PESUDONYMOUS AND RAPID ROAMING VERIFICATION USING GROUP SIGNATURE

K. Shankari[1], N. Sivakumar[2] , K. Lokeshwari[3]

[1]M.Phil., Reasearch Scolar, Department of Computer Application, Indo American College, Cheyyar.
[2]M.Sc., M.Phil., B.Ed., Assistant Professor, Department of Computer Application, Indo-American College,Cheyyar.
[3]M.C.A., M.Phil., Assistant Professor, Department of Computer Application, Arulmigu Meenakshi Amman College of Engineering, Vadamavandal, Thiruvannamalai.

Abstract: *- Global Information Network has been universally utilized in the realistic life due to its dominance of communicating everywhere and every-time. By cause of an advanced technology enhancement in the auto electronic economics technology, people use to utilize the cellular communication to access the information. This distinctive attribute is foremost to a modern tendency that mobile users are eager to roam to global communication to attain improved utilities. Anyhow, the distinctive attribute of unprotected network and superior prominent discontinuation in global communication cause it hard to blueprint a protected and rapid roaming verification scheme for this modern tendency. Despite the fact few extant analyst would have been concentrate on scheming protected verification obligations for global communication or issuing migrating verification obligations for historic cellular communication, these systematic plans cannot provide sufficient conditions for the migrating network in global network and import in unfavorable problems, like confidential exposure or unbearable verification lag. Noticing following issues have not been well handled, in this system we architecture a Pseudonymous and rapid roaming verification scheme for global communication. In our systematic plans, applied the group signature to implement the invisibility for mobile users, and consider that the spacecraft have lower calculating ability and make them to have the clear-cut verification methods to neglect the actual time involvement of the local connection network control (HNC) while verifying the mobile users. The outcome of safeguard and achievement investigation displays that the prospective plan could supply the sufficient surveillance features, when achieving a slight verification lag.*

Keywords—Retrieve Verification authentication, invisibility, roaming, global information network

1. INTRODUCTION

The appeal for communicating when ever and where ever is enhancing more emergency with speeding up of the proliferation process [1]. Global information network (GIN) which had introduced in this platform and also been appliance earlier in actual life. It utilizes unreal ground spacecraft as broadcast stations to transfer radio waves to attain vast limits of network connection.

In this forthcoming, global communication can be established as an Interplanetary Internet that associate space shuttle with globe's earthbound network connection to pillar the future space analysis and global Internet connection [2]. Analysis with the universal cellular network systems, such as nuclear connection [3] and ground networks [4], satellite connection scheme has the distinctive of universal range covering, huge capability, and bandwidth-on-demand flexibility and would not be finite due to difficult topographical actions among several communication ends [5].

Likewise, migratory benefit is again crucial needed to be issued by global communication: Correspondingly, leads to the overhead engaging features, users in general cellular connection are higher eager to access global communication to acquire network services, along with the roaming service, exclusively in some uttermost protocols, like ocean, desert, or in earth tremor crash places, where unavailable of the core location for signers to approach general wireless networks.

Alternatively, furnishing global roaming in present and future generation communication networks to sharpen the connection convenience and migratory aspects is predominant requirement for at present connection enhancement [6]. To help the surveillance and peculiarity of migratory benefit, it is demand for global communication to set up a defended roaming verification protocol [7]. In common wireless networks, roaming verification protocols are organized into dual types: three-party roaming verification scheme and dual-party roaming verification system. Three-party roaming verification system, like [8] and [9], commonly checks the migratory signer at its local assistant, so that the external assistant could not able to learn user's privacy.

Anyhow, they want more synergy and could not be appliance in the global communication architecture, as the global communication has a long proliferation lag around spacecraft and the landscape. Also for lower ground path spacecraft (lower ground path) which is nearby to the earth, there are up to 500 to 2,000 KM [10] so distances from the earth, and appropriately along with 10 to 40ms proliferation delay. This long proliferation lag will take in an intolerable verification lag to these tripal-party migratory verification services.

Although, two party roaming verification schemes authenticate roaming members without compelling the participation of their local server and often feel necessity for small communication, which could cut down the verification delay. Anyhow, for alive two party verification schemes, they still could not be implemented directly to global communication. Since they commonly have some tedious time-consuming processes of checking cancellation agenda in the above-mentioned design.

Concurrently, the long proliferation delay could not be automatically diminished, as numerous interactions bounded by satellites and landscape devices still alive in these blueprints. Absolutely, satellites can able to transfer complexity computation, with the growth of satellite hardware technology.

Influence by this modern feature, we can employ the spacecraft as the attester rather than landscape servers, which could hugely decreases the interactions bounded by the spacecraft and the landscape servers, so as to subordinate verification delay. Moreover, not only the long proliferation delay challenge, guarantee concern for the migratory synopsis in global communication is also difficult to be approved.

Initially, the susceptibility of global communication leads to some mischievous aggression like interference, alteration, recapitulation, and impersonation (acting) attacks are calmly corrupt the system. Secondly, the hugely unprotected links of global communication can be used by hackers to bargain user's confidentiality through overhear the unprotected channel [7]. At last, also the foreign network attributes could be hidden attackers who could easily acknowledge user's confidentiality by tracing user's identification and locations.

Inspecting the protest that the long proliferation delay and security susceptibility exist in global communication, and still no alive verification scheme could be directly implemented to improved solution to the issues. In this blueprint, we introduce a group signature depended verification scheme to safeguard user's privacy and afford fast access verification for migratory signers.

In our service, each LEO with assured computing power perform as a authentifier to check mobile users while they raise the request to approach the global communication, which could hugely cut short the verification delay and communication messages. Mean time, the deploymentation of group signature could adequately provide user invisibility, so that user's confidentiality would not be exposed to alien connection attributes.

Exclusively, our expected scheme does the coming important supplement:

1) In the paper we reinforced the verification function of LEO satellites, and introduced a rapid roaming verification service, which provides a fast attain validation bounded by users and satellites. Furthermore, a pre-conversation system is deployed to rapid the verification process.

2) Our recommended scheme is depended on group signature, which makes it to possible for spacecraft to verify the users without existing in the home server, and also afford strengthen users invisibility and assurance to its security concerns.

3) Recognizing the extraordinary component of global communication, a well structured cancellation mechanism is also integrated into the architecture of global communication which is foundation for dynamic user's cancellation. Even supposing the cancellation mechanism brings in few adequate overhead; it helps to cut short the duration amount to implement the cancellation list verifying when authenticating users.

2. LITERATURE REVIEW

M. Perry, K. O'hara, A. Sellen, B. Brown, and R. Harper [1] described about mobility users and understanding access information everywhere and every-time. The fast and stimulating move regarding utilization of mobile technologies has gradually assured users and concerns with the capability to use aside from the office and on the roaming. The new trends of engaged sustain by these technologies are generally define in order of approach to instruction and people anytime, anywhere. This system assures a survey of mobile users that features has various character of approach to isolated users and instruction, and various facets of *anytime, anywhere*.

Four features in mobile work are identified: the role of designing, working in "dead time," penetrating distant technological and descriptive attributes, and guiding the actions of faraway companion. On reverse by these issues, we could have good information about role of technology and device uses in mobile work and recognize the convenience for the implement of particular automation explanation platform to mobile workers.

J. Mukherjee and B. Ramamurthy[2]Analysis about forthcoming space inspection appeals a Space connections which can be able to join satellite with each other and consecutively with ground earth bound Internet and thus adequately move the information. There are higher than hundreds of alive satellite instructions throughout the global which connect in outer space at present. Anyhow, the approach of a galactic network is only in its construction stage. Assumable limit of general standards and analysis is necessary earlier across the board deployment happens to cause IPN achievable. They also analyzed image of at current space connection mechanization and construction. It has a conversation about the Inter-planetary Internet and lag forgiving Networking approach with the different space connections which are deployed at present. Along with analysis the important space communication architecture and actions

that still needed comprehensive research and development.

Y. Hu and V. O. Li[5] have analysis that in a spacecraft based network system, satellites are utilised to interposing contrary connection division and to afford universal forthright network access to residency and organization. Also examined Spacecraft-depended network structures and examine numerous approach control, routing, spacecraft transit, and consolidate spacecraft communication into the universal network.

Y. Jiang, C. Lin, X. Shen, and M. Shi[8] discussed about two innovative reciprocal verification and key transaction obligation with invisibility are introduced for various ramble synopsis in the universal portability connections. The current aspect in the introduced obligation includes identification invisibility and former period key restoration. Identification of invisibility assures locomotive users confidentiality in the roaming communication system. Former period key evolution gradually restores the period key for locomotive signers and shortens the exposure of utilizing a negotiate period key to connect with visitation connection. It has exhibit that the computing the complication of the introduced obligation which is identical to the extant ones, when the surveillance has been automatically enhanced.

I. F. Akyildiz, H. Uzunalio˘glu, and M. D. Bender[10] Lower ground path (LEO) spacecraft connections would act an vital performance in the derive instruction framework. Spacecraft in the low earth orbits afford connections with diminished all over suspension and adequate regularity utilization. Anyhow, few issues are needed to be resolved prior the LEO satellite systems can be successfully deployed. Among of these issues is the deliver management. The open-minded of this paper is to analysis the essential approach of LEO spacecraft connections and the handover survey.

3. PROPOSED SYSTEM

3.1 Overview

In this sector, we initially provide the synopsis of the prospective Pseudonymous and Rapid roaming verification system. In the consecutive, we publish a brief definition of the obligation, which chiefly subsist of five levels:

- System inception
- Pre-Conversation
- User Attestation
- User Identification Announce
- Active User Enlistment and Revocation.

The study of the proposed obligation is described in below diagram. After the system inception, in each and every sphere, the portal location (GS) provides a Pre-Conversation instruction to all of controlled LEOs in leading, which consist of a framework for key conversation.

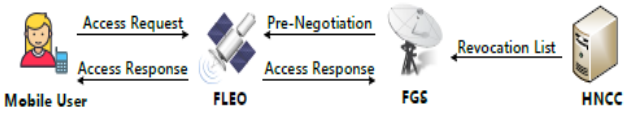

Fig:3.1 Overview

A mobile signers needs to propose the external communication at the beginning which wants to appeal to its local communication domination intermediate to bring back the related access keys. While the signers navigate to a external communication, first to be allow an approach appeal to the approach point of external communication (i.e., lower earth path), which also add a impression that could enquiry the capability of the signers. If the enquiry is gone through, FLEO will provide an approach reply to the signer and FGS subsequently. The approach reply has two key conversation particularizations that could then be utilized to construct a secured connection between the signers and FGS. Furthermore, HNCC regularly announce the cancellation list to signers, so that the uninterrupted signer could change their confidential key to the just finished.

To check the authority of roaming signers, group signature is popularized in our design, in which the local communication intermediate performance like group manager, and empower FLEOs as the authorizer to verify in case the approach appeal is signed by a recognized roaming signers (a group member).

Accordingly the HNCC could be disconnected while the substantiation proceeding. Hence, the authentication lag and communication could be hugely decreased. Furthermore, group signature can contribute good invisibility for the migratory signers, which entrusted external communication attribute are inadequate to accommodation signer's privacy.

3.2 System inception Phase

In the system inception phase, each and every network communication center could be consider as key circulation intermediary (KDC) in its region, which initially achieve and charge ECDSA's authenticating key combination for its gate station and lower ground path. For accuracy and without bias of universality, in the upcoming section, we shorten the system miniature with lower ground path and gate station that are joined with the user's network in all the sectors. Also we provide the key combination for the gate station and lower ground path.

Then each and every network communication center acts as the group manager, and initializes its group. Initially, network communication center chooses a generator in the group at consistently at arbitrary. Then choose arbitrary

numbers and at the last NCC selects a arbitrary number and calculate.

Hence the group global key which could be telecast to all lower ground path in its sector. While a mobile user archives to its network communication center, the network communication center initially achieve an individual key. Later network communication center produces identity network communication center to the user secretly. At last, network communication center saves the tuple in a signer's initial form for releasing user's uniqueness. It needs to be notice that its only achieving once at the starting place of the implement of proposed system. Due to this we could neglect the calculation of the cost for this level.

Subsequently, the universal mediator (TTP) achieves ECDSA's verifying key combination for all network communication centers in various sectors. We assign the key combination for alien network communication center and local network communication center, which could utilized for transferring the instruction among various sectors.

Initially, alien network communication center achieve the instructions in which it has alien lower ground path's universal key, alien network communication center's recognize alien network communication center, alien lower ground path guideline that are utilized for calculating the origin of alien network communication center, and a time clock ts0.

At last alien network communication center gives the instruction and the impression to home network communication center. The instruction would be saved by the home network communication center, in case the time clock ts0 is in a range of allowed limited compared to actual time, and the impression is checked profitably by home network communication center.

If a registry signer has the roaming demand, its network communication center needs to secretly provide instructions to the registering signer in this level. Later the home network communication center come up with the message, at a point of the home network communication center could recognize of home network communication center in a advanced time clock. Then home network communication center impression it with its individual key and gives to alien network communication center. In case the checking for time clock and impression stamp are got through, alien network communication center provides the group global key to all lower ground paths in its sector.

3.3 Pre-Conversation Phase

The Pre-Conversation section would be carried out among each and every lower ground path and ground station in the entire sector. In this aspect, each and every ground station provides a Pre-Conversation instruction MGS to the lower ground path. This information have a guidance ground station (rGS is an arbitrary character chosen by the ground station), which would be used in the verification stage for session key concordance.

A tamest ts2 is besides combined for conflicting reiteration outbreak. Additionally, the ground station prediction the Pre-Conversation instructions with its particular suggestion key sessionGS by ECDSA's indication design as EC: Sign (sessionGS; ground station). Later the GS provides the registered information to lower ground path.

Initially lower ground path analysis even if the time flag ts2 is in a period could permit the limit correlated along with its certain time, and justify the designation GS by ECDSA's authenticating algorithm EC:Verify(pkGS; GS) later once received this information. If the couple of the verifications are valid, the lower ground path repository MGS. Adequately, this aspect could be systematically achieved to amend the communication attributes for upcoming contracting the probability of the time period key flow.

3.4 User Attestation Phase

User Attestation phase has been activated while a locomotive signers migrates to an external connection, and needs to reach the system for access maintenance. In view of this level, the alien lower ground path must verify the roaming user's identity from the user's access appeal legally. In case the verification is gone through, a secret communication could be implemented in addition bounded by the locomotive signers and alien gate station explains this method in following design.

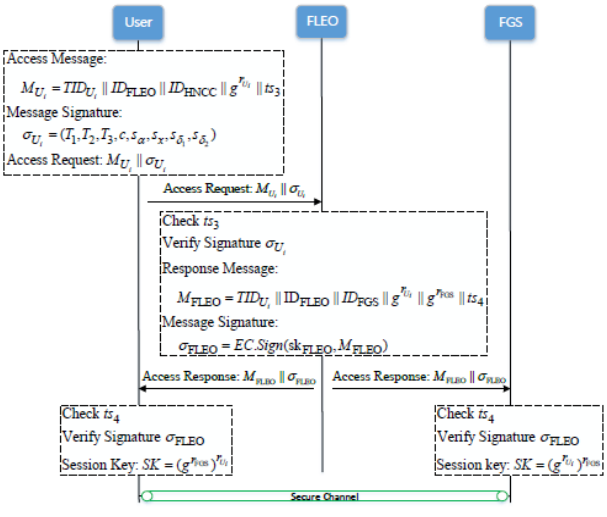

Fig:3.2 Attestation Phase Design

(Noted that, following system, it importantly spotlight on locomotive verification system for global communication, the verification for achieving the local communication could even also be can also be accomplished by carrying out the upcoming verification procedure with resorting

attributes of alien lower ground path and alien gate station as its regional sector lower ground path and gate station.)

1. In this phase initially produces an access appeal, which has connection appeal information with the parallel designation. The connection approach appeal message is a meanwhile existence (not linked in indifferent way along with the signer's absolute integrity), the arbitrary number chosen and introduced ID for home network communication connection is as the identity of local network communication connection, and ID alien lower ground path is the identification of the alien lower ground path which is impelling to interact to the user could identification by using their path parameter in which are obtain the system inception phase. Added to a timestamp is also produced and joined along to the continuous the feedback incursions. The signatures which are various calculating outputs along with a hash value which are choose orbit numbers. The complicated designation produces actions which are depended against the group signature design. After producing the connection appeal, the signers give it to the respective alien lower ground path. It must be notice that few could be pre-calculated and repository by the signers to rise up user verification.

2. For all the collected access appeal, the particular alien lower ground path checks the instructions and produces the approach feedback instructions. Initially, the alien lower ground path verifies in case the time consolidate is not beyond a permitted limited range correlated with its actual time. The FLEO checks in case the signature is authenticated, once in case positive If the verification have not gone through, the FLEO will deny the approach appeal; else ways, the FLEO gather the respective Pre-Conversation instructions which has been repository in the Pre-Conversation section, and produce response information, where timestamp is a new one, ID for alien lower ground path's is alien lower ground path's identification. Then alien lower ground path signatures the feedback information Msg for alien lower ground path by its individual key session key for alien lower ground path. At last, the alien lower ground path gives the approach feedback information with the respective signature to the locomotive signers and alien gate station.

3. Beginning with getting the approach response information from the alien lower ground path, the signers and alien gate station corresponding appliance to authorize a secret connection among them.

The signer and alien gate station initially verify the timestamp. Later they check the impression of alien lower ground path by achieve EC: Verify (public key for alien lower ground path, alien lower ground path). If the authentication is profitably done through, the signer could be able to calculate the period key SK = (ground alien gate station), although the FGS capture the period key SK by calculating SK = (grUi) r alien gate station.

3.5 Signer Identification Announce

To declare users identity, the HNCC receives its indication and the approach information from the alien lower ground path. By passing the input to the group universal key and the respective group manager's individual key, the signature declare actions can be established.

At the beginning HNCC valid in case the user identity is a accurate signature on message, the signature reply actions will be stopped once the reply is noted as fake, else, HNCC could calculate the signer's individual key. Later HNCC could supplementary get the signer's actual existence by taking a vision on the signer's index table respective to the individual key reclaimed from the signature.

3.6 Active User Enlistment and Revocation

Aggressive user's accession means the system grant a new user registry to the scheme after system inception at any time. This is more precious for a constructive migratory authentication system. While a new signer Unew registered to home network communication connection, at first choose a number arbitrary xnew 2R Z p, and calculates Xnew = 1 +ynew g in this proposed scheme. Later the home network communication connection gives Unew's individual key (Xnew; ynew) and alternative scheme guidelines (i.e., universal key alien lower ground path; ID home network communication connection; path attributes) to the user secretly. It is no worth where there are no adequate actions for the real signers in the scheme while new arrival signers register to the level. Anyhow, few signers might be left over from the system because of key loss, illegitimate utility, etc.

To cancel these signers, home network communication connection must regularly release a cancellation lists which has removed signer's individual keys (e.g., (Xj; yj)) to unrevealed signers. Assuming the dynamic and static signers and topography of global communication, described a mechanism for cancellation lists distribution as shown in below diagram.

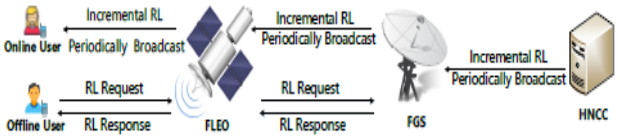

Fig:3.3 Cancellation Design

In view of satellites and locomotive users are efficiency-defined, we accept the additional update of cancellation listing (RL), which is, home network communication connection regularly telecast the expanded entire to the alien gate station, which is later telecast through alien lower ground path to the active users. Concurrently, alien gate station stores the entire cancellation regional in regional recollection while this actions.

To get sure on the full cancellation listing are coincident in which all alien gate stations in various domains, earlier a alien gate station does not get the additional cancellation lists from other sector network communication connection at the telecast time, it should appeal to the network communication connection for the additional RL.

Anyhow, few disconnected signers who might be omission one or few changes of additional RL should take as a initial appeal the removed section of cancelling list access from alien gate station. Once the appeal is received from the offline signer, the FGS examine up its regional full RL to get the removed cancellation list whole for user, and gives back to the user who are at disconnected mode.

Once these actions are achieved, both the connected and disconnected signers obtain the added cancellation list passage for them. After getting the recent cancellation lists, both the connected and disconnected users could change their individual key to the recent.

Despite the cancellation-support structure brings in some subsequent overhead of network and calculation, signers could achieve the actions disconnectedly, and the achievement study considers that our cancellation mechanism is efficient.

Beginning of the sequence of gate stations in all the sector is very tiny and the external communication properties alien lower ground path and alien gate stations are needed to action a limited simple actions in our system, like promoting and ascending RL, it is efficient to implement this cancellation structure in current global communication system.

More basically, the blueprinting cancellation design leads to stimulate the verification action, considering the checker (alien lower ground path) is no more mandatory to action the time-exhausting activity of verifying cancellation list during verifying the signers (as in few previous schemes).

GROUP SIGNATURE

Introduction

Digital signatures attitude in clash with confidentiality, in appropriate with continue to invisibility of signatory and unlink ability of expressed signatures. Diversely, their unforgettable authenticates the signatory as the base of the registered document. That one may to achieve both accuracy and privacy it seem fundamental to disconnect universal substantiation performance from the instruction that would merely verify the signer. This could be done, for comparatively, by estimate a association of hidden signers and committing that verification is attained with recognition to the entire group.

GROUP BASED VERIFICATION

In the dependence of group verification which access signers could checks themselves on grace of some group, instead of depended on particular user. That is, the verification procedures do not performance any instruction that can be utilized as respect for some particular user. On account of all uncover information can be able to link some group of signers, group-based verification is a desirable access for ability to provide user privacy. Along with these desirable signers are assumed as being authenticated in case they could commit a confirmation belongs to the group membership.

Notify that group depended verification is usually used for the design of approach control, where specific are usually allocated to groups and approval to approach and achieve on particular attributes is permitted according to these assignments. However group-based verification approach stimulate to digital signatures.

CONCEPT OF GROUP SIGNATURE

The abstraction of group signatures follows group-based verification to accomplish confidentiality of signers across hidden verifiers. At foremost, group signatures deploy the coming idea: Entire hidden signers are treated as representative of some particular group. Each signer will be provided a signature on favor of the integrated group.

Suchlike group signature is openly verifiable by utilizing the universal key of the integrated group, which issues invisibility of the certain signer. Anyhow, there avails a devoted, perhaps honourable party, which could be able to link the group signatory to the particularity of the signer.

4. OBJECTIVES

The phenomenon of the study as follows,

1. Strengthened verification function of LEO satellites
2. Fast roaming verification scheme.
3. Fast access verification among signers and spacecraft.
4. Additionally, a pre-conversation structure is deployed to quick the verification.
5. A strong users invisibility and guarantees its security requirements.
6. Well designed cancellation mechanism.
7. Support dynamic user's cancellation.
8. It avoids the time cost to implement the cancellation list checking when authenticating users.

5. CONCLUSIONS

Global information network could disjunction the territorial limitation and supply extensively analysis correlate along classic network. The tendency of migrating to universal informative connection would be an advanced distinctive attribute of the forthcoming connection, which

benefit for conspiring a advanced migrating verification systematic plan for Global information network.

When objection extant for blueprinting a migrating verification scheme for global connection because of its exclusive surrounding (e.g., the potent and ambiguous topography, the huge unprotected associations, the lengthy discontinuation). Excite by the priority of signers verification lag and invisibility for migrating, we architecture a Pseudonymous and rapid roaming verification protocol.

In this system we used the group signature and highlight the verification of alien lower ground path and alien lower ground path, which factor the alien lower ground path could directly verify roaming signers to approach the alien connection instead of the substantive-time crisis of local connection dominance instead of confidentiality exposure. Additionally, a cancellation structure created especially for this scheme is integrated into the migrating verification device to reinforcement signer's cancellation.

Despite less number of upward is imported in mature to the cancellation structure; it could hugely diminish the verification lag. In extension, the scheme alleviates an equipment of further exacting guarantee appearance, when appreciate a diminished verification lag and lower connection hanging.

REFERENCES

[1] I. F. Akyildiz, H. Uzunalio˘glu, and M. D. Bender, "Handover management in low earth orbit (LEO) satellite networks," Mobile Networks and Applications, vol. 4, no. 4, pp. 301–310, 1999.

[2] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual verification and key agreement scheme with user anonymity for secure communication in global mobility networks," IEEE Systems Journal, vol. 10, no. 4, pp. 1370–1379, 2016.

[3] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual verification and key exchange protocols for roaming services in wireless mobile networks," IEEE Transactions on Wireless Communications, vol. 5, no. 9, pp. 2569– 2577, 2006.

[4] F. Li, L. Yang, W. Wu, L. Zhang, and Z. Shi, "Research status and development trends of security assurance for space-ground integration information network," Journal on Communications, vol. 37, no. 11, pp. 156–168, 2016.

[5] T. B. Zahariadis, K. G. Vaxevanakis, C. P. Tsantilas, N. A. Zervos, and N. A. Nikolaou, "Global roaming in next-generation networks," IEEE Communications Magazine, vol. 40, no. 2, pp. 145–151, 2002.

[6] Y. Hu and V. O. Li, "Satellite-based internet: a tutorial," IEEE Communications Magazine, vol. 39, no. 3, pp. 154–162, 2001.

[7] Q. A. Arain, D. Zhongliang, I. Memon, S. Arain, F. K. Shaikh, A. Zubedi, M. A. Unar, A. Ashraf, and R. Shaikh, "Privacy preserving dynamic pseudonym based multiple mix-zones verification protocol over road networks," Wireless Personal Communications, vol. 95, no. 2, pp. 505–521, 2017.

[8] G. Miao, J. Zander, K. W. Sung, and S. B. Slimane, Fundamentals of Mobile Data Networks. Cambridge University Press, 2016.

[9] J. Mukherjee and B. Ramamurthy, "Communication technologies and architectures for space network and interplanetary internet," IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 881–897, 2013.

[10] M. Perry, K. O'hara, A. Sellen, B. Brown, and R. Harper,"Dealing with mobility: understanding access anytime, anywhere," ACM Transactions on Computer-Human Interaction, vol. 8, no. 4, pp. 323–347, 2001.