(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 12/24 (2006.01)
H04L 12/28 (2006.01)
H04L 9/32 (2006.01)

(45) 공고일자 2006년12월20일
(11) 등록번호 10-0657315
(24) 등록일자 2006년12월07일

(21) 출원번호 10-2005-0044213(분할)
(22) 출원일자 2005년05월25일
심사청구일자 2005년05월25일
(62) 원출원 특허10-2004-0008343
원출원일자 : 2004년02월09일

(65) 공개번호 10-2005-0059027
(43) 공개일자 2005년06월17일

(30) 우선권주장 60/525,701 2003년12월01일 미국(US)

(73) 특허권자 삼성전자주식회사
경기도 수원시 영통구 매탄동 416

(72) 발명자 김명선
경기 의왕시 삼동 대우아파트 105-104

장용진
경기 의왕시 이동 218-74

남수현
서울 서초구 방배2동 435-26 102호

이재홍
경기 수원시 영통구 매탄3동 1250-8 206호

(74) 대리인 리앤목특허법인
이해영

심사관 : 신성길

전체 청구항 수 : 총 18 항

(54) 홈 네트워크 시스템 및 그 관리 방법

(57) 요약

UPnP 프로토콜을 기반으로, 사용자 인터페이스를 통해 사용자가 직접 도메인의 구성 기기들의 가입 및 탈퇴 등을 제어하고 도메인의 구성 기기들의 변동을 효과적으로 제어할 수 있는 홈 네트워크 시스템 및 관리 방법이 개시된다. 홈 네트워크 시스템은 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하여 상기 도메인을 구성하는 피제어 기기에게 소정의 도메인 키를 제공하고, 상기 도메인의 구성에 변동이 발생할 때마다 새로운 도메인 키를 생성하여 상기 도메인에 남아 있는 피제어 기기에게 제공하는 마스터 기기와, 상기 도메인의 구성을 사용자가 직접 변경할 수 있도록 사용자 인터페이스를 제공하는 컨트롤 포인트를 포함한다.

대표도

도 13

특허청구의 범위

청구항 1.

소정 프로토콜을 기반으로 DRM(Digital Rights Management)이 적용되는 도메인을 형성하는 방법에 있어서,

(a) 디바이스가 상기 도메인의 형성을 관리하는 컨트롤 포인트로 상기 도메인을 포함하는 네트워크에 연결되었음을 알리는 단계;

(b) 상기 알림을 수신한 컨트롤 포인트가 상기 디바이스로부터 상기 디바이스의 DRM 정보를 획득하는 단계; 및

(c) 상기 획득된 DRM 정보에 기초하여 상기 도메인을 형성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 2.

제 1 항에 있어서,

상기 소정 프로토콜은 UPnP(Universal Plug and Play)인 것을 특징으로 하는 방법.

청구항 3.

제 2 항에 있어서,

상기 (a) 단계는 상기 UPnP의 디스커버리 단계에서 SSDP(Simple Service Discovery Protocol)를 이용하여 상기 네트워크에 연결되었음을 알리는 것을 특징으로 하는 방법.

청구항 4.

제 2 항에 있어서,

상기 (b) 단계는 상기 UPnP의 디스크립션 단계에서 HTTP(Hypertext Transfer Protocol) GET를 통하여 상기 DRM 정보를 획득하는 것을 특징으로 하는 방법.

청구항 5.

제 1 항에 있어서,

상기 DRM 정보는 상기 DRM이 적용되는 도메인에서의 상기 디바이스의 역할을 나타내는 디바이스 모드를 포함하고,

상기 (c) 단계는 상기 디바이스 모드에 기초하여 상기 도메인을 형성하는 것을 특징으로 하는 방법.

청구항 6.

제 1 항 내지 제 5 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 7.

소정 프로토콜을 기반으로 DRM(Digital Rights Management)이 적용되는 도메인을 구성하는 디바이스를 인식하는 방법에 있어서,

(a) 상기 디바이스가 상기 도메인을 포함하는 네트워크에 연결되었음을 통보받는 단계; 및

(b) 상기 통보 여부에 따라 상기 디바이스로부터 상기 디바이스의 DRM 정보를 선택적으로 획득함으로써 상기 디바이스를 인식하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 8.

제 7 항에 있어서,

상기 소정 프로토콜은 UPnP(Universal Plug and Play)인 것을 특징으로 하는 방법.

청구항 9.

제 8 항에 있어서,

상기 (a) 단계는 상기 UPnP의 디스커버리 단계에서 SSDP(Simple Service Discovery Protocol)를 이용하여 상기 네트워크에 연결되었음을 통보받는 것을 특징으로 하는 방법.

청구항 10.

제 8 항에 있어서,

상기 (b) 단계는 상기 UPnP의 디스크립션 단계에서 HTTP(Hypertext Transfer Protocol) GET를 통하여 상기 DRM 정보를 획득하는 것을 특징으로 하는 방법.

청구항 11.

제 7 항에 있어서,

상기 DRM 정보는 상기 DRM이 적용되는 도메인에서의 상기 디바이스의 역할을 나타내는 디바이스 모드를 포함하고,

상기 (b) 단계는 상기 디바이스 모드에 기초하여 상기 디바이스의 역할을 인식하는 것을 특징으로 하는 방법.

청구항 12.

제 6 항 내지 제 11 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 13.

소정 프로토콜을 기반으로 DRM(Digital Rights Management)이 적용되는 도메인을 구성하는 디바이스의 DRM 정보를 제공하는 방법에 있어서,

(a) 상기 디바이스가 상기 도메인을 포함하는 네트워크에 연결되었음을 알리는 단계; 및

(b) 상기 알림을 수신한 컨트롤 포인트로 상기 디바이스의 DRM 정보를 제공하는 단계를 포함하고,

상기 컨트롤 포인트는 상기 도메인의 형성을 관리하는 것을 특징으로 하는 방법.

청구항 14.

제 13 항에 있어서,

상기 소정 프로토콜은 UPnP(Universal Plug and Play)인 것을 특징으로 하는 방법.

청구항 15.

제 14 항에 있어서,

상기 (a) 단계는 상기 UPnP의 디스커버리 단계에서 SSDP(Simple Service Discovery Protocol)를 이용하여 상기 네트워크에 연결되었음을 알리는 것을 특징으로 하는 방법.

청구항 16.

제 14 항에 있어서,

상기 (b) 단계는 상기 UPnP의 디스크립션 단계에서 HTTP(Hypertext Transfer Protocol) GET를 통하여 상기 DRM 정보를 제공하는 것을 특징으로 하는 방법.

청구항 17.

제 13 항에 있어서,

상기 DRM 정보는 상기 DRM이 적용되는 도메인에서의 상기 디바이스의 역할을 나타내는 디바이스 모드를 포함하고,

상기 디바이스 모드는 상기 도메인의 형성에 참조되는 것을 특징으로 하는 방법.

청구항 18.

제 13 항 내지 제 17 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 홈 네트워크의 도메인에 존재하는 기기들의 관리 방법에 관한 것으로서, 특히 사용자 인터페이스를 통해 사용자가 직접 도메인의 구성 기기들의 가입 및 탈퇴 등을 제어하고 도메인의 구성 기기들의 변동을 효과적으로 제어할 수 있는 홈 네트워크 시스템 및 관리 방법에 관한 것이다.

최근 홈 네트워크에 대한 관심이 높아지면서, 홈 네트워크상에서 컨텐츠를 보호하기 위한 기술들이 제안되고 있는데, 톰슨사에서 제안한 'SmartRight', 시스코사에서 제안한 'OCCAM(Open Conditional Content Access Management)', IBM사에서 제안한 'xCP Cluster Protocol'과 같은 것들이 대표적인 예라고 할 수 있다.

'SmartRight'는 홈 네트워크를 구성하는 각각의 기기(device)마다 공개키 인증서(public key certificate)를 포함하고 있는 스마트 카드(smart card)를 구비하여 이 스마트 카드를 이용하여 기기 상호간에 상기 인증서를 교환함으로써 홈 네트워크를 위한 키(key)를 생성하는 방식이다.

'OCCAM'은 홈 네트워크내의 기기들이 각각의 컨텐츠에 대한 고유의 티켓(ticket)을 이용하여 컨텐츠를 사용하는 방식이다.

'xCP Cluster Protocol'은 브로드 인크립션(broad encryption) 기반의 기술로서, 클러스터(cluster)라는 도메인 개념을 도입하여 이 클러스터에 속한 기기들 간에는 컨텐츠를 자유롭게 사용하도록 하는 방식이다.

도 1에는 마스터 기기(Master Device)(110)와 슬레이브 기기(Slave Device)(120, 130, 140)로 구성된 인증된 홈 도메인(100)이 예시되어 있으며, 마스터 기기(110)와 슬레이브 기기(120, 130, 140) 사이에 도메인 관리를 수행한다.

이와 같은 마스터-슬레이브 구조에 따라 'xCP Cluster Protocol'을 기반으로 하는 컨텐츠 재생 과정을 도 2를 참조하여 설명한다. 도 2에 따른 컨텐츠 재생 과정은 크게 클러스터 형성 과정(S200), 기기 인증 과정(S210), 컨텐츠 암호화 과정(S220) 및 컨텐츠 복호화 과정(S230)으로 나누며 세부적으로 살펴보면 다음과 같다. 임의의 홈 네트워크에 최초로 접속한 서버는 상기 네트워크에 대한 바인딩 ID(IDb)를 생성한다(S200). 이 때, 상기 바인딩 ID는 상기 서버가 제조될 당시에 설정된 고유의 식별자이거나, 사용자가 임의로 정한 고유의 식별자일 수 있다. 이렇게 바인딩 ID가 생성되면 바인딩 ID로 식별되는 클러스터(cluster)가 형성된다.

상기 서버에 존재하는 컨텐츠를 이용하고자 하는 기기는 자신의 디바이스 키 셋(device key set)을 이용하여 MKB(Media Key Block)로부터 미디어 키(Media Key, Km)를 추출한다(S212). 그리고 나서, 상기 기기는 상기 단계(S212)에서 추출한 미디어 키(Km)와 기기 자신의 식별자인 IDp를 이용하여 기기 자신의 고유 키인 Kp를 생성한다(S214). 상기 기기는 기기 인증을 받기 위해 상기 서버에 대하여 기기 인증을 요청한다(S216). 즉, 상기 기기는 상기 클러스터 내에 또는 상기 홈 네트워크 외부에 존재하는 기기 인증을 위한 서버에게 자신의 고유한 식별자인 IDp와 자신이 어떤 종류의 기기인지를 나타내는 유형 식별자인 'type'과 기기 자신의 식별자인 IDp와 'type'의 해시값 h=MAC(IDp||type)Kp를 상기 서버로 전송한다.

상기 서버는 Km과 IDp로부터 Kp'를 구하고, 상기 Kp'를 이용하여 얻어진 해시값 h'=MAC(IDp||type)Kp'를 상기 기기로부터 수신했던 상기 해시값 h와 비교하여 동일한지 여부를 확인한다. 만일 h값과 h'값이 동일한 경우에는 상기 기기에게 Kp를 이용하여 IDb를 암호화한 E(IDb)Kp와 상기 기기의 고유한 아이디 IDp를 전송하고, 서버 자신의 인증테이블 'auth.tab'에 상기 IDp를 추가한다. 이 때, 상기 기기는 상기 서버로부터 수신한 E(IDb)Kp로부터 IDb를 추출함으로써 기기 인증이 이루어지게 된다(S218).

한편, 기기 인증이 끝나고 나면, 상기 서버는 상기 기기에게 전송할 컨텐츠를 암호화한다(S220). 우선, IDb, auth.tab, Km을 이용하여 바인딩 키(Kb)를 생성하는데, 이 때 상기 바인딩 키(Kb)는 Kb=H[IDb H[auth.tab],Km]과 같은 식을 만족한다(S222).

바인딩 키(Kb)가 생성된 후에 상기 서버는 컨텐츠를 보호하기 위해 타이틀 키(Kt)로 상기 컨텐츠를 암호화한다(S224). 한편, 각각의 컨텐츠에는 복사 제어 정보(copy control information), 외부 전달 허용 여부, 사용 권한, 사용 허용 기간 등이 포함된 UR(Usage Rule) 정보가 포함되어 있는데, 상기 Kb를 이용하여 E(Kt??H[UR])Kb와 같이 UR 정보와 타이틀 키(Kt)를 암호화한다(S226).

한편, 상기 기기는 상기 서버로부터 상기 auth.tab을 수신하고 기추출한 Km과 IDb를 이용하여 Kb=H[IDb??H[auth.tab],Km]로부터 바인딩 키(Kb)를 얻으며(S232), E(Kt??H[UR])Kb로부터 타이틀 키(Kt)를 추출한 후(S234), 상기 추출된 타이틀 키(Kt)를 이용하여 상기 서버로부터 수신한 컨텐츠를 복호한다(S236).

이와 같이 동작하는 xCP Cluster Protocol은 도메인에 포함될 기기의 선택과정이 없이 통신 범위 안의 모든 기기가 자동으로 가입할 수 있고, 또한 각각의 기기들이 새롭게 바인딩 키(Kb)를 만들 때마다 auth.tab을 서버로부터 수신하여 계산해야 하는 불편함이 있다. 따라서, 사용자의 제어에 따라 홈 도메인의 구성 기기를 결정할 수 있으며 외부와 독립된 홈 도메인을 구축하여 보다 안전하게 컨텐츠를 보호할 필요가 있다.

한편, 최근에는 UPnP(Universal Plug and Play)를 기반으로 한 홈 네트워크 관리 방법이 광범위하게 제안되고 있다. UPnP는 원래 컴퓨터 주변 장치를 범용 컴퓨터에 연결만 하면 자동으로 인식될 수 있도록 하는 표준화된 기능을 의미하며, 나아가 컴퓨터 주변 장치 뿐만 아니라 가전 제품 및 무선 장비 등을 네트워크에 접속시켰을 때 이를 자동으로 인식할 수 있는 홈 네트워크 미들웨어 표준으로 발전하고 있다. 또한, UPnP는 기존의 표준 인터넷 프로토콜을 사용하기 때문에 기존의 네트워크에 매끄럽게 통합이 가능하고, 특정 운영체제나 물리적 매체에 의존하지 않는 등 많은 장점이 있다. 그러나, 아직까지 UPnP를 이용하여 도메인 관리를 구현하는 방법은 알려져 있지 않으므로, UPnP를 이용하여 효과적으로 도메인 관리를 구현하는 방법을 강구할 필요가 있다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은, 사용자가 직접 도메인 형성을 제어하고 외부와 독립된 도메인을 보다 안전하게 구축할 수 있는 홈 네트워크 관리 방법을 제공하는 것이다.

또한, 본 발명의 목적은, 기존의 표준 인터넷 프로토콜을 사용하는 네트워크에 매끄럽게 통합이 가능한 UPnP 기반의 홈 네트워크 시스템을 제공하는 것이다.

또한, 본 발명의 목적은, 홈 네트워크의 도메인의 구성 기기들의 변동을 사용자가 직접 제어하고 구성 기기의 변동에 따른 새로운 도메인 키의 생성을 마스터 기기가 담당하고 슬레이브 기기들은 마스터 기기에서 생성된 도메인 키를 전달받도록 함으로써 도메인 구성 변경에 따른 도메인 키 변경의 절차를 간소화하는 것이다.

또한, 본 발명의 목적은, 도메인 ID와 도메인 키 이외에도 도메인이 공유하는 정보로서 세션 ID를 도입함으로써 빈번한 도메인 키의 변경을 방지하는 것이다.

발명의 구성

상기와 같은 목적을 달성하기 위하여 본 발명은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하여 상기 도메인을 구성하는 피제어 기기에게 소정의 도메인 키를 제공하고, 상기 도메인의 구성에 변동이 발생할 때마다 새로운 도메인 키를 생성하여 상기 도메인에 남아 있는 피제어 기기에게 제공하는 마스터 기기와, 상기 도메인의 구성을 사용자가 직접 변경할 수 있도록 사용자 인터페이스를 제공하는 컨트롤 포인트를 포함하는 홈 네트워크 시스템을 제공한다.

이 때, 상기 마스터 기기는 상기 도메인을 형성하는 피제어 기기에게 소정의 컨텐츠를 제공하고, 상기 도메인 키는 상기 소정의 컨텐츠를 암호화하는 데 이용되는 컨텐츠 키를 암호화하는 데 이용될 수 있으며, 또한, 상기 도메인 키는 상기 소정의 컨텐츠를 제공받는 피제어 기기의 공개키를 이용하여 암호화되고 상기 암호화된 도메인 키는 상기 공개키와 쌍을 이루는 소정의 비밀키로 해독될 수 있다.

또한, 상기 홈 네트워크 시스템은 UPnP를 기반으로 구성될 수 있고, 상기 도메인 키는 상기 도메인을 형성하는 기기들의 기기 정보를 이용하여 생성될 수 있으며, 상기 컨트롤 포인트는 상기 마스터 기기 및 상기 도메인을 형성하는 피제어 기기의 동작에 필요한 정보를 상기 마스터 기기 및 상기 도메인을 형성하는 피제어 기기에게 전달할 수 있다.

또한, 상기 도메인은 상기 도메인을 형성하는 구성 기기들의 변동에 따라 변동되는 세션 ID를 공유하며, 상기 마스터 기기는 상기 도메인에 커넥트되는 기기의 세션 ID가 자신의 세션 ID와 동일하지 않을 경우에 상기 커넥트된 기기에게 자신이 보유하고 있는 도메인 키를 전달하는 것이 바람직하다.

이 때, 상기 피제어 기기는 슬레이브 상태와 게스트 상태를 기기 모드로서 가질 수 있으며, 상기 마스터 기기는, 상기 도메인에 커넥트되는 기기의 세션 ID가 자신의 세션 ID와 동일하지 않고 또한 상기 커넥트된 기기가 자신이 보유하고 있는 슬레이브 기기 리스트에 존재하는 경우에, 상기 커넥트된 기기에게 자신이 보유하고 있는 도메인 키를 전달하는 것이 바람직하다.

더 나아가, 상기 슬레이브 기기 리스트에 상기 커넥트된 기기가 존재하지 않는 경우에, 상기 커넥트된 기기의 기기 모드는 게스트 상태로 변경될 수 있다. 또한, 상기 마스터 기기는 상기 도메인에 커넥트되는 기기의 도메인 ID가 자신이 보유하고 있는 도메인 ID와 일치하지 않는 경우에는 상기 도메인 키를 상기 커넥트된 기기에게 전달하지 않는 것이 바람직하다. 또한, 상기 마스터 기기는 상기 도메인에 커넥트되는 기기의 기기 모드가 슬레이브 상태가 아닌 경우에는 상기 도메인 키를 상기 커넥트된 기기에게 전달하지 않는 것이 바람직하다.

또한, 상기 세션 ID는 고유 ID 이외에도 날짜 정보 및/또는 버전 정보를 더 포함하는 것이 바람직하다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하여 상기 도메인을 구성하는 피제어 기기에게 소정의 도메인 키를 제공하는 마스터 기기, 및 사용자 인터페이스를 제공하는 컨트롤 포인트를 포함하는 홈 네트워크 시스템의 관리 방법에 있어서, (a) 상기 사용자 인터페이스를 통한 사용자의 지시에 따라 상기 도메인의 구성을 변경하는 단계와, (b) 상기 마스터 기기에서, 상기 도메인의 구성 변경에 따라 새로운 도메인 키를 생성하는 단계와, (c) 상기 생성된 도메인 키를 상기 도메인에 남아 있는 피제어 기기에게 제공하는 단계를 포함하는 홈 네트워크 관리 방법을 제공한다.

이 때, 상기 홈 네트워크 시스템은 UPnP를 기반으로 구성될 수 있고, 상기 도메인 키는 상기 도메인을 형성하는 기기들의 기기 정보를 이용하여 생성될 수 있다.

또한, 상기 홈 네트워크 관리 방법은 (d) 상기 도메인의 구성 기기들의 변동에 따라 변동되는 세션 ID를 상기 도메인의 구성 기기들이 공유하는 단계와, (e) 상기 도메인에 커넥트되는 기기의 세션 ID가 상기 도메인의 세션 ID와 동일하지 않을 경우에 상기 커넥트된 기기에게 상기 도메인의 도메인 키를 제공하는 단계를 더 포함하는 것이 바람직하다.

이 때, 상기 피제어 기기는 슬레이브 상태와 게스트 상태를 기기 모드로서 가질 수 있으며, 상기 (e) 단계는, 상기 도메인에 커넥트되는 기기의 세션 ID가 상기 도메인의 세션 ID와 동일하지 않고, 또한 상기 커넥트된 기기가 상기 마스터 기기가 보유하고 있는 슬레이브 기기 리스트에 존재하는 경우에 상기 커넥트된 기기에게 상기 도메인 키를 제공하는 것이 바람직하다.

더 나아가, 상기 (e) 단계는, 상기 도메인에 커넥트되는 기기가 상기 슬레이브 기기 리스트에 존재하지 않는 경우에 상기 커넥트된 기기의 기기 모드를 게스트 상태로 설정하는 것이 바람직하고, 상기 (e) 단계는, 상기 도메인에 커넥트되는 기기의 도메인 ID가 상기 도메인의 도메인 ID와 일치하지 않는 경우에 상기 도메인 키를 상기 커넥트된 기기에게 제공하지 않는 단계를 포함하는 것이 바람직하며, 상기 (e) 단계는, 상기 도메인에 커넥트되는 기기의 기기 모드가 슬레이브 상태가 아닌 경우에는 상기 도메인 키를 상기 커넥트된 기기에게 제공하지 않는 단계를 포함하는 것이 바람직하다.

또한, 상기 세션 ID는 고유 ID 이외에도 날짜 정보 및/또는 버전 정보를 더 포함하는 것이 바람직하다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하는 마스터 기기를 포함하는 홈 네트워크 시스템의 홈 네트워크 관리 제어 장치에 있어서, 상기 도메인의 구성을 사용자가 직접 변동할 수 있도록 사용자 인터페이스를 제공하는 사용자 인터페이스 제공부와, 상기 사용자 인터페이스를 통한 사용자 입력에 따라 상기 도메인의 구성 기기들의 동작에 필요한 정보를 상기 도메인의 구성 기기들에게 제공하는 기기 동작 정보 제공부를 포함하는 홈 네트워크 관리 제어 장치를 제공한다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하는 마스터 기기를 포함하는 홈 네트워크 시스템의 홈 네트워크 관리 제어 장치에 있어서, 상기 도메인의 구성을 사용자가 직접 변동할 수 있도록 사용자 인터페이스를 제공하는 사용자 인터페이스 제공부와, 상기 홈 네트워크 관리 제어 장치에 접속하는 기기를 검출하는 기기 검출부와, 상기 접속된 기기의 정보를 상기 마스터 기기에게 제공하고 상기 마스터 기기에서의 처리 결과를 상기 접속된 기기에게 제공하는 기기 동작 정보 제공부를 포함하는 홈 네트워크 관리 제어 장치를 제공한다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하는 마스터 기기에 있어서, 상기 피제어 기기의 인증을 수행하는 피제어 기기 관리부와, 상기 도메인을 식별하는 도메인 ID를 생성하여 상기 도메인의 구성 기기에게 제공하는 도메인 ID 관리부와, 상기 도메인의 구성 변동에 따라 변동하는 세션 ID를 생성하여 상기 도메인의 구성 기기에게 제공하는 세션 ID 관리부와, 상기 도메인의 구성 변동에 따라 변동하는 도메인 키를 생성하여 상기 도메인의 구성 기기에게 제공하는 도메인 키 관리부를 포함하는 마스터 기기를 제공한다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 하나 이상의 피제어 기기들 중 적어도 일부와 함께 도메인을 형성하는 마스터 기기에 의해 상기 피제어 기기를 관리하는 방법에 있어서, (a) 상기 피제어 기기의 인증을 수행하는 단계와, (b) 상기 도메인을 식별하는 도메인 ID를 생성하여 상기 도메인의 구성 기기에게 제공하는 단계와, (c) 상기 도메인의 구성 변동에 따라 변동하는 세션 ID를 생성하여 상기 도메인의 구성 기기에게 제공하는 단계와, (d) 상기 도메인의 구성 변동에 따라 변동하는 도메인 키를 생성하여 상기 도메인의 구성 기기에게 제공하는 단계를 포함하는 피제어 기기 관리 방법 및 이 방법을 실행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 슬레이브 상태와 게스트 상태를 기기 모드로서 가질 수 있는 하나 이상의 피제어 기기들 중 기기 모드가 슬레이브 상태인 슬레이브 기기와 함께 도메인을 형성하는 마스터 기기에 있어서, 상기 도메인에 접속하는 기기의 인증 및 기기 모드 판별을 수행하며, 슬레이브 기기 리스트를 생성 및 변경하고 상기 접속 기기가 상기 슬레이브 기기 리스트에 존재하는지 여부를 판별하는 피제어 기기 관리부와, 상기 도메인을 식별할 수 있는 도메인 ID를 생성하고, 상기 마스터 기기와 상기 접속 기기의 도메인 ID를 비교하는 도메인 ID 관리부와, 상기 도메인의 구성 변동에 따라 변동하는 상기 마스터 기기의 세션 ID를 상기 접속 기기의 세션 ID와 비교하는 세션 ID 관리부와, 상기 도메인의 구성 변동에 따라 변동하는 도메인 키를 생성하고, 상기 도메인 ID 관리부의 비교 결과 일치하고 상기 세션 ID 관리부의 비교 결과 일치하지 않으며 상기 피제어 기기 관리부의 판별 결과 상기 접속 기기가 상기 슬레이브 기기 리스트에 존재하면 상기 마스터 기기의 도메인 키를 상기 접속 기기에게 제공하는 도메인 키 관리부를 포함하는 마스터 기기를 제공한다.

상기와 같은 목적을 달성하기 위해 본 발명의 다른 국면은, 슬레이브 상태와 게스트 상태를 기기 모드로서 가질 수 있는 하나 이상의 피제어 기기들 중 기기 모드가 슬레이브 상태인 슬레이브 기기와 함께 도메인을 형성하는 마스터 기기에 의한 피제어 기기 관리 방법에 있어서, (a) 상기 도메인에 접속하는 기기를 인증하는 단계와, (b) 상기 인증이 성공하면, 상기 접속 기기의 기기 모드를 판별하는 단계와, (c) 상기 단계 (b)의 판별 결과, 상기 접속 기기의 기기 모드가 슬레이브 상태인 경우에는, 상기 도메인의 구성 변동에 따라 변동하는 상기 마스터 기기의 세션 ID를 상기 접속 기기의 세션 ID와 비교하는 단계와, (d) 상기 단계 (c)의 비교 결과, 일치하지 않으면 슬레이브 상태인 피제어 기기들을 나타내는 슬레이브 기기 리스트에 상기 접속 기기가 존재하는지를 판별하는 단계와, (e) 상기 단계 (d)의 판별 결과, 존재하면 상기 도메인의 구성 변동에 따라 변동하는 상기 마스터 기기의 도메인 키를 상기 접속 기기에게 제공하는 단계를 포함하는 피제어 기기 관리 방법 및 이 방법을 실행하는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 제공한다.

이 때, 적어도 상기 (c) 단계 이전에 상기 도메인을 식별할 수 있으며 상기 도메인의 구성 기기에 의해 공유되는 도메인 ID와 상기 접속 기기의 도메인 ID를 비교하는 단계를 더 포함하되, 상기 단계 도메인 ID가 일치하지 않으면 후속 단계들을 진행하지 않는 것이 바람직하다.

이하에서는, 첨부된 도면을 참조하여 본 발명의 실시예를 설명한다.

도 3은 공개키 기반 구조(Public Key Infrastructure)의 도메인 형성 방법을 나타내는 흐름도이다. 이하의 설명을 위해, 컨텐츠를 제공하는 서버에 대해 컨텐츠를 요청하는 각종 기기는 기기 제조시에 각각의 기기마다 고유한 비밀키 집합과 공개키 또는 공개키 생성 기능을 갖고 있는 것으로 가정한다. 이 때, 상기 비밀키 집합은 브로드캐스팅 암호 방식을 통해 제공되는 비밀 정보 블록(Secret Information Block; SIB)으로부터 비밀값을 추출하는 데 사용된다. 상기 SIB는 기기들의 폐기(revocation) 여부를 검증하기 위한 정보로서, 폐기 처분된 기기들은 SIB로부터 의도된 비밀값을 추출할 수 없고, 정당한 기기들은 공통된 비밀값을 추출할 수 있다.

단일의 도메인 내에는 도메인 형성에 관여하는 서버(320)가 존재하는데, 상기 서버(320)는 외부 서버(310)로부터 브로드캐스트 암호(Broadcast Encryption) 방식에 의해 SIB를 전달받는다(S332). 그리고 나서, 도메인 내에 있는 기기들(330)이 유선 또는 무선 네트워크를 통하여 자신의 존재를 서버(320)에 알리거나 서버(320)가 기기들(330)을 찾음으로써 서버(320)가 기기들(330)의 존재를 인식하게 된다(S334).

서버(320)는 자신이 인식한 기기들(330)을 디스플레이 장치를 통하여 사용자에게 제공하고, 사용자는 상기 디스플레이 장치를 통해 나타난 기기들 중 도메인에 등록하고자 하는 기기들(330)을 선택한다(S336). 그리고 나서, 서버(320)는 사용자에 의해 선택된 기기들(330)에 대하여 외부 서버(310)로부터 기수신한 SIB를 전달하고(S338), 상기 SIB를 수신한 기기들(330)은 상기 SIB로부터 비밀값을 추출하고(S340), 상기 추출된 비밀값을 이용하여 자신의 공개키에 대한 인증서를 작성한다(S342).

상기 기기들(330)이 상기 인증서와 기기의 고유 식별자(ID), 기기 자신이 갖고 있는 공개키를 서버(320)로 전달하면(S344), 서버(320)는 인증서를 검증함으로써 기기들의 정당성을 검증하고(S346), 인증된 기기들의 고유 식별자(ID)와 공개키를 기록한 인증 목록을 작성한다(S348). 이 때, 인증 가능한 기기들의 개수는 사용자에 의해 임의로 제한할 수도 있다.

서버(320)가 인증 목록을 작성한 후, 상기 인증 목록에 있는 기기들에 대한 정보와 서버 자신이 생성한 난수(random number)를 이용하여 고유한 도메인 아이디와 도메인 키를 생성한다(S350). 이 때, 상기 도메인 키는 사용자의 선택에 의해 형성된 도메인에 속하는 기기들만이 공유하는 비밀키로서, 상기 도메인을 구성하는 구성원들이 변경될 때마다 같이 변경되고, 상기 도메인 아이디는 다른 도메인과 구별하기 위한 식별자로서 사용된다.

서버(320)는 도메인 내에 있는 인증된 기기들(330)에게 각각의 기기들의 공개키를 이용하여 상기 도메인 아이디와 상기 도메인 키를 암호화하여 전달하고(S352), 상기 기기들(330)은 자신의 비밀키를 이용하여 상기 도메인 키를 복구함으로써(S354), 컨텐츠를 이용하기 위한 도메인이 형성된다. 컨텐츠 공유를 위한 도메인이 형성되면 서버(320)는 컨텐츠를 컨텐츠 키에 의해 암호화하고 상기 컨텐츠 키는 상기 도메인 키에 의해 암호화된다. 암호화된 컨텐츠는 컨텐츠를 이용하고자 하는 기기들이 도메인 키를 이용하여 복호함으로써 컨텐츠를 이용할 수 있게 된다.

도 4는 본 발명에 따른 도메인 형성 방법을 UPnP에 적용한 예를 나타낸 블록도이다. 도 1과 동일한 구성요소에 대해서는 동일한 참조 부호를 사용한다. 각각의 피제어 기기(Controlled Device: 이하 'CD'로 지칭되기도 한다)(110 내지 160)들은 컨트롤 포인트(Control Point: 이하 'CP'로 지칭되기도 한다)(190)에 의하여 명령을 주고 받고, 각 기기가 가지는 서비스를 제공한다. 피제어 기기들(110 내지 160) 중에서 하나의 기기를 마스터 키기(110)로 설정하고 그 이외의 기기 중에서 사용자가 선택한 기기들을 슬레이브 기기(120, 130, 140)로 설정하여 도메인을 형성할 수 있다.

피 제어 기기 중에서 마스터나 슬레이브로 설정되지 않는, 즉 도메인에 포함되지 않는 기기들(150, 160)은 게스트(guest)라고 명명한다. 마스터 기기(110)와 슬레이브 기기들(120 내지 140)은 인증된 홈 도메인을 형성하고, CP(190)와 피제어 기기들(110 내지 160) 전체는 홈 네트워크(200)를 형성한다.

도 5는 CP(190)와 CD(120 내지 160)간에 수행되는 일반적인 UPnP 동작을 나타낸 도면이다. 먼저, 주소 지정(Addressing) 단계가 수행된다. UPnP 네트워킹의 기반은 TCP/IP 프로토콜이며 이 프로토콜의 핵심은 주소 지정 기능이다. 각 기기는 동적 호스트 구성 프로토콜(Dynamic Host Configuration Protocol; DHCP) 클라이언트를 가지고 있어야 하며, 기기가 맨 처음 네트워크에 연결되면 DHCP 서버를 검색한다. 만약 DHCP 서버가 있으면 해당 기기는 할당된 IP 주소를 사용하게 된다. 만약 사용 가능한 DHCP 서버가 없는 경우에는 기기는 주소를 확보하기 위해 '자동 IP(Auto IP)'를 사용하게 된다.

다음으로, 디스커버리(Discovery) 단계이다. 일단, 기기가 네트워크에 연결되고 적절한 주소가 지정되면 검색 작업이 진행될 수 있다. 검색 작업은 SSDP(Simple Service Discovery Protocol)을 이용하여 처리한다. 기기가 네트워크에 추가되면 SSDP는 이 기기가 제공하는 서비스를 네트워크 상에 있는 컨트롤 포인트에 알리는 역할을 한다.

UPnP 네트워킹의 다음 단계는 디스크립션(Description) 단계이다. 컨트롤 포인트가 기기를 검색하기는 하였지만, 컨트롤 포인트는 여전히 기기에 대하여 알고 있는 정보가 아주 적다. 이 컨트롤 포인트가 기기 및 기기의 기능에 대한 정보를 자세하게 파악하여 상호작용을 하려면, 컨트롤 포인트는 검색 메시지와 해당되는 기기가 제공하는 URL로부터 기기 설명 내용을 확인해야 한다. 기기에 대한 UPnP 설명은 XML로 표현되어 있으며, 공급 업체 고유의 제조 정보(모델명, 일련번호, 제조업체 이름, 제조업체 URL 등)를 포함하고 있다. 이 설명은 또한 제어, 이벤트 및 프리젠테이션을 위한 URL 뿐만 아니라 많은 내장된 기기 및 서비스에 관한 목록도 포함하고 있다.

상기 주소 지정, 검색, 디스크립션 단계 이후에는 본격적인 UPnP 동작 단계가 수행된다. 이러한 단계는, 제어(Control), 이벤트 작업(Eventing) 및 프리젠테이션(Presentation) 등의 동작을 통하여 이루어진다. 상기 제어(Control) 동작을 보면, 컨트롤 포인트는 기기의 디스크립션을 확보한 후에 기기 제어를 위한 필수적 작업을 수행한다. 기기를 제어하기 위하여 컨트롤 포인트는 기기의 서비스에 동작 명령을 보낸다. 그러기 위해서 컨트롤 포인트는 적절한 제어 메시지를 해당 서비스에 대한 제어 URL(기기 설명서에 있음)로 보낸다. 제어 매시지도 SOAP(Simple Object Access Protocol)를 사용하여 XML로 표현된다. 해당 서비스는 이 제어 메시지에 대한 응답으로서 특정 동작 값이나 장애 코드를 제공한다.

또한, 상기 이벤트 작업(Eventing)의 동작을 보면, 각 기기들은 상기한 명령을 받아, 자신의 상태의 변화가 발생하면 이를 이벤트 메시지를 통하여 컨트롤 포인트에 알린다. 이러한 메시지는 한 개 이상의 상태 변수 이름 및 이들 변수들의 현재 값을 포함하고 있으며, XML 형식으로 표현되고 GENA(Generic Event Notification Architecture)를 통하여 포맷된다. 이벤트 내용은 주기적으로 갱신되어 지속적으로 컨트롤 포인트에 통보되며, GENA를 사용하여 가입을 취소할 수도 있다.

그리고, 상기 프리젠테이션(Presentation) 동작을 보면, 만약 기기가 프리젠테이션용 URL을 가지고 있다면, 컨트롤 포인트는 이 URL을 통하여 페이지를 검색할 수 있고 이 페이지를 브라우저에 로드할 수 있으며, 사용자들은 상기 페이지를 이용하여 기기를 제어하거나 기기 상태를 조회할 수 있다. 이 기능들을 수행할 수 있는 수준은 프리젠테이션 페이지 및 기기의 특정 기능에 달려있다.

도 6은 UPnP 기반의 홈 네트워크 형성 과정 중에서 마스터 기기를 정하는 과정을 보여주고 있다. 먼저, 전체 피제어 기기들(110 내지 160)이 컨트롤 포인트(190)에 SSDP를 이용하여 자신이 홈 네트워크에 연결되었음을 알린다(S601). 그러면, 컨트롤 포인트(190)는 상기 기기들(110 내지 160)로부터 디바이스 정보 및 DRM 정보를 HTTP를 통하여 얻는다(S602). 상기 디바이스 정보는 UPnP에서 사용하는 일번적인 기기 정보를 의미하고, 상기 DRM 정보는 디바이스 속성(Device Attribute)과 디바이스 모드(Device Mode)를 의미한다. 여기서, 디바이스 속성은 피제어 기기가 enmasterable인지 dismasterable인지를 결정하는 값으로서, 피제어 기기가 도메인 마스터로 작동할 수 있는지 여부를 알려주는 정보이다. 그리고, 디바이스 모드는 마스터(master), 슬레이브(slave), 게스트(guest) 중 현재 어떤 것으로 동작하는지를 결정하는 값이다. 초기에 피제어 기기는 모두 게스트(guest)로 설정되어 있다가, 이후 마스터나 슬레이브로 설정되면 상기 디바이스 모드 값이 변경된다.

상기 DRM 정보 중 디바이스 모드에서 마스터로 동작하는 피제어 기기가 있는지를 판단하여 마스터로 동작하는 기기가 없는 경우에는 enmasterable인 피제어 기기 중 하나를 마스터로 선택한다(S603). 이와 같은 마스터를 설정하는 것은 컨트롤 포인트(190)의 사용자 인터페이스(User Interface)를 통하여 사용자가 직접 선택하는 과정을 통해 이루어진다. 상기 사용자 인터페이스의 예를 도 9a에 나타내었다. 상기 사용자 인터페이스에서는 마스터로 동작할 수 있는 기기 'main nexus'와 'sub nexus'를 나타내고 있고 이들은 현재 게스트로 설정되어 있다. 이 기기 중 사용자가 마스터로 서정하고자 하는 기기를 체크하면 된다. 본 예에서는 피제어 기기1(110)이 마스터로 결정되었다.

다음으로, 컨트롤 포인트(190)는 SOAP를 통하여 상기 마스터로 설정된 피제어 기기1(110)로부터 관리자 인증 정보를 얻는다(S604). 이러한 관리자 인증 정보는 예컨대 마스터 기기의 스마트 카드로부터 불러올 수 있으며, 상기 마스터로 결정한 사용자가 관리자인지를 확인하는 절차에서 필요하다. 컨트롤 포인트(190)에서는 상기 관리자 인증 정보를 이용하여 사용자 인터페이스를 출력하고 사용자로부터 관리자 ID 및 패스워드를 입력받는 방식으로 관리자 인증을 한다(S605). 도 9b에는 이러한 사용자 인터페이스의 예가 도시되어 있다.

관리자 인증을 거친 후 컨트롤 포인트(190)는 피제어 기기1(110)을 도메인 마스터로 설정하고 컨트롤 포인트 자신이 갖고 있던 디바이스 리스트를 피제어 기기1(110)로 제공한다(S606). 이후로는 피제어 기기1(110)의 디바이스 모드 값은 '마스터'가 된다. 마스터로 설정된 기기(110)는 초기에는 자신만을 구성원으로 하는 새로운 도메인을 생성한다(S607).

도 7은 도 6의 마스터 기기를 정하는 과정에 이은 기기 인증(device authentication) 과정을 보여주고 있다. 먼저, 도메인 마스터(110)에서 상기 도 3의 설명 과정에서와 같은 방법으로 외부의 서버를 통하여 새로운 SIB를 전달받는다(S711). 그러면, 컨트롤 포인트(190)는 나머지 피제어 기기(120 내지 160)에게 SOAP를 이용하여 상기 SIB가 저장된 URL 정보를 전달해 준다(S712). 상기 나머지 피제어 기기(120 내지 160)는 상기 URL에 존재하는 SIB를 HTTP를 통하여 얻는다(S713). 그리고, 상기 얻은 SIB를 이용하여 비밀값을 추출하고, 상기 비밀값과 자신이 갖고 있는 디바이스 ID 및 공개키를 이용하여 인증서(certificate)를 생성한다(S714). 이러한 인증서는 불법 기기들을 구별하기 위한 것으로 예컨대, 특정 제조자가 생산하는 기기만을 합법적인 기기로 인정하는 인증 정책을 유지한다면 그 제조자 이외의 제조자가 생산한 기기는 불법 기기로 간주될 것이다.

그 후, 컨트롤 포인트(190)가 마스터 기기(110)에게 상기 인증서가 저장된 URL 정보를 SOAP를 통하여 전달하면(S715), 상기 마스터 기기(110)는 상기 나머지 피제어 기기(120 내지 160)로부터 HTTP를 이용하여 인증서, 디바이스 ID 및 공개키를 얻는다(S716). 그리고, 상기 얻은 인증서를 검증하고 인증 기기에 대한 목록을 작성한다(S717). 이와 같이 인증서를 검증하여 불법적인 기기로 간주된 기기는 이후 도메인에서 제외되며, 슬레이브 기기로 지정될 가능성이 없다.

도 8은 도 7의 기기 인증 과정에 이은 슬레이브 기기를 정하는 과정을 보여주고 있다. 먼저, 컨트롤 포인트(190)는 상기 인증서 검증 결과 합법적인 기기로 인증된 기기(120 내지 140)들을 대상으로 SOAP를 이용하여 도메인 속성(domain attribute)을 검증한다(S821). 상기 도메인 속성에는 도메인 키, 도메인에 속하는 기기의 명칭, 도메인에 속하는 기기의 수 등이 해당될 것이다. 만약, 상기 기기들에 도메인 속성이 존재하지 않는 경우에는 컨트롤 포인트(190)는 상기 기기들의 리스트를 사용자 인터페이스를 통해 디스플레이하고(S822), 사용자로 하여금 슬레이브 기기를 선택하도록 한다(S823). 도 9c에는 합법적인 기기들(120 내지 140)의 리스트를 나타낸 사용자 인터페이스의 예를 나타내었다. 사용자는 이들 리스트 중에서 도메인에 포함시키고자 하는 기기들을 체크함으로써 슬레이브 기기를 선택할 수 있다. 이와 같은 슬레이브 기기는 마스터 기기와는 달리 복수의 기기가 선택될 수도 있다. 이 후, 도 6에서의 마스터 선택 과정과 마찬가지로 관리자 인증 정보를 얻어서(S824), 관리자 인증을 하는 과정(S825)을 거친다.

다음으로, 컨트롤 포인트(190)는 상기 리스트 중에서 선택된 슬레이브 기기의 리스트를 SOAP를 통해 마스터 기기(110)로 전달하는 한편(S826), SOAP를 통해 상기 선택된 기기들을 슬레이브 모드로 설정한다(S827). 슬레이브 모드로 설정된 기기들은 이후로는 디바이스 모드 값을 '슬레이브'로 갖는다. 그 다음, 마스터 기기(110)는 상기 슬레이브 리스트를 이용하여 도메인 ID 및 도메인 키를 생성한다(S828). 그리고, 슬레이브 기기에 대한 공개키를 이용하여 도메인 ID와 도메인 키를 암호화한다(S829). 또한, 마스터 기기(110)는 슬레이브로 선택된 기기들에 대한 슬레이브 기기 리스트를 저장한다.

다음으로, 컨트롤 포인트(190)는 도메인 속성 값을 저장하고 있는 마스터 기기의 URL 정보를 SOAP를 통해 상기 슬레이브로 설정된 기기들에게 전달한다(S830). 그러면, 상기 슬레이브로 설정된 기기들이 상기 URL에 존재하는 도메인 속성을 HTTP를 통하여 얻어온다(S831). 전술한 바와 같이, 상기 도메인 속성은 도메인 키, 도메인에 속하는 기기의 명칭, 도메인에 속하는 기기의 수 등의 정보를 포함한다.

도 10 내지 도 12는 도 6 내지 도 8과는 달리 컨트롤 포인트(190)의 기능 중에서 중요한 부분을 떼어서 마스터 기기(110)로 이관한 경우의 동작 과정을 보여주는 흐름도이다. 이 때, 컨트롤 포인트(190)는 사용자 인터페이스에 관련된 일을 처리하도록 기능을 한정한다. 결국, 마스터 기기(110)는 피제어 기기로서의 기능과 컨트롤 포인트로서의 기능 중 컨트롤 포인트(190)가 갖는 기능 이외의 기능을 더 갖는다. 결과적으로, 컨트롤 포인트(190)가 하는 일이 많이 줄어들었고, 만일 컨트롤 포인트(190)가 불법 기기인 경우에도 보안상 문제점이 발생하지 않는다. 또한, 마스터 기기에 사용자 인터페이스가 존재하지 않아도 문제가 없게 된다.

도 10은 마스터 기기를 정하는 과정을 나타낸 것인데, 이 과정 동인 기기1(110)은 오직 피제어 기기로서만 동작하므로 도 6에서의 동작과 동일하다.

도 11은 도 10의 마스터 기기를 정하는 과정에 이은 기기 인증 과정을 나타낸 것이다. 먼저, 컨트롤 포인트(190)는 마스터 기기(110)에 SOAP를 통해 기기 인증 과정이 시작됨을 알린다(S1101). 본 과정에서 마스터 기기(110)는 CD로 동작한다. 그러면, 마스터 기기(110)(CP로 동작)는 나머지 피제어 기기들(120 내지 160)에게 SOAP를 이용하여 상기 SIB를 직접 전달해 준다(S1102). 그러면, 상기 나머지 피제어 기기들(120 내지 160)은 상기 얻은 SIB를 이용하여 비밀값을 추출하고, 상기 비밀값과 자신이 갖고 있는 디바이스 ID 및 공개키를 이용하여 인증서(certificate)를 생성한다(S1103).

그 후, 상기 나머지 피제어 기기들(120 내지 160)은 마스터 기기(110)(CP로 동작)에게 SOAP를 이용하여 상기 인증서, 디바이스 ID 및 공개키를 직접 전달한다(S1104). 그러면, 상기 마스터 기기(110)는 상기 전달받은 인증서를 검증하고 각 기기에 대한 인증 목록을 작성한다(S1105). 이와 같이 인증서를 검증하여 불법적인 기기로 간주된 기기는 이후 도메인에서 제외되며, 슬레이브 기기로 지정될 가능성이 없다. 그리고, 마스터 기기(110)(CD로 동작)는 GENA를 이용하여 컨트롤 포인트(190)에 상기 검증한 기기의 ID를 이벤트 메시지로 통지한다(S1106). 그러면, 컨트롤 포인트(190)는 SOAP를 이용하여 상기 기기의 검증 결과를 마스터 기기(110)(CD로 동작)로부터 얻어온 후(S1107), 사용자 인터페이스를 통하여 검증 결과 기기가 불법적인가 여부를 외부로 표시한다(S1108).

도 12는 도 11의 기기 인증 과정에 이은 슬레이브 기기를 정하는 과정을 나타낸 것이다. 먼저, 컨트롤 포인트(190)는 상기 인증서 검증 결과 합법적인 기기로 인증된 기기(120 내지 160)들을 대상으로 SOAP를 이용하여 도메인 속성(domain attribute)을 검증한다(S1201). 만약, 상기 기기들에 도메인 속성이 존재하지 않는 경우에는 컨트롤 포인트(190)는 상기

기기들의 리스트를 사용자 인터페이스를 통하여 디스플레이하고(S1202), 사용자로 하여금 슬레이브 기기를 선택하도록 한다(S1203). 도 9c에서는 합법적인 기기들의 리스트를 나타낸 사용자 인터페이스의 예를 나타내었다. 사용자는 이들 리스트 중에서 도메인에 포함시키고자 하는 기기들을 체크함으로써 슬레이브 기기를 선택할 수 있다. 이후, 상기 도 6에서의 마스터 선택 과정과 마찬가지로 관리자 인증 정보를 얻어서(S1204), 관리자 인증을 하는 과정(S1205)을 거친다.

다음으로, 컨트롤 포인트(190)가 마스터 기기(110)(CD로 동작)에 상기 리스트 중에서 선택된 슬레이브 기기(120 내지 140)의 리스트를 SOAP를 통하여 전달한다(S1206). 그 다음, 마스터 기기(110)는 도메인 ID 및 도메인 키를 생성한다(S1207). 한편, 도메인 ID는 다른 도메인과의 식별에 이용되는 것으로서 해당 도메인에 고유한 것이면 어떻게 생성되더라도 상관없다. 따라서, 도메인 ID는 난수 생성기로부터 생성된 난수이거나 또는 슬레이브 기기들의 디바이스 ID들과 임의의 난수를 합성한 값의 해시값일 수 있으며, 특정한 방법에 한정되어 생성되는 것은 아니다. 또한, 도메인 키는 도메인 ID와 마찬가지로 난수 생성기로부터 생성된 난수이거나 슬레이브 기기들의 디바이스 ID와 임의의 난수를 합성한 값의 해시값이 될 수 있다. 그러나, 도메인 키는 도메인의 구성 기기들의 변동에 따라 변동되는 것이므로 슬레이브 기기들의 디바이스 ID를 이용하여 생성되는 것이 보다 바람직할 것이다.

다음으로, 도메인 ID와 도메인 키가 생성되면, 슬레이브 기기에 대한 공개키를 이용하여 도메인 ID와 도메인 키를 암호화한다(S1208). 상기 마스터 기기(110)(CP로 동작)는 직접 SOAP를 통하여 상기 선택된 기기들을 슬레이브 모드로 설정을 하고, 상기 설정된 기기들의 도메인 속성을 전달한다(S1209). 또한, 마스터 기기(110)는 슬레이브로 선택된 기기들에 대한 슬레이브 기기 리스트를 저장한다.

도 13은 본 실시예에 따라 현재 생성되어 있는 인증된 도메인에 게스트(guest)로 있던 피제어 기기들(150, 160)이 슬레이브(slave)로서 추가(join)되는 경우의 동작을 보여주는 흐름도이다. 또한, 도 13은 컨트롤 포인트의 중요한 기능이 마스터 기기로 이관되고 컨트롤 포인트는 주로 사용자 인터페이스 기능만을 수행하는 경우의 동작을 보여주고 있다.

슬레이브 기기를 추가하기 위해 사용자가 컨트롤 포인트(190)가 제공하는 사용자 인터페이스를 통해 슬레이브 기기 추가 메뉴를 선택하면, 컨트롤 포인트(190)는 상기 인증서 검증 결과 합법적인 기기로 인증된 기기(120 내지 160)들을 대상으로 SOAP를 이용하여 도메인 속성(domain attribute)을 검증한다(S1201). 만약, 상기 기기들에 도메인 속성이 존재하지 않는 기기들(150, 160)이 존재하는 경우에 이 기기들의 리스트를 사용자 인터페이스를 통해 디스플레이하고(S1302), 사용자로 하여금 슬레이브 기기를 선택하도록 한다(S1303). 사용자는 도 9c와 같은 사용자 인터페이스 화면을 통해 합법적인 인증을 받은 기기 중에서 게스트 상태인 기기들을 체크함으로써 슬레이브 기기를 선택할 수 있다. 이후, 상기 도 6에서의 마스터 선택 과정과 마찬가지로 관리자 인증 정보를 얻어서(S1304), 관리자 인증을 하는 과정(S1305)을 거친다.

다음으로, 컨트롤 포인트(190)가 마스터 기기(110)에 상기 리스트 중에서 선택된 슬레이브 기기(150, 160)의 리스트를 SOAP를 통하여 전달한다(S1306). 그 다음, 마스터 기기(110)는 이전에 슬레이브 기기로 선택된 기기들(120 내지 140)의 리스트와 현재 새롭게 슬레이브 기기로 선택된 슬레이브 기기들(150, 160)의 기기 정보(예컨대, 디바이스 ID)를 이용하여 새로운 도메인 키를 생성한다(S1307). 즉, 도메인 키는 도메인의 구성원들이 공유해야 할 비밀키이기 때문에 도메인의 구성 기기들의 정보를 이용하여 생성되는 것이 바람직하며, 따라서 도메인의 구성 기기 변경에 따라 새로운 도메인 키를 생성한다. 이 때, 도메인 ID는 외부 도메인과의 식별을 위한 식별자이므로 마스터 기기(110)가 변하지 않는 한 변하지 않는다. 그리고, 슬레이브 기기에 대한 공개키를 이용하여 새로운 도메인 키를 암호화한다(S1308). 상기 마스터 기기(110)는 직접 SOAP를 통하여 상기 선택된 기기들을 슬레이브 모드로 설정을 하고, 새로운 도메인 키를 포함하는 새로운 도메인 속성을 슬레이브 기기로 전달한다(S1309).

이상은 인증된 도메인에 새로운 슬레이브 기기를 추가(join)하는 과정을 설명하였지만, 슬레이브로 설정되어 있던 기기들을 인증된 도메인에서 탈퇴(leave)시키기 위해 사용자는 컨트롤 포인트(190)가 제공하는 사용자 인터페이스 화면을 통해 기기의 탈퇴(leave)를 선택할 수 있다. 이 때에도, 도 13에 도시된 과정과 유사하게 탈퇴한 슬레이브 기기를 마스터 기기(110)의 슬레이브 기기 리스트에서 삭제하고 남아 있는 슬레이브 기기들의 정보를 이용하여 새로운 도메인 키를 생성한다.

한편, 본 명세서에서 추가(join) 및 탈퇴(leave)라는 용어는 슬레이브 기기가 컨트롤 포인트를 통한 사용자의 허가에 의해 슬레이브 리스트를 변경함으로써 도메인의 구성이 변경되는 경우를 나타낸다. 따라서, 추가(join) 및 탈퇴(leave)는, 컨트롤 포인트를 통한 사용자의 허가에 의하지 않고 슬레이브 기기가 컨트롤 포인트에 물리적으로 부가되거나 슬레이브 기기의 전원이 '온'되는 경우와 같이 슬레이브 기기가 도메인에 커넥트(connect)되는 것과, 컨트롤 포인트를 통한 사용자의 허가에 의하지 않고 슬레이브 기기가 컨트롤 포인트로부터 물리적으로 떼어지거나 슬레이브의 기기의 전원이 '오프'되는 경우와 같이 슬레이브 기기가 도메인으로부터 디스커넥트(disconnect)되는 것과 구별된다.

한편, 인증된 도메인의 슬레이브 기기들(예컨대, 120 내지 140) 중 슬레이브 기기(120)가 탈퇴하고 그 사이에 다른 게스트 기기들(예컨대, 150, 160) 중 게스트 기기(150)가 인증된 도메인에 슬레이브 기기로 추가된 경우에는 슬레이브 기기의 추가에 따라 도 13과 같은 과정을 거쳐 새로운 도메인 키를 생성하면 되고, 탈퇴했던 슬레이브 기기(120)가 다시 도메인에 추가되는 경우에는 슬레이브 기기(120)의 기기 정보를 반영하여 새로운 도메인 키를 생성하면 되므로 문제가 없다. 그러나, 슬레이브 기기의 추가 및 탈퇴는 사용자의 의사에 따라 결정되는 것으로서 그리 자주 발생하는 상황이 아니지만, 예컨대 슬레이브 기기가 전자 제품인 경우에는 전원이 온/오프 되는 상황(즉, 커넥트/디스커넥트되는 상황)이 자주 발생하기 때문에 그 때마다 도메인 키를 변경하는 것은 번거로울 뿐만 아니라 시스템에도 부담이 된다.

따라서, 본 발명은 슬레이브 기기의 추가/탈퇴 및 커넥트/디스커넥트 상황을 구분하기 위한 식별자로서 '세션 ID(session ID)'를 도입하였다. 세션 ID는 슬레이브 기기의 추가/탈퇴에 따라 변동되고, 슬레이브 기기의 커넥트/디스커넥트에 따라서는 변동되지 않으며, 마스터와 슬레이브가 공유한다. 또한, 세션 ID는 도메인 ID와 마찬가지로 랜덤하게 생성되거나 도메인의 구성 기기들의 정보를 이용하여 생성될 수 있으며, 슬레이브 기기의 공개키로 암호화해서 슬레이브 기기로 전달되는 것이 바람직하다. 또한, 세션 ID는 고유 ID, 날짜 정보 및 버전 정보 등을 포함할 수 있다.

한편, 슬레이브 기기가 도메인에 커넥트 또는 디스커넥트되는 상황에 따라 몇 가지 고려해야 할 문제가 있다.

도 14에 도시된 바와 같이, 슬레이브 기기(S1)가 컨트롤 포인트(CP)로부터 디스커텍트되었다가 소정 시간 이후에 다시 컨트롤 포인트(CP)에 커넥트되는 경우에는 디스커넥트시와 커넥트시에 마스터 기기(M)와 슬레이브 기기들(S1, S2, S3)들이 공유하는 세션 ID 및 도메인 키의 변동이 없으므로 슬레이브 기기(S1)는 디스커넥트되기 전의 도메인 키를 이용하여 컨텐츠를 이용할 수 있다.

그러나, 도 15에 도시된 바와 같이, 슬레이브 기기(S1)가 컨트롤 포인트(CP)로부터 디스커넥트된 상태에서 다른 슬레이브 기기(S4)가 도메인에 추가된 경우에는 마스터 기기(M)와 슬레이브 기기들(S1, S2, S3, S4)들이 공유하는 세션 ID 및 도메인 키가 변경되기 때문에, 슬레이브 기기(S1)가 다시 도메인에 커넥트되는 경우에 슬레이브 기기(S1)는 도메인이 공유하고 있는 컨텐츠를 제대로 재생하거나 이용할 수 없게 된다. 따라서, 마스터 기기(M)는 새롭게 도메인에 커넥트되는 기기의 세션 ID와 마스터 기기의 세션 ID를 비교하여 세션 ID가 일치하지 않는 경우에는, 슬레이브 기기(S4)의 추가시에 새롭게 생성된 도메인 키(DK2)를 슬레이브 기기(S1)에게 전달한다. 또한, 슬레이브 기기(S1)가 디스커넥트되는 동안 슬레이브 기기(S2)가 탈퇴하는 경우에도 마스터 기기(M)의 세션 ID와 도메인 키가 변경되기 때문에 도 15에서와 같은 절차가 진행된다. 컨트롤 포인트(CP)는 소정의 기기가 커넥트되는 경우에 이를 감지하여 그 기기의 세션 ID를 마스터 기기(M)에게 전달하는 역할을 하며, 마스터 기기(M)로부터의 정보를 도메인의 구성 기기들에게 전달하는 역할을 한다.

한편, 마스터 기기(M)에 저장되어 있는 슬레이브 리스트는 사용자가 컨트롤 포인트를 통해 변경하지 않는 한 슬레이브 기기의 커넥트 및 디스커넥트시에는 변경되지 않는다. 따라서, 슬레이브 기기(S1)가 디스커넥트된 동안에 사용자가 슬레이브 기기(S1)를 슬레이브 리스트에서 삭제하였다면, 슬레이브 기기(S1)는 슬레이브 기기의 지위를 상실하게 된다. 그러나, 디스커넥트된 슬레이브 기기(S1)는 여전히 기기 모드가 슬레이브 상태로 설정되어 있기 때문에, 슬레이브 기기(S1)가 다시 커넥트되는 경우에 마스터 기기(M)는 세션 ID 이외에도 슬레이브 리스트에 슬레이브 기기(S1)가 존재하는지도 검사하여 슬레이브 리스트에 존재하지 않는 기기의 기기 모드를 게스트 모드로 변경해 줄 필요가 있다. 그렇지 않으면, 실질적으로 게스트 상태인 슬레이브 기기(S1)가 사용자의 허가없이 새로운 도메인 키를 공유하게 되어 시스템 전체의 구조가 붕괴된다.

도 16에는 도메인에 새롭게 커넥트되는 기기에 대한 처리 과정을 보여준다. 컨트롤 포인트가 도메인에 커넥트되는 새로운 기기를 발견하면(S1601), 도 7에서와 같은 기기 인증 과정을 거쳐(S1603) 인증이 실패하면 커넥트된 기기를 불법 기기로 간주하여 절차를 종료하고 인증이 성공하면, 커넥트된 기기의 기기 모드가 슬레이브 상태인지를 확인한다(S1605).

커넥트된 기기의 기기 모드가 게스트 상태인 경우에는 이후의 절차 진행이 의미가 없으므로 절차를 종료하고 커넥트된 기기의 모드가 슬레이브 상태인 경우에는 마스터 기기와 세션 ID가 동일한지를 판단한다(S1607). 만약, 커넥트된 기기의 세션 ID가 마스터 기기와 세션 ID가 동일하다면, 도메인 키도 변경이 없기 때문에 그래도 절차를 종료한다. 그러나, 세션 ID가 동일하지 않다면 마스터 기기가 보유한 도메인 키와 커넥트된 기기가 보유한 도메인 키가 동일하지 않다는 의미이기 때문에 새로운 도메인 키를 커넥트된 기기에게 전달할 필요가 있다. 그러나, 마스터 기기와 커넥트된 기기의 세션 ID가 동일하지 않다고 해서 곧바로 커넥트된 기기에게 새로운 도메인 키를 전달하는 것은, 전술한 바와 같이 실질적으로 기기 모드가 게스트 상태인 기기를 슬레이브 기기로 인정하는 것이 되기 때문에, 커넥트된 기기가 마스터 기기(M)가 보유하고 있는 슬레이브 리스트에 존재하는 지를 검사해야 한다(S1609).

검사 결과 커넥트된 기기가 슬레이브 리스트에 존재한다면, 커넥트된 기기는 슬레이브 기기로서의 지위를 그대로 유지하고 있다고 여겨지기 때문에 새로운 도메인 키를 커넥트된 기기로 전송하며(S1611), 그렇지 않을 경우에는 커넥트된 기기의 기기 모드를 게스트로 변경한다(S1613). 기기 모드가 게스트로 변경된 커넥트된 기기는 도 8와 같은 과정을 거쳐 슬레이브 기기로 선택될 수 있다.

한편, 슬레이브 기기가 여러 개의 도메인에 참여할 수 있는 멀티 도메인 정책을 취할 경우에는 세션 ID를 비교하기 전에 도메인 ID를 비교함으로써 해당 도메인 ID를 보유하지 않은 커넥트된 기기에 대해서는 후속 절차(S1605 내지 S1611)를 진행할 필요없이 절차를 종료할 수도 있다. 또한, 멀티 도메인 정책을 취하지 않아서 슬레이브 기기가 하나의 도메인 ID만 가질 수 있는 경우에도 다른 도메인에 참가해서 도메인 ID가 변경된 기기에 대해서도 후속 절차(S1605 내지 S1611)를 진행할 필요없이 절차를 종료할 수도 있다. 따라서, 이 경우에는, 적어도 단계(S1607) 이전에, 커넥트된 기기의 도메인 ID와 현재 도메인의 도메인 ID를 비교하는 단계를 추가한다.

전술한 바와 같이, 세션 ID는 고유 ID 이외에도 날짜 정보 및/또는 버전 정보를 더 포함할 수도 있다. 세션 ID에 날짜 정보나 버전 정보를 포함하게 되면 과거의 세션 ID와 현재의 세션 ID를 보다 분명하게 구별할 수가 있어서, 이러한 정보를 이용해 여러 가지 서비스를 제공할 수 있다. 예컨대, 마스터 기기가 디스커넥트되었을 때, 컨트롤 포인트는 슬레이브 기기들의 세션 ID의 날짜 정보와 버전 정보를 확인하는데, 이 때 도메인 ID는 같고 세션 ID가 다를 경우에는 슬레이브 기기가 디스커넥트되어 있는 동안에 도메인의 구성이 변경되었음을 알 수 있다. 따라서, 마스터가 도메인에 없는 경우에도 날짜 정보나 버전 정보를 이용하여 가장 최신의 세션 ID와 도메인 키를 가지고 있는 슬레이브 기기를 이용하여 나머지 슬레이브 기기들의 세션 ID와 도메인 키를 변경할 수 있다.

도 17에는 본 발명이 적용되는 도 4에 도시된 컨트롤 포인트(190)의 구성예가 도시되어 있다. 컨트롤 포인트(190)는 사용자에게 도 9a 내지 도 9c와 같은 사용자 인터페이스를 제공하기 위한 사용자 인터페이스 제공부(192)와, 컨트롤 포인트(190)에 접속하는 기기들의 동작에 필요한 정보를 마스터 기기와 슬레이브 기기에게 제공하는 기기 동작 정보 제공부(194)와 컨트롤 포인트(190)에 접속하는 기기들을 검출하기 위한 기기 검출부(196)를 포함한다.

인터페이스 제공부(192)는 사용자 인터페이스 화면에 기기 리스트 표시 및 기기 인증 결과 표시를 수행한다. 사용자는 사용자 인터페이스 제공부(192)가 제공하는 사용자 인터페이스를 통해 마스터 기기 및 슬레이브 기기의 선택, 그리고 슬레이브 리스트의 변경 등을 수행할 수 있으며, 기기 인증 결과에 따라 마스터 기기에 불법 기기 목록을 저장할 수도 있다. 기기 동작 정보 제공부(194)는 도 6 내지 도 8 및 도 10 내지 도 12에 도시된 바와 같이, 기기들의 동작에 필요한 정보들을 기기들에게 전달한다. 기기 검출부(196)는 컨트롤 포인트(190)에 커넥트되거나 디스커넥트되는 기기들을 탐지하여 해당 기기들의 정보를 기기 동작 정보 제공부(194)에 전달하고 기기 동작 정보 제공부(194)는 예컨대, 이 정보들을 기기들에게 전달함으로써 도 16에 도시된 절차들을 수행할 수 있도록 한다.

도 18에는 본 발명이 적용되는 도 4에 도시된 마스터 기기(110)의 구성예가 도시되어 있다. 마스터 기기(110)는, 컨트롤 포인트(190)를 통해 마스터 기기(110)에 접속한 피제어 기기의 인증, 기기 모드 판별 및 슬레이브 기기 리스트 관리 등을 수행하는 피제어 기기 관리부(113)와, 도메인 ID의 생성 및 도메인에 접속하는 기기의 도메인 ID 검사 등을 수행하는 도메인 ID 관리부(115)와, 세션 ID의 생성, 변경 및 도메인에 접속하는 기기의 세션 ID 검사 등을 수행하는 세션 ID 관리부(117)와, 도메인 키의 생성, 변경 및 슬레이브 기기로의 도메인 키 제공 등을 수행하는 도메인 키 관리부(119)를 포함한다.

피제어 기기 관리부(113)는, 도 7 또는 도 11의 흐름도에 따라 도메인에 접속하는 피제어 기기의 인증을 수행하여 도 16의 단계(S1603)에서 기기 인증 성공 여부를 판단한다. 이 때, 인증이 실패하면 접속된 피제어 기기를 불법 기기로 간주하여 불법 기기 리스트에 따로 저장할 수 있다. 또한, 피제어 기기 관리부(113)는 도 16의 단계(S1605)에서 도메인에 접속하는 피제어 기기의 기기 모드가 슬레이브 상태인지 아니면 게스트 상태인지를 판별한다. 이 때, 슬레이브 상태가 아니라면 에러 신호를 출력하며, 사용자는 에러 신호에 따라 접속된 피제어 기기를 정상 절차에 따라 슬레이브 기기로 다시 등록하든지 아니면 그대로 방치할 수도 있다. 또한, 피제어 기기 관리부(113)는 컨트롤 포인트를 통한 사용자의 지시에 따라 슬레이브 기기 리스트를 작성 및 변경하고, 도 16의 단계(S1609)에서는 마스터 기기(110)와 세션 ID가 일치하지 않는 접속 기기가 슬레이브 기기 리스트에 존재하는지를 판별하여, 존재하지 않으면 접속 기기의 기기 모드를 게스트로 변경하도록 접속 기기를 제어한다.

도메인 ID 관리부(115)는 도메인 ID를 생성하여 도메인의 구성 기기에게 제공하고, 도메인에 새로운 피제어 기기가 접속한 경우에는 적어도 도 16의 단계(S1607) 이전에 마스터 기기(110)의 도메인 ID와 도메인에 접속한 피제어 기기의 도메인 ID를 비교하여, 일치하지 않으면 에러 신호를 출력하고, 사용자는 에러 신호에 따라 소정의 처리를 수행한다.

세션 ID 관리부(117)는 세션 ID를 생성하고, 슬레이브 기기 리스트의 변동에 따라 새로운 세션 ID를 생성하며, 도 16의 단계(S1607)에서는 도메인에 접속한 기기와 마스터 기기(110)의 세션 ID를 비교하여, 세션 ID가 일치하지 않으면 해당 접속 기기에게 마스터 기기(110)의 세션 ID를 제공한다.

도메인 키 관리부(119)는, 도메인 키를 생성하고 도메인의 구성 변동에 따라 새로운 도메인 키를 생성하며, 생성된 도메인 키를 슬레이브 기기에게 제공한다.

발명의 효과

이상과 같이, 본 발명에 따르면, 사용자가 직접 도메인 형성을 제어하고 외부와 독립된 도메인을 보다 안전하게 구축할 수 있는 효과가 있다.

또한, 본 발명에 따르면, 기존의 표준 인터넷 프로토콜을 사용하는 네트워크에 매끄럽게 통합이 가능한 UPnP 기반의 홈 네트워크 시스템을 구현할 수 있는 효과가 있다.

또한, 본 발명에 따르면, 홈 네트워크의 도메인의 구성 기기들의 변동을 사용자가 직접 제어하고 구성 기기의 변동에 따른 새로운 도메인 키의 생성을 마스터 기기가 담당하고 슬레이브 기기들은 마스터 기기에서 생성된 도메인 키를 전달받도록 함으로써 도메인 구성 변경에 따른 도메인 키 변경의 절차를 간소화하는 효과가 있다.

또한, 본 발명에 따르면, 도메인 ID와 도메인 키 이외에도 도메인이 공유하는 정보로서 세션 ID를 도입함으로써 빈번하게 발생하는 슬레이브 기기의 커넥트/디스커넥트시에는 도메인 키를 변경하지 않음으로써 빈번한 도메인 키의 변경을 방지할 수 있는 효과가 있다.

도면의 간단한 설명

도 1은 일반적인 도메인 관리의 구조를 나타낸 도면이다.

도 2는 종래의 마스터-슬레이브 구조에 따라 'xCP Cluster Protocol'을 기반으로 하는 컨텐츠 재생 과정을 나타낸 흐름도이다.

도 3은 공개키 기반 구조의 도메인 형성 방법을 나타내는 흐름도이다.

도 4는 본 발명의 실시예에 따른 도메인 형성 방법을 UPnP에 적용한 예를 나타낸 블록도이다.

도 5는 컨트롤 포인트와 피제어 기기들 간에 수행되는 일반적인 UPnP 동작을 나타낸 도면이다.

도 6은 본 발명의 실시예에 관련되어 마스터 기기를 정하는 과정을 나타낸 흐름도이다.

도 7은 도 6의 과정에 이은 기기 인증 과정을 나타낸 흐름도이다.

도 8은 도 7의 과정에 이은 슬레이브 기기를 정하는 과정을 나타낸 흐름도이다.

도 9a 내지 도 9c는 컨트롤 포인트가 제공하는 사용자 인터페이스 화면의 구성예이다.

도 10은 본 발명의 실시예에 관련되어 마스터 기기를 정하는 다른 과정을 나타낸 흐름도이다.

도 11은 도 10의 과정에 이은 기기 인증 과정을 나타낸 흐름도이다.

도 12는 도 11의 과정에 이은 슬레이브 기기를 정하는 과정을 나타낸 흐름도이다.

도 13은 본 발명의 실시예에 따른, 도메인 키의 생성 과정을 나타낸 흐름도이다.

도 14는 슬레이브 기기의 커넥트/디스커넥트에 따른 도메인 상태를 설명하기 위한 도면이다.

도 15는 슬레이브 기기의 커넥트/디스커넥트에 따른 다른 도메인 상태를 설명하기 위한 도면이다.

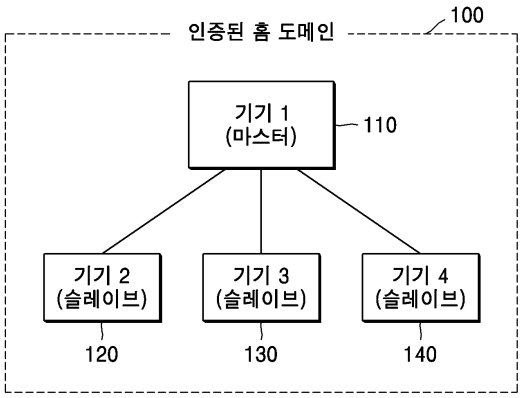
도 16은 본 발명의 실시예에 따라, 도메인에 새롭게 접속하는 기기에 대한 처리 과정을 나타내는 흐름도이다.

도 17은 본 발명의 실시예에 따른, 컨트롤 포인트의 블록도이다.

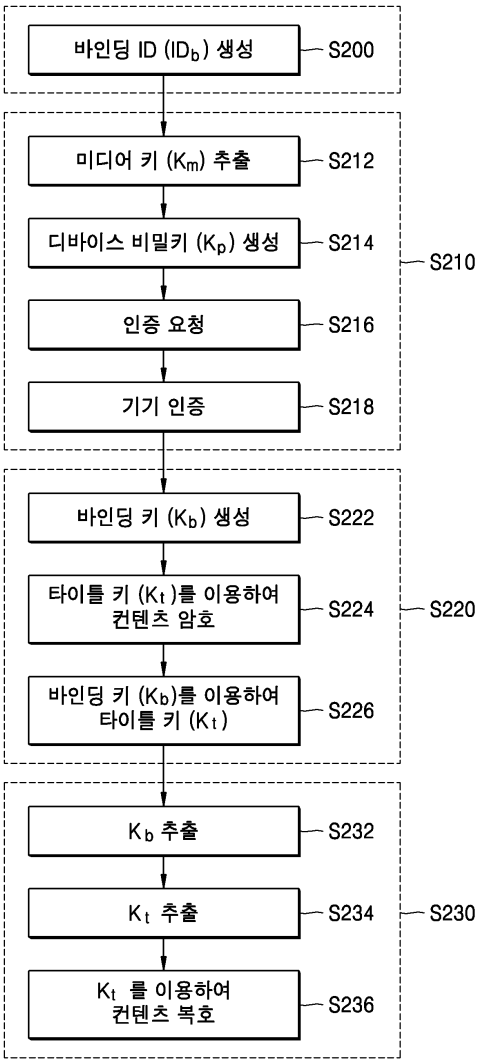
도 18은 본 발명의 실시예에 따른, 마스터 기기의 블록도이다.

도면

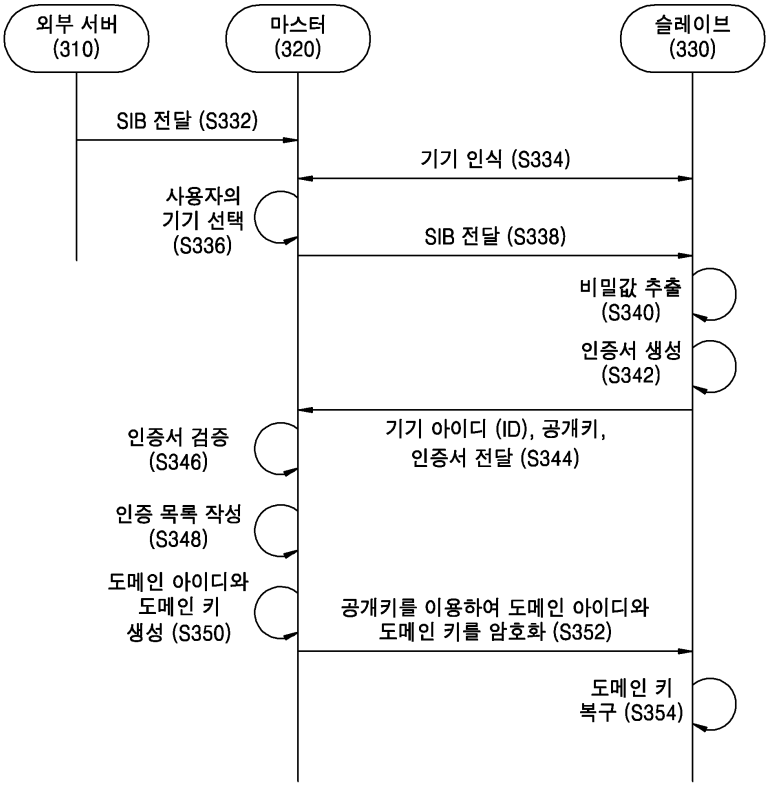
도면1



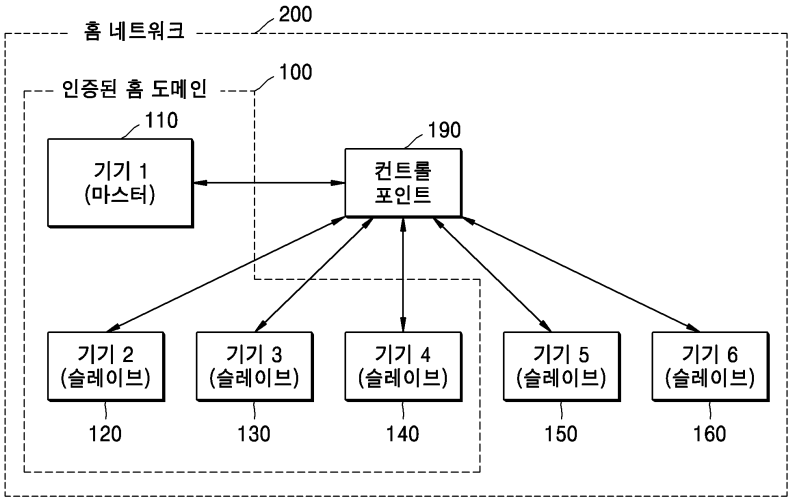
도면2


바인딩 ID (ID_b) 생성
S200
미디어 키 (K_m) 추출
S212
디바이스 비밀키 (K_p) 생성
S214
인증 요청
S216
기기 인증
S218
S210
바인딩 키 (K_b) 생성
S222
타이틀 키 (K_t)를 이용하여 컨텐츠 암호
S224
바인딩 키 (K_b)를 이용하여 타이틀 키 (K_t)
S226
S220
K_b 추출
S232
K_t 추출
S234
K_t 를 이용하여 컨텐츠 복호
S236
S230

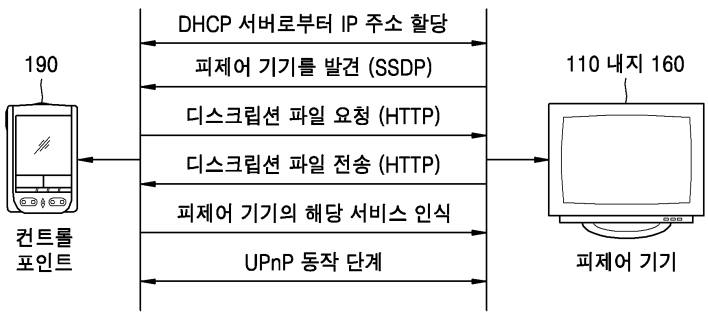
도면3


외부 서버
(310)
마스터
(320)
슬레이브
(330)
SIB 전달 (S332)
기기 인식 (S334)
사용자의
기기 선택
(S336)
SIB 전달 (S338)
비밀값 추출
(S340)
인증서 생성
(S342)
기기 아이디 (ID), 공개키,
인증서 전달 (S344)
인증서 검증
(S346)
인증 목록 작성
(S348)
도메인 아이디와
도메인 키
생성 (S350)
공개키를 이용하여 도메인 아이디와
도메인 키를 암호화 (S352)
도메인 키
복구 (S354)

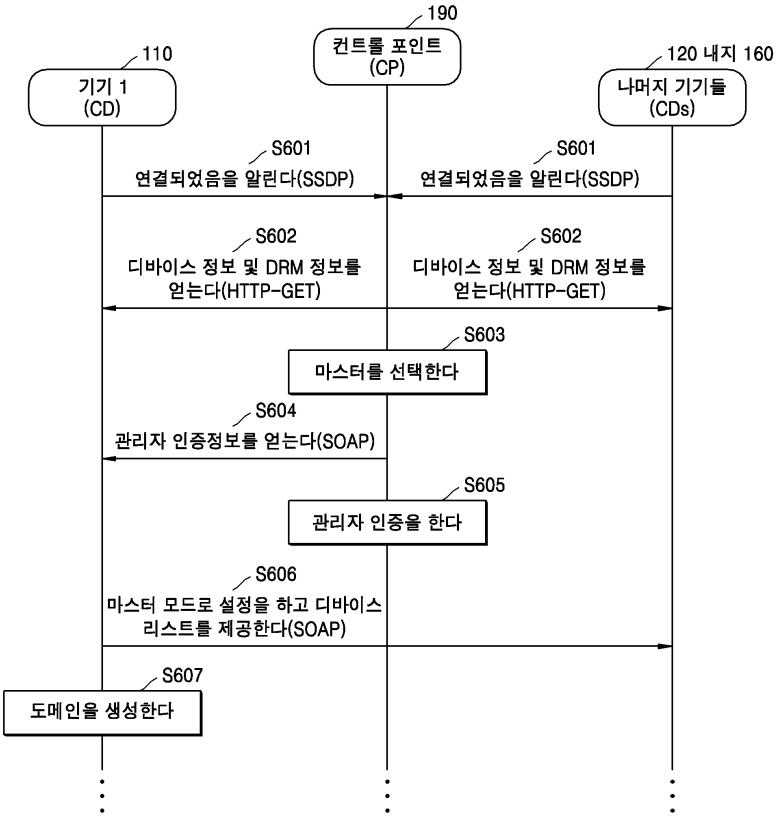
도면4


홈 네트워크
200
인증된 홈 도메인
100
110
기기 1
(마스터)
190
컨트롤
포인트
기기 2
(슬레이브)
기기 3
(슬레이브)
기기 4
(슬레이브)
기기 5
(슬레이브)
기기 6
(슬레이브)
120
130
140
150
160

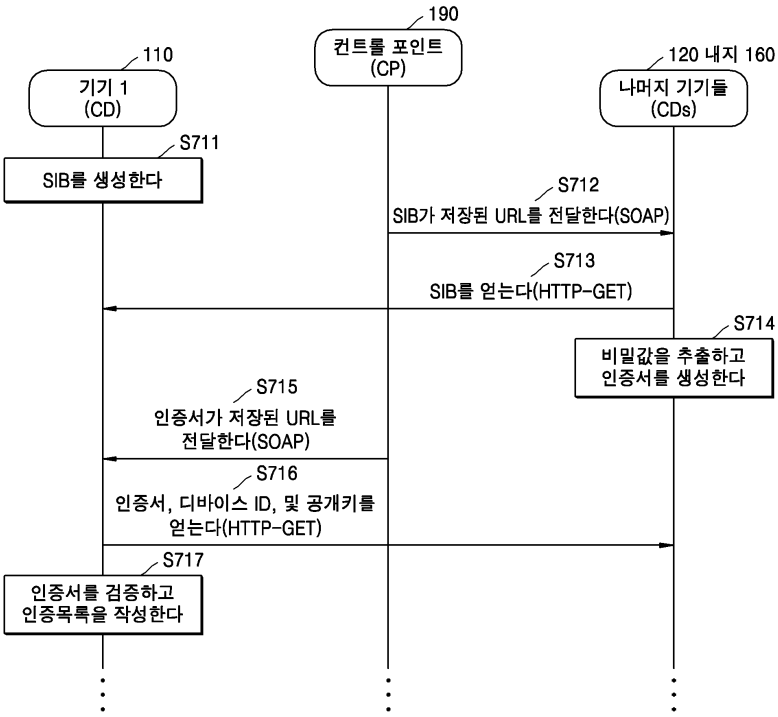
도면5


DHCP 서버로부터 IP 주소 할당
피제어 기기를 발견 (SSDP)
디스크립션 파일 요청 (HTTP)
디스크립션 파일 전송 (HTTP)
피제어 기기의 해당 서비스 인식
UPnP 동작 단계
190
컨트롤
포인트
110 내지 160
피제어 기기

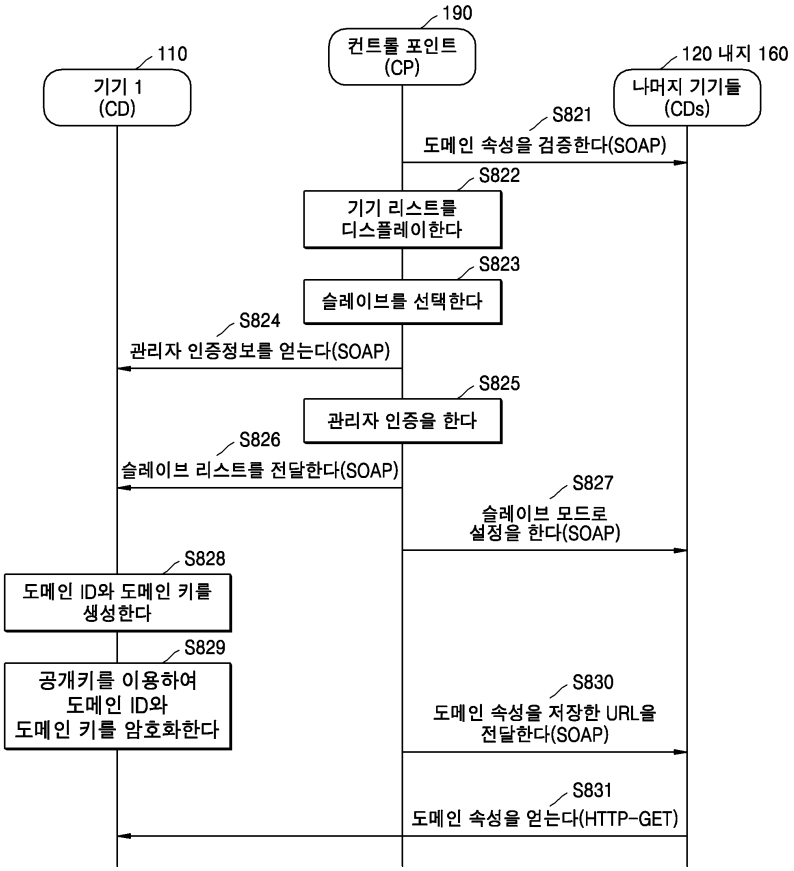
도면6


190
컨트롤 포인트
(CP)
110
기기 1
(CD)
120 내지 160
나머지 기기들
(CDs)
S601
연결되었음을 알린다(SSDP)
S601
연결되었음을 알린다(SSDP)
S602
디바이스 정보 및 DRM 정보를
얻는다(HTTP-GET)
S602
디바이스 정보 및 DRM 정보를
얻는다(HTTP-GET)
S603
마스터를 선택한다
S604
관리자 인증정보를 얻는다(SOAP)
S605
관리자 인증을 한다
S606
마스터 모드로 설정을 하고 디바이스
리스트를 제공한다(SOAP)
S607
도메인을 생성한다

도면7


190
컨트롤 포인트
(CP)
110
기기 1
(CD)
120 내지 160
나머지 기기들
(CDs)
S711
SIB를 생성한다
S712
SIB가 저장된 URL를 전달한다(SOAP)
S713
SIB를 얻는다(HTTP-GET)
S714
비밀값을 추출하고
인증서를 생성한다
S715
인증서가 저장된 URL를
전달한다(SOAP)
S716
인증서, 디바이스 ID, 및 공개키를
얻는다(HTTP-GET)
S717
인증서를 검증하고
인증목록을 작성한다

도면8



도면9a

FRIENDLY NAME	MODE	FLAG
MAIN NEXUS	GUEST	V
SUB NEXUS	GUEST	

도면9b

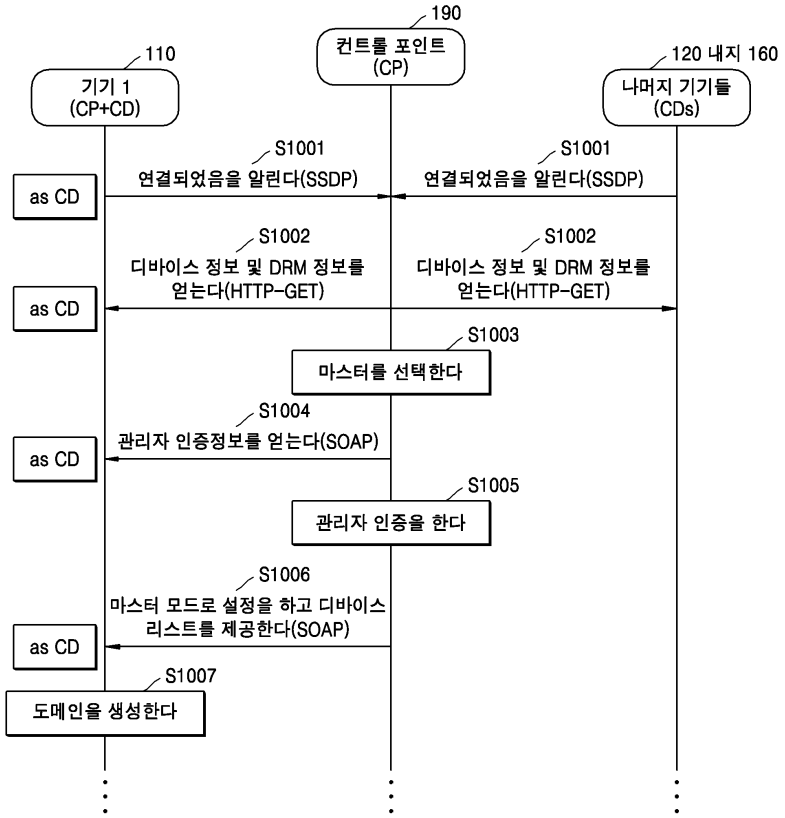
관리자 인증

ID:0314620157
PASSWORD: ....

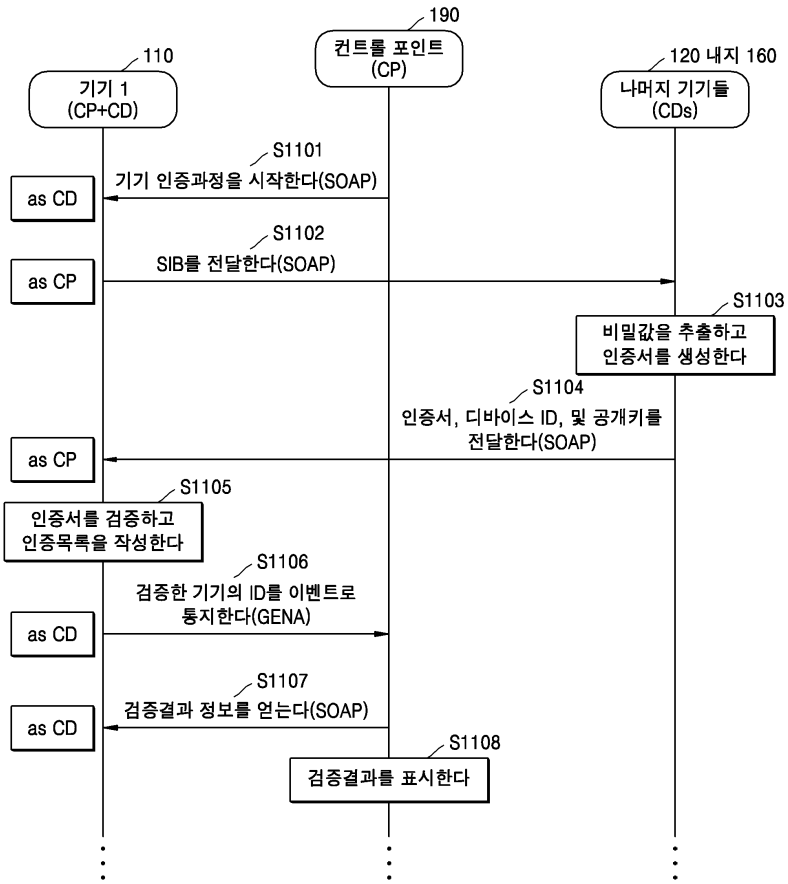
도면9c

FRIENDLY NAME	MODE	FLAG
SUB NEXUS	GUEST	V
NOTE PC1	GUEST	V
NOTE PC2	GUEST	V

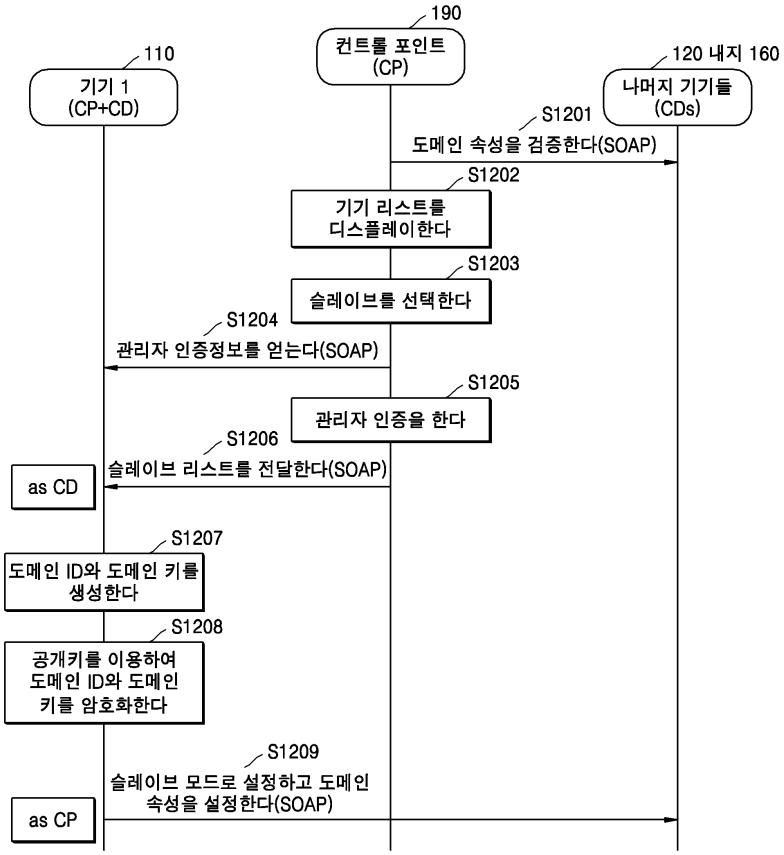
도면10


190
컨트롤 포인트
(CP)
110
기기 1
(CP+CD)
120 내지 160
나머지 기기들
(CDs)
S1001
연결되었음을 알린다(SSDP)
S1001
연결되었음을 알린다(SSDP)
as CD
S1002
디바이스 정보 및 DRM 정보를
얻는다(HTTP-GET)
S1002
디바이스 정보 및 DRM 정보를
얻는다(HTTP-GET)
as CD
S1003
마스터를 선택한다
S1004
관리자 인증정보를 얻는다(SOAP)
as CD
S1005
관리자 인증을 한다
S1006
마스터 모드로 설정을 하고 디바이스
리스트를 제공한다(SOAP)
as CD
S1007
도메인을 생성한다

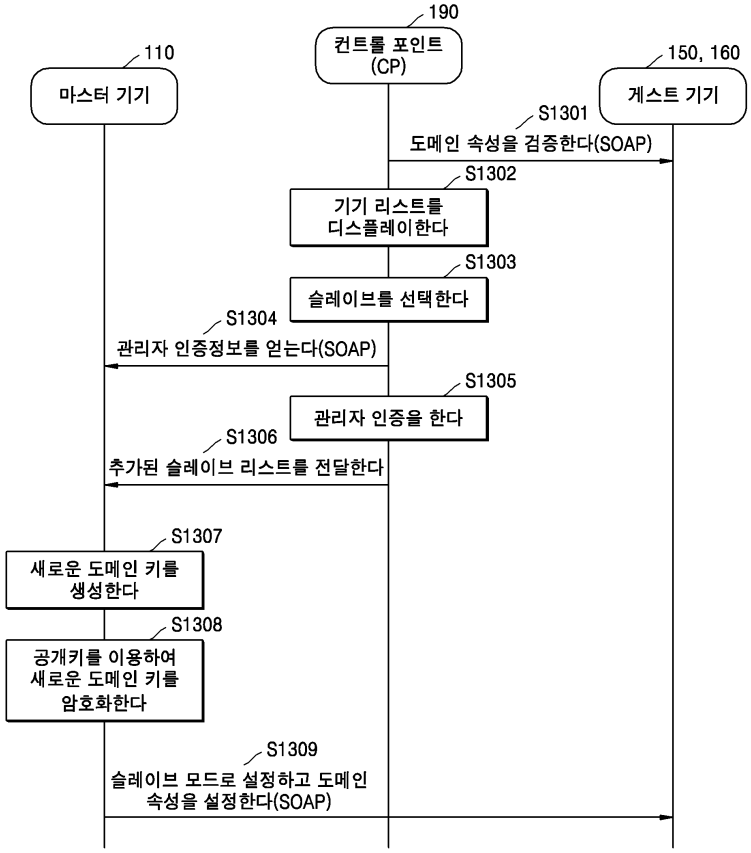
도면11


190
컨트롤 포인트
(CP)
110
기기 1
(CP+CD)
120 내지 160
나머지 기기들
(CDs)
S1101
기기 인증과정을 시작한다(SOAP)
as CD
S1102
SIB를 전달한다(SOAP)
as CP
S1103
비밀값을 추출하고
인증서를 생성한다
S1104
인증서, 디바이스 ID, 및 공개키를
전달한다(SOAP)
as CP
S1105
인증서를 검증하고
인증목록을 작성한다
S1106
검증한 기기의 ID를 이벤트로
통지한다(GENA)
as CD
S1107
검증결과 정보를 얻는다(SOAP)
as CD
S1108
검증결과를 표시한다

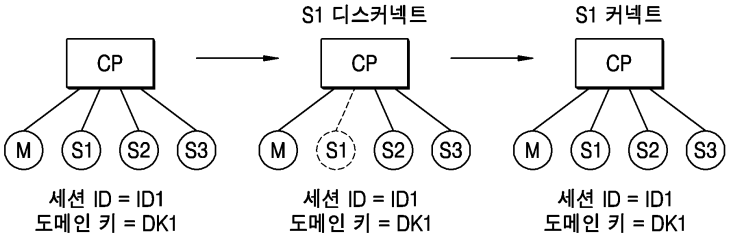
도면12


190
컨트롤 포인트
(CP)
110
기기 1
(CP+CD)
120 내지 160
나머지 기기들
(CDs)
S1201
도메인 속성을 검증한다(SOAP)
S1202
기기 리스트를
디스플레이한다
S1203
슬레이브를 선택한다
S1204
관리자 인증정보를 얻는다(SOAP)
S1205
관리자 인증을 한다
S1206
슬레이브 리스트를 전달한다(SOAP)
as CD
S1207
도메인 ID와 도메인 키를
생성한다
S1208
공개키를 이용하여
도메인 ID와 도메인
키를 암호화한다
S1209
슬레이브 모드로 설정하고 도메인
속성을 설정한다(SOAP)
as CP

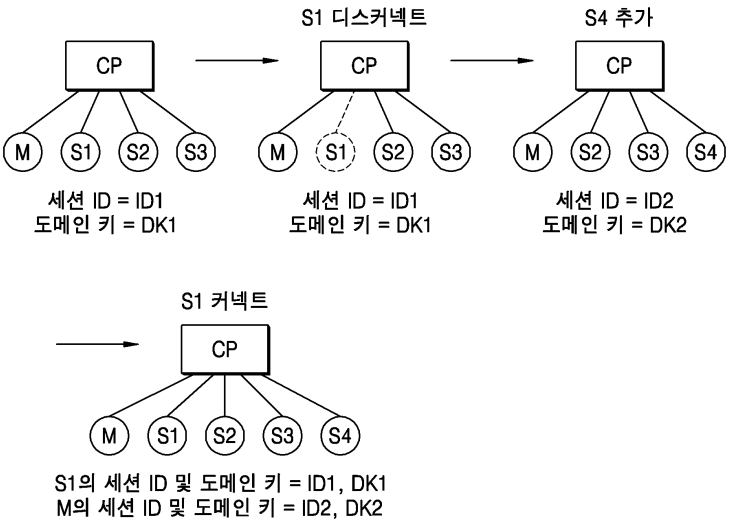
도면13


190
컨트롤 포인트
(CP)
110
마스터 기기
150, 160
게스트 기기
S1301
도메인 속성을 검증한다(SOAP)
S1302
기기 리스트를
디스플레이한다
S1303
슬레이브를 선택한다
S1304
관리자 인증정보를 얻는다(SOAP)
S1305
관리자 인증을 한다
S1306
추가된 슬레이브 리스트를 전달한다
S1307
새로운 도메인 키를
생성한다
S1308
공개키를 이용하여
새로운 도메인 키를
암호화한다
S1309
슬레이브 모드로 설정하고 도메인
속성을 설정한다(SOAP)

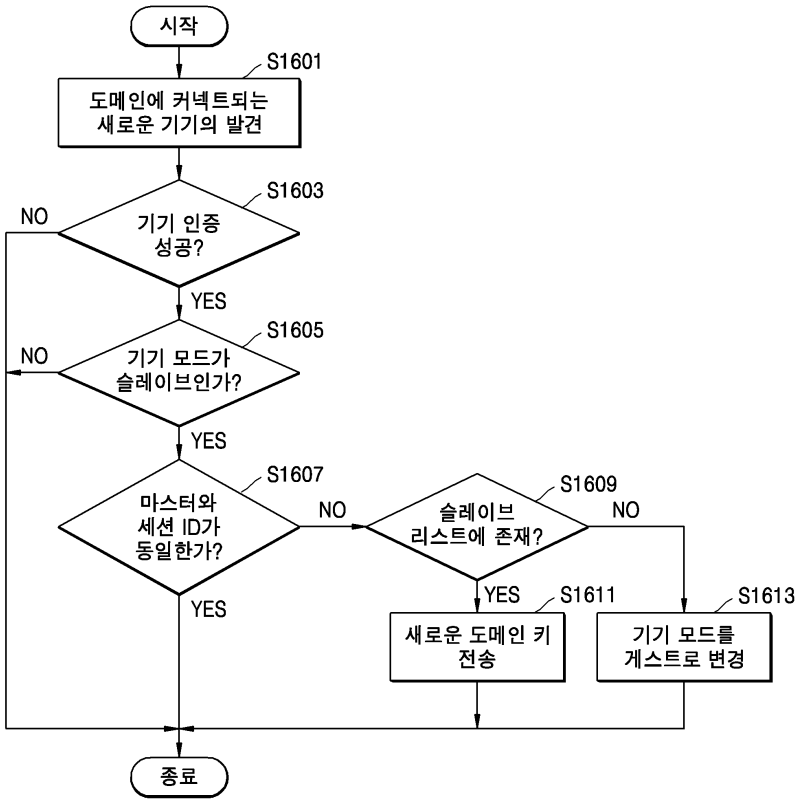
도면14



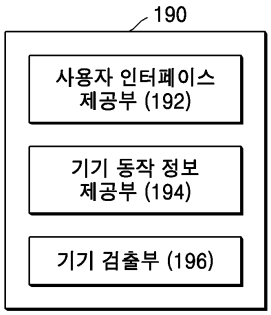
도면15



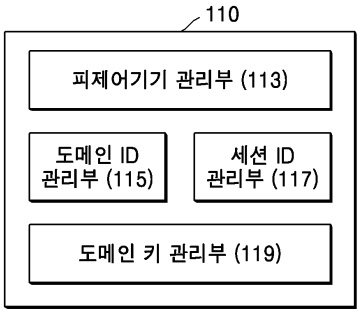
도면16



도면17


190
사용자 인터페이스 제공부 (192)
기기 동작 정보 제공부 (194)
기기 검출부 (196)

도면18


110
피제어기기 관리부 (113)
도메인 ID 관리부 (115)
세션 ID 관리부 (117)
도메인 키 관리부 (119)