Key Management Infrastructure and Application Supporting Framework based on Beidou Satellite Navigation System

Yu Wang[1], Wei jie Han[1], Yuan Tian[2]

[1] Department of Information Equipment Equipment Academy Beijing, China
[2] Department of Graduate Management Equipment Academy Beijing, China
zenheart@126.com, aashin@126.com

Abstract - Beidou Satellite Navigation System can provide accurate time services, location services, speed services, safe and reliable short message service for end users. The paper establishes key management infrastructure and application supporting framework on the basis of Beidou Satellite Navigation System, propose a key distribution and management scheme, designs a identity authentication method based on Beidou's accurate time services and identity authentication method against cheating based on Beidou's RDSS and RNSS. This solution will provide strong support for the security system construction of Beidou Satellite Navigation System.

Index Terms - Beidou Satellite Navigation System, Key management infrastructure, identity authentication

1. Introduction

Traditional key management infrastructure and application supporting framework [1] consists core layer, client layer, agent layer, service layer and system layer. Core layer implements the management of key generation, key distribution, key renewal and key recovery. Client layer supports terminal devices, management and application of user keys. Agent layer fulfills the task of key management and application with servers on the behalf of clients. Service layer provide access control, security audit, integrity protection for service application system. System layer provide specific security system support.

Beidou Satellite Navigation System [2] can provide accurate time services, location services, speed services, safe and reliable short message service for end users. On the basis of these characteristics, the establishment of key management infrastructure and application supporting framework, will overcome the shortcoming of key distribution difficulty using symmetric key system. It will also reduce complexity of key management using public key cryptosystem. Through the safe, trust short message channel of Beidou, it achieves cross-domain distributed key distribution. It provides accurate timestamp for network user, which is needed by identity authentication and key exchange. It effectively prevents replay attacks and improve the security and efficiency of protocol. It achieves fine-grained access control and accurate key division, based on Beidou network users' location, speed, time attributes. This way improves the system's safety and control. For this purpose, the article proposes a security infrastructure, as well as the method of key distribution and management. It takes identity authentication as an example to further illustrate the advantage of this information security protection system based on Beidou satellite navigation system.

2. Security Infrastructure Architecture Based On Beidou Satellite Navigation System

Key management infrastructure and application supporting framework based on Beidou Satellite Navigation System implements management strategy based on target node location and time characteristics, using location, speed, time information supplied by Beidou Satellite Navigation System. The strategy is core of application supporting framework, which support upper-layer application, as shown in Fig. 1.The concrete strategy includes:

(1) Based on Beidou network users' location information, it issues digital certificates restricted by space area.

(2) Based on Beidou network users' time information, it issues digital certificates restricted by time.

(3) Based on Beidou network users' location information, it updates unicast keys, multicast keys, and initial password.

(4) Based on Beidou network users' time information, it updates unicast keys, multicast keys, and initial password.

In client layer, it realizes digital signature, negotiation and distribution of session keys and multicast key[3], based on location, speed, time information provided by Beidou Satellite Navigation System. Including:

(1) It provides RDSS based key distribution, using Beidou's trust channel.

(2) It provides key management based on time and space domain, using Beidou's location, speed, time information.

Agent layer fulfills the task of key management and application with servers on the behalf of clients. It implements access control, authorization service, security audit services, one-time password generation service and identity authentication service, based on Beidou Satellite Navigation System's key distribution gateway, identity authentication system, access control system, message transmission system, security audit system. Including:

(1) Fair service based on Beidou's precision time.

(2) One-time password generation service based on Beidou's precision time.

(3) Identity authentication service based on precise timestamp and location information.

(4) Digital signature service based on Beidou's location, time, speed characters.

(5) Fine-grained access control and authorization service based on Beidou's location, time, speed characters.

(6) security audit services based on Beidou's location, time, speed characters.

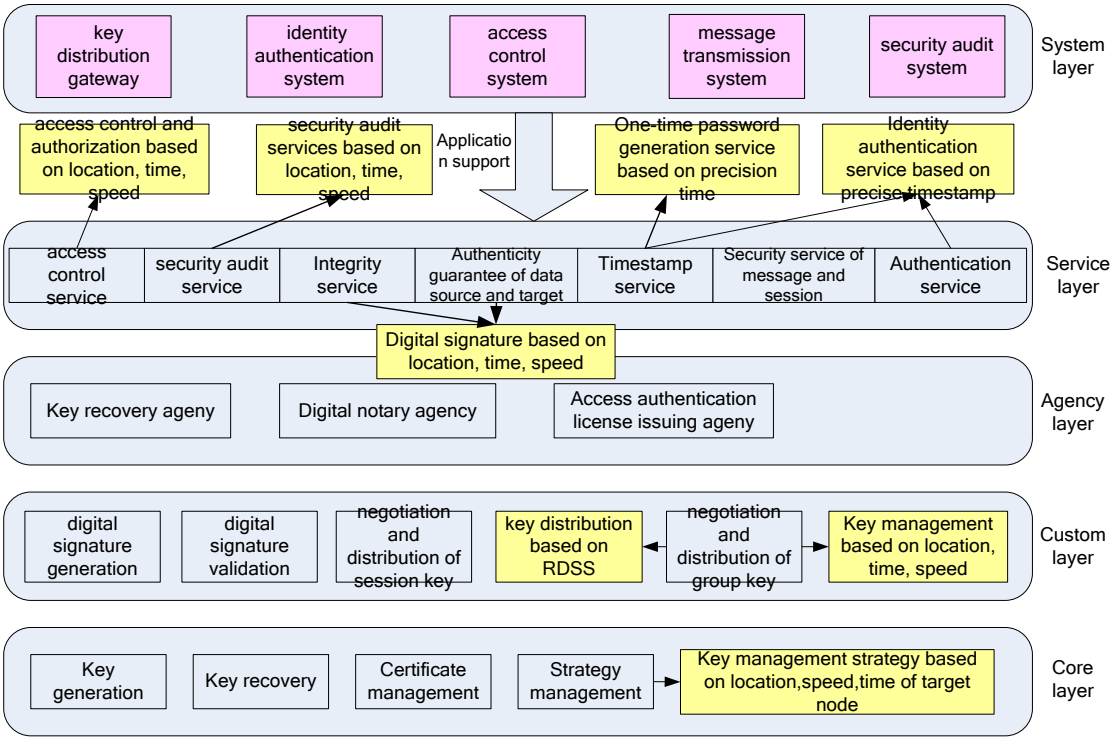

Fig. 1 Key management infrastructure and application supporting framework based on Beidou's RDSS and RNSS sketch

3. Key Management Method based on Beidou Satellite Navigation System

Key management is the infrastructure of information system and network security protection system. Key management includes key generation, distribution, negotiation, update, recovery and destruction. It is the basic of data encryption, identity authentication, integrity protection, access control, security audit services.

In the traditional key management system, the initial master key is distributed manually. It is safe, trust, reliable. But session key is exchanged through unsafe, unreliable channels. Key management is either based on one-key cryptosystem. or, based on public key cryptosystem. The former cannot meet the requirement of key distribution on a large scale, The latter can meet the requirement but the management of public digital certificates is complex. Beidou Satellite Navigation System will provide users accurate time services, location services, speed services, safe and reliable short message service. The trust RDSS and RNSS system based on Beidou Satellite Navigation System, will distribute keys for users in untrusted network, safely and reliably. It will solve the problem of key distribution difficult in traditional key management system.

In the process of key distribution, Beidou network user access Beidou Satellite Navigation System through active network terminal. Then registration is completed in key management center. key management center realizes Beidou network users' unicast and multicast key distribution in active or passive way using short message secure channel provided by Beidou's RDSS, according to network users' request and preset management strategy. The keys include key pair in public key cryptosystem, key in one-key cryptosystem, the seeds of dynamic password key. The method can effectively solve the security problem of traditional key distribution through untrusted channel, and also it reduces complexity of key distribution. As shown is Fig. 2.

According to Beidou network users' application fields, scenarios, range, it divides users into different management domains, using time and location information provided by Beidou Satellite Navigation System. Each domain has a key management center. It is responsible for network users' key distribution in a domain.

Aim at key management center based on public key cryptosystem(equivalent to public key infrastructure's certificate Authority), this framework constructs hierarchical key management system in, using safe channel provided by Beidou RDSS. It implements hierarchy administration. For Beidou network users in different key management domain, key distribution and trust relationship is constructed through upper key management center.

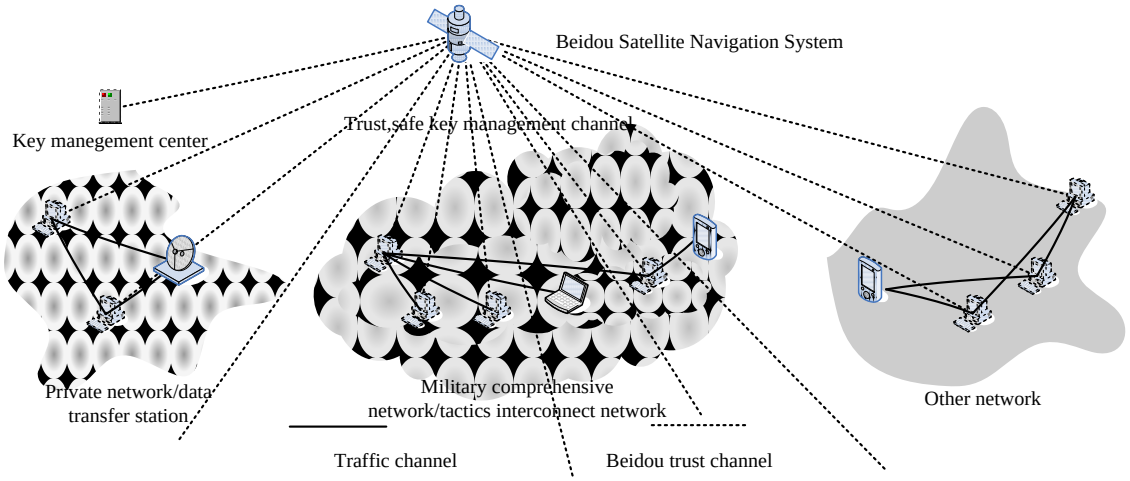

Fig. 2 Key distribution sketch based on Beidou Satellite Navigation System

Aim at key management center based on one-key cryptosystem (equivalent to Key Distribution center), this framework constructs equivalent key management system in, using safe channel provided by Beidou RDSS. It implements P2P reliable key distribution management. The key management center trust with each other. It provide key backup on demand. It further increases the robustness. As shown in Fig. 3.

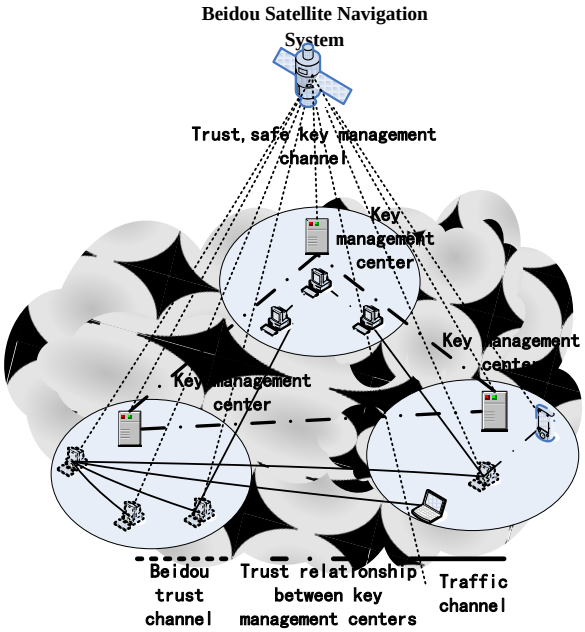

Fig. 3 equivalent key management system sketch based on Beidou Satellite Navigation System

4. Identity Management Methods based on Beidou Satellite Navigation System

Acknowledgment

Whether based on one-key cryptosystem or public key cryptosystem[4], in order to effectively resist message replay attack and parallel session attack, identity authentication protocol usually user timestamp or nonce to ensure timeliness of authentication information. But, the biggest difficulty of timestamp is precise synchronization between communication parties. The shortcoming of dynamic nonce is low efficiency of protocol.

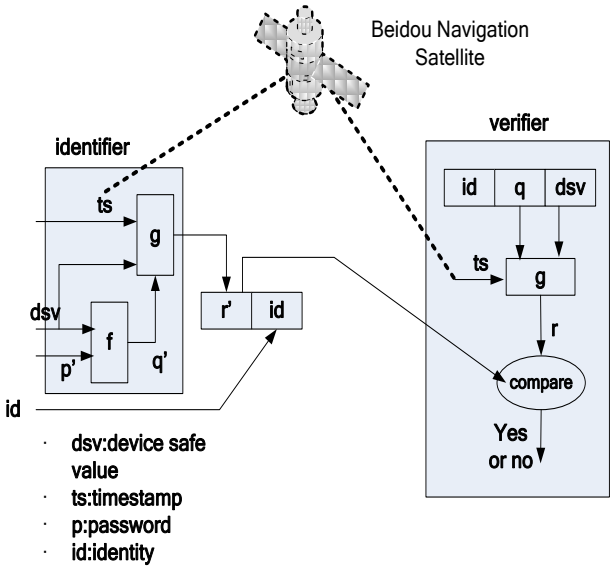

Fig. 4 Identity authentication based on Beidou precise clock

Beidou Satellite Navigation System will provide users precise time service. Through secure channel, it provides accurate timestamp for network user, that is needed by identity authentication and key exchange. It provides precise clock synchronization for one-time password generation, which is needed by protocol based on dynamic password authentication. It not only prevents replay attack, but improves security of authentication exchange, efficiency of identity authentication. In addition, Beidou Satellite Navigation System can provide users precise location service. It will detect the attacks that attackers pretend to be valid users to complete identity fraud on different geographic location.

The identity management methods based on Beidou's RDSS and RNSS construct an integrated, trusted, uniform identity directory system that covers all the users. It uses the unique terminal identifiers, which link to Beidou users' attribute information. This system can also realize reliable identity management of Beidou network users, using speed and location information provided by Beidou Satellite Navigation System.

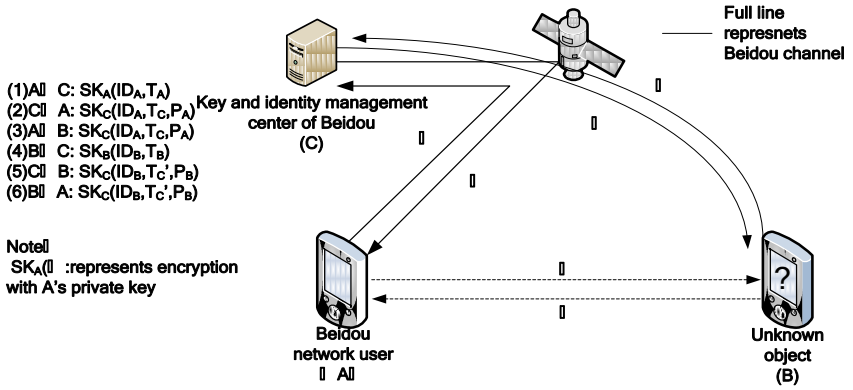

Fig. 5 identity authentication method against cheating based on Beidou RDSS and RNSS

Using time information provided by Beidou Satellite Navigation System, it implement Beidou users' identity authentication based on timestamp. It realizes precise clock synchronization for one-time password, as shown in Fig. 4

When a Beidou network user verifies an unknown object's identity, in order to prevent identity fraud, it detect whether it is a deceitful user. Take the identity authentication protocol based on public key cryptosystem as an example; the steps are as follows :(as shown in Fig. 5)

(1) Beidou network user A send the authentication request to key and identity management center C. A signs the message with its private key, which contains its identity IDA, current timestamp TC and its current location PA.The signed message is sent to C through Beidou channel.

(2) Key and identity management center C verified A's signature with public key. If the signature is legal, it signs the message with its private key that contains A's identity IDA, current timestamp TC and A's current location PA. The message is returned to A.

(3) Beidou user A forward the message from C.

(4) B verifies whether the signature is legal, with C's public key. It verifies whether the timestamp TC is legal and location PA is correct. If it pass the validation, A's identity is correct. Then B signs the message with its private key, that contain B's identity IDB, current timestamp TB. The message is sent to C through Beidou's channel.

(5) Key and identity management center C verifies the message from B with B's public key. If the signature is valid, it verifies timestamp TB. Then it signs the message with its private key, which contain B's identity IDB, current timestamp TC, B's current location PB. The message is returned to B.

(6) B forwards the message from C to A. A verifies the signature with C's public key, verified timestamp TC and B's location. If it pass the validation, B's identity is correct.

The advantages of this method are: Key and identity management center C is trusted third party. Timestamp provided by Beidou Satellite Navigation System can resist replay attacks. It can detect the attacks that attackers pretend to be valid users to complete identity fraud on different geographic location. From the aspects of time and space, it further improves reliability of identity authentication.

The authentication method authenticates both A and B. If only B is needed to authenticate, it can be simplified as (1),(2),(3). In addition, in authentication protocol based on one-key cryptosystem, time and location information provided by Beidou Satellite Navigation System can also be added to improve reliability and safety of identity authentication.

4. Conclusion

Compared with current key and identity management system, Key management infrastructure and application supporting framework based on Beidou Satellite Navigation System uses Beidou network user's time, location, speed information to distribute keys dynamically in real time. It implements centralized management of identity and keys. It provides fine-grained access control. It has the characteristics of high security, expandability, low management costs, wide application range.

References

[1] M. King, B. Zhu, and S. Tang, "Optimal path planning," *Mobile Robots*, vol. 8, no. 2, pp. 520-531, March 2001.

[2] H. Simpson, *Dumb Robots*, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.

[3] M. King and B. Zhu, "Gaming strategies," in Path Planning to the West, vol. II, S. Tang and M. King, Eds. Xian: Jiaoda Press, 1998, pp. 158-176.

[4] B. Simpson, et al, "Title of paper goes here if known," unpublished.

[5] J.-G. Lu, "Title of paper with only the first word capitalized," *J. Name Stand. Abbrev.*, in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Translated J. Magn. Japan*, vol. 2, pp. 740-741, August 1987 [*Digest 9th Annual Conf. Magnetics Japan*, p. 301, 1982].

[7] M. Young, *The Technical Writer's Handbook*, Mill Valley, CA: University Science, 1989.