안전한 TRS를 위한 그룹 키 관리 기법†

박장수*, 박용석**, 안정철**, 이임영*

*순천향대학교 컴퓨터학부

**국가보안기술연구소

A Group Key Management Scheme for Secure TRS

Jang-Su Park*, YongSeok Park**,JungChul Ahn**, ImYeong Lee*

*Division of Computer, SoonChunHyang University

**National Security Research Institute

요 약

TRS 시스템은 기존의 자가무전기를 발전시킨 시스템으로 각 사용자가 하나의 주파수만 사용하던 기존 이동통신과는 달리 무선중계국의 많은 주파수를 다수의 사용자가 공동으로 사용하는 무선 이동통신이다. 이러한 TRS 시스템은 여러 개의 그룹으로 구성되어 통신이 이루어지기 때문에 그룹내 안전하게 통신을 하기 위해서는 그룹 키 관리 기법을 이용하여 안전한 통신을 제공해야 한다. 따라서 본 논문에서는 TRS 시스템에서 안전한 그룹 키 관리 기법을 제안하고자 한다.

I. 서론

현재 우리나라는 국가적인 재난에 대비해 각 국가기관의 무선통신망을 하나로 통합하는 사업으로 행정자치부에서 분리된 소방방재청이 주관하고 있다. 올해 7월부터 내년 2월까지 139억원을 들여 서울, 성남, 안양, 광명, 군포, 과천, 시흥, 의왕 등 경기 일부와 13개 기관을 시범 사업 진행할 계획이다. 사업 대상은 국정원, 국방부, 경찰청, 소방방재청 등 국가기관 7곳과 서울시 경기도 등 자치단체 2곳, 한국철도공사, 한국전력공사 등 공공기관 4곳이다. 소방방재청에서는 불시에 일어나는 재해로부터 국민의 재산과 생명을 보호하기 위하여 국가 통합지휘 무선통신망을 유럽의 표준 기술인 TETRA로 선정하여 현재 활발히 연구가 진행되고 있다[3,4].

이러한 국가 통합 지휘 무선 통신망은 여러 그룹으로 구성되어 통신이 이루어지며, 정당한 그룹 사용자에게만 수신을 허용하기 때문에 구성원들이 공유하고 있는 그룹키로 암호화하여 통신을 해야 한다. 하지만 그룹 구성원의 가입/탈퇴가 자유로운 동적인 그룹에서는 데이터의 기밀성을 제공하기 위해서, 그룹 멤버들이 데이터를 암호화하고 복호화 할 수 있는 키를 관리하여야 한다[1,5,6].

따라서 본 논문에서는 그룹 키 관리를 제안함으로써 안전한 TRS 시스템을 이용할 수 있도록 제공하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 TRS의 개요에 대해 간략하게 설명을 한다. 3장에서는 TRS에서의 키 관리 요구사항에 대해 알아보고, 4장에서는 키 관리 방식을 제안한다. 마지막으로 5장에서는 결론을 맺는다.

II. TRS의 개요

TRS(Trunked Radio System)란 주파수의 이용의 효율성을 높이기 위해 여러 개의 주파수를 다수의 가입자가 공동으로 이용하는 무선 통신 시스템이다. TRS는 이미 널리 사용되고 있는 차량전화나 휴대전화에 비해 서비스 종류가 다양하고 가격도 저렴하여 주로 기업 등에서 업무용으로 적합한 통신 서비스이다.

† 본 연구는 국가보안기술연구소의 위탁 연구 과제 지원으로 수행되었음

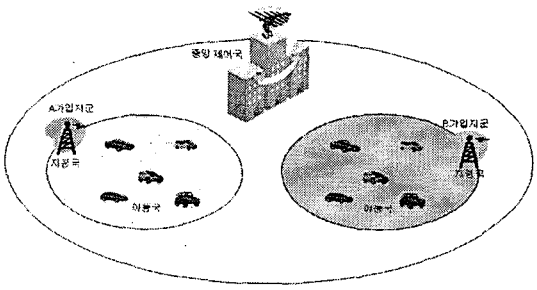

그림 1 : TRS 개요

즉 TRS는 하나의 단말기로 이동전화는 물론 무선데이터, 양방향 무선호출 등의 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, 유통 사업 분야, 보안서비스 등에 적합하다. 이와 같은 TRS 서비스는 서비스 방식에 있어서 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 1백 30여명 이상이 동시에 통화를 할 수 있다. 즉 그룹통화를 할 수 있다는 점이 TRS의 가장 큰 장점이라 할 수 있다 [5,6,7].

III. TRS에서의 키 관리 요구사항

TRS는 구성원의 가입이나 탈퇴가 자유로운 동적인 그룹에서 통신이 이루어진다. 따라서 안전성을 위한 요구 조건으로 다음과 같다.

- 그룹 키 비밀성(Group Key Secrecy) : 도청자가 그룹 키를 알아내는 것은 계산상 불가능해야 한다.
- 후방향 비밀성(Backward Secrecy) : 가입하는 구성원이 가입 이전의 그룹 키를 알 수 없도록 해야 한다.
- 전방향 비밀성(Forward Secrecy) : 탈퇴한 구성원이 탈퇴 이후 그룹 키를 알 수 없도록 해야 한다.
- 정당한 사용자 인증(User Authentication) : 그룹 가입을 요청하는 사용자가 정당한 사용자인지 판단할 수 있어야 한다.

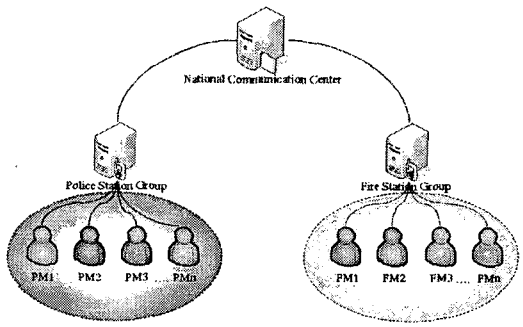

그림 2 : 제안 방식 구조

IV. 제안 방식

본 장에서는 국가 통합 지휘 무선 통신망에서의 그룹 키 관리 기법을 제안하고자 한다. 그림 2에서와 같이 기본 구조는 중앙의 국가 통합 지휘 센터(National Communication Center)와 경찰청(Polices Station), 소방서(Fire Station) 등 각 국가 기관이 연결되어 있고 각 국가 기관의 사용자들로 구성되어있다. 본 제안 방식은 각 국가 기관의 그룹에 사용자의 가입/탈퇴를 관리하는 부분만 언급한다.

1. 시스템 계수

다음은 본 논문에서 사용되는 시스템 계수이다.

- PM_i : i번째 Police Member
- PGM : Police Group Manager
- ID_* : *의 ID
- CER_* : *의 인증서
- $*\_r$: *의 생성한 랜덤수
- SK_* : *의 세션 키
- GK : 그룹 키
- K_{PR_*} : *의 Private Key
- K_{PU_*} : *의 Public Key
- X_* : 그룹 키 구성 인자
- Sig_* : *의 서명

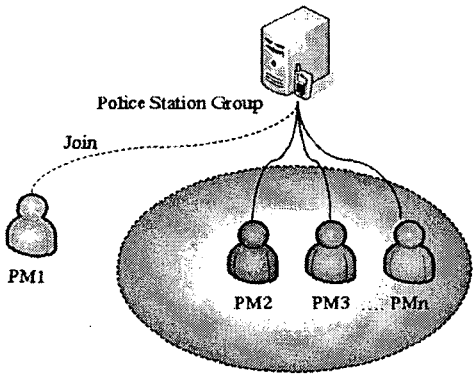

그림 3 : 사용자 가입

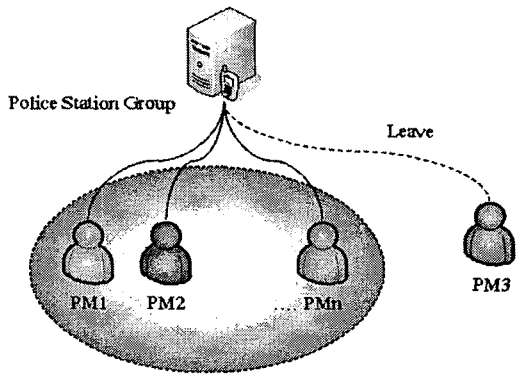

그림 4 : 사용자 탈퇴

2. 제안 방식 동작 과정

제안 방식은 국가 기관인 경찰 그룹의 모델로 제시되며, 초기 사용자 등록 단계, 그룹 키 생성 및 분배 단계, 사용자의 그룹 가입 단계, 사용자 탈퇴 단계로 나누어 볼 수 있다.

1) 초기 사용자 등록 단계

① 사용자는 사용자의 ID, 인증서, 사용자가 생성한 랜덤수를 경찰 그룹 관리자의 공개키로 암호화하여 경찰 그룹 관리자에게 전송한다.

$$E_{K_{PU\_PGM}}[ID_{PM_1},\ CER_{PM_1},\ PM_1\_r]$$

② 경찰 그룹 관리자는 사용자의 공개키로 경찰 그룹 관리자의 ID, 경찰 그룹 관리자가 생성한 랜덤수, 세션키에 서명한 데이터, 사용자가 생성한 랜덤수를 세션키로 암호화한 데이터를 사용자에게 전송한다.

$$E_{K_{PU\_PM_1}}[ID_{PGM} \parallel PGM\_r \parallel Sig\_PGM[SK\_PM_1] \parallel E_{SK\_PM_1}[PM_1\_r]]$$

③ 사용자는 자신의 생성한 랜덤수와 경찰 그룹 관리자가 생성한 랜덤수를 XOR 연산을 취해 세션키로 암호화하여 경찰 그룹 관리자에게 전송한다.

$$E_{SK\_PM_1}[PM_1\_r \oplus PGM\_r]$$

④ 경찰 그룹 관리자는 세션 키로 복호화하여 데이터를 획득한 후 사용자와 같은 연산을 취해 데이터를 생성해서 비교한 후 서로 같다면 정당한 사용자로부터 전송되어졌다고 판단되어 사용자의 ID, 사용자의 세션 키, 생성한 그룹 키 구성 인자를 등록한다.

$$PM_1\_r \oplus PGM\_r \stackrel{?}{=} PM_1\_r \oplus PGM\_r$$

$$X_{PM_1} : h(PM_1\_r \oplus PGM\_r \parallel E_{K_{PR\_PGM}})$$

위의 과정을 통해 초기 사용자 등록이 끝나면 그룹 사용자들의 그룹 키를 생성 한다.

2) 그룹 키 생성 및 분배 단계

그룹 키는 경찰 그룹 관리자가 생성하여 분배한다.

① 경찰 그룹 관리자는 사용자 초기 등록 단계에서 생성한 그룹 키 구성 인자를 이용하여 그룹 키를 생성한다.

$$GK = g^{\sum_{i=1}^{n} X_{PM_i}}$$

② 그룹 키의 초기 분배는 각 사용자의 세션 키로 암호화 하여 전송한다.

$$E_{SK_{Join}}[\neq w\_GK]$$

3) 사용자의 그룹 가입 단계

사용자의 그룹 가입 단계는 초기 사용자 등록 단계와 동일하며, 새로운 그룹 키 생성과 분배하는 과정에서 차이가 있다.

① 경찰 그룹 관리자는 새로운 사용자가 그룹에 가입 되었을 때 새로운 사용자 그룹 키 구성 인자만 기존의 그룹 키에 곱셈 연산을 취한다.

$$\neq w\_GK = g^{\sum_{i=1}^{n} X_{PM_i}} * g^{X_{Join}}$$

② 새로운 그룹 키를 생성을 한 후, 기존의 그룹 키

로 암화를 취해 그룹 사용자들에게 전송을 하고, 새로 가입한 사용자에게는 세션 키로 암호화 하여 전송한다.

$$E_{GK}[\neq w\_GK] \text{ and } E_{SK_{Join}}[\neq w\_GK]$$

4) 사용자 탈퇴 단계

기존의 경찰 그룹 사용사중 탈퇴를 경찰 그룹 관리자에게 요청 하면, 경찰 그룹 관리자는 그룹 키를 갱신 시켜 기존 그룹 사용자에게 전송해야 한다.

① 경찰 그룹 관리자는 탈퇴를 원하는 사용자의 그룹 키 구성 인자를 나누어 그룹 키를 갱신한다.

$$Modify\_GK = g^{\sum_{i=1}^{n} X_{PM_i}} / g^{X_{Leave}}$$

② 갱신 시킨 그룹 키를 탈퇴자를 제외한 그룹 사용자에게 각 사용자의 세션 키로 암호화 하여 분배한다.

$$all\,SK \rightarrow E_{SK\_*}[Modify\_GK]$$

3. 제안방식 분석

- 그룹 키 비밀성(Group Key Secrecy) : 그룹키 구성 인자인 X_{PMi}는 경찰 그룹 관리자가 생성해서 가지고 있기 때문에 그룹 키를 제 3의 악의적인 공격자는 알 수 없다. 또한 정당한 그룹 사용자도 임의적으로 그룹 키를 변경하고 알아낼 수 없다.

$$X_{PMi} : h(PM_i\_r \oplus PGM\_r \parallel E_{K_{PR}PGM})$$

$$GK = g\sum_{i=1}^{n} X_{PM_i}$$

- 후방향 비밀성(Backward Secrecy) : 새로 가입하는 사용자는 $\neq w_GK$로 자신의 그룹 키 구성 인자를 알 수 없어 가입 이전의 그룹 키를 획득 할 수 없으므로 후방향 비밀성을 제공한다.
- 전방향 비밀성(Forward Secrecy) : 그룹을 탈퇴한 사용자는 자신의 그룹 키 구성 인자를 알 수 없어, 탈퇴 이후의 $Modify_GK$를 획득 할 수 없다. 따라서 전방향 비밀성을 제공한다.
- 정당한 사용자 인증(User Authentication) : 그룹 가입을 요청하는 사용자는 초기 등록 과정을 거쳐 정당한 사용자인지 확인이 가능하다.

$$PM_1\_r \oplus PGM\_r \stackrel{?}{=} PM_1\_r \oplus PGM\_r$$

V. 결론

본 논문에서는 국가 통합 지휘망의 일부분인 국가기관의 그룹 하나의 동작과정을 중점적으로 연구하여 그룹 키 관리를 제안 하였다. 하지만 그룹 사용자의 탈퇴 시 갱신된 그룹 키 분배 과정에서 모든 사용자의 세션 키로 암호화하여 전송되므로 비효율적이다. 따라서 향후 분배하는 과정을 효율적으로 개선시키는 방향에 지속적으로 연구를 할 것이다. 또한 국가 망 전체 모델에서의 그룹간의 이동 및 전체 일괄 통신을 고려하여 연구를 진행 할 것이다.

[참고문헌]

[1] I. Ingemarsson, D. Tang and C. Wong, "A Conference key distribution system," IEEE Trans., It-28, 1982, pp.714-720. Communications Security, pp 103-111, 2003.

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

[3] 김응배, 김경아, 홍영삼, "국가통합지휘무선통신망 기술표준 및 기술 동향", 한국 통신 학회지, 23권 2호, 2006년

[4] 오갑근, 박동하, "국가통합지휘무선통신망 구축계획 및 현황", 한국 통신 학회지, 23권 2호, 2006년

[5] 이덕규, 박용석, 안정철, 이임영, "TRS를 위한 효율적인 키 분배 방식에 관한 연구", 한국정보보호학회 하계 학술 발표대회, pp275-278, 2005

[6] 이덕규, 박용석, 안정철, 이임영, "TRS 상의 Tree를 이용한 효율적인 키 분배", 한국정보처리학회 추계 학술 발표대회, pp949-952, 2005

[7] 이영완, "TRS 시스템 기술과 현황", 한국 통신 학회지, 23권 2호, 2006년