한국항행학회 논문지 제12권 제3호 2008년 6월

임베디드 시스템에서 효율적인 키 갱신을 적용한 Traitor Tracing

A Traitor Tracing Using an Efficient Key Renewal in Embedded System

박종혁*, 이덕규**, 여상수***, 김태훈****, 이 승*****, 조성언******

Jong Hyuk Park*, Deok-Gyu Lee**, Sang-Soo Yeo***, Tai-hoon Kim****, Seung Lee***** and Seong-eon Cho******

요 약

브로드캐스트 메시지가 전송되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 먼저 세션키를 복호화하고 이 세션키를 통하여 디지털 정보를 얻게 된다. 이와 같이 사용자는 브로드캐스터가 전송하는 키를 이용하여 메시지나 세션키를 획득하게 되는데, 이러한 과정에서 브로드캐스터가 키를 생성하고 분배하는 과정이 필요하다. 또한 사용자가 탈퇴나 새로운 가입 시에 효율적인 키 갱신이 필요하게 되며 사용자의 악의적인 행동이나 기타 공격자에 대한 공격에 대해 추적하고 확인할 수 있어야 한다. 이를 실현할 수 있는 방식이 Traitor Tracing 방법으로 본 논문에서는 공격자 확인과, 추적을 행할 수 있으며, 키 생성에서 각 사용자의 키가 효율적인 갱신 주기를 가질 수 있도록 Proactive 방식을 이용하여 제안한다.

Abstract

If the broadcast message is sent, first of all, the privileged users will decode the session key by using his or her personal key, which the user got previously. The user willget the digital information through this session key. As shown above, the user will obtain messages or session keys using the keys transmitted from a broadcaster, which process requires effective ways for the broadcaster to generate and distribute keys. In addition, when a user wants to withdraw or sign up, an effective process to renew a key is required. It is also necessary to chase and check users' malicious activities or attacking others. This paper presents a method called Traitor Tracing to solve all these problems. Traitor tracing can check attackers and trace them. It also utilizes a proactive way for each user to have effective renewal cycle to generate keys.

Keywords : Broadcast Message, Embedded System, distribution keys

* 경남대학교 컴퓨터공학부(Dept. of Computer Science and Engineering)
** 한국전자통신연구원 보네트워크보안연구팀(ETRI, HomeNetwork Security Research Team)
*** (주)BTWorks 연구팀장
**** 한남대학교 멀티미디어학부(Dept. of Multimedia, Hannam Univ.)
***** 대림대학 자동화시스템과(Dept. of Automated Systems, Daelim College)
****** 순천대학교 정보통신공학부(Division of Iformation Communication, Sunchon National Univ.)
· 교신저자 (Corresponding Author) : 조성언
· 접수일자 : 2008년 4월 15일

I. 서 론

키를 제공하는 방식 중에 하나인 공개키 방식은 세션키를 암호화하기 위한 그룹의 암호화키는 하나이고 이를 복호하기 위한키는 여러 개의 무수히 많은 키를 이용함으로써 서버는 세션키를 암호화하고 각 사용자에게는 서로 다른 키를 이용하여 복호화 할 수 있도록 되어 있다[3][4][7][8].

브로드캐스트 암호화 기법에서 중요한 것은 오직 사전에 허가받은 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전달되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 디지털 정보를 얻게 된다. 브로드캐스트 암호화에 있어 가장 중요한 것은 키 생성, 분배, 갱신이다.

하지만 이러한 브로드캐스트 암호화 기법에서도 사용자가 키를 악의적인 목적을 가지고 이용하였을 경우에는 불법적인 사용자가 누구인지 추적이 어렵게 된다. 불법사용자의 추적은 사용자가 알 수 없는 간단한 디지털 정보를 숨겨서 불법 복제자가 누구인지를 추적하게 하는 기법이다. 본 논문에서는 불법 복제를 하기 위해 결탁하거나 기타 행위를 하는 사용자를 불법 사용자라고 부르고 이러한 불법 사용자를 찾아내는 기법을 불법 사용자 추적 기법이라 하겠다.

본 논문에서는 임베디드 시스템에서 불법 사용자를 추적함에 있어 사전에 최대한 사용자의 불법 행위를 방지하기 위해 사용자에게 제공되는 키에 proactive 방식을 적용하였으며, 이를 바탕으로 사용자가 불법적인 행위를 하였을 경우 효율적으로 불법 사용자를 추적할 수 있도록 제안하였다. 이는 새로운 형태의 불법 사용자 추적 기법을 제안을 의미한다. 제안 방식에서 브로드캐스트 메시지는 권한블록, 암호블록으로 구성된다. 또한 사용자가 등록과 더불어 개인키를 제공 받음에 있어 공격자로부터 효율적으로 키를 변형하고 후에 불법 사용자 추적에 있어 고유한 사용자에서 불법 사용자를 추출하는데 더욱 효과적이도록 설계하였다.

본 논문은 임베디드 시스템, 브로드캐스트 암호화와 불법 사용자 추적의 개요를 살펴 본 후, 제안 방식의 각 단계에 관하여 살펴본다. 또한 제안 방식 분석을 통하여 제안 방식에 대해 고찰하며, 마지막으로 결론을 맺도록 한다.

Ⅱ. 임베디드 컴퓨팅과 불법 사용자추적 개요

2-1 브로드캐스트 암호화 개요

브로드캐스트 암호화는 한명의 송신자와 다수의 수신자간의 프로토콜이다. 즉 송신자는 하나의 암호화키를 갖고 있고 메시지를 암호화해서 브로트캐스트하면 정당한 수신자만이 암호문을 복호화 할 수 있는 키를 갖고 있어서 그 메시지를 얻을 수 있다. 브로드캐스트 암호화는 컨텐츠 제공자가 암호화된 형태로 수많은 정보를 전송하고 정당한 사용자만이 암호화된 정보를 복호화 할 수 있게 하는 많은 시나리오에 적용될 수 있다. 전형적인 예로, Pay-TV를 들 수 있으며 많은 브로드 캐스트 암호화 기법들이 제시되고 있다. 최초로 제시되었던 Cho외 2명이 제안한 브로드캐스트 암호화 기법은 다음과 같이 세단계로 구성된다[1][5][6][9]~[13](그림 1 참조)

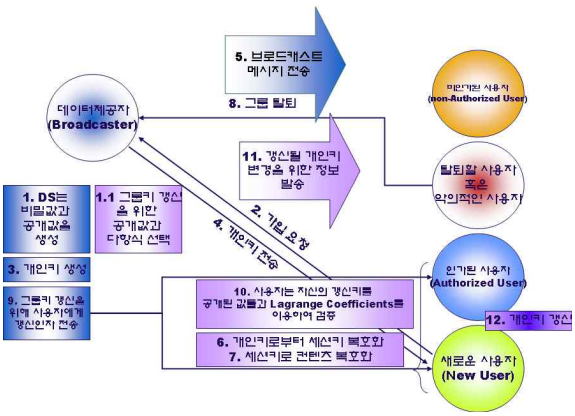

그림 1. 브로드캐스트 암호화 개요
Fig 1. Overview of Broadcast Encryption

- 컨텐츠 제공자 초기화: 컨텐츠 제공자는 모든 사용자들에게 필요한 정보를 생성하고 이것을 초기 기록이라 명명한다.
- 사용자 초기화: 개개인의 사용자들은 컨텐츠 제공자에게 등록하는 단계이다. 이 단계 후 사용자가 저장하는 정보는 사용자의 개인키(Personal Key)이고 컨텐츠 제공자는 각 사용자 초기화 단

계 후에 각 사용자에 대한 초기 기록을 갱신한다.

- 세션 송신: 컨텐츠 데이터는 세션키로 암호화 되고 이 세션키는 세션이라 부르는 작은 부분들로 분할되어 전송된다. 이 때 각 세션은 각각 다른 부분 세션키로 암호화되어 전송되고 정당한 사용자들이 자기들의 개인키를 가지고 부분 세션키를 복호화 할 수 있게 함으로써 실제 데이터를 얻을 수 있게 해주는 세션키를 얻게 한다.

2-2 불법 사용자 추적 개요

불법 사용자 추적은 복제와 분배와 같은 불법적인 사용자를 찾는데 목적을 가진다. 사용자가 알 수 없는 간단한 디지털 정보를 숨겨서 불법 사용자가 누구인지를 추적하게 하는 기법으로 불법 복제를 하기 위해 결탁이나 기타 불법 행위를 하는 사용자들을 불법 사용자라고 칭하고 이러한 불법 사용자를 찾아내는 기법을 불법 사용자 추적 기법이라 한다. 불법 사용자 추적을 통해 불법 복제등과 같은 불법 행위를 차단할 수 있고 그에 따라 디지털 정보의 흐름은 원활히 이뤄질 수 있을 것이다.

불법 사용자 추적 기법의 기본적인 방법과 필요한 사항을 간략히 설명하면 다음과 같다.(그림 2 참조)

- 불법 사용자 추적 기법의 기본 방법 : 불법 사용자를 찾는 기본적인 방법은 디지털 정보를 암호화 한 뒤 등록되어 있는 각각의 사용자들에게 전송해주게 된다. 정당한 사용자들은 암호화된 디지털 정보를 복호화 하여 원래의 디지털 정보를 볼 수 있게 해주는 디코더를 가지고 있게 된다. 불법 사용자는 암호화된 디지털 정보를 복호화 할 수 있는 불법 디코더(Pirate Decoder)를 만든 뒤 자신에게 등록된 사용자에게 나눠주게 된다.

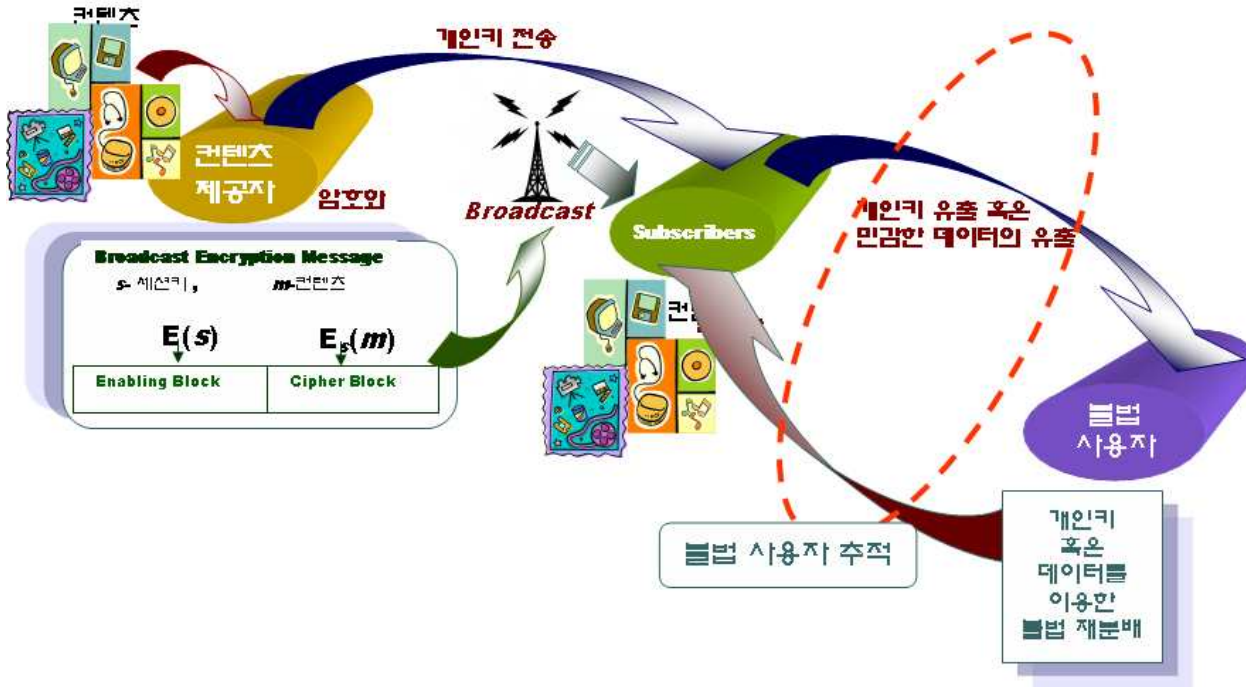

그림 2. 불법 사용자 추적 개요
Fig 2. Overview of Illegal User Trail

불법 사용자 추적은 이러한 불법 디코더를 찾는 것이다.

하지만 위와 같은 불법 디코더를 찾는 방법에는 문제가 있다. 암호화된 디지털 정보를 복호화 할 수 있는 불법 디코더를 사용하지 않고 정당한 디코더를 통해 원래의 디지털 정보를 복호화한 후 그 디지털 정보를 불법 사용자에 의해 재분배를 통해 전송하거

나 복호화 하는 키를 인터넷 등을 통해 공개하게 된다면 위와 같은 불법 디코더를 찾아내는 방법은 사용될 수 없다. 이러한 경우에는 디지털 정보 내에 추적할 수 있는 특정한 정보를 삽입하여 해결할 수 있다. 디지털 정보에 정보를 삽입한 뒤 불법 전송이 발생하게 되면 그 안에 숨겨진 정보를 통해서 누가 불법 행위를 하는지 찾게 된다.

- 첨가되는 정보의 안전성: 불법 사용자를 찾아낼 때 디지털 정보 안에 사용하게 될 정보로 인해 디지털 정보 자체가 변화할 수 있다. 정보를 첨가시켜도 원래의 디지털 정보의 내용이 거의 변화가 없는 방법이 사용되어야만 불법 사용자가 정보가 첨가돼 있다는 사실을 알 수 없게 된다. 또한 디지털 정보의 내용을 변경하는 등의 행위를 통해 첨가된 정보를 고치거나 제거할 수 없어야 한다.
- 불법 사용자에 대한 탐지: 디지털 정보 안에 정보를 삽입한 뒤, 삽입한 정보를 통해 불법 사용자를 추적할 때 정당한 사용자를 불법 사용자로 오인할 수 있는 경우가 발생할 수 있다. 정당한 사용자를 잘못하여 불법사용자로 만든다면 큰 문제점이 될 수 있다. 모든 불법 사용자는 찾아내지만 정당한 사용자를 잘못 고발하지 않는 그러한 기법을 사용할 필요가 있다.

이러한 정보에 대한 기술로는 디지털 워터마킹(watermarking)을 사용할 수 있는데, 디지털 워터마킹은 디지털 정보 내에 특정한 정보를 삽입하는 기술로 포함되는 정보는 원본 디지털 정보의 내용을 거의 손상시키지 않고, 필요할 때는 추출할 수 있다.

Ⅲ. 기존 방식

본 장에서는 우선 제안방식에 기본이 되는 ChFN의 구조를 간략하게 설명한다.

컨텐츠 제공자 설정 단계에서는 우선 컨텐츠 제공자는 b개의 키를 갖는 l개의 집합을 생서한다. 단 $l > k$이고 $b^l > N$이다. 여기서 k공모자들이 공모할 수 있는 공모자 수에 대한 상한이고 N 사용자의 수이다. 아래 표기에서 i번째 집합은 $key_{i,1},...,key_{i,b}$로 표기한다.

사용자 설정단계는 각각의 사용자는 제공자가 생성한 l개의 집합으로부터 하나씩의 키를 획득하게 된다. 사용자들은 자신만의 id에 대응하는 codeword $(c_1,c_2,....,c_l) \in \{1,...,b\}^l$에 대응하는 개인키 key_{1,c_1}, ... key_{l,c_l}를 획득하게 된다. 세션 송신 단계는 컨텐츠 제공자는 각 세션키를 S를 l개의 랜덤한 부분 세션키 $S_1,S_2,...,S_l$의 값을 $\oplus$를 하여 만든다. 모든 집합들에 대하여 세션 불럭은 i번째 집합에 있는 키들을 가지고 각각의 부분 세션키 S_i를 암호화한 값으로 구성된다. 사용자들은 각 i번째 집합에 대응하는 하나의 키들을 갖고 있기 때문에 b개의 암호문 중에서 하나를 복호화 할 수 있고 따라서 전체 세션키 S를 얻어냄으로써 실제 컨텐츠를 세션키를 이용해 얻어 낼 수 있다.

공모자 추적은 추적을 하기 위한 기본적인 가정으로 우선 컨텐츠 제공자가 불법 디코더를 열어보고 각 집합으로부터 하나의 키를 발견할 수 있다는 것이다. 만약 불법 디코더가 공모자들이 자신들의 키를 조합해서 만든 불랙박스와 같은 형태로 주어진다면 다음과 같은 절차에 의해 집합 i에서 사용된 하나의 키의 인덱스를 알아낼 수 있다. 집합 i안의 키의 인덱스 $j = 1,2,...,b-1$에 대해서 컨텐츠 제공자는 세션블럭을 j번째까지는 집합 i에 있지 않은 랜덤한 키를 사용해서 암호화를 하고 j이후는 집합 i에 있는 키들을 가지고 암호화를 한다. 이 권한블럭을 입력을 넣어 많은 테스트를 시행해서 각 j에 대해 올바르게 복호화가 될 확률이 $j-1$에 대해 올바르게 복호화될 확률인 기준 임계치보다 작다면 컨텐츠 제공자는 $key_{i,j}$가 불법 디코더안에 있다고 결론짓는다. 키를 찾은 후의 추적은 다음과 같은 기본적인 원리로 진행된다. 만약 k명의 공모자들이 불법 디코더를 만들기 위해 l개의 키들을 제공했다면 k명의 공모자중에서 적어도 한명은 $1/k$개의 키들을 제공해야만 한다. 컨텐츠 제공자는 불법 디코더 안에 $1/k$개 이상의 키가 존재하는 사용자들을 공모자로 간주한다.

Ⅳ. 제안 방식

제안방식은 컨텐츠 제공자와 n명의 사용자로 구성되어 있다. 각 사용자들은 개인키를 전송받게 되는데, 개인키는 권한 블록에 포함된 세션키를 복호화하는데 필요하며, 개인키는 각 사용자에게 3개씩 전송되며 이는 사용자가 컨텐츠 제공자간에 동기화를 통해 브로드캐스트 메시지를 해당 개인키로 복호화하게 된다. 전체 사용자 3명을 A, B, C라 보았을 때, A에게 전송되는 키는 i-3, i-2 , i-1이 되고, B에게 전송되는 키는 i-1, i, i+1이 되며, 마지막으로 C의 키는 i+1, i+2, i+3이 된다. 다음과 같이 사용자에게 키를 3쌍씩 나눠주는 것은 두 가지의 목적을 가진다. 우선 각 사용자의 키를 주기적으로 반복시켜 공격자로부터 사용자의 키를 동일하게 사용하지 않는 목적을 가지고, 다음은 사용자가 불법적인 목적으로 사용되었을 경우 키 쌍은 전체적으로 이동하게 된다. 이 때 불법적인 목적을 가지고 사용되었다면 불법적으로 사용된 키가 교집합으로 형성되게 되며, 이에 대한 정확한 불법 사용자를 추적할 수 있게 된다. 다음은 제안 방식의 단계과 가정에 대해 살펴본다.(그림 3 참조)

초기 단계 : 시스템 변수를 설정하는 단계로써 컨텐츠 제공자는 참여할 사용자 수를 예측하고 공개키와 개인키를 생성하게 되는데, 사용자의 수보다 3배 많은 키를 구성한다.

등록 단계 : 컨텐츠 제공자와 디지털 정보를 수신하기 원하는 사용자 사이에 진행되는 프로토콜로써 이때 사용자는 컨텐츠 제공자로부터 키 쌍을 받게 된다.

그림 3. 제안 방식 흐름도

Fig 3. Flowchart of Proposed Method

브로드캐스트 메시지 암호화 단계 : 브로드캐스트 암호화 메시지를 생성하는 단계로서 사용자는 컨텐츠 제공자와 우선 사용할 키에 대해 동기화를 한다. 전송되는 브로드캐스트 메시지가 불법적으로 사용되

어졌다면, 불법 디코더 내에 포함되는 복호화 키는 컨텐츠 제공자가 각 사용자에게 분배한 개인키 중 하나일 것이다.

복호화 단계 : 각 사용자는 자신의 개인키를 이용한 복호화 과정을 통하여 브로드캐스트 메시지로부터 디지털 정보를 획득하게 된다. 이때 사용자는 자신이 가진 키에 대해 분별할 수 없으며 사용자는 자신의 키 쌍을 이용하여 복호만 가능하다.

키 갱신 단계 : 컨텐츠 제공자는 새로운 다항식을 값을 이용하여 키 변경과 관련된 정보를 브로드캐스트하고 각 사용자는 전송받은 값을 이용하여 자신의 개인키를 변경한다. 이때 사용자는 자신이 가지고 있는 3개에 키 쌍에 대해 각각 수행되며, 사용자가 선택할 수 없고 자동적으로 진행된다.

불법 사용자 추적 및 사용자 탈퇴 단계 : 컨텐츠 제공자가 불법 디코더를 발견하면 불법 사용자를 찾기 위해 브로드캐스트 메시지를 디코더에 입력하여 키 갱신이 진행되도록 한다. 불법 디코더는 이것이 키 갱신을 위한 것인지 불법 사용자 추적을 위한 것인지 구별 할 수 없다. 또한 불법 사용자의 키 쌍 중에서 2개가 동시에 나타나는 사용자는 불법 사용자임을 확실히 알 수 있게 된다.

4-1 기본 배경

본 제안방식은 방송, 컨텐츠 제공과 같은 컨텐츠 유포에 있어 다수에 전송하는 시나리오를 토대로 진행된다. 컨텐츠를 제공하고 이를 암호화한 후 사용자에게 제공하는 방식은 기존의 방식과 동일하게 진행된다. 하지만 여기서 불법 사용자 추적에 있어 두 사용자로 나뉘어 질수 있는데, 우선 첫 번째 불법 사용자는 불법 디코더를 획득하여 이를 통해 불법적인 행위를 하는 사용자이고, 두 번째 사용자는 불법 디코더를 사용하지 않고 획득한 컨텐츠를 이용하여 불법적인 유통시킨 사용자로 분리할 수 있다. 우선 앞서 언급한 불법 사용자의 경우는 다시 2부분으로 분리할 수 있다. 하나의 경우는 불법 디코더 제작자와 사용자가 결탁하여 불법 디코더를 만드는 경우이고, 다른 하나의 경우는 불법 사용자가 통신로상의 정보를 획득하여 이를 바탕으로 제작하는 경우이다. 결탁의 경우 본 제안방식에서 사용자에게 키를 3개씩 나눠줌으로써 이를 이용하여 결탁 공모자를 추적할 수 있으며, 통신로상의 정보를 계속적으로 변화시키기 위해 3개의 키를 이용하여 사용자와 컨텐츠 제공자 사이에 동기화를 통해 키를 변경 시킬 수 있다. 이러한 경우를 제외하고 불법 사용자가 컨텐츠를 획득하여 이를 이용하여 불법적인 유통을 시키는 경우는 본 제안방식에서 설명하지 않고 기존 DRM(Digital Rights Management)등과 같은 컨텐츠 보안에서 참조하는 것으로 한다.

4-2 제안방식 흐름

본 제안 방식은 다음과 같은 특징을 가지고 있다. 우선 컨텐츠 제공자는 시스템 알고리즘과 그와 관계된 변수를 설정하는데 사용자의 키를 쉽게 갱신하고 불법 사용자로부터 사용자의 키를 안전하게 보관할 수 있도록 갱신 인자를 삽입하고 사용자들은 후에 컨텐츠 제공자에 등록하며 이때 할당되어있는 개인키를 전송받게 된다. 후에 컨텐츠 제공자는 메시지를 브로드캐스트 하고자 할 때 브로드캐스트 될 데이터를 세션키로 암호화한 암호문과 정당한 개인키를 가지고 있는 사용자만이 세션키를 획득하도록 권한블록을 구성한다. 사용자는 메시지를 획득하기 위해 자신이 가지고 있는 개인키를 이용하여 복호화할 수 있다. 브로드캐스트 암호화 메시지를 전송하고 복호화하는 단계에서는 사용자와 서버간의 키 사용에 따른 동기를 맞추도록 한다. 컨텐츠 제공자가 불법 사용자를 발견하였을 경우, 사용된 개인키에 발급받은 사용자를 결정하고자 한다면, 정당한 사용자들이 자신들의 개인키를 조합해서 정당하지 않은 개인키를 만들어서 브로드캐스트 된 데이터를 복호화 할 수 있는 경우 컨텐츠 제공자는 새롭게 만들어진 메시지의 입력과 출력사이의 관계를 살핌으로써 사용된 캐인키를 알 수 있다.

사용자들의 최대 불법 수는 k이고 발견된 불법 사용자자들에 대한 추출 임계치는 z(즉, 불법 사용자의 개인키가 3개씩 설정되어 있으므로 사용자를 확실히 구분지을 수 있다.) 큰 소수인 위수 q를 갖는 그룹 G_q 이다.

4-2-1 초기화 단계 및 브로드캐스트 메시지 암호화/복호화 단계

Step 1. 컨텐츠 제공자는 사용자($i=1,\cdots,2u+2$)를 예측하여 이에 대해 랜덤수(β)를 선택한다. 이때 사용되는 랜덤수는 사용자의 키를 갱신하기 위한 갱신인자로 사용된다.

Step 2. 컨텐츠 제공자는 Z_q상에서 계수 z를 갖는 다항식 $f(x)=\sum_{t=0}^{z}\beta_t a_t x^t$를 선택한다. 컨텐츠 제공자는 다항식을 비밀키로 하고 공개키를 다음과 같이 설정하고 모든 사용자들에게 공개한다.

$$\langle g, g^{\beta_0 a_0}, g^{f(1)}, \ldots, g^{f(2z+2)} \rangle \text{ 공개}$$

Step 3. 컨텐츠 제공자는 사용자가 등록할 때 컨텐츠 제공자는 사용자에게 개인키 $((i,f(i-1)),(i,f(i)),(i,f(i+1)))$를 전송한다. 사용자는 자신이 받은 키가 정확한 값인지 검증을 시행한다. 이때 컨텐츠 제공자는 첫 번째 키로서 검증을 수행하도록 유도한다. 사용자에게 키와 함께 동기화 과정에서 갱신할 수 있는 값을 같이 전송한다.

$$g^{\beta_0 a_0} = \prod_{t=0}^{z} g^{f(x_t)\lambda_t}, \quad (1)$$

단 $x_0=1, x_2=2, \ldots, x_{2z+1}=z, x_{2z+2}=i$이다.

Step 4. 컨텐츠 제공자는 사용자와 통신을 개시하기 전에 사용자와의 동기화 과정을 행하고, 이에 사용자는 최초 받은 갱신값을 이용하여 자신의 개인키를 갱신하고 이를 바탕으로 사용하게 된다. 이와 같은 과정이 종료되면, 컨텐츠 제공자는 사용되지 않은 정보를 선택하고 랜덤수 $r \in Z_q$를 선택한 뒤 권한 블록을 계산한다.

$$C = \langle sg^{r\beta_0 a_0}, g^{r\cdot}\left(j_1, g^{rf(j_1)}\right), \ldots g^{r\cdot}\left(j_z, g^{rf(j_{2z+2})}\right) \rangle \quad (2)$$

$$(j_1,f(j_1)), (j_2,f(j_2)), \ldots, (j_{2z+2},f(j_{2z+2})),$$

그리고 메시지를 세션키로 암호화 한 뒤 C와 암호화한 메시지를 전송한다.

Step 5. 사용자는 컨텐츠 제공자로부터 받은 C와 암호화한 메시지로부터 세션키를 획득하는 과정은 다음과 같다.

$$s = sg^{r\beta_0 a_0} / \left[\left(g^r\right)^{f(i)\lambda_z} \circ \prod_{t=0}^{z-1} \left(g^{rf(x_t)}\right) \right], \quad (3)$$

단 $x_0=j_1, x_2=j_2, \ldots, x_{2z+1}=j_{2z+2}, x_{2z+2}=j_i$이다.

4-2-2 키 갱신 단계

Step 1. 사용자 j가 컨텐츠 제공자에게 탈퇴요청

Step 2. 컨텐츠 제공자는 기존 사용자의 개인키를 갱신하기 위해 갱신요소인 β에서 사용자 j의 갱신요소를 제거

Step 3. 컨텐츠 제공자는 탈퇴 사용자의 갱신요소를 제거한 후 개인키를 갱신하고 사용자에게 전송한

각 사용자에게 키 쌍 3개를 전송하였으므로 갱신에 해당하는 $B=(\beta_{i-1},\beta_i,\beta_{i+1})$의 3개에 해당하는 공유정보들을 고정하고 사용되지 않은 공유 정보를 이용하여 권한 블록을 구성하게 되면 사용자 j는 사용할 수 없게 된다.

$$\left(\beta_{i-1}, g^{rf(\beta_{i-1})}\right), \ldots, \left(\beta_{i+1}, g^{rf(\beta_{i+1})}\right) \Rightarrow \left(j_1, g^{rf(j_1)}\right), \ldots, \left(j_{z-3}, g^{rf(j_{z-3})}\right) \quad (4)$$

4-2-3 공모자 추적 단계

공모자 추적은 키 갱신 과정에서 WGT가 제안한 방법을 적용한다 WGT에서는 두가지 공모자 추적 방식을 제안하고 있는데 이 방식을 제안 방식에 맞추어 설명한다.

Step 1. 컨텐츠 제공자는 불법 사용자로 추정되는 사용자 집합 $\{c_1, c_2, \ldots, c_m\}, (m \le k)$를 구성한다.

Step 2. 불법 사용자를 추적하기위해 정보를 권한 블록에 다음과 같이 첨부한다.

$$\langle sg^{r\beta_0 a_0}, g^{r\cdot}\left(c_1, g^{rf(c_1)}\right), \ldots g^{r\cdot}\left(c_m, g^{rf(c_m)}\right) \rangle \quad (5)$$

다른 방법은 불법 사용자만이 권한 블록을 복호화 할 수 있는 방식으로 컨텐츠 제공자는 $\{(c_1,f(c_1)),\ldots,(c_m,f(c_m))\}$를 해의 일부로 하고 나머지 근들은 $f(x)$와 일치하지 않는 새로운 다항식

$h(x)$를 선택한다.

이렇게 하고 불법 사용자가 발견된 후에 컨텐츠 제공자는 불법 사용자의 키를 사용해서 만들어진 불법 개인키들이 브로드캐스트 된 데이터를 복호화 할 수 없게 할 수 있다. $\{c_1, c_2, \cdots, c_m\}, (m \le k)$가 컨텐츠 제공자에 의해 찾아진 공모자들이라 하고 그들의 공유 정보를 다른 사용자들의 개인키들을 바꾸지 않으면서 다음과 같은 방법에 의해 추출할 수 있다. 컨텐츠 제공자는 권한 블록의 처음 m개의 공유정보들을 $\left(c_1, g^{rf(c_1)}\right), \ldots, \left(c_m, g^{rf(c_m)}\right)$으로 고정하고 나머지 $z-m$개의 사용되지 않은 공유정보 $\left(j_1, g^{rf(j_1)}\right), \ldots, \left(j_{z-m}, g^{rf(j_{z-m})}\right)$로 권한 블록을 구성한다.

Ⅴ. 제안 방식 분석

본 논문에서는 기존의 방식보다 효율적인 키 생성과 키 갱신을 위한 브로드캐스트 암호화 방식과 함께 사용자 추적을 위해 사용자에게 키 쌍을 제공하는 방식을 제안하였다. 본 제안 방식들의 안전성은 이산대수의 문제에 기반을 두고 있다. 기존의 방식에 비해 사용자의 참여, 키 갱신, 사용자의 탈퇴 혹은 연산량에 있어 효율성을 나타내고 있다. 본 장에서는 제안 방식에 대해 고찰한다.

5-1 키 갱신

기존 KPS(Key Predistribution Scheme)에서는 키가 생성되고 분배가 되어진 후 이를 이용하여 암호화하여 메시지를 전송하게 된다. 전송된 메시지를 사용자가 확인한 후 한 세션이 종료되면 키를 새로 생성하여 전송되거나, 키에 대하여 공격이 이루어진 경우 키를 갱신하지 아니하고 전체적으로 다시 생성하게 된다. 하지만 제안 방식들에서는 사용자의 가입 혹은 탈퇴가 발생하면 기존 사용자들의 키를 갱신하고 사용이 가능하다. 키 갱신은 초기 키 생성 시에 키 갱신 요소인 β 인자를 삽입하게 된다. 차후 사용자 탈퇴/강제 탈퇴 등과 같은 상황이 발생되면 서버는 탈퇴자의 키 갱신 정보인 β 인자를 삭제하고 제공함으로써 사용자는 간단한 연산으로 키 갱신을 마치게 된다.

5-2 초기 예측 오류에 따른 재연산

제안 방식의 경우 서버가 시스템을 설정하고 관리해야한다. 만일 서버가 유동적인 사용자를 관리한다면 사용자에 대한 예측이 올바르게 이뤄져야한다. 그러므로 서버는 초기 예측에 대한 오류가 발생하였을 경우 재연산이나 혹은 추가 연산을 실시해야 한다. 하지만 기존 방식의 경우에서는 이러한 사용자 예측 오류에 대하여 수행할 수 있는 연산이 없다. 본 논문에서 제공하는 방식에서는 서버가 시스템을 설정하는데 사용자에 대한 예측 연산을 원활히 할 수 있도록 r과 같이 연산을 통해 이뤄질 수 있도록 제안하였다. 또한 랜덤한 수 r에 대해서는 Z_q상에서 생성하게 되며 r에 대해서 사전에 예측 사용자보다 많은 수를 만들면 해결할 수 있다.

5-3 선택 암호문 공격에 대한 안전한 스킴

적응적 선택 암호문 공격에 안전한 암호시스템을 설계할 수 있는 것은 매우 좋은 성질로써 본 절에서는 Boneh와 Franklin의 방식과 유사한 방식으로 제안 방식의 변형을 가함으로써 적응적 선택 암호문 공격에 안전한 불법 사용자 추적 스킴을 제안한다.

컨텐츠 제공자는 Z_q위에서 z를 갖는 다항식 $f(x) = \sum_{t=0}^{z} \beta_t a_t x^t$를 선택하며, $a, b, x_1, x_2, y_1, y_2 \in Z_q$를 선택한다.

컨텐츠 제공자의 비밀키는 $\langle f(x), a, b \rangle$이고 공개키는 $\langle g, g^{\beta_0 a_0}, g^{f(1)}, \ldots, g^{f(z)}, g^{r\beta a}, g^{r\beta b}, c, d, H \rangle$로 모든 사용자에게 공개한다. 사용자가 컨텐츠 제공자에게 등록할 때 컨텐츠 제공자는 사용자에게 개인키를 제공한다. 사용자는 받은 키가 정확한 값인지 앞장과 동일한 방법으로 검증한다. 컨텐츠 제공자는 랜덤하게 z개의 사용되지 않은 공유정보를 선택하고 이를 바탕으로 권한 블록을 계산한다. 사용자는 브로드캐스트된 권한 블록으로부터 개인키를 이용해 세션키를 획득한다. 검증이 성공하면 선택 암호문 공격에 안전함을 알 수 있다.

Ⅵ. 결 론

브로드캐스트 암호화 기법은 공개된 네트워크상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다. 브로드캐스트 암호화 기법에서는 중요한 것은 오직 사전에 허가된 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전송되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 디지털 정보를 얻게 된다. 이와 같이 사용자는 브로드캐스터가 전송하는 키를 이용하여 메시지나 세션키를 획득하게 되는데, 이러한 과정에서 브로드캐스터가 키를 생성하고 분배하는 과정이 필요하다. 또한 사용자가 탈퇴나 새로운 가입 시에 효율적인 키 갱신이 필요하게 된다. 인가된 사용자이외에는 브로드캐스트 되는 메시지에 대해 아무런 정보를 얻어낼 수 없으며, 인가된 사용자는 사전에 전송된 개인키를 이용하여 세션키를 취득할 수 있게 된다. 본 논문에서는 불법 사용자를 추적함에 있어 사전에 최대한 사용자의 불법 행위를 방지하기 위해 사용자에게 제공되는 키에 proactive 방식을 적용하였으며, 이를 바탕으로 사용자가 불법적인 행위를 하였을 경우 효율적으로 불법 사용자를 추적할 수 있도록 제안하였다. 이는 새로운 형태의 불법 사용자 추적 기법을 제안을 의미한다. 제안 방식에서 브로드캐스트 메시지는 권한블록, 갱신블록, 암호블록으로 구성된다. 또한 사용자가 등록과 더불어 개인키를 제공 받음에 있어 공격자로부터 효율적으로 키를 변형하고 후에 불법 사용자 추적에 있어 고유한 사용자에서 불법 사용자를 추출하는데 더욱 효과적이도록 설계하였다.

감사의 글

이 논문은 경남대학교 연구비 지원에 의하여 연구되었음

참 고 문 헌

[1] Amos Fiat and Moni Naor, "Broadcast Encryption", *Crypto'93*, pp. 480-491, 1993

[2] A. Narayana, "Practical Pay TV Schemes", *to appear in the Proceedings of ACISP03*, July, 2003

[3] C. Blundo, Luiz A. Frota Mattos and D.R. Stinson, "Generalized Beimel-Chor schemes for Broadcast Enryption and Interactive Key Distribution", *Theoretical Computer Science,* vol. 200, pp. 313-334, 1998.

[4] Carlo Blundo, Luiz A. Frota Mattos and Douglas R. Stinson, " Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution", *In Advances in Cryptology - Crypro '96*, Lecture Notes in Computer Science 1109, pp. 387-400.

[5] Carlo Blundo and A. Cresti, "Space Requirements for Broadcast Encryption", *EUROCRYPT 94*, LNCS 950, pp. 287-298, 1994

[6] Donald Beaver and Nicol So, "Global, Unpredictable Bit Generation Without Broadcast", *EUROCRYPT 93*, volume 765 of Lecture Notes in Computer Science, pp. 424-434. Springer-Verlag, 1994, 23-27 May 1993.

[7] Ignacio Gracia, Sebastia Martin and Carles Padro, "Improving the Trade-off Between Storage and Communication in Broadcast Encryption Schemes", 2001

[8] Juan A. Garay, Jessica Staddon and Avishai Wool, "Long-Lived Broadcast Encryption", *In Crypto 2000,* volume 1880 of Springer Lecture Notes in Computer Science, pages 333--352, 2000.

[9] Michel Abdalla, Yucal Shavitt, and Avishai Wool, "Towards Marking Broadcast Encryption Practical", *IEEE/ACM Transactions on Networking,* 8(4):443--454, August 2000.

[10] Yevgeniy Dodis and Nelly Fazio, "Public Key Broadcast Encryption for Stateless Receivers", *ACM Workshop on Digital Rights Management,* 2002

[11] R. Ostrovsky and M. youg, "How to withstand mobile virus attacks", *in Proc. 10th ACM symp. on*

principles of Distributed Computation. pp. 51-61, 1991

[12] H.K.A. Herzberg, S. Jarecki and M. Yung, "Proactive Secret Sharing or: How to Cope With Perpertual Leakage", *Crypto95,* LNCS. 1995

[13] 임채덕, 김홍남, 박승민, 김두헌, 김선자, 김채규, 임기욱, "임베디드 소프트웨어 기술동향 및 산업 발전 동향", *정보통신연구진흥지*, 4권 3호, 2002

[14] 권오혁, "Embedded System, RTOS", *삼성 SDS IT Review,* 2003

[15] 장정숙, 전용희, "임베디드 시스템 보안", *한국정보통신학회지*, 22권 8호, pp 81-97, 2005

박 종 혁(朴鍾烇)

2001년 순천향대학교 공학사
2003년 고려대학교 공학석사
2007년 고려대학교 공학박사
2002년 한화 에스엔씨 기술연구소
2007년~현재 경남대학교 컴퓨터공학부 전임강사
관심분야 : 유비쿼터스 및 RFID보안

이 덕 규(李悳揆)

2001년 순천향대학교 공학사
2003년 순천향대학교 공학석사
2006년 순천향대학교 공학박사
2006년~현재 한국전자통신연구원 정보보호연구단
관심분야 : 유비쿼터스 및 RFID보안

여 상 수(呂相壽)

1997년 중앙대학교 공학사
1999년 중앙대학교 공학석사
2005년 중앙대학교 공학박사
2006년 단국대학교 정보컴퓨터학부 강의전임강사
2007년 Kyushu University 방문연구원
2008년~현재 (주)BTWorks 연구팀장
관심분야 : 임베디드 소프트웨어

김 태 훈(金泰勳)

1995년 성균관대학교 공학사
1997년 성균관대학교 공학석사
1999년 (주)신도리코 기술연구소 연구원
2002년 성균관대학교 공학박사
2004년 한국정보보호진흥원 선임연구원
2006년 국군기무사령부 사무관
2007년 이화여자대학교 연구교수
2007년~현재 한남대학교 멀티미디어학부 조교수
관심분야 : 대형시스템정보보호, 정보보증

이 승(李 勝)

1988년 성균관대학교 공학사
1990년 성균관대학교 공학석사
2000년 성균관대학교 공학박사
1993년~현재 대림대학 자동화시스템과 부교수
관심분야 : 임베디드 시스템 설계, 자동화체계

조 성 언(趙誠彦)

1989년 한국항공대학교 항공통신정보공학과 공학사
1991년 한국항공대학교 대학원 항공통신정보공학과 공학석사
1997년 한국항공대학교 대학원 항공전자공학과 공학박사
1997년~현 재 순천대학교 정보통신공학부 부교수
관심분야: 무선통신시스템, Wireless USN