



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0111871  
(43) 공개일자 2022년08월10일

(51) 국제특허분류(Int. Cl.)  
G01V 3/12 (2006.01) H04B 1/40 (2015.01)  
H04B 17/00 (2015.01) H04M 1/19 (2006.01)  
(52) CPC특허분류  
G01V 3/12 (2013.01)  
H04B 1/40 (2013.01)  
(21) 출원번호 10-2021-0015203  
(22) 출원일자 2021년02월03일  
심사청구일자 2021년02월03일

(71) 출원인  
인하대학교 산학협력단  
인천광역시 미추홀구 인하로 100(용현동, 인하대 학교)  
(72) 발명자  
노영태  
경기도 성남시 분당구 판교로 393, 204동 203호(삼평동, 붓달마을2단지이지더원아파트)  
(74) 대리인  
양성보

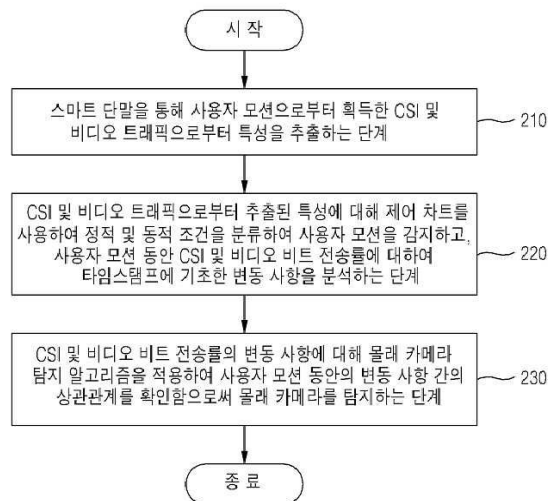
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 몰래 카메라 탐지 시스템

(57) 요약

몰래 카메라 탐지 방법 및 시스템이 제시된다. 본 발명에서 제안하는 몰래 카메라 탐지 방법은 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계, CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 단계 및 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계를 포함한다.

대표도 - 도2



(52) CPC특허분류

**H04B 17/00** (2013.01)

**H04M 1/19** (2021.01)

이 발명을 지원한 국가연구개발사업

|             |                                                   |
|-------------|---------------------------------------------------|
| 과제고유번호      | 1711119389                                        |
| 과제번호        | 2020R1A4A1018774                                  |
| 부처명         | 과학기술정보통신부                                         |
| 과제관리(전문)기관명 | 한국연구재단                                            |
| 연구사업명       | 기초연구실지원사업                                         |
| 연구과제명       | 모바일 디지털 치료제 개발을 위한 데이터 기반 치료제 전달 수용도 최적화 원천 기술 개발 |

|         |                         |
|---------|-------------------------|
| 기 여 율   | 1/4                     |
| 과제수행기관명 | 한국과학기술원                 |
| 연구기간    | 2020.07.01 ~ 2023.02.28 |

이 발명을 지원한 국가연구개발사업

|             |                                   |
|-------------|-----------------------------------|
| 과제고유번호      | 1711108372                        |
| 과제번호        | 2016R1C1B2011415                  |
| 부처명         | 과학기술정보통신부                         |
| 과제관리(전문)기관명 | 한국연구재단                            |
| 연구사업명       | 이공분야기초연구사업                        |
| 연구과제명       | 강화학습을 활용한 SDN WiFi 네트워크의 UX 개선 기술 |
| 기 여 율       | 1/4                               |
| 과제수행기관명     | 인하대학교                             |
| 연구기간        | 2018.03.01 ~ 2021.02.28           |

이 발명을 지원한 국가연구개발사업

|             |                                       |
|-------------|---------------------------------------|
| 과제고유번호      | 1711073301                            |
| 과제번호        | 2017M3C4A7083534                      |
| 부처명         | 과학기술정보통신부                             |
| 과제관리(전문)기관명 | 한국연구재단                                |
| 연구사업명       | 차세대정보·컴퓨팅기술개발                         |
| 연구과제명       | 긍정 컴퓨팅을 위한 설득적 인터랙션 SW 원천 기술 및 플랫폼 개발 |
| 기 여 율       | 1/4                                   |
| 과제수행기관명     | 한국과학기술원                               |
| 연구기간        | 2018.03.01 ~ 2021.05.31               |

이 발명을 지원한 국가연구개발사업

|             |                                                      |
|-------------|------------------------------------------------------|
| 과제고유번호      | 1711120302                                           |
| 과제번호        | 2020-0-01965-001                                     |
| 부처명         | 과학기술정보통신부                                            |
| 과제관리(전문)기관명 | 정보통신기획평가원                                            |
| 연구사업명       | 방송통신산업기술개발사업                                         |
| 연구과제명       | [Ezbaro] (2단계 : 기술개발) 디지털 피노타이핑 기반 다차원적 우울 탐지 플랫폼 개발 |
| 기 여 율       | 1/4                                                  |
| 과제수행기관명     | (주)휴노                                                |
| 연구기간        | 2021.01.01 ~ 2021.12.31                              |

## 명세서

### 청구범위

#### 청구항 1

스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계;

CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 단계; 및

CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계

를 포함하는 몰래 카메라 탐지 방법.

#### 청구항 2

제1항에 있어서,

사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계는,

원시 CSI로부터 사용되지 않는 DC 서브캐리어를 제외한 데이터 서브캐리어를 수집하고, 수집된 데이터 서브캐리어의 진폭과 위상 응답을 활용하여 사용자의 모션을 감지하기 위한 CSI 특성을 추출하고,

비디오 트래픽의 패킷 길이 분포(Packet Length Distribution; PLD) 특성 및 대역폭 안정성 특성(Bandwidth stability feature)을 포함하는 2차원 특성 벡터를 분석함으로써 혼합 트래픽으로부터 비디오 트래픽을 식별하여 특성을 추출하는

몰래 카메라 탐지 방법.

#### 청구항 3

제1항에 있어서,

CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계는,

몰래 카메라 탐지 알고리즘을 통해 비디오 트래픽의 패킷 길이 분포(PLD)를 분석하여, 패킷 길이 분포가 발견되면 소스와 대상의 MAC 주소를 반환하고, 발견된 패킷 길이 분포에 관한 후보 몰래 카메라들이 사용자를 기록하고 있는지 여부를 확인한 후, 소스 MAC 주소와 대상 MAC 주소 중에서 신호 강도가 가장 높은 송신기를 찾아 CSI 추출을 위해 저장하고, 후보 몰래 카메라의 패킷을 스니핑하고 비트 전송률을 계산하며, 추출된 CSI 및 계산된 비트 전송률을 분석하여 몰래 카메라의 가용성을 탐지하는

몰래 카메라 탐지 방법.

#### 청구항 4

스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 특성 추출부;

CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 모션 분류부; 및

CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 몰래 카메라 탐지 알고리즘 수행부

를 포함하는 몰래 카메라 탐지 시스템.

**청구항 5**

제4항에 있어서,

특성 추출부는,

원시 CSI로부터 사용되지 않는 DC 서브캐리어를 제외한 데이터 서브캐리어를 수집하고, 수집된 데이터 서브캐리어의 진폭과 위상 응답을 활용하여 사용자의 모션을 감지하기 위한 CSI 특성을 추출하고,

비디오 트래픽의 패킷 길이 분포(Packet Length Distribution; PLD) 특성 및 대역폭 안정성 특성(Bandwidth stability feature)을 포함하는 2차원 특성 벡터를 분석함으로써 혼합 트래픽으로부터 비디오 트래픽을 식별하여 특성을 추출하는

몰래 카메라 탐지 시스템.

**청구항 6**

제1항에 있어서,

모션 분류부는,

몰래 카메라 탐지 알고리즘을 통해 비디오 트래픽의 패킷 길이 분포(PLD)를 분석하여, 패킷 길이 분포가 발견되면 소스와 대상의 MAC 주소를 반환하고, 발견된 패킷 길이 분포에 관한 후보 몰래 카메라들이 사용자를 기록하고 있는지 여부를 확인한 후, 소스 MAC 주소와 대상 MAC 주소 중에서 신호 강도가 가장 높은 송신기를 찾아 CSI 추출을 위해 저장하고, 후보 몰래 카메라의 패킷을 스니핑하고 비트 전송률을 계산하며, 추출된 CSI 및 계산된 비트 전송률을 분석하여 몰래 카메라의 가용성을 탐지하는

몰래 카메라 탐지 시스템.

**청구항 7**

사용자 단말에 설치되는 어플리케이션의 파일을 배포하는 파일 배포 시스템에 있어서,

상기 사용자 단말의 요청에 따라 상기 파일을 전송하는 파일 전송부

를 포함하고,

상기 어플리케이션은,

스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 특성 추출 모듈;

CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 모션 분류 모듈; 및

CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 몰래 카메라 탐지 알고리즘 수행 모듈

을 포함하는 것을 특징으로 하는 파일 배포 시스템.

**발명의 설명****기술 분야**

[0001] 본 발명은 몰래 카메라 탐지 시스템에 관한 것으로, 더욱 상세하게는 WiFi 카메라의 비디오 비트 전송률 및 채널 상태 정보(Channel States Information; CSI)를 활용한 몰래 카메라 탐지 시스템에 관한 것이다.

**배경 기술**

[0002] 최근, 모텔, 호텔, 에어비앤비, 화장실 등과 같은 다양한 사적인 장소에 숨겨진 몰래 카메라는 엄청난 사생활 문제를 제기하고 있다. 최첨단 솔루션인 DeWiCam[4]은 카메라의 트래픽 패턴(즉, 비트 전송률)과 스마트 단말의 가속도계 판독값 사이의 상관 관계를 이용하여 몰래 카메라를 탐지한다. 그러나, 그것은 두 가지 중요한 단점이

있다: (1) 사용자가 동작 감지를 위한 가속도계 센서 사용을 위해 스마트 단말을 휴대해야 한다. (2) 점프, 손 흔들기, 및 장시간 보행 등을 포함하는 약간의 작업 집약적인 동작이 필요하다. 이는 사용자에게 불편을 주고 마지막으로 기존 솔루션의 실행 가능성을 제한한다.

[0003] 기술의 발전으로 HD(High Definition) 오디오 및 비디오, WiFi 연결 등 필요한 모든 기능을 내장하고 있는 소형 카메라의 제작이 가능해졌다. 또한 이러한 소형 카메라는 일상 생활의 물체(예를 들어, 전원 콘센트, USB 충전기 및 연기 감지기 등)에 쉽게 탑재할 수 있다[7]. 하지만, 이러한 발전은 그것의 불법적인 사용을 가능하게 한다. 호텔 객실, 에어비앤비, 화장실 또는 탈의실[3] [10] 등과 같은 개인 구역에 배치될 수 있어 개인의 프라이버시를 침해한다.

[0005] 도 1은 몰래 카메라로 프라이버시를 침해하는 예시를 나타내는 도면이다.

[0006] 도 1을 참조하면, 한쪽 끝에는 카메라가 숨겨져 있는 장소(예를 들어, 드레스 스탠드)에 장착되어 있으며, 피해자는 카메라가 설치된 것을 알지 못한다. 이러한 몰래 카메라는 비밀리에 대상 영역을 기록하고 WiFi 연결을 통해 원격(즉, 클라우드) 또는 로컬 스토리지로 비디오를 계속 스트리밍한다. 한편, 범죄자는 비디오를 다운로드 받아 협박이나 다른 불법적인 목적으로 더 많이 사용할 수 있다.

[0007] 몰래 카메라는 지난 몇 년 동안 엄청난 사생활 문제를 제기해 왔다. 이러한 우려를 완화하기 위해 몰래 카메라를 탐지하기 위한 하드웨어와 소프트웨어 기반 노력이 이루어지고 있다. 상용 하드웨어 기반 솔루션은 시장에 출시되고 있지만, 인근 RF 장치로부터의 방해[1, 2]와 그 부피가 크고 엄청난 비용[14] 때문에 신뢰할 수 없다. 최근 종래기술에서, Cheng은 몰래 카메라 탐지를 위한 신뢰할 수 있는 인간 보조 식별 모델인 DeWiCam [4]를 제안했다. 이것은 몰래 카메라의 고유 패턴 트래픽(즉, 비트 전송률)과 스마트 단말의 가속도계 관측값 사이의 상관 관계를 기반으로 몰래 카메라의 존재를 식별한다. 그럼에도 불구하고, 그것은 본질적으로 해결책을 비실용적으로 만드는 두 가지 중요한 단점을 포함하고 있다. 첫째, 사용자는 스마트 단말의 가속도계를 통해 스마트 단말의 움직임을 감지하기 위해 스마트 단말을 휴대해야 한다. 둘째, 몰래 카메라를 적절하게 탐지하기 위해 작업 집약적인 동작(예를 들어, 손을 흔들고, 점프하고, 더 오랜 시간 동안 걷는 동작) 등의 작업 집약적인 동작이 필요하다.

## 발명의 내용

### 해결하려는 과제

[0008] 본 발명이 이루고자 하는 기술적 과제는 WiFi 카메라의 비디오 비트 전송률 변동과 사용자 모션으로부터 수동적으로 획득한 채널 상태 정보(Channel States Information; CSI)를 활용하는 몰래카메라 탐지를 제공하는데 있다. 제안하는 몰래카메라 탐지를 통해 수동적 감지를 지원하며 작업 집약적인 동작이 필요하지 않고, 사전 핑거 프린팅(finger printing)이나 사전 정의된 임계값이 필요하지 않으므로 추가 설정 없이 거의 모든 환경에서 효율적으로 작업할 수 있다.

### 과제의 해결 수단

[0009] 일 측면에 있어서, 본 발명에서 제안하는 몰래 카메라 탐지 방법은 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계, CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 단계 및 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계를 포함한다.

[0010] 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계는 원시 CSI로부터 사용되지 않는 DC 서브캐리어를 제외한 데이터 서브캐리어를 수집하고, 수집된 데이터 서브캐리어의 진폭과 위상 응답을 활용하여 사용자의 모션을 감지하기 위한 CSI 특성을 추출하고, 비디오 트래픽의 패킷 길이 분포(Packet Length Distribution; PLD) 특성 및 대역폭 안정성 특성(Bandwidth stability feature)을 포함하는 2차원 특성 벡터를 분석함으로써 혼합 트래픽으로부터 비디오 트래픽을 식별하여 특성을 추출한다.

[0011] CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계는 몰래 카메라 탐지 알고리즘을 통해 비디

오 트래픽의 패킷 길이 분포(PLD)를 분석하여, 패킷 길이 분포가 발견되면 소스와 대상의 MAC 주소를 반환하고, 발견된 패킷 길이 분포에 관한 후보 몰래 카메라들이 사용자를 기록하고 있는지 여부를 확인한 후, 소스 MAC 주소와 대상 MAC 주소 중에서 신호 강도가 가장 높은 송신기를 찾아 CSI 추출을 위해 저장하고, 후보 몰래 카메라의 패킷을 스니핑하고 비트 전송률을 계산하며, 추출된 CSI 및 계산된 비트 전송률을 분석하여 몰래 카메라의 가용성을 탐지한다.

[0012] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 몰래 카메라 탐지 시스템은 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 특성 추출부, CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 모션 분류부 및 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 몰래 카메라 탐지 알고리즘 수행부를 포함한다.

### 발명의 효과

[0013] 본 발명의 실시예들에 따른 몰래카메라 탐지 방법 및 장치는 WiFi 카메라의 비디오 비트 전송률 변동과 사용자 모션으로부터 수동적으로 획득한 채널 상태 정보(Channel States Information; CSI)를 활용할 수 있다. 제안하는 몰래카메라 탐지기를 통해 수동적 감지를 지원하며 작업 집약적인 동작이 필요하지 않고, 사전 핑거 프린팅이나 사전 정의된 임계값이 필요하지 않으므로 추가 설정 없이 거의 모든 환경에서 효율적으로 작업할 수 있다.

### 도면의 간단한 설명

[0014] 도 1은 몰래 카메라로 프라이버시를 침해하는 예시를 나타내는 도면이다.  
 도 2는 본 발명의 일 실시예에 따른 몰래 카메라 탐지 방법을 설명하기 위한 흐름도이다.  
 도 3은 본 발명의 일 실시예에 따른 몰래 카메라 탐지 시스템의 구성을 나타내는 도면이다.  
 도 4는 본 발명의 일 실시예에 따른 몰래 카메라 탐지 알고리즘을 나타내는 도면이다.  
 도 5는 본 발명의 일 실시예에 따른 CSI 기능과 비트 레이트를 함께 사용한 카메라의 기록 여부 감지를 설명하기 위한 도면이다.  
 도 6은 본 발명의 일 실시예에 따른 몰래 카메라 탐지 시스템의 성능을 종래기술들과 비교한 도면이다.  
 도 7은 본 발명의 일 실시예에 따른 카메라 AP와 스마트 단말 간의 서로 다른 RSSI 레벨에 대해 설명하기 위한 도면이다.  
 도 8은 본 발명의 일 실시예에 따른 다양한 레벨의 신호 강도에서 SpyCamDetector의 성능 평가 결과를 나타내는 도면이다.

### 발명을 실시하기 위한 구체적인 내용

[0015] 본 발명의 실시예에 따르면, 앞서 언급한 문제를 해결하기 위해 WiFi 카메라의 비디오 비트 전송률 변동과 사용자 이동[9]으로부터 수동적으로 획득한 채널 상태 정보(CSI)를 활용하는 몰래 카메라 탐지 시스템(이하, SpyCamDetector)를 제안한다. SpyCamDetector는 CSI 및 비디오 비트 전송률에 대한 타임스탬프를 기반으로 변동 사항을 검사하고 이러한 변동 사항이 몰래 카메라의 존재 탐지와 상관 관계가 있는지 여부를 확인한다. 그러나 SpyCamDetector에서 CSI 활용할 경우 다음과 같이 처리해야 할 과제도 발생한다:

[0016] 1. 다중 경로의 영향: CSI의 특징은 다중 경로 효과로 인한 산란(예를 들어, 가구) 및 실내 크기의 영향을 크게 받는다는 점이다. 이 때문에 하드 코딩된 임계값 또는 기계 학습 기반 분류는 다른 설정에서 제대로 작동하지 않는다. 이를 위해 제안하는 SpyCamDetector는 제어차트 방식[16]을 채택하여 환경변화에 따른 임계값을 조정하고 높은 정밀도로 동작을 탐지한다. 다양한 실내 크기에서 SpyCamDetector의 성능을 평가하고 평균 약 99%의 탐지율을 확인했다.

[0017] 2. 신호 강도의 영향: 몰래 카메라의 존재를 정확하게 감지하기 위해서는, 몰래 카메라, AP, 스마트 단말이 통신 범위에 있어야 한다. 최적의 설정을 위해 몰래 카메라, AP, 스마트 단말 간의 강한 RSSI 레벨( $\leq -50\text{dBm}$ )은 100%의 탐지율을 보인다. 반대로 몰래 카메라와 AP는 양호한 RSSI 레벨( $\leq -60\text{dBm}$ )이지만 스마트 단말과 몰래 카메라 사이의 RSSI가 불량( $\leq -70\text{dBm}$ )인 최악의 경우 탐지율은 87.5%이다.



- [0018] 3. PNLoS에서 노이즈의 영향: 몰래 카메라 위치로의 PNLoS(Person-in-Non-Line-of-Sight)의 모션으로 인한 왜곡도 주변 노이즈로 감지 오류를 유발한다. 이 효과는 스마트 단말이 CSI 소스(몰래 카메라 또는 AP)보다 낮은 RSSI 레벨을 가질 때 중요하다. 그러나 CSI 소스의 양호한 RSSI 레벨에서는 이러한 효과는 무시할 수 있다. 전자의 경우 9.8 ~ 12.5%의 거짓 경보율을 달성했고 후자의 경우는 2.7%였다.
- [0019] 본 발명의 실시예에 따르면, 사용자의 노력을 최소화하기 위해 CSI 판독값을 활용하고 사용자의 모션 동안 WiFi 카메라가 관찰하는 비트 전송률 변동과의 상관관계를 확인한다. 종래기술들과 비교하여, 제안하는 SpyCamDetector가 쉽고(수동적 감지) 효과적인(즉, 높은 탐지율과 짧은 지연 시간)임을 확인한다.
- [0020] SpyCamDetector의 구현 가능성을 확인하기 위해 CSI와 비디오 트래픽으로부터 추출된 특성, 모션 분류 및 상관관계 탐지 알고리즘을 통합하여, SpyCamDetector 어플리케이션을 제안한다. 이후, 다양한 실생활 시나리오, 즉, 다양한 실내 크기(즉, 다중 경로의 효과), 카메라-AP에서 스마트 단말까지 다양한 RSSI 레벨(즉, 신호 강도의 효과) 및 PNLoS 동작(즉, PNLoS로부터의 노이즈의 효과)에 의한 CSI 노이즈에서 SpyCamDetector의 성능을 평가한다. 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0022] 종래 기술에 따른 무선 카메라 RF 탐지기 [1] 및 Spy RF 신호 탐지기 [2])는 무선 카메라의 RF 신호를 탐지하도록 설계되었다. 그러나 이러한 장치는 신뢰할 수 없으며 2.4GHz 또는 5GHz에서 작동하는 다른 RF 장치에 의해 쉽게 방해받을 수 있다. Spy 카메라 헌터 [14]는 무선 카메라로 스트리밍되는 비디오를 감지하고 표시한다. 이 장치는 1.2GHz, 2.4GHz, 5.8GHz와 같은 다양한 주파수에서 작동한다. 하지만, 그것은 최근에는 널리 사용되지 않는 PAL, NTSC, SECAM과 같은 아날로그 비디오 소스로부터의 스트리밍만 식별한다. 하드웨어 기반 솔루션을 사용할 수 없는 이유는 비용이 많이 들고 휴대할 수 없기 때문이다.
- [0023] 최근, 몰래 카메라를 탐지하기 위한 어플리케이션 기반 솔루션에 대한 몇 가지 기술들이 제안되었다. Wu[17]는 동시 관측의 유사성이라고 불리는 카메라 탐지 기술을 제시하여, 알려진 기록(즉, 동일한 환경에서 사용자의 스트리밍)과 각 네트워크 장치 사이의 데이터 전송의 타이밍 패턴을 비교했다. 그러나 이 작업은 오프라인 교육이 필요하며 확률적 장면에는 적합하지 않다. Liu[8]는 플래싱(flicking) LED 회로를 사용하여 카메라를 프로브하고 그에 대한 카메라의 비트 전송률을 조사한다. 그럼에도 불구하고 이를 위해서는 외부 자극 회로가 필요하며 빛에도 취약하다. Lagesse[6]는 외부 WiFi가 비규칙 모드인 스마트 단말을 사용하여 주변을 기록하는 웹 카메라(즉, 몰래 카메라)의 트래픽을 스니핑(sniff)한다. 그 몰래 카메라는 플래싱 빛에 자극을 받는다. 이를 바탕으로, 카메라 트래픽은 혼합 트래픽과 구별된다.
- [0024] 또 다른 종래기술에서, Cheng은 모니터 모드로 스마트 단말을 필요로 하고 공중에서 무선 신호를 포착하는 최첨단 솔루션인 DeWiCam [4]를 제안했다. 고유한 트래픽 패턴(즉, 패킷 길이 분포)과 이동 시 스마트 단말 가속에 기초하여, 두 가지 사이의 상관 관계를 분석하고 무선 몰래 카메라의 존재를 확인한다. 그럼에도 불구하고 DeWiCam은 다음과 같이 두 가지 중요한 단점 때문에 실용적이지 못하다: (1) 사용자 모션을 감지하기 위해 가속도계 센서를 사용하기 때문에 사용자는 스마트 단말을 휴대해야 한다(즉, 수동 모드 감지를 지원하지 않음), (2) 정밀한 스파이 탐지를 위해 노동 집약적인 동작(예를 들어, 점프, 손 흔들기, 장시간 보행)이 필요하다.
- [0025] 본 발명에서 제안하는 SpyCamDetector는 종래기술의 DeWiCam에 의해 초래된 모든 단점을 해결한다. 제안하는 SpyCamDetector는 패시브 모드 감지(즉, 스마트 단말을 휴대할 필요가 없음)를 지원하며, (2) 노동 집약적인 모션(즉, 급격한 이동 또는 긴 보행)이 필요하지 않다.
- [0027] 도 2는 본 발명의 일 실시예에 따른 몰래 카메라 탐지 방법을 설명하기 위한 흐름도이다.
- [0028] 제안하는 몰래 카메라 탐지 방법은 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출하는 단계(210), CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석하는 단계(220) 및 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지하는 단계(230)를 포함한다.
- [0029] 단계(210)에서, 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출한다. 이때, 원시 CSI로부터 사용되지 않는 DC 서브캐리어를 제외한 데이터 서브캐리어를 수집하고, 수집된 데이

터 서버캐리어의 진폭과 위상 응답을 활용하여 사용자의 모션을 감지하기 위한 CSI 특성을 추출한다. 비디오 트래픽으로부터 특성을 추출은 비디오 트래픽의 패킷 길이 분포(Packet Length Distribution; PLD) 및 대역폭 안정성 특성(Bandwidth stability feature)을 포함하는 2차원 특성 벡터를 분석함으로써 혼합 트래픽으로부터 비디오 트래픽을 식별하여 특성을 추출한다.

- [0030] 단계(220)에서, CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석한다.
- [0031] 단계(230)에서, CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지한다.
- [0032] 몰래 카메라 탐지 알고리즘을 통해 비디오 트래픽의 패킷 길이 분포(PLD)를 분석하여, 패킷 길이 분포가 발견되면 소스와 대상의 MAC 주소를 반환한다. 발견된 패킷 길이 분포에 관한 후보 몰래 카메라들이 사용자를 기록하고 있는지 여부를 확인한 후, 소스 MAC 주소와 대상 MAC 주소 중에서 신호 강도가 가장 높은 송신기를 찾아 CSI 추출을 위해 저장한다. 이후, 후보 몰래 카메라의 패킷을 스니핑하고 비트 전송률을 계산하며, 추출된 CSI 및 계산된 비트 전송률을 분석하여 몰래 카메라의 가용성을 탐지한다.
- [0034] 도 3은 본 발명의 일 실시예에 따른 몰래 카메라 탐지 시스템의 구성을 나타내는 도면이다.
- [0035] 도 3에 도시한 바와 같이, 몰래 카메라 탐지 시스템은 특성 추출부(310), 모션 분류부(320) 및 몰래 카메라 탐지 알고리즘 수행부(330)로 이루어진 프로세서(300), 메모리(301), 네트워크 인터페이스(302)를 포함하여 구성될 수 있다.
- [0036] 메모리(301)는 OS(operating system)와 몰래 카메라 탐지 서비스 루틴에 해당되는 명령어를 포함하는 프로그램이 저장될 수 있다. 몰래 카메라 탐지 서비스는 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 통해 사용자 의도에 최대한 적합한 몰래 카메라 탐지 결과를 제공할 수 있다. 도 2를 통해 설명한 몰래 카메라 탐지 시스템에서 수행되는 단계들은 메모리(301)에 저장된 프로그램에 의해 실행될 수 있다. 예를 들어, 메모리(301)는 하드디스크, SSD, SD 카드 및 기타 저장매체일 수 있다.
- [0037] 네트워크 인터페이스(302)는 몰래 카메라 탐지 서비스를 이용하는 사용자 단말들과의 통신을 위해 몰래 카메라 탐지 시스템을 네트워크에 결합할 수 있다.
- [0038] 프로세서(300)는 메모리(301)에 저장된 프로그램의 명령어에 따라 처리하는 장치로서, CPU 등의 마이크로프로세서가 포함될 수 있다. 프로세서(300)의 세부 구성은 다음과 같다.
- [0039] 프로세서(300)는 특성 추출부(310), 모션 분류부(320) 및 몰래 카메라 탐지 알고리즘 수행부(330)를 포함한다.
- [0040] 특성 추출부(310)는 스마트 단말을 통해 사용자 모션으로부터 획득한 CSI 및 비디오 트래픽으로부터 특성을 추출한다. 이때, 원시 CSI로부터 사용되지 않는 DC 서버캐리어를 제외한 데이터 서버캐리어를 수집하고, 수집된 데이터 서버캐리어의 진폭과 위상 응답을 활용하여 사용자의 모션을 감지하기 위한 CSI 특성을 추출한다. 비디오 트래픽으로부터 특성을 추출은 비디오 트래픽의 패킷 길이 분포(Packet Length Distribution; PLD) 및 대역폭 안정성 특성(Bandwidth stability feature)을 포함하는 2차원 특성 벡터를 분석함으로써 혼합 트래픽으로부터 비디오 트래픽을 식별하여 특성을 추출한다.
- [0041] 모션 분류부(320)는 CSI 및 비디오 트래픽으로부터 추출된 특성에 대해 제어 차트를 사용하여 정적 및 동적 조건을 분류하여 사용자 모션을 감지하고, 사용자 모션 동안 CSI 및 비디오 비트 전송률에 대하여 타임스탬프에 기초한 변동 사항을 분석한다.
- [0042] 몰래 카메라 탐지 알고리즘 수행부(330)는 CSI 및 비디오 비트 전송률의 변동 사항에 대해 몰래 카메라 탐지 알고리즘을 적용하여 사용자 모션 동안의 변동 사항 간의 상관관계를 확인함으로써 몰래 카메라를 탐지한다.
- [0043] 몰래 카메라 탐지 알고리즘을 통해 비디오 트래픽의 패킷 길이 분포(PLD)를 분석하여, 패킷 길이 분포가 발견되면 소스와 대상의 MAC 주소를 반환한다. 발견된 패킷 길이 분포에 관한 후보 몰래 카메라들이 사용자를 기록하고 있는지 여부를 확인한 후, 소스 MAC 주소와 대상 MAC 주소 중에서 신호 강도가 가장 높은 송신기를 찾아 CSI 추출을 위해 저장한다. 이후, 후보 몰래 카메라의 패킷을 스니핑하고 비트 전송률을 계산하며, 추출된 CSI 및 계산된 비트 전송률을 분석하여 몰래 카메라의 가용성을 탐지한다. 이한, 도 4 내지 도 8을 참조하여 본 발명에



서 제안하는 몰래 카메라 탐지 방법 및 시스템에 관하여 더욱 상세히 설명한다.

먼저, CSI에서 특성 추출에 관하여 설명한다. 본 발명의 실시예에 따른 몰래 카메라 탐지 시스템(이하, SpyCamDetector)의 수신기에 수신된 원시 CSI는 파일럿과 사용되지 않는 DC 서브캐리어를 포함하는 64개의 서브캐리어로 구성될 수 있다. 여기서 원치 않는 서브캐리어를 걸러내고 나머지 데이터 서브캐리어(예를 들어, 48개)를 수집한다. 원시 CSI 값은 다음과 같이 나타낼 수 있다:

$$H = [H_1, H_2, \dots, H_i, \dots, H_N]^T, i \in [1, 48], \quad (1)$$

여기서 N은 서브 캐리어 수이다.  $H_i$  서브캐리어는 다음과 같이 정의할 수 있다:

$$H_i = |H_i|e^{j\sin\{\angle H_i\}}, \quad (2)$$

여기서  $|H_i|$ 와  $\angle H_i$ 는 각각 i번째 서브캐리어의 진폭과 위상 응답을 나타낸다. 진폭 [18], 위상 [19] 또는 두 파라미터[11]를 모두 활용하여 목표 영역에서 사용자의 모션을 감지하기 위해 다양한 접근법을 적용할 수 있다. 연산 부담을 줄이기 위해 진폭 구성 요소에서 CSI 특성을 추출하여 모션을 감지하면 된다. 이렇게 하려면 수신된 패킷에 대하여 길이 n의 윈도우 W를 슬라이드하여 각 열의 피어슨(Pearson) 상관[18]을 계산한다. 이에 따라 각 열의 패킷 하나와 나머지 패킷(즉, n-1) 간의 상관 관계가 계산된다. 상관 결과는  $\times$  행렬 형태로 저장된다. 행렬은 n의 크기에 의해 추가로 정규화되고 고유 벡터는 정규화된 상관 행렬에서 계산된다. 마지막으로 CSI 특성은 다음과 같이 고유 벡터와 분리된다:

$$CSI_{feature} = \max(eigenvector). \quad (3)$$

예를 들어, 정적 케이스(즉, 환경 내 모션이 없음)의 경우 고유값은 1과 같거나 매우 가깝다. 반대로, 모션이 환경에서 포착됨에 따라 1 아래에서 급격히 변동하기 시작한다.

다음으로 비디오 트래픽 특성 추출에 관하여 설명한다.

최신 WiFi 카메라는 H.264 [13] 압축 기술을 사용한다. 이 압축 기술은 장면 변경 없이 작은 크기의 데이터 패킷을 사용하여 데이터 크기를 최소화한다. 그러나 카메라가 모니터링 영역에서 모션을 관찰하면 전체 크기 및 작은 크기의 패킷이 모두 전송된다. 카메라 트래픽은 다음과 같은 특성을 포함하는 2차원 특성 벡터 [4]를 분석함으로써 혼합 트래픽(예를 들어, 노트북, IPTV, 스마트 단말 등)으로부터 식별된다: (1) 일시적 패킷 길이 분포(Packet Length Distribution; PLD) 특성: H.264 압축의 결과로 트래픽이 폴사이즈 및 소형 패킷으로 구성되어 있으며 이는 다른 장치의 트래픽과 구별된다. 이 특성은 패킷 수 n에 대해 CDF를 사용하여 추출된다. (2) 대역폭 안정성 특성: 카메라 트래픽이 다른 장치에 비해 상대적으로 안정적이다. 이 특성은 각 흐름의 순간 대역폭의 표준 편차로 계산된다. 카메라 흐름이 식별된 후 비트 전송률은 전송된 패킷의 페이로드 부분에서 계산된다.

다음으로, CSI 및 비디오 트래픽에서 추출한 특성에 대한 정적 및 동적 케이스를 분류하기 위해 제어 차트 방법을 사용한다 [16].

과거 데이터를 기반으로 세 개의 라인을 확인할 수 있다. 중심 라인은 과거 데이터의 평균 라인이고, 제어 라인, 즉 제어 상한(Upper Control Limit; UCL) 및 제어 하한(Lower Control Limit; LCL)이 있다 [16]. 데이터가 UCL 또는 LCL을 초과하면 특이치로 취급될 수 있다. 여기서 제어 차트 방법은 비트 전송률과 CSI 동작 탐지에 모두 사용된다. 두 특성은 모두 정적 상태에서 몇 초 동안 기록된다. 사용자가 이동을 시작하면 동작 감지로 예상되는 특이치가 발생한다.

마지막으로, 몰래 카메라 탐지(SpyCamDetector) 알고리즘을 수행한다.

도 4는 본 발명의 일 실시예에 따른 몰래 카메라 탐지 알고리즘을 나타내는 도면이다.

몰래 카메라 탐지 알고리즘은 몰래 카메라 탐지를 위한 이벤트 흐름을 설명한다. 알고리즘의 흐름은 다음과 같이 요약된다. 먼저, 스마트 단말의 WiFi를 모니터링 모드로 전환하고 패킷 길이 분포(PLD)를 검사한다. [4]에 설명된 형식에 따라 카메라의 PLD가 발견되면 소스(다시 말해, 카메라)와 대상(AP)의 MAC 주소를 반환한다. 대상 위치에서 여러 대의 카메라를 사용할 수 있으므로 각 카메라를 검사하여 감시된 영역에 사용자를 기록하고

있는지 여부를 확인한다. 라인(2)에서, 소스 MAC와 대상 MAC 중에서 신호 강도가 가장 높은 송신기를 찾는다. *MacBESTRSSI* 은 CSI 추출을 위해 저장된다. 라인(5)에서, 후보 몰래 카메라의 패킷을 스니핑하고 해당 카메라 패킷에서 비트 전송률을 계산한다. 라인(6)에서, *MacBESTRSSI* 에서 발신되는 신호의 CSI를 추출한다. 라인(7)에서, DetectRecoring() 서브루틴에 의해 두 특성(다시 말해, CSI 및 비트 전송률)을 분석하여 몰래 카메라의 가용성을 분석한다.

[0060] 도 5는 본 발명의 일 실시예에 따른 CSI 기능과 비트 레이트를 함께 사용한 카메라의 기록 여부 감지를 설명하기 위한 도면이다.

[0061] 본 발명의 일 실시예에 따른 각 카메라의 기록 감지는 도 5에 도시된 바와 같이, 시작 시 0초부터 5초까지 사용자는 정적이다. 이 기간 동안 CSI는 안정적이고 급격한 변동을 보이지 않는 반면, 비트 전송률은 카메라의 하드웨어 특징으로 인해 버스트를 가진다. 그럼에도 불구하고 실제 비트 전송률에 영향을 주지 않고 불필요한 버스트를 제거하기 위해 햄플(Hample) 필터를 사용하고 제어 차트를 사용하여 제어 한계(UCL 및 LCL)를 도출했다. 이후, 사용자가 5초에서 20초까지 모션을 시작하면 비트 전송률과 CSI 특성이 모두 그에 따라 변동한다. 비트 전송률 및 CSI 특성으로부터의 이러한 변화는 제어 차트 방법에 의해 특이치로 간주되고 여기서 기록을 감지할 수 있다. 마지막으로 사용자가 동작을 20초에서 25초까지 멈추면 CSI와 비트 전송률 특성이 다시 안정적으로 뒀을 확인할 수 있다.

[0062] 본 발명의 실시예에 따른 몰래 카메라 탐지 시스템의 성능을 확인하기 위하여 Nexmon의 오픈 소스 GitHub 저장소[12]를 사용하여 루팅된 Nexus-5 스마트 단말에 모니터링 특성을 구현했다. Nexmon은 Nexus-5의 bcm4339 Broadcom WiFi 칩 드라이버를 일부 수정하여 무선 트래픽으로부터 패킷을 스니핑할 수 있게 했다.

[0063] 본 발명의 실시예에 있어서, 카메라-AP에서 패킷을 감지하고 스마트 단말의 메모리 안에 PCAP 파일로 임시로 저장한다. 예를 들어, 몰래 카메라 탐지 시스템의 어플리케이션(SpyCamDetector)을 Android 어플리케이션으로 구현할 수 있다. 이 어플리케이션은 이러한 파일에서 비트 전송율 및 CSI 특성을 추출하여 몰래 카메라의 기록을 탐지한다.

[0064] 본 발명의 실시예에 따른 몰래 카메라 탐지 시스템의 성능을 확인하기 위한 실험 설정에서, 가해자가 방의 어느 곳이나 WiFi 카메라를 설치할 수 있다고 가정한다. 대상 영역이 완전히 가려져 있는 경우, 카메라는 예상치 못한 패키지에 놓여진다. 한 대의 카메라로 영역을 완전히 커버하지 않은 경우 가해자는 여러 대의 카메라를 사용할 수 있다. 카메라는 외부 메모리를 사용할 수 있지만 가해자는 관심 대상을 기록하기 위해 카메라를 상당히 오랫동안 보관할 수 있다. 가해자는 실시간으로 비디오에 액세스하여 카메라에 WiFi 연결이 필요하다. 또한 가해자는 몰래 카메라와 AP 사이에 합리적인 신호 강도(즉, 강한 또는 양호한 수준의 RSSI)를 갖도록 한다.

[0065] 동일 설정에서, 사용자는 호텔, 모텔, 에어비앤비 등 개인 대여 공간에서 몰래 카메라를 탐지하기 위해 설치된 카메라의 위치를 미리 알 필요는 없다. 문제 설정을 보다 사실적으로 만들기 위해 다양한 RF 기기(예를 들어, 노트북, 태블릿 및 스마트 단말 등)에서 주변 환경에 사용할 수 있는 충분한 무선 트래픽을 추가로 고려한다. 사용자는 루팅된 Nexus 5 스마트 단말 상에서 제한하는 몰래 카메라 탐지 시스템의 어플리케이션 SpyCamDetector를 실행한다. SpyCamDetector는 WiFi 네트워크에 연결하지 않고 DEATTI(2.4GHz) 및 VSTA(듀얼 밴드)라는 두 개의 무선 WiFi 카메라에서 무선 트래픽을 스니핑한다. 또한 각 카메라와 AP 사이의 RSSI 레벨을 강함( $RSSI \leq -50dBm$ ), 양호( $RSSI \leq -60dBm$ ), 불량( $RSSI \leq -70dBm$ )으로 분류한다. 또한 카메라-AP의 RSSI 레벨을 스니핑 장치에 대한 다양한 조합으로 분류했다. 본 발명에서는 패킷의 무선 탭 헤더에서 RSSI 정보를 수집하고 최대 RSSI 레벨을 가진 CSI 소스를 선택한다.

[0067] 도 6은 본 발명의 일 실시예에 따른 몰래 카메라 탐지 시스템의 성능을 종래기술들과 비교한 도면이다.

[0068] 도 6(a) 내지 도 6(c)는 가속도계 및 CSI 기능의 민감도 분석 결과를 나타내고, 도 6(d)는 제한하는 SpyCamDetector와 종래기술의 DeWiCam의 성능을 비교한 결과를 나타내고, 도 6(e) 및 도 6(f)는 다중 경로 환경에서 성능 평가 결과를 나타내는 도면이다.

[0069] 본 발명의 실시예에 따른 몰래 카메라 탐지 시스템의 성능을 종래기술들과 비교하면, 가속도계와 CSI 판독값을 측정하여 이 판독값이 걷기, 점프, 흔들기 및 정적 조건과 같은 사용자의 다양한 활동을 어떻게 반영하는지 확

인할 수 있다. 가속도계와 CSI 관독값에서 모두 20개의 데이터 샘플을 수집한다. 각 데이터 샘플 지속 시간은 10초 동안 기록되었다.

[0070] 도 6(a) 및 도 6(b)에는 점프, 걷기, 흔들기 및 정적의 네 가지 활동에 관한 가속도계( $m/s^2$  단위) 및 CSI(고유 특성)의 원시 관독값이 표시된다. 두 도면 모두 점프와 흔들기의 관독값이 정적 및 걷기보다 더 큰 변동을 보인다는 것을 보여주며, 이는 관독값이 활동 강도와 긍정적인 관계가 있음을 반영한다. 이를 통해 가속도계와 비교한 CSI가 활동을 반영하기에 신뢰할 수 있고 민감한 요소임을 확인할 수 있다.

[0071] 다양한 실내 크기의 효과. 다중 경로(즉, 소규모 페이딩)의 영향을 측정하기 위해 표 1과 같이 다양한 방 크기에 대한 SpyCamDetector의 성능을 평가했다.

[0072] <표 1>

| Room type     | restroom | small     | medium | large |
|---------------|----------|-----------|--------|-------|
| Dimension (m) | 2 × 2.5  | 3.5 × 3.5 | 4 × 5  | 8 × 8 |

[0073]

[0074] 각 실내 크기에 대해 탐지율을 표시하기 위해 50개의 데이터 샘플을 수집했다. 도 6(d)을 참조하면 SpyCamDetector의 탐지율이 나와 있다. 모든 설정의 평균 탐지율은 약 99%이다. 더 작은 실내에서 다중 경로 효과가 더 커지기 때문에 화장실에서 성능이 약간 저하되는 것을 볼 수 있다. 그러나 SpyCamDetector는 여전히 신뢰성이 있다. 도 6(f)는 수신기 작동 특성(Receiver Operator Characteristic; ROC)의 그림을 나타내고 도 6(d)과 유사한 추세를 보여준다. 본 발명의 실시예에 따르면 큰 방, 중간 방, 작은 방, 화장실의 ROC 곡선 아래 면적을 각각 99.16%, 98.11%, 98.28%, 94.4%로 기록한다.

[0076] 도 7은 본 발명의 일 실시예에 따른 카메라 AP와 스마트 단말 간의 서로 다른 RSSI 레벨에 대해 설명하기 위한 도면이다.

[0077] PNLoS 신호 강도와 노이즈의 영향에 있어서, SpyCamDetector에 대한 신호 강도의 영향을 측정하기 위해, 도 7과 같이 카메라-AP와 스마트 단말 사이의 RSSI 값의 다른 조합으로 SpyCamDetector의 성능을 측정한다. 카메라-AP 간 RSSI가 좋지 않은 것은 AP에 대한 신호 강도가 낮을 때(즉, 낮은 대역폭) 카메라를 설치하지 않았기 때문에, 카메라-AP 간 강력한 RSSI가 카메라-AP 간 RSSI보다 더 나은 결과를 보여주므로 카메라-AP 간 RSSI가 좋지 않은 것은 현실적인 설정이 아니기 때문에 카메라-AP 간 RSSI가 좋은 결과를 제공한다. 카메라-AP 사이에 고정된 RSSI로, 스마트 단말과 카메라 사이의 RSSI가 강하고, 양호하고, 불량한 동시에 스마트 단말과 AP 사이의 RSSI가 강하고, 양호하고, 불량한 위치를 찾는다. 표 2에 표시된 것처럼 가능한 조합은 9개라고 가정할 수 있다.

[0078] <표 2>

| Case | Link btn camera & smartphone | Link btn AP & smartphone | Practically possible |
|------|------------------------------|--------------------------|----------------------|
| 1    | Strong                       | Strong                   | ✓                    |
| 2    | Strong                       | Good                     | ✓                    |
| 3    | Strong                       | Poor                     | ×                    |
| 4    | Good                         | Strong                   | ✓                    |
| 5    | Good                         | Good                     | ✓                    |
| 6    | Good                         | Poor                     | ✓                    |
| 7    | Poor                         | Strong                   | ×                    |
| 8    | Poor                         | Good                     | ✓                    |
| 9    | Poor                         | Poor                     | ✓                    |

[0079]

[0080] 케이스 3과 케이스 7의 결과는 두 가지 경우 모두 물리적으로 불가능하기 때문에 생략했다. 예를 들어 케이스 3(AP-스마트 단말 링크 불량 및 카메라-스마트 단말 링크 강함)의 스마트 단말 위치는 스마트 단말 카메라가 강한 RSSI를 가지고 있기 때문에 찾을 수 없다. 케이스 7에도 이와 비슷한 원인을 갖는다.

[0081] 대상자와 주변 노이즈의 CSI 변동을 구분하기 위해 두 사람의 걷기 즉, 카메라에 대한 PLoS와 PNLoS의 걷기 일

정을 확인했다. PLoS 걷기 일정은 정적 10초, 도보 20초, 정적 10초 등으로 진행되었고, PNL0S 걷기 일정은 정적 10초, 10초 걷기를 40초간 주기적으로 수행하였다. 각 케이스 당 40초 간의 데이터 샘플 20개를 채취했다.

[0083] 도 8은 본 발명의 일 실시예에 따른 다양한 레벨의 신호 강도에서 SpyCamDetector의 성능 평가 결과를 나타내는 도면이다.

[0084] 도 8(a)는 다양한 RSSI 레벨에서의 탐지율을 나타내고, 도 8(b)는 서로 다른 RSSI 레벨에서 잘못된 정보 비율을 나타내는 도면이다.

[0085] 도 8(a)에 도시된 바와 같이, 스마트 단말(스니핑 장치)과 카메라와 AP 사이의 연결이 강하거나 양호할 때 탐지율은 100%이다(케이스 1, 2, 4, 5). 케이스 6과 8의 경우, SpyCamDetector는 카메라-스마트 단말 또는 AP-스마트 단말 중 하나에서 우수한 RSSI 링크를 지능적으로 선택하여 100% 탐지율을 달성할 수 있다. 케이스 9의 경우 탐지율은 카메라 소스에서 85%로, AP 소스에서 87.5%로 약간 저하된다. 도 8(b)는 PNL0S의 효과를 보여준다. 이러한 거짓 경보(즉, 위양성률[false positive rate])는 PLoS가 정지 상태이지만 PNL0S가 걸었을 때 트리거되었다. 카메라-스마트 단말 또는 AP-스마트 단말 중 하나의 링크가 포함된 케이스는 강력한 RSSI(예를 들어, 케이스 1, 2, 4)를 가지며 0%의 잘못된 위양성률을 보여준다. 그러나, 양호한 RSSI는 2.7%(예를 들어, 케이스 6)와 3%(예를 들어, 케이스 8)의 위양성률을 나타내며, 반면 불량 RSSI는 9.8%(케이스 6)와 10.7%(케이스 8)의 거짓 정보 비율을 나타낸다. CSI 소스의 양호한 RSSI 레벨에서는 이러한 효과는 무시할 수 있었다. RSSI가 불량한 RSSI를 가지는 경우(예를 들어, 케이스 9), 거짓 정보 비율은 15%(카메라 소스) 및 12.7%(AP 소스)이다. 요약하자면, 그 결과는 스마트 단말을 사용자 가까이에서 두면 신뢰할 수 있는 성능을 얻을 수 있다는 것을 분명히 보여준다.

[0087] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 컨트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPA(field programmable array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0088] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0089] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은



기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

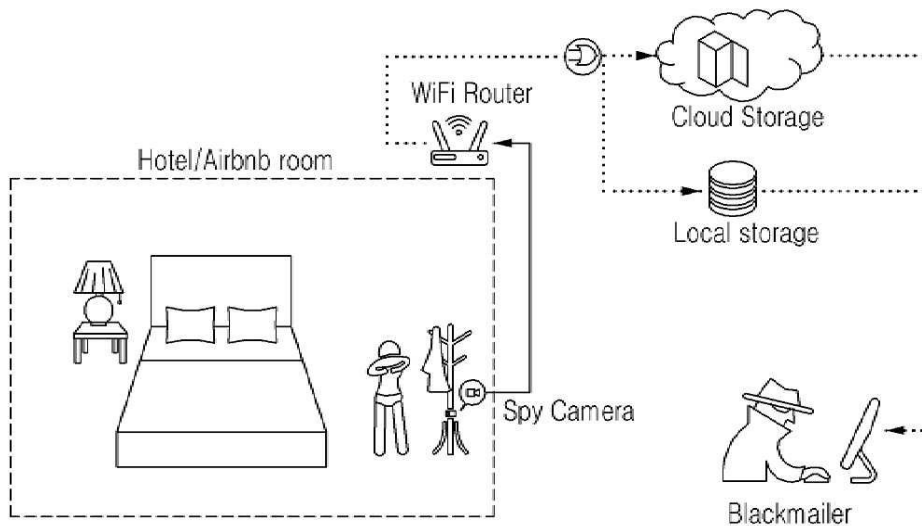
- [0090] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0091] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.
- [0093] <참고 문헌>
- [0094] [1] Amazon. 2012. Wireless Camera RF Detector with Built-in Flashlight. Retrieved Nov 03, 2020 from <https://tinyurl.com/y3hn87sz>
- [0095] [2] Amazon. 2019. Anti Spy RF Signal Detector. Retrieved Nov 03, 2020 from <https://tinyurl.com/y5wjsbgp>
- [0096] [3] A. Carter. 2019. Study says guests are finding hidden cameras inside rental properties, hotel rooms. Retrieved Oct 23, 2020 from <https://tinyurl.com/y7ukmt9r>
- [0097] [4] Yushi Cheng, Xiaoyu Ji, Tianyang Lu, and Wenyan Xu. 2019. On detecting hidden wireless cameras: A traffic pattern-based approach. IEEE Transactions on Mobile Computing 19, 4 (2019), 907-921.
- [0098] [5] Matthew S Gast. 2013. 802.11 ac: a survival guide: Wi-Fi at gigabit and beyond. " O'Reilly Media, Inc.".
- [0099] [6] Brent Lagesse, Kevin Wu, Jaynie Shorb, and Zealous Zhu. 2018. Detecting spies in iot systems using cyber-physical correlation. In 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 185-190.
- [0100] [7] Tian Liu, Ziyu Liu, Jun Huang, Rui Tan, and Zhen Tan. 2018. Detecting wireless spy cameras via stimulating and probing. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services. 243-255.
- [0101] [8] Tian Liu, Ziyu Liu, Jun Huang, Rui Tan, and Zhen Tan. 2018. Detecting wireless spy cameras via stimulating and probing. In Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services. 243-255.
- [0102] [9] Yongsan Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi sensing with channel state information: A survey. ACM Computing Surveys (CSUR) 52, 3 (2019), 1-36.
- [0103] [10] C. Mengxiao. 2017. Hidden camera found in H&M store's changing room. Retrieved Oct 21, 2020 from <https://tinyurl.com/y7psdcxr>
- [0104] [11] Kun Qian, Chenshu Wu, Zheng Yang, Yunhao Liu, Fugui He, and Tianzhang Xing. 2018. Enabling contactless detection of moving humans with dynamic speeds using CSI. ACM Transactions on Embedded Computing Systems (TECS) 17, 2 (2018), 1-18.
- [0105] [12] Matthias Schulz, Daniel Wegemer, and Matthias Hollick. 2016. Using NexMon, the C-based WiFi firmware modification framework. In Proceedings of the 9<sup>th</sup> ACM Conference on Security & Privacy in Wireless and Mobile Networks. 213-215.
- [0106] [13] Heiko Schwarz, Detlev Marpe, and Thomas Wiegand. 2007. Overview of the scalable video coding extension of the H. 264/AVC standard. IEEE Transactions on circuits and systems for video technology 17, 9 (2007), 1103-1120.



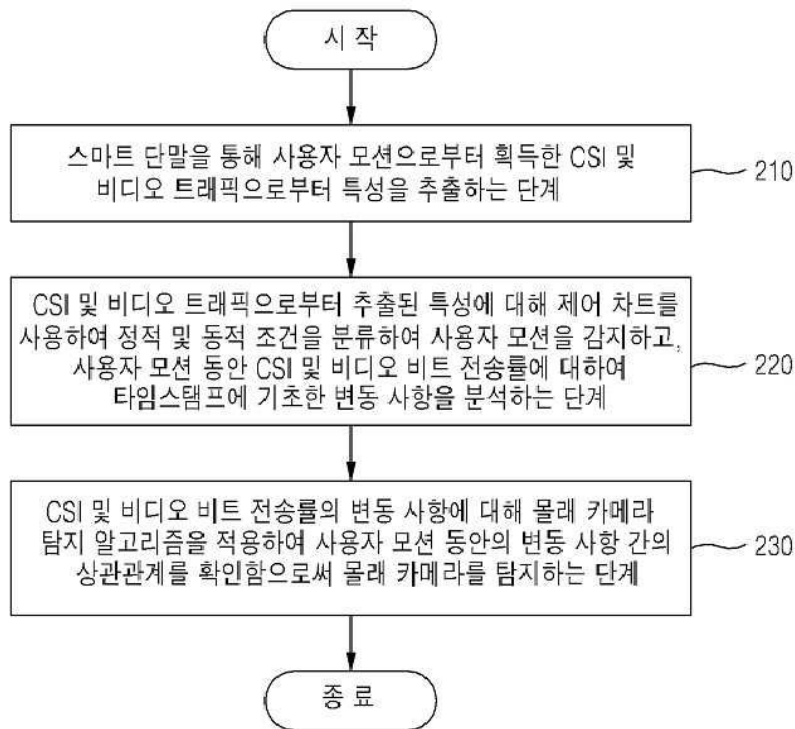
- [0107] [14] Signal. [n.d.]. The Signal Jammer. Retrieved July 17, 2020 from <https://tinyurl.com/y2hlznnw>
- [0108] [15] N. Smith. 2019. South Korean woman commits suicide after doctor filmed her using spycam, reports say. Retrieved Oct 18, 2020 from <https://tinyurl.com/y52x98pk>
- [0109] [16] NR Tague. 2004. The Quality Toolbox, ASQ (American Society for Quality). Quality Press.
- [0110] [17] Kevin Wu and Brent Lagesse. 2019. Do You See What I See? Detecting Hidden Streaming Cameras Through Similarity of Simultaneous Observation. In 2019 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, 1-10.
- [0111] [18] Jiang Xiao, Kaishun Wu, Youwen Yi, Lu Wang, and Lionel M Ni. 2012. Fimd: Finegrained device-free motion detection. In 2012 IEEE 18th International conference on parallel and distributed systems. IEEE, 229-235.
- [0112] [19] Jie Xiong and Kyle Jamieson. 2013. Arraytrack: A fine-grained indoor location system. In Presented as part of the 10th USENIX Symposium on Networked Systems Design and Implementation NSDI 13. 71-84.

## 도면

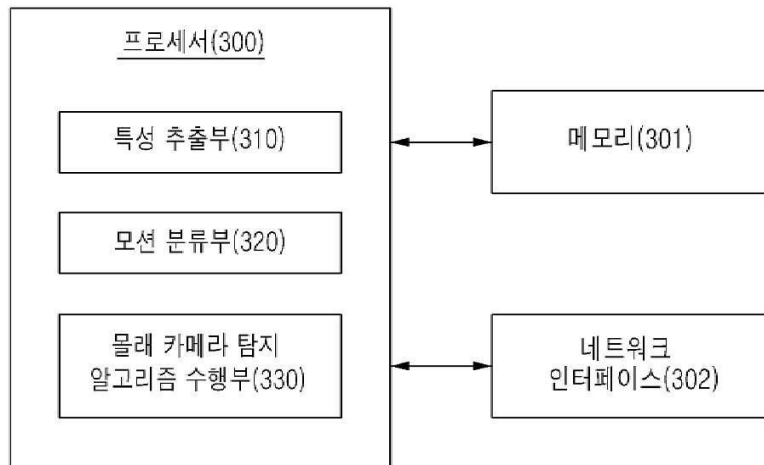
### 도면1



도면2



도면3



도면4

---

Algorithm : PSEUDOCODE FOR SPYCAMDETECTOR

---

Output: SpyCamList []

```

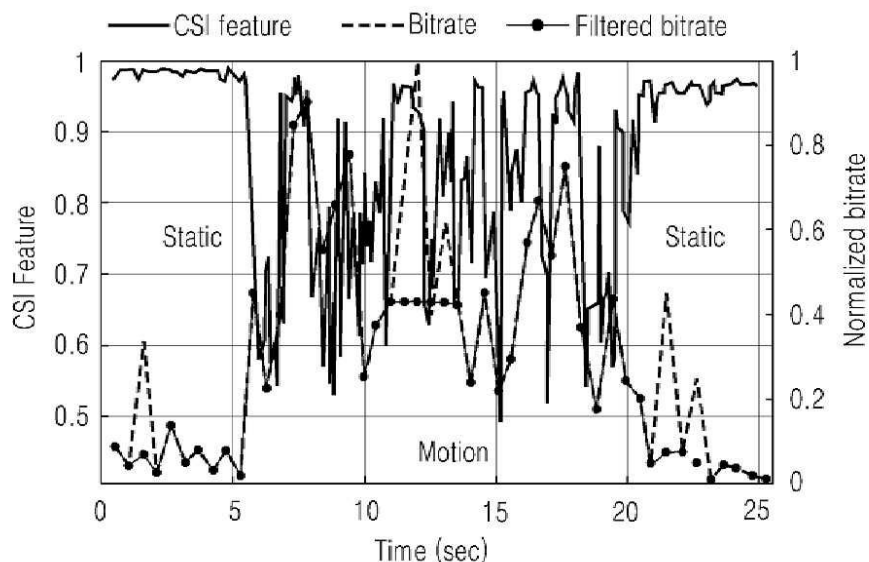
1: begin
2:   Find candidate spy cameras MacCAM[] by inspecting the Packet Legth
   Distribution
3:   Extract the MAC address of the source with maximu RSSI either from the
   camera or AP: MacBESTRSSI ;
4:   foreach i ∈ MacCAM[] do
5:     Sniff the PacketsCAM from MacCAM[i] ;
6:     Extract the CSIBESTRSSI CSI data from the MacBESTRSSI ;
       // Detect the motion by correlating the fluctuation
       from bitrate and csi
7:     isSpyCam ← DetectRecording(PacketsCAM,CsiBESTRSSI) ;
8:     if is SpyCam == true then
9:       Add MacCAM[i] to the SpyCamList[] ;
10:   return SpyCamList[];

11:Subroutine DetectRecording(PacketsCAM,CsiBESTRSSI):
12:   Calculate the motion detection with timestamp motionBITRATE[] from
   bitrate got from PacketsCAM ;
13:   Calculate the motion detection with timestamp motionCSI[] from
   CsiBESTRSSI ;
14:   Dectct the spy camera isSpyCam by correlating the motion detections
   from bitrate and CSI based on timestamp;
15:   return isSpyCam;

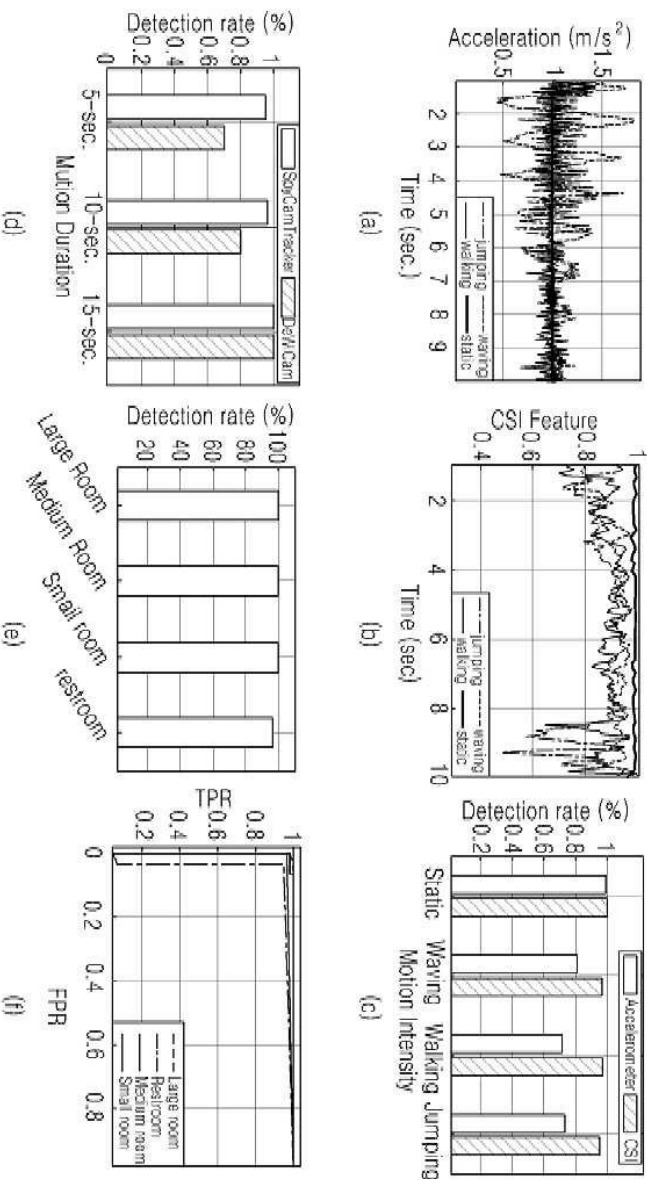
```

---

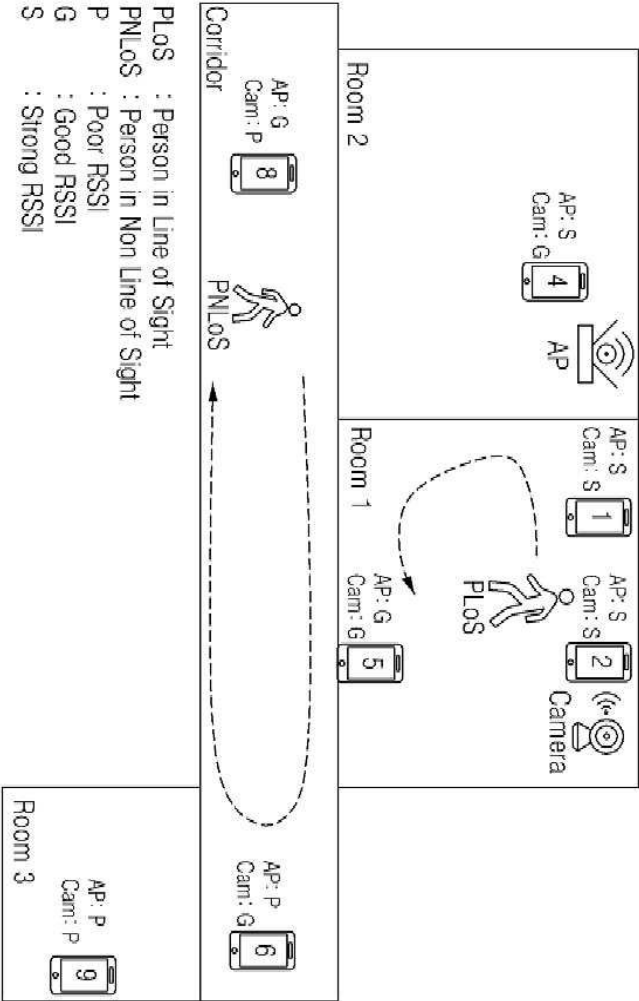
도면5



도면6



도면7





도면8

