(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[7]
H04L 9/08

(45) 공고일자 2004년06월07일
(11) 등록번호 10-0434721
(24) 등록일자 2004년05월25일

(21) 출원번호 10-2001-0080576
(22) 출원일자 2001년12월18일

(65) 공개번호 10-2003-0050177
(43) 공개일자 2003년06월25일

(73) 특허권자 이임영
충남 천안시 쌍용3동 라이프아파트 102동 1103호

(72) 발명자 이임영
충남 천안시 쌍용3동 라이프아파트 102동 1103호

박희운
충청남도아산시모종동한라동백아파트101-2105

(74) 대리인 특허법인 원전

심사관 : 문태진

(54) 유 · 무선 통합 멀티캐스트 키 관리 방법

요약

유선 및 무선 네트워크 상에서 특정 그룹을 대상으로 서비스를 제공함에 있어 안전성, 효율성 및 확장성을 제공하기 위한 유 · 무선 통합 멀티캐스트 키 관리 방법에 관한 것으로서, 멀티캐스트 서비스제공을 위한 도메인 및 그룹 초기화 과정과, 서비스를 받고자 하는 사용자들이 그룹에 멤버로 가입하는 그룹멤버 가입 과정과, 실제 멀티캐스트 서비스를 제공하는 멀티캐스트 메시지 전송 과정과, 무선 멀티캐스트 서비스 사용자를 위한 유 · 무선 원격 호스트 접속 및 인증 과정과, 그룹멤버 변동 시 키 갱신을 위한 신규멤버 가입 및 기존멤버 탈퇴 과정과, 그룹 합병 및 그룹 분할 과정을 포함하여 이루어진다.

대표도

도 1

색인어

유 · 무선 통합 멀티캐스트, 확장성, 안정성, 효율성, 그룹 키 관리

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 유 · 무선 통합 멀티캐스트 그룹 키 관리 기법의 진행절차를 나타낸 흐름도,
도 2는 도 1의 도메인 및 그룹 초기화 절차를 상세히 나타낸 흐름도,
도 3은 도 1의 그룹 멤버 가입 절차를 상세히 나타낸 흐름도,
도 4a 내지 도 4e는 도 3의 멀티캐스트 메시지 전송 절차를 경우별로 상세히 나타낸 흐름도,

도 5는 도 1의 유·무선 원격 호스트 접속 및 인증 절차를 상세히 나타낸 흐름도,
도 6은 도 1의 신규 멤버 가입 및 기존 멤버 탈퇴 절차를 상세히 나타낸 흐름도,
도 7은 도 1의 그룹 분할 및 그룹 합병 절차를 상세히 나타낸 흐름도이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 유·무선 통합 멀티캐스트 그룹 키 관리방법에 관한 것으로서, 보 다 상세하게는 유선 및 무선 네트워크 환경에서 특정 그룹을 대상으로 하는 그룹 기반 서비스 제공에 있어 각 그룹을 도메인 형식의 동적인 관리를 통해 효율적으로 그룹 키를 관리하고 그룹 확장에 따른 확장성을 제공하며, 무선 이동 통신상에서 멀티캐스트 서비스 제공 시 단말기를 통한 효율적인 키 갱신을 유도함과 동시에 사용자의 익명성을 보장할 수 있는 유·무선 통합 멀티캐스트 그룹 키 관리 방법에 관한 것이다.
멀티캐스트란 한 송신자로부터 데이터를 여러 수신자에게 전송할 수 있는 방법으로 멀티캐스트 그룹을 운영하여 그룹에 참가한 수신자에게만 데이터를 전송하는 기법을 의미한다. 사용자가 정보를 수신하려면 멀티캐스트 그룹에 참가하면 되고, 해당된 그룹을 떠나면 더 이상 정보를 수신하지 않게 된다.
기존의 유선 멀티캐스트 그룹 키 관리 방법으로는 Spanning Tree 방법, Clique 방법, Iolus 방법, SMKD 방법, KL 방법, DK 방법, KYH 방법 등이 있다. 다음은 이 방법들 중 대표적인 몇 가지 방법에 대해 설명한다.
Clique 방법은 Diffee-Hellman 방법을 이용하여 그룹 내에 같은 속성을 갖는 소규모 그룹을 구성하는 방법이다. 본 방법의 설명에 앞서 수식에 사용되는 기호들은 다음과 같이 정의한다. · MBR_i : 그룹 멤버 i (i=1,2,3, ... , n : n은 멤버의 수) · g^m : 키 생성 (m : 키 생성 값) · Ni : i의 키 생성 인자 · i, j. k : 그룹 멤버의 색인 · p : 멤버의 색인 · g : 밑수 그룹 키 생성을 위해 멤버들은 다음과 같은 과정을 거쳐 그룹 초기 키 동의 과정을 수행한다.
· $MBR_i \rightarrow MBR_{i+1}$: $\{g^{((N1...Ni)/Nk)} \parallel k\ [1, i]\}, g^{N1...Ni}$
· $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Ni)/Ni)} \parallel i\ [1, n]\}$
멤버 가입에 있어서 이 방법은 버스형 네트워크 또는 링(Ring)형 구조에 적합하도록 구성되어 있기 때문에 키 동의 시 누가 마지막으로 키 동의에 참여하느냐에 따라 동적 또는 정적으로 구분된다.
동적 그룹 제어의 경우 다음과 같은 과정을 수행한다.
· $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn')/Nk)} \parallel k\ [1, n]\}, g^{N1...Nn}$
· $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn'Nn+1)/Ni)} \parallel i\ [1, n]\}$
정적 그룹 제어에 있어서는 다음과 같다.
· $MBR_{n+1} \rightarrow MBR_n$: $\{g^{((N1...Nn-1)/Ni)} \parallel i\ [1, n-1]\}, g^{N1...Nn-1}$
· $MBR_n \rightarrow MBR_{n+1}$: $\{g^{((N1...Nn)/Ni)} \parallel i\ [1, n]\}, {}^{g}N1...Nn$
· $MBR_{n+1} \rightarrow MBR_i$: $\{g^{((N1...Nn+1)/Ni)} \parallel i\ [1, n]\}$
기존 타 그룹의 멤버 가입의 경우 멤버들 사이에 다음과 같은 과정을 수행한다.
· $MBR_{n+j} \rightarrow MBR_{n+j+1}$: $\{g^{((N1...Nn+j)/Nk)} \parallel k\ [1, n+j]\}, g^{N1...Nn\ Nn+1...Nn+j}$
· $MBR_{n+m} \rightarrow MBR_i$: $\{g^{((N1...Nn+m)/Ni)} \parallel i\ [1, n+m]\}$
그룹 멤버의 탈퇴가 일어나면 멤버들은 다음과 같은 과정을 수행한다.
· $MBR_n \rightarrow MBR_i$: $\{g^{((N1...Nn)/Ni)} \parallel i\ [1, n-1] \wedge i \neq p\}$
이 방법은 버스형 또는 링(Ring)형 네트워크 구조에서 적용 가능한 방법이다. 키 분배를 위해서 각 멤버는 공개키 방법에 기반한 Diffee-Hellman 방법을 적용하고 있다. 이때 멀티캐스트 통신을 위해서는 모든 멤버가 키 생성에 관여함으로 새로운 멤버 가입 및 기존 멤버 탈퇴 시 전 멤버 사이에 새로운 키를 생성해야 하는 번거로움이 발생한다. 또한 데이터의 중로에 있는 자(man-in the-middle attack)에 의해 제 3자에 의한 도청이 가능하다는 문제점을 안고 있다.
Iolus 방법의 경우, 대규모 그룹을 여러 개의 소규모 그룹으로 분할하여 멤버쉽 변동에 따라 키 변경의 영향을 받는 멤버 수를 줄이는 방법이다.
이 방법에서 사용되는 표기들은 다음과 같다.
· GSC : Group Security Controller
· GSI : Group Security Intermediary
· GSA : Group Security Agent
· K_{GSA_MBRi} : GSA와 멤버 i사이의 비밀 키
· K_{SGRP} : Subgroup을 위한 키
· K_{SGRP}' : Update된 키
· Sig_{MBRi} : 멤버 i의 서명
· R : 랜덤 값
· M : 메시지
· GRP_END : 멀티캐스팅 종결 확인 메시지

그룹 초기화 단계에서는 GSC가 Access Control List(ACL)를 작성하며, 여기에는 보안 정책관련 정보를 포함하고 있다. GSI 및 그 외의 멤버는 GSC의 ACL에 맞춰 그룹에 가입하게 된다.
그룹 가입 단계에 대해 상세히 설명하도록 한다. 먼저 참여자들은 GSA에게 그룹 가입 요구서를 안전한 유니캐스트 채널을 통해 전달한다. GSA는 그룹 가입 요구서를 확인하고 비밀키 $K_{GSA-MBR}$ 을 생성하여. DB에 개인신상 정보와 함께 저장한다. 저장이 끝난 다음 그룹에 가입한 멤버들에게 안전한 유니캐스트 채널을 통해 $K_{GSA-MBR}$ 을 분배한다. 기존의 Subgroup 공통키 K_{SGRP} 를 K_{SGRP} '로 갱신한 다음 GRP_KEY_UPDATE 메시지 $K_{SGRP}(K_{SGRP}')$를 생성하여 멤버들에게 전송한다.
그룹 재신임 단계는 그룹 가입이 수행된 다음 참여자들이 그 그룹에 지속적으로 남기를 원한다면, 안전한 유니캐스트 채널을 통해 그룹 재신임 메시지를 전달해야 한다. 그룹 재신임이 이루어지면, GSA는 네트워크 프레임워크(Network framework)가 최적 상태가 되도록 재조정한다.
다음은 그룹 탈퇴 과정을 상세히 살펴보기로 한다. 그룹 탈퇴가 성립할 조건은 멤버가 Subgroup에서 탈퇴하기 위해 LEAVE 요청서를 GSA에게 전송할 경우와 GSA가 멤버를 강제 탈퇴시키려 할 경우이다. 그룹 탈퇴가 발생할 경우 GSA는 K_{SGRP} 를 K_{SGRP} '로 갱신 시켜야 하며, 그룹 가입 때와는 달리 메시지 $K_{SGA-MBR1}(K_{SGRP}') \| K_{SGA-MBR2}(K_{SGRP}') \| .. \| K_{SGA-MBRn}(K_{SGRP}')$를 생성하여 남아 있는 멤버에게 변경된 K_{SGRP} '를 안전하게 멀티캐스트 전송한다.
메시지 전송 단계는 메시지 전송 유형 1과 메시지 전송 유형 2를 제공한다. 먼저 메시지 전송 유형 1을 살펴보면, 송신자는 전송 메시지(M)를 K_{SGRP} 로 암호화하여 로컬 서브그룹(local subgroup)에게 전송한다. GSI는 전송 메시지를 복호화하고 다시 상위 그룹의 K_{SGRP} 로 암호화하여 전송하며, 동일한 방법으로 나머지 GSI는 이 정보를 받아서 복호화하고 하위 GSI에게 암호화하여 전송한다. 다음으로 메시지 전송 유형 2의 절차를 살펴보기로 한다. 송신자는 전송 메시지(M)를 직접 암호화하는 대신에 랜덤 값(R)을 생성하여 $Sig_{MBRi}(R(M) \| K_{SGRP}(R))$와 같이 암호화를 수행하고, R을 K_{SGRP} 로 암호화하여 연접한 다음 자신의 서명(Sig_{MBRi})을 붙여 local subgroup에게 전송한다. GSI는 수신된 정보에 인증 및 복호화를 수행한 다음, 동일 방법으로 자신의 서명을 붙여 하위 GSI에게 전송시킴으로써 정당성을 제공한다. 메시지 전송 유형 2의 장점은 유형 1에서 제공하지 못하는 메시지 신뢰성 및 무결성을 제공하는 것이다.
키 갱신에 있어 갱신은 주로 멤버 변동 시에 발생되며, 이때 키 변동을 위한 link는 이미 약속되어 있는 안전한 채널을 기초로 수행한다.
마지막으로 멀티캐스팅 종결 단계를 살펴보면, GSC는 멀티캐스팅이 안전하게 수행된 것을 확인한 다음, GRP_END를 해당 subgroup의 GSA에게 전송하고 이를 다시 멤버에게 전송함으로써 종결시킨다.
이 방법은 각 멤버쉽이 Tree-Based 계층 구조로 구성된다. 각 멤버의 가입/탈퇴 시 Subgroup 내에서만 키의 변경이 일어남으로, Clique 방법의 문제점을 개선하고 있다. 그러나 보안 관리 센터(GSC)의 오류 및 부정이 발생할 경우 멀티캐스트 서비스가 불가능하다. 동시에 각 Subgroup간의 통신시 중간 관리자간에 의해 메시지 암/복호화를 별도로 수행해야 하고, 메시지 전송 유형 2를 사용할 경우 서명 확인을 위한 별도의 공개키 관리 센터 및 암호 방법을 적용해야 하는 단점이 있다.
한편, Domain GKMP 방법은 internet-draft로 제안된 그룹 키 관리 프로토콜이다. DKD(Domain Key Distributor)가 관리하는 한 개의 도메인은 여러 개의 Area로 나뉘어져 있으며, 각각의 Area에는 AKD(Area Key Distributor)가 할당되어져 있고 멀티캐스트 사용자들은 각 Area 내에 분산되어 있다. DKD는 도메인내의 모든 멀티캐스트 메시지의 암/복호화에 사용되는 유일한 그룹 키인 MKey를 생성하고 또한 AKD들에게 안전하게 전송하는 역할을 수행한다. DKD 및 모든 AKD들은 그들만으로 구성된 All-KD-Group이라는 그룹에 속해 있으며, 본 그룹 내에서만 사용되는 All-KD-Key라는 비밀키를 가지고 있다.
DKD는 All-KD-Key를 이용하여 멀티캐스트 형식으로 모든 AKD들에게 MKey를 전송할 수 있으며, 또는 DKD와 개개의 AKD들 사이에 설정된 AKD-Private-Key들을 이용하여 유니캐스트의 형식으로 MKey를 개별적으로 전송할 수도 있다. 이러한 선 택사항을 부여한 이유는 요구되는 보안 요구 사항에 따라 적절한 전송방법을 선택할 수 있게 하기 위함이다. AKD와 그에 속한 사용자들은 Area-Group-Key라는 비밀키를 공유하게 되며 본 키는 해당 Area 외부에는 알려져 있지 않다. DKD로부터 MKey를 전달받은 AKD는 사용자들에게 MKey를 연속하여 전달하는데 이때 Area-Group-Key를 이용하여 멀티캐스트 형식으로 전송할 수도 있고, 또는 AKD와 개개의 사용자들 사이에 설정된 Member-Private-Key를 통하여 유니캐스트 형식으로 전달될 수 있다. 즉, 일정한 시간이 지나서 단순히 MKey를 갱신하는 경우라면 Area-Group-Key를 이용한 멀티캐스트의 방법이 충분하지만, Leave/Join operation의 경우라면 개개의 사용자들과의 사이에 설정된 Member-Private-Key를 이용하여 'Backward and Forward Secrecy'를 보장하여야 한다.
타 도메인과의 멀티캐스트 통신은 TE(Translating Entity)를 통하여 이루어지는데 도메인으로부터 메시지가 들어오는 경우 TE는 해당 메시지를 복호화한 후 다시 본 도메인의 MKey로 암호화하여 전달하게 된다. 따라서 TE는 다른 도메인의 MKey도 저장하고 있어야 한다.
이 방법은 각 그룹을 도메인 형식으로 구성함으로서 동적인 멤버쉽 변화에 유연성을 제공하고 있다. 그러나 멀티캐스트 메시지 전송을 위해 각 도메인별로 각각의 멀티캐스트 키를 보유하고 있다. 따라서 도메인간의 메시지 전송 시 매번 암/복호화 과정을 수행해야 하는 번거로움이 발생한다.
전술한 바와 같은 종래의 고정 IP 기반 멀티캐스트 그룹 키 관리 방법들은 그룹 멤버의 변동에 따른 키 갱신에 있어 효율적으로 대처하고 있지 못하며, 네트 워크 상에서 제 3자에 의한 도청 및 전송 정보의 위조와 같은 불법행위에 노출되어 있다는 보안상 취약점을 가지고 있다. 또한 현재까지 무선 환경을 고려한 멀티캐스트 서비스의 경우 그 연구가 미비한 상태이다.

발명이 이루고자 하는 기술적 과제

본 발명은 유선 및 무선 네트워크 환경에서의 멀티캐스트 서비스 제공에 있어 효율적으로 그룹 키를 관리하고 안전성과 확장성을 제공하기 위한 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법 및 프로토콜을 제공하는 것을 목적으로 한다.
본 발명의 다른 목적은 무선 통신상에서 안전한 멀티캐스트 서비스 제공을 위해 사용자들의 위치 익명성을 보장하고 계산 능력이 떨어지는 단말기를 고려하여 효율적으로 그룹 키를 관리할 수 있는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법을 제공하는 것이다.
본 발명의 또 다른 목적은 멀티캐스트 서비스 제공 시 키 분배와 메시지 전송에 있어서 전송부와 제어부로 나누어 전송부에서는 메시지 전송을 담당하고 제어부에서는 키 관리만을 담당함으로서 키 관리 센터의 부정을 방지하고 연산량과 통신량에 있어 효율성을 제공하는 것이다.
본 발명의 또 다른 목적은 멤버 변동 시 해당 그룹 공통키를 재분배하지 않고 그룹 키 갱신정보만을 제공하여 사용자들이 직접 키를 갱신하게 함으로서 키 갱신에 따른 안전성과 신뢰성을 제공함과 동시에 그룹 변동 발생 시 도메인 형식의 동적인 관리를 통해 동적 그룹 변동에 따른 공정성과 확장성을 제공하는 것이다.
이러한 목적들을 달성하기 위한 본 발명은 각 관리자들의 상호인증을 통한 제 1 과정과, 그룹 초기자에 의해 그룹 멤버 리스트를 생성하여 그룹을 초기화하는 제 2 과정과, 상기 제 2 과정을 통해 초기화된 그룹에 멤버로 가입하는 제 3 과정과, 상기 제 3 과정 후 멀티캐스트 메시지를 전송하는 제 4 과정과, 이동성을 갖는 멤버를 위해 유선 또는 무선으로 원격 호스트를 통해 멀티캐스트 서비스를 지원하기 위한 제 5 과정과, 그룹 멤버 변동 시 남아 있는 멤버들의 보안을 위한 제 6 과정과, 그룹 내 또는 그룹 간 협의를 통한 그룹 합병 및 그룹 분할의 제 7 과정을 포함하여 이루어지는 것을 특징으로 한다.
본 발명에 따른 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법의 세부적 특징으로는 멤버 변동 시 최소한의 키 갱신을 유도하기 위하여 각 그룹은 도메인 형식과 계층적 서브 구조로 이루어져 있으며, 각 구조는 제어부와 전송부로 구분하여 키 관리 및 메시지 전송을 수행하고 인증 및 메시지 암호화를 위해 공개키 기반 구조를 적용함과 동시에 익명성 및 지불 인증을 위해 수신자 지정 그룹 서명 방법을 이용하는 점이다.

발명의 구성 및 작용

이하, 첨부된 도면을 참조로 본 발명을 설명한다. 먼저 본 발명에 의해 구현될 수 있는 유 · 무선 통합 멀티캐스트 키 관리 방법의 요구사항을 살펴보기로 한다.
첫째, 일반적인 요구사항
① 무결성: 멀티캐스트 정보는 전송 도중에 불법적인 제 3자로부터 위조 및 변경되어서는 안된다.
② 인증성: 송 · 수신 정보의 무결성과 정당한 멤버들로부터 멀티캐스트 메시지가 생성 및 수신되었음을 확인할 수 있어야 한다.
③ 부인 봉쇄: 참여 개체간에 전송 및 수신 사실을 부인할지라도 당사자 및 제 3자의 확인이 가능해야 한다.
④ 비밀성: 전송 및 저장되는 멀티캐스트 정보는 불법적인 제 3자로부터 보호되어야 한다.
둘째, 동적 그룹 변동에 따른 요구사항
① 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.
② 확장성: 멀티캐스트 서비스 그룹 참여자의 변동에 따른 동적인 키 관리 기법이 필요하다.
셋째, 무선 및 원격 호스트 서비스를 위한 요구사항
① 익명성: 멀티캐스트 멤버의 위치는 허가된 실체 외에는 확인할 수 없어야 한다.
② 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/수신해야한다. 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.
넷째, 무선 멀티캐스트 키 분배 및 갱신을 위한 요구사항
① 통신 병목 현상 : 무선 단말기의 특성상 효율성 유지를 위해 통신 메시지의 길이는 작아야 하며, 통신 회수는 최소가 되어야 한다.
② 키 갱신 준비 단계 overhead : 멀티캐스트 키의 분실 또는 멤버의 탈퇴에 따른 키 갱신은 별도의 준비 단계로 인한 overhead를 최소화시켜야 한다.
③ 그룹 멤버간 단합 방지 : 그룹에 속한 멤버라 할지라도 향후 사용될 멀티캐스트 키를 알 수 있어서는 안된다.
④ 2명 이상의 동시 갱신 허용 : 2명 이상의 멤버가 자신들의 단말기를 분실하거나 탈퇴할지라도, 키 갱신 회수는 최소화되어야 한다.
도 1은 본 발명에 따른 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법의 절차를 나타낸 흐름도이다. 크게 도메인 및 그룹 초기화 과정(S1)과, 그룹멤버 가입 과정(S2)과, 멀티캐스트 메시지 전송 과정(S4)과, 유 · 무선 원격 호스트 접속 및 인증 과정(S5)과, 신규멤버 가입 및 기존멤버 탈퇴 과정(S6)과, 그룹 합병 및 그룹 분할 과정(S7)으로 이루어진다.
본 발명에서는 멤버 변동 시 최소한의 키 갱신을 유도하기 위하여 각 그룹을 도메인 형식과 계층적 서브 구조로 나누어 동적으로 관리하고 있으며, 각 구조는 제어부와 전송부로 구분하여 키 관리 및 메시지 전송을 수행함으로서 키 관리의 효 율성을 제공함은 물론 각 관리자의 부정을 방지하고 있다. 또한 인증 및 메시지 암호화를 위해 공개키 기반

구조를 적용함으로서 별도의 기반구조 구축 없이 적용이 가능하고 익명성 및 지불 인증을 위해 수신자 지정 그룹 서명 방법을 이용하여 무선 환경에서의 멀티캐스트 서비스 제공에 있어 안전성을 높이고 있다.

본 발명에서 표기되는 기호들은 다음과 같이 정의한다.

· DKM_i : 도메인 키 관리자 i(i = 1, 2, ... , k : k는 도메인 키 관리자 수)
· DMB_i : Domain Border i(i = 1, 2, ... , k : k는 Border의 수)
· DKA_i : 도메인 키 중간 관리자 i(i = 1, 2, ... , j : j는 도메인 키 중간 관리자 수)
· SGB_i : Subgroup Border i(i = 1, 2, ... , j : j는 Subgroup Border의 수)
· MGB_i : Multicast Group Border i(i = 1, 2, ... , k : k는 Border의 수)
· GML : 그룹 멤버 리스트
· PKM : 도메인 키 (중간)관리자들 및 각 Border의 공개키 관리자
· MBR_i : 그룹 멤버 i (i = 1, 2, 3, ... , n : n은 멤버의 수)
· R : 라우터
· GI : 그룹 초기자
· Sig_* : *의 서명
· MKey : PKM에 의해 생성된 멀티캐스트 키
· K_{PP} , K_{PS} : PKM의 공개키 및 개인키
· K_{DPi} , K_{DSi} : 각 DKM_i 의 공개키 및 개인키
· K_{DAPi} , K_{DASi} : 각 DKA_i 의 공개키 및 개인키
· K_{DMBPi} , K_{DMBSi} : 각 DMB_i 의 공개키 및 개인키
· K_{MGBPi} , K_{MGBSi} : 각 MGB_i 의 공개키 및 개인키
· K_{SGBPi} , K_{SGBSi} : 각 SGB_i 의 공개키 및 개인키
· K_{D_DAi} : DKM_i 와 DKA_i 사이의 공통키
· K_{MSi} : 그룹 멤버 MBR_i 의 비밀키
· K_{DAi_Msj} : 각 DKA_i 가 관리하는 멤버들과의 공통키(Subgroup 공통키)
· Hdr : 메시지 전송 시 송신 그룹과 수신 그룹의 식별 정보
· ID_* : *의 식별자
· IP_* : *의 IP 주소
· M : 멀티캐스팅 메시지
· K_{GSi} , K_{GVi} : 수신자 지정 그룹 서명용 키 및 확인 키
· T, Tr : 멤버가 생성하는 Time-Stamp 및 원격 호스트가 제공하는 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_i 가 생성하는 큰 소수(j는 키 갱신 순번)
· Ter_i : 각 사용자의 무선 터미널 (i={1, 2, ..., n})
· Y_{ij} , Y_{ij}^{-1} : Subgroup 공통키 은닉 정보 및 역수
· S_{ij} : DKA_i 에 의해 생성되는 Subgroup 멤버 i의 비밀 정보
· Ref_key : Subgroup 공통키 갱신 정보

먼저 도메인 및 그룹 초기화 과정(S1)을 상세히 살펴보기로 한다. 도 2는 본 발명에 따른 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법의 도메인 및 그룹 초기화 단계를 상세히 나타낸 흐름도이다. DKM_i , DKA_i 및 각 Border는 안전한 유니캐스트 채널을 통해 자신의 공개키 인증서를 PKM으로부터 수신한다.

· PKM : $Cert(ID_{DKMi} \| K_{DPi} \| IP_{DKMi}) \rightarrow DKM_i$
: $Cert(ID_{DKAi} \| K_{DAPi} \| IP_{DKAi}) \rightarrow DKA_i$
: $Cert(ID_{MGBi} \| K_{MGBPi} \| IP_{MGBi}) \rightarrow MGB_i$
: $Cert(ID_{DMBi} \| K_{DMBPi} \| IP_{DMBi}) \rightarrow DMB_i$
: $Cert(ID_{SGBi} \| K_{SGBPi} \| IP_{SGBi}) \rightarrow SGB_i$ ·····(S11)

각 도메인은 DKM_i 를 정점으로 멤버들을 분할하여 담당하는 각 DKA_i 를 계층적으로 관리한다. 공개키 인증서 수신이 끝나게 되면 도메인 상의 각 관리자들은 상호 인증을 수행한다(S12).

GI는 그룹 멤버 리스트(GML)를 작성하여 자신의 식별자 ID_{GI} 와 함께 서명을 수행하여 PKM에게 전송한다.

· GI : $Sig_{GI}(ID_{GI} \| GML) \rightarrow PKM$
: $GML = (ID_{MBR1} \| \cdots \| ID_{MBRn})$ ·····(S13)

PKM은 서명 확인을 통해 GI 및 GML을 인증하고(S14) 멀티캐스트 서비스를 위한 MKey를 생성한다(S15). 단, MKey는 그룹이 형성될 때, 오직 관련된 Border들(SGB_i , DMB_i , MGB_i)에게만 제공함으로서 신뢰성을 높이고 있다.

· PKM : $K_{BPi}(MKey \| Sig_{PKM}(ID_{PKM})) \rightarrow$ 각 Border (SGB_i , DMB_i , MGB_i)
: $K_{BPi} \in \{K_{SGBPi}, K_{DMBPi}, K_{MGBPi}\}$ ·····(S16)

PKM은 해당 Domain에게 공개키를 이용하여 안전하게 GML을 전송한다.

· PKM : $K_{DPi}(GML \| Sig_{PKM}(GML)) \rightarrow DKM_i$ ·····(S17)

본 발명에 따른 그룹 멤버 가입 과정은 도 3의 흐름도를 이용하여 설명하기로 한다. DKM_i 는 도메인 내에서 DKA_i 와의 통신 시 사용할 K_{D_DAi} 를 생성하여 유니캐스트 채널을 통하여 안전하게 DKA_i 에게 전송한다.

· $DKM_i : K_{DAPi}(K_{D\_DAi} \| Sig_{PKM}(K_{D\_DAi})) \rightarrow DKA_i$ ·····(S21)

그룹에 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i에게 자신을 인증한다.(S22) 이때 멤버 가입 대상자들 중 무선 멀티캐스팅 서비스를 필요로 할 경우(S23), 무선 멀티캐스트 서비스 요청을 다음과 같이 K_{DAPi}를 이용하여 안전하게 전송한다(S24).

· $MBR_i : K_{DAPi}(ID_{MBRi} \| K_{MSi} \| Req\_{}_{WMS} \| Sig_{MSi}(ID_{MBRi} \| K_{MSi} \| Req\_{}_{WMS})) \rightarrow DKA_i$

· $Req\_{}_{WMS} = \{0, 1\}$ ·····(S24)

DKA_i는 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행(S25)하고 다음과 같이 그룹 가입 멤버 리스트를 생성해 DKM_i에게 전송한다.(S26)

· $DKA_i : K_{D\_DAi}(Sig_{DKAi}(ID_{MBR1} \| \cdots \| ID_{MBRi})) \rightarrow DKM_i$

DKM_i는 각 DKA_i로부터 수신된 그룹 가입 멤버 리스트에 대해 복호 및 인증을 수행한 다음 GML과 비교 확인한다.(S27) GML과 수신된 정보가 다른 경우가 발생하는데, 하나는, 멤버가 가입 신청을 하였다가 취소하는 경우로서 이런 경우에는 GML에서 가입하지 않은 사용자의 ID를 삭제하고 PKM에게 통보한다. 두 번째는, GML에 기입된 멤버 이외에 타인이 가입하는 경우로서 DKA_i에게 이 사실을 통보하고 멀티캐스트 관련키를 분배하지 않으면 된다.

DKA_i는 Subgroup 키 갱신 정보를 다음과 같이 생성한 후에, 수신된 비밀키 K_{MSi}를 이용하여 각 멤버에게 K_{DAi_Ms1}, Subgroup 키 갱신 정보 및 수신자 지정 그룹 서명 키 K_{GSi}를 안전하게 전송해 준다. 동시에 이 K_{DAi_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi}는 DKM_i 및 SGB_i에게 안전하게 전송된다. (S28)

· P_j (j={1, ..., m}) 생성 및 멤버 비밀 정보 계산

$GCD(S_{ij}, S_{ik}) = 1$ (단, $S_{ij} \neq S_{ik}$)

· K_{DAi_Msj} 생성 및 그룹 키 은닉 정보 및 역수 계산

$Y_{ij} = K_{DAi\_Msj}^{Sij} \bmod P_j$, Y_{ij}^{-1} (단, j = {2, ..., n})

· Subgroup 키 갱신 정보 생성

$Ref\_key = (S_{i1}, Y_{i1}, Y_{i1}^{-1}, ..., S_{im}, Y_{im}, Y_{im}^{-1})$

· $DKA_i : K_{MSi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow MBR_i$

: $K_{D\_DAi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow DKM_i$

: $K_{SGBPi}(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow SGB_i$

각 멤버는 무선 멀티캐스팅을 위해, 수신된 Subgroup 키 갱신 정보를 스마트 카드와 같은 저장 공간에 저장한다.(S29)

본 발명에 따른 메시지 전송 과정은 도 4a의 흐름도에 나타낸 바와 같다. 멀티캐스트 메시지 전송부로서 오직 멤버들 MBR_i와 각 보더(Border)들만이 관여한다. 이 단계는 도메인 내 각 멤버들에게 메시지를 전송하는 내부 전송 과정(A,B)과 타 도메인 및 다른 멀티캐스트 그룹에 속한 멤버들에게 보내는 외부 전송 과정(C,D)으로 분류된다.

내부 전송 과정은 도메인 전체로 전송(A)과 특정 서브그룹(Subgroup)으로의 전송 과정(B)으로 나누어진다. 도메인 전체 전송의 수행과정은 도 4b의 흐름도에서 도시된 바와 같다. 각 멤버들은 K_{DAi_Ms1}를 이용하여 멀티캐스트 메시지 M을 암호화한 다음 SGB_i에게 전송한다.

· $MBR_i : K_{DAi\_Ms}(M) \rightarrow SGB_i$ ·····(A11)

SGB_i는 수신된 정보를 복호화하고, 멀티캐스트 메시지 M을 MKey로 암호화하여 각 SGB_i'에게 전송한다.

· $SGB_i : K_{DAi\_Ms1}(K_{DAi\_Ms1}(M)) = M$

· $SGB_i : Mkey(M) \rightarrow SGB_i'$

: $SGB_i \neq SGB_i'$ ·····(A12)

각 SGB_i는 수신된 정보를 복호화하고 이를 자신이 속한 그룹의 공통키로 암호화하여 그룹 멤버들에게 전송한다.

· $SGB_i : MKey(MKey(M)) = M$

: $K_{DAi\_Ms1}'(M) \rightarrow MBR_i'$

: K_{DAi_Ms1}'는 DKA_i'와 그 Subgroup에 속한 멤버들간의 Subgroup 공통키

: $MBR_i \neq MBR_i'$ ·····(A13)

각 Subgroup의 멤버 MBR_i'는 K_{DAi_Ms1}'로 수신된 정보를 복호화하여 메시지를 확인한다.

· $MBR_i' : K_{DAi\_Ms1}'(K_{DAi\_Ms1}'(M)) = M$ ·····(A14)

다음은 특정 서브그룹(Subgroup)으로의 전송 과정(B)을 도 4c의 흐름도를 이용하여 상세히 살펴보기로 한다. 각 멤버들은 K_{DAi_Ms1}을 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB_i에게 전송한다.

· $MBR_i : K_{DAi\_Ms1}(Hdr \| M) \rightarrow SGB_i$ ·····(B1)

SGB_i는 암호화되어 수신된 정보를 복호화 한다.

· $SGB_i : K_{DAi\_Ms1}(K_{DAi\_Ms1}(Hdr \| M)) = Hdr \| M$

SGB_i는 Hdr을 확인하고 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 자신의 서명과 함께 SGB_{i+1}에게 전송한다.

· $SGB_i : (Hdr \| Sig_{SGBi}(Hdr) \| MKey(M)) \rightarrow SGB_{i+1}$ ·····(B2)

해당 SGB_{i+1}는 Hdr과 서명을 확인하고 수신된 정보를 복호화한다. 복호된 멀티캐스트 메시지 M을 자신이 속한 서브그룹(Subgroup) 공통키로 암호화하여 서브그룹(Subgroup)멤버들에게 전송한다.

· SGB_{i+1} : Hdr, $Sig_{SGBi}(Hdr)$ 확인

: $MKey(MKey(M)) = M$

: $K_{DAi+1\_Ms1}(M) \rightarrow MBR_{i+1}$

: K_{DAi+1_Ms1} 는 DKA $_{i+1}$ 과 그 Subgroup에 속한 멤버들간의 Subgroup 공통키…(B3)
서브그룹(Subgroup)의 멤버 MBR $_{i+1}$ 은 K_{DAi+1_Ms1} 로 수신된 정보를 복호화하여 메시지를 확인한다.
· MBR $_{i+1}$: K_{DAi+1_Ms1} (K_{DAi+1_Ms1} (M)) = M ……(B4)
외부로의 전송 과정(C,D)은 도메인에서 도메인으로의 전송(C)과 멀티캐스트 그룹간 메시지 전송 과정(D)으로 나누어 볼 수 있다. 먼저 도메인에서 도메인으로의 전송과정을 도 4d의 흐름도를 이용하여 상세히 살펴본다. 각 멤버들은 K_{DAi_Ms1} 를 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB $_i$ 에게 전송한다.
· MBR $_i$: K_{DAi_Ms1} (Hdr ‖ M) → SGB $_i$ ……(C1)
SGB $_i$ 는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB $_i$ 에게 전송한다.
· SGB $_i$: K_{DAi_Ms1} (K_{DAi_Ms1} (Hdr ‖ M)) = Hdr ‖ M
: (Hdr ‖ Sig $_{SGBi}$ (Hdr) ‖ MKey(M)) → DMB $_i$ ……(C2)
DMB $_i$ 는 Hdr을 확인하고 인접 도메인 Border DMB $_{i+1}$ 에게 전송한다.
· DMB $_i$: (Hdr ‖ Sig $_{SGBi}$ (Hdr) ‖ MKey(M)) → DMB $_{i+1}$ ……(C3)
DMB $_{i+1}$ 은 Hdr과 서명을 확인하고 해당 도메인에 속한 모든 SGB $_{i+1}$ 에게 전송한다.
· DMB $_{i+1}$: MKey(M) → SGB $_{i+1}$ ……(C4)
전송된 메시지는 각 SGB $_{i+1}$ 에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.
· SGB $_{i+1}$: Mkey(MKey(M)) = M
: K_{DAi+1_Ms1} (M) → MBR $_{i+1}$
: K_{DAi+1_Ms1} 는 DKA $_{i+1}$ 와 그 Subgroup에 속한 멤버들간의 Subgroup 공통키…(C5)
각 DKA $_{i+1}$ 에 속한 Subgroup의 모든 멤버 MBR $_{i+1}$ 은 K_{DAi+1_Ms1} 로 복호화하여 메시지를 확인한다.
· MBR $_{i+1}$: K_{DAi+1_Ms1} (K_{DAi+1_Ms1} (M)) = M ……(C6)
다음은 멀티캐스트 그룹간 메시지 전송 과정(D)이다. 멀티캐스트 그룹간 메시지 전송 시에는 PKM과 연결되어 있는 MGB $_i$ 를 통해 이루어지며, 모든 전송과정은 도메인에서 도메인으로의 전송과정과 동일하다.
각 멤버들은 K_{DAi_Ms1} 을 이용하여 멀티캐스트 메시지 M과 식별자 Hdr을 암호화한 다음 자신이 속한 SGB $_i$ 에게 전송한다.
· MBR $_i$: K_{DAi_Ms1} (Hdr ‖ M) → SGB $_i$ ……(D1)
SGB $_i$ 는 암호화되어 수신된 정보를 복호화한 후에 Hdr을 확인하고 자신의 서 명과 함께 복호된 멀티캐스트 메시지 M을 MKey로 암호화하여 DMB $_i$ 에게 전송한다.
· SGB $_i$: K_{DAi_Ms1} (K_{DAi_Ms1} (Hdr ‖ M)) = Hdr ‖ M
: (Hdr ‖ Sig $_{SGBi}$ (Hdr) ‖ MKey(M)) → DMB $_i$ ……(D2)
DMB $_i$ 는 Hdr을 확인하고 MGB $_i$ 에게 전송한다.
· DMB $_i$: (Hdr ‖ Sig $_{SGBi}$ (Hdr) ‖ MKey(M)) → MGB $_i$ ……(D3)
MGB $_i$ 는 Hdr을 확인하고 MGB $_{i+1}$ 에게 전송한다.
· MGB $_i$: (Hdr ‖ Sig $_{SGBi}$ (Hdr) ‖ MKey(M)) → MGB $_{i+1}$ ……(D4)
MGB $_{i+1}$ 은 Hdr과 서명을 확인하고 해당 멀티캐스트 그룹에 속한 모든 DMB $_{i+1}$ 에게 전송한다.
· MGB $_{i+1}$: MKey(M) → DMB $_{i+1}$ ……(D5)
전송된 메시지는 각 DMB $_{i+1}$ 에 의해 해당 도메인의 모든 SGB $_{i+1}$ 에게 전송된다.
· DMB $_{i+1}$: MKey(M) → SGB $_{i+1}$ ……(D6)
전송된 메시지는 각 SGB $_{i+1}$ 에 의해 복호화된 다음 각 그룹의 모든 멤버들에게 암호화되어 전송된다.
· SGB $_{i+1}$: Mkey(MKey(M)) = M
: K_{DAi+1_Ms1} (M) → MBR $_{i+1}$
: K_{DAi+1_Ms1} 는 DKA $_{i+1}$ 와 그 Subgroup에 속한 멤버들간의 Subgroup 공통키 …(D7)
각 DKA $_{i+1}$ 에 속한 Subgroup의 모든 멤버 MBR $_{i+1}$ 은 K_{DAi+1_Ms1} 로 복호화하여 메시지를 확인한다.
· MBR $_{i+1}$: K_{DAi+1_Ms1} (K_{DAi+1_Ms1} (M)) = M ……(D8)
유 · 무선 원격 호스트 접속 및 인증은 도 5에 나타낸 바와 같다. 이동성을 가지는 멤버(MBR $_i$)는 사용 매체에 따라 유선 또는 무선으로 원격 호스트를 통해 멀티캐스트 서비스를 지원 받아야 하므로, 자신의 인증 과정은 필수적이다. 이때, 자신의 익명성을 제공받기 위해 가명 ID와 수신자 지정 그룹 서명을 수행한다.
멤버는 원격 호스트에서 사용할 자신의 가명 식별자 ID $_N$ 를 생성한다. 또한 서비스 개시를 위한 Time-Stamp를 생성하여 지불 인증을 받을 DKM $_i$ 와 가명 식별자를 수신자 지정 그룹 서명을 수행하고 다음과 같이 원격 호스트에게 전송한다. 가명 식별자를 사용하는 이유는 제 3자로부터 자신의 신분을 숨기기 위해서이다.
· ID $_N$ ‖ K_{GSi} (ID $_N$ ‖ ID $_{Nr}$ ‖ DKM $_i$ ‖ T) → RH $_i$ ……(S51)
원격 호스트는 수신자 지정 서명을 확인한 다음, 멀티캐스트 서비스 수행을 위해 도메인 Border와 채널을 형성한다.(S52)
멤버(MBR $_i$)가 이동성이 빨라 Hand-off가 발생될 경우(S53), 원격 호스트 RH $_i$ 는 다음 원격 호스트 RH $_{i+1}$ 및 DKM $_i$ 에게 다음의 정보를 전송해 준다.
· K_{RHPi+1} (ID $_{Nr}$ ‖ Tr) ‖ K_{GSi} (ID $_N$ ‖ ID $_{Nr}$ ‖ T) → RH $_{i+1}$
· K_{DPi} (ID $_{Nr}$ ‖ Tr) ‖ K_{GSi} (ID $_N$ ‖ ID $_{Nr}$ ‖ DKM $_i$ ‖ T) → DKM $_i$ ……(S54)
멤버 정보를 수신하면, DKM $_i$ 는 다음과 같이 지불 확인 정보를 RH $_i$ 에게 전송한다. 이를 통해 RH $_i$ 는 지불 인증을 받게 된다.

· $ID_{Nr} \| K_{DAPi}(ID_N \| Tr\text{-}T)$ ·····(S55)

RH_{i+1} 은 수신된 정보를 확인한 다음, 상기 (S52) 과정을 수행한다.

사용자 요구에 의해 멀티캐스트 접속이 완료되면, 멤버 MBR_i 에게 다음의 정보를 각각 전송한다.

· $ID_{Nr+1} \| Tr_{+1} \| K_{RSi+1}(ID_N \| ID_{Nr+1} \| Tr \| Tr_{+1}) \rightarrow MBR_i$ ·····(S56)

MBR_i 는 수신정보를 확인한 후에, 다음 정보를 생성해 RH_{i+1} 에게 전송한다.

· $ID_N \| K_{GSi}(ID_N \| ID_{Nr+1} \| DKM_i \| Tr \| Tr_{+1}) \rightarrow RH_{i+1}$ ·····(S57)

RH_{i+1} 은 다음의 정보를 DKM_i 에게 전송한다.

· $K_{DPi}(ID_{Nr+1} \| Tr_{+1}) \| K_{GSi}(ID_N \| ID_{Nr+1} \| DKM_i \| Tr \| Tr_{+1}) \rightarrow DKM_i$ ·····(S58)

DKM_i 는 RH_i 에게 지불인증정보를 전송함으로써 지불 인증을 수행한다.

도 6은 본 발명에 따른 신규 멤버 가입 및 기존 멤버 탈퇴 단계를 상세히 나타낸 흐름도이다. 신규 멤버 가입 단계는 도 3의 멤버 가입 단계와 동일한 과정을 수행하여 이루어진다. 그룹에 신규 멤버로 가입할 사용자들은 자신의 서명을 이용하여 DKA_i 에게 자신을 인증하고 자신의 비밀키 K_{MSi} '를 K_{DAPi} 로 암호화하여 안전하게 전송한다.

· $MBR_i : K_{DAPi}(ID_{MBRi}' \| K_{MSi}' \| Req\_{}_{WMS} \| Sig_{MSi}'(ADD \| ID_{MBRi}' \| K_{MSi}' \| Req\_{}_{WMS})) \rightarrow DKA_i$

· $Req\_{}_{WMS} = \{0, 1\}$

: ADD는 신규 가입 대상자임을 나타내는 식별자

DKA_i 는 신규 가입 대상자들로부터 받은 메시지를 복호화하여 인증을 수행하고 다음과 같이 신규 가입 멤버 정보를 생성해 DKM_i 에게 전송한다.

· $DKA_i : K_{D\_DAi}(Sig_{DKAi}(ADD \| ID_{MBRi}')) \rightarrow DKM_i$

DKM_i 는 DKA_i 로부터 수신된 그룹 신규 가입 멤버 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 PKM에게 전송한다.

· $DKM_i : GML \rightarrow GML'$

: $GML' = (ID_{MBR1} \| \cdots \| ID_{MBRn} \| ID_{MBRi}')$

: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$

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

DKA_i 는 (S28)과 동일한 과정을 통해 K_{DAi_Ms1} , Subgroup 키 갱신 정보 및 K_{GSi} 를 안전하게 신규 가입 멤버에게 전송해 준다. 신규 멤버 가입시에는 K_{DAi_Ms1} 에 대한 별도의 변화는 필요 없게 된다.

· $DKA_i : K_{MSi}'(K_{DAi\_Ms1} \| Ref\_key \| K_{GSi}) \rightarrow MBR_i'$

기존 멤버 탈퇴 또는 무선 단말기 분실 시에는 기존 멤버를 보호하고 불법 사용을 방지하기 위해 기존의 K_{DAi_Ms1} 을 갱신하여야 한다. 이를 통해 그룹 탈퇴자와 악성 침입자로부터 기존 멤버들에 대한 보안성을 획득할 수 있다. 도 6은 탈퇴나 단말기 분실에 따른 처리를 나타낸 흐름도이다.

그룹 탈퇴를 희망하는 멤버가 있거나, 무선 단말기를 분실하였을 경우는 다음과 같은 정보를 생성하여 DKA_i 에게 안전하게 전송한다.

· $MBR_i : K_{DAPi}(Sig_{MSi}(DEL \| ID_{MBRi})) \rightarrow DKA_i$ ·····(C61)

: DEL은 그룹 탈퇴 희망자 또는 단말기 분실자임을 나타내는 식별자

DKA_i 는 다음과 같은 정보를 생성해 DKM_i 에게 전송한다.

· $DKA_i : K_{D\_DAi}(Sig_{DKAi}(DEL \| ID_{MBRi})) \rightarrow DKM_i$ ·····(C62)

DKM_i 는 DKA_i 로부터 수신된 정보에 대해 복호 및 인증을 수행한 다음 GML의 내용을 수정한다. 수정된 GML'을 안전하게 PKM에게 전송한다.

· $DKM_i : GML \rightarrow GML'$

: $GML' = (ID_{MBR1} \| \cdots \| ID_{MBRi-1} \| ID_{MBRi+1} \| \cdots \| ID_{MBRn})$

: $K_{DPi}(Sig_{DKMi}(GML')) \rightarrow PKM$ ·····(C63)

PKM은 GML'의 수정 내용을 확인한 다음 GML을 GML'으로 교체한다.(C64)

DKA_i 는 Subgroup 갱신을 위해 기존의 멤버들 MBR_i', DKM_i 및 SGB_i 에게 Subgroup 갱신 관련 부가 정보를 전송한다.

· $P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}, ..., P_j, S_{ij}, Y_{ij}, Y_{ij}^{-1}$ ·····(C65)

MBR_i', DKM_i 및 SGB_i 에는 아래와 같은 처리과정을 통해 새로운 Subgroup 공통키 K_{DAi+1_Msj} 를 생성한다. 이를 통해 이동 중인 기존 멤버들도 간편하게 키 갱신을 수행할 수 있다.

· 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
: $K=(\prod_{j=1}^{i} K_j) \bmod n$
그룹 합병 및 그룹 분할 단계는 도 7에 나타낸 바와 같다. 그룹 합병을 원하는 DKA_i는 그룹 합병 요구 메시지를 다음과 같이 통고한다.
· DKA_j : Hdr ‖ K_{DAj_Ms1} (Request) → SGB_j
· SGB_j : Hdr ‖ Sig_{SGBi} (Hdr) ‖ MKey(Request) → SGB_i
· SGB_i : K_{DAi_Ms1} (Request) → DKA_i ·····(S71)
DKA_i는 Border를 통해 받은 전송 정보를 복호화하여 확인하고 그룹 합병을 결정한다.(S72)
그룹 합병이 결정되면(S73) 그룹 합병 승인 메시지를 DKA_j에게 전송(S74)하고 승인 메시지를 받은 DKA_j는 그룹 멤버 리스트 GML_j를 DKA_i에게 전송한다.(S75)
DKA_i는 새로운 공통키 K_{DAi+j_Ms1}을 생성하여 DKM_i에게 그룹 합병 정보와 새로운 공통키 K_{DAi+j_Ms}, 공통키 갱신정보 Ref_key 및 DKA_j의 그룹 멤버 리스트 GML_j를 함께 전송한다.
· DKA_i : K_{D_DAi} (Sig_{DKAi} (Union ‖ GML_j ‖ Ref_key ‖ K_{DAi+j_Ms1})) → DKM_i
여기에서 Union은 그룹 합병 정보 식별자를 의미한다. ·····(S76)
DKM_i는 DKA_i로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성하여 PKM에게 전송한다.
· DKM_i : GML_{i+j}
: $GML_{i+j} = (GML_i + GML_j)$
: K_{DPi} (Sig_{DKMi} (GML_{i+j})) → PKM ·····(S77)
DKA_i는 신규 멤버 가입 과정과 동일한 과정을 통해 새로운 공통키 K_{DAi+j_Ms1}, Subgroup 키 갱신 정보 및 K_{GSi} 등을 모든 멤버들 MBR_i와 SGB_i에게 전송하고, DKA_j에게는 DKA_i의 그룹 멤버 리스트 GML_i를 함께 전송한다.
· DKA_i : K_{BPi} (K_{DAi+j_Ms1} ‖ Ref_key) → SGB_i
: K_{DAi_Ms} (K_{DAi+j_Ms1} ‖ Ref_key) → MBR_i
: Hdr ‖ K_{DAj_Ms} (GML_i ‖ K_{DAi+j_Ms1} ‖ Ref_key) → DKA_j
DKA_j는 키 갱신 과정과 동일한 과정을 수행한다.
· DKA_j : K_{BPj} (K_{DAi+j_Ms1} ‖ Ref_key) → SGB_j
: K_{DAj_Ms} (K_{DAi+j_Ms1} ‖ Ref_key) → MBR_j
: K_{D_DAj} (Sig_{DKAj} (Union ‖ GML_i ‖ K_{DAi+j_Ms1} ‖ Ref_key)) → DKM_j
: Union은 그룹 합병 정보 식별자
DKM_j는 DKA_j로부터 수신된 그룹 합병 정보에 대해 복호 및 인증을 수행한 다음 새로운 그룹 멤버 리스트 GML_{i+j}를 생성한다.
· DKM_j : GML_{i+j}
: $GML_{i+j} = (GML_i + GML_j)$ ·····(S78)
합병된 그룹에서의 그룹의 분할은 그룹 합병과는 달리 그룹 분할 정보를 DKA_{i+j}, DKM_{i+j}, SBG_{i+j}, 모든 그룹 멤버 MBR_{i+j}에게 전달하고 이를 전달받은 각 개체는 해당 그룹 키를 삭제한다. 또한 DKM_{i+j}와 PKM_{i+j}는 그룹의 멤버 리스트 GML_{i+j}를 삭제함으로써 완료된다.
기존 그룹DKA_i가 분할될 경우 새로 생성되는 그룹의 DKA_j와 SGM_j가 생성되며, 각 그룹은 다음과 같은 과정으로 새로운 GML과 그룹 키를 생성하게 된다.
기존 그룹의 DKA_i는 기존 멤버 탈퇴 시와 같은 방법으로 GML과 그룹 키를 갱신하고 새로 생성된 그룹의 DKA_j는 그룹 멤버 가입단계와 같은 과정을 수행한다.
이상에서 본 발명에 대한 기술 사상을 첨부 도면과 함께 서술하였지만 이는 본 발명의 가장 양호한 실시 예를 예시적으로 설명한 것이지 본 발명을 한정하는 것은 아니다. 또한, 이 기술 분야의 통상의 지식을 가진 자이면 누구나 본 발명의 기술 사상의 범주를 이탈하지 않는 범위 내에서 다양한 변형 및 모방이 가능함은 명백한 사실이다.

발명의 효과

이상에서 설명한 바와 같이 본 발명은 종래의 유선 멀티캐스트 그룹 키 관리 구조에 있어 멤버 변동에 따른 키 갱신과 그룹 확장성 문제를 도메인 형식과 계층적 서브 구조를 통해 최소한의 키 갱신을 유도함과 동시에 확장성을 제공하고 있으며, 유선 환경뿐만 아니라 무선 환경에서의 서비스까지도 고려하여 무선 멀티캐스트 서비스 제공 시 수신자 지정 그룹 서명 방법을 통한 사용자의 위치 익명성을 보장하고 무선 그룹 키 갱신 방법을 통해 계산량이 상대적으로 떨어지는 무선 단말기에서도 효율적으로 그룹 키를 갱신하도록 함으로서 키 갱신의 효율성을 제공하고 있다.
이와 함께 본 발명은 공개키 기반 구조를 적용함으로서 향후 별도의 기반구조 구축 없이 유 · 무선 멀티캐스트 서비스를 제공할 수 있으며, 멀티캐스트 서비스 제공시 키 관리를 담당하는 제어부와 메시지 전송을 담당하는 전송부로 나누어 관리함으로서 키 관리 센터의 부정을 방지함과 동시에 메시지 전송 시 연산량 및 통신량에 있어 효율성을 제공하고 있다.

따라서 본 발명은 그룹 키 관리의 효율성과 확장성을 제공함은 물론 공개 네트워크 상에서의 불법 행위로부터 안전하게 멀티캐스트 서비스를 제공할 수 있는 요소들을 포함하고 있다. 또한, 네트워크 및 이동 통신의 발전으로 향후 정보화 사회는 전자 상거래 서비스 및 그룹 기반 서비스 등 더욱 다양한 응용 서비스들을 제공하게 될 것이다. 이러한 유선 및 무선 통신 환경 상에서 안전성과 효율성 및 확장성을 제공하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법의 제안은 전자 상거래 서비스 및 그룹 기반 응용 서비스들의 발전에 기여하는데 큰 효과가 있을 것이라 판단된다.

(57) 청구의 범위

청구항 1.

공개키 기반 구조하에 공개키 관리 기관(PKM)이 각 관리자에게 공개키 인증서를 전송하고 상호 인증을 통해 도메인을 초기화하는 제 1 과정과,
상기 제 1 과정을 통해 생성된 도메인에 그룹을 초기화하고 그룹 키를 생성하여 해당 보더(Border)에게만 전송하는 제 2 과정과,
상기 제 2 과정을 통해 생성된 그룹에 멤버로 가입을 원하는 사용자들을 인증하고 서브그룹(Subgroup) 키 갱신 정보를 생성하여 각 멤버 및 참여 개체에게 전송하는 제 3 과정과,
멀티캐스트 메시지 전송 시 외부 전송과정과 내부 전송과정으로 구분하여 전송 주체와 해당 보더(Border)에 의해 메시지를 전송하는 제 4 과정과,
이동성을 갖는 멤버를 고려한 원격 호스트 접속 및 인증과정과 원격 호스트 핸드오프(Hand-off) 및 지불 인증을 수행하는 제 5 과정과,
그룹 멤버 변동 시 서브그룹(Subgroup)키 갱신 정보를 통해 새로운 공통키를 생성하는 제 6 과정과,
동적 그룹 확장성을 고려하여 그룹 합병 및 그룹 분할을 수행하는 제 7 과정을 포함하여 이루어지는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

청구항 2.

제 1 항에 있어서; 상기 제 1 과정은,
공개키관리기관(PKM)이 각 참여요소에게 공개키 인증서를 전송하는 제 1 단계(1-1)와,
각 관리자들의 상호 인증을 수행하는 제 2 단계(1-2)와,
그룹초기자(GI)가 그룹멤버리스트(GML)를 작성하여 자신의 식별자와 함께 서명하여 공개키 관리 기관(PKM)에 전송하는 제 3 단계(1-3)와,
공개키관리기관(PKM)에서 그룹 초기자(GI)와 그룹멤버리스트(GML)를 인증하는 제 4 단계(1-4)와,
공개키관리기관(PKM)에서 멀티캐스트 서비스를 위한 멀티캐스트 키(Mkey)를 생성하는 제 5 단계(1-5)와,
공개키관리기관(PKM)에서 관련된 보더(border)들에게 상기 멀티캐스트 키를 전송하는 제 6 단계(1-6)와,
공개키관리기관(PKM)에서 해당 도메인에게 공개키를 이용하여 상기 그룹멤버리스트(GLM)을 전송하는 제 7 단계(1-7)로 이루어지는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

청구항 3.

제 1 항에 있어서; 상기 제 2 과정은,
각 도메인 키 관리자(DKM)가 공통키를 생성하여 각 도메인 키 중간관리자(DKA)에게 전송하는 제 1 단계(2-1)와,
각 도메인 키 중간관리자가 멤버로 가입할 사용자의 인증 정보를 수신하는 제 2 단계(2-2)와,
각 도메인 키 중간관리자가 수신된 메시지를 복호화하여 인증을 수행하는 제 3 단계(2-3)와,
각 도메인 키 중간관리자가 그룹가입 멤버리스트를 도메인 키 관리자(DKM)에게 전송하는 제 4 단계(2-4)와,
각 도메인 키 관리자가 수신한 그룹가입멤버리스트를 복호화하여 인증하는 제 5 단계(2-5)와,
각 도메인 키 중간관리자가 서브그룹키 갱신정보 및 수신자 지정그룹 서명키를 각 멤버에게 전송하는 제 6 단계(2-6)와,
각 멤버가 수신 받은 서브그룹키 갱신정보를 소정의 저장공간에 저장하는 제 7 단계(2-7)로 이루어지는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

청구항 4.

제 3 항에 있어서;
상기 제 2 단계(2-2)에서 멤버가입 대상자의 사용자 인증 요구 메시지에는 무선 멀티캐스트 서비스 요청이 포함된 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

청구항 5.

제 1 항에 있어서; 멀티캐스트 메시지 전송에 의해 수행되는 상기 제 4 과정에서 제어부와 전송부로 나누어 제어부에서는 키 관리만을 수행하고 메시지 전송 시 전송부의 보더(Border)들만이 관여하는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

청구항 6.

제 1 항에 있어서; 그룹 키 갱신 정보를 통해 수행되는 상기 제 6 과정에서 멤버 변동 시 키를 재분배하는 것이 아닌 그룹 키 갱신 정보를 통해 사용자들이 직접 그룹 키를 갱신하는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

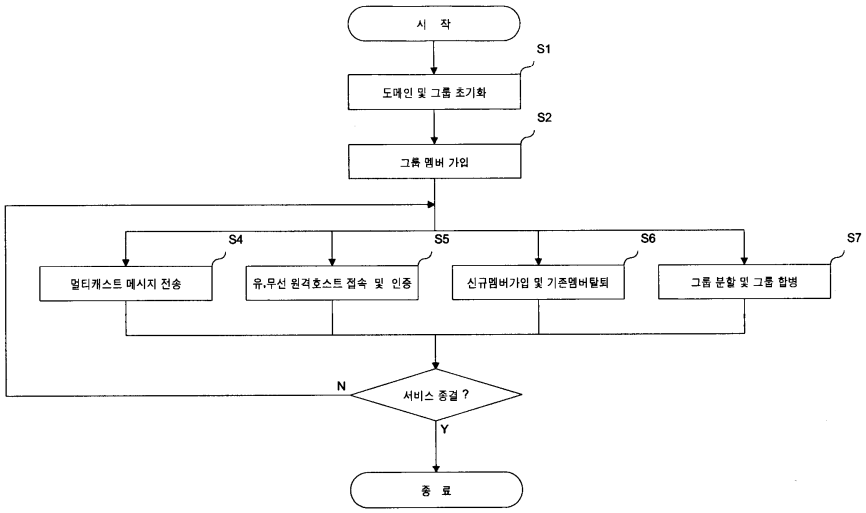
청구항 7.

제 1 항에 있어서;

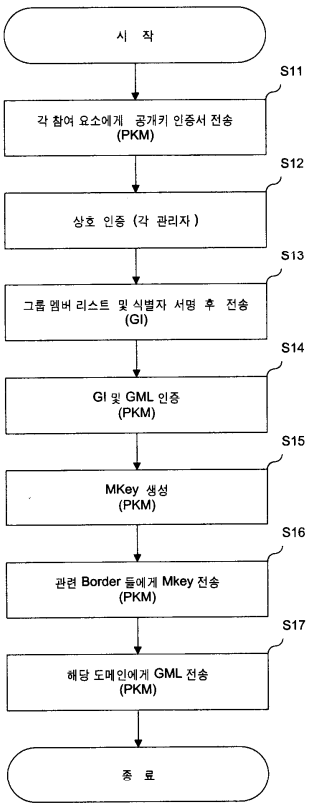
이동성을 갖는 멤버를 고려한 원격 호스트 접속 및 인증과정과 원격 호스트 핸드오프(Hand-off) 및 지불 인증을 수행하는 제 5 과정과, 서브그룹(Subgroup)키 갱신 정보를 통해 새로운 공통키를 생성하는 제 6 과정에서 수신자 지정 그룹 서명 방법 적용하여 이동성을 갖는 사용자들의 위치 익명성을 보장함과 동시에 신원 보장이 가능하다는 것을 특징으로 하는 유 · 무선 통합 멀티캐스트 그룹 키 관리 방법.

도면

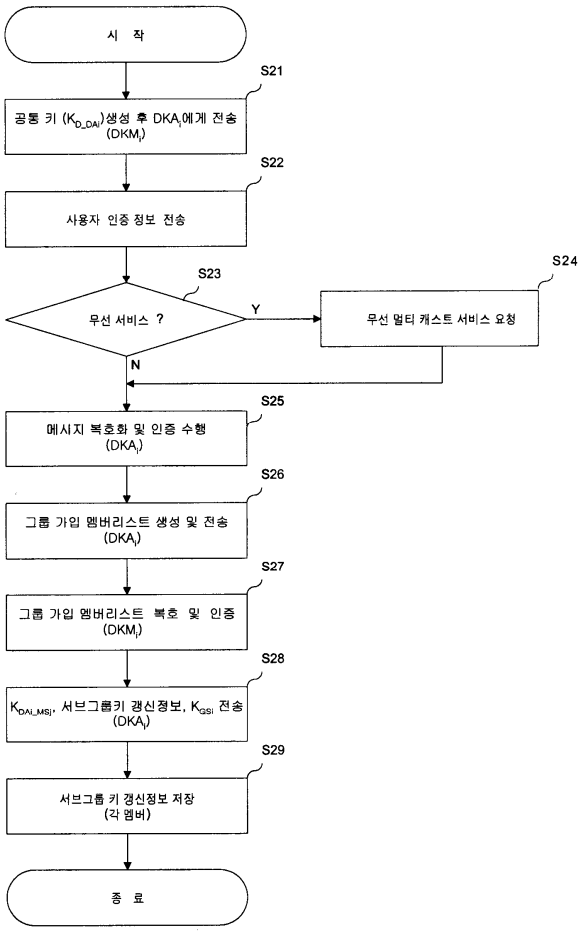
도면1



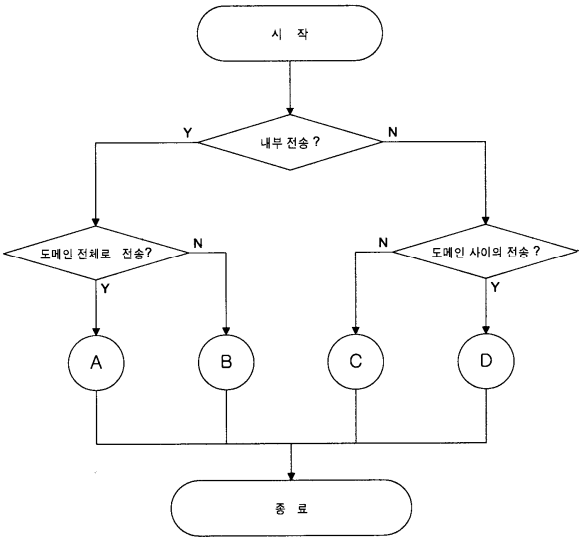
도면2



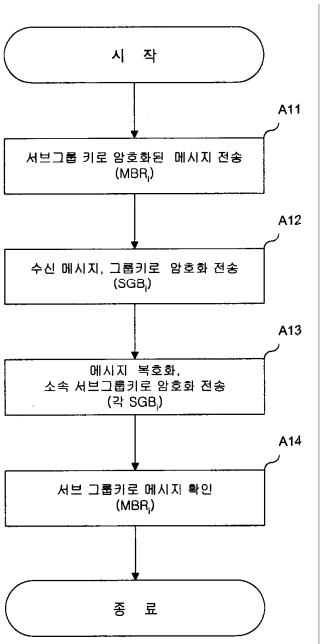
도면3


시 작
S21
공통 키 (K_{D_DAI})생성 후 DKA_i에게 전송 (DKM_i)
S22
사용자 인증 정보 전송
S23
무선 서비스 ?
Y
S24
무선 멀티 캐스트 서비스 요청
N
S25
메시지 복호화 및 인증 수행 (DKA_i)
S26
그룹 가입 멤버리스트 생성 및 전송 (DKA_i)
S27
그룹 가입 멤버리스트 복호 및 인증 (DKM_i)
S28
K_{DAi_MSi}, 서브그룹키 갱신정보, K_{GSI} 전송 (DKA_i)
S29
서브그룹 키 갱신정보 저장 (각 멤버)
종 료

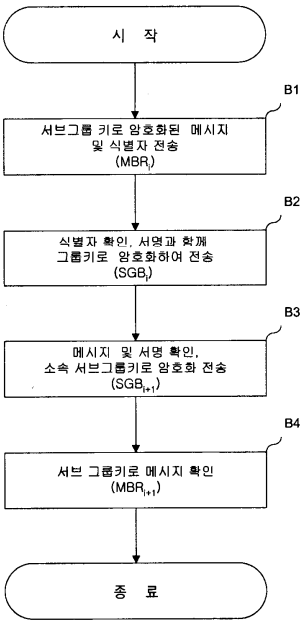
도면4a


시 작
내부 전송 ?
Y
N
도메인 전체로 전송?
N
Y
도메인 사이의 전송 ?
N
Y
A
B
C
D
종 료

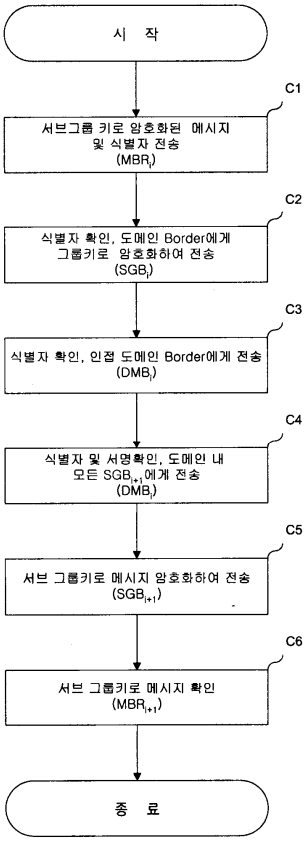
도면4b


시 작
A11
서브그룹 키로 암호화된 메시지 전송
(MBR_i)
A12
수신 메시지, 그룹키로 암호화 전송
(SGB_i)
A13
메시지 복호화,
소속 서브그룹키로 암호화 전송
(각 SGB_i)
A14
서브 그룹키로 메시지 확인
(MBR_i)
종 료

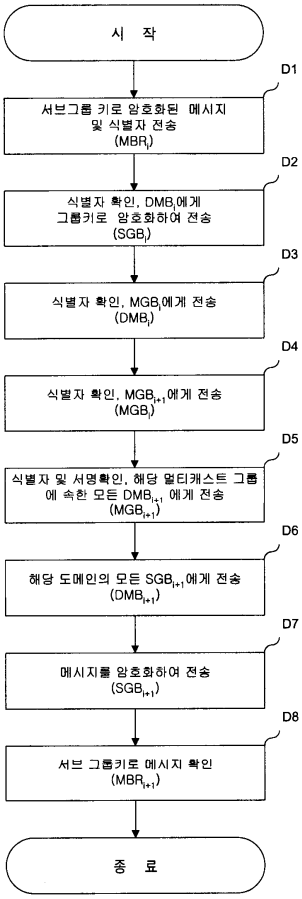
도면4c


시 작
B1
서브그룹 키로 암호화된 메시지
및 식별자 전송
(MBR_i)
B2
식별자 확인, 서명과 함께
그룹키로 암호화하여 전송
(SGB_i)
B3
메시지 및 서명 확인,
소속 서브그룹키로 암호화 전송
(SGB_{i+1})
B4
서브 그룹키로 메시지 확인
(MBR_{i+1})
종 료

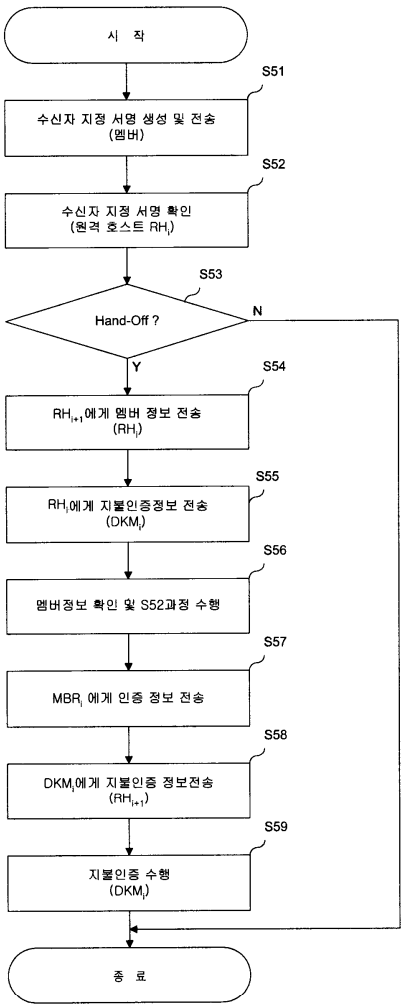
도면4d


시 작
C1
서브그룹 키로 암호화된 메시지 및 식별자 전송 (MBR_i)
C2
식별자 확인, 도메인 Border에게 그룹키로 암호화하여 전송 (SGB_i)
C3
식별자 확인, 인접 도메인 Border에게 전송 (DMB_i)
C4
식별자 및 서명확인, 도메인 내 모든 SGB_{i+1}에게 전송 (DMB_i)
C5
서브 그룹키로 메시지 암호화하여 전송 (SGB_{i+1})
C6
서브 그룹키로 메시지 확인 (MBR_{i+1})
종 료

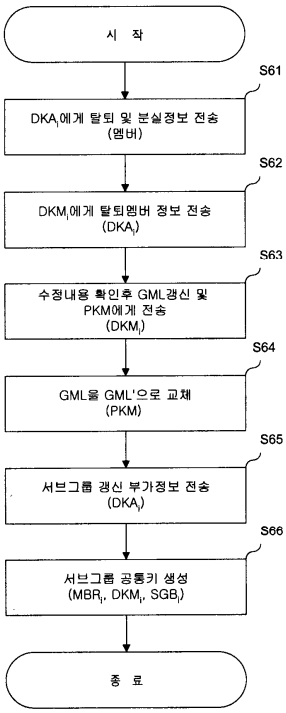
도면4e


시 작
D1
서브그룹 키로 암호화된 메시지 및 식별자 전송 (MBR_i)
D2
식별자 확인, DMB_i에게 그룹키로 암호화하여 전송 (SGB_i)
D3
식별자 확인, MGB_i에게 전송 (DMB_i)
D4
식별자 확인, MGB_{i+1}에게 전송 (MGB_i)
D5
식별자 및 서명확인, 해당 멀티캐스트 그룹에 속한 모든 DMB_{i+1} 에게 전송 (MGB_{i+1})
D6
해당 도메인의 모든 SGB_{i+1}에게 전송 (DMB_{i+1})
D7
메시지를 암호화하여 전송 (SGB_{i+1})
D8
서브 그룹키로 메시지 확인 (MBR_{i+1})
종 료

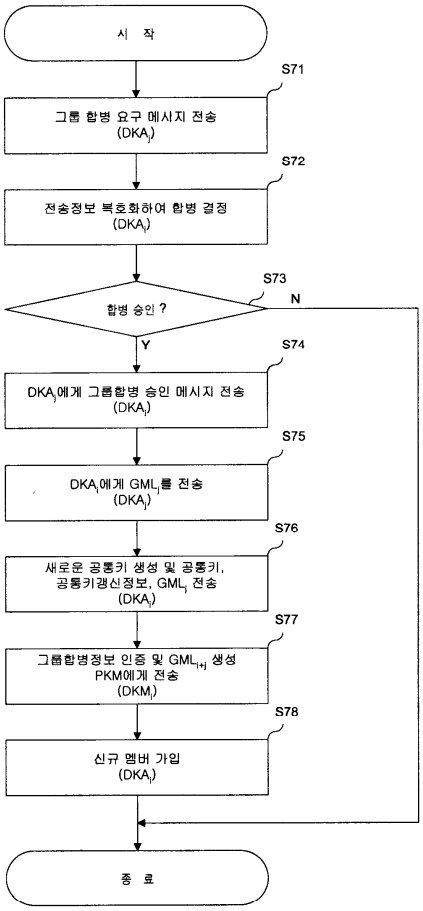
도면5


시 작
S51
수신자 지정 서명 생성 및 전송
(멤버)
S52
수신자 지정 서명 확인
(원격 호스트 RH_i)
S53
Hand-Off ?
N
Y
S54
RH_{i+1}에게 멤버 정보 전송
(RH_i)
S55
RH_i에게 지불인증정보 전송
(DKM_i)
S56
멤버정보 확인 및 S52과정 수행
S57
MBR_i 에게 인증 정보 전송
S58
DKM_i에게 지불인증 정보전송
(RH_{i+1})
S59
지불인증 수행
(DKM_i)
종 료

도면6


시 작
S61
DKA_i에게 탈퇴 및 분실정보 전송
(멤버)
S62
DKM_i에게 탈퇴멤버 정보 전송
(DKA_i)
S63
수정내용 확인후 GML갱신 및
PKM에게 전송
(DKM_i)
S64
GML을 GML'으로 교체
(PKM)
S65
서브그룹 갱신 부가정보 전송
(DKA_i)
S66
서브그룹 공통키 생성
(MBR_i, DKM_i, SGB_i)
종 료

도면7


시 작
S71
그룹 합병 요구 메시지 전송
(DKA$_j$)
S72
전송정보 복호화하여 합병 결정
(DKA$_i$)
S73
합병 승인 ?
N
Y
S74
DKA$_j$에게 그룹합병 승인 메시지 전송
(DKA$_i$)
S75
DKA$_i$에게 GML$_i$를 전송
(DKA$_i$)
S76
새로운 공통키 생성 및 공통키,
공통키갱신정보, GML$_i$ 전송
(DKA$_i$)
S77
그룹합병정보 인증 및 GML$_{i+j}$ 생성
PKM에게 전송
(DKM$_i$)
S78
신규 멤버 가입
(DKA$_j$)
종 료