情報保護學會論文誌
第13券 第6號, 2003. 12

효율적인 Self-Healing 키 분배 기법

홍 도 원*†‡, 강 주 성*, 신 상 욱**

Efficient Self-Healing Key Distribution Scheme

Dowon Hong*†‡, Ju-Sung Kang*, Sang-Uk Shin**

요 약

Staddon 등에 의해 제안된 취소 능력을 가진 Self-healing 키 분배 기법은[1] 동적 그룹의 멤버들이 신뢰할 수 없는 채널 상에서 그룹 키를 설정할 수 있게 하며, 더욱이 그룹을 탈퇴하거나 가입하는 멤버들에 의한 공모 공격에 안전하다. 이 프로토콜에서 그룹 멤버는 몇 몇 패킷들을 잃어버린 경우에도 그룹 매니저에게 추가적인 전송을 요청하지 않고 이전에 받은 패킷들을 이용하여 여전히 그룹 키를 복구할 수 있다. 이 프로토콜에서 그룹 멤버의 저장량은 $O(m^2 \log p)$ 이고, 그룹 매니저에 의해 브로드캐스트되는 메시지 크기는 $O((mt^2+mt)\log p)$ 이다. 여기에서 m은 세션의 횟수이고, t는 공모할 수 있는 최대 그룹 멤버의 크기이고, p는 암호적 키로 사용할 수 있는 충분히 큰 소수이다. 본 논문에서는 $O(m \log p)$ 의 저장량과 $O((t^2+mt)\log p)$ 의 통신량으로 기존의 기법과 같은 목적을 달성할 수 있는 더욱 효율적인 취소 능력을 가진 Self-healing 키 분배 기법을 제안한다. 우리는 그룹 멤버와 매니저의 입장에서 추가적인 계산량의 증가없이 그룹 멤버의 저장량을 최적으로 줄이고 그룹 매니저에 의해 브로드캐스트되는 메시지 크기를 효율적으로 줄인다.

ABSTRACT

The self-healing key distribution scheme with revocation capability proposed by Staddon et al.[1] enables a dynamic group of users to establish a group key over an unreliable network, and has the ability to revoke users from and add users to the group while being resistant to collusion attacks. In such a protocol, if some packet gets lost, users are still capable of recovering the group key using the received packets without requesting additional transmission from the group manager. In this scheme, the storage overhead at each group member is $O(m^2 \log p)$ and the broadcast message size of a group manager is $O((mt^2+mt)\log p)$, where m is the number of sessions, t is the maximum number of colluding group members, and p is a prime number that is large enough to accommodate a cryptographic key. In this paper we describe the more efficient self-healing key distribution scheme with revocation capability, which achieves the same goal with $O(m \log p)$ storage overhead and $O((t^2+mt)\log p)$ communication overhead. We can reduce storage overhead at each group member and the broadcast message size of the group manager without adding additional computations at user's end and group manager's end.

keyword : *Self-healing key distribution, revocation capability*

Ⅰ. 서 론

안전한 그룹 통신에서 가장 중요한 분야 중 하나는 키 자원의 안전한 분배와 관련된 그룹 키 관리 분야이다. 그룹 키 관리 시스템은 그룹 멤버들 사이에 그룹 키라 불리는 공유 키 (또는 세션키)를 설정

* 한국전자통신연구원 정보보호연구본부({dwhong, jskang}@etri.re.kr)
** 부경대학교 전자컴퓨터정보통신공학부(shinsu@pknu.ac.kr)
† 주저자, ‡ 교신저자, 논문접수일 : 2003년 8월 20일, 심사완료일 : 2003년 11월 13일

하고 유지한다. 빈번한 멤버쉽의 변화가 있는 큰 그룹의 경우, 이 공유 키는 멤버쉽의 변화가 있을 때마다 갱신되어야 하며, 존재하는 그룹 멤버들에게 안전하게 재분배되어야 한다. 그룹 키를 갱신하는 가장 간단한 방법은 그룹 매니저가 각각의 그룹 멤버들과 공유하고 있는 비밀 키들을 이용하여 새로운 그룹 키를 각각 암호화하여 개별 멤버들에게 전송하는 것이다. 이 방법은 그룹 크기에 따라 갱신 비용이 선형적으로 증가하므로 확장성을 가지지 못한다.

최근에 많은 확장성을 가진 그룹 키 갱신 기법들이 제안되었다.[2~6] 또한 그룹 멤버쉽이 변경될 때마다 그룹 키가 갱신되는 대신에 주기적으로 갱신되는 방법도 제안되고 있다.[7~8] 더욱이 몇 몇 논문들은 멤버들이 취소 능력을 가진 경우를 다루고 있다.[9,5,6]

그러나 위의 모든 논문들은 네트워크가 신뢰되는 경우를 가정하고 있다. 신뢰되지 않는 네트워크에서의 키 분배 기법은 아직 깊이 있게 연구되지는 않았다. [10]과 [11]의 저자들은 상호 작용하지 않는 방법으로 패킷 분실에 대처할 수 있는 방법을 제안하였다. [10]에서는 오류 정정(error-correcting) 기법이 사용되었고, [11]에서는 패킷에 짧은 힌트 메시지를 부가하였다.

최근에 신뢰되지 않는 네트워크 상에서의 주기적인 키 갱신 기법으로 주목할 만한 결과가 발표되었다. Staddon 등에 의해 제안된 취소 능력을 가진 Self-healing 키 분배 기법은[1] 동적 그룹의 멤버들이 신뢰할 수 없는 채널 상에서 그룹 키를 설정할 수 있게 하며, 더욱이 그룹을 탈퇴하거나 가입하는 멤버들에 의한 공모 공격에 안전하다. 이 프로토콜에서 각각의 그룹 멤버들에게 세션키를 분배하기 위하여 그룹 매니저는 채널을 통해 패킷들을 브로드캐스트한다. 몇 몇 패킷이 분실되더라도 그룹 멤버는 그룹 매니저에게 추가적인 전송을 요청하지 않고 이전에 받은 패킷들을 이용하여 잃어버린 그룹 키를 복원할 수 있게 한다. "self-healing" 과정을 통하여 잃어버린 키를 복구하기 위해서는 사용자가 잃어버린 특정 키가 보내어진 세션의 전, 후에 그룹의 멤버여야 한다는 요구조건만 필요하다. Self-healing 키 복구 기법의 장점은 네트워크 트래픽과 그룹 매니저의 계산량을 감소시키며, 트래픽 분석을 통한 사용자 노출 위험을 줄인다.

본 논문에서는 Staddon 등에 의해 제안된 취소 능력을 가진 Self-healing 키 분배 기법을 개선하였다. 브로드캐스트되는 메시지를 분석하여 masking 다항식의 수를 감소시켜, 그룹 멤버의 저장량을 $m^2 \log p$ 에서 $m \log p$ 로 최적으로 줄이고 또한 그룹 매니저에 의해 브로드캐스트되는 메시지 크기를 $O((mt^2+mt)\log p)$ 에서 $O((t^2+mt)\log p)$ 로 줄이는 효율적이고 안전한 취소 능력을 가진 Self-healing 키 분배 기법을 제안한다. 여기에서 m은 세션의 회수이고, t는 공모할 수 있는 최대 그룹 멤버의 크기이고, p는 암호적 키로 사용할 수 있는 충분히 큰 소수이다. 우리의 모든 결과는 그룹 멤버와 매니저의 입장에서 추가적인 계산량 증가없이 얻어진다.

본 논문은 다음과 같이 이루어진다. 2절에서는 제안되는 통신 모델에서 사용되는 기호와 개념들을 정의한다. 3절에서는 [1]에서 제안된 기본적인 기법을 기술하고, 향상된 새로운 기법을 제안하고 안전성 증명을 제공한다. 4절은 결론이다.

II. 모 델

본 논문에서 우리가 고려하는 모델은 [1]에서 제안된 모델과 비슷하다. 네트워크에서 통신 개체들은 브로드캐스트되는 메시지에 대한 접근을 통제하기 위해 그룹들을 형성한다고 가정한다. 네트워크의 주기는 세션이라 불리는 시간 구간으로 분할된다.

그룹 매니저는 합법적인 많은 그룹 멤버들에게 세션키(또는 그룹 키)를 분배할 책임이 있다. 세션키를 분배할 때, 세 번의 세션(연속적일 필요는 없음) 사이에 있는 멤버가 첫 번째와 세 번째 브로드캐스트 메시지를 이용하여 중간 세션에 대응하는 세션키를 복구할 수 있으면, 키 분배 기법이 self-healing 성질을 가지고 있다고 한다. 또한, t명의 그룹에서 탈퇴한 멤버가 공모하여도 새로운 세션키를 알아내지 못하면 키 분배 기법이 t-revocation 성질을 가지고 있다고 한다.

한 명의 그룹 매니저와 n명의 사용자 $U_1, \cdots, U_n$가 있는 설정을 고려하자. 모든 계산은 유한체 F_p에서 행해진다. 여기에서 p는 암호적 키로 사용할 수 있는 충분히 큰 소수이다. 각 사용자 U_i는 그룹 멤버가 세션키를 복구하는 데에 사용할 수 있는 모든 정보를 나타내는 개인 키 $S_i \subseteq F_p$를 저장한다. $H(\cdot)$는 정보 이론의 엔트로피 함수를 나타낸다.[12] Self-healing 키 분배 기법의 정의를 기술하는데 필요한 엔트로피 함수의 기본 성질들은 [1]을 참조하라.

세션들의 횟수를 m이라 하고, j번째 세션에서 그룹 멤버가 아닌 사용자들의 집합을 R_j라 하자. 만약

$U_i \notin R_j$ 이면, U_i는 세션 j에서 그룹 멤버 (또는 활동적인 사용자)이다. 세션키 K_j ($j=1,\cdots,m$)는 그룹 매니저로부터 브로드캐스트되는 메시지 B_j를 통해 그룹 멤버들에게 전송된다. 임의의 그룹 멤버 U_i는 j번째 세션키 K_j를 브로드캐스트되는 메시지 B_j와 개인 키 S_i에 의해 결정한다. $Z_{i,j}$를 사용자 U_i가 B_j와 S_i로부터 얻는 모든 정보라고 하자. S_i, B_j, K_j, $Z_{i,j}$를 위의 요소들과 관련된 랜덤 변수들이라 하자.

제안하는 기법을 분명하게 하기 위해 다음의 정의가 필요하다.

[정의 1]

Revocation 성질을 가진 self-healing 세션키 분배 기법[1]

$t, i \in \{1,\cdots,n\}$, $j \in \{1,\cdots,m\}$ 라 하자.

1. 다음을 만족하면 Λ를 세션키 분배 기법이라 한다.

(a) 임의의 멤버 U_i에 대해, 키 K_j는 B_j와 S_i로부터 얻어지는 $Z_{i,j}$로부터 결정된다. 즉, 다음이 성립한다.

$H(K_j | Z_{i,j}) = 0$, $H(Z_{i,j} | B_j, S_i) = 0$.

(b) 임의의 부분집합 $C \subseteq \{U_1,\cdots,U_n\}$ s.t. $|C| \le t$, $U_i \notin C$에 대해, C에 있는 사용자들은 S_i에 관한 어떤 정보도 알 수 없다. 즉, 다음이 성립한다.

$H(S_i | \{S_{i'}\}_{U_{i'} \in C}, B_1, \cdots, B_m) = H(S_i)$.

(c) 멤버들 $U_1,\cdots,U_n$이 브로드캐스트되는 메시지 B_j를 통해 알 수 있는 것을 브로드캐스트되는 메시지들이나 개인 키들 만으로는 결정할 수 없다. 즉, 다음이 성립한다.

$H(Z_{i,j} | B_1, \cdots, B_m) = H(Z_{i,j} | S_1, \cdots, S_n)$
$= H(Z_{i,j})$.

2. 다음을 만족하면 Λ는 t-revocation 성질을 가지고 있다고 정의한다. 만약 주어진 임의의 집합 $R \subseteq \{U_1,\cdots,U_n\}$ ($|R| \le t$)에 대해, 그룹 매니저가 모든 $U_i \notin R$인 U_i는 세션키 K_j ($j=1,\cdots,m$)를 복구 할 수 있지만 모든 탈퇴한 사용자는 복구할 수 없는 B_j를 브로드캐스트할 수 있다. 즉, 다음이 성립한다.

$H(K_j | B_j, S_i) = 0$,

$H(K_j | B_j, \{S_{i'}\}_{U_{i'} \in R}) = H(K_j)$.

3. 임의의 $1 \le j_1 < j < j_2 \le m$에 대하여 다음을 만족하면 Λ는 self-healing 성질을 가지고 있다고 정의한다.

(a) 세션 j_1과 j_2에서 그룹 멤버인 임의의 U_i에 대해, 키 K_j는 $\{Z_{i,j_1}, Z_{i,j_2}\}$에 의해 결정된다. 즉, 다음이 성립한다.

$H(K_j | Z_{i,j_1}, Z_{i,j_2}) = 0$.

(b) 임의의 부분집합 $C, D \subset \{U_1,\cdots,U_n\}$ ($C \cap D = \emptyset$, $|C \cup D| \le t$)에 대해, 집합 $\{Z_{i,k}\}_{U_i \in C, 1 \le k \le j_1} \cup \{Z_{i,k}\}_{U_i \in D, j_2 \le k \le m}$는 K_j에 대한 어떤 정보도 가지지 않는다. 즉 다음이 성립한다.

$H(K_j | \{Z_{i,k}\}_{U_i \in C, 1 \le k \le j_1} \cup \{Z_{i,k}\}_{U_i \in D, j_2 \le k \le m})$
$= H(K_j)$.

정의의 첫 번째 부분은 세션키 분배 기법에서 반드시 만족해야하는 조건을 서술한다. 두 번째와 세 번째는 t-revocation 성질과 self-healing 성질을 정의한다.

Ⅲ. 취소 능력을 가진 향상된 Self-Healing 키 분배 기법

[1]에서 제안된 self-healing 키 분배 기법에서 기본적인 방법은 secret sharing[13] 기법을 사용하여 패킷 분실로부터 복구할 수 있는 사용자의 능력을 유지한다. 각각의 브로드캐스트되는 메시지로부터 멤버들은 현재의 세션키와 이전과 이후 세션키들을 구할 수 있는 share들을 복구한다. 이 기법에서 공모 공격에 대한 안전성을 제공하기 위하여, 다른 사용자에 의해 복구되는 share들은 서로 다르다. Share들의 값들을 결정하기 위해 충분히 높은 차수의 여러 개의 독립인 masking 다항식을 이용하여, 공모 공격에 저항할 수 있는 요구되는 수준을 달성한다.

본 논문에서 제안된 기법의 효율성 향상은 본질적으로 masking 다항식의 효율적인 선택에 기인한다. 본 논문에서 우리는 그룹 매니저가 세션마다 한 개의 랜덤한 난수를 이용하면 필요한 masking 다항식의 수를 충분히 줄일 수 있음을 보일 것이다. 따라서 masking 다항식의 수가 줄면 각 그룹 멤버의 저장량과 그룹 매니저의 통신량을 줄일 수 있다.

3.1 취소 능력을 가진 Self-Healing 키 분배 기법

여기서는 제안된 기법을 이해하기 위해 필요한 [1]에서 제안된 t-revocation 능력을 가진 self-healing

키 분배 기법을 기술한다.

[1]의 Construction 3 t-revocation 능력을 가진 self-healing 키 분배 기법

1. 설정: t는 양의 정수, $N \in F_p$ 은 사용자 인덱스와 일치하지 않는 수라 하자. 그룹 매니저는 차수 t인 m개의 랜덤한 다항식 $f_1(x), \cdots, f_m(x) \in F_p[x]$ 과 m개의 랜덤한 키들 $K_1, \cdots, K_m \in F_p$ 을 선택하고, 각 $j=1, \cdots, m$ 에 대하여 다항식 $g_j(x) = K_j - f_j(x)$ 를 정의한다. 또한, 그룹 매니저는 $F_p[x, y]$ 에 속하는 m^2개의 다항식들 $\{h_{i,j}(x, y)\}_{i=1,\cdots,m, j=1,\cdots,m}$, $h_{i,j}(x, y) = a_{0,0}^{i,j} + a_{1,0}^{i,j}x + a_{0,1}^{i,j}y + \cdots + a_{t,t}^{i,j}x^t y^t$ 을 랜덤하게 선택한다. $v \in \{1, \cdots, n\}$ 에 대해, 사용자 U_v는 안전한 통신 채널을 통해 그룹 매니저로부터 개인 키 $S_v = \{h_{i,j}(v, v)\}_{i=1,\cdots,m, j=1,\cdots,m}$ 를 얻는다.

2. 브로드캐스트: A_j, $R_j \subseteq \{U_1, \cdots, U_n\}$, $|R_j| \le t$ 를 각각 세션 j에서 활동적인 사용자와 취소된 사용자들의 집합이라 하자. 그룹 매니저는 다음 성질을 만족하는 부분 집합 $W_j = \{w_1^j, w_2^j, \cdots, w_t^j\} \subseteq F_p$ 를 선택한다. 여기에서, R_j에 있는 사용자들의 인덱스는 모두 W_j에 포함되고, A_j에 있는 사용자들의 어떤 인덱스도 W_j에 포함되지 않는다. 그리고 $N \notin W_j$ 이다. 그룹 매니저는 $B_j = B_j^1 \cup B_j^2$ 를 브로드캐스트한다. 여기에서

$$B_j^1 = \{f_1(x) + h_{1,j}(N, x), \cdots, f_{j-1}(x) + h_{j-1,j}(N, x), K_j + h_{j,j}(N, x), g_{j+1}(x) + h_{j+1,j}(N, x), \cdots, g_m(x) + h_{m,j}(N, x)\}$$

이고 $B_j^2 = \{w_l^j, \{h_{i,j}(w_l^j, x)\}_{i=1,\cdots,m}\}_{l=1,\cdots,t}$ 이다.

3. 세션키와 share들 복구: j번째 세션에 있는 취소하지 않은 그룹 멤버 U_v에 대해, U_v는 다항식 $\{\{h_{i,j}(w_l^j, x)\}_{i=1,\cdots,m}\}_{l=1,\cdots,t}$ 를 $x=v$에서 계산한 값 $\{\{h_{i,j}(w_l^j, v)\}_{i=1,\cdots,m}\}_{l=1,\cdots,t}$ 와 개인 키 $\{h_{i,j}(v, v)\}_{i=1,\cdots,m, j=1,\cdots,m}$ 를 이용하여 다항식 $\{h_{i,j}(x, v)\}_{i=1,\cdots,m}$ 를 구할 수 있다. 그러면 $x=N$ 을 $\{h_{i,j}(x, v)\}_{i=1,\cdots,m}$ 에 대입하여 세션키 K_j와 share들 $\{f_i(v)\}_{i=1,\cdots,j-1}$ 와 $\{g_i(v)\}_{i=j+1,\cdots,m}$ 를 복구할 수 있다.

4. 그룹 멤버 추가: 그룹 매니저가 세션 j' 부터 새로운 멤버를 추가하기 원하면, 새로운 멤버에게 이전에 사용한 적이 없는 유일한 인덱스 $v' \in F_p$ 를 할당하고 현재와 미래의 세션키를 구할 수 있는 개인 키 $\{h_{i,j}(v', v')\}_{i=j',\cdots,m, j=j',\cdots,m}$ 을 계산하여 안전한 통신 채널을 통해 제공한다.

위의 Construction 3에서 그룹 멤버들의 저장량은 $m^2 \log p$ 이고 그룹 매니저가 브로드캐스트하는 메시지 크기는 $O((mt^2 + mt)\log p)$ (엄밀하게 $(mt^2 + 2mt + m + t)\log p$)이다. 새로운 세션키를 생성하기 위해 사용자가 저장해야 하는 개인키의 크기와 그룹매니저가 세션마다 브로드캐스트하는 메시지의 크기는 다음과 같은 하한을 가진다. 다음 보조정리들은 [1]에서 얻어진 결과들이다.

[보조정리 1] 무조건적으로 안전한 임의의 self-healing 키 분배 기법에서 임의의 사용자 U_v, $v \in 1, \cdots, n$에 대해 다음이 성립한다.

$$H(U_v) \ge m \log p .$$

보조정리 1의 부등식에 의하면 모든 사용자는 적어도 $m\log p$ 비트의 개인키를 저장해야만 한다.

[보조정리 2] 무조건적으로 안전한 (취소 능력을 가지지 않은) self-healing 키 분배 기법에서 브로드캐스트되는 메시지 B_j ($j \in 1, \cdots, m$)에 대해 다음이 성립한다.

$$H(B_j) = \Omega(mt)\log p .$$

보조정리 2의 결과와 취소 능력을 같이 고려하면 취소능력을 가진 self-healing 키 분배 기법에서 브로드캐스트되는 메시지 B_j, $j \in 1, \cdots, m$ 크기의 하한은 다음을 만족한다:

$$|B_j| \ge \max\{t^2 \log p,\ mt \log p\} .$$

이런 관점에서 [1]의 construction 3은 그룹멤버의 저장량과 그룹 매니저의 통신량 측면에서 향상될 여지가 있다.

3.2 취소 능력을 가진 향상된 Self-Healing 키 분배 기법

이 절에서는 [1]의 Construction 3 보다 향상된 기법을 제안한다. 다음과 같은 사실을 주목하라.

Construction 3에서 브로드캐스트되는 메시지를 주의 깊게 관찰하면, 이전에 구해진 share들을 통해 유용한 masking 다항식을 복구할 수 없도록 다항식 $\{f_i(x)\}_{i=1,\cdots,j-1}$와 $\{g_i(x)\}_{i=j+1,\cdots,m}$는 각각 서로 다른 masking 다항식 $\{h_{i,j}(N,x)\}_{i=1,\cdots,j-1}$와 $\{h_{i,j}(N,x)\}_{i=j+1,\cdots,m}$에 의해 숨겨진다. 그리고 세션키는 다항식 $\{h_{j,j}(N,x)\}$로 masking된다. 하지만 이런 효과를 얻기 위해 각 세션마다 m개의 독립인 masking 다항식을 이용하는 것은 브로드캐스트 메시지의 전송량과 해당 세션에서 share들을 구하기 위해 그룹 멤버가 저장해야 하는 개인키의 저장량을 크게 만든다.

각 세션마다 정당한 그룹 멤버만 구할 수 있는 랜덤한 한 개의 난수를 그룹 매니저가 선택하면, 한 개의 masking 다항식에서 얻어지는 여러 개의 종속인 masking 다항식들을 사용하여 충분히 세션키와 share들을 보호할 수 있는 기법을 제안한다. 제안되는 기법에서는 세션 j에서 세션키 K_j를 보호하기 위해 한 개의 masking 다항식 $h_{j,j}(x,y)$가 일단 사용되면, 그룹 매니저는 같은 세션에서 다항식 $\{f_1(x),\cdots, f_{j-1}(x), g_{j+1}(x),\cdots,g_m(x)\}$를 보호하기 위해 구해진 masking 다항식을 재사용할 수 있다. 단지 이전에 구해진 다항식들의 share 값들을 이용할 수 없도록 추가적인 값(임의의 난수)이 한 개 필요할 뿐이다.

제안된 기법에서는 다음과 같이 다항식들이 브로드캐스트된다: $\{r_j(f_1(x)+h_{j,j}(N,x)),\cdots,r_j(f_{j-1}(x)$
$+h_{j,j}(N+j-2,x)),K_j+h_{j,j}(N+j-1,x)$,
$r_j(g_{j+1}(x)+h_{j,j}(N+j,x)),\cdots,r_j(g_m(x)+$
$h_{j,j}(N+m-1,x)),r_j+h_{j,j}(N+m,x)\}$.

여기에서 r_j는 그룹 매니저에 의해 랜덤하게 선택된 난수이다. 비록 $h_{j,j}(N+k_1,x)$와 $h_{j,j}(N+k_2,x)$ $(0\le k_1<k_2\le m-1)$가 종속일 수도 있지만, $r_j(f_{k_1+1}(x)$ $+h_{j,j}(N+k_1,x))$와 $r_j(g_{k_2+1}(x)+h_{j,j}(N+k_2,x))$는 항상 독립이다. 그룹 멤버의 인덱스 $i\in\{1,\cdots,n\}$에 대한 $h_{j,j}(N+k_1,i)$와 $h_{j,j}(N+k_2,i)$의 값들을 모른다면(두 값이 종속일 수도 있다), 취소된 사용자는 r_j의 값과 $f_{k_1+1}(i)$와 $g_{k_2+1}(i)$의 관계를 알 수 없다. 따라서 모든 취소된 사용자들은 임의의 그룹 멤버 U_v에 대해 다항식 $\{h_{j,j}(x,v)\}$에서 기껏해야 t개의 다른 점들만 얻을 수 있으며, 취소된 세션의 세션키에 대한 어떤 정보도 구할 수 없다.

위에서 기술한 것에 기반하여 효율적인 self-healing 세션키 분배 기법을 제안한다. 제안된 기법은 그룹 매니저의 통신 오버헤드를 Construction 3의 $O((mt^2+mt)\log p)$에서 $O((t^2+mt)\log p)$으로 향상시키고 각 그룹 멤버의 저장량을 $m^2\log p$에서 $m\log p$로 최적으로 줄인다.

[제안 기법] t-revocation 능력을 가진 개선된 self-healing 키 분배 기법

1. 설정: t와 m은 양의 정수이고, N은 사용자 인덱스와 일치하지 않는 수로 $N+m\in F_p$이다. 그룹 매니저는 랜덤한 m개의 차수 t인 다항식 $f_1(x),\cdots,f_m(x)\in F_p[x]$과 m개의 랜덤한 세션키들 $K_1,\cdots,K_m\in F_p$을 선택하고, 각 $j=1,\cdots,m$에 대하여 다항식 $g_j(x)=K_j-f_j(x)$를 정의한다. 또한, 그룹 매니저는 $F_p[x,y]$에 속하는 m개의 다항식 $\{h_i(x,y)\}_{i=1,\cdots,m}$, $h_i(x,y)=a^i_{0,0}+a^i_{1,0}x+a^i_{0,1}y+\cdots+a^i_{t,t}x^ty^t$를 랜덤하게 선택한다. 각 $v\in\{1,\cdots,n\}$에 대해, 사용자 U_v는 안전한 통신 채널을 통해 그룹 매니저로부터 개인키 $S_v=\{h_i(v,v)\}_{i=1,\cdots,m}$를 얻는다.

2. 브로드캐스트: A_j, $R_j\subseteq\{U_1,\cdots,U_n\}$, $|R_j|\le t$를 각각 세션 j에서 활동적인 사용자와 취소된 사용자들의 집합이라 하자. 그룹 매니저는 다음 성질을 만족하는 부분 집합 $W_j=\{w^j_1,w^j_2,\cdots,w^j_t\}\subseteq F_p$를 선택한다. R_j에 포함되는 모든 사용자들의 인덱스는 W_j에 포함되고, A_j에 포함되는 사용자들의 어떤 인덱스도 W_j에 포함되지 않는다. 그리고 $N\notin W_j$이다. 그룹 매니저는 각 세션마다 랜덤한 수 $r_j\in F_p$를 선택하여 계산한 메시지 $B_j=B^1_j\cup B^2_j$를 브로드캐스트한다. 여기에서

$$B^1_j=\{r_j(f_i(x)+h_j(N+i-1,x))\}_{i=1,\cdots,j-1}\cup\{K_j+h_j(N+j-1,x)\}\cup\{r_j(g_i(x)+h_j(N+i-1,x))\}_{i=j+1,\cdots,m}\cup\{r_j+h_j(N+m,x)\},$$

$$B^2_j=\{w^j_1,\cdots,w^j_t,h_j(w^j_1,x),\cdots h_j(w^j_t,x)\}.$$

3. 세션키와 share들 복구: j번 째 세션에서 취소되지 않은 사용자 U_v가 j번 째 세션키 분배 메시지를 수신하면, U_v는 다항식 $\{h_j(w^j_i,x)\}_{i=1,\cdots,t}$를 $x=v$에서 계산한 값 $\{h_j(w^j_i,v)\}_{i=1,\cdots,t}$과 개인 키 $h_j(v,v)$를 이용하여 다항식 $h_j(x,v)$를 구할 수 있다. 그러면 U_v는 $x=N+m$을 $h_j(x,v)$에 대입하여 난수

r_j를 계산하고, $x=N,\cdots,N+m-1$을 $h_j(x,v)$에 대입하여 세션키 K_j와 share들 $\{f_i(v)\}_{i=1,\cdots,j-1}$, $\{g_i(v)\}_{i=j+1,\cdots,m}$를 복구할 수 있다.

4. 그룹 멤버 추가: 그룹 매니저가 세션 j'부터 새로운 멤버를 추가하기를 원하면, 새로운 멤버에게 이전에 사용되지 않은 유일한 인덱스 $v'\in F_p$를 할당하고, 현재와 미래의 세션에 대응하는 개인키 $\{h_i(v',v')\}_{i=j',\cdots,m}$을 계산하여 안전한 통신 채널을 통해 제공한다.

[1]의 Construction 3에서 실제로 필요로 하는 각 세션 j의 masking 다항식은 $\{h_{i,j}(N,y)\}_{i=1,\cdots,m}$이다. 여기서 N은 고정된 상수이다. 따라서 필요로 하는 정보를 세 변수 i,j,y의 함수로 생각할 수 있다. 제안된 기법에서도 세 변수의 함수인 $h_j(x,y)$를 필요로 한다. 그러므로 브로드캐스트 메시지 B_j의 첫 번째 부분 B_j^1에서 통신 오버헤드는 거의 동일하다. 그렇지만 B_j의 두 번째 부분 B_j^2에서 통신 오버헤드는 한 개의 masking 다항식만을 필요로 하기 때문에 $(mt^2+m+t)\log p$에서 $(t^2+2t)\log p$로 줄어든다. 따라서 전체적으로 그룹 매니저의 통신 오버헤드는 $O((mt^2+mt)\log p)$에서 $O((t^2+mt)\log p)$로 개선된다. 더욱이, 전체 세션을 통해 $F_p[x,y]$에 속하는 m개의 다항식만을 필요로 하기 때문에 그룹 멤버가 저장해야 하는 개인키의 저장량이 $m^2\log p$에서 $m\log p$로 현저하게 줄어든다. 보조정리 1에 의하면 이 값은 그룹 멤버가 적어도 저장해야 하는 최소한의 크기이다.

제안된 기법은 Construction 3보다 적은 브로드캐스트 크기와 저장량을 요구하면서도, 여전히 좋은 보안 성질들을 유지한다.

[정리 1] 제안된 기법은 t-revocation 능력을 가진 무조건적으로 안전한 self-healing 세션키 분배 기법이다.

(*증명*) 제안된 기법이 정의 1에 열거한 모든 조건들을 만족한다는 것을 증명할 필요가 있다.

1. (a) 그룹 멤버 U_v의 세션키 복구는 제안된 기법의 단계 3에 기술되었다. 따라서
$H(\boldsymbol{K}_j|\boldsymbol{B}_j,\boldsymbol{S}_v)=H(\boldsymbol{K}_j|\boldsymbol{Z}_{v,j})=0$ 이다.
(b) 임의의 부분 집합 $C\in\{U_1,\cdots,U_n\}$, $|C|\le t$와 그룹 멤버 $U_v\notin C$에 대해 C의 사용자들의 공모가 임의의 $j\in\{1,\cdots,m\}$에 대해 $h_j(v,v)$를 결정할 수 없다는 것을 보일 것이다. W를 C에 속한 사용자 인덱스의 집합이라고 하자. C에 속하는 사용자들의 공모는 $x=i'\in W(v\notin W)$에 대한 다항식 $h_j(x,v)$에서 기껏해야 t개의 점들을 안다. 따라서 각 다항식의 차수가 t이면, $h_j(v,v)$는 C에 속한 사용자들에게 F_p에서 랜덤하게 분포된 값들로 보인다. $h_j(\cdot,\cdot)$에 관한 어떤 정보도 다른 브로드캐스트 메시지에 포함되지 않기 때문에, 다음이 성립한다. $H(h_j(v,v)|\{\boldsymbol{S}_i\}_{U_i\in C},\boldsymbol{B}_1,\cdots,\boldsymbol{B}_m)=H(h_j(v,v))$.
(c) $\{f_i(x)\}_{i=1,\cdots,m}$, $\{h_i(x,y)\}_{i=1,\cdots,m}$, $\{r_i\}_{i=1,\cdots,m}$들은 그룹 매니저에 의해 랜덤하게 선택되었음으로, $\boldsymbol{Z}_{i,j}=\{f_1(i),\cdots,f_{j-1}(i),K_j,g_{j+1}(i),\cdots,g_m(i),r_j\}$가 브로드캐스트 메시지들이나 개인키들 단독으로는 결정될 수 없다. 즉, 다음이 성립한다.
$H(\boldsymbol{Z}_{i,j}|\boldsymbol{B}_1,\cdots,\boldsymbol{B}_m)=H(\boldsymbol{Z}_{i,j})$
$=H(\boldsymbol{Z}_{i,j}|\boldsymbol{S}_1,\cdots,\boldsymbol{S}_n)$.

2. t명의 취소된 사용자들의 집합 R에 속한 사용자들이 공모한다고 가정하자. R에 속하는 사용자들의 공모는 $\{h_j(i',x):U_{i'}\in R\}\cup\{h_1(i',i'),\cdots,h_m(i',i')\}_{U_{i'}\in R}$을 안다. 취소된 사용자들에게 $h_j(N+m,i)$는 F_p에서 랜덤하게 분포된 것으로 보이므로, 난수 r_j에 관한 어떤 정보도 알 수 없다. 그러므로 취소된 사용자들에게 $\{h_j(N+j-1,i)\}_{j=1,\cdots,m}$ 점들은 각각 F_p에서 랜덤하게 분포된 것으로 보인다. 따라서 $i=1,\cdots,n$에 대해 취소된 사용자들은 다항식 $\{h_j(x,i)\}$에 관해 기껏해야 t개의 점만을 알 수 있다. 모든 $j=1,\cdots,m$과 모든 i에 대해 취소된 사용자들은 $h_j(N+j-1,i)$에 관한 어떤 정보도 알지 못함으로, $h_j(N+j-1,x)$에 관한 어떤 정보도 알 수 없고, 결과적으로 K_j에 관한 정보를 가지지 못한다. 따라서 다음이 성립한다.
$H(\boldsymbol{K}_j|\boldsymbol{B}_j,\{\boldsymbol{S}_{i'}\}_{U_{i'}\in R})=H(\boldsymbol{K}_j)$.

3. (a) 제안된 기법의 단계 3에서, 세션 j_1과 j_2 $(1\le j_1<j<j_2\le m)$에서 멤버인 임의의 U_i에 대해 U_i는 $\{f_1(i),\cdots,f_{j_1-1}(i),g_{j_1+1}(i),\cdots,g_j(i),\cdots,g_m(i)\}$와 $\{f_1(i),\cdots,f_j(i),\cdots,f_{j_2-1}(i),g_{j_2+1}(i),\cdots,g_m(i)\}$를 복구할 수 있다. 따라서 $K_j=g_j(i)+f_j(i)$는 Z_{i,j_1}과 Z_{i,j_2}로부터 재구성될 수 있다.
(b) 임의의 disjoint 부분집합 $C,D\subset\{U_1,\cdots,U_n\}$ $(C\cap D=\emptyset,\ |C\cup D|\le t)$와 $1\le j_1<j<j_2\le m$에 대해 $\{Z_{i',k}\}_{U_{i'}\in C,1\le k\le j_1}$과 $\{Z_{i',k}\}_{U_{i'}\in D,j_2\le k\le m}$을 고려하자. K_j를 복구하기 위해 $C\cup D$는 어떤 i에

대해 $f_j(i)$와 $g_j(i)$ 모두를 복구하거나 또는 $h_j(N+j-1,i)$를 복구해야 한다. D에서 사용자들은 세션 j_1에서 취소되었고 C에서 사용자들은 세션 j_2에서 취소되었기 때문에 $C \cup D$는 $\{g_j(i')\}_{U_{i'} \in C}$와 $\{f_j(i')\}_{U_{i'} \in D}$만을 복구할 수 있다. 위의 증명 2에서 설명한대로 취소된 사용자들은 그룹 매니저가 선택한 난수 r_j와 $\{h_j(N+j-1,i)\}_{j=1,\cdots,m}$점들에 대한 어떤 정보도 알지 못한다. 따라서 모든 취소된 멤버들은 $\{r_j(f_i(x)+h_j(N+i-1,x))\}_{i=1,\cdots,j-1}$과 $\{r_j(g_i(x)+h_j(N+i-1,x))\}_{i=j+1,\cdots,m}$ 중 어떤 값도 알 수 없으며, 결국 어떤 유효한 masking 다항식의 값도 구할 수 없다. 따라서 취소된 멤버들은 브로트캐스트되는 메시지들과 자신들이 알고 있는 모든 정보를 이용하여도 임의의 $i \in \{1,\cdots,n\}$에 대해 다항식 $h_j(x,i)$에서 기껏해야 t개의 점만을 알 수 있다. $|C \cup D| \le t$이고 C와 D의 교집합이 공집합이고 $f_j(x)$, $g_j(x)$, $h_j(x,i)$가 차수 t이기 때문에, $C \cup D$의 사용자들의 공모는 K_j를 복구할 수 없다. 즉, 다음이 성립한다.

$$H(\boldsymbol{K_j} | \{\boldsymbol{Z}_{i',k}\}_{U_i \in C, 1 \le k \le j_1} \cup \{\boldsymbol{Z}_{i',k}\}_{U_i \in D, j_2 \le k \le m}) = H(\boldsymbol{K_j}).$$

Ⅳ. 결 론

본 논문에서는 self-healing 키 분배를 향상시킬 수 있는 기법을 제안하였다. 더욱이, [1]에서 제안된 기법의 통신량을 향상시키고, 그룹 멤버의 저장량을 효율적으로 줄였다. 앞으로 좀 더 통신량을 줄일 수 있는 효과적인 기법에 대한 연구와 secret sharing을 사용하지 않는 안전하고 효율적인 self-healing 키 분배 기법에 대한 연구가 계속 진행되어야 할 것으로 보인다.

참 고 문 헌

[1] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-Healing Key Distribution with Revocation," *In Proc. of the IEEE Symposium on Security and Privacy*, pp.224~240, 2002.

[2] C. Wong, M. Gouda and S. Lam, "Secure Group Communications Using Key Graphs," *In Proc. of the ACM SIGCOMM'98*, pp.68~79, 1998.

[3] D. Wallner, E. Harder and R. Agee, "Key Management for Multicast: Issues and Architectures," *IETF Request For Comments, RFC 2627*, June 1999.

[4] D. McGrew and A. Sherman, "Key Estabilishment in Large Dynamic Groups Using One-Way Function Trees," *TIS Report No.0755*, 1998.

[5] D. Naor, M. Naor and J. Lotspiech, "Revocation and Tracing Schemes for Stateless users," *In Advances in Cryptology-Crypto '01, LNCS 2139*, pp. 41~62, 2001.

[6] D. Halevy and A. Shamir, "The LSD Broadcast Encryption Scheme," *In Advances in Cryptology-Crypto '02, LNCS 2442*, pp.47~60, 2002.

[7] Y. Yang, X. Li, X. Zhang and S. Lam, "Reliable group rekeying: Design and Performance Analysis," *In Proc. of ACM SIGCOMM 2001*, pp.27~38, 2001.

[8] X. Li, Y. Yang, M. Gouda and S. Lam, "Batch Rekeying for Secure Group Communications," *In Proc. of World Wide Web Conference 10 (WWW10)*, pp.525~534, 2001.

[9] D. Naor and B. Pinkas, "Efficient Trace and Revoke Schemes," *Financial Cryptography 2000, LNCS 1962*, pp.1~21, 2000.

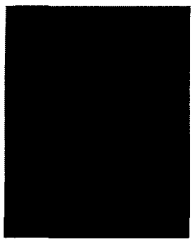
[10] A. Perrig, D. Song and J. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution," *In Proc. of the IEEE Symposium on Security and Privacy*, pp.247~262, 2001.

[11] C. Wong and S. Lam, "Keystone: A Group Key Management Service," *In International Conference on Telecommunications, ICT 2000*, pp.1~5, 2000.

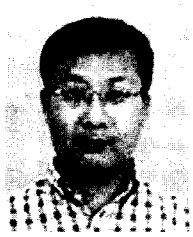
[12] T. M. Cover and J. A. Thomas, "Elements of Information Theory", John Wiley & Sons, 1991.

[13] A. Shamir, "How to Share a Secret," *In Communications of the ACM*, 22, pp.612~612, 1979.

〈著者紹介〉



홍 도 원 (Dowon Hong)
1994년 2월 : 고려대학교 이과대학 수학과(학사)
1996년 2월 : 고려대학교 수학과(석사)
2000년 2월 : 고려대학교 수학과(박사)
2000년 4월~현재 : 한국전자통신연구원 선임연구원
<관심분야> 암호 이론, 정보보호 이론, 이동통신 정보보호



강 주 성 (Ju-Sung Kang)
1989년 2월 : 고려대학교 이과대학 수학과(학사)
1991년 2월 : 고려대학교 수학과(석사)
1996년 2월 : 고려대학교 수학과(박사)
1997년 12월~현재 : 한국전자통신연구원 선임연구원
<관심분야> 암호 이론, 정보보호 이론, 이동통신 정보보호

신 상 욱 (Sang-Uk Shin)
1995년 2월 : 부산수산대학교(현 부경대학교) 전자계산학과(학사)
1997년 2월 : 부경대학교 전자계산학과(석사)
2000년 2월 : 부경대학교 전자계산학과(박사)
2000년 4월~2003년 8월 : 한국전자통신연구원 선임연구원
2003년 9월~현재 : 부경대학교 전자컴퓨터정보통신공학부
<관심분야> 정보보호, 이동통신 정보보호