A Context-Based Secure Handover Mechanism for Space-Ground-Integrated Network

Hang Zhao*
Beijing University of Posts and Telecommunications, Beijing, China
zh1165053991@gmail.com

Abstract

This paper suggests a context-based secure handover mechanism for the frequent handover problem of satellite access nodes due to its high-speed motion in Space-Ground-Integrated Network. This approach applies Private Key Generator (PKG) in identity-based cryptography for key management and distribution to evade the transport, verification, storage, and other overheads of certificates in Public Key Infrastructure(PKI), and its context mechanism transmits the authentication information and session key of the specific mobile node in advance to the next satellite access node, thereby avoiding the delay and communication interrupt due to recertification during a handover, optimizing the handover efficiency, and guaranteeing the session continuity.

Keywords: Space-Ground-Integrated Network, Context, Satellite Handover

1 Introduction

As the constantly developing demands for national security, Aeronautics and Astronautics, emergency rescue, etc. In recent years, the Space-Ground-Integrated Network is highly concerned as one of the significant coping technologies[15].

Space-Ground-Integrated Network is based on the terrestrial network and supplemented by the space network, covering natural spaces like oceans, lands, air, and space[20].They are the infrastructures that may provide various users' activities with information assurance[8]. The construction of global Space-Ground-Integrated Network offers comprehensive support for air-sea-land communication, weather forecasting, resource prospection, emergency rescue, etc. Moreover, Space-Ground-Integrated Network may contribute to the rapid development of regional information industries. Space-Ground-Integrated Network centers on the multiple terrestrial network nodes to expedite the emergence of innovative technologies based on the regional industry-university-research cooperative innovation and drive the development of the industries related to the Space-Ground-Integrated Network, including internet, future network, mobile communication network, big data, internet of things, information service, and Artificial Intelligence (AI) [9].

The handover technique may be one of the key techniques for the Space-Ground-Integrated Network; particularly in the case of Low Earth Orbit (LEO) satellite networks[12]. LEO satellites' fast velocity relative to the earth due to their lower orbit altitude contributes to frequent satellite handovers; in this case, a secure handover mechanism can be particularly important for guaranteeing users' session continuity and optimizing the delay and packet loss during handovers.This paper has investigated the handover strategy in the mobility management mechanism to propose a context-based secure handover mechanism for Space-Ground-Integrated Network.This study is by the vision of offering inspiration for construction of space-integrated-ground network and expediting the development of the specific field.

The remainder of the paper is structured as follows. Section 2 introduces some knowledge of satellite

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 6, Article No. 5 (November 1, 2020)
*Corresponding author: Tel: +86-13951179091

communication system which is an important part of space-integrated-ground network. Section 3 is an introduction to some related works on handover technology in recent years. From Section 4 to Section 5, the paper proposes a context-based secure handover mechanism and analyzes its performance. Finally,we conclude the whole paper in Section 6.

2 Satellite Communications

The Space-Ground-Integrated Network relies on the terrestrial network and are expanded by the space-based network, they apply unified architecture, technological regime, and standard specification and are interconnected by the space-based network, ground network, and mobile communication network [17]. The space-based network consists of several communication satellites as a supplementary composition for the ground communication network. Being unconstrained by geography and time, the satellite communication network is capable of realizing global communications at any given time, which may partly be the reason of satellite communication technology is becoming a crucial component for the Space-Ground-Integrated Network.

According to the orbit altitudes, communication satellites can be divided into the Geosynchronous Earth Orbit (GEO), the Medium Earth Orbit (MEO), and LEO [16]. GEO is located above the equator by 35800km and may not realize real-time communication and Quality of Service (Qos) for its prolonged delay of signal transmission, link attenuation, and large antenna dimension[10]; MEO is located between 5000 and 215000km, its broadband services may not satisfy the requirements likewise despite the transmission delay is superior to GEO significantly[3]; and LEO is located between 500 and 2000km, the transmission delay of the satellite-earth path is merely between $1/50$ and $1/7$ of the GEO 's. Besides, based on the constellation platform consisting of multiple inter-satellite links, the LEO satellite network solves the low elevation communication problems in polar regions. The LEO satellite network is characterized by global seamless coverage, short transmission delay, low power consumption, and strong invulnerability and is considered to be superior to GEO and MEO in real-time and interactive broadband services, it has significant advantages for the future development of Space-Ground-Integrated Network [2]. To meet the increasing demands for communication of the Space-Ground-Integrated Network, replacing GEO by LEO to be the satellite access node to carry the communication system has become an inexorable tendency.

The LEO constellation may realize a convenient access channel for the Space-Ground-Integrated Network for its short time delay, strong signal, low cost, achievability for mass production, and other features. On the other hand, the high velocity of LEO satellites relative to the ground due to their lower orbit altitude and the limited coverage of a single satellite lead to a situation that the satellite that provides services to a specific user in the current moment may not continue its work for the given user in the next moment. Thus, to maintain the communication continuity, ground terminals may have to handover among various satellites frequently, thereby making mobile handover management an important and urgent problem in satellite networks.

3 Related Works

Handover indicates a mobile terminal or user enters from the coverage area by a network access point into the coverage area by another point in the communication process, where a specific handover mechanism is required for ensuring the communication's continuity. The handover technique is one of the key elements to guarantee QoS.

In the case of satellite handover, Chowdhury et al. [2] have analyzed multiple handover management

solutions in satellite networks and have given a detailed classification for satellite handover modes. In light of the summary of handover schemes in Chowdhury's article, Ding et al. [4] designed a threshold-based spot-beam LEO satellite network handover solution. Duan et al. [5] suggested a location-based inter- satellite minimum-delay handover scheme, which fully utilizes the characteristics of satellite constellations to choose the "nearest" satellite as the access point during a handover based on the two users' locations, thereby decreasing the delay and complexity of the handover notably. In a graph-based satellite handover framework, Wu et al. [18] used a simplified turbulence model to forecast the visibility of the future satellites and draw the future handover graph; in this case, users may choose the shortest pathway for handover according to the handover graph, increasing the handover efficiency. To improve the overall performance for the frequent handovers of satellite nodes, some studies[19] have introduced the software defined networking technique in satellite networks. Despite these solutions have optimized the handover efficiency from various perspectives, they are not easily to be implemented in the actual satellite networks where the resource capabilities are unbalanced, the link delay is prolonged, and the networks are highly dynamic. Otherwise, some of these schemes consider no security requirements during the handover process.

4 Context-Based Secure Handover Mechanism

4.1 System Model

The Space-Ground-Integrated Network is available for various access modes. This paper focuses on the handover solution of the mobile ground node accesses to the communication via the LEO constellation. For this architectural pattern, satellites allow users to access and are capable of processing the users' communications. User terminals and the targeted satellites build secure communication links by means of mutual authentication and key agreement, thus the satellite handover involves only the matters between the users and the satellites.

The handover process may concern the following entities: Mobile Node (MN), Previous Access Router (PAR), and New Access Router (NAR). The distribution and interrelation of all entities in the network structure refer to Figure 1 below. While the satellites are moving at speed, the ground MN is quasi-stationary. In this case, most handovers occur for the rapid transition of satellite coverage due to the high-speed LEO satellites. Each satellite is responsible for a certain communication region; as it moves, the specific communication region changes. As shown in Figure 1, MN accessed to the network for communication via PAR, whereas considering the condition that the satellites are moving at high speed, MN's data flow must be shifted from PAR to NAR to ensure the session continuity when the specific MN enters at the overlap between PAR's and NAR's communication regions and is separating from the coverage area of PAR.

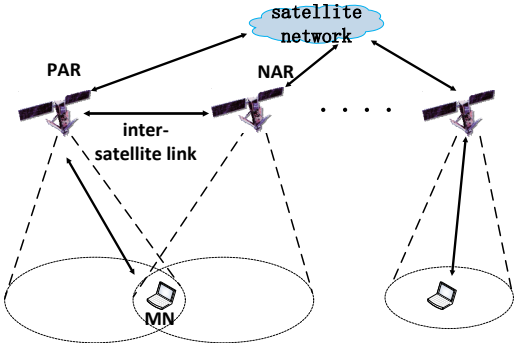

Figure 1: Network Architecture during a Handover

4.2 Handover Solution

The speed of satellites relative to the Earth is fast and the coverage of a satellite is limited, users have to experience inter- satellite handovers during a communication. However, when a user is switching to another satellite, it involves the selection of the targeted satellite, the transmission of the valid user identity authentication, and the communications continuity, security, and other issues during the satellite handover process.

As for communications continuity, the solution is suggested as a handover scheme based on the Context Transfer Protocol (CTP)[11]. Before MN comes to a given event (i.e., a handover), the scheme may transfer the necessary context information in advance to better support the node's mobility. CTP may reduce packet loss and shorten delay, while applying CTP in the handover process may contribute to the communications continuity and handover efficiency.

Science and technology are advancing, and security issues are getting more and more attention[7, 14]. From the security dimension, the solution is based on Identity-Based Cryptography(IBC)[13, 1] and adopts PKG as the Trusted Third Party (TTP) to generate entities and manage the private key in the system.

4.2.1 Initialization

To apply identity-based cryptography in the solution, it shall first initialize the corresponding cryptography parameters prior to the deployment of all network nodes. The initialization includes global parameter generating, and private key generating. The global parameter generating stage indicates the general PKG generating and disclosing Global Parameter params according to the given security parameters. The private key generating stage is aimed at the entities in the system, the PKG calculate the private key and transmit it to the given entity securely. These entities store their private keys secretly for future encryption or signature process. Eventually, each network node receives the global system parameter and its key pair.

Bilinear pairing can be an important tool for the PKG cryptography to realize a series of security protocol algorithms, such as encryption, signature, and signature verification. Suppose G_1 is the additive cyclic group generated by Generator P, where its order is p; and G_2 has a multiplicative cyclic group, whose order is p likewise, where p is a prime number. The alleged bilinear pairing indicates Mapping $e : G_1 \times G_2 \to G_2$ with the following 3 features:

1) Bilinearity: For any $a, b \in Z_p$, and $P, Q \in G_1$, there is $e(aP, bQ) = e(P, Q)^{ab}$.

2) Non-Degeneracy: $P,Q \in G_1$ is existing to make $e(P,Q) \neq 1_{G_2}$, where 1_{G_2} is the identity element of G_2.

3) Calculability: For all $P,Q \in G_1$, there are operative algorithms to calculate $e(P,Q)$.

In satellite communication networks, a mobile node must be approved by any satellite access point to acquire the network services. Suppose the current satellite is PAR and the next satellite after the handover is NAR. The session key negotiation process of MN and PAR can be specified as below:

MN chooses $a \in Z_p$ randomly and calculates aP. Where P is the public generator in Additive Group G_1, p is the order of the group and a prime number. Secretly, MN stores a and sends aP to PAR. Likewise, PAR chooses $a \in Z_p$randomly, calculates bP, and sends it to MN. In this case, PAR may calculate Session Key SK_0 via bilinear mapping using aP, PAR's Private Key SK_{par}, MN's Public Key PK_{mn}, and PKG's public key, and MN may adopt the same approach to calculate Session Key SK_0 based on bP, MN's Private Key SK_{mn}, PAR's Public Key PK_{par}, and PKG's public key.

4.2.2 Handover Process

The handover process can mainly be divided into 2 stages: the pre-authentication stage for transferring the context information and the handover stage where a handover is triggered by MN entering the Coverage of NAR. Supposing that MN and PAR have completed the mutual authentication and agreed on Session Key SK_0 in the access stage. The general handover process is shown in Figure 2.

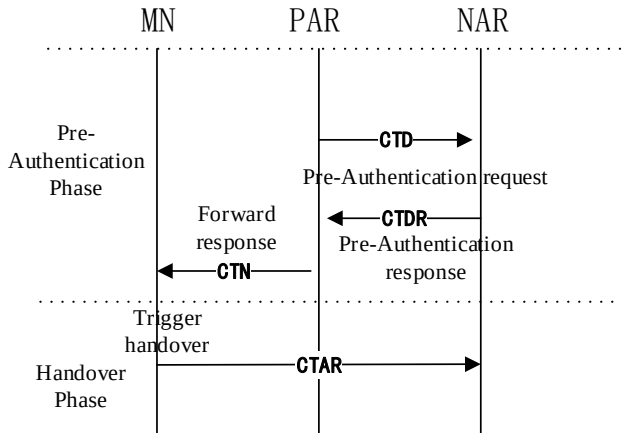

Figure 2: Context-Based Secure Handover Process

(1) Pre-Authentication Phase

The operation of satellite constellation follows their orbital positions and ephemerides rigidly. When MN remains in the coverage of PAR, PAR may calculate the time T for MN to start its handover and the next satellite NAR based on the predictable satellite trail.

a) At $T - T_{th}$, PAR packages the context information of the current MN to be Context Transfer Data (CTD) message and send it to NAR; where T_{th} is the preset handover threshold. The CTD message includes MN's Identity ID_{MN}, Authentication Algorithm Applied AA, Expected Handover Time T, and Handover Session Key SK_1 produced by SK_0 via a random generation function to encrypt the communication between MN and NAR,

$$SK_1 = PRF(SK_0, R) \tag{4.1}$$

where PRF is the pseudo-random generation function, R is the random number.
In addition, CTD contains the signature generated using PAR's Private Key SK_{par}. The message format from MN to NAR is shown below:

$$CTD = \{\{ID_{MN}, AA, T, SK_1\}||Sign_{PAR}\{ID_{MN}, AA, T, SK_1\}\} \tag{4.2}$$

b) Once NAR receives the CTD message, it may apply PAR's public key for authentication. The message may be decapsulated if the authentication approves, NAR acquire the information and reserve the corresponding communications resources for MN at a specific time or execute other procedures. Afterwards, ANR sends Context Transfer Data Replay (CTDR) to PAR. Similarly, the CTDR message requires the signature by NAR's private key.

c) Likewise, PAR receives the CTDR message, verifies it with NAR's public key, and sends Context Transfer Notification (CTN) to MN if the authentication approves. The CTN message contains the identity of NAR Node, Session Key SK_1, the signature generated, etc. In turn, MN receives CTN and conducts authentication, the information will be preserved if the authentication approves.

d) During the whole message passing process, the messages are encrypted with specific encryption keys. Specifically, MN and PAR use Session Key SK_0 for encryption and authentication, whereas Session Key SK_1 may be applicable between MN and NAR, and PAR and NAR apply the default encryption modes between satellites.

(2) Handover Phase

The studies concerning satellite handover selection and handover time are mainly based on the predictability of satellite trails and Received Signal Strength (RSS). In the case of Iridium, the covering time of a single satellite for a given site on Earth is between 8 and 11 minutes routinely, accordingly it may forecast the new satellite to be switched according to the ephemeris that the satellite system follows[6].

a) When MN is located in the overlap of PAR's and NAR's communication coverage regions, the handover process is imminent due to any reason, such as the current satellite access point's signal is weakening. PAR has notified MN about the next satellite (i.e., NAR) in the CTN message, MN, thus, may send Context Transfer Activate Request (CTAR) to NAR directly. CTAR contains the

identities of MN, PAR, and NAR, Current Timestamp T_{MN}, etc. The CTAR message may be encrypted and verified with Session Key SK_1.

b) Once NAR Node receives the CTAR message, it verifies

$$|T_{Now} - T_{MN}| \leq \Delta t \tag{4.3}$$

where, T_{Now} is the current timestamp, and Δt is the system threshold. If the authentication approves, NAR search the corresponding context information, acquires Session Key SK_1, and decrypts and verifies the CTAR message, followed by activating the session connection and completing the entire handover process.

5 Results and Analyses

This paper's security is generally based on identity-based cryptography, and PKG as TTP for generating and encryption key management for the system. Moreover, the solution is capable of defense known attack means to guarantee the security requirements during handover.

(1) The access authentication premises the accomplishment of the mutual authentication between MN and PAR. Thus, a mobile node has yet not accomplished the mutual authentication with a satellite access point may not enter the pre-authentication phase. The request and response messages for pre-authentication must be signed with PAR's and NAR's private keys, other entities may not fabricate a message without the private key.

(2) The security of the message delivery of MN, PAR, and NAR is guaranteed by the session keys. The session key between MN and NAR is derived by Random Function PRF, the unidirectionality of PRF guarantees the subsequent nodes may not acquire the previous session keys. And the random numbers added in the session keys also refrain PAR from deducing the subsequent session keys with its session key.

From the performance dimension, this paper applies CTP to transmit the authentication information in advance to improve handover efficiency. Generally, it requires 4 transmissions of context information to accomplish a handover. In the following part, we shall analyze the improvement of the proposed Context-Based Secure Handover (CBSH) relative to a Basic Handover (BH) that does not apply the context mechanism from the handover delay and the throughput perspectives. In this case, it uses the OPNET network simulation tool to simulate typical LEO satellites. Table 1 shows the parameters of the satellite constellation.

Table 1: Parameters of the satellite constellation

Constellation parameter	LEO
Inclination(°)	86
Altitude(km)	780
Number of planes	66
Number of satellites per plane	11

First, we have analyzed the impact of the processing time of the ground terminal node' cryptographic algorithm on the handover delay and analyzed the variation of the handover delay by increasing the mobile node's processing time. The result after multiple simulations is shown in Figure 3 below. As we can observe from the figure that the context-based secure handover mechanism may shorten the handover delay significantly, and the handover delay differences between the two solutions are becoming even more obvious as the mobile node's decreasing processing capacity. In this case, the context mechanism conducts the access authentication in advance and the context passing process evades the delay due to the re-authentication cryptographic operation during a handover.

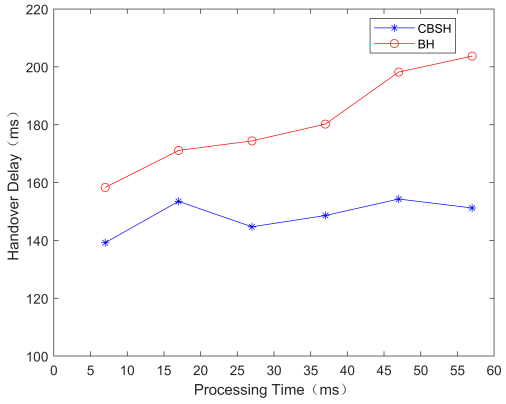

Figure 3: Handover Delay

The throughput means during a handover are shown in Figure 4 below. As we can see, the throughputs of both solutions come to a reduction when a handover occurs and increase progressively to a similar value. The context-based handover scheme has a more moderate throughput decline, which indicates it may realize a lower packet loss rate and offer preferable network QoS.

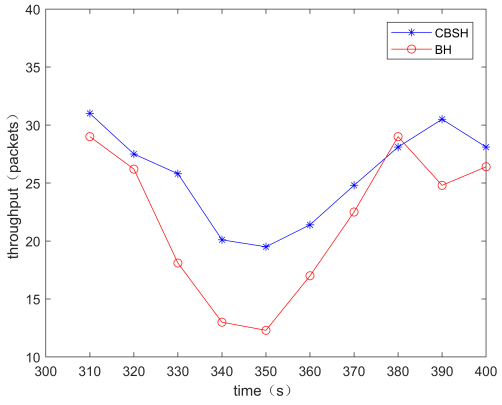

Figure 4: Throughput during a Handover

6 Conclusion

This paper centers on the handover problem in the mobile management for Space-Ground-Integrated Network to exploit the predictable satellite orbits to suggest a context-based secure handover mechanism, which is characterized by transferring the necessary context information in advance. It conducts key management and distribution based on identity-based cryptography to avoid the various overheads in the certificates in PKI, such as transport, verification, and storage. Furthermore, this paper transfers the authentication information and the session key of the mobile node earlier to the next satellite access point based on the context mechanism to evade the authentication delay and communication interrupt that are likely to occur in handovers to optimize the handover efficiency and guarantee the session continuity. Finally, the study verifies the mechanism's reliability via a security analysis and a performance analysis.

References

[1] J. C. Cha and J. H. Cheon. An identity-based signature from gap diffie-hellman groups. In *Proc. of the 6th International Workshop on Theory & Practice in Public Key Cryptography: Public Key Cryptography (PKC'03), Miami, FL, USA*, volume 2567 of *Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, January 2003.

[2] P. K. Chowdhury, M. Atiquzzaman, and W. Ivancic. Handover schemes in satellite networks: State-of-the-art and future research directions. *IEEE Communications Surveys & Tutorials*, 8(4):2–14, 2007.

[3] A. Ciurte and R. Danescu. Automatic detection of meo satellite streaks from single long exposure astronomic images. In *Proc. of the 2015 International Conference on Computer Vision Theory & Applications (VISAPP'15), Lisbon, Portugal*. IEEE, January 2015.

[4] D. Ding, D. T. Ma, and J. B. Wei. A threshold-based handover prioritization scheme in leo satellite networks. In *Proc. of the 4th International Conference on Wireless Communications (WiCom'08), Dalian, China*, October 2008.

[5] C. Duan, J. Feng, H. Chang, B. Song, and Z. Xu. A novel handover control strategy combined with multi-hop routing in leo satellite networks. In *Proc. of the 2018 International Parallel and Distributed Processing Symposium Workshops (IPDPSW'18), Vancouver, BC, Canada*, pages 845–85, May 2018.

[6] R. T. Hu, Z. Y. Wu, and Z. hui Li. Study of the handover management of the high-speed mobile user satellites in the leo satellite network. In *The 16th Annual Academic Conference for Satellite Communications*.

[7] S. Kim, J. Park, K. Lee, I. You, and K. Yim. A brief survey on rootkit techniques in malicious codes. *Journal of Internet Services and Information Security*, 2(3/4):134–147, 2012.

[8] H. W. Li, Q. Wu, and K. Xu. Progress and tendency of space and earth integrated network. *Science & Technology Review*, 34(14):95–106, 9 2016.

[9] J. S. Li. Brief discussion of the significance of building space-ground integration information networks. *Smart Partner*, (08):92–92, 2020.

[10] W. Li, F. Fabra, D. Yang, A. Rius, M. Martín-Neira, C. Yin, Q. Wang, and Y. Cao. Initial results of typhoon wind speed observation using coastal gnss-r of beidou geo satellite. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, 2016.

[11] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli. Context transfer protocol (cxtp). IETF RFC4067, July 2005. `https://tools.ietf.org/html/rfc4067`, [Online; Accessed on October 1, 2020].

[12] X. H. Meng. Research on low orbit satellite communication access and switching strategy. *Information & Communications*, (12):209–209, 3 2015.

[13] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of the 1984 Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO'84), Santa Barbara, California, USA*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[14] Sharma, Vishal, You, Ilsun, Leu, Fang-Yie, Atiquzzaman, and Mohammed. Secure and efficient protocol for fast handover in 5g mobile xhaul networks. *Journal of Network and Computer Applications*, 102:38–57, January 2018.

[15] J. R. Shen. Some thoughts of chinese integrated space-ground network system. *Engineering Science*, 8(10):19–30, 11 2006.

[16] F. Vatalaro, G. E. Corazza, C. Caini, and C. Ferrarelli. Analysis of leo, meo, and geo global mobile satellite systems in the presence of interference and fading. *IEEE Journal on Selected Areas in Communications*, 13(2):291–300, 2006.

[17] W. Wu, P. Qin, X. Feng, and H. J. Liu. Reflections on the development and construction of space-ground integration information network. *Telecommunications Science*, 33(12):1–9, 2 2017.

[18] Z. Wu, F. Jin, J. Luo, Y. Fu, J. Shan, and G. Hu. A graph-based satellite handover framework for leo satellite communication networks. *IEEE Communications Letters*, 20(8):1547–1550, 2016.

[19] B. Yang, Y. Wu, X. Chu, and G. Song. Seamless handover in software-defined satellite networking. *IEEE Communications Letters*, 2016.

[20] N. T. Zhang, K. L. Zhao, and G. L. Liu. Thought on constructing the integrated space-terrestrial information network. *Journal of Chinese Academy of Electronic Sciences*, 10(3):223–230, 8 2015.

Author Biography

Hang Zhao received the B.S. degree in Information Security from Anhui University Of Science & Technology in 2014. Currently he is taking a master's course at School of Cyber space security, Beijing University of Posts and Telecommunications. His research interests include Network Communications and Security and Privacy in Network.