Application of Improved SSL in Data Security Transmission of Mobile Database System

RUIFENG WANG, XIAOHUA ZHANG, DECHAO XU
College of Automation & Electrical Engineering
Lanzhou Jiaotong University
Lanzhou, 730070
CHINA
Email: zhang0212460@yeah.net

Abstract: - The existing SSL (Secure Socket Layer) protocol which mobile database system is using has many drawbacks, such as large amount of communication, computational complexity of encryption algorithm and the workload imbalance. In order to solve these problems, the paper proposes an improved SSL protocol. It decomposes the private key into independent elements which reducing the computational complexity and implementing parallel computing, at the same time it put part of decryption calculation to the client so that balancing the workload and shortening the running time of the algorithm. The improved SSL protocol exchanges certificate identifier instead of certificate entities between client and server, which reduces the message payload. The improved SSL protocol improves the decryption speed and reduces the handshake communication load compared to the original SSL protocol.

Key-Words: - Mobile database, security transmission, improved SSL protocol, RSA encryption algorithm, identity authentication

1 Introduction

Mobile database system realizes data synchronization transmission via wireless network, its instability and weak immunity leads to illegal users easier to theft and tamper with transmission data. So that it results in leakage of synchronous data and error information transmission. If important information related to security changes will lead to a major accident. Therefore it is very important to improve the security of transmission data.

Literatures [1-3] guaranteed the security of data transmission through taking encryption algorithm to encrypt the radio transmission link, but computational complexity of the algorithm currently used results in transmission delay increasing. Literatures [4-8] proposed to verify the identity of the terminal to prevent unauthorized users from logging system to steal data. However it needs to pass the certification entity to verify its effectiveness, resulting in increased traffic loads and client computing, and reducing efficiency of the system.

The paper puts forward an improved SSL protocol to achieve safe and efficient data transmission in mobile database systems. The improved SSL protocol decomposes the private key into independent elements to decrease the mode of power operation, at the same time it will decompose part of the decryption module and power operation, so that ensure the security of transmission data and reduce computational complexity. And the improved RSA algorithm performance is compared with the traditional algorithm, the simulation results show that the improved algorithm performance is better. It authenticates clients to transfer unique identification of certificate by storing server certificates in clients, effectively reducing the communication load protocol to improve transmission efficiency.

2 Mobile Database System Data Synchronization Transmission

The application of mobile database system is more and more popular with the rapid development of wireless communication technology and mobile computing technology. The instability of wireless network and frequent breakout lead to leakage of transmission data[1]. Mobile database SQL Server CE establishes a secure channel based on SSL protocol in order to guarantee security of data transmission and integrity. Mobile database SQL Server CE provides remote data access and merge replication, ensures that the data of SQL Server CE

in the mobile client can be reliably transmitted. And it can offline operate database, then sync with the server, which makes SQL Server CE ideal database in mobile and wireless environment. Before the SSL connection, it is necessary to create reliable TCP connections between client and server[2]. Identity authentication server of SSL protocol provides authentication through the certificate entity first. Then the SQL Server CE client proxy sends HTTP requests to SQL Server CE server agent request. SSL handshake protocol consults encryption algorithm and session key which is used to encrypt data. Finally it can transfer synchronize data through SSL channel which ensures confidentiality and integrity of transmission data. It will describe the working process of the SSL protocol to achieve data security transmission below. Then it will put forward improvement measures which are aimed at improving the efficiency and security of transmission data based on the SSL protocol performance defects.

3 SSL Protocol

SSL Protocol has record protocol and handshake protocol two layers. Record protocol packets, compresses, encrypts and encapsulates the high-layer data. Handshake protocol which running on the record protocol is used for identity authentication, negotiation encryption algorithm, key exchange before the data[3].

3.1 Working process of the SSL protocol

The working process of the SSL protocol is composed of shaking hands and data transmission. Handshake protocol completes connection before data transmission, SSL protocol working process as shown in figure 1, the main working process as follows. (1)The client and server swap hello message which mainly includes random number r_c and r_s, the session id SID, protocol version number V and a suite SecNeg encryption algorithm, to establish SSL security connection. (2)The server sends certificate, server-key-exchange and certificate request, finally sends server- hello-done news which indicates server hello phase end. (3)Client sends its certificate, the function of key generation and certificate- verify the result of the server certificate verification after it receives server- hello-done news. (4)The client and server send change cipher-spec and finished message each other. (5)They use the negotiated keys to send data after the handshake finally.

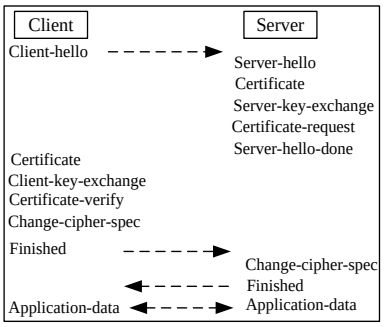

Fig.1. Working process of SSL protocol.

3.1.1 Identity authenticationl

Handshake protocol implements the communication on both sides of the identity authentication through the digital certificate. Certificate Authority(CA) which is got by Public Key Infrastructure (PKI) provides the mechanism provides and manages the digital certificate and verifies the authenticity of identity[4]. The server will first calculate the server certificate hash value by the hash algorithm, then use its own private key to encrypt hash which form digital signature, finally it will send certificate information and signature to the client. The client calculates the content of CA after it receives the information, and it uses the public key to decrypt the signature that get hash value compared with the value of the client. If they are the same, the server authentication is successful. Server for client authentication methods is similar, so as to realize two-way authentication.

3.1.2 Principle of RSA encryption algorithm

It uses the RSA encryption algorithm which has encryption key (KU) and decryption key (KR) two keys to exchange session key in the SSL handshake protocol[5]. The algorithm detailed process as follows. (1)Select two prime numbers p and q;(2) Calculate n and $\varphi(n)$, $n=pq$, $\varphi(n)= (p-1)(q-1)$, $\varphi(n)$ is the euler function for n; (3) Generate a random number e with $\varphi(n)$ co-prime, namely gcd(e , $\varphi(n)$)=1, and $1<e<\varphi(n)$, it will get the public key KU = (e, n); (4) Get the private key by calculating d meet $de\equiv 1 \bmod \varphi(n)$,it said the product of d and e do modular arithmetic result must be equal to 1; (5) Suppose M as transmission data, C as encrypted data, $C \equiv M^e (\bmod n)$, the receiver after receiving the cipher decryption to get the original data $M \equiv C^d (\bmod n)$.

3.2 Performance defect and improvement project of the SSL protocol

The communication load leaps during the handshake due to it is required to transfer certificate entity for identity authentication and verify its effectiveness. The SSL handshake uses RSA encryption algorithm to exchange session keys, due to the algorithm computational complexity, slow speed, and workload imbalance. They result in a decline in overall system performance. This paper

proposes an improved SSL protocol for SSL above defects to reduce the communication load, improve the efficiency of data transmission, to ensure the high-efficiency and safety of the synchronous data.

In the improvement of the SSL protocol, it will be uniquely corresponding to each certificate a certificate identity CID and put certificate list in advance to the prover. It will effectively avoid transferring certificate of entity each other in the process of shaking hands. It only needs to send the CID in the process of the SSL handshake, the prover according to the CID find the corresponding certificate entity in the list[6]. It greatly reduces the amount of communication and improves handshake protocol connection speed. Since the client storage capacity, computing power, power management are limited, encryption algorithm the SSL handshake protocol chose also affects overall system performance. According to the characteristics of the mobile environment, the paper puts forward an improved algorithm which improves the safety and efficiency of the system.

If modulus $n=pq$ with special form $p=as+b$ and $q=cs+d$, this form of prime numbers of (p, q) constitutes a weak key of RSA cryptography system. Assume f/e is p/q the best approximation value, e and f are relatively prime and $f<e<2f$, $s=\sqrt{n/(ef)}$, the s adjoint polynomials about n as shown in formula(1).

$$f_{n/s}(x) = ax^2 + bx + c \tag{1}$$

The discriminant formula (1): if $\Delta = b^2 - 4ac \geq 0$,it has two rational root, it can be represented as formula(2), p and q are two prime factors by computing. if $\Delta = b^2 - 4ac < 0$, it is looking for {e, f} and calculate the s, at the same time seeking p, q trough the discriminant polynomial. It can search for integer {e, f} in small scope if the primes are smaller, and get s decoding algorithm easily. In order to improve the security of RSA algorithm, it is necessary to increase the private key d resulting in larger power operation, spending a lot of time and storage space, increasing system performance overhead.

$$f_{n/s}(x) = (a_p x + b_p)(a_q x + b_q) = pq \tag{2}$$

The improved RSA algorithm will break down d into a number of different block using vector $D = (d_1, d_2, \cdots, d_k)$ indicating which can be a separate operation, so it can efficiently perform encryption operations. At the same server transfers part of decryption computation to the client, balancing its workload. It can achieve parallel processing to meet more connection requests. The algorithm basic idea is that server broken down private key d:

$$\mathrm{d} = f_1 d_1 + f_2 d_2 + \cdots + f_k d_k \,(\mathrm{mod}\,\varphi(n)) \tag{3}$$

In formula (3), fi, di were separately c bit, n bit random vector , ck determines its safety. Send vector first to the client, The client according to vector D that the server send to and the formula (4) calculates the vector Z each element sent to the server.

$$z_i = x^{d_i} \,(\mathrm{mod}\, n), 1 \leq i \leq k \tag{4}$$

It can see the calculation of vector Z elements only associated with the vector D from the Eq.(4). The vector D each element is independent, so it can parallel computing each element of vector Z, improving the client encryption speed. Then the server decrypts the session key according to the vector Z and formula (5).

$$\prod_{i=1}^{k} z_i^{f_i} = \prod_{i=1}^{k} x^{f_i d_i} = x^d \,(\mathrm{mod}\, n) \tag{5}$$

In the improved RSA algorithm, it decompose large numbers of power operation into small modulus power operation of M_p, M_q, they respectively by Eq.(6) and Eq.(7) calculated, fi and gi are c bit random value, dp and dq can be parallel computed alone through Eq. (8) and Eq. (9), then server completes the decryption operation through the formula (10).

$$M_{\mathrm{p}} = \prod_{i=1}^{k} z_i^{f_i} \,(\mathrm{mod}\, p) = \prod_{\mathrm{i}=1}^{k} x^{f_i d_p} \tag{6}$$

$$M_{\mathrm{q}} = \prod_{i=1}^{k} z_i^{g_i} \,(\mathrm{mod}\, q) = \prod_{\mathrm{i}=1}^{k} \mathrm{x}^{\mathrm{f_i} d_q} \tag{7}$$

$$\mathrm{d}_p = \sum_{i=1}^{k} f_i d_i \,\mathrm{mod}(p-1) \tag{8}$$

$$\mathrm{d}_q = \sum_{i=1}^{k} g_i d_i \,\mathrm{mod}(q-1) \tag{9}$$

$$\mathrm{x}^d = M_p n_p + M_q n_q \,(\mathrm{mod}\, n) \tag{10}$$

$$\mathrm{n}_p = q(q^{-1}(\mathrm{mod}\, p)) \tag{11}$$

$$n_q = p(p^{-1}(\mathrm{mod}\, q)) \tag{12}$$

It performs decryption operation by the formula (10). The server respectively calculates np, nq through Eq.(11) and Eq.(12) in advance.

4 Analysis of the Improved SSL Protocol Performance

In this paper, it will analyze the performance of the improved SSL protocol from data security, data

traffic and efficiency three indicators. The security intensity of standard RSA algorithm is determined by the key length which is in 1024 ~1536 bit key length guaranteeing security. In the improved RSA algorithm, the safety of d_p and d_q ensure the confidentiality. After the illegal users get vector, they can get d_p and d_q by searching all the possible values of vector F and G which have k elements[7]. Each element has c bit, so it will need to test 2ck through the exhaustive search. When ck > 72 the security is quite pretty with RSA key length 1024~1536 bit by calculating, therefore the improvement of SSL protocol still has high security.

While the improved SSL handshake protocol in identity authentication, it only sends CID instead certificate of entity, reducing the amount of communication data , improving the handshake protocol connection speed greatly. The handshake transmission message in SSL protocol and improvement is as shown in tablel . Among them, null indicates the field is empty, n means transfer certificate number. The client and server certificate both need to be verified after sending certificate-verify message, therefore take n for 2[8].

Table 1 : The Comparison of Handshake Message Length

message order	handshake message	message length of original SSL protocol	message length of improved SSL protocol
1	Client-hello	$\|r_c\|+\|SID\|+\|SecNeg\|+\|V\|$	$\|r_c\|+\|SID\|+\|SecNeg\|+\|V\|$
2	Server-hello	$\|r_s\|+\|SID\|+\|V\|$	$\|r_s\|+\|SID\|+\|V\|$
3	Certificate	|Cert|	|CID|
4	Server-key-exchange	|SecNeg|	|SecNeg|
5	Certificate-request	|CertificateType|+|CertificateAuthorites|	|CertificateType|+|CertificateAuthorites|
6	Server-hello-done	null	null
7	Certificate-verify	|Cert|×n+|H(m)|	|CID| +|H(m)|
8	Client-key-exchange	|SecNeg|	|SecNeg|
9	Change-cipher-spec	|Change-cipher-spec|	|Change-cipher-spec|
10	Finished	|md5-hash|	|md5-hash|
11	Change-cipher-spec	|Change-cipher-spec|	|Change-cipher-spec|
12	Finished	|md5-hash|	|md5-hash|

The length of the parameters in Table Ⅰ as follows: |rc|=|rs|=20Byte, |SID|=4 Byte, |SecNeg|=3Byte, |V|= lByte, |H()|=20Byte, |Change-cipher-spec|=1Byte, |CID|=8Byte,|md5-hash|=16Byte,|CertificateType|=1Byte, |CertificateAuthorites|=2 Byte, SSL certificate length is estimated 1 KB.

Each message estimating length results are shown in Table Ⅱ . Transmission and verification certificate is a major cause of leading to the SSL protocol big traffic from Table Ⅱ . The improved SSL handshake protocol transfers CID instead of the certificate reducing the traffic in the process of shaking hands. Its data traffic reduces from 3188 to 132 byte, is 4% of the original traffic, speeding up the SSL protocol handshake, enhancing the working efficiency of the system. Hence it can deal with more the SSL connection requests.

Table 2: The Message Length of Two Protocols (Unit: Byte)

length of handshake message	message order												total
	1	2	3	4	5	6	7	8	9	10	11	12	
original SSL protocol	28	25	1024	3	3	0	2068	3	1	16	1	16	3188
improved SSL protocol	28	25	8	3	3	0	28	3	1	16	1	16	132

The paper improves the efficiency of SSL through improved RSA encryption algorithm. It uses c++ language to program the standard RSA algorithm and the improved algorithm. It adopts expand Euclid algorithm to realize gcd(e,φ(n)) and e-1(mod φ(n)) and uses the basic method to realize mode of power operation. The (len (p), len (q)) that len(p), len(q) respectively delegatep, q digits indicates the size of RSA algorithm[9]. The algorithms independently run 100 times for different digits of prime. The paper will compare efficiency of the improved algorithm with stand algorithm from system initialization and decryption operation two aspects.

The performance comparison of two kinds of algorithm initialized is shown in figure 2. The

initialization execution time of two kinds of algorithm is fundamentally the same before (len (p), len (q)) = (80, 60). The initialization execution time of the improved RSA algorithm is about 410s when (len(p), len(q))=(90,70), and the standard algorithm is about 390s from the figure 2 Although the improved RSA algorithm requires a certain time for the private decomposition, the initialization time consuming is not significantly increasing with the increase of prime bits and the improved algorithm only initializes once and performance loss is not obvious. Hence running speed of the improved algorithm has quickened significantly in the back of the module and power operation once the algorithm is built.

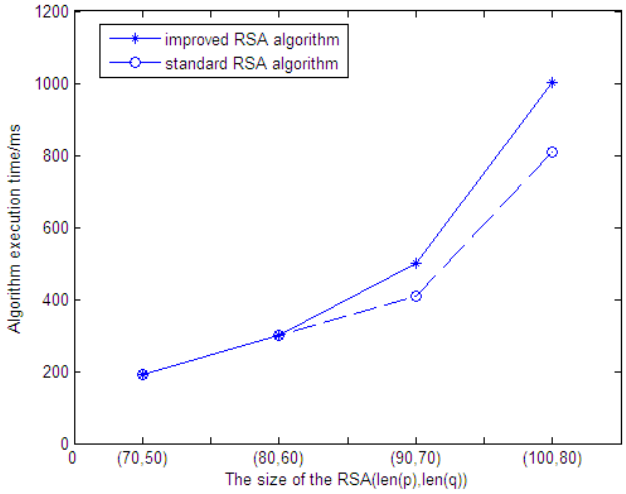

Fig.2 Comparison of Initialization performance

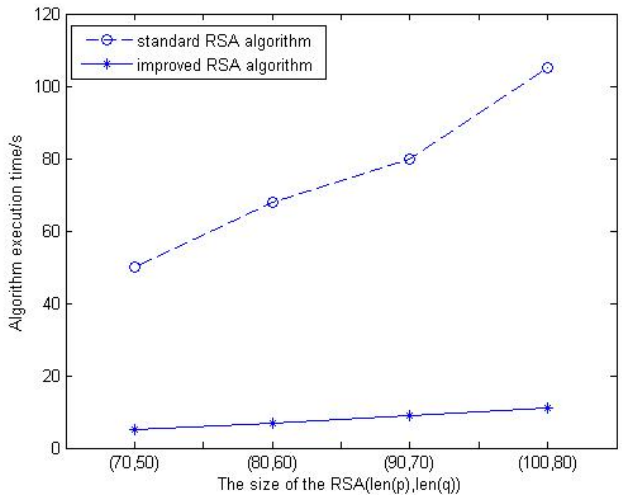

Fig.3 Comparison of decryption performance

The decryption performance comparison of two algorithms is shown in figure 3.The improved RSA algorithm decryption performance is standard algorithm about 7 times when (len(p), len(q))=(80,60) from the figure 3, and the effect is more significant with the increase of prime bit. The improved RSA algorithm decryption performance is standard algorithm neraly 10 times when (len(p), len(q))=(100,80).The improved RSA algorithm will greatly improve the decryption speed, shorten the handshake connection time, handle more requests, improve the system efficiency. Because it decomposes private key d that M_p, M_q are composed of various small module power operation completing parallel processing and calculates the d_p, d_q, n_p, n_q in advance. At the time the server transfers part of decryption computation to the client reducing workload.

5 Conclusion

The paper proposes an improved SSL protocol to realize synchronous data secure transmission in view of the security problem of synchronization data in mobile database system. The improved SSL protocol decomposes the private key of RSA algorithm reducing the mode of power operation and pre-processes part of the decryption module so that reducing the overall running time and improving the implementation efficiency of the SSL protocol. At the same time it prestores server certificate on the client to abandon transferring certificate of entity in the process of the SSL handshake to reduce the communication load of the protocol by passing the CID. The improvements of the SSL protocol guarantee synchronous data securely and efficiently transports in mobile database system.

References:

[1] M.R. Chen, X. Zhang and K. He, “Scheme of improvement and chosen-ciphertext security of public key encryption,” *Journal of computer*, vol.36, no.6, pp.1149-1154, 2013.

[2] PanosK. Chrysanthis, “Transaction Processing in Mobile Computing Environment,” *IEEE on Advances in Parallel and Distributed Systems*, vol.11, no.10, pp.77-82, 1999.

[3] L. H. Yeo, A. Zaslavsky, “Submission of Transactions from Mobile Workstations in a CooPerative Multidatabase Processing Environment,” *Proc. 14th IEEE CS International Conference on Distributed Computing Systems*. Poland. 1994, pp.372-379.

[4] S. Acharya, M. Franklin and S. Zdonik, “Dissemination-based data delivery using

broadcast disks," *IEEE Personal Communications*, pp.50-60, Dec. 1995.

[5] C. Su, L. Tassiulas, "Broadcast scheduling for information distribution," *Proc. of IEEE Infocom*, Los Alamitos, 1997, pp.109-117.

[6] M. Nicola and M. Jarke, "Performance modeling of distributed and replicated databases," *IEEE Transaction on Knowledge & Data Engineering*, vol.7, pp.645-672, 2000.

[7] G.D. Walborn, P.K. Chrysanthis, "Supporting Semantics-based Transaction Processing in Mobile Database Applications," *Proceedings of 14th IEEE Symposium on Reliable Distributed Systems*, vol.09, pp.31-40, 1995.

[8] E,U. Grenoble, "Mobile Databases: a Report on Open Issues and Research Directions," *ACM SIGMOD Record*, vol.33, no.2, pp.78-83, 2004.

[9] J. Backhouse, H. Caro, A. McDonnell, "Toward Public-Key Infrastructure Inter-operability," *Communications of the ACM*, vol.46, no.6, pp.98-100, 2003.