Research on Mobile Network Payment Security Protocol based on Symmetric Cryptography

Wang Linjing, Zhang Peijiang

Henan University of Traditional Chinese Medicine, Zhengzhou 450008,China

Xuexi123@163.com

Keywords: Mobile payment, Symmetric cryptography, Security protocol, Hash mechanism, 4G network.

Abstract. With the rapid development of network technology and mobile terminal equipment, mobile payment has become a trend. Due to the complexity of payment environment, the payment terminal equipment performance is limited, mobile payment security protocol is essential with a high degree of security. This paper not only proposes a Hash symmetric password authentication mechanism, which is used in the mobile payment security protocol, but also design the password authentication and error analysis control scheme, and then they is carried out the security test in the 4G network infrastructure. Through the test, it is found that its cipher technology is more than 99% on the acceptance rate of the correct data and the dropping rate of attack data, it not only has higher security, and it is easy to implement and promote.

Introduction

Mobile payment has been developing rapidly in recent years, it has become a popular application direction in the mobile field, but also has a strong market potential. The smooth progress of mobile payment process need to the payment security protocol, which requires a password security authentication mechanism [1,2]. Mobile secure payment protocol based on symmetric cryptography can greatly improve the computing efficiency, and the use of Hash can effectively reduce resource consumption, to further improve the operating speed of the system, the design can be widely used in the 4G mobile security payment mechanism, promoting the formation of mobile payment uniform standards.

Mobile Network Payment Service Implementation and Security Authentication

At present, the payment method of the mobile business mainly consists of four kinds, including SMS authentication, voice authentication technology, wireless authentication protocol and unstructured supplementary data technology [3-5]. In the payment, the system needs to use a certain security authentication protocol to ensure the security of the system, the following are the four mobile payment mode.

Short message authentication technology. SMS authentication technology is to complete the payment via SMS authentication. On the current market, all mobile phones are basically supporting SMS transceiver functions, so SMS authentication technology can be a lot of promotion in the mobile payment system, at the same time the payment technology is simple and low cost. However, the security of the technology is lower, and the short message has the delay efficiency, it can not determine the sending and receiving time of the short message, and this kind of payment method will affect the normal operation, so this method is generally used in small payment occasions.

Voice authentication technology. The payment process uses the telephone method to check the information, including identity authentication, payment information and so on, the method has higher stability and real-time performance, but the operation is more troublesome and time consuming, the cost of payment is relatively large, and security is not high.

Wireless authentication protocol technology. Wireless authentication technology is that the user goes through the internet, and people can complete the certification payments through the

transmission and receiving data, this method is greatly influenced by the network, but it is good general and the hardware requirements are lower.

Unstructured supplementary data technology. Using the method of unstructured supplementary data mainly uses the mobile phone to send a specific symbol, these symbols as a verification symbol can determine the operation that is completed, the method is simple and relatively high security, but it is higher requirements for terminal equipment.

Symmetric Cryptography and Security Protocols based on Hash

Based on the mobile payment system of public key cryptography, it needs a lot of computing although it has advantages in the realization of digital signature, users need to use terminal equipment to store signature authentication information and public key certificate [6,7]. In general, a public key password is corresponding to a certificate authority, which brings huge additional information for the mobile payment system. Due to the limitation of the device, the public key cryptography system is not suitable for mobile payment system, and the symmetric encryption mechanism includes encryption and decryption, message authentication and Hash, which has a great advantage in computing efficiency [8-10]. The computational efficiency of public key and symmetric cryptography is shown in Table 1.

Table 1. The comparison efficiency of public key cryptography and symmetric cryptography

Operation	Time(s)	Iteration number
DES	7.28	Encryption and decryption 100000
SHA	19.35	100000
1024bit RSA signature verification	50.25	10000
2048 bit RSA signature verification	156.32	10000

Table 1 shows the comparison efficiency of public key cryptography and symmetric cryptography, it can be seen from the above comparison that the symmetric cryptosystem has a large advantage in computing efficiency than public key cryptography. Considering the terminal equipment performance of mobile payment system and the limit of computing environment, we need to use the symmetric cryptography in the mobile payment system.

Each side of the symmetric encryption algorithm uses the same key to encrypt or decrypt, its efficiency is very high, and it is the most commonly used in the network for a large amount of data transmission [11,12].

Most mobile payment uses mobile devices to complete, its processing speed and battery power, etc. on the payment process will have a certain impact, so the traditional public key authentication system is not used in the mobile payment system, and the calculation speed of Hash chain is fast and has lower occupancy resources, which can be used in mobile payment system.

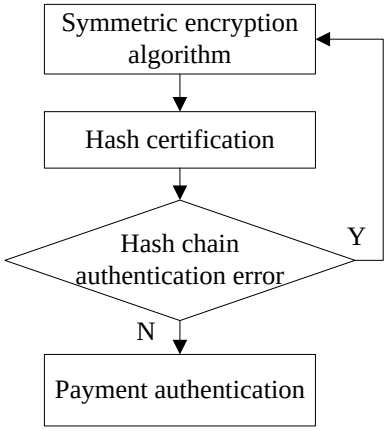

Fig. 1 The symmetric payment password authentication mechanism based on Hash

Figure 1 shows the symmetric payment password authentication mechanism based on Hash, using one-way Hash function carries out mobile payment password authentication mechanism, in which the main idea is to pick a random x_0 integer as a seed, and using one-way Hash function computes N recursive iterative repetition x_0, so as to obtain a Hash chain, the chain length is N,

$h(x_0), h^2(x_0), ..., h^l(x_0), ..., h^{(N-1)}(x_0), h^N(x_0)$, in which behind the data is calculated by the front data Hash. x_0 is the initial value of the encryption system, it is the premise of the system; if the value is invalid, the whole secret system is invalid, $h^N(x_0)$ is the root node of the whole system. When the user is registered, the system sends the user's identity ID and the root node information $(ID, h^{N-1}(x_0))$ to seed the server; when the system need to pay a password authentication, $(ID, h^N(x_0))$ sends to the server, and server uses the identity authentication ID to find $h^N(x_0)$, if the two values are equal, then they verify through; if the value is not equal, the verification is not through.

When there are a data packet loss or malicious attacks, authentication will not be passed, and the security certification center will not make the operation of the replacement node; when the users carry out authentication, they has used the current node, and people will use the next node when the next time need to certification.

When authentication is not passed, the authentication center will return the error information, and the current node does not change, the counter will error information accumulation that is 1; if the authentication continues to make mistakes, when the number of errors exceed the upper limit, then the authentication center will notify the user to lock the user system, people need to re register or more advanced password authentication system lock, so that mobile payment authentication system is more secure and reliable.

Mobile Payment Symmetric Cryptography Security Test

Mobile network is one of the four basic technologies in networking, in which mobile payment is an important application. In order to verify the reliability of the proposed symmetric cryptography, this paper tests the authentication performance of its data. The test framework is shown in Figure 2.

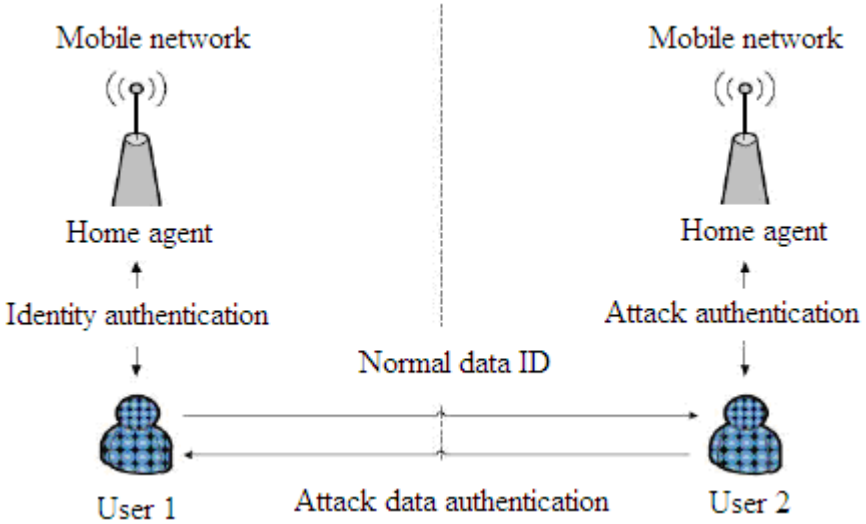

Fig. 2 Mobile network security simulation test framework

Authentication mechanism is a key part of mobile security payment system, authentication mechanism can prevent user privacy information exposure and avoid data security attacks. In order to verify the reliability of the proposed Hash symmetric cryptography, this paper tests the correct packet of data packets and the acceptance and dropping rate of the attack data packets, in which the results are shown in Table 2.

Table 2. Data acceptance performance test

Experiment number	Correct data packet		Attack packets	
	Accept	Discard	Accept	Discard
1	5000	0	0	5000
2	5000	0	0	5000
3	5000	1	1	4999
4	5000	0	2	4998

Table 2 shows the data receiving performance test of correct data packets and attack packets, it can be seen from the table that the acceptance rate of correct data packet is close to 100%, in which the discarded packet is only one; the drop rate of attack packets is also close to 100%, in which the most acceptable rate is only two, the reliability of data authentication is very high.

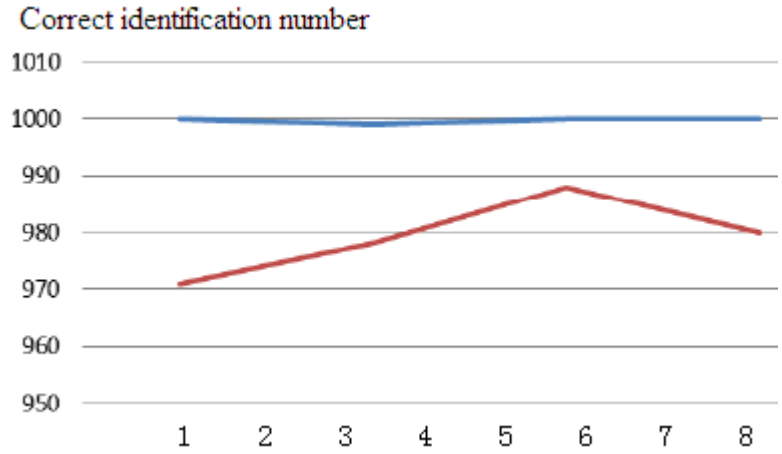

Fig.3 Discarding the proportion of forged data packets

Figure 3 shows the comparison curve of discarding the ratio of forged data packets. In order to verify the reliability of the Hash symmetric secret technology, this study compared with the ordinary secret technology. Through the comparison, it is found that the attack of Hash symmetric secret technology is higher, the average identification rate is 99.7875%, which not only can almost identify all the deception, but also does not affect the normal communication, which has higher reliability and feasibility as well as lower ambiguity.

Summary

According to the theory of Hash function, this paper proposes a kind of symmetric cryptographic mechanism for mobile network security, and analyzes the security authentication and error control scheme. In order to verify the security and stability of the mechanism, the data authentication function is tested. The test shows that the acceptance rate of correct data packets and the dropping rate of attack data packets are high, and the average identification rate is 99.7875%, it is the basic identification of all the attack data without affecting the normal communication, its reliability and feasibility are higher.

References

[1] Y.F. Pu, W. Zhang, S.H. Teng. Cooperative network intrusion detection based on decision tree. Journal of Jiangxi Normal University, 2014, 34 (3): 302-307.

[2] F. Wang, H.Q. Lu, S.Y Song. Damage assessment system based on combat simulation. Journal of PLA University of Science and Technology, 2013 (2): 139-143.

[3] H.M. Wang , Y. Zhang. Research on the data model of joint operations simulation. System simulation, 2013, 20(15): 4186-4188.

[4] M.X. Ze , J. He. The design and implementation of battlefield situation3D graphics simulation system. Computer, 2014: 313-316.

[5] C. Yang , C.J. Cao, J.F. Ma. The network authentication protocol Mesh of General combination security. Xi'an University of Electronic Science and technology, 2013,34 (5): 814-517.

[6] Z. Li , J. Liu , L. Yue. The design and implementation of self organization network simulation platform. Computer science, 2014, 35(1): 24-26,30.

[7] X.G. Zhao, F.X. Zhu , D. Wu. Research and implementation of UAV AdHoc network simulation in the environment. System simulation, 2013, 20(23): 6409-6413.

[8] Z.J. Zhu , Z.C. Le , R. Zhu. Research and implementation of OBS network simulation platform based on NS2. Journal of communication, 2014, 30(9): 128-134.

[9] Y. Cao. Research onservice innovation and information technology in the library development. Journal of Jilin Institute of Chemical Technology, 2014, 28(6): 73-75.

[10] F. Hong, Z.M. Wu. Hurst index adaptive estimation method based on the wavelet. Journal of software, 2014, 16 (9): 1685-1689.

[11] Y.L.Li, G.Z. Liu, H.J. Wang. Analysis of a self-similar data stream Hurst parameter wavelet. The electronic and information technology, 2013.25 (1): 100-106.

[12] L.F. Lv, H. Dai, J.Z. Sun. An improved block Davidson method for solving large symmetric eigenvalue problems. Journal of Tianjin University, 2014, 40 (5): 559-562.