(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년07월22일
(11) 등록번호 10-1538555
(24) 등록일자 2015년07월15일

(51) 국제특허분류(Int. Cl.)
H04W 24/00 (2009.01) *H04B 7/04* (2006.01)
(21) 출원번호 10-2013-0145958
(22) 출원일자 2013년11월28일
심사청구일자 2013년11월28일
(65) 공개번호 10-2015-0061797
(43) 공개일자 2015년06월05일
(56) 선행기술조사문헌
논문1: IEEE ICTC (2013.10)*
논문2: IEEE (2012.03)
KR1020090127016 A
KR1020110006121 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국과학기술원
대전광역시 유성구 대학로 291(구성동)
(72) 발명자
하정석
대전 유성구 대학로 291, (구성동, 한국과학기술원)
임상훈
대전 유성구 대학로 291, (구성동, 한국과학기술원)
(74) 대리인
양성보

전체 청구항 수 : 총 5 항 심사관 : 이준석

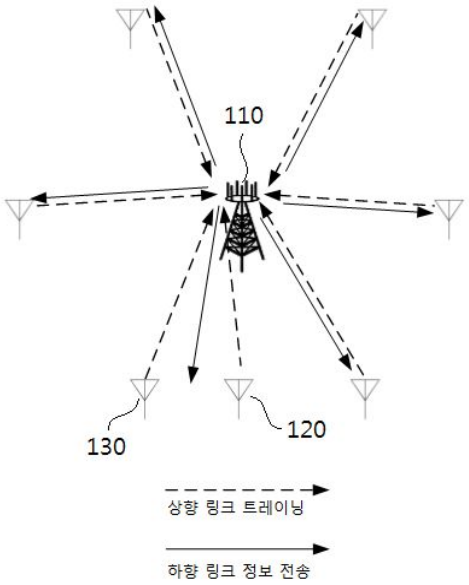
(54) 발명의 명칭 **시분할 이중통신 다중 사용자 다중 안테나 환경에서 파일럿 오염 공격을 검출하는 방법 및 시스템**

(57) 요 약

기지국에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 방법은 상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신하는 단계; 상기 수신된 신호를 이용하여 상기 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응

(뒷면에 계속)

대 표 도 - 도1



하는 채널 추정 정보를 추출하는 단계; 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 상기 채널 추정 정보에 기초하여 상기 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득하는 단계; 및 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법을 적용하여 상기 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계를 포함한다.

또한, 사용자 단말에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 방법은 하향 링크 정보 전송 과정 동안 기지국에서 생성한 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 수신하는 단계; 상기 상향 링크 트레이닝 시퀀스 전력을 이용하여 상기 하향 링크 정보에 포함되는 하향 링크 채널 이득에 대한 파일럿 오염 공격이 존재하지 않는 경우의 기대값을 계산하는 단계; 및 상기 기대값 및 상기 하향 링크 정보에 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계를 포함한다.

이 발명을 지원한 국가연구개발사업

과제고유번호	2012R1A1B3002684
부처명	교육부
연구관리전문기관	한국연구재단
연구사업명	이공분야기초연구사업 일반연구자지원사업 기본연구
연구과제명	차세대 무선 네트워크의 보안 강화를 위한 계층간 최적화 기술 연구
기 여 율	1/1
주관기관	한국과학기술원
연구기간	2013.05.01 ~ 2014.04.30

명 세 서

청구범위

청구항 1

다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경 아래, 기지국에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 방법에 있어서,

상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신하는 단계;

상기 수신된 신호를 이용하여 상기 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응하는 채널 추정 정보를 추출하는 단계;

일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 상기 채널 추정 정보에 기초하여 상기 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득하는 단계; 및

상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법을 적용하여 상기 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계

를 포함하고,

상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는

상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값과 오 경보 확률(False Alarm Probability)의 값을 결정하기 위해 미리 설정된 변수값을 비교하는 단계; 및

상기 비교 결과, 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값이 상기 미리 설정된 변수값보다 큰 경우, 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재한다고 판단하는 단계

를 포함하고,

상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값은 하기 수학식에 의하여 결정되는 기지국에서 파일럿 오염 공격을 검출하는 방법.

[수학식]

$$\frac{\|\mathbf{y}_\ell\|^2}{(1+c_\ell)M} - \ln\left\{\frac{\|\mathbf{y}_\ell\|^2}{(1+c_\ell)M}\right\}$$

상기 $\|\mathbf{y}_\ell\|^2$은 상기 상향 링크 트레이닝 시퀀스의 전력이고, 상기 c_ℓ은 $p_u\beta_\ell N_u$이고, 상기 p_u는 상기 복수의 사용자 단말들 각각의 상향 링크 전송 전력이고, 상기 β_ℓ은 상기 상향 링크 트레이닝 시퀀스를 모사하여 상기 모사한 상향 링크 트레이닝 시퀀스를 전송하는 공격자 단말의 대규모 페이딩 요소(Large Scale Fading Factor)이고, 상기 N_u는 미리 결정된 값이고, 상기 M은 안테나 개수이다.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는

상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하는 경우의 상기 상향 링크 트레이닝 시퀀스 전력이 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하지 않는 경우의 상기 상향 링크 트레이닝 시퀀스 전력보다 높은 특성을 이용하여 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계인 기지국에서 파일럿 오염 공격을 검출하는 방법.

청구항 4

제1항에 있어서,

상기 복수의 사용자 단말들로부터 수신된 신호는

상기 복수의 사용자 단말들 각각의 상향 링크 전송 전력, 상기 복수의 사용자 단말들 각각의 대규모 페이딩 요소(Large Scale Fading Factor) 및 복소 가우시안(Complex Gaussian) 잡음을 포함하는 기지국에서 파일럿 오염 공격을 검출하는 방법.

청구항 5

제1항에 있어서,

상기 채널 추정 정보를 추출하는 단계는

상기 수신된 신호 및 상기 적어도 하나의 사용자 단말이 전송하는 상기 상향 링크 트레이닝 시퀀스에 기초하여 상기 채널 추정 정보를 계산하는 단계

를 포함하는 기지국에서 파일럿 오염 공격을 검출하는 방법.

청구항 6

제1항에 있어서,

상기 상향 링크 트레이닝 시퀀스 전력을 획득하는 단계는

상기 채널 추정 정보 및 상기 채널 추정 정보에 벡터 전치(Transpose) 연산을 적용한 결과에 기초하여 상기 상향 링크 트레이닝 시퀀스 전력을 계산하는 단계

를 포함하는 기지국에서 파일럿 오염 공격을 검출하는 방법.

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 시분할 이중통신(Time Division Duplex; TDD) 다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 시스템 및 그 방법에 관한 기술로서, 기지국 또는 사용자 단말에서 파일럿 오염 공격을 검출하기 위한 신호 처리 및 검출 기술을 포함하는 정보 보안 기술에 관한 것이다.

배 경 기 술

[0002] Massive MIMO 시스템은 기지국에서 많은 수의 안테나를 이용하여 통신 셀 내부의 다수의 사용자 단말로 통신 서비스를 제공하는 통신 시스템이다. 기존의 다중 사용자 다중 안테나 환경에서는 셀 내부에서 서비스하고자 하는 사용자 단말의 수 K가 늘어남에 비례하여 간섭 신호의 영향이 크게 증가하였고, 전체 통신 시스템의 처리율 증대에 있어 병목 현상이 발생하는 단점이 있다. 이러한 문제를 해결하기 위한 다양한 기술이 학계에서 제안되었으나, 이들은 공통적으로 높은 복잡도의 송수신 시스템을 솔루션으로 제안하였다. Massive MIMO 시스템은 많은 수의 기지국 안테나를 이용하여 간단한 선형 필터만으로 사용자 단말간 간섭의 영향을 제거하고 전송 전력을 최소화 하는 기술이다. 따라서, Massive MIMO 시스템은 단순한 빔 성형만으로도 간섭의 영향을 크게 줄임으로써 저 복잡도의 송수신 구조를 갖추며 높은 주파수 효율을 제공할 수 있다.

[0003] Massive MIMO 시스템에서 하향 링크를 통해서 각 사용자 단말로 정보를 전송하기 위해서는 기지국에서의 하향 링크 채널 정보(Channel State Information; CSI)가 요구된다. 기지국은 하향 링크 채널정보를 바탕으로 각 사용자 단말로의 빔 성형 벡터를 생성한다. 또한, 수십에서 수백 개에 달하는 기지국 안테나와 사용자 단말들 사이의 채널 행렬을 효과적으로 추정하기 위해서는 채널 상반성(Channel Reciprocity)에 기초하여 채널 추정이 이뤄진다. 채널 상반성에 의해 같은 주파수 대역 상관 시간(Coherence Time) 이내에서는 기지국으로부터 사용자 단말로의 채널과 그 반대 방향인 사용자 단말로부터 기지국으로 향하는 채널이 동일한 채널 응답을 갖는다. 따라서, 시분할 이중통신 시스템에서는 다음의 두 과정을 통해서 효과적으로 채널이 추정된다. 첫 번째, K개의 사용자 단말들은 서로 직교하는 K개의 상향 링크 트레이닝 시퀀스를 동시에 기지국으로 전송한다. 두 번째, M개의 안테나를 갖는 기지국은 첫 번째 단계에서 수신된 신호를 토대로 M×K 채널 행렬을 추정한다. Massive MIMO 시스템은 일반적으로 안테나 개수 M이 서비스하고 있는 사용자 단말의 개수 K보다 훨씬 많기 때문에, 이러한 과정을 통해서 채널 추정하는 것이 매우 효율적이다.

[0004] 이 때, 상술한 기지국의 채널 추정과정에서, 공격자가 시스템 외부에서 악의적인 목적으로 제어권을 확보할 수 있는 수단이 존재한다면, Massive MIMO 시스템의 서비스를 방해하거나 심지어 공격자가 정보 수신을 도청하는 치명적인 결과가 초래될 수 있다. 이러한 공격 방식은 파일럿 오염 공격으로 학계에 의해 명명되었다. 구체적으로, 파일럿 오염 공격은 공격자가 기지국이 각 사용자 단말로의 빔 성형 벡터를 만드는 과정을 공격자가 의도하는 방향으로 제어하는 형태의 공격이다. 따라서, 공격자는 파일럿 오염 공격을 통해서 도청 하고자 하는 대상 신호의 수신 신호 감도를 의도하는 방향으로 조정할 수 있다. 그러나 파일럿 오염 공격을 조기에 탐지하는 검출 기술은 아직까지 연구된 바 없다.

[0005] 이에, 본 명세서에서는 파일럿 오염 공격을 기지국 또는 사용자 단말에서 조기에 검출하는 기술을 제안한다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예에 따르면, 시분할 이중통신 다중 사용자 다중 안테나 환경 아래, 기지국 또는 사용자 단말에서 일반화된 최대 우도 검출 기법을 이용함으로써, 파일럿 오염 공격을 검출하는 방법, 장치 및 시스템을 제공한다.

[0007] 또한, 본 발명의 실시예에 따르면, 파일럿 오염 공격을 검출하는 과정에서, 파일럿 오염 공격이 존재하는 경우 상향 링크 트레이닝 시퀀스 전력이 높아지는 특성을 이용하는 방법, 장치 및 시스템을 제공한다.

[0008] 또한, 본 발명의 실시예에 따르면, 파일럿 오염 공격을 검출하는 과정에서, 파일럿 오염 공격이 존재하는 경우 하향 링크 채널 이득이 낮아지는 특성을 이용하는 방법, 장치 및 시스템을 제공한다.

과제의 해결 수단

[0009] 본 발명에 실시예에 따르면, 다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경 아래, 기지국에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 방법은 상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신하는 단계; 상기 수신된 신호를 이용하여 상기 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응하는 채널 추정 정보를 추출하는 단계; 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 상기 채널 추정 정보에 기초하여 상기 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득하는 단계; 및 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법을 적용하여 상기 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계를 포함한다.

[0010] 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값과 오 경보 확률(False Alarm Probability)의 값을 결정하기 위해 미리 설정된 변수값을 비교하는 단계; 및 상기 비교 결과, 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값이 상기 미리 설정된 변수값보다 큰 경우, 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재한다고 판단하는 단계를 포함할 수 있다.

[0011] 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하는 경우의 상기 상향 링크 트레이닝 시퀀스 전력이 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하지 않는 경우의 상기 상향 링크 트레이닝 시퀀스 전력보다 높은 특성을 이용하여 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계일 수 있다.

[0012] 상기 복수의 사용자 단말들로부터 수신된 신호는 상기 복수의 사용자 단말들 각각의 상향 링크 전송 전력, 상기 복수의 사용자 단말들 각각의 대규모 페이딩 요소(Large Scale Fading Factor) 및 복소 가우시안(Complex Gaussian) 잡음을 포함할 수 있다.

[0013] 상기 채널 추정 정보를 추출하는 단계는 상기 수신된 신호 및 상기 적어도 하나의 사용자 단말이 전송하는 상기 상향 링크 트레이닝 시퀀스에 기초하여 상기 채널 추정 정보를 계산하는 단계를 포함할 수 있다.

[0014] 상기 상향 링크 트레이닝 시퀀스 전력을 획득하는 단계는 상기 채널 추정 정보 및 상기 채널 추정 정보에 벡터 전치(Transpose) 연산을 적용한 결과에 기초하여 상기 상향 링크 트레이닝 시퀀스 전력을 계산하는 단계를 포함할 수 있다.

[0015] 본 발명에 실시예에 따르면, 다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경 아래, 사용자 단말에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 방법은 하향 링크 정보 전송 과정 동안 기지국에서 생성한 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 수신하는 단계; 상기 상향 링크 트레이닝 시퀀스 전력을 이용하여 상기 하향 링크 정보에 포함되는 하향 링크 채널 이득에 대한 파일럿 오염 공격이 존재하지 않는 경우의 기대값을 계산하는 단계; 및 상기 기대값 및 상기 하향 링크 정보에 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계를 포함한다.

[0016] 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는 상기 하향 링크 정보를 이용하여 상기 하향 링크 채널 이득에 대한 추정치를 계산하는 단계; 상기 계산된 추정치 및 상기 기대값 사이의 차이값과 미리 설정된 변수값을 비교하는 단계; 및 상기 비교 결과, 상기 계산된 추정치 및 상기 기대값 사이의 차이값이 미리 설정된 변수값보다 큰 경우, 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재한다고 판단하는 단계를 포함할 수 있다.

[0017] 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계는 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하는 경우의 상기 하향 링크 채널 이득이 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재하지 않는 경우의 상기 하향 링크 채널 이득보다 낮은 특성을 이용하여 상기 파일럿 오염 공격이 존재하는지 여부를 판단하는 단계일 수 있다.

[0018] 상기 하향 링크 정보 및 상기 상향 링크 트레이닝 시퀀스 전력을 수신하는 단계는 상기 기지국에서 상기 상향

링크 트레이닝 과정 동안 복수의 사용자 단말들로부터 수신된 신호를 이용하여 상기 복수의 사용자들 각각의 채널 추정 정보를 추출하는 단계; 상기 기지국에서 상기 채널 추정 정보에 기초하여 상기 복수의 사용자 단말들 각각으로부터 수신된 상기 상향 링크 트레이닝 시퀀스 전력 및 상기 복수의 사용자들 각각의 프리코딩 벡터를 생성하는 단계; 및 상기 기지국에서 상기 하향 링크 정보 및 상기 상향 링크 트레이닝 시퀀스 전력을 변조하고, 변조된 벡터를 상기 프리코딩 벡터를 이용하여 전송하는 단계를 더 포함할 수 있다.

[0019] 상기 다중 사용자 다중 안테나 환경의 통신 시스템은 시분할 이중통신(Time Division Duplex; TDD) 기법을 사용할 수 있다.

[0020] 본 발명의 실시예에 따르면, 다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경 아래, 기지국에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 시스템은 상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신하는 수신부; 상기 수신된 신호를 이용하여 상기 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응하는 채널 추정 정보를 추출하는 추출부; 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 상기 채널 추정 정보에 기초하여 상기 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득하는 획득부; 및 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법을 적용하여 상기 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 판단부를 포함한다.

[0021] 상기 판단부는 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값과 오경보 확률(False Alarm Probability)의 값을 결정하기 위해 미리 설정된 변수값을 비교하고, 상기 비교 결과, 상기 상향 링크 트레이닝 시퀀스 전력에 상기 일반화된 최대 우도 검출 기법이 적용된 값이 상기 미리 설정된 변수값보다 큰 경우, 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재한다고 판단할 수 있다.

[0022] 본 발명의 실시예에 따르면, 다중 사용자 다중 안테나(Multi-User Multiple Input Multiple Output; MU-MIMO) 환경 아래, 사용자 단말에서 파일럿 오염 공격(Pilot Contamination Attack)을 검출하는 시스템은 하향 링크 정보 전송 과정 동안 기지국에서 생성한 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 수신하는 수신부; 상기 상향 링크 트레이닝 시퀀스 전력을 이용하여 상기 하향 링크 정보에 포함되는 하향 링크 채널 이득에 대한 파일럿 오염 공격이 존재하지 않는 경우의 기대값을 계산하는 계산부; 및 상기 기대값 및 상기 하향 링크 정보에 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단하는 판단부를 포함한다.

[0023] 상기 판단부는 상기 하향 링크 정보를 이용하여 상기 하향 링크 채널 이득에 대한 추정치를 계산하고, 상기 계산된 추정치 및 상기 기대값 사이의 차이값과 미리 설정된 변수값을 비교하며, 상기 비교 결과, 상기 계산된 추정치 및 상기 기대값 사이의 차이값이 미리 설정된 변수값보다 큰 경우, 상기 적어도 하나의 사용자 단말에 대한 상기 파일럿 오염 공격이 존재한다고 판단할 수 있다.

발명의 효과

[0024] 본 발명의 실시예에 따르면, 시분할 이중통신 다중 사용자 다중 안테나 환경 아래, 기지국 또는 사용자 단말에서 일반화된 최대 우도 검출 기법을 이용함으로써, 파일럿 오염 공격을 검출하는 방법, 장치 및 시스템을 제공할 수 있다.

[0025] 또한, 본 발명의 실시예에 따르면, 파일럿 오염 공격을 검출하는 과정에서, 파일럿 오염 공격이 존재하는 경우 상향 링크 트레이닝 시퀀스 전력이 높아지는 특성을 이용하는 방법, 장치 및 시스템을 제공할 수 있다.

[0026] 또한, 본 발명의 실시예에 따르면, 파일럿 오염 공격을 검출하는 과정에서, 파일럿 오염 공격이 존재하는 경우 하향 링크 채널 이득이 낮아지는 특성을 이용하는 방법, 장치 및 시스템을 제공할 수 있다.

[0027] 또한, 본 발명의 실시예에 따르면, 파일럿 오염 공격을 검출함으로써, 정보 보안을 위한 추가적인 후속 조치를 용이하게 할 수 있는 방법, 장치 및 시스템을 제공할 수 있다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 일실시예에 있어서, 파일럿 오염 공격 검출이 수행되는 시분할 이중통신 다중 사용자 다중 안테나 시스템을 나타낸 도면이다.

도 2는 본 발명의 일실시예에 있어서, 기지국에서 파일럿 오염 공격을 검출하는 방법을 나타낸 플로우 차트이다.

도 3은 본 발명의 일실시예에 있어서, 사용자 단말에서 파일럿 오염 공격을 검출하는 방법을 나타낸 플로우 차트이다.

도 4는 본 발명의 일실시예에 있어서, 기지국 및 사용자 단말에서의 파일럿 오염 공격 검출 성능을 나타낸 도면이다.

도 5는 본 발명의 일실시예에 있어서, 기지국에서 파일럿 오염 공격을 검출하는 시스템을 나타낸 블록도이다.

도 6은 본 발명의 일실시예에 있어서, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템을 나타낸 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 이하, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 또한, 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0030] 도 1은 본 발명의 일실시예에 있어서, 파일럿 오염 공격 검출이 수행되는 시분할 이중통신 다중 사용자 다중 안테나 시스템을 나타낸 도면이다.

[0031] 도 1을 참조하면, 본 발명의 일실시예에 따른 파일럿 오염 공격 검출이 수행되는 시분할 이중통신 다중 사용자 다중 안테나 시스템은 하나의 기지국(110)과 복수의 사용자 단말을 포함하는 통신 네트워크에서 수행되는 것을 전제로 설명한다. 이하, 파일럿 오염 공격 검출이 수행되는 시분할 이중통신 다중 사용자 다중 안테나 시스템은 시스템으로 기재하기로 한다. 또한, 시스템은 하나의 기지국(110)과 복수의 사용자 단말이 포함되는 통신 네트워크 외에, 복수의 기지국 및 복수의 사용자 단말이 포함되는 통신 네트워크에도 적용 가능할 수 있다.

[0032] 시스템은 M개의 안테나들을 갖는 기지국(110) 및 단일 안테나를 갖는 K개의 사용자 단말들을 포함한다. 이 때, 기지국(110)은 복수의 사용자 단말들로 하향 링크 정보를 전송함으로써, 통신 서비스를 K개의 사용자 단말들로 제공할 수 있다. 여기서, 하향 링크 정보 전송은 상향 링크 트레이닝 과정, 채널 추정 및 프리코딩 벡터 생성 과정 및 하향 링크 정보 전송 과정을 통하여 수행될 수 있다.

[0033] 상향 링크 트레이닝 과정에서, K개의 사용자 단말들은 길이 N_u의 서로 직교하는 K개의 상향 링크 트레이닝 시퀀스 $\{\sqrt{N_u}\boldsymbol{\psi}_\ell\}_{\ell=1}^{K}$를 동시에 기지국(110)으로 전송할 수 있다. 이 때, 기지국(110)이 K개의 사용자 단말들로부터 수신하는 신호인, $M \times N_u$ 행렬 Y는 수학식 1과 같이 나타낼 수 있다.

[0034] <수학식 1>

[0035]
$$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{p_u \beta_k N_u}\,\mathbf{h}_k \boldsymbol{\psi}_k + \mathbf{W}$$

[0036] 여기서, p_u는 K개의 사용자 단말들 각각의 상향 링크 전송 전력일 수 있고, β_k는 k번째 사용자 단말의 대규모 페이딩 요소(Large Scale Fading Factor)로서, 상향 링크 전송 전력 및 대규모 페이디 요소는 기지국(110)과 통신하는 모든 사용자 단말들에게 공개된 정보일 수 있다. 또한, $\mathbb{W}$는 $M \times N_u$ 복소 가우시안(Complex Gaussian) 잡음 행렬로서, 행렬의 각 원소는 서로 독립적이고, 평균값 0에 분산값 1을 가질 수 있다. 또한, 소규모 페이딩 채널 $\{\mathbf{h}_k\}_{\ell=1}^{K} = \{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_K\}$는 복소 가우시안 분포를 따르고, 서로 다른 사용자 단말간의 채널은 서로 동일하지만, 독립적인 분포를 $\mathcal{CN}(\mathbf{0}, \mathbf{I})$로 따른다고 가정한다.

[0037] 본 발명의 일실시예에서는 공격자 단말(120)이 ℓ번째 사용자 단말인, 적어도 하나의 사용자 단말(130)에 대해

파일럿 오염 공격을 수행하는 것을 전제로 파일럿 오염 공격을 검출하는 방법을 설명하기로 한다.

[0038] 공격자 단말(120)은 적어도 하나의 사용자 단말(130)이 전송하는 상향 링크 트레이닝 시퀀스를 모사하여, 적어도 하나의 사용자 단말(130)이 전송하는 시점과 동일한 시점에 모사한 상향 링크 트레이닝 시퀀스를 기지국(110)으로 전송할 수 있다. 이에, 기지국(110)은 K개의 사용자 단말들로부터 수학식 2와 같은 신호인 행렬 Y를 수신할 수 있다.

[0039] <수학식 2>

[0040] $$\mathbf{Y} = \sum_{k=1}^{K} \sqrt{p_u \beta_k N_u}\mathbf{h}_k \boldsymbol{\psi}_k + \sqrt{p_e \beta_e N_u}\mathbf{h}_e \boldsymbol{\psi}_\ell + \mathbf{W}$$

[0041] 여기서, p_e는 공격자 단말(120)의 상량 링크 전송 전력일 수 있고, β_e는 공격자 단말(120)의 대규모 페이딩 요소일 수 있다. 이 때, 공격자 단말(120)이 시스템에 비협조적이므로, 공격자 단말(120)의 상향 링크 전송 전력 및 대규모 페이디 요소는 기지국(110) 및 기지국(110)과 통신하는 모든 사용자 단말들에게 공개되지 않은 정보로 가정한다.

[0042] 채널 추정 및 프리코딩 벡터 생성 과정에서, 기지국(110)은 수학식 2와 같은 수신된 신호인 행렬 Y를 이용하여 적어도 하나의 사용자 단말(130)에 대응하는 채널 추정 정보를 추출할 수 있다. 예를 들어, 기지국(110)은 수학식 2와 같은 수신된 신호인 행렬 Y에 각 사용자 단말에 대한 상향 링크 트레이닝 시퀀스의 벡터 전치 연산(Transpose)을 적용한 결과인 $\boldsymbol{\psi}_\ell^\dagger$를 곱함으로써, 채널 추정에 요구되는 충분 통계량(Sufficient Statistics)인 채널 추정 정보를 계산할 수 있다. 이 때, ℓ번째 적어도 하나의 사용자 단말(130)로의 채널 $\mathbf{h}_\ell$의 채널을 추정하는 채널 추정 정보인 $\mathbf{y}_\ell = \mathbf{Y}\boldsymbol{\psi}_\ell^\dagger$은 수학식 3과 같다.

[0043] <수학식 3>

[0044] $$\mathbf{y}_\ell = \sqrt{c_\ell}(\mathbf{h}_\ell + w\mathbf{h}_e) + \mathbf{w}_\ell$$

[0045] 여기서, $\mathrm{c}_\ell = p_u \beta_\ell N_u$이고, $\mathrm{w} = \sqrt{\frac{p_e \beta_e}{p_u \beta_\ell}}$이다.

[0046] 또한, 기지국(110)은 $p_e\beta_e$ 또는 w를 알 수 없으므로, 채널 추정 정보 $\mathbf{y}_\ell$로부터 수학식 4와 같은 정합 필터(Matched Filter; MF) 프리코딩 벡터를 생성할 수 있다.

[0047] <수학식 4>

[0048] $$\mathbf{a}_\ell = \frac{\mathbf{y}_\ell}{\|\mathbf{y}_\ell\|} = \frac{\sqrt{c_\ell}(\mathbf{h}_\ell + w\mathbf{h}_e) + \mathbf{w}_\ell}{\|\mathbf{y}_\ell\|}$$

[0049] 채널 추정 정보인 $\mathbf{y}_\ell$은 두 개의 채널 $\mathbf{h}_\ell$, $\mathbf{h}_e$의 선형 조합으로 나타나기 때문에, 공격자 단말(120)은 w를 조절함으로써, 프리코딩 벡터의 방향을 임의로 기지국(110)에서 공격자 단말(120)로 향하는 채널 방향인 $\mathbf{h}_e$쪽으로 전환할 수 있다.

[0050] 하향 링크 정보 전송 과정에서, 기지국(110)은 이진 위상 편이(Binary Phase Shift Keying) 방식으로 복수의 사

용자 단말들로 보내고자 하는 정보를 변조하여 $\{\mathbf{q}_k\}_{k=1}^{K}$를 생성할 수 있다. 그 후, 기지국(110)은 복수의 사용자 단말 각각의 $\{\mathbf{a}_k\}_{k=1}^{K}$를 이용하여 빔 성형을 수행한 후에, 복수의 사용자 단말들 각각으로 전송할 수 있다.

[0051] 이 때, 적어도 하나의 사용자 단말(130)이 수신하는 하향 링크 정보는 수학식 5와 같다. 수학식 5에서 $\mathbf{z}_\ell$은 복소 가우시안 잡음으로 평균값 0이고, 공분산 행렬은 $\mathbf{I}$로 가정한다.

[0052] <수학식 5>

[0053] $$\mathbf{r}_\ell = \left(\frac{\mathbf{h}_\ell^T \mathbf{a}_\ell}{\sqrt{M}}\right)\mathbf{q}_\ell + \sum_{k\neq\ell}\left(\frac{\mathbf{h}_\ell^T \mathbf{a}_k}{\sqrt{M}}\right)\mathbf{q}_k + \mathbf{z}_\ell$$

[0054] 이하, 위에서 상술한 시분할 이중통신 다중 사용자 다중 안테나 환경에서, 파일럿 오염 공격을 검출하는 방법을 기재하기로 한다. 구체적으로, 도 2를 참조하여, 기지국에서 ℓ번째 사용자 단말인 적어도 하나의 사용자 단말(130)에 대한 파일럿 오염 공격을 검출하는 방법을 기재하고, 도 3을 참조하여, 사용자 단말에서 ℓ번째 사용자 단말인 적어도 하나의 사용자 단말(130)에 대한 파일럿 오염 공격을 검출하는 방법을 기재하기로 한다.

[0055] 도 2는 본 발명의 일실시예에 있어서, 기지국에서 파일럿 오염 공격을 검출하는 방법을 나타낸 플로우 차트이다.

[0056] 도 2를 참조하면, 본 발명의 일실시예에 따른 기지국에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신한다(210). 이 때 수신된 신호는 수학식 2와 같이 표현될 수 있다.

[0057] 또한, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 수신된 신호를 이용하여 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응하는 채널 추정 정보를 추출한다(220). 이 때, 채널 추정 정보는 수학식 3과 같이 표현될 수 있다.

[0058] 또한, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 채널 추정 정보에 기초하여 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득한다(230). 이 때, 상향 링크 트레이닝 시퀀스 전력은 수학식 6과 같이 나타낼 수 있다.

[0059] <수학식 6>

[0060] $$\|\mathbf{y}_\ell\|^2 = \mathbf{y}_\ell^\dagger \mathbf{y}$$

[0061] 여기서, $\|\mathbf{y}_\ell\|^2$은 기지국이 M개의 안테나를 통해 수신한 상량 링크 트레이닝 시퀀스 전력이고, 일반화된 최대 우도 검출 기법을 적용하기 위한 충분 통계치로서, 채널 추정 정보에 벡터 전치 연산을 적용한 결과를 채널 추정 정보에 곱함으로써, 계산될 수 있다.

[0062] 또한, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단한다(240). 예를 들어, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 시퀀스 전력 $\|\mathbf{y}_\ell\|^2$에 수학식 7과 같이 일반화된 최대 우도 검출 기법을 적용하여 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다.

[0063] <수학식 7>

$$\ln \mathbf{\Lambda_1}(\mathbf{y}_\ell) = \frac{\|\mathbf{y}_\ell\|^2}{(1+c_\ell)M} - \ln\left\{\frac{\|\mathbf{y}_\ell\|^2}{(1+c_\ell)M}\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda'$$

[0064]

[0065] 이 때, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법이 적용된 값인 $\ln \mathbf{\Lambda_1}(\mathbf{y}_\ell)$과 오 경보 확률(False Alarm Probability)의 값을 결정하기 위해 미리 설정된 변수값인 λ'을 비교하고, 비교 결과, 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법이 적용된 값인 $\ln \mathbf{\Lambda_1}(\mathbf{y}_\ell)$이 미리 설정된 변수값인 λ'보다 큰 경우, 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재한다고 판단할 수 있다.

[0066] 여기서, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는 경우의 상향 링크 트레이닝 시퀀스 전력이 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하지 않는 경우의 상향 링크 트레이닝 시퀀스 전력보다 높은 특성을 이용하여 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다.

[0067] 또한, 도면에는 도시되지 않았지만, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 파일럿 오염 공격이 존재하는 경우, 이에 대한 후속 조치를 실행할 수 있다.

[0068] 도 3은 본 발명의 일실시예에 있어서, 사용자 단말에서 파일럿 오염 공격을 검출하는 방법을 나타낸 플로우 차트이다.

[0069] 도 3을 참조하면, 본 발명의 일실시예에 따른 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 하향 링크 정보 전송 과정 동안 기지국에서 생성한 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 수신한다(310).

[0070] 이 때, 도면에는 도시되지 않았지만, 기지국은 상향 링크 트레이닝 과정 동안 복수의 사용자 단말들로부터 수신된 신호를 이용하여 복수의 사용자들 각각의 채널 추정 정보를 추출할 수 있다. 여기서, 수신된 신호는 수학식 2와 같이 표현될 수 있고, 채널 추정 정보는 수학식 3과 같이 표현될 수 있다. 또한, 기지국은 채널 추정 정보에 기초하여 복수의 사용자 단말들 각각으로부터 수신된 상향 링크 트레이닝 시퀀스 전력인 $\|\mathbf{y}_\ell\|^2$ 및 복수의 사용자들 각각의 프리코딩 벡터 $\{\mathbf{a}_k\}_{k=1}^K$를 생성할 수 있다. 여기서, 상량 링크 트레이닝 시퀀스 전력은 수학식 6과 같이 표현될 수 있다. 또한, 기지국은 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 이진 위상 편이 방식으로 변조하여 $\{\mathbf{q}_k\}_{k=1}^K$를 생성하고, 변조된 벡터를 프리코딩 벡터 $\{\mathbf{a}_k\}_{k=}^K$를 이용하여 전송할 수 있다.

[0071] 또한, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 시퀀스 전력을 이용하여 하향 링크 정보 $\mathbf{r}_\ell$에 포함되는 하향 링크 채널 이득에 대한 파일럿 오염 공격이 존재하지 않는 경우의 기대값을 계산한다(320). 여기서, 하향 링크 정보는 수학식 5와 같이 표현될 수 있고, 하향 링크 채널 이득은 ℓ번째 사용자 단말의 채널 $\mathbf{h}_\ell$ 및 프리코딩 벡터 $\mathbf{a}_k$의 곱으로 표현되는 $\frac{\mathbf{h}_\ell^T \mathbf{a}_\ell}{\sqrt{M}}$ 일 수 있다. 또한, 기대값 μ_{g_0}은 파일럿 오염 공격이 존재하지 않는 경우의 평균값으로, 수학식 8과 같이 표현될 수 있다.

[0072] <수학식 8>

$$\mu_{g_0} = \frac{\|\mathbf{y}_\ell\|\sqrt{c_\ell}}{\sqrt{M}\{1+c_\ell\}}$$

[0073]

[0074] 반면에, 파일럿 오염 공격이 존재하는 경우의 하향 링크 채널 이득 $\frac{\mathbf{h}_\ell^T \mathbf{a}_\ell}{\sqrt{M}}$의 평균값 μ_{g_1}은 수학식 9와 같이 표현될 수 있다.

[0075] <수학식 9>

[0076] $$\mu_{g_1} = \frac{\|\mathbf{y}_\ell\|\sqrt{c_\ell}}{\sqrt{M}\{1+(1+w^2)c_\ell\}}$$

[0077] 또한, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 기대값 및 하향 링크 정보에 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단한다(330).

[0078] 이 때, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 하향 링크 정보를 이용하여 하향 링크 채널 이득에 대한 추정치를 계산하고, 계산된 추정치 및 기대값 사이의 차이값과 미리 설정된 변수값을 비교하며, 비교 결과, 계산된 추정치 및 기대값 사이의 차이값이 미리 설정된 변수값보다 큰 경우, 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재한다고 판단할 수 있다. 예를 들어, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 상향 링크 트레이닝 시퀀스 전력 $\|\mathbf{y}_\ell\|^2$ 및 하향 링크 정보 $\mathbf{r}_\ell$를 이용하여 일반화된 최대 우도 검출 기법을 적용하기 위한 충분 통계량을 수학식 10과 같이 획득할 수 있다.

[0079] <수학식 10>

[0080] $$\Lambda_2(\mu_{g_0}, \mathbf{r}_\ell) = \frac{1}{N_d}\sum_{n=1}^{N_d}|\Re\{r_\ell(n)\}| - \mu_{g_0}$$

[0081] 여기서, $\frac{1}{N_d}\sum_{n=1}^{N_d}|\Re\{r_\ell(n)\}|$는 하향 링크 채널 이득에 대한 추정치로서, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 추정치 $\frac{1}{N_d}\sum_{n=1}^{N_d}|\Re\{r_\ell(n)\}|$와 기대값 μ_{g_0} 사이의 차이값이 미리 설정된 변수값인 특정 경계값 λ''보다 큰 경우, 파일럿 오염 공격이 존재한다고 판단할 수 있다.

[0082] 이 때, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는 경우의 하향 링크 채널 이득이 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하지 않는 경우의 하향 링크 채널 이득보다 낮은 특성을 이용하여 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다. 예를 들어, 공격자 단말이 더 높은 전력으로 파일럿 오염 공격을 수행하면 빔 성형 벡터의 방향이 공격자 단말의 채널 방향으로 틀어진 만큼 ℓ번째 사용자 단말의 하향 링크 채널 이득이 줄어들기 때문에, 파일럿 오염 공격이 검출될 수 있다.

[0083] 위에서 상술한 파일럿 오염 공격을 검출하는 원리는 수학식 11로도 설명할 수 있다.

[0084] <수학식 11>

[0085] $$\frac{1}{N_d}\sum_{n=1}^{N_d}|\Re\{r_\ell(n)\}| > \mu_{g_0} - \sqrt{\frac{\sigma_n^2 \ln\lambda}{N_d}}$$

[0086] 여기서, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 기대값 μ_{g_0}에 적당한 마진 $\sqrt{\frac{\sigma_n^2 \ln\lambda}{N_d}}$ 을 두고, 이를 추정치 $\frac{1}{N_d}\sum_{n=1}^{N_d}|\Re\{r_\ell(n)\}|$ 와 비교함으로써, 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다.

[0087] 또한, 도면에는 도시되지 않았지만, 기지국에서 파일럿 오염 공격을 검출하는 시스템은 파일럿 오염 공격이 존재하는 경우, 이에 대한 후속 조치를 실행할 수 있다.

[0088] 도 4는 본 발명의 일실시예에 있어서, 기지국 및 사용자 단말에서의 파일럿 오염 공격 검출 성능을 나타낸 도면이다.

[0089] 도 4를 참조하면, 본 발명의 일실시예에 따른 기지국에서의 파일럿 오염 공격 검출 성능은 원 모양 실선인 그래프들(410, 420)로 나타낸다. 또한, 본 발명의 일실시예에 따른 사용자 단말에서의 파일럿 오염 공격 검출 성능은 네모 모양 실선인 그래프들(430, 440, 450)으로 나타낸다.

[0090] 여기서, 기지국 및 사용자 단말에서의 파일럿 오염 공격 검출 성능을 나타내기 위한 시스템 변수는 다음과 같다. 사용자 단말에서의 상향 링크 전송 전력 p_u은 10dB로 기지국의 하향 링크 전송 전력 p_d는 20dB로 설정하였다. 또한, 대규모 페이딩 요소($\beta_1 = \beta_2 = \cdots = \beta_K = \beta_e$)는 모두 1로 정규화하였다. 또한, 기지국의 안테나 개수 M은 100개 및 400개로 설정하였고, 서비스를 제공받는 사용자 단말 개수인 K는 50으로 설정하였다. 또한, 상향 링크 트레이닝 시퀀스의 길이 N_u는 50 및 100으로 설정하였고, 하향 링크 트레이닝 시퀀스의 길이 역시 50 및 100으로 설정하였다. 또한, 오 경보 확률의 값을 결정하기 위해 미리 설정된 변수값인 λ' 및 미리 설정된 변수값인 특정 경계값 λ''은 0.01이 되도록 설정하였다.

[0091] 기지국에서의 파일럿 오염 공격 검출 성능과 관련된 그래프들(410, 420) 및 사용자 단말에서의 파일럿 오염 공격 검출 성능과 관련된 그래프들(430, 440, 450)을 살펴보면, 하향 링크 심볼의 개수 N_d가 증가할수록 채널 이득에 대한 추정이 정확해지므로, 파일럿 오염 공격 검출 성능이 향상되는 것을 알 수 있다. 또한, 안테나 개수 M이 증가함에 따라, 파일럿 오염 공격 검출 성능이 향상되는 것을 알 수 있다. 예를 들어, M=400, N_u=50, N_d=100인 경우, w^2가 -9dB일 때 99%의 파일럿 오염 공격을 검출할 수 있다.

[0092] 도 5는 본 발명의 일실시예에 있어서, 기지국에서 파일럿 오염 공격을 검출하는 시스템을 나타낸 블록도이다.

[0093] 도 5를 참조하면, 본 발명의 일실시예에 따른 기지국에서 파일럿 오염 공격을 검출하는 시스템은 수신부(510), 추출부(520), 획득부(530) 및 판단부(540)를 포함한다.

[0094] 수신부(510)는 상향 링크 트레이닝 과정에서 복수의 사용자 단말들로부터 복수의 사용자 단말들 각각이 전송하는 상향 링크 트레이닝 시퀀스를 포함하는 신호를 수신한다.

[0095] 추출부(520)는 수신된 신호를 이용하여 복수의 사용자 단말들 중 적어도 하나의 사용자 단말에 대응하는 채널 추정 정보를 추출한다.

[0096] 획득부(530)는 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하기 위해, 채널 추정 정보에 기초하여 적어도 하나의 사용자 단말로부터 수신된 상향 링크 트레이닝 시퀀스 전력을 획득한다.

[0097] 판단부(540)는 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단한다.

[0098] 이 때, 판단부(540)는 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법이 적용된 값과 오 경보 확률(False Alarm Probability)의 값을 결정하기 위해 미리 설정된 변수값을 비교하고, 비교 결과, 상향 링크 트레이닝 시퀀스 전력에 일반화된 최대 우도 검출 기법이 적용된 값이 미리 설정된 변수값보다 큰 경우, 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재한다고 판단할 수 있다.

[0099] 또한, 판단부(540)는 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는 경우의 상향 링크 트레이닝 시퀀스 전력이 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하지 않는 경우의 상향 링크 트레이닝 시퀀스 전력보다 높은 특성을 이용하여 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다.

[0100] 도 6은 본 발명의 일실시예에 있어서, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템을 나타낸 블록도이다.

[0101] 도 6을 참조하면, 본 발명의 일실시예에 따른 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 수신부(610), 계산부(620) 및 판단부(630)를 포함한다.

[0102] 수신부(610)는 하향 링크 정보 전송 과정 동안 기지국에서 생성한 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 수신한다.

[0103] 계산부(620)는 상향 링크 트레이닝 시퀀스 전력을 이용하여 하향 링크 정보에 포함되는 하향 링크 채널 이득에 대한 파일럿 오염 공격이 존재하지 않는 경우의 기대값을 계산한다.

[0104] 판단부(630)는 기대값 및 하향 링크 정보에 일반화된 최대 우도 검출(Generalized Likelihood Ratio Test; GLRT) 기법을 적용하여 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는지 여부를 판단한다.

[0105] 이 때, 판단부(630)는 하향 링크 정보를 이용하여 하향 링크 채널 이득에 대한 추정치를 계산하고, 계산된 추정치 및 기대값 사이의 차이값과 미리 설정된 변수값을 비교하며, 비교 결과, 계산된 추정치 및 기대값 사이의 차이값이 미리 설정된 변수값보다 큰 경우, 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재한다고 판단할 수 있다.

[0106] 또한, 판단부(630)는 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하는 경우의 하향 링크 채널 이득이 적어도 하나의 사용자 단말에 대한 파일럿 오염 공격이 존재하지 않는 경우의 하향 링크 채널 이득보다 낮은 특성을 이용하여 파일럿 오염 공격이 존재하는지 여부를 판단할 수 있다.

[0107] 또한, 도면에는 도시되지 않았지만, 사용자 단말에서 파일럿 오염 공격을 검출하는 시스템은 기지국에서, 상향 링크 트레이닝 과정 동안 복수의 사용자 단말들로부터 수신된 신호를 이용하여 복수의 사용자들 각각의 채널 추정 정보를 추출할 수 있고, 채널 추정 정보에 기초하여 복수의 사용자 단말들 각각으로부터 수신된 상향 링크 트레이닝 시퀀스 전력 및 복수의 사용자들 각각의 프리코딩 벡터를 생성하며, 하향 링크 정보 및 상향 링크 트레이닝 시퀀스 전력을 변조하고, 변조된 벡터를 프리코딩 벡터를 이용하여 전송할 수 있다.

[0108] 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, 콘트롤러, 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 애플리케이션을 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 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0109] 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 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)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.

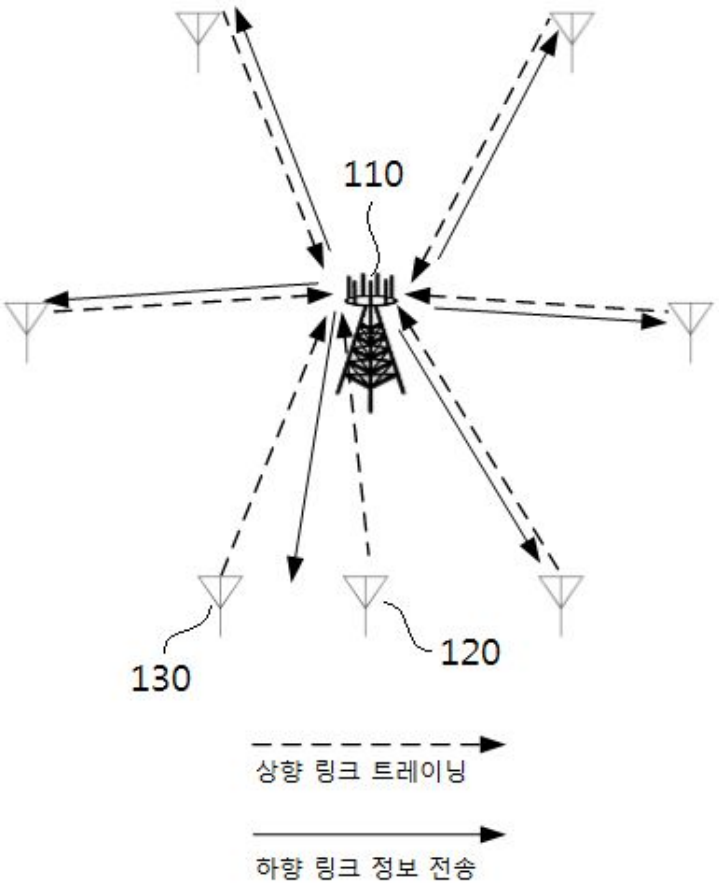
[0110] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0111] 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.

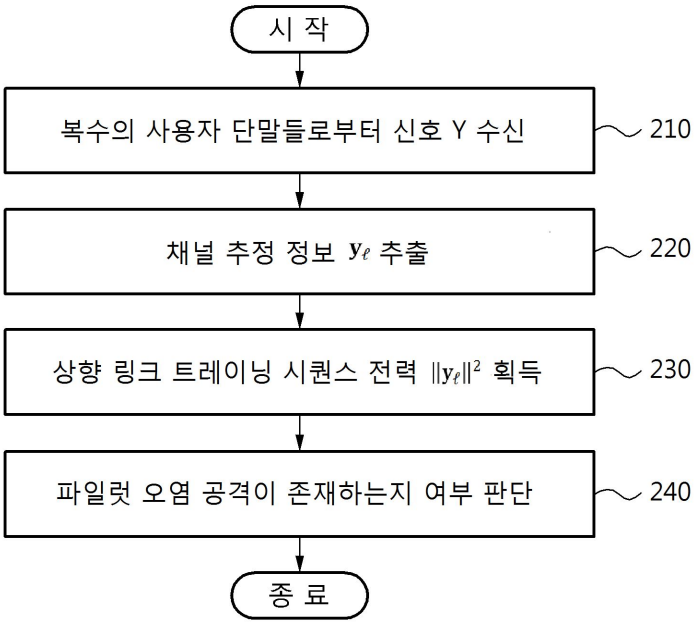
[0112] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

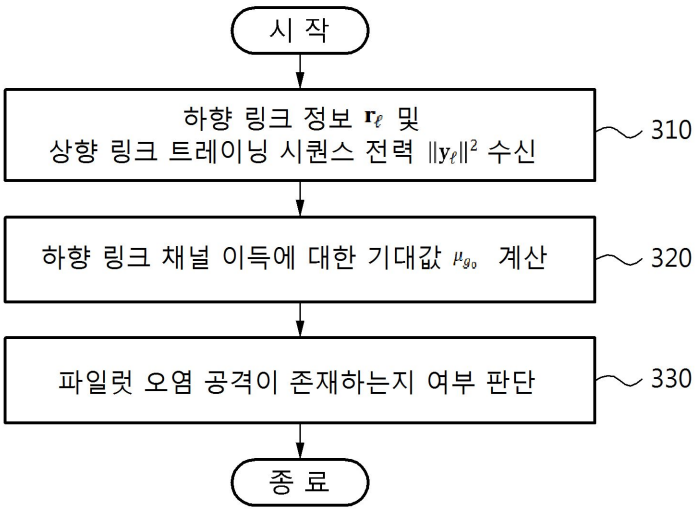
도면1



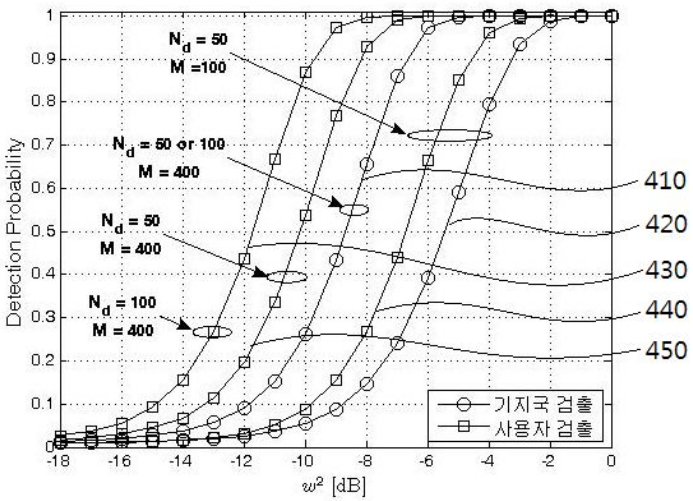
도면2


시 작
복수의 사용자 단말들로부터 신호 Y 수신
210
채널 추정 정보 $\mathbf{y}_\ell$ 추출
220
상향 링크 트레이닝 시퀀스 전력 $\|\mathbf{y}_\ell\|^2$ 획득
230
파일럿 오염 공격이 존재하는지 여부 판단
240
종 료

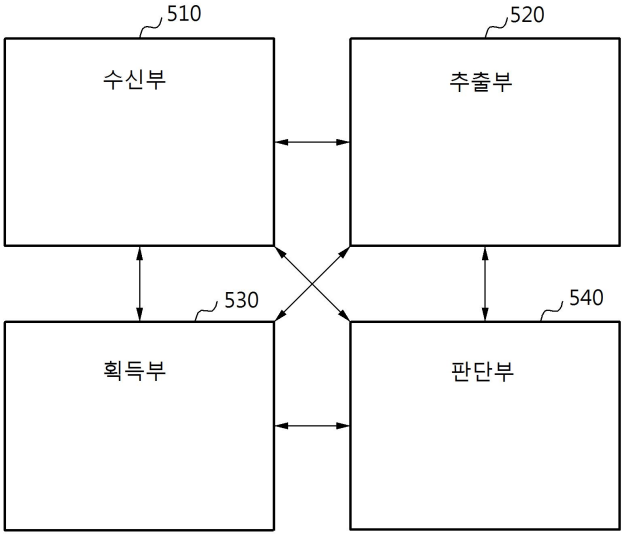
도면3


시 작
하향 링크 정보 $\mathbf{r}_\ell$ 및
상향 링크 트레이닝 시퀀스 전력 $\|\mathbf{y}_\ell\|^2$ 수신
310
하향 링크 채널 이득에 대한 기대값 μ_{g_0} 계산
320
파일럿 오염 공격이 존재하는지 여부 판단
330
종 료

도면4


Detection Probability
ω² [dB]
N_d = 50
M =100
N_d = 50 or 100
M = 400
N_d = 50
M = 400
N_d = 100
M = 400
410
420
430
440
450
기지국 검출
사용자 검출

도면5


510
520
수신부
추출부
530
540
획득부
판단부

도면6