Toward Secure and Lightweight Access Authentication in SAGINs

Su Yao, Jianfeng Guan, Yinan Wu, Ke Xu, and Mingwei Xu

Abstract

Space-air-ground integrated networks (SAGINs) allow mobile nodes to gain access to the Internet anywhere and at any time, which has significantly broadened the communication coverage all over the world. Different from other heterogeneous networks, SAGINs have the characteristics of dynamic network and wide coverage, which make it vulnerable to various malicious attacks. To improve the security of SAGINs, researchers are facing many sophisticated challenges, in which access authentication is the primary problem to be solved because is mainly used to prevent illegal nodes from accessing SAGINs for network services. Therefore, it is crucial to design a secure and lightweight access authentication scheme for SAGINs. In this article, we propose an identity-based mutual authentication scheme (IMAS), which consists of three segments and five procedural phases. Multicast communication is first introduced in access authentication for re-authentication message transmission, which can greatly reduce authentication delay and signaling overhead during handover. Our further qualitative analysis shows that IMAS has proper security characteristics which can meet various security requirements. In addition, from the perspective of performance evaluation, IMAS has outperformed the existing schemes especially when mobile nodes change their access points frequently and need to be re-authenticated for accessing requests.

Introduction

With the skyrocketing development of various communication technologies, the era of the Internet of Everything from terrestrial networks to space communication infrastructures is coming. Space-air-ground integrated networks (SAGINs), including geosynchronous Earth orbit (GEO) satellites, medium Earth orbit (MEO) satellites, low Earth orbit (LEO) satellites, unmanned aerial vehicles (UAVs), and terrestrial networks, have emerged to ensure high data rate, low latency, high reliability, and simple connectivity of everything, anywhere and anytime [1, 2].

Considering that different kinds of satellites can serve as access points, SAGINs can provide mobile nodes (MNs) with a wide variety services from telephone to the Internet of Things (IoT) [3]. Compared to terrestrial networks, the majority of data transmission in SAGINs is through the air interfaces. Therefore, the communication in SAGINs has several defects, for example, vulnerable communication channels and limited resources in the space network nodes, both of which will lead to malicious attacks. As a result, the security of SAGINs is becoming an widely concerned issue especially when adversaries are accessing the network and launching deadly unknown attacks.

As the first line of network defense, access authentication is a crucial technology to identify the legitimacy of MNs that will access the network, and to prevent illegal ones [4]. Therefore, designing secure access authentication architecture is critical for SAGINs to prevent any access request from unauthorized MNs and to effectively avoid the vulnerability of data transmission.

The lightweight characteristic is also a widely concerning issue for access authentication in SAGIN scenarios due to the limited resources in satellites and other flight nodes such as UAVs and airships. Therefore, we propose an identity-based mutual authentication scheme (IMAS) via satellite proxy authentication function to reduce resource consumption in this article. Even when the number of MNs increases, the resource consumption will remain in a relative constant value.

The contributions of this article are summarized as follows:

- Based on the characteristics of SAGINs, we propose the IMAS, which mainly consists of four communication entities, including MN, proxy authentication center (PAC), terrestrial gateway station (TGS), and network authentication center (NAC), and utilizes the broadcast capability of PAC such as LEO satellites to optimize the mutual authentication via broadcast messages signed by PAC.
- To solve the access authentication message storm problem when lots of MNs are re-authenticated at the same time, we design the multicast access authentication mechanism between MN and PAC, which can easily reduce redundant signaling messages.
- To validate the security and light weight of the proposed architecture, authentication delay and signaling overhead analyses are conducted by simulation evaluations, and the analytical results prove that IMAS is appropriate for establishing the access authentication system in SAGINs.

The remainder of this article is organized as follows. We first describe the state-of-the-art research efforts related to the access authentication of SAGINs. Then we design the access authentication

Su Yao, Ke Xu, and Mingwei Xu are with Tsinghua University; Ke Xu and Mingwei Xu are also with Peng Cheng Laboratory (PCL); Jianfeng Guan (corresponding author) and Yinan Wu are with Beijing University of Posts and Telecommunications.

Digital Object Identifier: 10.1109/MWC.001.2000132

1536-1284/20/$25.00 © 2020 IEEE

Although SAGINs have lots of advantages in terms of abundant radio frequency resources, large coverage, long communication distance, fast deployment, and little interference compared to the terrestrial network, their authentication mechanism is still confronted with new challenges.

segments for SAGINs. Following that, we introduce the secure and lightweight access authentication procedure of IMAS in detail. Furthermore, the performance evaluation is presented. Finally, the last section concludes our work, and summarizes the challenges and future work.

Existing Access Authentication Schemes for SAGINs

The existing access authentication mechanisms are mainly based on public key infrastructure (PKI), symmetric encryption, hash function, combinatorial public key (CPK), and identity-based cryptography (IBC). In the past few years, many access authentication solutions have been proposed to provide secure and efficient communications for SAGINs by directly adopting traditional authentication mechanisms. Although SAGINs have lots of advantages in terms of abundant radio frequency resources, large coverage, long communication distance, fast deployment, and little interference compared to the terrestrial network [5], their authentication mechanism is still confronted with new challenges.

First, the openness of satellite communication requires mutual authentication between satellites and MNs to avoid potential security threats such as impersonation. Most current authentication schemes support mutual authentication. However, the mutual authentication schemes based on PKI introduce heavy computation delay and signaling cost. Therefore, some IBC-based schemes are proposed [6] that can offer great security guarantees. However, the original design of IBC is difficult to use in a SAGIN because the single public key generator of IBC may become a bottleneck. More recently, Zhou *et al.* [7] proposed a hierarchical identity-based signature over lattice (L-HIBS) based on a mobile access authentication mechanism to settle the insufficiencies of existing access authentication methods such as high computational complexity, large authentication delay, and no resistance to quantum attacks. Furthermore, to exploit the natural broadcast property of SAGINs, Zhao *et al.* [8] proposed an identity-based efficient and lightweight mutual authentication scheme to optimize the authentication process in which the MN authenticates the network control center (NCC) by broadcasting.

Second, the long transmission delay between satellites and NCC results in large authentication delay. The traditional authentication schemes in SAGINs usually perform the authentication between MNs and terrestrial facilities, and the satellites are not involved in the essential authentication process but only forward the authentication messages. Therefore, some schemes employ satellites for the authentication to reduce the transmission delay. For example, Meng *et al.* [9] proposed a proxy signature-based authentication scheme to reduce latency.

Third, the resource-limited onboard processing (OBP) of satellites requires lightweight authentication to reduce the computation cost caused by encryption operations such as signature and verification. For example, Lee *et al.* [10] proposed a simple and efficient authentication scheme based on hash functions and exclusive-OR operations. However, Jurcut *et al.* [11] pointed out that Lee's scheme confronted the desynchronization attacks and improved it by incorporating a resynchronization phase.

Fourth, the velocity of satellites, especially LEO satellites, is fast, which may result in frequent intra-satellite and inter-satellite handovers. Therefore, a fast re-authentication mechanism should be considered in access authentication schemes. For example, Xue *et al.* [12] introduced the batch verification mechanism when a group of users switch to another satellite to improve the handover efficiency.

Furthermore, some blockchain-based authentication schemes are proposed to provide authentication, privacy protection, and data security. For example, Li *et al.* [13] proposed an authentication protocol for the LEO satellite network by combining IBC and blockchain. More recently, Zhao *et al.* [14] proposed a hash-chain-based authentication mechanism by simplifying the blockchain.

All the above access authentication schemes for SAGINs have their own advantages and shortcomings. Although they can solve some problems, with the increasing number of potential users, the demands of security, light weight, and scalability are urgent. Therefore, we propose the IMAS for SAGINs, aiming to solve these challenges.

Access Authentication Segment Design of IMAS

On the basis of the "control and data separation" idea, the IMAS consists of three segments including the authentication segment, the control segment, and the access segment, as shown in Fig. 1.

The authentication segment consists of PAC in space and a terrestrial access authentication center such as NAC, and it is responsible for unicast authentication and multicast authentication in SAGINs, including communication key distribution, MN and PAC registration, authentication strategy establishment, and multicast group assignment.

The control segment is responsible for forwarding authentication data through space controllers and terrestrial controllers. Space controllers including all kinds of satellites forward the authentication data to terrestrial controllers in the unicast authentication stage. Terrestrial controllers such as gateway stations forward the terrestrial authentication data to NACs.

The access segment consists of all kinds of access entities authenticated by NACs, such as various terrestrial and space mobile communication nodes.

In IMAS, the entities in the access segment first send access authentication requests to the control layer for authentication, and then these requests are forwarded to the authentication segment through space and terrestrial controllers. Finally, based on the authentication strategy, the PAC and the NAC in the authentication segment respond to the request to the control layer and finish the whole authentication procedure.

In our design, we introduce a brand new access authentication scheme, where the access satellites can group-authenticate the MN as a proxy of NAC to avoid the access re-authentication message storm problem of MNs and the bottleneck in access satellites, thereby reducing the long authentication delay and the high authentication cost.

Compared to the GEO and MEO satellites, the LEO satellites are much closer to Earth. Therefore, LEO satellites have shorter transmission delay and

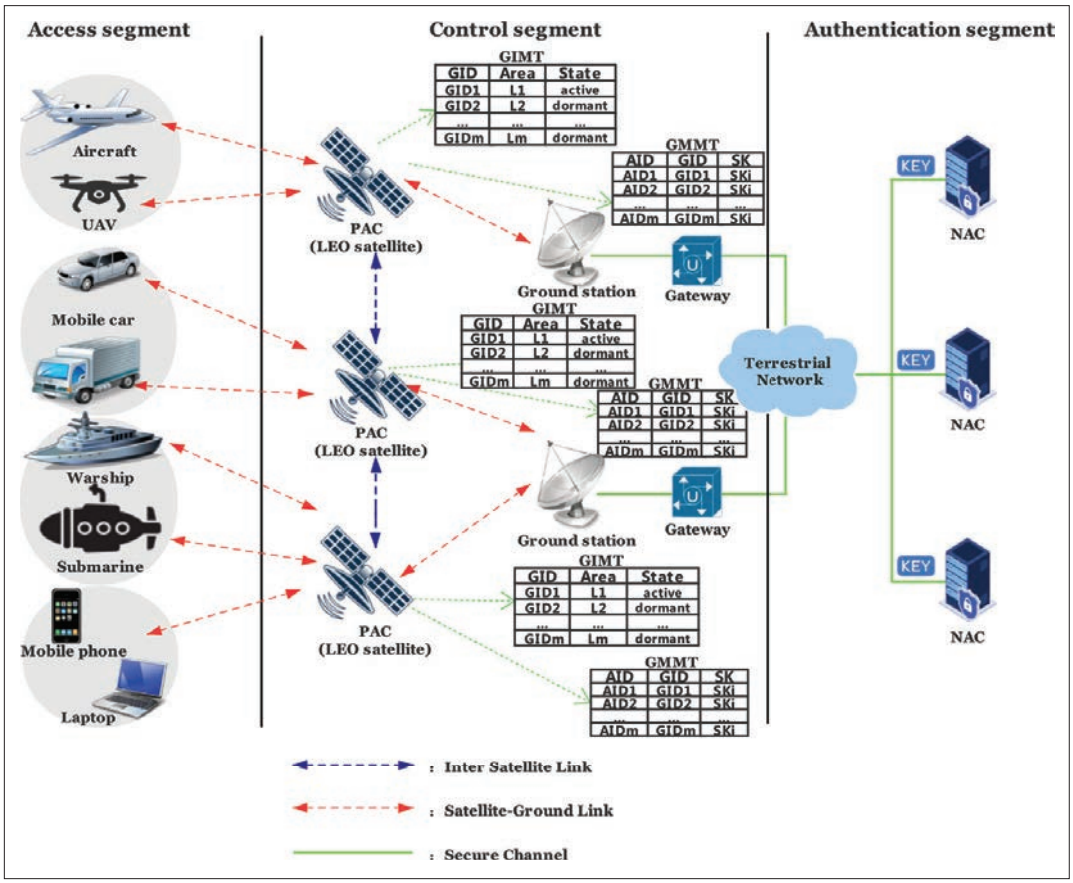

FIGURE 1. The authentication model for SAGINs.

lower transmission cost. Hence, once LEO satellites serve as PACs, SAGINs can provide efficient and reliable access authentication for MNs.

Access Authentication Procedure of IMAS

In this section, we discuss the access authentication procedure of IMAS in detail. As shown in Fig. 2, IMAS can be divided into five procedures: the initialization phase, the registration phase, the broadcast authentication phase, the unicast authentication phase, and the multicast authentication phase. Some notations used in this article are shown as follows:

- ID_{MN}: The real identity of MN
- AID_{MN}: The access identifier of an MN in IPv6 address
- LID_{PAC}: IPv6 link local address of PAC
- GID_{MN}: The group identifier of MN
- PCK_{mn}: The long-term public key of MN
- PTK_{mn}: The long-term private key of MN
- PCK_{pac}: The long-term public key of PAC
- PTK_{pac}: The long-term private key of PAC
- SK: The shared group session key of MN

As shown in Fig. 2, there are four types of network entities involved in the IMAS authentication process, including MN; NAC, which is responsible for accessing authentication service for MNs; PAC, which provides the proxy authentication service functions; and TGS, which provides authentication message transfer between PAC and NAC. More specifically, NAC serves as a private key generator (PKG) for private key generation and update, public key parameters generating, and session key agreement. For simplicity, it is assumed that PAC and TGS have already established a secure channel and finished mutual authentication. The detailed procedure of IMAS is illustrated as follows.

Initialization Phase

In this phase, NAC chooses the Kasahara and Sakai scheme [15] to initialize the public key parameters, and then publishes the parameters to other entities in SAGINs. Based on these parameters, MN and PAC can calculate the public key with each other. Meanwhile, PAC initializes two information tables: the group identifier mapping table (GIMT), which is used to manage the whole group in its coverage range, and the group member mapping table (GMMT) which is used to manage the group members in the *i*th group. The GIMT consists of group ID, PAC coverage area, PAC handover sequence, and optional state such as active or dormant, while the GMMT includes access ID of MN (AID_{MN}), group ID of MN (GID_{MN}), and shared group session key (SK) of MN. Based on the PAC coverage area, the number of groups as well as the handover sequence can be assigned in advance. In this phase, the state of each group is set to be dormant. Assume that there are *l* PACs in SAGINs and *n* MNs, which can be divided into *m* groups. All the above information is illustrated in Table 1 in detail. To reduce the redundant signaling overhead, PAC processes the MNs in form of group based on geographic areas that are divided in advance and mapped to different groups. All the users in the specific region area *S* will join the group after they have finished the authentication, and the PAC that covers *S* will also join the group. In this case, they can adopt the multicast to transmit the signaling messages to reduce the cost.

Compared to the GEO and MEO satellites, the LEO satellites are much closer to the Earth. Therefore, the LEO satellites have shorter transmission delay and lower transmission cost. Hence, once LEO satellites serve as PACs, SAGINs can provide efficient and reliable access authentication for MNs.

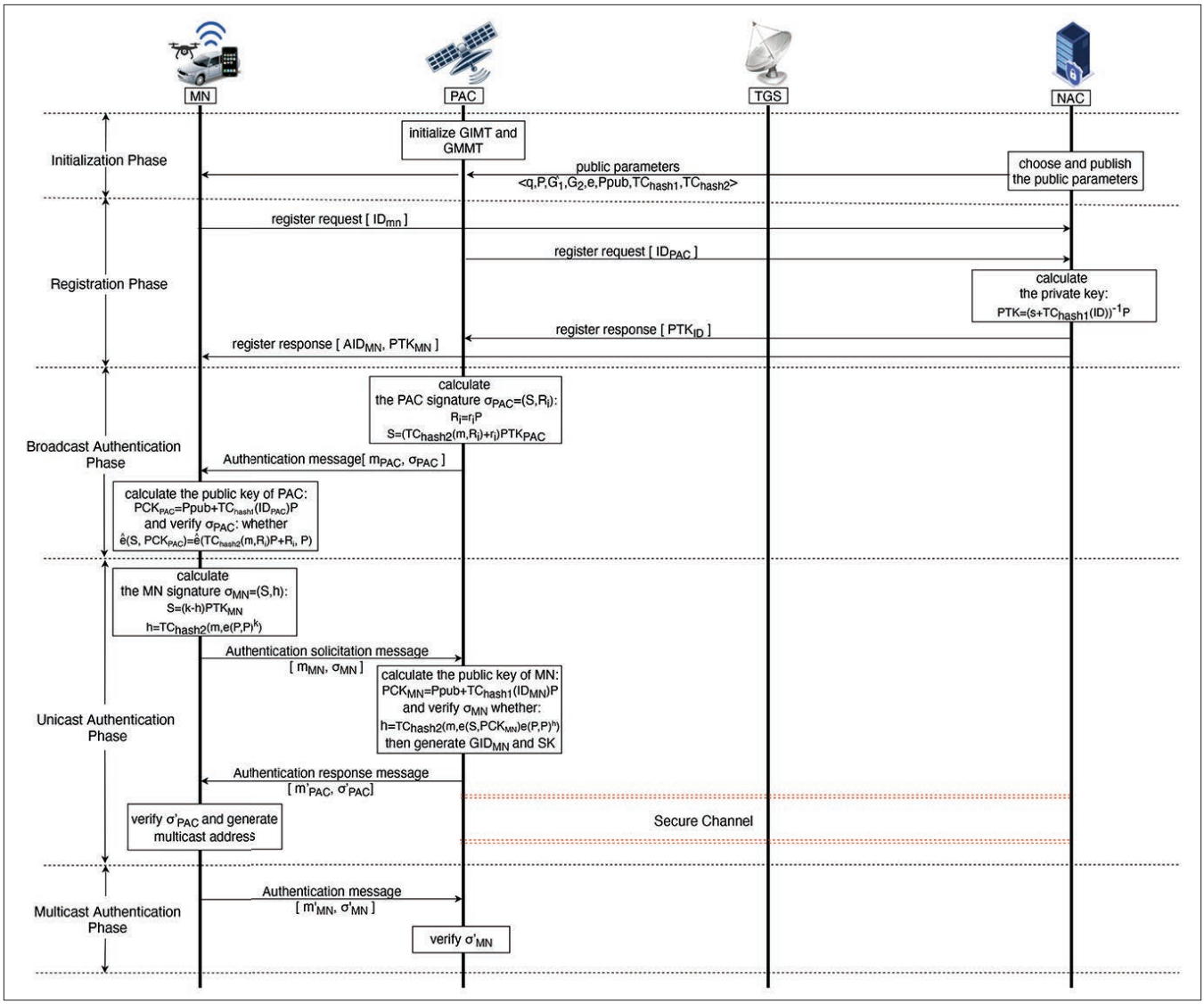

FIGURE 2. The proposed access authentication procedure for SAGINs.

Group ID	Coverage area	Switching sequence	State
GID_1	L_1	(t_1, PAC_i), (t_2, PAC_{i+1}), ⋯, (t_n, PAC_{I-i+1})	Active/dormant
GID_2	L_2	(t_1, PAC_i), (t_2, PAC_{i+1}), ⋯, (t_n, PAC_{I-i+1})	Active/dormant
…	…	…	…
GID_m	L_m	(t_1, PAC_i), (t_2, PAC_{i+1}), ⋯, (t_n, PAC_{I-i+1})	Active/dormant

TABLE 1. The group information covered by PAC.

Registration Phase

In this phase, identity-based signature is designed for mutual authentication between MN and NAC. Before they perform the authentication, MN and PAC should register with NAC using their identities for the corresponding private keys. After calculating their private keys, PTK_{mn} and PTK_{pac} will be sent in a secure communication channel by NAC (e.g., offline transmission). After acquiring their private keys, PAC and MN can encrypt their messages with signatures. Only through the public key of the corresponding sender can the receiver verify the signature and authenticate the identity of the sender. To protect the privacy of MN, NAC will generate the access identifier AID_{MN} for each MN during the registration phase based on the real identity of MN ID_{MN}. Meanwhile, PAC will generate the link local address LID_{PAC} by itself as the interface unicast address. In order to reduce the handover delay between MN and PAC, it is assumed that different PACs will maintain the same link local unicast address LID_{PAC} to reduce the address configuration delay.

Broadcast Authentication Phase

Generally, a mutual authentication procedure begins when an MN requests access to communicate with other nodes. However, different from terrestrial network nodes, the PAC has large broadcast areas. Thus, at the beginning of the mutual authentication procedure, the PAC periodically broadcasts authentication messages, which include random numbers and timestamp using its private key signature. After receiving the broadcast authentication message, the MN calculates the public key of the PAC according to the public key parameters given in the initialization phase

and verifies the PAC signature to authenticate the identity of the PAC. Therefore, the MN can authenticate the PAC during this phase to prevent the PAC impersonation attack.

Unicast Authentication Phase

After verifying the correctness of the PAC signature through the broadcast authentication messages, MNs start to solicit the authentication to the PAC. An MN first sends the authentication solicitation message including random numbers, timestamp, and geographic location, which are signed by its private key. Similarly, after receiving the authentication solicitation message from the MN, PAC calculates the public key of each MN and verifies the corresponding signature. If the signature is correct, the MN can be proved to be a legal user. Then the PAC generates the shared group session key *SK* for the MN and adds the AID of the MN AID_{MN} to the corresponding group GID_{MN} according to the MN's geographic location. Finally, the PAC sends the authentication response message, which includes *SK* and GID_{MN}. The MN receives this message and obtains *SK* and GID_{MN} by the PAC public key, which has been calculated before. Based on the group identifier GID_{MN}, the MN generates its multicast address that will be used in the next phase. Therefore, the PAC and the MN finish mutual identity authentication, and the MN can access the SAGINs legally.

Multicast Authentication Phase

When a PAC moves in the LEO, its coverage area changes accordingly. As a result, MNs need to be re-authenticated by the new PAC. Due to the large numbers of MNs, there will be lots of concurrent authentication solicitation messages during the handover, which may cause a message storm. Therefore, IMAS adopts the multicast authentication method to reduce the redundant access authentication messages. Once a group member has been authenticated, the whole group will be authenticated, and authentication messages from the rest of the group will be ignored. In this phase, the group member sends an access re-authentication message to the multicast address using the shared group session key *SK*, and the other members in the same group will suppress their own re-authentication messages and wait for the multicast reply message from PAC. The group member receives the message from PAC, which has verified the identity of the MN. Finally, the state of GID_{MN} is changed from dormant to active, and all the group members in this group have been authenticated. To provide security assurance, group session key *SK* should be updated to prevent potential forward attack, backward attack, and conspiracy attack.

To sum up, IMAS not only realizes the mutual authentication between MN and PAC using identity signatures when an MN accesses SAGINs initially, but it also gives a secure and lightweight multicast authentication scheme for the MN to re-access SAGINs. This effectively reduces the frequency of authentication message interactions in the same group and achieves high concurrent authentication.

Performance Evaluation

In this section, we first analyze the security characteristics of IMAS using qualitative analysis. In addition, compared to the existing authentication schemes, we quantitatively analyze the performance and discuss the simulation results.

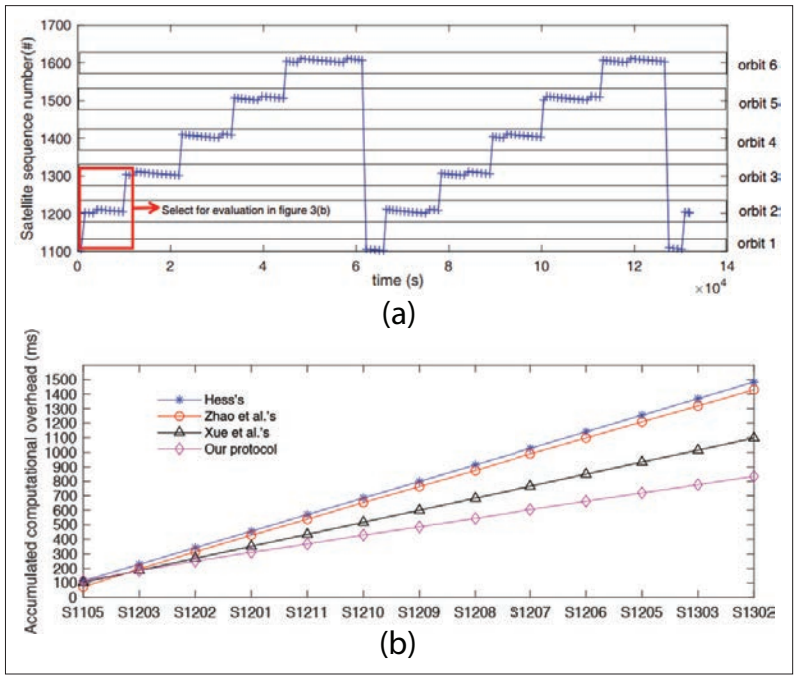

FIGURE 3. The simulation results of different authentication schemes: a) the handover sequence of MNs in a specific location for one day; b) the accumulated computational overhead from 04:00 to 06:00.

Security Analysis

The security characteristics of IMAS cover the following aspects.

Mutual Authentication: The IMAS realizes mutual authentication between MN and PAC during the broadcast authentication and unicast authentication phases. More specifically, in the broadcast phase, the MN authenticates the PAC based on the broadcast authentication messages sent by the PAC, which is encrypted by the PAC's private key to ensure the legitimacy of the PAC. In the unicast phase, the PAC authenticates the MN based on the authentication solicitation message encrypted by the MN's private key to prevent the illegal nodes from accessing SAGINs.

Unforgeability: Only those PACs authorized by the NAC can serve as proxies of the NAC. The proxy certificate of each valid PAC is signed by the NAC. Considering that private keys can be preserved securely, the malicious attackers cannot forge the proxy authentication.

User Anonymity and Traceability: In the registration phase, access identifier AID_{MN} is distributed to each MN by the NAC for message transmission instead of real identity ID_{MN}. Since the real identity of the MN is not revealed in the wireless links, the proposed scheme can protect user privacy and provide user anonymity. Once an anomalous behavior of the MN has been detected, the NAC can track the real identity of the malicious MN.

Minimum Trust Parties: NAC is assumed to be trustworthy because the MNs have to register with their real identities and obtain their private keys for accessing to SAGINs. Therefore, IMAS provides the services as PKG, and no extra trust party is needed.

IMAS not only realizes the mutual authentication between MN and PAC using identity signatures when an MN accesses to SAGINs initially, but it also gives a secure and lightweight multicast authentication scheme for MN to re-access SAGINs. This effectively reduces the frequency of authentication message interactions in the same group and achieves the high concurrent authentication.

Phase	MN signature	MN verification	PAC signature	PAC verification
Broadcast authentication phase	\	$TC_{hash1} + TC_{hash2} + 2TC_{add} + 2TC_{mul1} + 2TC_p$	$TC_{hash2} + TC_{mul1}$	\
Unicast authentication phase	$TC_{hash2} + TC_{mul1}$	$TC_{hash2} + TC_{mul1} + TC_{add} + 2TC_p$	$TC_{hash2} + TC_{mul1}$	$TC_{hash1} + TC_{hash2} + TC_{add} + 2TC_{mul1} + TC_{mul2} + TC_p$ + TCexp
Multicast authentication phase	$TC_{hash2} + TC_{mul1}$	\	\	$TC_{hash2} + TC_{mul2} + TC_p$

TABLE 2. The computational delay of IMAS.

Stolen-Verifier Attacks: In IMAS, only non-sensitive information is stored in the NAC. Even if the attacker gains access to the NAC and is thus able to steal the identities and passwords, the attacker cannot obtain the signatures without knowing the private key of the PAC and the MNs. Therefore, the proposed scheme can resist stolen-verifier attacks.

Performance Analysis

We adopt the Iridium satellite system to analyze the performance, in which each orbit plane has 11 satellites (named 01∼11), and there are 66 satellites in the system. The model setting is J4, and the antenna half cone angle of each satellite is 62°. The satellite sequence number consists of two parts, the first and the second number present the orbit plane, and the third number and the fourth number are the satellite sequence number. For example, 1101 means the 1st satellite in the 11 orbit plane.

We select 108° east longitude and 31° north latitude as the location of MNs, and calculate the satellite handover sequence by analyzing the duration of satellites that cover the given location. In the simulation, an MN can access multiple satellites at the same time, and handover strategy is to select the satellite with the longest connection time. Finally, the order and quantity of handovers of the satellite within one day are obtained as shown in Fig. 3a, and there are 154 intra-satellite handovers, the average duration time for each satellite is 856 s, and the average overlap time is about 3 minutes.

Authentication Computation Delay: The authentication delay refers to the timespan from the time when an MN requests access to SAGINs to the time mutual authentication has finished. Therefore, the authentication delay mainly consists of the authentication message transmission delay and the time cost of computational overhead. Considering that authentication message transmission delay is dependent on the network topology and network capability, we mainly focus on the authentication computation delay in this section. To calculate the computational delay conveniently, seven operations are defined as follows:

- TC_{add}: the time of two-point addition operation in an elliptic curve
- TC_{mul1}: the time of one-point multiplication operation in an elliptic curve
- TC_{mul2}: the time of two-point multiplication operation in an elliptic curve
- TC_{hash1}: the time of one-way hash operation
- TC_{hash2}: the time of one-way hash operation in an elliptic curve
- TC_{exp}: the time of one-point exponentiation operation in an elliptic curve
- TC_p: the time of two-point paring operation in an elliptic curve

Since computational delay dominates in the above operations, some other operations such as subtraction are neglected. In the simulation, the fastest singular elliptic curve E: $y^2 = x^3 + x$ is generated on the finite field, where the length of prime number is 160 bits. The simulation is implemented in the Ubuntu 16.04.6 LTS system with 2G memory and 2.70 GHz single-core Intel CPU. Based on the PBC library and the GMP library, the tested time overhead of the above operations can be obtained.

Scheme	MN-PAC	PAC-TGS	TGS-NAC
Lee *et al.* [10]	$N \times 2$	$N \times 2$	$N \times 2$
Xue *et al.* [12]	$N \times 2$	$N \times 1$	0
Zhao *et al.* [8]	$F + N$	$N \times 1$	$N \times 1$
Our scheme (initial authentication)	$F + N \times 2$	0	0
Our scheme (re-authentication)	N/i	0	0

TABLE 3. The comparison of signaling overhead.

The computational delay of IMAS in one whole authentication procedure is shown in Table 2. Assume the initial access authentication starts at the beginning of the simulation time (the start time is at 04:00) when the MN attaches to satellite 1105. Ten MNs have been chosen during 04:00–06:00 for the performance comparison of computational delay during this period. As we can get from Fig. 3a, satellites mainly hand over from the 1*th* orbital plane to the 3rd one. From the initial attached satellite 1101 to the final access satellite 1303, the accessed satellites of MNs have changed 12 times. According to the procedure of IMAS, the initial authentication phase consists of all the computation procedures shown in Table 2. Once the MN has finished the authentication, the following authentication only consists of multicast authentication. Therefore, the computational delay of IMAS during the above period can be obtained. As shown in Fig. 3b, IMAS has an obvious advantage over other schemes. The reason is that MNs in the multicast authentication phase can be re-authenticated in the form of a group without involving the whole access authentication process, which can reduce the re-authentication computational delay for each node.

Signaling Overhead: The signaling overhead can be evaluated by the number of message interactions in the whole authentication process. Table 3 gives the comparison of signaling overhead between IMAS and other schemes when the authentication requests are from the N MNs. In a traditional authentication method such as Lee's scheme [10], all the access authentication of an MN can only be conducted by an NAC. Therefore, there are at least N × 6 signaling message interactions in the whole process for the mutual authentication between the MN

and the NAC. In Xue's scheme [12], the PAC can authenticate the legitimacy of an MN without the participation of NAC. As a result, there is no signaling message between the TGS and the NAC. However, in this scheme, a PAC should interact through one signaling message with a TGS. Therefore, the total number of signaling messages is $N \times 3$. In Zhao's scheme [8], the PAC broadcasts F authentication request messages in one switching period for its legal identity authentication. Generally, for the massive number of mobile nodes, N is usually much larger than F. Due to the fact that the PAC does not provide the proxy authentication service, the MN needs to be authenticated by the NAC. Therefore, there is $F + 3N$ authentication messages in the whole authentication process to achieve mutual authentication. From the above analysis, we can conclude that there are $F + N \times 2$ messages between the MN and the PAC for mutual authentication.

Compared to other existing schemes, IMAS has better performance on signaling overhead, especially when the MNs have been densely distributed and need to be re-authenticated frequently. Furthermore, IMAS can decrease the burden of PAC when MN needs to be re-authenticated for legitimacy after it has been switched to the adjacent satellite. While in other schemes, MN is assumed to restart the whole authentication process and the signaling overhead is almost the same as that in the first time access authentication, in IMAS, the authentication messages are transmitted by multicast, which will greatly decrease the number of messages between the PAC and other MNs in the same group. For the average group member i, there are about N/i messages exchanged for the MN re-authentication.

Conclusion

This article proposes a secure and lightweight access authentication scheme called IMAS for SAGINs, and the proposed scheme consists of three functional modules and five procedural phases, which provide four essential security characteristics. With the adoption of multicast authentication, IMAS has greatly reduced the authentication computation delay and signaling overhead, especially when a large number of mobile nodes are involved in re-authentication by a new access point for link switching. Moreover, the performance analysis results prove that IMAS is appropriate for establishing the access authentication system in SAGINs. Future work is to improve the security of PKG to avoid a single point of failure, and the available methods include adopting distributed PKG or lightweight blockchain to enhance the reliability and security.

Acknowledgments

This research was supported in part by the National Key R&D Program (2018YFB1800402) and National Natural Science Foundation of China Grants 61802222, 61825204, and 61932016), and the Beijing Outstanding Young Scientist Program with No. BJJWZYJH01201910003011, and sponsored by CCF-Tencent Open Fund WeBank Special Funding.

References

[1] S. Yao *et al.*, "SI-STIN: A Smart Identifier Framework for Space and Terrestrial Integrated Network," *IEEE Network*, vol. 33, no. 1, Jan./Feb. 2019, pp. 8–14.
[2] J. Liu *et al.*, "Space-Air-Ground Integrated Network: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 20, no. 4, 4th qtr. 2018, pp. 2714–41.
[3] K. Xu, Y. Qu, and K. Yang, "A Tutorial on the Internet of Things: From a Heterogeneous Network Integration Perspective," *IEEE Network*, vol. 30, no. 2, Mar./Apr. 2016, pp. 102–08.
[4] W. Tang *et al.*, "Flexible and Efficient Authenticated Key Agreement Scheme for BANs Based on Physiological Features," *IEEE Trans. Mobile Computing*, vol. 18, no. 4, 2019, pp. 845–56.
[5] Y. Su *et al.*, "Broadband LEO Satellite Communications: Architectures and Key Technologies," *IEEE Wireless Commun.*, vol. 26, no. 2, Apr. 2019, pp. 55–61.
[6] Y. Zhong and J. Ma, "A Highly Secure Identity-based Authenticated Key-exchange Protocol for Satellite Communication," *J. Commun. Networks*, vol. 12, no. 6, 2010, pp. 592–99; https://doi.org/10.1109/JCN.2010.6388306.
[7] Z. Yi *et al.*, "An Access Authentication Algorithm based on a Hierarchical Identity-based Signature over Lattice for the Space-ground Integrated Network," *Proc. 2019 Int'l. Conf. Advanced Commun. Technologies and Networking*, Apr. 2019, pp. 1–9.
[8] B. Zhao *et al.*, "Toward Efficient Authentication for Space-Air-Ground Integrated Internet of Things," *IJDSN*, vol. 15, no. 7, 2019; https://doi.org/10.1177/1550147719860390.
[9] W. Meng *et al.*, "Low-Latency Authentication Against Satellite Compromising for Space Information Network," *Proc. 2018 IEEE 15th Int'l. Conf. Mobile Ad Hoc and Sensor Systems*, Oct. 2018, pp. 237–44.
[10] C.-C. Lee, C.-T. Li, and R.-X. Chang, "A Simple and Efficient Authentication Scheme for Mobile Satellite Communication Systems," *Int'l. J. Satellite Commun. Networking*, vol. 30, no. 1, 2012, pp. 29–38; https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.993.
[11] A. D. Jurcut *et al.*, "A Novel Authentication Mechanism for Mobile Satellite Communication Systems," *Proc. 2019 IEEE Wireless Commun. and Networking Conf. Wksp.*, Apr. 2019, pp. 1–7.
[12] K. Xue *et al.*, "A Secure and Efficient Access and Handover Authentication Protocol for Internet of Things in Space Information Networks," *IEEE Internet of Things J.*, vol. 6, no. 3, June 2019, pp. 5485–99.
[13] S. Li, M. Liu, and S. Wei, *A Distributed Authentication Protocol Using Identity-Based Encryption and Blockchain for LEO Network*, Dec. 2017, pp. 446–60.
[14] C. Zhao *et al.*, "Authentication Scheme Based on Hash-chain for Space-Air-Ground Integrated Network," *Proc. IEEE ICC 2019*, May 2019, pp. 1–6.
[15] R. Sakai and M. Kasahara, "ID Based Cryptosystems With Pairing on Elliptic Curve," *IACR Cryptology ePrint Archive*, vol. 2003, 2003, p. 54; http://eprint.iacr.org/2003/054.

Biographies

Su Yao (yaosu@tsinghua.edu.cn) received his Ph.D. degree from the National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University. Since 2017, he has undertaken postdoctoral research in the Department of Computer Science and Technology, Tsinghua University. Currently, he serves in the Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University, as an assistant research fellow. His research interests include future network architecture, IoT security, and space and terrestrial integrated network security.

Ke Xu [SM] (xuke@tsinghua.edu.cn) received his Ph.D. from the Department of Computer Science and Technology at Tsinghua University, where he serves as a full professor. He has published more than 200 technical papers and holds 11 U.S. patents in the research areas of next-generation Internet, blockchain systems, the Internet of Things, and network security. He is a member of ACM. He is an Editor of the *IEEE IoT Journal*. He is Steering Committee Chair of IEEE/ACM IWQoS.

Jianfeng Guan (jfguan@bupt.edu.cn) received his B.S. degree in telecommunication engineering from Northeastern University, Shenyang, Liaoning Province, China, in 2004, and his Ph.D degree in Communication and Information System from Beijing Jiaotong University, China, in 2010. From 2010 to 2015, he was a lecturer with the Institute of Network Technology, Beijing University of Posts and Telecommunications. Since 2016, he has been an assistant professor. His research interests include future network architecture, network security, and mobile Internet.

Yinan Wu (ynwu@bupt.edu.cn) received his B.S. degree from the School of Computer Engineering at Jimei University in 2019. He is currently a graduate student in cyberspace security with the School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications. His research interests include network security and SAGIN.

Mingwei Xu (xumw@tsinghua.edu.cn) received his B.Sc. and Ph.D. degrees from Tsinghua University. He is currently a full professor with the Department of Computer Science and Technology, Tsinghua University. His research interests include computer network architecture, high-speed router architecture, and network security.

The performance analysis results prove that IMAS is appropriate for establishing the access authentication system in SAGINs. Future work is to improve the security of PKG to avoid a single point of failure, and the available methods include adopting distributed PKG or lightweight blockchain to enhance the reliability and security.