情報保護學會論文誌
第16卷 第4號, 2006. 8

효율적인 동보메시지 암호화를 위한 2-부분 차집합 기법*

장 지 용,[1†] 양 대 헌,[2‡] 송 주 석[1]
[1]연세대학교, [2]인하대학교

2-Subset Difference Scheme for Broadcast Encryption*

JiYong Jang,[1†] DaeHun Nyang,[2‡] JooSeok Song[1]
[1]Yonsei University, [2]Inha University

요 약

동보메시지 암호화는 중앙에서 동보 메시지를 전송할 때, 권한이 있는 사용자들만이 받은 메시지를 해독하고 열람할 수 있도록 암호화해서 보내는 기술이다. 본 논문에서는 기존의 "Subset Difference'(SD) 기법을 기반으로 한 효율적인 동보메시지 암호화 기법을 제안하고자 한다. 이를 통해서 전송 부하를 약 50% 정도 줄일 수 있었으며, 계산량이 다소 늘었을 뿐, 필요로 하는 저장 공간은 늘지 않았다.

ABSTRACT

Broadcast Encryption allows a center to broadcast encrypted message to a set of users so that only privileged users can decrypt them. In this paper, we propose an efficient broadcast encryption scheme based on the "Subset Difference" (SD) scheme. It reduces the transmission overhead by 50 percent while the storage overhead remains the same but the computational overhead somewhat increases.

Keywords : *Information Security, Broadcast Encryption, Subset Difference Scheme*

Ⅰ. 서 론

Fiat와 Naor[1]에 의해서 처음 소개된 동보메시지 암호화는 중앙에서 동보메시지를 전송할 때 권한이 있는 사용자들만이 받은 메시지를 복호하고 열람할 수 있도록 암호화해서 전송하는 기술이다. 이러한 기술은 저작권이 있는 음악, 영화, 책 등의 미디어의 배포나 유료 케이블 TV 방송 등에 적용되어 권한이 있는 사용자들만이 해당 컨텐츠를 이용할 수 있도록 하는데 사용될 수 있다. 트리 구조에 기반한 Complete Subtree (CS) 기법과 Subset Difference (SD) 기법[2]이 Naor 등에 의해서 제안되었고, Layered SD 기법[3]이 Halevy와 Shamir에 의해서 제안되었다. 최근에는 일방향 해쉬 체인을 이용한 Punctured Interval (PI) 기법[4]이 Jho 등에 의해서 제안되었으며, 기존의 동보메시지 암호화 기법을 효율적으로 적용시킬 수 있는 일반화된 형태의 기법[5]이 Hwang 등에 의해서 제안되었다.

일반적으로 동보메시지 암호화 기술의 효율성은 전송 부하, 저장 공간 부하, 계산량 부하의 3가지 측

접수일: 2006년 3월 14일 ; 채택일: 2006년 8월 3일
* 본 연구는 한국과학재단 특정기초연구(R01-2006-000-10614-0)지원으로 수행되었음.
† 주저자, souljang@emerald.yonsei.ac.kr
‡ 교신저자, nyang@inha.ac.kr

면에서 측정된다. 본 논문에서는 전송 부하를 줄이는 데 목표를 두고, 기존의 SD기법을 발전시킨 효율적인 동보메시지 전송기법인 "2-Subset Difference scheme"을 제시한다. 이 기법에서 우리는, 권한이 있는 사용자를 커버하는 겹치지 않는 부분집합의 개수를 기존의 SD기법에 비해 절반으로 줄여 전송되는 메시지의 길이를 권한을 상실한 사용자의 수와 동일한 r로 줄였다.

II. 기존 연구

본 논문에서 제시하는 기법은 Subset Difference Scheme을 기반으로 하고 있기에 이에 대해서 우선 간략하게 살펴본다.

초기에 중앙에서는 사용자들을 n개의 leaf 노드에 대응시킨 완전 이진 트리(complete binary tree)를 구성한다. 하나의 부분집합은 (v_i,v_j)와 같이 노드 페어로 표현되며, 이 경우 v_i가 v_j의 선조 노드가 된다. 부분집합 $S_{i,j}$는 v_i를 root로 하는 부분트리의 leaf 노드들에서 v_j를 root로 하는 부분트리의 leaf 노드를 제외한 노드들을 포함한다. 다른 동보메시지 암호화 기법과 마찬가지로 SD 기법도 3단계 -초기설정, 암호화, 복호화-로 구성된다.

1. 초기설정

각 부분집합들에 다음과 같이 키를 할당한다. G를 주어진 입력에 대해 3배 길이의 출력을 만드는 pseudo random sequence generator ($G:\{0,1\}^n \rightarrow \{0,1\}^{3n}$)라고 하고, $G_L(\cdot)$을 G의 출력 중 왼쪽 1/3, $G_R(\cdot)$을 오른쪽 1/3, $G_M(\cdot)$을 가운데 1/3로 정의한다. 노드 v_i의 레이블 L_i에 대해 왼쪽 자식노드의 레이블은 $G_L(L_i)$, 오른쪽 자식노드의 레이블은 $G_R(L_i)$가 되며, 노드 v_i의 키는 $G_M(L_i)$가 된다. 이러한 레이블링을 반복적으로 수행하게 되면, 노드 v_i의 후손 노드인 v_j의 레이블을 유도해낼 수 있으며 이렇게 유도된 레이블을 $L_{i,j}$라 표기한다. 부분집합 $S_{i,j}$에 할당되는 키 $K_{i,j}$는 $G_M(L_{i,j})$가 된다. 높이가 k인 부분트리 T_i에 속한 유저는 k개의 레이블을 받으며 부분트리의 높이는 0부터 $\log(n)$까지 가능하므로, 각 사용자가 저장하게 되는 레이블(키)의 전체 개수는 $1+\sum_{k=0}^{\log(n)} k=\frac{1}{2}log^2(n)+\frac{1}{2}log(n)+1$ 가 된다. (권한을 상실한 사용자가 없는 경우에 쓰이는 키 1개를 더 고려)

2. 암호화

중앙에서 세션 키 K를 선택하고 권한이 있는 사용자 집합 $\overline{R}$을 겹치지 않게 부분집합 $S_{i_1,j_1},S_{i_2,j_2},\ldots,S_{i_m,j_m}$으로 분할한다. 세션 키 K는 $K_{i_1,j_1},K_{i_2,j_2},\ldots,K_{i_m,j_m}$로 각각 암호화되고 메시지 M은 세션 키 K로 암호화된다. 그런 다음, 중앙에서는 헤더 $<(i_1,j_1),\ldots,(i_m,j_m),E_{K_{i_1,j_1}}(K),\ldots,E_{K_{i_m,j_m}}(K)>$와 몸체 $<E_K(M)>$로 구성된 암호화된 메시지를 전송하고, 이는 권한이 있는 사용자들만이 복호할 수 있게 된다. 겹치지 않는 부분집합들의 모임인 커버는 다음과 같이 구성된다. 집합 R(권한을 상실한 사용자 집합)과 root 노드를 포함하는 Steiner Tree ST(R)을 시작으로 하여 최종적으로 노드가 한 개 남을 때까지 다음을 반복적으로 수행한다. ST(R)에서 2개의 leaf 노드 v_i와 v_j를 선택하고 이 두 노드 외에는 다른 leaf 노드를 갖지 않는 최소 공통 선조노드인 v를 찾는다. v_p와 v_q를 v의 자식노드라 하자. 이 때 v_p는 v_i의, v_q는 v_j의 선조 노드이다. 만약 $v_p \neq v_i$이면, 부분집합 $S_{p,i}$를 커버에 추가하고, $v_q \neq v_j$이면, 부분집합 $S_{q,j}$를 커버에 추가한다. 이제 v의 모든 후손 노드를 제거하고 v를 leaf 노드로 만든다. 이를 반복하고 나면, 최종적으로 커버는 최대 $2r-1$개의 부분집합을 갖게 된다.

3. 복호화

권한이 있는 사용자 $u \in N \setminus R$ 는 우선 자신이 속한 부분집합 $S_{i,j}$를 헤더의 인덱스를 보고 찾는다. 물론, v_j는 u의 선조가 아니다. 레이블 $L_{i,j}$를 계산해 내기 위해 사용자는 레이블 L_i에 G를 최대 $\log(n)$번 적용해야한다. 사용자는 구해진 $K_{i,j}$를 통해 세션 키 K를 얻게 되고, 메시지를 복호하여 M을 열람할 수 있게 된다.

SD 기법에 대한 자세한 사항은 논문[2]을 참조하기 바란다.

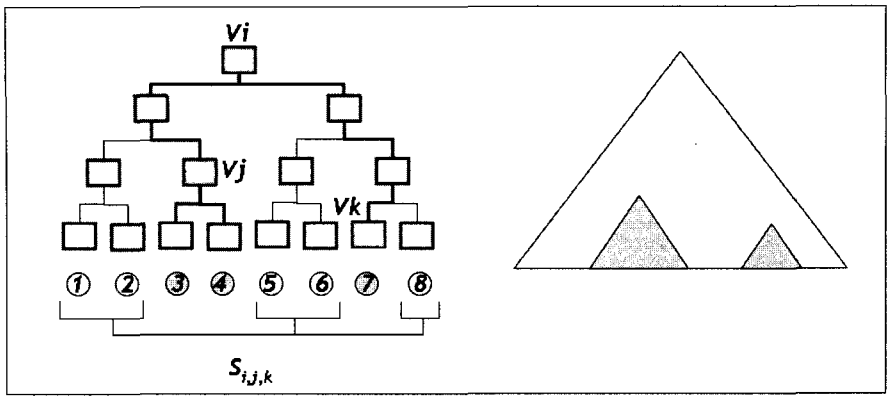

그림 1. 2-Subset Difference scheme에서의 부분집합 $S_{i,j,k}$

Ⅲ. 제안하는 기법

본 논문에서 우리는 제안하는 2-Subset Difference Scheme을 통해 메시지 헤더의 길이를 줄이고 전송 부하를 낮추는 데 중점을 두었다.

부분집합 $S_{i,j}$는 v_i를 root로 하는 부분트리의 leaf 노드들에서 v_j를 root로 하는 부분트리의 leaf 노드들을 제외한 노드들을 포함한다고 정의하였다. 이때, v_j를 root로 하는 부분트리의 leaf(사용자)들은 (연속된) 권한을 상실한 사용자들을 의미하게 된다. 기존 SD 기법에서는 하나의 부분집합이 하나의 (연속된) 권한을 상실한 사용자 집합을 포함할 수 있었다. 우리의 주된 아이디어는 하나의 부분집합에서 하나 이상의 (본 논문에서는 2개의) 권한을 상실한 사용자 집합을 포함할 수 있도록 하는 것이다. 이렇게 함으로써 전체 부분집합의 개수를 줄일 수 있게 되고 전송 부하 또한 낮출 수 있다. 지금부터 2-SD 기법에 대해서 자세히 살펴보겠다.

기존 SD 기법과 마찬가지로 초기에 중앙에서는 사용자들을 n개 leaf 노드에 대응시킨 완전 이진 트리를 구성한다. 부분집합 $S_{i,j,k}$를 그림 1과 같이 v_i를 root로 하는 부분트리의 leaf 노드들에서 v_j와 v_k를 각각 root로 하는 부분트리의 leaf 노드들을 제외시킨 노드들의 집합이라 표기한다. 2-SD 기법의 3단계 과정은 다음과 같다.

1. 초기설정

기존 SD 기법과 유사하게 pseudo random sequence generator G를 이용하여 노드들의 레이블을 부여한다. (G함수와 레이블링의 방법은 II.1 절을 참조하기 바란다.) 그 다음 v_i를 root로 하는 부분트리 T_i에 속한 각 사용자 u는 v_i의 자손이면서 u의 선조가 아닌 노드들의 레이블을 저장하게 된다. 세션 키를 암호화할 때 쓰이는 부분집합의 키는 권한을 상실한 사용자 집합을 2개 포함할 경우 $K_{i,j,k}$이며, $K_{i,j}$와 $K_{i,k}$를 XOR한 $K_{i,j} \oplus K_{i,k}$의 결과값과 동일하다. $K_{i,j}$는 부분집합 $S_{i,j}$의 키로 $G_M(L_{i,j})$이며, $K_{i,k}$는 부분집합 $S_{i,k}$에 할당되는 키로 $G_M(L_{i,k})$이다. 권한을 상실한 사용자 집합을 1개 포함할 경우, 부분집합의 키는 기존 SD 기법과 동일한 형태의 $K_{i,j}$가 된다.

2. 암호화

중앙에서 전송할 암호화된 메시지(메시지의 헤더와 몸체)를 구성하는 방법은 기존 SD 기법과 유사하다. 다만 권한이 있는 사용자를 커버하는 부분집합을 생성하는 과정에 있어서 차이가 있다. 중앙에서는 메시지를 암호화할 세션 키 K를 생성하고 권한이 있는 사용자 집합 $\overline{R}$을 겹치지 않는 부분집합들로 나누어 커버를 생성하게 된다. 이렇게 생성된 각 부분집합의 키로 세션 키를 암호화하게 된다. 집합 R(권한을 상실한 사용자 집합)과 root 노드를 포함하는 Steiner Tree ST(R)을 구성하고 다음과 같이 커버에 부분집합들을 추가해 나간다. ST(R)에서 두 leaf 노드 v_j와 v_k를 선택하고 이 두 노드 외에는 leaf 노드를 갖지 않는 최소 공통 부모 노드 v_i를 찾는다. 이

표 1. CS, SD, LSD, 2-SD 기법의 복잡도

Scheme	Transmission Overhead	Storage Overhead	Computation Overhead
Complete Subtree[2]	$r\log(n/r)$	$O(\log(n))$	$\log\log(n)$
Subset Difference[2]	$2r-1$	$O(\log^{2}(n))$	$\log(n)$
Layered SD[3]	$4r-2$	$O(\log^{3/2}(n))$	$\log(n)$
2-Subset Difference	r	$O(\log^{2}(n))$	$2\log(n)$

렇게 찾아진 v_i의 자식노드를 v_p와 v_q라 하며, 이 때 v_p는 v_j의 선조 노드이고 v_q는 v_k의 선조 노드이다. 이에 대해 다음과 같이 부분집합을 커버에 추가한다.

1) $v_p \neq v_j$이고 $v_q \neq v_k$이면 부분집합 $S_{i,j,k}$를 커버에 추가한다.
2) $v_p \neq v_j$이고 $v_q = v_k$이면 부분집합 $S_{p,j}$를 커버에 추가한다.
3) $v_p = v_j$이고 $v_q \neq v_k$이면 부분집합 $S_{q,k}$를 커버에 추가한다.
4) $v_p = v_j$이고 $v_q = v_k$이면 추가되는 부분집합이 없다.

위와 같이 해당되는 부분집합을 커버에 추가한 다음, v_i의 모든 후손 노드를 제거하고 이를 leaf 노드로 만든다. 이와 같은 과정을 최종적으로 하나의 노드가 남을 때까지 반복하게 된다.

3. 복호화

권한이 있는 사용자 $u \in N \setminus R$는 먼저 자신이 속한 부분집합 $S_{i,j,k}$(또는 $S_{i,j}$)를 찾는다. 부분집합 키 $K_{i,j,k}$를 얻기 위해서는 $K_{i,j}$와 $K_{i,k}$가 필요하며, 레이블 $L_{i,j}$는 레이블 L_i에 G를 최대 $\log(n)$번 적용하면 유도해낼 수 있다. 레이블 $L_{i,k}$ 또한 이와 유사하게 유도해낼 수 있다. 부분집합 키 $K_{i,j,k} = K_{i,j} \oplus K_{i,k}$를 계산한 다음, 사용자는 세션 키 K를 구해내 메시지를 복호할 수 있다.

Ⅳ. 안전성 분석

위에서 이미 언급했듯이 부분집합 키 $K_{i,j,k}$를 $K_{i,j}$와 $K_{i,k}$를 XOR한 값으로 정의하였다. 그림 1에서 사용자 3, 4가 $K_{i,k}$를 알 수도 있지만, $K_{i,j}$를 알 수 없기 때문에 $K_{i,j,k}$를 유도해낼 수 없다. 마찬가지로 사용자 7 또한 $K_{i,j,k}$를 계산해낼 수 없다. 또한 XOR한 결과 값을 부분집합 키로 정의하였기 때문에 2-SD기법은 기존의 SD 기법과 동일한 수준의 안전성을 제공하고, 전송 부하를 줄이면서도 동일한 수준의 저장 공간 부하만을 필요로 한다.

Ⅴ. 효율성 비교 분석

n은 전체 사용자의 수, r은 권한을 상실한 사용자의 수를 각각 의미한다.

정리1 : 2-Subset Difference scheme 은 최대 r의 메시지 헤더길이, $\frac{1}{2}log^{2}(n)+\frac{1}{2}log(n)+1$ 개의 저장해야할 키 정보, $2\log(n)$ 번의 연산을 필요로 한다.

증명 : 커버를 구성할 때, 한 번의 과정을 수행하고 나면 최대 1개의 부분집합이 커버에 추가되고 leaf 노드의 개수는 1개씩 줄어든다. Steiner Tree에서, 최초 r개의 leaf 노드에서 시작하여 최종적으로 1개의 노드가 남을 때까지 과정이 반복되므로 총 $r-1$번의 과정이 수행되게 된다. 따라서 $r-1$번의 모든 과정을 마치고 나면 최대 $r-1$개의 부분집합이 생성된다. 이 후, 마지막 검사를 하면서 1개의 부분집합이 추가될 수 있다. 따라서 커버 크기는 최대 r이 된다. 부분집합의 키는 $K_{i,j}$와 $K_{i,k}$를 XOR한 값이다. 두 키 모두를 기존 SD 기법에서 저장한 키 정보들로부터 구할 수 있기 때문에, 기존 SD 기법과

비교해서 추가적으로 저장해야하는 키 정보는 없다. 따라서 각 사용자마다 저장해야하는 레이블(키) 개수는 $\frac{1}{2}log^2(n)+\frac{1}{2}log(n)+1$ 이다. 부분집합 키 $K_{i,j,k}$를 계산할 때, 레이블 $L_{i,j}$는 레이블 L_i에 G를 최대 $\log(n)$번 적용하여 유도해낼 수 있고, 레이블 $L_{i,k}$ 또한 동일한 방법으로 구할 수 있다. 결과적으로 세션 키를 구하기 위해 $2\log(n)$번의 연산과정이 필요하다. ■

표 1은 CS, SD, LSD와 본 논문에서 제시한 2-SD 기법의 전송 부하, 저장 공간 부하, 계산량 부하의 복잡도를 나타낸 것이다. 2-SD 기법의 계산량 부하는 최악의 경우 $2\log(n)$이고, 기존 SD 기법과 마찬가지로 하나의 부분집합이 단지 하나의 권한을 상실한 집합만을 포함할 경우 $\log(n)$이다. 따라서 계산량 부하는 평균적으로 $1.5\log(n)$이 된다.

Ⅵ. 결 론

본 논문에서는 Subset Difference scheme에 기반한 2-Subset Difference scheme을 제안하였다. 2-SD 기법은 계산량 부하가 약간 늘어난 대신, 전송 부하를 절반가량 줄였다. 또한 메시지 헤더의 길이가 r 밖에 되지 않아 권한을 상실한 사용자의 수가 늘어나는 경우에도 유동적으로 적용될 수 있다.

참 고 문 헌

[1] A. Fiat and M. Naor, "Broadcast Encryption," *In Advances in Cryptology: CRYPTO 1993*, LNCS vol.773, pp. 480-491, 1993.

[2] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," *In Advances in Cryptology: CRYPTO 2001*, LNCS vol. 2139, pp. 41-62, 2001.

[3] D. Halevy and A. Shamir, "The LSD Broadcast Encryption Scheme," *In Advances in Cryptology: CRYPTO 2002*, LNCS vol.2442, pp. 47-60, 2002.

[4] NS. Jho, JY. Hwang, JH. Cheon, M. Kim, DH. Lee and ES. Yoo, "One-way chain Based Broadcast Encryption Scheme," *In Advances in Cryptology: Eurocrypt 2005*, LNCS vol.3494, pp.559-574, 2005.

[5] JY. Hwang, DH. Lee, and J. Lim, "Generic Transformation for Scalable Broadcast Encryption Schemes," *In Advances in Cryptology: CRYPTO 2005*, LNCS vol.3621, pp.276-292, 2005.

〈著者紹介〉

장 지 용 (JiYong Jang) 학생회원
2005년 연세대학교 기계전자공학부 학사
2005년 ~ 현재 연세대학교 컴퓨터과학과 대학원 석사과정
〈관심분야〉 암호프로토콜, 무선 네트워크 보안, 이동통신기술

양 대 헌 (DaeHun Nyang) 정회원
1994년 2월 : 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월 ~ 2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월 ~ 현재 : 인하대학교 정보통신대학원 조교수
〈관심분야〉 암호이론, 암호프로토콜, 인증 프로토콜, 무선 네트워크 보안

송 주 석 (JooSeok Song) 정회원
1976년 서울대학교 전기공학과 학사
1979년 한국과학기술원 전기 및 전자공학 석사
1988년 Univ. of California at Berkeley, 컴퓨터과학 박사
1988년 ~ 1989년 Assistant Professor in Naval Postgraduate School
1989년 ~ 현재 연세대학교 컴퓨터과학과 정교수
2006년 ~ 현재 한국정보보호학회장
〈관심분야〉 Information Security, Cryptography, Protocol Engineering