TRS 상의 개별/그룹 통신을 위한 효율적인 키 분배 기법

이 덕 규[†] · 박 용 석[††] · 안 정 철[†††] · 이 임 영[††††]

요 약

주파수공용통신(TRS: Trunked Radio Service)이란 무선통신을 하는 사람이 특정한 주파수를 이용하던 종래의 무선통신방식과는 달리 중계소에 할당된 소수의 주파수를 다수의 이용자가 공동으로 사용하는 방식을 말한다. TRS 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. 위와 같은 여러 목적에 따라 다양한 형태의 연결이나 그룹 통신이 이뤄질 경우, 여러 가지 형태의 공격에 노출될 수 있으며, 대규모 통신을 위한 키 분배 혹은 설정에 많은 문제점을 가질 수 있다. 본고에서는 TRS 상에서 안전한 통신을 수행하는데 있어 필수 요소인 그룹 키 분배 방식을 고찰하며, 통신 횟수를 줄이면서도 참여자 인증을 수행할 수 있는 효율적인 그룹 키 분배 방식을 제안하였다.

키워드 : TRS, 개별 통신, 그룹 통신, 키 분배

A Efficient Key Distribution Scheme for Individual/Group Communication on TRS

Deok-Gyu Lee[†] · Yong Suk Park[††] · Joung Chul Ahn[†††] · Im-Yeong Lee[††††]

ABSTRACT

It used exclusively the radio communication where is the TRS(Trunked Radio Service) at frequency where the person whom it does is specific with hitherto radio communication method differently frequency of the decimal which is allocated to the relay station it talks the at the room which the multiple user uses with commonness. The TRS system the most big feature is the region multiple group and order communication method. The TRS the composition of system is composed of the multi mind group, the each group is composed of the terminal of the users who have the objective which is similar relates in business contents. With above it follows in same multi objective and the connection of the form which is various or group communication accomplishes and quality case, a possibility a or of having many problem point in key distribution for a large scale communication there is it could be exposed to attack of the form which is various. There is a place where it accomplishes the communication which is safe at the TRS from research which it sees it investigates group key distribution method which is an essential element. The method which it sees when it reduces a communication frequency, it stands but is the user, it proposes the efficient group key distribution method it will be able to accomplish.

Key Words : TRS, Individual Communication, Group Communication, Key Distribution

1. 서 론

주파수공용통신(TRS: Trunked Radio Service)란 무선통신을 하는 사람이 특정한 주파수를 이용하던 종래의 무선통신방식과는 달리 중계소에 할당된 소수의 주파수를 다수의 이용자가 공동으로 사용하는 방식을 말한다. 일정한 주파수를 전용하도록 되어 있는 기존 이동전화와 같은 셀룰러시스템과 달리 간선전화시스템은 독립된 각각의 채널을 하나로 묶어 다수의 이용자가 공용하도록 한 방식으로 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 운영 능력이 가능하다. 하지만 주파수를 공용으로 사용하는 데서 오는 단점이 있다. 통화내용의 누설 등 특수한 업무를 위해서는 별도의 비밀통화기능이 필요하다는 단점 등이 있다. 또한 다자간의 많은 정보들의 교환이 이뤄지는 망으로 인해 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 있으며, 메시지

† 준 회 원 : 한국전자통신연구원 정보보호연구단 Post-Doc.(교신저자)
†† 정 회 원 : 국가보안기술연구소 연구원
††† 정 회 원 : 국가보안기술연구소 팀장
†††† 종신회원 : 순천향대학교 정보기술공학부 정교수
논문접수 : 2005년 11월 22일, 심사완료 : 2006년 11월 7일

의 송신자 및 수신자를 정확히 확인하기 위해 인증 분야가 요구되고 있는 실정이다[1,2].

현재 많은 연구가 진행 중인 암호 시스템 상에서 핵심적인 부분을 차지하는 것이 바로 '키 관리'부분이다. 즉 아무리 암호화 시스템이 훌륭하다 할지라도 키가 노출되거나 분배에 있어 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. 이와 같이 TRS에 있어서도 그룹 통신을 위해 각 참여자에게 키가 생성 및 분배가 안전하게 이뤄져야 한다. 본 연구에서는 여러 가지 안전성 분석을 통해 TRS에서 적합한 개별/그룹 통신을 제공할 수 있는 프로토콜을 제안한다. 우선 2장에서 TRS 개요 및 기존에 제시된 논문 방식들에 관하여 분석하고, 3장에서는 TRS 상에서 두명 이상의 가입자들이 비밀 통신을 수행하려 할 경우 안전하게 키 분배를 하기 위한 보안 요구 사항을 살펴본다. 4장에서는 앞서 분석한 기존 방식의 문제점을 개선한 새로운 방식을 제안하고, 5장에서는 본 방식과 관련하여 요구사항에 대한 분석을 하며, 기존 방식과의 비교 분석을 통해 제안 방식의 효율성에 대해 살펴보고, 마지막으로 6장에서 결론으로 마친다.

2. TRS 개요 및 기존 방식 분석

본 장에서는 TRS 개요와 기존 멀티캐스트 키 분배 방식에 대해 살펴본다. 기존 멀티캐스트는 여러 가지가 있지만, 본 논문에서는 키 관리 부분을 주된 관심 대상으로 기존 시스템 보다는 키 관리 측면에서의 멀티캐스트 키 관리에 대해 살펴보도록 한다. 기존 멀티캐스트 키 관리 시스템은 확장하여 TRS 시스템에 이용 가능하다.

2.1 TRS 개요

TRS는 Trunked Radio system을 뜻하는 것으로 주파수 이용의 효율성을 높이기 위해 여러 개의 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, 양방향 무선 호출 등의 기능을 발휘할 수 있으며 다양한 부가서비스를 이용할 수 있는 장점을 갖고 있다. 특히 TRS가 일반 공중통신망(PSTN: Public Switched Telephone Network)과 연결되면 이동전화의 기능을 그대로 발휘할 수 있다.

TRS 서비스는 1960년대 미국에서 무선통신 서비스에 대한 수요가 폭증하면서 나타난 주파수 부족현상을 해결하기 위한 수단으로 개발되어 1977년 8월부터 미국에서 상업용으로 이용되기 시작했다. 또 일본에서는 1982년 10월 이동무선센터가 동경지역을 대상으로 서비스를 시작했고, 영국에서는 밴드스리사가 1987년부터 서비스에 들어갔다. 국내에서는 1988년 서울올림픽을 계기로 TRS 서비스가 도입되어 올림픽 기간 동안 각국의 보도기관을 위한 통신지원용으로 10개의 TRS 채널을 운영한 것이 국내 TRS 서비스의 효시이다. 이어 연안 선박들에 대한 자동전화 서비스를 목적으로 지금의 한국TRS가 1991년 2월 정부로부터 허가를 받아 12월부터 부산항만 일대를 대상으로 서비스에 들어갔다. 한국TRS는 그 후 1993년 5월부터 11월까지 열린 대전엑스포 기간 동안 TRS 서비스를 운영한데 이어 1994년 7월에는 인천 지역에서 본격적인 서비스를 제공하기 시작하여 지금은 전국을 대상으로 서비스를 하고 있다. TRS는 또 상업용 서비스 업체 외에 일부 대기업들이 자가 통신망으로 구축 활용하고 있기도 하며 경찰청이나 교통방송 검찰청 등에서도 자가 업무용으로 TRS망을 구축, 통신에 활용하고 있다. 또한 TRS는 대형운수업체나 택시회사, 대규모 현장관리업무, 유통 사업 분야, 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 1 대 1 개별통신은 물론 1 대 130대 이상이 동시에 통화를 할 수 있다. 즉 그룹 통화를 할 수 있다는 점이 TRS의 가장 큰 장점이라 할 수 있다. 이와 같은 TRS의 그룹 통화는 큰 장점을 가지고 있음에도 불구하고 키의 대한 관리로 인해 많은 문제점을 가지고 있다. 이와 같은 문제는 1 대 1 통신, 소규모 그룹 통신, 대규모 그룹 통신 등에서 키 관리의 어려움을 발생 시킬 수 있다. 또한 각 제공되는 여러 키에 대해 전체적인 관리나 사용자의 참가, 탈퇴에 따른 사용자 키 관리의 문제점도 발생할 수 있다. 이와 같이 여러 가지 문제점에 대해 본 논문에서는 신뢰 기관에 등록하고 전체 사용되는 키는 TRS 센터에서 관리하여 좀 더 효율적인 방법을 제시한다.

2.2 기존 키 분배 방식

본 절에서는 기존 그룹에서의 키 분배 방식에 대해 분석한다. 기존 방식에 대한 분석은 아래의 [표 1]을 기준으로 한다. 기존 방식은 멀티캐스트 그룹 키 분배 방식에 대해 제안되었던 방식으로 본 논문에서는 기존 멀티캐스트 그룹 키 분배 방식이 TRS상에서의 그룹 키 분배 방식으로 일반화하여 사용될 수 있으므로 이에 대한 분석으로 대신하고자 한다[5-7].

2.2.1 Group Key Management Protocol

Group Key Management Protocol(GKMP)는 그룹키를 생성하고 유지할 수 있게 해준다. 이 기법은 GC가 Group Traffic Encryption Key(GTEK)와 Group Key Encryption Key(GKEK)를 포함하는 Group Key Packet(GKP)를 생성한다. 키를 갱신할 때는 GTEK를 이용하여 새로운 키를 그룹 멤버에게 전달한다. 그러나 GKEK는 모든 구성원에게 알려주는 키로써, 그룹을 탈퇴한 멤버도 역시 갱신된 키를 알 수 있으므로 후에 기밀성을 보장할 수 없다는 단점이 있다[7].

2.2.2 Dunigan and Cao's Group Key Management

Dunign와 Cao는 GKMP(Group Key Management Protocol)와 유사한 그룹키 관리를 제안했다[8]. 이것은 상위 그룹 관리자와 하위 그룹 관리자로 구성되어있다. 상위 그룹 관리자는 각 그룹의 하위 그룹 관리자를 할당하는데 이때, 이전에 할당된 하위 그룹 관리자가 없는 경우, 그 그룹의 최초의 멤버가 그룹 관리자가 된다. 각 그룹의 멤버는 앞의 GKMP와 유사하게 GTEK와 GKEK라는 두개의 키를 받는다. GTEK로 그룹 메시지를 암호화하고 GKEK를 이용하여 새로운 키 쌍 GTEK, GKEK를 암호화하여 분배한다. 이 기법도 GKMP와 같은 단점을 가진다.

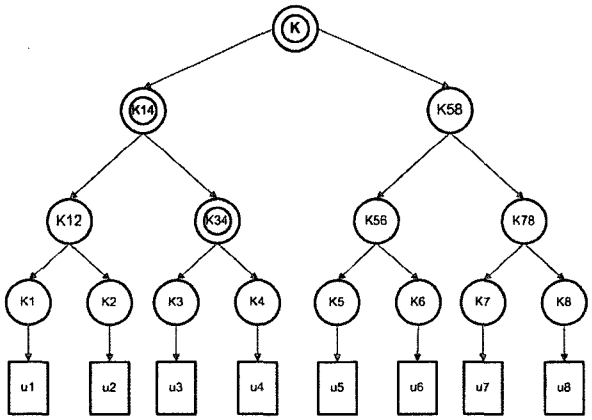
2.2.3 Scalable extension of Group Key Management Protocol

Poovendran이 GKMP의 문제점을 다음과 같이 제기하였다. 비록 GKMP이 모든 멤버들에게 접근 통제를 허락하더라도 단지 GC(Group Controller)만이 새로운 키를 생성할 수 있으므로 GC가 위협을 받게 되면 그룹 전체에 영향을 미친다. Proovendran은 한 명의 GC를 3명의 GC로 대치하고 3명의 GC 중 2명 이상이 있어야 새로운 키를 생성할 수 있고, 같은 2명의 GC가 연속적으로 새로운 키를 생성할 수 없도록 제안하였다. 따라서 한명의 GC가 실패할 확률보다 2명의 GC가 동시에 실패할 확률이 작기 때문에 앞의 방법들보다 신뢰할만하다. 그러나 이 기법도 역시 구성원이 바뀌었을 때의 문제를 해결하지는 못했다[9].

2.2.4 Hierarchical Binary Tree

Walner와 Caronni가 Hierarchical Binary Tree(HBT)를 제안했다. 이 기법은 키 트리를 관리하는 현 명의 그룹 관리자가 있다. 트리의 노드는 모두 KEK를 포함하고 있으며, 트리의 앞은 그룹의 구성원에 해당하고 KEK로 구성되어 있다. 트리의 루트는 그룹키를 갖고 있다. 각 그룹의 멤버는 $\log_2^n$개의 키를 소유하고 있다. 예를 들어, 구성원 U_1은 K_1, K_{12}, K_{14}, K의 키를 소유하고 있다.

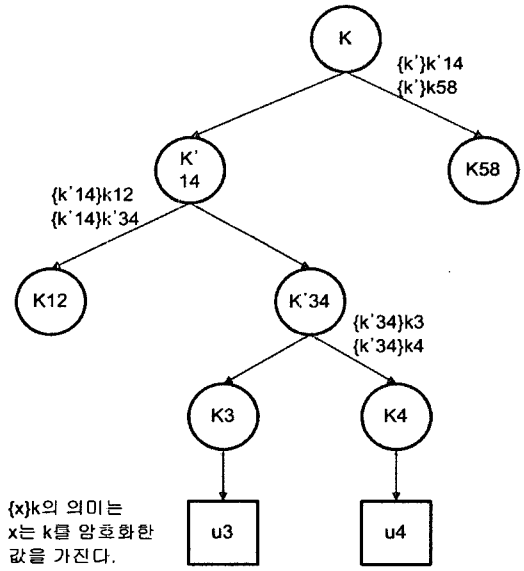
새로 참가하는 멤버는 최하위 자식 노드 또는 leaf를 의미하고 이 최종 멤버의 부모에서 루트까지의 모든 KEK들을 모두 바꿔어야 한다. 키 갱신 메시지는 갱신될 키를 그 노드의 상대적인 자식 노드의 KEK로 암호화한 것으로 구성되어 있다. 그 메시지의 크기는 많아야 $O(2 \log_2 n)$이다. (그림 1)에서 보듯이 영향을 받은 KEK들을 보여주는 예이다. 비밀키 K_3를 받은 새로운 구성원 U_3와 그의 최하위



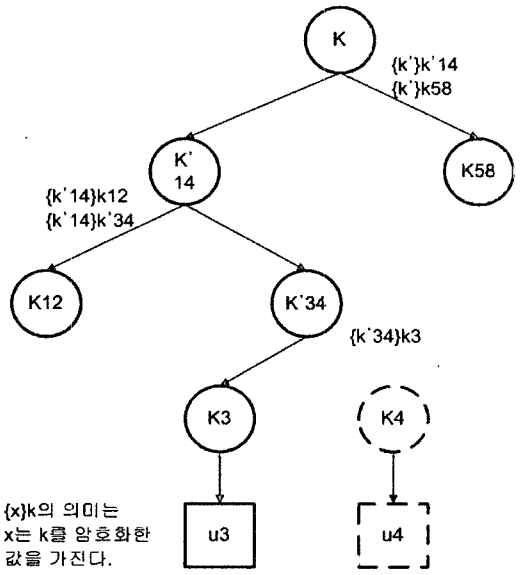
(그림 1) 구성원이 트리에 참가했을 때 영향을 미치는 EKE
(u^*: 사용자, K^*: 키 정보)

〈표 1〉 기존 방식

방식	특징
Group Key Management Protocol	• Group Key Packet(GKP)를 생성 • GTEK를 이용하여 새로운 키를 그룹 멤버에게 전달 • 탈퇴한 멤버는 갱신된 키를 알 수 있으므로 후에 기밀성을 보장할 수 없음
Dunigan and Cao's Group Key Management	• 각 그룹의 멤버는 GTEK와 GKEK라는 두개의 키 획득 • GTEK로 그룹 메시지를 암호화 • GKEK를 이용하여 새로운 키 쌍 GTEK, GKEK를 암호화하여 분배 • GKMP와 같은 단점을 가진다.
Scalable extension of Group Key Management Protocol	• GC(Group Controller)만이 새로운 키를 생성 • GC가 위협을 받게 되면 그룹 전체에 영향 • 구성원이 바뀌었을 때의 문제를 해결하지는 못함
Hierarchical Binary Tree	• 키 트리를 관리하는 현 명의 그룹 관리자 존재 • 트리의 노드는 모두 KEK를 포함 • 트리의 루트는 그룹키를 갖고 있다. 각 그룹의 멤버는 $\log_2^n$개의 키를 소유



(그림 2) 기초 HBT에서 구성원이 참가했을 때 필요한 암호화



(그림 3) 기초 HBT에서 구성원이 삭제되었을 때 필요한 암호화

노드 K_{34}의 노드에 붙는다. K_3에서부터 K까지의 길에 있는 노드들에게 K_{34}, K_{14}, K가 바뀌어야 한다. (그림 2)에서 새로 바뀐 $KEK(K_{34}^{'}, K_{14}^{'}, K^{'})$들을 보여준다. 마지막으로 이 새로운 KEK들은 각각의 상대적인 하위 노드의 KEK로 암호화된다. $K_{34}^{'}$는 K_3과 K_4로 암호화되고, $K_{14}^{'}$는 K_3과 K_{12}와 $K_{34}^{'}$로 암호화되며, K는 $K_{14}^{'}$와 K_{58}로 암호화된다. 키 갱신 메시지의 크기는 커봐야 $O(2\log_2 n)$개의 키로 구성 되어 있다. 멤버를 제거하는 것도 유사한 과정에 의해 이뤄진다. (그림 3)에서 살펴보면 멤버가 그룹에서 떠날 때 제거되는 멤버의 부모 노드의 KEK와 그 노드에서부터 루트까지의 노드에 의해 포함되는 모든 KEK들이 바뀌어야 한다. 키 갱신 메시지는 갱신되는 각각의 KEK들을 그 자식 노드의 KEK로 암호화 된 것으로 구성된다. 멤버 U_4가 그룹을 떠날 때, 키 K_{34}, K_{14}, K가 바뀌어야 한다. 따라서 새로 $K_{34}^{'}$, $K_{14}^{'}$, $K^{'}$이 생성되고, 이들은 노드의 상대적인 자식 노드의 키들로 암호화 되며, 예외는 $K_{34}^{'}$은 단지 K_3으로만 암호화 된다.

3. TRS 키 분배를 위한 요구사항

TRS상에서 키 분배를 위한 요구 사항들은 다음과 같다.

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 TRS용 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.

다음은 TRS에 적용하기 위한 요구사항에 대해 정리한다.

1) TRS Center 관리 : TRS 시스템에서는 각 그룹을 관리하는 관리자가 있으며, 전체 그룹, 개별 그룹 및 각 참여자에 관한 키를 분배할 수 있어야한다.
2) Trust Center 존재 유/무 : 인증 센터로써 최초 TRS center에게 각 참여자에게 전송될 키에 대한 정보를 발급하며, 전체 그룹 키에 대해서 갱신할 수 있어야 한다. 또한 TRS center에서 관리하는 그룹에서 생성할 수 있는 키가 분배되어야 한다.
3) 중계 노드 증가에 따른 중계 노드 키 증가 : 중계 노드가 증가와 상관없이 그룹에 속한 참여자는 동일한 그룹키가 생성되어야 한다.
4) 각 개체간의 상호 인증 : 각 개체는 서로 인증될 수 있어야하며, 상위 기관과의 인증도 할 수 있어야 한다.
5) 그룹 설정 시 병목 현상 문제 : 전체 그룹 및 개별 그룹을 설정하고 키를 분배하는데 있어 그룹 설정 상에서의 병목 현상은 발생하지 않아야한다.
6) 개별 키 생성의 용이 : 전송되는 키를 이용하여 각 참여자는 자신의 개별키를 생성할 수 있으며, 갱신이 용이해야 한다.
7) 그룹 키와 개별 키의 생성 : 그룹키 뿐만 아니라 개별키의 생성이 가능해야하며, 이는 TRS 상에서 그룹 통신뿐 아니라 개별 통신이 이뤄지기 때문이다.

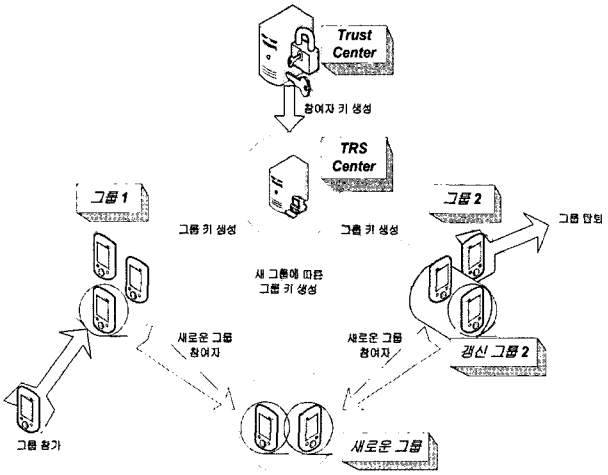
8) 키 갱신에 따른 키 갱신 그룹의 범위 : 전체 그룹에 따른 키는 전체 그룹을 대상으로 키 갱신이 발생되어야 하며, 개별 그룹에서의 키 갱신은 각 그룹에서 이뤄져야 한다.
9) 참가자 이동에 따른 키 갱신 : 참가자가 자신의 그룹을 벗어나 다른 그룹에 참여할 경우 기존 그룹과 신규 그룹의 키는 갱신되어야 한다.
10) 참여자 증가에 따른 키 증가 : 초기 참여자외에 새로운 참여자가 참가한다 하더라도 기존의 키를 갱신되어야 하고, 사용되는 키의 증가는 없어야 한다.
11) TRS 적용 가능성 : 그룹 통신에 적합한 키 분배 프로토콜이라 할지라도 TRS상에서 사용이 가능해야하며 각 개체의 특성에 적합하도록 설계되어야 한다.

4. 제안 방식

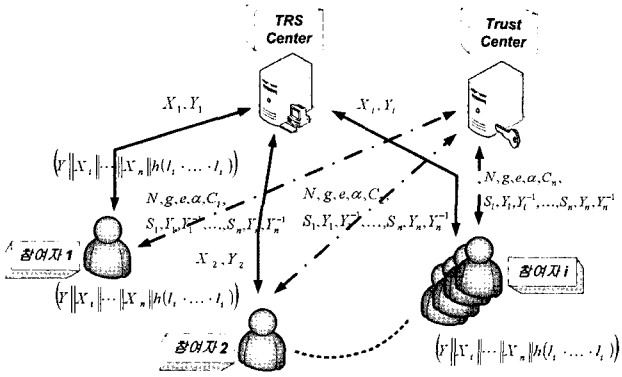
본 제안 방식은 ID-based 공개키 암호 시스템에 근거한다[3,4].

2절에서 기술한 기존 멀티캐스트 방식에 비하여 각 참여자는 키 인증과 TRS Center를 통해 안전성을 확보하고 있으며, 키 생성 시 2회 통신으로서 효율성도 높이고 있다. 특히 비밀 정보 생성을 위해 참여하는 TC(Trusted Center)는 키 생성에 별도로 참여하지 않음으로서, TC에 의한 부정의 소지를 막고 있다.

본 제안 방식의 시나리오는 (그림 4)와 같이 이뤄지며, 기본적으로 그룹 1과 그룹 2가 생성되어 있을 때, 기존 그룹은 그대로 유지하면서 그룹 1의 참여자와 그룹 2의 참여자가 새로운 그룹으로 그룹 통신을 원할 경우, 기존의 키를 그대로 이용하면서 각 참여자들에게 새로운 그룹 키를 생성하여 분배한다. 하지만 기존 방식에서는 전체 그룹을 새롭게 각각의 그룹 1, 그룹 2, 새로운 그룹을 각각 생성하고 있다. 이에 본 방식에서는 기존 그룹 1과 2의 참여자는 계속



(그림 4) 제안 방식 시나리오



(그림 5) 그룹 키 생성 단계

적인 통신을 지속하면서 새로운 그룹의 키 생성과 갱신 측면에서 많은 오버헤드 발생을 줄이고, 각 그룹 내의 참여자 간 개별 통신을 실시하고자 하는 경우에도 그룹에서의 키와는 별도로 새로운 키를 수립하는 방식을 제안한다.

4.1 참여 객체와 시스템 계수

본 방식에서 사용되는 참여 객체는 TRS Center, Trust Center, 그리고 참여자로 구성된다. 또한 본 논문에서는 공개키 암호시스템에 근거하여 수행한다.

- *TC* : *Trust Center*로 모든 참여자 정보와 *TRS Center* 정보를 가진다. 참여자의 그룹키 생성을 위해 참여자로부터 정보가 등록되고, 등록된 정보는 *TRS Center*로 전송하여 키 생성에 사용된다. 또한 최초 참여자 그룹은 정해지며, 이 정보 또한 *TRS Center*에 제공된다.
- *TRS Center* : Trunked Radio System Cnter로써 *TC*로부터 참여자 정보를 제공받아 키 생성을 수행한다. 최초 그룹에 대한 키 생성뿐만 아니라 신규 그룹에 대한 키 생성도 모두 *TRS Center*에서 수행한다.
- 참여자 : 그룹 통신의 주체가 되며 최초 등록은 *TC*를 통해서 실시한다. 등록 후 *TRS Center*로부터 자신이 가입된 그룹의 키를 제공받아 사용한다.

본 방식의 시스템 계수는 다음과 같다.

- *TC* : *Trust Center*로 *TRS Center* 키 생성을 위한 비밀 정보 생성 기관(신뢰할 수 있는 제 3자)
- *TRS Center* : 참여자 키 분배 노드
- NA_i : 새로운 그룹 생성 참여자들 ($i=1,2,\ldots,n$)
- A_i : 참여자들 ($i=1,2,\ldots,n$)
- $f(\ ), h(\ )$: 일방향 해쉬 함수
- ID_i : 참여자 A_i의 ID
- (e, d) : $ed=1 \bmod L$이 되는 공통 공개키 및 비밀키
- l_i $(=f(ID_i, j))$: 참여자 ID_i 정보

- X_i, NX_i : 참여자가 생성하는 키 구성 요소(개별, 그룹, 신규 그룹 키 생성 시 사용)
- Y_i, NY_i : 참여자가 생성하는 키 구성 요소(개별, 그룹, 신규 그룹 키 생성 시 사용)
- C_i : 참여자 키 생성에 필요한 검증 요소
- K : TRS 그룹 통신용 키
- NK : TRS에서 새로운 그룹 통신용 키
- $E_k(\ )$: 암호화 함수
- S_i : 참여자 i의 비밀키
- Y_i, Y_i^{-1} : 참여자 i의 그룹키 은닉 정보 및 역수

4.2 각 단계별 구성

본 논문은 크게 개별 참여자 키 생성 단계, 그룹 키 생성 단계, 신규 그룹 키 생성 단계로 이뤄지며, 세 가지 단계에서 기본적으로 이뤄지는 참여자 등록을 거쳐 세부 단계로서 각각의 키 생성 단계로 이뤄진다. 다음 각 단계별 기술에 앞서 참여자 등록 단계를 기술하고 각각의 단계에 대해 기술한다. 본 논문에서 그룹 키 생성과 관련된 부분은 (그림 5)와 같다. 각 단계에서 이뤄지는 키 생성은 다음과 같이 이뤄지며 최종적으로 참여자들에게 키가 분배되며, 참여자들은 자신의 키를 이용하여 메시지를 전송하게 된다.

4.2.1 참여자 등록 단계

- TC (*Trust Center* : 키 발급을 위한 비밀 정보 생성 기관)

: 참여자 A_i가 ID_i를 TC에 등록하게 되면 다음과 같은 일을 수행한다. 이때 TC는 최초 그룹에 대한 참여자 정보를 가지고 있으며, 이 그룹 정보는 *TRS Center*에 전송된다.

Step 1. TC에서는 세 개의 큰 소수 p, q, g를 생성하고 비밀리에 유지한다.

Step 2. TC는 다음 조건을 만족하는 정수 (e, d)를 결정한다.

$$ed = 1 \pmod{L} \qquad L = lcm((p-1)(q-1))$$

Step 3. 각 참여자 A_i에 대하여 다음과 같이 C_i를 계산하고, 개별 키 생성을 위해 α_i값을 생성한다.

$$l_i = f(ID_i, j) \quad (i = 1,2,\ldots,n \;\; j = 1,2,\ldots,k)$$

$$C_i = l_i^d \bmod n$$

Step 4. 큰 소수 $P_i (i = 1,\ldots,n)$를 생성하여 안전하게 저장하고, 참여자 탈퇴에 대한 새로운 그룹 키 갱신을 위한 참여자 비밀키 정보 $GCD(S_i, S_j) = 1$(단, $S_i \neq S_j$)를 계산한다. 현재 그룹 키 생성 정보 K_1에 대칭 은닉 정보 및 역수를 계산한다.

$$Y_i = K_i^{S_i} \pmod{P_i}, \quad Y_i^{-1}$$

: TC는 참여자 i의 참여 유무를 판단한 다음 $(n, g, e, \alpha_i, C_i, S_1, Y_1, Y^{-1}, S_2, Y_2, Y_2^{-1}, \ldots, S_n, Y_n, Y_n^{-1})$를 스마트 카드에 저장하여 각 참여자에게 전달한다. 이때, p, q, d는 TC만이 알고 있는 정보이다. 저장되는 값 중 $(S_i, Y_i, Y_i^{-1})(i = 1, 2, \ldots, n)$는 참여자 탈퇴 등으로 인한 그룹 키 갱신에 사용되는 시스템 계수이다.

4.2.2 개별 참여자 키 생성 단계

- 참여자 A_i

: 참여자 A_i는 랜덤 수 $r_i \in Z_n$을 선택한다.

Step 1. 각 참여자는 키를 생성하기 위하여 $X_i = g^{r_i e} \bmod n$와 $Y_i = (C_i \cdot X_i)^e \bmod n$을 계산한다.

Step 2. 각 참여자는 계산된 값 X_i, Y_i과 $h(l_i)$를 연접한 정보 $(X_i \| Y_i \| h(l_i))$를 소속 *TRS Center*에 전송한다.

- *TRS Center*

: *TRS Center*는 TC로부터 그룹에 대한 정보와 각 참여자의 정보 (n, g, e, α_i, C_i)를 전송받는다.

Step 1. *TRS Center*는 $h(Y_i / X_i^e \bmod n) = h(l_i)$을 계산한다.

: 같으면 전송된 정보가 정당한 참여자로부터 온 것임을 확인하고, X_i, Y_i중 Y_i을 보관한다. *TRS Center*는 각 참여자의 개별키 PK_i를 다음과 같이 생성한다.

$$PK_i = (X_i)^{\alpha_i} \bmod n$$

Step 2. 참여자는 확인된 메시지를 받고 자신이 생성한 X_i를 이용하여 자신의 개별키 PK_i를 계산한다.

$$PK_i = (X_i)^{\alpha_i} \bmod n$$

Step 3. 참여자는 생성된 개별키 PK_i를 이용하여 암호문을 전송한다.

$$E_{PK_i}(M)$$

4.2.3 그룹 키 생성 단계

- *TRS Center*

: *TRS Center*는 각 참여자 A_i가 개별 키 생성 단계에서 전송한 정보 $(X_i \| Y_i \| h(l_i))$를 이용한다. 또한 *TRS Center*는 최초 그룹의 설정은 TC에서 정해진 참여자 $(i = 1,\ldots,k)$에 의해 설정한다.

Step 1. *TRS Center* 는 정해진 참여자(k명)에 대하여 $Y = (Y_1 * Y_2 * \cdots * Y_k) \bmod n$을 계산하고, $(Y \| X_1 \| \ldots \| X_k \| h(l_1 * \cdots * l_k))$를 그룹의 각 참여자에게 전송한다.

• 참여자 A_i

: 참여자 A_i는 다음이 성립하는지 확인한다.

Step 1. $h(Y/(X_1 * \cdots * X_k)^e \bmod n) = h(l_1 * \cdots * l_k)$을 계산한다.

: 같다면 전송된 정보가 *TRS Center*로부터 온 것임을 검증하고, 자신의 속한 그룹의 인원수를 확인한다.

Step 2. 각 참여자는 확인한 인원수 정보와 X_i정보들을 이용하여 $K=(\prod_{i=1}^{k} X_i) \bmod n$을 계산하여 그룹 키를 획득한다.

Step 3. 생성한 그룹 키 K를 이용하여 그룹 통신을 한다.

4.2.4 신규 그룹 키 생성 단계

본 절에서의 신규 그룹은 기본적으로 두 개의 그룹이 생성되어 있을 때, 기존 그룹은 그대로 유지하면서 기존 그룹의가 새로운 그룹으로 그룹 통신을 원할 경우를 의미한다. 이때, 기존 그룹 키는 그대로 유지하면서 참여자들에게 신규 그룹의 키를 생성하여 분배하는 방식이다.

• 새로운 그룹 생성 참여자 NA_i

: 새로운 그룹 생성 참여자 NA_i는 그룹 생성을 위해 랜덤수 $a_i \in Z_n$를 선택하여 자신의 개별 키에 다음과 같이 NX_i, NY_i 생성하고 *TRS Center*에 전송한다.

Step 1. 참여자는 $NX_i (= g^{r \cdot e^{a_i}} \bmod n)$와 $NY_i (= (C_i \cdot NX_i)^e \bmod n)$을 계산하고, $h(l_i)$를 연접한 정보 $(NX_i \| NY_i \| h(l_i))$를 소속 *TRS Center*에 전송한다.

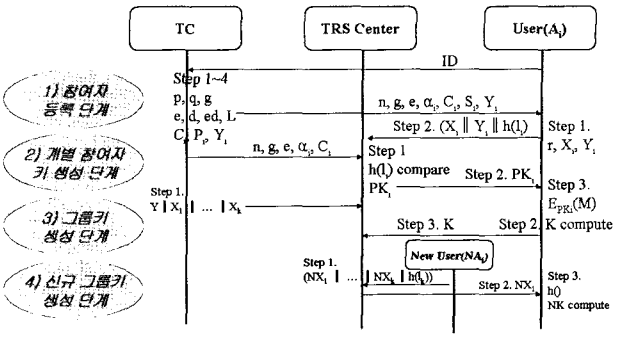
• *TRS Center*

: *TRS Center*는 새로운 그룹 참여자(j명)에 대해 다음이 성립하는지 확인한다.

Step 1. *TRS Center* 는 다음 $h(NY_i/NX_i^e \bmod n) = h(l_i)$ 을 계산한다.

: 같으면 전송된 정보가 정당한 참여자로부터 온 것임을 확인하게 된다. *TRS Center*는 $NY=(NY_1 * NY_2 * \cdots * NY_j) \bmod n$를 계산해 수신자의 NX_i와 연접해 각 참여자에게 전송한다.

Step 2. *TRS Center*는 다음과 같이 NY을 계산하고, $(NY \| NX_1 \| \ldots \| NX_j \| h(l_1 * \cdots * l_j))$를 새로운 참여자에게 전송한다.



(그림 6) 각 단계별 흐름도

• 새로운 그룹 생성 참여자 NA_i

: 새로운 그룹 생성 참여자 NA_i는 다음이 성립하는지 확인한다.

Step 1. $h(NY/(NX_1 * \cdots * NX_j)^e \bmod n) = h(l_1 * \cdots * l_j)$을 계산한다.

: 검증이 완료되면 새로운 그룹 생성 참여자들 간에 사용할 수 있는 그룹 키를 생성한다.

Step 2. 각 참여자는 다음의 연산 $NK=(\prod_{i=1}^{j} NX_i) \bmod n$을 수행하여 키를 획득한다.

Step 3. 생성한 키 NK를 이용하여 그룹 통신을 이용한다. 이때 생성된 키는 각 그룹에 속한 참여자에 해당하는 키 정보이다.

4.2.5 그룹 키 갱신 단계

다음은 참여자 탈퇴에 따른 그룹키 갱신 단계에 대한 과정이다.

• 새로운 그룹 키 갱신

: 본 과정에서는 2명의 참여자 A_x, A_w가 탈퇴한 경우를 가정하고 기술한다.

Step 1. *TRS Center*는 탈퇴 참여자를 확인하고, A_x, A_w를 제외한 모든 참여자들에게 다음의정보를 전송한다.

$$(P_x, S_x, Y_x, Y_x^{-1}), (P_w, S_w, Y_w, Y_w^{-1})$$

step 2. 참여자 i는 수신된 정보를 이용하여 다음을 만족하는 a_t, b_t $(t \in \{x, w\})$를 계산한다. a_t, b_t는 확장된 유크리드 알고리즘을 이용하여 polynomial time 안에 계산 가능하다.

$$a_w * S_w + b_w * S_i = 1$$

$$a_x * S_x + b_x * S_i = 1$$

〈표 2〉 멀티캐스트 키 분배에 따른 제안방식과 기존방식간의 비교 분석

항목 \ 대상	Clique	기존 CA	Iolus	GKMP	DK	제안 방식
메시지 암호키의 수	3	n-1	3	5	7	3
암호 방식 (대칭, 대칭)	(O,O)	(O,O)	(O,O)	(O,X)	(O,O)	(O,O)
참가자 증가에 따른 키 증가	X	X	X	X	X	X
탈퇴자에 대한 참가자 보안성	O	O	O	O	O	O
참가자 수에 따른 중계 라우터 키의 양	변화 없음	증가	증가	증가	증가	변화 없음
상호 인증성	O	O	O	O	O	O
통신 신뢰성	X	O	X	O	O	O
병목현상 극복	O	X	X	O	O	O
키 갱신 범위	ALL	ALL	Sub-Group	Sub-Group	ALL	Sub-Group
메시지 전송시 암/복호화 회수	1	n	j	k	1	2
통신 회수	2(n-1)	n+1	j+js	j+js+1	j+n	js+1
키 분배 방식 적용(통신 회수)	2(n-1)	n+1	j+js	j+js+1	j+n	js+1
키 분배 방식 적용(연산량)	Z(n-1)	Z(n+1)	Z(j+js)	Z(j+js+1)	Z(j+n)	Z(js+1)

k : 도메인 수 j : 중간 관리자(중계 라우터) 수 s: subgroup 멤버 수 n: 그룹 멤버들의 수 Z = (n+2)c+k(c+1)

〈표 3〉 TRS 적용에 따른 기존 방식과 제안방식 비교 분석

항목 \ 대상	중앙집중식 방식		분산형방식		분산 서브 그룹형 방식	제안방식
	CA	GKMP	Clique	DK	Iolus	
TRS Center 관리	O	O	X	X	X	O
Trust Center 필요성	일부 필요	일부 필요	필요	필요	필요	필요
중계 노드 증가에 따른 중계 노드 키 증가	증가	증가	변화없음	변화없음	증가	변화없음
각 개체간의 상호 인증	O	O	O	O	O	O
그룹 설정 시 병목 현상 문제	X	O	O	X	X	O
개별 키 생성의 용이	X	X	X	X	X	X
그룹 키와 개별 개인키의 생성	O	X	X	X	X	O
키 갱신에 따른 키 갱신 그룹의 범위	ALL	일부 Subgroup	ALL	ALL	일부 Subgroup	Subgroup
참가자 이동에 따른 키 갱신	X	X	O	O	X	O
참여자 증가에 따른 키 증가	X	X	X	X	X	X
TRS 적용 가능성	O	O	X	X	X	O

O : 제공, △ : 일부 제공, X: 제공하지 못함

: 각 참여자는 다음을 계산한다.

$a_i < 0$인 경우,

$$\left(Y_w^{-1}\right)^{-a_w} \cdot Y_i^{b_w} \pmod{P_w} = K_w^{a_w \cdot S_w + b_w \cdot S_i} \pmod{P_1} = K_w'$$

$$\left(Y_x^{-1}\right)^{-a_x} \cdot Y_i^{b_x} \pmod{P_x} = K_x^{a_x \cdot S_x + b_x \cdot S_i} \pmod{P_1} = K_x'$$

$b_i < 0$인 경우,

$$Y_w^{a_w} \cdot \left(Y_i^{-1}\right)^{-b_w} \pmod{P_w} = K_w^{a_w \cdot S_w + b_w \cdot S_i} \pmod{P_1} = K_w'$$

$$Y_x^{a_x} \cdot \left(Y_i^{-1}\right)^{-b_x} \pmod{P_x} = K_x^{a_x \cdot S_x + b_x \cdot S_i} \pmod{P_1} = K_x'$$

: 참여자는 계산된 정보를 통해 새로운 그룹키 RK를 갱신한다.

$$RK = \prod_{t=1}^{2} K_t' \pmod{n} \quad (t \in \{x, w\})$$

4.2.6 신규 참여자 가입 단계

신규 참여자가 기존 그룹에 가입할 때 다음의 과정을 따른다.

- *TC*

: 신규 참여자가 기존 그룹에 가입하고자 하는 경우 신규 참여자 A_{New}가 ID_{New}를 *TC*에 등록하고, *TC*는 신규 참여자의 그룹 참여 정보를 *TRS Center*에 전송한다. 이후 과정은 참여자 등록 단계에서 *Step 1.* ~ *Step 3.* 의 과정을 수행하고 신규 참여자에게 $(n, g, e, \alpha_{New}, C_{New})$를 스마트카드에 발급하여 전송한다.

- 신규 참여자 A_{New}

: 신규 참여자 A_{New}는 랜덤수 $r_{New} \in Z_n$을 선택하고 개별 참여자 키 생성 단계를 거쳐 X_{New}, Y_{New}를 생성한다.

- *TRS Center*

:신규 참여자의 X_{New}, Y_{New}에 대하여 신규 참여자에 포함된 그룹키 정보 $h\left(Y/\left(X_1 \cdot \cdots \cdot X_{\neq w} \cdot \cdots \cdot X_k\right)^e \bmod n\right) = h\left(l_1 \cdot \cdots \cdot l_{\neq w} \cdot \ldots \cdot l_k\right)$를 전송하면 기존 그룹 참여자들은 정보와 그룹에 대한 인원수를 재확인하고 그룹키를 생성한다.

5. 기존 방식과 제안 방식의 비교 분석

본 제안 방식은 각 참여자들과 TRS Center가 인증을 통해 해쉬된 신원 정보을 확인할 수 있게 함으로서 제 3자의 불법적 행위를 방지할 수 있으며, TC가 키 생성에 참여하지 않으므로 신뢰성을 높일 수 있었다. 또한, TRS Center를 도입함으로서 중간 단계의 안전성을 확보할 뿐만 아니라, 참여자들의 통신량에 대한 총 라운드 수를 2회로 줄임으로서 효율성을 확보하고 있다. <표 2>는 각 방식별 특징을 비교 분석한 것이다.

또한 본 논문의 3장에서 제시한 TRS 키 분배를 위한 요구사항에 따른 분석에 의하면 안전성 측면에서 키 분배 프로토콜은 제 3자에 의한 불법적 행위로부터 안전성을 획득하여야한다. 위 문제점에 대하여 본 논문의 제안 방식은 공개키 방식을 이용하여 안전성을 제공하였으며, 특히 참여자가 초기 TC에 값을 등록할 때 $C_i \equiv l_i^d \bmod n$으로 하여 제공되는 l_i에 대해 안전성을 확보하였다. 또한 키 생성에 있어 참여자는 각 X_i, Y_i를 계산하여 전송함으로써 이전 등록 단계에서 분배된 정보를 가지고 있지 않는 참여자는 계산이 불가함으로써 안전성을 유지하였다.

다음은 인증성으로 모든 TRS 참여자들은 키 인증을 통해 출처 및 무결성을 확인할 수 있어야 하는데 본 제안방식 키 생성 단계에서 본 요구사항을 만족할 수 있도록 설계하였다. 본 논문에서 참여자는 각 X_i, Y_i를 계산하여 $X_i, Y_i, h(l_i)$를 전송하게 되면 이에 대한 키 인증은TRS Center에서 이뤄지게 된다.$\left(h\left(Y_i / X_i^e \bmod n\right) = h(l_i)\right)$ 또한 전체 참여자 키 인증은 각 수신자의 X_i값을 연접하여 참여자에게 전송함으로써 전체 키 인증 및 참여자 측에서의 키 인증이 이뤄지게 된다. 각 참여자는 $K = \left(\prod_{i=1}^{n} X_i\right) \bmod n$을 수행함으로써 키를 획득하고 키에 대한 인증과정을 마치게 된다. 각 구조를 그룹 키 분배 방식에 적용했을 경우 사용자 측면에서의 연산량을 구하여 비교 분석해 본다, 먼저 각 키 분배 방식에 따른 지수승(Exponential) 연산량을 구해보면 다음과 같다.

U = 2k : Diffie-Hellman 방식의 Exponential 연산량
W = nc : ITW 방식의 Exponential 연산량
X = ck(3+n)+6c : KO 방식의 Exponential 연산량
Y = c(2n+4) : BD 방식의 Exponential 연산량

여기서 c는 상수이고 k는 키 크기이다. 각 방식의 Exponential 연산량은 키 분배에 참여하는 멤버와 라우터에서 계산되어 지는 연산량이므로 각 방식별 키 분배 방식에 따른 연산량을 구해보면 다음 <표 3>과 같다. 여기서 중계 라우터간의 키 분배에 있어 사용되어 지는 키가 불확실하며, 사용자 측면에서의 연산량을 살펴보기 때문에 라우터 간의 키 분배 연산량은 고려하지 않는다. 따라서 본 논문에서 제시하고자 하는 연산량 측면과 통신횟수, 마지막으로 키의 생성에서 살펴보았을 때 기존방식보다 장점을 가진다고 할 수 있다.

마지막으로 통신 횟수에 대한 요구 사항으로써 이는 회의 참여자 수와는 상관없이 일정해야함을 의미한다. 각각의 객체에 따른 통신 회수를 살펴보면 TC는 자신이 생성한 (n, g, e, α, C_i)를 연산하여 스마트 카드에 저장하여 참여자에게 전송함으로 이에 대한 통신횟수는 고려하지 않는다. *TRS Center*는 참여자에게서 전송되어온 키에 대한 인증과정을 거치게 됨으로 총 2회의 통신으로써 제공할 수 있게 된다. 마지막으로 각 참여자는 2회의 통신으로 제공될 수 있는데 이는 기존 방식에서 보다 참여자가 증가할지라도 통신횟수는 그대로 유지되면서 빠르게 키 분배를 할 수 있는 장점을 가지고 있다.

6. 결 론

주파수공용통신 시스템은 미국과 일본에서는MCA(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 ID-based 방식에 근거하고 있으며, 각 참여자들과 TRS Center가 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, TRS Center를 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.

참 고 문 헌

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

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

[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,

pp.175-184, 1988.

[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, pp.429-433, 1988.

[6] E. Brickell, P. Lee and Y. Yacobi, "Secure Audio teleconference," Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science 293, pp.418-42, 1988..

[7] H. Harney and C. Muckenhirn, "Group key management protocol (GKMP) architecture," RFC 2094.

[8] T. Dunigan and C. Cao. Group Key Management. Technical. Report ORNL/TM-13470, 1998.

[9] R. Poovendram, S. Ahmed, S. Corson, and J. Baras. A Scalable Extension of Group Key Management Protocol. 2nd Annual ATRIP Conference, pp.187.191, February, 1998.

[10] Guang-huei Chiou, Wen-Tsuen Chen, "Secure Broadcasting Using the Secure Lock," IEEE Transactions on Software Engineering, Vol.15, Issue 8, pp.929-934, 1989.

[11] D.A.McGrew and A.T.Sherman, "Key Establishment in Large Dynamic Groups: Using One-Way Function Trees," Technical Report 0755, TIS Labs, 1998.

[12] A. Aziz, T. Markson and Prafullchandra, "Simple Key-Management Internet Protocols(SKIP)," IETF fraipsec-skip-03.txt, Oct., 1995.

[13] A. Ballardie, "Scalable Multicast Key Distribution," RFC1949, May, 1996.

[14] A. Ballardie, "Core Based Tree(CBT)Multicast Routing Architecture," Request for Comments2201, Internet Activities Board, Oct., 1997.

[15] C. Perkins, "IP mobility support," RFC 2002.

[16] D.A.McGrew and A.T.Sherman, "Key Establishment in Large Dynamic Groups: Using One-Way Function Trees," Technical Report 0755, TIS Labs, 1998.

[17] H. Harney and C. Muckenhirn, "Group Management Protocol(GKMP) Architecture," IETF RFC 2094, 1997.

[18] K. Matsuura, Y. Zheng and H. Imai, " Compact and Flexible Resolution of CBT Multicast Key-Distribution," WWCA98, 1998.

[19] M. Moyer, J. Rao and P. Rohatgi, "A Survey of Security Issues in Multicast Communications," IEEE Network, Nov/Dec, 1999.

[20] R. Poovendram, S. Ahmed, S. Corson, and J. Baras. A Scalable Extension of Group Key Management Protocol. 2nd Annual ATRIP Conference, pp. 187.191, February, 1998.

[22] T. Dunigan and C. Cao. Group Key Management. Technical. Report ORNL/TM-13470, 1998.

[23] 박희운, 이임영, "효율적인 회의용 키 분배 방식에 관한 연구", 한국통신정보보호학회 충청지부, 1999.

[24] 김봉한, 이명선, 이재광, "Mbone 구현을 위한 IP멀티캐스트 라우팅 프로토콜", 정보처리학회지, Vol.6, No.4, 1999.

이 덕 규

e-mail : deokgyulee@etri.re.kr

2001년 2월 순천향대학교 컴퓨터공학과 (학사)

2003년 2월 순천향대학교 전산학과(석사)

2006년 2월 순천향대학교 전산학과(박사)

2006년 9월~현재 한국전자통신연구원 정보보호연구단 Post-Doc.

관심분야 : Broadcast Encryption, Key management, Ubiquitous

박 용 석

e-mail : parkys@etri.re.kr

1995년 2월 경북대학교 전자공학과(공학사)

1997년 2월 경북대학교 전자공학과(공학석사)

1997년~1999년 LG전자

2000년~현재 국가보안기술연구소 연구원

관심분야 : 이동통신 정보보호

안 정 철

e-mail : jcahn@etri.re.kr

1987년 2월 한양대학교 전자공학과(학사)

1990년 2월 전북대학교 전자공학과(석사)

1996년 9월 동경공업대학 전자공학(박사)

1990년 2월~1999년 12월 한국전자통신연구원 선임연구원

2000년 1월~현재 국가보안기술연구소 팀장

관심분야 : 회로 및 시스템, 이동통신, 정보보호응용

이 임 영

e-mail : imylee@sch.ac.kr

1981년 8월 홍익대학교 전자공학과(학사)

1986년 3월 오사카대학 통신공학전공(석사)

1989년 3월 오사카대학 통신공학전공(박사)

1989년 1월~1994년 2월 한국전자통신연구원 선임연구원

1994년 3월~현재 순천향대학교 정보기술공학부 정교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안