부정자 추적 기법을 이용한 디지털 방송용 컨텐츠 보호 시스템 모델

서병만*, 김소진**, 최재귀**,박지환*
*부경대학교 대학원 전자계산학과
**부경대학교 대학원 정보보호학과
E-mail: bmseo@shannon.pknu.ac.kr

Contents Protection System Model for Digital Broadcasting Using Traitor Tracing Scheme

Byong-Mahn Seo*, So-Jin Kim**, Jae-Gwi Choi**, Ji-Hwan Park*
*Dept. of Computer Science, Pukyong National University
**Dept. of Information Security, Pukyong National University

요 약

부정자 추적 기법(traitor tracing)은 컨텐츠에 대한 무단 배포, 불법 복사 등의 부정 행위를 한 부정자(traitor)를 추적할 수 있는 방식이다. 본 논문은 부정자 추적 기법을 이용하여 디지털 방송용 컨텐츠 보호 시스템 모델을 구성하고자 한다. 기존의 traitor tracing 기법들이 암호학적 측면에서 키 유출에 대한 부정을 추적하기 위한 방식들이었다면, dynamic traitor tracing 기법과 sequential traitor tracing 기법은 복호화된 후의 컨텐츠에 대한 부정 배포를 막기 위한 방식이다. 본 논문에서는 sequential traitor tracing 기법을 기반으로 하여 컨텐츠 암호화 키 생성 및 전송 그리고 키 유출에 대한 추적 기능까지 제공하는 부정자 추적 기법을 제안하여 디지털 방송용 컨텐츠 보호 시스템에 대한 모델을 구성하고자 한다.

1. 서론

최근 방송과 통신 그리고 컴퓨터의 융합과 Cable TV 및 위성 방송의 성장으로 방송 시장의 구조가 변하고 있다. 이에 따라 가입자는 보다 전문화된 채널 및 개별화된 양질의 서비스를 받을 수 있다. 그러나 현재의 방송 시스템들은 단순한 사용자 인증을 통한 저작권 보호만을 수행하고 있으므로 컨텐츠의 불법 유통이나 무단 사용에는 거의 무방비한 상태다. 그러므로 실시간 방송 환경하에서 무단 사용 및 부정 배포를 방지할 수 있는 보호 시스템이 요구된다.

부정자 추적 기법(traitor tracing scheme)은 컨텐츠에 대한 무단 배포, 불법 복사 등의 부정 행위를 한 부정자(traitor)를 추적할 수 있는 방식이다. 이러한 부정자 추적 기법은 복호키에 대한 유출 방지와 복호된 컨텐츠에 대한 재전송 방지의 두 가지 흐름으로 나누어 볼 수 있다. B.Chor등에 의해 처음 제안된 기법[1]은 컨텐츠 제공자(distributor)가 컨텐츠를 암호화하고, 이를 복호화할 수 있는 키(personal key)를 수신자마다 다르게 분배함으로 이후에 pirate decoder를 구성한 부정자/공모자들(colluders)중 적어도 한 명을 식별할 수 있는 방식이다. 그러나 이 기법은 사용자의 수 (n)가 많아짐에 따라 컨텐츠 제공자가 배포해야 할 정보도 $\log(n)$ 만큼 증가하게 되고, 결탁하는 사용자의 수 (k)를 적게 하면 안전성도 떨어지는 문제가 있다. 더욱이 컨텐츠 제공자가 직접 사용자의 개별키를 생성함으로 부인 방지 기능을 제공하지 못하는 단점이

있다. 이 문제는 B.Pfitzman이 제안한 기법[2]에서 해결되었으나, 이 방식 역시 B.Chor등의 기법[1]을 전제로 하였기 때문에 계산량과 전송량의 문제는 해결하지 못하였다. 이후 D. Boneh는 하나의 키로 컨텐츠를 암호화하고, 이 컨텐츠를 복호화할 수 있는 키는 사용자마다 유일하게 할당할 수 있는 방식[3]을 제안하였다. 이 기법은 하나의 키로 컨텐츠를 암호화하였으나, 사용자마다 복호키가 유일하므로 사용자끼리 공모해서 pirate decoder를 생성하면 부정자를 추적할 수 있다. 뿐만 아니라, 해당 공모자 모두를 추적할 수 있는 방식이다. 그러나 이 방식 역시 B.Chor등의 방식[1]과 마찬가지로 컨텐츠 제공자와 사용자가 비밀정보(복호키)를 동시에 알고 있으므로 부인 방지 기능은 제공하지 못한다. 한편, K.Kurosawa는 agent를 이용하여 부인 방지 기능을 제공한 기법[4]을 제안하였으나, 일정 수 이상의 agent가 공모하게 되면, 대칭형 traitor tracing 기법이 되므로 정확한 의미의 비대칭형 traitor tracing 기법은 아니다.

위에서 언급한 부정자 추적 기법들[1-4]은 기존의 인가받은 사용자 또는 사용자들이 pirate decoder를 생성하여 이를 인가되지 않은 사용자들에게 판매하는 상황에서 키를 유출한 부정자를 추적하는 연구들이다. 따라서 복호화된 컨텐츠의 재전송(the original content rebroadcast)에 대한 문제는 전혀 고려되지 않았으므로 실제 적용에는 한계가 있다. 컨텐츠 자체의 불법 재전송에 대한 문제는 dynamic traitor tracing 기법[5]에서 본격적으로 제기되었다. A.Fiat등이 제안한 이 기법[5]은 original content에 워터마크를 삽입하여 실시간 유료 컨텐츠에 대한 부정 copy 발견시에 해당 워터마크를 추출하여 부정자 0명 추적 → 부정자 1명 추적→ … → k 부정자 추적의 순으로 모든 부정자를 찾아낼 수 있는 기법이다. 그러나 이 방식은 지연 재전송(delayed rebroadcast) 공격에선 단 한 명의 부정자도 추적할 수 없는 점과 실시간 계산량이 높다는 문제점이 지적되었다[6]. 이후 R.S.Naini등이 sequential traitor tracing 기법[6]을 제안함으로 이 문제를 개선하고자 하였다.

본 논문에서는 sequential traitor tracing 기법을 기반으로 하여 컨텐츠 자체의 불법 재전송, 컨텐츠 암호화 키 생성 및 전송 그리고 복호화 키 유출에 대한 추적 기능까지 포함한 디지털 방송용 컨텐츠 보호 시스템을 구성하고자 한다.

논문의 구성은 다음과 같다. 2장은 관련 연구로 다수의 사용자를 위한 암호화 방식을 설명하고, 3장에서는 제안 방식을 기술한다. 4장에서는 제안 방식의 고찰을, 마지막으로 5장에서는 결론 및 향후 과제를 제시한다.

2. 관련 연구

2.1 Encryption/Decryption Method

본 절에서는 Y.U.Lyuu가 제안한 암·복호 기법[7]을 설명한다. 제안 방식에서는 이 방식을 이용하여 전송되는 정보량을 최소화하고자 한다.

[초기화]

s는 security 파라메타이고, n은 전체 사용자 수이다.각 사용자 i는 $s-bit$의 $p_i=2q_i+1$(q_i:소수)를 선택한다. 편의상 $p_1 < p_2 < \cdots < p_n$라 둔다. $M=\Pi_{i=1}^{n} p_i$이고, g는 각 p_i의 공통 원시근이라 둔다. g의 존재 가능성은 [7]에 증명되어 있다.

[키 생성]

① 각 사용자 i는 각자 자신의 비밀키 $d_i \in Z_{p_i}^*$를 선택하여 공개키 $\beta_i=g^{d_i} \pmod{p_i}$를 계산한 다음, 분배자(distributor)에게 (β_i, p_i)를 전송한다.

② 분배자는 다음과 같이 β를 계산하고, 여기에서 공개키는 (β, M, g)가 된다.

$$\beta=\sum_{i=1}^{n}\beta_i M_i y_i \pmod{M}, M_i=M/p_i$$

$$M_i y_i=1 \pmod{p_i}, 1\le i\le n$$

여기서 $\beta=\beta_i \pmod{p_i}$이다. [중국인의 나머지 정리]

[암호화]

분배자(distributor)는 x를 암호화하기 위해 난수 $r\in Z_{p-1}$를 선택하고, 다음의 암호문 $C=(z_1, z_2)$를 계산한다.

$$z_1=g^r \pmod{M}, z_2=x\beta^r \pmod{M}$$

[복호화]

각 사용자는 자신의 비밀키 d_i를 이용하여 컨텐츠를 복호화할 수 있다.

$$z_2(z_1^{d_i})^{-1} \pmod{p_i} = x$$

3. 제안 방식

제안 방식은 sequential traitor tracing[6]기법을 기반으로 하여 방송용 컨텐츠 보호 시스템 모델을 구성하고자 한다. Sequential traitor tracing기법은 컨텐츠 자체 배포에 대한 부정자 추적 기능뿐 아니라, 지연 재전송(delayed rebroadcast) 공격에도 안전하다는 점에서 그 의의가 크다. 그러나 pirate decoder(키 유출)에 대한 추적 기능을 제공하지 못하고, 실제 그룹키 관리 및 컨텐츠 암·복호화 방법은 효율적인 방법을 사용한다는 가정하에 제시되고 있는 문제가 있다.

본 제안 방식은 sequential traitor tracing기법에서 가정한 컨텐츠 암·복호화 방식을 구체적으로 제안함으로서 컨텐츠 불법 재전송에 대한 부정자 추적 기능, 암·복호화키 생성 및 전송 그리고 키 유출에 대한 부정자 추적 기능까지 제공한다. 이는 dynamic traitor tracing 기법[5]에도 적용할 수 있다. 시스템 매개변수는 다음과 같다.

<표1> 시스템 매개변수

d_u	사용자 u의 비밀키, $d_u \in Z_{p_u}^*$
β_u	사용자 u의 공개키, $\beta_u \equiv g^{d_u} \bmod p_u$
p_u	사용자 u의 modulus
s_i	i번째 세그먼트 $(1 \le i \le h)$
s_{ij}	i번째 세그먼트의 j-version $(1 \le j \le q)$
w_j	q개의 워터마크 $w_1, w_2, \ldots, w_q$
G_{ij}	세그먼트 i의 j-version에 할당된 사용자그룹
M_{ij}	G_{ij}의 공통 modulus

[Step 1] Key generation

① 사용자 u는 개인 비밀키 d_u를 선택하고, 컨텐츠 제공자에게 (β_u, p_u)를 전송한다.

[Step 2] Watermark Embedding

① 컨텐츠 제공자는 컨텐츠를 h개의 세그먼트로 분리시킨다. $content = s_1 \| \ldots \| s_{h-1} \| s_h$

② 컨텐츠 제공자는 q개의 워터마크 $(w_1, \ldots, w_q)$를 생성한 후, 각 세그먼트 s_i에 각 워터마크를 삽입한 q개의 copy (s_{ij})를 만들어 둔다.

③ 사용자는 mark 할당 테이블에 따라 미리 q개의 그룹으로 나누어져 있음을 전제로 한다. (세그먼트마다 사용자의 그룹은 바뀐다.)

[Step 3] Contents Encryption

① 컨텐츠 제공자는 G_{ij}에 해당하는 사용자들의 공개키를 이용하여 아래와 같이 $\beta_{G_{ij}}$를 계산한다. 예를 들어, 사용자 1,3,5가 세그먼트 2의 3-version에 할당되었다면, $\beta_{G_{23}}$의 값은

$$\beta_{G_{23}} \equiv \beta_1 M_1 y_1 + \beta_3 M_3 y_3 + \beta_5 M_5 y_5 \bmod M_{G_{23}}$$

$$M_u = M_{G_{ij}} / p_u,\ M_{u y_u} \equiv 1,\ \beta_{G_{ij}} \equiv \beta_u \bmod p_u$$

이 된다.

② 컨텐츠 제공자는 난수 r_i를 선택하고, ①에서 계산한 값을 이용하여 각 s_{ij}를 암호화 (z_{ij}, z_{ij}')하여 사용자에게 전송한다.

$$z_{ij} = g^{r_i} \pmod{M_{G_{ij}}}$$

$$z_{ij}' = s_{ij} \cdot \beta_{G_{ij}}^{r_i} \pmod{M_{G_{ij}}}$$

[Step 4] Contents Decryption

수신자 u는 자신의 비밀키 d_u를 이용하여 각 세그먼트를 순서대로 복호하면서 방송을 수신한다.

$$s_{ij} \equiv z_{ij}'(z_{ij}^{d_u})^{-1} \bmod p_u$$

$$\equiv s_{ij}\beta_{G_{ij}}^{r_i} \cdot (g^{r_i})^{-1} \bmod p_u$$

$$\equiv s_{ij}\beta_u^{r_i} \cdot (g^{r_i})^{-1} \equiv s_{ij} g^{d_u r_i} \cdot g^{d_u r_i^{-1}}$$

$$\equiv s_{ij}$$

[Step 5] Tracing

부정자 추적은 pirate decoder가 입수된 경우, 또는 컨텐츠 자체가 불법 재배포된 경우, 두 가지 측면에서 모두 가능하다.

(1) Pirate decoder를 입수할 경우:

컨텐츠 제공자는 모든 부정자를 찾기 위해 다음의 식을 n번 반복 수행한다.

① 공개값 β와 동일한 α_u를 다음과 같이 구한다.

$$\alpha_u \equiv \beta \bmod M_u$$

$$\beta = \sum_{u=1}^{n} \beta_u M_u y_u \pmod{M}, M_u = M/p_u$$

$$M = p_1 \cdots p_n,\ M_u y_u = 1 \pmod{p_u}, 1 \le u \le n$$

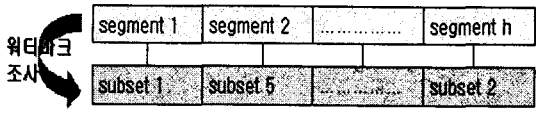
② 임의의 평문 P_x을 선택하여 (α_u, g, M_u)로 암호화한다.

$$z_{ij} \equiv g^r,\ z'_{ij} \equiv P_x \alpha_u^r \bmod M_u$$

③ z'_{ij}를 black-box decoder에 입력하여 출력값으로 원 컨텐츠 P_x을 얻지 못하면 사용자 u는 부정자이다.

(2) 복호된 컨텐츠에 대한 부정 사용이 있을 경우:

이 경우는 실시간 on-line feedback을 통해 부정자를 추적한다. 그러므로 실시간 방송 중에 부정 재전송 컨텐츠가 발견되면, 컨텐츠의 각 세그먼트에서 워터마크를 추출하여 증거로 채택하고, 해당 그룹을 찾는다. 추출된 워터마크와 연결된 그룹들의 관계를 조사하면 모든 부정자들을 추적할 수 있다.



$$\therefore sub1 \cap sub5 \cap \ldots \cap sub2 \cong T = \{traitors\}$$

<그림1> 불법 재전송된 컨텐츠에서의 부정자 추적

4. 제안 방식의 고찰

제안 방식에서 사용된 암호 알고리즘 및 워터마킹 알고리즘은 안전하다고 가정한다.

(1) 키 유출에 대한 부정자 추적 기능 제공

제안 방식은 sequential traitor tracing 기법과는 달리 pirate decoder를 발견했을 경우에도 모든 부정자를 추적할 수 있다. (제안방식의 step 5 참조)

(2) 컨텐츠 자체의 불법 재배포에 대한 부정자 추적 기능

제안 방식은 일정 정도의 세그먼트를 보면 사용자를 특정할 수 있도록 각 사용자에게 다른 워터마크를 할당하는 방법을 사용하였으므로 컨텐츠가 복호된 후 불법 재배포가 행해져도 부정자를 추적할 수 있다.

(3) Long-lived Key

제안 방식은 또한 사용자의 탈퇴나 가입 등으로 그룹 구성원의 변경이 있더라도 사용자들은 자신의 키 변경없이도 이용 가능하다. 즉 분배자만 사용자의 공개키를 이용하여 컨텐츠 암호화키를 다시 생성하면 되므로 사용자는 편리하게 시스템을 이용할 수 있다. 이 때 컨텐츠 제공자는 탈퇴자 또는 부정자의 공개키 값을 제외하거나, 가입자의 정보를 새로 추가하여 암호화키를 만들 수 있다.

5. 결론

본 논문에서는 부정자 추적 기법을 이용한 디지털 방송용 컨텐츠 보호 시스템 모델을 구성하였다. 제안 방식에서는 원본 컨텐츠에 대한 재전송을 효과적으로 막을 수 있는 방식[6]과 암호화 방식[7]을 수정·적용하여 컨텐츠 자체의 불법 재배포에 대한 부정자 추적 기능뿐 아니라 키 유출에 대한 부정자 추적 기능, 그리고 사용자의 가입과 탈퇴시 비밀키의 재생성이 필요없는 long -lived한 속성까지 제공하는 부정자 추적 기법을 제안하였다. 이는 방송용 컨텐츠 보호 시스템에 하나의 모델이 될 것이라 기대된다. 그러나 제안한 방식은 컨텐츠 제공자가 삽입된 워터마크 및 사용자의 할당 테이블을 알고 있는 대칭형 구조로 부인방지와 관련된 문제가 발생할 수 있으므로 앞으로 이 부분을 연구할 필요가 있다.

참고문헌

[1] B.Chor, A.Fiat and M.Naor, "Traitor tracing", Proceedings of Crypto, LNCS 839, p.257-270, 1994

[2] B.Pfitzmann, "Trial of Traced Traitor",Workshop on Information Hiding, LNCS 1174, 1996

[3] D. Boneh and M. Franklin., "An Efficient Public Key Traitor Tracing Scheme", Proceedings Crypto 99, LNCS 1666, p.338-353, 1999

[4] K.Kurosawa and Y.Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes", Proceeding EuroCrypto 98, LNCS 1403, p.145-157, 1998

[5] A.Fiat and T.Tassa, "Dynamic Traitor Traci ng", Proceedings Crypto 99, p.354-371, 1999

[6] R.Safavi-Naini and Y.Wang, "Sequential Traitor Tracing", IEEE Trans. on Information Theory, Vol.49, No.5, MAY 2003.

[7] Yuh-Dauh Lyuu and Ming-Luen Wu. "A Fully Public-Key Traitor-Tracing Scheme." WSEAS Transactions on Circuits, 1, Issue 1, 2002, 88--93.