유·무선 멀티캐스트 키 관리 기법 제안

박희운*O, 이임영*, 박원주**, 나재훈**
*순천향대학교 정보기술공학부
**한국전자통신연구원 정보보호기술본부 인터넷보안연구팀
phu24@hotmail.com, imylee@sch.ac.kr, {wjpark, jhnah}@etri.re.kr

A Proposing The Wire and Wireless Multicast Key Management Scheme

Hee-Un Park*O, Im-Yeong Lee*, Won-Joo Park**, Jae-Hoon Nah**
*Division of Information Technology, Soon-chun-hyang University
**Internet Security Research Team, Information Security Technology Department, ETRI

요 약

통신 및 컴퓨터의 보급 발전을 통해 새로운 정보 사회의 패러다임이 정립되고 있다. 특히 유·무선 네트워크 상에서 그룹 기반 통신 응용 서비스의 요구 증가는 더욱 빠르고 정확한 정보 통신의 한 축으로서 매우 중요한 의미를 부여받고 있다. 이러한 필요성에 따라 멀티캐스트 기반 구조에 대한 연구가 활발히 진행되고 있다. 그러나 유·무선 멀티캐스트 키 관리 구조에 대한 안전성과 효율성 및 확장성 부분에 대한 해결책은 아직 미비한 상태이다. 본 연구에서는 유선 및 무선에서 멀티캐스트 서비스 지원을 위해 필요한 요구 사항들을 고찰함과 동시에 안전성과 효율성 및 확장성을 제공하는 새로운 멀티캐스트 키 관리 기법을 제안한다.

1. 서론

인터넷과 같은 공용 네트워크의 발전과 컴퓨터의 보급 확산은 개인 매체를 통한 전세계적인 정보 공유의 새로운 정보화 패러다임을 가시화 시키고 있다. 동시에 무선 통신 서비스의 확대는 단순한 개인 PC를 넘어서 공용 가시화 네트워크의 범위를 한층 높이고 있다. 이러한 상황에서 사용자들은 단순한 유·무선 통신에서 벗어나 다자간 통신 회의, 원격 의료 진단 및 상담 등 다양한 서비스를 요구하고 있다. 이러한 요구들은 기본적으로 그룹 기반의 서비스를 전재로 하고 있으며, 현재 가장 각광 받고 있는 방식 중의 하나가 멀티캐스트 기법이다.[1]~[5]

멀티캐스트란 그룹에 참가한 멤버들을 대상으로 단일 송신자로부터 그룹에 소속된 멤버들에게 안전한 데이터 전송을 수행하는 방법을 의미한다. 이때 그룹 멤버가 해당 그룹을 떠나면 더 이상 정보를 수신할 수 없어야 한다. 동시에 멀티캐스트 기법은 기존의 통신 방식에 대해 그룹에 참가한 송신자의 전송 오버헤드, 네트워크 대역폭 및 지연을 감소시키는 장점을 제공한다.

그러나 멀티캐스트 서비스는 인터넷 및 공중파를 그 매체로 하기 때문에, 보안상의 취약성에 노출되고 있다. 특히 불법적인 제 3자의 도청이나 전송 정보의 위조는 그 대표적인 예가 된다.

이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위해 다양한 암호 기법들이 적용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요하다. 동시에 회원의 가입 및 탈퇴 그리고, 무선 이동 상에서의 익명성 및 Hand-Off 허용을 위해서는 확장성이 보장되어야 한다.[6]~[10]

현재 유·무선 멀티캐스트 키 관리 분야와 관련하여, 그 중요성에도 불구하고 해결책들은 미흡한 상황이다. 따라서 본 연구는 향후 광범위하게 적용될 유·무선 멀티캐스트 서비스에서 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고찰함과 동시에 새로운 멀티캐스트 키 관리 기법을 제안하고, 요구 사항 만족도 측면에서 비교 분석을 수행한다.

2. 유·무선 멀티캐스트 키 관리를 위한 요구사항

다자간 통신을 전재로 하는 멀티캐스트 서비스는 여러 위협 요소에 노출되어 있다. 다음은 유·무선 멀티캐스트 키 관리를 위해 요구되는 사항을 기술한 것이다.

2.1 일반적인 요구 사항

- **무결성** : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- **인증성** : 송·수신 정보의 무결성 및 정당한 멤버들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- **접근 제어** : 정당한 그룹의 소속원만이 멀티캐스트 정보에 접근할 수 있다.
- **부인 봉쇄** : 참여 개체간에 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자의 확인이 가능해야 한다.

본 연구는 2001년도 한국전자통신연구원 위탁연구과제 지원 사업을 통해 수행된 것입니다.

- **비밀성** : 전송 및 저장되는 멀티캐스트 정보는 불법적인 제 3자로부터 보호되어야 한다.

2.2 동적 그룹 변동에 따른 요구 사항

- **공정성** : 멀티캐스트 키의 접근은 허가된 그룹 멤버만이 가능하며, 키 갱신 프로토콜은 필수적이다. 이를 위해 서버의 독단 및 제 3자와의 불법적 결탁을 방어하기 위한 공정성이 확보되어야 한다.
- **확장성** : 멀티캐스트 서비스 그룹 참여자의 변동에 따른 동적인 키 관리 기법이 필요하다.

2.3 무선 및 원격 호스트 서비스를 위한 요구 사항

- **익명성** : 멀티캐스트 멤버의 위치는 허가된 실체 외에는 확인할 수 없어야 한다.
- **Hand-Off 허용** : Mobile IP상에서 가입자는 이동성을 가지고 있다는 특성을 가지고 있다. 이때 가입자가 새로운 셀(Cell) 범위로 진입할 경우, 새로운 원격 호스트와 새로운 세션키를 통해 메시지를 송/수신해야 한다. 이를 위한 인증 및 안전성 확보는 필수적인데, 이러한 일련의 과정을 Hand-Off 과정이라 한다. 이동성을 갖는 사용자에 있어 Hand-Off 허용 여부는 중요한 의미를 갖는다.

2.4 무선 멀티캐스트 키 분배 및 갱신관련 요구사항

- **통신 병목 현상** : 무선 단말기의 특성상 효율성 유지를 위해 통신 메시지의 길이는 작아야 하며, 통신 횟수는 최소가 되어야 한다.
- **키 갱신 준비 단계 overhead** : 멀티캐스트 키의 분실 또는 멤버의 탈퇴에 따른 키 갱신은 별도의 준비 단계로 인한 overhead를 최소화시켜야 한다.
- **그룹 멤버간 담합 방지** : 그룹에 속한 멤버라 할지라도 향후 사용될 멀티캐스트 키를 확인할 수 없어야 한다.
- **2명 이상의 동시 갱신 허용** : 2명 이상의 멤버가 자신들의 단말기를 분실하거나 탈퇴할지라도, 키 갱신 횟수는 최소화되어야 한다.

3. 유·무선 통합 멀티캐스트 키 관리 구조 제안

본 방식은 상기 제시되었던 요구 사항을 만족하기 위하여 수신자 지정 그룹 서명 방식과 무선 그룹 키 갱신 방식을 적용한다. [7],[9]

3.1 구성 요소 및 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수 및 구성 요소를 기술하고 있다.

- DKM_i : 도메인 키 관리자 i
- DMB_i : Domain Border i
- DKA_i : 도메인 키 중간 관리자 i
- SGB_i : Subgroup Border i
- MGB_i : Multicast Group Border i
- GML : 그룹 멤버 리스트
- PKM : 각 참여 개체들의 공개키 관리자
- MBR_i : 그룹 멤버 i
- R, GI : 라우터 및 그룹 초기자
- MKey : PKM에 의해 생성된 멀티캐스트 키
- K_{PP}, K_{PS} : PKM의 공개키 및 개인키
- K_{DPi}, K_{DSi} : 각 DKM_i의 공개키 및 개인키
- K_{DAPi}, K_{DASi} : 각 DKA_i의 공개키 및 개인키
- K_{DMBPi}, K_{DMBSi} : 각 DMB_i의 공개키 및 개인키
- K_{MGBPi}, K_{MGBSi} : 각 MGB_i의 공개키 및 개인키
- K_{SGBPi}, K_{SGBSi} : 각 SGB_i의 공개키 및 개인키
- K_{D_DAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MSi} : 그룹 멤버 MBR_i의 비밀키
- K_{DAi_Msj} : 각 DKA_i와 멤버들과의 공통키
- ID_*, IP_*, Sig_* : *의 식별자, IP 주소 및 서명
- M, Hdr : 멀티캐스트 메시지 및 식별 정보
- K_{GSi}, K_{GVi} : 수신자 지정 그룹 서명/확인 키
- T, Tr : 멤버 및 원격 호스트의 Time-Stamp
- RH_i : 원격 호스트 i
- Req_WMS : 무선 멀티캐스트 서비스 요청
- K_{RPi}, K_{RSi} : 원격 호스트 i의 공개키 및 개인키
- P_j : DKA_i가 생성하는 큰 소수
- Ter_i : 각 사용자의 무선 터미널 (i={1, 2, ..., n})
- Y_{ij}, Y_{ij}^{-1}: Subgroup 공통키 은닉 정보 및 역수
- S_{ij} : DKA_i에 의해 생성되는 Subgroup 멤버 i의 비밀 정보
- Ref_key : Subgroup 공통키 갱신 정보

3.2 시스템 프로토콜

3.2.1 도메인 초기화 단계

1) DKM_i, DKA_i 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 PKM으로부터 수신한다.
2) 각 도메인은 DKM_i를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다.

3.2.2 그룹 초기화 단계

1) GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 ID_{GI}와 함께 서명을 수행하여 PKM에게 전송한다.
2) PKM은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들(SGB_i, DMB_i, MGB_i)에게만 제공함으로서 신뢰성을 높이고 있다.
3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

3.2.3 그룹 멤버 가입 단계

1) DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{D_DAi}를 생성하여 유니캐스트 채널을 통하여 안전하게 DKA_i에게 전송한다.
2) 그룹에 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i에게 자신을 인증한다. 이때 멤버 가입 대상자들 중 무선 멀티캐스팅 서비스를 필요로 할 경우, 무선 멀티캐스트 서비스 요청을 다음과 같이 K_{DAPi}를 이용하여 안전하게 전송한다.
   - MBR_i : $K_{DAPi}(ID_{MBRi}||K_{MSi}||Req\_WMS||Sig_{MSi}(ID_{MBRi}||K_{MSi}||Req\_WMS)) \rightarrow DKA_i$
     $Req\_WMS = \{0, 1\}$
3) DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 그룹 가입 멤버 리스트를 생성해 DKM_i에게 안전하게 전송한다.
4) DKM_i는 각 DKA_i로부터 수신된 그룹 가입 멤버 리스트에

대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.

5) DKA_i는 Subgroup 키 갱신 정보를 다음과 같이 생성한 후에, 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{IDAi_Ms1}, Subgroup 키 갱신 정보 및 수신자 지정 그룹 서명 키 K_{GSi}를 안전하게 전송해 준다. 동시에 이 K_{IDAi_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi}는 DKM_i 및 SGB_i에게 안전하게 전송된다.

- $P_j(j=\{1, ..., m\})$ 생성 및 멤버 비밀 정보 계산
  : $GCD(S_{ij}, S_{ik}) = 1$ (단, $S_{ij} \neq S_{ik}$)
- K_{IDAi_Msj} 생성, 그룹 키 은닉 정보 및 역수 계산
  : $Y_{ij} = K_{IDAi\_Msj}^{Sij} \bmod P_j, \quad Y_{ij}^{-1}$
- Subgroup 키 갱신 정보 생성
  : $Ref\_key = (S_{i1}, Y_{i1}, Y_{i1}^{-1}, ..., S_{im}, Y_{im}, Y_{im}^{-1})$

6) 각 멤버는 무선 멀티캐스팅을 위해, 수신된 Subgroup 키 갱신 정보를 스마트 카드와 같은 저장 공간에 저장한다.

3.2.4 멀티캐스트 메시지 전송 단계

메시지 전송 단계는 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 Border들만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정과 타 도메인 및 다른 멀티캐스트 그룹에 속한 멤버들에게 보내는 외부 전송 과정으로 분류된다. 본 절에서는 외부 전송 과정을 기술하도록 한다.

1) 외부 전송 과정

가) 도메인에서 도메인으로의 전송

(1) 각 멤버들은 K_{IDAi_Ms1}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

(2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB_i에게 전송한다.

(3) DMB_i는 Hdr을 확인하고 인접 도메인 Border DMB_{i+1}에게 전송한다.

(4) DMB_{i+1}은 Hdr과 서명을 확인하고 해당 도메인에 속한 모든 SGB_{i+1}에게 전송한다.

(5) 전송된 메시지는 각 SGB_{i+1}에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.

(6) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{IDAi+1_Ms1}로 복호화하여 메시지를 확인한다.

나) 멀티캐스트 그룹간 메시지 전송

멀티캐스트 그룹간 메시지 전송 시에는 PKM과 연결되어 있는 MGB_i를 통해 이루어지며, 모든 전송과정은 도메인에서 도메인으로의 전송과정과 동일하다.

(1) 각 멤버들은 K_{IDAi_Ms1}을 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

(2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB_i에게 전송한다.

(3) DMB_i는 Hdr을 확인하고 MGB_i에게 전송한다.

(4) MGB_i는 Hdr을 확인하고 MGB_{i+1}에게 전송한다.

(5) MGB_{i+1}은 Hdr과 서명을 확인하고 해당 멀티캐스트 그룹에 속한 모든 DMB_{i+1}에게 전송한다.

(6) 전송된 메시지는 각 DMB_{i+1} 에 의해 해당 도메인의 모든 SGB_{i+1}에게 전송된다.

(7) 전송된 메시지는 각 SGB_{i+1}에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.

(8) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{IDAi+1_Ms1}로 복호화하여 메시지를 확인한다.

3.2.5 유·무선 원격 호스트 접속 및 인증

1) 원격 호스트 접속 및 인증

그룹 멤버가 자유로운 이동성을 가질경우, 유선 또는 무선으로 원격 호스트를 통해 멀티캐스트 서비스를 지원받아야 하므로, 자신의 인증 과정은 필수적이다. 이 때, 자신의 익명성을 제공받기 위해 가명 ID와 수신자 지정 서명을 수행한다.[7], [9]

가) 멤버는 원격 호스트에서 사용할 ID_N를 생성한다. 또한 서비스 개시를 위한 Time-Stamp를 생성하여, 지불 인증을 받을 DKM_i와 가명 식별자를 수신자 지정 서명을 수행해 원격 호스트에게 전송한다. 가명 식별자를 사용하는 이유는 제 3자로부터 자신의 신분을 숨기기 위해서이다.

나) 원격 호스트는 수신자 지정 서명을 확인한 다음, 멀티캐스트 서비스 수행을 위해 도메인 Border와 안전한 채널을 형성한다.

2) 원격 호스트 Hand-off 및 지불 인증

가) 멤버 MBR_i가 이동성이 빨라 Hand-off가 발생될 경우, 원격 호스트 RH_i는 주위 원격 호스트 RH_{i+1} 및 DKM_i에게 다음의 정보를 전송해 준다.

- $K_{RHPi+1}(ID_{Nr}||Tr)||K_{GSi}(ID_N||ID_{Nr}||T) \rightarrow RH_{i+1}$
- $K_{IDPi}(ID_{Nr}||Tr)||K_{GSi}(ID_N||ID_{Nr}||DKM_i||T) \rightarrow DKM_i$

나) 멤버 정보를 수신하면, DKM_i는 다음과 같이 지불 확인 정보를 RH_i에게 전송한다. 이를 통해 RH_i는 지불 인증을 받게 된다.

- $ID_{Nr}||K_{IDAPi}(ID_N||Tr-T)$

다) RH_{i+1}은 수신된 정보를 확인한 다음, 4)-(2)의 과정을 수행한다. 사용자 요구에 의해 멀티캐스트 접속이 완료되면, 멤버 MBR_i에게 다음의 정보를 각각 전송한다.

- $ID_{N+1}||Tr_{+1}||K_{RSi+1}(ID_N||ID_{Nr+1}||Tr||Tr_{+1}) \rightarrow MBR_i$

라) MBR_i는 수신정보를 확인한 후에, 다음 정보를 생성해 RH_{i+1}에게 전송한다.

- $ID_N||K_{GSi}(ID_N||ID_{Nr+1}||DKM_i||Tr||Tr_{+1}) \rightarrow RH_{i+1}$

마) RH_{i+1}은 다음의 정보를 DKM_i에게 전송한다.

- $K_{IPH}(ID_{N+1}||Tr_{+1})||K_{GSi}(ID_N||ID_{N+1}||DKM_i||Tr||Tr_{+1})$

바) DKM_i는 2)-나) 과정을 수행함으로서 지불 인증을 수행한다.

3.2.6 신규 멤버 가입 및 기존 멤버 탈퇴 단계

1) 신규 멤버 가입

신규 멤버 가입은 멤버 가입 단계와 동일한 과정을 통해 수행된다.

2) 기존 멤버 탈퇴/무선 단말기 분실

기존 멤버 탈퇴 또는 무선 단말기 분실 시에는 기존 멤버를 보호하고 불법 사용을 방지하기 위해 기존의 K_{IDAi_Ms1}을 갱신하여야 한다. 이를 통해 그룹 탈퇴자와 악성 침입자로부터 기존 멤버들을 보호할 수 있다.

가) 그룹 탈퇴를 희망하는 멤버가 있거나, 무선 단말기를 분실하였을 경우, 다음과 같은 정보를 생성하여

DKA_i에게 안전하게 전송한다.

- MBR_i : $K_{IDAPi}(Sig_{MSi}(DEL||ID_{MBRi}))$

  : DEL→ 탈퇴 희망자 또는 단말기 분실자

나) DKA_i는 다음의 정보를 생성해 DKM_i에게 전송한다.

- DKA_i : $K_{ID\_DAi}(Sig_{DKAi}(DEL||ID_{MBRi}))$

다) DKM_i는 DKA_i로부터 수신된 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.

라) PKM은 GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.

마) DKA_i는 Subgroup 갱신을 위해 기존의 멤버들 MBR_i', DKM_i 및 SGB_i에게 Subgroup 갱신 관련 부가 정보를 전송한다.

- $P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}, ..., P_j, S_{ij}, Y_{ij}, Y_{ij}^{-1}$

바) MBR_i', DKM_i 및 SGB_i에는 다음과 같은 과정을 통해 새로운 Subgroup 공통키 K_{IDAi+1_Msj}를 생성한다. 이를 통해 이동 중인 기존 멤버들도 간편하게 키 갱신을 수행할 수 있다.

- 다음을 만족하는 a_t, b_t(t∈{1, 2}) 계산

  : $a_1 * S_{i1} + b_1 * S_{e1} = 1$

  ⋯ $a_j * S_{ij}' + b_j * S_{ej} = 1$

- $a_t < 0$일 때, 다음을 계산

  : $(Y_{i1}^{-1})^{-a1} * Y_{e1}^{b1} \bmod P_1$

  $= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$

  ⋯ $(Y_{ij}^{r-1})^{-aj} * Y_{ej}^{bj} \bmod P_j$

  $= K_j^{aj*Sij'+bj*Sej} \bmod P_j = K_j$

- $b_t < 0$ 이면, 다음을 계산

  : $Y_{i1}^{a1} * (Y_{e1}^{-1})^{-b1} \bmod P_1$

  $= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$

  ⋯ $Y_{ij}^{aj} * (Y_{ej}^{-1})^{-bj} \bmod P_2$

  $= K_j^{aj*Sij'+bj*Sej} \bmod P_j = K_j$

- 계산 정보를 통해 새로운 Subgroup 공통키 갱신

  : $K = (\prod_{j=1}^{t} K_j) \bmod n$

3.3 새로운 방식의 특징

다음은 유·무선 멀티캐스트 키 관리 구조 요구 사항에 기초하여 제안 방식의 특징을 분석한 결과이다.

1) 무결성 및 인증성

: 키 생성과 분배시 모든 정보는 대칭키 및 공개키 암호 방식을 이용하므로, 무결성 및 인증성을 획득하고 있다.

2) 접근 제어

: 멀티캐스트 메시지는 각 Sub 그룹 멤버의 공통키와 보더의 Mkey를 통해서 멤버에게 전송되므로, 멤버 이외의 사용자들은 접근이 불가능하다.

3) 부인 봉쇄

: 키 생성 시 전송되는 각 정보에 대해 디지털 서명 기법을 사용하므로, 부인 봉쇄가 가능하다.

4) 비밀성

: 멀티캐스트 정보의 송·수신시 공통키를 사용하므로 비밀성을 확보하고 있다.

5) 공정성 및 확장성

: 멤버 가입 및 탈퇴에 따른 그룹 참여자의 변동시 오직 Sub 그룹 내에서만 키 갱신이 일어나므로 확장성 부분에서 효율성을 확보하고 있으며, 키 분배 및 갱신 과는 별도로 보더에게 Mkey가 제공되므로, 그룹 멤버로 가입하기 전에는 불법적 결탁이 생길 수 없다.

6) 익명성 및 Hand-Off 허용

: 본 방식은 원격 호스트 접근시 수신자 지정 그룹 서명 방식을 사용하므로 사용자 익명성이 보장되며, 이동성 보장을 위한 Hand-Off 프로토콜이 구성되어 있다.

7) 무선 멀티캐스트 키 분배 및 갱신

: 본 방식은 새로이 제안된 무선 그룹 키 갱신 방식을 통해 통신 병목 현상, 키 갱신시 overhead, 그룹 멤버 간 담합 방지 및 2명 이상의 동시 키 갱신을 수행함으로서 안전성을 확보하고 있으며, 그 횟수를 최소화함으로서 효율성을 높이고 있다.

4. 결론

현대 사회는 정보 통신 분야의 발전과 더불어 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 유·무선 멀티캐스트 서비스는 기본적으로 다자간 통신을 요구함으로서 안전성, 효율성 및 확장성 부분에서 취약성을 드러내고 있다.

본 논문에서는 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았으며, 요구 사항들 만족하는 새로운 멀티캐스트 키 관리 구조를 제안하고 분석하였다. 이를 통해 향후 더욱 다양해지는 멀티캐스트 관련 서비스 분야에서 적극적으로 대처할 수 있으리라 기대된다.

참고문헌

[1] M. Steiner, G. Tsudik and M. Waidner, "Diffie-Hellman Key distribution extended to group," In ACM Symposium on Computer and Communication Security, 1996.

[2] G. Caronni, M. Walldvogel and D. Plattner, "Efficient Security for Large Dynamic Multicast Groups," WETIC '98, 1998.

[3] S. Mittra, "Iolus : A Framework for Scalable Secure Multicasting," 1997.

[4] A. Ballardie, "Scalable Multicast Key distribution," RFC1949, May, 1996.

[5] T. Maufer and C. Semeria, "Introduction to IP Multicast Routing," draftietf-mboned-intro-multicast- 00.txt, Mar, 1997.

[6] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC'95, pp.II-68 ~ II-71, 1995.

[7] 박희운, 이임영, "안전한 수신자 지정 그룹 서명 방식에 대한 고찰," 한국멀티미디어학회 추계학술발표논문집, 1999, 11

[8] E. Brickell, P. Lee and Y. Yacobi, "Secure Audio teleconference," Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science 293, pp.418-426, 1988.

[9] 박희운, 이임영, "효율적인 이동통신 그룹키 갱신 방식 제안," 한국정보과학회 춘계학술발표대회, pp.832~ 834, 2001, 4, 28

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