(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년12월17일
(11) 등록번호 10-0874015
(24) 등록일자 2008년12월08일

(51) Int. Cl.
H04L 12/22 (2006.01) *H04L 12/28* (2006.01)
H04L 12/24 (2006.01)
(21) 출원번호 10-2007-0056830
(22) 출원일자 2007년06월11일
심사청구일자 2007년06월11일
(56) 선행기술조사문헌
KR1020060070309 A*
(뒷면에 계속)

(73) 특허권자
스콥정보통신 주식회사

(72) 발명자
정현철

이희조

(74) 대리인
유미특허법인

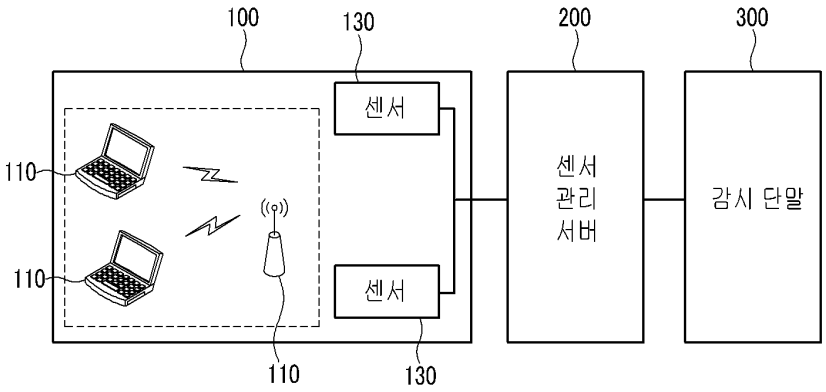
전체 청구항 수 : 총 10 항 심사관 : 양찬호

(54) 무선랜 침입 방지 시스템 및 방법

(57) 요 약

무선랜 침입 방지 시스템은 보안영역 내에 설치된 복수의 센서로부터 무선랜 기기에 대한 복수의 무선랜 감시 정보를 수신하고, 복수의 무선랜 감시 정보를 바탕으로 무선랜 기기가 악성 무선랜 기기인지를 판단한다. 무선랜 기기가 악성 무선랜 기기인 경우, 복수의 무선랜 감시 정보를 바탕으로 악성 무선랜 기기의 위치 정보를 생성하고, 악성 무선랜 기기에 대한 통신 차단 메시지를 생성한다. 이후 복수의 센서로 통신 차단 메시지를 전송하여 통신 차단 메시지에 따라 악성 무선랜 기기가 통신을 중단하도록 한다. 이를 통해 무선랜 침입 방지 시스템은 보안영역 내의 정보가 무선랜을 통해 외부로 정보가 유출되는 것을 방지한다.

대 표 도 - 도1



(56) 선행기술조사문헌
KR1020060132701 A*
KR1020050052462 A
JP2007028268 A
KR1020030005761 A
JP2005341062 A
KR1020060011000 A
*는 심사관에 의하여 인용된 문헌

특허청구의 범위

청구항 1

복수의 센서를 통해 하나의 무선랜 기기를 감시하여 무선랜 침입을 방지하는 방법에 있어서,

상기 복수의 센서에 각각 대응하는 복수의 무선랜 감시 정보 및 상기 복수의 센서에 각각 대응하는 복수의 신호 강도 정보를 수신하는 단계;

상기 복수의 무선랜 감시 정보를 바탕으로 상기 무선랜 기기가 악성 무선랜 기기인지를 판단하는 단계;

상기 무선랜 기기가 악성 무선랜 기기인 경우, 상기 복수의 신호 강도 정보를 바탕으로 상기 악성 무선랜 기기의 위치 정보를 생성하는 단계;

상기 위치 정보를 바탕으로 상기 악성 무선랜 기기에 대한 통신 차단 메시지를 생성하는 단계; 및

상기 복수의 센서 중 어느 하나의 센서로 상기 통신 차단 메시지를 전송하여 상기 통신 차단 메시지에 따라 상기 악성 무선랜 기기가 통신을 중단하도록 하는 단계를 포함하는 무선랜 침입 방지 방법.

청구항 2

제1항에 있어서,

상기 복수의 센서의 각각의 위치 정보는 미리 정해지고,

상기 위치 정보를 생성하는 단계는

상기 복수의 신호 강도 정보를 바탕으로 상기 복수의 센서에 각각 대응하는 복수의 거리 정보를 생성하는 단계; 및

상기 복수의 센서의 각각의 위치 정보 및 상기 복수의 거리 정보를 바탕으로 상기 위치 정보를 생성하는 단계를 포함하는 무선랜 침입 방지 방법.

청구항 3

제1항에 있어서,

상기 통신 차단 메시지를 전송하는 단계는

상기 위치 정보를 바탕으로 상기 복수의 센서 중 상기 악성 무선랜 기기와 가장 가까운 센서로 상기 통신 차단 메시지를 전송하는 단계를 포함하는 무선랜 침입 방지 방법.

청구항 4

복수의 센서로부터 상기 복수의 무선랜 기기에 각각 대응하는 복수의 무선랜 감시 정보를 수신하는 단계;

상기 복수의 무선랜 감시 정보를 바탕으로 상기 복수의 무선랜 기기 중 악성 무선랜 기기를 검출하는 단계;

상기 악성 무선랜 기기에 대응하는 통신 차단 메시지를 생성하는 단계; 및

상기 복수의 센서 중 일부의 센서로 상기 통신 차단 메시지를 전송하여 상기 일부의 센서가 상기 통신 차단 메시지를 상기 복수의 무선랜 기기로 전송하도록 하는 단계를 포함하고,

상기 검출하는 단계는

상기 복수의 무선랜 기기 중 허용된 인증 방법 리스트 또는 허용된 암호화 방법 리스트에 포함된 인증 방법 또는 암호화 방법을 사용하지 않는 무선랜 기기를 상기 악성 무선랜 기기로 결정하는 단계를 포함하는 무선랜 침입 방지 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

제4항에 있어서,

상기 검출하는 단계는

상기 복수의 무선랜 기기 중 허용된 통신 프로토콜 리스트에 포함된 통신 프로토콜을 사용하지 않는 무선랜 기기를 상기 악성 무선랜 기기로 결정하는 단계를 더 포함하는 무선랜 침입 방지 방법.

청구항 9

제4항에 있어서,

상기 검출하는 단계는

상기 복수의 무선랜 기기 중 허용된 기기 리스트에 포함되지 않는 무선랜 기기와 통신하는 무선랜 기기를 상기 악성 무선랜 기기로 결정하는 단계를 더 포함하는 무선랜 침입 방지 방법.

청구항 10

무선랜 기기를 감시하여 무선랜 침입을 방지하는 시스템에 있어서,

상기 무선랜 기기가 전송하는 패킷을 수집하고, 상기 패킷을 바탕으로 복수의 무선랜 감시 정보 및 복수의 신호 강도 정보를 생성하는 복수의 센서; 및

상기 복수의 무선랜 감시 정보를 바탕으로 상기 무선랜 기기가 악성 무선랜 기기인지를 판단하고, 상기 무선랜 기기가 상기 악성 무선랜 기기인 경우 상기 복수의 신호 강도 정보를 바탕으로 상기 악성 무선랜 기기의 위치 정보를 생성하는 센서 관리 서버를 포함하는 무선랜 침입 방지 시스템.

청구항 11

제10항에 있어서,

상기 센서 관리 서버는

상기 복수의 무선랜 감시 정보를 바탕으로 상기 무선랜 기기가 미리 정해진 보안 수준을 침해하는 악성 무선랜 기기인지를 판단하는 악성 무선랜 기기 검출부; 및

상가 무선랜 기기가 상기 악성 무선랜 기기인 경우, 상기 복수의 신호 강도 정보에 각각 대응하는 복수의 거리 정보 및 미리 정해진 상기 복수의 센서의 각각의 위치 정보에 따라 상기 악성 무선랜 기기의 위치 정보를 생성하는 위치 정보 생성부를 포함하는 무선랜 침입 방지 시스템.

청구항 12

제11항에 있어서,

상기 센서 관리 서버는

상기 악성 무선랜 기기의 위치 정보를 바탕으로 상기 악성 무선랜 기기에 대응하는 무선랜 침입 정보를 생성하는 무선랜 침입 정보 생성부를 더 포함하는 무선랜 침입 방지 시스템.

청구항 13

제12항에 있어서,

상기 센서 관리 서버는 상기 무선랜 침입 정보에 대응하는 통신 차단 메시지를 상기 복수의 센서 중 어느 하나의 센서로 전송하고,

상기 센서는 상기 통신 차단 메시지에 따라 상기 악성 무선랜 기기의 통신을 차단하는 무선랜 침입 방지 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<7> 본 발명은 무선랜 침입 방지 시스템에 관한 것이다. 특히 본 발명은 보안 영역 내의 무선랜 시스템에 대한 불법 행위를 감지하여 차단하는 무선랜 침입 방지 시스템에 관한 것이다.

<8> 무선랜 시스템은 무선랜 액세스 포인트(Wireless LAN Access Point, AP)와 무선랜 단말을 포함한다. 이때 무선랜 시스템이 IEEE 802.11i에서 제안한 무선랜 보안 표준에 따르는 경우, 무선랜 시스템 내부의 AP와 무선랜 단말에 대해서만 인증, 및 암호화를 수행한다. 이에 따라 무선랜 시스템 외부의 AP 또는 무선랜 단말이 무선랜 보안 영역 내의 무선랜 단말에 접속하여 무선랜 보안 영역 내의 정보가 유출되는 문제점이 있다.

발명이 이루고자 하는 기술적 과제

<9> 본 발명이 이루고자 하는 기술적 과제는 무선랜 보안 영역 내의 모든 무선랜 기기를 탐지하고 감시하여 무선랜 시스템으로의 침입을 방지하는 시스템 및 방법을 제공하는 것이다.

발명의 구성 및 작용

<10> 본 발명의 실시예에 따른 무선랜 침입 방지 방법은 복수의 센서로부터 무선랜 기기에 대한 복수의 무선랜 감시 정보를 수신하는 단계, 복수의 무선랜 감시 정보를 바탕으로 무선랜 기기가 악성 무선랜 기기인지를 판단하는 단계, 무선랜 기기가 악성 무선랜 기기인 경우, 복수의 무선랜 감시 정보를 바탕으로 악성 무선랜 기기의 위치 정보를 생성하는 단계, 악성 무선랜 기기에 대한 통신 차단 메시지를 생성하는 단계, 및 복수의 센서로 통신 차단 메시지를 전송하여 통신 차단 메시지에 따라 악성 무선랜 기기가 통신을 중단하도록 하는 단계를 포함한다.

<11> 이때 복수의 무선랜 감시 정보 각각은 무선랜 기기에 대한 신호 강도를 포함하고, 위치 정보를 생성하는 단계는 복수의 무선랜 감시 정보에 각각 포함된 복수의 신호 강도에 대응하는 복수의 거리를 바탕으로 위치 정보를 생성하는 단계를 포함한다.

<12> 또한 이때 통신 차단 메시지를 전송하는 단계는 위치 정보를 바탕으로 복수의 센서 중 악성 무선랜 기기와 가장 가까운 센서로 통신 차단 메시지를 전송하는 단계를 포함한다.

<13> 본 발명의 다른 실시예에 따른 무선랜 침입 방지 방법은 복수의 센서로부터 복수의 무선랜 기기에 각각 대응하는 복수의 무선랜 감시 정보를 수신하는 단계, 복수의 무선랜 감시 정보를 바탕으로 복수의 무선랜 기기 중 악성 무선랜 기기를 검출하는 단계, 악성 무선랜 기기에 대응하는 통신 차단 메시지를 생성하는 단계, 및 복수의 센서 중 일부의 센서로 통신 차단 메시지를 전송하여 일부의 센서가 통신 차단 메시지를 복수의 무선랜 기기로 전송하도록 하는 단계를 포함한다.

<14> 이때 검출하는 단계는 복수의 무선랜 기기 중 해킹 툴을 사용하는 무선랜 기기가 있는 경우, 해킹 툴을 사용하는 무선랜 기기를 악성 무선랜 기기로 결정하는 단계를 포함한다.

<15> 또한 이때 검출하는 단계는 복수의 무선랜 기기 중 서비스 거부 공격을 하는 무선랜 기기가 있는 경우, 서비스 거부 공격을 하는 무선랜 기기를 악성 무선랜 기기로 결정하는 단계를 포함한다.

<16> 또한 이때 검출하는 단계는 복수의 무선랜 기기 중 허용된 인증 방법 리스트 또는 허용된 암호화 방법 리스트에 포함된 인증 방법 또는 암호화 방법을 사용하지 않는 무선랜 기기를 악성 무선랜 기기로 결정하는 단계를 포함한다.

<17> 또한 이때 검출하는 단계는 복수의 무선랜 기기 중 허용된 통신 프로토콜 리스트에 포함된 통신 프로토콜을 사용하지 않는 무선랜 기기를 악성 무선랜 기기로 결정하는 단계를 포함한다.

<18> 또한 이때 검출하는 단계는 복수의 무선랜 기기 중 허용된 기기 리스트에 포함되지 않는 무선랜 기기와 통신하

는 무선랜 기기를 악성 무선랜 기기로 결정하는 단계를 포함한다.

<19> 본 발명의 다른 실시예에 따른 무선랜 침입 방지 시스템은 무선랜 기기, 센서, 및 센서 관리 서버를 포함한다. 무선랜 기기는 무선 채널을 통해 패킷을 전송한다. 센서는 무선랜 기기가 전송하는 패킷을 바탕으로 무선랜 감시 정보를 생성하고, 무선랜 기기를 제어한다. 센서 관리 서버는 무선랜 감시 정보에 대응하는 무선랜 침입 정보를 생성하고, 센서를 제어한다.

<20> 이때 무선랜 침입 방지 시스템은 무선랜 침입 정보에 대응하는 무선랜 제어 명령에 따라 센서 관리 서버를 제어하는 감시 단말을 더 포함한다.

<21> 또한 이때 센서 관리 서버는 무선랜 시스템 감시부와 센서 제어부를 포함한다. 무선랜 시스템 감시부는 센서로부터 무선랜 감시 정보를 수신하고, 무선랜 감시 정보에 대응하는 무선랜 침입 정보를 생성하며, 무선랜 침입 정보를 감시 단말로 전송한다. 센서 제어부는 감시 단말로부터 무선랜 제어 명령을 수신하고, 무선랜 제어 명령에 대응하는 무선랜 제어 메시지를 생성하며, 무선랜 제어 메시지를 센서로 전송한다.

<22> 또한 이때 센서는 무선랜 기기 감시부, 및 무선랜 기기 제어부를 포함한다. 무선랜 기기 감시부는 무선랜 기기가 전송하는 패킷을 수집하고, 수집한 패킷으로부터 무선랜 기기에 대응하는 무선랜 감시 정보를 추출하며, 무선랜 감시 정보를 센서 관리 서버로 전송한다. 무선랜 기기 제어부는 센서 관리 서버로부터 무선랜 제어 메시지를 수신하고, 무선랜 제어 메시지를 무선랜 기기로 전송한다.

<23> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<24> 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "…부", "…기", "모듈", "블록" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

<25> 이제 본 발명의 실시예에 따른 무선랜 침입 방지 시스템 및 방법에 대하여 도면을 참고로 하여 상세하게 설명한다.

<26> 다음은 도 1을 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 시스템에 대해 설명한다.

<27> 도 1은 본 발명의 실시예에 따른 무선랜 침입 방지 시스템의 구성도이다.

<28> 도 1에 도시된 바와 같이 본 발명의 실시예에 따른 무선랜 침입 방지 시스템은 무선랜 시스템(100), 센서 관리 서버(200), 및 감시 단말(300)을 포함한다.

<29> 무선랜 시스템(100)은 복수의 무선랜 기기(110)와 복수의 센서(130)를 포함한다. 무선랜 시스템(100)은 복수의 무선랜 기기(110)를 포함하는 무선 네트워크를 구축한다.

<30> 무선랜 기기(110)는 무선 네트워크를 구성하고, 다른 무선랜 기기(110)와 무선 네트워크를 통해 데이터를 교환한다. 무선랜 기기(110)는 데이터를 암호화하여 전송할 수 있고, 이때 암호화 방식은 미리 정의된다. 무선랜 기기(110)에는 액세스 포인트(Access Point, AP), 유무선 IP 공유기, 무선 랜카드, 무선 프린터, 안테나, 무선네트워크 카메라 등이 있다.

<31> 센서(130)는 무선랜 기기(110)를 감시하고 제어한다. 센서(130)는 무선랜 기기(110)가 전송하는 패킷을 통해 무선랜 기기(110)를 감시하고, 센서 관리 서버(200)의 제어에 따라 무선랜 기기(110)를 제어한다.

<32> 센서 관리 서버(200)는 센서(130)를 통해 무선랜 시스템(100)을 감시하고, 감시 단말(300)의 제어에 따라 센서(130)를 제어한다.

<33> 감시 단말(300)는 서버(200)를 제어한다. 이때 감시 단말(300)은 통신망을 통해 센서 관리 서버(200)를 제어할 수 있다. 또한 이때 감시 단말(300)은 센서 관리 서버(200)에 포함될 수도 있다.

<34> 다음은 도 2를 참고하여 본 발명의 실시예에 따른 무선랜 시스템의 센서에 대해 설명한다.

<35> 도 2는 본 발명의 실시예에 따른 센서의 구성도이다.

<36> 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 센서(130)는 무선랜 기기 감시부(131)와 무선랜 기기 제어부(133)를 포함한다.

<37> 무선랜 기기 감시부(131)는 무선랜 기기(110)가 전송하는 패킷을 통해 무선랜 기기(110)를 감시한다. 무선랜 기기 감시부(131)는 패킷 수집부(131a), 무선랜 감시 정보 추출부(131b), 및 무선랜 감시 정보 전송부(131c)를 포함한다.

<38> 패킷 수집부(131a)는 무선랜 기기(110)가 전송하는 모든 패킷을 수집한다.

<39> 무선랜 감시 정보 추출부(131b)는 패킷 수집부(131a)가 수집한 패킷으로부터 무선랜 기기(110)에 대응하는 무선랜 감시 정보를 추출한다.

<40> 무선랜 감시 정보 전송부(131c)는 무선랜 감시 정보 추출부(131b)가 추출한 무선랜 감시 정보를 센서 관리 서버(200)로 전송한다.

<41> 무선랜 기기 제어부(133)는 센서 관리 서버(200)의 제어에 따라 무선랜 기기(110)를 제어한다. 무선랜 기기 제어부(133)는 무선랜 제어 메시지 수신부(133a), 및 무선랜 제어 메시지 전송부(133b)를 포함한다.

<42> 무선랜 제어 메시지 수신부(133a)는 센서 관리 서버(200)로부터 무선랜 제어 메시지를 수신한다.

<43> 무선랜 제어 메시지 전송부(133b)는 무선랜 제어 메시지 수신부(133a)가 수신한 무선랜 제어 메시지를 무선랜 기기(110)로 전송한다.

<44> 다음은 도 3을 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 시스템의 센서 관리 서버에 대해 설명한다.

<45> 도 3은 본 발명의 실시예에 따른 센서 관리 서버의 구성도이다.

<46> 도 3에 도시된 바와 같이 본 발명의 실시예에 따른 센서 관리 서버(200)는 무선랜 시스템 감시부(210), 및 센서 제어부(230)를 포함한다.

<47> 무선랜 시스템 감시부(210)는 복수의 센서(130)를 통해 무선랜 시스템(100)을 감시한다. 무선랜 시스템 감시부(210)는 무선랜 감시 정보 수신부(211), 악성 무선랜 기기 검출부(213), 위치 정보 생성부(215), 무선랜 침입 정보 생성부(217), 및 무선랜 침입 정보 전송부(219)를 포함한다.

<48> 무선랜 감시 정보 수신부(211)는 센서(130)로부터 무선랜 감시 정보를 수신한다. 이때 무선랜 감시 정보 수신부(211)는 복수의 센서(130)로부터 하나의 무선랜 기기(110)에 대한 복수의 무선랜 감시 정보를 수신할 수 있다. 또한 이때 무선랜 감시 정보 수신부(211)는 하나의 센서(130)로부터 복수의 무선랜 기기(100)에 각각 대응하는 복수의 무선랜 감시 정보를 수신할 수도 있다.

<49> 악성 무선랜 기기 검출부(213)는 무선랜 감시 정보 수신부(211)가 수신한 무선랜 감시 정보를 바탕으로 무선랜 시스템(100)의 보안 수준을 침해하는 무선랜 기기(이하 '악성 무선랜 기기'라고 함)를 검출한다.

<50> 위치 정보 생성부(215)는 무선랜 감시 정보를 바탕으로 악성 무선랜 기기 검출부(213)가 검출한 악성 무선랜 기기의 위치 정보를 생성한다.

<51> 무선랜 침입 정보 생성부(217)는 무선랜 감시 정보와 악성 무선랜 기기의 위치 정보를 바탕으로 무선랜 침입 정보를 생성한다.

<52> 무선랜 침입 정보 전송부(219)는 무선랜 침입 정보를 감시 단말(300)로 전송한다.

<53> 센서 제어부(230)는 감시 단말(300)의 제어에 따라 센서(130)를 제어한다. 센서 제어부(230)는 무선랜 제어 명령 수신부(231), 무선랜 제어 메시지 생성부(233), 및 무선랜 제어 메시지 전송부(235)를 포함한다.

<54> 무선랜 제어 명령 수신부(231)는 감시 단말(300)로부터 무선랜 제어 명령을 수신한다.

<55> 무선랜 제어 메시지 생성부(233)는 무선랜 제어 명령 수신부(231)가 수신한 무선랜 제어 명령에 대응하는 무선랜 제어 메시지를 생성한다.

<56> 무선랜 제어 메시지 전송부(235)는 무선랜 제어 메시지 생성부(233)가 생성한 무선랜 제어 메시지를 센서(130)로 전송한다.

<57> 다음은 도 4를 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 시스템의 감시 단말에 대해 설명한다.

<58> 도 4는 본 발명의 실시예에 따른 감시 단말의 구성도이다.

<59> 도 4에 도시된 바와 같이 본 발명의 실시예에 따른 감시 단말(300)은 무선랜 침입 정보 수신부(310), 무선랜 침입 정보 출력부(330), 무선랜 제어 명령 입력부(350), 및 무선랜 제어 명령 전송부(370)를 포함한다.

<60> 무선랜 침입 정보 수신부(310)는 센서 관리 서버(200)로부터 무선랜 침입 정보를 수신한다.

<61> 무선랜 침입 정보 출력부(330)는 무선랜 침입 정보 수신부(310)가 수신한 무선랜 침입 정보를 출력한다.

<62> 무선랜 제어 명령 입력부(350)는 무선랜 침입 정보에 대한 무선랜 제어 명령을 입력 받는다.

<63> 무선랜 제어 명령 전송부(370)는 무선랜 제어 명령을 센서 관리 서버(200)로 전송한다.

<64> 다음은 도 5와 도 6을 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 방법에 대해 설명한다.

<65> 도 5는 본 발명의 실시예에 따른 무선랜 침입 방지 방법의 순서도이다.

<66> 도 5에 도시된 바와 같이, 먼저 무선랜 시스템(100)의 무선랜 기기(110)가 패킷을 전송하면(S101), 센서(130)의 무선랜 기기 감시부(131)가 패킷을 수집한다(S103). 무선랜 기기 감시부(131)의 패킷 수집부(131a)는 무선랜 기기(110)가 전송한 모든 패킷을 수집한다. 이때 복수의 센서(130)가 무선랜 기기(110)가 전송한 패킷을 수집할 수 있다.

<67> 다음 센서(130)의 무선랜 기기 감시부(131)는 수집한 패킷으로부터 무선랜 감시 정보를 추출한다(S105). 무선랜 기기 감시부(131)의 무선랜 감시 정보 추출부(131b)는 패킷 수집부(131a)가 수집한 패킷으로부터 무선랜 감시 정보를 추출한다. 무선랜 감시 정보 추출부(131b)가 추출한 무선랜 감시 정보는 무선랜 기기 정보와 무선랜 위협 탐지 정보를 포함한다.

<68> 무선랜 기기 정보는 무선랜 기기의 종류, 맥 주소(MAC 주소), 아이피 주소(IP 주소), 통신 방식, 신호 강도, 암호화 방식, 채널 정보, 및 발견된 시간 등을 포함한다.

<69> 무선랜 기기의 종류는 패킷을 전송한 무선랜 기기(110)의 종류를 나타낸다. 맥 주소는 패킷을 전송한 무선랜 기기(110)의 물리 주소를 나타낸다. 아이피 주소는 패킷을 전송한 무선랜 기기(110)의 네트워크 주소를 나타낸다. 통신 방식은 무선랜 기기(110)가 패킷을 전송할 때 사용한 통신 방식을 나타내는 것으로 IEEE 802.11a, IEEE 802.11b, IEEE 802.11g 등이 있을 수 있다. 신호 강도는 센서가 수집한 패킷의 신호 강도를 나타낸다. 암호화 방식은 패킷이 암호화된 방식을 나타내는 것으로 유선급 프라이버시(Wired Equivalent Privacy, WEP), 임시 키 무결성 프로토콜(Temporal Key Integrity Protocol, TKIP), 위상 편이 방식(Phase Shift Keying, PSK), 고급 암호 표준(Advanced Encryption Standard, AES), 전송 계층 보안(Transport Layer Security, TLS), Tunneled TLS(TTLS), 보호 확장성 인증 프로토콜(Protected Extensible Authentication Protocol, PEAP) 등이 있을 수 있다. 채널 정보는 무선랜 기기(100)가 패킷을 전송하기 위해 사용한 채널에 관한 정보를 나타낸다. 발견된 시간은 센서(130)가 무선랜 기기(110)를 발견한 시간을 나타낸다.

<70> 무선랜 위협 탐지 정보는 패킷 목적지 정보, 해킹 툴(hacking Tool) 사용 여부, 인증 및 암호화 정보, 액세스 포인트(Access Point, AP) 설정 정보, 서비스 거부(Denial of Service, DoS) 공격 여부 등을 포함한다.

<71> 패킷 목적지 정보는 패킷의 최종 목적지를 나타낸다. 해킹 툴 사용 여부는 패킷을 전송한 무선랜 기기(110)가 다른 무선랜 기기(110)의 정보를 해킹하거나 네트워크에 침입하기 위해 해킹 툴을 사용하는지를 나타낸다. 인증 및 암호화 정보는 패킷을 전송한 무선랜 기기(110)가 인증 또는 암호화를 수행하는지 여부를 나타낸다. AP 설정 정보는 패킷을 전송한 무선랜 기기(110)와 통신하는 AP에 대한 설정 정보를 나타낸다. DoS 공격 여부는 패킷을 전송하는 무선랜 기기(110)가 서비스 거부 공격을 받는지 또는 서비스 거부 공격을 시도하는지를 나타낸다.

<72> 이후 센서(130)의 무선랜 기기 감시부(131)가 무선랜 감시 정보를 센서 관리 서버(200)로 전송하면, 센서 관리 서버(200)의 무선랜 시스템 감시부(210)가 무선랜 감시 정보를 수신한다(S107). 무선랜 기기 감시부(131)의 무선랜 감시 정보 전송부(131c)가 무선랜 감시 정보를 센서 관리 서버(200)로 전송하고, 무선랜 시스템 감시부(210)의 무선랜 감시 정보 수신부(211)가 센서(200)로부터 무선랜 감시 정보를 수신한다. 이때 센서 관리 서버(200)는 센서(130)로부터 복수의 무선랜 기기(110)에 각각 대응하는 복수의 무선랜 감시 정보를 수신할 수 있다. 또한 이때 센서 관리 서버(200)는 복수의 센서(130)로부터 하나의 무선랜 기기(110)에 대한 복수의 무선랜 감시 정보를 수신할 수도 있다.

<73> 다음 센서 관리 서버(200)의 무선랜 시스템 감시부(210)는 무선랜 감시 정보를 바탕으로 악성 무선랜 기기를 검출한다(S109). 무선랜 시스템 감시부(210)의 악성 무선랜 기기 검출부(213)가 무선랜 감시 정보를 바탕으로 악성 무선랜 기기를 검출한다. 이때 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 검색하여 복수의 무선랜 기기(110) 중에서 악성 무선랜 기기를 검출한다. 이때 악성 무선랜 기기는 무선랜 시스템(100)의 보안 수준에 따라 미리 정의된다.

<74> 이하에서는 악성 무선랜 기기에 해당하는 경우와 악성 무선랜 기기 검출부가 악성 무선랜 기기를 검출하는 방법을 자세히 설명한다.

<75> 악성 무선랜 기기에 해당하는 경우에는 무선랜 기기(110)가 허용되지 않는 무선랜 기기와 통신하는 경우, 무선랜 기기(110)가 허용되지 않는 인증 방법 또는 허용되지 않는 암호화 방법을 따르는 경우, 무선랜 기기(110)가 무선랜 해킹 툴을 사용하는 경우, 무선랜 기기(110)가 무선랜 DoS 공격을 하는 경우, 무선랜 기기(110)가 허용되지 않는 통신 프로토콜을 사용하는 경우 등이 있다.

<76> 먼저 무선랜 기기(110)가 허용되지 않는 무선랜 기기와 통신하는 경우에는 무선랜 기기(110)가 무선랜 시스템(100) 외부의 단말 또는 AP와 통신하는 경우, 무선랜 기기(110)가 무선랜 시스템(100) 내부의 인증되지 않은 단말 또는 AP와 통신하는 경우 등이 있을 수 있다. 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 바탕으로 통신 허용 기기 리스트에 포함되지 않는 무선랜 기기와 통신하는 무선랜 기기(110)를 악성 불법 무선랜 기기로 결정한다. 이때 통신 허용 기기 리스트는 미리 정의될 수 있다. 또한 이때 악성 무선랜 기기 검출부(213)는 감시 단말(300)로부터 통신 허용 기기 리스트를 수신할 수도 있다. 또한 이때 감시 단말(300)은 통신 허용 기기 리스트를 주기적으로 갱신할 수 있다.

<77> 다음 무선랜 기기(110)가 허용되지 않는 인증 방법 또는 허용되지 않는 암호화 방법을 따르는 경우에는 무선랜 기기(110)가 미리 정의된 인증 방식에 따르지 않아 무선랜 기기(110) 내부의 정보가 유출 되는 경우와 무선랜 기기(110)가 미리 정의된 암호화 방식을 따르지 않고 패킷을 전송하여 패킷의 정보가 유출되는 경우 등이 있다. 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 바탕으로 허용된 인증 방법 리스트 또는 허용된 암호화 방법 리스트에 포함되는 인증 방법 또는 암호화 방법을 사용하지 않는 무선랜 기기(110)를 악성 무선랜 기기로 결정한다. 이때 허용된 인증 방법 리스트 또는 허용된 암호화 방법 리스트는 미리 정의될 수 있다. 또한 이때 악성 무선랜 기기 검출부(213)는 허용된 인증 방법 리스트 또는 허용된 암호화 방법 리스트를 감시 단말(300)로부터 수신할 수도 있다. 또한 이때 감시 단말(300)은 허용된 인증 방법 리스트와 허용된 암호화 방법 리스트를 주기적으로 갱신할 수 있다.

<78> 다음 무선랜 기기(110)가 무선랜 해킹 툴을 사용하는 경우에는 무선랜 기기(110)에 무선랜 해킹 툴이 설치되어 무선랜 시스템(100) 외부로 무선랜 기기(110)에 대한 정보를 유출하는 경우 등이 있다. 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 바탕으로 무선랜 해킹 툴을 사용하는 무선랜 기기(110)를 악성 무선랜 기기로 결정한다.

<79> 다음 무선랜 기기(110)가 무선랜 DoS 공격을 하는 경우에는 무선랜 기기(110)가 직접 무선랜 DoS 공격을 수행하는 경우, 무선랜 시스템(100) 외부의 무선랜 기기가 무선랜 기기(110)를 제어하여 DoS 공격을 수행하는 경우 등이 있다. 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 바탕으로 DoS 공격을 수행하는 무선랜 기기(110)를 악성 무선랜 기기로 결정한다.

<80> 다음 무선랜 기기(110)가 허용되지 않는 통신 프로토콜을 사용하는 경우, 악성 무선랜 기기 검출부(213)는 복수의 무선랜 감시 정보를 바탕으로 허용된 통신 프로토콜 리스트에 포함되는 통신 프로토콜을 사용하지 않는 무선랜 기기(110)를 악성 무선랜 기기로 결정한다. 이때 허용된 통신 프로토콜 리스트는 미리 정의될 수 있다. 또한 이때 악성 무선랜 기기 검출부(213)는 허용된 통신 프로토콜 리스트를 감시 단말(300)로부터 수신할 수 있다. 또한 이때 감시 단말(300)은 허용된 통신 프로토콜 리스트를 주기적으로 갱신할 수 있다.

<81> 다시 도 5를 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 방법에 대해 설명한다.

<82> 이후 센서 관리 서버(200)의 무선랜 시스템 감시부(210)는 악성 무선랜 기기의 위치 정보를 생성한다(S111). 무선랜 시스템 감시부(210)의 위치 정보 생성부(215)는 무선랜 감시 정보를 바탕으로 악성 무선랜 기기 검출부(213)가 검출한 악성 무선랜 기기의 위치 정보를 생성한다.

<83> 이하에서는 도 6을 참고하여 본 발명의 실시예에 따른 무선랜 시스템 감시부의 위치 정보 생성부가 악성 무선랜 기기의 위치 정보를 생성하는 방법을 설명한다.

<84> 도 6은 본 발명의 실시예에 따른 위치 정보 생성부가 악성 무선랜 기기의 위치 정보를 생성하는 방법을 도시한 도면이다.

<85> 위치 정보 생성부(215)는 무선랜 감시 정보에 포함된 신호 강도를 통해 악성 무선랜 기기의 위치 정보를 생성한다.

<86> 도 6에 도시된 바와 같이, 3개의 센서(130)가 악성 무선랜 기기가 전송한 패킷으로부터 3개의 센서에 각각 대응하는 3개의 신호 강도를 추출하면, 위치 정보 생성부(215)는 3개의 신호 강도 각각을 거리로 변환하여 3개의 센서(S_1, S_2, S_3)에 각각 대응하는 3개의 센서로부터 기기까지의 거리(d_1, d_2, d_3)를 생성한다.

<87> 위치 정보 생성부(290)는 3개의 센서(130)에 각각 대응하는 3개의 센서 위치(S_1, S_2, S_3)를 중심점으로 하고, 3개의 센서(130)에 각각 대응하는 3개 거리(d_1, d_2, d_3)를 반지름으로 하는 3개의 원이 모두 통과하는 교점을 무선랜 기기(110)의 위치로 결정한다. 이때 각 센서(130)에 대응하는 센서 위치는 미리 정의된다. 또한 이때 신호 강도에 따른 거리가 미리 정의될 수도 있다.

<88> 다시 도 5를 참고하여 본 발명의 실시예에 따른 무선랜 침입 방지 방법에 대해 설명한다.

<89> 다음 센서 관리 서버(200)의 무선랜 시스템 감시부(210)는 무선랜 침입 정보를 생성한다(S113). 무선랜 시스템 감시부(210)의 무선랜 침입 정보 생성부(217)는 무선랜 감시 정보와 악성 무선랜 기기의 위치 정보를 바탕으로 악성 무선랜 기기에 대한 무선랜 침입 정보를 생성한다. 무선랜 침입 정보는 무선랜 감시 정보와 악성 무선랜 기기의 위치 정보를 포함할 수 있다.

<90> 이후 센서 관리 서버(200)의 무선랜 시스템 감시부(210)가 무선랜 침입 정보를 감시 단말(300)로 전송하면, 감시 단말(300)이 무선랜 침입 정보를 수신한다(S115). 무선랜 시스템 감시부(210)의 무선랜 침입 정보 전송부(219)가 무선랜 침입 정보를 전송하고, 감시 단말(300)의 무선랜 침입 정보 수신부(310)가 무선랜 침입 정보를 수신한다.

<91> 다음 감시 단말(300)의 무선랜 침입 정보 출력부(330)는 무선랜 침입 정보 수신부(310)가 수신한 무선랜 침입 정보를 출력한다(S117). 무선랜 침입 정보 출력부(330)는 무선랜 침입 정보를 사용자가 볼 수 있도록 출력한다.

<92> 이후 감시 단말(300)의 무선랜 제어 명령 입력부(350)는 통신 차단 명령을 입력한다(S119). 무선랜 제어 명령 입력부(350)는 사용자와 인터페이스를 수행하여 무선랜 침입 정보에 따라 악성 무선랜 기기에 대한 통신 차단 명령을 입력한다. 무선랜 제어 명령 입력부(350)는 악성 무선랜 기기의 통신을 차단하기 위한 통신 차단 명령을 입력한다.

<93> 다음 감시 단말(300)의 무선랜 제어 명령 전송부(370)가 통신 차단 명령을 센서 관리 서버(200)로 전송하면, 센서 관리 서버(200)의 센서 제어부(230)가 통신 차단 명령을 수신한다(S121). 이때 센서 제어부(230)의 무선랜 제어 명령 수신부(231)가 통신 차단 명령을 수신한다.

<94> 이후 센서 관리 서버(200)의 센서 제어부(230)는 통신 차단 메시지를 생성한다(S123). 센서 제어부(230)의 무선랜 제어 메시지 생성부(233)는 통신 차단 명령에 따라 통신 차단 메시지를 생성한다. 이때 통신 차단 메시지는 악성 무선랜 기기의 MAC 주소 또는 IP 주소를 포함할 수 있다.

<95> 다음 센서 관리 서버(200)의 센서 제어부(230)가 통신 차단 메시지를 센서(130)로 전송하면, 센서(130)의 무선랜 기기 제어부(133)가 통신 차단 메시지를 수신한다(S125). 센서 제어부(230)의 무선랜 제어 메시지 전송부(235)가 통신 차단 메시지를 센서(130)로 전송하고, 무선랜 기기 제어부(133)의 무선랜 제어 메시지 수신부(133a)가 센서 관리 서버(200)로부터 통신 차단 메시지를 수신한다. 이때 무선랜 제어 메시지 전송부(235)는 악성 무선랜 기기의 위치 정보를 바탕으로 악성 무선랜 기기와 가장 가까운 센서로 통신 차단 메시지를 전송할 수 있다.

<96> 이후 센서(130)의 무선랜 기기 제어부(133)가 통신 차단 메시지를 무선랜 기기(110)로 전송하면, 무선랜 기기(110)가 통신 차단 메시지를 수신한다(S127). 이때 무선랜 기기 제어부(133)의 무선랜 제어 메시지 전송부(133b)는 통신 차단 메시지에 포함된 MAC 주소 또는 IP 주소에 대응하는 무선랜 기기(110)로 통신 차단 메시지를 전송할 수 있다. 또한 이때 센서(130)는 악성 무선랜 기기와 통신하는 무선랜 기기로 통신 차단 메시지를 전송할 수도 있다. 또한 이때 센서(130)는 무선랜 시스템(100) 내의 모든 무선랜 기기(110)로 통신 차단 메시지를 전송할 수도 있다.

<97> 다음 무선랜 기기(110)는 통신 차단 메시지에 따라 통신을 중단한다(S129).

<98> 본 발명의 실시예는 이상에서 설명한 장치 및/또는 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하기 위한 프로그램, 그 프로그램이 기록된 기록 매체 등을 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

<99> 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

<100> 이상에서 설명한 본 발명에 따라 무선랜 침입 방지 시스템은 센서를 통해 무선랜 기기의 패킷을 감시하여 악성 무선랜 기기의 통신을 차단하고, 무선랜 시스템 외부로 정보가 유출되는 것을 방지한다.

도면의 간단한 설명

<1> 도 1은 본 발명의 실시예에 따른 무선랜 침입 방지 시스템의 구성도이다.

<2> 도 2는 본 발명의 실시예에 따른 센서의 구성도이다.

<3> 도 3은 본 발명의 실시예에 따른 센서 관리 서버의 구성도이다.

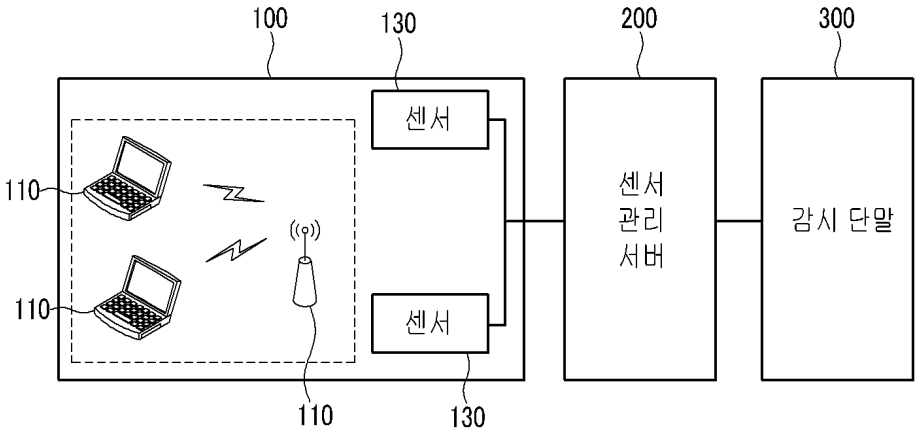
<4> 도 4는 본 발명의 실시예에 따른 감시 단말의 구성도이다.

<5> 도 5는 본 발명의 실시예에 따른 무선랜 침입 방지 방법의 순서도이다.

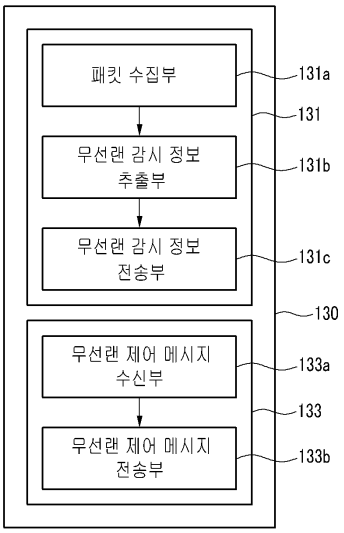
<6> 도 6은 본 발명의 실시예에 따른 위치 정보 생성부가 악성 무선랜 기기의 위치 정보를 생성하는 방법을 도시한 도면이다.

도면

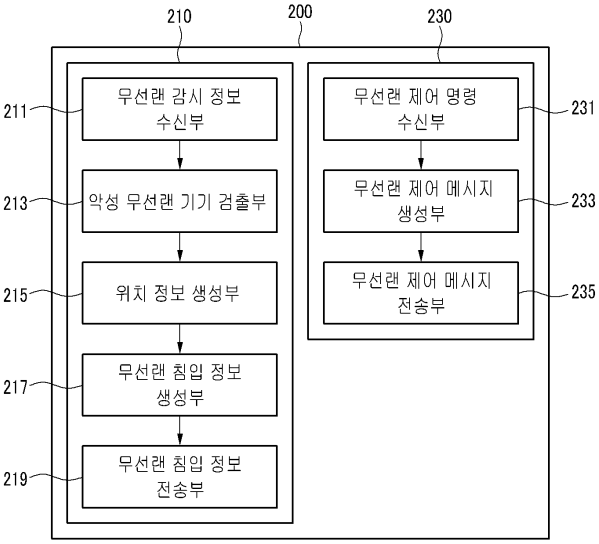
도면1



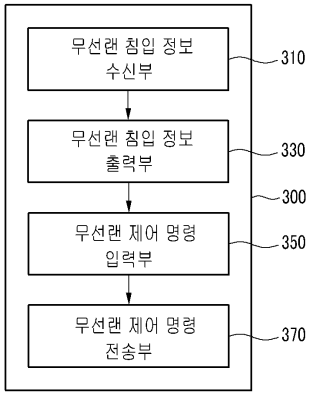
도면2


패킷 수집부
131a
131
무선랜 감시 정보 추출부
131b
무선랜 감시 정보 전송부
131c
130
무선랜 제어 메시지 수신부
133a
133
무선랜 제어 메시지 전송부
133b

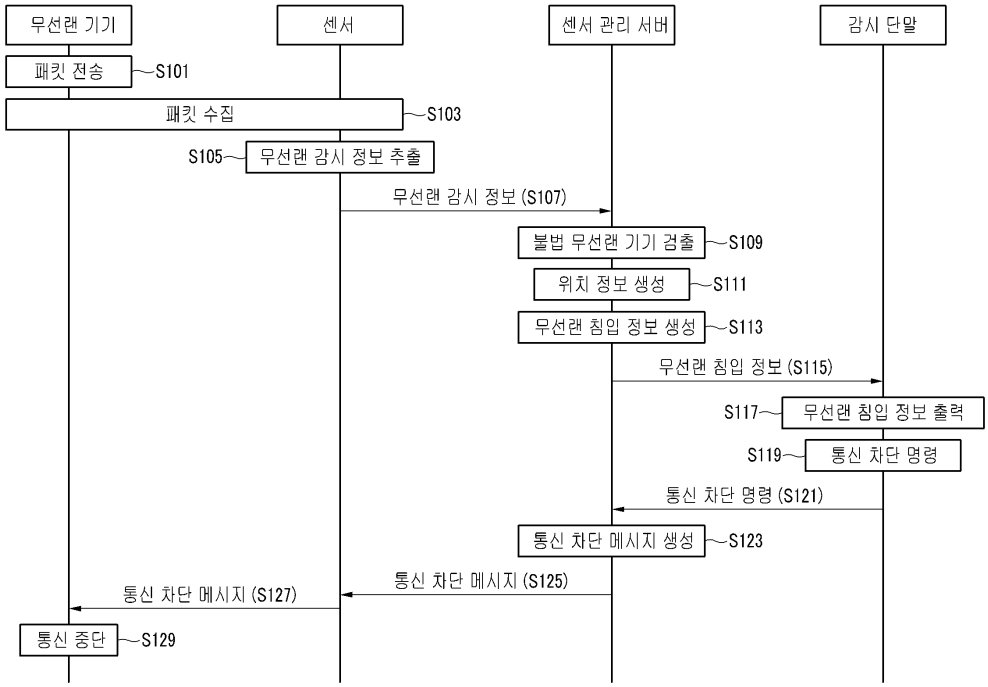
도면3


210
200
230
211
무선랜 감시 정보 수신부
213
악성 무선랜 기기 검출부
215
위치 정보 생성부
217
무선랜 침입 정보 생성부
219
무선랜 침입 정보 전송부
무선랜 제어 명령 수신부
231
무선랜 제어 메시지 생성부
233
무선랜 제어 메시지 전송부
235

도면4


무선랜 침입 정보 수신부
310
무선랜 침입 정보 출력부
330
300
무선랜 제어 명령 입력부
350
무선랜 제어 명령 전송부
370

도면5


무선랜 기기
센서
센서 관리 서버
감시 단말
패킷 전송
S101
패킷 수집
S103
S105
무선랜 감시 정보 추출
무선랜 감시 정보 (S107)
불법 무선랜 기기 검출
S109
위치 정보 생성
S111
무선랜 침입 정보 생성
S113
무선랜 침입 정보 (S115)
S117
무선랜 침입 정보 출력
S119
통신 차단 명령
통신 차단 명령 (S121)
통신 차단 메시지 생성
S123
통신 차단 메시지 (S125)
통신 차단 메시지 (S127)
통신 중단
S129

도면6