通信情報保護學會論文誌
第6卷 第3號, 1996. 9

Diffie-Hellman 방법의 위성망에서의 응용

박 정 현*, 이 상 호**

Applied to Satellite Network of Modified Diffie-Hellman Scheme

Park, Jeong-Hyun* Lee, Sang-Ho**

요 약

본 논문에서는 Diffie - Hellman방법을 위성을 이용한 다중 방송통신망에 적용하여 키 분배하는 방법을 제안하고 있다.

Abstract

This paper presented a key distribution scheme based on the Yacobi scheme that does not use the secret key provided by key distribution center as a power, but uses instead a random number generated by the user. The scheme is independent of the exposure of the secret key. Then this paper described modified Diffie-Hellman schemes based on the the discrete logarithm and prime resolution into factors. The modified DH scheme was applied to point-to-multicasting, and broadcasting networks via satellite.

I. Introduction

Satellite communications has been used for broadcasting services and long-haul transmissions. Moreover, many applications using satellite on the information age will be appeared in the near future. However, satellite communications are vulnerable to unauthorized access to the transmitted data. Security is becoming an essential requirement of satellite network. Strong security technology is required to protect users' sensitive or valuable information

* 한국전자통신연구소
** 충북대학교

within the satellite communications. This paper describes the modified key distribution scheme based on the Yacobi and presents the modified schemes based on the Diffie-Hellman(DH) and ID(Identity). And then the modified scheme based on DH and ID is applied to point-to-multicasting, and broadcasting networks via satellite. The applied protocol based on the DH scheme can help the vulnerable problems of satellite communications in point-to-multicasting and broadcasting networks via satellite and it will be widely used when satellite network expand to private networks.

II. Modified Key Distribution Schemes

The Diffie-Hellman(DH) scheme has the disadvantage that user k can impersonate user i to user j and can then make a working key. User i and user j must change their secret key and working key periodically. This scheme also requires a basically reliable key distribution center. Moreover, since each user's modulus differs from that of the other users, it requires rather complicated processing. Yacobi scheme is also susceptible to passive attack when S_i and S_j (secret keys from center) are disclosured. Okamoto-Tanaka scheme is similar to the DH scheme and solves the public key management problem by introducing the ID concept. This is a relatively secure scheme. Under passive attack, this scheme's security depends on solving $g^{e.Ri.Rj}$ from $g^{e.Ri}$ and $g^{e.Rj}$(e : encryption key, R_i/R_j : random numbers from user i/j, g : primitive element in $GF(n)$, n is product of prime number p and q). Under impersonation attack from disguised user j, it depends on finding X and R that satisfy $X = ID_j^{-1/e} \bmod n$. Blom proposed a symmetric key generation system(SKGS) based on secret key sharing systems. A trusted authority generates a matrix G of size $k \times n$ and a secret matrix D of size $k \times k$. The i th column of G, namely g_i , is set as the address of user i or the like. Then, the authority delivers the i th row S_i of G^TD to user i. In the communication phase, user i uses S_ig_j as a working key to user j. Since G^TDG is a symmetric matrix, the working key equals S_jg_i, which can be generatd by user j. In this system, any k users among all n users can obtain the top secret matrix D in cooperation with each other, while k - 1 or fewer users cannot. Weak points in the SKGS are the difficulty in choosing a suitable size for integer k and the large memory space required for maintaining S_i. Tanaka proposed a key distribution system similar to the SKGS using the RSA(Rivest, Shamir, Adleman) cryptosystem. Tsujii, Itoh, and Kurosawa showed the threshold type of cryptosystem based on the ElGamal cryptosystem [4].

This section describes the modified key distribution scheme independent of the exposure of secret key based on Yacobi scheme. This scheme does not use secret key provided by key distribution center as own secret key but use random key generated by himself. There are also two modified key distribution schemes based on the Diffie-Hellman scheme. The second modified

scheme based on the DH can authenticate directly between users or among one sender and multi users with the same security level as Okamoto and Tanaka scheme.

A. Initial Key Generation and Distribution

The procedure of initial key generation and distribution are as follows.

1) When the network is set up, the key generation center produces two prime numbers p and q, each about 256 bits long and then determines a prime number e and an integer d, satisfying $e.d \{\mathrm{mod}(p-1).(q-1)\} = 1$, with both e and d less than $n = p.q$.

2) It also determines an integer g, which is a primitive element in $GF(p)$ and $GF(q)$.

3) For user i whose identification information is ID_i, the center calculates integers $S_i(i = 1, 2, ...) : S_i = ID_i^{-d} \pmod n$, where $S_i^e \cdot ID_i \pmod n = 1$.

4) Then, the center stores the set of integers (n, g, e, S_i) in the smart card for user i and distributes it to him.

5) For user j whose identification information is ID_j, the center calculates integers $S_j(j = 1, 2, ...) : S_j = ID_j^{-d} \pmod n$, where $S_j^e \cdot ID_j \pmod n = 1$.

6) Then, the center stores the set of integers (n, g, e, S_j) in the smart card for user j and distributes it to him.

7) After smart cards are distributed to all users, the users can authenticate each other. The integer d can be aborted after all the cards are distributed. If there are no new users expected, even the key generation center can close down. Hence, d is kept secret from any user, S_i is known only to user i, and n, g, e and ID_i are common to all the users.

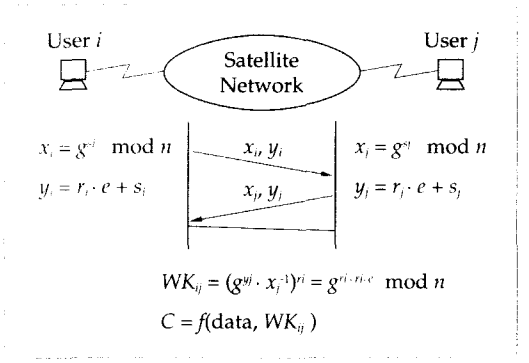
B. Modified Key Distribution Scheme based on the Yacobi Scheme

Initial key generation and distribution from key distribution center are same.

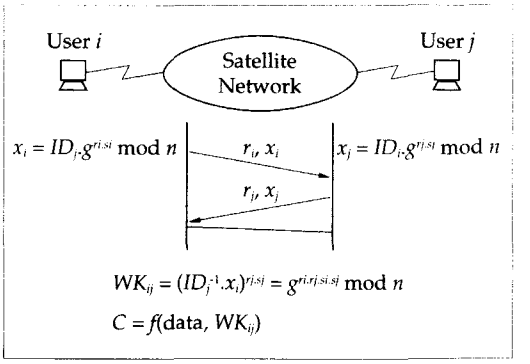
1) When users i and j wish to obtain a working key as a secret key, user i generates a random number r_i and sends user j the integer $x_i : x_i = g^{si} \pmod n$ and $y_i = r_i.e + s_i$.

2) User j also generates a random number r_j and sends user i the integer $x_j : x_j = g^{sj} \pmod n$ and $y_j = r_j.e + s_j$.

3) Then, users i and j compute working keys WK_i and WK_j, repectively, as follows : $WK_{ij} = WK_j = WK_i = (g^{yi} \cdot x_j^{-1})^{ri} = g^{ri.rj.e} \pmod n$. Figure 1 illustrates the working key generation phase based on the modified Yacobi scheme.



(Figure 1) Working Key Generation based on the Modified Yacobi Scheme



(Figure2) Working Key Generation based on the Modified DH Scheme

C. Modified Key Distribution Scheme 1 based on the DH Scheme

Initial key generation and distribution from key distribution center are same.

1) When users i and j wish to obtain a working key as a secret key, user i generates a random number r_i and sends user j the integer x_i : $x_i = ID_i \cdot g^{r_i s_i} \pmod n$.

2) User j also generates a random number r_j and sends user i the integer x_j : $x_j = ID_i \cdot g^{r_j s_j} \pmod n$.

3) Then, users i and j compute working keys WK_i and WK_j using $S_i^c \cdot ID_i \pmod n = 1$, repectively, as follows : $WK_{ij} = WK_j = WK_i = (ID_j^{-1} \cdot x_i)^{r_i s_j} = g^{r_i r_j s_i s_j} \pmod n$. Figure 2 illustrates the working key generation phase based on the modified DH scheme.

D. Modified Key Distribution Scheme 2 based on the DH Scheme

Another way based on the DH scheme is as follows.

Initial key generation and distribution from key distribution center are same.

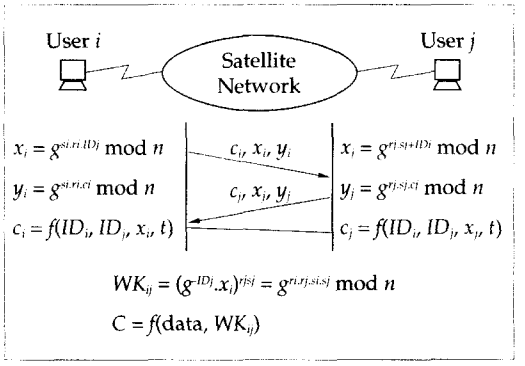
1) When users i and j wish to obtain a working key as a secret key, user i generates a random number r_i and sends user j the integer x_i ($x_i = g^{r_i s_i + ID_j} \pmod n$), y_i ($y_i = g^{r_i s_i c_i} \pmod n$) and $c_i = \text{hash}(x_i, ID_i, ID_j, t)$.

2) User j also generates a random number r_j and sends user i the integer x_j ($x_j = g^{r_j s_j + ID_i} \pmod n$), $y_j (y_j = g^{r_j s_j c_j} \pmod n)$ and $c_j = \text{hash}(x_j, ID_i, ID_j, t)$.

3) Then, users i and j compute working keys WK_i and WK_j, repectively, as follow : $WK_{ij} = WK_j = WK_i = (g^{-ID_j} \cdot x_i)^{r_j s_j} = g^{r_i r_j s_i s_j} \pmod n$.

4) User j can authenticate the sender, if the following equation holds : $S_j = x_i^{c_i'}/(y_i g^{ID_i c_i'} ID_i^d) \pmod n$

Where c_i' is the number calculated by user j with c_i. This is direct authentication. If x_i is changed to another number by an unauthorized user, c_i' is not equal to c_i as c_i is dependent on x_i. t is the time stamp with date and time. The schemes described above have an improved security level because they use the discrete logarithm function and prime resolution into factors. The schemes do not use the secret key generated by center as a power, but use the random number generated by the user. Figure 3 illustrates the working key generation as a secret key and authentication phase.



(Figure 3) Working Key Generation and Authentication based on the DH Scheme

E. Characteristics of Modified Key Distribution Schemes

1) The modified Yacobi scheme is independent of the exposure of the secret key. Because the scheme does not use the secret key provided by key distribution center as a power, but uses instead a random number generated by the user.

2) The modified Diffie-Hellman(DH) and ID(identity) is better on the exposure of secret key.

3) The second modified DH scheme has direct mutual authentication between user i and user j.

4) The second modified DH scheme also has non-repudiation function which can protect the deny of it after sending and receiving the data.

5) The second modified DH scheme is able to defend the network from impostors.

6) The second modified DH scheme has the same security level as the Okamoto and Tanaka scheme because the scheme is based on the discrete logarithm and prime resolution into factors.

7) The second modified DH scheme does not require any key distribution center to be active in each communication.

8) The second modified DH scheme randomly determined the working keys.

III. Applied to Satellite Network

Modern networks provide point-to-multipoint communication services such as

electronic mail, multiple teleconference, electronic transfer using satellite data network, and direct satellite broadcasting using satellite broadcasting networks. Ciphering algorithms and key distribution schemes are required to secure these services. This section presents that the modified DH scheme is applied to point-to-broadcasting communications via satellite called satellite broadcasting communications and to multicasting communications using satellite called satellite data communications.

A. Broadcasting Communication via Satellite [2]

Assume that transmitter station provides the key generation and management function.

1) Users register their ID_s at the transmitter station.

2) Transmitter station i generates x_i ($x_i = g^{ri,si+IDj} \pmod n$), y_i ($y_i = g^{ri,si,ci} \pmod n$) and $c_i = \text{hash}(x_i, ID_i, ID_j, t)$ for all users.

3) Transmitter station i generates the group working key $W_k = g^{\Pi ri,si} \pmod n$.

4) Transmitter station stores r_j, s_i, c_j, x_j, y_j, w_k, n, e, and d into smart cards for each user and transfers it to each user by mail or other transfer scheme.

5) User j receives a smart card with r_j, s_j, c_j, x_j, y_j, w_k, n, e, and d from the transmitter station and inserts it into his set-top box.

6) After that, user j can authenticate the transmitter station, and t receives broadcast programs transmitted from the transmitter station.

This scheme will be more efffective when adapted to CATV(Cable Television) using satellite.

B. Multicasting Data Communication via Satellite [2]

Assume a star network and users have a sequential key generation and distribution function in the network. It is also assumed that the key management center has already generated each user's unique key including s, e, d, ID, p, q, n for each user, stored this information in smart cards and transfered the cards to each user by mail or other transfer scheme.

1) User i generates a random number r_i and sends user $i + 1$ the x_i ($x_i = g^{ri,si+IDj} \pmod n$), y_i ($y_i = g^{ri,si,ci} \pmod n$) and $c_i = \text{hash}(x_i, ID_i, ID_j, t)$.

2) User i receives x_{i-1}, y_{i-1} and c_{i-1} from user i - 1 and then authenticates each other.
$S_{ri,si,ci} = x_{i-1}^{ci-1'}/(y_{i-1}.g^{IDi,ci-1}.\ ID_i^d) \pmod n$, where c_{i-1}' is the number calculated by user i with c_{i-1}. This is direct authentication. If x_{i-1} is changed to another number by an unauthorized user, c_{i-1}' is not equal to c_{i-1} since c_{i-1} is dependent on x_{i-1}.

3) If authentication is successful, it means that the message received by user i is transmitted via i-1, i-2, i-3, ..., i-j+1. User i then sends c_i, x_i and y_i to user i+1. x_i ($x_i = g^{r_i s_i + ID_j} \pmod n = g^{\prod (r_{i-k} s_{i-k} + ID_{i-k})} \pmod n$), y_i ($y_i = g^{r_i s_i c_i} \pmod n = g^{\prod (r_{i-k} s_{i-k} c_{i-k})} \pmod n$), $c_i = \text{hash}(x_i, ID_i, ID_j, t) = \text{hash}(x_{i-k}, ID_{i-k}, ID_{i+1}, t)$).

4) When the last user of the group receives x, c, y and authenticates it to the group, the working key of the group is generated as follows : the group working key, $W_k = g^{\prod r_i s_i} \pmod n$.

5) Now, the group has secure communication by using the specified cryptography algorithm in the group using the group working key.
This scheme will be more efffect if applied to VSAT (Very Small Aperture Terminal) data communication using satellite.

IV. Conclusions

Existing key distribution schemes encounter key management problems when changing key and adding new users. This paper presented a modified Yacobi scheme that does not use the secret key provided by center as a power, but uses instead a random number generated by the user. Because the modified Yacobi scheme is independent of the exposure of the secret key. Then this paper described modified DH schemes based on the discrete logarithm and prime resolution into factors as a kind of public key distribution scheme. The second modified DH scheme has direct mutual authentication between user i and user j. The second modified DH scheme also has a non-repudiation service which can protect the deny of sending and receiving after send/receive data from user and it can defend the network from impostors. The second modified DH scheme has the same security level as the Okamoto and Tanaka scheme because the scheme is based on the discrete logarithm and prime resolution into factors. The second modified DH scheme randomly determined the working keys. The second modified DH scheme was applied to point-to-multicasting, and broadcasting networks for working key between users in satellite communications. The applied protocol based on the second modified DH scheme can help the vulnerable satellite data communication problem over VSAT networks via satellite or satellite broadcasting services such as CATV via satellite, and will be widely extended when these networks expand to private networks.

References

[1] A. Shamir, "Identy-based Cryptosystems and Signature Schemes", Proc. Crypto 84, pp.47-53, 1984.

[2] I. Ingemarson, D.Tang, C.K. Wong, "A Conference Key Distribution System", IEEE Trans. IT-28, No.5, pp.714-720, 1982.

[3] K. Koyama, K. Ohta, "Identy-based

conference key distribution systems", Proc. Crypto 87, pp.175-184, 1984.

[4] EIJI OKAMOTO, KAZUE TANAKA, "Key Distribution System based on identification information", IEEE Journal on selected areas in communications, Vol.7, No.4, pp.481-485, May 1989.

[5] Jeong-Hyun Park, Sang-Ho Lee, "Secure Protocol for VSAT Network", 한국통신정보보호학회 논문지, 제5권 제3호, 1995.12.

[6] Douglas R. Stinon, "Cryptography : Theory and Practice", CRC press, 1995.

[7] Warwick Ford, "Computer Communications Security", PTR Prentice Hall, 1994.

[8] William Stallings, "Network and Internetwork Security", Prentice-Hall, Inc., 1995.

□ 著者紹介

박 정 현

Senior Engineer, Imformation Infrastructure Network section at ETRI in Korea (1982.3-Present).

M.S, Soongsil Graduate School (Electronics Engineering Department) in Korea (1985).

B.S, Soongsil University (Electronics Engineering Department) in Korea (1982).

Research interest : Security protocol, Cryptology, Satellite communication.

이 상 호

B.S., Soongsil University (Computer Science Department) in Korea (1976).

M.S., Soongsil Graduate School (Computer Science Department) in Korea(1981).

Ph.D., Soongsil Graduate School (Computer Science Department) in Korea(1989).

Professor, Chungbuk National University (Computer Science Department) in Korea (1981-Present)

Post Doc, UBC in Canada (1992.9-1993.8).

Research interset : Protocol engineering, Simulation, Software engineering, Cryptology.