(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0027037
(43) 공개일자 2016년03월09일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)
(52) CPC특허분류
H04L 63/08 (2013.01)
H04L 63/105 (2013.01)
(21) 출원번호 10-2016-7002175
(22) 출원일자(국제) 2014년06월26일
심사청구일자 없음
(85) 번역문제출일자 2016년01월25일
(86) 국제출원번호 PCT/US2014/044362
(87) 국제공개번호 WO 2014/210322
국제공개일자 2014년12월31일
(30) 우선권주장
61/841,068 2013년06월28일 미국(US)
14/314,999 2014년06월25일 미국(US)

(71) 출원인
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
린 제임스 민루
미국 06511 코네티컷주 뉴 헤이븐 오렌지 스트리트 595
(74) 대리인
특허법인코리아나

전체 청구항 수 : 총 30 항

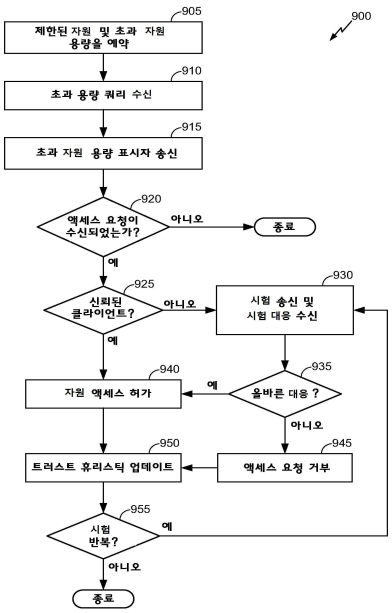
(54) 발명의 명칭 **IoT 자원 액세스 네트워크들에서 제어 부하를 감소시키기 위한 트러스트 휴리스틱 모델**

(57) 요 약

본 개시물은 IoT 자원 액세스 네트워크에서 제어 부하를 감소시키기 위한 트러스트 휴리스틱 모델에 관한 것이다. 예를 들어, 인증 노드는 자원에 대한 액세스를 요청하는 클라이언트 노드를 시험하고, 클라이언트 노드가 그 시험에 대해 정확하게 대응하는 경우에 액세스를 허가하고, 또는 대안적으로, 클라이언트 노드가 그

(뒷면에 계속)

대 표 도 - 도9



시험에 대해 부정확하게 대응하는 경우에 액세스를 거부할 수도 있다. 또한, 그 시험에 대한 대응에 기초하여, 클라이언트 노드는 트러스트 레벨을 할당받을 수도 있고, 그 트러스트 레벨은 연속적인 시험-및-대응 교환들 및/또는 다른 IoT 네트워크 노드들과의 상호작용들에 기초하여 동적으로 업데이트될 수도 있다. 예를 들어, 자원 액세스 제어 부하를 감소시키기 위해, 클라이언트 노드가 시간에 걸쳐 연속적인 시험들에 대해 정확하게 대응하는 경우에, 후속하는 시험-및-대응 간격들이 감경 또는 제거될 수도 있는 한편, 시간에 걸쳐 연속적인 시험들에 대해 부정확하게 대응하는 클라이언트 노드들은 자원을 액세스하는 것이 차단되거나 IoT 네트워크로부터 금지당할 수도 있다.

(52) CPC특허분류
H04L 63/30 (2013.01)
H04L 67/16 (2013.01)

명 세 서

청구범위

청구항 1

사물 인터넷 (IoT) 네트워크에서의 제어된 자원 액세스 방법으로서,

요청 노드에 의해, 상기 IoT 네트워크에서 제 1 제어된 자원에 대한 액세스를 요청하는 단계로서, 상기 제 1 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함하는, 상기 제 1 제어된 자원에 대한 액세스를 요청하는 단계;

제 1 게이트키퍼 노드로부터 수신된 시험 메시지 (challenge message) 에 대해 대응하는 단계; 및

상기 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 상기 제 1 제어된 자원에 대한 요청된 상기 액세스를 수신하는 단계를 포함하고,

상기 제 1 게이트키퍼 노드는 상기 요청 노드가 하나 이상의 연속적인 시험 메시지들에 대해 정확하게 대응하는 것에 응답하여 상기 인증 절차를 주기적으로 완료하기 위한 요건을 감소시키는, 제어된 자원 액세스 방법.

청구항 2

제 1 항에 있어서,

상기 시험 메시지 및 상기 시험 메시지에 대한 대응은 상기 IoT 네트워크와 연관된 제어 채널을 통해 교환되는, 제어된 자원 액세스 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는 상기 요청 노드가 상기 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 상기 요청 노드와 연관된 트러스트 레벨 (trust level) 을 증가시키는, 제어된 자원 액세스 방법.

청구항 4

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는, 상기 인증 절차를 주기적으로 완료하기 위한 요건을 감소시키기 위해 상기 요청 노드에 후속 시험 메시지를 송신하기 전의 간격을 증가시키는, 제어된 자원 액세스 방법.

청구항 5

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는, 상기 요청 노드로부터 상기 시험 메시지에 대한 부정확한 대응을 수신하는 것에 응답하여 상기 요청 노드와 연관된 트러스트 레벨을 감소시키는, 제어된 자원 액세스 방법.

청구항 6

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는, 상기 요청 노드가 상기 시험 메시지에 대해 부정확하게 대응하고 하나 이상의 연속적인 시험 메시지들에 대해 부정확하게 대응하는 것에 응답하여, 상기 요청 노드가 상기 IoT 네트워크를 통해 통신하는 것을 일시적으로 차단하는, 제어된 자원 액세스 방법.

청구항 7

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는, 상기 요청 노드가 상기 시험 메시지에 대해 부정확하게 대응하고 시간에 걸쳐 하

나 이상의 연속적인 시험 메시지들에 대해 대해 계속하여 부정확하게 대응하는 것에 응답하여, 상기 요청 노드가 상기 IoT 네트워크를 통해 통신하는 것을 영구적으로 금지하는, 제어된 자원 액세스 방법.

청구항 8

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는, 상기 IoT 네트워크가 새로운 네트워크 액세스 계층으로 이전하는 것에 응답하여 상기 요청 노드에 할당된 트러스트 레벨에 따라 상기 인증 절차를 주기적으로 완료하기 위한 요건을 조정하는, 제어된 자원 액세스 방법.

청구항 9

제 1 항에 있어서,

제 2 게이트키퍼 노드로부터 제 2 제어된 자원에 대한 액세스를 요청하는 단계를 더 포함하고, 상기 제 2 게이트키퍼 노드는, 상기 요청 노드와, 상기 요청 노드와 하나 이상의 이전 상호작용들을 갖는 신뢰된 노드 사이의 트러스트 레벨에만 기초하여 상기 제 2 제어된 자원에 대한 액세스를 상기 요청 노드에 대해 허가할지 여부를 결정하는, 제어된 자원 액세스 방법.

청구항 10

제 9 항에 있어서,

제 2 IoT 네트워크는 상기 제 2 제어된 자원, 상기 제 2 게이트키퍼 노드, 또는 상기 요청 노드와 상기 하나 이상의 이전 상호작용들을 갖는 상기 신뢰된 노드 중 하나 이상을 포함하는, 제어된 자원 액세스 방법.

청구항 11

제 9 항에 있어서,

상기 요청 노드와 연관된 상기 트러스트 레벨은 각각 개별 트러스트 레벨을 갖는 노드들과 연관된 허가된 자원 액세스를 정의하는 트러스트 휴리스틱 논리 모델에서의 N 개의 트러스트 레벨들 중 하나를 포함하는, 제어된 자원 액세스 방법.

청구항 12

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는 상기 제 1 제어된 자원에 대한 액세스를 통제하는 통제 노드를 포함하는, 제어된 자원 액세스 방법.

청구항 13

제 1 항에 있어서,

상기 제 1 게이트키퍼 노드는 상기 요청 노드와, 상기 제 1 제어된 자원에 대한 액세스를 통제하는 통제 노드 사이에 메시지들을 중계하는 중간 노드를 포함하는, 제어된 자원 액세스 방법.

청구항 14

제 1 항에 있어서,

상기 제 1 제어된 자원은 소비율과 동일하거나 소비율을 초과하는 생산율을 갖는 무제한의 자원을 포함하는, 제어된 자원 액세스 방법.

청구항 15

제 1 항에 있어서,

상기 제 1 제어된 자원은 생산율을 초과하는 소비율을 갖는 한정된 자원을 포함하는, 제어된 자원 액세스 방법.

청구항 16

제 15 항에 있어서,

상기 제 1 게이트키퍼 노드는 상기 한정된 자원에 대한 할당된 액세스를 갖는 중간 노드를 포함하고, 상기 중간 노드에 대해 할당된 상기 액세스는 상기 중간 노드가 필요로 하는 제 1 부분 및 하나 이상의 요청 노드들에 공급될 수 있는 여분의 부분을 포함하는, 제어된 자원 액세스 방법.

청구항 17

제 16 항에 있어서,

상기 제 1 제어된 자원에 대한 액세스를 요청하는 단계는,

중간 노드에 할당된 상기 한정된 자원의 총 여분의 부분을 결정하기 위해 상기 한정된 자원에 대한 할당된 액세스를 갖는 하나 이상의 중간 노드들을 접촉하는 단계; 및

중간 노드에 할당된 상기 한정된 자원의 상기 총 여분의 부분이 상기 요청 노드가 필요로 하는 상기 한정된 자원의 양을 충족하거나 초과한다는 결정에 응답하여, 상기 하나 이상의 중간 노드들이 상기 요청 노드가 필요로 하는 양의 상기 한정된 자원을 공급하도록 요청하는 단계를 더 포함하는, 제어된 자원 액세스 방법.

청구항 18

제 17 항에 있어서,

상기 시험 메시지에 대해 대응하는 단계는,

상기 하나 이상의 중간 노드들에게 상기 요청 노드가 필요로 하는 양의 상기 한정된 자원을 공급하도록 요청하는 것에 응답하여, 상기 하나 이상의 중간 노드들로부터 상기 시험 메시지를 수신하는 단계; 및

각각의 중간 노드에 상기 시험 메시지에 대한 정확한 대응을 송신하는 것에 응답하여, 상기 하나 이상의 중간 노드들로부터 필요한 양의 상기 한정된 자원을 수신하는 단계를 더 포함하는, 제어된 자원 액세스 방법.

청구항 19

사물 인터넷 (IoT) 디바이스로서,

IoT 네트워크에서 제어된 자원에 대한 액세스를 요청하는 수단으로서, 상기 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함하는, 상기 제어된 자원에 대한 액세스를 요청하는 수단;

게이트키퍼 노드로부터 수신된 시험 메시지 (challenge message) 에 대해 대응하는 수단; 및

상기 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 상기 제어된 자원에 대한 요청된 상기 액세스를 수신하는 수단을 포함하고,

상기 게이트키퍼 노드는 상기 IoT 디바이스가 하나 이상의 연속적인 시험 메시지들에 대해 정확하게 대응하는 것에 응답하여 상기 인증 절차를 주기적으로 완료하기 위한 요건을 감소시키는, 사물 인터넷 디바이스.

청구항 20

컴퓨터-실행가능 명령들을 기록한 컴퓨터-판독가능 저장 매체로서,

사물 인터넷 (IoT) 디바이스 상에서 상기 컴퓨터-실행가능 명령들을 실행하는 것은 상기 IoT 디바이스로 하여금,

IoT 네트워크에서 제어된 자원에 대한 액세스를 요청하게 하고,

게이트키퍼 노드로부터 수신된 시험 메시지 (challenge message) 에 대해 대응하게 하며; 그리고

상기 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 상기 제어된 자원에 대한 요청된 상기 액세스를 수신하게 하며,

상기 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함하고,

상기 게이트키퍼 노드는 상기 IoT 디바이스가 하나 이상의 연속적인 시험 메시지들에 대해 정확하게 대응하는 것에 응답하여 상기 인증 절차를 주기적으로 완료하기 위한 요건을 감소시키는, 컴퓨터-판독가능 저장 매체.

청구항 21

사물 인터넷 (IoT) 네트워크에서 자원 액세스를 제어하는 방법으로서,

게이트키퍼 노드에서, 요청 노드로부터 상기 IoT 네트워크에서의 제어된 자원을 액세스하기 위한 요청을 수신하는 단계로서, 상기 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함하는, 상기 제어된 자원을 액세스하기 위한 요청을 수신하는 단계;

상기 요청 노드에 시험 메시지 (challenge message) 를 송신하는 단계;

상기 요청 노드로부터 상기 시험 메시지에 대한 대응을 수신하는 단계; 및

상기 시험 메시지에 대한 수신된 상기 대응에 기초하여 상기 제어된 자원에 대한 액세스를 상기 요청 노드에 대해 허가할지 여부를 결정하는 단계를 포함하고,

상기 게이트키퍼 노드는, 상기 시험 메시지에 대한 상기 수신된 대응이 정확했는지 여부에 기초하여 상기 인증 절차를 주기적으로 완료하기 위한 상기 요청 노드에 대한 상기 요건을 추가적으로 조정하는, 자원 액세스를 제어하는 방법.

청구항 22

제 21 항에 있어서,

상기 시험 메시지에 대한 상기 수신된 대응이 정확했다는 결정에 응답하여, 상기 요청 노드에 대해 상기 제어된 자원에 대한 액세스를 허가하는 단계; 및

상기 시험 메시지에 대한 상기 수신된 대응이 정확했다는 결정에 응답하여, 상기 요청 노드에 할당된 트러스트 레벨 (trust level) 을 증가시키고, 상기 요청 노드에 후속 시험 메시지를 송신하기 전의 간격을 증가시키는 단계를 더 포함하는, 자원 액세스를 제어하는 방법.

청구항 23

제 21 항에 있어서,

상기 시험 메시지에 대한 상기 수신된 대응이 부정확했다는 결정에 응답하여, 상기 요청 노드에 대해 상기 제어된 자원에 대한 액세스를 거부하는 단계; 및

상기 시험 메시지에 대한 상기 수신된 대응이 부정확했다는 결정에 응답하여, 상기 요청 노드에 할당된 트러스트 레벨을 감소시키는 단계를 더 포함하는, 자원 액세스를 제어하는 방법.

청구항 24

제 23 항에 있어서,

상기 요청 노드가 하나 이상의 연속적인 시험 메시지들에 대해 부정확하게 대응하는 것에 응답하여, 상기 요청 노드가 상기 IoT 네트워크를 통해 통신하는 것을 차단하는 단계를 더 포함하는, 자원 액세스를 제어하는 방법.

청구항 25

제 21 항에 있어서,

상기 IoT 네트워크가 새로운 네트워크 액세스 계층으로 이전하는 것에 응답하여 상기 요청 노드에 할당된 트러스트 레벨에 따라 상기 인증 절차를 주기적으로 완료하기 위한 요건을 조정하는 단계를 더 포함하는, 자원 액세스를 제어하는 방법.

청구항 26

제 21 항에 있어서,

상기 시험 메시지에 대한 상기 수신된 대응에 기초하여 상기 요청 노드에 트러스트 레벨을 할당하는 단계로서,

상기 요청 노드에 할당된 상기 트러스트 레벨은 각각 개별 트러스트 레벨을 갖는 노드들과 연관된 허가된 자원 액세스를 정의하는 트러스트 휴리스틱 논리 모델에서의 N 개의 트러스트 레벨들 중 하나를 포함하는, 상기 요청 노드에 트러스트 레벨을 할당하는 단계; 및

상기 요청 노드에 할당된 상기 트러스트 레벨을 상기 IoT 네트워크에서 하나 이상의 자원들에 대한 액세스를 통제하는 다른 노드에 통신하는 단계를 더 포함하고,

상기 IoT 네트워크에서의 상기 다른 노드는 상기 요청 노드에 할당된 상기 트러스트 레벨에만 기초하여, 통제된 상기 하나 이상의 자원들에 대한 액세스를 상기 요청 노드에 대해 허가할지 여부를 결정하는, 자원 액세스를 제어하는 방법.

청구항 27

제 21 항에 있어서,

상기 게이트키퍼 노드는 상기 제어된 자원에 대한 액세스를 할당받았고, 상기 게이트키퍼에 할당된 상기 액세스는 상기 게이트키퍼 노드에 의해 필요한 제 1 부분 및 상기 요청 노드에 공급될 수 있는 여분의 부분을 포함하는, 자원 액세스를 제어하는 방법.

청구항 28

제 27 항에 있어서,

상기 제어된 자원에 대한 액세스를 상기 요청 노드에 대해 허가할지 여부를 결정하는 단계는, 상기 시험 메시지에 대한 상기 수신된 대응이 정확했다는 결정에 응답하여, 상기 제어된 자원에 대한 상기 할당된 액세스의 상기 여분의 부분을 상기 요청 노드에 공급하는 단계를 포함하는, 자원 액세스를 제어하는 방법.

청구항 29

제 28 항에 있어서,

상기 게이트키퍼 노드에게 상기 제어된 자원에 대한 상기 할당된 액세스의 상기 여분의 부분을 공급하도록 상기 요청 노드가 요청하는 것에 응답하여, 상기 게이트키퍼 노드는 상기 요청 노드에 상기 시험 메시지를 송신하는, 자원 액세스를 제어하는 방법.

청구항 30

제 21 항에 있어서,

상기 제어된 자원은, 소비율과 동일하거나 소비율을 초과하는 생산율을 갖는 무제한의 자원 또는 생산율을 초과하는 소비율을 갖는 한정된 자원 중 하나 이상을 포함하는, 자원 액세스를 제어하는 방법.

발명의 설명

기 술 분 야

[0001] **관련 출원들에 대한 상호-참조**

[0002] 본 특허 출원은, "TRUST HEURISTIC MODEL FOR REDUCING CONTROL LOAD IN IOT RESOURCE ACCESS NETWORKS" 라는 제목으로 2013년 6월 28일 출원된 미국 출원 제 61/841,068 호 및 2014년 6월 25일 출원된 미국 출원 제 14/314,999 호의 이익을 주장하고, 그 전체가 참조에 의해 본원에 명시적으로 통합된다.

[0003] **기술 분야**

[0004] 본 명세서에 설명된 다양한 실시형태들은 일반적으로, 트러스트 휴리스틱 모델 (trust heuristic model) 을 이용하여 사물 인터넷 (Internet of Things; IoT) 자원 (resource) 액세스 네트워크들에서 제어 부하 (control load) 를 감소시키는 것에 관한 것이다.

배 경 기 술

[0005] 인터넷은 서로 통신하기 위해 표준 인터넷 프로토콜 스위트 (예컨대, 송신 제어 프로토콜 (Transmission

Control Protocol; TCP) 및 인터넷 프로토콜 (Internet Protocol; IP)) 을 사용하는 상호접속된 컴퓨터들 및 컴퓨터 네트워크들의 글로벌 시스템이다. 사물 인터넷 (IoT) 은 단지 컴퓨터들 및 컴퓨터 네트워크들만이 아닌 일상 개체들이, IoT 통신 네트워크 (예컨대, 애드-혹 시스템 또는 인터넷) 를 통해 판독가능, 인식가능, 위치결정가능, 어드레싱가능, 및 제어가능할 수 있다는 아이디어에 기초하고 있다.

[0006] 다수의 시장 경향들이 IoT 디바이스들의 개발을 추진시키고 있다. 예를 들어, 증가하는 에너지 비용들이 미래의 소비에 대한, 이를테면 전기 차량들과 공공 충전 스테이션들에 대한 지원과 스마트 그리드들에서 정부의 전략적 투자를 추진시키고 있다. 증가하는 보건 (health care) 비용들 및 노령화 인구 (aging populations) 는 원격/접속된 보건 및 신체단련 (fitness) 서비스들에 대한 개발을 추진시키고 있다. 가정에서의 기술 혁명은, 'N' 플레이 (예컨대, 데이터, 음성, 비디오, 보안, 에너지 관리 등) 를 시판하고 홈 네트워크들을 확장하는 서비스 제공자들에 의한 통합 (consolidation) 을 포함한 새로운 "스마트" 서비스들에 대한 개발을 추진시키고 있다. 빌딩들은 기업 시설들에 대한 운영 비용들을 감소시키는 수단으로서 더 스마트해지고 더욱 편리해지고 있다.

[0007] IoT에 대한 다수의 핵심 애플리케이션들이 있다. 예를 들어, 스마트 그리드들과 에너지 관리의 영역에서, 공익 기업들은 가정들 및 사업장들로의 에너지의 전달을 최적화할 수 있으면서도 고객들은 에너지 사용량을 양호하게 관리할 수 있다. 가정 및 빌딩 자동화의 영역에서, 스마트 홈들 및 빌딩들은 가정 또는 사무실에서 가전기기들부터 플러그 인 전기 차량 (plug-in electric vehicle, PEV) 보안 시스템들까지 임의의 디바이스 또는 시스템 전체에 걸쳐 가상적으로 중앙 제어를 할 수 있다. 자산 추적의 영역에서, 기업들, 병원들, 공장들, 및 다른 대규모 조직들은 고가의 장비, 환자들, 차량들 등의 로케이션들을 정확히 추적할 수 있다. 건강과 웰빙의 영역에서, 의사들은 환자들의 건강을 원격으로 모니터링할 수 있으면서도 사람들은 신체단련 루틴들의 진행을 추적할 수 있다.

[0008] 이와 같이, 가까운 미래에, IoT 기술들에서의 증가하는 발달은 가정에서, 운송수단들에서, 직장에서, 그리고 많은 다른 장소들에서 사용자를 둘러싸는 수많은 IoT 디바이스들을 초래할 것이다. 많은 경우들에서, IoT 네트워크들은 상이한 IoT 가능 디바이스들이 액세스를 필요로할 수도 있는 다양한 자원들을 포함할 수도 있고, 이에 의해, 제어되는 자원들에 대한 액세스를 인증 (authenticate) 하거나 그 외에 통제 (regulate) 하기 위해 제어 메커니즘들이 사용될 수도 있다. 따라서, 특정 제어된 자원을 액세스하는 IoT 가능 디바이스들은 제어되는 자원에 대한 액세스를 주기적으로 인증하기 위해 "올웨이즈-온 (always-on)" 네트워크 접속을 필요로할 수도 있고, 이는, 제어되는 자원에 대한 액세스를 통제 또는 그 외에 제어하는 서버들 또는 다른 인증 엔티티들 (entities) 이, 제어되는 자원을 액세스하는 서비스들을 방해하고 클라이언트들이 그 서비스들에 액세스하는 것을 방지할 수도 있는 실질적인 제어 부하를 경험할 수도 있기 때문에, 다양한 문제점들을 초래할 수도 있다. IoT 개념에 적응될 때, 네트워크가, 제어되는 자원을 액세스하기 위해 제어 채널을 통해 통신하는 다양한 디바이스들을 포함하는 경우에, 제어 채널 상의 과도한 트래픽 (traffic) 은 잠재적으로 자원 사용을 방해할 수 있을 것이다. 따라서, IoT 네트워크들에서 제어된 자원들에 대한 액세스를 인증 또는 그 외에 제어하기 위해 이용되는, 제어 부하들을 감경하기 위해 이용될 수도 있는 메커니즘들에 대한 필요성이 존재한다.

발명의 내용

과제의 해결 수단

[0009] 이하에서는 트러스트 휴리스틱 모델을 이용하여 사물 인터넷 (IoT) 자원 액세스 (access) 네트워크들에서 제어 부하를 감소시키기 위한 본 명세서에서 개시된 메커니즘들과 연관된 하나 이상의 양태들 및/또는 실시형태들에 관한 간단한 개요를 제시한다. 이와 같이, 이하의 개요는 모든 고려되는 양태들 및/또는 실시형태들에 관한 확장적 개관으로서 고려되어서도 아니되며, 이하의 개요는 모든 고려되는 양태들 및/또는 실시형태들에 관련된 주요한 또는 결정적 요소들을 식별하거나 임의의 특정 양태 및/또는 실시형태와 연관된 범위를 기술하기 위한 것으로서 간주되어서도 아니된다. 따라서, 이하의 개요는 트러스트 휴리스틱 모델을 이용하여 IoT 자원 액세스 네트워크들에서 제어 부하를 감소시키기 위한 본 명세서에서 개시된 메커니즘들에 관한 하나 이상의 양태들 및/또는 실시형태들에 관련된 소정의 개념들을 이하 제시되는 상세한 설명에 앞서 단순한 형태로 제시하기 위한 목적만을 갖는다.

[0010] 하나의 예시적인 양태에 따르면, IoT 자원 액세스 네트워크에서 제어 부하를 감소시키기 위해 사용되는 트러스트 휴리스틱 모델은, 제어된 자원을 액세스하기를 원하는 요청 노드와, 제어된 자원을 통제하거나, (예컨대, 요청 노드가 통제 노드에 직접 접촉할 수 없는 경우에) 요청 노드와 제어된 자원을 통제하는 노드 사이에 액세스

를 중계하기 위한 중재자로서 작용하는 인증 노드 사이에 사용되는 시험-및-대응 메커니즘 (challenge-and-response mechanism) 에 기초할 수도 있다. 예를 들어, 인증 노드는 제어된 자원에 대한 액세스를 요청하는 노드에 시험 (challenge) 을 전송하고, 그 시험에 대한 대응 (response) 에 기초하여 요청된 액세스를 허가할지 여부를 결정할 수도 있다. 이와 같이, 인증 노드는, 요청 노드가 시험에 대해 정확하게 대응하는 경우에 요청된 액세스를 일반적으로 허가하고, 또는 대안적으로, 요청 노드가 시험에 대해 부정확하게 대응하는 경우에 요청된 액세스를 거부할 수도 있다. 또한, 인증 노드는, 초기 시험에 대한 대응이 정확했거나 부정확했는지 여부에 기초하여 요청 노드에 적절한 트러스트 레벨을 할당할 수도 있고, 요청 노드에 할당되는 트러스트 레벨은 연속적인 시험-및-대응 교환들 및/또는 IoT 네트워크에서의 다른 노드들과의 상호작용들에 기초하여 동적으로 업데이트될 수도 있다.

[0011] 다른 예시적인 양태에 따르면, 시험-및-대응 메커니즘들은 종래에는, 시험에 대한 초기 정확한 대응 후에 시간에 따라 아무것도 변하지 않는 것을 보장하고 요청 노드를 주기적으로 재인증하기 위해 규칙적인 간격들로 반복되고, 이는 (예컨대, 무선 시스템에서) 제어 채널 상의 과도한 트래픽으로 인해 불필요한 대역폭을 점유하고 성능을 감소시킬 수도 있다. 반면에, 본 명세서에서 개시된 트러스트 휴리스틱 모델은 시험-및-대응 교환들 또는 자원 액세스를 제어하기 위해 그 외에 사용될 수도 있는 다른 트래픽과 연관된 제어 부하를 감소시킬 수도 있다. 예를 들어, 하나의 실시형태에서, 요청 노드가 초기 시험에 대해 정확하게 대응한 후에, 요청 노드가 시간에 걸쳐 하나 이상의 연속적인 시험들에 대해 계속 정확하게 대응하는 경우에 후속하는 시험들 사이의 간격들은 증가될 수도 있다. 또한, 요청 노드는, 인증 노드 및/또는 IoT 네트워크에서의 다른 노드들이 이전의 상호작용들로부터 그 요청 노드를 신뢰 (trust) 하는 경우에 시험들에 정확하게 대응할 필요 없이 제어된 자원에 대한 액세스를 허가받을 수도 있다. 대안적으로, 요청 노드가 시간에 걸쳐 하나 이상의 연속적인 시험들에 대해 부정확한 대응들을 계속하여 제공하는 경우에, 요청 노드는 제어된 자원을 액세스하는 것이 차단되거나 IoT 네트워크로부터 완전히 금지당할 수도 있다.

[0012] 또 다른 예시적인 양태에 따르면, 본 명세서에서 개시된 트러스트 휴리스틱 모델은 따라서, 시간에 걸쳐서 발생하는 연속적인 시험-및-대응 교환들에 기초하여 IoT 네트워크에서 2 개 이상의 노드들 사이의 트러스트를 모델링할 수도 있다. 또한, 트러스트는, 사람이 타인들과의 관계를 지인, 동료, 친구, 절친한 친구 등으로 분류할 수도 있는 것과 유사한 방식으로 상이한 레벨들로 모델링될 수도 있고, 여기서, 제어된 자원들에 대한 액세스는 IoT 네트워크에서의 노드들이 트러스트를 모델링하는 것을 허용하기 위해 유사한 경로들을 따라 정렬될 수 있다. 예를 들어, 트러스트 휴리스틱 모델은, 요청 노드들이 IoT 네트워크 내로 허용되고/되거나 IoT 네트워크로 포워딩되거나 그 외에 IoT 네트워크로 중계되는 메시지들을 가지도록 허용될 수도 있는 알려지지 않은 트러스트 레벨 (Unknown Trust level), 요청 노드들이 풍부한 또는 무제한의 (infinite) 자원들에 액세스하도록 허용될 수도 있는 예비적 트러스트 레벨 (Preliminary Trust level), 요청 노드들이 제한된, 제약된, 또는 다른 한정된 (finite) 자원들에 대해 액세스 허가될 수도 있는 신뢰된 레벨 (Trusted level), 요청 노드들이 보호된 자원들에 액세스하도록 허용될 수도 있는 확신 레벨 (Confidant level), 및 다수의 연속적인 시험들에 대해 정확하게 대응하는 것에 실패한 요청 노드들이 IoT 네트워크로부터 금지당할 수도 있는 신뢰되지 않는 레벨 (Not Trusted level) 을 포함할 수도 있다. 따라서, 트러스트 휴리스틱 모델은 일반적으로 N 개 (예컨대, 상기 설명된 예시적인 트러스트 휴리스틱 모델에서 5 개) 의 트러스트 레벨들을 가질 수도 있고, 노드는 시간에 걸친 IoT 네트워크에서의 다른 노드들 및 자원들과의 상호작용들에 기초하여 특정 트러스트 레벨을 할당받을 수도 있다. 예를 들어, 하나의 실시형태에서, 트러스트 휴리스틱 모델에서의 N 개의 트러스트 레벨들은 어떤 범위 내에서 정의될 수도 있고, 특정 노드는, 그 범위 내에서 디폴트 (default) 트러스트 메트릭 (metric) 을 처음에 할당받을 수도 있고, 이는 시험-및-대응 교환들, 다른 노드들 및 자원들과의 상호작용들, 또는 그 노드에 할당할 적절한 트러스트 레벨을 결정하기 위한 시간에 걸친 다른 적합한 기준들에 기초하여 후속하여 증가 또는 감소될 수도 있다.

[0013] 또 다른 예시적인 양태에 따르면, IoT 네트워크에서의 제어된 자원 액세스를 위한 방법은, 요청 노드에 의해, IoT 네트워크에서 제 1 제어된 자원에 대한 액세스를 요청하는 단계를 포함할 수도 있고, 자원에 대한 액세스는 인증 절차 (authentication procedure) 를 주기적으로 완료하기 위한 요건을 포함할 수도 있으며, 이 방법은, 제 1 게이트키퍼 (gatekeeper) 노드 (예컨대, 제어된 자원을 통제하는 통제 노드, 요청 노드와 제어된 자원을 통제하는 통제 노드 사이에 메시지들을 중계하는 중간 노드 등) 로부터 수신된 시험 메시지에 대해 대응하는 단계 및 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 자원에 대한 요청된 액세스를 수신하는 단계를 더 포함할 수도 있고, 여기서, 제 1 게이트키퍼 노드는 요청 노드가 하나 이상의 연속적인 시험 메시지들에 정확하게 대응하는 것에 응답하여 인증 차를 주기적으로 완료하기 위한 요건을 감경할 수도 있다. 예를 들어, 하나의 실시형태에서, 게이트키퍼 노드는, 인증 절차를 주기적으로 완료하기 위한 요건을 감경하기 위해 요청 노

드에 후속 시험 메시지를 송신하기 전에 간격을 증가시키고, 이에 의해 시험 메시지 및 그에 대한 대응을 교환하기 위해 사용되는 제어 채널 상의 부하를 감소시킬 수도 있다.

[0014] 또 다른 예시적인 양태에 따르면, IoT 네트워크에서 제어된 자원 액세스를 위한 방법은, 제 1 게이트키퍼 노드가, 시험 메시지에 대한 부정확한 대응을 제공하는 요청 노드로부터 수신하는 것에 응답하여 요청 노드와 연관된 트러스트 레벨을 감소시키는 것을 더 포함할 수도 있다. 또한, 제 1 게이트키퍼 노드는, 요청 노드가 시험 메시지에 대해 부정확하게 대응하고 시간에 걸쳐 하나 이상의 연속적인 시험 메시지들에 대해 계속하여 부정확하게 대응하는 것에 응답하여, 요청 노드가 IoT 네트워크를 통해 통신하는 것을 일시적으로 차단 및/또는 요청 노드가 IoT 네트워크를 통해 통신하는 것을 영구적으로 금지할 수도 있다. 또한, 하나의 실시형태에서, 제 1 게이트키퍼 노드는, IoT 네트워크가 새로운 네트워크 액세스 계층으로 이전 (migrating) 하는 것에 응답하여 요청 노드에 할당된 트러스트 레벨에 따라 인증 절차를 주기적으로 완료하기 위한 요건을 조정할 수도 있다 (예컨대, 예비적 트러스트 레벨을 갖는 노드들에 대해서는 여전히 시험들이 발행될 수도 있고, 신뢰된 상태를 갖는 노드들은 단일 시험을 발행받을 수도 있고, 확신 상태를 갖는 노드들에 대해서는 어떤 시험들도 발행되지 않을 수도 있다).

[0015] 또 다른 예시적인 양태에 따르면, 제어된 자원 액세스를 위한 방법은, 제 2 게이트키퍼 노드로부터 (예컨대, 그 IoT 네트워크 또는 다른 IoT 네트워크에서의) 제 2 제어된 자원에 대한 액세스를 요청하는 단계를 더 포함할 수도 있고, 여기서, 제 2 게이트키퍼 노드는, (예컨대, 요청 노드가 인증 절차를 완료할 것을 요구함이 없이) 요청 노드와, 요청 노드와 하나 이상의 이전 상호작용들을 갖는 신뢰된 노드 사이의 트러스트 레벨에만 기초하여 제 2 제어된 자원에 대한 액세스를 요청 노드에 대해 허가할지 여부를 결정할 수도 있다. 예를 들어, 하나의 실시형태에서, 요청 노드와 연관된 트러스트 레벨은 각각 개별 트러스트 레벨을 갖는 노드들과 연관된 허가된 자원 액세스를 정의하는 트러스트 휴리스틱 논리 모델에서의 N 개의 트러스트 레벨들 중 하나를 포함할 수도 있다. 더욱이, 다른 이용 경우들에서, 제 2 제어된 자원, 제 2 게이트키퍼 노드, 및/또는 신뢰된 노드가 그 IoT 네트워크 또는 다른 IoT 네트워크에 위치될 수도 있다.

[0016] 또 다른 예시적인 양태에 따르면, IoT 네트워크에서의 제어된 자원은 일반적으로 소비율과 동일하거나 소비율을 초과하는 생산율을 갖는 무제한의 자원 또는 생산율을 초과하는 소비율을 갖는 한정된 자원을 포함할 수도 있다. 제어된 자원이 생산율을 초과하는 소비율을 갖는 한정된 자원을 갖는 후자의 경우에, 게이트키퍼 노드는 한정된 자원에 대한 할당된 액세스를 갖는 중간 노드를 포함할 수도 있고, 중간 노드에 대해 할당된 액세스는 중간 노드가 필요로 하는 제 1 부분 및 하나 이상의 요청 노드들에 공급될 수 있는 여분의 부분 (extra portion) 을 포함할 수도 있다. 이와 같이, 제어된 자원에 대한 액세스를 요청할 때, 거기에 할당된 한정된 자원의 총 여분의 부분을 결정하기 위해 한정된 자원에 대한 할당된 액세스를 갖는 하나 이상의 중간 노드들을 접촉하고, 거기에 할당된 한정된 자원의 총 여분의 부분이 요청 노드가 필요로 하는 한정된 자원의 양을 충족하거나 초과한다는 결정에 응답하여, 하나 이상의 중간 노드들이 요청 노드가 필요로 하는 한정된 자원의 양을 공급하도록 요청할 수도 있다. 이러한 맥락에서, 요청 노드는, 하나 이상의 중간 노드들이 요청 노드가 필요로 하는 한정된 자원의 양을 공급하도록 요청하는 것에 응답하여, 하나 이상의 중간 노드들로부터 시험 메시지를 수신하고, 각각의 중간 노드에 시험 메시지에 대한 정확한 대응을 송신하는 것에 응답하여, 하나 이상의 중간 노드들로부터 필요한 한정된 자원의 양을 수신할 수도 있다.

[0017] 또 다른 예시적인 양태에 따르면, IoT 디바이스는, IoT 네트워크에서 제어된 자원에 대한 액세스를 요청하는 수단으로서, 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함할 수도 있는, 제어된 자원에 대한 액세스를 요청하는 수단, 게이트키퍼 노드로부터 수신된 시험 메시지에 대해 대응하는 수단, 및 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 제어된 자원에 대한 요청된 액세스를 수신하는 수단을 포함할 수도 있고, 게이트키퍼 노드는 IoT 디바이스가 하나 이상의 연속적인 시험 메시지들에 정확하게 대응하는 것에 응답하여 인증 절차를 주기적으로 완료하기 위한 요건을 감경할 수도 있다.

[0018] 또 다른 예시적인 양태에 따르면, 컴퓨터-판독가능 저장 매체는 컴퓨터-실행가능 명령들을 거기에 기록할 수도 있고, IoT 디바이스 상에서 컴퓨터-실행가능 명령들을 실행하는 것은 IoT 디바이스로 하여금, IoT 네트워크에서 제어된 자원에 대한 액세스를 요청하게 하고, 게이트키퍼 노드로부터 수신된 시험 메시지에 대해 대응하게 하며, 그리고 시험 메시지에 대해 정확하게 대응하는 것에 응답하여 제어된 자원에 대한 요청된 액세스를 수신하게 할 수도 있고, 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함할 수도 있고, 게이트키퍼 노드는 IoT 디바이스가 하나 이상의 연속적인 시험 메시지들에 정확하게 대응하는 것에 응답하여 인증 절차를 주기적으로 완료하기 위한 요건을 감경할 수도 있다.

[0019] 또 다른 예시적인 양태에 따르면, IoT 네트워크에서 자원 액세스를 제어하는 방법은, 다른 것들 중에서도, 요청 노드로부터 IoT 네트워크에서의 제어된 자원을 액세스하기 위한 요청을 수신하는 단계로서, 제어된 자원에 대한 액세스는 인증 절차를 주기적으로 완료하기 위한 요건을 포함하는, 상기 제어된 자원을 액세스하기 위한 요청을 수신하는 단계, 요청 노드에 시험 메시지를 송신하는 단계, 요청 노드로부터 시험 메시지에 대한 대응을 수신하는 단계, 및 시험 메시지에 대한 수신된 대응에 기초하여 제어된 자원에 대한 액세스를 요청 노드에 대해 허가할지 여부를 결정하는 단계를 포함할 수도 있고, 시험 메시지에 대한 수신된 대응이 정확했는지 여부에 기초하여 인증 절차를 주기적으로 완료하기 위한 요청 노드에 대한 요건이 조정될 수도 있다.

[0020] 본 명세서에서 설명된 트러스트 휴리스틱 모델을 이용하여 IoT 자원 액세스 네트워크들에서 제어 부하를 감소시키기 위한 본 명세서에서 개시된 메커니즘들과 연관된 다른 목적들 및 이점들은 첨부된 도면들과 상세한 설명에 기초하여 당해 기술분야에서 통상의 지식을 가진 자 (이하, '통상의 기술자' 라 함) 에게 명백할 것이다.

도면의 간단한 설명

[0021] 본 개시물의 양태들 및 그것에 수반되는 많은 이점들의 더 완전한 이해는 그것들이 본 개시물의 예시를 위해서만 제시되고 본 개시물의 제한은 아닌 첨부 도면들에 관련하여 고려되는 경우의 다음의 상세한 설명을 참조하여 더 잘 이해됨에 따라 쉽게 획득될 것이다.

도 1a 내지 도 1e 는, 본 개시물의 다양한 양태들에 따른, 무선 통신 시스템의 예시적인 하이-레벨 시스템 아키텍처들을 나타낸다.

도 2a 는 본 개시물의 다양한 양태들에 따른 예시적인 사물 인터넷 (IoT) 을 나타내고, 도 2b 는 본 개시물의 다양한 양태들에 따른 예시적인 수동 IoT 디바이스를 나타낸다.

도 3 은 본 개시물의 다양한 양태들에 따른, 기능성을 수행하도록 구성된 로직을 포함하는 예시적인 통신 디바이스를 나타낸다.

도 4 는 본 개시물의 다양한 양태들에 따른 예시적인 서버를 나타낸다.

도 5 는 본 개시물의 하나의 양태에 따른, IoT 자원 액세스 네트워크에서 제어 부하를 경감시키기 위해 이용될 수도 있는 예시적인 트러스트 휴리스틱 모델을 나타낸다.

도 6 은 본 개시물의 하나의 양태에 따른, IoT 자원 액세스 네트워크에서 제어된 자원에 대해 하나 이상의 클라이언트들이 액세스를 요청할 수도 있는 예시적인 통신 시나리오들을 나타낸다.

도 7 은 본 개시물의 하나의 양태에 따른, 트러스트 휴리스틱 모델을 이용하여 IoT 자원 액세스 네트워크에서 제어 부하가 감소될 수도 있는 예시적인 통신 시나리오들을 나타낸다.

도 8 은 본 개시물의 하나의 양태에 따른, IoT 네트워크에서의 클라이언트가, 제어된 자원에 대해 액세스를 요청하고 트러스트 휴리스틱 모델에 기초하여 그것과 연관된 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법을 나타낸다.

도 9 는 본 개시물의 하나의 양태에 따른, IoT 네트워크에서 제어된 자원에 대한 예약된 액세스를 갖는 중간 노드가, 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법을 나타낸다.

도 10 은 본 개시물의 하나의 양태에 따른, IoT 네트워크에서 제어된 자원에 대한 예약된 액세스를 갖지 않는 중간 노드가, 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법을 나타낸다.

도 11 은 본 개시물의 하나의 양태에 따른, IoT 네트워크에서 제어된 자원에 대한 액세스를 통제하는 중간 노드가, 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0022] 사물 인터넷 (IoT) 자원 액세스 네트워크에서의 제어 부하가 트러스트 휴리스틱 모델을 이용하여 감소될 수도 있는 예시적인 실시형태들에 관련된 구체적인 예들을 나타내기 위해 다양한 양태들이 이하의 설명 및 관련 도면들에서 개시된다. 대체 실시형태들은 통상의 기술자에게는 본 개시물을 읽을 시 명확할 것이고, 본 개시물

의 범위 또는 사상으로부터 벗어남 없이 구축되고 실용화될 수도 있다. 덧붙여, 잘 알려진 엘리먼트들은 본원에서 개시된 양태들 및 실시형태들의 관련 세부사항들을 모호하게 하지 않기 위해서 상세히 설명되지 않을 것이거나 또는 생략될 수도 있다.

[0023] 단어 "예시적"은 본원에서는 "예, 사례, 또는 예시로서 역할을 한다"는 의미로 사용된다. "예시적인" 것으로서 본원에서 설명되는 어떤 실시형태라도 다른 실시형태들보다 바람직하거나 유익하다고 생각할 필요는 없다.

마찬가지로, "실시형태들"이란 용어는 모든 실시형태들이 논의되는 특징, 이점 또는 동작 모드를 포함할 것을 필요로 하지 않는다.

[0024] 본원에서 사용되는 기술용어는 특정 실시형태들만을 설명하고 본원에서 개시된 임의의 실시형태들로 제한하는 것으로 해석되어야 한다. 본원에서 사용되는 바와 같이, 문맥이 다르다고 명확히 나타내지 않는 한, 단수형들 "a", "an", 및 "the" 는 복수형도 포함하는 것을 의도하고 있다. "포함한다", "포함하는", "구비한다" 및/또는 "구비하는"이란 용어들은, 본원에서 사용될 때, 언급된 특징들, 정수들, 단계들, 동작들, 엘리먼트들, 및/또는 구성요소들의 존재를 명시하지만, 하나 이상의 다른 특징들, 정수들, 단계들, 동작들, 엘리먼트들, 구성요소들, 및/또는 그 그룹들의 존재 또는 추가를 배제하지는 않는다는 것이 추가로 이해될 것이다.

[0025] 게다가, 많은 양태들은 예를 들어 컴퓨팅 디바이스의 엘리먼트들에 의해 수행될 액션들의 시퀀스들의 측면에서 설명된다. 본원에서 설명되는 다양한 액션들은 특정 회로들 (예, 주문형 집적 회로 (ASIC)) 에 의해, 하나 이상의 프로세서들에 의해 실행되는 프로그램 명령들에 의해, 또는 양 쪽 모두의 조합에 의해 수행될 수 있음이 이해될 것이다. 덧붙여, 본원에서 설명되는 액션들의 이들 시퀀스는 실행 시 연관된 프로세서로 하여금 본원에서 설명된 기능을 수행하도록 할 컴퓨터 명령들의 대응하는 세트를 저장하고 있는 임의의 형태의 컴퓨터 판독가능 저장 매체 내에 완전히 수록된다고 생각될 수 있다. 그래서, 본 개시물의 다양한 양태들은 다수의 상이한 형태들로 실시될 수도 있으며, 그 형태들의 전부는 청구된 요지의 범위 내 있는 것이라고 의도되고 있다. 덧붙여서, 본원에서 설명된 양태들의 각각에 대해, 임의의 그런 양태들 중 대응하는 형태는 예를 들어 설명된 액션을 수행"하도록 구성된 로직"으로서 본원에서 설명될 수도 있다.

[0026] 본원에서 사용되는 바와 같이, "사물 인터넷 디바이스" (또는 "IoT 디바이스") 라는 용어는 어드레스가능 인터페이스 (예컨대, 인터넷 프로토콜 (IP) 어드레스, 블루투스 식별자 (ID), 근접장 통신 (near-field communication; NFC) ID 등) 를 갖고 유선 또는 무선 접속을 통해 정보를 하나 이상의 다른 디바이스들로 송신할 수 있는 임의의 개체 (예컨대, 가전기기, 센서 등) 를 지칭하는데 사용된다. IoT 디바이스가 수동적 통신 인터페이스, 이를테면 신속 대응 (quick response; QR) 코드, 라디오-주파수 식별 (radio-frequency identification; RFID) 태그, NFC 태그 등 또는 능동적 (active) 통신 인터페이스, 이를테면 모뎀, 트랜시버, 송신기-수신기 등을 가질 수도 있다. IoT 디바이스가 중앙 프로세싱 유닛 (CPU), 마이크로프로세서, ASIC 등에 내장될 수 있고 및/또는 그것들에 의해 제어/모니터링될 수 있는 그리고 로컬 애드-혹 네트워크 또는 인터넷과 같은 IoT 네트워크에 대한 접속을 위해 구성될 수 있는 특정 세트의 속성들 (예컨대, IoT 디바이스가 온인지 또는 오프인지, 개방인지 또는 폐쇄인지, 유휴인지 또는 활동인지, 태스크 실행을 위해 이용가능한지 또는 사용중 (busy) 인지 등과 같은 디바이스 상태 또는 스테이터스, 냉각 또는 가열 기능, 환경 모니터링 또는 레코딩 기능, 광 방출 기능, 사운드 방출 기능 등) 을 가질 수 있다. 예를 들어, IoT 디바이스들에 IoT 네트워크와 통신하기 위한 어드레스가능 통신 인터페이스가 장비되는 한, IoT 디바이스들은 냉장고들, 토스터들, 오븐들, 전자레인지들, 냉동고들, 식기세척기들, 접시들, 수공구들, 의류 세탁기들, 의류 건조기들, 난로들 (furnaces), 에어 컨디셔너들, 서모스탯들 (thermostats), 텔레비전들, 조명 기구들, 진공 청소기들, 스프링클러들, 전기 계량기들, 가스 계량기들 등을 비제한적으로 포함할 수도 있다. IoT 디바이스들은 셀 폰들, 데스크톱 컴퓨터들, 랩톱 컴퓨터들, 태블릿 컴퓨터들, 개인 정보 단말기들 (PDA들) 등을 또한 포함할 수도 있다.

따라서, IoT 네트워크는 인터넷 접속성을 통상 갖지 않는 디바이스들 (예컨대, 식기세척기들 등) 에 더하여 "레거시" 인터넷 액세스가능 디바이스들 (예컨대, 랩톱 또는 데스크톱 컴퓨터들, 셀 폰들 등) 의 조합을 포함할 수도 있다.

[0027] 도 1a 는 본 개시물의 일 양태에 따른 무선 통신 시스템 (100A) 의 하이레벨 시스템 아키텍처를 도시한다. 무선 통신 시스템 (100A) 은 텔레비전 (110), 실외 에어 컨디셔닝 유닛 (112), 서모스탯 (114), 냉장고 (116), 그리고 세탁기 및 건조기 (118) 를 포함하는 복수의 IoT 디바이스들을 구비한다.

[0028] 도 1a 를 참조하면, IoT 디바이스들 (110-118) 은 에어 인터페이스 (108) 와 직접 유선 접속 (109) 으로서 도 1a 에서 도시된 물리적 통신 인터페이스 또는 계층을 통해 액세스 네트워크 (예컨대, 액세스 포인트 (125)) 와 통신하도록 구성된다. 에어 인터페이스 (108) 는 무선 인터넷 프로토콜 (IP), 이를테면 IEEE 802.11을 준수

할 수 있다. 비록 도 1a 가 에어 인터페이스 (108) 를 통해 통신하는 IoT 디바이스들 (110-118) 과 직접 유선 접속 (109) 을 통해 통신하는 IoT 디바이스 (118) 를 예시하지만, 각각의 IoT 디바이스는 유선 또는 무선 접속, 또는 양쪽 모두를 통해 통신할 수도 있다.

[0029] 인터넷 (175) 은 다수의 라우팅 에이전트들 및 프로세싱 에이전트들 (편의를 위해 도 1a 에서 도시되지 않음) 을 포함한다. 인터넷 (175) 은 이질적인 디바이스들/네트워크들 간에 통신하기 위한 표준 인터넷 프로토콜 스위트 (예컨대, 송신 제어 프로토콜 (TCP) 및 인터넷 프로토콜 (IP)) 를 사용하는 상호접속된 컴퓨터들 및 컴퓨터 네트워크들의 글로벌 시스템이다. TCP/IP는 데이터가 포맷팅, 어드레싱, 송신, 라우팅 및 목적지에서 수신되어야 하는 방법을 특정하는 엔드 대 엔드 접속성을 제공한다.

[0030] 도 1a 에서, 컴퓨터 (120), 이를테면 데스크톱 또는 개인용 컴퓨터 (PC) 가, (예컨대, 이더넷 접속 또는 Wi-Fi 또는 802.11 기반 네트워크를 통해) 인터넷 (175) 에 직접적으로 접속되어 있는 것으로서 도시되어 있다. 컴퓨터 (120) 는 인터넷 (175) 에 대한 유선 접속, 이를테면 모뎀 또는 라우터에 대한 직접 접속을 가질 수도 있는데, 이 접속은, 일 예에서, (예컨대, 유선 및 무선 양쪽 모두의 접속성을 갖는 Wi-Fi 라우터의 경우) 액세스 포인트 (125) 자체에 해당할 수 있다. 대안으로, 유선 접속을 통해 액세스 포인트 (125) 와 인터넷 (175) 에 연결되어 있는 대신에, 컴퓨터 (120) 는 에어 인터페이스 (108) 또는 다른 무선 인터페이스를 통해 액세스 포인트 (125) 에 접속될 수도 있고, 에어 인터페이스 (108) 를 통해 인터넷 (175) 에 액세스할 수도 있다.
비록 데스크톱 컴퓨터로서 도시되었지만, 컴퓨터 (120) 는 랩톱 컴퓨터, 태블릿 컴퓨터, PDA, 스마트 폰 등일 수도 있다. 컴퓨터 (120) 는 IoT 디바이스일 수도 있고 그리고/또는 IoT 네트워크/그룹, 이를테면 IoT 디바이스들 (110-118) 의 네트워크/그룹을 관리하는 기능성을 포함할 수도 있다.

[0031] 액세스 포인트 (125) 는, 예를 들어, 광학적 통신 시스템, 이를테면 FiOS, 케이블 모뎀, 디지털 가입자 회선 (digital subscriber line; DSL) 모뎀 등을 통해 인터넷 (175) 에 접속될 수도 있다. 액세스 포인트 (125) 는 표준 인터넷 프로토콜들 (예컨대, TCP/IP) 을 사용하여 IoT 디바이스들 (110-120) 및 인터넷 (175) 과 통신할 수도 있다.

[0032] 도 1a 를 참조하면, IoT 서버 (170) 가 인터넷 (175) 에 접속된 것으로 도시되어 있다. IoT 서버 (170) 는 복수의 구조적으로 별개의 서버들로서 구현될 수 있거나, 또는 다르게는 단일 서버에 해당할 수도 있다. 일 양태에서, IoT 서버 (170) 는 (점선에 의해 나타낸 바와 같이) 옵션적이고, IoT 디바이스들 (110-120) 의 그룹은 피어-투-피어 (peer-to-peer; P2P) 네트워크일 수도 있다. 이러한 경우에, IoT 디바이스들 (110-120) 은 에어 인터페이스 (108) 및/또는 직접 유선 접속 (109) 을 통해 서로 직접적으로 통신할 수 있다. 대안으로, 또는 덧붙여, IoT 디바이스들 (110-120) 의 일부 또는 전부는 에어 인터페이스 (108) 및 직접 유선 접속 (109) 과는 독립적인 통신 인터페이스로 구성될 수도 있다. 예를 들어, 에어 인터페이스 (108) 가 Wi-Fi 인터페이스에 해당하면, IoT 디바이스들 (110-120) 중 하나 이상은 서로 또는 다른 블루투스 또는 NFC 가능 디바이스들과 직접적으로 통신하기 위한 블루투스 또는 NFC 인터페이스들을 가질 수도 있다.

[0033] 피어-투-피어 네트워크에서, 서비스 발견 체계들이 노드들의 존재, 그것들의 능력들, 및 그룹 맴버십을 멀티캐스트할 수 있다. 피어-투-피어 디바이스들은 이 정보에 기초하여 연관들 및 후속 상호작용들을 확립할 수 있다.

[0034] 본 개시물의 일 양태에 따라, 도 1b 는 복수의 IoT 디바이스들을 포함하는 다른 무선 통신 시스템 (100B) 의 하이레벨 아키텍처를 도시한다. 대체로, 도 1b 에 도시된 무선 통신 시스템 (100B) 은 위에서 매우 상세히 설명되었던 도 1a 에 도시된 무선 통신 시스템 (100A) 과는 동일한 및/또는 실질적으로 유사한 다양한 컴포넌트들 (예컨대, 에어 인터페이스 (108) 및/또는 직접 유선 접속 (109) 을 통해 액세스 포인트 (125) 와 통신하도록 구성된, 텔레비전 (110), 실외 에어 컨디셔닝 유닛 (112), 서모스탯 (114), 냉장고 (116), 그리고 세탁기 및 건조기 (118) 를 포함한 다양한 IoT 디바이스들, 인터넷 (175) 에 직접적으로 접속하는 및/또는 액세스 포인트 (125) 를 통해 인터넷 (175) 에 접속하는 컴퓨터 (120), 그리고 인터넷 (175) 을 통해 액세스가능한 IoT 서버 (170) 등) 을 포함할 수도 있다. 이처럼, 설명의 간결함 및 편의를 위해, 도 1b 에 도시된 무선 통신 시스템 (100B) 에서의 특정한 컴포넌트들에 관련한 다양한 세부사항들은 동일한 또는 유사한 세부사항들이 도 1a 에 도시된 무선 통신 시스템 (100A) 에 관련하여 위에서 이미 제공되었던 결과로 여기서는 생략될 수도 있다.

[0035] 도 1b 를 이제 참조하면, 무선 통신 시스템 (100B) 은 감독자 디바이스 (130) 를 포함할 수도 있는데, 감독자 디바이스는 다르게는 IoT 관리자 (130) 또는 IoT 관리자 디바이스 (130) 라고 지칭될 수도 있다. 이처럼, 다음의 설명이 "감독자 디바이스" (130) 라는 용어를 사용하는 경우, 통상의 기술자는 IoT 관리자, 그룹 소유자, 또는 유사한 기술용어에 대한 임의의 언급들이 감독자 디바이스 (130) 또는 동일한 또는 실질적으로 유

사한 기능을 제공하는 다른 물리적 또는 논리적 컴포넌트를 지칭할 수도 있다는 것을 이해할 것이다.

[0036] 하나의 실시형태에서, 감독자 디바이스 (130) 는 무선 통신 시스템 (100B) 에서의 다양한 다른 컴포넌트들을 일반적으로 관찰, 모니터링, 제어, 또는 그렇지 않으면 관리할 수도 있다. 예를 들어, 감독자 디바이스 (130) 는 무선 통신 시스템 (100B) 에서의 다양한 IoT 디바이스들 (110-120) 에 연관된 속성들, 활동들, 또는 다른 상태들을 모니터링 또는 관리하기 위해 에어 인터페이스 (108) 및/또는 직접 유선 접속 (109) 을 통해 액세스 네트워크 (예컨대, 액세스 포인트 (125)) 와 통신할 수 있다. 감독자 디바이스 (130) 는 인터넷 (175) 에 대해 그리고 옵션으로는 IoT 서버 (170) (점선으로 도시됨) 에 대해 유선 또는 무선 접속을 가질 수도 있다. 감독자 디바이스 (130) 는 다양한 IoT 디바이스들 (110-120) 에 연관된 속성들, 활동들, 또는 다른 상태들을 추가로 모니터링 또는 관리하는데 사용될 수 있는 정보를 인터넷 (175) 및/또는 IoT 서버 (170) 로부터 획득할 수도 있다. 감독자 디바이스 (130) 는 자립형 디바이스일 수도 있거나 또는 IoT 디바이스들 (110-120) 중 하나, 이를테면 컴퓨터 (120) 일 수도 있다. 감독자 디바이스 (130) 는 물리적 디바이스 또는 물리적 디바이스 상에서 실행중인 소프트웨어 애플리케이션일 수도 있다. 감독자 디바이스 (130) 는 IoT 디바이스들 (110-120) 에 연관된 모니터링된 속성들, 활동들, 또는 다른 상태들에 관련한 정보를 출력할 수 있고 그것들에 연관된 속성들, 활동들, 또는 다른 상태들을 제어 또는 그렇지 않으면 관리하기 위해 입력 정보를 수신할 수 있는 사용자 인터페이스를 포함할 수도 있다. 따라서, 감독자 디바이스 (130) 는 다양한 컴포넌트들을 일반적으로 포함할 수도 있고 무선 통신 시스템 (100B) 에서 상기 다양한 컴포넌트들을 관찰, 모니터링, 제어, 또는 그렇지 않으면 관리하기 위해 다양한 유선 및 무선 통신 인터페이스들을 지원할 수도 있다.

[0037] 도 1b 에 도시된 무선 통신 시스템 (100B) 은 (능동적 IoT 디바이스들 (110-120) 과는 대조적으로) 무선 통신 시스템 (100B) 의 부분에 커플링될 수 있거나 또는 그렇지 않으면 무선 통신 시스템 (100B) 의 부분이 될 수 있는 하나 이상의 수동적 IoT 디바이스들 (105) 을 포함할 수도 있다. 대체로, 수동적 IoT 디바이스들 (105) 은 바코드식 디바이스들, 블루투스 디바이스들, 무선 주파수 (RF) 디바이스들, RFID 태그식 디바이스들, 적외선 (IR) 디바이스들, NFC 태그식 디바이스들, 또는 단거리 인터페이스를 통해 질의될 경우 자신의 식별자 및 속성들을 다른 디바이스에 제공할 수 있는 임의의 다른 적합한 디바이스를 포함할 수도 있다. 능동적 IoT 디바이스들은 수동적 IoT 디바이스들의 속성들에서의 변경들을 검출, 저장, 통신 및 그 변경들에 따른 작용 등을 할 수도 있다.

[0038] 예를 들어, 수동적 IoT 디바이스들 (105) 은 RFID 태그 또는 바코드를 각각이 갖는 커피 잔 및 오렌지 쥬스 용기를 포함할 수도 있다. 커피 잔 및/또는 오렌지 쥬스 용기 수동적 IoT 디바이스들 (105) 이 추가 또는 제거되었을 경우를 검출하기 위해 RFID 태그 또는 바코드를 판독할 수 있는 적절한 스캐너 또는 판독기를 캐비넷 IoT 디바이스와 냉장고 IoT 디바이스 (116) 가 각각 가질 수도 있다. 캐비넷 IoT 디바이스가 커피 잔 수동적 IoT 디바이스 (105) 의 제거를 검출하는 것과 냉장고 IoT 디바이스 (116) 가 오렌지 쥬스 용기 수동적 IoT 디바이스의 제거를 검출하는 것에 응답하여, 감독자 디바이스 (130) 는 캐비넷 IoT 디바이스 및 냉장고 IoT 디바이스 (116) 에서 검출된 활동들에 관련한 하나 이상의 신호들을 수신할 수도 있다. 감독자 디바이스 (130) 는 그 다음에 사용자가 오렌지 쥬스를 커피 잔으로 마시고 있다고 그리고/또는 오렌지 쥬스를 커피 잔으로 마실 가능성이 있다고 유추할 수도 있다.

[0039] 비록 전술한 바가 RFID 태그 또는 바코드 통신 인터페이스의 일부 형태를 갖는 것으로서 수동적 IoT 디바이스들 (105) 을 설명하지만, 수동적 IoT 디바이스들 (105) 은 이러한 통신 능력들을 갖지 않는 하나 이상의 디바이스들 또는 다른 물리적 개체들을 포함할 수도 있다. 예를 들어, 특정한 IoT 디바이스들은 수동적 IoT 디바이스들 (105) 을 식별하기 위해 수동적 IoT 디바이스들 (105) 에 연관된 형상들, 사이즈들, 컬러들, 및/또는 다른 관찰가능 특징들을 검출할 수 있는 적절한 스캐너 또는 판독기 메커니즘들을 가질 수도 있다. 이런 방식으로, 임의의 적합한 물리적 개체는 자신의 아이덴티티 및 속성들을 통신할 수도 있고, 무선 통신 시스템 (100B) 의 부분이 될 수도 있고, 감독자 디바이스 (130) 로 관찰, 모니터링, 제어, 또는 그렇지 않으면 관리될 수도 있다. 게다가, 수동적 IoT 디바이스들 (105) 은 도 1a 의 무선 통신 시스템 (100A) 의 부분에 커플링될 수도 있거나 또는 상기 부분이 될 수도 있고 실질적으로 유사한 방식으로 관찰, 모니터링, 제어, 또는 그렇지 않으면 관리될 수도 있다.

[0040] 본 개시물의 다른 양태에 따라, 도 1c 는 복수의 IoT 디바이스들을 포함하는 다른 무선 통신 시스템 (100C) 의 하이레벨 아키텍처를 도시한다. 대체로, 도 1c 에 도시된 무선 통신 시스템 (100C) 은 위에서 더욱 상세히 설명되었던 도 1a 및 도 1b 에 각각 도시된 무선 통신 시스템들 (100A 및 100B) 과는 동일한 및/또는 실질적으로 유사한 다양한 컴포넌트들을 포함할 수도 있다. 이처럼, 설명의 간결함 및 편의를 위해, 도 1c 에 도시된 무선 통신 시스템 (100C) 에서의 특정한 컴포넌트들에 관련한 다양한 세부사항들은 동일한 또는 유사한 세부

사항들이 도 1a 및 도 1b 에 각각 도시된 무선 통신 시스템들 (100A 및 100B) 에 관련하여 위에서 이미 제공되었던 결과로 여기서는 생략될 수도 있다.

[0041] 도 1c 에 도시된 통신 시스템 (100C) 은 IoT 디바이스들 (110-118) 및 감독자 디바이스 (130) 간의 예시적인 피어-투-피어 통신들을 도시한다. 도 1c 에 도시된 바와 같이, 감독자 디바이스 (130) 는 IoT 감독자 인터페이스를 통해 IoT 디바이스들 (110-118) 의 각각과 통신한다. 게다가, IoT 디바이스들 (110 및 114), IoT 디바이스들 (112, 114, 및 116), 및 IoT 디바이스들 (116 및 118) 은 서로 직접적으로 통신한다.

[0042] IoT 디바이스들 (110-118) 은 IoT 그룹 (160) 을 구성한다. IoT 디바이스 그룹 (160) 이 사용자의 홈 네트워크에 접속된 IoT 디바이스들과 같은 논리적으로 연결된 IoT 디바이스들의 그룹이다. 비록 도시되지 않았지만, 다수의 IoT 디바이스 그룹들은 서로에게 접속될 수도 있고 및/또는 인터넷 (175) 에 접속된 IoT 슈퍼에이전트 (140) 를 통해 서로 통신할 수도 있다. 하이 레벨에서, 감독자 디바이스 (130) 는 그룹 내 통신들을 관리하는 반면, IoT 슈퍼에이전트 (140) 는 그룹 간 통신들을 관리할 수 있다. 비록 별개의 디바이스들로서 도시되었지만, 감독자 디바이스 (130) 와 IoT 슈퍼에이전트 (140) 는 동일한 디바이스 (예컨대, 자립형 디바이스 또는 IoT 디바이스, 이를테면 도 1a 에서의 컴퓨터 (120)) 일 수도 있거나, 또는 그런 디바이스 상에 존재할 수도 있다. 대안으로, IoT 슈퍼에이전트 (140) 는 액세스 포인트 (125) 의 기능에 해당할 수도 있거나 또는 그 기능을 포함할 수도 있다. 또 다른 대체예로서, IoT 슈퍼에이전트 (140) 는 IoT 서버, 이를테면 IoT 서버 (170) 의 기능에 해당할 수도 있거나 또는 그 기능을 포함할 수도 있다. IoT 슈퍼에이전트 (140) 는 게이트웨이 기능 (145) 을 캡슐화할 수도 있다.

[0043] 각각의 IoT 디바이스 (110-118) 는 감독자 디바이스 (130) 를 피어로서 취급할 수 있고 속성/스키마 업데이트들을 감독자 디바이스 (130) 로 송신할 수 있다. IoT 디바이스가 다른 IoT 디바이스와 통신할 것이 필요한 경우, 그 IoT 디바이스는 감독자 디바이스 (130) 로부터 당해 IoT 디바이스에 대한 포인터를 요청한 다음 피어로서의 타겟 IoT 디바이스와 통신할 수 있다. IoT 디바이스들 (110-118) 은 공통 메시징 프로토콜 (common messaging protocol; CMP) 을 사용하여 피어-투-피어 통신 네트워크를 통해 서로 통신한다. 2 개의 IoT 디바이스들이 CMP 가능식이고 공통 통신 전송을 통해 접속되는 한, 그 IoT 디바이스들은 서로 통신할 수 있다. 프로토콜 스택에서, CMP 계층 (154) 은 애플리케이션 계층 (152) 아래에 있고 전송 계층 (156) 및 물리 계층 (158) 위에 있다.

[0044] 본 개시물의 다른 양태에 따라, 도 1d 는 복수의 IoT 디바이스들을 포함하는 다른 무선 통신 시스템 (100D) 의 하이레벨 아키텍처를 도시한다. 대체로, 도 1d 에 도시된 무선 통신 시스템 (100D) 은 위에서 더욱 상세히 설명되었던 도 1c 에 각각 도시된 무선 통신 시스템들 (100A 내지 100C) 과는 동일한 및/또는 실질적으로 유사한 다양한 컴포넌트들을 포함할 수도 있다. 이처럼, 설명의 간결함 및 편의를 위해, 도 1d 에 도시된 무선 통신 시스템 (100D) 에서의 특정한 컴포넌트들에 관련한 다양한 세부사항들은 동일한 또는 유사한 세부사항들이 도 1a 내지 도 1c 에 각각 도시된 무선 통신 시스템들 (100A 내지 100C) 에 관련하여 위에서 이미 제공되었던 결과로 여기서는 생략될 수도 있다.

[0045] 인터넷 (175) 은 IoT의 개념을 사용하여 통제될 수 있는 "자원"이다. 그러나, 인터넷 (175) 은 통제되는 자원의 단지 하나의 예이고, 임의의 자원이 IoT의 개념을 사용하여 통제될 수 있다. 통제될 수 있는 다른 자원들은, 전기, 가스, 저장소, 보안 등을 비제한적으로 포함한다. IoT 디바이스가 자원에 접속되어서 그 자원을 통제할 수도 있거나, 또는 그 자원은 인터넷 (175) 을 통해 통제될 수 있다. 도 1d 는 여러 자원들 (180), 이를테면 천연 가스, 가솔린, 온수, 및 전기를 도시하고, 이 자원들 (180) 은 인터넷 (175) 에 부가하여 및/또는 그 인터넷을 통해 통제될 수 있다.

[0046] IoT 디바이스들은 자신들의 자원 (180) 의 사용을 통제하기 위해 서로 통신할 수 있다. 예를 들어, 토스터, 컴퓨터, 및 헤어드라이어와 같은 IoT 디바이스들은 자신들의 전기 (자원 (180)) 사용을 통제하기 위해 블루투스 통신 인터페이스를 통해 서로 통신할 수도 있다. 다른 예로서, 데스크톱 컴퓨터, 전화기, 및 태블릿 컴퓨터와 같은 IoT 디바이스들은 자신들의 인터넷 (175) (자원 (180)) 에 대한 액세스를 통제하기 위해 Wi-Fi 통신 인터페이스를 통해 통신할 수도 있다. 또 다른 예로서, 스토브, 의류 건조기, 및 온수기와 같은 IoT 디바이스들은 그것들의 가스 사용을 통제하기 위해 Wi-Fi 통신 인터페이스를 통해 통신할 수도 있다. 대안으로, 또는 덧붙여, 각각의 IoT 디바이스는 IoT 디바이스들로부터 수신된 정보에 기초하여 자신들의 자원 (180) 사용을 통제하는 로직을 갖는 IoT 서버, 이를테면 IoT 서버 (170) 에 접속될 수도 있다.

[0047] 본 개시물의 다른 양태에 따라, 도 1e 는 복수의 IoT 디바이스들을 포함하는 다른 무선 통신 시스템 (100E) 의 하이레벨 아키텍처를 도시한다. 대체로, 도 1e 에 도시된 무선 통신 시스템 (100E) 은 위에서 더욱 상세히

설명되었던 도 1a 내지 도 1d 에 각각 도시된 무선 통신 시스템들 (100A 내지 100D) 과는 동일한 및/또는 실질적으로 유사한 다양한 컴포넌트들을 포함할 수도 있다. 이처럼, 설명의 간결함 및 편의를 위해, 도 1e 에 도시된 무선 통신 시스템 (100E) 에서의 특정한 컴포넌트들에 관련한 다양한 세부사항들은 동일한 또는 유사한 세부사항들이 도 1a 내지 도 1d 에 각각 도시된 무선 통신 시스템들 (100A 내지 100D) 에 관련하여 위에서 이미 제공되었던 결과로 여기서는 생략될 수도 있다.

[0048] 통신 시스템 (100E) 은 2 개의 IoT 디바이스 그룹들 (160A 및 160B) 을 포함한다. 다수의 IoT 디바이스 그룹들은 서로에게 접속될 수도 있고 및/또는 인터넷 (175) 에 접속된 IoT 슈퍼에이전트를 통해 서로 통신할 수도 있다. 하이 레벨에서, IoT 슈퍼에이전트가 IoT 디바이스 그룹들 간에 그룹 간 통신들을 관리할 수도 있다. 예를 들어, 도 1e 에서, IoT 디바이스 그룹 (160A) 은 IoT 디바이스들 (116A, 122A, 및 124A) 과 IoT 슈퍼에이전트 (140A) 를 포함하는 한편, IoT 디바이스 그룹 (160B) 은 IoT 디바이스들 (116B, 122B, 및 124B) 과 IoT 슈퍼에이전트 (140B) 를 포함한다. 이처럼, IoT 슈퍼에이전트들 (140A 및 140B) 은 인터넷 (175) 에 접속하고 인터넷 (175) 을 통해 서로 통신할 수도 있고 및/또는 IoT 디바이스 그룹들 (160A 및 160B) 간의 통신을 용이하게 하기 위해 서로 직접 통신할 수도 있다. 더욱이, 비록 도 1e 는 IoT 슈퍼에이전트들 (140A 및 140B) 을 통해 서로 통신하는 2 개의 IoT 디바이스 그룹들 (160A 및 160B) 을 예시하지만, 통상의 기술자는 임의의 수의 IoT 디바이스 그룹들이 IoT 슈퍼에이전트들을 사용하여 서로 적절히 통신할 수도 있다는 것을 이해할 것이다.

[0049] 도 1a 내지 도 1e 에 각각 도시된 예시적인 무선 통신 시스템들 (100A-100E) 에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 는 다양한 IoT 디바이스들 (110-120) 및/또는 수동적 IoT 디바이스들 (105) 을 하나 이상의 소형 및 관련 IoT 디바이스 그룹들 (160) 로 편성하여 IoT 디바이스 그룹들 (160) 내의 및/또는 사이에서 자원들 (180) 을 공유하는 것을 가능하게 할 수도 있다 (예를 들어, IoT 디바이스 그룹들 (169) 에서 IoT 디바이스들 (110-120) 및/또는 수동적 IoT 디바이스들 (105) 사이에서 공유될 수도 있는 다양한 자원들 (180) 과 연관된 사용을 제어할 수도 있다). 예를 들어, 하나의 실시형태에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 는, 무선 통신 시스템들 (100A-100E) 에서의 각각의 IoT 디바이스 (110-120) 및/또는 수동적 IoT 디바이스 (105) 를 디바이스 특정 전역 고유 식별자 (예컨대, D_GUID) 및 그룹 특정 전역 고유 식별자 (예컨대, G_GUID) 로 표현할 수 있고, 무선 통신 시스템들 (100A-100E) 에서 공유된 각각의 자원 (180) 을 자원 특정 전역 고유 식별자 (예컨대, R_GUID) 로 더 표현할 수 있는 분산 네트워크 서비스 (예컨대, 클라우드 서비스) 를 제공할 수도 있다. 따라서, D_GUID들, G_GUID들, 및 R_GUID들은 특정 IoT 디바이스 그룹 (160) 내에서 및/또는 여러 상이한 IoT 디바이스 그룹들 (160) 간에 자원들 (180) 의 공유를 제어 또는 아니면 통합조정하는데 사용될 수도 있다.

[0050] 예를 들어, 도 1a 내지 도 1e 에서 도시된 예시적인 무선 통신 시스템들 (100A-100E) 에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에는 다양한 IoT 디바이스들 (110-120) 및/또는 수동적 IoT 디바이스들 (105) 을 나타내는 하나 이상의 D_GUID들이 준비될 수도 있다. 덧붙여, 새로운 디바이스가 IoT 네트워크에 접속한 후에 파워 업 됨에 또는 그렇지 않으면 IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에게 등록됨에 응답하여, 새로운 디바이스가 도달되는 것을 허용하기 위해 새로운 D_GUID가 새로운 디바이스에 할당될 수도 있고 다양한 속성들 (예컨대, 설명, 로케이션, 유형 등) 이 새로운 디바이스에 할당된 D_GUID에 연관될 수도 있다. 하나의 실시형태에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에는 IoT 네트워크 내의 공유된 자원들 (180) 에 대응하고 디바이스들이 동작하거나 또는 그렇지 않으면 상호작용하기 위해 필요로 할 수도 있는 R_GUID들이 추가로 준비될 수도 있다. 예를 들어, 자원들 (180) 은 로케이션, 가정 (household), 또는 자원들 (180) 에 연관된 다른 적합한 속성들에 따라 콘텍스트 내에서 고유하게 식별될 수도 있는 물, 전기, 햇빛, 도로, 식품, 또는 임의의 다른 적합한 자원 (180) 을 일반적으로 포함할 수도 있다. 더욱이, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에는, 함께 작업하는 각각의 IoT 디바이스 그룹 (160) 을 나타내는 G_GUID들이 준비될 수도 있다 (예컨대, 가정에서, 잔디 스프링클러, 온수기, 냉장고, 욕조 등이 공유된 수자원들 (180) 상에서 모두가 동작할 수도 있다). G_GUID들은 IoT 디바이스 그룹 (160) (예컨대, 가정, 로케이션, 소유자 등) 및 그 속에서 공유되는 자원들 (180) 에 연관된 콘텍스트를 정의하는 다양한 속성들을 더 포함할 수도 있다. 하나의 실시형태에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에는, 다양한 IoT 디바이스들 (110-120) 및 수동적 IoT 디바이스들 (105) 이 할당되는 IoT 디바이스 그룹들 (160), 그 속에서 공유되는 자원들 (180), 및 자원들 (180) 에 대한 경합 액세스를 제어하는 임의의 선취 정책들 외에도, 다양한 IoT 디바이스들 (110-120) 및 수동적 IoT 디바이스들 (105) 간의 계층구조들, 랭킹들, 우선순위들, 또는 다른 관계들을 정의하는 다양한 정책들이 추가로 준비될 수도 있다.

[0051] 하나의 실시형태에서, 다양한 D_GUID들, G_GUID들, R_GUID들, 및 정책들을 갖는 적절히 준비된 IoT 서버 (170) 및/또는 감독자 디바이스 (130) 를 가짐에 응답하여, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 는 그 다음에 다양한 IoT 디바이스 그룹들 (160) 과 그에 의해 공유되는 다양한 자원들 (180) 을 발견할 수도 있다. 예를 들어, 하나의 실시형태에서, R_GUID에는 특정한 공유된 자원 (180) 에 대한 액세스를 요청하는 디바이스들에 대응하는 하나 이상의 D_GUID들이 정적으로 준비 또는 그렇지 않으면 연관될 수도 있다. 다른 예에서, 특정한 공유된 자원 (180) 에 액세스하기 원하는 디바이스가 그것에 연관된 로케이션, 설명, 또는 다른 적합한 속성들에 기초하여 IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에게 조회할 수도 있고 그 디바이스는 그 다음에 IoT 서버 (170) 및/또는 감독자 디바이스 (130) 가 그 디바이스에게 반환하는 리스트로부터 적절한 자원 (180) 을 선택할 수도 있다. 더 나아가, 하나의 실시형태에서, 하나 이상의 자원들 (180) 에는 IoT 디바이스들 (110-120) 이 자원들 (180) 을 동적으로 발견하기 위하여 판독할 수 있는 RFID, 바 코드, 또는 다른 적합한 데이터가 태깅될 수도 있다. 더욱이, 하나의 실시형태에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 는 적합한 사용자 인터페이스에 입력된 정보 또는 콘텍스트에 기초하여 IoT 디바이스 그룹들 (160) 을 발견하는 조회 메커니즘을 채용할 수도 있다 (예컨대, 2 개의 IoT 디바이스 그룹들 (160) 에 연관된 소유자들은 2 개의 IoT 디바이스 그룹들 (160) 간의 상호작용을 개시하기 위해 G_GUID들을 교환할 수도 있다). 다른 예에서, IoT 서버 (170) 및/또는 감독자 디바이스 (130) 에게 프로비저닝된 허가 (permissions), 규칙들, 또는 다른 정책들에 기초하여, 2 이상의 IoT 디바이스 그룹들 (160) 은, 그 2 이상의 IoT 디바이스 그룹들 (160) 이 각각의 IoT 디바이스 그룹 내에 공유된 자원들을 사용하는 것을 가능하게 하기 위해 영구적으로 또는 일시적으로 병합될 수 있다. 또한, 이하 추가로 자세히 설명되는 바와 같이, 트러스트 휴리스틱 모델은, 공유된 자원들 (180) 에 대한 액세스를 요청하는 IoT 디바이스들이 적절한 인증 크리덴셜들 (authentication credentials) 을 가지고, 동일한 공유된 자원 (180) 에 대한 경합하는 요청들을 해결하고, 또는 그 외에, 공유된 자원들 (180) 에 대한 액세스를 통제하는 것과 연관된 제어 부하를 감소시킬 수도 있는 방식으로 공유된 자원들 (180) 에 대한 액세스를 제어하는 것을 보장하기 위해 무선 통신 시스템들 (100A-100E) 에서 구현될 수도 있다.

[0052] 도 2a 는 본 개시물의 양태들에 따른 IoT 디바이스 (200A) 의 하이레벨 예를 도시한다. 외부 외관들 및/또는 내부 컴포넌트들이 IoT 디바이스들 간에 상당히 상이하지만, 대부분의 IoT 디바이스들은 어떤 종류의 사용자 인터페이스를 가질 것이며, 이런 사용자 인터페이스는 디스플레이와 사용자 입력을 위한 수단을 포함할 수도 있다. 사용자 인터페이스가 없는 IoT 디바이스들은 유선 또는 무선 네트워크, 이를테면 도 1a, 도 1b, 및 도 1d 에서의 에어 인터페이스 (108) 를 통해 원격으로 통신될 수 있다.

[0053] 도 2a 에 도시된 바와 같이, IoT 디바이스 (200A) 에 대한 일 구성예에서, IoT 디바이스 (200A) 의 외부 케이싱은 당해 분야에서 알려진 바와 같이, 다른 컴포넌트들도 있지만 무엇보다도, 디스플레이 (226), 전원 버튼 (222), 및 2 개의 제어 버튼들 (224A 및 224B) 로 구성될 수도 있다. 디스플레이 (226) 는 터치스크린 디스플레이일 수도 있으며, 이 경우 제어 버튼들 (224A 및 224B) 은 필요하지 않을 수도 있다. 비록 IoT 디바이스 (200A) 의 부분으로서 명시적으로 도시되진 않았지만, IoT 디바이스 (200A) 는 Wi-Fi 안테나들, 셀룰러 안테나들, 위성 포지션 시스템 (SPS) 안테나들 (예컨대, 위성 포지셔닝 시스템 (GPS) 안테나들) 등을 비제한적으로 포함하는, 하나 이상의 외부 안테나들 및/또는 외부 케이싱에 내장된 하나 이상의 통합형 안테나들을 포함할 수도 있다.

[0054] 비록 IoT 디바이스들, 이를테면 IoT 디바이스 (200A) 의 내부 컴포넌트들이 상이한 하드웨어 구성들로 실시될 수 있지만, 내부 하드웨어 컴포넌트들에 대한 기본 하이레벨 구성은 도 2a 에서 플랫폼 (202) 으로서 도시되어 있다. 플랫폼 (202) 은 네트워크 인터페이스 (예컨대, 도 1a, 도 1b, 및 도 1d 에서의 에어 인터페이스 (108)) 및/또는 유선 인터페이스를 통해 송신된 소프트웨어 애플리케이션들, 데이터 및/또는 커맨드들을 수신 및 실행할 수 있다. 플랫폼 (202) 은 국소적으로 저장된 애플리케이션들을 또한 독립적으로 실행할 수 있다. 플랫폼 (202) 은 하나 이상의 프로세서들 (208), 이를테면 프로세서 (208) 라고 일반적으로 지칭될 마이크로제어기, 마이크로프로세서, 주문형 집적회로, 디지털 신호 프로세서 (DSP), 프로그램가능 로직 회로, 또는 다른 데이터 프로세싱 디바이스에 동작적으로 커플링된 유선 및/또는 무선 통신을 위해 구성된 하나 이상의 트랜시버들 (206) (예컨대, Wi-Fi 트랜시버, 블루투스 트랜시버, 셀룰러 트랜시버, 위성 트랜시버, GPS 또는 SPS 수신기 등) 을 포함할 수 있다. 프로세서 (208) 는 IoT 디바이스의 메모리 (212) 내의 애플리케이션 프로그래밍 명령들을 실행할 수 있다. 메모리 (212) 는 판독 전용 메모리 (ROM) 또는 랜덤 액세스 메모리 (RAM), 전기적으로 소거가능 프로그래밍가능 ROM (EEPROM), 플래시 카드들, 또는 컴퓨터 플랫폼들에 공통인 임의의 메모리 중 하나 이상을 포함할 수 있다. 하나 이상의 입출력 (I/O) 인터페이스들 (214) 은 도시된 바와 같은 디스플레이 (226), 전원 버튼 (222), 제어 버튼들 (224A 및 224B) 과 같은 다양한 I/O 디바이스들과,

IoT 디바이스 (200A) 에 연관된 임의의 다른 디바이스들, 이를테면 센서들, 액추에이터들, 릴레이들, 밸브들, 스위치들 등과 프로세서 (208) 가 통신하고 그것들을 제어하는 것을 허용하도록 구성될 수 있다.

[0055] 따라서, 본 발명의 양태가 본원에서 설명된 기능들을 수행하는 능력을 포함하는 IoT 디바이스 (예컨대, IoT 디바이스 (200A)) 를 포함할 수 있다. 통상의 기술자에 의해 이해될 바와 같이, 다양한 로직 엘리먼트들은 개별 엘리먼트들, 프로세서 (예컨대, 프로세서 (208)) 상에서 실행되는 소프트웨어 모듈들 또는 본원에서 개시된 기능을 달성하는 소프트웨어 및 하드웨어의 임의의 조합으로 실시될 수 있다. 예를 들어, 트랜시버 (206), 프로세서 (208), 메모리 (212), I/O 인터페이스 (214) 는 본원에서 개시된 다양한 기능들을 로드, 저장 및 실행하는데 모두가 협업적으로 사용될 수 있고 그래서 이러한 기능들을 수행하는 로직은 다양한 엘리먼트들에 전체에 걸쳐 분산될 수도 있다. 대안으로, 그 기능은 하나의 개별 컴포넌트에 통합될 수 있다. 그러므로, 도 2a 의 IoT 디바이스 (200A) 의 특징부 (feature) 들은 단지 예시적인 것으로 간주되는 것이고 본 개시물은 도시된 특징부들 또는 배치구성으로 제한되지는 않는다.

[0056] 도 2b 는 본 개시물의 양태들에 따른 수동적 IoT 디바이스 (200B) 의 하이레벨 예를 도시한다. 대체로, 도 2b 에 도시된 수동적 IoT 디바이스 (200B) 는 위에서 더욱 상세히 설명되었던 도 2a 에 도시된 IoT 디바이스 (200A) 와는 동일한 및/또는 실질적으로 유사한 다양한 컴포넌트들을 포함할 수도 있다. 이처럼, 설명의 간결함 및 편의를 위해, 도 2b 에 도시된 수동적 IoT 디바이스 (200B) 에서의 특정한 컴포넌트들에 관련한 다양한 세부사항들은 동일한 또는 유사한 세부사항들이 도 2a 에 도시된 IoT 디바이스 (200A) 에 관련하여 위에서 이미 제공되었던 결과로 여기서는 생략될 수도 있다.

[0057] 도 2b 에 도시된 수동적 IoT 디바이스 (200B) 는 수동적 IoT 디바이스 (200B) 가 프로세서, 내부 메모리, 또는 특정한 다른 컴포넌트들을 갖지 않을 수도 있다는 점에서 도 2a 에 도시된 IoT 디바이스 (200A) 와는 일반적으로 상이할 수도 있다. 대신, 하나의 실시형태에서, 수동적 IoT 디바이스 (200B) 는 수동적 IoT 디바이스 (200B) 가 제어된 IoT 네트워크 내에서 관찰, 모니터링, 제어, 관리, 또는 그렇지 않으면 알려지는 것을 허용하는 I/O 인터페이스 (214) 또는 다른 적합한 메커니즘만을 포함할 수도 있다. 예를 들어, 하나의 실시형태에서, 수동적 IoT 디바이스 (200B) 에 연관된 I/O 인터페이스 (214) 는, 단거리 인터페이스를 통해 조회될 경우 수동적 IoT 디바이스 (200B) 에 연관된 식별자 및 속성들을 다른 디바이스 (예컨대, 수동적 IoT 디바이스 (200B) 에 연관된 속성들에 관련한 정보를 검출, 저장, 통신, 그 정보에 작용, 또는 그렇지 않으면 프로세싱할 수 있는 능동적 IoT 디바이스, 이를테면 IoT 디바이스 (200A)) 로 제공할 수 있는 바코드, 블루투스 인터페이스, 무선 주파수 (RF) 인터페이스, RFID 태그, IR 인터페이스, NFC 인터페이스, 또는 임의의 다른 적합한 I/O 인터페이스를 포함할 수도 있다.

[0058] 비록 전술한 바가 일부 형태의 RF, 바코드, 또는 다른 I/O 인터페이스 (214) 를 갖는 것으로서 수동적 IoT 디바이스 (200B) 를 설명하지만, 수동적 IoT 디바이스 (200B) 는 이러한 I/O 인터페이스 (214) 를 갖지 않는 디바이스 또는 다른 물리적 개체를 포함할 수도 있다. 예를 들어, 특정한 IoT 디바이스들은 수동적 IoT 디바이스 (200B) 를 식별하기 위해 수동적 IoT 디바이스 (200B) 에 연관된 형상들, 사이즈들, 컬러들, 및/또는 다른 관찰가능 특징들을 검출할 수 있는 적절한 스캐너 또는 판독기 메커니즘들을 가질 수도 있다. 이런 방식으로, 임의의 적합한 물리적 개체는 제어된 IoT 네트워크 내에서 자신의 아이덴티티 및 속성들을 통신할 수도 있고 관찰, 모니터링, 제어, 또는 그렇지 않으면 관리될 수도 있다.

[0059] 도 3 은 기능을 수행하도록 구성된 로직을 포함하는 통신 디바이스 (300) 를 도시한다. 통신 디바이스 (300) 는 IoT 디바이스들 (110-120), IoT 디바이스 (200A), 인터넷 (175) 에 커플링된 임의의 컴포넌트들 (예컨대, IoT 서버 (170)) 등을 비제한적으로 포함하는 위에서 언급된 통신 디바이스들 중 임의의 것에 해당할 수 있다. 따라서, 통신 디바이스 (300) 는 도 1a 내지 도 1e 의 무선 통신 시스템들 (100A-E) 을 통해 하나 이상의 다른 엔티티들과 통신하도록 (또는 통신을 용이하게 하도록) 구성되는 임의의 전자 디바이스에 해당할 수 있다.

[0060] 도 3 을 참조하면, 통신 디바이스 (300) 는 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 을 포함한다.

일 예에서, 통신 디바이스 (300) 가 무선 통신 디바이스 (예컨대, IoT 디바이스 (200A) 및/또는 수동적 IoT 디바이스 (200B)) 에 해당한다면, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 무선 트랜시버와 같은 무선 통신 인터페이스 (예컨대, 블루투스, Wi-Fi, Wi-Fi 다이렉트, LTE (Long-Term Evolution) 다이렉트 등) 및 연관된 하드웨어 (예컨대, RF 안테나, 모뎀, 변조기 및/또는 복조기 등) 를 포함할 수 있다. 다른 예에서, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 유선 통신 인터페이스 (예컨대, 직렬 접속, USB 또는 파이어와이어 (Firewire) 접속, 인터넷 (175) 이 액세스될 수 있는 이더넷 접속 등) 에 해당할 수 있다.

따라서, 통신 디바이스 (300) 가 어떤 유형의 네트워크 기반 서버 (예컨대, 애플리케이션 (170)) 에 해당한다면, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은, 일 예에서, 네트워크 기반 서버를 이더넷 프로토콜을 통해 다른 통신 엔티티들에 접속시키는 이더넷 카드에 해당할 수 있다. 추가의 예에서, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 통신 디바이스 (300) 가 자신의 로컬 환경을 모니터링할 수 있게 하는 감지 (sensory) 또는 측정 하드웨어 (예컨대, 가속도계, 온도 센서, 광 센서, 로컬 RF 신호들을 모니터링하기 위한 안테나 등) 를 포함할 수 있다. 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은, 실행되는 경우, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 의 연관된 하드웨어가 자신의 수신 및/또는 송신 기능(들)을 수행하는 것을 허용하는 소프트웨어를 또한 포함할 수 있다. 그러나, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 소프트웨어에 단독으로 대응하지 않고, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 자신의 기능을 달성하기 위해 하드웨어에 적어도 부분적으로 의존한다.

[0061] 도 3 을 참조하면, 통신 디바이스 (300) 는 정보를 프로세싱하도록 구성된 로직 (310) 을 더 포함한다. 일 예에서, 정보를 프로세싱하도록 구성된 로직 (310) 은 적어도 프로세서를 포함할 수 있다. 정보를 프로세싱하도록 구성된 로직 (310) 에 의해 수행될 수 있는 프로세싱 유형의 구현예들은, 결정들을 수행하는 것, 접속들을 확립하는 것, 상이한 정보 옵션들 간에 선택들을 하는 것, 데이터에 관련된 평가들을 수행하는 것, 측정 동작들을 수행하기 위해 통신 디바이스 (300) 에 커플링된 센서들과 상호작용하는 것, 하나의 포맷에서부터 다른 포맷으로 (예컨대, .wmv 내지 .avi 등과 같은 상이한 프로토콜들 간에) 정보를 변환하는 것 등을 비제한적으로 포함한다. 예를 들어, 정보를 프로세싱하도록 구성된 로직 (310) 에 포함된 프로세서는, 본원에서 설명된 기능들을 수행하도록 설계된 범용 프로세서, DSP, ASIC, 필드 프로그램가능 게이트 어레이 (FPGA) 또는 다른 프로그램가능 로직 디바이스, 개별 게이트 또는 트랜지스터 로직, 개별 하드웨어 컴포넌트들, 또는 그것들의 임의의 조합에 해당할 수 있다. 범용 프로세서가 마이크로프로세서일 수도 있지만, 대체예에서, 그 프로세서는 기존의 임의의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신 (state machine) 일 수도 있다. 프로세서가 컴퓨팅 디바이스들의 조합 (예컨대, DSP 및 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들의 조합, 또는 임의의 다른 이러한 구성) 으로 또한 구현될 수도 있다. 정보를 프로세싱하도록 구성된 로직 (310) 은, 실행되는 경우, 자신의 프로세싱 기능(들)을 정보를 프로세싱하도록 구성된 로직 (310) 의 연관된 하드웨어가 수행하는 것을 허용하는 소프트웨어를 또한 포함할 수 있다. 그러나, 정보를 프로세싱하도록 구성된 로직 (310) 은 소프트웨어에 단독으로 대응하지 않고, 정보를 프로세싱하도록 구성된 로직 (310) 은 자신의 기능을 달성하기 위해 하드웨어에 적어도 부분적으로 의존한다.

[0062] 도 3 을 참조하면, 통신 디바이스 (300) 는 정보를 저장하도록 구성된 로직 (315) 을 더 포함한다. 일 예에서, 정보를 저장하도록 구성된 로직 (315) 은 적어도 비일시적 메모리 및 연관된 하드웨어 (예컨대, 메모리 제어기 등) 를 포함할 수 있다. 예를 들어, 정보를 저장하도록 구성된 로직 (315) 에 포함된 비일시적 메모리는 RAM, 플래시 메모리, ROM, 소거가능 프로그램가능 ROM (EPROM), EEPROM, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 당해 분야에서 알려진 임의의 다른 형태의 저장 매체에 해당할 수 있다. 정보를 저장하도록 구성된 로직 (315) 은, 실행되는 경우, 자신의 저장 기능(들)을 정보를 저장하도록 구성된 로직 (315) 의 연관된 하드웨어가 수행하는 것을 허용하는 소프트웨어를 또한 포함할 수 있다. 그러나, 정보를 저장하도록 구성된 로직 (315) 은 소프트웨어에 단독으로 대응하지 않고, 정보를 저장하도록 구성된 로직 (315) 은 자신의 기능을 달성하기 위해 하드웨어에 적어도 부분적으로 의존한다.

[0063] 도 3 을 참조하면, 통신 디바이스 (300) 는 정보를 제시하도록 구성된 로직 (320) 을 옵션으로 더 포함한다. 일 예에서, 정보를 제시하도록 구성된 로직 (320) 은 적어도 출력 디바이스 및 연관된 하드웨어를 포함할 수 있다. 예를 들어, 출력 디바이스는, 비디오 출력 디바이스 (예컨대, 디스플레이 스크린, USB, HDMI 등과 같이 비디오 정보를 전달할 수 있는 포트), 오디오 출력 디바이스 (예컨대, 스피커들, 마이크로폰 잭, USB, HDMI 등과 같이 오디오 정보를 전달할 수 있는 포트), 진동 디바이스 및/또는 정보가 통신 디바이스 (300) 의 사용자 또는 오퍼레이터에 의해 실제로 출력될 수 있거나 또는 출력을 위해 포맷팅될 수 있게 하는 임의의 다른 디바이스를 포함할 수 있다. 예를 들어, 통신 디바이스 (300) 가 도 2a 에 도시된 바와 같은 IoT 디바이스 (200A) 및/또는 도 2b 에 도시된 바와 같은 수동적 IoT 디바이스 (200B) 에 해당한다면, 정보를 제시하도록 구성된 로직 (320) 은 디스플레이 (226) 를 포함할 수 있다. 추가의 예에서, 정보를 제시하도록 구성된 로직 (320) 은 로컬 사용자를 갖지 않는 특정한 통신 디바이스들, 이를테면 네트워크 통신 디바이스들 (예컨대, 네트워크 스위치들 또는 라우터들, 원격 서버들 등) 에 대해 생략될 수 있다. 정보를 제시하도록 구성된 로직 (320) 은, 실행되는 경우, 자신의 제시 기능(들)을 정보를 제시하도록 구성된 로직 (320) 의 연관된 하드웨어가 수행하는 것을 허용하는 소프트웨어를 또한 포함할 수 있다. 그러나, 정보를 제시하도록 구성된 로직 (320) 은 소프트웨어에 단독으로 대응하지 않고, 정보를 제시하도록 구성된 로직 (320) 은 자신의 기능을 달성하기 위해

하드웨어에 적어도 부분적으로 의존한다.

[0064] 도 3 을 참조하면, 통신 디바이스 (300) 는 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 을 옵션으로 더 포함한다. 일 예에서, 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은 적어도 사용자 입력 디바이스 및 연관된 하드웨어를 포함할 수 있다. 예를 들어, 사용자 입력 디바이스는 버튼들, 터치스크린 디스플레이, 키보드, 카메라, 오디오 입력 디바이스 (예컨대, 마이크로폰 또는 마이크로폰 잭 등과 같이 오디오 정보를 전달할 수 있는 포트), 및/또는 정보가 통신 디바이스 (300) 의 사용자 또는 오퍼레이터로부터 수신될 수 있게 하는 임의의 다른 디바이스를 포함할 수 있다. 예를 들어, 통신 디바이스 (300) 가 도 2a 에 도시된 바와 같은 IoT 디바이스 (200A) 및/또는 도 2b 에 도시된 바와 같은 수동적 IoT 디바이스 (200B) 에 해당한다면, 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은 버튼들 (222, 224A, 및 224B), (터치스크린이면) 디스플레이 (226) 등을 포함할 수 있다. 추가의 예에서, 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은 로컬 사용자를 갖지 않는 특정한 통신 디바이스들, 이를테면 네트워크 통신 디바이스들 (예컨대, 네트워크 스위치들 또는 라우터들, 원격 서버들 등) 에 대해 생략될 수 있다. 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은, 실행되는 경우, 자신의 입력 수신 기능(들)을 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 의 연관된 하드웨어가 수행하는 것을 허용하는 소프트웨어를 또한 포함할 수 있다. 그러나, 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은 소프트웨어에 단독으로 대응하지 않고, 로컬 사용자 입력을 수신하도록 구성된 로직 (325) 은 자신의 기능을 달성하기 위해 하드웨어에 적어도 부분적으로 의존한다.

[0065] 도 3 을 참조하면, 305 내지 325의 구성된 로직들은 도 3 에서 별개의 또는 전혀 다른 블록들로서 도시되어 있지만, 개별 구성된 로직이 자신의 기능을 수행하게 하는 하드웨어 및/또는 소프트웨어는 부분적으로 중복될 수 있다는 것이 이해될 것이다. 예를 들어, 305 내지 325의 구성된 로직들의 기능을 용이하게 하는데 사용되는 임의의 소프트웨어가 정보를 저장하도록 구성된 로직 (315) 에 연관된 비일시적 메모리에 저장될 수 있어서, 305 내지 325의 구성된 로직들 각각은 그 기능 (즉, 이 경우, 소프트웨어 실행) 을 정보를 저장하도록 구성된 로직 (315) 에 의해 저장된 소프트웨어의 동작에 적어도 부분적으로 기초하여 수행한다. 비슷하게, 구성된 로직들 중 하나에 직접적으로 연관되는 하드웨어는 다른 구성된 로직들에 의해 가끔 차용되거나 또는 사용될 수 있다. 예를 들어, 정보를 프로세싱하도록 구성된 로직 (310) 의 프로세서는 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 에 의해 송신되기 전에 데이터를 적절한 포맷으로 포맷팅할 수 있어서, 정보를 수신 및/또는 송신하도록 구성된 로직 (305) 은 정보를 프로세싱하도록 구성된 로직 (310) 에 연관된 하드웨어 (즉, 프로세서) 의 동작에 적어도 부분적으로 기초하여 자신의 기능 (즉, 이 경우, 데이터의 송신) 을 수행한다.

[0066] 일반적으로, 명시적으로 달리 언급되지 않는 한, 본 개시물 전체에 걸쳐 사용된 바와 같은 "하도록 구성된 로직"이란 어구는 하드웨어로 적어도 부분적으로 구현되는 일 양태를 언급하도록 의도되고, 하드웨어와는 독립적인 소프트웨어 전용 구현예들에 매핑하도록 의도되진 않는다. 또한, 다양한 블록들에서의 구성된 로직 또는 "하도록 구성된 로직"은 특정 로직 게이트들 또는 엘리먼트들로 제한되지 않고, 본원에서 설명된 기능을 (하드웨어 또는 하드웨어 및 소프트웨어의 조합 중 어느 하나를 통해) 수행하는 능력을 일반적으로 지칭한다는 것이 이해될 것이다. 따라서, 다양한 블록들에서 도시된 바와 같은 구성된 로직들 또는 "하도록 구성된 로직"은 단어 "로직"을 공유함에도 불구하고 로직 게이트들 또는 로직 엘리먼트들로서 반드시 구현되지는 않는다. 다양한 블록들에서의 로직 간의 다른 상호작용들 또는 협력은 아래에서 더 상세히 설명되는 양태들의 관점에서 통상의 기술자에게 명확할 것이다.

[0067] 다양한 실시형태들은 다양한 상업적으로 입수가능한 서버 디바이스들 중 임의의 것, 이를테면 도 4 에 도시된 서버 (400) 상에 구현될 수도 있다. 일 예에서, 서버 (400) 는 위에서 설명된 IoT 서버 (170) 의 하나의 구성예에 해당할 수도 있다. 도 4 에서, 서버 (400) 는 휘발성 메모리 (402) 와 대용량 비휘발성 메모리, 이를테면 디스크 드라이브 (403) 에 커플링된 프로세서 (401) 를 구비한다. 서버 (400) 는 프로세서 (401) 에 커플링된 플로피 디스크 드라이브, 콤팩트 디스크 (CD) 또는 DVD 디스크 드라이브 (406) 를 또한 구비할 수도 있다. 서버 (400) 는 다른 브로드캐스트 시스템 컴퓨터들 및 서버들에 커플링된 로컬 영역 네트워크와 같은 네트워크 (407) 와의 데이터 접속들을 확립하기 위해 프로세서 (401) 에 또는 인터넷에 커플링된 네트워크 액세스 포트들 (404) 을 또한 구비할 수도 있다. 도 3 의 맥락에서, 도 4 의 서버 (400) 가 통신 디바이스 (300) 의 하나의 구현예를 예시함으로써, 정보를 송신 및/또는 수신하도록 구성된 로직 (305) 은 네트워크 (407) 와 통신하기 위해 서버 (400) 에 의해 사용되는 네트워크 액세스 포인트들 (404) 에 해당하며, 정보를 프로세싱하도록 구성된 로직 (310) 은 프로세서 (401) 에 해당하고, 정보를 저장하는 로직 구성 (315) 은 휘발성 메모리 (402), 디스크 드라이브 (403) 및/또는 디스크 드라이브 (406) 의 임의의 조합에 해당한다는 것이 이해될 것이다. 정보를 제시하도록 구성된 옵션적 로직 (320) 과 로컬 사용자 입력을 수신하도록 구성된 옵션적

로직 (325) 은 도 4 에서 명시적으로 도시되지 않고 그것에 포함되거나 또는 포함되지 않을 수도 있다. 따라서, 도 4 는 통신 디바이스 (300) 가, 도 2a 에서와 같은 IoT 디바이스 구현예 외에도, 서버로서 구현될 수도 있다는 것을 입증하는 것을 돕는다.

[0068] 일반적으로, 상기 언급된 바와 같이, IoT 기술들에서의 증가하는 발전은 가정에서, 운송수단들에서, 직장에서, 그리고 많은 다른 장소들에서 사용자를 둘러싸는 수많은 IoT 디바이스들을 초래할 것이고, 이에 의해, 많은 IoT 네트워크들은 상이한 IoT 디바이스들이 액세스하기를 원할 수도 있는 제어된 자원들에 대한 액세스를 인증 또는 그 외에 통제하기 위한 제어 메커니즘들을 구현할 수도 있다. 보다 상세하게는, 제어 메커니즘들은, 제어된 자원들에 대한 액세스를 요청하는 IoT 디바이스들이 적절한 인증 크리덴셜들을 가지고, 동일한 제어된 자원에 대한 경합하는 요청들을 해결하고, 또는 그 외에, 자원 액세스를 제어하는 것을 보장하기 위해 이용될 수도 있다. 예를 들어, IoT 개념을 이용하여 통제될 수 있는 예시적인 자원들은 네트어크 액세스, 전기, 가스, 스토리지, 경비, 천연 가스, 가솔린, 온수, 또는, IoT 디바이스들이 액세스할 필요가 있을 수도 있는 임의의 다른 적합한 계산적, 물리적, 또는 논리적 자원을 포함할 수도 있다. 따라서, (예컨대, 다양한 디바이스들이 제어된 자원들에 액세스하기 위해 제어 채널을 통해 통신하는 경우에) 제어된 자원들에 대한 액세스를 통제하기 위해 IoT 네트워크에서 사용되는 제어 채널 상의 과도한 트래픽은 잠재적으로 제어된 자원들과 연관된 사용을 방해할 수 있을 것이기 때문에, 본 명세서에서 더 상세하게 설명되는 양태들 및 실시형태들은 IoT 네트워크에서 제어된 자원에 대한 액세스를 통제하는 것과 연관된 제어 부하를 감소시키기 위해 트러스트 휴리스틱 모델을 이용할 수도 있다.

[0069] 보다 상세하게는, 본 개시물의 하나의 양태에 따르면, 도 5 는 IoT 자원 액세스 네트워크에서 제어 부하를 감소시키기 위해 이용될 수도 있는 예시적인 트러스트 휴리스틱 모델 (500) 을 나타낸다. 하나의 실시형태에서, 트러스트 휴리스틱 모델 (500) 은, 제어된 자원 (예컨대, 자원 A, 자원 B, 자원 Z 등) 을 액세스하기를 원하는 요청 노드와, 제어된 자원을 통제하거나, (예컨대, 요청 노드가 통제 노드와의 직접적인 접촉을 허용하는 통신 범위를 갖지 않는 경우에) 요청 노드와 제어된 자원을 통제하는 노드 사이에 액세스를 중계하기 위한 중재자로서 작용하는 인증 노드 사이에 사용되는 시험-및-대응 메커니즘에 기초할 수도 있다. 예를 들어, 요청 노드로부터 제어된 자원을 액세스하기 위한 요청을 수신하는 것에 응답하여, 인증 노드는 요청 노드에 시험을 전송하고, 그 시험에 대한 대응에 기초하여 (예컨대, 시험에 대한 정확한 대응은 요청 노드가 패스워드, 일반 인증 증서, 또는 다른 공유된 비밀에 기초하여 트러스트를 검증하기 위해 사용될 수 있는 하나 이상의 크리덴셜들을 갖는 것에 의존할 수도 있다) 제어된 자원에 대한 액세스를 요청 노드에게 허가할지 여부를 결정할 수도 있다.
이와 같이, 인증 노드는 일반적으로, 요청 노드가 시험에 대해 정확하게 대응하는 경우에 제어된 자원에 대한 액세스를 요청 노드에 대해 허가하고, 또는 대안적으로, 요청 노드가 시험에 대해 부정확한 대응을 제공하는 경우에 요청 노드가 제어된 자원에 대해 액세스하는 것을 거부할 수도 있다. 또한, 인증 노드는, 초기 시험에 대한 응답이 정확했는지 또는 부정확했는지 여부에 기초하여 요청 노드에 대해 적절한 트러스트 레벨을 할당할 수도 있고, 요청 노드에 할당된 트러스트 레벨은 연속적인 시험-및-대응 교환들 및/또는 IoT 네트워크에서의 다른 노드들과의 상호작용들에 기초하여 동적으로 업데이트될 수도 있다.

[0070] 특히, 종래의 시험-및-대응 메커니즘은 일반적으로, 시험에 대한 초기 정확한 대응 후에 시간 경과에 따라 아무것도 변화하지 않은 것을 보장하기 위해서 그리고 요청 노드를 주기적으로 재인증하기 위해서 규칙적인 간격들로 반복될 수도 있고, 이는 (예컨대, 무선 시스템에서) 불필요한 대역폭을 점유하고 제어 채널 상의 과도한 트래픽으로 인해 성능을 감소시킬 수도 있다. 반면, 도 5 에 도시된 트러스트 휴리스틱 모델 (500) 은 시험-및-대응 교환들 또는 그 외에 자원 액세스를 제어하기 위해 사용될 수도 있는 다른 트래픽과 연관된 제어 부하를 감소시키기 위해 사용될 수도 있다. 예를 들어, 하나의 실시형태에서, 인증 노드는, 요청 노드로부터 제어된 자원을 액세스하기 위한 요청을 수신하는 것에 응답하여 요청 노드에 초기 시험을 발행할 수도 있고, 요청 노드가 하나 이상의 연속적인 시험들에 대해 정확하게 대응하는 경우에 후속하는 시험들 사이의 간격들은 증가될 수도 있다. 또한, 인증 노드는, IoT 네트워크에서의 인증 노드 및/또는 다른 노드들이 이전의 상호작용들로부터 요청 노드를 신뢰하는 경우에 시험-및-대응 메커니즘을 채용함이 없이 제어된 자원에 대한 액세스를 요청 노드에 대해 허가할 수도 있고, 또는 대안적으로, 요청 노드가 하나 이상의 연속적인 시험들에 대해 부정확한 응답을 제공하는 경우에 요청 노드가 제어된 자원을 액세스하는 것을 차단하거나 IoT 네트워크로부터 완전히 요청 노드를 금지할 수도 있다.

[0071] 따라서, 트러스트 휴리스틱 모델 (500) 은 시간에 걸쳐 발생하는 연속적인 시험-및-응답 교환들에 기초하여 IoT 네트워크에서의 2 개 이상의 노드들 및/또는 다른 IoT 네트워크들에서의 2 개 이상의 노드들 사이에 트러스트를 모델링하기 위해 이용될 수도 있다. 또한, 트러스트는, 사람이 타인들과의 관계를 지인, 동료, 친구, 절친

한 친구 등으로 분류할 수도 있는 것과 유사한 방식으로 상이한 레벨들로 모델링될 수도 있고, 여기서, 제어된 자원들에 대한 액세스는 IoT 네트워크에서의 노드들 및/또는 다른 IoT 네트워크들에서의 노드들이 트러스트를 모델링하는 것을 허용하기 위해 유사한 경로들을 따라 정렬될 수 있다. 예를 들어, 도 5 를 참조하면, 트러스트 휴리스틱 모델 (500) 은, 요청 노드들이 IoT 네트워크 내로 허용되고/되거나 IoT 네트워크로 포워딩되거나 그 외에 IoT 네트워크 내에 중계되는 메시지들을 가지도록 허용될 수도 있는 알려지지 않은 트러스트 레벨 (Unknown Trust level) (510), 요청 노드들이 풍부한 또는 무제한의 자원들 (예컨대, 전기) 에 액세스하도록 허용될 수도 있는 예비적 트러스트 레벨 (Preliminary Trust level) (520), 요청 노드들이 제한된, 제약된, 또는 다른 한정된 자원들 (예컨대, Wi-Fi 대역폭) 에 대해 액세스하도록 허용될 수도 있는 신뢰된 레벨 (Trusted level) (530), 요청 노드들이 보호된 자원들 (예컨대, 데이터베이스 레코드들) 에 액세스하도록 허용될 수도 있는 확신 레벨 (Confidant level) (540), 및 다수의 연속적인 시험들에 대해 정확하게 대응하는 것에 실패한 요청 노드들이 IoT 네트워크로부터 금지당할 수도 있는 신뢰되지 않는 레벨 (Not Trusted level) (550) 을 포함할 수도 있다. 따라서, 트러스트 휴리스틱 모델 (500) 은 일반적으로 N 개 (예컨대, 도 5 에 도시된 예시적인 트러스트 휴리스틱 모델 (500) 에서 5 개) 의 트러스트 레벨들을 가질 수도 있고, 노드는 시간에 걸친 IoT 네트워크에서의 다른 노드들 및 자원들과의 상호작용들에 기초하여 특정 트러스트 레벨을 할당받을 수도 있다. 예를 들어, 하나의 실시형태에서, 트러스트 휴리스틱 모델 (500) 에서의 N 개의 트러스트 레벨들은 어떤 범위 (예컨대, -100 에서부터 +100 까지) 내에서 정의될 수도 있고, 특정 노드는 제로 (0) 트러스트 메트릭을 처음에 할당받을 수도 있고, 이는 그 후에 시험-및-대응 교환들, 다른 노드들 및 자원들과의 상호작용들, 또는 그 노드에 할당할 적절한 트러스트 레벨을 결정하기 위한 시간에 걸친 다른 적합한 기준들에 기초하여 후속하여 증가 또는 감소될 수도 있다.

[0072] 예를 들어, 도 5 를 참조하면, Node_new 는 IoT 네트워크에 새롭게 도입된 후에 알려지지 않은 트러스트 레벨 (510) 을 처음에 가질 수도 있는 한편, Node_abc 및 Node_def 는 인증 노드로부터의 초기 시험에 대해 정확하게 대응하는 것에 기초하여 예비적 트러스트 레벨 (520) 을 가지고 풍부한 자원 A 에 액세스하도록 허용될 수도 있다. 또한, Node_klm 및 Node_nop 는 연속적인 시험들에 대해 정확하게 대응한 후에 신뢰된 레벨 (530) 을 할당받고 풍부한 자원 A 에 추가하여 제한된 자원 B 에 액세스하도록 허용될 수도 있으며, Node_klm 및 Node_nop 가 연속적인 시험들에 대해 대응하도록 요구되기 전의 간격들이 증가될 수도 있다. 또한, Node_xyz 는 연속적인 시험들에 대해 추가로 정확한 대응들을 제공한 후에 확신 트러스트 레벨 (540) 을 할당받고 제한된 자원 B 및 풍부한 자원 A 에 추가하여 보호된 자원 Z 에 대해 액세스하도록 허용될 수도 있으며, Node_xyz 가 또 다른 시험에 대해 대응하도록 요구되기 전의 간격이 더 증가될 수도 있고, 또는, 또 다른 시험에 대해 대응하기 위한 요건이 완전히 제거될 수도 있다. 하지만, Node_bad 는 하나 이상의 시험들에 대해 정확하게 대응하는 것에 실패했을 수도 있고, 결과적으로 Node_bad 가 신뢰되지 않은 상태 (550) 를 갖게 될 수도 있으며, 이에 의해, Node_bad 는 소정의 기간 동안 IoT 네트워크를 통해 통신하는 것이 금지되거나 IoT 네트워크로부터 완전히 금지당할 수도 있어, 인가된 노드들이 Node_bad 로부터의 트래픽을 무시할 수 있고, 이에 의해 (예컨대, 스팸 (spam), 무차별 대입 공격 (brute force attacks), 서비스 거부 공격 (denial-of-service attacks) 등을 방지하기 위해) 잠재적으로 쓸모없는 데이터로 제어 채널을 넘치게 할 Node_bad 로 인한 IoT 네트워크에 대한 방해들을 회피할 수도 있다.

[0073] 또 다른 실시형태에서, 도 5 에 도시된 트러스트 휴리스틱 모델 (500) 은 다른 접속 메커니즘을 통한 접속들을 통제하기 위해 이용될 수 있다. 보다 구체적으로, 도 1d 와 관련하여 상기 설명된 바와 같이, IoT 서버 (170) 는 인터넷 (175) 을 이용한 또는 이용하지 않은 접속을 통제할 수도 있다. 이와 같이, 도 5 에서 지배된 기저 네트워크가 새로운 네트워크 액세스 계층으로 이전된 경우에, 이전의 경험에 기초하여 다른 노드들에 대해 다른 거동들 (behaviors) 이 존재할 수 있을 것이다. 예를 들어, 하나의 실시형태에서, 이전 (migration) 은 모든 노드들이 일부 셀룰러 인터페이스로부터 Wi-Fi 인터페이스로 변경하는 경우일 수 있을 것이다. 다른 예에서, 이전은 하나의 Wi-Fi 인터페이스로부터 다른 Wi-Fi 인터페이스로의 (예컨대, 802.11a 인터페이스로부터 802.11n 인터페이스로의) 변경일 수 있을 것이다. 어느 경우에도, 네트워크에서 일어나는 이전 또는 핸드오프 (handoff) 에 기초하여, 도 5 에 도시된 트러스트 휴리스틱 모델 (500) 은 상이한 트러스트 레벨들을 갖는 노드들에 대해 상이한 거동들을 제공할 수도 있다. 예를 들어, 예비적 트러스트 레벨 (520) 을 갖는 노드들 (예컨대, Node_abc 및 Node_def) 은 여전히 시험들이 발행될 수 있을 것이고, 신뢰된 상태 (530) 를 갖는 노드들 (예컨대, Node_klm 및 Node_nop) 은 단일 시험을 발행받을 수도 있으며, 확신 상태 (540) 를 갖는 노드들 (예컨대, Node_xyz) 은 어떤 시험들도 발행되지 않을 수도 있다. 이와 같이, 성공적인 시험-및-응답 교환 또는 다른 적합한 인증 절차를 주기적으로 완료하기 위한 요건은 IoT 네트워크가 새로운 네트워크 액세스 계층으로 이전하는 것에 응답하여 상이한 노드들에 할당되는 트러스트 휴리스틱 모델 (500) 에

서의 트러스트 레벨들에 따라 조정될 수도 있다.

[0074] 본 개시물의 하나의 양태에 따르면, 도 6 은 클라이언트 IoT 디바이스들이 IoT 네트워크에서 제어된 자원들에 대해 액세스를 요청할 수도 있는 소정의 예시적인 통신 시나리오들을 나타내는 한편, 도 7 은 IoT 네트워크에서의 제어 부하가 본 명세서에서 개시된 트러스트 휴리스틱 모델을 이용하여 감소될 수도 있는 소정의 예시적인 통신 시나리오들을 나타낸다. 도 6 및/또는 도 7 에서 도시되고 본 명세서에서 사용된 바와 같이, "노드 R" 이라는 용어는 IoT 네트워크에서의 제어된 자원을 일반적으로 지칭할 수도 있고, "노드 A" 라는 용어는 제어된 자원 노드 R 에 대해 액세스를 예약 (reserve) 하기를 원하는 클라이언트 IoT 디바이스를 일반적으로 지칭할 수도 있으며, "노드 B" 라는 용어는 제어된 자원 노드 R 에 대한 액세스를 통제하는 IoT 네트워크에서의 노드를 일반적으로 지칭할 수도 있고, "노드 C" 라는 용어는 제어된 자원 노드 R 에 대한 예약된 액세스를 갖는 중간 노드를 일반적으로 지칭할 수도 있으며, "노드 D" 라는 용어는 제어된 자원 노드 R 에 대한 예약된 자원을 갖지 않는 중간 노드를 일반적으로 지칭할 수도 있으며, "노드 T" 라은 용어는 노드 A 와 연관된 하나 이상의 트러스트 관련들을 모델링하기 위해 이용될 수도 있는 노드 A 와 이전의 상호작용들을 갖는 노드를 일반적으로 지칭할 수도 있다.

[0075] 하나의 실시형태에서, 본 명세서에서 추가로 자세히 설명되는 바와 같이, IoT 네트워크에서의 특정 노드 R 은 일반적으로 한정된 자원 또는 무제한의 자원으로 고려될 수도 있고, 여기서, 노드 R 에 대한 액세스를 통제하기 위해 이용되는 메커니즘들은 노드 R 이 한정된 또는 무제한의 자원에 대응하는지 여부에 의존하여 변화할 수도 있다. 보다 상세하게는, 무제한의 자원은 일반적으로, 소비율과 동일하거나 그것을 초과하는 생산율을 가질 수도 있고, 액세스 병목현상들을 가지지 않을 수도 있다 (예컨대, 데이터베이스에 대한 액세스는, 데이터베이스를 액세스하는 것은 거기에 저장된 정보를 고갈시키지 않기 때문에, 게다가, 그 외에 데이터베이스에 대한 액세스를 제한할 수도 있는 무선 대역폭은 데이터베이스에서의 병목현상으로서 고려되지 않을 수도 있기 때문에, 무제한의 것으로 고려될 수도 있을 것이다).

[0076] 반면, 한정된 자원은 일반적으로 생산율을 초과하는 소비율, 제약된 전달 메커니즘들, 또는 양자 모두를 가질 수도 있다. 예를 들어, 발전기가 생산하는 전력은, 발전기들이 통상적으로 전력을 고정된 비율로 생산하고 이에 의해 생산된 전력이 소비되는 비율은 실질적인 클라이언트들이 발전기에 액세스하는 기간 동안 생산율을 초과할 수도 있기 때문에, 한정된 자원으로 고려될 수도 있다. 다른 예에서, 한번에 오직 하나의 프로그램의 레코딩을 지원할 수 있는 접속을 갖는 디지털 비디오 레코더 (DVR) 는, 2 개의 동시적인 프로그램들이 거기에 기록될 수 없기 때문에, 제약된 전달 메커니즘을 갖는 한정된 자원으로 고려될 수도 있다. 또 다른 예에서, DVR 은, 사용자가 3 개의 DVR 들 상에 프로그램을 기록하기를 원하고 접속은 한 번에 2 개의 프로그램들을 기록하는 것만을 지원하며, DVR 들 상에서 이용가능한 저장 용량은 하나의 프로그램만을 수용할 수 있는 경우에, 제한된 양 및 제약된 전달 메커니즘을 갖는 한정된 자원으로 고려될 수도 있다. 통상의 기술자는 제어된 자원이 무제한의 또는 한정된 것으로 고려될 수도 있는지 여부에 관한 상기 개념들은 많은 다른 예들 및 사용 케이스들에 적용될 수 있음을 이해할 것이다.

[0077] 제어된 자원에 대한 액세스를 통제하기 위해 이용되는 전통적인 액세스 모드들에서, 특정 엔티티 (entity) (예컨대, 인증 서버) 는 제어된 자원에 대한 게이트키퍼일 수도 있고, 제어된 자원에 대해 클라이언트들이 거기에 액세스하기를 요청하는 것에 응답하여 클라이언트들을 인정할 지 여부를 결정할 수도 있다. 하지만, 피어-투-피어 (P2P) 액세스 모드들에서, (예컨대, 게이트키퍼 엔티티가 클라이언트와 연관된 통신 범위 내에 속하지 않기 때문에) 클라이언트는 게이트키퍼 엔티티와 통신할 수 없을 수도 있고, 이에 의해, 클라이언트는 중간 또는 에지 노드를 통해 제어된 자원을 액세스하기 위해 제어된 자원에 대한 액세스를 갖는 중간 또는 에지 노드와 대신 통신할 수도 있다. 따라서, 도 6 에 도시된 예시적인 통신 시나리오들은 IoT 네트워크에서 제어된 자원에 대한 액세스를 통제하기 위해 이용될 수도 있는 다양한 전통적인 액세스 모드들 및/또는 종래의 P2P 액세스 모드들을 일반적으로 나타낼 수도 있고, 도 7 에 관한 후속하는 설명은 본 명세서에서 설명된 트러스트 휴리스틱 모델이 어떻게 IoT 네트워크에서 제어 부하를 감소시키기 위해 전통적인 액세스 모드들 및/또는 종래의 P2P 액세스 모드들을을 증강시킬 수도 있는지를 보여줄 수도 있다.

[0078] 특히, 도 6 은, 클라이언트 노드 A 가 제어된 자원 노드 R 에 대한 액세스를 예약하기를 원하고, 노드 B 가 제어된 자원 노드 R 에 대한 액세스를 통제하는 하나의 예시적인 통신 시나리오 (610) 를 나타낸다. 또한, 각각의 점선들은 노드 A 및 노드 B 와 연관된 통신 범위들을 보여주고, 이는 서로 교차하며, 이에 의해, 노드 A 는 노드 B 와 직접 통신할 수 있고, 종래의 메커니즘들이 제어된 자원 노드 R 에 대한 액세스를 통제하기 위해 이용될 수도 있다. 하나의 실시형태에서, 시험-및-응답 메커니즘은 제어된 자원 노드 R 에 대한 액세스를 인증하거나 그 외에 제어하기 위해 노드 A 와 노드 B 사이에서 이용될 수도 있고, 여기서, 노드 B 는 노드 A 로

부터의 액세스 요청에 응답하여 노드 A 에 시험을 전송하고 그 시험에 대한 대응에 기초하여 제어된 자원 노드 R 에 대한 액세스를 노드 A 에게 허가할 지 여부를 결정할 수도 있다. 예를 들어, 시험-및-응답 메커니즘은 공유된 비밀 (예컨대, 패스워드, 일반적인 인증 메커니즘 등) 에 기초하여 트러스트를 검증하기 위해 이용될 수 있는 증서를 갖는 인증 노드 및 요청 노드에 의존할 수도 있다. 또한, 노드 B 는 (예컨대, 제어된 자원 노드 R 이 한정된 것인지 또는 무제한의 것인지 여부에 의존하여) 노드 A 에 대해 허가된 액세스를 제한할 수도 있고, 또는 대안적으로, 노드 A 에게 제어된 자원에 대한 제한되지 않은 액세스를 제공할 수도 있다. 예를 들어, 노드 A 는 DSL 모뎀을 나타낼 수도 있고, 노드 B 는 인터넷 서비스 프로바이더 (ISP) 를 나타낼 수도 있으며, 노드 R 은 ISP 가 DSL 모뎀에 할당하는 제한된 대역폭을 나타낼 수도 있다. 상대적인 예에서, 노드 A 는 무선 액세스 포인트 (WAP) 에 접속하는 무선 디바이스를 나타낼 수도 있고, 노드 B 는 WAP 를 나타낼 수도 있으며, 노드 R 은 WAP 가 노드 A 에게 허가하는 제한되지 않은 대역폭을 나타낼 수도 있다 (예컨대, 비록 ISP 로부터 WAP 에게 할당되는 대역폭이 제한될 수도 있지만, WAP 는 WAP 에 할당된 대역폭을 액세스하는 무선 디바이스에 대해 어떤 제한들도 부과하지 않을 수도 있다).

[0079] 여전히 도 6 을 참조하면, 노드 A 가 노드 B 로부터의 시험에 대해 성공적으로 대응하고 제어된 자원 노드 R 에 대해 요청된 액세스를 획득하는 것으로 귀결되는 통신 시나리오 (610) 에 응답하여, 통신 시나리오 (620) 는 노드 A 가 어떻게 제어된 자원 노드 R 에 대한 액세스를 예약한 중간 노드 C 가 될 수도 있는지를 보여준다. 통신 시나리오 (620) 에서, 노드 C 는 따라서, 노드 B 와의 직접적인 접촉을 허용하는 통신 범위를 가지지 않는 다른 노드 A 로부터 노드 B 에 대한 액세스 요청들을 중계할 수 있는 중간 노드일 수도 있다. 유사한 점에서, 통신 시나리오 (630) 는 제어된 자원 노드 R 애 대한 예약된 액세스를 갖지 않음에도 불구하고 노드 A 로부터 액세스 요청들을 수신하고 노드 B 에 그 액세스 요청들을 중계할 수 있는 중간 노드 D 를 포함한다. 예를 들어, 통신 시나리오들 (620 및 630) 에서, 노드 C 및 노드 D 는 노드 A 및 노드 B 로부터 수신된 액세스 요청들을 각각 중계할 수도 있고, 제어된 자원 노드 R 에 대한 액세스를 제어하기 위해 서로 직접 통신할 수 없는 노드 A 와 노드 B 사이에 시험-및-대응 메시지들을 후속하여 중계할 수도 있다. 하지만, 노드 A 와 노드 B 사이에 시험-및-대응 메시지들을 중계하는 중간 노드들 C 및 D 는, 노드들 C 및 D 가 중간 노드들을 통한 것을 제외하고는 서로 직접 통신할 수 없는 노드 A 와 노드 B 사이의 통신을 대신에 일반적으로 가능하게 한다는 점에서, 제어된 자원 노드 R 에 대해 액세스 허가되지 않을 수도 있다. 이와 같이, 통신 시나리오들 (620 및 630) 에서, 노드 C 및 노드 D 는 적어도 제어된 자원 노드 R 에 대한 액세스를 통제하는 노드 B 의 관점으로부터는 일반적으로 논리적으로 동등할 수도 있다.

[0080] 도 7 을 참조하면, 본 명세서에서 개시된 트러스트 휴리스틱 모델이 어떻게 IoT 네트워크에서 제어 부하를 감소시킬 수도 있는지를 보여주기 위한 소정의 통신 시나리오들이 예시된다. 예를 들어, 통신 시나리오 (710) 에서, 제어된 자원 노드 R 에 대한 액세스를 예약하기를 원하는 클라이언트 노드 A 는, 제어된 자원 노드 R 에 대한 예약된 액세스를 갖는 중간 노드 C 및 제어된 자원 노드 R 에 대한 예약된 액세스를 갖지 않는 중간 노드 D 를 접촉하도록 노드 A 에게 허용하는 통신 범위를 가질 수도 있다. 또한 중간 노드 C 및 중간 노드 D 는 제어된 자원 노드 R 에 대한 액세스를 통제하는 노드 B 와의 직접적인 접촉을 허용하는 각각의 통신 범위들을 가질 수도 있다. 따라서, 하나의 실시형태에서, 노드 A 는 일반적으로, 수직으로 및 수평으로 일반화될 수 있는 중간 노드 C 및 중간 노드 D 를 통해 제어된 자원 노드 R 을 액세스할 수도 있다. 보다 구체적으로, 노드 C 및 노드 D 는 많은 다른 노드들이 노드 A 및/또는 노드 B 에 관해 알 수도 있거나 노드 A 및/또는 노드 B 의 적합한 통신 범위 내에 있을 수도 있다는 점에서, 수직으로 일반화될 수 있다. 예를 들어, 통신 시나리오 (710) 에서 노드 C 및 노드 D 는 노드 A 와 연관된 통신 범위 및 노드 B 와 연관된 통신 범위 내에서 각각의 통신 범위들을 갖는다. 유사하게, 통신 시나리오 (720) 에서, 노드 C_1, 노드 C_2, 및 노드 T 는 노드 A_1 과 연관된 통신 범위 내에서 각각의 통신 범위들을 가지며, 더욱이, 노드 T 는 노드 A_1 과 연관된 트러스트를 모델링하기 위해 이용될 수 있는 이전의 상호작용들로부터 노드 A_1 에 관해 안다. 또한, 노드 C 및 노드 D 는, 노드 B 와 요청 클라이언트 사이에 하나 이상의 다중 중간 노드들이 존재할 수 있을 것이라는 점에서 수평으로 일반화될 수 있다. 예를 들어, 통신 시나리오 (710) 에서 나타난 바와 같이, 노드 A 는 하나의 중간 노드 (예컨대, 노드 C 또는 노드 D 중 어느 일방) 를 통해 노드 B 에 도달할 수 있다. 다른 예에서, 통신 시나리오 (720) 는 노드 A_1 과 노드 B 사이의 다중 중간 노드들을 보여주고, 여기서, 노드 A_1 은, 노드 A_1 과 노드 B 사이의 중간 노드에 추가하여, 노드 C_2 를 통해 노드 B 에 도달할 수 있고, 노드 A_1 은 노드 C_1 단독을 통해 노드 B 에 도달할 수 있다. 통상의 기술자는, 어떻게 요청 클라이언트 노드 A 가 수평으로 및/또는 수직으로 일반화될 수 있는 하나 이상의 중간 노드들을 통해 노드 B 를 접촉하는지에 관한 상기 개념들이 많은 다른

통신 시나리오들 및 사용 케이스들에 적용될 수 있음을 이해할 것이다.

[0081] 본 개시의 하나의 양태에 따르면, 트러스트 휴리스틱 모델을 이용하여 IoT 네트워크에서의 제어된 자원에 대한 액세스를 요청하는 것과 연관된 제어 부하를 감소시키기 위해 이용될 수도 있는 다양한 메커니즘들이 이하 설명될 것이다. 하나의 실시형태에서, 특히 통신 시나리오 (720) 를 참조하면, 제어된 자원 노드 R 은 제한된 또는 한정된 자원일 수도 있고, 제한된 자원에 대한 액세스를 예약하는 각 노드 C 는 노드 B 가 거기에 $R + e$ 를 할당할 것을 요청할 수도 있고, 여기서, R 은 노드 C 가 필요로 하는 제어된 자원 노드 R 의 양을 나타내는, 제로보다 크거나 같은 값을 가질 수도 있고, e 는 노드 C 가 예약한 제어된 자원 노드 R 의 일부 여분의 양 (예컨대, 노드 C 가 요청 노드 A 에 공급할 수 있는 과잉의 양) 을 나타내는, 제로보다 더 큰 값을 가질 수도 있다. 따라서, 클라이언트 노드 A_1 이 그 후에 노드 B 에 의해 통제되는 제어된 자원 노드 R 에 대한 액세스를 예약하기를 원할 때, 클라이언트 노드 A_1 은 처음에 그것과 연관된 통신 범위 내의 모든 노드 C 들을 접촉할 수도 있다. 예를 들어, 통신 시나리오 (720) 에서 나타낸 바와 같이, 클라이언트 노드 A_1 은 각 노드 C 가 스스로에 대해 예약한 여분의 용량 e 에 관해 문의하기 위해 노드 C_1 및 노드 C_2 를 초기에 접촉할 수도 있다. 따라서, 노드 A_1 이 필요로 하는 제어된 자원의 양 (R_a) 이 각 노드 C 가 스스로에 대해 예약한 여분의 용량 e 의 합 ($e_1 + e_2$) 을 초과하지 않는 경우에, 중간 노드 C_1 및 중간 노드 C_2 는 노드 A_1 에 대해 시험을 발행하고 노드 A_1 이 그 시험에 대해 성공적인 대응을 리턴하는 것에 응답하여 노드 A_1 에 요청된 자원 R_a 를 공급할 수도 있다.

[0082] 또한, 시험-및-대응 메커니즘은, 아무것도 변화하지 않은 것을 보장하기 위해서 그리고 노드 A_1 을 주기적으로 재인증하기 위해서 종래에는 규칙적인 간격들로 반복될 수도 있는 반면, 본 명세서에서 개시된 트러스트 휴리스틱 모델은 (예컨대, 무선 시스템에서 불필요한 대역폭을 점유하는 것을 회피하기 위해) 제어 부하를 감소시킬 수도 있다. 예를 들어, 노드 C_1 및 노드 C_2 는, 노드 A_1 이 노드 C_1 및 노드 C_2 로부터 자원을 요청할 때 노드 A_1 에 대해 초기 시험을 발행하고 하나 이상의 연속적인 대응들 후에 시험 간격을 감경할 수도 있다. 대안적으로, 노드 C_1 및/또는 노드 C_2 가 다른 상호작용들로부터 노드 A_1 을 아는 경우에는, 노드 C_1 및/또는 노드 C_2 는 시험-및-대응 메커니즘을 채용함이 없이 노드 A_1 에게 액세스를 허가할 수도 있다. 따라서, IoT 네트워크에서 상이한 노드들 사이에서 시간에 걸쳐 발생할 수도 있는 연속적인 시험-및-대응 교환들에 기초하여, IoT 네트워크에서의 2 개 이상의 노드들 사이의 신뢰 및/또는 불신은, (예컨대, 도 5 에서 도시된 바와 같이 그리고 상기 더 자세히 설명된 바와 같이) 사람이 타인들과의 관계를 지인, 동료, 친구, 절친한 친구 등으로 분류할 수도 있는 것과 유사한 방식으로 상이한 레벨들로 구축 또는 그 외에 모델링될 수도 있다.

[0083] 또한, IoT 네트워크는 일반적으로, 하나 이상의 유선 인터페이스들 및/또는 하나 이상의 에어 인터페이스들 (예컨대, Wi-Fi 에어 인터페이스, 셀룰러 에어 인터페이스 등) 을 포함할 수도 있는 여러 상이한 통신 인터페이스들 상에서 형성되거나 그 외에 그것들을 포함할 수도 있다. 따라서, 하나의 실시형태에서, 본 명세서에서 기술된 트러스트 휴리스틱 모델을 구현하는 IoT 네트워크는 상이한 유선 및/또는 에어 인터페이스들을 포함하고, 요청 노드들이 IoT 네트워크를 통해 통신하기 위해 이용하는 통신 인터페이스에 기초하여 특정 요청 노드들과 연관된 트러스트 레벨을 결정할 수도 있다. 예를 들어, 하나의 실시형태에서, 보안 Wi-Fi 접속들을 통해 통신하는 요청 노드들은 비보안 Wi-Fi 접속들을 통해 통신하는 노드들보다 더 높은 트러스트 레벨을 가질 수도 있고, 셀룰러 인터페이스들을 통해 통신하는 요청 노드들은 Wi-Fi 인터페이스들을 통해 통신하는 노드들보다 더 낮은 트러스트 레벨을 가질 수도 있으며, 유선 접속들을 통해 통신하는 요청 노드들은 에어 인터페이스들을 통해 통신하는 노드들보다 더 높은 트러스트 레벨을 가질 수도 있는 등이다. 하지만, 통상의 기술자는, IoT 네트워크와 통신하기 위해 이용되는 특정 인터페이스에 기초하여 요청 노드들에 할당될 수도 있는 특정 트러스트 레벨은 IoT 네트워크와 연관된 특정 상황에 따라 적합하게 변화될 수도 있음을 이해할 것이다.

[0084] 따라서, IoT 네트워크에서의 모든 노드들은 수개의 제어된 자원들을 통해 상호작용할 가능성이 높을 수도 있기 때문에, 트러스트 휴리스틱 모델은 제어된 자원들에 대한 액세스를 제어하기 위해 필요한 시험-및-응답 메시지들을 실질적으로 감소시키고 이에 의해 IoT 네트워크에서의 제어 부하를 실질적으로 감소시킬 수도 있다. 예를 들어, 하나의 예시적인 이용 경우에서, 노드 C_1 은 제어된 자원들 X, Y, 및 Z 에 대한 액세스를 가질 수도 있고, 노드 C_2 는 제어된 자원들 V, W, 및 X 에 대한 액세스를 가질 수도 있다. 새로운 클라이언트 노드 A_1 이 환경으로 도입되고 제어된 자원 Z 를 액세스하기 위해 노드 C_1 과 처음으로 상호작용하는 것에 응답하여, 노

드 A_1 과 노드 C_1 사이에 트러스트가 모델링될 수도 있다. 클라이언트 노드 A_1 이 그 후에 노드 A_1 과 어떤 이전의 상호작용들도 가지지 않은 노드 C_2 로부터 자원 W 를 요청하는 경우에, 노드 C_2 는 다른 디바이스들이 노드 A_1 과의 사이에 어떤 트러스트 관계를 가지고 있는지 여부를 결정하기 위해 (예컨대, 디바이스들의 "이웃(neighborhood)" 에서) 그것의 통신 범위 내의 다른 디바이스들에 대해 질의할 수도 있다. 예를 들어, 노드 C_2 가 노드 C_1 에 대해 질의하고 (예컨대, 제어된 자원 X 와 연관된 상호작용들에 기초하여) 노드 C_1 과 트러스트 관계를 가지는 경우에, 노드 C_2 는 성공적인 시험-및-대응을 요구함이 없이 자원 W 에 대한 액세스를 노드 A_1 에 대해 허가할 수도 있다. 이와 같이, 트러스트 휴리스틱 모델은 제어된 자원들에 대한 액세스를 통제하기 위해 사용되는 쿼리들 (queries) 및 제어 부하를 감소시킬 수도 있고, 여전히 모든 디바이스들이 제어된 자원들에 대한 액세스를 수신하는 것을 가능하게 할 수도 있다. 추가적으로, 자원 액세스를 제어하기 위해 실질적으로 더 적은 성공적인 시험-및-대응들이 필요할 수도 있기 때문에, 복잡한 시험-및-응답 메커니즘들을 개발하기 위한 프로세싱 부하는 실질적으로 감소될 수 있다. 또한, 트러스트 휴리스틱 모델은 추가된 보안 확장을 제공할 수도 있고, 여기서, 시험들에 대해 다수회 성공적으로 대응하는 것에 실패한 요청 노드 A 는 (예컨대, 스팸, 무차별 대입 공격, 서비스 거부 공격 등을 방지하기 위해) 소정 기간 동안 IoT 네트워크를 통해 통신하는 것이 차단되거나 IoT 네트워크로부터 완전히 금지될 수도 있다. 이와 같이, 트러스트 휴리스틱 모델은 인가된 노드들로 하여금 악성 범죄자들로부터의 트래픽을 무시하는 것을 허용하고 이에 의해 제어 채널 상에 넘쳐나는 쓸모없는 데이터로 인한 IoT 네트워크에 대한 방해들을 회피할 수도 있다.

[0085] 또한, 하나의 실시형태에서, 본 명세서에 개시된 트러스트 휴리스틱 모델은 신뢰된 노드들과 연관된 아이덴티티들에 기초하여 제어 부하를 실질적으로 감소시키는 것에 추가하여 IoT 네트워크에서 각각의 제어된 자원에 기초하여 트러스트를 모델링하기 위해 사용될 수도 있다. 예를 들어, 하나의 실시형태에서, 특정 제어된 자원들은 노드들이 그것에 대한 액세스를 얻기 위해 소정의 트러스트 레벨 (예컨대, 도 5 에서 도시된 예시적 트러스트 레벨 (520)) 과 상관시키는 제 1 클리어런스 레벨 (clearance level) 을 갖도록 요구할 수도 있다. 이와 같이, 특정 노드가, 제 1 클리어런스 레벨을 필요로 하는 제어된 자원에 액세스하기 위한 적절한 클리어런스를 제공하는 트러스트 레벨을 가지고, 그 노드가 그 제어된 자원을 액세스할 때 책임감을 보여주는 (예컨대, 할당된 몫을 초과하지 않는) 경우에, 그 노드는 그렇지 않으면 더 높은 클리어런스 레벨을 요구하는 제어된 자원들에 대해 액세스하기 위한 명목상의 트러스트를 얻을 수도 있다. 따라서, 하나의 실시형태에서, 트러스트 휴리스틱 모델은 자원 단위로 거기에 대한 트러스트를 구축하고 상이한 자원들 사이에 트러스트의 하위 부분을 전송하기 위해 사용될 수도 있어, 노드들이 액세스하도록 허용되는 자원들과 노드들이 어떻게 상호작용하는지에 기초하여 노드들에 할당되는 클리어런스 레벨은 명목적으로 증가되고/거나 후속하여 협정될 수도 있다.

[0086] 본 개시의 하나의 양태에 따르면, 도 8 은 IoT 네트워크에서의 클라이언트가 제어된 자원에 대한 액세스를 요청하고 트러스트 휴리스틱 모델에 기초하여 그것과 연관된 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법 (800) 을 나타낸다. 특히, 블록 805 에서 클라이언트는 그 클라이언트가 액세스를 예약하기를 원하는 필요한 자원을 처음에 식별하고, 후속하여 블록 810 에서 그 식별된 자원이 제한된 (즉, 한정된 또는 그 외에 제약된) 자원 또는 무제한의 (즉, 제한되지 않은 및 제약되지 않은) 자원인지 여부를 결정할 수도 있다. 식별된 자원이 제한된 것이라는 결정에 응답하여, 클라이언트는 그 다음, 블록 815 에서 클라이언트가 필요로 하는 제어된 자원의 양을 나타내는 양 R 을 결정할 수도 있다. 클라이언트는 그 다음, 식별된 자원에 대한 액세스를 예약한 그것과 연관된 통신 범위 내의 모든 이웃 노드들을 접촉할 수도 있다. 예를 들어, 상기 언급된 바와 같이, 제한된 자원에 대한 액세스를 예약하는 각각의 이웃 노드는 제어된 자원에 대한 액세스를 통제하는 노드로부터 $R + e$ 를 요청할 수도 있고, 여기서, R 은 노드가 필요로 하는 제어된 자원의 양을 나타내고, e 는 제어된 자원의 일부 여분의 양을 나타낸다. 따라서, 블록 825 에서, 클라이언트는 각각의 이웃 노드가 스스로에 대해 예약한 여분의 용량 e 에 관해 문의하기 위해 제어된 자원에 대한 액세스를 예약한 모든 이웃 노드들을 처음에 접촉하고, 클라이언트가 필요로 하는 제어된 자원의 양 (R_a) 이 각각의 이웃 노드가 스스로에 대해 예약한 여분의 용량 e 의 합 ($e_1 + e_2 + \ldots e_n$) 을 초과하지 않는지 여부를 결정할 수도 있다.

[0087] 하나의 실시형태에서, 클라이언트가, 각각의 이웃 노드가 스스로에 대해 예약한 여분의 용량 e 의 합이 블록 815 에서 결정된 자원 요건들을 충족시키기에 충분하다고 결정하는 경우에, 클라이언트는 그 후에, 블록 835 에서 이웃 노드들로부터 여분의 자원 용량에 대한 액세스를 요청할 수도 있다. 다르게는, 클라이언트가, 각각의 이웃 노드가 스스로에 대해 예약한 여분의 용량 e 의 합이 블록 815 에서 결정된 자원 요건들을 충족시키기에 충분하지 않다고 결정하거나 필요한 자원이 무제한의 것이라고 결정하는 경우에, 클라이언트는, 블록 835 에서 중간 노드로부터 자원에 대한 액세스를 요청하기 이전에, 블록 830 에서 자원 액세스를 요청하기 위한 적절

한 중간 노드를 식별할 수도 있다. 어느 경우에도, 클라이언트는 그 후에, 블록 840 에서 자원 액세스 요청에 응답하여 시험이 수신되었는지 여부를 결정할 수도 있다.

[0088] 예를 들어, 클라이언트가, 요청이 송신되었던 이웃 노드 및/또는 중간 노드와 어떤 이전 상호작용들을 가지지 않은 경우에, 블록 840 에서 수신 노드는 시험을 발행할 수도 있고, 블록 845 에서 클라이언트는 시험에 대한 대응을 후속하여 송신할 수도 있다. 이와 같이, 블록 845 에서 클라이언트가 시험에 대한 성공적인 대응을 송신하는 것에 응답하여 블록 850 에서 시험을 발행한 노드는 클라이언트에 요청된 자원을 공급하고/거나 제어된 자원에 대한 액세스를 통제하는 노드에 그 요청을 중계할 수도 있고, 이 경우에, 클라이언트는 그 다음, 블록 855 에서 자원을 액세스할 수도 있다. 하지만, 블록 845 에서 클라이언트가 시험에 대한 성공적인 대응을 송신하는 것에 실패한 경우에, 블록 850 에서 클라이언트는 자원에 대한 액세스가 거부될 수도 있고, 이 경우에, 클라이언트는 블록 835 로 되돌아가서 액세스를 요청하기를 다시 시도할 수도 있다. 다르게는, 블록 805 에서 자원에 대한 액세스가 허가되지 않았다고 결정하는 것에 응답하여, 클라이언트는 블록 830 (미도시)으로 돌아가서 (예컨대, 여분의 용량을 갖는 이웃 노드가 클라이언트에게 자원을 할당할 수 없었던 경우에) 다른 중간 노드를 통해 자원을 액세스하기를 시도하고/거나 상기 언급된 전통적인 액세스 모드들에 의존할 수도 있다 (예컨대, 중간 노드들을 통해 자원에 대한 액세스를 요청하기를 계속 시도하는 대신에 직접 게이트키퍼를 접촉하는 것을 시도).

[0089] 블록 840 으로 돌아가서, 클라이언트가, 요청이 송신되었던 이웃 노드 및/또는 중간 노드와 어떤 상호작용들을 가지거나 이웃 및/또는 중간 노드가 그 외에 클라이언트가 신뢰될 수 있다고 결정할 수 있었던 경우에, 클라이언트는 블록 840 에서 시험을 수신하지 않을 수도 있고, 대신에 성공적인 시험-및-응답을 필요로 함이 없이 블록 855 에서 자원에 대한 액세스가 허가될 수도 있다. 다르게는, 클라이언트가 시험들에 대해 성공적으로 대응하는 것을 다수회 실패했을 수도 있고 따라서 소정 기간 동안 IoT 네트워크를 통해 통신하는 것이 차단되거나 완전히 IoT 네트워크로부터 금지되었을 수도 있기 때문에, 블록 840 에서 클라이언트는 시험을 수신하지 않을 수도 있다. 이 경우에, 클라이언트는 유사하게 블록 835 로 돌아가서 클라이언트가 차단되었던 기간이 만료한 후에 액세스를 요청하는 것을 다시 시도하고/거나 블록 830 (미도시) 으로 돌아가서 클라이언트가 차단된 기간이 만료한 후에 다른 중간 노드를 통해 자원을 액세스하기를 시도할 수도 있다. 하지만, 통상의 기술자라면, 클라이언트가 IoT 네트워크로부터 완전히 금지되었거나 그 외에 시험에 대한 성공적인 대응을 송신하는 것에 실패한 경우에는 클라이언트가 사실 적절한 인증 크리덴셜들을 가지지 못하였기 때문에 클라이언트가 액세스를 요청하기를 다시 실시하는 임의의 시도들은 마찬가지로 실패할 수도 있음을 이해할 것이다.

[0090] 본 개시의 하나의 양태에 따르면, 도 9 는 IoT 네트워크에서 제어된 자원에 대한 액세스를 예약한 중간 노드가 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법 (900) 을 나타낸다. 특히, 블록 905 에서 중간 노드는 처음에 제어된 자원에 대한 액세스를 통제하는 노드와 통신하여 통제 노드가 중간 노드에게 $R + e$ 를 할당할 것을 요청할 수도 있고, 여기서, R 은 중간 노드가 필요로 하는 제어된 자원의 양을 나타내고, e 는 중간 노드가 예약한 제어된 자원의 일부 여분의 양 (예컨대, 중간 노드가 하나 이상의 요청 노드들에 공급할 수 있는 과잉 양) 을 나타낸다. 하나의 실시형태에서, 통제 노드는 중간 노드로부터의 요청을 인증하기 위해 시험-및-대응 메커니즘을 채용할 수도 있고, 여기서, 통제 노드는 중간 노드로부터의 요청에 응답하여 중간 노드에 시험을 전송하고 중간 노드가 그 시험에 대해 성공적으로 응답하는 경우에 그 요청을 허가할 수도 있다.

[0091] 하나의 실시형태에서, 중간 노드는 그 다음, 블록 910 에서 제어된 자원에 액세스하기를 원하는 클라이언트 노드로부터 초과 용량 쿼리를 수신할 수도 있다.예를 들어, 클라이언트 노드가 제어된 자원에 대한 액세스를 예약하기를 원할 때, 클라이언트 노드는 블록 905 에서 각각의 중간 노드가 스스로에 대해 예약한 여분의 용량 e 에 관해 문의하기 위해 클라이언트 노드와 연관된 통신 범위 내의 모든 중간 노드들을 접촉할 수도 있다. 이에 따라, 중간 노드는 그 후에 블록 915 에서, 블록 905 에서 중간 노드가 예약한 여분의 용량 e 를 나타내는 정보를 클라이언트 노드에 송신할 수도 있고, 여기서, 클라이언트 노드가 필요로 하는 제어된 자원의 양 (R_a) 이 각각의 중간 노드가 스스로에 대해 예약한 여분의 용량 e 의 합 ($e_1 + e_2 + \ldots e_n$) 을 초과하지 않는 경우에 클라이언트 노드는 중간 노드로부터 그 여분의 용량 e 를 일반적으로 요청할 수도 있다. 이와 같이, 블록 920 에서 중간 노드는 액세스 요청이 클라이언트 노드로부터 수신되었는지 여부를 결정할 수도 있고, 이는 R_a 가 각각의 중간 노드가 스스로에 대해 예약한 여분의 용량 e 의 합을 초과하는 경우에 발생하지 않을 수도 있고, 이 경우에 방법 (900) 은 그러면 종료될 수도 있다. 또한, 자원에 대한 액세스를 예약한 중간 노드들이 최대 용량에 있거나 그 외에 클라이언트 노드에 여분의 용량 e 을 공급할 수 없는 경우에, 클라이언트 노드는 아직

제어된 자원에 대한 액세스를 예약하지는 않았지만 제어된 자원에 대한 액세스를 통제하는 노드에 도달할 수 있는 통신 범위를 갖는 다른 중간 노드 (예컨대, 도 6 및 도 7 에서 도시된 바와 같은 노드 D) 로부터 제어된 자원에 대한 액세스를 요청할 수도 있고, 노드 D 는 그러면 자원에 대한 액세스를 예약할 수도 있고, 이에 의해, 클라이언트 노드로부터의 액세스 요청에 응답하여 노드 C 가 된다. 다르게는, 클라이언트 노드는 상기 언급된 전통적인 액세스 모드들에 의존하여, 예약된 액세스를 갖는 중간 노드들이 클라이언트 노드에게 R_a 를 공급할 수 없는 경우에 제어된 자원을 통제하는 노드 (예컨대, 도 6 및 도 7 에서 도시된 바와 같은 노드 B) 를 직접 접촉하기를 시도할 수도 있다.

[0092] 그렇지 않으면, R_a 가 각각의 중간 노드가 스스로에 대해 예약한 여분의 용량 e 의 합을 초과하지 않는 경우에, 블록 920 에서 중간 노드는 액세스 요청을 수신할 수도 있다. 다르게는, 비록 모든 여분의 용량 e 가 사용되었고 따라서 클라이언트 노드에게 R_a 를 공급하기 위해 사용될 수 없는 경우에도, 중간 노드는, 중간 노드가 최대 용량에 있지 않은 경우에 (미도시) 추가적인 여분의 용량 e 를 예약하기 위해 제어된 자원을 액세스하기를 시도할 수도 있고, 이 경우에, 중간 노드는, 클라이언트 노드에게 R_a 를 공급하기 위해 충분한 추가적인 여분의 용량 e 를 성공적으로 예약하는 것에 응답하여 블록 915 에서 클라이언트 노드에게 업데이트된 초과 자원 용량 표시자를 송신할 수도 있다. 이와 같이, R_a 가 중간 노드들을 통해 공급될 수 있는 것을 나타내는 블록 915 에서 송신된 초과 자원 용량 표시자 (또는 업데이트된 초과 자원 용량 표시자) 에 응답하여 클라이언트 노드는 그 후에 중간 노드에게 액세스 요청을 송신할 수도 있다. 어느 경우에도, 중간 노드가 R_a 를 공급할 충분한 여분의 용량을 갖는 것으로 인해 클라이언트 노드로부터 액세스 요청을 수신하는 경우에, 중간 노드는 그러면 블록 925 에서 클라이언트 노드가 알려진 트러스트 관계를 갖는지 여부를 결정할 수도 있다. 예를 들어, 새로운 클라이언트 노드가 환경에 도입되고 처음에 제어된 자원에 액세스하기 위해 중간 노드와 상호작용하는 것에 응답하여, 중간 노드가 클라이언트 노드에게 발행한 하나 이상의 시험들에 대해 클라이언트 노드가 성공적으로 대응하는 경우에 클라이언트 노드와 중간 노드 사이에 트러스트가 모델링될 수도 있고, 이 경우에, 블록 925 에서 중간 노드는 클라이언트 노드가 신뢰된 클라이언트라고 결정할 수도 있다. 다르게는, 중간 노드가 클라이언트 노드와 임의의 이전의 상호작용들을 갖지 않은 경우에, 중간 노드는 다른 디바이스들이 클라이언트 노드와 임의의 신뢰 관계를 가지는지 여부를 결정하기 위해 (예컨대, 디바이스들의 "이웃" 에서) 그것의 통신 범위 내의 다른 디바이스들에 대해 질의할 수도 있고, 이 경우에, 블록 925 에서 중간 노드는 클라이언트 노드가 신뢰된 클라이언트라고 유사하게 결정할 수도 있다. 이와 같이, 클라이언트 노드가 신뢰된 클라이언트라고 중간 노드가 결정하는 경우에, 블록 940 에서 중간 노드는 클라이언트 노드에게 여분의 용량 e 를 허가할 수도 있다. 그렇지 않으면, (예컨대, 중간 노드가 클라이언트 노드와 임의의 이전 상호작용들을 가지지 않았고 어떤 이웃 디바이스들도 클라이언트 노드와 이전의 상호작용들을 가지지 않았기 때문에) 클라이언트 노드가 신뢰된 클라이언트가 아니라고 중간 노드가 결정하는 경우에, 블록 930 에서 중간 노드는 클라이언트 노드에게 시험을 송신하고 블록 935 에서 클라이언트 노드가 그 시험에 대해 정확하게 대응하는지 여부를 결정할 수도 있다. 클라이언트 노드가 그 시험에 대해 정확하게 대응하는 경우에 블록 940 에서 중간 노드는 클라이언트 노드에게 여분의 용량 e 를 허가할 수도 있고, 또는 대안적으로, 클라이언트 노드가 그 시험에 대해 성공적으로 대응하는 것에 실패한 경우에 블록 945 에서 액세스 요청을 거부할 수도 있다.

[0093] 하나의 실시형태에서, 중간 노드는 그 다음, 블록 950 에서 클라이언트 노드와 연관된 트러스트 휴리스틱을 업데이트할 수도 있다. 예를 들어, 중간 노드는, 클라이언트 노드로부터의 시험에 대한 하나 이상의 연속적인 정확한 대응들 후에 시험 간격을 감경하거나, 클라이언트 노드가 시험에 대해 여러 번 성공적으로 대응한 후에 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정할 수도 있다. 따라서, IoT 네트워크에서의 2 개 이상의 노드들 사이의 트러스트는 시간에 걸친 성공적인 시험-및-대응 교환들에 응답하여 구축 또는 그 외에 모델링될 수 있다. 또한, 트러스트는, 사람이 타인들과의 관계를 지인, 동료, 친구, 절친한 친구 등으로 분류할 수도 있는 것과 유사한 방식으로 상이한 레벨들로 모델링될 수도 있다. 예를 들어, 도 5 에서 도시되고 이하 더 자세히 설명되는 바와 같이, 자원들은 노드들이 트러스트를 구축하도록 허용하는 것과 유사한 경로들을 따라서 정렬될 수 있고, 여기서, 클라이언트 노드로 하여금 IoT 네트워크 내로 허용하고, 포워딩되거나 중계된 메시지들을 가지고, 풍부한 또는 무제한의 자원들 (예컨대, 전기) 을 액세스하도록 허용되고, 제한된, 제약된, 또는 다른 한정된 자원들 (예컨대, Wi-Fi) 에 대한 액세스가 허용되고, 및/또는, 보호된 자원들 (예컨대, 데이터베이스 레코드들) 에 대한 액세스가 허용되도록, 블록 950 에서 트러스트 휴리스틱이 업데이트될 수도 있다. 다르게는, 클라이언트 노드가 시험에 대해 성공적으로 대응하지 못했고 따라서 블록 945 에서 중간 노드가 거부한 경우에, 클라이언트 노드와 연관된 트러스트 레벨을 감소시키고/거나 소정의 기간 동안 클라

이언트 노드가 IoT 네트워크를 통해 통신하는 것을 차단하거나 클라이언트 노드가 여러 번 시험들에 대해 성공적으로 대응하는 것에 실패한 경우에 IoT 네트워크로부터 완전히 클라이언트 노드를 금지하기 위해, 트러스트 휴리스틱은 블록 950 에서 업데이트될 수도 있다. 따라서, 트러스트 휴리스틱을 적합하게 업데이트하는 것에 응답하여, 중간 노드는 그 다음, (예컨대, 클라이언트 노드가 충분히 높은 트러스트 레벨 이외의 무언가를 가지는 경우에) 블록 955 에서 추가적인 시험-및-대응 교환들이 필요할 수도 있는지 여부를 결정할 수도 있고, 시험 간격이 만료된 후에 시험-및-대응 교환을 반복하기 위해 블록 930 으로 돌아갈 수도 있다. 그렇지 않으면, (클라이언트 노드가 충분히 높은 트러스트 레벨을 갖는 경우에) 블록 955 에서 중간 노드가 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정하는 경우에, 방법 (900) 은 클라이언트 노드가 어떤 추가적인 시험들에 대해 대응할 필요 없이 제어된 자원을 액세스하도록 허가되는 것으로 종료될 수도 있다.

[0094] 본 개시의 하나의 양태에 따르면, 도 10 은, IoT 네트워크에서 제어된 자원에 대한 예약된 액세스를 갖지 않는 중간 노드가 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법 (1000) 을 나타낸다. 특히, 제어된 자원에 대한 예약된 액세스를 갖는 특정 중간 노드들이, 클라이언트 노드가 필요로 하는 제어된 자원의 양을 공급하기에 충분한 초과 용량을 가지지 않는다고 클라이언트 노드가 결정하는 것에 응답하여, 블록 1005 에서 중간 노드는 클라이언트 노드로부터 중계 요청을 수신할 수도 있다. 예를 들어, 클라이언트 노드가 통제 노드를 직접 접촉하는 것을 허용하는 통신 범위를 클라이언트 노드가 갖지 않는 경우에, 클라이언트 노드는 제어된 자원에 대한 액세스를 통제하는 노드에 도달하기 위해 중계 요청을 일반적으로 송신할 수도 있고, 이에 의해, 중간 노드는 클라이언트 노드 대신에 하나 이상의 홉들 (hops) 을 통해 통제 노드와 통신할 수도 있다. 하나의 실시형태에서, 중계 요청을 수신하는 것에 응답하여, 중간 노드는 그 다음, 블록 1010 에서 클라이언트 노드가 알려진 트러스트 관계를 갖는지 여부를 결정할 수도 있다.

[0095] 예를 들어, 새로운 클라이언트 노드가 환경으로 도입되고, 처음에 제어된 자원에 액세스하기 위해 중간 노드와 상호작용하는 것에 응답하여, 중간 노드가 클라이언트 노드에게 발행한 하나 이상의 시험들에 대해 클라이언트 노드가 성공적으로 대응하는 경우에 클라이언트 노드와 중간 노드 사이에 트러스트가 모델링될 수도 있고, 이 경우에, 블록 1010 에서 중간 노드는 클라이언트 노드가 신뢰된 클라이언트라고 결정할 수도 있다. 다르게는, 중간 노드가 클라이언트 노드와 임의의 이전의 상호작용들을 갖지 않은 경우에, 중간 노드는 다른 디바이스들이 클라이언트 노드와 임의의 신뢰 관계를 가지는지 여부를 결정하기 위해 (예컨대, 디바이스들의 "이웃" 에서) 그것의 통신 범위 내의 다른 디바이스들에 대해 질의할 수도 있고, 이 경우에, 블록 1010 에서 중간 노드는 클라이언트 노드가 신뢰된 클라이언트라고 유사하게 결정할 수도 있다. 이와 같이, 클라이언트 노드가 신뢰된 클라이언트라고 중간 노드가 결정하는 경우에, 블록 1025 에서 중간 노드는 클라이언트 노드로부터의 액세스 요청을 중계할 수도 있다. 그렇지 않으면, (예컨대, 중간 노드가 클라이언트 노드와 임의의 이전 상호작용들을 가지지 않았고 어떤 이웃 디바이스들도 클라이언트 노드와 이전의 상호작용들을 가지지 않았기 때문에) 클라이언트 노드가 신뢰된 클라이언트가 아니라고 중간 노드가 결정하는 경우에, 블록 1015 에서 중간 노드는 클라이언트 노드에게 시험을 송신하고 블록 1020 에서 클라이언트 노드가 그 시험에 대해 정확하게 대응하는지 여부를 결정할 수도 있다. 중간 노드는 그 다음, 클라이언트 노드가 그 시험에 대해 정확하게 대응하는 경우에 블록 1025 에서 클라이언트 노드로부터의 액세스 요청을 통제 노드에 중계할 수도 있고, 또는, 클라이언트 노드가 그 시험에 대해 성공적으로 대응하는 것에 실패한 경우에 블록 1030 에서 액세스 요청을 거부할 수도 있다.

[0096] 하나의 실시형태에서, 중간 노드는 그 다음, 블록 1035 에서 클라이언트 노드와 연관된 트러스트 휴리스틱을 업데이트할 수도 있다. 예를 들어, 중간 노드는, 클라이언트 노드로부터의 시험에 대한 하나 이상의 연속적인 정확한 대응들 후에 시험 간격을 감경하거나, 클라이언트 노드가 시험에 대해 여러 번 성공적으로 대응한 후에 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정할 수도 있다. 따라서, IoT 네트워크에서의 2 개 이상의 노드들 사이의 트러스트는 시간에 걸친 성공적인 시험-및-대응 교환들에 응답하여 구축 또는 그 외에 모델링될 수 있다. 예를 들어, 도 5 에서 도시되고 이하 더 자세히 설명되는 바와 같이, 클라이언트 노드로 하여금 IoT 네트워크 내로 허용하고, 포워딩되거나 중계된 메시지들을 가지고, 풍부한 또는 무제한의 자원들 (예컨대, 전기) 을 액세스하도록 허용되고, 제한된, 제약된, 또는 다른 한정된 자원들 (예컨대, Wi-Fi) 에 대한 액세스가 허용되고, 및/또는, 보호된 자원들 (예컨대, 데이터베이스 레코드들) 에 대한 액세스가 허용되도록, 블록 1035 에서 트러스트 휴리스틱이 업데이트될 수도 있다. 다르게는, 클라이언트 노드가 시험에 대해 성공적으로 대응하지 못했고 따라서 블록 1030 에서 중간 노드가 중계 요청을 거부한 경우에, 클라이언트 노드와 연관된 트러스트 레벨을 감소시키고/거나 소정의 기간 동안 클라이언트 노드가 IoT 네트워크를 통해 통신하는 것을 차단하거나 클라이언트 노드가 여러 번 시험들에 대해 성공적으로 대응하는 것에 실패한 경우에 IoT 네

트워크로부터 완전히 클라이언트 노드를 금지하기 위해, 트러스트 휴리스틱은 블록 1035 에서 업데이트될 수도 있다. 따라서, 트러스트 휴리스틱을 적합하게 업데이트하는 것에 응답하여, 중간 노드는 그 다음, (예컨대, 클라이언트 노드가 충분히 높은 트러스트 레벨 이외의 무언가를 가지는 경우에) 블록 1040 에서 추가적인 시험-및-대응 교환들이 필요할 수도 있는지 여부를 결정할 수도 있고, 시험 간격이 만료된 후에 시험-및-대응 교환을 반복하기 위해 블록 1015 로 돌아갈 수도 있다. 그렇지 않으면, (예컨대, 클라이언트 노드가 충분히 높은 트러스트 레벨을 갖는 경우에) 블록 1040 에서 중간 노드가 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정하는 경우에, 방법 (1000) 은 클라이언트 노드가 어떤 추가적인 시험들에 대해 대응할 필요 없이 액세스 요청들을 자동적으로 중계되게 하도록 허가되는 것으로 종료될 수도 있다.

[0097] 본 개시의 하나의 양태에 따르면, 도 11 은 IoT 네트워크에서 제어된 자원에 대한 액세스를 통제하는 노드가 트러스트 휴리스틱 모델에 기초하여 IoT 네트워크에서 제어 부하를 감소시키기 위해 수행할 수도 있는 예시적인 방법 (1100) 을 나타낸다. 특히, 블록 1105 에서, 통제 노드는 블록 1105 에서 이에 의해 통제되는 제어된 자원에 대해 액세스하기 위한 하나 이상의 요청들을 처음에 수신할 수도 있다. 하나의 실시형태에서, 블록 1110 에서 통제 노드는 제어된 자원에 대해 액세스하기 위한 다수의 요청들이 존재하는지 여부를 결정할 수도 있고, 제어된 자원에 대해 액세스하기 위한 다수의 요청들이 수신되었다고 결정하는 것에 응답하여 블록 1115 에서 통제 노드는 제어된 자원에 액세스하기 위한 임의의 경합하는 요청들을 해결할 수도 있다. 예를 들어, 하나의 실시형태에서, 다양한 클라이언트 노드들 및/또는 중간 노드들은, 유사한 활동들을 수행하는 것, 특정 제어된 자원들에 대해 함께 작업하는 것, 또는 그 외에, 소정의 특성들을 갖는 것에 기초하여 하나 이상의 그룹들로 조직화될 수도 있고, 그 그룹들은 다양한 그룹들 및/또는 그룹들로 조직화된 다양한 그룹들 및/또는 다양한 클라이언트 노드들 중에서 순위를 정하거나 그 외에 상대적인 우선순위들을 정의하기 위해 계층적인 방식으로 조직화될 수도 있다.

[0098] 이에 따라, 하나의 실시형태에서, (예컨대, 하나 또는 N 개의 사용자들이 한번에 한정된 또는 그 외에 제한된 자원에 액세스하는 것을 제한하는 것, 최대 사용 지속기간, 소정의 위치 또는 시간 등을 포함하는) 다수의 요청들이 수신되었던 노드들과 연관된 상대적인 순위들 또는 우선순위들, 제어된 자원에 대한 액세스를 제어하는 특정 정책들, 상이한 노드들이 서로 상호작용하고 자원 액세스를 공유하는 것을 가능하게 하는 정책들, 제어된 자원이 어떻게 활용될 수도 있는지를 통제하는 정책들에 기초하여, 블록 1115 에서 통제 노드는 경합하는 요청들을 해결할 수도 있다. 예를 들어, 통제 노드는, 액세스 요청들을 송신한 노드들이 제어된 자원에 대한 액세스가 허가될 순서, 각 노드가 제어된 자원을 액세스할 수 있는 최대 지속기간, 각 액세스 요청이 적합하게 만족될 수 있는 것을 보장하기 위해 다양한 노드들에 할당할 제어된 자원의 양들을 결정하기 위해 경합하는 요청들을 해결할 수도 있고, 또는 그 외에, (특히 제어된 자원이 제한된 양, 제약된 전달 메커니즘, 또는 다른 한정된 특성들을 갖는 경우에) 제어된 자원에 대한 임의의 경합을 해결할 수도 있다. 다른 예에서, (예컨대, 제어된 자원이 점유되었거나, 선점될 수 없는 더 높은 우선순위의 노드가 제어된 자원에 대한 플로어 (floor) 를 현재 유지하고 있는 등의 이유 때문에) 제어된 자원이 이용가능하지 않다고 통제 노드가 결정하는 경우에, 통제 노드는 블록 1105 에서 수신되었던 액세스 요청 및/또는 블록 1115 에서 그와 경합하는 다른 액세스 요청들을, 자원이 충분히 이용가능하게 될 때까지, 큐잉할 수도 있고, 자원이 충분히 이용가능하게 될 때, 통제 노드는 수신된 액세스 요청을 인증하기 위한 절차를 개시하기 위해 블록 1120 으로 진행할 수도 있다.

[0099] 하나의 실시형태에서, 블록 1120 에서, 통제 노드는 그 다음, 블록 1115 에서 경합하는 액세스 요청들을 적합하게 해결하는 것 또는 대안적으로 블록 1110 에서 제어된 자원에 대해 액세스하기 위한 다수의 경합하는 요청들이 계류 중이지 않다고 결정하는 것에 응답하여, 블록 1105 에서 수신된 액세스 요청을 송신한 요청 노드가 알려진 신뢰 관계를 갖는지 여부를 결정할 수도 있다. 예를 들어, 새로운 노드가 환경으로 도입되고, 처음에 제어된 자원에 액세스하기 위해 통제 노드와 상호작용하는 것에 응답하여, 통제 노드가 요청 노드에게 발행한 하나 이상의 시험들에 대해 요청 노드가 성공적으로 대응하는 경우에 요청 노드와 통제 노드 사이에 트러스트가 모델링될 수도 있고, 이 경우에, 블록 1120 에서 통제 노드는 요청 노드가 신뢰된 클라이언트라고 결정할 수도 있다. 다르게는, 통제 노드가 요청 노드와 임의의 이전의 상호작용들을 갖지 않은 경우에, 통제 노드는 요청 노드와의 임의의 신뢰 관계가 모델링되었는지 여부를 결정하기 위해 다른 디바이스들에 대해 질의할 수도 있고, 이 경우에, 블록 1120 에서 통제 노드는 요청 노드가 신뢰된 클라이언트라고 유사하게 결정할 수도 있다.

이와 같이, 요청 노드가 신뢰된 클라이언트라고 통제 노드가 결정하는 경우에, (도 6 및 도 7 을 참조하여 상기 더 자세히 설명된 방식으로) 블록 1135 에서 통제 노드는 요청 노드로부터의 액세스 요청을 허가할 수도 있다. 그렇지 않으면, (예컨대, 통제 노드가 요청 노드와 임의의 이전 상호작용들을 가지지 않았고 어떤 이웃 디바이스들도 요청 노드와 이전의 상호작용들을 가지지 않았기 때문에) 요청 노드가 신뢰된 클라이언트가 아니라고 통제 노드가 결정하는 경우에, 블록 1125 에서 통제 노드는 요청 노드에게 시험을 송신하고 블록 1130

에서 요청 노드가 그 시험에 대해 정확하게 대응하는지 여부를 결정할 수도 있다. 통제 노드는 그 다음, 요청 노드가 그 시험에 대해 정확하게 대응하는 경우에 블록 1135 에서 액세스 요청을 허가할 수도 있고, 또는 다르게는, 요청 노드가 그 시험에 대해 성공적으로 대응하는 것에 실패한 경우에 블록 1140 에서 액세스 요청을 거부할 수도 있다.

[0100] 하나의 실시형태에서, 통제 노드는 그 다음, 블록 1145 에서 요청 노드와 연관된 트러스트 휴리스틱을 업데이트할 수도 있다. 예를 들어, 통제 노드는, 요청 노드로부터의 시험에 대한 하나 이상의 연속적인 정확한 대응들 후에 시험 간격을 감경하거나, 요청 노드가 시험에 대해 여러 번 성공적으로 대응한 후에 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정할 수도 있다. 따라서, IoT 네트워크에서의 2 개 이상의 노드들 사이의 트러스트는 시간에 걸친 성공적인 시험-및-대응 교환들에 응답하여 구축 또는 그 외에 모델링될 수 있다. 예를 들어, 도 5 에서 도시되고 이하 더 자세히 설명되는 바와 같이, 요청 노드로 하여금 IoT 네트워크 내로 허용하고, 포워딩되거나 중계된 메시지들을 가지고, 풍부한 또는 무제한의 자원들 (예컨대, 전기) 을 액세스하도록 허용되고, 제한된, 제약된, 또는 다른 한정된 자원들 (예컨대, Wi-Fi) 에 대한 액세스가 허용되고, 및/또는, 보호된 자원들 (예컨대, 데이터베이스 레코드들) 에 대한 액세스가 허용되도록, 블록 1145 에서 트러스트 휴리스틱이 업데이트될 수도 있다. 다르게는, 요청 노드가 시험에 대해 성공적으로 대응하지 못했고 따라서 블록 1140 에서 통제 노드가 중계 요청을 거부한 경우에, 요청 노드와 연관된 트러스트 레벨을 감소시키고/거나 소정의 기간 동안 요청 노드가 IoT 네트워크를 통해 통신하는 것을 차단하거나 요청 노드가 여러 번 시험들에 대해 성공적으로 대응하는 것에 실패한 경우에 IoT 네트워크로부터 완전히 요청 노드를 금지하기 위해, 트러스트 휴리스틱은 블록 1145 에서 업데이트될 수도 있다. 따라서, 트러스트 휴리스틱을 적합하게 업데이트하는 것에 응답하여, 통제 노드는 그 다음, (예컨대, 요청 노드가 충분히 높은 트러스트 레벨 이외의 무언가를 가지는 경우에) 블록 1150 에서 추가적인 시험-및-대응 교환들이 필요할 수도 있는지 여부를 결정할 수도 있고, 시험 간격이 만료된 후에 시험-및-대응 교환을 반복하기 위해 블록 1125 로 돌아갈 수도 있다.

그렇지 않으면, (예컨대, 요청 노드가 충분히 높은 트러스트 레벨을 갖는 경우에) 블록 1150 에서 중간 노드가 더 이상 추가적인 시험-및-대응 교환들이 필요하지 않다고 결정하는 경우에, 방법 (1100) 은 요청 노드가 어떤 추가적인 시험들에 대해 대응할 필요 없이 액세스 요청들을 자동적으로 중계되게 하도록 허가되는 것으로 종료될 수도 있다.

[0101] 정보 및 신호들이 다양한 상이한 기술들 및 기법들 중의 임의의 것을 사용하여 표현될 수도 있다는 것을 통상의 기술자는 이해할 것이다. 예를 들어, 위의 설명 전체에 걸쳐 언급될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩 (chip) 들은 전압들, 전류들, 전자기파들, 자기적 장들 또는 입자들, 광학적 장들 또는 입자들, 또는 그것들의 임의의 조합에 의해 표현될 수도 있다.

[0102] 게다가, 본원에 개시된 양태들에 관련하여 설명되는 다양한 예시적 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양쪽 모두의 조합들로 구현될 수도 있다는 것을 통상의 기술자는 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 교환가능성을 명백하게 예증하기 위하여, 다양한 예시적 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들이 일반적으로 그것들의 기능성의 관점에서 설명되어 있다. 이러한 기능성이 하드웨어 또는 소프트웨어 중 어느 것으로 구현되는지는 전체 시스템에 부과되는 특정 애플리케이션 및 설계 제약들에 달려있다. 통상의 기술자는 설명된 기능성을 각 특정 애플리케이션에 대하여 다양한 방식들로 구현할 수도 있지만, 이러한 구현 결정들은 본 개시물의 범위로부터의 일탈하는 것으로 해석되지 않아야 한다.

[0103] 본원에서 개시된 양태들에 관련하여 설명된 다양한 구체적 논리 블록들, 모듈들, 및 회로들은 본원에서 설명된 기능들을 수행하도록 설계된 범용 프로세서, 디지털 신호 프로세서 (DSP), 주문형 집적회로 (ASIC), 필드 프로그램가능 게이트 어레이 (FPGA) 또는 다른 프로그램가능 로직 디바이스, 개별 게이트 또는 트랜지스터 로직, 개별 하드웨어 컴포넌트들, 또는 그것들의 임의의 조합으로 구현되거나 실시될 수도 있다. 범용 프로세서가 마이크로프로세서일 수도 있지만, 대체예에서, 그 프로세서는 기존의 임의의 프로세서, 제어기, 마이크로제어기, 또는 상태 머신 (state machine) 일 수도 있다. 프로세서가 컴퓨팅 디바이스들의 조합 (예컨대, DSP 및 마이크로프로세서의 조합, 복수의 마이크로프로세서들의 조합, DSP 코어와 협력하는 하나 이상의 마이크로프로세서들의 조합, 또는 임의의 다른 이러한 구성) 으로 또한 구현될 수도 있다.

[0104] 본원에서 개시된 양태들에 관련하여 설명된 방법들, 시퀀스들 및/또는 알고리즘들은 직접적으로 하드웨어로 구현되거나, 프로세서에 의해 실행되는 소프트웨어 모듈로서 구현되거나, 이들 두 가지의 실시될 수도 있다. 소프트웨어 모듈이 RAM, 플래시 메모리, ROM, EPROM, EEPROM, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM 또는 당해 분야에서 알려진 임의의 다른 형태의 저장 매체 내에 존재할 수도 있다. 예시적인 저장 매체가

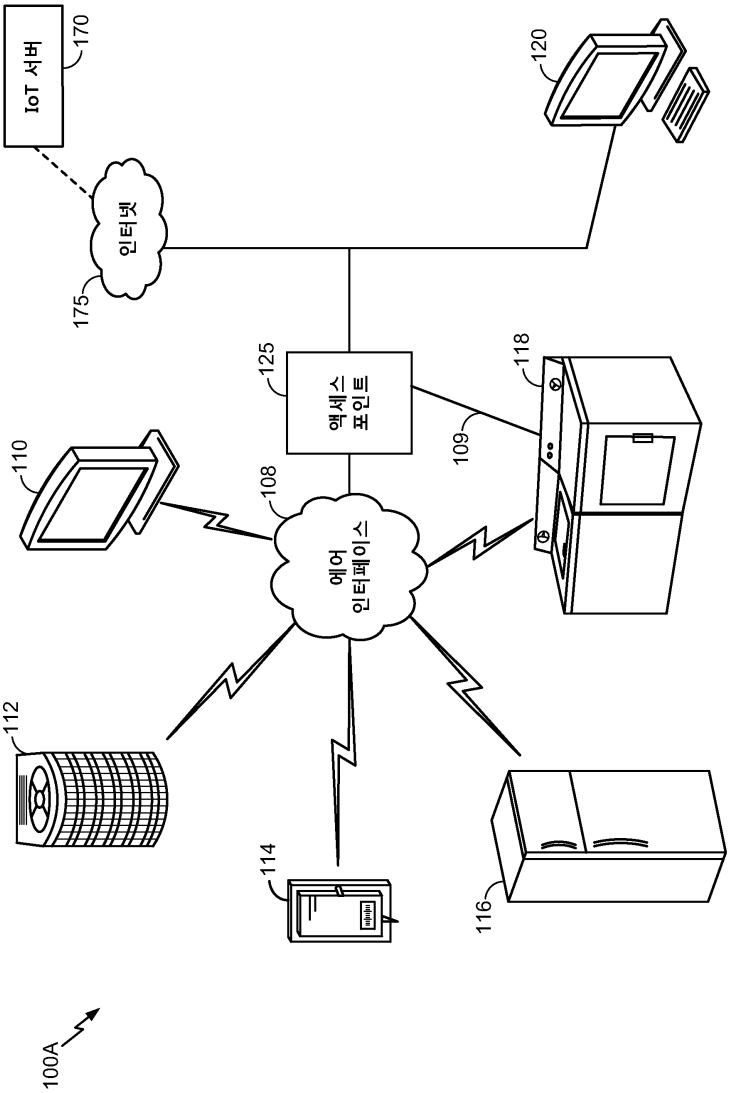
프로세서에 커플링되어서 그 프로세서는 저장 매체로부터 정보를 읽을 수 있고 그 저장 매체에 정보를 쓸 수 있다. 대체예에서, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서와 저장 매체는 ASIC 내에 존재할 수도 있다. ASIC은 IoT 디바이스 내에 존재할 수도 있다. 대체예에서, 프로세서와 저장 매체는 사용자 단말에 개별 컴포넌트들로서 존재할 수도 있다.

[0105] 하나 이상의 예시적인 양태들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어, 또는 그것들의 임의의 조합으로 구현될 수도 있다. 소프트웨어로 구현된다면, 기능들은 하나 이상의 명령들 또는 코드로서 컴퓨터 판독가능 매체 상에 저장되거나 전송될 수도 있다. 컴퓨터 판독가능 매체들은 한 장소에서 다른 장소로의 컴퓨터 프로그램의 전송을 용이하게 하는 임의의 매체를 포함하는 컴퓨터 저장 매체들 및 통신 매체들 양쪽 모두를 포함한다. 저장 매체들은 컴퓨터에 의해 액세스 가능한 임의의 이용가능한 매체들일 수도 있다. 비제한적인 예로서, 이러한 컴퓨터 판독가능 매체들은 RAM, ROM, EEPROM, CD-ROM 또는 다른 광 디스크 스토리지, 자기 디스크 스토리지, 또는 다른 자기 저장 디바이스들, 또는 소망의 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 운반하거나 저장하는데 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속이 컴퓨터 판독가능 매체로 적절히 칭해진다. 예를 들어, 소프트웨어가 웹사이트, 서버, 또는 다른 원격 자원으로부터 동축 케이블, 광섬유 케이블, 연선 (twisted pair), DSL, 또는 무선 기술들 이를테면 적외선, 라디오, 및/또는 마이크로파를 이용하여 송신된다면, 동축 케이블, 광섬유 케이블, 연선, DSL, 또는 적외선, 라디오, 및 마이크로파와 같은 무선 기술들은 매체의 정의에 포함된다. 디스크 (disk 및 disc) 는 본원에서 사용되는 바와 같이, CD, 레이저 디스크, 광 디스크, DVD, 플로피 디스크 (floppy disk) 및 블루레이 디스크 (blu-ray disc) 를 포함하는데, disk들은 보통 데이터를 자기적으로 및/또는 레이저들로 광적으로 재생한다. 상기한 것들의 조합들은 또한 컴퓨터 판독가능 매체들의 범위 내에 포함되어야 한다.

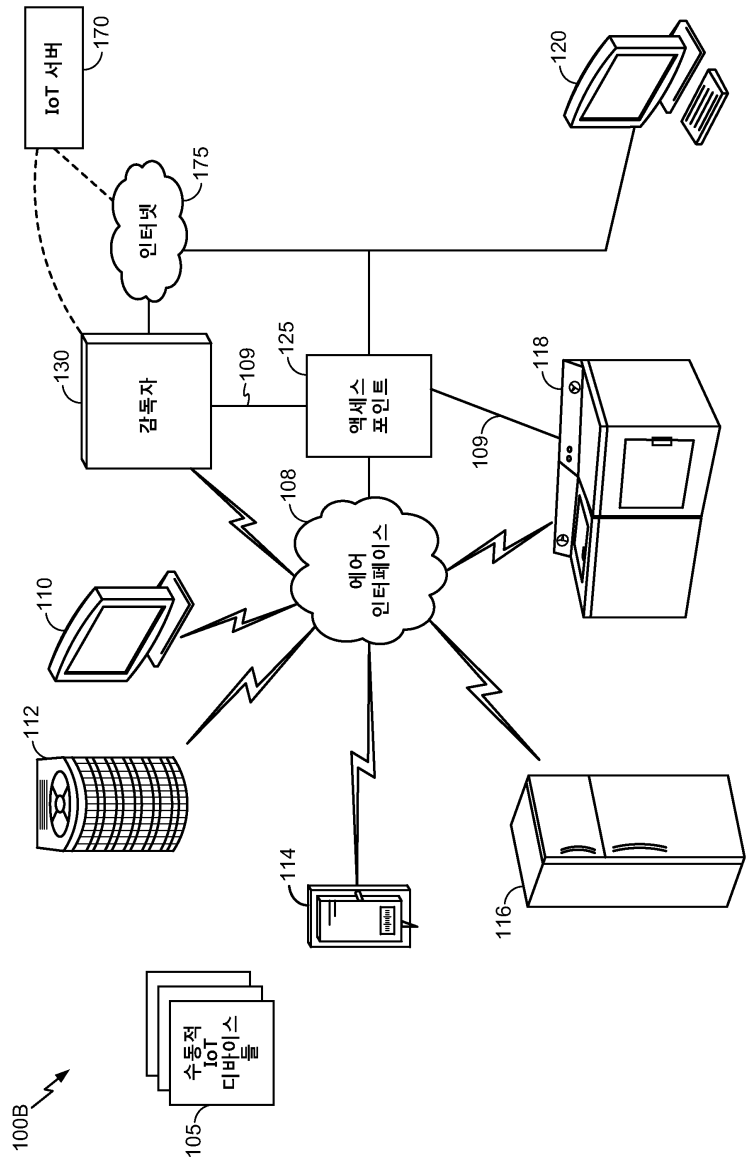
[0106] 전술한 개시물이 본 개시의 구체적인 양태들을 보여주지만, 갖가지 변경들 및 변형들이 첨부의 청구항들에 의해 정의된 바와 같은 본 개시물의 범위로부터 벗어남 없이 본원 내에서 만들어질 수 있다는 것에 주의해야 한다. 본원에서 설명된 본 개시물의 양태들에 따른 방법 청구항들의 기능들, 단계들 및/또는 액션들은 임의의 특정한 순서로 수행될 필요는 없다. 더욱이, 본 개시물의 엘리먼트들이 단수형으로 설명되고 청구되었을 수도 있지만, 단수형에 대한 제한이 명시적으로 언급되지 않는 한 복수형이 의도된 것이다.

도면

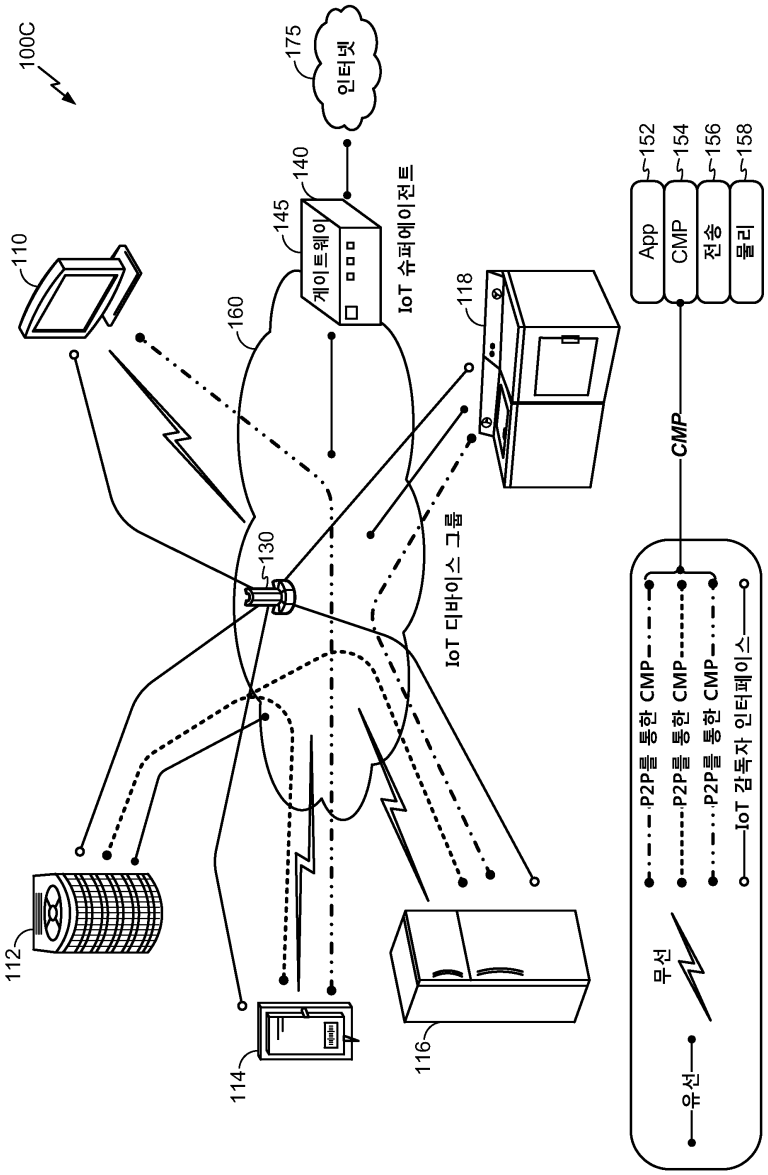
도면1a


IoT 서버
170
120
인터넷
175
125
액세스 포인트
118
109
110
108
에어 인터페이스
112
114
116
100A

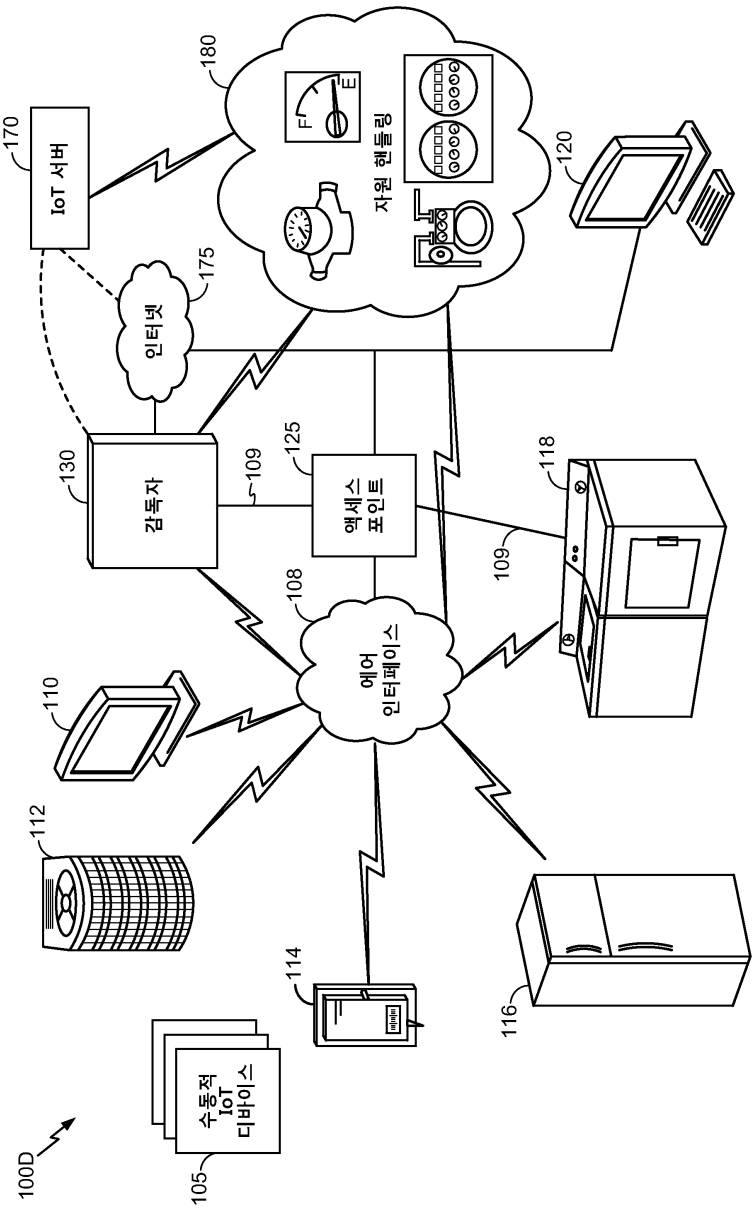
도면1b


IoT 서버
170
인터넷
175
120
감독자
130
109
액세스 포인트
125
118
109
에어 인터페이스
108
110
112
114
116
수동적 IoT 디바이스들
105
100B

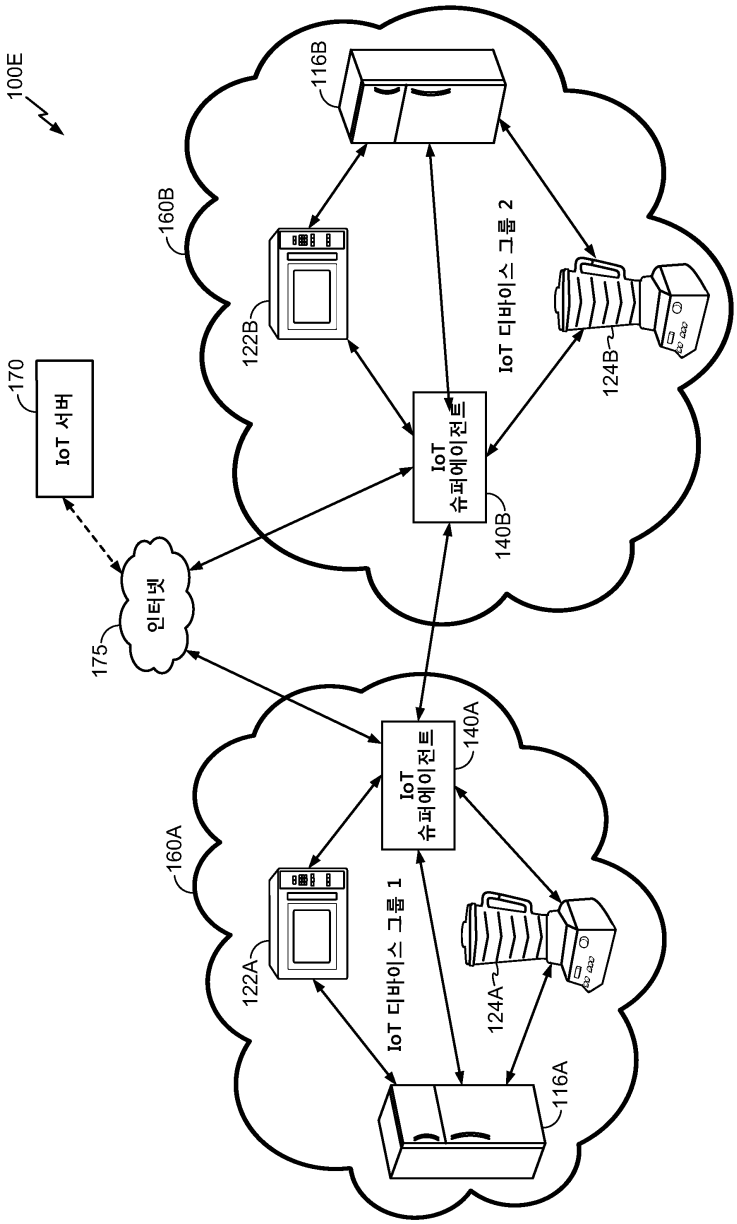
도면1c


100C
175
인터넷
140
145
게이트웨이
IoT 슈퍼에이전트
110
160
118
152
154
156
158
App
CMP
전송
물리
CMP
130
IoT 디바이스 그룹
112
114
116
P2P를 통한 CMP
P2P를 통한 CMP
P2P를 통한 CMP
IoT 감독자 인터페이스
무선
유선

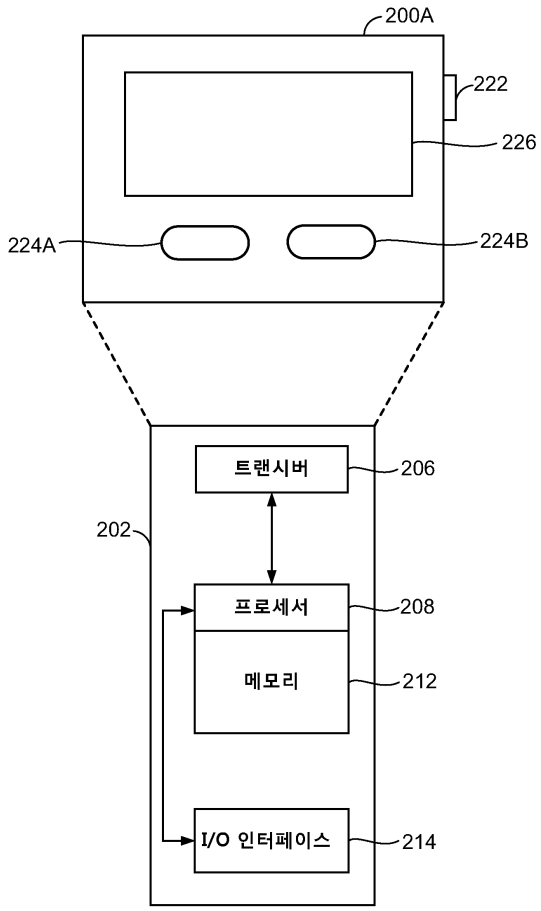
도면1d


100D
IoT 서버
170
180
자원 핸들링
F
E
120
인터넷
175
감독자
130
109
125
액세스 포인트
118
109
108
에어 인터페이스
110
112
114
116
수동적 IoT 디바이스
105

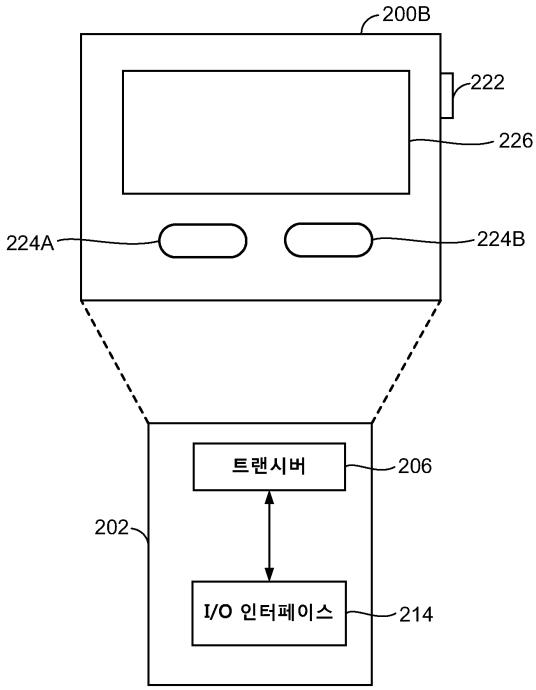
도면1e


100E
116B
160B
122B
IoT 디바이스 그룹 2
124B
170
IoT 서버
IoT
슈퍼에이전트
140B
인터넷
175
140A
160A
IoT 디바이스 그룹 1
122A
124A
116A

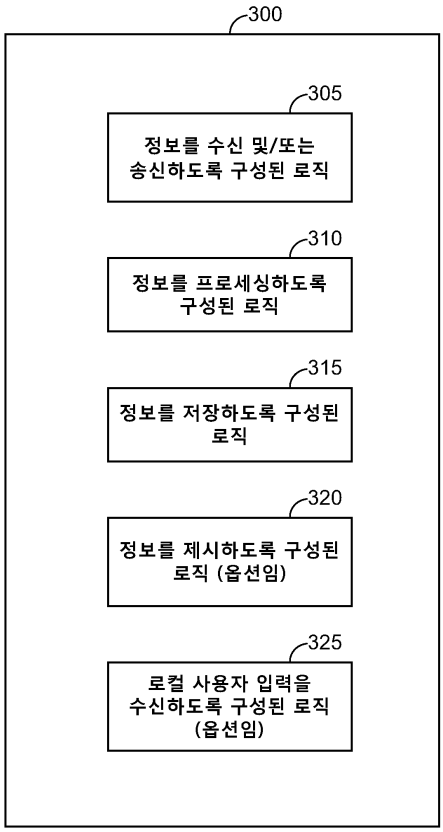
도면2a


200A
222
226
224A
224B
트랜시버
206
202
프로세서
208
메모리
212
I/O 인터페이스
214

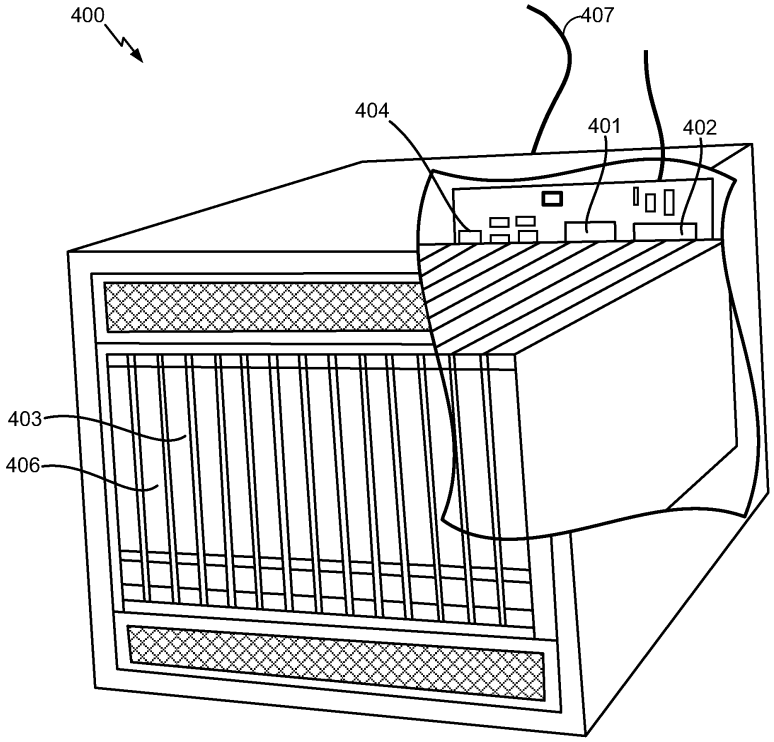
도면2b


200B
222
226
224A
224B
트랜시버
206
202
I/O 인터페이스
214

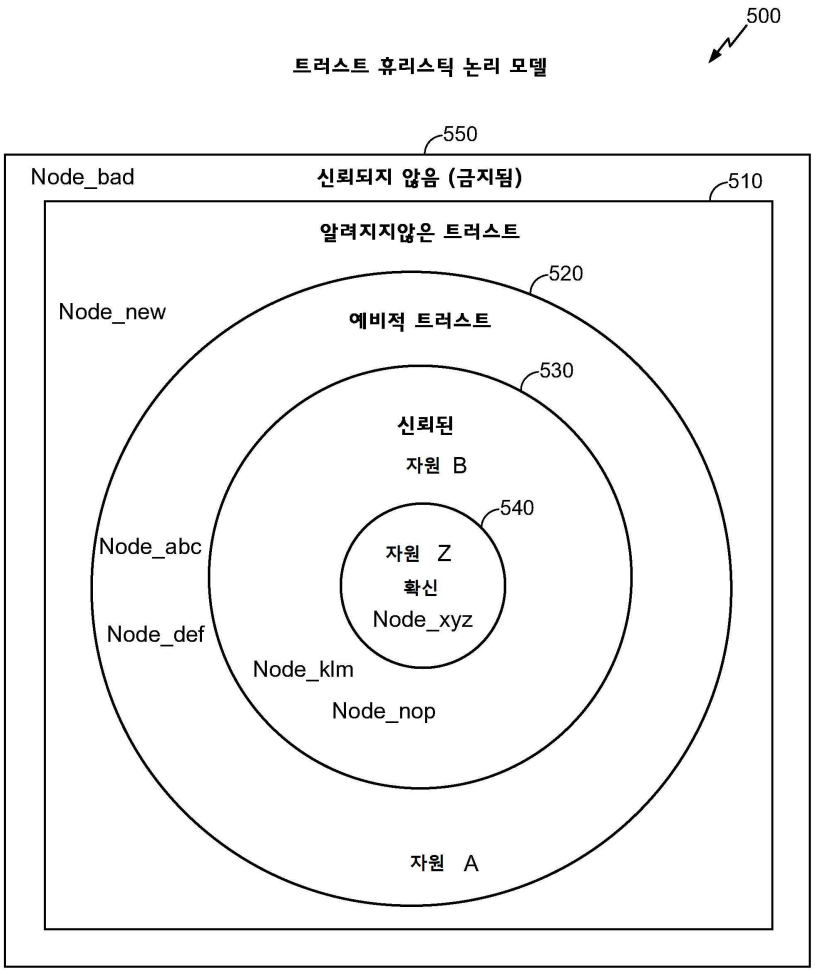
도면3


300
305
정보를 수신 및/또는 송신하도록 구성된 로직
310
정보를 프로세싱하도록 구성된 로직
315
정보를 저장하도록 구성된 로직
320
정보를 제시하도록 구성된 로직 (옵션임)
325
로컬 사용자 입력을 수신하도록 구성된 로직 (옵션임)

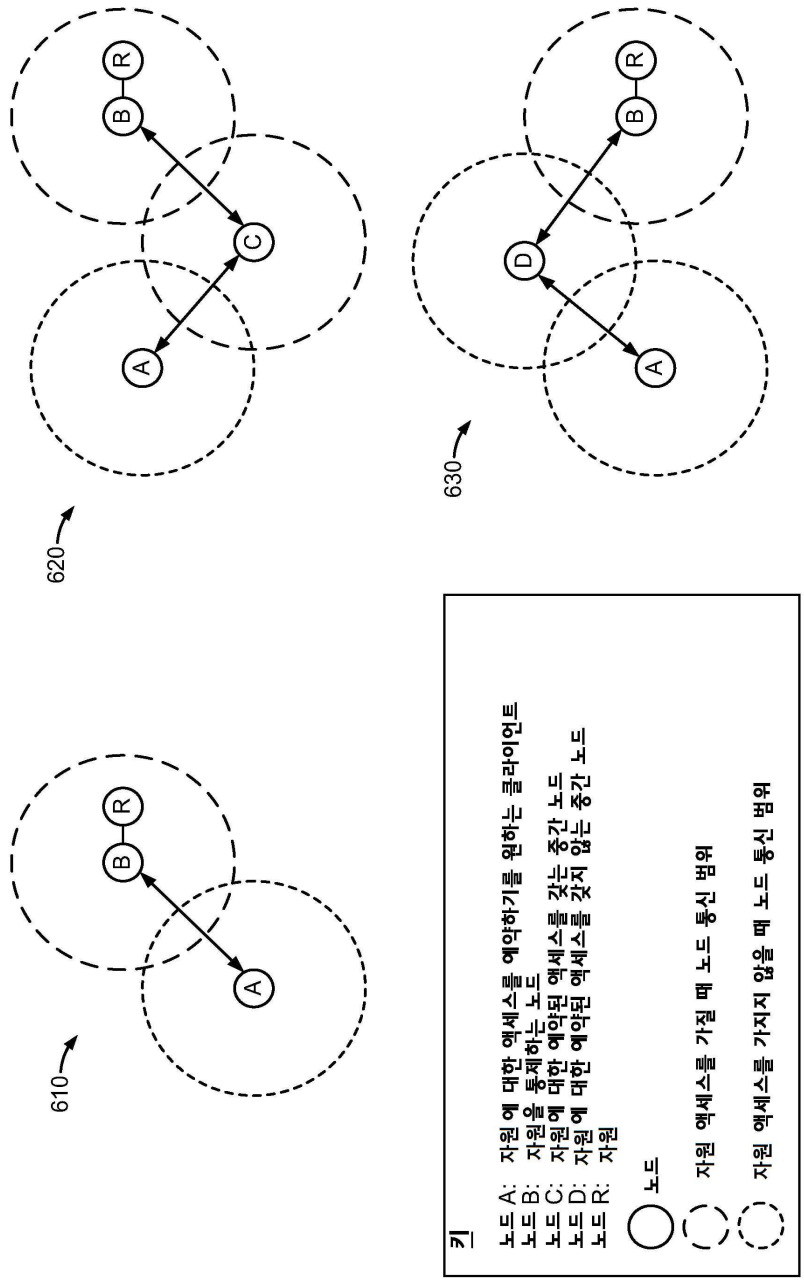
도면4



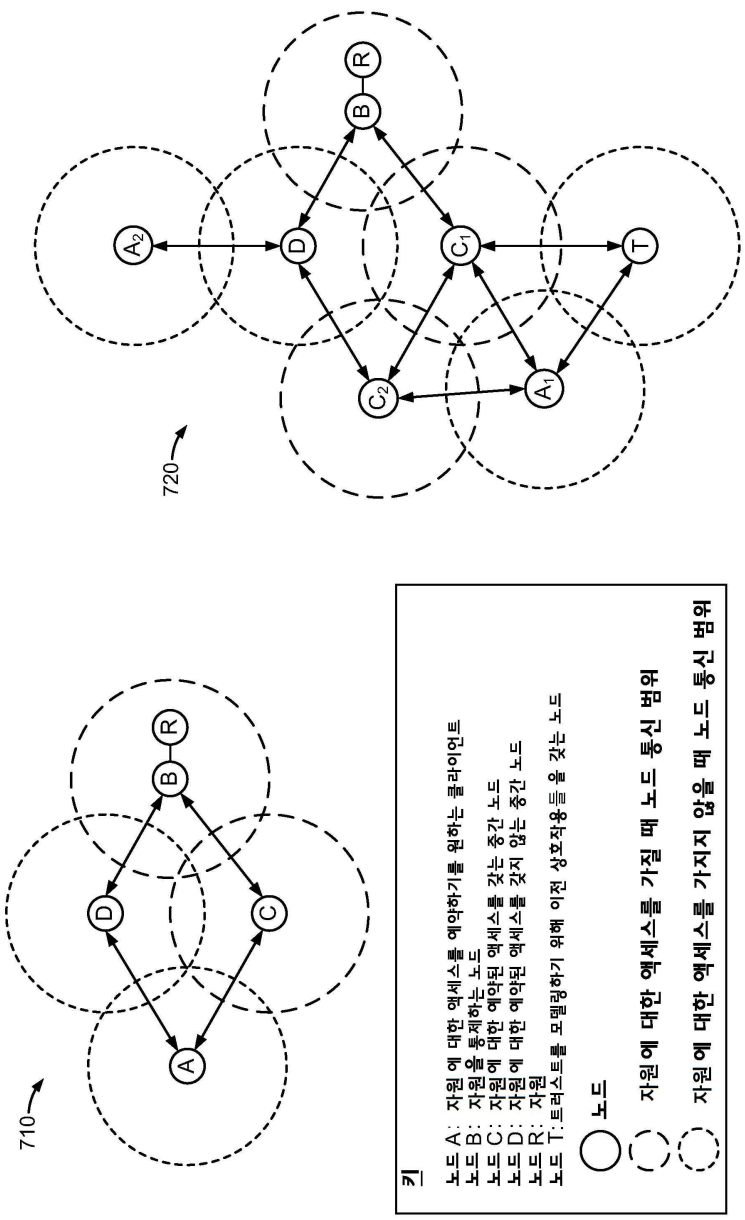
도면5


500
트러스트 휴리스틱 논리 모델
550
Node_bad
신뢰되지 않음 (금지됨)
510
알려지지않은 트러스트
520
Node_new
예비적 트러스트
530
신뢰된
자원 B
540
Node_abc
자원 Z
확신
Node_xyz
Node_def
Node_klm
Node_nop
자원 A

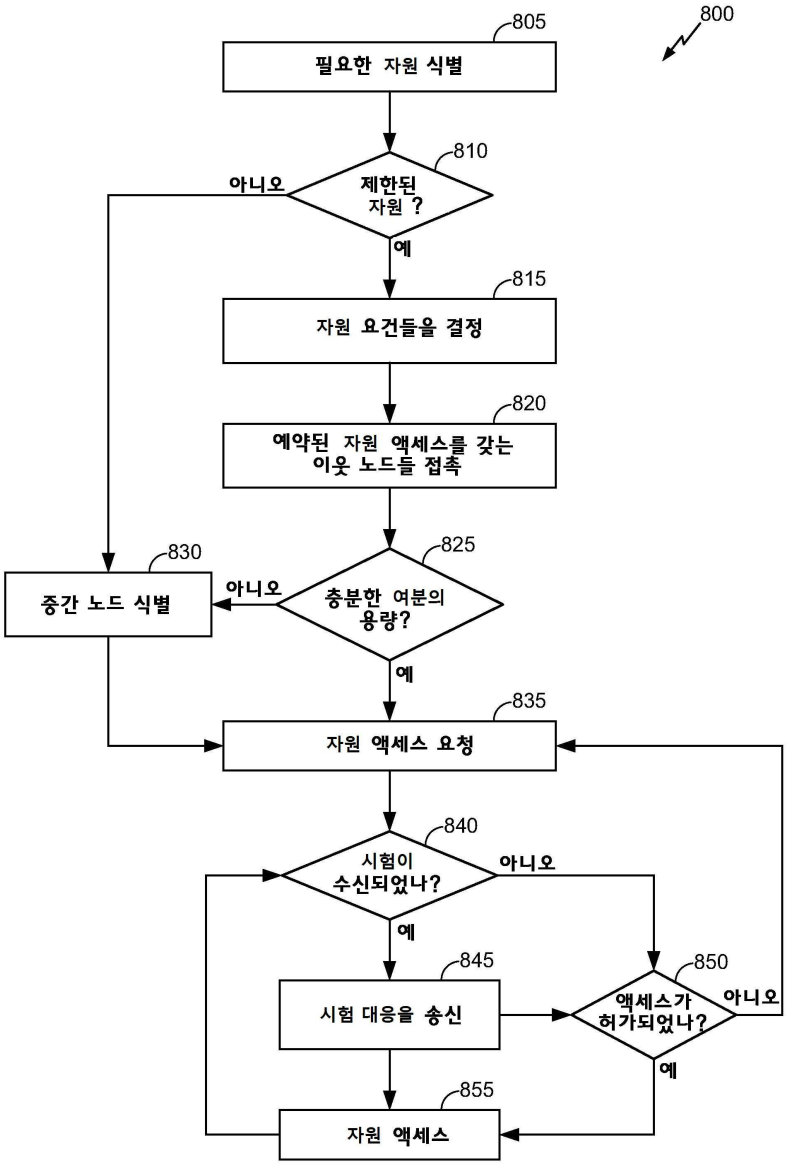
도면6


610
620
630
A
B
C
D
R
키
노드 A: 자원에 대한 액세스를 예약하기를 원하는 클라이언트
노드 B: 자원을 통제하는 노드
노드 C: 자원에 대한 예약된 액세스를 갖는 중간 노드
노드 D: 자원에 대한 예약된 액세스를 갖지 않는 중간 노드
노드 R: 자원
노드
자원 액세스를 가질 때 노드 통신 범위
자원 액세스를 가지지 않을 때 노드 통신 범위

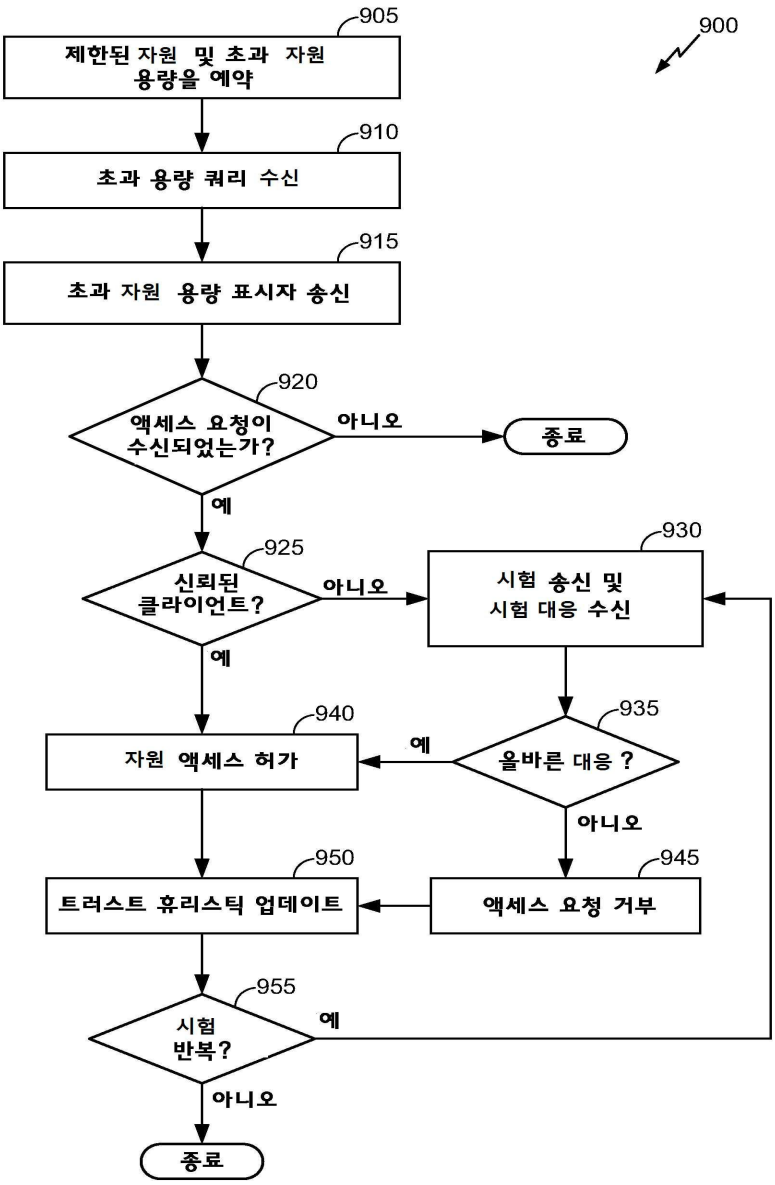
도면7


710
720
A
B
C
D
R
A2
C1
C2
A1
T
키
노드 A: 자원에 대한 액세스를 예약하기를 원하는 클라이언트
노드 B: 자원을 통제하는 노드
노드 C: 자원에 대한 예약된 액세스를 갖는 중간 노드
노드 D: 자원에 대한 예약된 액세스를 갖지 않는 중간 노드
노드 R: 자원
노드 T: 트래스트를 모델링하기 위해 이전 상호작용들을 갖는 노드
노드
자원에 대한 액세스를 가질 때 노드 통신 범위
자원에 대한 액세스를 가지지 않을 때 노드 통신 범위

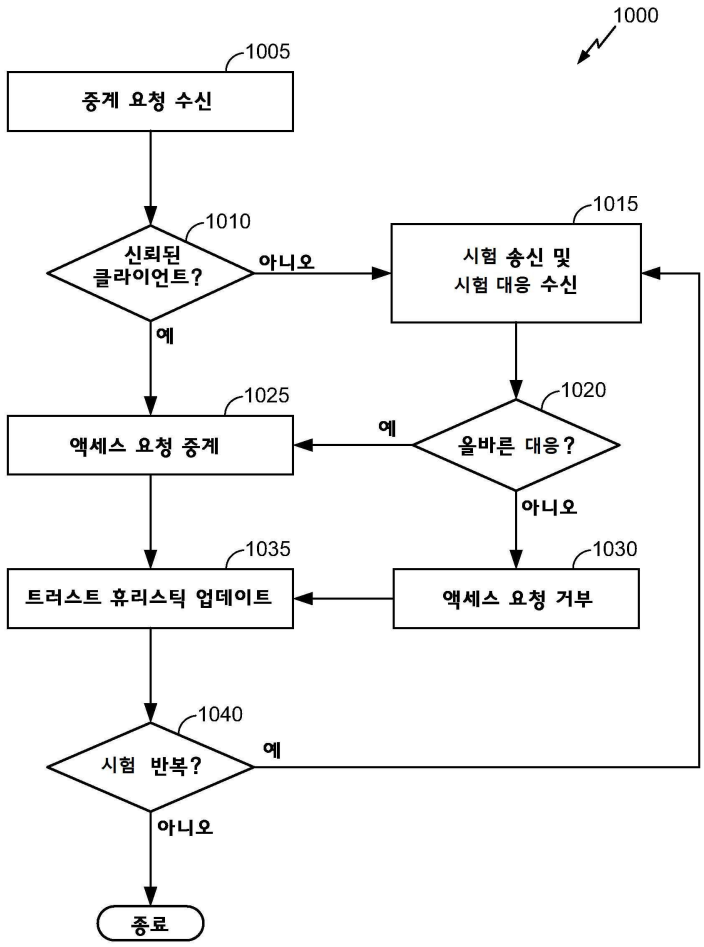
도면8


800
805
필요한 자원 식별
810
제한된 자원 ?
아니오
예
815
자원 요건들을 결정
820
예약된 자원 액세스를 갖는 이웃 노드들 접촉
825
충분한 여분의 용량?
830
중간 노드 식별
아니오
예
835
자원 액세스 요청
840
시험이 수신되었나?
아니오
예
845
시험 대응을 송신
850
액세스가 허가되었나?
아니오
예
855
자원 액세스

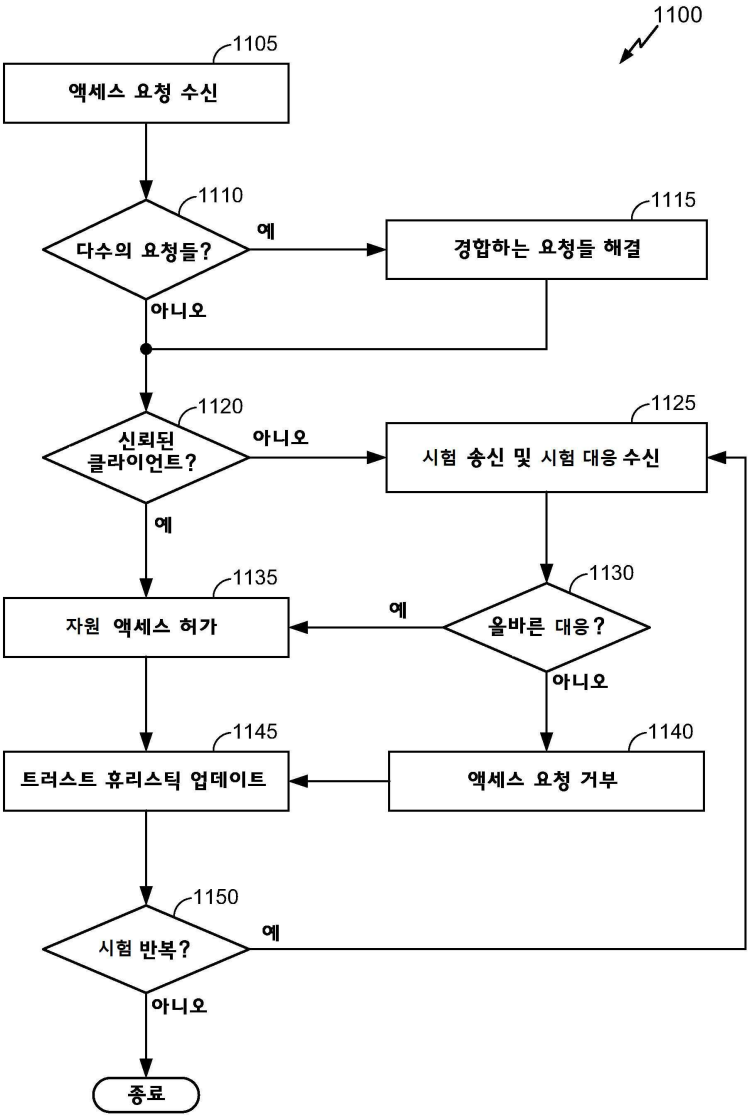
도면9


900
905
제한된 자원 및 초과 자원 용량을 예약
910
초과 용량 쿼리 수신
915
초과 자원 용량 표시자 송신
920
액세스 요청이 수신되었는가?
아니오
종료
예
925
신뢰된 클라이언트?
아니오
930
시험 송신 및 시험 대응 수신
예
935
올바른 대응 ?
예
940
자원 액세스 허가
아니오
945
액세스 요청 거부
950
트러스트 휴리스틱 업데이트
955
시험 반복?
예
아니오
종료

도면10


1000
1005
중계 요청 수신
1010
신뢰된 클라이언트?
아니오
예
1015
시험 송신 및 시험 대응 수신
1020
올바른 대응?
예
아니오
1025
액세스 요청 중계
1030
액세스 요청 거부
1035
트러스트 휴리스틱 업데이트
1040
시험 반복?
예
아니오
종료

도면11


1100
1105
액세스 요청 수신
1110
다수의 요청들?
예
1115
경합하는 요청들 해결
아니오
1120
신뢰된 클라이언트?
아니오
1125
시험 송신 및 시험 대응 수신
예
1130
올바른 대응?
예
1135
자원 액세스 허가
아니오
1140
액세스 요청 거부
1145
트러스트 휴리스틱 업데이트
1150
시험 반복?
예
아니오
종료