Journal of Communications and Information Networks
Vol.1, No.1, Jun. 2016
DOI: 10.11959/j.issn.2096-1081.2016.006

Review paper

Survey on key security technologies for space information networks

LIU Jianwei[1], LIU Weiran[1], WU Qianhong[1], LI Dawei[1], CHEN Shigang[2]

1. School of Electronic and Information Engineering, Beihang University, Beijing 100191, China
2. Department of Computer and Information of Science and Engineering, University of Florida, Gainesville FL 32611, USA

Abstract: SIN (Space Information Network) is expected to play an increasing role in providing real-time, flexible, and integrated communication and data transmission services in an efficient manner. Nowadays, SIN has been widely developed for position navigation, environment monitor, traffic management, counter-terrorism, etc. However, security is a major concern in SIN, since the satellites, spacecrafts, and aircrafts are susceptible to a variety of traditional/specific network-based attacks, including eavesdropping, session hijacking, and illegal accessing. The network architecture and security issues of SIN were reviewed. Various security requirements were discussed that should be considered when designing SIN. And existing solutions proposed to meet these requirements were surveyed. The key challenges and key technologies that still require extensive research and development for securing SIN were indentifed.

Key words: space information network, network architecture, data encryption, key management, access authentication

Citation: LIU J W, LIU W R, WU Q H, et al. Survey on key security technologies for space information networks[J]. Journal of communications and information networks, 2016, 1(1): 72-85.

1 Introduction

Space is one of the most important and strategic resource in science and technology for nations. SIN is an integrated network that transfers and processes massive data collected by entities in the space. SIN expands human activities into the sky, out to the seas, even in the deep space. As a heterogeneous network, SIN is able to obtain, transmit, and process data from the space, while maintaining seamless communication services with terrestrial networks. Meanwhile, SIN can also be easily and quickly deployed, as a cost-effective solution in areas where deploying ground fiber networks is too expensive[1]. SIN can be used for position navigation, earth observation, timing synchronization, warning detection, disaster relief, etc. Nowadays, such integrated networks have been widely developed to better our life.

Although SIN offers great potential, there are still significant challenges needed to be addressed. Among them, security is becoming an increasingly important aspect[1]. Various nodes, e.g., air vehicles, space vehicles, and stratospheric platforms, are connected in SIN, which improves the interoperability between nodes on the space and base stations on the ground. Adversaries may attack such an integrated network, by the methods of spectrum eavesdropping, data tempering, entity disguise, denial of service, and illegal

Manuscript received Mar. 01, 2016; accepted Apr. 19, 2016
This work is partially supported by The National Basic Research Program of China (973 program) (No.2012CB315905), The National Natural Science Foundation of China (No.61272501, No.61370190, No.61003214), The Natural Science Foundation of Beijing (No.4132056).

access. Compared with traditional networks, SIN is one of the key infrastructure for some nations. Failure of SIN security would leak top-secret information, which may lead to serious consequences.

For security attacks against SIN, a famous example is that an American Lockheed Martin RQ-170 Sentinel UAV (Unmanned Aerial Vehicle) was captured by Iranian forces at the city of Tabas in northeastern Iran on December 4, 2011[2]. The department of Defense stated that the UAV was flying a mission over western Afghanistan when control was lost[3]. Investigations showed that some unknown party jammed the GPS signal channel of the UAV so that it was forced into auto-pilot. Then, a false signal was sent to the UAV for the purpose of landing at a wrong location. The key technique is to jam and spoof the GPS signal that is used for the UAV to locate itself, which is not difficult, as the paper detailing how to do so has been available since 2002[4].

Another well-known security attack against SIN relates to the death of Muammar Gaddafi, who was the deposed leader of Libya[5]. Gaddafi was found hiding in a culvert west of Sirte and captured by National Transitional Council forces. He was killed shortly on October 20, 2011. Around that time, Gaddafi published a recorded speech by using a satellite phone, advocating his supporters to fight unceasingly. However, the U.S. AirForce RC-135 reconnaissance aircraft intercepted the signal from the satellite phone call made by Gaddafi, locating his position.

Existing practical attack methods warn us that enhanced security mechanisms must be applied to secure SIN. However, there are various challenges in designing suitable security mechanisms. SIN is a complex network consisting of various sub-networks, e.g., distributed satellite networks, hierarchical networks, and the Internet. This brings difficulties for security management since distinct sub-networks have distinct security requirements. Besides, SIN has the features of heterogenous compositions, open transportation links, and dynamic data transformations that bring new challenges for securing SIN.

In this article, we consider typical security risks and corresponding solutions in SIN. We focus on the abstract network architecture of SIN, and define its security requirements. Then, we review existing solutions to address these security requirements, while pointing out the drawbacks and challenges for these solutions. We describe potential cryptographical approaches that may be developed for constructing robust and scalable security mechanisms meeting the characteristics of SIN.

The rest of the article is organized as follows. In Section 2, we describe the abstract network architecture of SIN. Section 3 lists security issues and security requirements of SIN. Next, we demonstrate the state of SIN security in Section 4. Section 5 indicates security challenges in SIN, and the key techniques that require extensive studies and researches to be applied in SIN. We finally conclude the article in Section 6.

2 Network architecture of SIN

The most natural way to define the network architecture of SIN is to classify entities in SIN based on their distances of orbits from Earth. We follow the well-accepted classification method for SIN[6]. The abstract network architecture of SIN can be described in Fig.1.

Definition 1 (Definition of space information network). SIN is an integrated information infrastructure, which transforms and processes massive data collected by entities that are deployed in space. The space ranges from NEO (Near Earth Orbit), LEO (Low Earth Orbit) and MEO (Medium Earth Orbit), GEO (Geosynchronous Orbit), to DS (Deep Space). The entities include aerospace craft, spacecraft, aerostatics, parts of which are commonly interconnected.

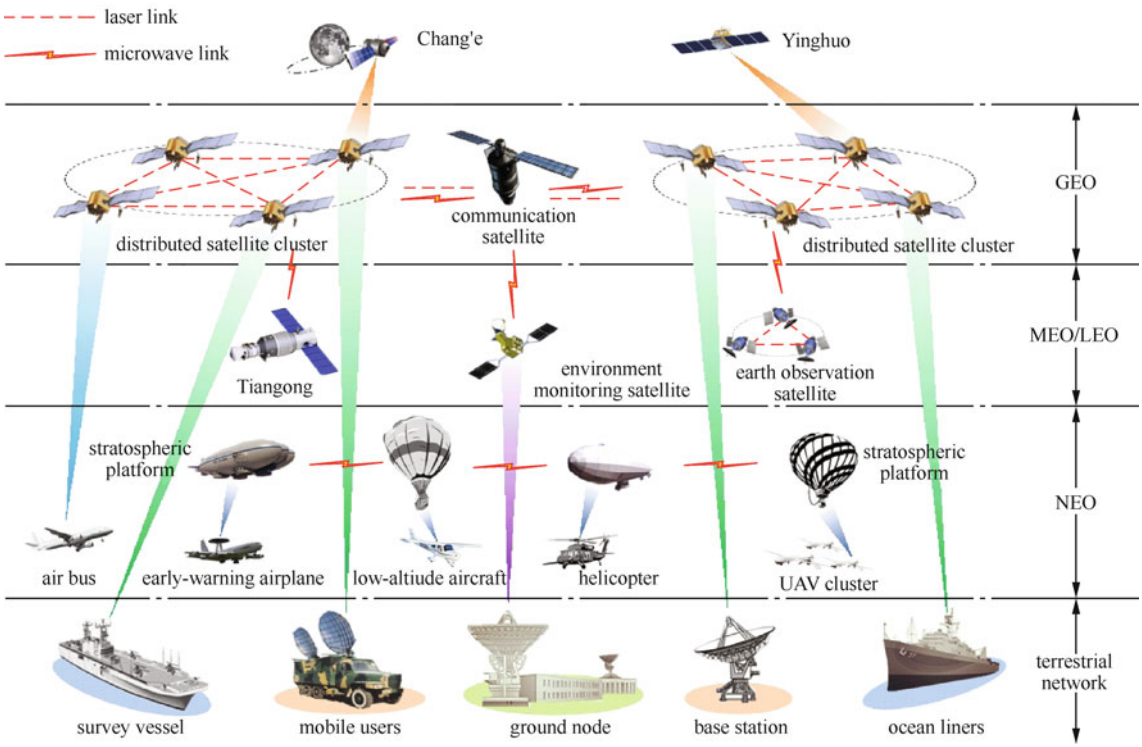


Figure 1 Abstract network architecture of SIN

There are four layers in SIN according to the entities' positions, namely GEO, LEO and MEO, NEO, and Ground. We discuss the following SIN components and their proper characteristics:

- GEO satellites, including GEO communication satellites and relay satellites. The satellites' speed at GEO matches the Earth's rotation speed, thus keeping relative rest with respect to the Earth ground. This feature brings convenience for these satellites to be the data transmission station of SIN. Satellites at GEO are commonly used for the space backbone network nodes in SIN. They are responsible for transmitting, processing, and forwarding data between entities and users. Meanwhile, they act as the network managers for SIN.
- MEO/LEO spacecrafts, including environment monitoring satellites and earth observation satellites. Spacecrafts on these two orbits always act as data collectors in SIN. For example, earth observation satellites, as one of the most typical entities at LEO, acquire earth observation data and directly send the data back to the base stations. If there is no available base stations when requiring data transmission, earth observation satellites are able to transmit the data to nodes in space backbone and access networks, which will then forward the data back to the territorial network. Commands to MEO/ LEO spacecrafts are sent directly from the base stations, or indirectly from relay satellites.
- NEO aircrafts, including stratospheric platforms, low-altitude aircrafts, and air buses. Since NEO aircrafts are very close to the earth, they can realize bidirectional communications and data transmissions to the base stations with small delay. In addition, parts of NEO aircrafts can self-organize as a network cluster to provide Internet services

for terminal users on earth.

- Terrestrial networks, including base stations, ground nodes, and mobile terminal users. They can be stand-alone servers (base stations), or a cluster of user nodes organized by traditional / advanced networks, e.g., LAN (Local Area Network)[1], and MANET (Mobile Ad hoc Networks)[7].

3 Security requirements of SIN

3.1 Data confidentiality and data integrity

Satellite channels are wireless broadcast media, which makes it possible for anyone to receive the data content. Therefore, a malicious adversary on the ground with the right equipment can eavesdrop the data transmission content. Due to the fact that data transmitted between satellites and terrestrial nodes often contain sensitive information, e.g., user location, military commands, failure of data confidentiality in SIN may lead to serious security issues for a nation.

Data confidentiality can be achieved by message encryption. When transmitting data in a satellite channel, the sender should encrypt the data under a cryptographic key, while the receiver must do the decryption operation with a corresponding key. However, not all existing encryption schemes can be directly applied to ensure data confidentiality in SIN. On one hand, satellites are considered to have limited computation capabilities. The encryption schemes applied in SIN must be lightweight in order to limit the additional computation overhead on satellites. On the other hand, the data transmitted between satellites and ground nodes often have large volume, e.g., high-definition pictures or long videos. Encryption schemes should be designed so that the overall network performance is not affected.

Along with data eavesdropping, satellite channels can occasionally incur high burst errors or long propagation delays. To make the matters worse, a malicious adversary may be able to modify the data content whenever he detects burst errors, and acts as the actual satellite to transmit data to the ground nodes. This kind of active attack method brings more harmful security issue for SIN. Data integrity must be guaranteed so that any piece of content will not be lost or modified during its transmission.Therefore, data transmission protocols should have a built in mechanism that ensures correct data transmission, or recovers data from loss.

3.2 Register, usage, and revocation

When incorporating encryption schemes into SIN, the problem of distributing keys between users, that is, key management, is an accompanying challenge. However, there are distinct security requirements for different space missions and applications. Keymanagement schemes must be designed to support these security requirements.

Key management schemes for SIN should support symmetric/asymmetric key management, where asymmetric key management would enable user access and key exchange, while symmetric key management enables lightweight data encryption/decryption operations. Also, since satellites, airspaces and aircrafts are often organized in a hierarchical and distributed manner, it will be difficult to design an unique key management mechanism to satisfy various secure communication/secure access requirements. An possible solution path is to design an extensive key management scheme that supports centric/distributed key management.

3.3 Access authentication and access control

In SIN, users and satellites need bidirectional communications. Since satellite channels are wireless broadcast media, an adversary with the right equipment

can pretend to be a legitimate user and send spurious control and command messages to the satellites, thus manipulating the satellites to perform unintended operations.

This kind of attacks can be prevented by using access authentication methods. When receiving the control and command messages, entities in SIN should be able to verify whether the message sender is properly authenticated. This will require suitable authentication mechanisms, e.g., handoff authentication and access control. Unfortunately, since SIN is typically a heterogeneous network, where entities may frequently join or leave the network due to their position changes. Meanwhile, their moving speed in SIN will be fast, especially for the ones in GEO. The authentication procedure must be completed in milliseconds to ensure fast handoff. This brings additional challenges to design authentication schemes in SIN.

4 The state of the art for SIN security

Since SIN is strategically important for a nation, developed countries and academic organizations have dedicated manpower and material resources to carry out relevant research. In this section, we give an overview of the state of the art for SIN and SIN security.

The Security Working Group in CCSDS (Consultative Committee for Space Data Systems) devotes to security guidance and security standards formulation for SIN. In 1999, CCSDS published "SCPS-SP (Space Communications Protocol Specifications-Security Protocol)"[8], providing end-to-end confidentiality, integrity, and authenticity of data service for satellite-terrestrial information-centric networks. In 2003, CCSDS published "Next Generation Space Internet (NGSI) - End-to-End Security for Space Mission Communications"[9]. In this standard, they introduced trusted gateway to implement protocol switching between terrestrial network and SCPS, ensuring strong inter-operability. Meanwhile, they recommended the IKE (Internet Key Exchange) protocol[10], which was designed based on ISAKMP (Internet Security Association and Key Management Protocol), being the key exchange standard in SIN. In 2006, CCSDS published "Security Threats Against Space Mission"[11] and "The Application of CCSDS Protocols to Secure-Systems"[12], analyzing security threats in space communications, and providing security frameworks for space missions based on CCSDS standards. A series of security protocols and encryption algorithm standards were released by CCSDS to be the guidance of secure data transmission in space communications, including "CCSDS Cryptographic Algorithms"[13] and "Security Architecture for Space Data Systems"[14]. Nowadays, many space agencies and commercial institutions follow the CCSDS standards, including ISS (International Space Station), NASA GSFC (Goddard Space Flight Center), NASA JPL (Jet Propulsion Laboratory), and ESA (European Space Agency). In China, CAST (China Academy of Space Technology), CASI (China Aerospace Standardization Institution), and BITTT (Beijing Institute of Tracking and Telecommunications Technology) devote long-term studies for CCSDS standards, and follow these standards to design security mechanisms for Manned Space Project, Manned Spacecraft System, and Chang'e Projects.

However, security protocols released by CCSDS aim at achieving minimum bit error rate and minimum communication overhead. These protocols only provide simple end-to-end security communication services. In practice, adversaries may often have overpowering attack capabilities. How to prevent active attacks remains a challenge for securing SIN.

The United States pays much attention for the formulation and implementation of SIN. It strives to develop such an integrated information system. Around 1990s, United States Department of Defence submitted a military doctrine to the Congress, named Network-centric Warfare[15], which is a new theory of

warfare to show how to use information and communication technologies to improve situation analysis, accurately control inventory, and speed of command. Later, in order to improve on CNS/ATM (Communication, Navigation and Surveillance/Air Traffic Management), FAA (Federal Aviation Administration) proposed the NAS (National Airspace System) project, which now becomes one of the most complex aviation systems in the world that provide control for the airspace, navigation facilities and airports of the United States, along with their associated information, services, rules, regulations, policies, procedures, personnel and equipment. In 2003, FAA introduced the OEP (Operational Evolution Partnership) plan, which is a blueprint to the future of airspace infrastructure constructions. In addition, Boeing Company works on Integrated Battlespace programs[16]. The concept is to transfer information acquired from national, military and commercial reconnaissance and surveillance assets through a robust communications network involving space, airborne and ground-based assets.

European Union hopes to establish its own SIN centering on Galileo position system. The European IST (Information Society Technologies) funded BRAIN (Broadband Radio Access for IP-based Network) project, which is working on the next generation of mobile radio systems through a common IP network platform[17]. Based on the BRAIN architecture model, SHAMAN (Security Heterogeneous Access for Mobile Application and Networks) project studied the protection and security required for users, information and services in the next generatio mobile communications under the heterogeneous network settings. The basic idea is to evolve from the enhanced GSM/GPRS system to an "all-IP" system based on Internet protocols. Therefore, existing IP-based security authentication mechanisms, e.g., JFK (Just Fast Keying)[18], IKEv2 (Internet Key Exchange Protocol version 2)[19], SRP (Secure Remote Password)[20] that are proposed by EFIT (Internet Engineering Task Force), can be applied to implement heterogeneous access in BRAIN. SHAMAN focuses more on leveraging the advanced Public Key Cryptography to address security issues in the future generation of mobile communications.

Russia released "Russian Federal Space Program for 2006-2015" in 2005. This program enhances and improves the effectiveness of the space utilization to achieve the objectives of the Russian Federation, which cover economical, social, scientific, cultural and other areas, in addition to the benefits of the Russian security. Japan released "e-Japan Priority Policy Program", which proposed a novel heterogeneous network architecture named MIRAI ("future" in Japanese). MIRAI includes three basic entities: Common Core Network, Basic Access Network, and Multi-service Terminals. MIARI aims to introduce an flexible and extensible network architecture for the future generation of communication networks.

China started late on the research of SIN. Its main research can be classified into two categories: (1) analyzing and applying existing security schemes and protocols proposed by CCSDS; (2) designing improved security algorithms and protocols based on traditional techniques. In 2006, Rongjun Shen, an Academician of Chinese Academy of Engineering, pointed out the current situation that space-ground protocols are not unified for different spacecrafts in spaceflight missions[21]. Therefore, space mission data cannot be shared through one integrated network. He analysed the demand of future space missions and demonstrated the importance for China to develop its integrated SIN system. Shiquan Min surveyed the characteristics, compositions, architectures and protocol features of SIN[22]. He emphasized that security risks and security solutions for SIN must be considered ahead of time before designing and implementing SIN-based network protocols. Nowadays, SIN and related security research have been enacted asthe

preferential parts of the State Technology Support Plan. Besides, network security architecture and key security technologies for SIN have become a major research area for SIN.

Although the studies of security architecture for SIN have made progress in recent years, obstacles and challenges remain for SIN security in China. There mainly exist the following five challenges.

- No existing security model is suitable for describing the security risks for SIN.
- No formal definition describes the security features and security requirements for SIN.
- No thorough security architecture that satisfies the security requirements for SIN is introduced.
- No algorithm/protocol standards and no concrete algorithm/protocol schemes are formulated.
- No simulation and validation platforms are available to verify the efficiency and security of the schemes.

5 Security technologies and key security challenges

5.1 Formal security models

The security of existing algorithms and protocols for SIN are based on informally empirical analyses. They may have potential security loopholes when these algorithms and protocols are deployed in the real system. Therefore, a formal security model for SIN must be defined by considering the functionalities, characteristics, and security requirements of SIN. This is the foundation of SIN security research.

When defining the security model of SIN, the following four aspects should be considered.

- The security model should consider the capabilities of adversaries, including the services they can be obtained or accessed, the computation capabilities they may have, and the storage capabilities they may own.
- The security model should precisely define the security functionalities that SIN must have, that is, the security goal of SIN.
- The security model should formally define what the proposes of adversaries are, i.e., what results obtained by the adversaries imply that the system is definitely broken.
- The security model should give a security proof methodology so that the algorithm and protocol designers can follow the given methodology to prove the security of the proposed schemes.

In this way, the model will provide a sound foundation to ensure the security. The potential security loopholes will be theoretically covered by the model, so that the proposed schemes following the security model will be robust when being applied in SIN.

5.2 Lightweight cryptographic algorithms and protocols

Secure data transmission and processing in SIN need to meet complex requirements. The basic idea is to decompose requirements based on data processing procedures: data generation, data transmission, data storage, and data sharing. Then, one can propose corresponding algorithms, protocols, schemes to meet the different security requirements. There are existing cryptographic primitives, schemes and protocols proposed in SIN settings.

Lightweight and fast encryption. Since entities in space suffer from the limitations of computation and communication capabilities, lightweight and fast encryption schemes provide the tradeoff between efficiency and security. CCSDS has released the standard and recommendations for civil aviation, named “CCSDS Cryptographic Algorithms”[13]. In this standard, CCSDS analysed the candidate encryption and authentication algorithms for SIN. To ensure minimum security requirements, the standard recommended AES (Advanced Encryption Standard) to

be the primary encryption algorithm used in SIN[23]. There are five encryption modes in AES, namely ECB (Electronic Codebook Book), CBC (Cipher Block Chaining), OFB (Output FeedBack), CFB (Cipher FeedBack), and CTR (Counter). Among these modes, CTR is a relatively new mode that transforms AES to be a stream-like cipher. Also, this mode supports parallel encryption operations, which can be implemented efficiently by hardware. CCSDS recommended using the CTR mode in AES to encrypt data before transmitting. Zhen, et al.[24] proposed a new security architecture based on a lightweight public key scheme, DPK (Derivable Public Key). Then, combining DPK with AES, they introduced a lightweight encryption scheme by eliminating the need for distributing and storing public keys. In this way, their scheme supports authentication for broadcast communications. Bogdanov, et al.[25] proposed an AES-based ALE (Authenticated Lightweight Encryption) algorithm. The basic operation of ALE is the AES round transformation and the AES-128 key schedule. It is a single-pass authenticated encryption algorithm with high-speed parallel implementations. However, lightweight encryption algorithms aim at achieving the best bit rate. This may bring latent security loopholes for the designed schemes.

Encryption with error correction. In SIN, satellite channels have high burst errors caused by bad weather, cosmic rays, or electromagnetic disturbance. Hence, there is a need to ensure that the data transmitted in the channel are not modified or lost. Encryption with error correction can possibly solve the above challenge. Li, et al.[26] combined AES with LDPC (Low Density Parity Check Code) to design an AES-based encryption scheme with error correction. The proposed scheme is named SEEC (Satellite Encryption and Error Correction). By their simulation, the method shows a great error correction capability with encryption. Vladimirova, et al.[27] gave a security model on-board earth observation satellites. Combining AES with an error correction mechanism, they implemented a new hardware-based fault-tolerant algorithm. Aiming at small earth observation satellites, Banu and Vladimirova[28] presented a novel fault-tolerant enhancement of AES that can be applied in all five encryption modes of AES. The approach is based on the Hamming Error Correction Code. Implementation and simulation on a FPGA (Field Programmable Gate Array) showed that the proposed method has low-power overhead while achieving error correction in encryption.

Authenticated encryption. In SIN, cryptographic algorithms and protocols should guarantee the privacy and the authenticity of data being transmitted between two entities in a satellite channel. In practice, the system designers always acquire these two security requirements by separate algorithms and protocols, thus incurring additional computation and communication overhead. AE (Authentication Encryption) is a novel cryptographic primitive that meets both of these goals[29]. The ISO/IEC 19772:2009 standard for AE[30] defines generic composition Encrypt-then-MAC[31,32], and five dedicated AE schemes: OCB2 (Offset CodeBook 2)[33], SIV (Synthetic Initialization Vector)[34], CCM (Counter with CBC-MAC)[35], EAX (Environmental Audio Extensions)[36], and GCM (Galois/Counter Mode)[37]. CCSDS recommended using the GCM mode for AE[38], since it has minimum latency and minimum operation overhead, while the block cipher operations can be easily pipelined or parallelized. Zhang, et al.[39] adopted the GCM mode of AE in the context of space communications. They designed a framework of CCSDS tele-command system to provide the confidentiality, integrity and authentication of tele-command information by integrating the GCM intothe data link layer of the tele-command protocol. Weiss[40] discussed the development of the CCSDS algorithm standards, stating that AE is highly encouraged for all space missions in the GCM mode.

Key challenges. Entities in space suffer from lim-

itations of computation and communication capabilities. When applying existing schemes or designing new schemes for SIN, one must consider the storage and computation overheads. Therefore, selecting suitable cryptographic algorithms and protocols, or proposing new ones based on SIN, should consider the following properties.

- The cryptographic algorithms must be lightweight and fast. One possible selection may be the standards and recommendations published by CCSDS for civil aviation. However, it is necessary for the system designers to evaluate whether the standards by CCSDS are suitable for unified SIN.
- It will sometimes be necessary for the cryptographic algorithms to simultaneously achieve data confidentiality and data integrity. It will be even better if efficient cryptographic algorithms with error correcting capability are developed for SIN.
- It is desired to realize data authentication and data confidentiality in one procedure, where we design cryptographic algorithms and protocols with authentication capability.

5.3 Cross-domain key distribution & update

Since different sub-networks in SIN have different space missions and functionalities, each of sub-networks has deterministic security boundary. The system designers always consider sub-networks as individual network systems, and apply individual security algorithms and protocols. This leads to protocol incompatibility among sub-networks in SIN. Therefore, a key to establish an integrated SIN is to design cross-domain key distribution and key management schemes that can be applied in all sub-networks.

In general, the hierarchical centralized key management mode is encouraged for SIN. A global key management center, which is responsible for key management of the whole SIN, is deployed in the terrifical network. Sub-security domains are divided according to the functionalities of the sub-networks in SIN, each of which employs a second-tier individual key management center[41,42].

There are two kinds of keys to be managed, i.e., symmetric keys for fast encryption/decryption and asymmetric keys for key exchange and authentication. For symmetric key management, CCSDS recommended IKE protocol[10], which is part of ISAKMP (Internet Association and Key Management Protocol), to be the standard of key management in SIN. Although IKE provides a flexible and efficient key management mechanism, its operations are relatively complicated. Research has been carried out to introduce other key management techniques to SIN. Chen, et al.[43] introduced a self-verification authentication mechanism to support bidirectional authentication in key exchange. Their mechanism does not rely on PKI (Public Key Infrastructure), and requires interaction between nodes in the space and the trusted nodes on the ground. Wang, et al.[44] constructed a distributed multi-level security infrastructure for SIN, along with a multi-level key management model, authentication model, access control model, and intrusion detection model. The security of their work relies on the security of PKI.

PKI requires complicated certificate management. IBC (Identity-Based Cryptosystem) is an alternative to PKI in the key management system. In IBC, users' public keys are described by the users' identities so that there is no need for PKI to manage users' public keys nor their certificates. The concept of IBC was introduce by Shamir[45]. He also proposed a practical Identity-Based Signature scheme. However, it took a long time for researchers to construct practical IBE (Identity-Based Encryption) schemes, which make IBC applicable in practice. In 2001, Bonth and Franklin[46,47] leveraged the bilinear group algebra structure to construct the first practical IBE scheme that can be prov-

en secure in the random oracle model. Subsequently, Waters[48] and Gentry[49] respectively proposed IBE schemes that are secure in the standard model. In SIN settings, Luo, et al.[50] proposed an Identity-Based distributed key management scheme that can solve the problems of concentrating key management and over-consumption on certificate maintenance in SIN.

As an extension of IBE, HIBE (Hierarchical IBE) models users in a hierarchy, which is applicable in SIN for managing users in a hierarchy manner. In 2002, Horwitz and Lynn[51] introduced the concept of HIBE, and constructed a practical HIBE scheme supporting 2-level hierarchy. The first fully functional HIBE scheme was subsequently introduced by Gentry and Silverberg[52]. Several HIBE schemes were later constructed to meet various functionality[53] and security requirements[54]. Howarth, et al.[55] addressed efficient hierarchical key management in SIN. They proposed and analysed an interworking solution between multilayer IPSec (Internet Protocol Security) and LKH (Logical Key Hierarchy) which performs key management with low traffic costs. Roy-Chowdhury, et al.[1] suggested a hierarchical key management approach for adding data security to group communication in SIN.

For multicasting in SIN, Hubenko, et al.[56] presented a novel multicasting architecture to increase system scalability for secure key management in the LEO system of SIN. Sun, et al.[57] proposed SMGKM (Satellite Multiple Group Key Management), supporting both group and subgroup key management. Their scheme is suitable for multiple group key management under dynamic satellite multicast environment. In 2014, Liu, et al.[58] introduced a new cryptographic primitive, called HIBBE (Hierarchical Identity-Based Broadcast Encryption), which extended HIBE to support broadcast. Recent results show that HIBBE is suitable for supporting distributed key management and secure communications[59,60].

Key challenges. Although advanced cryptographic primitives, e.g., IBE, HIBE, HIBBE, have specific attractive features, they require the algebra structure of bilinear groups and algebra operations of high computation cost. Unless there is a major breakthrough to improve the efficiency of the algebra operations in bilinear groups, the alternative solution is to deploy PKI (Public Key Infrastructures) for realizing unified key management. The heterogeneity of SIN requires hierarchical PKI. Therefore, a key challenge is to correctly design root PKI, while connecting distributed PKI in a hierarchical manner by the help of trusted chain technique. The following research needs to be carried out for key management in SIN.

- Designing dynamic trusted models for SIN.
- Proposing key distribution and key update schemes that can effectively manage keys used for end-to-end data encryption and entity authentication.
- Developing lightweight cryptographic protocols for key exchange, key update and key revocation.

5.4 Efficient access authentication

Access authentication mechanism is to prevent unauthorized devices or terminals from accessing SIN. When a node tries to access SIN, the identity and the privilege of that user should be authenticated, and only the legitimate ones are able to access. When a node wishes to communicate with other entities in SIN, a bidirectional authentication procedure should be executed to distinguish an illegal entity from a legitimate one.

In SIN, access authentication can be classified into two categories: handoff authentication and access control. Handoff authentication, on one hand, ensures that mobile entities in SIN can be efficiently handoff to adjacent routers or switchers for maintaining seamless communication services. We say horizontal handoff if a node requires handoff when moving

in the same layer of the sub-network, and vertical handoff if a node requires cross-domain sub-network handoff. Handoff in the same sub-network, i.e., horizontal handoff, is simple and efficient, since security architectures, algorithms and protocols can be designed in an unified way. However, vertical handoff should be designed by considering different security mechanisms among several sub-networks. Liu, et al.[61] analysed the general mobility models of mobile nodes and identified a set of performance evaluation models. Based on the proposed models, they presented a novel vertical handoff decision algorithm, named SAVA (Self-Adaptive Vertical handoff Algorithm). Huang, et al.[62] presented SAPs (Seamless Authentication Protocols) for vertical handoff in wireless heterogeneous networks to reduce authentication delay. Khan, et al.[63] presented security handover schemes for vertical handover in heterogeneous wireless networks.

Access control, on the other hand, ensures that new entities must be authorized whenever, wherever and whoever they request to access the network. Chen and Dirk-Japp Plas[64] addressed end-user authentication at the network level. They provided transparent end-user authentication schemes based on the UMTS (Universal Mobile Telecommunications System) authentication framework. To implement security control mechanisms in SIN, Guo, et al.[65] presented a bidirectional authentication and key negotiation protocol with a signature-based authentication scheme by using the Diffie-Hellman key exchange technique. They leveraged a universal composition security model[66,67] to prove its security. Moreover, WAPI (WLAN Authentication and Privacy Infrastructure), WEP (Wired Equivalent Privacy), 802.11i, and TPM (Trusted Platform Module)[68] also have potential to be applied for access control in SIN.

Key challenges. When a mobile terminal or a ground node accesses SIN, the system needs to verify the user identity by appropriate authentication protocols depending on which sub-network the user belongs to. The user may access the entity or acquire service which belongs to another sub-network of SIN. In this situation, when there is no SA (Security Association) between these two sub-networks, it requires the existence of RA (Roaming Agreement), allowing users to dynamically generatea temporary and valid SA associated with his accessing sub-network, thus realizing secure access. Existing access frameworks and authentication protocols more or less have some deficiencies. For example, UMTS-AKA (Universal Mobile Telecommunications System Authentication and Key Agreement) is over-complicated[69], while EAP-AKA (Extensible Authentication Protocol for Authentication and Key Agreement) cannot provide identity privacy[70]. It is strongly recommended to design new authentication frameworksand lightweight authentication protocols to meet the security access requirements. The following topics are potential research areas for access authentication of SIN.

- Designing unified authentication frameworks.
- Proposing trusted secure access control mechanisms for user access authentication.
- Introducing efficient horizontal handoff/vertical handoff authentication schemes.
- Realizing dynamic detection and protection methods to prevent latent attacks.

6 Conclusion

In this article, we have defined an abstract network architecture of SIN, and identified security risks and challenges of SIN. We also identified research problems and key technologies for securing SIN. Space is the chief strategic resource for a nation. There is still a big gap in theoretical and technological research for implementing integrated SIN, especially in China. It is of great importance for studying and developing key security technologies for SIN.

References

[1] ROY-CHOWDHURY A, BARASJOHN S, HADJITHEODOSIOU M, et al. Security issues in hybrid networks with a satellite component[J]. IEEE wireless communications, 2005, 12(6): 50-61.

[2] WIKIPEDIA. Iran-U.S. RQ-170 Incident[EB/OL]. 2011. https://en.wikipedia.org/wiki/Iran-U.S._RQ-170_incident.

[3] MAJUMDAR D. Iran's captured RQ-170: How bad is the damage?[EB/OL]. 2011. http://www.airforcetimes.com/news/2011/12/defense-iran-captured-rq-170-how-bad-120911/.

[4] WARNER J S, JOHNSTON R G. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing[J]. Journal of security administration, 2002, 25(2): 19-27.

[5] WIKIPEDIA. Death of muammar gaddafi[EB/OL]. 2011. https://en.wikipedia.org/wiki/Death of Muammar Caddafi.

[6] MUKHERJEE J, RAMAMURTHY B. Communication technologies and architectures for space network and interplanetary internet[J]. IEEE communications surveys and tutorials, 2013, 15(2): 881-897.

[7] LIU J, LIU C, GUO K. A key management and authentication model for ad hoc network[C]//Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), c2007: 1-5.

[8] CCSDS 713.5-B-1. Space communication protocol specification (SCPS)-security protocol[S]. The Consultative Committee for Space Data Systems (CCSDS), 1999.

[9] CCSDS 733.5-O-0.1. Next generation space internet (NGSI) - end-to-end security for space mission communications[S]. The Consultative Committee for Space Data Systems (CCSDS), 2003.

[10] RFC 2409. The Internet key exchange (IKE)[Z]. Network Working Group, 1998.

[11] CCSDS 350.1-G-1. Security threats against space missions[S]. The Consultative Committee for Space Data Systems (CCSDS), 2006.

[12] CCSDS 350.0-G-2. The application of CCSDS protocols to secure systems[S]. The Consultative Committee for Space Data Systems (CCSDS), 2006.

[13] CCSDS 350.9-G-1. CCSDS cryptographic algorithms[S]. The Consultative Committee for Space Data Systems (CCSDS), 2014.

[14] CCSDS 351.0-M-1. Security architecture for space data systems[S]. The Consultative Committee for Space Data Systems (CCSDS), 2012.

[15] ALBERTS D S, GARSTKA J J, STEIN F P. Network centric warfare: developing and leveraging information superiority[M]. Command and Control Research Program Publication Series, 2000.

[16] SIMONSEN E. Integrated defense systems[EB/OL]. https://www.boeing.com/news/frontiers/archive/2005/october/i_ids3 html.

[17] MOHR W. Broadband radio access for IP-based networks in the IST BRAIN project[C]//Proceedings of the International Conference on Telecommunications (ICT 2000), c2000: 22-25.

[18] AIELLO W, BELLOVIN S M, BLAZE M, et al. Just fast keying: Key agreement in a hostile internet[J]. ACM transactions on information and system security, 2004, 7(2): 242-273.

[19] ERONEN P. Internet key exchange protocol version 2 (IKEv2)[S]. Internet Engineering Task Force (ITEF). 2010.

[20] WU T. The SRP authentication and key exchange system[S]. Internet Engineering Task Force (ITEF). 2000.

[21] SHEN R J. Some thoughts of Chinese integrated space-ground network system[J]. Engineering science, 2006, 8(10): 19-30.

[22] MIN S. Discussion on space-based integrated information network[J]. Space international, 2013, 8: 46-54.

[23] DAEMEN J, VINCENT R. The design of Rijndael: AES-the advanced encryption standard[M]. Berlin Heidelberg: Springer, 2002.

[24] ZHEN J, LI J, LEE M J, et al. A lightweight encryption and authentication scheme for wireless sensor networks[J]. International journal of security and networks, 2006, 1(3-4): 138-146.

[25] BOGDANOV A, MENDEL F, REGAZZONI F, et al. ALE: AES-based lightweight authenticated encryption[C]//Proceedings of the 20th International Workshop on Fast Software Encryption (FSE 2013), Singapore, c2013: 447-466.

[26] LI N, LIN K, LIN W, et al. A joint encryption and error correction method used in satellite communications[J]. China communications, 2014, 11(3): 70-79.

[27] VLADIMIROVA T, BANU R, SWEETING M. On-board security services in small satellites[C]//Proceedings of the IEEE 23rd International Conference on Geoscience and Remote Sensing Symposium (IGARSS 2006), c2006. 1-15.

[28] BANU R, VLADIMIROVA T. Fault-tolerant encryption for space applications[J]. IEEE transactions on aerospace and electronic systems, 2009, 45(1): 266-279.

[29] FLEISCHMANN E, FORLER C, LUCKS S. McOE: a family of almost foolproof on-line authenticated encryption schemes[C]//Proceedings of the 19th International Workshop on Fast Software Encryption (FSE 2012), c2012: 196-215.

[30] ISO/IEC 19772:2009. Information security-Security techniques-Authenticated Encryption[S]. International Organization for Standardization, 2009.

[31] BELLARE M, NAMPREMPRE C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm[C]//Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2000), c1976: 531-545.

[32] BELLARE M, NAMPREMPRE C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm[J]. Journal of cryptology, 2008, 21(4): 469-491.

[33] ROGAWAY P. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC[C]//Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2004), c2004: 16-31.

[34] ROGAWAY P, SHRIMPTON T. A provable-security treatment of the key-wrap problem[C]//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic

Techniques (EUROCRYPT 2006), c2006: 373-390.
[35] DWORKIN M J. Special Publication 800-38C: recommendation for block cipher modes of operation: the ccm mode for authentication and confidentiality[S]. National Institute of Standards and Technology, 2005.
[36] BELLARE M, ROGAWAY P, WAGNER D. The EAX mode of operation[C]//Proceedings of the 11th International Workshop on Fast Software Encryption (FSE 2004), c2004: 389-407.
[37] MCGREW D A, VIEGA J. The security and performance of the Galois/Counter Mode (GCM) of operation[C]//Proceedings of the 5th International Conference on Cryptology in India (INDOCRYPT 2004), c2004: 343-355.
[38] DWORKIN M J. Special Publication 800-38D: recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC[S]. National Institute of Standards and Technology, 2007.
[39] ZHANG L, ZHOU J, TANG C. Research on application of AEAD techniques for CCSDS telecommand protocol[J]. Journal of electronics and information security, 2009, 31(2): 343-348.
[40] WEISS H. CCSDS standardization of security algorithms for civil space missions[S]. American Institute of Aeronautics and Astronzautics, 2012.
[41] LYU X, MU Y, LI H. Non-interactive key establishment for bundle security protocol of space DTNs[J]. IEEE transactions on information forensics and security, 2014, 9(1): 5-13.
[42] ZHOU J, SONG M, SONG J, et al. Autonomic group key management in deep space DTN[J]. Wireless personal communications, 2014, 77(1): 269-287.
[43] CHENG T H, LEE W B, CHEN H B. A self-verification authentication mechanism for mobile satellite communication systems[J]. Computers and electrical engineering, 2009, 35(1): 41-48.
[44] WANG Y, LU Y, WU Z, et al. Constructing multi-level and multilayer security infrastructure of space information system[J]. Journal of astronautics, 2007, 28(5): 1081-1085.
[45] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of the 14th Annual International Cryptology Conference Santa Barbara (CRYPTO 1984), c1984: 47-53.
[46] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Proceedings of the 21st Annual International Cryptology Conference (CRYPTO 2001), c2001: 213-229.
[47] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[J]. SIAM journal on computing, 2003, 32(3): 586-615.
[48] WATERS B. Efficient identity-based encryption without random oracles[C]//Proceedings of the 23rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2005), c2005: 114-127.
[49] GENTRY C. Practical identity-based encryption without random oracles[C]//Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2006), c2006: 445-464.
[50] LUO C, LI W, XING H, et al. Research on identity-based distributed key management in space network[J]. China communications, 2010, 32(1): 183-188.
[51] HORWITZ J, LYNN B. Toward hierarchical identity-based encryption[C]//Proceedings of the 20th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2002), c2002: 466-481.
[52] GENTRY C, SILVERBERG A. Hierarchical ID-based cryptography[C]//Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2002), c2002: 548-566.
[53] GENTRY C, HALEVI S. Hierarchical identity based encryption with polynomially many levels[C]//Proceedings of the 6th Theory of Cryptography Conference (TCC 2009), c2009: 437-456.
[54] LEWKO A, WATERS B. New techniques for dual system encryption and fully secure HIBE with short ciphertexts[C]//Proceedings of the 7th Theory of Cryptography Conference (TCC 2010), c2010: 455-479.
[55] HOWARTH M P, IYENGAR S, SUN Z, et al. Dynamics of key management in secure satellite multicast[J]. IEEE journal on selected areas in communications, 2004, 22(2): 308-319.
[56] HUBENKO J V, RAINES R, BALDWIN R, et al. A secure and efficient satellite-based multicast architecture[C]//IEEE Radio and Wireless Symposium, FL, USA, c2008: 227-230.
[57] SUN Y, MA H, ZHENG G, et al. Multiple group shared key management for satellite multicast[J]. Journal of astronautics, 2013, 34(6): 824-832.
[58] LIU W, LIU J, WU Q, et al. Hierarchical identity-based broadcast encryption[C]//Proceedings of the 19th Australasian Conference on Information Security and Privacy (ACISP 2014), c2014: 242-257.
[59] LIU W, LIU X, LIU J, et al. Auditing and revocation enabled role-based access control over outsourced private EHRs[C]//Proceedings of the 17th International Conference on High Performance Computing and Communications (HPCC 2015), New York, USA, c2015: 336-341.
[60] LIU W, LIU J, WU Q, et al. Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption[J]. International journal of information security, 2016, 15(1): 35-50.
[61] LIU M, LI Z, GUO X, et al. Evaluation and improvement of vertical handoff algorithms in heterogeneous wireless networks[J]. Journal of software, 2007, 11(3): 1652-1659.
[62] HUANG S C, ZHU H, ZHANG W. SAP: seamless authentication protocol for vertical handoff in heterogeneous wireless networks[C]//Proceedings of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE 2006), Seoul, South Korea, c2006.
[63] KHAN M W. Secure and efficient vertical handover in heterogeneous wireless networks[J]. International journal of advanced networking and applications, 2013, 5(2): 1908-1912.
[64] CHEN H, PLAS D. Transparent end-user authentication across heterogeneous wireless networks[C]//Proceedings of the IEEE 58th Vehicular Technology Conference (VTC 2003), Orlando, Florida, USA, c2003: 2088-2092.
[65] GUO Y, WANG C, WANG L. Universally composable authen-

tication and key exchange protocol for access control in spatial information networks[J]. Acta electronica sinica, 2010, 38(10): 2358-2364.

[66] CANETTI R. Universally composable security: A new paradigm for cryptographic protocols[C]//Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS 2001), Las Vegas, Nevada, USA, c2001: 136-145.

[67] CANETTI R, KRAWCZYK H. Universally composable notions of key exchange and secure channels[C]//Proceedings of the 20th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2002), c2002: 337-351.

[68] SHEN C, ZHANG H, WANG H, et al. Researches and developes of trusted computing[J]. Scientia sinica: informationis, 2010, 40(2): 139-166.

[69] MJØLSNES S, TSAY J. Computational security analysis of the UMTS and LTE authentication and key agreement protocols[S]. Cornell University Library. 2012.

[70] MUN H, HAN K, KIM K. 3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA[C]//Proceedings of the IEEE Wireless Telecommunications Symposium (WTS 2009), Prague, Czechoslovakia, c2009: 1-8.

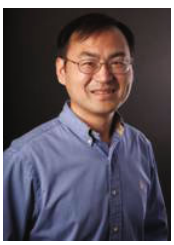
About the authors

LIU Jianwei was born in Shandong. He received the B.S. and M.S. degrees in Electronic and Information from Shandong University, Shandong, China in 1985 and 1988, respectively. He received his Ph.D. degree in Communication and Electronic System from Xidian University Shaanxi, China in 1998. He is now a professor of Electronic and Information Engineering at Beihang University, Beijing, China. His current research interests include wireless communication network, cryptography, and information & network security. (Email: liujianwei@buaa.edu.cn)

LIU Weiran [corresponding author] was born in Beijing. He received the B.S. degree from Beihang University, Beijing, China in 2012. He is currently working toward the Ph.D. degree in Electronic and Information Engineering, Beihang University, Beijing, China. His research interests include applied cryptography and cloud security. (Email: liuweiran900217@gmail.com)

WU Qianhong was born in Sichuan. He received the Ph.D. degree in Cryptography from Xidian University, Shaanxi, China in 2004. Since then, he has been with Wollongong University (Australia) as an associate research fellow, with Wuhan University (China) as an associate professor, with Universitat Rovira i Virgili (Catalonia) as a research director, and now with Beihang University (China) as a professor. He is a member of IACR, ACM and IEEE. His current research interests include cryptography, data security and privacy, and information theory. (Email: qianhong.wu@buaa.edu.cn)

LI Dawei was born in Shandong. He received the B.S. degree from Beihang University, Beijing, China in 2015. He is currently working toward the Ph.D. degree in Electronic and Information Engineering, Beihang University, Beijing, China. His research interests include applied cryptography and mobile security. (Email: lidaweibuaa@163.com)



CHEN Shigang received the B.S. degree in computer science from the University of Science and Technology of China in 1993. He received the M.S. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 1996 and 1999, respectively. After graduation, he was with Cisco Systems for three years before joining the University of Florida in 2002. He served on the technical advisory board for Protego Networks in 2002-2003. He now is a professor with the Department of Computer and Information Science and Engineering at the University of Florida. His research interests include computer networks, Internet security, wireless communications, and distributed computing. He received IEEE Communications Society Best Tutorial Paper Award in 1999 and US National science Foundation (NSF) CAREER Award in 2007. He holds 12 US patents. He is an associate editor for IEEE/ACM Transactions on Networking. He is an IEEE fellow. (Email: sgchen@cise.ufl.edu)