(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년07월28일
(11) 등록번호 10-1762906
(24) 등록일자 2017년07월24일

(51) 국제특허분류(Int. Cl.)
H04W 40/02 (2009.01) *H04L 12/70* (2013.01)
H04L 12/741 (2013.01) *H04L 29/06* (2006.01)
H04W 12/06 (2009.01) *H04W 40/24* (2009.01)
H04W 80/04 (2009.01) *H04W 84/18* (2009.01)
(52) CPC특허분류
H04W 40/02 (2013.01)
H04L 45/741 (2013.01)
(21) 출원번호 10-2016-7001528
(22) 출원일자(국제) 2014년06월23일
심사청구일자 2016년01월19일
(85) 번역문제출일자 2016년01월19일
(65) 공개번호 10-2016-0019966
(43) 공개일자 2016년02월22일
(86) 국제출원번호 PCT/US2014/043691
(87) 국제공개번호 WO 2014/209896
국제공개일자 2014년12월31일
(30) 우선권주장
13/926,312 2013년06월25일 미국(US)
(56) 선행기술조사문헌
KR1020120014887 A*
IETF RFC 6272
IETF RFC 4347
IETF RFC 5238
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
구글 인코포레이티드
미국 캘리포니아 마운틴 뷰 엠피시어터 파크웨이 1600 (우:94043)
(72) 발명자
에릭슨, 그랜트 엠.
미국 94304 캘리포니아 팔로 알토 한센 웨이 900
브로스, 크리스토퍼 에이.
미국 94304 캘리포니아 팔로 알토 한센 웨이 900
(74) 대리인
특허법인 남앤드남

전체 청구항 수 : 총 20 항 심사관 : 황운철

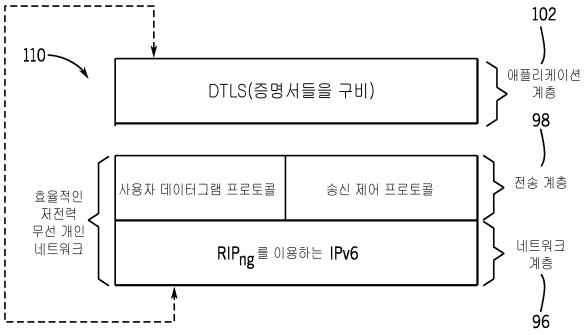
(54) 발명의 명칭 **IPv6 프로토콜을 위한 효율적인 네트워크 계층**

(57) 요 약

전자 디바이스는, 전자 디바이스로 하여금 그 전자 디바이스를 무선 메시 네트워크를 통해 다른 전자 디바이스에 무선으로 결합시킬 수 있게 할 수 있는 네트워크 인터페이스를 포함할 수 있다. 전자 디바이스는 또한, 라우팅 정보 프로토콜-차세대(RIPng; Routing Information Protocol-Next Generation) 라우팅 메커니즘 및 네트워크 인

(뒷면에 계속)

대 표 도 - 도5



터페이스를 이용하여 무선 메시 네트워크를 경유하는 다른 전자 디바이스에 대한 적어도 하나의 데이터 경로를 결정할 수 있는 프로세서를 포함할 수 있다. 다른 전자 디바이스에 대한 적어도 하나의 데이터 경로를 식별한 후, 프로세서는, 식별된 데이터 경로(들)가 데이터그램 전송 계층 보안(Datagram Transport Layer Security) 프로토콜을 이용하여 안전한지 여부를 결정할 수 있다. 식별된 데이터 경로(들)가 안전한 것으로 결정되는 경우, 프로세서는 안전한 데이터 경로(들)를 통해 IPv6(Internet Protocol version 6) 데이터 패킷들을 다른 전자 디바이스로 전송할 수 있다.

(52) CPC특허분류
H04L 45/745 (2013.01)
H04L 63/0823 (2013.01)
H04W 12/06 (2013.01)
H04W 40/24 (2013.01)
H04W 80/045 (2013.01)
H04W 84/18 (2013.01)

명 세 서

청구범위

청구항 1

제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스로서,

트랜시버를 포함하고, 데이터그램 전송 계층 보안(DTLS; Datagram Transport Layer Security) 세션을 상기 제 2 전자 디바이스와의 무선 통신을 통해 확립하여 상기 전자 디바이스로 하여금 상기 무선 메시 네트워크에 조인하게 하기 위해서 상기 무선 메시 네트워크의 상기 제 2 전자 디바이스와 통신하도록 구성된 네트워크 인터페이스를 포함하고,

상기 네트워크 인터페이스는:

암호 슈트(suite) 및 키에 기초한 제 2 키를 생성하고, 후속 통신에서 상기 제 2 키를 활용하고;

상기 DTLS 세션의 확립에 응답하여, 상기 네트워크 인터페이스를 통해 네트워크 키를 수신하고 - 상기 네트워크 키는 상기 무선 메시 네트워크와 연관됨 -; 그리고

상기 네트워크 키를 활용하여 상기 무선 메시 네트워크에서 디바이스들과 통신하도록 추가로 구성되고,

상기 DTLS 세션은, 상기 암호 슈트 및 상기 키에 기초하여 상기 무선 메시 네트워크를 통해 확립되고, 상기 전자 디바이스와 상기 제 2 전자 디바이스는 상기 키에 기초하여 상기 암호 슈트를 활용하는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 2

제 1 항에 있어서,

상기 키는, 공중 키, 사설 키, 또는 상기 전자 디바이스와 상기 제 2 전자 디바이스 간의 통신을 확립하는 비밀 키를 결정하는데 사용되는, 이들의 임의의 조합을 포함하는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 3

제 1 항에 있어서,

상기 키는, 상기 DTLS 세션을 확립하기 전에 상기 전자 디바이스에 저장되는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 4

제 1 항에 있어서,

상기 네트워크 인터페이스는, 안전한 통신 채널이 확립된 후 제 2 키를 수신하도록 구성되는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 5

제 1 항에 있어서,

상기 전자 디바이스는, 상기 전자 디바이스 또는 상기 제 2 전자 디바이스 중 적어도 하나로부터 상기 키의 수신에 응답하여 제 2 키를 생성하기 위해 상기 암호 슈트를 활용하는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 6

제 1 항에 있어서,

상기 제 1 전자 디바이스와 상기 제 2 전자 디바이스 간의 차후의 통신들은 제 2 키를 활용하여 암호화되는, 제

2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 7

제 6 항에 있어서,

상기 제 2 키는 통신을 확립하기 위한 세션 키를 포함하는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 8

제 6 항에 있어서,

상기 제 2 키는 상기 제 1 전자 디바이스 또는 상기 제 2 전자 디바이스에 저장되는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 9

제 1 항에 있어서,

상기 무선 메시 네트워크는 저전력 무선 표준을 이용하고, 상기 저전력 무선 표준은 효율적인 저전력 무선 개인 네트워크(ELoWPAN; efficient low power wireless personal network) 표준을 포함하는, 제 2 전자 디바이스를 지닌 무선 메시 네트워크에 조인하도록 구성된 전자 디바이스.

청구항 10

전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법으로서,

데이터그램 전송 계층 보안(DTLS; Datagram Transport Layer Security) 세션을 확립하여 상기 전자 디바이스로 하여금 상기 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 트랜시버를 포함하는 네트워크 인터페이스를 이용하여 상기 무선 메시 네트워크의 제 2 전자 디바이스와, 상기 전자 디바이스의 네트워크 인터페이스를 통해 무선으로 통신하는 단계;

암호 슈트 및 키에 기초한 제 2 키를 생성하고, 후속 통신에서 상기 제 2 키를 활용하는 단계;

상기 확립에 응답하여, 상기 네트워크 인터페이스를 통해 네트워크 키를 수신하는 단계 - 상기 네트워크 키는 상기 무선 메시 네트워크와 연관됨 -; 및

상기 네트워크 키를 활용하여 상기 무선 메시 네트워크에서 다른 디바이스와 통신하는 단계

를 포함하고,

상기 DTLS 세션은, 상기 암호 슈트 및 상기 키에 기초하여 상기 무선 메시 네트워크를 통해 확립되고, 상기 전자 디바이스와 상기 제 2 전자 디바이스는 상기 키에 기초하여 상기 암호 슈트를 활용하는, 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법.

청구항 11

제 10 항에 있어서,

상기 전자 디바이스 또는 상기 제 2 전자 디바이스 중 적어도 하나로부터의 상기 키의 수신에 응답하여 제 2 키를 생성하기 위해 상기 암호 슈트를 활용하는 단계를 포함하는, 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법.

청구항 12

제 10 항에 있어서,

상기 제 1 전자 디바이스와 상기 제 2 전자 디바이스 간의 차후의 통신들을 제 2 키를 통해 암호화하는 단계를 포함하는, 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법.

청구항 13

제 12 항에 있어서,

상기 제 2 키는 통신을 확립하기 위한 세션 키를 포함하는, 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법.

청구항 14

제 10 항에 있어서,

상기 무선 메시 네트워크는 IEEE 802.15.4 표준에 기초하는 저전력 무선 표준을 이용하는, 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 상기 전자 디바이스의 통신을 인증하는 방법.

청구항 15

명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체로서,

상기 명령들은,

전자 디바이스의 트랜시버를 포함하는 네트워크 인터페이스를 이용하여, 데이터그램 전송 계층 보안(DTLS; Datagram Transport Layer Security) 세션을 무선 통신을 통해 확립하여 상기 전자 디바이스로 하여금 무선 메시 네트워크에 조인하게 하기 위해서 무선 메시 네트워크의 제 2 전자 디바이스와, 상기 전자 디바이스의 네트워크 인터페이스를 통해 무선으로 통신하고;

암호 슈트 및 키에 기초한 제 2 키를 생성하고, 후속 통신에서 상기 제 2 키를 활용하고;

상기 DTLS 세션의 확립에 응답하여, 상기 네트워크 인터페이스를 통해 네트워크 키를 수신하고 - 상기 네트워크 키는 상기 무선 메시 네트워크와 연관됨 -; 그리고

상기 네트워크 키를 활용하여 상기 무선 메시 네트워크에서 디바이스들과 통신하도록 구성되고,

상기 DTLS 세션은, 상기 암호 슈트 및 상기 키에 기초하여 상기 무선 메시 네트워크를 통해 확립되고, 상기 전자 디바이스와 상기 제 2 전자 디바이스는 상기 키에 기초하여 상기 암호 슈트를 활용하는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 16

제 15 항에 있어서,

상기 키는, 공중 키, 사설 키, 또는 상기 전자 디바이스와 상기 제 2 전자 디바이스 간의 통신을 확립하는 비밀 키를 결정하는데 사용되는, 이들의 임의의 조합을 포함하는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 17

제 15 항에 있어서,

상기 키는 상기 DTLS 세션을 확립하기 전에 상기 전자 디바이스에 저장되는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 18

제 15 항에 있어서,

상기 전자 디바이스는, 상기 전자 디바이스 또는 상기 제 2 전자 디바이스 중 적어도 하나로부터 상기 키의 수신에 응답하여 제 2 키를 생성하기 위해 상기 암호 슈트를 활용하는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 19

제 15 항에 있어서,

상기 제 1 전자 디바이스와 상기 제 2 전자 디바이스 간의 차후의 통신들은 제 2 키를 활용하여 암호화되는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

청구항 20

제 15 항에 있어서,

상기 무선 메시 네트워크는 저전력 무선 표준을 이용하고, 상기 저전력 무선 표준은, LR-WPAN(low-rate wireless personal area network)들에 대응하는 IEEE 802.15.4 네트워크에 기초하는 효율적인 저전력 무선 개인 네트워크(ELoWPAN) 표준을 포함하는, 명령들을 포함하는 비일시적 컴퓨터 판독가능 저장 매체.

발명의 설명

배 경 기 술

[0001]본 섹션은 본 기술의 다양한 양상들과 관련될 수 있는 다양한 기술의 양상들에 대해 독자에게 소개하려는 것이며, 본 기술은 아래에서 설명되고 그리고/또는 청구된다. 본 논의는 본 개시물의 다양한 양상들의 보다 양호한 이해를 돕기 위한 배경 정보를 독자에게 제공하는 것을 도울 것으로 여겨진다. 따라서, 이러한 언급들이 이러한 견지에서 기재된 것으로서, 종래 기술의 인정으로서 기재된 것이 아니라는 것을 이해해야 한다.

[0002]현재, 수많은 전자 디바이스들이 무선 네트워크들로 연결될 수 있다. 예를 들어, 스마트 계량기 기술은 거주자 특성들과 연관된 전기 에너지 소비 데이터를 모니터링, 과금 등을 위한 유틸리티로 다시 통신시키기 위한 무선 네트워크를 사용한다. 이와 같이, 전자 디바이스들이 서로 통신할 수 있게 하는 다수의 무선 네트워킹 표준들이 현재 이용가능하다. 일부 스마트 계량기 구현들은, 예를 들어, 전자 디바이스들로 하여금 스마트 계량기와 통신할 수 있게 하기 위해서 6LoWPAN(employ Internet Protocol version 6 (IPv6) over Low power Wireless Personal Area Network)들을 채용한다. 그러나, 6LoWPAN과 같이 현재 이용가능한 무선 네트워킹 표준들은 일반적으로, 하나 이상의 실질적인 시나리오들의 경우 거주지나 집 전체에 걸쳐 배치된 전자 디바이스들을 지원하도록 제대로 장착되어 있지 않을 수 있다. 즉, 현재 이용가능한 무선 네트워킹 표준들은, 하나 이상의 알려진 실질적인 제약들을 고려하여 안전하면서도 단순한 소비자 친화적인 방식으로 네트워크들의 모든 전자 디바이스들을 효율적으로 연결하지 않을 수 있다. 또한, 하나 이상의 실제 시나리오들의 경우, 현재 이용가능한 무선 네트워킹 표준들은 새로운 전자 디바이스들을 애드 혹 방식으로 기존의 무선 네트워크에 추가시키는 효율적인 방식을 제공하지 않을 수 있다.

[0003]추가적으로, 집에서 그리고 집 주변에서 사용하기 위한 전자 디바이스들을 위한 무선 네트워크 표준을 제공할 경우, 상이한 디바이스들이 네트워크에 액세스하는 방법을 학습하는 오픈 프로토콜을 제공하는 무선 네트워크 표준을 사용하는 것이 유리할 것이다. 또한, 홈과 연관될 수 있는 전자 디바이스들의 수가 주어지면, 각각의 디바이스가 고유 IP 어드레스를 가질 수 있고 인터넷을 통해, 홈 환경의 로컬 네트워크 등을 통해 액세스될 수 있도록 무선 네트워크 표준이 IPv6(Internet Protocol version 6) 통신을 지원할 수 있다는 점에서 유리할 것이다. 또한, 전자 디바이스들이 최소의 전력량을 이용하여 무선 네트워크 내에서 통신하게 하는 무선 네트워크 표준이 유리할 것이다. 이러한 특징들을 염두에 두면서, 오픈 프로토콜을 구비하고 집안 그리고 집 주변의 전자 디바이스들 용으로 사용될 수 있는 저전력, IPv6-기반 무선 메시 네트워크 표준을 제공하는 맥락에서 각각의 알려진 현재 이용가능한 무선 네트워킹 표준에 의해 하나 이상의 단점들이 제시된다는 것을 생각한다. 예를 들어, Bluetooth®, Dust Networks®, Z-wave®, WiFi, 및 ZigBee®와 같은 무선 네트워크 표준들은 상기 언급된 원하는 특징들 중 하나 이상의 것을 제공하는 데에 실패했다.

[0004]예를 들어, Bluetooth®는 일반적으로, 단파장 무선 송신들을 통해 단거리에 걸쳐 통신하기 위한 무선 네트워크 표준을 제공한다. 이와 같이, Bluetooth®의 무선 네트워크 표준은 집 전체에 걸쳐 배치된 다수의 전자 디바이스들의 통신 네트워크를 지원하지 않을 수 있다. 더욱이, Bluetooth®의 무선 네트워크 표준은 무선 메시 통신 또는 IPv6 어드레스들을 지원하지 않을 수 있다.

[0005]상기 언급된 바와 같이, Dust Networks®에 의해 제공된 무선 네트워크 표준은 또한, 집에 배치되어 있는 전자 디바이스들이 서로 효율적으로 통신할 수 있게 하는 하나 이상의 특징들에 대해 하나 이상의 단점들을 가져올 수 있다. 특히, Dust Networks® 무선 네트워크 표준은 Dust Networks®의 네트워크에서 동작하는 디바이스들과 인터페이싱하기 위해 다른 것들에 의해 사용될 수 있는 오픈 프로토콜을 제공하지 않을 수 있다. 대신, Dust Networks®는 조립 라인들, 화학 공장들 등과 같은 산업 환경들에 위치된 디바이스들 간의 통신을 용이하

게 하도록 설계될 수 있다. 이와 같이, Dust Networks® 무선 네트워크 표준은, 각각의 디바이스가 다른 디바이스들로 통신하고 다른 디바이스들로부터의 명령들을 청취할 수 있는 미리정의된 시간 윈도우들을 갖는 신뢰할 수 있는 통신 네트워크를 제공하는 것에 관한 것일 수 있다. 이러한 방식으로, Dust Networks® 무선 네트워크 표준은, 집에서 사용하기 위한 가전 기기 디바이스들로 구현하기에는 경제적이지 않을 수 있는 정교하고 상대적으로 값비싼 무선 송신기들을 요구할 수 있다.

[0006]Dust Networks® 무선 네트워크 표준과 같이, Z-wave®과 연관된 무선 네트워크 표준은 오픈 프로토콜이 아닐 수 있다. 대신, Z-wave® 무선 네트워크 표준은, 특정 트랜시버 칩을 그의 디바이스에 임베딩한 허가된 클라이언트들에 대해서만 이용가능할 수 있다. 더욱이, Z-wave® 무선 네트워크 표준은 IPv6-기반 통신을 지원하지 않을 수 있다. 즉, Z-wave® 무선 네트워크 표준은 Z-wave® 디바이스 상에서 생성된 데이터를 인터넷을 통해 송신될 수 있는 IP-기반 데이터로 트랜슬레이팅하기 위한 브리지 디바이스를 필요로 할 수 있다.

[0007]이제, Z-wave® 무선 네트워크 표준들을 참고하면, Z-wave®는 ZigBee® Pro 및 ZigBee® IP로 흔히 알려진 2개의 표준들을 갖는다. 또한, ZigBee® Pro는 무선 메시 네트워킹에 대한 지원의 맥락에서 하나 이상의 단점들을 가질 수 있다. 대신, ZigBee® Pro는 ZigBee® Pro 네트워크의 각각의 디바이스 간의 통신을 용이하게 하는 중앙 디바이스에 적어도 부분적으로 의존할 수 있다. 이 중앙 디바이스에 대한 증가하는 전력 요건들에 부가하여, 특정 무선 트래픽을 프로세싱하거나 또는 리젝팅하기 위해 온 상태로 있는 디바이스들은 디바이스들의 하우징들 내부에 추가 열을 발생시킬 수 있으며, 이는 디바이스에 의해 획득되는 온도 검침값들과 같은 일부 센서 검침값들을 변경시킬 수 있다. 이러한 센서 검침값들은 집안의 각각의 디바이스가 동작할 수 있는 방법을 결정하는 데에 유용할 수 있기 때문에, 센서 검침값들을 변경시킬 수 있는 디바이스 내부에서 불필요한 열 발생을 방지하는데 유리할 수 있다. 추가로, ZigBee® Pro는 IPv6 통신을 지원하지 않을 수 있다.

[0008]이제 ZigBee® IP를 참고하면, ZigBee® IP는 직접 디바이스-투-디바이스 통신의 맥락에서 하나 이상의 단점들을 가져올 수 있다. ZigBee® IP는 중앙 라우터 또는 디바이스로 디바이스 데이터를 중계함으로써 통신의 촉진에 관한 것이다. 이와 같이, 중앙 라우터 또는 디바이스는 일정한 전력공급을 요구할 수 있고 따라서 디바이스들 사이에서 통신하기 위한 저전력 수단을 제공하지 않을 수 있다. 더욱이, ZigBee® IP는 하나의 네트워크에서 사용될 수 있는 노드들의 수(즉, 네트워크 당 ~20 노드들)에 실질적인 한계를 가질 수 있다. 추가로, ZigBee® IP는, 각각의 ZigBee® IP 연결식 디바이스에 대해 추가 전력을 암시할 수 있는 고 대역폭, 프로세싱, 및 메모리 요건들을 나타낼 수 있는 RPL("Ripple" routing protocol)을 사용한다.

[0009]상기 언급된 ZigBee® 무선 네트워크 표준들과 같이, WiFi의 무선 네트워크는 저전력 요건들을 갖는 디바이스들 중에서 통신들을 가능하게 한다는 점에서 하나 이상의 단점들을 나타낼 수 있다. 예를 들어, WiFi의 무선 네트워크 표준은 또한 각각의 네트워크 디바이스가 항상 전원이 켜진 상태로 있을 것을 요구할 수 있고, 더욱이 중앙 노드 또는 허브의 존재를 요구할 수 있다. 본 기술에서 알려진 바와 같이, WiFi는 비교적 높은 대역폭 데이터 송신들(예를 들어, 스트리밍 비디오, 싱킹(syncing) 디바이스들)에 대해 이상적일 수 있는 상대적 공통 무선 네트워크 표준이다. 이와 같이, WiFi 디바이스들은 통상적으로, 디바이스들 간의 데이터 송신들의 일정한 스트림을 지원하는 연속식 전원 또는 재충전가능한 배터리들에 결합된다. 또한, WiFi의 무선 네트워크는 무선 메시 네트워킹을 지원하지 않을 수 있다.

발명의 내용

[0010]본원에 개시된 특정 실시예들의 요약이 아래에 제시된다. 이러한 양상들은 단지 이러한 특정 실시예들의 간단한 요약을 독자에게 제공하며 이러한 양상들은 이러한 개시물의 범위를 제한하도록 의도되지 않는다는 것을 이해해야 한다. 실제로, 본 개시물은 아래에 제시되지 않을 수 있는 다양한 양상들을 포함할 수 있다.

[0011]본 개시물의 실시예들은, 전자 디바이스가 동일한 건물 내에 배치된 다른 전자 디바이스와 무선으로 통신할 수 있도록 빌딩(예를 들어, 집 또는 사무실)에 배치될 수 있는 온도 조절 장치와 같은 전자 디바이스에 관한 것이다. 일 실시예에서, 전자 디바이스는, 전자 디바이스로 하여금 그 전자 디바이스를 무선 메시 네트워크를 통해 다른 전자 디바이스에 무선으로 결합하게 할 수 있는 네트워크 인터페이스를 포함할 수 있다. 전자 디바이스는 또한, 라우팅 정보 프로토콜-차세대(RIPng; Routing Information Protocol-Next Generation) 라우팅 메커니즘 및 네트워크 인터페이스를 이용하여 무선 메시 네트워크를 경유하는 다른 전자 디바이스에 대한 적어도 하나의 데이터 경로를 결정할 수 있는 프로세서를 포함할 수 있다. 다른 전자 디바이스에 대한 적어도 하나의 데이터 경로를 식별한 후, 프로세서는, 식별된 데이터 경로(들)가 데이터그램 전송 계층 보안(Datagram Transport Layer Security) 프로토콜을 이용하여 안전한지 여부를 결정할 수 있다. 식별된 데이터 경로(들)가 안전한 것으로 결정되는 경우, 프로세서는 안전한 데이터 경로(들)를 통해 IPv6(Internet Protocol version 6)

데이터 패킷들을 다른 전자 디바이스로 전송할 수 있다. 그 결과, 전자 디바이스는 그 자신과 비교적 사용자 입력이 거의 없는 동일한 건물 내에 배치된 다른 전자 디바이스 간의 안전한 통신 네트워크를 확립할 수 있다.

[0012]상기 언급된 특징들의 다양한 개선점들이 본 개시물의 다양한 양상들과 관련하여 존재할 수 있다. 추가 특징들이 또한 마찬가지로 이러한 다양한 양상들에 포함될 수 있다. 이러한 개선점들 및 추가 특징들은 개별적으로 또는 임의의 조합으로 존재할 수 있다. 예를 들어, 예시된 실시예들 중 하나 이상의 것과 관련하여 아래에 논의된 다양한 특징들은 본 개시물의 상술된 양상들 중 어느 양상 단독으로 또는 이들의 임의의 조합으로 포함될 수 있다. 상기 제시된 간단한 요약은 독자들이 본 개시물의 실시예들의 특정 양상들 및 맥락들에 익숙해지게 하도록 의도될 뿐, 청구범위로 제한하는 것으로 의도되지 않는다.

도면의 간단한 설명

[0013]본 개시물의 다양한 양상들은 다음의 상세한 설명을 읽고 도면들을 참고하면서 더욱 잘 이해될 수 있다.

[0014]도 1은, 일 실시예에 따른 효율적인 네트워크 계층 프로토콜을 이용하여 홈 환경에 배치된 다른 디바이스들과 통신할 수 있는 일반적 디바이스의 블록도를 도시한다.

[0015]도 2는, 일 실시예에 따른, 도 1의 일반 디바이스가 효율적인 네트워크 계층 프로토콜을 통해 다른 디바이스들과 통신할 수 있는 홈 환경의 블록도를 도시한다.

[0016]도 3은, 일 실시예에 따른, 도 2의 홈 환경에 도시된 디바이스들과 연관된 예시적인 무선 메시 네트워크를 도시한다.

[0017]도 4는, 일 실시예에 따른, 도 2의 홈 환경을 위한 통신 시스템을 특징으로 하는 OSI(Open Systems Interconnection) 모델의 블록도를 도시한다.

[0018]도 5는, 일 실시예에 따른, 도 4의 OSI 모델의 효율적인 네트워크 계층의 상세도를 도시한다.

[0019]도 6은, 일 실시예에 따른, 도 5의 효율적인 네트워크 계층의 라우팅 메커니즘으로서 RIPng(Routing Information Protocol - Next Generation) 네트워크를 구현하는 방법의 흐름도를 도시한다.

[0020]도 7a 내지 도 7d는, 일 실시예에 따른 도 6의 방법의 RIPng 네트워크가 구현될 수 있는 방법의 예를 도시한다.

[0021]도 8은, 일 실시예에 따른, 보안 증명서를 도 1의 일반적인 디바이스에 임베딩하는 것을 포함하는 제조 프로세스의 블록도를 도시한다.

[0022]도 9는, 일 실시예에 따른, 도 5의 효율적인 네트워크 계층에서 데이터그램 전송 계층 보안(DTLS) 프로토콜을 이용하는 도 2의 홈 환경의 디바이스들 간의 예시적인 핸드쉐이크 프로토콜을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0023]본 개시물의 하나 이상의 특정 실시예들이 아래에 설명될 것이다. 이러한 설명된 실시예들은 현재 개시된 기술들의 예들일 뿐이다. 추가로, 이러한 실시예들의 간결한 설명을 제공하기 위한 일환으로, 실제 구현의 모든 특징들이 본 명세서에 설명되지 않을 수 있다. 임의의 이러한 실제 구현의 개발 시, 임의의 엔지니어링 또는 설계 프로젝트에서와 같이, 수많은 구현-특정 결정들은, 구현들 간에 변할 수 있는 시스템-관련 및 비지니스-관련 제약들을 준수하며 개발자의 특정 목적들을 달성하기 위해서 이루어져야 한다는 것을 인식해야 한다. 더욱이, 이러한 개발 노력은 복잡하고 시간을 많이 소모하지만, 그럼에도 불구하고 본 개시물의 이점을 갖는 당업자들에게는 설계, 제조 및 제조의 일상적인 업무일 수 있다는 것을 인식해야 한다.

[0024]본 개시물의 다양한 실시예들의 엘리먼트들을 도입할 때, 단수 표현이 엘리먼트들 중 하나 이상의 것이 존재한다는 것을 의미하도록 의도된다. 용어는 "구비하는", "포함하는" 및 "갖는"은 포괄적인 것이고 나열된 엘리먼트들 이외에 추가 엘리먼트들이 존재할 수 있다는 것을 의미하도록 의도된다. 추가로, 본 개시물의 "일 실시예" 또는 "실시예"에 대한 언급들은, 언급된 특징들을 또한 포함하는 추가 실시예들의 존재를 배제하는 것으로 해석되는 것을 의도하지 않는다는 것을 이해해야 한다.

[0025]본 개시물의 실시예들은 일반적으로, 홈 환경에서 서로 통신하고 있는 디바이스들에 의해 사용될 수 있는 효율적인 네트워크 계층에 관한 것이다. 일반적으로, 집에 거주하는 소비자들은, 이들의 디바이스들 모두가 효율적으로 동작하도록 그들의 집안에서 다양한 디바이스들의 동작을 조정하는 것이 유익하다는 것을 알 수 있다.

예를 들어, 온도 조절 디바이스는 집의 온도를 검출하고 검출된 온도에 기초하여 다른 디바이스들(예를 들어, 조명들)의 액티비티를 조정하기 위해 사용될 수 있다. 이 예에서, 온도 조절 디바이스는 집 밖의 온도가 일광 시간들에 대응한다는 것을 나타낼 수 있는 온도를 검출할 수 있다. 온도 조절 디바이스가 이후, 집에 이용가능한 일광이 있을 수 있고 따라서 조명을 턴 오프해야 한다는 것을 조명 디바이스로 전달할 수 있다.

[0026]그들의 디바이스들을 효율적으로 동작시키는 것 이외에, 소비자들은 일반적으로, 최소량의 셋업 또는 초기화를 수반하는 사용자-친화적 디바이스들을 사용하기를 선호한다. 즉, 소비자들은 일반적으로, 연령이나 기술적 전문지식과 무관하게 거의 모든 개인이 수행할 수 있는 소수의 초기화 단계들을 수행한 후 전적으로 작동하는 디바이스들을 구매하기 선호할 것이다.

[0027]이점을 염두에 두면서, 디바이스들로 하여금 최소의 사용자 관여로 홈 환경 내에서 서로 간에 데이터를 효율적으로 통신하게 하기 위해서, 디바이스들은 이들의 통신을 관리하기 위해 효율적인 네트워크 계층을 사용할 수 있다. 즉, 효율적인 네트워크 계층은, 집안의 수많은 디바이스들이 무선 메시 네트워크를 통해 서로 통신할 수 있는 통신 네트워크를 확립할 수 있다. 통신 네트워크가 인터넷 프로토콜 버전 6(IPv6) 통신을 지원할 수 있으므로, 각각의 연결된 디바이스는 고유 인터넷 프로토콜(IP) 어드레스를 가질 수 있다. 더욱이, 각각의 디바이스가 집에 통합될 수 있게 하기 위해서, 각각의 디바이스가 낮은 전력량을 이용하여 네트워크 내에서 통신하는 것이 유용할 수 있다. 즉, 디바이스들이 저 전력을 이용하여 통신할 수 있게 함으로써, 디바이스들은 연속 전원에 결합되지 않고 집안 어디에도 배치될 수 있다.

[0028]효율적인 네트워크 계층은 이와 같이, 데이터가 2개 또는 그보다 많은 디바이스들 간에 전달될 수 있는 절차를 확립할 수 있으므로, 통신 네트워크의 확립이 사용자 입력을 거의 수반하지 않고, 디바이스들 간의 통신이 에너지를 거의 수반하지 않으며, 통신 네트워크 그 자체가 안전하다. 일 실시예에서, 효율적인 네트워크 계층은, 그의 라우팅 메커니즘으로서 RIPng(Routing Information Protocol-Next Generation)를 채용하고 그의 보안 메커니즘으로서 데이터그램 전송 계층 보안(DTLS) 프로토콜을 사용할 수 있는 IPv6-기반 통신 네트워크일 수 있다. 이와 같이, 효율적인 네트워크 계층은, 연결된 디바이스들 사이에서 통신된 정보를 보호하면서 디바이스들을 집에 추가하거나 또는 제거하기 위한 단순한 수단을 제공할 수 있다.

[0029]도입부로서, 도 1은 홈 환경 안에 있는 다른 유사한 디바이스들과 통신할 수 있는 일반 디바이스(10)의 예를 도시한다. 일 실시예에서, 디바이스(10)는 하나 이상의 센서들(12), 사용자-인터페이스 컴포넌트(14), 전원(16)(예를 들어, 전원 연결 및/또는 배터리를 포함함), 네트워크 인터페이스(18), 프로세서(20) 등을 포함할 수 있다. 특정 센서들(12), 사용자-인터페이스 컴포넌트들(14), 및 전원 구성들은 각각의 디바이스들(10)과 동일할 수도 또는 유사할 수도 있다. 그러나, 일부 실시예들에서, 각각의 디바이스(10)는, 디바이스 타입 또는 모델에 기초하여 특정 센서들(12), 사용자-인터페이스 컴포넌트들(14), 전원 구성들 등을 포함할 수 있다는 것을 주목해야 한다.

[0030]특정 실시예에서, 센서들(12)은 가속도, 온도, 습도, 물, 공급되는 전력, 근접성, 외부 모션, 디바이스 모션, 사운드 신호들, 초음파 신호들, 광 신호들, 화재, 연기, 일산화탄소, GPS(global-positioning-satellite) 신호들, RF(radio-frequency), 다른 전자기적 신호들 또는 필드들 등과 같은 다양한 특성들을 검출할 수 있다. 이와 같이, 센서들(12)은 온도 센서(들), 습도 센서(들), 위험-관련 센서(들) 또는 다른 환경 센서(들), 가속도계(들), 마이크로폰(들), 카메라(들)(예를 들어, 전하 결합 디바이스 또는 비디오 카메라들)을 포함하는 광학 센서들, 능동적 또는 수동적 방사 센서들, GPS 수신기(들) 또는 라디오주파수 식별 검출기(들)을 포함할 수 있다. 도 1이 하나의 센서를 이용하는 실시예를 도시하지만, 많은 실시예들은 다수의 센서들을 포함할 수 있다. 일부 예시들에서, 디바이스(10)는 하나 이상의 주된 센서들과 하나 이상의 보조 센서들을 포함할 수 있다. 여기서, 주(primary) 센서(들)은 디바이스의 핵심 동작에 중심이 되는 데이터(예를 들어, 온도 조절 장치에서 온도를 감지하는 것 또는 연기 검출기에서 연기를 감지하는 것)를 감지할 수 있는 반면, 보조 센서(들)는 에너지-효율의 목적들 또는 스마트-동작 목적들을 위해 사용될 수 있는 다른 타입의 데이터(예를 들어, 모션, 광 또는 소리)를 감지할 수 있다.

[0031]디바이스(10) 내의 하나 이상의 사용자-인터페이스 컴포넌트들(14)은 사용자로부터 입력을 수신하고 그리고/또는 정보를 사용자에게 제공할 수 있다. 수신된 입력은 셋팅을 결정하는 데에 사용될 수 있다. 특정 실시예들에서, 사용자-인터페이스 컴포넌트들은 사용자의 움직임에 응답하는 기계적 또는 가상 컴포넌트를 포함할 수 있다. 예를 들어, 사용자는 슬라이딩 컴포넌트를 (예를 들어, 수직 또는 수평 트랙을 따라) 기계적으로 이동시키거나 또는 회전가능한 고리를 (예를 들어, 원형 트랙을 따라) 기계적으로 회전시킬 수 있거나, 또는 터치 패드를 따라 사용자의 움직임이 검출된 수 있다. 이러한 움직임들은, 사용자-인터페이스 컴포넌트(104)의 절대

포지션에 기초하여 또는 사용자 인터페이스 컴포넌트들(104)의 변위에 기초하여 결정될 수 있는 셋팅 조정(예를 들어, 회전가능한 고리 컴포넌트가 10° 회전할 때마다 1° F씩 세트 포인트 온도를 조정하는 것)에 대응할 수 있다. 물리적으로 그리고 가상적으로 이동가능한 사용자-인터페이스 컴포넌트들은 사용자로 하여금 명백한 연속체(continuum)의 일 부분을 따라 셋팅을 설정하게 할 수 있다. 이와 같이, 사용자는, (예를 들어, 상하 버튼들이 사용되었던 경우와 같이) 2개의 별개의 옵션들 사이에서 선택하도록 한정되지 않을 수 있지만, 가능한 셋팅 값들의 범위를 따라 셋팅을 신속하고 직관적으로 정의할 수 있다. 예를 들어, 사용자-인터페이스 컴포넌트의 움직임의 크기는 셋팅 조정의 크기와 연관될 수 있으므로, 사용자는 큰 움직임으로 셋팅을 극적으로 변경할 수 있거나 또는 작은 움직임으로 셋팅을 미세하게 튜닝할 수 있다.

[0032]사용자-인터페이스 컴포넌트들(14)은 또한, 하나 이상의 버튼들(예를 들어, 상하 버튼들), 키패드, 숫자패드, 스위치, 마이크로폰, 및/또는 (예를 들어, 제스처들을 검출하는) 카메라를 포함할 수 있다. 일 실시예에서, 사용자-인터페이스 컴포넌트(14)는 (예를 들어, 셋팅을 조정하기 위해서) 고리를 회전시킴으로써 그리고/또는 (예를 들어, 조정된 셋팅을 선택하거나 또는 옵션을 선택하기 위해서) 고리를 안쪽으로 클릭함으로써 사용자가 컴포넌트와 상호작용하게 할 수 있는 클릭-앤드-회전 원형 고리 컴포넌트를 포함할 수 있다. 다른 실시예에서, 사용자-인터페이스 컴포넌트(14)는 (예를 들어, 디바이스의 전력 또는 알람 상태가 변경되었음을 나타내기 위해) 제스처들을 검출할 수 있는 카메라를 포함할 수 있다. 일부 예들에서, 디바이스(10)는, 복수의 타입들의 셋팅들을 설정하기 위해 사용될 수 있는 하나의 주(primary) 입력 컴포넌트를 구비할 수 있다. 사용자-인터페이스 컴포넌트들(14)은 또한, 예를 들어, 시각적 디스플레이(예를 들어, 박막-트랜지스터 디스플레이 또는 유기 발광 다이오드 디스플레이) 및/또는 오디오 스피커를 통해 사용자에게 정보를 제공하도록 구성될 수 있다.

[0033]전원 컴포넌트(16)는 파워 연결 및/또는 로컬 배터리를 포함할 수 있다. 예를 들어, 파워 연결은 디바이스(10)를 배선 전압원과 같은 전원에 연결시킬 수 있다. 일부 예들에서, (예를 들어, 재충전가능한) 로컬 배터리를 반복적으로 충전하기 위해서 AC 전원이 사용될 수 있으므로, AC 전원이 사용가능하지 않을 경우 디바이스(10)에 전력을 공급하기 위한 배터리는 나중에 사용될 수 있다.

[0034]네트워크 인터페이스(18)는, 디바이스(10)로 하여금 디바이스들 간에 통신을 할 수 있게 하는 컴포넌트를 포함할 수 있다. 일 실시예에서, 네트워크 인터페이스(18)는 그의 OSI(Open Systems Interconnection) 모델의 부분으로서 효율적인 네트워크 계층을 이용하여 통신할 수 있다. 일 실시예에서, 도 5을 참고하여 아래에 보다 상세하게 설명될 효율적인 네트워크 계층은 디바이스(10)로 하여금 RIPng 라우팅 메커니즘과 DTLS 보안 방식을 이용하여 IPv6-타입 데이터 또는 트래픽을 무선으로 통신하게 할 수 있다. 이와 같이, 네트워크 인터페이스(18)는 무선 카드 또는 일부 다른 트랜시버 연결을 포함할 수 있다.

[0035]프로세서(20)는 다양한 상이한 디바이스 기능들 중 하나 이상의 기능들을 지원할 수 있다. 이와 같이, 프로세서(20)는 본원에 설명된 기능들 중 하나 이상의 기능들을 실행하고 그리고/또는 실행하게 하도록 구성되고 프로그래밍된 하나 이상의 프로세서들을 포함할 수 있다. 일 실시예에서, 프로세서(20)는, 로컬 메모리(예를 들어, 플래시 메모리, 하드 드라이브, 랜덤 액세스 메모리), 특수 목적 프로세서들 또는 주문형 집적 회로들, 이들의 조합에 저장되는 컴퓨터 코드를 실행하고 그리고/또는 다른 타입들의 하드웨어/펌웨어/소프트웨어 프로세싱 플랫폼들을 이용하는 범용 프로세서들을 포함할 수 있다. 추가로, 프로세서(20)는 중앙 서버들 또는 클라우드-기반 시스템들, 이를 테면, AJAX(Asynchronous JavaScript and XML) 또는 유사한 프로토콜들을 이용하여 클라우드 서버로부터 제공된 명령들을 실행하는 JVM(Java virtual machine)의 실행에 의해 원격적으로 실행되거나 또는 지배되는 알고리즘들의 로컬화된 버전들 또는 이와 대응관계에 있는 알고리즘들로서 구현될 수 있다. 예로서, 프로세서(20)는, 로케이션(예를 들어, 하우스 또는 룸)이 (예를 들어, 하나 이상의 임계치들과 관련하여) 특정수의 사람들에 의해 점유되거나 또는 특정인에 의해 점유되는지 여부를 비롯하여 점유된 시기를 검출할 수 있다. 일 실시예에서, 본 검출은, 예를 들어, 마이크로폰 신호들을 분석하는 것, (예를 들어, 디바이스 앞의) 사용자 움직임들을 검출하는 것, 문들 또는 차고 문들의 열림과 닫힘을 검출하는 것, 무선 신호들을 검출하는 것, 수신된 신호의 IP 어드레스를 검출하는 것, 시간 윈도우 내에서 하나 이상의 디바이스들의 동작을 검출하는 것 등에 의해 발생할 수 있다. 또한, 프로세서(20)는 특정 점유자들 또는 오브젝트들을 식별하기 위한 이미지 인식 기술을 포함할 수 있다.

[0036]특정 실시예들에서, 프로세서(20)는 또한 고전력 프로세서 및 저전력 프로세서를 포함할 수 있다. 고전력 프로세서는 사용자 인터페이스 컴포넌트(14) 등을 동작시키는 것과 같은 계산 집약적인 연산들을 실행할 수 있다. 반면, 저전력 프로세서는, 위험이나 온도를 센서(12)로부터 검출하는 것과 같은 덜 복잡한 프로세스들을 관리할 수 있다. 일 실시예에서, 저전력 프로세서는 계산 집약적 프로세스들에 대한 고전력 프로세서를 웨이크

(wake)하거나 초기화할 수 있다.

[0037]일부 예들에서, 프로세서(20)는 바람직한 셋팅들을 예상하고 그리고/또는 이러한 셋팅들을 구현할 수 있다. 예를 들어, 존재 검출에 기초하여, 프로세서(20)는, 예를 들어, 집에 또는 특정한 룸에 아무도 없을 경우 전력을 절약하기 위해서 또는 사용자 선호들(예를 들어, 일반적인 집에서의 선호들 또는 사용자-특정 선호들)에 맞추기 위해 디바이스 셋팅들을 조정할 수 있다. 다른 예로서, 특정인, 동물이나 또는 오브젝트(예를 들어, 어린이, 애완동물 또는 분실물)의 검출에 기초하여, 프로세서(20)는 사람, 동물 또는 물건이 있는 장소의 청각적 또는 시각적 인디케이터를 개시할 수 있거나 또는 특정 조건들(예를 들어, 밤이나 조명이 꺼진 경우) 하에서 인정되지 않은 사람이 검출되는 경우 알람이나 보안 피처를 개시할 수 있다.

[0038]일부 예들에서, 디바이스들이 서로 상호작용할 수 있으므로 제 1 디바이스에 의해 검출된 이벤트가 제 2 디바이스의 동작들에 영향을 준다. 예를 들어, 제 1 디바이스는, (차고 안의 움직임을 검출하는 것, 차고 안의 조명의 변경을 검출하는 것, 또는 차고문의 열림을 검출하는 것에 의해) 사용자가 차고 안으로 들어갔음을 검출할 수 있다. 제 1 디바이스는 이러한 정보를 효율적인 네트워크 계층을 통해 제 2 디바이스로 전송할 수 있음으로써, 제 2 디바이스는, 예를 들어, 집 온도 셋팅, 조명 셋팅, 음악 셋팅, 및/또는 보안-알람 셋팅을 조정할 수 있다. 다른 예로서, 제 1 디바이스는 (예를 들어, 모션 또는 갑작스러운 조명 패턴 변경들의 검출에 의해) 사용자가 전면 문에 접근하는 것을 검출할 수 있다. 제 1 디바이스는, 예를 들어, (예를 들어, 도어벨의 소리와 같은) 일반적인 청각적 또는 시각적 신호가 제공되게 하거나 또는 (예를 들어, 사용자가 점유하고 있는 방안 방문자의 존재를 알리는) 위치-특정 청각적 또는 시각적 신호가 제공되게 할 수 있다.

[0039]예로서, 디바이스(10)는 Nest® 학습 온도 조절 장치(Learning Thermostat)와 같은 온도 조절 장치를 포함할 수 있다. 여기서, 온도 조절 장치는, 온도 센서들, 습도 센서들 등과 같은 센서들(12)을 포함할 수 있으므로, 온도 조절 장치는, 그 온도 조절 장치가 배치되는 건물 안의 현재 기후 조건들을 결정할 수 있다. 온도 조절 장치를 위한 전원 컴포넌트(16)는 로컬 배터리일 수 있으므로, 온도 조절 장치는 연속식 전원과 매우 가까운 곳에 위치되는 것을 고려하지 않고 빌딩 내 어디든지 배치될 수 있다. 로컬 배터리를 이용하여 온도 조절 장치에 전원이 공급되기 때문에, 온도 조절 장치는 그의 에너지 사용을 최소화할 수 있어서, 배터리가 거의 교체되지 않는다.

[0040]일 실시예에서, 온도 조절 장치는 사용자-인터페이스 컴포넌트(14)로서 상부에 배치되는 회전가능한 링을 구비할 수 있는 원형 트랙을 포함할 수 있다. 이와 같이, 사용자는 회전가능한 링을 이용하여 온도 조절 장치와 상호작용하거나 또는 온도 조절 장치를 프로그래밍할 수 있어, 온도 조절 장치는 난방, 환기 및 에어-컨디셔닝(HVAC; heating, ventilation, and air-conditioning) 유닛 등을 제어함으로써 빌딩의 온도를 제어한다. 일부 예들에서, 온도 조절 장치는, 그의 프로그래밍에 기초하여 빌딩이 비워질 수 있는 시기를 결정할 수 있다. 예를 들어, 온도 조절 장치는 연장된 시간 기간 동안 HVAC 유닛이 파워 오프된 상태를 유지하도록 프로그래밍될 수 있다면, 온도 조절 장치는, 빌딩이 이 시간 기간 동안 비게 될 것이라는 것을 결정할 수 있다. 여기서, 온도 조절 장치는, 빌딩이 비어있는 상태라는 것을 결정할 경우 조명 스위치들 또는 다른 전자 디바이스들을 턴 오프하도록 프로그램밍될 수 있다. 이와 같이, 온도 조절 장치는 조명 스위치 디바이스와 통신하기 위해 네트워크 인터페이스(18)를 사용할 수 있으므로, 온도 조절 장치는, 빌딩이 빈 것으로 결정될 경우 조명 스위치 디바이스에 신호를 전송할 수 있다. 이러한 방식으로, 온도 조절 장치는 빌딩의 에너지 사용을 효율적으로 관리할 수 있다.

[0041]앞의 내용을 염두에 두면서, 도 2는, 도 1의 디바이스(10)가 효율적인 네트워크 계층을 통해 다른 디바이스들과 통신할 수 있는 홈 환경(30)의 블록도를 도시한다. 도시된 홈 환경(30)은 하우스, 사무실 빌딩, 차고, 또는 모바일 홈과 같은 구조물(32)을 포함할 수 있다. 디바이스들은 또한, 전체 구조물(32), 이를 테면, 아파트, 콘도, 사무실 공간 등을 포함하지 않는 홈 환경에 통합될 수 있다는 것을 인식할 것이다. 추가로, 홈 환경(30)은 실제 구조물(32) 외부의 디바이스들을 제어하고 그리고/또는 그 디바이스들에 결합될 수 있다. 확실히, 홈 환경(30) 내 몇 개의 디바이스들이 전혀 구조물(32) 내부에 물리적으로 있을 필요가 없다. 예를 들어, 풀 가열기(34) 또는 관개 시스템(36)을 제어하는 디바이스는 구조물(32) 외부에 위치될 수 있다.

[0042]도시된 구조물(32)은 벽들(40)을 통해 서로 적어도 부분적으로 분리되는 다수의 룸들(38)을 포함한다. 벽들(40)은 내부 벽들이나 또는 외부 벽들을 포함할 수 있다. 각각의 룸(38)은 바닥(42) 및 천장(44)을 더 포함할 수 있다. 디바이스들이 벽(40), 바닥(42), 또는 천장(44)에 장착되고, 통합되고 그리고/또는 지지될 수 있다.

[0043]홈 환경(30)은, 임의의 다양한 유용한 홈 목적들을 제공하기 위해서 서로 그리고/또는 클라우드-기반 서

버 시스템들과 끊김없이 통합될 수 있는 지능적인, 멀티-감지, 네트워크 연결식 디바이스들을 비롯한 복수의 디바이스들을 포함할 수 있다. 홈 환경(30)에 도시된 디바이스들 중 하나, 2 이상 또는 각각은 하나 이상의 센서(12), 사용자 인터페이스(14), 전원(16), 네트워크 인터페이스(18), 프로세서(20) 등을 포함할 수 있다.

[0044]예시적인 디바이스들(10)은 Nest® 학습 온도 조절 장치-1세대 T100577 또는 Nest® 학습 온도 조절 장치-2세대 T200577와 같은 네트워크 연결식 온도 조절 장치(46)를 포함할 수 있다. 온도 조절 장치(46)는 주변 기후 특징들(예를 들어, 온도 및/또는 습도)을 검출하고 난방, 환기 및 에어-컨디셔닝(HVAC) 시스템(48)을 제어할 수 있다. 다른 예시적인 디바이스(10)는 위험 검출 유닛(50), 이를 테면, Nest®에 의한 위험 검출 유닛을 포함할 수 있다. 위험 검출 유닛(50)은 홈 환경(30) 내의 위험한 물체의 존재 및/또는 위험한 조건(예를 들어, 연기, 화재, 또는 일산화탄소)을 검출할 수 있다. 추가적으로, "스마트 도어벨"로 지칭될 수 있는 출입구 인터페이스 디바이스들(52)은 사람이 일 위치로 접근하는 것 또는 사람이 일 위치에서 떠나는 것을 검출하고, 청각적 기능을 제어하고, 청각적 또는 시각적 수단을 통해 사람의 접근 또는 출발을 알리거나, 또는 (예를 들어, 보안 시스템을 활성화하거나 또는 비활성화하는) 보안 시스템 상의 셋팅들을 제어할 수 있다.

[0045]특정 실시예들에서, 디바이스(10)는 주변 조명 조건들을 검출하고, 룸-점유 상태들을 검출하고, 하나 이상의 조명들의 파워 및/또는 디밍(dim) 상태를 제어할 수 있는 조명 스위치(54)를 포함할 수 있다. 일부 예들에서, 조명 스위치들(54)은 천정 팬과 같은 팬의 전력 상태 또는 속도를 제어할 수 있다.

[0046]추가적으로, 벽 플러그 인터페이스(56)는 룸 또는 엔클로저의 점유를 검출하고 (예를 들어, 집에 아무도 없으면 플러그에 전력이 공급되지 않도록) 하나 이상의 벽 플러그에 대한 전원 공급을 제어할 수 있다. 홈 환경(30) 내의 디바이스(10)는, 가전제품(58), 이를 테면, 냉장고들, 난로들 및/또는 오븐들, 텔레비전들, 세탁기들, 건조기들, (구조물(32) 내부 및/또는 외부의) 조명들, 스테레오들, 인터컴 시스템들, 차고문 오프너들, 바닥 팬들, 천정 팬들, 집전체의 팬들, 벽 에어 컨디셔너들, 풀 가열기들(34), 관개 시스템들(36), 보안 시스템들 등을 더 포함 할 수 있다. 도 2의 설명들이 특정 디바이스들과 연관된 특정 센서들 및 기능성들을 식별할 수 있지만, (명세서 전체에 걸쳐 설명된 바와 같이) 다양한 센서들 및 기능들 중 임의의 것이 디바이스(10)에 통합될 수 있다는 것을 인식할 것이다.

[0047]프로세싱 및 감지 능력들을 포함하는 것 이외에도, 상술된 예시적인 디바이스들 각각은, 임의의 다른 디바이스와 그리고 임의의 클라우드 서버로 또는 세계 어느 곳에도 네트워크 연결되는 임의의 다른 디바이스로 데이터 통신들 및 정보 공유를 할 수 있다. 일 실시예에서, 디바이스들(10)은 도 5를 참고로 하여 아래에 설명될 효율적인 네트워크 계층을 통해 통신들을 송신하고 수신할 수 있다. 일 실시예에서, 효율적인 네트워크 계층은, 디바이스들(10)로 하여금 무선 메시 네트워크를 통해 서로 통신하게 할 수 있다. 이와 같이, 특정 디바이스들은 무선 중계기들로서 역할을 할 수 있고 그리고/또는 서로 직접적으로 연결되지 않을 수 있는 (즉, 하나의 홉이 있는) 홈 환경의 디바이스들 사이에서 브리지들로서 기능할 수 있다.

[0048]일 실시예들에서, 무선 라우터(60)는 추가로, 무선 메시 네트워크를 통해 홈 환경(30)의 디바이스들(10)과 통신할 수 있다. 무선 라우터(60)는 이후, 인터넷(62)과 통신할 수 있으므로, 각각의 디바이스(10)는 인터넷(62)을 통해 중앙 서버 또는 클라우드-컴퓨팅 시스템(64)과 통신할 수 있다. 중앙 서버 또는 클라우드-컴퓨팅 시스템(64)은, 특정 디바이스(10)와 연관된 제조업자, 지원 엔티티 또는 서비스 제공자와 연관될 수 있다. 이와 같이, 일 실시예에서, 사용자는, 전화 또는 인터넷-연결식 컴퓨터와 같은 일부 다른 통신 수단을 이용하기보다는 디바이스 그 자체를 이용하여 고객 지원에 접속할 수 있다. 또한, (예를 들어, 이용가능할 경우, 구매될 경우, 또는 정기적인 간격들로) 소프트웨어 업데이트들이 중앙 서버 또는 클라우드-컴퓨팅 시스템(64)으로부터 디바이스들로 자동으로 전송될 수 있다.

[0049]네트워크 연결에 의해서, 디바이스들(10) 중 하나 이상의 것은 추가로, 사용자가 디바이스에 근접해 있지 않더라도 사용자로 하여금 디바이스와 상호작용하게 할 수 있다. 예를 들어, 사용자가 컴퓨터(예를 들어, 데스크탑 컴퓨터, 랩탑 컴퓨터, 또는 태블릿) 또는 다른 휴대용 전자 디바이스(예를 들어, 스마트폰)(66)를 이용하여 디바이스와 통신할 수 있다. 웹페이지 또는 애플리케이션은 수신된 통신들에 기초하여 사용자로부터 통신을 수신하고 디바이스(10)를 제어할 수 있다. 또한, 웹페이지 또는 애플리케이션은 디바이스의 동작에 대한 정보를 사용자에게 제공할 수 있다. 예를 들어, 사용자가 디바이스에 대한 현재 설정 포인트 온도를 보고 인터넷(62)에 연결될 수 있는 컴퓨터를 이용하여 이 온도를 조정할 수 있다. 이 예에서, 온도 조절 장치(46)는 효율적인 네트워크 계층을 이용하여 생성된 무선 메시 네트워크를 통해 현재 설정 포인트 온도 보기 요청을 수신할 수 있다.

[0050]특정 실시예에서, 홈 환경(30)은 또한, 벽 플러그 인터페이스들(56)에 의해, 비록 코어스하더라도 (온/오

프) 제어될 수 있는 오래된 종래의 세탁기/드라이어들, 냉장고들 등과 같은 다양한 비-통신적 레거시 가전기기들(68)을 포함할 수 있다. 홈 환경(30)은, 다양한 부분 통신형 레거시 가전기기들(70), 이를 테면, 위험 검출 유닛들(50) 또는 조명 스위치들(54)에 의해 제공된 IR 신호들에 의해 제어될 수 있는 적외선(IR) 제어식 벽 에어 컨디셔너들 또는 다른 IR-제어식 디바이스들을 더 포함할 수 있다.

[0051]상기 언급된 바와 같이, 상술된 예시적인 디바이스들(10) 각각은 무선 메시 네트워크를 확립할 수 있으므로 데이터가 각각의 디바이스(10)로 통신될 수 있다. 도 2의 예시적인 디바이스를 염두에 두면서, 도 3은 상술된 예시적인 디바이스들 중 일부 디바이스들 간의 통신을 촉진시키기 위해서 이용될 수 있는 예시적인 무선 메시 네트워크(80)를 도시한다. 도 3에 도시된 바와 같이, 온도 조절 장치(46)는, 위험 검출 유닛(50)에 그리고 조명 스위치(54)에 무선으로 연결될 수 있는 플러그 인터페이스(56)에 대한 직접 무선 연결을 구비할 수 있다. 동일한 방식으로, 조명 스위치(54)는 가전기기(58) 및 휴대용 전자 디바이스(66)에 무선으로 결합될 수 있다. 가전기기(58)는 풀 가열기(34)에만 결합될 수 있고 휴대용 전자 디바이스(66)는 관개 시스템(36)에만 결합될 수 있다. 관개 시스템(36)은 출입구 인터페이스 디바이스(52)에 대한 무선 연결을 구비할 수 있다. 도 3의 무선 메시 네트워크(80)의 각각의 디바이스가 무선 메시 네트워크(80) 내의 노드에 대응할 수 있다. 일 실시예에서, 효율적인 네트워크 계층은 RIPng 프로토콜 및 DTLS 프로토콜을 이용하여 그 각각의 노드 송신 데이터를 지정할 수 있으므로, 데이터는 노드들 사이에서 최소수의 홉들을 통해 목적지 노드로 안전하게 이송될 수 있다.

[0052]일반적으로, 효율적인 네트워크 계층은 도 4에 도시된 바와 같은 OSI(Open System Interconnection) 모델(90)의 부분일 수 있다. OSI 모델(90)은 앱스트랙션(abstraction) 계층들에 대한 통신 시스템의 기능들을 도시한다. 즉, OSI 모델은 네트워킹 프레임워크를 지정하거나 또는 디바이스들 간에 통신들이 구현될 수 있는 방법을 지정할 수 있다. 일 구현에서, OSI 모델은 6개의 계층들: 물리 계층(92), 데이터 링크 계층(94), 네트워크 계층(96), 전송 계층(98), 플랫폼 계층(100) 및 애플리케이션 계층(102)을 포함할 수 있다. 일반적으로, OSI 모델(90)의 각각의 계층은 그 각각의 계층의 상부 계층을 서빙할 수도 있고, 그 각각의 계층의 하부 계층에 의해 서빙될 수도 있다.

[0053]이점을 염두에 두면서, 물리 계층(92)은, 서로 통신할 수 있는 디바이스들에 하드웨어 사양들을 제공할 수 있다. 이와 같이, 물리 계층(92)은 디바이스들이 서로 연결될 수 있는 방법을 확립하고, 통신 리소스들이 디바이스들 간에 공유될 수 있는 방법의 관리를 지원할 수 있는 식이다.

[0054]데이터 링크 계층(94)은 디바이스들 간에 이송될 수 있는 데이터의 양을 지정할 수 있다. 일반적으로, 데이터 링크 계층(94)은, 송신되고 있는 데이터 패킷들이 송신 프로토콜의 부분으로서 비트들로 인코딩되고 디코딩될 수 있는 방식을 제공할 수 있다.

[0055]네트워크 계층(96)은, 목적지 노드로 이송되는 데이터가 라우팅되는 방법을 지정할 수 있다. 네트워크 계층(96)은 또한, 이송되는 데이터의 무결성이 유지되는 것을 보증하기 위해서 애플리케이션 계층(102) 내 보안 프로토콜과 인터페이싱할 수 있다.

[0056]전송 계층(98)은, 소스 노드로부터 목적지 노드까지 데이터의 투명한 이송을 지정할 수 있다. 전송 계층(98)은 또한, 데이터의 투명한 이송이 신뢰할 수 있는 상태를 유지하는 방법을 제어할 수 있다. 이와 같이, 전송 계층(98)은, 목적지 노드로 이송하기 위해 의도된 데이터 패킷들이 목적지 노드에 정말로 도달했다는 것을 확인하기 위해 사용될 수 있다. 전송 계층(98)에 사용될 수 있는 예시적인 프로토콜들은 TCP(Transmission Control Protocol) 및 UDP(User Datagram Protocol)를 포함할 수 있다.

[0057]플랫폼 계층(100)은 전송 계층(98) 내부에 지정된 프로토콜에 따라 디바이스들 간의 연결들을 확립할 수 있다. 플랫폼 계층(100)은 또한 애플리케이션 계층(102)이 사용할 수 있는 형태로 데이터 패킷들을 트랜슬레이트할 수 있다. 애플리케이션 계층(102)은 사용자와 직접 인터페이싱할 수 있는 소프트웨어 애플리케이션을 지원할 수 있다. 이와 같이, 애플리케이션 계층(102)은 소프트웨어 애플리케이션에 의해 정의된 프로토콜들을 구현할 수 있다. 예를 들어, 소프트웨어 애플리케이션은 파일 이송, 전자 메일 등과 같은 서비스들을 제공할 수 있다.

[0058]이제, 도 5를 참고하면, 일 실시예에서, 네트워크 계층(96) 및 전송 계층(98)은 효율적인 저전력 무선 개인 네트워크(ELoWPAN)(110)를 형성하기 위한 특정 방식으로 구성될 수 있다. 일 실시예에서, ELoWPAN(110)는, 로우-레이트 무선 개인 영역 네트워크들(LR-WPAN들)에 대응할 수 있는 IEEE 802.15.4 네트워크에 기초할 수 있다. ELoWPAN(110)은, 네트워크 계층(96)이 인터넷 프로토콜 버전 6(IPv6)에 기초한 통신 프로토콜을 이용하여 홈 환경(30)에서 디바이스들(10) 간에 데이터를 라우팅할 수 있다는 것을 지정할 수 있다. 이와 같이, 각각의

디바이스(10)는, 각각의 디바이스(10)에 홈 환경(30) 주위의 인터넷, 로컬 네트워크 등을 통해 그 자신을 식별하기 위해 사용하기 위한 고유 어드레스를 제공하는 128-비트 IPv6 어드레스를 포함할 수 있다.

[0059]일 실시예에서, 네트워크 계층(96)은, 데이터가 라우팅 정보 프로토콜-차세대(RIPng; Routing Information Protocol-Next Generation)를 이용하여 디바이스들 간에 라우팅될 수 있는 것을 지정할 수 있다. RIPng는 소스 노드와 목적지 노드 사이의 다수의 홉들에 기초하여 무선 메시 네트워크를 통해 데이터를 라우팅하는 라우팅 프로토콜이다. 즉, RIPng는, 데이터가 라우팅될 방법을 결정할 경우 최소 수의 홉들을 사용하는 소스 노드로부터 목적지 노드로의 라우트를 결정할 수 있다. 데이터를 무선 메시 네트워크를 통해 이송하는 것을 지원하는 것 이외에도, RIPng는 IPv6 네트워킹 트래픽을 지원할 수 있다. 이와 같이, 각각의 디바이스(10)는 자신을 식별하기 위한 고유 IPv6 어드레스 및 데이터의 라우팅 시 목적지 노드를 식별하기 위한 고유 IPv6 어드레스를 사용할 수 있다. RIPng가 노드들 간에 데이터를 전송할 수 있는 방법에 관한 추가적인 상세들이 도 6을 참고로 하여 아래에 설명될 것이다.

[0060]상기 언급된 바와 같이, 네트워크 계층(96)은 또한 이송되는 데이터의 무결성을 관리하기 위해 애플리케이션 계층(102)을 통해 보안 프로토콜과 인터페이싱할 수 있다. 도 5에 도시된 바와 같이, 효율적인 네트워크 계층은, 애플리케이션 계층(102)의 데이터그램 전송 계층 보안(DTLS) 프로토콜을 이용하여 디바이스들 간에 데이터가 안전하게 이송되게 한다. 일반적으로, 효율적인 네트워크 계층은 디바이스들(10) 간의 통신 경로(pathway)가 안전한지 여부를 애플리케이션 계층(102)의 DTLS 프로토콜을 이용하여 결정할 수 있다. 통신 경로가 안전한 것으로 결정된 후, 효율적인 네트워크 계층은 디바이스들(10) 간의 안전한 데이터 이송들을 촉진할 수 있다. 이러한 방식으로, 효율적인 네트워크 계층은 송신 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 등을 이용한 데이터 이송들을 가능하게 할 수 있다. DTLS 프로토콜에 관한 추가 상세들이 도 8 및 도 9를 기준으로 하여 아래에 설명될 것이다.

[0061]도 5에 도시된 네트워크 계층(96)은 본원에서 상기 언급된 효율적인 네트워크 계층을 특징으로 한다. 즉, 효율적인 네트워크 계층은 RIPng를 이용하여 IPv6 데이터를 라우팅한다. 더욱이, 효율적인 네트워크 계층은, 디바이스들 간의 안전한 데이터 이송을 위해 DTLS 프로토콜을 사용하는 애플리케이션 계층(102)과 인터페이싱할 수 있다. 그 결과, 전송 계층(98)이 데이터에 대한 다양한 타입들의 (예를 들어, TCP 및 UDP) 이송 방식들을 지원할 수 있다.

[006]이제 도 6을 참고하면, 도 6은, RIPng를 이용하여 도 3의 무선 메시 네트워크(80)의 각각의 디바이스(10)에 대한 라우팅 테이블을 결정하기 위해 사용될 수 있는 방법(120)의 흐름도를 도시한다. 방법(120)은 홈 환경(30)의 각각의 디바이스(10)에 의해 수행될 수 있으므로, 각각의 디바이스(10)는, 무선 메시 네트워크(80) 내 각각의 노드가 서로 연결될 수 있는 방법을 나타내는 라우팅 테이블을 생성할 수 있다. 이와 같이, 각각의 디바이스(10)는 데이터를 목적지 노드로 라우팅하는 방법을 독립적으로 결정할 수 있다. 일 실시예에서, 디바이스(10)의 프로세서(20)는 네트워크 인터페이스(18)를 이용하여 방법(120)을 수행할 수 있다. 이와 같이, 디바이스(10)는 센서(12)와 연관되거나 또는 프로세서(18)에 의해 결정되는 데이터를 네트워크 인터페이스(18)를 경유하여 홈 환경(30)의 다른 디바이스들(10)로 전송할 수 있다.

[0063]방법(120)의 다음 논의는 방법(120)의 다양한 블록들을 명확하게 도시하기 위해서 도 7a 내지 도 7d에 대하여 설명될 것이다. 이를 염두에 두고 도 6 및 도 7a 둘 모두를 참고하면, 블록(122)에서, 디바이스(10)는 요청(132)을 임의의 다른 디바이스(10)로 전송할 수 있는데, 이는 요청 디바이스(10)에 대해 직접적일 수 있다(즉, 제로 홉). 요청(132)은 개별 디바이스(10)로부터의 라우팅 정보 모두에 대한 요청을 포함할 수 있다. 예를 들어, 도 7a를 참고하면, 노드 1의 디바이스(10)는 요청(132)을 노드 2의 디바이스(10)로 전송하여 노드 2의 메모리에 포함된 라우트들(즉, N2의 라우트들) 모두를 전송할 수 있다.

[0064]블록(124)에서, 요청 디바이스(10)는 각각의 디바이스(10)의 각각의 메모리에 포함된 라우트들 모두를 포함할 수 있는 각각의 디바이스(10)로부터 메시지를 수신할 수 있다. 라우트들은, 무선 메시 네트워크(80)의 각각의 노드가 서로 연결될 수 있는 방법을 지정할 수 있는 라우팅 테이블에서 조직될 수 있다. 즉, 라우팅 테이블은, 데이터가 이송되는 소스 노드부터 목적지까지 데이터가 어느 중간 노드들로 이송될 수 있을지를 지정할 수 있다. 상기 예와 도 7b를 다시 참고하면, N2의 라우트들에 대한 노드 1의 요청에 응답하여, 블록(124)에서, 노드 2는 노드 2의 메모리 또는 스토리지에 포함된 라우트들 모두(N2의 라우트들(144))를 노드 1로 전송할 수 있다. 일 실시예에서, 무선 메시 네트워크(80)의 각각의 노드는 요청(132)을 도 7a에 도시된 바와 같은 그의 인접한 노드로 전송할 수 있다. 응답으로, 각각의 노드는 이후, 도 7b에 도시된 바와 같이 그의 라우트들을 그의 인접 노드로 전송할 수 있다. 예를 들어, 도 7b는, 각각의 노드가, N1의 라우트들(142), N2의 라우트들

(144), N3의 라우트들(146), N4의 라우트들(148), N5의 라우트들(150), N6의 라우트들(152), N7의 라우트들(154), N8의 라우트들(156), 및 N9의 라우트들(158)로 도시된 바와 같이 그의 라우트 데이터를 각각의 인접 노드로 전송하는 방법을 도시한다.

[0065]처음에, 각각의 노드는, 노드가 직접 연결(즉, 제로 홉)할 수 있는 노드들을 알 수 있다. 예를 들어, 처음에는, 노드 2가 노드 1, 노드 3 및 노드 4에 직접적으로 연결되는 방법만을 알 수 있다. 그러나, N1의 라우트들(142), N3의 라우트들(146), 및 N4의 라우트들(148)의 수신 후, 노드 2의 프로세서(20)는, N1의 라우트들(142), N3의 라우트들(146), 및 N4의 라우트들(148)과 함께 포함된 정보 모두를 포함하는 라우팅 테이블을 구축할 수 있다. 이와 같이, 다음 시간 노드 2가 그의 라우트들 또는 라우팅 테이블(즉, N2의 라우트들(144))에 대한 요청을 수신하고, 노드 2는, N1의 라우트들(142), N2의 라우트들, N3의 라우트들(146) 및 N4의 라우트들(148)을 포함하는 라우팅 테이블을 전송할 수 있다.

[0066]이를 염두에 두고 도 6을 다시 참고하면, 블록(126)에서 요청 디바이스(10)는 인접 디바이스(10)로부터 수신된 라우팅 정보를 포함시키기 위해 그의 로컬 라우팅 테이블을 업데이트할 수 있다. 특정 실시예에서, 각각의 디바이스(10)가 주기적으로 방법(120)을 수행할 수 있으므로, 각각의 디바이스(10)는, 무선 메시 네트워크(80) 내의 각각의 노드가 서로 연결될 수 있는 방법을 특징으로 하는 업데이트된 라우팅 테이블을 포함한다. 상기 언급된 바와 같이, 방법(120)이 수행될 때마다, 각각의 디바이스(10)는, 인접 디바이스(10)가 그의 인접 디바이스들로부터 수신된 정보로 그의 라우팅 테이블을 업데이트했다면 그 인접 디바이스(10)으로부터 추가 정보를 수신할 수 있다. 그 결과, 각각의 디바이스(10)는, 무선 메시 네트워크(80) 내 각각의 노드가 서로 연결될 수 있는 방법을 이해할 수 있다.

[0067]도 7c는, 예를 들어, 방법(120)을 이용하여 노드 1에서 디바이스(10)에 의해 결정되었을 수 있는 라우팅 테이블(172)을 도시한다. 이 예에서, 라우팅 테이블(172)는, 목적지 노드로서 무선 메시 네트워크(80) 내의 각각의 노드, 노드 1과 각각의 목적지 노드 간의 중간 노드들, 및 노드 1과 목적지 노드 간의 홉들의 수를 지정할 수 있다. 홉들의 수는, 목적지 노드로 전송되는 데이터가 목적지 노드에 도달하기 전에 중간 노드로 포워딩될 수 있는 횟수에 대응한다. 특정 목적지 노드로 데이터를 전송할 경우, RIPng 라우팅 방식은 최소 수의 홉들을 수반하는 라우트를 선택할 수 있다. 예를 들어, 노드 1이 데이터를 노드 9로 전송하도록 의도하는 경우, RIPng 라우팅 방식은, 노드들(2, 4, 6, 7 및 8)을 경유하여 데이터를 라우팅하는 것이 5개의 홉들을 포함하는 것과는 대조적으로 4개의 홉들을 포함하는 노드들(2, 4, 5 및 8)을 통해 데이터를 라우팅할 것이다.

[0068]RIPng 라우팅 방식을 이용함으로써, 각각의 디바이스(10)는, 데이터가 목적지 노드로 라우팅될 방법을 독립적으로 결정할 수 있다. 반면에, 6LoWPAN 디바이스들에서 사용된 RPL("Ripple" Routing Protocol)과 같은 종래의 라우팅 방식들은 무선 메시 네트워크의 구조를 아는 유일한 노드일 수 있는 중앙 노드를 통해 데이터를 라우팅할 수 있다. 보다 구체적으로, RPL 프로토콜은 계층식으로 구조화될 수 있는 DAG(directed acyclic graph)에 따라 무선 메시 네트워크를 생성할 수 있다. 상부에 위치된 이 계층은, 노드의 연결들 각각에 대한 랭크를 결정하기 위해서 요청들을 하위 레벨 노드들로 주기적으로 멀티캐스트할 수 있는 경계 라우터를 포함할 수 있다. 본질적으로, 데이터가 소스 노드로부터 목적지 노드로 이송될 경우, 데이터는, 노드들의 계층을 높인 후 다시 낮춰 목적지 노드로 이송될 수 있다. 이러한 방식으로, 더 높은 계층에 위치된 노드들은 더 낮은 계층에 위치된 노드들보다 더 빈번하게 데이터를 라우팅할 수 있다. 더욱이, RPL 시스템의 경계 라우터는 또한, 이것이 데이터가 계층을 경유하여 라우팅되는 방법을 제어하기 때문에 더욱 빈번하게 동작할 수 있다. 종래의 RPL 시스템에서, 본원에 교시된 RIPng 시스템과는 대조적으로, 일부 노드들은, 소스 노드와 목적지 노드에 대한 그의 위치로 인해서가 아니라 계층 내의 그의 위치로 인한 것에 단순히 기초하여 더욱 빈번하게 데이터를 라우팅할 수 있다. RPL 시스템 하에서 더 자주 데이터를 라우팅하는 이러한 노드들은 더 많은 에너지를 소비할 수 있고 따라서 저 전력을 이용하여 동작하는 홈 환경(30) 내 디바이스들(10)과 구현하기에 적합하지 않을 수 있다. 더욱이, 상기 언급된 바와 같이, 경계 라우터 또는 RPL 시스템의 임의의 다른 고-레벨 노드가 온도 조절 장치(46)에 대응하는 경우, 증가된 데이터 라우팅 액티비티는 온도 조절 장치(46) 내부에 생성된 열을 증가시킬 수 있다. 그 결과, 온도 조절 장치(46)의 온도 검침값은 홈 환경(30)의 온도를 부정확하게 나타낼 수 있다. 다른 디바이스들(10)이 온도 조절 장치(46)의 온도 검침값에 기초하여 특정 동작들을 수행할 수 있기 때문에, 그리고 온도 조절 장치(46)가 그의 온도 검침값에 기초하여 다양한 디바이스들(10)로 커맨드들을 전송할 수 있기 때문에, 온도 조절 장치(46)의 온도 검침값이 정확하다는 것을 보장하는 것이 유리할 수 있다.

[0069]디바이스들(10) 중 어느 것도 균형이 맞지 않는 시간의 양으로 데이터를 라우팅하지 않는다는 것을 보장하는 것 이외에도, RIPng 라우팅 방식을 이용함으로써, 새로운 디바이스들(10)이 사용자에 의한 최소의 노력으로 무선 메시 네트워크에 추가될 수 있다. 예를 들어, 도 7d는 무선 메시 네트워크(80)에 새로운 노드 10이 추

가되는 것을 도시한다. 특정 실시예들에서, 노드 10이 일단 (예를 들어, 노드 4를 통해) 무선 메시 네트워크(80)에 대한 연결을 확립하면, 노드 10에 대응하는 디바이스(10)는, 무선 메시 네트워크(80)의 각각의 노드로 데이터가 라우팅될 수 있는 방법을 결정하기 위해서 상술된 방법(120)을 수행할 수 있다. 무선 메시 네트워크(80)의 각각의 노드가 이미 여러 번 방법(120)을 수행했다면, 노드 10의 디바이스(10)는 노드 4의 디바이스(10)로부터 무선 메시 네트워크(80)의 전체 라우팅 구조를 수신할 수 있다. 동일한 방식으로, 디바이스들(10)은 무선 메시 네트워크(80)로부터 제거될 수 있고 각각의 노드는 방법(120)을 다시 수행함으로써 비교적 용이하게 그의 라우팅 테이블을 업데이트할 수 있다.

[0070]RIPng 라우팅 방식을 이용하여 라우팅 방식을 확립한 후, ELoWPAN(110)은 홈 환경(30) 내 각각의 디바이스(10) 간의 데이터 통신들을 보장하기 위해서 애플리케이션 계층(102)을 통해 DTLS 프로토콜을 사용할 수 있다. 상기 언급된 바와 같이, 안전한 통신 경로가 2개의 통신 디바이스들 사이에 존재한다는 것을 보장한 후, ELoWPAN(110)은, 전송 계층(98)으로 하여금 안전한 통신 경로를 통해 임의의 타입의 데이터(예를 들어, TCP 및 UDP)를 전송할 수 있게 할 수 있다. 일반적으로, 무선 메시 네트워크(80)에 추가된 새로운 디바이스들(10)이 무선 메시 네트워크에서 보다 신속하게 다른 디바이스들(10)로 효율적으로 통신하기 위해 UDP 데이터 이송들을 사용할 수 있다. 더욱이, UDP 데이터 이송들은 일반적으로, 전달의 보장이 없기 때문에 데이터를 전송하거나 또는 포워딩하고 있는 디바이스(10)에 의해 더 적은 에너지를 사용한다. 이와 같이, 디바이스들(10)은 UDP 데이터 이송을 이용하여 비임계적 데이터(예를 들어, 룸에 사람이 존재하는 것)를 전송할 수 있음으로써, 디바이스(10) 내의 에너지를 절약한다. 그러나, 적절한 당사자가 데이터를 수신하는 것을 보장하기 위해서 임계적 데이터(예를 들어, 연기(smoke) 알람)가 TCP 데이터 이송을 통해 전송될 수 있다.

[0071]상기한 것을 염두에 두고, ELoWPAN(110)은 디바이스들(10) 간에 데이터가 통신되는 것을 보장하기 위해 DTLS 프로토콜을 사용할 수 있다. 일 실시예에서, DTLS 프로토콜은 핸드쉐이크 프로토콜을 이용하여 데이터 이송들을 보장할 수 있다. 일반적으로, 핸드쉐이크 프로토콜은, 각각의 디바이스(10)에 의해 제공될 수 있는 보안 증명서를 이용하여 각각의 통신 디바이스를 인증할 수 있다. 도 8은, 보안 증명서가 디바이스(10) 내부에 임베딩될 수 있는 방법을 도시하는 제조 프로세스(190)의 예를 도시한다.

[0072]도 8을 참고하면, 디바이스(10)의 신뢰되는 제조업자(192)에게 각각의 제조된 디바이스를 위해 사용할 수 있는 다수의 보안 증명서들이 제공될 수 있다. 이와 같이, 홈 환경(30)에 사용되고 무선 메시 네트워크(80)에 결합될 수 있는 디바이스(10)를 제조하는 동안, 신뢰되는 제조업자(192)가 제조 프로세스(190) 동안 증명서(194)를 디바이스(10)로 임베딩할 수 있다. 즉, 증명서(194)는 디바이스(10)의 제조 동안 디바이스(10)의 하드웨어로 임베딩될 수 있다. 증명서(194)는 공중 키, 사설 키, 또는 무선 메시 네트워크(80) 내의 상이한 통신 디바이스들을 인증하기 위해서 사용될 수 있는 다른 암호 데이터를 포함할 수 있다. 그 결과, 일단 사용자가 디바이스(10)를 수신하면, 사용자는, 디바이스(10)를 초기화하거나 또는 중앙 보안 노드 등에 등록하지 않고 무선 메시 네트워크(80)로 디바이스(10)를 통합시킬 수 있다.

[0073]6LoWPAN 디바이스들에서 사용된 PANA(Protocol for Carrying Authentication for Network Access)와 같은 종래의 데이터 통신 보안 프로토콜들에서, 각각의 디바이스(10)는 특정 노드(즉, 인증 에이전트)를 이용하여 그 자신을 인증할 수 있다. 이와 같이, 데이터가 임의의 2개의 디바이스들(10) 간에 이송되기 전에, 각각의 디바이스(10)는 인증 에이전트 노드를 이용하여 그 자신을 인증할 수 있다. 인증 에이전트 노드는 이후, 그 인증의 결과를 인포스먼트(enforcement) 포인트 노드(인증 에이전트 노드와 함께 위치될 수 있음)로 전달할 수 있다. 인포스먼트 포인트 노드는 이후, 그 인증들이 유효하다면 2개의 디바이스들(10) 간의 데이터 통신 링크를 확립할 수 있다. 더욱이, PANA에서, 각각의 디바이스(10)는, 각각의 디바이스(10)에 대한 인증이 유효하다는 것을 확인할 수 있는 인포스먼트 포인트 노드를 경유하여 서로 통신할 수 있다.

[0074]이와 같이, 노드들 간의 데이터 이송들을 보장하기 위해서 PANA보다는 DTLS 프로토콜을 이용함으로써, 효율적인 네트워크 계층은 인증 에이전트 노드, 인포스먼트 포인트 노드, 또는 둘 모두를 과도하게 이용하는 것을 방지할 수 있다. 즉, 효율적인 네트워크 계층을 이용한 어느 노드도 무선 메시 네트워크 내의 노드들 간의 각각의 데이터 이송을 위해 인증 데이터를 프로세싱할 수 없다. 그 결과, 효율적인 네트워크 계층을 이용한 노드들은, PANA 프로토콜 시스템에서의 인증 에이전트 노드 또는 인포스먼트 포인트 노드에 비해 더 많은 에너지를 절약할 수 있다.

[0075]이를 염두에 두고, 도 9는 디바이스들 서로 간에 데이터를 이용할 경우 디바이스들(10) 간에 사용될 수 있는 예시적인 핸드쉐이크 프로토콜(200)을 도시한다. 도 9에 도시된 바와 같이, 노드 1의 디바이스(10)는 노드 2의 디바이스(10)로 메시지(202)를 전송할 수 있다. 메시지(202)는, 암호 슈트들, 해쉬 및 압축

알고리즘들, 및 랜덤 번호를 포함할 수 있는 헬로우(hello) 메시지일 수 있다. 노드 2의 디바이스(10)는 이후, 노드 2의 디바이스(10)가 노드 1의 디바이스(10)로부터 메시지(202)를 수신했음을 확인할 수 있는 메시지(204)로 응답할 수 있다.

[0076]노드 1과 노드 2 사이의 연결을 확립한 후, 노드 1의 디바이스는 다시 메시지(202)를 노드 2의 디바이스(10)로 전송할 수 있다. 노드 2의 디바이스(10)는 이후, 노드 2로부터의 헬로우 메시지, 노드 2로부터의 증명서(194), 노드 2로부터의 키 교환, 및 노드 1에 대한 증명서 요청을 포함할 수 있는 메시지(208)로 응답할 수 있다. 메시지(208)의 헬로우 메시지는 암호 슈트들, 해쉬 및 압축 알고리즘들, 및 랜덤 번호를 포함할 수 있다. 증명서(194)는 도 8을 참고로 하여 상술된 바와 같이 신뢰된 제조업자(192)에 의해 디바이스(10) 내부에 임베딩된 보안 증명서일 수 있다. 키 교환은, 2개의 노드들 간의 통신 채널을 확립하기 위해 비밀 키를 결정하기 위해 사용될 수 있는 공중 키, 사설 키, 또는 다른 암호화 정보를 포함할 수 있다. 일 실시예에서, 키 교환이 개별 노드들에 위치된 대응하는 디바이스(10)의 증명서(194)에 저장될 수 있다.

[0077]메시지(208)에 응답하여, 노드 1의 디바이스(10)는, 노드 1로부터의 증명서(194), 노드 1로부터의 키 교환, 노드 2의 증명서 확인, 및 노드 1로부터의 변경 암호 스펙을 포함할 수 있는 메시지(210)를 전송할 수 있다. 일 실시예에서, 노드 1의 디바이스(10)는 노드 2의 증명서(194)와 노드 1로부터의 키 교환을 사용하여 노드 2의 증명서(194)를 확인할 수 있다. 즉, 노드 1의 디바이스(10)가, 노드 2로부터 수신된 증명서(194)가 노드 2의 증명서(194)와 노드 1로부터의 키 교환에 기초하여 유효하다는 것을 확인할 수 있다. 노드 2로부터의 증명서(194)가 유효하다면, 노드 1의 디바이스(10)는 변경 암호 스펙 메시지를 노드 2의 디바이스(10)로 전송하여 2개의 노드들 간의 통신 채널이 안전하다는 것을 알릴 수 있다.

[0078]유사하게, 메시지(210)의 수신 시, 노드 2의 디바이스(10)는 노드 1의 증명서(194)와 노드 2로부터의 키 교환을 사용하여 노드 1의 증명서(194)를 확인할 수 있다. 즉, 노드 2의 디바이스(10)는, 노드 1로부터 수신된 증명서(194)가 노드 1의 증명서(194)와 노드 2로부터의 키 교환에 기초하여 유효하다는 것을 확인할 수 있다. 노드 1로부터의 증명서(194)가 유효하다면, 노드 2의 디바이스(10)는 또한 변경 암호 스펙 메시지를 노드 1의 디바이스(10)로 전송하여 2개의 노드들 간의 통신 채널이 안전하다는 것을 알릴 수 있다.

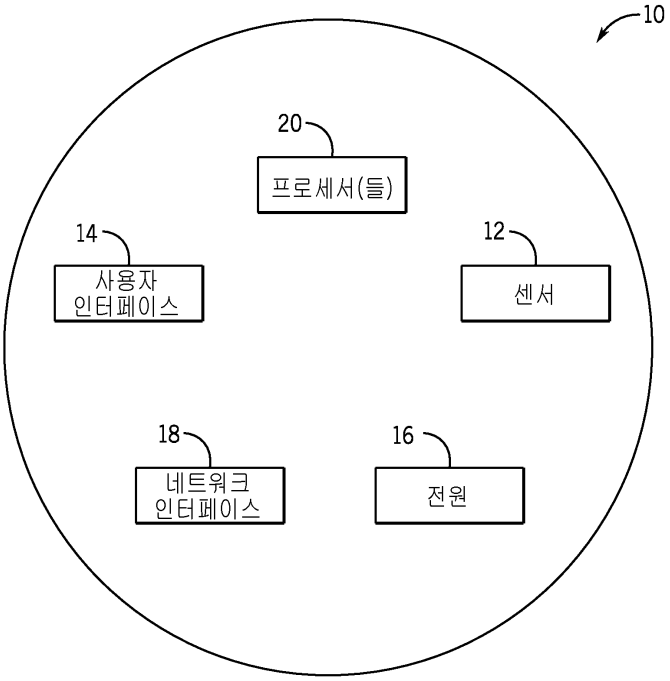
[0079]통신 채널이 안전하다는 것을 확립한 후, 노드 1의 디바이스(10)은 그룹-단위 네트워크 키(214)를 노드 2의 디바이스(10)로 전송할 수 있다. 그룹-단위 네트워크 키(214)는 ELoWPAN(110)과 연관될 수 있다. 이러한 방식으로, 새로운 디바이스들이 ELoWPAN(110)에 조인함에 따라, ELoWPAN(110) 내부에서 통신하기 위해 사전에 인증된 디바이스들이 새로운 디바이스 액세스들을 ELoWPAN(110)으로 제공할 수 있다. 즉, ELoWPAN(110) 내에서 통신하도록 사전에 인증된 디바이스들은 그룹 단위 네트워크 키(214)를 새로운 디바이스들로 제공할 수 있으며, 이는 새로운 디바이스들로 하여금 ELoWPAN(110) 내의 다른 디바이스들과 통신할 수 있게 할 수 있다. 예를 들어, 그룹 단위 네트워크 키(214)는, 적절하게 인증되었고 그리고 그룹 단위 네트워크 키(214)에 사전에 제공되었던 다른 디바이스들과의 통신을 위해 사용될 수 있다. 일 실시예에서, 일단 변경 암호 스펙 메시지가 노드 1의 디바이스(10)와 노드 2의 디바이스(10) 사이에서 교환되었으면, 모델 번호, 디바이스 능력들 등과 같은 식별 정보가 디바이스들 사이에서 통신될 수 있다. 그러나, 노드 2의 디바이스(10)가 그룹 단위 네트워크 키(214)를 수신한 후, 디바이스(10) 상에 배치된 센서들로부터의 데이터, 디바이스(10)에 의해 수행된 데이터 분석 등과 같은 추가 정보가 디바이스들 사이에서 통신될 수 있다.

[0080]제조 프로세스 동안 디바이스(10) 내부에 보안 증명서를 임베딩함으로써, 디바이스(10)는, 디바이스(10)에 대한 보안 또는 인증 프로세스들의 확립에 의해 사용자들과 관련되지 않을 수 있다. 더욱이, 디바이스(10)는, 중앙 인증 에이전트 노드와는 대조적으로 핸드쉐이크 프로토콜에 기초하여 노드들 사이에서 데이터가 안전하게 이송된다는 것을 보장할 수 있기 때문에, 무선 메시 네트워크(80) 에서의 데이터 이송들의 보안은 보안을 위해 하나의 노드에 의존하지 않을 수 있다. 대신, 효율적인 네트워크 계층은, 일부 노드가 이용가능하지 않을 때조차도 데이터가 노드들 사이에서 안전하게 이송될 수 있다는 것을 보장할 수 있다. 이와 같이, 효율적인 네트워크 계층은, 데이터 메시지들을 안전하게 하기 위해 하나의 노드에 의존하지 않기 때문에 보안 문제들에 있어 훨씬 덜 취약할 수 있다.

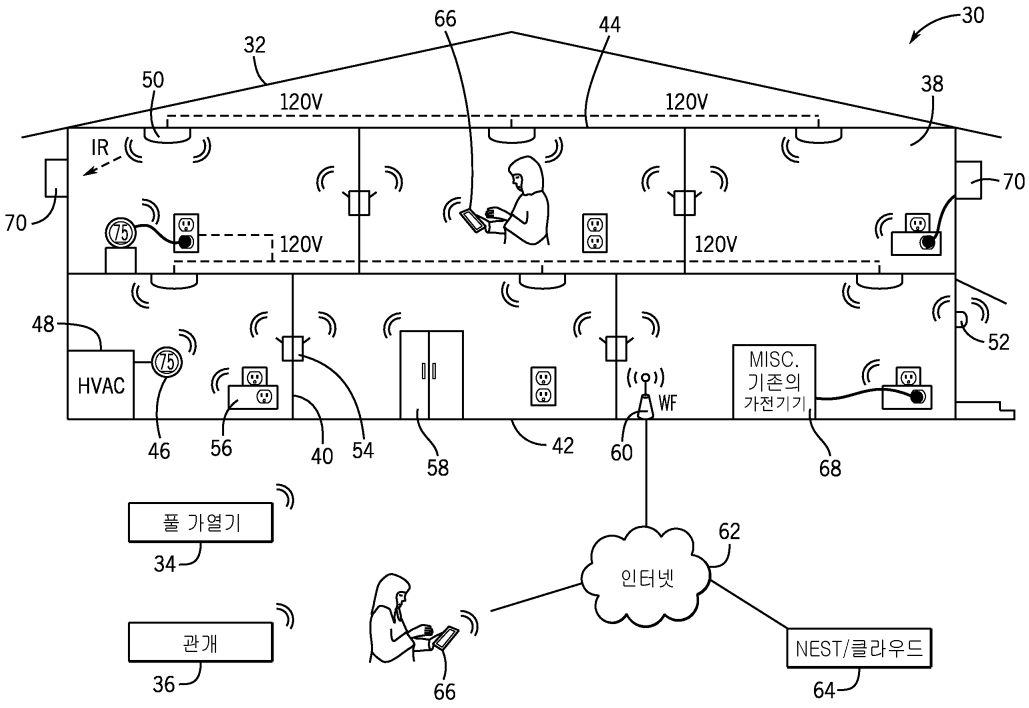
[0081]상술된 특정 실시예들은 예로서 나타내어졌으며, 이러한 실시예들은 다양한 변경들 및 대안적인 형태들이 가능할 수 있다는 것을 이해해야 한다. 또한, 청구범위들은 개시된 특정한 형태들로 제한되도록 의도되기 된다기보다는, 본 개시물의 정신 및 범위에 있는 모든 변경들, 등가물들 및 대안들을 포함하도록 의도된다는 것을 이해해야 한다.

도면

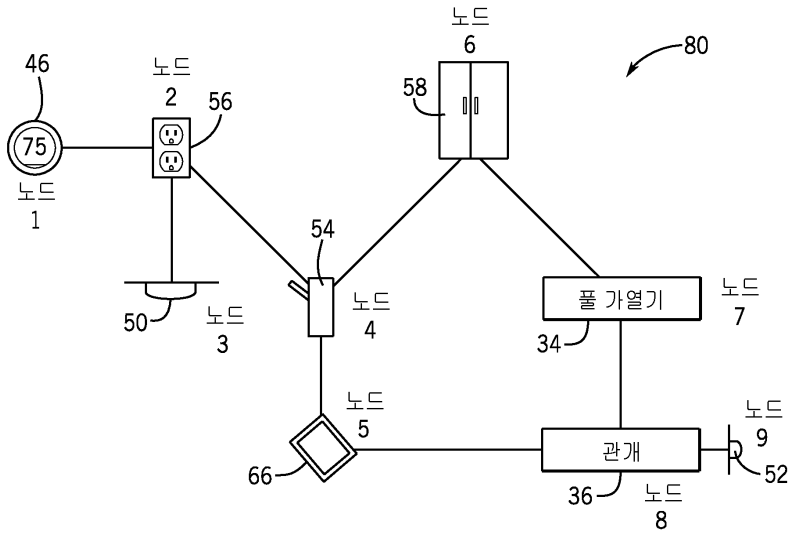
도면1


10
20
프로세서(들)
14
사용자
인터페이스
12
센서
18
네트워크
인터페이스
16
전원

도면2


30
66
44
32
50
120V
120V
38
IR
70
70
75
120V
120V
48
52
HVAC
75
MISC.
기존의
가전기기
WF
46
56
40
54
58
42
60
68
풀 가열기
34
62
인터넷
관개
36
66
NEST/클라우드
64

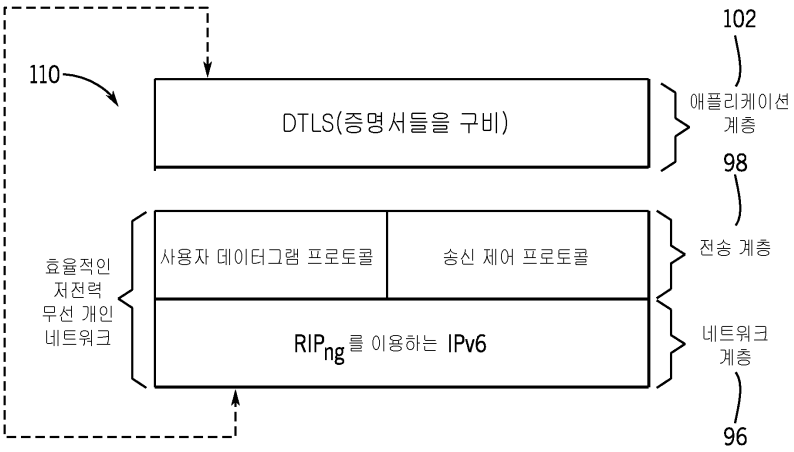
도면3


노드
6
80
46
노드
2
56
58
75
노드
1
54
50
노드
3
노드
4
풀 가열기
노드
7
34
노드
5
노드
9
관개
66
52
36
노드
8

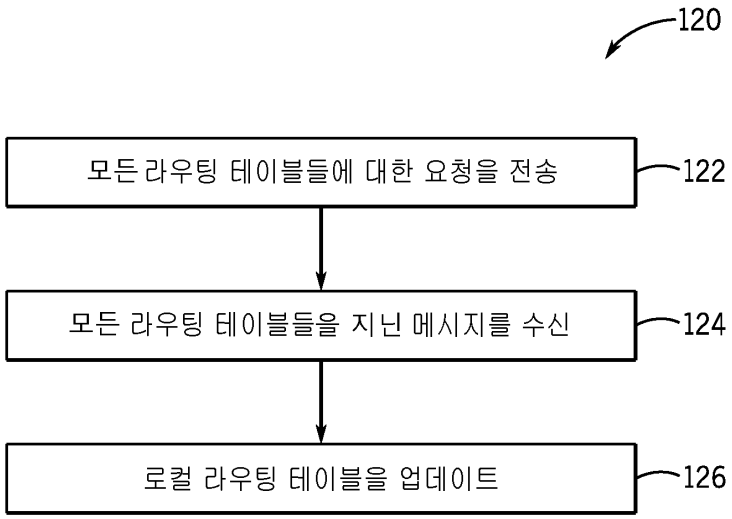
도면4


90
애플리케이션 계층
102
플랫폼 계층
100
전송 계층
98
네트워크 계층
96
데이터 링크 계층
94
물리 계층
92

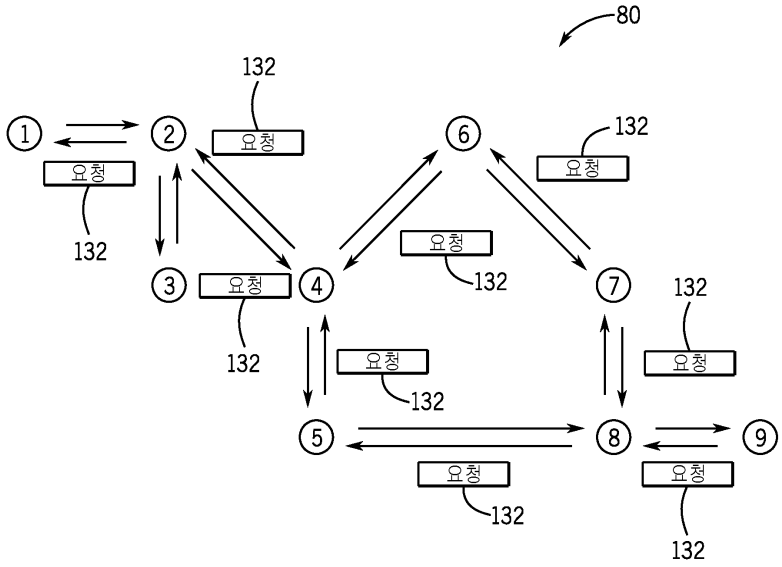
도면5


102
110
DTLS(증명서들을 구비)
애플리케이션
계층
98
사용자 데이터그램 프로토콜
송신 제어 프로토콜
전송 계층
효율적인
저전력
무선 개인
네트워크
RIPng를 이용하는 IPv6
네트워크
계층
96

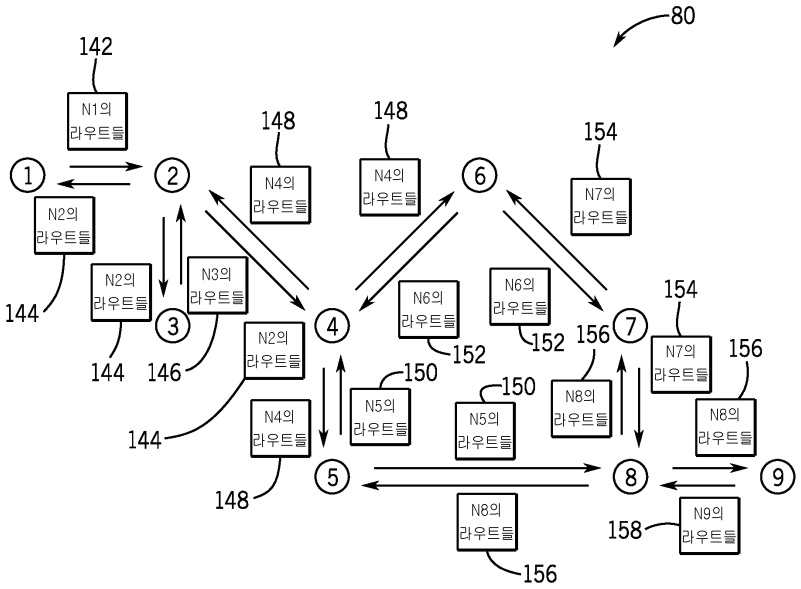
도면6


120
모든 라우팅 테이블들에 대한 요청을 전송
122
모든 라우팅 테이블들을 지닌 메시지를 수신
124
로컬 라우팅 테이블을 업데이트
126

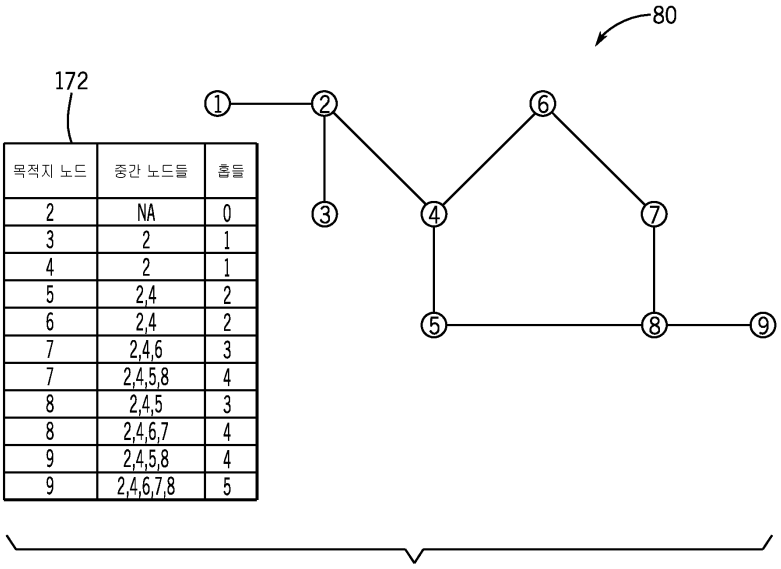
도면7a


80
132
요청
1
2
3
4
5
6
7
8
9

도면7b

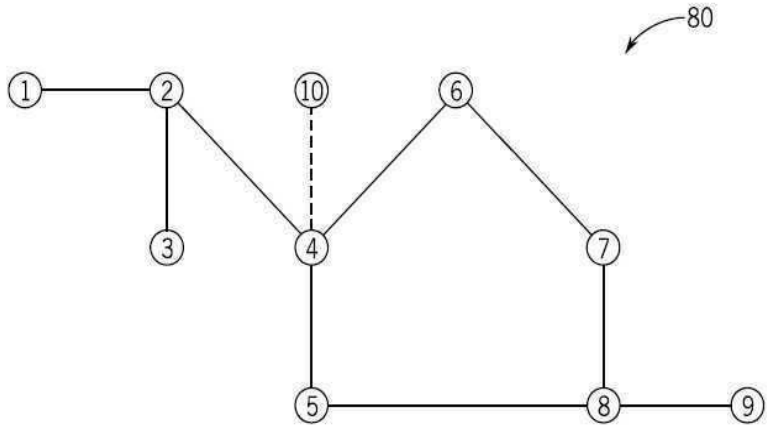


도면7c

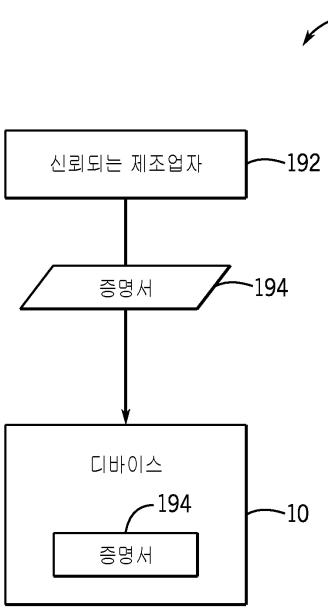


목적지 노드	중간 노드들	홉들
2	NA	0
3	2	1
4	2	1
5	2,4	2
6	2,4	2
7	2,4,6	3
7	2,4,5,8	4
8	2,4,5	3
8	2,4,6,7	4
9	2,4,5,8	4
9	2,4,6,7,8	5

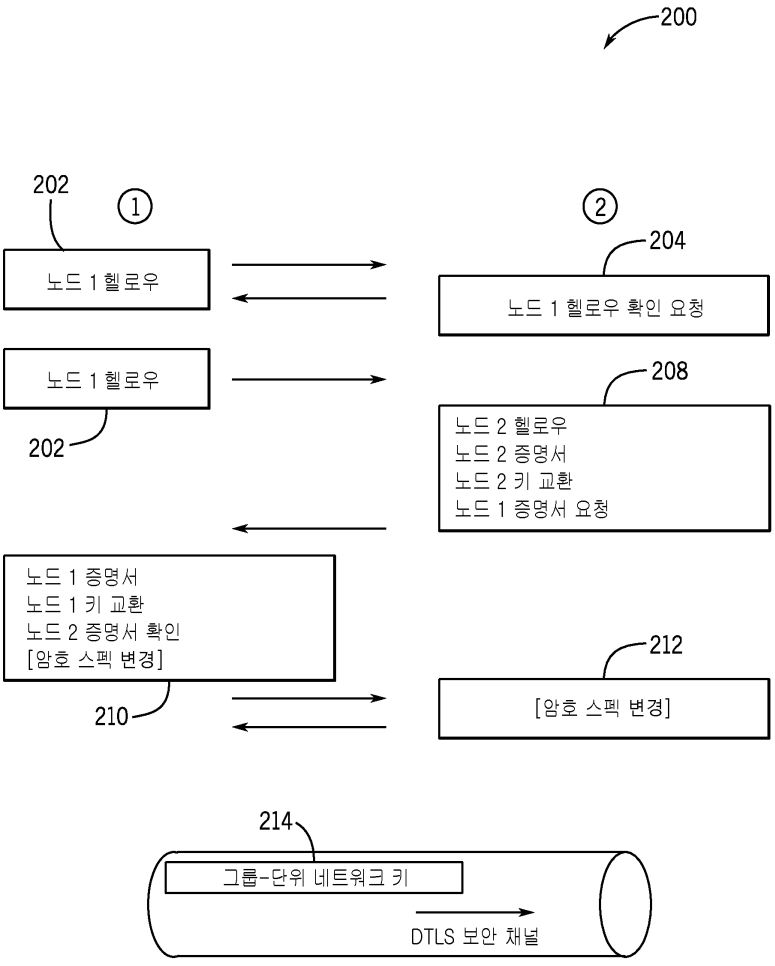
도면7d



도면8



도면9


200
202
1
노드 1 헬로우
노드 1 헬로우
202
2
204
노드 1 헬로우 확인 요청
208
노드 2 헬로우
노드 2 증명서
노드 2 키 교환
노드 1 증명서 요청
노드 1 증명서
노드 1 키 교환
노드 2 증명서 확인
[암호 스펙 변경]
210
212
[암호 스펙 변경]
214
그룹-단위 네트워크 키
DTLS 보안 채널