제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

멀티캐스트 서비스 가용성을 보장하는 동적 키관리 구조

박희운*, 신동명*
*한국정보보호진흥원 기술표준팀
e-mail:{hupark, dmshin}@kisa.or.kr

A Dynamic Key Management Scheme for Multicast Service Availability

Hee-Un Park*, Dong-Myung Shin*
*Security Technology Standardization Team, KISA

요 약

멀티캐스트 서비스는 안전하고 신뢰성 있는 멤버간 그룹 통신을 위해 다양한 암호학적 기법들을 적용한다. 이러한 암호 기법들은 기본적으로 안전한 키 관리를 그 전제조건으로 한다. 그러나 악의적 사용자의 공격 또는 예상치 못한 재해 등으로 인해 키 관리 기능이 일부 상실될 경우, 멀티캐스트 서비스에 대한 신뢰성 및 가용성은 떨어지게 된다.

본 논문에서는 멤버 가입 및 탈퇴가 자유로운 동적 멀티캐스트 서비스 상에서 효율적으로 적용 가능한 키 관리 구조와 키 관리 기능 상실시 이를 극복할 수 있는 방안을 제안한다. 이를 통하여 키 관리상의 신뢰성과 효율성을 제공함은 물론, 멀티캐스트 서비스에 대한 가용성을 한층 강화할 수 있으리라 판단된다.

1. 서론

정보 사회의 발전을 통해 사용자들은 단순한 통신에서 벗어나 다자간 통신 회의 및 의료 분야에서 다양한 서비스를 요구하고 있다. 이들 서비스는 특정 그룹 멤버들을 대상으로 하며, 멀티캐스트 기법은 가장 각광을 받고 있는 방식 중에 하나이다[1]~[7].

멀티캐스트란 그룹에 참가한 한 송신자로부터 다수의 참여자에게 메시지 전송이 가능한 방법을 의미한다. 그러나 멀티캐스트 서비스는 인터넷과 같은 공개된 네트워크를 이용하므로 도청, 위조 및 불법 사용 등과 같은 취약성에 노출되어 있다. 이러한 불법 행위로부터 안전성과 신뢰성을 확보하기 위한 방안으로 암호 시스템이 이용되고 있다. 그러나 키의 노출 여부는 전송 정보의 안전성과 직결되므로 매우 중요시 다뤄져야 한다. 동시에 회원의 가입 및 탈퇴를 위하여 확장성이 보장되어야 한다.

현재 멀티캐스트 관련하여 다양한 연구가 진행되고 있으나, 키 관리에 대한 해결책들은 완전치 못한 상황이다. 특히 악의적 사용자에 의한 공격 또는 예상치 못한 자연 재해 등으로 인해 키 관리 기능이 일부 마비될 경우, 이를 대처할 방안에 대한 연구는 아직까지 초기 단계에 머무르고 있다.

따라서 본 연구는 멤버 가입 탈퇴가 자유로운 동적 멀티캐스트 서비스에서 신뢰성 및 확장성을 제공하기 위하여 요구되는 사항들을 고려함과 동시에 안전한 멀티캐스트 키 관리 구조를 제안한다. 또한 멀티캐스트 키 관리 장애 허용(Fault Tolerance) 기법을 제안함으로서 멀티캐스트 서비스의 신뢰성과 가용성을 보장하고 있다. 이러한 구조적 특성들과 제시된 요구사항들을 근거로 안전성, 효율성, 확장성 및 가용성 부분에서 그 효용성을 검증할 것이다.

2. 요구사항

멀티캐스트 구조는 다자간 통신을 전제로 하고 있기 때문에 여러 위협 요소에 노출되어 있다. 특히 안전한 통신을 위해 사용되는 키의 관리는 매우 중요한 요소로서, 다음은 이를 위해 요구되는 사항을 기술한 것이다[8].

- **기밀성** : 불법적인 제 3자로부터 멀티캐스트 정보는 보호되어야 한다. 이를 위해 다양한 암호 기법이 적용될 수 있다.
- **무결성** : 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
- **인증성** : 송·수신된 멀티캐스트 정보가 불법적인 변조 없이 정당한 멤버들로부터 생성 및 수신되었음을 확인할 수 있어야 한다.
- **부인 봉쇄** : 멀티캐스트 서비스 멤버간에 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자가 이를 확인 할 수 있어야 한다.
- **접근 제어** : 정당한 그룹의 멤버만이 멀티캐스트 정보에 접근할 수 있다.
- **공정성** : 멀티캐스트에서 사용되는 키들은 허가된 그룹 멤

버에게만 안전하게 전송되어야 한다.

- **확장성** : 멤버 가입 탈퇴에 따른 동적인 키 관리 기법이 필요하다.
- **가용성** : 임의 공격 및 재해가 발생하여 키 관리 기능이 일부 상실된다 하더라도, 서비스는 지속적으로 이뤄져야 한다.

3. 동적 멀티캐스트 키 관리 구조 제안

본 방식은 도메인-Subgroup 구조를 형성함으로서 멤버 가입 및 탈퇴시 최소한의 키 갱신을 유도하며, 동적인 계층 관리를 수행한다. 동시에 구조적으로 키 관리 제어부와 메시지 전송부로 이원화함으로서 키 관리 담당자의 부담을 줄이고 메시지 전송 과정에서 발생 가능한 부정 및 오버헤드를 막고 있다. 또한 임의 공격 및 자연재해로부터 키 관리 서비스의 가용성을 높이기 위해 3가지 방식을 제시한다. 이는 인증 및 메시지 암호화를 위하여 적용되는 PKI와 함께 이질적인 통신망에서 안전성과 효율성 및 가용성을 높이는 효과를 제공한다.

3.1 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술하고 있다.

- DKM_i : 도메인 키 관리자
- DKA_i : 도메인 키 중간 관리자 i
- B_i, GI : Border i 및 그룹 초기자
- GML : 그룹 멤버 리스트
- PKM : 도메인 키 (중간)관리자들 및 각 Border의 공개키 관리자
- MBR_i : 그룹 멤버 i
- $MKey$: PKM에 의해 생성된 멀티캐스트 키
- K_{*_P}, K_{*_S} : *의 공개키 및 개인키, ($* \in \{PKM, DKM_i, DKA_i, MBR_i, B_i, GI\}$)
- K_{DKMi_DKAi} : DKM_i와 DKA_i 사이의 공통키
- K_{MBRi} : 그룹 멤버 MBR_i의 비밀키
- K_{DKAi_MBRj} : 각 DKA_i가 관리하는 멤버들과의 공통키
- Ref_key : Subgroup 공통키 갱신 정보
- Hdr : 메시지 전송 시 송신 그룹과 수신 그룹의 식별 정보
- ID_*, IP_* : *의 식별자 및 IP 주소
- $Cert()$: PKM이 생성하는 공개키 인증서
- M : 멀티캐스팅 메시지
- Y_{ij}, Y_{ij}^{-1}: Subgroup 공통키 은닉 정보 및 역수
- S_{ij} : DKA_i에 의해 생성되는 Subgroup 멤버 i의 비밀 정보
- P_j : DKA_i가 생성하는 큰 소수(j는 키 갱신 순번)

3.2 시스템 구성

본 논문에서는 동적 멀티캐스트 키 관리 시스템 구성을 위해 도메인 초기화, 그룹 초기화, 그룹 멤버 가입, 메시지 송수신, 장애 허용을 위한 시스템 재구성 및 키 갱신 등으로 기술한다.

3.2.1 도메인 초기화 단계

1) DKM_i, DKA_i 및 각 Border는 PKI를 이용해 자신의 공개키 인증서를 PKM으로부터 수신한다.
   - PKM : $Cert(ID_*||*의\ 공개키||IP_*) \rightarrow \{DKM_i, DKA_i, B_i\}$
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.
   - GI : $K_{GI\_S}(ID_{GI}||GML) \rightarrow PKM$
   : $GML = (ID_{MBR1}||\cdots||ID_{MBRn})$
2) PKM은 서명 확인을 통해 GI 및 GML을 인증하고 멀티캐스트 서비스를 위한 MKey를 생성한다. 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들에게만 제공함으로서 안전성과 신뢰성을 높이고 있다.
   - PKM : $K_{Bi\_P}(MKey||K_{PKM\_S}(ID_{PKM})) \rightarrow$ 각 $Border$
3) PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.
   - PKM : $K_{DKMi\_P}(GML||K_{PKM\_S}(GML)) \rightarrow DKM_i$

3.2.3 그룹 멤버 가입 단계

1) DKM_i는 도메인 내에서 DKA_i와의 통신 시 사용할 K_{DKMi_DKAi}를 생성 및 서명을 수행하여 유니캐스트 채널을 통해 안전하게 DKA_i에게 전송한다.
   - DKM_i : $K_{DKAi\_P}(K_{DKMi\_DKAi}||K_{DKMi\_S}(K_{DKMi\_DKAi})) \rightarrow DKA_i$
2) 그룹에 멤버로 가입할 사용자들은 자신의 식별자, 비밀키에 서명을 수행함으로서 DKA_i에게 자신을 인증한다.
   - MBR_i : $K_{DKAi\_P}(ID_{MBRi}||K_{MBRi}||K_{MBRi\_S}(ID_{MBRi}||K_{MBRi})) \rightarrow DKA_i$
3) DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 그룹 가입 멤버 리스트를 생성해 DKM_i에게 전송한다.
   - DKA_i : $K_{DKMi\_DKAi}(K_{DKAi\_S}(ID_{MBR1}||\cdots||ID_{MBRi})) \rightarrow DKM_i$
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_{MBRi}를 이용하여 각 멤버에게 K_{DKAi_MBRi}, Subgroup 키 갱신 정보를 안전하게 전송해 준다. 동시에 이 정보는 DKM_i 및 SGB_i에게 안전하게 전송된다.
   - $P_j (j = \{1, \ldots, m\})$ 생성 및 멤버 비밀 정보 계산, $GCD(S_{ij}, S_{ik}) = 1$ (단, $S_{ij} \neq S_{ik}$)
   - K_{DKAi_MBRi} 생성 및 그룹 키 은닉 정보 및 역수 계산
     : $Y_{ij} = K_{DAi\_Msj}^{Sij} \bmod P_j$, Y_{ij}^{-1}
     (단, $j = \{2, \ldots, n\}$)
   - Subgroup 키 갱신 정보 생성
     $Ref\_key = (S_{i1}, Y_{i1}, Y_{i1}^{-1}, \ldots, S_{im}, Y_{im}, Y_{im}^{-1})$
   - DKA_i : $K_{MBRi}(K_{DKAi\_MBRi}||Ref\_key||K_{GSi}) \rightarrow MBR_i$

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 논문에서는 외부 전송 과정 중 도메인에서 도메인으로의 전송 부분을 기술한다.

1) 각 멤버들은 K_{DAi_Ms1}를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 B_i에게 전송한다.
- MBR_i : $K_{DKAi\_MBR1}(Hdr||M) \rightarrow B_i$

2) SGB_i는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 인접 도메인의 B_{i+1}에게 전송한다.
- B_i : $K_{DKAi\_MBRi}(K_{DKAi\_MBRi}(Hdr||M))=Hdr||M$
: $(Hdr||K_{Bi\_S}(Hdr)||MKey(M)) \rightarrow B_{i+1}$

3) B_{i+1}은 Hdr과 서명을 확인한 다음, 해당 메시지를 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.
- B_{i+1} : $K_{Bi\_P}(K_{Bi\_S}(Hdr)) = Hdr$
: $Mkey(MKey(M)) = M$
: $K_{DKAi+1\_MBRi}(M) \rightarrow MBR_{i+1}$
: K_{DKAi+1_MBRi}는 DKA_{i+1}와 그 Subgroup에 속한 멤버들 간의 Subgroup 공통키

4) 각 DKA_{i+1}에 속한 Subgroup의 모든 멤버 MBR_{i+1}은 K_{DKAi+1_MBRi}로 복호화하여 메시지를 확인한다.
- MBR_{i+1} : $K_{DKAi+1\_MBRi}(K_{DKAi+1\_MBRi}(M)) = M$

3.2.5 키 갱신 단계

멀티캐스트 서비스는 멤버의 가입 및 탈퇴가 매우 자유롭다. 따라서, 멤버 변동에 따른 키 갱신은 매우 중요한 의미를 갖는다. 신규 멤버 가입시에는 그룹 멤버 가입과 동일한 과정을 수행하면 되지만, 기존 멤버 탈퇴 시에는 별도의 프로세싱이 필요하다. 다음은 이에 대한 프로토콜을 기술한다.

1) 그룹 탈퇴 시, 다음과 같은 정보를 생성하여 DKA_i에게 안전하게 전송한다.
- MBR_i : $K_{DKAi\_P}(K_{MBRi\_S}(DEL||ID_{MBRi})) \rightarrow DKA_i$
: DEL은 그룹 탈퇴 희망자임을 나타내는 식별자

2) DKA_i는 다음과 같은 정보를 생성해 DKM_i에게 전송한다.
- DKA_i : $K_{DKMi\_DKAi}(K_{DKAi\_S}(DEL||ID_{MBRi})) \rightarrow DKM_i$

3) DKM_i는 DKA_i로부터 수신된 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.
- DKM_i : $K_{PKM\_P}(K_{DKMi\_P}(GML')) \rightarrow PKM$

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

5) DKA_i는 Subgroup 키 갱신을 위해 기존의 멤버들 MBR_i', DKM_i 및 B_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}

6) MBR_i', DKM_i 및 B_i에는 다음과 같은 과정을 통해 새로운 Subgroup 공통키 K_{DKAi+1_MBRi}를 생성한다.
- 다음을 만족하는 a_t, b_t($t \in \{1, 2\}$) 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
: $(Y_{i1}^{-1})^{-a1} * Y_{e1}^{b1} \bmod P_1$
$= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$
:
$(Y_{ij}'^{-1})^{-aj} * Y_{ej}^{bj} \bmod P_j$
$= K_j^{aj*Sij'+bj*Sej} \bmod P_j = K_j$
- $b_t < 0$ 이면, 다음을 계산
: $Y_{i1}^{a1} * (Y_{e1}^{-1})^{-b1} \bmod P_1$
$= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$
:
$Y_{ij}'^{aj} * (Y_{ej}^{-1})^{-bj} \bmod P_2$
$= K_j^{aj*Sij'+bj*Sej} \bmod P_j = K_j$
- 계산된 정보를 통해 새로운 Subgroup 공통키 갱신
: $K_{DKAi+1\_MBRi} = (\prod_{j=1}^{t} K_j) \bmod n$

3.2.6 장애 허용을 위한 시스템 재구성 단계

임의의 공격 또는 자연 재해로 인해 멀티캐스트 키 관리 서버가 그 기능을 상실할 경우가 발생된다 하더라도 키 관리 서비스는 지속적으로 유지되어야 신뢰성을 제공할 수 있게 된다. 이와 같은 장애 허용 서비스를 위해서 다음과 같이 가정한다.

- 각 Subgroup의 키 관리 정보는 DKM_i가 관리하는 DB에 저장된다.
- 본 논문에서는 DKA_i가 기능을 상실했다고 가정하며, DKM_i, MBR_i, DKA_i' 등이 DKA_i의 권한 승계를 통해 지속적인 키 관리 서비스 제공한다.

1) MBR_i의 권한 승계

(1) 본 방식은 장애 허용시 DKA_i 기능 상실에 대비해 Subgroup 멤버들에게 우선 순위를 지정함으로서, 그 권한을 승계할 수 있도록 하는 방식이다. 각 멤버들은 다음과 같이 우선 순위대로 정렬되어 있으며, 이 정보는 그룹 멤버 가입시 DKM_i에게 전송된 상태이다.
- $(ID_{MBR1}||\cdots||ID_{MBRi})$

(2) 키 관리 서버로 활동할 멤버는 자신의 식별자, 비밀키에 서명을 수행함으로서 DKM_i에게 자신을 인증한다.
- MBR_i : $K_{DKMi\_P}(ID_{MBRi}||K_{MBRi}$
$||K_{MBRi\_S}(ID_{MBRi}||K_{MBRi})) \rightarrow DKM_i$

(3) DKM_i는 대상 MBR_i에 대해 3.2.3-1)를 수행한 다음, 해당 Subgroup의 리스트와 MBR_i의 ID에 자신의 서명을 수행하여 안전하게 전송한다.

(4) MBR_i는 DKM_i의 서명이 붙은 멤버 리스트와 자신의 ID에 K_{DKAi_MBRi} 키로 암호화하여 동보 전송한다.
- MBR_i : $K_{DKAi\_MBRi}(GML_{\_part}||ID_{\_MBRi}) \rightarrow MBR_i'$

(5) 각 멤버는 전송된 암호문을 복호화 함으로서 MBR_i를 인증하고 MBR_i에게 메시지 link를 수행한다.
- 본 방식은 Subgroup 내에서 키 관리에 대한 가용성을 해결한다는 측면에서는 바람직하나, 각 멤버에 대한 신뢰도를 어떻게 확인할 것인지에 대한 세부적인 방법론이 필요하다.

2) DKA_i'의 권한 승계

본 방식은 도메인내의 서로 다른 그룹이 합병됨을 의미한다. 두 그룹의 합병을 통한 권한 승계는 다음과 같은 과정으로 수행된다.

(1) B_i는 그룹 합병 요구 메시지를 다음과 같이 통고한다.

- B_i : $Hdr||K_{DKAi\_MBRi}(Request||GML_{part1}) \rightarrow B_i'$
- B_i' : $K_{DKAi\_MBRi}'(Request||GML_{part1}) \rightarrow DKA_i'$

(2) DKA_i'는 Border를 통해 받은 전송 정보를 복호화하여 확인하고 그룹 합병을 결정한다. 그룹 합병이 결정되면 그룹 합병 승인 메시지를 B_i에게 전송한다.

(3) DKA_i'는 새로운 공통키 K_{DKAi_MBRi}'을 생성하여 DKM_i에게 새로운 공통키 K_{DKAi_MBRi}', 통합 그룹 멤버 리스트 $GML_{part1+2}$을 함께 전송한다.

- DKA_i' : $K_{DKM\_DKAi}(K_{DKAi\_S}(GML_{part1+2}||K_{DKAi\_MBRi}')) \rightarrow DKM_i$

(4) DKM_i는 DKA_i'로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 $GML_{part1+2}$를 생성하여 PKM에게 전송한다.

- $K_{PKM\_P}(K_{DKMi\_S}(GML_{part1+2})) \rightarrow PKM$

(5) DKA_i'는 3.2.3-5)와 동일한 과정을 통해 새로운 공통키 K_{DKAi_MBRi}, Subgroup 키 갱신 정보 등을 모든 멤버들 MBR_i와 SGB_i에게 전송한다.

- 본 방식은 키 관리 정책 및 신뢰성 부분에서는 우수하나, 통합에 따른 부가적인 통신량 증가가 발생될 수 있다.

3) DKM_i의 권한 승계

(1) 이 방식은 상기 1) 및 2) 방식이 불가능할 경우 사용가능한 방식으로, DKA_i가 관리하던 Subgroup의 멤버 리스트에 자신의 서명을 붙여, K_{DKAi_MBRi} 키로 암호화하여 동보 전송한다.

- DKM_i : $K_{DKAi\_MBRi}(K_{DKMi\_S}(GML_{part})) \rightarrow MBR_i$

(2) 각 멤버는 전송된 암호문을 복호화 함으로서 DKM_i를 인증하고 DKM_i에게 메시지 link를 수행한다.

- 본 방식은 DKM_i에게 overhead를 가중시키게 되는데, 모든 DKA_i의 기능 마비시 1:all 성형 네트워크를 형성하게 됨으로서, 고유기능을 상실할 수 있다는 문제점이 있다.

3.3 제안 방식 분석

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

1) 기밀성

멀티캐스트 정보의 송·수신시 공통키를 사용하므로 비밀성을 확보하고 있다.

2) 무결성 및 인증성

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

3) 부인 봉쇄

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

4) 접근 제어

멀티캐스트 메시지는 각 Subgroup 멤버의 공통키와 Border의 Mkey를 통해서 멤버에게 전송되므로, 멤버 이외의 사용자들은 접근이 불가능하다.

5) 공정성 및 확장성

멤버 가입 및 탈퇴에 따른 그룹 참여자의 변동시 오직 Subgroup 내에서만 키 갱신이 일어나므로 확장성 부분에서 효율성을 확보하고 있으며, 키 분배 및 갱신과는 별도로 Border에게 Mkey가 제공되므로, 그룹 멤버로 가입하기 전에는 불법적 결탁이 이뤄질 수 없다.

6) 가용성

장애에 따른 기능 상실에 대해, 복구 기능을 부여함으로서 지속적인 서비스가 가능하다.

4. 결론

지식 정보화 사회의 발전을 통해 다양한 멀티캐스트 관련 서비스 요구가 증대되고 있다. 그러나 멀티캐스트 서비스는 기본적으로 다자간 통신을 요구함으로서 다양한 취약성을 드러내고 있다.

본 논문에서는 멀티캐스트 서비스 상에서 이러한 취약성을 극복하기 위해 필요한 요구 사항을 살펴보았고, 동적 확장성을 제공하는 안전한 멀티캐스트 키 관리 구조를 제안하였다. 또한 동적 멤버 변동에 따른 갱신 방식과 장애 허용에 따른 가용성을 보장하는 방식을 제안하였다. 이를 통해 제안된 방식은 안전성, 신뢰성, 확장성 및 가용성을 제공하면서 통합 환경에 능동적으로 대처할 수 있는 효율적인 구조로 이루어져 있음을 확인하였다. 따라서 본 방식은 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] "멀티캐스트를 위한 키 분배 메커니즘 설계 및 구현" ETRI 최종 보고서, 1999.

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

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

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

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