TRS 상의 Tree를 이용한 효율적인 키 분배

이덕규*, 박용석**, 안정철**, 이임영*
*순천향대학교 정보기술공학부
**국가보안기술연구소
e-mail:{hbrhcdbr, imylee}@sch.ac.kr

An Efficient Key Distribution Using Tree for TRS

DeokGyu Lee*, YongSeok Park**,JungChul Ahn**, ImYeong Lee*
*Division of Information Technology Engineering,
Soonchunhyang University
**National Security Research Institute

요 약

RS 시스템의 가장 큰 특징은 일대 다수의 그룹 및 지령 통신방식이다. TRS 시스템의 구성은 여러 개의 그룹으로 구성되며, 각 그룹은 업무내용에 관련된 유사한 목적을 가진 사용자들의 단말기로 구성된다. 다양한 형태의 공격에 노출될 수 있으며, 대규모 통신을 위한 키 분배 혹은 설정에 많은 문제점을 가질 수 있다. 본 고에서는 TRS 상에서 안전한 통신를 수행하는데 있어 필수 요소인 회의용 키 분배 방식을 고찰한다. 본 방식은 통신 회수를 줄이면서도 사용자 인증을 수행할 수 있는 효율적인 Tree 기반의 회의용 키 분배 방식을 제안한다.

1. 서론

주파수공용통신(TRS: Trunked Radio Service)란 무선통신을 하는 사람이 특정한 주파수를 전용하던 종래의 무선통신방식과는 달리 중계소에 할당된 소수의 주파수를 다수의 이용자가 공동으로 사용하는 방상을 말한다.

일정한 주파수를 전용하도록 되어 있는 기존 이동전화 등 셀룰러시스템과 달리 간선전화시스템은 독립된 각각의 채널을 하나로 묶어 다수의 이용자가 공용하도록 한 방식이다. 즉 주파수의 활용 폭을 극대화한 것을 특징으로 하는 시스템이다. 때문에 16개 채널을 이용할 때 기존 휴대전화의 경우 500명 정도의 수용이 가능하지만 TRS는 이보다 10배 규모인 5,000명까지도 공용능력이 가능하다. 하지만 주파수를 공용으로 사용하는 데서 오는 단점이 있다. 통화내용의 누설 등 특수한 업무를 위해서는 별도의 비밀통화기능이 필요하다는 단점 등이 있다. 다자간의 많은 정보들의 교환이 이뤄지는 망에서 정보들은 해커나 그 밖의 요소들로부터 위조나 불법 변경 등의 위협을 받고 있다. 따라서 정당한 수신자를 제외한 다른 사람들로부터 메시지의 안전성을 확보하기 위해 암호 시스템의 연구가 활발히 진행되고 있다. 또한 이 메시지의 송신자 및 수신자를 정확히 확인하기 위해 인증 분야가 요구되고 있는 실정이다. 현재 많은 연구가 진행중인 암호 시스템 상에서 핵심적인 부분을 차지하는 것이 바로 '키 관리'부분이다. 즉 아무리 암호화 시스템이 훌륭하다 할지라도 키가 노출되거나 분배를 정확하고 안전하게 수행할 수 없다면, 그 암호 시스템은 불안전할 수밖에 없는 것이 된다. 특히, 여러 사람들이 암호화 통신을 요구하는 상황에서는, 상대방의 키가 정확히 도착되었는지 확인하는 것이 무엇보다 중요한 사항이 되므로 키 분배 분야에 있어 각별한 주의를 기울여야 할 것이다. 본 고에서는 TRS 상에서 두 명 이상의 가입자들이 비밀 통신을 수행하려 할 경우 안전하게 키 분배를 하기 위한 요구 사항을 살펴보고, 새로운 방식을 제

† 본 연구는 국가보안기술연구소의 위탁 연구 과제 지원으로 수행되었음

안한다.

2. TRS 개요

TRS는 Trunked Radio system을 뜻하는 것으로 주파수 이용의 효율성을 높이기 위해 여러개의 주파수를 다수의 가입자가 공동으로 이용하는 무선통신 시스템이다. TRS는 이미 널리 사용되고 있는 차량전화나 휴대전화에 비해 서비스 종류가 다양하고 가격도 저렴하여 주로 기업 등에서 업무용으로 적합한 통신 서비스이다. 즉 TRS는 하나의 단말기로 이동전화는 물론 무선데이터, 양방향무선호출등의 기능을 발휘할 수 있으며 다양한 부가서비스를 이용할 수 있는 장점을 갖고 있다. 특히 TRS가 일반 공중통신망(PSTN)과 연결되면 이동전화의 기능을 그대로 발휘할 수 있다. 이에 따라 TRS는 대형운수업체나 택시회사, 대규모 현장관리업무, 유통사업분야, 보안서비스 등에 적합하다. 이 같은 TRS 서비스는 서비스 방식에 있어서는 기존의 워키토키라고 불리는 무전기와 비슷하나 통화권이 기지국을 중심으로 무전기는 2km 정도에 불과하지만 TRS는 최대 50km에 달한다. 또 혼신이 없고 보안성이 뛰어나다는 장점을 가지고 있다. 뿐만 아니라 TRS는 1개의 주파수 채널로 1대1 개별통신은 물론 1백30여명 이상이 동시에 통화를 할 수 있다. 즉 그룹통화를 할 수 있다는 점이 TRS의 가장 큰 장점이라 할 수 있다.

TRS 서비스는 지난 1960년대 미국에서 무선통신 서비스에 대한 수요가 폭증하면서 나타난 주파수 부족현상을 해결하기 위한 수단으로 개발되어 지난 1977년 8월부터 미국에서 본격적으로 상업용으로 이용되기 시작했다.

또 일본에서는 지난 82년 10월 재단법인 이동무선센터가 동경지역을 대상으로 서비스를 시작했고 영국에서는 밴드스리사가 지난 87년부터 서비스에 들어갔다. 국내에서는 지난 1988년 서울올림픽을 계기로 TRS 서비스가 도입되어 올림픽 기간 동안 각국의 보도기관을 위한 통신지원용으로 10개의 TRS 채널을 운영한 것이 국내 TRS 서비스의 효시이다. 이어서 연안 선박들에 대한 자동전화 서비스를 목적으로 지금의 한국TRS의 전신인 한국항만전화(주)가 지난 91년 2월 정부로부터 허가를 받아 그해 12월부터 부산 항만 일대를 대상으로 서비스에 들어갔다. 한국항만전화는 그후 지난 93년 5월부터 11월까지 열린 대전엑스포 기간동안 TRS 서비스를 운영한데 이어 94년 7월에는 인천 지역에 상륙, 육상에서 본격적인 서비스를 제공하기 시작하여 지금은 전국을 대상으로 서비스를 하고있다. TRS는 또 상업용 서비스 업체외에 일부 대기업들이 자가통신망으로 구축 활용하고 있기도 하며 경찰청이나 교통방송 검찰청 등에서도 자가업무용으로 TRS망을 구축, 통신에 활용하고 있다.

2.1 TRS 키분배를 위한 요구 사항

TRS 키 분배를 위해 필요한 사항들은 여러 가지가 있겠지만, 그 중 주요한 사항들을 다음과 같이 정리하였다.

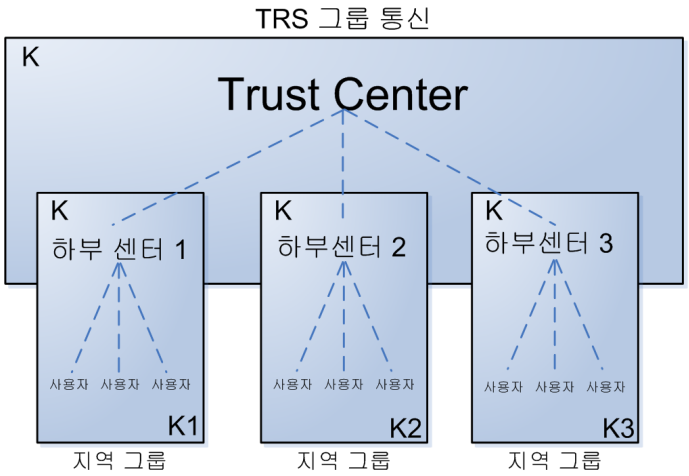
1) 안전성 : 키 분배 프로토콜은 제 3자에 의한 불법적 행위로부터 안전성을 획득하여야 한다.
2) 인증성 : 모든 회의 참여자들은 키 인증을 통해 출처 및 무결성을 확인할 수 있어야 한다.
3) 통신 회수 : 통신 회수는 회의 참여자 수와는 상관없이 일정해야 한다.

물론 안전하고 정확한 회의용 키 분배를 위해서 1), 2) 항목은 기본적으로 만족되어야 한다. 뿐만 아니라, 다자간 통신에서 통신 회수의 증가는 효율성을 떨어뜨리므로 통신 회수 역시 고려해 보아야 할 요구 사항이다. 이와 같은 요구사항을 만족시키는 제안 방식에 대해 설명한다.

3. 제안 방식

본 제안 방식은 Tree 기반의 공개키 암호 시스템에 근거한다. 기존의 방식에 비하여 각 참여자는 키 인증 부분과 Bridge를 통해 안전성을 확보하고 있다. 또한 키 생성시 2번 정도의 통신 회수를 요구함으로서 효율성을 높이고 있다. 특히 비밀 정보 생성을 위해 참여하는 TC(Trusted Center)는 키 생성에 별도로 참여하지 않음으로서, 부정의 소지를 막고 있다. 최종 TC는 하부의 센터에 인증서를 발급하고 발급받은 하부 센터는 자신에 속한 사용자에게 인증서를 발급함으로써 그룹의 관리의 편리성과 함께 사용자의 편리성도 도모할 수 있다. 또한 사용자의 추가, 탈퇴가 원활히 이뤄질 수 있다. 이에 본 논문에서는 Tree 기반의 키 분배에 대하여 제안하고 이를 살펴보도록 한다. 다음의 그림은 본 제안방식의 전

체 도식이다.



(그림 1) 제안 방식 개요도

3.1 시스템 계수

본 방식에서 사용되는 시스템 계수는 아래와 같다. 전체 5 참여자로 구성되며, 각각은 공개키 암호 시스템에 근거한다.

- TC : 하부 센터 비밀 정보 생성 기관(신뢰된 제 3자)
- $Bridge$: 하부 센터 키 분배 노드
- A_i : 하부 센터들 ($i=1,2,\ldots,n$)
- B_i : 참여자 ($i=1,2,\ldots,n$)
- f : 일방향 해쉬 함수
- L_i : 각 하부 센터들의 정보 ($i=1,2,\ldots,n$)
- ID_i : 하부 센터 A_i의 ID
- l_i $(=f(ID_i,j))$: 참여자 ID 정보
- (e,d) : $ed=1 \bmod L$이 되는 공통 공개키 및 비밀키
- $X_i=g^{ri e} \bmod n$: 각 참여자가 생성하는 키 구성 요소
- $Y_i=S_i g^{X_i ri} \bmod n$: 각 참여자가 생성하는 키 확인 요소
- K : TRS 통신용 키
- $h(\ )$: 안전한 일방향 해쉬 함수

3.2 프로토콜

본 방식의 제안방식은 아래의 과정을 거친다. 참여자 등록 단계와 키 생성 단계로 구성된다. 각 단계에서 세부단계는 내용과 같이 이뤄지며 최종적으로 사용자들에게 키가 분배되며, 사용자들은 자신의 키를 이용하여 메시지를 전송하게 된다.

(1) 참여자 등록 단계

- TC

: 하부 센터 A_i가 ID_i를 키 발급 센터(TC)에 등록하게 되면 TC는 아래 단계와 같은 일을 수행한다. 이때 하부 센터에 등록 되어 있는 사용자 정보 L_i도 동시 등록한다.

Step 1. TC에서는 두 개의 큰 소수 p, q를 생성하고 비밀리에 유지한다.

Step 2. 조건을 만족하는 정수 (e,d)를 결정한다.

$ed=1 \pmod L$ $\quad L=lcm((p-1)(q-1))$

Step 3. 하부 센터 A_i에 대하여 C_i를 계산해 낸다.

$l_i=f(ID_i,j)$ $(i=1,2,\ldots,m\ j=1,2,\ldots,k)$

$l_i=C_i^e \bmod n$

$C_i=l_i^d \bmod n$

: TC는 참여자의 참 유무를 판단한 (n, g, e, C_i)를 스마트 카드에 저장해 전송한다. 이때, p, q, d는 TC만이 알고 있는 정보이다.

(2) 키 생성 단계

- 하부 센터 A_i

: 하부 센터 A_i는 랜덤 수 $r_i \in Z_n$을 선택하여 아래와 같이 X_i, Y_i를 계산한다.

Step 1. 하부 센터는 $X_i=g^{rie} \bmod n$을 계산하고, $Y_i=C_i g^{X_i ri} \bmod n$을 계산한다.

Step 2. 계산된 값과 $h(l_i)$를 연접한 정보 $(X_i \| Y_i \| h(l_i))$를 소속 $Bridge$에 전송한다.

- $Bridge$

: $Bridge$는 아래의 단계가 성립하는지 확인한다.

Step 1. $Bridge$ 는 $h(Y_i^e / X_i^{X_i} \bmod n)=h(l_i)$ 을 계산한다.

: 같으면 전송된 정보가 정당한 사용자로부터 온 것임을 확인하게 된다. $Bridge$는 아래와 같이 계

산해 수신자의 X_i와 연접해 각 참여자에게 전송한다.

Step 2. $Y=(Y_1 * Y_2 * \cdots * Y_n)^e \bmod n$을 계산한다.

Step 3. $(Y \| X_1 \| \cdots \| X_n \| h(l_1 * \cdots * l_n))$를 각 참여자에게 전송한다.

- 하부 센터 A_i

: 하부 센터 A_i는 아래의 단계가 성립하는지 확인한다.

Step 1. $h(Y^e/(X_1^{X_1} * \cdots * X_n^{X_n}) \bmod n)=h(l_1 * \cdots * l_n)$을 계산한다.

: 같다면 전송된 정보가 정당한 회의 참여자들로부터 온 것임을 확인하게 된다. 각 하부 센터들은 아래와 같이 키를 생성한다.

Step 2. 각 하부 센터는 $K=(\prod_{i=0}^{n} X_i) \bmod n$을 수행하여 키를 획득한다.

- 참여자 B_i

: 하부 센터에서 분배된 키에 각각의 하부 센터가 설정하는 키 정보를 삽입하고 이를 참여자 B_i에 각각 분배함으로써 전체 그룹 통신에 사용되는 키와 함께 현재 자신이 속한 그룹의 키도 함께 전송받음 으로써 키 분배가 이뤄지게 된다.

Step 1. 하부 센터 A_i 는 획득한 K정보에 자신이 생성한 정보와 사용자 정보를 아래의 연산을 통해 키를 생성하여 전송한다.

$$UK \equiv K^a L_i \bmod n$$

Step 2. 사용자는 전송받은 정보를 다음의 연산을 통해 검증하고 키 KU를 획득한다.

$$KU=((K^a L_i)/L_i) \bmod n$$

본 논문은 Tree에 기반하여 하부센터에 키를 분배하고, 키를 분배받은 하부센터는 다시 자신에 속한 사용자에게 키를 제공하는 방식이다. 제안된 방식은 TRS와 같이 사용자가 전체 그룹 혹은 여러 그룹으로 나뉘어 통신을 하고자 할 때, 사용자의 이동뿐만 아니라 그룹 참가와 탈퇴가 자유롭게 이뤄질 수 있다. 또한, 각 요구사항에 대하여 하부센터 뿐만 아니라 사용자에 대한 요구사항도 만족하고 있다.

4. 결론

주파수공용통신 시스템은 미국과 일본에서는 MCA(Multi Channel Access), 한국과 유럽에서는 TRS(Trunked Radio System)이라고 한다. TRS는 기존의 무전기나 워키토키의 성능을 크게 발전시킨 시스템으로 서비스 제공자가 고지대에 무선중계 설비를 구축하여 기업체, 개인 등 다수의 가입자가 다수의 주파수를 공유하여 상대방과 다양한 형태의 통신을 할 수 있는 통신방식이다.

본 고에서 제안한 방식은 Tree에 기반한 키 분배 방식에 근거하고 있으며, 각 하부 센터들과 Bridge가 인증을 통해 해쉬된 신원 정보을 확인할 수 있게 함으로서 제 3자의 불법적 행위를 방지할 수 있다. 또한, TC가 키 생성에 참여하지 않으므로 신뢰성을 높일 뿐만 아니라, Bridge를 도입함으로서 중간 단계의 안전성을 확보하였다. 이러한 특성 외에도, 참여자들의 총 라운드 수를 2회로 줄임으로서 효율성을 확보하고 있다. 따라서 본 방식은 TRS 상에서 대규모 통신, 다자간 비밀 통신 등에 효과적으로 응용될 수 있으리라 기대된다.

참고문헌

[1] W. Diffie and M. Hellan, "New Direction in cryptography," IEEE Trans., IT-22, 1976, pp.644-654

[2] I. Ingemarsson, D. Tang and C. Wong, "A Conference key distribution system," IEEE Trans., It-28, 1982, pp.714-720.

[3] K. Koyama and K. Ohta, "Identity-based conference key distribution systems," Proceedings of Crypto '87, lecture Notes in omputer Science no. 293, Springer-Verlag, 1988, pp.175-184.

[4] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution Systems," EUROCRYPT '94, pp.279-290

[5] Y. Yacobi, "Attack on the Koyama-Ohta Identity-based key distribution systems," Proceedings of Cryto'87, Lecture Notes in Computer Science no. 293, Springer-Verlag, 1988, pp.429-433.