



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년01월04일
(11) 등록번호 10-1935373
(24) 등록일자 2018년12월28일

(51) 국제특허분류(Int. Cl.)
H04W 12/06 (2009.01) H04L 29/06 (2006.01)
H04W 12/08 (2009.01) H04W 64/00 (2009.01)
(52) CPC특허분류
H04W 12/06 (2013.01)
H04L 63/107 (2013.01)
(21) 출원번호 10-2017-0168591
(22) 출원일자 2017년12월08일
심사청구일자 2017년12월08일
(56) 선행기술조사문헌
JP2016140088 A*
KR1020110115805 A*
KR1020170014351 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
소재우
서울특별시 마포구 독막로28길 10, 101동 1204호
(신수동, 밤섬정남아너스빌)
정혜라
서울특별시 마포구 백범로 35, R관 709호
(74) 대리인
특허법인충현

전체 청구항 수 : 총 15 항

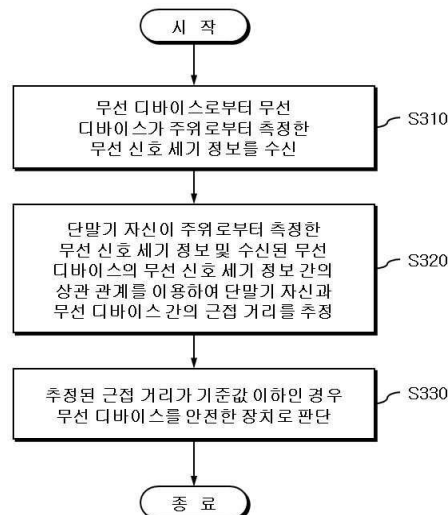
심사관 : 이준석

(54) 발명의 명칭 무선 신호 변동 기반의 단말기와 무선 디바이스 간의 인증 방법 및 장치

(57) 요약

본 발명은 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 기술에 관한 것으로, 단말기가 무선 디바이스로부터 무선 디바이스가 주위로부터 측정한 무선 신호 세기 정보를 수신하고, 단말기 자신이 주위로부터 측정한 무선 신호 세기 정보 및 수신된 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기 자신과 무선 디바이스 간의 근접 거리를 추정하며, 추정된 근접 거리가 미리 설정된 기준값 이하인 경우 무선 디바이스를 안전한 장치로 판단한다.

대표도 - 도3



(52) CPC특허분류

H04W 12/08 (2013.01)

H04W 64/00 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1D1A1B03934150

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원사업

연구과제명 5G/LPWA HetNet 환경에서 Massive 드론 서비스를 위한 무선 접속 기술 연구

기 여 율 1/1

주관기관 서강대학교 산학협력단

연구기간 2016.11.01 ~ 2019.10.31

명세서

청구범위

청구항 1

네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 방법에 있어서,

단말기가 무선 디바이스로부터 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신하는 단계;

상기 단말기가 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하되 상기 단말기 및 상기 무선 디바이스 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 단계; 및

추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 단말기가 상기 무선 디바이스를 안전한 장치로 판단하는 단계를 포함하는 인증 방법.

청구항 2

삭제

청구항 3

제 1 항에 있어서,

상기 단말기 및 상기 무선 디바이스는,

무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 무선 신호 세기를 측정하되, 무선 채널의 수 만큼 신호 측정을 반복하여 신호 세기의 집합을 구축하는 것을 특징으로 하는 인증 방법.

청구항 4

제 1 항에 있어서,

상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 단계는,

무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정된 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산출하는 단계; 및

상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간의 거리와 공분산 사이의 관계를 도출하는 단계를 포함하는 인증 방법.

청구항 5

제 1 항에 있어서,

안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하는 단계를 더 포함하는 인증 방법.

청구항 6

제 5 항에 있어서,

상기 단말기와 상기 무선 디바이스 간의 암호화 방식을 결정하는 단계를 더 포함하고,

상기 인증하는 단계는, 결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증하는 것을 특징으로 하는 인증 방법.

청구항 7

제 5 항에 있어서,

상기 인증하는 단계는,

안전한 장치로 판단된 상기 무선 디바이스로부터 수신된 공개키를 이용하여 상기 단말기가 세션키를 암호화하는 단계; 및

상기 단말기가 암호화된 상기 세션키를 상기 무선 디바이스에 전송하여 상기 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 상기 세션키를 추출하도록 유도하는 단계를 포함하는 인증 방법.

청구항 8

제 5 항에 있어서,

인증에 성공한 경우, 상기 단말기와 상호 무선 디바이스 간에 암호화된 세션 채널을 생성하고, 상기 단말기가 생성된 상기 암호화된 세션 채널을 통해 상기 무선 디바이스와 통신하는 단계를 더 포함하는 인증 방법.

청구항 9

제 1 항, 제 3 항 내지 제 8 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 10

네트워크를 통해 연결되는 무선 디바이스와 인증을 시도하는 단말기에 있어서,

무선 통신을 통해 무선 신호를 수신하는 통신부;

통신부를 통해 수신된 무선 신호에 기초하여 무선 디바이스가 안전한 장치인지 여부를 판단하는 프로그램을 저장하는 메모리; 및

상기 프로그램을 구동하여 무선 디바이스에 대한 인증을 처리하는 프로세서를 포함하되,

상기 메모리에 저장된 프로그램은,

상기 통신부를 통해 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신하고, 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하되 상기 단말기 및 상기 무선 디바이스 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하며, 추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 무선 디바이스를 안전한 장치로 판단하는 명령어를 포함하는 단말기.

청구항 11

삭제

청구항 12

제 10 항에 있어서,

상기 메모리에 저장된 프로그램은,

무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 상기 통신부를 통해 무선 신호 세기를 측정하되, 무선 채널의 수만큼 신호 측정을 반복하여 신호 세기의 집합을 구축하는 것을 특징으로 하는 단말기.

청구항 13

제 10 항에 있어서,

상기 메모리에 저장된 프로그램은,

무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정된 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산

출하고, 상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간의 거리와 공분산 사이의 관계를 도출함으로써, 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 것을 특징으로 하는 단말기.

청구항 14

제 10 항에 있어서,

상기 메모리에 저장된 프로그램은,

안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하는 명령어를 더 포함하는 단말기.

청구항 15

제 14 항에 있어서,

상기 메모리에 저장된 프로그램은,

상기 단말기와 상기 무선 디바이스 간의 암호화 방식을 결정하는 명령어를 더 포함하고,

결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증하는 것을 특징으로 하는 단말기.

청구항 16

제 14 항에 있어서,

상기 메모리에 저장된 프로그램은,

안전한 장치로 판단된 상기 무선 디바이스로부터 수신된 공개키를 이용하여 상기 단말기가 세션키를 암호화하고, 상기 단말기가 암호화된 상기 세션키를 상기 무선 디바이스에 전송하여 상기 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 상기 세션키를 추출하도록 유도하는 명령어를 포함하는 단말기.

청구항 17

제 14 항에 있어서,

상기 메모리에 저장된 프로그램은,

인증에 성공한 경우, 상기 단말기와 상호 무선 디바이스 간에 암호화된 세션 채널을 생성하고, 상기 단말기가 생성된 상기 암호화된 세션 채널을 통해 상기 무선 디바이스와 통신하는 명령어를 더 포함하는 단말기.

발명의 설명

기술 분야

[0001] 본 발명은 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 기술에 관한 것으로, 특히 무선 신호 변동을 이용하여 사물인터넷(Internet Of Things, IoT) 환경에서 IoT 디바이스를 인증하는 인증 방법 및 그 방법에 따른 단말기에 관한 것이다.

배경 기술

[0002] 사물 인터넷(Internet Of Things, IoT)이란, 인터넷을 기반으로 모든 사물을 연결하여 사람과 사물, 사물과 사물 간의 정보를 상호 소통하는 지능형 기술 및 서비스를 말한다. 사물 인터넷은 생활 속 사물들을 유무선 네트워크로 연결하여 가전제품, 전자기기, 헬스케어, 원격검침, 스마트홈, 스마트카 등 다양한 분야에서 이용될 수 있다. 이에 따라, 기존의 네트워크 인프라는 점차적으로 스마트 워크 환경에서 스마트 홈 네트워크 및 오피스 네트워크 플랫폼으로 발전하고 있다. 사물 인터넷 기반의 스마트 워크 환경으로의 진화는 다양한 서비스 도메인에서 디바이스 이동이 증가될 것이며, 스마트 워크 디바이스 간의 협업에 의한 새로운 서비스가 증가할 것이다.

[0003] 이러한 환경이 확산됨에 따라 IoT 디바이스들이 널리 설치되면서 IoT 디바이스 인증 문제가 중요한 이슈로 대두되고 있다. 사물 인터넷 기반의 스마트 워크 환경은 수많은 디바이스가 연결되고, 무선 네트워크 기반으로 동작하기 때문에, 다양한 보안 위협의 발생 가능성이 증가하며, 네트워크에 대한 불법적인 접근이 가능하다.

따라서, 디바이스에 대한 안전성 확인을 통해 스마트 워크 환경에서 비인가 디바이스의 서비스 이용을 차단하고, 정당한 디바이스만 접근 가능해야 한다. 즉, 다양한 보안 기술을 스마트 워크 환경에 적용하여, 정당한 디바이스를 통해서만 안전하고 효율적인 서비스를 제공받을 수 있게 하는 한 단계 강화된 보안의 필요성이 제기되고 있다.

- [0004] 기존의 디바이스 인증/인가 기술은 단일 도메인의 디바이스 간 상호인증을 위해 공인인증 기관을 통해 인증을 제공하거나, ID/PW를 이용하여 인증을 제공하는 등의 방식이 있다. 그러나 사물 인터넷 기반의 스마트 워크 환경과 같은 멀티 도메인 환경을 위해서, 추가적인 디바이스 인증/인가 기술의 개발이 필요하다. 또한, 기존의 디바이스 인증/인가 기술을 센서 디바이스에 응용하기에는 연산량 등의 문제가 발생할 수 있으며, 별도의 인증 서버를 활용한 KEY 혹은 인증서 확인 방식은 모든 사물이 연결되는 IoT 환경에는 적합하지 않다는 지적도 존재한다.

선행기술문헌

비특허문헌

- [0005] (비특허문헌 0001) Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," IEEE Internet of Things J., vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

발명의 내용

해결하려는 과제

- [0006] 본 발명이 해결하고자 하는 기술적 과제는, 종래의 IoT 디바이스 인증 기술들이 별도의 인증 서버를 요구하고 있다는 한계를 극복하고, 중간자(man in the middle attack, MITM) 공격을 비롯한 도청과 위장 공격에 취약하다는 약점을 해결하고자 한다.

과제의 해결 수단

- [0007] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 방법은, 단말기가 무선 디바이스로부터 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신하는 단계; 상기 단말기가 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 단계; 및 추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 단말기가 상기 무선 디바이스를 안전한 장치로 판단하는 단계를 포함한다.
- [0008] 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법에서, 상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 단계는, 상기 단말기 및 상기 무선 디바이스 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 근접 거리를 추정할 수 있다.
- [0009] 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법에서, 상기 단말기 및 상기 무선 디바이스는, 무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 무선 신호 세기를 측정하되, 무선 채널의 수만큼 신호 측정을 반복하여 신호 세기의 집합을 구축할 수 있다.
- [0010] 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법에서, 상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하는 단계는, 무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정된 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산출하는 단계; 및 상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간의 거리와 공분산 사이의 관계를 도출할 수 있다.
- [0011] 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법은, 안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하는 단계를 더 포함할 수 있다. 또한, 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법은, 상기 단말기와 상기 무선 디바이스 간의 암호화 방식을 결정하는 단계를 더 포함하고, 상기 인증하는 단계는, 결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증할 수 있다. 또한, 상기 인증하는 단계는, 안전한 장치로 판단된 상기 무선 디바이스로부터 수신된 공개키를 이

용하여 상기 단말기가 세션키를 암호화하는 단계; 및 상기 단말기가 암호화된 상기 세션키를 상기 무선 디바이스에 전송하여 상기 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 상기 세션키를 추출하도록 유도하는 단계를 포함할 수 있다. 나아가, 일 실시예에 따른 단말기와 무선 디바이스 간의 인증 방법은, 인증에 성공한 경우, 상기 단말기와 상호 무선 디바이스 간에 암호화된 세션 채널을 생성하고, 상기 단말기가 생성된 상기 암호화된 세션 채널을 통해 상기 무선 디바이스와 통신하는 단계를 더 포함할 수 있다.

[0012] 한편, 이하에서는 상기 기재된 단말기와 무선 디바이스 간의 인증 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[0013] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 무선 디바이스와 인증을 시도하는 단말기는, 무선 통신을 통해 무선 신호를 수신하는 통신부; 통신부를 통해 수신된 무선 신호에 기초하여 무선 디바이스가 안전한 장치인지 여부를 판단하는 프로그램을 저장하는 메모리; 및 상기 프로그램을 구동하여 무선 디바이스에 대한 인증을 처리하는 프로세서를 포함하되, 상기 메모리에 저장된 프로그램은, 상기 통신부를 통해 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신하고, 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하며, 추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 무선 디바이스를 안전한 장치로 판단하는 명령어를 포함한다.

[0014] 일 실시예에 따른 무선 디바이스와 인증을 시도하는 단말기에서 상기 메모리에 저장된 프로그램은, 상기 단말기 및 상기 무선 디바이스 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정할 수 있다.

[0015] 일 실시예에 따른 무선 디바이스와 인증을 시도하는 단말기에서 상기 메모리에 저장된 프로그램은, 무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 상기 통신부를 통해 무선 신호 세기를 측정하되, 무선 채널의 수만큼 신호 측정을 반복하여 신호 세기의 집합을 구축할 수 있다.

[0016] 일 실시예에 따른 무선 디바이스와 인증을 시도하는 단말기에서 상기 메모리에 저장된 프로그램은, 무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정한 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산출하고, 상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간의 거리와 공분산 사이의 관계를 도출함으로써, 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정할 수 있다.

[0017] 일 실시예에 따른 무선 디바이스와 인증을 시도하는 단말기에서 상기 메모리에 저장된 프로그램은, 안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하는 명령어를 더 포함할 수 있다. 또한, 상기 메모리에 저장된 프로그램은, 상기 단말기와 상기 무선 디바이스 간의 암호화 방식을 결정하는 명령어를 더 포함하고, 결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증할 수 있다. 또한, 상기 메모리에 저장된 프로그램은, 안전한 장치로 판단된 상기 무선 디바이스로부터 수신된 공개키를 이용하여 상기 단말기가 세션키를 암호화하고, 상기 단말기가 암호화된 상기 세션키를 상기 무선 디바이스에 전송하여 상기 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 상기 세션키를 추출하도록 유도하는 명령어를 포함할 수 있다. 나아가, 상기 메모리에 저장된 프로그램은, 인증에 성공한 경우, 상기 단말기와 상호 무선 디바이스 간에 암호화된 세션 채널을 생성하고, 상기 단말기가 생성된 상기 암호화된 세션 채널을 통해 상기 무선 디바이스와 통신하는 명령어를 더 포함할 수 있다.

발명의 효과

[0018] 본 발명의 실시예들은, 단말기 주위로부터 측정된 무선 신호 세기 정보 및 무선 디바이스의 주위로부터 측정된 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기와 무선 디바이스 간의 근접 거리를 추정함으로써, 별도의 인증 서버 없이도 안전한 무선 디바이스를 검증할 수 있으며, 암호화된 세션 채널을 사용하여 무선 통신이 이루어지므로 중간자 공격을 비롯한 도청과 위장 공격에 강인하다는 장점을 갖는다.

도면의 간단한 설명

[0019] 도 1은 IoT 환경에서 Wi-Fi 비밀번호 스니핑(sniffing)이 발생하는 사례를 설명하기 위한 도면이다.

도 2는 본 발명의 실시예들이 제안하는 무선 신호 세기 측정을 이용한 디바이스 거리 추정 방법을 설명하기 위

한 도면이다.

도 3은 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 방법을 도시한 흐름도이다.

도 4는 본 발명의 실시예들이 제안하는 무선 신호 세기 측정 방식을 도시한 흐름도이다.

도 5는 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 과정을 각각의 주체를 중심으로 도시한 도면이다.

도 6은 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 무선 디바이스와 인증을 시도하는 단말기를 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 본 발명의 실시예들을 설명하기에 앞서, IoT 환경과 이러한 환경에서 IoT 디바이스를 인증하는 기술에 도입 가능한 다양한 방법론들을 살펴본 후, 각각의 개별 방법론들을 통해 예상되는 문제점들을 해결하기 위해 본 발명의 실시예들이 채택하고 있는 아이디어와 기술적 수단을 순차적으로 소개하도록 한다.
- [0021] IoT 디바이스를 인증함에 있어서, 게이트웨이와 컨트롤러를 이용하여 비대칭키 기반으로 IoT 디바이스를 인증하는 기법이나, IoT-OAuth 기반의 인증 기법이 고려될 수 있다. 그러나 이러한 기법들은 홈 Wi-Fi 환경에서 별도의 입력장치가 없는 IoT 디바이스를 인증하는데 어려운 점이 있다. 홈 Wi-Fi 환경에서 액세스 포인트(access point, AP)는 무선 클라이언트들과 Wi-Fi 접속 비밀번호를 공유하는 PSK(pre-shared key) 환경에 놓여지게 된다. 홈 Wi-Fi 환경에서 IoT 디바이스를 설치할 때, 많은 업체들은 스마트폰을 이용하여 Wi-Fi 비밀번호를 별도의 입력 장치를 가지고 있지 않은 IoT 디바이스에 전송한다. 따라서 공격자는 스마트폰과 IoT 디바이스간 트래픽을 스니핑하거나 IoT 디바이스로 위장하여 Wi-Fi 비밀번호를 알아낼 수 있다는 심각한 위험이 존재한다.
- [0022] IoT 디바이스의 안전성을 담보하기 위해, Wi-Fi 신호 세기를 이용하여 단말의 거리를 추정하는 기법이 고려될 수 있으나, Wi-Fi 신호 세기는 페이딩이 심하여 Wi-Fi 신호 세기만으로는 거리를 추정하기 어렵다는 점이 약점으로 지적된다. 또한 공격자가 가짜 IoT 디바이스로 동작하는 Wi-Fi 액세스 장치의 Wi-Fi 신호 세기를 조정하는 경우 거리를 추정할 수 없게 되는 문제점이 있다.
- [0023] 도 1은 IoT 환경에서 Wi-Fi 비밀번호 스니핑(sniffing)이 발생하는 사례를 설명하기 위한 도면이다. 앞서, 홈 Wi-Fi 환경에 설치되는 스마트 전원 스위치, 전등 스위치 등과 같은 IoT 디바이스는 별도의 입력 장치가 없어 홈 Wi-Fi AP에 접속하기 위해 스마트폰으로부터 비밀번호를 전송받아야 함을 설명하였다. 예를 들어, 벨킨에서 판매하는 위모(Wemo) 스마트 전원 스위치를 고려할 수 있다.
- [0024] S110 단계에서 위모 IoT 디바이스(20)는 전원이 인가되었을 때 Wi-Fi AP로 동작하며, 스마트폰(10)은 IoT 디바이스(20)에 접속한다. S120 단계에서 위모 IoT 디바이스(20)는 디바이스 ID와 MAC 주소를 스마트폰(10)에 전송한다. 이어서, S130 단계에서 스마트폰(10)은 디바이스 ID와 MAC 주소를 사용하여 Wi-Fi 비밀번호를 암호화하여 IoT 디바이스(20)에 전송한다. 그러나 IoT 디바이스 ID와 MAC 주소는 쉽게 노출되는 정보이며, 공격자(50)는 다른 IoT 디바이스의 펌웨어를 해킹하여 암호화 방식을 찾을 수 있다. 따라서 공격자(50)는 도청과 위장 공격을 통해 Wi-Fi 비밀번호를 획득할 수 있다.
- [0025] 따라서, 상기된 문제점들을 해결하기 위해서 안출된 본 발명의 실시예들은, Wi-Fi를 사용하는 홈 IoT(Internet of Things) 환경에서 별도의 인증 서버가 없으면서 디바이스를 움직일 필요 없이 중간자(man in the middle attack, MITM) 공격을 비롯한 다양한 도청과 위장 공격에 강인한 IoT 디바이스 인증 기법을 제안하고자 한다. 특히, 본 발명의 실시예들은 Wi-Fi 수신 세기의 상관 관계를 기반으로 스마트폰이 IoT 디바이스의 위치를 추정하고, 이를 기반으로 공격자 여부를 판단한 후 암호화된 채널을 통해 Wi-Fi 비밀번호를 전송하는 새로운 IoT 인증 기법을 제안한다.
- [0026] 이를 위해, 본 발명의 실시예들이 제안하는 스마트폰과 IoT 디바이스는 주변 Wi-Fi 신호 세기를 모니터링한다. 스마트폰은 스마트폰이 수신하는 Wi-Fi 신호 세기들과 IoT 디바이스가 수신하는 신호 세기들 간의 공분산을 기반으로 근접 거리를 판단한 후, 그 판단 결과에 따라 인증을 처리함으로써 공격자의 도청과 IoT 디바이스 위장 공격을 효율적으로 방어할 수 있다.
- [0027] 이하에서는 도면을 참조하여 본 발명의 실시예들을 구체적으로 설명하도록 한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 덧붙여, 명세서

전체에서, 어떤 구성 요소를 '포함'한다는 것은, 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라, 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0028] 본 발명에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "구비하다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0029] 특별히 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0030] 도 2는 본 발명의 실시예들이 제안하는 무선 신호 세기 측정을 이용한 디바이스 거리 추정 방법을 설명하기 위한 도면이다. 본 발명의 실시예들은 Wi-Fi 접속 비밀번호를 공유하는 홈 Wi-Fi 환경에서 별도의 입력장치가 없는 IoT 디바이스(20)를 설치하는 경우를 고려한다. 스마트폰(10)은 Wi-Fi 비밀번호를 IoT 디바이스(20)에 전송하여 IoT 디바이스(20)가 홈 Wi-Fi AP에 접속할 수 있도록 하여야 한다. 공격자는 무선 스니핑과 IoT 디바이스로 위장하여 Wi-Fi 비밀번호를 알아내려고 한다. 이하에서 스마트폰(10)은 단말기의 일례로 제시되었으며, IoT 디바이스(20)는 다양한 무선 디바이스의 일례로서 제시되었으며, 단말기 및 무선 디바이스 각각이 이러한 예시에 한정되지 않음은 당연하다.

[0031] 무선 채널에서 지역 확산, 쉐도우 페이딩 등의 채널 파라미터들은 공간적으로 상관 관계가 있다. Wi-Fi 채널 n 에서 AP m 으로부터 수신하는 신호의 세기를 $h_{m,n}$ 이라 하고, $h_{m,n}$ 의 평균과 분산을 각각 $\mu_{m,n}$ 와 $\sigma_{m,n}$ 로 표현하자. 그러면 다음의 수학적 식 1과 같이 변환된 신호 세기 $x_{m,n}$ 는 평균이 0이고 분산이 1인 정규분포 $N(0, 1)$ 을 따른다.

수학적 식 1

$$x_{m,n} = \frac{h_{m,n}}{10\sigma_{m,n}} - \frac{\mu_{m,n}}{\sigma_{m,n}}$$

[0032]

[0033] 여기서, $h_{m,n}$ 의 단위는 데시벨이다. AP는 동작 중에 Wi-Fi 무선 채널을 변경하지 않으므로 첨자 n 은 생략하여 사용한다.

[0034] 도 2와 같이 스마트폰(10) 및 IoT 디바이스(20) 주변에 여러 개의 Wi-Fi AP들이 존재할 수 있다. 스마트폰(10)과 IoT 디바이스(20)는 N 개의 무선랜 채널들에 대해 변환된 신호 세기들의 집합 (X_{phone} 과 Y_{device})을 각각 구축한다.

수학적 식 2

$$X_{\text{phone}} = \{x_1, x_2, \dots, x_{M_1}\}$$

[0035]

수학적 식 3

$$Y_{\text{device}} = \{y_1, y_2, \dots, y_{M_2}\}$$

[0036]

[0037] 여기서, M_1 은 스마트폰이 관측한 AP들의 개수이고, M_2 는 IoT 디바이스가 관측한 AP들의 개수이다.

[0038] AP m의 무선 채널에서 스마트폰이 수집한 신호 세기들을 x_m 이라 하고, IoT 디바이스가 수집한 신호 세기들을 y_m 이라 하자. 그러면 스마트폰과 IoT 디바이스 간의 거리 d와 (x_m, y_m) 의 공분산 사이의 관계는 다음의 수학적 4와 같다.

수학적 4

$$\rho_m = E(x_m y_m) = \exp\left(-\frac{d}{d_{ref}}\right)$$

[0039]

[0040] 여기서 d_{ref} 는 무선 채널 환경에 따라 결정되는 상수이다. 수학적 4로부터 스마트폰(10)과 IoT 디바이스(20) 간의 거리는 다음의 수학적 5와 같이 추정할 수 있다.

수학적 5

$$\tilde{d} = \frac{1}{M} \sum_{m=1}^M \ln \rho_m^{-d_{ref}}$$

[0041]

[0042] 수학적 5의 거리가 사전에 정의된 δ 보다 작으면 스마트폰(10)은 IoT 디바이스(20)가 근접 거리에 있다고 판단하고, 그렇지 않으면 IoT 디바이스(20)가 근접 거리에 없다고 판단한다.

[0043] 도 3은 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 단말기와 무선 디바이스 간의 인증 방법을 도시한 흐름도이다.

[0044] S310 단계에서, 단말기는 무선 디바이스로부터 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신한다.

[0045] S320 단계에서, 상기 단말기는 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정한다. 이를 위해, 상기 단말기 및 상기 무선 디바이스 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정한다.

[0046] 보다 구체적으로, 이 과정에서는, 무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정된 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산출하고, 상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간의 거리와 공분산 사이의 관계를 도출할 수 있다.

[0047] S330 단계에서, S320 단계를 통해 추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 단말기가 상기 무선 디바이스를 안전한 장치로 판단한다. 판단 결과, 안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증할 수 있다.

[0048] 도 4는 본 발명의 실시예들이 제안하는 무선 신호 세기 측정 방식을 도시한 흐름도이다.

[0049] S410 단계에서는 복수 개의 무선 채널 n을 설정한다. 단말기 및 무선 디바이스는, S420 단계를 통해 무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 무선 신호 세기를 측정한다. 구현의 관점에서, 단말기 및 무선 디바이스는 일정한 시간 간격 T 동안 주위로부터 수신되는 비컨 프레임(beacon frame)을 관찰할 수 있다. S430 단계에서는, 무선 채널 n에서 AP m으로부터 $X_{m,n}$ 을 구축하고, S440 단계 및 S450 단계를 통해 무선 채널의 수만큼 신호 측정 및 데이터 수집 과정(S420, S430)을 반복하여 신호 세기의 집합을 구축할 수 있다.

[0050] 도 5는 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 단말기(10)와 무선 디바이스(20) 간의 인증 과정을 각각의 주체를 중심으로 도시한 도면으로서, 제안하는 IoT 디바이스 인증 프로토콜 과정은 MITM 공격을 피하

기 위한 보안 처리 과정으로서 도출되었다.

- [0051] 본 발명의 실시예들은, 안전한 장치로 판단된 무선 디바이스를 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하게 된다. 이를 위해, 인증에 앞서, 상기 단말기와 상기 무선 디바이스 간의 암호화 방식을 결정하는 것이 바람직하며, 인증 과정에서는, 결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증할 수 있다.
- [0052] S510 단계(Wi-Fi 접속)에서, IoT 디바이스(20)는 전원이 인가되었을 때 Wi-Fi AP로 동작하면서 주변 Wi-Fi 신호를 측정하여 변환된 신호 세기들의 집합 Y_{device} 를 구축한다. 스마트폰(10)은, 예를 들어 별도의 IoT 디바이스 설정 앱을 실행할 때, 주변 Wi-Fi 신호를 측정하여 변환된 신호 세기들의 집합 X_{phone} 를 구축한다. 이와 더불어 스마트폰(10)은 Wi-Fi AP로 동작하는 IoT 디바이스(20)에 접속한다.
- [0053] S520 단계(스마트폰 "Hello")에서, 스마트폰(10)은 IoT 디바이스(20)에게 '암호화 방식'을 전송한다.
- [0054] S530 단계(IoT 디바이스 "Hello")에서, IoT 디바이스(20)는 스마트폰(10)에게 선호하는 암호화 방식, 측정된 신호 세기 집합 Y_{device} 및 랜덤하게 생성한 공개키를 전달한다.
- [0055] S540 단계(근접 거리 판단)에서, 스마트폰(10)은 수학적 5를 사용하여 계산된 추정 거리 $\tilde{d}$ 를 사용하여 IoT 디바이스(20)가 근접 거리에 있는지 판단한다. 이 과정에서는 (X_{phone}, Y_{device}) 에 기초하여 IoT 디바이스(20)의 근접 정도를 검사할 수 있다. 만약 IoT 디바이스(20)가 근접 거리에 있다고 판단하면 S550 단계로 진행하여 인증 과정을 처리하고, 그렇지 않으면 인증 과정을 종료한다.
- [0056] S550 단계(키 교환)에서, 스마트폰(10)은 S530 단계에서 수신한 공개키를 사용하여 암호화된 세션키(session key)를 IoT 디바이스(20)에 전달한다. IoT 디바이스(20)는 개인키를 사용하여 수신한 데이터를 복호화하여 세션키를 추출한다. 즉, 안전한 장치로 판단된 무선 디바이스로부터 수신된 공개키를 이용하여 단말기가 세션키를 암호화하고, 단말기가 암호화된 세션키를 무선 디바이스에 전송하여 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 세션키를 추출하도록 유도할 수 있다.
- [0057] S560 단계(Wi-Fi 비밀번호 전송)에서, 인증 성공에 따라 스마트폰(10)과 IoT 디바이스(20) 간에 암호화된 세션 채널을 생성하고, 스마트폰(10)은 암호화된 세션 채널을 사용하여 Wi-Fi 접속 비밀번호를 IoT 디바이스(20)에 전송한다.
- [0058] 도 6은 본 발명의 일 실시예에 따른 네트워크를 통해 연결되는 무선 디바이스(10)와 인증을 시도하는 단말기(20)를 도시한 블록도로서, 도 3을 통해 기술된 일련의 방법을 하드웨어 구현의 관점에서 재구성한 것이다. 따라서, 여기서는 설명의 중복을 피하고자 각 구성의 기능을 약술하도록 한다.
- [0059] 통신부(21)는, 무선 통신을 통해 무선 신호를 수신하는 구성이다.
- [0060] 메모리(23)는 통신부(21)를 통해 수신된 무선 신호에 기초하여 무선 디바이스가 안전한 장치인지 여부를 판단하는 프로그램을 저장하는 구성이며, 프로세서(25)는 메모리(23)에 저장된 상기 프로그램을 구동하여 무선 디바이스(10)에 대한 인증을 처리하는 구성이다.
- [0061] 여기서, 메모리(23)에 저장된 프로그램은, 상기 통신부(21)를 통해 상기 무선 디바이스가 주위로부터 측정된 무선 신호 세기 정보를 수신하고, 단말기 자신이 주위로부터 측정된 무선 신호 세기 정보 및 수신된 상기 무선 디바이스의 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정하며, 추정된 상기 근접 거리가 미리 설정된 기준값 이하인 경우, 상기 무선 디바이스를 안전한 장치로 판단하는 명령어를 포함한다. 특히, 상기 메모리(23)에 저장된 프로그램은, 상기 단말기(20) 및 상기 무선 디바이스(10) 주위의 무선 네트워크 식별자를 기준으로 각각의 근접 거리를 측정하여 이를 합산한 후 평균을 산출한 값을 기준으로 상기 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정할 수 있다.
- [0062] 구현의 관점에서, 상기 메모리(23)에 저장된 프로그램은, 무선 채널 별로 주위에 위치한 복수 개의 AP(access point)로부터 상기 통신부를 통해 무선 신호 세기를 측정하되, 무선 채널의 수만큼 신호 측정을 반복하여 신호 세기의 집합을 구축할 수 있다. 보다 구체적으로, 상기 메모리(23)에 저장된 프로그램은, 무선 채널에서 공간적인 상관 관계가 있는 채널 파라미터(parameter)를 이용하여 상기 단말기 또는 상기 무선 디바이스 자신이 각각 측정된 신호의 세기의 평균 및 분산으로부터 무선 채널에 대한 신호 세기의 변환값을 산출하고, 상기 단말기의 신호 세기의 변환값과 상기 무선 디바이스의 신호 세기의 변환값으로부터 상기 단말기와 상기 무선 디바이스 간

의 거리와 공분산 사이의 관계를 도출함으로써, 단말기 자신과 상기 무선 디바이스 간의 근접 거리를 추정할 수 있다.

[0063] 상기 메모리(23)에 저장된 프로그램은, 안전한 장치로 판단된 상기 무선 디바이스를 상기 단말기가 상호 간의 공개키 암호화 방식을 사용하여 인증하는 명령어를 더 포함할 수 있다. 이를 위해, 상기 메모리(23)에 저장된 프로그램은, 상기 단말기(10)와 상기 무선 디바이스(20) 간의 암호화 방식을 결정하는 명령어를 더 포함하고, 결정된 상기 암호화 방식에 따라 별도의 인증 서버 없이 상호 인증할 수 있다.

[0064] 또한, 상기 메모리(23)에 저장된 프로그램은, 안전한 장치로 판단된 상기 무선 디바이스로부터 수신된 공개키를 이용하여 상기 단말기가 세션키를 암호화하고, 상기 단말기가 암호화된 상기 세션키를 상기 무선 디바이스에 전송하여 상기 무선 디바이스가 보유하고 있는 개인키를 이용하여 복호화함으로써 상기 세션키를 추출하도록 유도하는 명령어를 포함할 수 있다. 나아가, 상기 메모리(23)에 저장된 프로그램은, 인증에 성공한 경우, 상기 단말기와 상호 무선 디바이스 간에 암호화된 세션 채널을 생성하고, 상기 단말기가 생성된 상기 암호화된 세션 채널을 통해 상기 무선 디바이스와 통신하는 명령어를 더 포함할 수 있다.

[0065] 상기된 본 발명의 실시예들에 따르면, 단말기 주위로부터 측정된 무선 신호 세기 정보 및 무선 디바이스의 주위로부터 측정된 무선 신호 세기 정보 간의 상관 관계를 이용하여 단말기와 무선 디바이스 간의 근접 거리를 추정함으로써, 별도의 인증 서버 없이도 안전한 무선 디바이스를 검증할 수 있으며, 암호화된 세션 채널을 사용하여 무선 통신이 이루어지므로 중간자 공격을 비롯한 도청과 위장 공격에 강인하다. 즉, 무선 도청에 관하여, 공개키/세션키가 공개되지 않는 이상 암호화된 세션 채널을 사용하여 전송하는 Wi-Fi 접속 비밀번호를 엿들을 수 없다.

[0066] 한편, IoT 디바이스 위장에 관하여, 스마트폰과 IoT 디바이스 간의 통신에서 만약 공격자가 IoT 디바이스와 동일한 SSID와 MAC를 사용하고, 높은 전송 전력을 사용하는 AP로 동작할 경우 스마트폰은 공격자의 AP에 Wi-Fi 접속하게 된다, 따라서 종래의 인증/보안 기법에서는 공격자의 위장 공격에 취약하여 스마트폰이 Wi-Fi 비밀번호를 공격자에게 전송할 수 있는 문제가 존재하였으나, 본 발명의 실시예들이 제안하는 인증 기법에서는 근접 거리를 판단하여 IoT 디바이스를 검증하므로 공격자의 위장 공격을 효과적으로 방어할 수 있다.

[0067] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0068] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0069] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0070] 10: 무선 디바이스 (IoT 디바이스)

20: 단말기 (스마트폰)

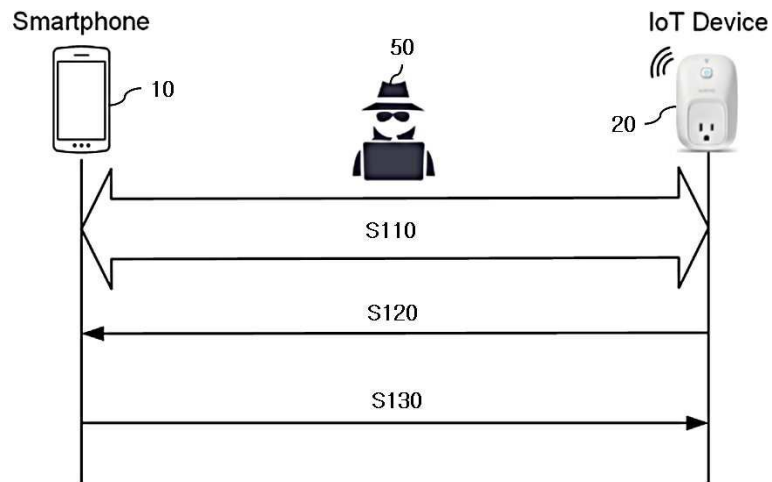
21: 통신부

23: 메모리

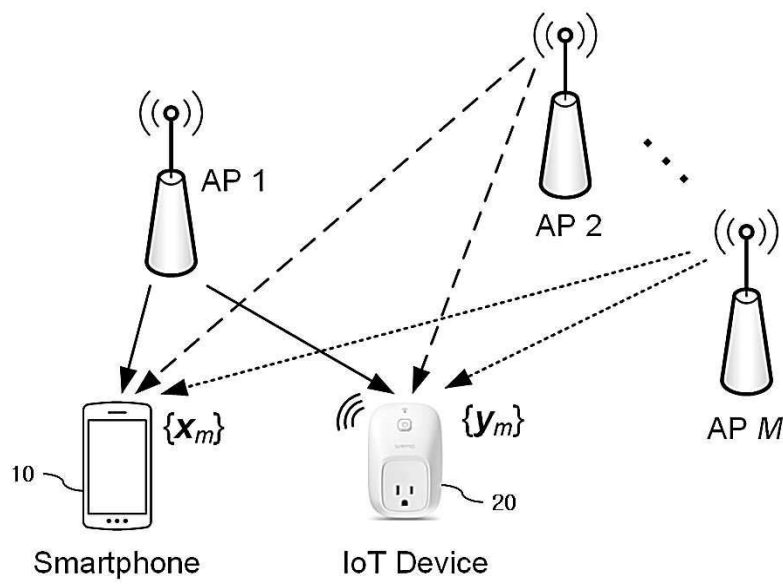
25: 프로세서

도면

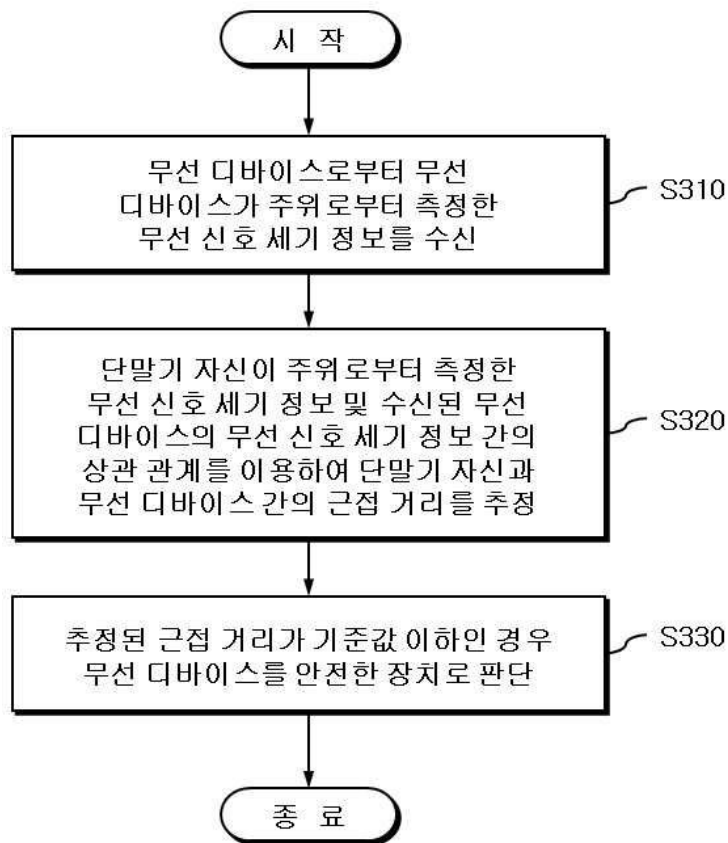
도면1



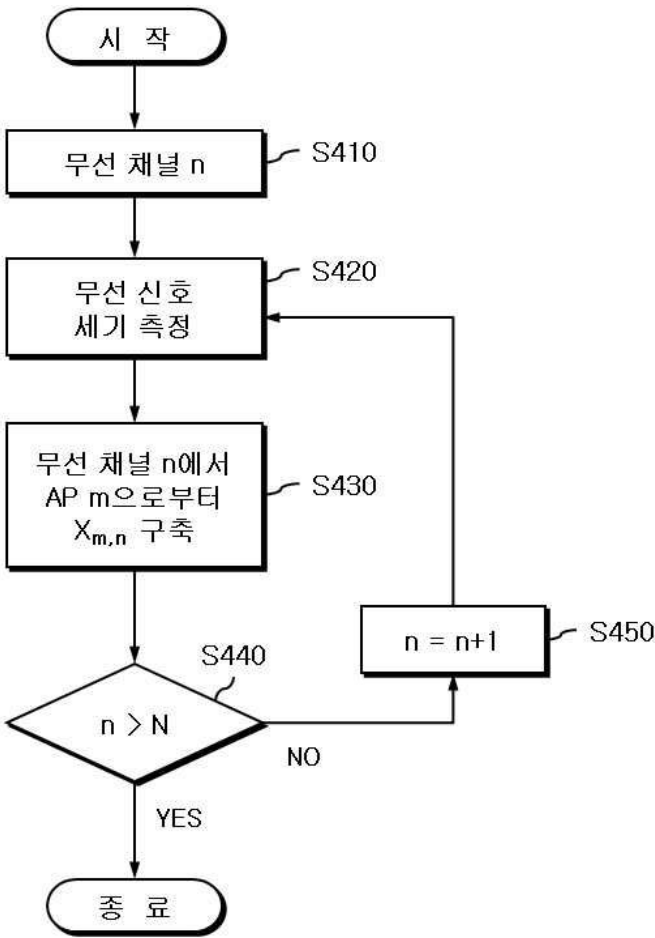
도면2



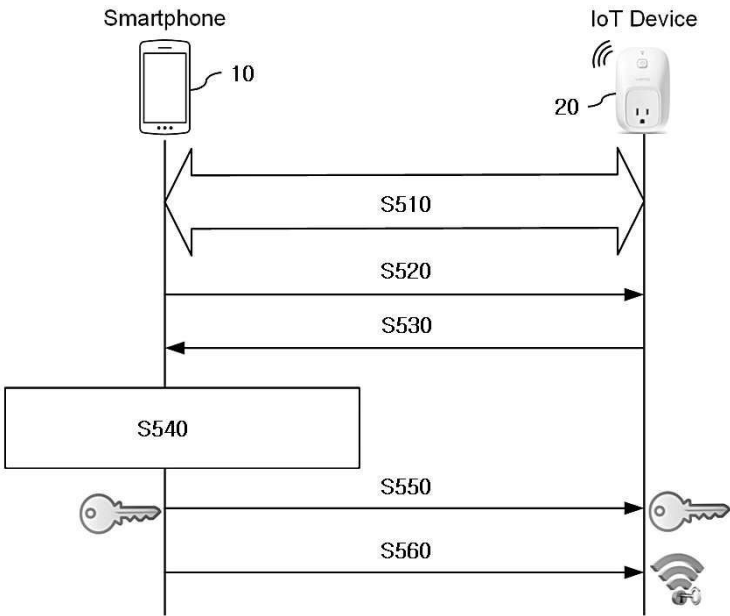
도면3



도면4



도면5



도면6

