(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월10일
(11) 등록번호 10-1601769
(24) 등록일자 2016년03월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 12/28* (2006.01)
(21) 출원번호 10-2014-0150478
(22) 출원일자 2014년10월31일
심사청구일자 2014년10월31일
(56) 선행기술조사문헌
박지예 외 2인, 한국통신학회논문지 '13-09 Vol.38B No. 09, "사물 인터넷 환경에서 경량화 장치 간 상호 인증 및 세션키 합의 기술" (2013.09. 공개)
KR1020130129538 A

(73) 특허권자
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 마포구 백범로25길 63 106동 401호
이정엽
서울 마포구 광성로4길 22-6
(74) 대리인
이지연

전체 청구항 수 : 총 6 항 심사관 : 문형섭

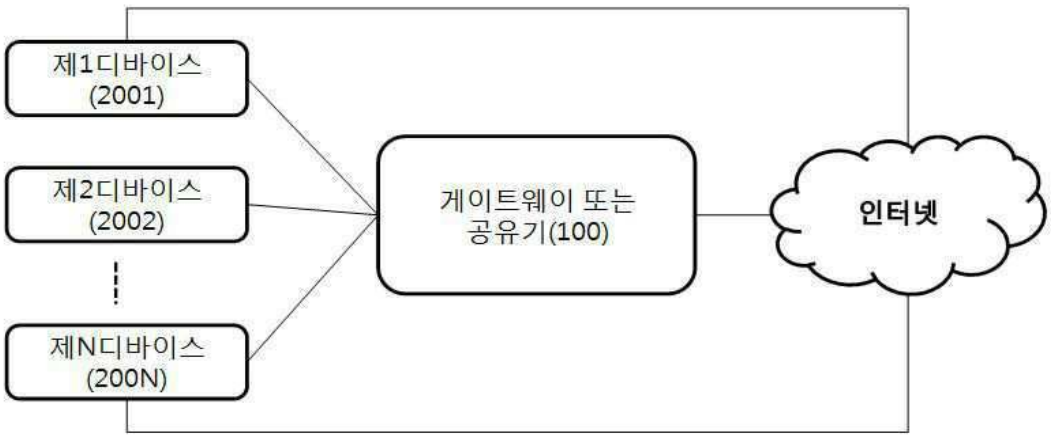
(54) 발명의 명칭 **소규모의 사물 인터넷 시스템 및 그를 위한 보안통신방법**

(57) 요 약

본 발명에 따르는 소규모의 사물 인터넷 시스템은, 디바이스들; 상기 디바이스들 중 둘 이상의 디바이스로부터 통신을 위한 등록요청이 발생되면, 그 둘 이상의 디바이스에 디바이스 ID를 부여함과 아울러, 그 둘 이상의 디바이스에 대한 디바이스 ID을 조합하여 통신경로정보를 생성하여 암호화하고, 상기 둘 이상의 디바이스에 대한 디

(뒷면에 계속)

대 표 도 - 도1



바이스 ID 각각과 암호화된 통신경로정보를 매칭하여 통신경로 등록정보를 생성하여 저장함과 아울러 상기 암호화된 통신경로정보를 해당 디바이스들로 전송하며, 어느 한 디바이스로부터 디바이스 ID와 암호화된 통신경로정보를 포함하는 통신요청메시지가 수신되면, 그 통신요청메시지에 포함되어 있는 암호화된 통신경로정보를 포함하는 통신경로등록정보들을 독출하고, 상기 통신경로등록정보들 중 상기 통신요청메시지를 송신한 디바이스의 디바이스 ID를 제외한 나머지 디바이스 ID들을 포함하는 통신경로등록정보들을 추출하고, 그 추출된 통신경로등록정보들에 포함된 디바이스 ID들의 디바이스들과 통신요청한 디바이스로 통신승인 메시지를 전송하는 게이트웨이 또는 공유기;를 구비하며, 상기 디바이스들은 암호화된 통신경로정보를 제공받아 저장하며, 상기 통신승인메시지를 수신받은 디바이스들은 서로 통신함을 특징으로 한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	H0301-14-1048
부처명	미래창조과학부
연구관리전문기관	정보통신산업진흥원
연구사업명	대학ICT연구센터육성지원사업
연구과제명	에너지 효율화를 위한 사물인터넷 플랫폼 개발 및 창의적 인재양성
기 여 율	1/1
주관기관	부산대학교 산학협력단
연구기간	2014.06.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

소규모의 사물 인터넷 시스템에 있어서,

디바이스들;

상기 디바이스들 중 둘 이상의 디바이스로부터 통신을 위한 등록요청이 발생되면, 그 둘 이상의 디바이스에 디바이스 ID를 부여함과 아울러, 그 둘 이상의 디바이스에 대한 디바이스 ID을 조합하여 통신경로정보를 생성하여 암호화하고, 상기 둘 이상의 디바이스에 대한 디바이스 ID 각각과 암호화된 통신경로정보를 매칭하여 통신경로등록정보를 생성하여 저장함과 아울러 상기 암호화된 통신경로정보를 해당 디바이스들로 전송하며,

어느 한 디바이스로부터 디바이스 ID와 암호화된 통신경로정보를 포함하는 통신요청메시지가 수신되면, 그 통신요청메시지에 포함되어 있는 암호화된 통신경로정보를 포함하는 통신경로등록정보들을 독출하고, 상기 통신경로등록정보들 중 상기 통신요청메시지를 송신한 디바이스의 디바이스 ID를 제외한 나머지 디바이스 ID들의 디바이스들로 상기 암호화된 통신경로정보가 포함된 통신요청 메시지를 송신하고, 그 통신요청 메시지에 응답하여 디바이스들로부터 인증성공 메시지가 수신되면, 그 디바이스들로 통신승인 메시지를 전송하는 게이트웨이 또는 공유기;를 구비하며,

상기 디바이스들은 암호화된 통신경로정보를 제공받아 저장하며,

상기 통신승인 메시지를 수신받은 디바이스들은 서로 통신하며,

상기 디바이스들은 통신요청 메시지가 수신되면, 그 통신요청 메시지에 포함된 암호화된 통신경로정보와 자신이 저장하고 있는 통신경로정보를 비교하여 유효한 통신요청인지를 인증함을 특징으로 하는 소규모의 사물 인터넷 시스템.

청구항 2

제1항에 있어서,

상기 게이트웨이 또는 공유기는, 상기 디바이스들과 외부 네트워크 사이를 인터페이스하며, 상기 디바이스들에 대해 IP 주소를 부여함을 특징으로 하는 소규모의 사물 인터넷 시스템.

청구항 3

제1항에 있어서,

상기 통신경로정보는 디바이스 ID들을 XOR하여 생성되며,

상기 통신경로정보의 암호화는 해싱으로 이루짐을 특징으로 하는 소규모의 사물 인터넷 시스템.

청구항 4

삭제

청구항 5

소규모의 사물 인터넷 시스템의 통신방법에 있어서,

게이트웨이 또는 공유기가, 디바이스들 중 둘 이상의 디바이스로부터 통신을 위한 등록요청이 발생되면, 그 둘 이상의 디바이스에 디바이스 ID를 부여함과 아울러, 그 둘 이상의 디바이스에 대한 디바이스 ID을 조합하여 통신경로정보를 생성하여 암호화하고, 상기 둘 이상의 디바이스에 대한 디바이스 ID 각각과 암호화된 통신경로정보를 매칭하여 통신경로등록정보를 생성하여 저장함과 아울러 상기 암호화된 통신경로정보를 해당 디바이스들로 전송하는 제1단계;

상기 디바이스들이 상기 암호화된 통신경로정보를 제공받아 저장하는 제2단계;

상기 게이트웨이 또는 공유기가, 어느 한 디바이스로부터 디바이스 ID와 암호화된 통신경로정보를 포함하는 통신요청메시지가 수신되면, 그 통신요청메시지에 포함되어 있는 암호화된 통신경로정보를 포함하는 통신경로등록정보들을 독출하고, 상기 통신경로등록정보들 중 상기 통신요청메시지를 송신한 디바이스의 디바이스 ID를 제외한 나머지 디바이스 ID들의 디바이스들로 상기 암호화된 통신경로정보가 포함된 통신요청 메시지를 송신하는 제3단계;

상기 디바이스들이, 상기 게이트웨이 또는 공유기로부터의 통신요청 메시지가 수신되면, 그 통신요청 메시지에 포함된 암호화된 통신경로정보와 자신이 저장하고 있는 통신경로정보를 비교하여 유효한 통신요청인지 인증하고 그에 따라 인증성공 메시지를 상기 게이트웨이 또는 공유기로 제공하는 제4단계;

상기 게이트웨이 또는 공유기가, 상기 디바이스들이 통신요청 메시지에 응답하여 인증성공 메시지가 제공하면, 그 디바이스들로 통신승인 메시지를 전송하는 제5단계를 구비하며,

상기 통신승인 메시지를 수신받은 디바이스들은 서로 통신함을 특징으로 하는 소규모의 사물 인터넷 시스템의 통신방법.

청구항 6

제5항에 있어서,

상기 게이트웨이 또는 공유기가, 상기 디바이스들과 외부 네트워크 사이를 인터페이스하며, 상기 디바이스들에 대해 IP 주소를 부여하는 단계를 더 구비함을 특징으로 하는 소규모의 사물 인터넷 시스템의 통신방법.

청구항 7

제5항에 있어서,

상기 통신경로정보는 디바이스 ID들을 XOR하여 생성되며,

상기 통신경로정보의 암호화는 해싱으로 이루어짐을 특징으로 하는 소규모의 사물 인터넷 시스템의 통신방법.

청구항 8

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 소규모의 사물 인터넷 기술에 관한 것으로, 더욱 상세하게는 소규모의 사물 인터넷을 형성하는 다수의 디바이스 사이의 통신경로에 대한 보안을 유지하는 소규모의 사물 인터넷 시스템 및 그를 위한 보안통신방법에 관한 것이다.

배 경 기 술

[0002] 사물 인터넷(Internet of Things, IoT)은 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 말한다. 이러한 사물 인터넷은 1999년 매사추세츠공과대학(MIT)의 오토아이디센터(Auto-ID Center) 소장 케빈 애시턴(Kevin Ashton)이 향후 RFID(전자태그)와 기타 센서를 일상생활에 사용하는 사물에 탑재한 사물인터넷이 구축될 것이라고 전망하면서 처음 사용한 것으로 알려져 있으며, 이후 시장분석 자료 등에 사용되면서 대중화되었다.

[0003] 상기 사물 인터넷은 기존의 유선통신을 기반으로 한 인터넷이나 모바일 인터넷보다 진화된 단계로 인터넷에 연결된 기기가 사람의 개입없이 상호간에 알아서 정보를 주고 받아 처리한다. 이와같이 사물이 인간에 의존하지 않고 통신을 주고받는 점에서 유비쿼터스나 M2M(Machine to Machine: 사물지능통신)과 비슷하기도 하지만, 통신장비와 사람과의 통신을 주목적으로 하는 M2M의 개념을 인터넷으로 확장하여 사물은 물론이고 현실과 가상세계의 모든 정보와 상호작용하는 개념으로 진화한 것이라 할 수 있다.

[0004] 이를 구현하기 위한 기술 요소로는 유형의 사물과 주위 환경으로부터 정보를 얻는 '센싱 기술', 사물이 인터넷에 연결되도록 지원하는 '유무선 통신 및 네트워크 인프라 기술', 각종 서비스 분야와 형태에 적합하게 정보를 가공하고 처리하거나 각종 기술을 융합하는 '서비스 인터페이스 기술' 등이 있으며, 대량의 데이터 등 사물 인터넷 구성 요소에 대한 해킹이나 정보 유출을 방지하기 위한 '보안 기술'도 필수적이다.

[0005] 이러한 사물 인터넷으로는 키를 가지고 접근하면 자동차 문의 잠금 장치가 자동으로 해제되고 키를 꽂지 않아도 시동을 걸 수 있는 '스마트 키', 전기·가스 또는 상하수도를 포함한 에너지를 효율적으로 관리하는 '스마트 그리드' 등이 있다.

[0006] 상기한 바와 같은 사물 인터넷을 이용하면 댁내 설비 네트워크 등과 같은 소규모의 네트워크를 형성할 수 있다. 상기 댁내 설비 네트워크를 형성하는 설비에는 도어락이나 금고 비밀번호, 움직임 센서, 온도센서 등이 포함될 수 있다.

[0007] 상기한 댁내 설비 네트워크는 어느 한 설비의 출력값을 다른 설비가 제공받아 특정 동작을 이행하는 등의 방식으로 고객에게 차별화된 서비스를 제공하고 있다. 예를들면, 움직임 센서 등을 통해 외부인이 있는 것으로 파악되면, 경보를 울리는 것 등이 될 수 있다.

[0008] 그런데 상기한 댁내 설비 네트워크는 설비 각각이 인터넷에 연결되기 때문에 보안에 취약한 위험이 존재한다. 예를들면, 외부인 침입여부를 판별하기 경보를 울리기 위한 센서들의 출력값들을 도리어 해당 댁내에 사람이 있는지 여부를 판별하는데에 사용할 수도 있기 때문이다.

[0009] 이에 종래에는 소규모의 사물 인터넷 시스템에서 디바이스들 사이에 송수신되는 데이터는 물론이고, 어느 디바이스와 어느 디바이스가 통신하는지에 대한 통신경로에 대한 보안도 강화시킬 수 있는 기술의 개발이 절실하게 요망되었다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 한국특허공개 제1020050116140호

(특허문헌 0002) 한국특허공개 제10-2008-0001574호

(특허문헌 0003) 한국특허공개 제10-2009-0044437호

(특허문헌 0004) 한국특허공개 제10-2010-0073827호

발명의 내용

해결하려는 과제

[0011] 본 발명은 소규모의 사물 인터넷을 구성하는 디바이스들 사이의 통신경로에 대한 보안을 강화시키는 소규모의 사물 인터넷 시스템 및 그를 위한 보안통신방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0012] 상기한 목적을 달성하기 위한 본 발명에 따르는 소규모의 사물 인터넷 시스템은, 디바이스들; 상기 디바이스들 중 둘 이상의 디바이스로부터 통신을 위한 등록요청이 발생되면, 그 둘 이상의 디바이스에 디바이스 ID를 부여함과 아울러, 그 둘 이상의 디바이스에 대한 디바이스 ID을 조합하여 통신경로정보를 생성하여 암호화하고, 상기 둘 이상의 디바이스에 대한 디바이스 ID 각각과 암호화된 통신경로정보를 매칭하여 통신경로 등록정보를 생성하여 저장함과 아울러 상기 암호화된 통신경로정보를 해당 디바이스들로 전송하며, 어느 한 디바이스로부터

디바이스 ID와 암호화된 통신경로정보를 포함하는 통신요청메시지가 수신되면, 그 통신요청메시지에 포함되어 있는 암호화된 통신경로정보를 포함하는 통신경로등록정보들을 독출하고, 상기 통신경로등록정보들 중 상기 통신요청메시지를 송신한 디바이스의 디바이스 ID를 제외한 나머지 디바이스 ID들을 포함하는 통신경로등록정보들을 추출하고, 그 추출된 통신경로등록정보들에 포함된 디바이스 ID들의 디바이스들과 통신요청한 디바이스로 통신승인 메시지를 전송하는 게이트웨이 또는 공유기;를 구비하며, 상기 디바이스들은 암호화된 통신경로정보를 제공받아 저장하며, 상기 통신승인메시지를 수신받은 디바이스들은 서로 통신함을 특징으로 한다.

발명의 효과

[0013] 상기한 본 발명은 소규모의 사물 인터넷을 구성하는 디바이스들 사이의 통신경로에 대한 보안을 강화시킬 수 있는 효과를 야기한다.

도면의 간단한 설명

[0014] 도 1은 본 발명의 바람직한 실시예에 따른 소규모의 사물 인터넷 시스템의 구성도.

도 2 및 도 3은 도 1의 각부에 대한 상세 구성도.

도 4 및 도 5는 본 발명의 바람직한 실시예에 따른 소규모 사물 인터넷 시스템의 보안통신방법의 흐름도.

도 6은 본 발명의 바람직한 실시예에 따른 통신경로정보를 예시한 도면.

발명을 실시하기 위한 구체적인 내용

[0015] 본 발명은 소규모의 사물 인터넷을 구성하는 디바이스들 사이의 통신 경로에 대한 보안을 강화시킬 수 있다.

[0016] <사물 인터넷 시스템의 구성>

[0017] 이러한 본 발명의 바람직한 실시예에 따른 사물 인터넷 시스템의 구성을 도 1을 참조하여 상세히 설명한다.

[0018] 상기 사물 인터넷 시스템은 기본적인 IoT 네트워크 구성을 나타내는 것으로 게이트웨이 또는 공유기(100)와 제1 내지 제N디바이스(2001~200N)로 구성된다.

[0019] 상기 게이트웨이 또는 공유기(100)는 도메인을 형성하며, 상기 제1 내지 제N디바이스(2001~200N)에 대해 NAT(Network Address translation)를 통해 IP를 부여함과 아울러 IP 주소 번역 테이블(IP Address translation table)을 통해 인터넷에 접속시킨다. 상기 제1 내지 제N디바이스(2001~200N)는 게이트웨이 또는 공유기(100)를 통해 무선으로 인터넷에 접속되며, NAT를 통해 IP를 할당받는다. 따라서 외부에서는 상기 사물 인터넷 도메인에 있는 디바이스들의 IP 주소를 알 수 없고, 게이트웨이 또는 공유기(100)가 구비하는 IP 주소 번역 테이블을 알 수 없기 때문에 접속할 수도 없다. 또한 상기 게이트웨이 또는 공유기(100)는 모든 통신경로에 대한 통신경로정보를 수집하고, 이 통신경로정보를 해쉬함수를 통해 암호화하며, 암호화된 통신경로정보와 통신주체가 되는 디바이스 ID를 매칭시켜 통신경로 등록정보를 생성하고, 이를 저장한다. 여기서, 상기 통신경로정보는, 통신주체가 되는 디바이스들의 디바이스 ID들을 XOR 연산하여 생성된다. 또한 제1 내지 제N디바이스(2001~200N) 각각은 내부에 경량의 웹서버를 가지며, 이를 통한 웹 페이지를 통해 디바이스의 여러 가지 기능들을 제어할 수 있게 한다. 또한 제1 내지 제N디바이스(2001~200N) 각각은 게이트웨이 또는 공유기(100)를 통해 외부 인터넷망과 연결되어 있으므로 외부 웹 페이지에서 정보수집을 할 수 있고 이를 통해 온톨로지를 구현할 수 있다. 여기서, 상기 온톨로지는 국제표준화기구(ISO)의 기술을 따르나, 이는 설계자 또는 사용자의 편이에 따라 변경될 수 있음은 물론이며 본 발명에 의해 당업자에게 자명하다.

[0020] 도 2는 본 발명의 바람직한 실시예에 따르는 게이트웨이 또는 공유기의 구성도이다.

[0021] 상기 게이트웨이 또는 공유기(100)는 디바이스 관리부(300), 연산부(308), 메모리부(314)로 구성된다. 상기 디바이스 관리부(300)는 제1 내지 제N디바이스(2001~200N) 각각과 인터넷 사이를 연결하는 인터넷 연결부(302), 도메인 내에 어떤 디바이스들이 있는지 정보를 관리하는 디바이스 등록부(304), 그리고 각 디바이스들의 IP 할

당 및 디바이스 ID를 할당해주는 IP 할당부 및 디바이스 ID 할당부(306)로 구성된다. 그리고 연산부(308)는 해싱함수부(310)와 XOR 연산부(312)로 구성된다. 상기 XOR 연산부(312)는 IP 할당부 및 디바이스 ID 할당부(306)에 의해 생성된 디바이스 ID를 수집하여 통신 주체가 되는 디바이스들의 디바이스 ID들에 대한 XOR 연산을 실행하여 통신경로정보를 생성한다. 그리고 해싱함수부(310)는 상기 통신경로정보를 해싱연산한다. 그리고 메모리부(314)는 디바이스 ID 저장부(316)와 XOR 연산결과 저장부(318)와 해싱결과 저장부(320)와 통신경로 등록정보 저장부(322)로 구성된다. 상기 디바이스 ID 저장부(316)는 IP 할당부 및 디바이스 ID 할당부(306)에서 생성한 디바이스 ID들을 저장하고, 상기 XOR 연산결과 저장부(318)는 상기 XOR 연산부(312)의 출력정보들인 통신경로정보를 임시 저장한다. 상기 해싱결과 저장부(320)는 상기 통신경로정보를 해싱하여 암호화한 암호화된 통신경로정보를 임시 저장한다. 그리고 상기 통신경로 등록정보 저장부(322)는 상기 암호화된 통신경로정보와 그 통신경로의 통신주체가 되는 디바이스들의 디바이스 ID들을 매칭시킨 통신경로 등록정보를 저장한다.

[0022] 본 발명에 따르는 해싱을 위한 해시함수로는 SHA256, SHA384, RMD256 등이 채용될 수 있으나, 이는 설계자 또는 사용자의 편이에 따라 변경될 수 있음은 물론이며 본 발명에 의해 당업자에게 자명하다.

[0023] 본 발명에 따르는 디바이스들(2001~200N)의 구성 및 동작은 고유기능을 제외하고는 동일하므로, 상기 디바이스들(2001~200N) 중 어느 한 디바이스의 구성 및 동작만을 도 3을 참조하여 설명한다.

[0024] 상기 디바이스는 인터넷 연결부(400)와 웹서버 생성부(402)와 메모리부(404)와 디바이스 기능부(406)로 구성된다. 상기 인터넷 연결부(400)는 게이트웨이 또는 공유기(100)와 연결되어 상기 게이트웨이 또는 공유기(100)를 통해 인터넷 또는 다른 디바이스와의 통신을 수행한다. 여기서, 상기 통신을 위한 프로토콜은 HTTP, Mqtt, CoAP 등이 채용될 수 있고, 통신방식으로는 WiFi, Zigbee, X10, BT 등이 채용될 수 있으나, 이는 설계자 또는 사용자의 편이에 따라 변경될 수 있음은 물론이며 본 발명에 의해 당업자에게 자명하다. 상기 웹서버 생성부(402)는 웹 서버를 생성하여 인터넷을 통해 접속한 사용자에게 디바이스 제어를 위한 정보를 제공한다. 상기 메모리부(404)는 소량으로 웹 서버 생성에 필요한 코드, 해시값 등을 저장하며, 저장소 형태는 보조기억매체, 캐시 형태 등 다양한 종류의 저장형태가 될 수 있다. 상기 디바이스 기능부(406)는 상기 메모리부(404)에 저장된 코드를 실행함과 아울러, 이에 따른 기능을 수행하다. 또한 상기 디바이스 기능부(406)는 상기 코드 실행 뿐 아니라 디바이스 자체 기능을 수행한다.

[0025] <디바이스 및 통신경로정보 등록방법>

[0026] 상기한 소규모 사물 인터넷 시스템에 적용 가능한 디바이스 및 통신경로정보 등록방법을 도 4의 흐름도를 참조하여 설명한다. 본 발명의 바람직한 실시예에 따른 게이트웨이 또는 공유기(100)는 소규모 사물 인터넷 시스템에 접근하는 모든 디바이스에 대해 디바이스 및 통신경로정보를 등록하나, 이하 설명의 편이상 제1 및 제2디바이스가 자신의 정보 및 통신경로를 등록하는 과정만을 설명한다.

[0027] 상기 게이트웨이 또는 공유기(100)는 제1 및 제2디바이스(2001,2002)로부터 디바이스 및 통신경로 등록이 요청되면(500단계), 상기 제1 및 제2디바이스(2001,2002)에 대해 디바이스 ID와 IP 주소를 부여함과 아울러 상기 디바이스 ID와 IP 주소를 해당 디바이스로 제공하여 안내한다(502단계).

[0028] 이후 상기 게이트웨이 또는 공유기(100)는 제1 및 제2디바이스(2001,2002)의 디바이스 ID를 XOR 연산하고, 그 연산 결과를 해싱하여 암호화된 통신경로정보를 생성한다. 또한 상기 게이트웨이 또는 공유기(100)는 암호화된 통신경로정보와 제1 및 제2디바이스의 디바이스 ID들을 각각 매칭시켜 통신경로 등록정보를 생성하여 저장함과 아울러, 제1 및 제2디바이스로 상기 암호화된 통신경로정보를 반환한다(504,506,508단계).

[0029] 이와같이 통신경로정보는 암호화되어 임의의 공격자가 디바이스를 공격하더라도 통신경로정보를 해독할 수 없게 하여, 해당 디바이스의 특정값이 다른 디바이스로 전달되어 미리 정해둔 특정 기능을 수행하게 하는지 등을 확인할 수 없게 한다. 예를들어, 제1센서의 센싱값이 소정 한계치를 벗어나는 경우에 도어를 자동으로 개방하도록 사물 인터넷 시스템을 구성하였을 때에, 악의의 공격자가 상기 도어에 접근하여 통신경로정보를 획득하더라도 그 통신경로정보가 자체가 암호화됨에 따라 상기 도어가 제1센서의 센싱값을 토대로 동작하는 것임을 확인할 수 없게 한다.

[0030] 이러한 보안 강화 효과는 사물 인터넷 시스템에 구비되는 디바이스의 개수가 늘어날수록 향상된다. 즉 디바이스의 개수가 5개인 경우에는 통신경로를 예측할 확률은 $1/{}_5P_2$이고, 디바이스의 개수가 30개인 경우에는 $1/{}_{30}P_2$가 된

다.

[0031] <디바이스간 통신과정>

[0032] 상기한 바와 같이 디바이스 및 통신경로정보 등록이 완료된 후에, 디바이스간 통신과정을 설명한다.

[0033] 어느 한 디바이스는 미리 설정된 기능의 수행을 위한 통신 요구가 발생되면, 통신요청 메시지를 생성하여 게이트웨이 또는 공유기(100)로 제공한다(600단계). 상기 통신요청 메시지는 자신의 디바이스 ID와 암호화된 통신경로정보를 포함한다. 예를들어, 도 6을 참조하면, 제1디바이스(2001)는 디바이스 ID(0001)와 암호화된 통신경로정보(1d533ec2e7d744e1ac9a2e874a5f269093234df3)로 구성되는 통신요청 메시지를 생성하여 게이트웨이 또는 공유기(100)로 제공할 수 있다.

[0034] 상기 통신요청 메시지를 수신한 게이트웨이 또는 공유기(100)는, 상기 통신요청 메시지에 포함된 암호화된 통신경로정보를 추출하고(602단계), 통신경로 테이블에서 상기 암호화된 통신경로정보를 포함하며 디바이스 ID가 상이한 통신경로 등록정보를 추출하고, 그 통신경로 등록정보에 포함된 디바이스 ID에 대응되는 디바이스로 통신요청 메시지를 전송한다(604단계). 상기 통신요청 메시지에는 자신의 ID와 암호화된 통신경로정보가 포함된다. 예를들어, 도 6을 참조하면, 게이트웨이 또는 공유기(100)는 통신경로 테이블에서 디바이스 ID(0001)는 상이한 상태에서 암호화된 통신경로정보(1d533ec2e7d744e1ac9a2e874a5f269093234df3)는 동일한 통신경로 등록정보를 추출하며, 이는 디바이스 ID는 0010이고 암호화된 통신경로정보는 1d533ec2e7d744e1ac9a2e874a5f269093234df3인 통신경로 등록정보가 될 수 있다.

[0035] 상기 통신요청 메시지를 수신한 디바이스(이하, 편이상 제2디바이스라 칭함)는, 상기 통신요청 메시지에 포함된 암호화된 통신경로정보를 추출하고, 그 암호화된 통신경로정보와 미리 저장된 암호화된 통신경로정보가 동일한지 여부를 토대로 유효한 통신요청인지를 인증한다(606단계).

[0036] 상기 통신요청이 유효하면, 상기 제2디바이스는 응답메시지를 생성하여 게이트웨이 또는 공유기(100)로 제공한다(608단계). 여기서, 상기 응답메시지에는 디바이스 ID와 암호화된 통신경로 정보가 포함되며, 도 6을 참조하면, 디바이스 ID는 0010이고 암호화된 통신경로정보는 1d533ec2e7d744e1ac9a2e874a5f269093234df3이 될 수 있다.

[0037] 상기 게이트웨이 또는 공유기(100)는 제1디바이스로부터의 통신요청 메시지에 포함된 통신경로메시지와 제2통신요청 메시지에 포함된 응답메시지에 포함된 응답메시지에 포함된 암호화된 통신경로정보가 용일한지 여부를 토대로 통신경로가 유효한지를 판단하고(612단계), 상기 통신경로가 유효하면 상기 제1 및 제2디바이스로 통신승인 메시지를 전송한다(614단계).

[0038] 상기 통신승인 메시지를 수신받은 제1 및 제2디바이스는 통신을 실행한다(616단계).

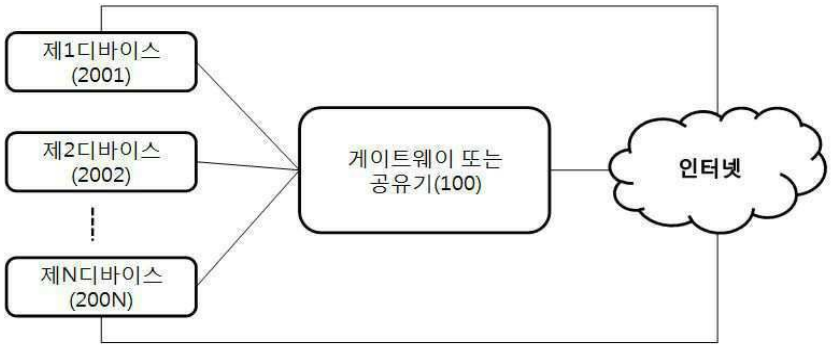
부호의 설명

[0039] 100 : 게이트웨이 또는 공유기

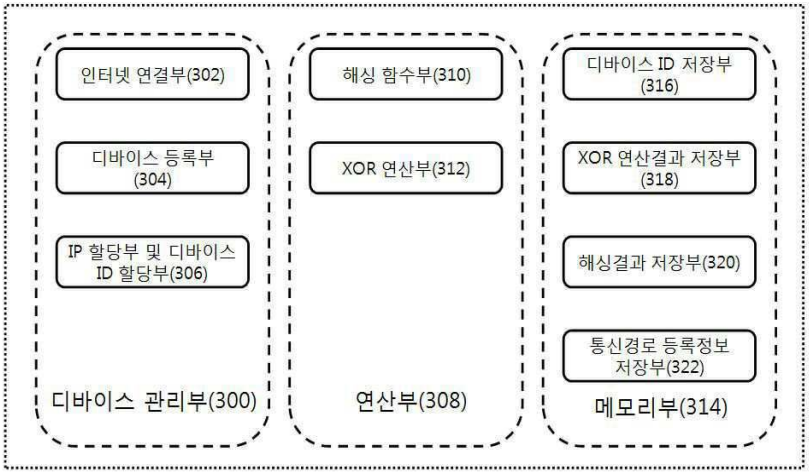
2001~200N : 제1 내지 제N 디바이스

도면

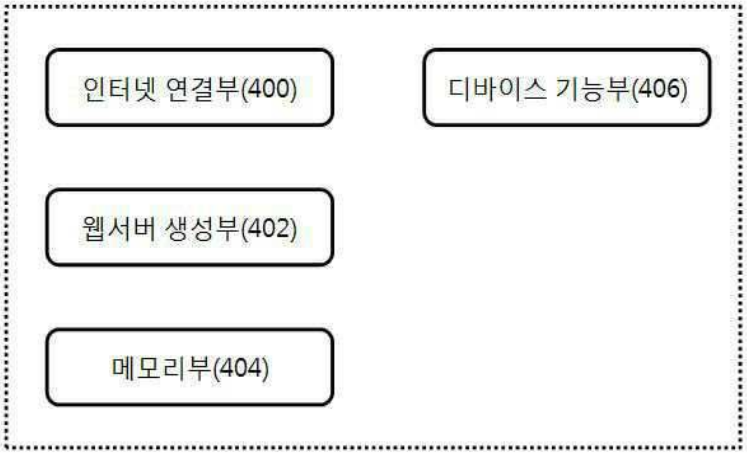
도면1



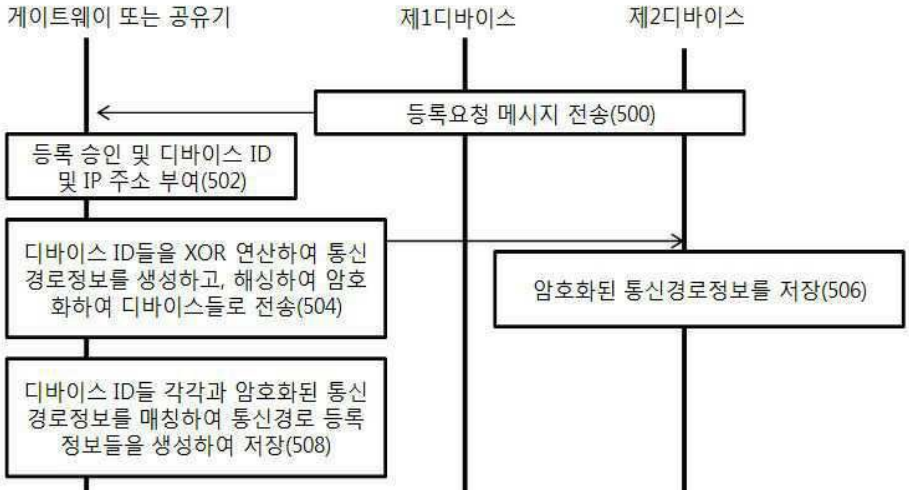
도면2



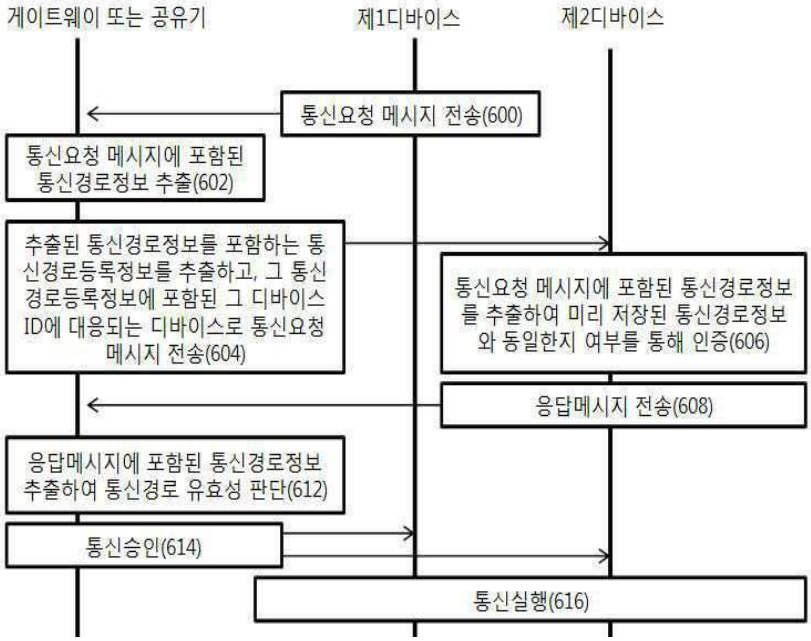
도면3



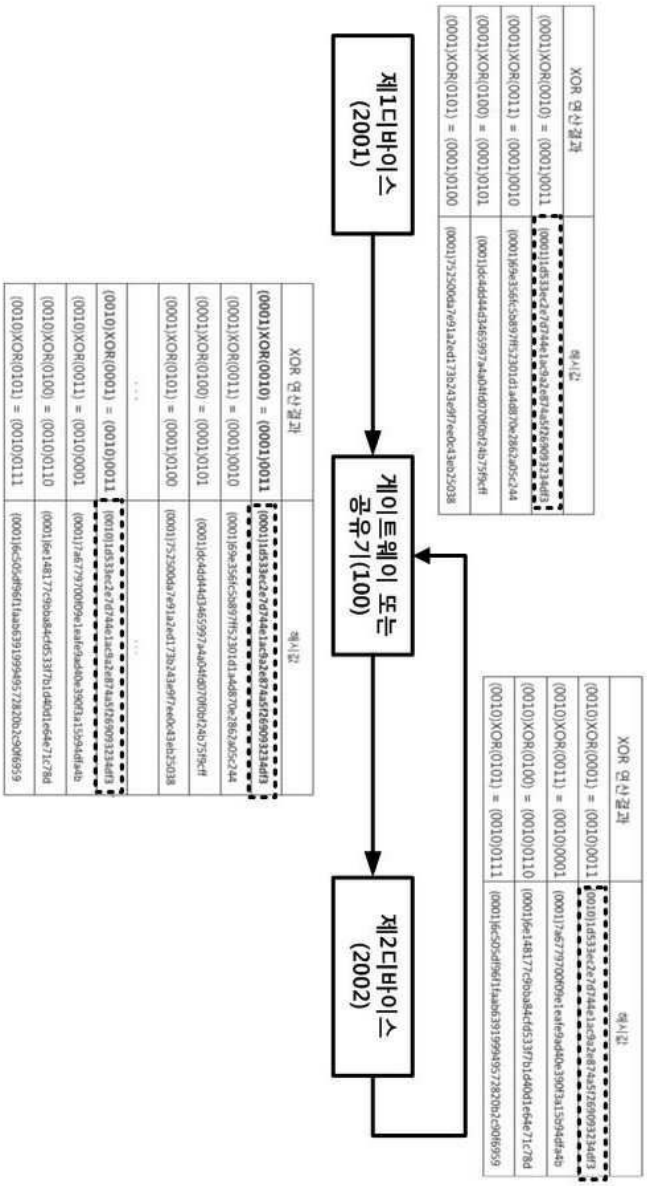
도면4


게이트웨이 또는 공유기
제1디바이스
제2디바이스
등록요청 메시지 전송(500)
등록 승인 및 디바이스 ID 및 IP 주소 부여(502)
디바이스 ID들을 XOR 연산하여 통신 경로정보를 생성하고, 해싱하여 암호화하여 디바이스들로 전송(504)
암호화된 통신경로정보를 저장(506)
디바이스 ID들 각각과 암호화된 통신 경로정보를 매칭하여 통신경로 등록 정보들을 생성하여 저장(508)

도면5


게이트웨이 또는 공유기
제1디바이스
제2디바이스
통신요청 메시지 전송(600)
통신요청 메시지에 포함된 통신경로정보 추출(602)
추출된 통신경로정보를 포함하는 통신경로등록정보를 추출하고, 그 통신경로등록정보에 포함된 그 디바이스 ID에 대응되는 디바이스로 통신요청 메시지 전송(604)
통신요청 메시지에 포함된 통신경로정보를 추출하여 미리 저장된 통신경로정보와 동일한지 여부를 통해 인증(606)
응답메시지 전송(608)
응답메시지에 포함된 통신경로정보 추출하여 통신경로 유효성 판단(612)
통신승인(614)
통신실행(616)

도면6


제1디바이스 (2001)
게이트웨이 또는 융유기(100)
제2디바이스 (2002)
XOR 연산결과
해시값
(0001)XOR(0010) = (0001)0011
(0001)XOR(0011) = (0001)0010
(0001)XOR(0100) = (0001)0101
(0001)XOR(0101) = (0001)0100
(0001)XOR(0010) = (0001)0011
(0001)XOR(0011) = (0001)0010
(0001)XOR(0100) = (0001)0101
(0001)XOR(0101) = (0001)0100
(0010)XOR(0001) = (0010)0011
(0010)XOR(0011) = (0010)0001
(0010)XOR(0100) = (0010)0110
(0010)XOR(0101) = (0010)0111
(0010)XOR(0001) = (0010)0011
(0010)XOR(0011) = (0010)0001
(0010)XOR(0100) = (0010)0110
(0010)XOR(0101) = (0010)0111