

**(19) 대한민국특허청(KR)**
(12) 공개특허공보(A)**(11) 공개번호** 10-2024-0177509
(43) 공개일자 2024년12월27일

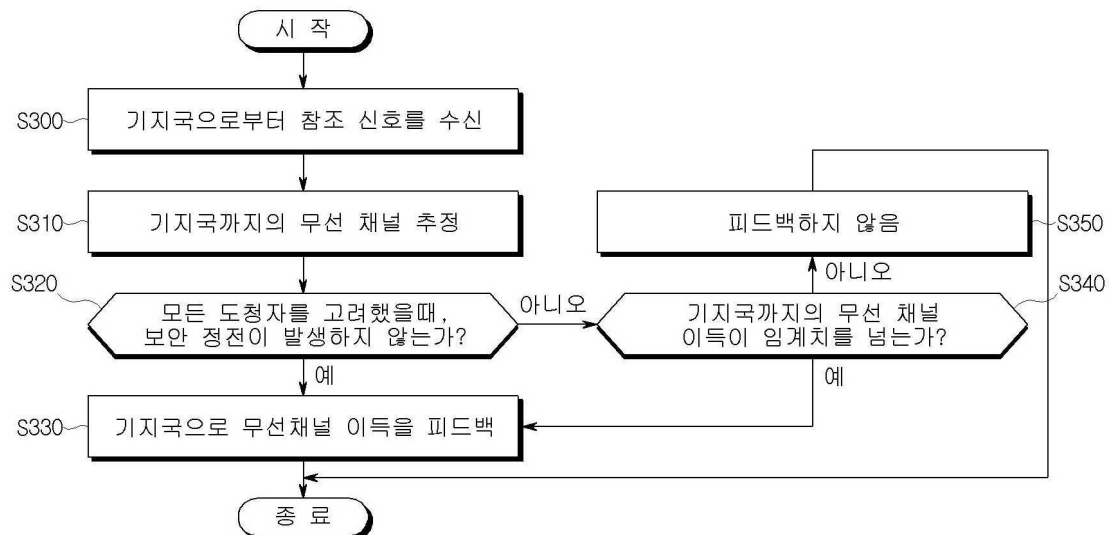
(51) 국제특허분류(Int. Cl.)
H04W 12/121 (2021.01) H04L 25/02 (2006.01)
H04L 9/40 (2022.01) H04W 72/542 (2023.01)
(52) CPC특허분류
H04W 12/121 (2021.01)
H04L 25/0202 (2013.01)
(21) 출원번호 10-2023-0078961
(22) 출원일자 2023년06월20일
심사청구일자 2023년06월20일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
고려대학교 세종산학협력단
세종특별자치시 조치원읍 세종로 2511 (고려대학교세종캠퍼스내)
(72) 발명자
정방철
대전광역시 서구 관저동로90번길 15, 103동 602호
(관저동, 관저리슈빌)
유희정
세종특별자치시 조치원읍 세종로 2511, 전자맞정
보공학과
(뒷면에 계속)
(74) 대리인
특허법인 정안

전체 청구항 수 : 총 10 항

(54) 발명의 명칭 무선 통신 시스템에서의 사용자 단말 피드백 방법**(57) 요약**

본 발명은 사용자 단말에서 보안 정전을 고려하여 피드백 여부를 결정하는 것으로, 사용자 단말의 무선 채널 이득 전송 방법은, 상기 기지국으로부터 참조 신호를 수신하는 단계, 수신한 상기 참조 신호에 기초하여 상기 기지국과의 무선 채널 이득을 추정하는 단계, 상기 사용자 단말이 상기 기지국으로 메시지를 전송할 시에 전송하는 메시지가 도착되는 보안 정전이 발생하는 지를 판단하는 제1 판단 단계 및 상기 제1 판단 단계에서 보안 정전이 발생하지 않는다고 판단하는 경우, 상기 기지국으로 상기 무선 채널 이득을 전송하는 단계를 포함할 수 있다.

대표도 - 도3

(52) CPC특허분류

H04L 63/1441 (2013.01)

H04L 63/16 (2013.01)

H04W 72/542 (2023.01)

(72) 발명자

손웅

대전광역시 동구 우암로277번길 33-1 (가양동)

이기훈

대전광역시 유성구 배울2로 78, 606동 402호 (관평동, 대덕테크노밸리6단지아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711137685
과제번호	2021R1A4A1032580
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	기초연구사업-기초연구실 지원사업
연구과제명	협력 지능형 엣지를 위한 테라헤르츠 무선 시스템 연구실
기 여 율	1/2
과제수행기관명	충남대학교 산학협력단
연구기간	2021.06.01 ~ 2024.02.29

이 발명을 지원한 국가연구개발사업

과제고유번호	1711160328
과제번호	2022-0-00704-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	6G핵심기술개발
연구과제명	초고속 이동체 지원을 위한 3D-NET 핵심 기술 개발
기 여 율	1/2
과제수행기관명	아주대학교산학협력단
연구기간	2022.04.01 ~ 2025.12.31

명세서

청구범위

청구항 1

기지국과 무선 네트워크로 연결된 사용자 단말의 무선 채널 이득 전송 방법에 있어서,
 상기 기지국으로부터 참조 신호를 수신하는 단계;
 수신한 상기 참조 신호에 기초하여 상기 기지국과의 무선 채널 이득을 추정하는 단계;
 상기 사용자 단말이 상기 기지국으로 메시지를 전송할 시에 전송하는 메시지가 도착되는 보안 정전이 발생하는
 지를 판단하는 제1 판단 단계;
 상기 제1 판단 단계에서 보안 정전이 발생하지 않는다고 판단하는 경우, 상기 기지국으로 상기 무선 채널 이득
 을 전송하는 단계를 포함하는, 사용자 단말의 무선 채널 이득 전송 방법.

청구항 2

제1항에 있어서,
 상기 제1 판단 단계에서 보안 정전이 발생한다고 판단하는 경우, 상기 무선 채널 이득이 미리 설정된 임계치를
 넘는지 판단하는 제2 판단 단계; 및
 상기 제2 판단 단계에서 상기 무선 채널 이득이 상기 임계치를 넘었다고 판단하는 경우에 상기 기지국으로 상기
 무선 채널 이득을 전송하고, 무선 채널 이득이 상기 임계치보다 작다고 판단하는 경우에 상기 기지국으로 상기
 무선 채널 이득을 전송하지 않는 단계를 포함하는, 사용자 단말의 무선 채널 이득 전송 방법.

청구항 3

제1항 또는 제2항에 있어서,
 상기 제1 판단 단계는,
 상기 기지국과 상기 무선 네트워크로 연결된 상기 사용자 단말을 제외한 적어도 하나의 다른 사용자 단말들을
 잠재적 도청자 단말로 설정하고, 상기 잠재적 도청자 단말에 의하여 도착되지 않고 전송할 수 있는 데이터 전송
 른 보안 전송률을 계산하는 단계; 및
 계산된 상기 보안 전송률을 목표 보안 전송률과 비교하여 보안 정전 확률을 계산하는 단계를 포함하는, 사용자
 단말의 무선 채널 이득 전송 방법.

청구항 4

제3항에 있어서,
 상기 보안 전송률은 상기 기지국과의 무선 채널 이득과 상기 사용자 단말과 상기 적어도 하나의 다른 사용자 단
 말 간의 무선 채널 이득에 기초하여 결정되는, 사용자 단말의 무선 채널 이득 전송 방법.

청구항 5

제2항에 있어서,
 상기 사용자 단말이 복수의 안테나를 구비하고, 상기 복수의 안테나 각각에 대해 무선 채널 이득을 추정하고,

상기 복수의 안테나 각각에 대해 추정된 무선 채널 이득 중에서 가장 큰 무선 채널 이득을 기초로 상기 제1 판단 단계 및 상기 제2 판단 단계를 수행하는, 사용자 단말의 무선 채널 이득 전송 방법.

청구항 6

기지국과 무선 네트워크로 연결된 사용자 단말에 있어서,

상기 기지국으로부터 전송되는 참조 신호를 수신하는 안테나; 및

수신한 상기 참조 신호에 기초하여 상기 기지국과의 무선 채널 이득을 추정하고, 상기 사용자 단말이 상기 기지국으로 메시지를 전송할 시에 전송하는 메시지가 도착되는 보안 정전이 발생하는 지를 판단(이하 제1 판단)하고, 상기 제1 판단에서 보안 정전이 발생하지 않는다고 판단하는 경우, 상기 기지국으로 상기 무선 채널 이득을 전송하도록 제어하는 프로세서를 포함하는, 사용자 단말.

청구항 7

제6항에 있어서,

상기 프로세서는,

상기 제1 판단에서 보안 정전이 발생한다고 판단하는 경우, 상기 무선 채널 이득이 미리 설정된 임계치를 넘는 지 판단(이하 제2 판단)하고,

상기 제2 판단에서 상기 무선 채널 이득이 상기 임계치를 넘었다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을 전송하고, 무선 채널 이득이 상기 임계치보다 작다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을 전송하지 않도록 결정하는, 사용자 단말.

청구항 8

제6항 또는 제7항에 있어서,

상기 프로세서는,

상기 기지국과 상기 무선 네트워크로 연결된 상기 사용자 단말을 제외한 적어도 하나의 다른 사용자 단말들을 잠재적 도착자 단말로 설정하고, 상기 잠재적 도착자 단말에 의하여 도착되지 않고 전송할 수 있는 데이터 전송률인 보안 전송률을 계산하고,

계산된 상기 보안 전송률을 목표 보안 전송률과 비교하여 보안 정전 확률을 계산하여 보안 정전이 발생하는 지를 판단하는, 사용자 단말.

청구항 9

제8항에 있어서,

상기 프로세서는,

상기 기지국과의 무선 채널 이득과 상기 사용자 단말과 상기 적어도 하나의 다른 사용자 단말 간의 무선 채널 이득에 기초하여 상기 보안 전송률을 계산하는, 사용자 단말.

청구항 10

제7항에 있어서,

복수의 안테나를 구비하고,

상기 프로세서는,

상기 복수의 안테나 각각에 대해 무선 채널 이득을 추정하고, 상기 복수의 안테나 각각에 대해 추정된 무선 채널 이득 중에서 가장 큰 무선 채널 이득을 기초로 상기 제1 판단 및 상기 제2 판단을 수행하는, 사용자 단말.

발명의 설명

기술 분야

[0001] 아래의 실시예들은 무선 통신 시스템에서의 사용자 단말의 피드백 방법에 관한 것이다.

배경 기술

[0003] 보안 통신(secure communication)은 학계와 산업에서 지금까지 꾸준히 중요하게 고려되고 있다. 특히 무선 통신 시스템에서는 송신기가 특정 수신기로 인코딩된 메시지를 전송할 때, 주변에 존재하는 통신 기기들은 인코딩된 메시지를 쉽게 수신할 수 있으며, 인코딩 방법을 알고 있다면, 디코딩이 가능하기 때문에 수신한 메시지의 내용을 매우 쉽게 파악할 수 있다.

[0004] 이렇게 원하지 않는 통신 기기가 전송한 메시지를 엿듣는 것을 도청(eavesdropping)이라 하며, 이러한 도청 문제를 해결하기 위해 연구자들은 물리계층 보안(physical-layer security, PLS) 성능 향상을 위한 연구들을 수행하고 있다.

[0005] 한편, 도청자가 존재하는 환경을 고려하기 위한 도청자 모델은, 큰 범주에서 수동적 도청자(passive eavesdropper), 능동적 도청자(active eavesdropper), 잠재 도청자(potential eavesdropper)로 나눌 수 있다. 수동적 도청자의 경우, 도청자는 별다른 동작을 수행하지 않으면서 도청만을 실시하므로, 그 존재를 알기 어렵고 또한 대응할 방안도 용이하지 않다. 능동적 도청자의 경우, 도청 뿐만 아니라 과일릿 신호 오염, 재밍, 거짓정보 피드백 등의 다양한 방법으로 공인 링크의 통신을 열화시키기 위한 동작을 수행하기도 하므로, 공인 기기들은 능동적 도청자의 존재 여부를 수동적 도청자 대비 쉽게 알 수 있고 관련된 대응 방안도 연구가 많이 되고 있다. 반면, 잠재 도청자의 경우, 동일 셀 내 존재하는 스케줄링을 받지 못한 공인 단말이 스케줄링 받은 다른 공인 단말의 잠재 도청자일 수 있거나 혹은 인접 네트워크에 존재하는 다른 공인 단말이 잠재 도청자일 수 있다. 따라서 기지국이 잠재 도청자까지의 무선 채널에 대한 정보를 알 수 있는 독특한 도청자이고, 이들에 대한 대응 방안도 도출될 필요가 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은, 잠재적 도청자가 존재하는 상향링크 무선 네트워크에서의 물리계층 보안 성능 향상을 위한 단말의 피드백 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0009] 본 발명의 일실시예에 따르면, 기지국과 무선 네트워크로 연결된 사용자 단말의 무선 채널 이득 전송 방법은 상기 기지국으로부터 참조 신호를 수신하는 단계, 수신한 상기 참조 신호에 기초하여 상기 기지국과의 무선 채널 이득을 추정하는 단계, 상기 사용자 단말이 상기 기지국으로 메시지를 전송할 시에 전송하는 메시지가 도청되는 보안 정전이 발생하는 지를 판단하는 제1 판단 단계, 상기 제1 판단 단계에서 보안 정전이 발생하지 않는다고 판단하는 경우, 상기 기지국으로 상기 무선 채널 이득을 전송하는 단계를 포함할 수 있다.

[0010] 본 발명의 일실시예에 따르면, 상기 방법은 추가적으로 상기 제1 판단 단계에서 보안 정전이 발생한다고 판단하는 경우, 상기 무선 채널 이득이 미리 설정된 임계치를 넘는지 판단하는 제2 판단 단계 및 상기 제2 판단 단계에서 상기 무선 채널 이득이 상기 임계치를 넘었다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을

전송하고, 무선 채널 이득이 상기 임계치보다 작다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을 전송하지 않는 단계를 포함할 수 있다.

[0011] 본 발명의 일실시예에 따르면, 상기 제1 판단 단계는 상기 기지국과 상기 무선 네트워크로 연결된 상기 사용자 단말을 제외한 적어도 하나의 다른 사용자 단말들을 잠재적 도청자 단말로 설정하고, 상기 잠재적 도청자 단말에 의하여 도청되지 않고 전송할 수 있는 데이터 전송률인 보안 전송률을 계산하는 단계 및 계산된 상기 보안 전송률을 목표 보안 전송률과 비교하여 보안 정전 확률을 계산하는 단계를 포함할 수 있다.

[0012] 본 발명의 일실시예에 따르면, 상기 보안 전송률은 상기 기지국과의 무선 채널 이득과 상기 사용자 단말과 상기 적어도 하나의 다른 사용자 단말 간의 무선 채널 이득에 기초하여 결정될 수 있다.

[0013] 본 발명의 일실시예에 따르면, 상기 사용자 단말이 복수의 안테나를 구비하는 경우, 상기 방법은 상기 복수의 안테나 각각에 대해 무선 채널 이득을 추정하고, 상기 복수의 안테나 각각에 대해 추정된 무선 채널 이득 중에서 가장 큰 무선 채널 이득을 기초로 상기 제1 판단 단계 및 상기 제2 판단 단계를 수행할 수 있다.

[0014] 본 발명의 일실시예에 따르면, 기지국과 무선 네트워크로 연결된 사용자 단말은 상기 기지국으로부터 전송되는 참조 신호를 수신하는 안테나 및 수신한 상기 참조 신호에 기초하여 상기 기지국과의 무선 채널 이득을 추정하고, 상기 사용자 단말이 상기 기지국으로 메시지를 전송할 시에 전송하는 메시지가 도청되는 보안 정전이 발생하는 지를 판단(이하 제1 판단)하고, 상기 제1 판단에서 보안 정전이 발생하지 않는다고 판단하는 경우, 상기 기지국으로 상기 무선 채널 이득을 전송하도록 제어하는 프로세서를 포함할 수 있다.

[0015] 본 발명의 일실시예에 따르면, 상기 프로세서는 상기 제1 판단에서 보안 정전이 발생한다고 판단하는 경우, 상기 무선 채널 이득이 미리 설정된 임계치를 넘는지 판단(이하 제2 판단)하고, 상기 제2 판단에서 상기 무선 채널 이득이 상기 임계치를 넘었다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을 전송하고, 무선 채널 이득이 상기 임계치보다 작다고 판단하는 경우에 상기 기지국으로 상기 무선 채널 이득을 전송하지 않도록 결정할 수 있다.

발명의 효과

[0017] 본 발명에서 제안하는 피드백 방법에 의하여 잠재 도청자가 존재하는 무선 네트워크에서의 물리계층 보안 성능(보안 정전 확률, 유효 보안 처리량)이 향상될 수 있다.

[0018] 또한, 본 발명에서 제안하는 피드백 방법은 페이딩(fading)이 있는 무선 네트워크에서 상향링크 전송을 위한 사용자 피드백과 사용자 스케줄링이 수행되는 환경에 보안 정전 확률을 감소시키거나 또는 유효 보안 전송률을 향상시켜 물리 계층 보안 성능을 향상시킬 수 있다.

도면의 간단한 설명

[0020] 도 1은 일실시예에 따른 잠재 도청자의 도청 시나리오를 나타내는 도면이다.

도 2는 일실시예에 따른 사용자 단말의 구성을 나타내는 도면이다.

도 3은 일실시예에 따른 사용자 단말이 피드백을 수행할 지를 결정하는 방법을 나타내는 흐름도이다.

도 4는 일실시예에 따른 유효 보안 처리량을 설명하기 위한 프레임 구조를 나타내는 도면이다.

도 5는 일실시예에 따른 본 발명에서 제시하는 피드백 방법을 적용한 경우, 기존 기회적 피드백(Opportunistic Feedback, OF) 방법 그리고 기준 지표인 이상적 하한(Ideal Lower-Bound, ILB) 방법 간의 보안 정전 확률(secrecy outage probability) 성능을 비교한 표를 나타내는 도면이다.

도 6은 일실시예에 따른 본 발명에서 제시하는 피드백 방법을 적용한 경우, 기존 기회적 피드백(Opportunistic Feedback, OF) 방법, 그리고 기준 지표인 이상적 하한(Ideal Lower-Bound, ILB) 방법 간의 유효 보안 처리량(effective secrecy throughput) 성능을 비교한 결과와 각 방법에 따른 피드백 확률을 비교한 결과를 나타내는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.
- [0022] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.
- [0023] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1구성요소는 제2구성요소로 명명될 수 있고, 유사하게 제2구성요소는 제1구성요소로도 명명될 수 있다.
- [0024] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.
- [0025] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [0026] 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 설명된 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.
- [0027] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미가 있다.
- [0028] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0029] 이하의 설명에서 동일한 식별 기호는 동일한 구성을 의미하며, 불필요한 중복적인 설명 및 공지 기술에 대한 설명은 생략하기로 한다.
- [0030] 본 발명의 실시 예에서 '통신' 및 '통신망'은 동일한 의미로 사용될 수 있다. 상기 두 용어들은, 파일을 사용자 단말, 다른 사용자들의 단말 및 다운로드 서버 사이에서 송수신할 수 있는 유무선의 근거리 및 광역 데이터 송수신망을 의미한다.
- [0031] 이하, 첨부한 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다.
- [0032] 도 1은 일실시예에 따른 잠재 도청자의 도청 시나리오를 나타내는 도면이다.
- [0033] 도 1을 참조하면, 다양한 실시예에 따라, 무선 네트워크에는 모든 사용자를 관리하는 기지국(200)과 공인 사용자 단말들(100, 220) 및 잠재적 도청자 단말들(210, 211)이 존재할 수 있다. 여기서, 잠재적 도청자 단말들(210, 211)은 인접한 다른 셀에 존재하거나 기지국으로부터 스케줄링(scheduling)을 통하여 자원 할당을 받지 못하여 전송 기회를 받지 못한 공인 사용자 단말일 수 있다. 잠재적 도청자 단말들(210, 211)은 다른 공인 사용자 단말들(100, 220)이 상향링크로 전송하는 메시지를 엿들을 수 있는 단말일 수 있다. 이 외에도 수동적 도청자 단말 또는 능동적 도청자 단말들이 있을 수 있으나, 본 실시 예에서는 수동적 도청자 단말 또는 능동적 도청자 단말에 대하여는 고려하지 않는다.
- [0034] 다양한 실시예에 따라, 한편 잠재적 도청자 단말들(210, 211)은 공인 사용자 단말이기 때문에 통상적으로는 도청을 시도하지 않을 수 있으나, 도청을 시도할 가능성도 있다. 이때, 잠재적 도청자 단말들(210, 211) 각각이 도청을 시도하는 확률(eavesdropping probability)(P_E)은 0과 1 사이의 값을 가질 수 있다. 이처럼, 특정 시도

확률에 따라 잠재적 도청자 단말들이 도청을 시도하는 실시 예를 무작위 도청 전략(random eavesdropping, RE)이라고 정의할 수 있다.

[0035] 다양한 실시예에 따라, 잠재적 도청자 단말들(210, 211)이 도청을 시도하는 확률(P_E)이 1이면, 항상 도청을 시도하는 것이므로 완전 도청 전략(full eavesdropping, FE)이라고 칭할 수 있다. 여기서, 잠재적 도청자 단말들(210, 211)의 사용자들은 서로 공모하여 도청을 시도하는 것이 아니므로 비공모(non-colluding) 도청자들이라고 할 수 있고, 서로 도청한 정보를 공유하지 않는다고 가정할 수 있다.

[0036] 다양한 실시예에 따라, 무선 네트워크에서 기지국(200)에 N_{MS} 개의 사용자 단말이 연결되어 있고, 스케줄링을 통해 전송 기회를 획득한 사용자 단말(100)이 i ($i \in \{1, 2, \dots, N_{MS}\}$)번째 사용자 단말인 경우, i 번째 사용자 단말로부터 기지국(200)까지의 무선 채널 계수는 $h_{B,i} \sim CN(0, \sigma_B^2)$ 의 분포를 따를 수 있다. 실제로는 복수의 사용자 단말이 스케줄링을 통해 전송 기회를 획득할 수 있으나, 본 실시예에서는 i 번째 사용자 단말만 고려하고, 나머지 사용자 단말의 동작은 i 번째 사용자 단말과 동일할 수 있다.

[0037] 그리고 N_E 개의 사용자 단말이 스케줄링을 통해 전송 기회를 획득하지 못한 잠재적 도청자 단말의 수인 경우, i 번째 사용자 단말로부터 $j \in \{1, 2, \dots, N_E\}$ 번째 잠재적 도청자 단말까지의 무선 채널 계수는 $h_{j,i} \sim CN(0, \sigma_E^2)$ 의 분포를 따를 수 있다.

[0038] 여기서 CN은 복소 가우시안 분포를 나타내며, σ_B^2 과 σ_E^2 은 각 무선 채널의 분산 값을 나타낸다. 일 실시예에 따라, $\sigma_B^2 = \sigma_E^2 = 1$ 로 가정할 수 있다. 또한, 한 번의 메시지 전송 중 채널이 변하지 않는 준정적 Rayleigh 페이딩 환경을 가정할 수 있다.

[0039] 다양한 실시예에 따라, 모든 공인 사용자 단말(100, 220, 210, 211)은 기지국(200)이 전송하는 파일럿 신호(pilot signal)에 대한 정보를 서로 알고 있으며, 이에 따라, 스케줄링을 통해 자원을 할당 받은 공인 사용자 단말(100, 220)은 스케줄링을 통해 자원을 할당 받지 못한 잠재적 도청자 단말(210, 211)의 무선 채널 계수를 알 수 있다.

[0040] 다양한 실시예에 따라, i 번째 사용자 단말이 기지국(200)으로 메시지를 전송할 때, 잠재적 도청자 단말에 의하여 도청되지 않고 메시지를 전송할 수 있는 보안 전송률(achievable secrecy-rate)은 다음 [수학식 1]로, 전송하는 메시지가 도청될 확률을 나타내는 보안 정전 확률(secrecy outage probability)은 다음 [수학식 2]로 각각 계산할 수 있다.

수학식 1

$$R_{sec,i} = \max \left[\log_2 \left(\frac{1 + |h_{B,i}|^2 \rho}{1 + \max_{j \in M_E} |h_{j,i}|^2 \rho} \right), 0 \right]$$

[0041]

수학식 2

$$P_{out,i} = \Pr(R_{sec,i}(M_E, \sigma_B^2, \sigma_E^2, \rho) < R_o)$$

[0042]

[0043]

여기서, M_E 는 N_E 개의 잠재적 도청자 단말 중 도청을 시도하는 도청자 단말의 집합(set)이고, $\rho(=\frac{P}{N_0})$ 는 송신 신호-대-잡음비(signal-to-noise ratio, SNR)이고, $h_{B,i}$ 는 i 번째 사용자 단말로부터 기지국까지의 무선 채널 계수이고, $h_{j,i}$ 는 i 번째 사용자 단말로부터 j 번째 도청자 단말까지의 무선 채널 계수이고, P 는 i 번째 사용자 단말의 송신 전력[W]이고, N_0 는 잡음 분산(noise variance) [W]이고, R_o [bps/Hz]는 보안 정전의 기준이 되는 목표 보안 전송률(target secrecy rate)로, 보안 전송률이 목표 보안 전송률보다 작은 경우, 보안 정전(secrecy outage)이 발생할 수 있다. 여기서, R_o 는 무선 네트워크에 따라 가변일 수 있다.

[0044]

도 2는 일실시예에 따른 사용자 단말의 구성을 나타내는 도면이다.

[0045]

도 2를 참조하면, 사용자 단말(100)은 프로세서(110), 입출력 인터페이스 모듈(120) 및 메모리(130)를 포함한다.

[0046]

사용자 단말(100)에 포함된 프로세서(110), 입출력 인터페이스 모듈(120) 및 메모리(130)는 상호 연결되어 있으며, 상호 데이터를 전송하는 것이 가능하다.

[0047]

다양한 실시 예에 따르면, 프로세서(110)는 메모리(130)에 저장된 프로그램들 또는 명령들을 실행시킬 수 있다. 여기서, 메모리(130)에는 사용자 단말(100)을 동작시키기 위한 동작프로그램(예컨대, OS)이 저장될 수 있다.

[0048]

다양한 실시 예에 따르면, 프로세서(110)는 사용자 단말(100)에 대한 정보를 관리하기 위한 프로그램을 실행시킬 수 있다.

[0049]

다양한 실시 예에 따르면, 프로세서(110)는 사용자 단말(100)의 동작을 관리하기 위한 프로그램을 실행시킬 수 있다.

[0050]

다양한 실시 예에 따르면, 프로세서(110)는 입출력 인터페이스 모듈(120)의 동작을 관리하기 위한 프로그램을 실행시킬 수 있다.

[0051]

다양한 실시예에 따라, 프로세서(110)는 입출력 인터페이스 모듈(120)을 통해 무선으로 연결된 기지국이 전송한 참조 신호를 획득할 수 있다. 여기서, 참조 신호는 간단히 RS(Reference Signal) 또는 적용되는 표준에 따라 파일럿 신호(pilot signal)로 지칭될 수도 있다. 또한, 기지국은 다중 입출력(Multiple Input Multiple Output, MIMO) 시스템일 수 있으나, 기지국 시스템이 이에 한정되는 것은 아니다.

[0052]

다양한 실시예에 따라, 프로세서(110)는 획득한 참조 신호를 기초로 다중 입출력 시스템에 포함된 안테나 각각에 대하여 채널을 추정할 수 있다. 그리고 가장 큰 무선 채널 이득을 가지는 안테나의 채널을 기초로 이하의 동작을 수행할 수 있다.

[0053]

다양한 실시예에 따라, 각 사용자 단말들은 모든 도청자 단말들까지의 무선 채널 이득에 대한 정보는 알 수 있으나, 도청을 시도하는 도청자 단말의 수에 대한 정보는 알지 못할 때, 즉, 잠재적 도청자 시나리오를 고려할 때, 잠재적 도청자에 의한 도청을 방지하기 위하여 프로세서(110)는 피드백을 진행할 수 있다. 여기서, 피드백은, 사용자 단말이 기지국으로부터 상향링크 전송 기회를 얻기 위해 사용자 단말 기지국간 무선 채널 이득(channel gain) 정보를 기지국으로 전송하는 것이다.

[0054]

프로세서(110)는 첫번째 단계와 두번째 단계의 2가지 조건에 기초하여 피드백을 전송할 것인지를 결정할 수 있으나, 첫번째 단계는 필수적으로 수행되나 두번째 단계는 부가적으로 수행될 수 있다.

[0055]

i) 첫번째 단계

- [0056] 다양한 실시예에 따라, 첫번째 단계는 모든 잠재적 도청자 단말이 도청을 시도한다는 가정 하에 보정 정전이 발생하지 않을 때, 자식인 피드백할 수 있는 가장 큰 값으로 피드백을 실시하여 기지국이 자신을 스케줄링할 수 있도록 유도하는 것이다.
- [0057] 프로세서(110)는 [수학식 1]을 이용하여 사용자 단말에서 기지국으로 데이터를 전송할 때의 보안 전송률을 계산할 수 있고, [수학식 2]를 이용하여 보안 정전 확률을 계산할 수 있다. 첫번째 단계의 계산에서는 N_E 개의 잠재적 도청자 단말 모두가 도청자 단말의 집합(M_E)에 포함되는 것으로 가정하여 보안 전송률 및 보안 정전 확률을 계산할 수 있다.
- [0058] 수학식 1에 의하여 계산된 보안 전송률이 목표 보안 전송률(R_o) 이상, 즉 $R_{sec,i}(|M_E|, \sigma_B^2, \sigma_E^2, \rho) \geq R_o$ 를 만족할 때, 프로세서(110)는 모든 도청자 단말의 도청여부는 알지 못하지만 모든 도청자 단말들이 도청을 시도한다고 가정하여 보안 정전이 발생하지 않았다고 결정할 수 있다.
- [0059] 다양한 실시예에 따라, 보안 정전이 발생하지 않았다고 결정한 경우, 프로세서(110)는 기지국이 사용자 단말을 스케줄링 할 수 있도록 유도하기 위하여 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)할 수 있다. 여기서, 스케줄링은 기지국이 사용자 단말들이 기지국으로 피드백한 무선 채널 이득 값들을 보고, 적어도 하나의 사용자 단말을 선택하여 상향링크 전송 기회를 주는 것을 의미한다. 또한, 사용자 단말의 무선 채널 이득 정보는 사용자 단말이 피드백 할 수 있는 가장 큰 값일 수 있으나, 사용자 단말의 무선 채널 이득 정보가 이에 한정되는 것은 아니다.
- [0060] ii) 두번째 단계
- [0061] 다양한 실시예에 따라, 프로세서(110)는 사용자 단말로부터 기지국까지의 무선 채널 계수를 기초로 기지국까지의 무선 채널 이득을 결정할 수 있다.
- [0062] 다양한 실시예에 따라, 계산한 보안 전송률이 목표 보안 전송률 미만이면, 프로세서(110)는 모든 도청자 단말의 도청여부는 알지 못하지만 모든 도청자 단말들이 도청을 시도한다고 가정하여 보안 정전이 발생했다고 결정할 수 있다.
- [0063] 다양한 실시예에 따라, 보안 정전이 발생했다고 결정한 경우, 기지국까지의 무선 채널 이득이 미리 설정된 임계치(ζ) 이상(사용자 단말이 i 번째 사용자 단말일 경우, $|h_{B,i}|^2 \geq \zeta$ 를 만족할 때)이면, 프로세서(110)는 기지국이 사용자 단말을 스케줄링 할 수 있도록 유도하기 위하여 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)할 수 있다. 여기서, 임계치는 무선 네트워크에 따라 변할 수 있다.
- [0064] 다양한 실시예에 따라, 보안 정전이 발생했다고 결정한 경우, 기지국까지의 무선 채널 이득이 미리 설정된 임계치 미만이면, 프로세서(110)는 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)하지 않을 수 있다.
- [0065] 다양한 실시예에 따라, 피드백을 수신한 기지국은 프로세서(110)가 입출력 인터페이스 모듈(120)을 통해 전송한 사용자 단말의 무선 채널 이득 정보를 기초로 사용자 단말에게 상향 링크 전송 기회를 부여할 수 있다.
- [0066] 입출력 인터페이스 모듈(120)은 네트워크를 통하여 외부 장치(예컨대, 기지국, 다른 사용자 단말 등)와 연결될 수 있다.
- [0067] 입출력 인터페이스 모듈(120)은 외부 장치로부터 데이터를 획득할 수 있다.
- [0068] 입출력 인터페이스 모듈(120)은 외부 장치로 데이터를 전송할 수 있다.
- [0069] 입출력 인터페이스 모듈(120)은 피드백 여부를 디스플레이 할 수 있다.
- [0070] 입출력 인터페이스 모듈(120)은 사용자의 입력을 획득할 수 있다.
- [0071] 입출력 인터페이스 모듈(120)은 사용자 단말과 통신적으로 연결될 별도의 장치일 수 있다.
- [0072] 입출력 인터페이스 모듈(120)은 외부 장치와 연결되기 위한 포트(예컨대, USB 포트)를 포함할 수 있다.
- [0073] 입출력 인터페이스 모듈(120)은 모니터, 터치스크린, 마우스, 전자펜, 마이크로폰, 키보드, 스피커, 이어폰, 헤드폰 또는 터치패드를 포함할 수 있다.

- [0074] 메모리(130)는 입출력 인터페이스 모듈(120)을 통해 획득한 데이터를 저장할 수 있다.
- [0075] 메모리(130)는 입출력 인터페이스 모듈(120)을 통해 전송한 데이터를 저장할 수 있다.
- [0076] 메모리(130)는 프로세서(110)가 계산한 보안 전송률을 저장할 수 있다.
- [0077] 메모리(130)는 프로세서(110)가 결정한 무선 채널 이득을 저장할 수 있다.
- [0078] 메모리(130)는 피드백 전송 여부를 저장할 수 있다.
- [0079] 도 3은 일실시예에 따른 사용자 단말이 피드백을 수행할 지를 결정하는 방법을 나타내는 흐름도이다.
- [0080] 도 3을 참조하면, 기지국과 통신적으로 연결된 사용자 단말이 수행하는 피드백 방법은, 사용자 단말이 기지국이 전송한 참조 신호를 수신하는 단계(S300), 사용자 단말이 수신한 참조 신호에 기초하여 기지국까지의 무선 채널을 추정하는 단계(S310), 모든 잠재적 도청자를 도청자로 고려하였을 때, 보안 정전이 발생하는 지 판단하는 단계(S320), 보안 정전이 발생하면 기지국까지의 무선채널 이득이 미리 설정한 임계치를 넘는지 판단하는 단계(S340), 모든 잠재적 도청자를 고려하였을 때 보안 정전이 발생하지 않거나 또는 무선채널 이득이 미리 설정한 임계치를 넘으면 사용자 단말이 기지국으로 무선 채널 이득 정보를 전송(피드백)하는 단계(S330) 및 그 외의 경우에 사용자 단말이 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)하지 않는 단계(S350)을 포함할 수 있다.
- [0081] 단계 S300에서, 사용자 단말은 통신적으로 연결된 기지국이 전송한 참조 신호를 획득할 수 있다.
- [0082] 단계 S310에서, 사용자 단말은 획득한 참조 신호를 기초로 다중 입출력 시스템에 포함된 수신 안테나 각각에 대하여 기지국과의 채널을 추정할 수 있다.
- [0083] 단계 S320에서, 사용자 단말은 수학적 식 1 및 수학적 식 2를 이용하여 사용자 단말에서 기지국으로 데이터를 전송할 때의 보안 정전이 발생하는 지를 판단할 수 있다. 이때, 잠재적 도청자 단말 모두가 도청자 단말의 집합(M_E)에 포함되는 것으로 가정하여 보안 전송률 및 보안 정전 확률을 계산할 수 있다.
- [0084] 단계 S320에서, 사용자 단말은 수학적 식 1에 따라 계산한 보안 전송률과 목표 보안 전송률(R_o)을 비교하여 보안 정전 확률을 수학적 식 2에 따라 계산할 수 있다. 여기서, 목표 보안 전송률은 무선 네트워크에 따라 변할 수 있다.
- [0085] 단계 S320에서, 계산한 보안 전송률이 목표 보안 전송률(R_o) 이상, 즉 $R_{sec,i}(|M_E|, \sigma_B^2, \sigma_E^2, \rho) \geq R_o$ 를 만족할 때, 사용자 단말은 모든 도청자 단말의 도청여부는 알지 못하지만 모든 도청자 단말들이 도청을 시도한다는 가정하에도 보안 정전이 발생하지 않았다고 결정할 수 있다. 그리고 계산한 보안 전송률이 목표 보안 전송률(R_o) 미만이면 보안 정전이 발생하였다고 결정할 수 있다.
- [0086] 사용자 단말이 단계 S320에서 보안 정전이 발생하지 않았다고 결정한 경우, 단계 S330으로 진행하여 사용자 단말은 기지국이 사용자 단말을 스케줄링 할 수 있도록 유도하기 위하여 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)할 수 있다.
- [0087] 사용자 단말이 단계 S320에서 보안 정전이 발생했다고 결정한 경우, 단계 S340으로 진행하여 사용자 단말은 기지국까지의 무선 채널 이득과 미리 설정된 임계치를 비교할 수 있다.
- [0088] 단계 S340에서, 기지국까지의 무선 채널 이득이 미리 설정된 임계치 이상(사용자 단말이 i 번째 사용자 단말일 경우, $|h_{B,i}|^2 \geq \zeta$ 를 만족할 때)이면, 사용자 단말은 기지국이 사용자 단말을 스케줄링 할 수 있도록 유도하기 위하여 단계 330으로 진행하여 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)할 수 있다. 여기서, 임계치는 무선 네트워크에 따라 변할 수 있다.
- [0089] 사용자 단말이 단계 S340에서 기지국까지의 무선 채널 이득이 미리 설정된 임계치(ζ) 미만이라고 판단하면, 사용자 단말은 기지국으로 사용자 단말의 무선 채널 이득 정보를 전송(피드백)하지 않을 수 있다.
- [0090] 이와 같이 도 3에 도시된 흐름도에 따르면, 사용자 단말은 모든 잠재적 도청자를 고려하더라도 보안 정전이 발생하지 않거나, 무선 채널 이득이 미리 설정된 임계치 이상이어서, 그 결과 수신 전력에 따라 기지국은 수신할

수 있지만 도청자 단말은 송신한 데이터를 수신하기 어려운 경우에만 피드백을 전송하여 스케줄링을 통해 자원을 할당 받을 수 있다. 즉, 보안 정전 가능성이 현저히 낮은 상황에서만 피드백을 전송하여 데이터를 전송할 자원을 할당받음으로써 보안 정전 가능성을 현저히 낮출 수 있다.

[0091] 도 4는 일실시예에 따른 유효 보안 처리량을 설명하기 위한 프레임 구조를 나타내는 도면이다.

[0092] 도 4의 프레임 구조를 참조하면, 매 상향 링크 전송 프레임은 $|M_{MS}|$ 개의 피드백 전송을 위한 타임 슬롯이 있고, T 시간의 상향 링크 전송을 위한 시간슬롯이 있다. 여기서, 피드백 전송을 위한 타임 슬롯의 수는 매 상향 링크 전송에서 변경될 수 있다.

[0093] 일 실시예에 따라, 사용자 단말은 다음 [수학식 3]을 이용하여 주어진 무선 네트워크에서의 유효 보안 처리량(effective secrecy throughput)을 계산할 수 있다.

수학식 3

$$\Psi(P_{out}) = \frac{R_o T (1 - P_{out})}{E[|M_{MS}|] \beta T + T} = \frac{R_o (1 - P_{out})}{N_{MS} P_{MS} \beta + 1}$$

[0094]

[0095] 여기서, P_{out} 은 무선 네트워크에 본 발명의 피드백 방법을 적용하였을 때, 주어진 무선 네트워크에서 달성할 수 있는 보안 정전 확률로, [수학식 2]로부터 도출될 수 있고, $E[\cdot]$ 는 평균(expectation)을 의미하고, P_{MS} 는 피드백 방법에 따른 개별 사용자의 피드백 확률이고, βT 는 사용자 단말이 피드백 시 점유 사용하는 시간슬롯의 길이인데, β 는 1보다 작은 실수값일 수 있다. T 는 상향링크 전송을 위한 시간슬롯의 길이이고, R_o [bps/Hz]는 보안 정전의 기준이 되는 목표 보안 전송률(target secrecy rate)이다.

[0096] 수학식 3을 참조하면, 유효 보안 처리량은 매 상향 링크 전송 프레임 시간동안 보안 정전 없이 전송될 수 있는 비트의 수를 나타낼 수 있다.

[0097] 도 5는 일실시예에 따른 본 발명에서 제시하는 피드백 방법을 적용한 경우, 기존 기회적 피드백(Opportunistic Feedback, OF) 방법 그리고 기준 지표인 이상적 하한(Ideal Lower-Bound, ILB) 방법 간의 보안 정전 확률(secrecy outage probability) 성능을 비교한 표를 나타내는 도면이다.

[0098] 도 5를 참조하면, 그래프(500)의 x축은 공인 사용자 단말의 수가 1개부터 30개 인 것을 나타내고, y축은 보안 정전 확률을 나타낸다.

[0099] 다양한 실시예에 따라, 잠재 도청자 단말 수는 4개, 도청 확률은 0.5, 기지국과 공인 사용자 단말간 무선 채널과 공인 사용자 단말과 잠재 도청자 단말간 무선 채널의 분산은 모두 1로 설정되고, 기지국의 송신 SNR은 10[dB], 기지국과 공인 사용자까지의 채널 목표 보안 전송률은 0.5[bps/Hz]로 설정된 모의 환경에서 도 5의 Proposed로 표시된 본 발명에 따른 보안 정전 확률(510)은 Conventional OF로 표시된 기존 기회적 피드백(OF) 방법의 보안 정전 확률(520)대비 낮은 것을 알 수 있다.

[0100] 다양한 실시예에 따라, 도 5의 그래프를 참조하면, 본 발명에 따른 보안 정전 확률(510)은 공인 사용자 단말의 수가 증가할수록 기존 기회적 피드백(OF) 방법의 보안 정전 확률(520) 대비 더 낮아지고, ILB로 표시된 이상적 하한 방법의 보안 정전 확률(530) 보다는 커지는 것을 알 수 있다.

[0101] 도 6은 일실시예에 따른 본 발명에서 제시하는 피드백 방법을 적용한 경우, 기존 기회적 피드백(Opportunistic Feedback, OF) 방법, 그리고 기준 지표인 이상적 하한(Ideal Lower-Bound, ILB) 방법 간의 유효 보안 처리량(effective secrecy throughput) 성능을 비교한 결과와 각 방법에 따른 피드백 확률을 비교한 결과를 나타내는 도면이다.

[0102] 도 6을 참조하면, 다양한 실시예에 따라, 그래프(600)의 x축은 공인 사용자 단말의 수가 1개부터 30개 인 것을 나타내고, 그래프의 좌측 y축은 유효 보안 처리량을 나타내고, 우측 y축은 피드백 확률을 나타낸다.

[0103] 다양한 실시예에 따라, 잠재 도청자 단말 수는 4개, 도청 확률은 0.5, 기지국과 공인 사용자 단말간 무선 채널과 공인 사용자 단말과 잠재 도청자 단말간 무선 채널의 분산은 모두 1로 설정되고, 기지국의 송신 SNR은 10[dB], 기지국과 공인 사용자까지의 채널 목표 보안 전송률은 0.5[bps/Hz]이고, 도 4에서 사용자 단말이 피드백 시 점유 사용하는 시간슬롯의 길이는 0.05로 설정된 모의 환경에서 도 6에 Proposed로 표시된 본 발명에 따른 유효 보안 처리량(610)은 Conventional OF로 표시된 기존 기회적 피드백(OF) 방법의 유효 보안 처리량(620) 및 ILB로 표시된 이상적 하한(Ideal Lower-Bound) 방법의 유효 보안 처리량(630) 대비 높은 것을 알 수 있다.

[0104] 다양한 실시예에 따라, 도 6을 참조하면, 본 발명에 따른 유효 보안 처리량(610)은 공인 사용자 단말의 수가 증가할수록 기존 기회적 피드백(OF) 방법의 유효 보안 처리량(620) 및 이상적 하한(Ideal Lower-Bound, ILB) 방법의 유효 보안 처리량(630) 대비 더 높아지는 것을 알 수 있다. 따라서, 공인 사용자 단말의 수가 증가할수록 본 발명에 따른 유효 보안 처리량(610)은 기존 기회적 피드백(OF) 방법의 유효 보안 처리량(620) 및 이상적 하한(Ideal Lower-Bound, ILB) 방법의 유효 보안 처리량(630) 대비 더 높아질 것으로 예측할 수 있다.

[0105] 다양한 실시예에 따라, 도 6을 참조하면, 본 발명에 따른 피드백 가능성(640)은 공인 사용자 단말의 수가 증가할수록 기존 기회적 피드백(OF) 방법의 피드백 가능성(650)보다 더 높아지는 것을 알 수 있다. 따라서, 공인 사용자 단말의 수가 매우 많은 경우를 가정하면 본 발명에 따른 피드백 가능성(640)은 기존 기회적 피드백(OF) 방법의 피드백 가능성(650)보다 더 높아질 것으로 예측할 수 있다.

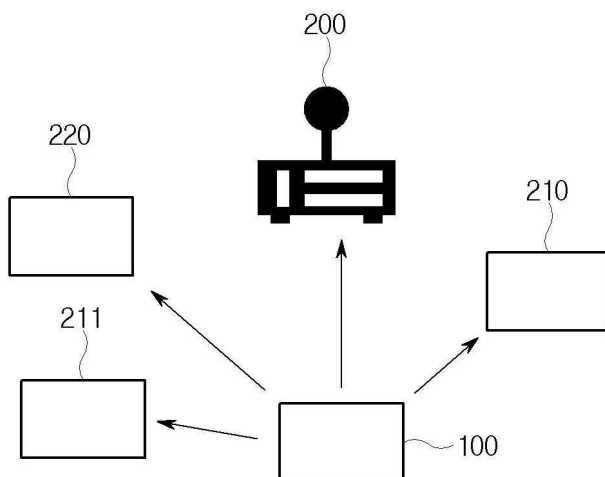
[0106] 본 개시는 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 개시의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

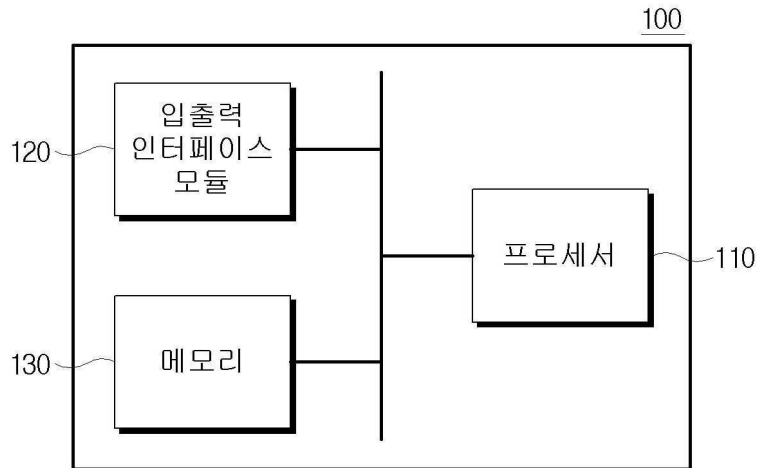
[0107] 100, 220... 공인 사용자 단말
210, 211... 잠재적 도청자 단말
200... 기지국

도면

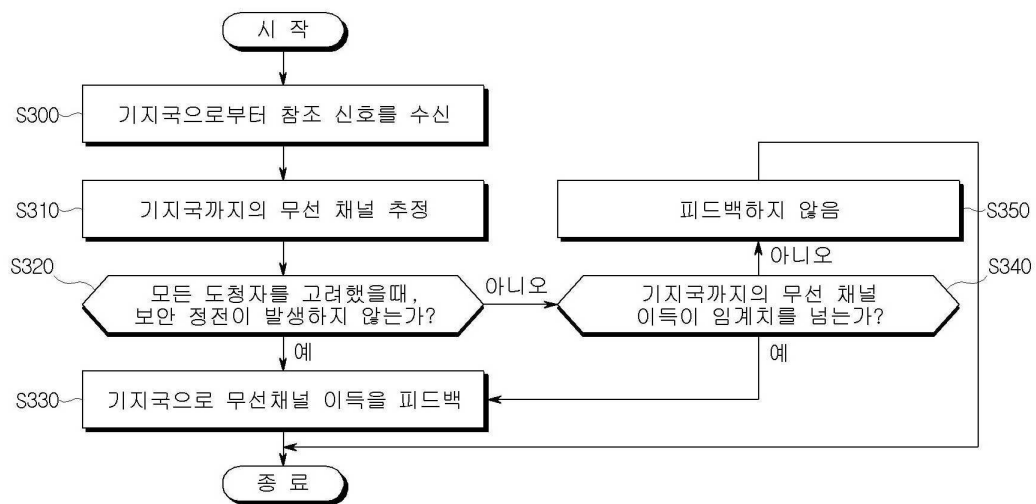
도면1



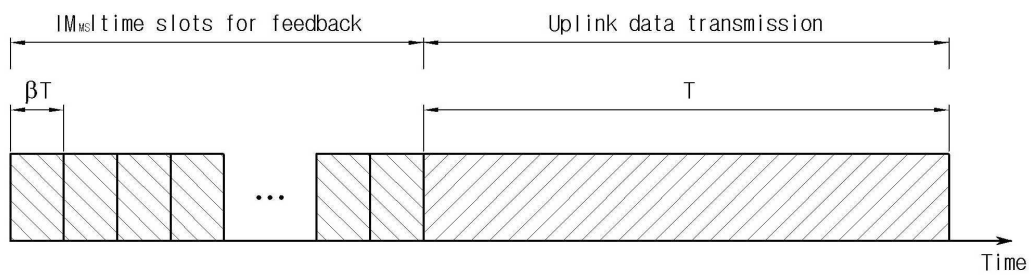
도면2



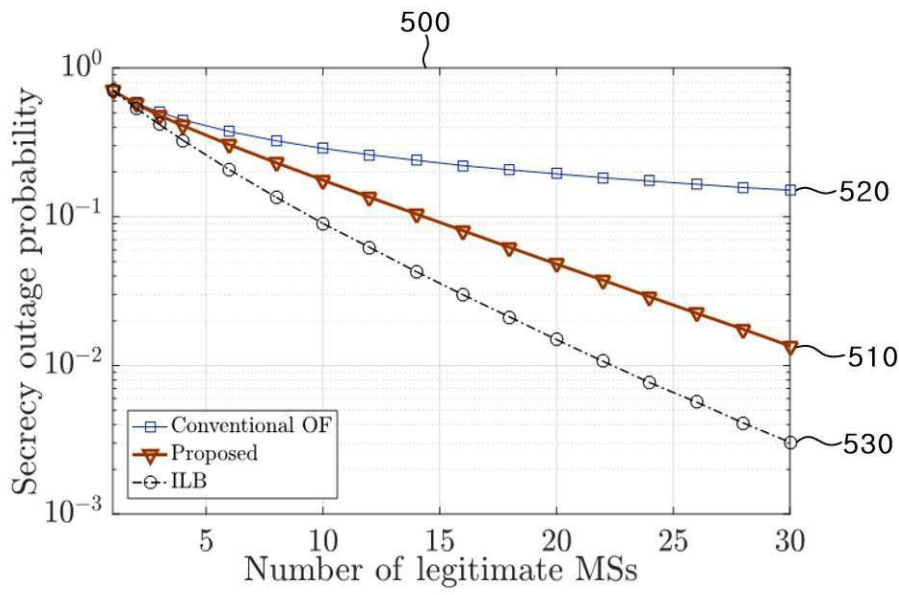
도면3



도면4



도면5



도면6

