The Research on NSSC Key Service Mechanism in Mobile Network

Zhiyi Fang[1.a],Ying Wang[1.b], Zelin Deng[2.c]，Fan Yang[2.d]

[1]College of Computer Science and Technology Jilin University Changchun, 130012, P.R. China

[2] Beijing ACEWAY Telecom Technology Co., Ltd

[a]fangzy@jlu.edu.cn,[b]yingw0517@stu.snnu.edu.cn,[c]dengzl@aceway.com.cn,[d]yangfan@aceway.com.cn

Keywords: NSSC, security, hybrid encryption method, DES, RSA

Abstract. Network Security Service Center (NSSC) is responsible for key distribution in network communication. This paper focuses on the security of key management mechanisms of mobile network service center, based on the traditional method of Key generation, and makes a certain research on the key generation algorithm. Analyzing the two traditional encryption algorithms: DES and RSA, this paper presents a hybrid encryption method which could apply to the network security service center (NSSC). Through comparative analysis, it proved the effectiveness and practicality of the hybrid encryption method (D_R).

Introduction

With the rapid development of wireless networks, the potential hazards are becoming increasingly prominent. Different from the traditional network, the characteristics of the mobile network node distribution dense, limited bandwidth, limited storage space and computing power, open to the environment, vulnerable to a variety of attacks and some other features, this makes it more difficult to obtain a higher level of security in a wireless network, transmission security issues is one of the particularly important issues. Key encryption transmission was the way to solve this problem. Generally, the generation and distribution of the Key is responsible for managing by the NSSC. It is defined as follows: If two users want to engage in a dialogue, before the dialogue they should to agree on a session key, because they do not have a session key, the key transfer cannot be transmitted in plaintext, so both need a trusted third party to help them through the key distribution. This third party is called Network Security Service Centre (NSSC).In this paper, choose the latter, Receiver gets the key from the initiator. By analysing the distribution of the key in security service centre, we conducted in-depth research on the choice of the key generation algorithm.

Related work

(a).Network Security Service Centre

Mobile security key distribution mainly has two ways: the receiver gets keys from NSSC and receiver gets the key from the originators, as shown in the Fig below:

Method of Fig 1 there is a problem: if A is the initiate of the dialogue, sending message M to B, then the receiver B should get the key E (kb, ks) from NSSC , and then get a message E (ks, M) from A , so that B can decrypt the received M. But B is likely to receive an encrypted message first, then gets the keys, and so cannot be to decrypt the message. Fig 2’s method is more convenient: NSSC transmits E (ka, kb) and E (kb, ks) to A, again by a transfers E (kb, ks) to B, A and B get key of ks, then a sends message to B. In this article security service center uses the second security services architecture , that avoids the responder side B’s packet which arrives ahead of the key, which is treated as rubbish disposal in Fig (a), to save the link bandwidth, shorter the time of packet distribution, but also improves the efficiency of communication.

(b).DES Encryption Algorithm

The earliest, the most famous secret key and symmetric key encryption algorithm DES (Data Encryption Standard) is developed by IBM in the 70s. DES is selected by American government in government's encryption standard, and then accepted by the National Bureau of Standards and the American National Standards Institute. The diagram below shows the schematic diagram of DES.

DES use 56-bit key to encrypt 64-bit data block. There are 16 identical stages of encryption processing, termed rounds. The keys used for each rounds are generated by the original 56-bit key.

(c). RSA Encryption Algorithm

RSA algorithm is the first only used for data encryption can be used for digital signature algorithms. It is easy to understand and operate, and very popular. Algorithm name to inventor named: Ron Rivest, Adi Shamir and Leonard Adleman. However, the security of RSA has not been proved theoretically. It has gone through a variety of attacks, has not been completely broken.

RSA's security depends on the decomposition of large numbers, but is equivalent to the integer factorization has not been proved theoretically. Suppose there is an algorithm without factoring large numbers, and then it certainly can be modified to become integer factorization algorithms. Currently, RSA algorithms have been some variants proved equivalent to integer factorization. Anyway, where n is the most obvious decomposition method of attack. Now, it has been able to break down more decimal place large prime numbers. Therefore, the modulus n must be selected larger, depending on the specific case.

A new hybrid (D_R) encryption mechanism

(a) Overview of Network Security Service Centre

NSSC is defined as follows: If two users want to engage in a dialogue, before the dialogue they should to agree on a session key, because they do not have a session key, the key transfer cannot be transmitted in plaintext, so both need a trusted third party to help them through the key distribution. This third party is called Network Security Service Centre (NSSC).

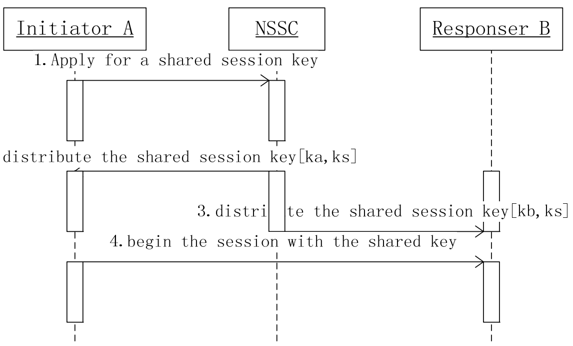

Fig 1 Receiver gets the key from the NSSC

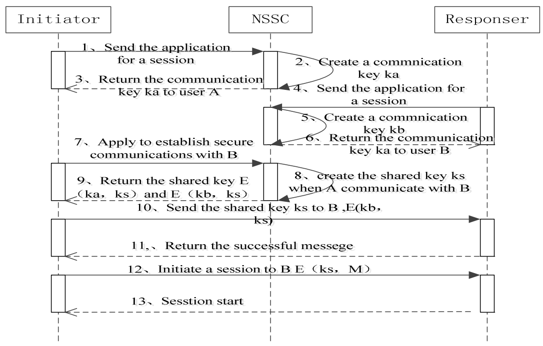

Fig 2 Security Service Centre interaction diagram

(b) Mechanism of Hybrid Encryption Algorithm

The mechanism of hybrid encryption algorithm D_R is the mixed use of DES encryption algorithm and RSA encryption algorithm, which combines the advantages of DES and RSA, and cleverly made up the problem of two kinds of encryption algorithm. Main idea: Based on the fast speed characteristics of DES encryption algorithm, adopts the DES algorithm to encrypt communication both sides specific communication content (including pictures, music, video, etc.)Between the user A and user B; Based on the high safety characteristics of RSA, in the network communication, RSA algorithm was used to encrypt the transmission key.

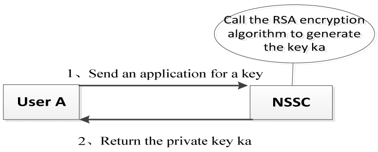

Fig 3 User applications the key for the session

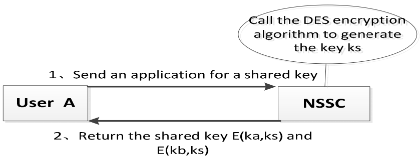

Fig 4 User session share the key

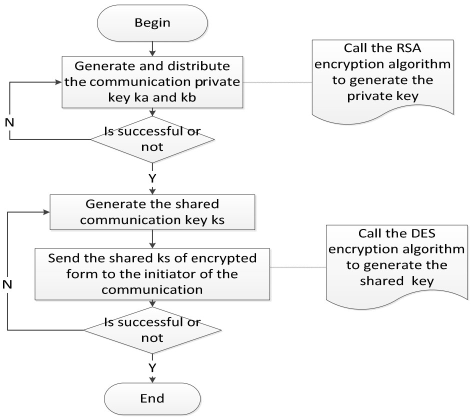

Fig 5 Security service canter key distribution diagram

Fig3 and Fig4is the specific application process of the hybrid encryption algorithm in the security service centre .The security service centre based on hybrid encryption algorithm, generally, is where using the DES encryption algorithm to generate a shared key used to realize secure communication between the two client and adopting symmetric encryption algorithm RSA to generate the key which is used to realize secure communication between the single client and the server. On one hand, it's a full use of the fast and highly efficiency characteristic of the DES, on the other hand, it takes the high safety characteristics of RSA into account. At the same time it makes up for the shortcomings of the low safety performance and the slow realizing speed in the encryption algorithm.

(c) Hybrid Encryption Algorithm Application Processes

The work process of the network security service centre based on hybrid encryption algorithm is similar to that of a traditional security service centre. There's certain change only on the choice of encryption algorithm. The specific flow chart is shown in Fig 5.

Fig 5 shows the workflow of the security service canter based on hybrid encryption algorithm. When two web clients communicate, security service canter work steps are as follows:

(1) Respectively, assign individual session key ka and kb for the user A and user B. Here, in view of the limited data quantity of the communication content, we use the RSA encryption algorithm to generate personal session key;

(2) receive the application for a session which needed a shared key;

(3) Generate a shared key ks used when the two clients communicate. Because both sides of the communication involve the transmission of large data files, we use the DES encryption algorithm to generate the shared key;

(4) Security service centre send two the shared key ks in the form of the ciphertext severally encrypted by the key ka and kb to the session initiator;

(5) After confirming the receipt of the shared key by both sides, the security service centre completed a communication key distribution.

Performance Testing and Evaluation

(a) Performance Analysis

This mechanism uses DES as the symmetric key algorithm, RSA as the public key algorithm. First, file encryption using DES algorithm, and then use the RSA key DES encryption algorithm. D_R hybrid encryption mechanisms underlying features are as follows:

(1) Provide documentation of two encryption methods, namely hybrid encryption D_R and DES encryption methods.

(2) D_R hybrid encryption mechanisms can verify the correctness of the key, because when the encryption, the encrypted key ciphertext is also stored in the file, and when decrypted, using the current key to decrypt the ciphertext key. If the resulting plaintext is the same with the current key, the current key should be correct.

(3) The hybrid encryption module in hybrid encryption mechanism also has a pair of RSA key error detection function, which primarily through decrypted DES key length to judge, because if the RSA key error, then decrypted DES key length must be over 16 bytes.

(4) D_R hybrid encryption mechanisms DES encryption can be a sub-DES encryption (DES encryption standard) and 3 times DES encryption. According to the key length, hybrid encryption mechanism automatically selects encryption scheme. When the key length is 64 or less, standard DES encryption will be used; when the key length over 64, the system will set the first two keys, and enable three times DES encryption, the key length of up to 112.

(b) The Comparison of mechanism in different encryption algorithms

Compared to the traditional network security service centre, the new network security service centre based on hybrid encryption algorithm both to enhance the response speed, and to maintain the security of the communication process, and thus enhance the overall efficiency of the security service centre. From the table we can conclude that Network Security Service Centre which is based on hybrid encryption algorithm has a distinct improvement compared with the traditional Security Service Centre, such as high security, high response speed and high practicability.

Table 1: Comparison of application effect

	NSSC(DES)	NSSC(RSA)	NSSC(RSA&DES)
Response speed	Fast	Little faster, big slower	Fast
Security	Weak	High	High
Scalability	Weak	Weak	Strong
Practicality	Weak	Weak	Strong

Conclusion

With the rapid development of information technology, people increasingly high demand for security on the network communications. Therefore, improving the security of network security services centre becomes particularly important. This paper is focus on the study of framework in the traditional network security services centre, and improved the encryption algorithm to enhance the security service centre’s overall performance. However, from reality, our model there is still much room for improvement, such as improved security architecture, encryption algorithm selection, etc. Therefore, to provide a more comprehensive security services architecture also requires us to do deeper research.

References

[1] M. Xu. Gaochao. Distributed Computing Systems, Beijing:High Education Press., pp. 124–141, January 2004.

[3] Liao Hsien-Chou, Chao Yun-Hsiang, A new data encryption algorithm based on the location of mobile users, JA: Information Technology Journal, vol. 7, pp. 63-69, 2008.

[4] Han Seung-Jo,Oh Heang-Soo,Park Jongan, Improved Data Encryption Standard (DES) algorithm, CA: Proceedings of the 1996 4th International Symposium on Spread Spectrum Techniques & Applications, ISSSTA'96, vol. 3, pp. 1310-1314, 1996.

[5] Nadeem Aamer, Javed M. Younus, A performance comparison of data encryption algorithms, CA: 1st International Conference on Information and Communication Technology, vol.2005, pp.84-89, 2005.