Efficient Key agreement protocol using Proxy server for Wireless communication

SOO-HYUN OH*, JIN KWAK*, SANG-MAN AHN*, DONG-HO WON*
*Information and Communications Security Laboratory
School of Information and Communications Engineering
Sungkyunkwan University
300 Chunchun-Dong, JangAn-Gu, Suwon, Kyunggi-Do
KOREA
{shoh, jkwak, smahn, dhwon}@dosan.skku.ac.kr

Abstract : A key agreement protocol is the most important part to establish a secure cryptographic system and the effort to standardize the key agreement protocols is in rapid progress. Several efficient and secure key agreement protocols have been proposed so far since Diffie-Hellman proposed a public key agreement system in 1976. But, since Diffie-Hellman based key agreement protocols need a lot of computation to establish the session key, they are not proper to apply wireless Internet environment.

In this paper, we propose the efficient key agreement protocol using proxy server. The proposed protocol supports the security of the Diffie-Hellman based protocol and the computation work of mobile user can be decreased using proxy server.

Key-Words : *Key agreement protocol, Wireless Internet, Diffie-Hellman problem, proxy-based cryptosystem, Active attack*

1. Introduction

Recently, wireless Internet services have been activated with mobile device such as cellular phone and PDA(Personal Digital Assistance).

On the behalf of the development of the mobile communication, users can access the Internet without a direct access to the network and use the services like ordering products, making a reservation and Internet banking.

Moreover, it needs to use cryptosystem as wired environment in order to offer the more secure wireless Internet service and key distribution protocol is the most important part to establish a secure cryptographic system.

However, wireless Internet environment falls behind wired communication environment in the computation capabilities of device and power supply device. So, it's very hard to apply public key crypto system as wired environment. Therefore, various studies are in progress to solve these kinds of problem nowadays.

There are some means of settle this trouble. One is the using of elliptic curve crypto system which using relatively short key and another is the method that the computation that demand device user keys upon on server.

The server-based method is used in digital signature and authentication systems that are lots of the computation depend on free option proxy server.

In this paper, we propose the efficient protocol in the wireless Internet environment which Diffie-Hellman based key agreement protocol is transformed into. This method has security of the existing protocol but the computation demands device user can be decreased using proxy server.

This paper is constructed as follows. In the section 2, we describe the dhHybrid protocol based on Diffie-Hellman problem among ANSI X9.42[1]. In the section 3, we propose the proxy-based key agreement protocol that is the variant scheme of dhHybrid protocol and can reduce computation work of end entity using mobile device and analyze properties of proposed protocol. In the section 4, we analyze the security of proposed protocol under several attacker models and finally make a conclusion in the section 5.

2. Related Works

The key distribution protocol is secure and efficient

mechanism to establish common shared secret value through insecure channel such as Internet. Several efficient and secure key distribution protocols have been proposed so far since Diffie-Hellman proposed a public key agreement system in 1976[2].

Key distribution protocol can be divided into two classes according to the type of computing the secrete session key. In key agreement protocol, user A and B compute the secret session key without any prior consultation. But in key transmission protocol, user A selects the secret session key one-sidedly then sends it to user B.

Also, key distribution protocol can be divided into two classes according to the type of using the cryptographic system. One is protocol using conventional cryptosystem and the other is protocol using public key cryptosystem.

But in conventional cryptographic system, two users have to share a secret key through the unsecured channel in advance, it is difficult to use in opened network. So public key based protocols are widely used.

Many key distribution protocols using public key cryptosystem have been proposed so far and the effort to standardize the key agreement protocols are in rapid progress. The typical standard documents of key distribution protocol are ANSI X9.42, ANSI X9.63, IEEE P1363, PKCS#3 and so on.

In this section, we describe the dhHybrid protocol based on Diifie-Hellman problem among ANSI X9.42 protocols and in the next section, propose the variant of this protocol.

The definitions of parameters used in this protocol are as follows. p is a large prime more than 512 bit and g is an element of Z_p with ord(g)=q. x_i is a static private key of user i, $y_i = g^{x_i} \bmod p$ is a static public key of user i and || means concatenation.

[dhHybrid protocol]

① User A selects random number $r_A \in Z_q$ and computes $t_A = g^{r_A} \bmod p$.

② User A sends his/her ephemeral public key t_A and static public key y_A to user B.

③ User B selects random number $r_B \in Z_q$ and computes $t_B = g^{r_B} \bmod p$.

④ User B sends his/her ephemeral public key t_B and static public key y_B to user A.

⑤ Both user A and B compute a shared secret value C as follows.

$$C = y_B^{x_A} \| t_B^{r_A} = y_A^{x_B} \| t_A^{r_B} = g^{x_A x_B} \| g^{r_A r_B} \bmod p$$

Both parties generate their common session key with two numbers of passes. This protocol also does not offer the entity authentication and key confirmation. But an implicit key authentication can be achieved with a static secret key. And mutual key freshness is guaranteed because both parties use random number in each session.

Also, user A and B have to execute 3 modular exponentiation to generate a session key. Therefore, dhHybrid protocol isn't proper to mobile communication environment using mobile devices with low computation capacity such as cellular phone and PDA(Personal Digital Assistance).

To solve this problem, in next section, we propose proxy-server based key agreement protocol which proxy server carry out heavy computation such as modular exponentiation and end users carry out only a light computation such as hash function and conventional cryptosystem.

3. Proposed Efficient Key agreement protocols using Proxy server

3.1 System parameters

The definitions of system parameters used in the proposed protocol are as follows.

- p : a large prime with $2^{511}<p<2^{512}$
- g : a primitive element in Z_p($g^{p-1} = 1 \bmod p$)
- x_A : user A's private key
- y_A : $y_A = g^{x_A} \bmod p$, user A's public key

- x_P : Proxy server's private key
- y_P : $y_P = g^{x_P} \bmod p$, Proxy server's public key
- x_B : Web server B's private key
- y_B : $y_B = g^{x_B} \bmod p$, Web server B's public key
- K_{AP} : common secret key between user A and proxy server
- E( )/D( ) : the encryption/decryption algorithm of symmetric cryptosystem

3.2 Proposed Protocol

The phase of session key establishment of proposed protocol is divided the phased of proxy key generation and session key generation.

The phase of proxy key generation, which a user selects proxy server and sends proxy information to the server, is executed only one time when user enters the proxy server. The method proposed by M. Mambo[6] is used in the proxy key delegation.

[Proxy key delegation]

① User A chooses a secret random number r from [1, ..., p-1] and computes $K = g^r \bmod p$ and $x_{AP} = x_A + r \cdot K \bmod p-1$.

② User A sends the generated values (x_{AP}, K) to the proxy agent over a secure channel.

③ The proxy server accepts x_{AP} as a valid proxy key from user A, if and only if $g^{x_{AP}} \equiv y_A \cdot K^K \bmod p$.

After user A sends proxy key to the proxy server, user A and web server B generate a shared secret value as follows.

[Generation of shared secret value]

If user A using mobile device wants to secure communication with web server B, he/she sends request message of session key generation to the proxy server.

① Proxy server selects random number $r_P \in_R Z_{p-1}$ and computes $t_p = g^{r_P} \bmod p$.

② Proxy server selects random number x∈[1, ... , p-1] and computes (r, s) as follows.

$$r = H(g^x \bmod p,\ t_p)$$
$$s = x / (r + x_{AP}) \bmod p-1$$

④ Proxy server transmits (y_{AP}, K, t_p, r, s) to web server B.

⑤ Web server B checks $y_{AP} = y_A \cdot K^K \bmod p$ and convince that proxy server requires the generation of session key by request of user A.

⑥ Web server B computes $r' = (y_{AP} \cdot g^r)^s \bmod p$ and checks $r = H(r', t_p)$.

⑦ Web server B selects $r_B \in_R Z_{p-1}$ computes $t_B = g^{r_B} \bmod p$ and sends (y_B, t_B) to proxy server.

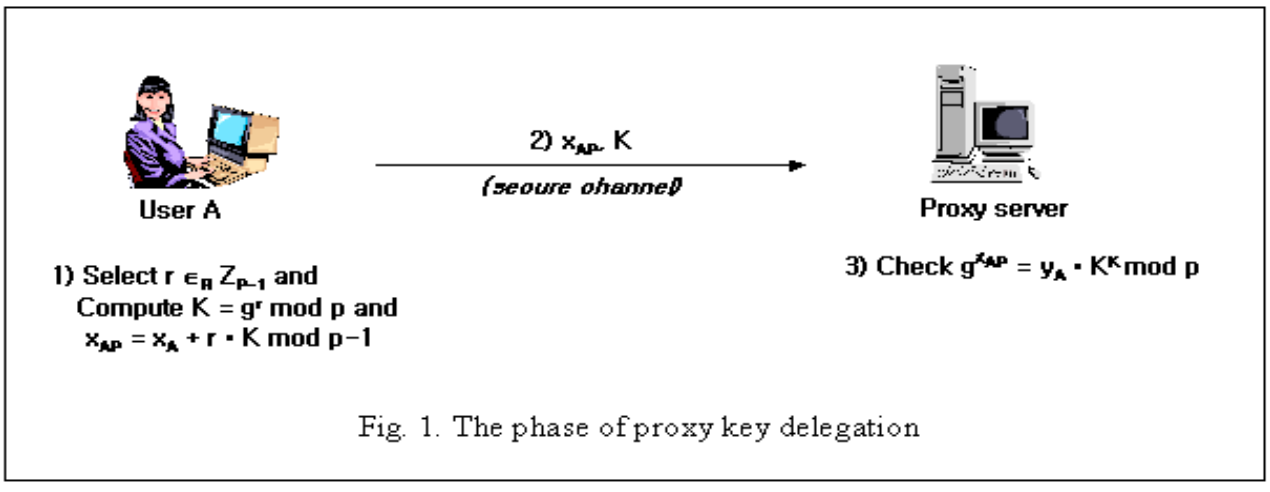

Fig. 1. The phase of proxy key delegation

⑧ Web server B generates a shred secret value C as follows.

$$C = y_A^{x_B} \| t_P^{r_B} = g^{x_A x_B} \| g^{r_A r_B} \bmod p$$

⑨ Proxy server computes $C' = t_B^{r_P} \bmod p$ and encrypts it using K_{AP}. Then, proxy server transmits $E_{K_{AP}}(C')$ to user A.

⑩ User A decrypts $E_{K_{AP}}(C')$ and obtains C'. Then, he/she generates $C = y_B^{x_A} \| C'$. (The value $y_B^{x_A}$ can be pre-computed because it is static value.)

⑪ Both user A and web server B compute the session key SK using key derivation function.

[Session key derivation function]

Let *hashlen* denote the length of the output of the hash function chosen, and let *maxhashlen* denote the maximum length of the input to the hash function.

- Inputs
  - C : A bit string denoting the shared secret value
  - *keylen* : An integer representing the length in bits of the session key SK to be generated
  - (optional) *OtherInfo* : A bit string consisting of some data shared by the two entities intended to shared the secret value C

- Actions
  - The key derivation function is computed as follows

1) Let d = $\lceil keylen / hashlen \rceil$
2) Initiate a counter as 00000001_{16}
3) For i = 1 to d
   i) compute h_i = H(C || counter || [*OtherInfo*])
   ii) Increment counter
   iii) Increment i
4) Compute SK = the leftmost *keylen* bits $h_1 || h_2 || ... || h_d$

- Output
  - The session key SK as a bit string of length *keylen* bits

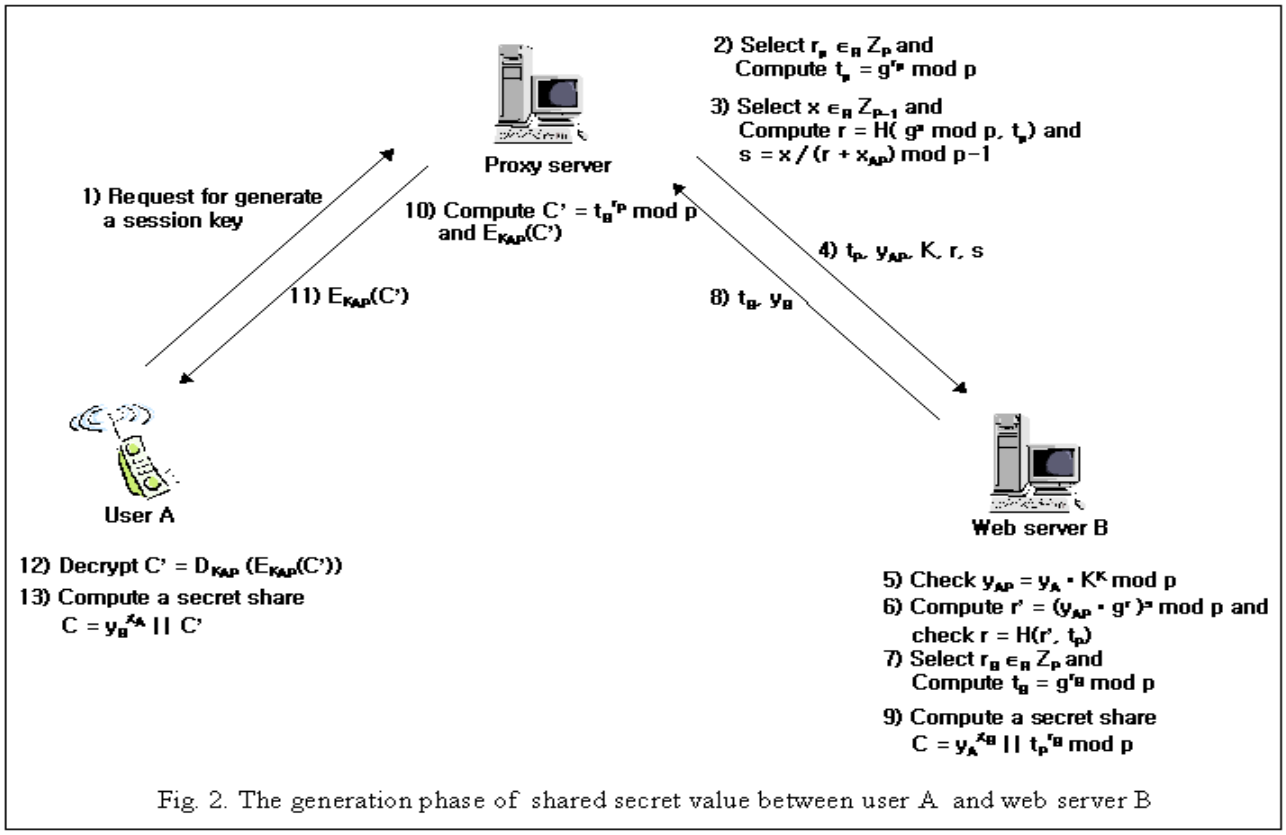

Fig. 2. The generation phase of shared secret value between user A and web server B

3.3 Properties of proposed protocols

The proposed protocol can provide mutual implicit key authentication and mutual key freshness same as dhHybrid scheme.

Although proxy server generates user A's ephemeral private/public key, it can't compute the session key between user A and web server B without user A's static public key.

Also, since proxy server carries out heavy computation such as modular exponentiation, proposed protocol can be reduced computational load of end user. So, it is suitable to wireless Internet environment using mobile devices with low computation capacity such as cellular phone and PDA.

Also, since $y_B^{x_A}$ is fixed value for each web server, for the server used frequently, the value of $y_B^{x_A}$ can be pre-computed and stored in mobile device. So, the computational load of mobile user to generate the session key can be reduced.

In other words, mobile user can establish different session key every session with web server by means of the hash function operation and decryption operation of the conventional cryptosystem.

Furthermore, dhHybrid protocol dose not provide any entity authentication about identity of the other side party. But, in the proposed protocol, any attacker cannot impersonate proxy server because web server B can authenticate the identity of proxy server.

Table 1 is summary of the comparison of dhHybrid and proposed protocol.

Table 1. Comparison of dhHybrid protocol and proposed protocol

	dhHybrid	Proposed protocol
Entity Authentication	Not provide the entity authentication	A web server B can convince identity of proxy server
Implicit key Authentication	Mutual	Mutual
Key freshness	Mutual	Mutual
Computational work of user A	**3 Modular Exponentiation**	**1 Modular Exponentiation**

4. Security Analysis

1) Can a proxy server compute the session key between user A and web server B?

Although proxy server generates user A's ephemeral private/public key, it can't compute the session key between user A and web server B without user A's static public key.

The difficulty of proxy server to compute the session key between user A and web server B is equivalent to Diffie-Hellman problem. So, the proxy server can't compute the session key if and only if Diffie-Hellman problem is infeasible.

2) Can the passive attacker compute the session key between user A and web server B?

In the proposed protocol, the passive attacker's difficulty of computation of session key between user A and web server B is equivalent to Diffie-Hellman problem. So, the passive attacker can't obtain the session key if and only if Diffie-Hellman problem is infeasible.

3) Can the attacker impersonate as a proxy server?

When an attacker tries to impersonate as proxy server to establish session key with web server B, he/she can't generate a valid digital signature (r, s) since he/she doesn't know secret proxy key x_{AP}. So, the attacker can't impersonate as proxy server.

4) Does the proposed protocol secure against active attackers?

- ***Active Impersonation(AI) attack*** : When an attacker tries to impersonate as user A to request for generating session key, he/she can't not only decrypt ciphertext received from proxy server but also compute session key because he/she doesn't know shared secret key K_{AP} and user A's static private key. So, in the proposed protocol, active impersonation is impossible.

- ***Key-Compromise Impersonation(KCI) attack*** : Even if an attacker obtains user A's private key, he/she can't compute the session key since he/she doesn't know the shared secret key of user A and server. Therefore, an attacker can't impersonate user A although he/she knows A's private key. But, an attacker can impersonate the web server

B if he/she obtains A's private key.

- ***Forward Secrecy(FS)*** : In the proposed scheme, session key still can be protected even if the private keys of both entities are compromised. So, proposed protocol can provide full forward secrecy.

- ***Known Key Security(KKS)*** : In the proposed scheme, since the both entity's random numbers are included in the session key, even if an adversary obtain the previous session key and key tokens, he cannot get any advantage from that information to compute the present session key. The ability of the adversary with that information is exactly the same as the one without any information. The proposed protocol is secure against both of known key passive(KKP) attack and known key impersonation(KKI) attack.

The result of security analysis of dhHybrid protocol and the proposed protocol is summarized in Table 2.

Table 2. Result of security analysis

	dhHybrid	Proposed protocol
AI	Secure	Secure
KCI	Any attacker can impersonate user A or web server B.	No attacker can impersonate user A
FS	provides full FS	provides full FS
KKP	Secure	Secure
KKI	Secure	Secure

5. Conclusion

Recently, wireless Internet services have been activated with mobile device such as cellular phone and PDA(Personal Digital Assistance).

Moreover, it needs to use cryptosystem as wired environment in order to offer the more secure wireless Internet service.

The key distribution protocol is the most important part to establish a secure cryptographic system. Several efficient and secure key agreement protocols have been proposed so far since Diffie-Hellman proposed a public key agreement system in 1976. But, since Diffie-Hellman based key agreement protocols need a lot of computation to establish the session key, they are not proper to apply wireless Internet environment.

In this paper, we propose the efficient key agreement protocol using proxy server. The proposed protocol supports the security of the Diffie-Hellman based protocol and the computation work of mobile user can be decreased using proxy server.

References:

[1] ANSI X9.42, "Agreement of symmetric Key on Using Diffie-Hellman Cryptography", 2001.

[2] W. Diffie, M.E. Hellman, "New directions in cryptography", IEEE Transaction of Information Theory, IT-22, 6, pp. 644-654, 1976.

[3] W. Diffie, P.C. Oorschot, M.J. Wiener, "Authentication and Authenticated Key Exchange", Designs, Codes and Cryptography, pp. 107-125, 1992.

[4] T. ElGamal, "A Public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory IT-31, pp. 469-472, 1985

[5] IEEE P1363, "Standard for Public-Key Cryptography", Working draft D13, 1999

[6] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures : Delegation of the power to sign message", IEICE Trans, on Fundamentals, E79-A(9):1338-1354, 1996

[7] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation", Proc. Third ACM Conference on Computer and Communications Security, pp.48-57, 1996

[8] Y. Zheng, "Shortened digital signature, signcryption and compact and unforgeable Key agreement schemes , IEEE P1363 Standard for Public Key Cryptography : Additional Techniques