i}(B), T_{r_i}(m)\right), \tag{18}$$

$$J\text{hap}_i' = \left(x_{\text{HAP}} + y_{\text{HAP}} + c_i'\right) X_i \bmod q. \tag{19}$$

If $J\text{hap}_i = J\text{hap}_i'$, HAP considers UAV_i to be a trusted node. After a certain time interval, HAP obtains the current timestamp t_{H1} and aggregates all the trusted UAV nodes' signatures using the session key SK_{HS} that has been previously negotiated with the SAT node. The aggregated result is:

$$Jg = J\text{sat}_1 \oplus \ldots \oplus J\text{sat}_n. \tag{20}$$

Finally, HAP sends $(\mathrm{Auth}, \mathrm{MAC}_{\mathrm{HAP}})$ to the SAT node, where $\mathrm{Auth} = \mathrm{Enc}(\mathrm{SK}_{\mathrm{HS}}, \mathrm{TID}_1, \ldots, \mathrm{TID}_n, \mathrm{TID}_{\mathrm{HAP}}, T_{r_1}(m), \ldots, T_{r_n}(m), Jg, t_{u1}, \ldots, t_{un}, t_{H1})$ and $\mathrm{MAC}_{\mathrm{HAP}} = H(\mathrm{Auth}, \mathrm{SK}_{\mathrm{HS}})$. *Auth* is generated by HAP using SK_{HS} for encryption. *Auth* enables the encrypted transmission of message content. $\mathrm{MAC}_{\mathrm{HAP}}$ is a message authentication code based on $\mathrm{SK}_{\mathrm{HS}}$, which ensures the integrity of messages.

(3) After receiving a message, the SAT node first verifies the freshness of the message by checking timestamps t_{H1} and $t_{u1}, \ldots, t_{un}$. Then, SAT computes the aggregate signature Jg' to verify the legitimacy of each UAV node.

$$c_i{}' = H\left(t_{u_i}, T_{x_i}(B), T_{r_i}(m)\right), \tag{21}$$
$$J\mathrm{sat}_i' = \left(x_{\mathrm{SAT}} + y_{\mathrm{SAT}} + c_i'\right) X_i \bmod q, \tag{22}$$
$$Jg' = J\mathrm{sat}_1' \oplus \ldots \oplus J\mathrm{sat}_n{}'. \tag{23}$$

If $Jg = Jg'$ holds, SAT considers each corresponding UAV node to be trusted. Then, SAT derives the temporary session key TSK_{si} between SAT and $\mathrm{UAV}_{\mathrm{i}}$ based on the Chebyshev polynomial using the following equation:

$$\mathrm{TSK}_{si} = T_{x_{\mathrm{SAT}}}\left(T_{x_i}(B)\right) \bmod q. \tag{24}$$

SAT obtains the current timestamp t_{S1}, selects a random number r_s and compute $T_{r_s}(m)$, where $m = H(\mathrm{TID}_{\mathrm{SAT}})$. Then SAT calculates the authentication response value $R\mathrm{sat}_i$:

$$R\mathrm{sat}_i = H\left(\mathrm{TSK}_{si}, \mathrm{TID}_i, \mathrm{TID}_{\mathrm{SAT}}, t_{S1}, t_{u1}, T_{r_s}(m)\right). \tag{25}$$

Finally, SAT sends $(\mathrm{ResAuth}, \mathrm{MAC}_{\mathrm{SAT}})$ as the authentication response message to HAP and computes session key $\mathrm{SK}_{si} = T_{rs}(T_{ri}(m)) \bmod q$ between SAT and $\mathrm{UAV}_{\mathrm{i}}$, where $\mathrm{ResAuth} = \mathrm{Enc}(\mathrm{SK}_{\mathrm{HS}}, \mathrm{TID}_1, \ldots, \mathrm{TID}_n, \mathrm{TID}_{\mathrm{SAT}}, R_{\mathrm{sat}_1}, \ldots, R\mathrm{sat}_n, T_{r_s}(m), t_{S1})$ and $\mathrm{MAC}_{\mathrm{SAT}} = H(\mathrm{ResAuth}, t_{H1}, \mathrm{SK}_{\mathrm{HS}})$. ResAuth is generated by SAT using $\mathrm{SK}_{\mathrm{HS}}$ for encryption. This enables the encrypted transmission of message content. $\mathrm{MAC}_{\mathrm{SAT}}$ is a message authentication code based on $\mathrm{SK}_{\mathrm{HS}}$, which ensures the integrity of messages sent by SAT.

(4) After receiving the message, HAP first determines the freshness of the message by checking the timestamp t_{S1}. Then, HAP generates a temporary session key TSK_{hi} by the following equation:

$$\mathrm{TSK}_{hi} = T_{x_{\mathrm{HAP}}}\left(T_{x_i}(B)\right) \bmod q. \tag{26}$$

Subsequently, HAP obtains the current timestamp t_{H2}, selects a random number r_h and compute $T_{r_h}(m)$, where $m = H(\mathrm{TID}_{\mathrm{SAT}})$. Then HAP generates the authentication response value:

$$Rhap_i = H\left(\mathrm{TSK}_{hi}, t_{H2}, R\mathrm{sat}_i, T_{r_h}(m)\right). \tag{27}$$

Finally, HAP broadcasts this message $(\mathrm{TID}_1, \ldots, \mathrm{TID}_n, \mathrm{TID}_{\mathrm{HAP}}, \mathrm{TID}_{\mathrm{SAT}}, R\mathrm{hap}_1, \ldots, R\mathrm{hap}_n, T_{r_h}(m), T_{r_s}(m), t_{S1}, t_{H2})$ and computes $\mathrm{SK}_{hi} = T_{rh}(T_{ri}(m)) \bmod q$.

(5) After receiving the message, UAV nodes first determine the freshness of the message based on the t_{H2}. Then, based on the received parameters, UAV_i nodes generate temporary session keys TSK_{hi} and TSK_{si} using the following equations:

$$\mathrm{TSK}_{hi} = T_{x_i}\left(T_{x_{\mathrm{HAP}}}(B)\right) \bmod q \tag{28}$$
$$\mathrm{TSK}_{si} = T_{x_i}\left(T_{x_{\mathrm{SAT}}}(B)\right) \bmod q \tag{29}$$

Then, UAV_i computes $R\mathrm{hap}_i'$ using the session key TSK_{hi} and TSK_{si}. If $R\mathrm{hap}_i = R\mathrm{hap}_i'$, the UAV_i has accomplished mutual identity authentication with HAP and SAT. Finally, UAV_i nodes computes session keys $\mathrm{SK}_{hi} = T_{ri}(T_{rh}(m)) \bmod q$ and $\mathrm{SK}_{si} = T_{ri}(T_{rs}(m)) \bmod q$ for HAP and SAT respectively.

Note: After completing the process in these two stages, secure connections have been established among nodes (SAT, HAP, and UAV), and they initiate sessions. Before the end of this session, the SAT node will select different random numbers as the new temporary identities for the UAV and HAP nodes and will select a random number to update the system parameter B. Finally, the SAT will send the aforementioned parameters to the UAV, HAP, and RC.

6 Security analysis

6.1 Informal security analysis

The proposed scheme in this paper primarily includes the SAT-HAP networking authentication stage and the SAT-UAV networking authentication stage. As the principles of the authentication protocols in these two stages are similar, this section primarily analyzes the security of the SAT-UAV networking authentication stage to assess the security of our proposed scheme.

(1) Achieving mutual authentication among SAT, HAP, and UAV nodes: In our scheme, we employ a signature-based authentication mechanism for the authentication of HAP nodes by satellite nodes, authentication of UAV nodes by satellite nodes, and authentication of UAV nodes by HAP nodes. Specifically, HAP and UAV nodes utilize their respective private keys during the signature generation process, ensuring that the signatures cannot be forged by attackers without knowledge of the signer's private key. Additionally, the recipient's public key is used during the signature calculation process, thus preventing attackers from conducting man-in-the-middle attacks. Taking the signature $J\text{sat}$ sent by HAP to the SAT as an example, we illustrate how to verify the signature.

$$\begin{aligned} J\text{sat} &= x_{\text{HAP}}(X_{\text{SAT}} + Y_{\text{SAT}} + cP) \bmod q \\ &= x_{\text{HAP}}(x_{\text{SAT}}P + y_{\text{SAT}}P + cP) \bmod q \\ &= x_{\text{HAP}}(x_{\text{SAT}} + y_{\text{SAT}} + c)P \bmod q \\ &= X_{\text{HAP}}(x_{\text{SAT}} + x_{\text{SAT}} + c) \bmod q. \end{aligned} \tag{30}$$

Equation (30) illustrates how SAT utilizes HAP's public key and SAT's private key to verify the signature of HAP. From this, the satellite unilaterally authenticates the UAV. Similarly, SAT unilaterally authenticates UAV, and HAP unilaterally authenticates UAV.

In the process of HAP authenticating SAT, UAV authenticating HAP, and UAV authenticating SAT, we employ a different mechanism. Let's illustrate the mechanism using HAP authenticating SAT as an example. After authenticating HAP, the SAT generates an authentication response value $R\text{sat}$, which is generated using the key $\text{TSK}_{\text{HS}} = T_{x_{\text{SAT}}}(T_{x_{\text{HAP}}}(B)) \bmod q$. The x_{SAT} in TSK_{HS} is the SAT's private key, making it resistant to forgery. Based on the commutative property of Chebyshev polynomials, HAP can calculate $\text{TSK}_{HS} = T_{x_{\text{HAP}}}(T_{x_{\text{SAT}}}(B)) \bmod q$ and verify the SAT's identity by checking the correctness of $R\text{sat}$. Similarly, UAV unilaterally authenticates HAP, and UAV unilaterally authenticates SAT. In conclusion, our solution successfully achieves mutual authentication between SAT, HAP and UAV nodes.

(2) Achieving key agreement: We illustrate the key agreement process between HAP and SAT as an example. The agreement of the session key $\text{SK}_{\text{HS}} = T_{r_2}(T_{r_1}(m)) \bmod q = T_{r_2}(T_{r_1}(m)) \bmod q$ is realized through the Diffie-Hellman (DH) problem based on the Chebyshev polynomial. The value of the session key SH_{HS} is solely determined by m, the randomly generated r_1 and r_2 from HAP and SAT respectively, as well as the corresponding $T_{r1}(m)$ and $T_{r2}(m)$. SAT and HAP can ensure the integrity of $T_{r1}(m)$, $T_{r2}(m)$ and authenticate the identity of the sender through private key signature and the hash value based on the temporary key ($R\text{sat}$). Even when $T_{r1}(m)$, $T_{r2}(m)$ and m are known, it is infeasible for an attacker to infer the values of r_1 and r_2 within linear time. HAP and SAT can uniquely derive the same key SH_{HS} based on $T_{r1}(m)$, $T_{r2}(m)$, ensuring the exclusivity of the key derivation process. Similarly, key establishment has been achieved between UAV and SAT, as well as between UAV and HAP.

(3) Perfect forward-backward security: During each session, HAP and SAT will choose new random numbers r_1 and r_2 to generate the session key SK_{HS}. Additionally, deriving x from $T_x(m)$ and m is extremely difficult. These two factors ensure that even in the event of leakage of the long-term master key, the past session keys or future session keys will not be compromised. This achieves perfect forward and backward secrecy in terms of key security.

(4) Achieving identity anonymity and unlinkability: During the authentication process of the proposed scheme, each participating node adopts a temporary identity, which is refreshed upon session completion. This ensures the attainment of anonymity for node identities within the scheme. Furthermore, in subsequent authentication instances, nodes employ new temporary identities, preventing adversaries from discerning whether the messages originate from the same node. As a result, the scheme achieves the desirable property of unlinkability.

Table 1. Comparison of security properties

Security properties	Our scheme	Scheme [29]	Scheme [30]	Scheme [31]
Mutual authentication	✓	✓	✓	✓
Key agreement	✓	✓	×	✓
Perfect forward-backward security	✓	×	×	✓
Identity anonymity	✓	✓	✓	✓
Unlinkability	✓	✓	✓	✓
Resilience against various protocol attacks	✓	✓	✓	✓
Avoiding third-party trust escrow issues	✓	×	×	×

(5) Resilience against replay attacks: Each message in the proposed scheme is equipped with a timestamp, which is protected from tampering by attackers through the use of signatures, hashing based on temporary session keys or session keys. Therefore, it ensures the freshness of each message, thereby preventing the occurrence of replay attacks.

(6) Resilience against man-in-the-middle attacks: In a Man-in-the-Middle Attack, an attacker impersonates an intermediary between the communicating parties during the communication process. The attacker can intercept and manipulate the content of messages without being detected by the communicating parties. In our proposed scheme, the session key agreement process between the two nodes incorporates private key signatures and hash values based on temporary keys to ensure the correspondence between the session key agreement parameters and the identity of the sender. Taking HAP and SAT as an example, the private key signature Jsat guarantees the authenticity of $T_{r1}(m)$ as provided by HAP, while Rsat ensures the authenticity of $T_{r2}(m)$ being provided by SAT. So our scheme effectively defends against man-in-the-middle attacks.

(7) Resilience against impersonation attacks: An impersonation attack refers to the act of an attacker impersonating a legitimate node's identity in order to gain unauthorized access. Our proposed scheme achieves mutual authentication between nodes through the use of private key signatures and hash value based on temporary keys. Taking HAP and SAT as an example, the private key signature Jsat ensures that SAT can authenticate HAP, while Rsat ensures that HAP can authenticate SAT. As a result, attackers are unable to carry out impersonation attacks.

(8) Avoiding third-party trust escrow issues: During the node registration process, RC is only responsible for computing partial public and private keys of the nodes. Since RC does not possess the complete public and private keys of the nodes, it can avoid third-party escrow issues.

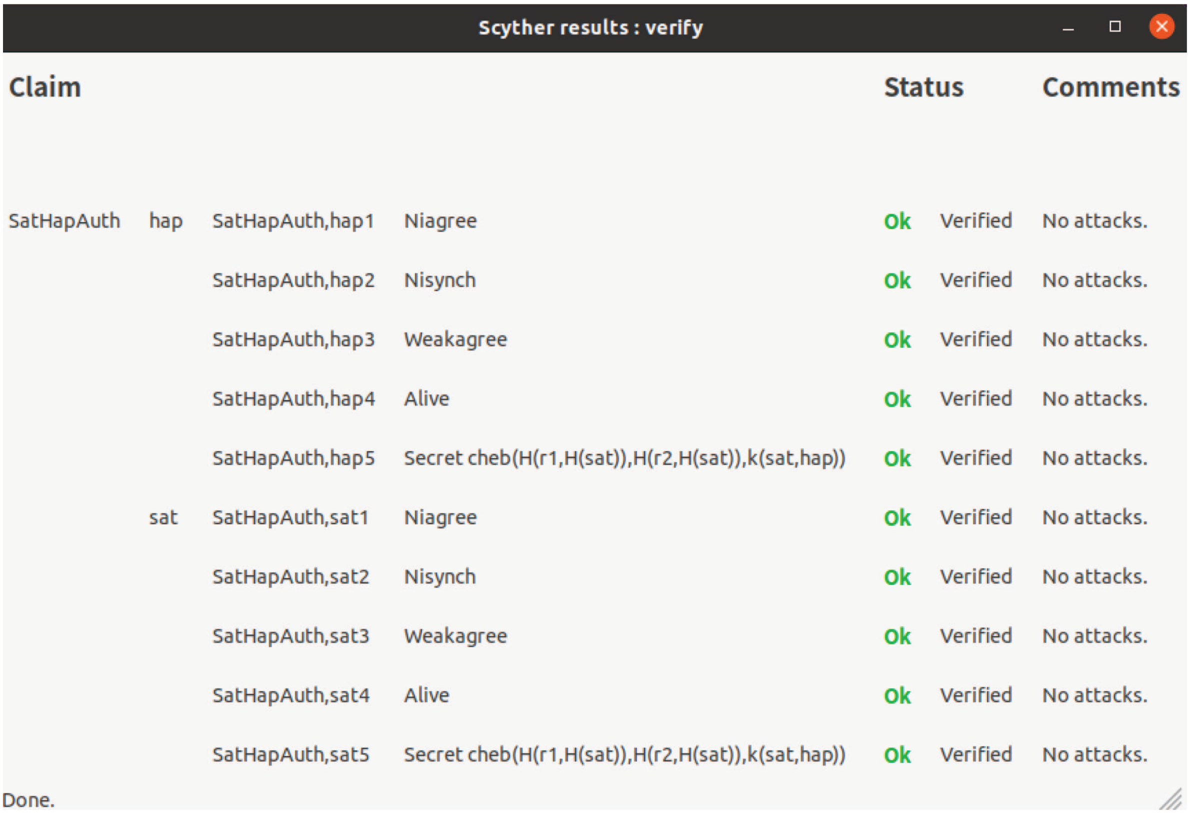
Finally, we compared the proposed scheme with other existing schemes in terms of all the aforementioned security properties. As shown in Table 1, our protocol exhibits superior security compared to other schemes.

6.2 Formal security analysis

In this section, we use a tool called Scyther [28] to assess the security of our proposed protocol. Scyther is a formal security analysis tool based on the SPDL language, which supports various threat models, including the Dolev-Yao model used in our paper. We can model the protocol using events, such as using a *claim* event to describe the security properties of our scheme's objectives and using *send* event and *recv* event to describe the interaction processes in our protocol. Through simulation analysis, we can determine whether our protocol meets the expected security properties.

Due to the node registration stage being executed in a secure environment, we primarily analyze the protocols in two stages: the SAT-HAP networking authentication stage and the SAT-UAV networking authentication stage. In the modeling of the SAT-HAP networking authentication stage, there are two participating roles: hap and sat. In the SAT-UAV networking authentication stage, there are three roles: uav, hap, and sat. Here, uav represents the UAV node, hap represents the HAP node, and sat represents the SAT node. We validate them from five dimensions: Niagree, Nisynch, Weakagree, Alive, and Secret.

As shown in Figures 5 and 6, the Secret indicates that the keys between our HAP and SAT, UAV and HAP, as well as UAV and SAT are secure. The Weakagree and Alive demonstrate that our nodes have



Claim				Status		Comments
SatHapAuth	hap	SatHapAuth,hap1	Niagree	Ok	Verified	No attacks.
		SatHapAuth,hap2	Nisynch	Ok	Verified	No attacks.
		SatHapAuth,hap3	Weakagree	Ok	Verified	No attacks.
		SatHapAuth,hap4	Alive	Ok	Verified	No attacks.
		SatHapAuth,hap5	Secret cheb(H(r1,H(sat)),H(r2,H(sat)),k(sat,hap))	Ok	Verified	No attacks.
	sat	SatHapAuth,sat1	Niagree	Ok	Verified	No attacks.
		SatHapAuth,sat2	Nisynch	Ok	Verified	No attacks.
		SatHapAuth,sat3	Weakagree	Ok	Verified	No attacks.
		SatHapAuth,sat4	Alive	Ok	Verified	No attacks.
		SatHapAuth,sat5	Secret cheb(H(r1,H(sat)),H(r2,H(sat)),k(sat,hap))	Ok	Verified	No attacks.

Done.

Figure 5. The verification result of Satellite-HAP networking authentication stage

achieved mutual authentication. The Niagree and Nisynch ensure the message synchronization among nodes in our scheme. The simulation results verify that the two networking authentication protocols can achieve mutual identity authentication, key establishment, and resist common protocol attacks such as replay attacks and man-in-the-middle attacks.

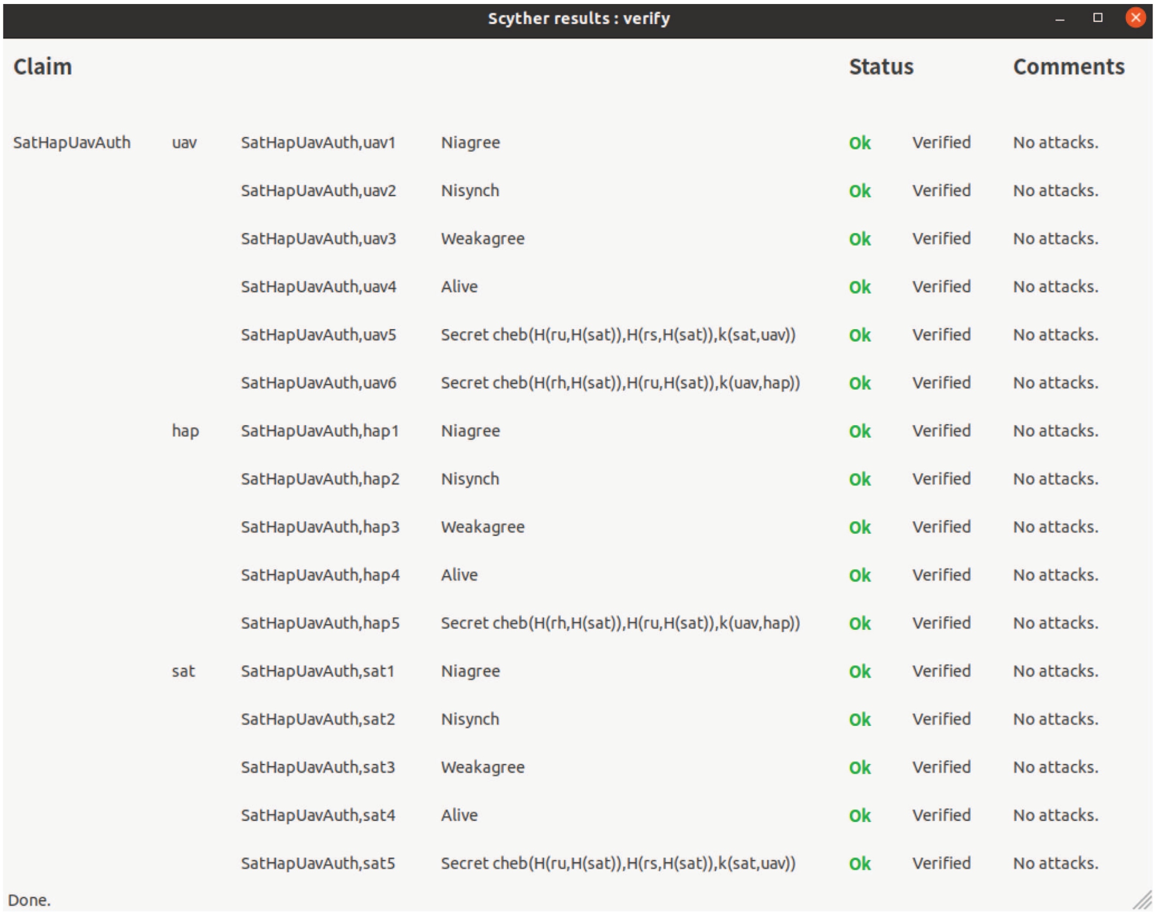
7 Performance analysis

To achieve secure networking between the SAT node and UAV nodes in the Space-Air integrated networks, our proposed scheme consists of two main stages: the SAT-HAP networking authentication stage and the SAT-UAV networking authentication stage. In this section, we compare our scheme with existing schemes [29–31] in terms of signaling, bandwidth, and computational overhead. To objectively assess the performance impact of each authentication scheme, we assume that after completing a networking authentication between the SAT-UAV node and HAP node, the HAP node assists in conducting group authentication for n UAV nodes, and we calculate the overall overhead during this authentication process.

7.1 Signaling overhead

In the context of Space-Air integrated networks, the large distance between unmanned aerial vehicle (UAV) and satellite nodes results in increased transmission delays. Additionally, due to the clustering nature of UAV operations, the large amount of authentication signaling can potentially lead to signaling conflicts. Moreover, UAV resources are limited, and the transmitted signals are susceptible to interference. Therefore, schemes with lower signaling overhead tend to demonstrate better performance in practical applications.

Table 2 presents the signaling overhead of our proposed scheme and other relevant schemes. Our SAT-HAP networking authentication stage requires 2 signaling exchanges and the SAT-UAV networking



```
Claim                                                                                                   Status              Comments

SatHapUavAuth   uav   SatHapUavAuth,uav1   Niagree                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,uav2   Nisynch                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,uav3   Weakagree                                                     Ok     Verified     No attacks.
                      SatHapUavAuth,uav4   Alive                                                         Ok     Verified     No attacks.
                      SatHapUavAuth,uav5   Secret cheb(H(ru,H(sat)),H(rs,H(sat)),k(sat,uav))             Ok     Verified     No attacks.
                      SatHapUavAuth,uav6   Secret cheb(H(rh,H(sat)),H(ru,H(sat)),k(uav,hap))             Ok     Verified     No attacks.
                hap   SatHapUavAuth,hap1   Niagree                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,hap2   Nisynch                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,hap3   Weakagree                                                     Ok     Verified     No attacks.
                      SatHapUavAuth,hap4   Alive                                                         Ok     Verified     No attacks.
                      SatHapUavAuth,hap5   Secret cheb(H(rh,H(sat)),H(ru,H(sat)),k(uav,hap))             Ok     Verified     No attacks.
                sat   SatHapUavAuth,sat1   Niagree                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,sat2   Nisynch                                                       Ok     Verified     No attacks.
                      SatHapUavAuth,sat3   Weakagree                                                     Ok     Verified     No attacks.
                      SatHapUavAuth,sat4   Alive                                                         Ok     Verified     No attacks.
                      SatHapUavAuth,sat5   Secret cheb(H(ru,H(sat)),H(rs,H(sat)),k(sat,uav))             Ok     Verified     No attacks.
Done.
```

Figure 6. The verification result of Satellite-UAV networking authentication stage

Table 2. Comparison of signaling and bandwidth overhead

	Signaling overhead	Bandwidth overhead (bits)
Our scheme	$n + 5$	$1728n + 2432$
Scheme [29]	$4n + 2$	$2816n + 1408$
Scheme [30]	$6n + 3$	$6592n + 3296$
Scheme [31]	$3n + 2$	$5184n + 2592$

authentication stage requires $(n + 3)$ exchanges. Therefore, the overall signaling overhead of our scheme can be represented as $(n + 5)$ exchanges. Figure 7 illustrates the variation of signaling overhead for each scheme with respect to the number of UAV nodes. In order to present a clearer and more intuitive comparison of our overhead with other schemes, we have employed a logarithmic scale in Figure 7. This approach also applies to Figures 8 and 9. It can be observed that our scheme exhibits better performance in terms of signaling overhead due to the utilization of HAP node aggregation for authentication signaling, which significantly reduces the number of signaling.

7.2 Bandwidth overhead

In achieving security equivalent to AES-128 bit [32], assuming the public key length based on finite field cryptographic system is 3072 bits, and the private key length is 256 bits. The point length on the elliptic curve is 512 bits. For the Hash algorithm, SM3-256 is used to generate the output, and the first 128 bits of the resulting data length are taken as the output value. The encryption algorithm employed is SM4

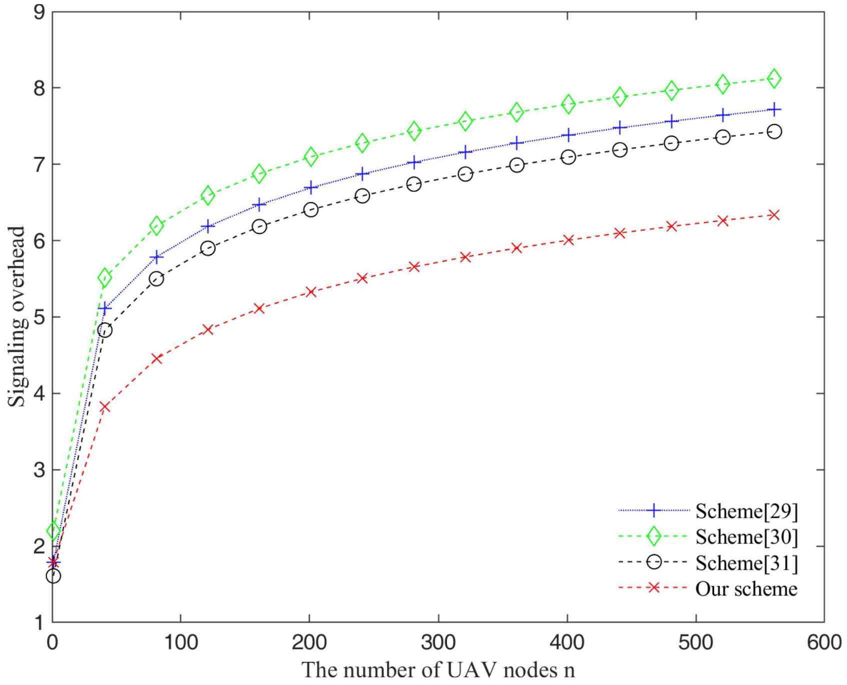


Figure 7. Comparison of signaling overhead

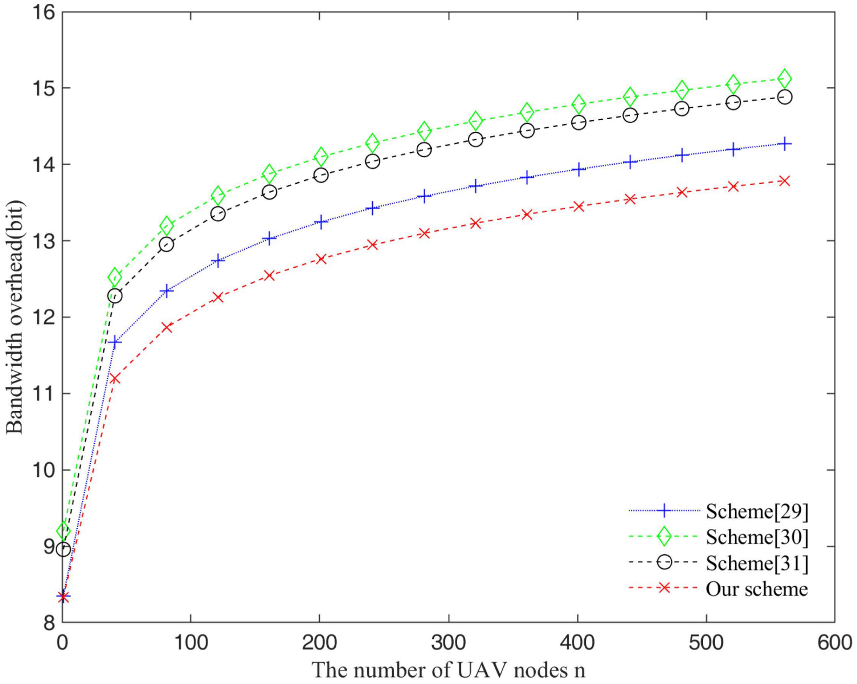


Figure 8. Comparison of bandwidth overhead

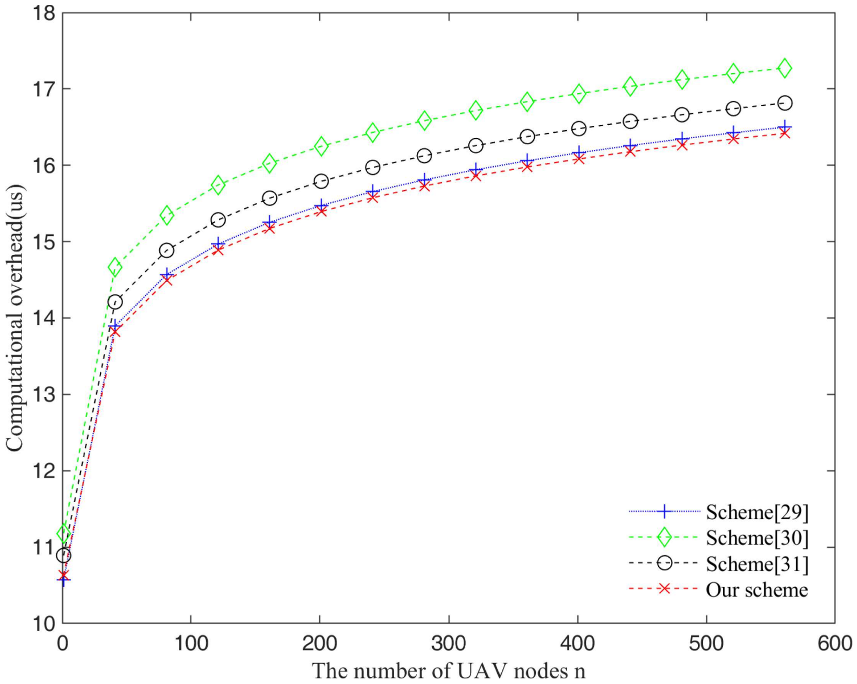


Figure 9. Comparison of computational overhead

Table 3. Comparison of computational overhead

	Computational overhead (ms)
Our scheme	$(9n+11)T_H+(8n+11)T_{\text{cheb}}+(6n+3)T_P+4T_{E/D}=24.036n+17.385$
Scheme [29]	$(22n+11)T_H+(4n+2)T_{\text{exp}}+(2n+1)T_{\text{asyE}}+(2n+1)T_{\text{asyD}}=26.078n+13.039$
Scheme [30]	$(8n+4)T_H+(19n+5)T_P+(8n+4)T_{E/D}=56.649n+14.919$
Scheme [31]	$(10n+5)T_H+(12n+6)T_P=35.768n+17.884$

with an output data length of 128 bits. The output data length for the Chebyshev polynomial is also 128 bits. The length of the random number is defined as 128 bits, and the lengths of the timestamp and identity identifier are 32 bits.

Table 2 presents the bandwidth overhead of our proposed scheme and other relevant schemes. In our scheme, the bandwidth overhead during the SAT-HAP networking authentication stage is 1024 bits, and the bandwidth overhead during the SAT-UAV networking authentication stage is $(1728n+1408)$bits. Therefore, the overall bandwidth overhead in the entire process can be represented as $(1728n+2432)$ bits. Figure 8 illustrates the variation of bandwidth overhead for each scheme with the number of UAV nodes. As shown in the figure, the comparative results indicate that the bandwidth overhead in our scheme performs better compared to other schemes. The utilization of aggregation and broadcasting mechanisms in our approach allows us to reduce redundant parts in messages and effectively decrease bandwidth overhead.

7.3 Computational overhead

We measured the computational overhead using a device with a Core(TM) i7-7500U CPU @ 2.70 GHz processor and utilized the MIRACL cryptographic library. The timings for various operations were tested, including hash operations $T_H=0.002ms$, symmetric encryption/decryption $T_{E/D}=0.004ms$, Chebyshev polynomial $T_{\text{cheb}}=0.766ms$, modular exponentiation $T_{exp}=2.808ms$, point multiplication $T_P=2.979ms$, asymmetric encryption $T_{\text{asyE}}=4.934ms$, asymmetric decryption $T_{\text{asyD}}=2.467ms$.

The computational overhead of each scheme is shown in Table 3. For our scheme, the computational overhead of the SAT-HAP networking authentication stage is denoted as $(6T_H + 6T_{\text{chep}} + 3T_P)$, and the computational overhead of the SAT-UAV networking authentication stage is denoted as $((9n + 5)T_H + (8n + 5)T_{\text{cheb}} + (6n)T_P + 4T_{E/D})$. Therefore, the total computation cost of our scheme is $((9n + 11)T_H + (8n + 11)T_{\text{cheb}} + (6n + 3)T_P + 4T_{E/D})$. The variation of computational overhead for each scheme with the number of UAV nodes is depicted in Figure 9. According to the results, our proposed scheme demonstrates superior computational overhead compared to the other comparative schemes. The utilization of the Chebyshev polynomial reduces the computational overhead of one-to-many authentication and key agreement between satellite and UAV nodes.

8 Discussion

This paper primarily focuses on designing a networking authentication scheme between UAV and satellite nodes in the Space-Air integrated networks. However, in practical scenarios, UAV nodes have poor endurance capabilities and are influenced by task assignments, resulting in frequent joining and leaving of nodes within the UAV group. Therefore, in the future, it is worth researching security networking authentication schemes for UAV groups and key update schemes for UAV group members.

9 Conclusion

Considering the combination of UAV networks and satellite networks in the Space-Air integration scenario, we propose a secure networking authentication scheme for SAT nodes and UAV nodes based on the elliptic curve public-key cryptography system and Chebyshev polynomial. Through informal security analysis and formal security simulation using Scyther, the results show that the proposed scheme can achieve mutual authentication, key agreement, identity anonymity and unlinkability, perfect forward and backward secrecy, and resistance against various protocol attacks. Performance analysis also demonstrates the superiority of our scheme over existing schemes in terms of signaling, bandwidth, and computational overhead.

Conflict of Interest

The authors declare no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Jin Cao and Hui Li identified the problem of security authentication for satellite and unmanned aerial vehicle (UAV) networking through research on the current status. Jin Cao compiled the latest research status on UAV networking and proposed research directions. Sheng Li and Xiaoping Shi jointly designed this scheme, with Sheng Li completing the node registration stage and SAT-HAP networking authentication stage, Xiaoping Shi completing the SAT-UAV networking authentication stage. Sheng Li conducted the security analysis, and Xiaoping Shi performed the performance analysis.

Acknowledgements

We would like to thank Xiongpeng Ren for providing helpful suggestions during the process of designing the scheme.

Funding

This work is supported by the National Key Research and Development Program of China (No. 2022YFB2902203), the National Natural Science Foundation of China (No. 62172317, No. 62102298) and the Fundamental Research Funds for the Central Universities (No. YJSJ23007).

References

[1] Chen SZ, Sun SH and Kang SL. System integration of terrestrial mobile communication and satellite communication-the trends, challenges and key technologies in B5G and 6G. China Commun 2020; **17**: 156–171

[2] Lin M, Huang QQ and Cola TD, et al. Integrated 5G-satellite networks: A perspective on physical layer reliability and security. IEEE Wirel Commun 2020; **27**: 152–159

[3] Hubenko VP, Raines RA and Mills RF, et al. Improving the global information grid's performance through satellite communications layer enhancements. IEEE Commun. Magazine 2006; **44**: 66–72

[4] Khawaja W, Guvenc I and Matolak DW, et al. A survey of air-to-ground propagation channel modeling for unmanned aerial vehicles. IEEE Commun. Surv. Tutorials 2019; **21**: 2361–2391

[5] Zhang W, Li LZ and Zhang N, et al. Air-ground integrated mobile edge networks: A survey. IEEE Access 2020; **8**: 125998–126018

[6] Liu JJ, Shi YP and Fadlullah ZM, et al. Space-air-ground integrated network: A survey. IEEE Commun Surv Tutorials 2018; **20**: 2714–2741

[7] Zhao XW, Zhang Y and Qin P, et al. Key technologies and development trends for a Space-Air-Ground integrated wireless optical communication network. Acta Electron Sin 2022; **50**: 1–17

[8] Wang P, Zhang J and Zhang X, et al. Convergence of satellite and terrestrial networks: A comprehensive survey. IEEE Access 2019; **8**: 5550–5588

[9] He DJ, Li XR and Chan S, et al. Security analysis of a space-based wireless network. IEEE Network 2019; **33**: 36–43

[10] Saeed N, Almorad H, Dahrouj H, et al. Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges. IEEE Open J Commun Soc 2021; **2**: 1505–1525

[11] Zhang N, Zhang S and Yang P, et al. Software defined space-air-ground integrated vehicular networks: Challenges and solutions. IEEE Commun Mag 2017; **55**: 101–109

[12] Semal B, Markantonakis K and Akram RN. A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks. In: Proceedings of 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). London, UK: IEEE, 2018: 1–8

[13] Srinivas J, Das AK and Kumar N, et al. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. IEEE Trans Veh Technol 2019; **68**: 6903–6916

[14] Ali Z, Chaudhry SA and Ramzan MS, et al. Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. IEEE Access 2020; **8**: 43711–43724

[15] Alladi T, Bansal G and Chamola V, et al. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. IEEE Trans Veh. Technol 2020; **69**: 15068–15077

[16] Alladi T, Chamola V and Kumar N. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. Comput. Commun 2020; **160**: 81–90

[17] Lei Y, Zeng L and Li YX, et al. A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access 2021; **9**: 53769–53785

[18] Melo CFE, e Silva TD and Boeira F, et al. Uavouch: A secure identity and location validation scheme for uav-networks. IEEE Access 2021; **9**: 82930–82946

[19] Yazdinejad A, Parizi RM and Dehghantanha A, et al. Enabling drones in the internet of things with decentralized blockchain-based security. IEEE Internet Things J 2020; **8**: 6406–6415

[20] Chen A, Peng K and Sha Z, et al. ToAM: A task-oriented authentication model for UAVs based on blockchain. EURASIP J Wirel Commun Networking 2021; 1–15

[21] Zhang L. Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 2008; **37**: 669–674

[22] Kocarev L and Tasev Z. Public-key encryption based on Chebyshev maps. Int Symp Circuits Syst 2003.

[23] Maze G. Algebraic Methods for Constructing One-way Trapdoor Functions. University of Notre Dame 2003.

[24] Mishkovski I and Kocarev L. Chaos-based public-key cryptography. In: Chaos-Based Cryptography: Theory, Algorithms and Applications. Berlin: Springer, 2011.

[25] Abbasinezhad-Mood D, Nikooghadam M. Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps. IEEE Trans Ind Inf 2018; **14**: 4815–4828

[26] Zhang L, Zhu Y and Ren W, et al. An energy-efficient authentication scheme based on chebyshev chaotic map for smart grid environments. IEEE Internet Things J 2021; **8**: 17120–17130

[27] Dolev D and Yao AC. On the security of public key protocols. IEEE Trans Inf Theor 1983; **29**: 198–208

[28] Cremers C. Scyther: semantics and Verification of Security Protocols. Netherlands: Eindhoven university of Technology, 2006.

[29] Ying BD, Nayak A. Anonymous and lightweight authentication for secure vehicular networks. IEEE Trans Veh Technol 2017; **66**: 10626–10636

[30] Chen CL, Deng YY and Weng W, et al. A traceable and privacy-preserving authentication for UAV communication control system. Electronics 2020; **9**: 62

[31] Bagga P, Das AK and Wazid M, et al. On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. IEEE Trans Veh Technol 2021; **70**: 1736–1751

[32] Elaine B. National Institute of Standards and Technology Special Publication 800-57 Part 1: Recommendation for Key Management: Part 1 – General. The United States: National Institute of Standards and Technology, 2018

Sheng Li received his B.E. degree in Information security from Xidian University, China, in 2019. He is working toward the Ph.D. degree at the Xidian University, China. His research interests include security authentication for unmanned aerial vehicle (UAV) networking and 5G/6G.

Jin Cao received the B.S. and Ph.D. degrees from Xidian University, Xi'an, China, in 2008 and 2015, respectively. Since July 2020, he has been a Professor with the School of Cyber Engineering, Xidian University. His research interests include wireless network security and 5G/6G networks.

Xiaoping Shi received her B.E. degree in Information security from Xidian University, China, in 2020. She is working toward the M.Sc. degree at the Xidian University, China. Her main research directions are 4G/5G networks and space-ground integrated network security authentication mechanisms.

Hui Li received the MA.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 1993 and 1998, respectively. Since June 2005, he has been a Professor with the School of Cyber Engineering, Xidian University. His current research interests include cryptography, information theory, and network coding.