Future Generation Computer Systems 27 (2011) 620–626

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

A secure broadcasting cryptosystem and its application to grid computing

Eun-Jun Yoon [a], Kee-Young Yoo [b,*]

[a] School of Computer Science and Engineering, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea

[b] Department of Computer Engineering, Kyungpook National University, 1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, South Korea

ARTICLE INFO

Article history:
Received 25 February 2010
Received in revised form
13 September 2010
Accepted 24 September 2010
Available online 1 October 2010

Keywords:
Network security
Broadcasting cryptosystem
Grid computing
Group communications

ABSTRACT

Security is one of the major requirements of grid computing. In grid computing environments, it should be guaranteed that efficient and secure authenticated broadcasting technologies have been applied for users and servers. In addition, it should be ensured that resources and data are not provided by an attacker. The main purpose of a broadcasting cryptosystem is to establish a secure communication channel from a sender to a group of legal receivers. Recently, several broadcasting cryptosystems have been proposed based upon various cryptographic techniques. However, many researchers pointed out the several security weaknesses in the many previously proposed broadcasting cryptosystems. This paper proposes a new secure broadcasting cryptosystem that can withstand various security attacks and is applicable to grid computing environment. As a result, the proposed broadcasting cryptosystem not only has advantages of the broadcasting cryptosystem, but also is more secure and practical compared with previous related broadcasting cryptosystems.

1. Introduction

Security is one of the major requirements of grid computing [1–8]. Grid technology enables complex interactions among computational and data resources. To be deployed in production computing environments, grid, however, needs to implement additional security mechanisms. In the grid computing environments, it should be guaranteed that efficient and secure authenticated broadcasting technologies have been applied for users and servers. In addition, it should be ensured that resources and data are not provided by an attacker. Recent compromises of user and server machines at grid sites have resulted in the need for efficient and secure authenticated broadcasting technologies based authentication and key exchange mechanisms [9–17].

The main purpose of a broadcasting cryptosystem is to establish a secure communication channel from a sender to a group of legal receivers [9,12,14,18–21]. In the broadcasting cryptosystem, a sender can broadcast an encrypted message to a group of legal receivers. Then, only legal receivers can decrypt the message, and illegal receivers cannot acquire any important information from the broadcast message.

Up to now, several broadcasting cryptosystems [9,12,14,18–28] have been proposed based upon various cryptographic techniques. However, the many previously proposed broadcasting cryptosystems [18–20] need many broadcasting messages for a group of legal receivers, and it is hard to add new users into the previous constructed groups. To eliminate these security flaws and provide flexibility, Liaw [21] proposed a secure broadcasting cryptosystem with fewer broadcasting messages based on the RSA cryptosystem and symmetric cryptosystem, which allows easy addition of new users into the active groups. However, Sun [22] showed that Liaw's broadcasting cryptosystem actually becomes infeasible since a prohibitively large amount of information must be kept by each user, and be sent as the re-key message for each broadcast. On the other hand, Tseng and Jan [23] also pointed out several security weaknesses in Liaw's cryptosystem in 2001. That is, Tseng and Jan showed that an intruder can break the security of the broadcasting cryptosystem because he/she can obtain the master secret key by means of a conspiracy attack. To remedy this attack, Tseng and Jan also proposed a modified broadcasting cryptosystem.

Nonetheless, in 2006, Masque and Peinado [24] pointed out that Tseng and Jan's broadcasting cryptosystem [23] actually does not work due to incorrect arithmetic and then presented a redefined Liaw's broadcasting cryptosystem, claiming to have solved all the various problems. In spite of all these efforts [21–24], in 2008, Zhu and Wu [29] showed that the redefined Liaw's scheme [24] is still insecure in that an unauthorized user is able to obtain the shared secret, which is only intended for certain privileged users. That is, in the Masque and Peinado broadcasting cryptosystem, any unauthorized user can actually obtain the secret session key, which is a secret only intended for the privileged group. However, Zhu–Wu did not provide an improvement of the redefined Liaw's broadcasting cryptosystem. In addition, we found that the redefined Liaw's broadcasting cryptosystem has other security problems.

This paper extends our previous works in [25] and then proposes a new secure authenticated broadcasting cryptosystem

* Corresponding author. Tel.: +82 53 950 5553; fax: +82 53 957 4846.
E-mail address: yook@knu.ac.kr (K.-Y. Yoo).

0167-739X/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2010.09.012

that not only can withstand various security attacks including Zhu–Wu's attack and our proposed attacks, but is also applicable to grid computing environments. As a result, the proposed broadcasting cryptosystem not only has advantages of the broadcasting cryptosystem, but also is more secure and practical compared with previous related broadcasting cryptosystems.

The remainder of this paper is organized as follows: Section 2 reviews the Zhu–Wu's cryptanalysis of the redefined Liaw's broadcasting cryptosystem. Section 3 presents an outline of the proposed attacks on the redefined Liaw's broadcasting cryptosystem. The proposed cryptosystem is presented in Section 4, while Sections 5 and 6 discuss its security and performance, respectively. Finally, Section 7 concludes the paper.

2. Related works

This section reviews the redefined Liaw's broadcasting cryptosystem proposed by Masque et al. in [24] and Zhu–Wu's cryptanalysis [29] of the cryptosystem [24], respectively. Fig. 1illustrates a general architecture of broadcasting cryptosystem.

2.1. Redefined Liaw's broadcasting cryptosystem

Fig. 2 illustrates the redefined Liaw's broadcasting cryptosystem [24]. The cryptosystem is based on some RSA-like arithmetic and is composed of three phases: system setup, broadcasting, and decryption.

2.1.1. System setup phase

In the system, there is a central authority server (CAS for short). The CAS is responsible for generating the system parameters and the keys for all users. Consider a system composed of n users $\{U_i\}_{i=1}^{n}$ under the coordination of CAS.

(1) CAS generates the public and private keys for every user $\{U_i\}_{i=1}^{n}$ in the system and defines the following system parameters: Let $N = pq$ be a public RSA modulus, where $p = 2p' + 1$, $q = 2q' + 1$, and p, q, p', q' are all large prime numbers. Let $\lambda(N) = lcm(p-1, q-1) = lcm(2p', 2q') = 2p'q'$ be the Euler totient function.
(2) CAS chooses an encryption function $f(x) = x^e \bmod \lambda(N)$.
(3) CAS chooses two exponents e and d such that $ed \equiv 1 \pmod{\lambda(N)}$.
(4) CAS chooses a system key $K_0 \in \mathbb{Z}_n$ and a random number r_c.
(5) CAS selects a prime number t_i for each user U_i, where $1 \le i < n$, such that $t_i^{-1} \bmod \lambda(N)$ exists.
(6) CAS assigns to U_i a private key K_i and a public key P_i as follows:

$$K_i = K_0^{t_i} \bmod N \tag{1}$$

$$P_i = f(t_i^{-1} r_c) = (t_i^{-1} r_c)^e \bmod \lambda(N). \tag{2}$$

(7) CAS $\rightarrow U_i$: K_i
CAS sends each private key K_i to U_i over a secure channel, where $1 \le i < n$.
(8) CAS publishes d, N and P_i which can be known to all, and keeps secure $e, K_0, r_c, \{t_i\}_{i=1}^{n}$, and any information on factorizing N.

2.1.2. Broadcasting phase

Assume that a sender $S = U_1$ wants to broadcast a message M to a group of users $\mathcal{G} = \{U_i\}_{i=2}^{a}$, where $a < n$. Then, the following steps have to be performed to broadcast a message M.

(1) $S \rightarrow$ CAS: $\mathcal{G}$
S sends the user identities $\mathcal{G} = \{U_i\}_{i=2}^{a}$ to CAS.
(2) CAS computes B and $f(B)$ as follows:

$$B = t_1 t_2 \ldots t_a \bmod N \tag{3}$$

$$f(B) = B^e \bmod \lambda(N). \tag{4}$$

(3) CAS $\rightarrow \{S, \mathcal{G}\}$: $f(B)$
CAS broadcasts $f(B)$ to both S and the legitimate receivers $\mathcal{G}$.
(4) S computes the common shared session key sk as follows:

$$\begin{aligned} sk &= K_1^{(f(B)P_1)^d} \bmod N \\ &= K_1^{(Bt_1^{-1} r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_1^{Bt_1^{-1} r_c} \bmod N \\ &= K_0^{Br_c} \bmod N. \end{aligned} \tag{5}$$

(5) S encrypts its message M as $C = E_{sk}(M)$.
(6) $S \rightarrow \mathcal{G}$: C
S broadcasts C to the legitimate receivers $\mathcal{G}$.

2.1.3. Decryption phase

When the legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^{a}$ receive C from the sender S, then the following steps have to be performed to get the message M from $C = E_{sk}(M)$.

(1) $\mathcal{G}$ compute the common shared session key sk from its private key K_i, public key P_i, and the received public parameter $f(B)$ as follows:

$$\begin{aligned} sk &= K_i^{(f(B)P_i)^d} \bmod N \\ &= K_i^{(Bt_i^{-1} r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_i^{Bt_i^{-1} r_c} \bmod N \\ &= K_0^{Br_c} \bmod N. \end{aligned} \tag{6}$$

(2) $\mathcal{G}$ decrypt C as $D_{sk}(C)$ and get the message M.

2.2. Zhu–Wu's cryptanalysis

Zhu and Wu [29] pointed out that an unauthorized user $U_j \notin \mathcal{G}\{S\}$, which is neither a member in the privileged group nor the sender, can easily obtain the common shared session key sk between the sender S and the legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^{a}$ in the redefined Liaw's broadcasting cryptosystem. That is, Zhu–Wu showed that U_j can simply derive the session key sk from the broadcast $f(B)$, just like the sender S or any intended receiver $U_i \in \mathcal{G}$ does as follows. By using an unauthorized user U_j's private key K_j, public key P_j, the CAS's public key d and the intercepted value $f(B)$, U_j can derive the shared session key sk from the following computation:

$$\begin{aligned} sk &= K_j^{(f(B)P_j)^d} \bmod N \\ &= K_j^{(Bt_j^{-1} r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_j^{Bt_j^{-1} r_c} \bmod N \\ &= K_0^{Br_c} \bmod N. \end{aligned} \tag{7}$$

Therefore, any $U_j \notin \mathcal{G}\{S\}$ can easily decrypt the ciphertext $C = E_{sk}(M)$ from S to recover the original message M because $K_0^{Br_c}$ is the same session key which is computed by S and $\mathcal{G} = \{U_i\}_{i=2}^{a}$.

3. Further cryptanalysis

This section shows that the redefined Liaw's broadcasting cryptosystem is vulnerable to the integrity violence of the session key from illegal modification, the session key modification attack and the message modification attack.

3.1. Integrity violence of the session key from illegal modification

The redefined Liaw's broadcasting cryptosystem is vulnerable to an integrity violence of the session key from illegal modification.

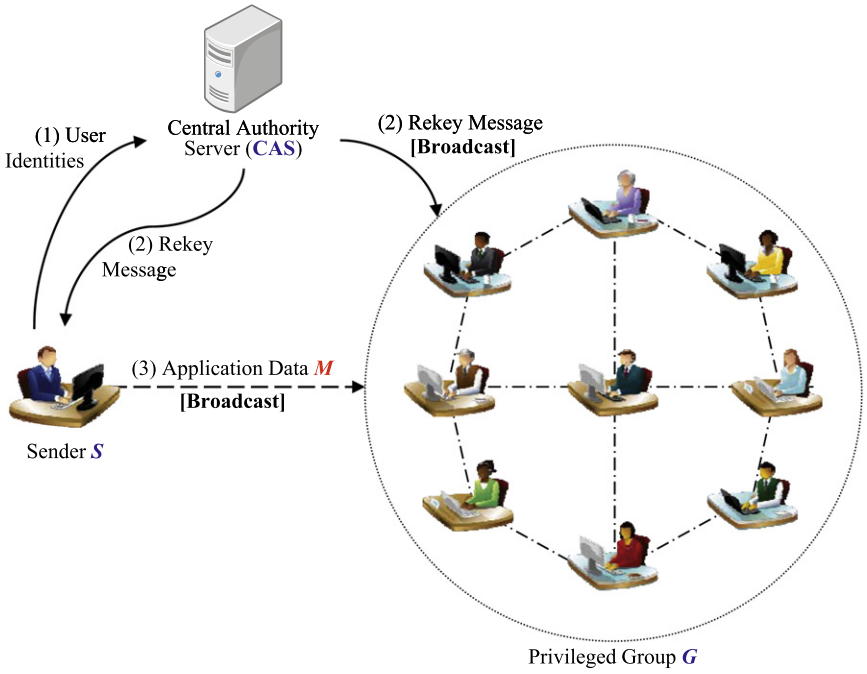

Fig. 1. General architecture of broadcasting cryptosystem.

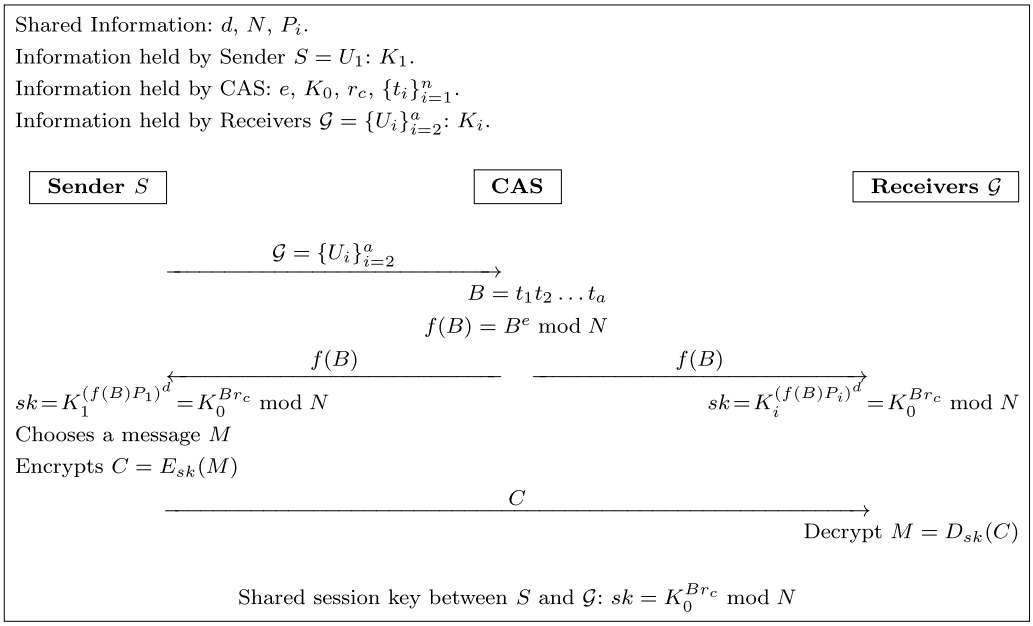

Fig. 2. The redefined Liaw's broadcasting cryptosystem.

Suppose that an attacker interposes the communication between CAS and users. Then, he/she can perform the illegal modification attack as follows:

(1) When CAS broadcasts $f(B)$ to both S and the legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^{a}$ in Step 3 of the broadcasting phase, an attacker intercepts it.
(2) The attacker chooses a random number t_x and broadcasts it to both S and $\mathcal{G}$.
(3) Upon receiving t_x, both S and $\mathcal{G}$ will derive the same wrong session key as follows:

$$\begin{aligned} sk^* &= K_i^{(t_x P_i)^d} \bmod N \\ &= K_i^{(t_x t_i^{-1} r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_i^{t_x t_i^{-1} r_c} \bmod N \\ &= K_0^{t_x r_c} \bmod N. \end{aligned} \tag{8}$$

From the above Eq. (8), we can see that sk^* is not equal to $sk = K_0^{Br_c}$. However, both S and $\mathcal{G}$ cannot detect the generation of this wrong session key because they have the same session key. From now, both S and $\mathcal{G}$ shall use the wrong session key in encrypting/decrypting their messages. Through this illegal modification attack, the attacker can neither obtain sk^* but can make two parties believe and use an unintended session key. In fact, an illegal modification attack is not a serious attack, since it cannot prevent the two communication parties from reaching a common secret key, even though this key is not the correct one.

Most important, the attacker cannot access the agreed common key from this illegal modification attack. However, since the Diffie–Hellman session key sk^* is invalid, it cannot guarantee the integrity of the session key. Therefore, the redefined Liaw's broadcasting cryptosystem is vulnerable to an integrity violence of the session key from illegal modification.

3.2. Session key modification attack

The redefined Liaw's broadcasting cryptosystem is vulnerable to session key modification attack as follows:

(1) When CAS broadcasts $f(B)$ to both S and $\mathcal{G} = \{U_i\}_{i=2}^{a}$ in Step 3 of the broadcasting phase, an attacker intercepts it.
(2) The attacker sets $t_x = 0$ and broadcasts it to both S and $\mathcal{G}$.
(3) Upon receiving t_x, both S and $\mathcal{G}$ will derive the same wrong session key as follows:

$$\begin{aligned} sk^* &= K_i^{(t_x P_i)^d} \bmod N \\ &= K_i^{(0 \cdot P_i)^d} \bmod N \\ &= K_i^0 \bmod N \\ &= 1 \bmod N. \end{aligned} \tag{9}$$

As a result, when the sender S encrypts its message M as $C = E_{sk}(M)$ and broadcasts it to the legitimate receivers $\mathcal{G}$, the attacker can also decrypt C by using the same wrong session key $sk^* = 1$. Therefore, the redefined Liaw's broadcasting cryptosystem is vulnerable to session key modification attack.

3.3. Message modification attack

The redefined Liaw's broadcasting cryptosystem is vulnerable to message modification attack as follows:

(1) When S broadcasts C to $\mathcal{G}$ in Step 6 of the broadcasting phase after encrypting its message M as $C = E_{sk}(M)$, an attacker intercepts it.
(2) The attacker sets $C^* = X$, where X is a random value, and broadcasts it to $\mathcal{G}$.
(3) Upon receiving $C^* = X$ from the attacker in the decryption phase, $\mathcal{G}$ will decrypt the meaningless message M^* as follows:

$$M^* = D_{sk}(C^*). \tag{10}$$

This message modification attack by the attacker can succeed because the legitimate receivers $\mathcal{G}$ do not verify the integrity of the decrypted message M^*. Therefore, the redefined Liaw's broadcasting cryptosystem is vulnerable to message modification attack.

4. Proposed authenticated broadcasting cryptosystem and its application to grid computing

This section first proposes a new authenticated broadcasting cryptosystem that can withstand the above described attacks and then presents its application to grid computing environments.

4.1. The proposed authenticated broadcasting cryptosystem

Fig. 3 illustrates the proposed authenticated broadcasting cryptosystem and it is composed of three phases: system setup, broadcasting, and decryption.

4.1.1. System setup phase

This phase is similar to the redefined Liaw's broadcasting cryptosystem. Consider a system composed of n users $\{U\}_{i=1}^{n}$ under the coordination of CAS.

(1) CAS performs same operations (1)–(6) like the redefined Liaw's broadcasting cryptosystem mentioned above.
(2) CAS chooses a secure one-way hash function $h(x)$, such as SHA-1 or SHA-256 [30,31].
(3) CAS $\rightarrow U_i$: $K_i = K_0^{t_i} \bmod N$
CAS sends each private key K_i to U_i over a secure channel, where $1 \le i < n$.
(4) CAS publishes d, N, $f(x)$, $h(x)$ and P_i which can be known to all, and keeps securely e, K_0, r_c, $\{t_i\}_{i=1}^{n}$, and any information on factorizing N.

4.1.2. Broadcasting phase

Assume that the sender $S = U_1$ wants to broadcast a message M to a group of users $\mathcal{G} = \{U_i\}_{i=2}^{a}$, where $a < n$. Then, the following steps have to be performed to broadcast a message M.

(1) $S \rightarrow$ CAS: $\mathcal{G}$
S sends the user identities $\mathcal{G}$ to CAS.
(2) CAS generates a random integer z and computes Z_l, where $1 \le l \le a$, as follows:

$$Z_l = E_{K_l}(z). \tag{11}$$

(3) CAS computes $B, f(B)$ and Y as follows:

$$B = t_1 t_2 \ldots t_a \bmod N \tag{12}$$

$$f(B) = B^e \bmod \lambda(N) \tag{13}$$

$$Y = h(z, f(B)). \tag{14}$$

(4) CAS $\rightarrow \{S, \mathcal{G}\}$: $\{Z_l, f(B), Y\}$
CAS broadcasts $Z_l, f(B)$ and Y to both S and $\mathcal{G}$.
(5) S decrypts Z_1 as $z = D_{K_1}(Z_1)$ and gets the random integer z.
(6) S verifies whether $Y \stackrel{?}{=} h(z, f(B))$. If this holds, then S authenticates the CAS. Otherwise, S stops the broadcasting phase.
(7) S computes the common shared session key sk as follows:

$$\begin{aligned} sk &= K_1^{z(f(B)P_1)^d} \bmod N \\ &= K_1^{z(Bt_1^{-1}r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_1^{zBt_1^{-1}r_c} \bmod N \\ &= K_0^{zBr_c} \bmod N. \end{aligned} \tag{15}$$

(8) S encrypts its message M as $C = E_{sk}(M)$.
(9) S computes a message authentication code $V = h(sk, M)$, where $h(\cdot)$ is a secure one-way hash function [30,31].
(10) $S \rightarrow \mathcal{G}$: $\{C, V\}$.
S broadcasts C and V to the legitimate receivers $\mathcal{G}$.

4.1.3. Decryption phase

When the legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^{a}$ receive C and V from the sender S, then the following steps have to be performed to get the message M from $C = E_{sk}(M)$.

(1) $\mathcal{G}$ decrypt Z_i as $z = D_{K_i}(Z_i)$ by using his/her private key K_i and get the random integer z.
(2) $\mathcal{G}$ verifies whether $Y \stackrel{?}{=} h(z, f(B))$. If this holds, then $\mathcal{G}$ authenticates the CAS. Otherwise, $\mathcal{G}$ stops the decryption phase.
(3) $\mathcal{G}$ computes the common shared session key sk from its private key K_i, public key P_i, and the received public parameter $f(B)$ as follows:

$$\begin{aligned} sk &= K_i^{z(f(B)P_i)^d} \bmod N \\ &= K_i^{z(Bt_i^{-1}r_c)^{ed} \bmod \lambda(N)} \bmod N \\ &= K_i^{zBt_i^{-1}r_c} \bmod N \\ &= K_0^{zBr_c} \bmod N. \end{aligned} \tag{16}$$

(4) $\mathcal{G}$ decrypts C as $D_{sk}(C)$ and gets the message M.
(5) $\mathcal{G}$ verifies whether $V \stackrel{?}{=} h(sk, M)$. If this holds, then $\mathcal{G}$ accepts the message M. Otherwise, $\mathcal{G}$ rejects it.

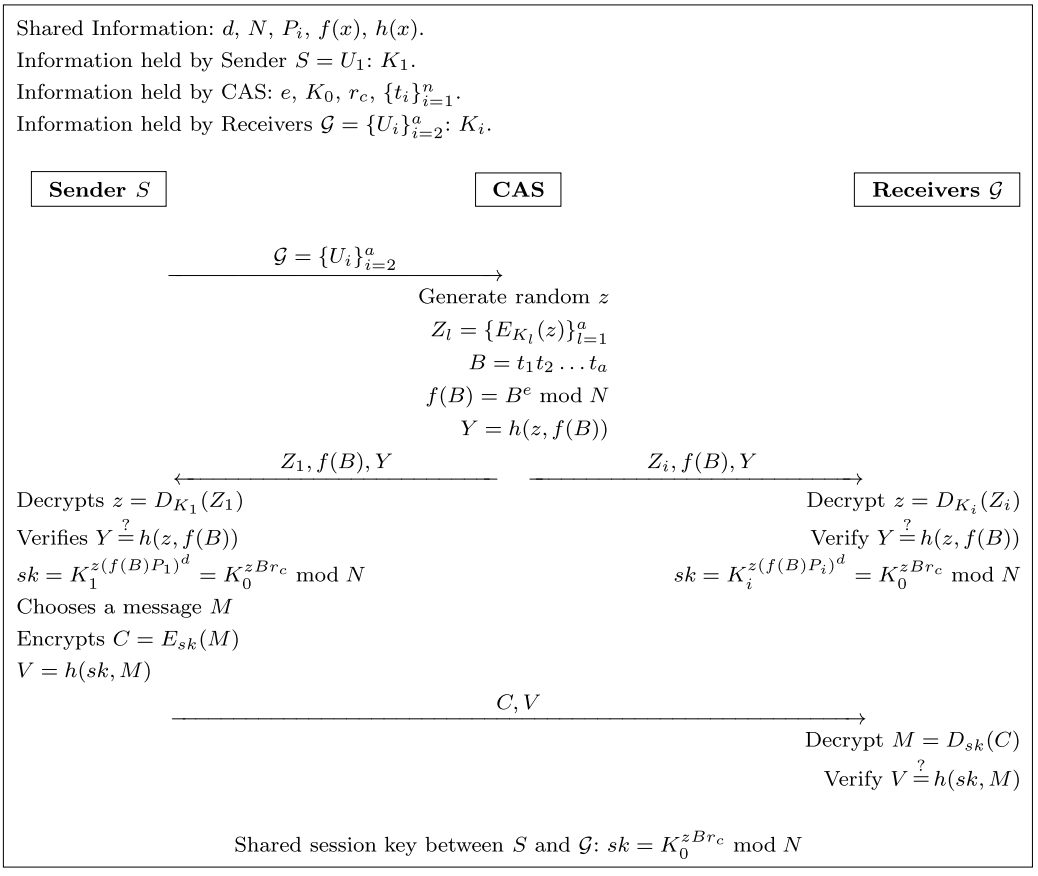

Fig. 3. The proposed authenticated broadcasting cryptosystem.

4.2. Application to grid computing environments

Grid computing is a computer network in which each computer's resources are shared with every other computer in the system. Processing power, memory and data storage are all community resources that authorized users can tap into and leverage for specific tasks. A grid computing system can be as simple as a collection of similar computers running on the same operating system or as complex as inter-networked systems comprised of every computer platform [2,32].

In most grid computing systems, only certain users are authorized to access the full capabilities of the network. Otherwise, the control node would be flooded with processing requests and nothing would happen due to deadlock. It is also important to limit access for security purposes. For that reason, most systems have authorization, authentication, key exchange, and secure broadcasting protocols [12]. These protocols limit network access to a select number of users. Other users are still able to access their own machines, but they cannot leverage the entire network [12,32].

Fig. 4 illustrates an application example of the proposed authenticated broadcasting cryptosystem. Assume that a user wants to access his/her company's grid network domain through his/her control server in order to perform some specific tasks. To securely coordinate the grid nodes' resources in the grid domain, the control server has to broadcast all task messages securely. In this scenario, the control server can perform the proposed authenticated broadcasting cryptosystem before he/she sends the task messages to the grid network domain. That is, after computing the common shared session key sk, the control server encrypts its task message TM as $C = E_{sk}(TM)$ and broadcasts it to the legitimate grid nodes. Then, the grid nodes can securely decrypt C as $D_{sk}(C)$ and get the task message TM.

5. Security analysis

This section provides the security analysis of the proposed authenticated broadcasting cryptosystem.

(1) Suppose that an attacker wants to derive the message M from C. The legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^a$ can derive the message M that came from the sender S by using the decryption phase proposed above. However, it is infeasible to derive the shared session secret key sk by only knowing the public keys of the sender S for any illegitimate receiver, because the security of our broadcasting cryptosystem is the same as the RSA public key cryptosystem, which is strongly believed to be computationally difficult to attack.

(2) Suppose that an attacker wants to find the shared session secret key sk. In this case, it is assumed that an illegitimate receiver is trying to evaluate the shared session secret key sk. Since an attacker does not have the private keys K_i, he/she cannot employ the decryption phase mentioned above.

(3) Suppose that an attacker wants to obtain the private keys K_i only known by user U_i. The attacker may come from legitimate receivers, since there is no information available to compute the private keys K_i. Hence, the proposed broadcasting cryptosystem can protect the security of K_i.

(4) Suppose that two legal users want to perform a conspiracy attack described in [23,24]. Two legal users U_x and U_y share their private keys $K_x = K_0^{t_x}$ and $K_y = K_0^{t_y}$, respectively. Since t_x and t_y are relatively prime, if two legal users can get t_x and t_y from $K_x = K_0^{t_x}$ and $K_y = K_0^{t_y}$, two numbers s and r can be obtained satisfying $rt_x + st_y = 1$ by the Euclidean algorithm. Then, the system secret key K_0 can be recovered by performing the following operation.

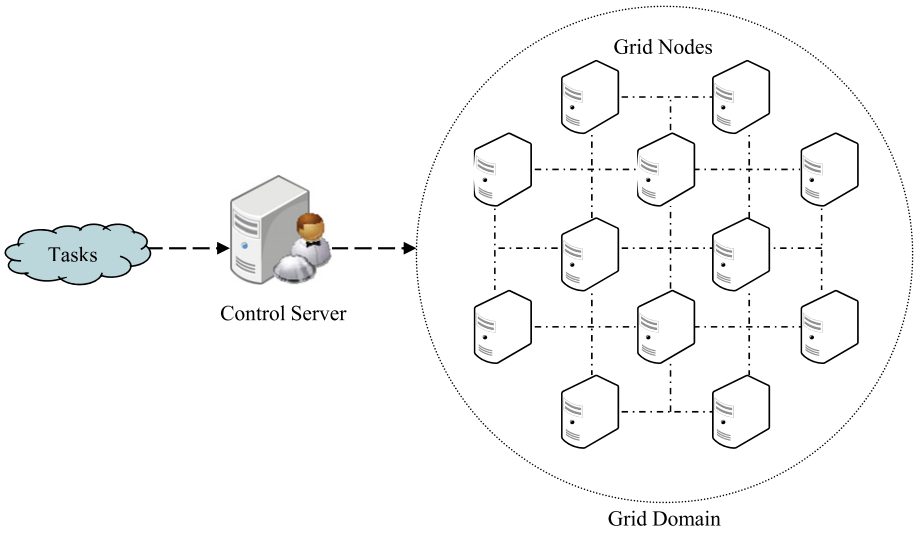

Fig. 4. General architecture of grid computing environment.

$$K_x^r K_y^s \bmod N = K_0^{t_x r} K_0^{t_y r} \bmod N = K_0^{t_x r + t_y r} \bmod N = K_0 \bmod N. \quad (17)$$

However, this conspiracy attack cannot be applied to the proposed broadcasting cryptosystem since the users do not know parameter t_i. To obtain t_i from $K_i = K_0^{t_i}$, he/she can solve the RSA factoring challenge problem. But it is computationally infeasible since modulus N is sufficiently large and t_i is always randomly generated in each session.

(5) Suppose that an attacker wants to find the RSA secret key e of CAS from $f(B) = B^e \bmod \lambda(N)$ and $P_i = (t_i^{-1} r_c)^e \bmod \lambda(N)$. In order to obtain e, a user should solve the equation $f(B) = B^e \bmod \lambda(N)$ and $P_i = (t_i^{-1} r_c)^e \bmod \lambda(N)$. However, it is computationally infeasible to get the private key e of CAS from $f(B)$ and P_i because of the RSA factoring challenge problem.

(6) Suppose that an attacker wants to perform the Zhu–Wu attack [29] to drive the shared session key sk. Unlike the redefined Liaw's broadcasting cryptosystem, in the proposed cryptosystem, the CAS generates a random number z and encrypts it with the private key K_i of both the sender S and the legitimate receivers $\mathcal{G} = \{U_i\}_{i=2}^{a}$, respectively. In addition, each receiver must decrypt $Z_i = E_{K_i}(z_i)$ by using its private key K_i to get the random number z_i and compute the shared session key $sk = K_0^{zBr_c} \bmod N$. Without knowing the random number z, the attacker cannot compute the shared session key sk. To get the random number z, the attacker must know the private key K_i of the legal users. Since K_i is never disclosed to the attacker, the attacker cannot compute the shared session key $sk = K_0^{zBr_c} \bmod N$. Therefore, the proposed broadcasting cryptosystem can resist the Zhu–Wu attack.

(7) The proposed broadcasting cryptosystem is secure to the integrity violence of the session key from illegal modification and the session key modification attack. The sender S and the legitimate receivers $\mathcal{G}$ always do verify the integrity of the decrypted message z and the received $f(B)$ by comparing whether $Y \stackrel{?}{=} h(z, f(B))$ in Step 6 of the broadcasting phase and Step 2 of the decryption phase, respectively. Without knowing the correct private key K_i, nobody can compute the correct value Z_i and $f(B)$. It means that the sender S and the legitimate receivers $\mathcal{G}$ can easily detect the received Z_i and $f(B)$ are modified by the attacker. Therefore, the proposed broadcasting cryptosystem is secure to the integrity violence of the session key from illegal modification and the session key modification attack.

(8) The proposed broadcasting cryptosystem is secure to the message modification attack. The legitimate receivers $\mathcal{G}$ always do verify the integrity of the decrypted message M by comparing whether $V \stackrel{?}{=} h(sk, M)$ in Step 5 of the decryption phase. Without knowing the correct session key $sk = K_0^{zBr_c} \bmod N$, nobody can get the correct message M by decrypting the received $C = E_{sk}(M)$. It means that the legitimate receivers $\mathcal{G}$ can easily detect the received Z_i, $f(B)$, C, and V are modified by the attacker. Therefore, the proposed broadcasting cryptosystem is secure to the message modification attack.

Table 1
Comparisons of computational costs and security.

Computation type	Masque–Peinado cryptosystem [24]			Our cryptosystem		
	Sender	CAS	Receiver	Sender	CAS	Receiver
Modular exponential operation	2	1	2	2	1	2
Symmetric encryption	1	0	0	1	a	0
Symmetric decryption	0	0	1	1	0	2
Hash operation	0	0	0	2	1	2
Zhu–Wu attack [29]		Insecure			Secure	
Integrity violence attack		Insecure			Secure	
Session key modification attack		Insecure			Secure	
Message modification attack		Insecure			Secure	

a: Number of users in a group $\mathcal{G} = \{U_i\}_{i=1}^{a}$.

6. Performance analysis

The performance comparison between Masque and Peinado's redefined Liaw's broadcasting cryptosystem [24] and our proposed broadcasting cryptosystem are shown in Table 1. In order to compare the computational workload, we considered the number of modular exponential operations, symmetric encryptions, symmetric decryptions, and hash operations in the broadcasting phase and the decrypting phase.

According to [33], the operation numbers per second performed in asymmetric encryptions/decryptions and modular exponential

operations, symmetric encryptions/decryptions, and hash function operations are 2, 2000, and 20,000, respectively. Since symmetric encryptions/decryptions and one-way hash function operations are much faster than the asymmetric encryptions/decryptions and modular exponential operations, the CAS that has powerful processors, a lot of memory and big storage subsystems can perform the computations efficiently. Particularly, we focus on the numbers of operations that both sender and each receiver need to perform because the user devices usually are not as powerful as the CAS system and thus are not suitable for computation intensive tasks. Compared with Masque–Peinado's cryptosystem, both the sender and each receiver must perform one extra symmetric decryption and two extra hash operations, respectively. However, these computations are required to provide strong security that can withstand the Zhu–Wu attack [29], integrity violence attack, session key modification attack, and message modification attack. Therefore, it can be seen that the proposed cryptosystem requires more computational costs than Masque–Peinado's cryptosystem to acquire better security.

7. Conclusions

The purpose of a broadcasting cryptosystem is to establish a secure communication channel from a sender to a group of legal receivers. This paper pointed out that the redefined Liaw's broadcasting cryptosystem is still insecure to the integrity violence of the session key from illegal modification, the session key modification attack and the message modification attack. In addition, this paper proposed a new authenticated broadcasting cryptosystem in order to overcome the weaknesses of the the redefined Liaw's broadcasting cryptosystem. Moreover, this paper also presented an application example to grid computing environments of the proposed cryptosystem. As a result, the proposed cryptosystem not only has the advantages of the redefined Liaw's broadcasting cryptosystem, but is also more secure and practical compared with previous related broadcasting cryptosystems.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Nos. 2010-0010106 and 2010-0011968) and partially supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2010.

References

[1] W. Chung, R. Chang, A new mechanism for resource monitoring in grid computing, Future Generation of Computer Systems 25 (1) (2009) 1–7.
[2] M. Smith, M. Schmidt, N. Fallenbeck, T. Dornemann, C. Schridde, B. Freisleben, Secure on-demand grid computing, Future Generation of Computer Systems 25 (3) (2009) 315–325.
[3] X. Zou, Y. Dai, X. Ran, Dual-level key management for secure grid communication in dynamic and hierarchical groups, Future Generation of Computer Systems 23 (6) (2007) 776–786.
[4] A. Joan, H. Jordi, JXTA resource access control by means of advertisement encryption, Future Generation of Computer Systems 26 (1) (2010) 21–28.
[5] D. Zou, W. Zheng, J. Long, H. Jin, X. Chen, Constructing trusted virtual execution environment in P2P grids, Future Generation of Computer Systems 26 (5) (2010) 769–775.
[6] F. Martinelli, P. Mori, On usage control for GRID systems, Future Generation of Computer Systems 26 (7) (2010) 1032–1042.
[7] J. Perez, J. Bernabe, J. Calero, F. Clemente, G. Perez, A. Skarmeta, Semantic-based authorization architecture for Grid, Future Generation of Computer Systems 27 (1) (2011) 40–55.
[8] X. Wang, J. Luo, M. Yang, Z. Ling, A potential HTTP-based application-level attack against Tor, Future Generation of Computer Systems 27 (1) (2011) 67–77.
[9] G. Vecchia, C. San, An optimized broadcasting technique for WK-recursive topologies, Future Generation of Computer Systems 5 (4) (1990) 353–357.
[10] I. Lin, M. Hwang, C. Chang, A new key assignment scheme for enforcing complicated access control policies in hierarchy, Future Generation of Computer Systems 19 (4) (2003) 457–462.
[11] J. Kwon, H. Yeom, Generalized data retrieval for pyramid-based periodic broadcasting of videos, Future Generation of Computer Systems 20 (1) (2004) 157–170.
[12] L. Liao, M. Manulis, Tree-based group key agreement framework for mobile ad-hoc networks, Future Generation of Computer Systems 23 (6) (2007) 787–803.
[13] Y. Na, I. Ko, S. Xu, A multilayered digital content distribution using a group-key based on web, Future Generation of Computer Systems 25 (3) (2009) 371–377.
[14] K. Huang, D. Zhang, DHT-based lightweight broadcast algorithms in large-scale computing infrastructures, Future Generation of Computer Systems 26 (3) (2010) 291–303.
[15] K. Wang, J. Li, L. Pan, Fast file dissemination in peer-to-peer networks with upstream bandwidth constraint, Future Generation of Computer Systems 26 (7) (2010) 986–1002.
[16] J. Barthes, OMAS—a flexible multi-agent environment for CSCWD, Future Generation of Computer Systems 27 (1) (2011) 78–87.
[17] Y. Liu, K. Li, Y. Jin, Y. Zhang, W. Qu, A novel reputation computation model based on subjective logic for mobile ad hoc networks, Future Generation Computer Systems (2010) doi:10.1016/j.future.2010.03.006.
[18] C. Chang, T. Wu, Broadcasting cryptosystem in computer networks using interpolating polynomials, Computer Systems Science and Engineering 6 (3) (1991) 185–188.
[19] G. Chiou, W. Chen, Secure broadcasting using the secure lock, IEEE Transactions on Software Engineering 15 (8) (1989) 929–934.
[20] W. Tzeng, M. Hwang, A conference key distribution scheme for multilevel security, in: Proceedings of the 4th National Conference Security, NCS 1995, pp. 47–52.
[21] H. Liaw, Broadcasting cryptosystem in computer networks, Computers & Mathematics with Applications 37 (1999) 85–87.
[22] H. Sun, Security of broadcasting cryptosystem in computer networks, Electronics Letters 35 (1999) 2108–2109.
[23] Y. Tseng, J. Jan, Cryptanalysis of Liaw's broadcasting cryptosystem, Computers & Mathematics with Applications 41 (2001) 1575–1578.
[24] J. Masque, A. Peinado, Cryptanalysis of improved Liaw's broadcasting cryptosystem, Journal of Information Science and Engineering 22 (2006) 391–399.
[25] E. Yoon, K. Yoo, Robust broadcasting cryptosystem in computer networks, in: Proceedings of the 2009 Workshops at the Grid and Pervasive Computing Conference, GPC 2009, pp. 153–159.
[26] W. Zhu, General weakness in certain broadcast encryption protocols employing the remainder approach, in: Proceedings of the 2008 IEEE International Conference on Communications, ICC 2008, pp. 1620–1624.
[27] M. Ramkumar, Broadcast authentication with preferred verifiers, International Journal of Network Security 4 (2) (2007) 166–178.
[28] M. Blaze, J. Ioannidis, A. Keromytis, T. Malkin, A. Rubin, Anonymity in wireless broadcast networks, International Journal of Network Security 8 (1) (2009) 37–51.
[29] W. Zhu, C. Wu, Security of the redefined Liaw's broadcasting cryptosystem, Computers & Mathematics with Applications 56 (2008) 1665–1667.
[30] B. Schneier, Applied Cryptography Protocols, Algorithms and Source Code in C: Second Edition, John Wiley & Sons Inc., 1995.
[31] A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.
[32] J. Strickland, How grid computing works, HowStuffWorks.com, 25 April 2008, http://communication.howstuffworks.com/grid-computing.htm.
[33] M. Steiner, G. Tsudik, M. Waidner, Refinement and extension of encrypted key exchange, ACM Operating Systems Review 29 (3) (1995) 22–30.

Eun-Jun Yoon received his M.Sc. degree in computer engineering from Kyungil University in 2002 and his Ph.D. degree in computer science from Kyungpook National University in 2006, South Korea. From 2007 to 2008, he was a full-time lecturer at the Faculty of Computer Information, Daegu Polytechnic College, South Korea. He is currently a 2nd BK21 contract professor at the School of Electrical Engineering and Computer Science, Kyungpook National University, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, mobile communications security, and steganography.

Kee-Young Yoo received his B.Sc. degree in education of mathematics from Kyungpook National University in 1976 and his M.Sc. degree in computer engineering from Korea Advanced Institute of Science and Technology in 1978, South Korea. He received his Ph.D. degree in computer science from Rensselaer Polytechnic Institute, New York, USA in 1992. Currently, he is a professor at the Department of Computer Engineering, Kyungpook National University, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, DRM security, and steganography. He has published over one hundred technical and scientific international papers on a variety of information security topics.