하이브리드 브로드캐스트 암호화 알고리즘

김대현, 두소영, 공은배
충남대학교 컴퓨터공학과
{dh999,sydoo,keb}@comeng.chungnam.ac.kr

Hybrid Broadcast Encryption

Daehyun Kim, Soyoung Doo, Eunbae Kong
Dept. of Computer Engineering Chungnam National Univ.

요 약

본 논문에서는 기존의 브로드캐스트 암호화 방식에 대한 고찰과 현재까지의 기술들의 단점을 보완할 수 있는 새로운 브로드캐스트 암호화 방식을 제안하였다. 브로드캐스트 암호화 방식은 비밀이 보장되지 않는 브로드캐스트 채널 상에서 특정 사용자만이 정보를 사용할 수 있도록 하기 위한 프로토콜이다. 이러한 시스템을 평가하는 중요한 비교 변수로는 전송량과 사용자가 보관하고 있어야 하는 해독키의 크기이다. 본 논문에서는 사용자를 일정 그룹으로 나누어서 암호키를 할당함으로써 사용자 개개인에게 암호키를 할당하는 경우 보다 전송량을 줄 일 수 있었고, 메시지는 하나의 세션키로 암호화 하고 이 세션키를 다시 암호화하여 메시지의 헤더에 첨가하여 전달함으로써 전송량을 확실히 줄일 수 있었다. 사용자를 임의의 그룹으로 구성하여 하나의 그룹에 일정 수 이상이 정보를 전달 받을 자격이 있다면 그 그룹의 암호키를 선택하여 세션키를 암호화하였다. 이 때 그룹에 있는 권한이 없는 사용자들이 정보를 전달받을 수 있으나, 이들의 크기는 실험 결과 그다지 문제가 되지 않을 정도로 작은 수임을 알 수 있었다.

1. 서 론

인터넷과 같이 비밀이 보장되지 않는 네트워크에서 특정 사용자가 속한 그룹에만 가치 있는 정보를 전달하기 위해서는 어떤 방법을 사용해야 할까? 모든 네트워크에서 정보를 특정 사용자에게만 안전하게 전달하는 가장 보편적인 방법은 정보 사용을 허가하고자 하는 사용자에게 미리 해독키를 비밀리에 전달하고 메시지를 이 키로 암호화 한 후 전달하는 것이다. 또 다른 사용자가 동일한 정보를 요구할 경우에도 같은 절차가 반복된다. 따라서, 정보 제공자는 각 사용자가 등록할 때 할당한 키를 사용하여 매번 암호화하고 각 사용자에게 전달하는 일을 반복 수행하게 된다.

N명의 사용자가 등록하였다면, N개의 키를 사용자에게 할당하고 N번의 암호화 과정을 통해 암호화된 메시지를 N번 전송하는 절차가 필요하다는 것을 의미한다. N이 커진다면 정보 제공 서버의 부하 또한 커지고 인터넷을 통해 동일한 정보를 동시에 다량으로 제공하고자 하는 경우 서버의 성능에 영향을 주게된다.

동일한 정보를 특정 사용자 그룹에 비밀스럽게 전달하고 허가된 사용자만이 이 정보를 활용할 수 있도록 하면서, 서버의 전송량을 줄이고자 하는 브로드캐스트 암호화 방식은 Fiat과 Naor[1]에 의해서 처음으로 제안되었다. 브로드캐스트 암호화 방식은 Fiat과 Naor가 제안한 이후로 여러 사람들이 보다 효율적인 방안을 꾸준히 제안하고있다[2][3][4][5].

본 논문에서는 현재 제안되어 있는 방식들 보다 전송량과 메모리 요구량이 적게 요구되는 브로드캐스트 암호화 방식을 제안한다. 논문의 구성은 우선 2장에서 브로드캐스트 암호화 방식에 대한 설명과 기존에 제안된 방식들을 살펴보고 3장에서 본 논문에서 제안하는 새로운 브로드캐스트 암호화 방법을 설명하며 4장에서 제안된 암호화 방법의 특징을 다른 암호화 방법들과 비교 검토한 후 결론을 맺는다.

* 본 연구는 과학기술부/한국과학재단 지정 충남대학교 소프트웨어연구센터의 지원에 의한 것입니다.

2. 브로드캐스트 암호화 방식

Fiat과 Naor[1]는 처음으로 브로드캐스트 암호화 방법을 소개하였다. 브로드캐스트 키 정보를 비밀스럽게 사용하는 방법으로 선택된 사용자 그룹만이 이 정보를 해독할 수 있도록 한다. k명의 사용자가 협잡하더라도 키 정보를 얻을 수 없다.

우선 사용자가 정보 제공자에게 등록할 경우 각 사용자는 i개의 함수를 할당 받는다. 이 함수는 1에서 m까지의 수에 맵핑되는데 이때 fi(x)와 fi(y)는 같지 않다. 각 사용자는 R(i,j)를 사용하여서 세션키를 얻게된다. R(i,j)에서 i는 fi()의 순서를 표시하는 i이고 j는 fi(x) 결과값이다. 정보제공자는 메시지 M을 전송하고자 할 때 M을 i개의 메시지로 나누어 이 메시지들을 ⊕연산을 통해서 원래의 메시지 M을 생성하도록 한다. 사용자는 R(i,j)를 사용하여 해독키의 위치를 알아내고 미리 가지고 있던 키를 사용하여 세션키를 알아낸 후 이 세션키를 사용하여 메시지 Mi를 해독한다. M1에서 Mi까지를 ⊕연산하여 원래의 M을 얻어낸다. 이 방법은 사용자가 너무 많은 수의 키정보를 가지고 있어야한다는 점에서 실질적이지 못하다고 평가되고 있다.

Michel과 Avishai[5]는 실질적인 브로드캐스트 암호화 알고리즘을 제안하였다. 이들은 우선 사용자의 전체 수를 임의로 정한 후 전체 사용자를 밸런스 트리를 사용하여 그룹을 구성한다. 이때 하나의 그룹은 하나의 암호키를 동일하게 가진다. 따라서 사용자가 등록하게되면 하나의 아이디를 할당 받게되고 이 아이디가 속해 있는 모든 그룹의 암호키를 전달받게 된다. 실제로 정보를 전달 받을 특정 사용자들이 타겟 그룹을 이루면 정보 제공자는 타겟 그룹에 속해있는 사용자 아이디가 트리의 어떤 노드들에 속해 있는지 가장 적합한 노드를 골라내게 된다. 이 과정을 통해서 최종적으로 선택된 노드에는 권한이 없는 사용자가 포함되어 있을 수도 있다. 즉, 이들의 브로드캐스트 암호화 방식은 정보를 특정 사용자에게만 전달하는 것이 아니라 허용 범위 내에서 권한이 없는 사용자들도 정보를 전달받을 수 있도록 구성되어 있다. 그러나, Michel과 Avishai에 의해면 이들의 수는 무시할 수 있을 만큼 적은 수임을 실험 결과로 제시하고 있다. 이렇게 정해진 그룹의 암호키를 사용해서 동일한 정보를 선택된 그룹수만큼 암호화 해서 전송한다. 이 방법은 권한이 없는 사용자에게도 정보가 전달될 수 있다는 점과 더불어 타겟 그룹에 따라서는 전송량이 엄청나게 커질 수 있다는 문제점을 가지고 있다.

브로드캐스트 암호화 방식과 유사한 연구로는 "Tracing Traitor"[2][3][4]라는 것이 있고 이들은 정당하지 않은 해독키를 사용하는 사용자의 해독키가 누구에 의해서 만들어 졌는지를 추적하기 위한 것이다. 정보 제공자가 전달하는 메시지는 헤더와 실제 정보로 이루어져 있다. 실제로 보내고자 하는 정보는 세션키로 암호화 되어 있고, 이 세션키는 각 사용자들의 해독키로 암호화 되어서 헤더를 구성한다. 사용자들이 등록하면 사용자에게는 세션키를 해독할 수 있는 해독키정보를 헤더로부터 얻을 수 있는 위치 정보가 전달 되게 된다. 이때 헤더의 크기는 사용자의 수가 증가할수록 커지게 된다. 이 암호화 방식은 특정 그룹에 속하지 않은 어떤 사용자도 정보를 사용할 수 없도록 한다.

브로드캐스트 암호화 프로토콜은 정보제공자로부터 사용자에게 전달되는 메시지의 전송량과 사용자가 보관해야하는 키의 수가 성능을 평가하는 변수로 고려된다.

3. 하이브리드 브로드캐스트 암호화 프로토콜

본 논문에서는 기존의 프로토콜들이 가지는 단점들을 보완하여 보다 효율적인 브로드캐스트 암호화 프로토콜을 설계하였다. 새로운 브로드캐스트 암호화 프로토콜은 그림1과 같은 알고리즘을 통해 특정 그룹의 암호키를 생성한다.

```
C <- ∅  C는 암호키의 집합
S={S1, S2,....., Si} 트리의 노드들
Q: 큐
K={u1,u2,...,un}:특정그룹
f = 2
1. Q에 S1을 추가한다.
2. Repeat
3. Q에서 Si를 꺼낸다.
4. if |Si -K| ≠ 0 then
       if   |Si| / |Si∩K| ≤ f then
                C <- C ∪{Si}
       else
                Si의 자식노드를 Q에 추가한다.
       endif
   endif
5. Until Q is empty
6. Return C
```

그림 1. 암호키 선택 알고리즘

사용자들의 그룹을 트리의 노드로 표현한다. 즉, 루트 노드는 모든 사용자를 포함하는 그룹이다. 트리의 상위계층을 크기가 같은 하위계층으로 나누고, 하위계층은 상위계층의 이분된 내용을 각 노드로 가지는 이진 트리이다. 각 노드에는 하나의 암호키가 할당된다. 사용자들이 특정 그룹(K)가 구성되면

암호키는 그림1과 같은 알고리즘에 의해서 선택된다.

암호키 집합이 선택되면 정보 제공자는 다음과 같이 전송 메시지를 구성한다. 암호화 하고자 하는 정보는 랜덤하게 생성된 Sk에 의해서 암호화 된다[6][7]. 세션키가 Sk 라면 전송될 메시지의 내용은 그림2와 같다.

$E_{S1k}[Sk]$ $E_{S2k}[Sk]$ ..... $E_{Sik}[Sk]$	Sk[Information]

Sk: Session key

Sik: 집합 C 에 선택된 그룹들의 암호키

그림 2. 전송 메시지 포맷

메시지를 하나의 키로 암호화 한 후에 이 키를 각 사용자에게 할당된 암호키로 암호화해서 전달하는 방법을 사용함으로써 총 메시지 전송량은 메시지크기 + 헤더크기가 된다. 이때 헤더의 크기가 전송에 미치는 영향은 다음 장에서 실험을 통해 고찰하였다. 헤더의 크기와 전송량은 다음과 같이 계산된다.

- H_SIZE = |C| x Key_SIZE
  * H_SIZE: 헤더의 크기, |C|: 선택된 그룹의 수
  * Key_SIZE: 암호키의 크기
- Transmit_SIZE_1 = Sizeof(Message) + H_SIZE

Michel과Avishai의 알고리즘에서 전송량은 다음과 같다.

- Transmit_SIZE_2 = Sizeof(Message) x |C|

암호키의 크기는 메시지의 크기에 비해 매우 작으므로 이것을 n 배하여 헤더에 넣는다고 하여도 메시지를 n번 전송하는 양보다 작다. 따라서, 키를 암호화해서 헤더에 추가하여 전달하는 경우 전송량을 줄일 수 있다.

4. 실험 및 결론

제안된 브로드캐스트 암호화 방식의 성능을 검증하기 위해서 전체 등록된 사용자를 1024명으로 하고, 사용자에게 전달하는 암호키는 사용자가 속한 임의의 그룹에 할당된 암호키로 하였다. 실험에서 중요하게 다룬 내용은 다음 두가지 이다.

1. 정보 제공자의 총 전송량
2. 각 사용자에게 할당된 암호키의 수

제안된 알고리즘의 성능을 평가하기 위해서 특정 사용자 그룹은 1024명중에서 랜덤하게 선택하였고, 1에서 1024명까지 순차적으로 증가하였다. 이것을 10번 반복하여 그 평균값을 구하였다. 그 결과는 그림 3과 같다.

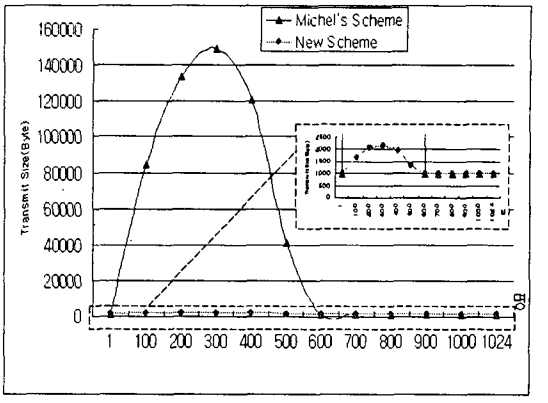

그림 4. 정보를 요청한 사용자 수와 전송량의 변화

그림3에서 가로축은 특정 서비스를 요구하는 사용자의 수를 나타내며 1에서 1024까지 증가하도록 했다. 세로축은 전체 전송량으로 단위는 Byte이다. 이때 메시지크기는 1024 Byte로 하였다. 본 논문에서 제안한 브로드캐스트 암호화 방식의 최대 전송량은 사용자가 285명일 때 2209 Byte가 되었다. 비교된 그래프는 Michel과 Avishai의 알고리즘으로 285명일 때 최대치 151790 Byte를 전송한다.

본 논문에서는 새로운 브로드캐스트 암호화 방법을 제안하였고 기존의 방법들과 비교하여 사용자 할당 암호키 수와 전송량을 확실히 줄일 수 있다는 것을 확인하였다.

Reference

[1] Amos Fiat and Moni Naor. "Broadcast Encryption", In Advances in Cryptology-CRYPTO'93 LNCS773, pp.480-491, 1994.

[2] Benny Chor, Amos Fiat, Moni Naor, "Tracing Traitors", In Advances in Cryptology-CRYPTO'94 LNCS839,pp.257-270, 1994.

[3] Birgit Pfitzmann, "Trials of Traced Traitors", In Advances in Cryptology-CRYPTO'96 LNCS1174,1996.

[4] Moni Naor, B.pinkas, "Threshold traitor tracing", In Advances in Cryptology-CRYPTO'98 LNCS1462,1998.

[5] Michel Abdalla, Yuval Shavitt, Avishai wool, "Towards Making Broadcast Encryption Practical", Financial Cryptography '99 LNCS1648, 1999.

[6] Bruce Schneier, Applied Cryptography, Wiley, 1996.

[7] Douglas R. Stinson, Cryptography Theory and Practice, CRC Press, 1995.