



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0102758
(43) 공개일자 2013년09월23일

(51) 국제특허분류(Int. Cl.)
H04K 3/00 (2006.01) H04B 7/06 (2006.01)
(21) 출원번호 10-2012-0023840
(22) 출원일자 2012년03월08일
심사청구일자 없음

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스
내 (서천동, 경희대학교)
(72) 발명자
신현동
경기도 수원시 영통구 영통동 청명마을주공아파트
404동 901호
정영민
경기도 성남시 분당구 야탑3동 매화마을 313동
305호
(74) 대리인
특허법인 신지

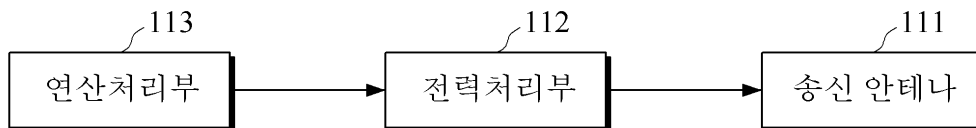
전체 청구항 수 : 총 9 항

(54) 발명의 명칭 무선 환경에서 보안 전송 방법 및 이를 구비한 송신장치

(57) 요약

본 발명에 따른 송신장치가 허가된 수신장치에 데이터를 보안 송신장치는 비밀 정보를 포함하는 비밀 신호와 전파 방해하는 인공 잡음이 포함된 송신 신호에서 비밀 신호와 인공 잡음 사이의 전력 할당비를 계산하는 연산처리부와 계산된 전력 할당비에 따라 송신 신호에 포함된 비밀 신호와 인공 잡음에 송신 전력을 온-오프로 할당하는 전력처리부 및 전력처리부로부터 수신된 송신 신호를 허가된 수신장치로 빔포밍하는 다수 개의 송신 안테나를 포함한다. MISOME가 존재하는 무선통신 환경에 있어서, 비밀 신호를 인공 잡음이 포함된 빔포밍을 통해 전송함으로써 보안 통신 환경을 제공한다. 또한, 비밀 신호와 인공 잡음 사이에 전력 할당을 송신전력을 온-오프 제어하여 할당하는 최적 전력 할당 기법을 통하여 보안 전송률을 높일 수 있다.

대표도 - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 2010-0014773

부처명 교육과학기술부

연구사업명 기초연구사업, 중견연구자지원사업

연구과제명 이중 무선 네트워크를 위한 네트워크 간섭제어 기술 및 다중접속 채널코딩 기술 개발

주관기관 경희대학교

연구기간 2011.05.01 ~ 2012.04.30

특허청구의 범위

청구항 1

다중 입력 단일 출력 다중 도청장치가 존재하는 무선 환경에서 허가된 수신장치에 데이터를 송신하는 보안 송신 장치는,

정보를 포함하는 비밀 신호와 전파 방해로 하는 인공 잡음이 포함된 송신 신호에서 상기 비밀 신호와 상기 인공 잡음 사이의 전력 할당비를 계산하는 연산처리부;

상기 계산된 전력 할당비에 따라 상기 송신 신호에 포함된 상기 비밀 신호와 상기 인공 잡음에 송신 전력을 온-오프로 할당하는 전력처리부; 및

상기 전력처리부로부터 수신된 상기 송신 신호를 상기 허가된 수신장치로 빔포밍하는 다수 개의 송신 안테나;

를 포함하는 것을 특징으로 하는 보안 송신장치.

청구항 2

제 1항에 있어서,

상기 비밀 신호에 대한 접근 권한은 상기 송신 신호의 상기 비밀 신호와 상기 인공 잡음 사이의 상기 신호 대 잡음비에 의해 결정되는 것을 특징으로 하는 보안 송신장치.

청구항 3

제 1항에 있어서,

상기 송신 신호의 보안 효과는 델타 보안 심볼 오류 확률(δ -Secrecy Symbol Error Probability)을 이용하여 평가하는 것을 특징으로 하는 보안 송신장치.

청구항 4

제 1항에 있어서,

상기 전력 할당비는 도청장치의 신호 대 잡음비의 비율에 따라 변화되는 것을 특징으로 하는 보안 송신장치.

청구항 5

제 1항에 있어서,

상기 도청장치는 상기 비밀 신호와 상기 인공 잡음을 포함하는 송신 신호를 수신하는 것을 특징으로 하는 보안 송신장치.

청구항 6

제 1항에 있어서,

상기 수신장치는 상기 비밀 신호만을 수신하는 것을 특징으로 하는 보안 송신장치.

청구항 7

다중 입력 단일 출력 다중 도청장치가 존재하는 무선 환경에서 송신장치가 데이터를 보안 송신하는 방법에 있어서,

비밀 정보를 포함하는 비밀 신호와 전파 방해로 하는 인공 잡음이 포함된 송신 신호 사이의 전력 할당비를 계산하는 단계;

상기 전력 할당비에 따라 상기 송신 신호에 송신 전력을 할당하는 단계; 및

상기 송신 전력이 할당된 송신 신호를 빔포밍(Beamforming)하는 단계;

를 포함하는 것을 특징으로 하는 보안 송신 방법.

청구항 8

제 7항에 있어서,

상기 전력 할당비에 따라 상기 송신 신호에 송신 전력을 할당하는 단계에서,

상기 송신 전력은 온-오프 방법으로 할당하는 것을 특징으로 하는 보안 송신 방법

청구항 9

제 8항에 있어서,

상기 온-오프 방법의 문턱값(Threshold)은 상기 송신장치의 안테나, 상기 도청장치의 안테나, 상기 수신장치의 신호 대 잡음비 및 상기 도청장치의 신호 대 잡음비를 이용하여 설정되는 것을 특징으로 하는 보안 송신 방법.

명세서

기술분야

[0001] 본 발명은 무선통신 환경에서 보안 전송률을 최적화하기 위한 보안 전송 기술에 관한 것이다.

배경기술

[0002] 최근 무선통신 관련 기술이 빠르게 발전하며 다양한 형태의 무선 통신 네트워크가 구축되고 있다. 무선통신은 전자기파를 이용하여 대기로 신호를 송출하거나 대기 중의 신호를 수신하여 통신을 수행하는 방식이다. 따라서 허가되지 않은 제 3자가 수신대상과 근접하여 위치하고 수신대상으로 송신되는 신호의 부호화 방식을 알고 있다면, 송신 신호를 도청하여 둘 사이의 비밀 정보를 쉽게 빼낼 수 있는 위험을 가지고 있다.

[0003] 일반적으로 데이터를 주고 받는 통신 노드 사이에 공유된 암호화키를 사용하여 신호를 스크램블(Scramble)하는 보안 방법을 이용하여 무선통신에서의 보안을 유지하고 있다. 이러한 보안 형태는 허가되지 않은 제 3자가 신호를 해독하기 어렵게 만드는 암호화 프로토콜(Cryptographic Protocol)을 사용한다.

[0004] 하지만 송신자와 수신자가 통신을 수행하는 과정에서, 허가되지 않은 제 3자가 둘 사이에서 송수신되는 데이터를 도청하는 통신 모델을 와이너에 의해 처음으로 제안되었다. 그 후로도 무선통신의 브로드캐스팅(Broadcasting) 특성 때문에 무선통신에서의 보안 전송률을 높이기 위한 방안들이 연구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 다중 입력 단일 출력 방식을 따르는 다수 개의 도청장치(150)(Multi Input Single Output Multiple Eavesdropper, MISOME)가 존재하는 무선 통신 환경에서 비밀 정보가 담겨있는 비밀 신호를 수신장치(130)에 송신하는 과정에서 도청장치(150)에 의한 도청을 차단하면서도 보안 전송률을 최대화 할 수 있는 전력할당 기법과 이러한 보안 방법이 구비된 송신장치(110)를 제공한다.

과제의 해결 수단

[0006] 본 발명에 따른 송신장치가 허가된 수신장치에 데이터를 보안 송신장치는 비밀 정보를 포함하는 비밀 신호와 전파 방해를 하는 인공 잡음이 포함된 송신 신호에서 비밀 신호와 인공 잡음 사이의 전력 할당비를 계산하는 연산 처리부와 계산된 전력 할당비에 따라 송신 신호에 포함된 비밀 신호와 인공 잡음에 송신 전력을 온-오프로 할당하는 전력처리부 및 전력처리부로부터 수신된 송신 신호를 허가된 수신장치로 빔포밍하는 다수 개의 송신 안테나를 포함한다.

[0007] 송신장치는 합법 채널의 송신 장치에 따른 에르고딕 레일리 페이딩 채널 이득(Ergodic Rayleigh-fading channel gains)에 따라 최대값을 가지는 보안 전송률을 계산한다. 그리고 보안 전송률을 바탕으로 최적 전력 할당비를 계산한다. 다음으로, 송신장치는 최적 전력 할당비에 따라 다중 채널의 송신신호에 송신전력을 온-오프로 할당한다. 이 때, 온-오프를 결정짓는 문턱값(threshold)은 송신장치의 안테나 수와 도청장치의 안테나 수 및 수신

장치와 도청장치의 신호 대 잡음비를 이용하여 설정된다. 다음으로, 전력 할당비에 따라 송신전력이 할당된 송신신호를 허가된 수신장치를 향하여 빔포밍한다.

발명의 효과

- [0008] 본 발명에 따르면, MISOME가 존재하는 무선통신 환경에 있어서, 비밀 신호를 인공 잡음이 포함된 빔포밍을 통해 전송함으로써 보안 통신 환경을 제공한다. 또한, 비밀 신호와 인공 잡음 사이에 전력 할당을 송신전력을 온-오프 제어로 할당하는 최적 전력 할당 기법을 통하여 보안 전송률을 높일 수 있다.

도면의 간단한 설명

- [0009] 도 1은 본 발명의 일 실시예에 따른 무선 보안 통신 시스템(100)을 도시한 구성도이다.
 도 2는 일 실시예에 따른 송신장치(110)의 세부 구성도이다.
 도 3은 일 실시예에 따른 송신장치의 데이터 송신방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0010] 이하, 첨부된 도면들을 참조하여 본 발명의 실시예를 상세하게 설명한다. 본 명세서에서 사용되는 용어들은 실시예에서의 기능을 고려하여 선택된 용어들로서, 그 용어의 의미는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 후술하는 실시예들에서 사용된 용어의 의미는, 본 명세서에 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우는 당업자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.
- [0011] 도 1은 본 발명에 따른 송신장치(110)가 구비된 무선 보안 통신 시스템(100)을 도시한 구성도이다.
- [0012] 도 1을 참조하면, 본 발명에 따른 송신장치(110)가 구비된 무선 보안 통신 시스템(100)은 송신장치(110), 수신장치(130) 및 도청장치(150)를 포함한다.
- [0013] 본 발명은 다중 입력 단일 출력 형태의 다중 도청장치(150)(Multi Input Single Output Multiple Eavesdropper, MISOME)가 존재하는 무선 통신 환경에서 비밀 정보가 담겨있는 비밀 신호를 수신장치(130)에 송신하는 과정에서 도청장치(150)에 의한 도청을 차단하여 보안성을 지킬 수 있는 방법과 이러한 보안 방법이 구비된 송신장치(110)를 제공한다.
- [0014] 송신장치(110)는 다수 개의 송신 안테나(111)를 구비하고, 송신 안테나(111)를 이용하여 수신장치(130)로 비밀 신호를 전송한다. 송신 장치(110)로부터 전송되는 신호는 비밀 신호(Confidential Signal)과 인공 잡음(Artificial Noise)를 포함한다. 비밀 신호는 보안을 필요로 하는 정보가 포함된 신호를 나타낸다. 인공 잡음은 무선 통신환경에서 보안성을 유지하기 위하여 만들어진 인공적인 잡음(Noise)로서, 신호에 포함되어 방해전파(Jammer) 역할을 한다. 송신장치(110)에서 송신되는 신호는 빔포밍(Beamforming) 기법을 이용하여 허가된 수신장치(130)를 향해서 신호를 송신한다.
- [0015] 수신장치(130)는 단일 안테나(131)를 구비하고, 송신장치(110)로부터 전송된 신호를 수신한다. 수신장치(130)로 수신된 신호는 빔포밍 기법에 의하여 방해전파 역할을 하는 인공 잡음이 배제된 비밀 신호만을 포함한다.
- [0016] 도청 장치(150)는 다중 입력 단일 출력 방식을 따르는 다수 개의 도청장치(Multi Input Single Output Multiple Eavesdropper, MISOME)이다. 송신장치(110)의 신호 송신 범위 내에 위치하며, 송신장치(110)에서 수신장치(130)로 송신되는 신호를 허가 받지 않고 다수의 도청 안테나(151)를 이용하여 도청한다. 송신장치(110)에서 송신되는 신호는 허가된 수신장치(130)에 대하여 빔포밍 기법을 적용하여 송신하기 때문에, 도청 장치(150)에서 다수의 안테나(151)를 이용하여 도청한 신호는 수신장치(130)에서 수신한 신호와 달리 비밀 신호와 인공 잡음이 모두 포함되어 있다. 따라서 도청장치(150)에서 도청한 신호는 인공 잡음에 의한 전파방해 때문에 비밀 신호를 완전하게 복원 할 수 없다.
- [0017] 도 2는 일 실시예에 따른 송신장치(110)의 세부 구성도이다.
- [0018] 도 2를 참조하면, 송신장치(110)는 연산처리부(113), 전력처리부(112) 및 다수 개의 송신 안테나(111)를 포함한다.
- [0019] 연산처리부(113)는 보안을 필요로 하는 정보가 포함된 비밀 신호와 도청장치에 의한 도청 방지를 위한 인공잡음

사이의 전력량을 조절하여 보안 전송률을 최대화 할 수 있는 최적의 전력 할당비를 계산한다.

- [0020] 전력처리부(112)는 연산처리부에 의해 결정된 비밀 신호와 인공 잡음의 전력 할당비에 따라 비밀 신호와 인공 잡음에 전력을 할당 할 수 있다. 채널 이득 파라미터의 크기와 도청 장치에 따라 미리 설정된 문턱값(Threshold)을 비교하여 온-오프(On-off)로 할당한다.
- [0021] 송신 안테나(111)는 송신장치에 다수 개가 구비되며, 전력처리부(112)에서 전력을 할당한 비밀 신호와 인공 잡음이 포함된 신호를 빔포밍 방법을 사용하여 허가된 수신장치로 송신한다.
- [0022] 인공 잡음이 포함된 빔포밍 기법에 의해 송신되는 신호 중에서 비밀 신호에는 채널 상태 정보(Channel Status Information, CSI)가 포함되어 있다. 비밀 신호는 채널 상태 정보가 완전한 정보(Full Channel Status Information)를 가지고 있을 경우, 데이터가 복원된다. 허가된 수신장치(130)로 송신된 신호는 인공 잡음을 거의 포함하지 않은 비밀 신호를 포함한다. 따라서, 완전한 채널 상태 정보를 가지고 데이터에 접근하기 때문에, 완전한 데이터를 복원할 수 있다. 하지만 도청장치(150)로 송신된 신호는 인공 잡음을 포함하여 완전한 채널 상태 정보가 아닌 단편적인 채널 상태 정보만을 가지고 있기 때문에, 완전한 데이터를 복원할 수 없다. 결국 비밀 신호에 대한 접근 권한은 수신된 신호에 있어서 비밀 신호와 인공 잡음 사이의 신호 대 잡음비(Signal to Noise power Ratio)에 의해 결정 될 수 있다.
- [0023] 송신장치(110)는 비밀 신호와 인공 잡음 사이의 신호 대 잡음비를 온-오프 전력제어를 통해 두 신호 사이의 전력량을 조절하여 할당한다. 송신장치(110)로부터 송신되는 신호에서 인공 잡음의 비율이 높아지면 보안성도 함께 높아질 수 있다. 하지만 한정된 채널 용량을 갖는 신호에서 인공 잡음의 비율이 높아지면 비밀 신호의 비율이 낮아지게 된다. 여기에서 채널 용량이란 데이터가 오류 없이 채널을 통해 상대방으로 송신되는 최대 데이터 전송률, 즉 비밀 신호와 인공 잡음을 포함하는 송신장치(110)가 송신할 수 있는 정보 송신 능력을 의미한다. 따라서 송신장치(110)는 최대 보안 전송률을 가지기 위하여 최적의 전력 할당 비를 가지도록 두 신호의 전력을 할당한다. 보안 전송률이란 데이터가 도청장치(150)의 도청 없이 합법 채널을 통해 허가된 수신장치(130)로 송신되는 최대 데이터 전송률, 즉 송신장치(110)로 송신되는 비밀 신호의 비율을 나타낸다.
- [0024] 도 3은 일 실시예에 따른 송신장치의 데이터 송신방법을 도시한 흐름도이다.
- [0025] 도 3을 참조하면, 송신장치는 합법 채널의 송신 장치에 따른 에르고딕 레일리 페이딩 채널 이득(Ergodic Rayleigh-fading channel gains)에 따라 최대값을 가지는 보안 전송률을 계산한다(301). 그리고 보안 전송률을 바탕으로 최적 전력 할당비를 계산한다(302). 본 발명의 일실시예에 따른 송신장치는 송신되는 신호에 포함된 비밀 신호와 인공 잡음 사이의 비율을 조절하여 보안성을 유지한다. 비밀 신호의 비율이 높아지면 도청장치에 의해 도청될 가능성이 높아질 수 있기 때문에, 비밀 신호와 인공 잡음의 비율을 조절할 필요가 있다. 따라서, 최대의 보안 전송률을 가지는 최적 전력 할당비를 계산한다.
- [0026] 다음으로, 송신장치는 최적 전력 할당비에 따라 다중 채널의 송신신호에 송신전력을 온-오프로 할당한다(303). 일 실시예에 따르면 안테나 수와 최적 전력 할당비에 기초하여 비밀 신호와 인공 잡음에 전력을 할당한다. 이때, 온-오프를 결정짓는 문턱값(threshold)은 송신장치의 안테나 수와 도청장치의 안테나 수 및 수신장치와 도청장치의 신호 대 잡음비를 이용하여 설정된다.
- [0027] 다음으로, 전력 할당비에 따라 송신전력이 할당된 송신신호를 허가된 수신장치를 향하여 빔포밍한다(304).
- [0028] 본 발명의 일실시예에 따른 송신장치(110)에 있어서, 비밀 신호와 인공 잡음 사이에 신호 대 잡음비를 각 신호의 전력을 통해 제어 할 때, 최대의 보안 전송률을 가질 수 있는 최적 전력 할당 기법은 후술하는 수식들을 참조하여 설명한다.
- [0029] 우선, 본 발명은 송신장치(110)는 다수 개의 송신 안테나(111)를 이용하여 인공 잡음이 포함된 빔포밍을 이용하여 신호를 단일 안테나를 가지는 수신장치(130)로 송신하고, 다중 입력 단일 출력 방식을 따르는 다중 도청 장치(150)는 n_e 개의 도청 안테나(151)를 이용하여 송신장치(110)로부터 송신된 신호를 도청한다고 가정한다. 이때, 수신장치(130)와 도청장치(150)로 수신되는 신호는 각각 식 1 및 식 2와 같다.

수학식 1

$$y_r = \sqrt{\frac{\text{snr}_r}{n_t}} \mathbf{h}_r \mathbf{x} + z_r$$

[0030]

수학식 2

$$y_e = \sqrt{\frac{\text{snr}_e}{n_t}} \mathbf{H}_e \mathbf{x} + \mathbf{z}_e$$

[0031]

[0032] 식 1 및 식 2에 있어서, y_r 은 수신장치(130)가 허가된 합법 채널을 통해 수신하는 신호를 나타내고, y_e 는 도청장치(150)가 허가 받지 않은 도청 채널을 통해 수신하는 신호를 나타낸다. 여기에서 합법 채널은 송신장치(110)으로부터 수신장치(130)으로 신호가 송신되는 허가된 통신 채널을 의미하고, 도청 채널은 도청장치(150)에 의하여

허가 받지 않은 도청 채널을 의미한다. $\mathbf{x} \in \mathbb{C}^{n_t}$ 은 전력 제한 $\mathbb{E}\{\mathbf{x}^\dagger \mathbf{x}\} = 1$ 을 충족시키는 전송 신호,

$\mathbf{h}_r \sim \tilde{\mathcal{N}}_{1, n_t}$ 는 합법 채널의 에르고딕 레일리 페이딩 채널 이득(Ergodic Rayleigh-fading channel gains),

$\mathbf{H}_e \sim \tilde{\mathcal{N}}_{n_e, n_t}$ 는 도청 채널의 에르고딕 레일리 페이딩 채널 이득, snr_r 은 수신장치(130)에 대한 평균 신호

대 잡음비, snr_e 는 도청장치(150)에 대한 평균 신호 대 잡음비, $z_r \sim \tilde{\mathcal{N}}_{1, 1}$ 는 수신장치(130)가 수신한 신호

의 부가 백색 가우스 잡음(Additive White Gaussian Noise), $\mathbf{z}_e \sim \tilde{\mathcal{N}}_{n_e, 1}$ 는 도청장치(150)가 수신한 신호

의 부가 백색 가우스 잡음, n_t 는 송신장치(110)의 안테나 수를 나타낸다. 그리고 $\mathbf{x}$, $\mathbf{h}_r$, $\mathbf{H}_e$, z_r 및 $\mathbf{z}_e$ 는 상호 독립적이다.

[0033] 비밀 통신에 있어서, 송신장치는 도청 장치에 간섭을 일으키는 인공 잡음을 사용할 수 있다. 본 발명에서, 전송 신호는 식 3과 같이 송신된 신호는 정보를 포함하는 비밀 신호와 인공 잡음으로 분리 될 수 있다.

수학식 3

$$\mathbf{x} = \sqrt{\lambda} \mathbf{u}_I s_I + \sqrt{\frac{1-\lambda}{n_t-1}} \mathbf{U}_A \mathbf{s}_A$$

[0034]

수학식 4

$$\mathbb{E}\{|s_I|^2\} = \mathbb{E}\{\|\mathbf{s}_A\|^2\} = 1$$

[0035]

[0036] 식 4는 전력 제한을 나타내는 수식으로 최대 전력 제한의 값은 1이다. $\mathbf{x}$ 는 비밀 신호와 인공 잡음으로 구성된 전송 신호를 나타낸다. $s_I \in \mathbb{C}$ 는 식 4의 전력 제한을 충족시키는 비밀 신호의 전송 신호,

$\mathbf{s}_A \sim \tilde{\mathcal{N}}_{n_t-1,1}$ 는 식 4의 전력 제한을 충족시키는 인공 잡음의 전송 신호, $\mathbf{u}_I$ 는 비밀 신호의 $n_t \times 1$ 의 형태를 가지는 빔포밍 벡터(Beamforming Vector), $\mathbf{U}_A$ 는 인공 잡음의 n_t 행 및 $(n_t - 1)$ 열을 가지는 빔포밍 행렬(Beamforming Matrix), λ 는 비밀 신호의 전력 할당 비를 나타낸다. $1 - \lambda$ 는 전력 제한 값 1에서 비밀 신호의 전력 할당 비 λ 를 뺀 값으로, 결국 λ 와 $1 - \lambda$ 는 비밀 신호와 인공 잡음 사이의 전력 할당 비를 의미한다. 전송한 내용과 같이 합법 채널을 통한 송신 신호는 완전한 채널 상태 정보를 가지고, 도청 채널은 단편적인 채널 상태 정보를 가진다. 단편적인 채널 상태 정보에 의해 채널 상태 정보의 통계량 지식을 참조한다고 가정하면, $\mathbf{u}_I = \mathbf{h}_r^\dagger / \|\mathbf{h}_r\|$ 즉 도청 장치가 없는 경우에 최적 빔포밍 벡터를 선택하는 것이 합리적이다. 허가된 수신장치는 채널 상태 정보의 통계량 지식을 참조하지 않기 때문에, $\mathbf{U}_A$ 는 $\mathbf{h}_r^\dagger$ 의 영공간(Null Space)에서 선택된다. 이러한 경우, 수신장치와 도청장치에 수신된 신호는 각각 식 5 및 식 6과 같다.

수학식 5

$$\mathbf{y}_r = \sqrt{\lambda \frac{\text{snr}_r}{n_t}} \|\mathbf{h}_r\| \mathbf{s}_I + \mathbf{z}_r$$

[0037]

수학식 6

$$\mathbf{y}_e = \sqrt{\lambda \frac{\text{snr}_e}{n_t}} \mathbf{g}_I \mathbf{s}_I + \sqrt{\frac{1 - \lambda}{n_t - 1} \frac{\text{snr}_e}{n_t}} \mathbf{G}_A \mathbf{s}_A + \mathbf{z}_e$$

[0038]

식5 및 식6은 $\mathbf{g}_I \triangleq \mathbf{H}_e \mathbf{u}_I$ 과 $\mathbf{G}_A \triangleq \mathbf{H}_e \mathbf{U}_A$ 을 만족한다. $[\mathbf{u}_I \ \mathbf{U}_A]$ 는 유니테리 행렬(Unitary Matrix)이기 때문에, $\mathbf{g}_I \sim \tilde{\mathcal{N}}_{n_e,1}$ 와 $\mathbf{G}_A \sim \tilde{\mathcal{N}}_{n_e, n_t-1}$ 는 독립적이다. 결국 가우시안 부호록(Gaussian Code Book)을 사용하여 주어진 $\mathbf{h}_r$ 에 대한 보안 전송률 R_s 는 식 7과 같다.

수학식 7

$$R_s = \max_{0 \leq \lambda \leq 1} \mathbb{E}_G \left\{ \underbrace{\ln \left(1 + \lambda \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2 \right) - \ln \left(1 + \lambda \frac{\text{snr}_e}{n_t} \mathbf{g}_I^\dagger \left(\mathbf{I} + \frac{1 - \lambda}{n_t - 1} \frac{\text{snr}_e}{n_t} \mathbf{G}_A \mathbf{G}_A^\dagger \right)^{-1} \mathbf{g}_I \right)}_{\triangleq R(\lambda)} \right\}$$

[0040]

여기에서, $\mathbf{G} = [\mathbf{g}_I \ \mathbf{G}_A]$.³을 만족한다.

[0041]

본 발명은 식 7의 최대의 보안 전송률을 달성할 수 있는 최적 전력 할당 기법을 제시한다. 먼저 낮은 SNR(low-SNR)을 가지는 약한(Weak) 도청장치 또는 높은 SNR(high-SNR)을 가지는 강한(Strong) 도청장치에 대한 최대 보안 전송률(식7)을 달성할 수 있는 최적 전력 할당을 결정한다.

[0042]

[0043] 최대 보안 전송률 R_s 를 성취할 수 있는 최적 전력 할당은 식 7에 의해 구할 수 있다. 하지만 전력 할당 비 λ 중에서 최대 보안 전송률을 가지는 최적 전력 할당 비 λ^* 는 $R(\lambda)$ 의 비 볼록형(Non-convexity) 때문에 분석적으로 결정하기 어렵다. 먼저, 약한 도청장치 또는 강한 도청장치를 위한 전력 할당 문제를 해결하고 이 결과를 일반적인 경우에 있어서, 근사 최적(Near-optimal) 해법으로 확장한다.

[0044] 약한 도청장치는 신호 대 잡음비 값이 1보다 아주 작은 도청장치를 의미한다. 이러한 경우, snr_e 의 값이 매우 작아지기 때문에 결국 식 8과 같이 가정할 수 있다.

수학식 8

$$\left(\mathbf{I} + \frac{1 - \lambda}{n_t - 1} \frac{\text{snr}_e}{n_t} \mathbf{G}_A \mathbf{G}_A^\dagger \right)^{-1} \approx \mathbf{I}$$

[0045]

[0046] 식 8에서 $W \sim \text{Erl}(n_e, 1)$ 로 놓으면, 식 7은 식 9와 같이 다시 변형이 가능하다.

수학식 9

$$R_s \approx \max_{0 \leq \lambda \leq 1} \left[\underbrace{\ln \left(1 + \lambda \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2 \right) - \mathbb{E}_W \left\{ \ln \left(1 + \lambda \frac{\text{snr}_e}{n_t} W \right) \right\}}_{\triangleq R_\downarrow(\lambda)} \right]$$

[0047]

[0048] 신호 대 잡음비 값이 1보다 작은 약한 도청장치에 있어서, $\lambda \in [0, 1]$ 인 조건에서 최대의 보안 전송률 $R_\downarrow(\lambda)$ 을 가지는 최적 전력 할당 비 $\lambda_\downarrow^*$ 는 식 10과 같다.

수학식 10

$$\lambda_\downarrow^* = \arg \max_{0 \leq \lambda \leq 1} R_\downarrow(\lambda)$$

[0049]

수학식 11

$$\zeta_\downarrow = \exp \left\{ e^{\frac{\text{snr}_r}{n_t}} \sum_{n=1}^{n_e} E_n \left(\frac{n_t}{\text{snr}_e} \right) \right\} - 1$$

[0050]

[0051] 식 11은 약한 도청장치 일 때 설정된 문턱값(Threshold) $\zeta_\downarrow$ 을 나타낸다. 식11의 문턱값을 가질 때, 최적 전력 할당 비 $\lambda_\downarrow^*$ 는 식12의 온-오프(On-off) 전력 할당 값을 가진다.

수학식 12

$$\lambda_{\downarrow}^* = \begin{cases} 1, & \text{if } \|\mathbf{h}_r\|^2 \geq \zeta_{\downarrow} \\ 0, & \text{otherwise} \end{cases}$$

[0052]

[0053] 식 12에 따르면, 송신장치는 수신장치의 합법 채널의 채널 이득 파라미터 크기 $\|\mathbf{h}_r\|^2$ 가 기설정된 문턱값 $\zeta_{\downarrow}$ 보다 크거나 동일하면 송신전력을 1로 할당하고, 문턱값 $\zeta_{\downarrow}$ 보다 작으면 송신전력을 0으로 할당한다.

[0054] 낮은 신호 대 잡음비를 가지는 도청장치에서, 송신장치는 모든 전력을 비밀 신호의 전송을 위해 사용한다. 이러한 경우, 열잡음(Thermal Noise)이 도청장치가 신호를 수신하는 것을 충분히 방해하기 때문에 도청장치에 간섭을 일으키는 인공 잡음을 사용할 필요가 없다. 결과적으로, 온-오프 전력 할당 값은 최적화된다.

[0055] n_e 와 snr_e 에 따라 온-오프 문턱값 $\zeta_{\downarrow}$ 는 증가하는 반면에, snr_r 에 따라 온-오프 문턱값 $\zeta_{\downarrow}$ 은 거꾸로 감소한다. snr_r 과 snr_e 값을 0으로 수렴시키면 식 13을 얻을 수 있다.

수학식 13

$$\begin{aligned} \lim_{\substack{\text{snr}_r, \text{snr}_e \rightarrow 0 \\ \text{snr}_e \rightarrow \alpha \\ \text{snr}_r \rightarrow \alpha}} \zeta_{\downarrow} &= \alpha \lim_{z \rightarrow \infty} z \left[\exp \left\{ e^z \sum_{n=1}^{n_e} E_n(z) \right\} - 1 \right] \\ &\stackrel{(a)}{=} \alpha \lim_{z \rightarrow \infty} e^z z \sum_{n=1}^{n_e} E_n(z) \\ &\stackrel{(b)}{=} \alpha \lim_{z \rightarrow \infty} \sum_{n=1}^{n_e} [1 - n E_{n+1}(z) e^z] \\ &= n_e \alpha \end{aligned}$$

[0056]

[0057] 다시 말해서, 이러한 특성은 합법 송신에 의한 전송 주파수가 snr_r 에 따라 증가함을 암시한다.

[0058] 강한(Strong) 도청장치는 도청 장치의 신호 대 잡음비 snr_e 가 1보다 큰 경우($\text{snr}_e \gg 1$)를 의미한다. 이러한 경우 식 14와 같이 가정할 수 있다.

수학식 14

$$\left(\mathbf{I} + \frac{1 - \lambda}{n_t - 1} \frac{\text{snr}_e}{n_t} \mathbf{G}_A \mathbf{G}_A^\dagger \right)^{-1} \approx \frac{n_t - 1}{1 - \lambda} \frac{n_t}{\text{snr}_e} \left(\mathbf{G}_A \mathbf{G}_A^\dagger \right)^{-1}$$

[0059]

[0060] 그리고 $Z = \mathbf{g}_I^\dagger (\mathbf{G}_A \mathbf{G}_A^\dagger)^{-1} \mathbf{g}_I$ 로 표현하면, $\text{snr}_r \gg 1$ 인 경우 식 7은 식 15로 표현할 수 있다.

수학식 15

$$R_s \approx \max_{0 \leq \lambda \leq 1} \left[\ln \left(\lambda \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2 \right) - \mathbb{E}_Z \left\{ \ln \left(1 + \frac{(n_t - 1)\lambda}{1 - \lambda} Z \right) \right\} \right]$$

$$= \max_{\kappa \geq 1} \underbrace{\left[\ln \left(\frac{1}{\kappa} \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2 \right) - \mathbb{E}_Z \left\{ \ln \left(1 + \frac{n_t - 1}{\kappa - 1} Z \right) \right\} \right]}_{\triangleq R_\uparrow(\kappa)}.$$

[0061]

수학식 16

$$\kappa^* = \arg \max_{\kappa \geq 1} R_\uparrow(\kappa)$$

[0062]

[0063] 신호 대 잡음비 값이 1보다 큰 강한 도청장치에 있어서, $\kappa \in [1, \infty]$ 인 조건에서 최대의 보안 전송률 $R_\uparrow(\kappa)$ 을 가지는 최적 전력 할당 비 κ^* 는 식 16과 같다. 식 17은 강한 도청장치의 문턱값 $\zeta_\uparrow$ 을 나타낸다.

수학식 17

$$\zeta_\uparrow = \frac{n_t}{\lambda_\uparrow^* \text{snr}_r} \left[\exp \left\{ \mathbb{E}_{Z_{\lambda_\uparrow^*}} \left\{ \ln \left(1 + \lambda_\uparrow^* \frac{\text{snr}_e}{n_t} Z_{\lambda_\uparrow^*} \right) \right\} \right\} - 1 \right]$$

$$= \frac{n_t}{\lambda_\uparrow^* \text{snr}_r} \left[\exp \left\{ \int_0^\infty \frac{\lambda_\uparrow^* \frac{\text{snr}_e}{n_t}}{1 + \lambda_\uparrow^* \frac{\text{snr}_e}{n_t} z} [1 - F_{Z_{\lambda_\uparrow^*}}(z)] dz \right\} - 1 \right]$$

$$= \frac{n_t}{\lambda_\uparrow^* \text{snr}_r} \left[\exp \left\{ \sum_{i=0}^{n_e-1} \sum_{j=0}^{n_e-1-i} \binom{n_t-1}{j} \frac{a_{\lambda_\uparrow^*}^j}{i!} \mathcal{I}_{n_t-1}^{i+j} \left(0, \lambda_\uparrow^* \frac{\text{snr}_e}{n_t}, a_{\lambda_\uparrow^*} \right) \right\} - 1 \right]$$

[0064]

[0065] 만약 $n_e = n_t - 1$ 인 경우 최적 κ^* 값은 식 18과 같은 고유한(Unique) 값을 나타낸다.

수학식 18

$$\kappa^* = n_t$$

[0066]

[0067] 만약 $n_e < n_t - 1$ 인 경우, κ^* 는 $\kappa \in \mathcal{A}$ 한 조건에서 식 19과 같은 해를 얻는다. $\mathcal{A}$ 는 식 20와 같다.

수학식 19

[0068]

$$\frac{1}{\kappa-1} - \frac{1}{\kappa} - \frac{n_t - n_e}{n_t(n_t - n_e)} {}_2F_1\left(1, n_t - n_e + 1; n_t + 1; \frac{n_t - \kappa}{n_t - 1}\right) = 0$$

수학식 20

[0069]

$$\mathcal{A} = \left[1 + \sqrt{\frac{(n_t-1)(n_e-1)}{n_t-n_e}}, 1 + \sqrt{\frac{(n_t-1)n_e}{n_t-1-n_e}} \right]$$

[0070]

높은 신호 대 잡음비를 가지는 강한 도청장치를 위한 최적 전력 할당비 $\lambda_{\uparrow}^*$ 는 $1/\kappa^*$ 와 같다. 이러한 최적 전력 할당비 값은 h_r 과 평균 SNRs 에 의존하지 않는다. 최적 전력 할당비 값은 단지 송신장치의 안테나 수 n_t 와 도청장치의 안테나 수 n_e 의 함수이다. 따라서 단순한 결정론적(deterministic) 전력 할당은 최대의 보안 전송률을 가지는데 충분하다. 강한 도청장치를 위한 어떠한 적응(Adaptive) 전력 할당도 시행할 필요가 없다.

[0071]

일반적으로 식7의 목적 함수가 비볼록형(Non0convexity)이기 때문에 분해적으로(Analytically) 전력 할당비의 최적값을 구하기 어렵다. 따라서, 전환(Switched) 전력 할당을 이용하여 최적 전력 할당비를 구한다.

수학식 21

[0072]

$$\lambda_s = \arg \max_{\lambda \in \{\lambda_{\uparrow}^*, \lambda_{\downarrow}^*\}} R(\lambda)$$

[0073]

변환 전력 할당에 있어서, 최적 전력 할당비 λ_s 는 식 21과 같다. 식 22은 변환 전력 할당의 문턱값 $\zeta_{\downarrow\uparrow}$ 를 나타낸다.

수학식 22

[0074]

$$\zeta_{\downarrow\uparrow} = \frac{n_t}{\text{snr}_r} \frac{\exp \left\{ \sum_{i=0}^{n_e-1} \left[e^{\frac{n_t}{\text{snr}_e}} E_{i+1} \left(\frac{n_t}{\text{snr}_e} \right) - \sum_{j=0}^{n_e-1-i} \binom{n_t-1}{j} \frac{a_{\lambda_{\uparrow}^*}^j}{j!} \mathcal{I}_{n_t-1}^{i+j} \left(0, \lambda_{\uparrow}^* \frac{\text{snr}_e}{n_t}, a_{\lambda_{\uparrow}^*} \right) \right] \right\} - 1}{1 - \lambda_{\uparrow}^* \exp \left\{ \sum_{i=0}^{n_e-1} \left[e^{\frac{n_t}{\text{snr}_e}} E_{i+1} \left(\frac{n_t}{\text{snr}_e} \right) - \sum_{j=0}^{n_e-1-i} \binom{n_t-1}{j} \frac{a_{\lambda_{\uparrow}^*}^j}{j!} \mathcal{I}_{n_t-1}^{i+j} \left(0, \lambda_{\uparrow}^* \frac{\text{snr}_e}{n_t}, a_{\lambda_{\uparrow}^*} \right) \right] \right\}}$$

[0075]

약한 도청장치, 강한 도청장치 및 변환 전력 할당의 문턱값 각각이 $\zeta_{\uparrow} < \zeta_{\downarrow} < \zeta_{\downarrow\uparrow}$ 을 만족하는 경우 변환 전력 할당의 전력 할당비 λ_s 는 식 23과 같다.

수학식 23

$$\lambda_s = \begin{cases} 1, & \text{if } \|h_r\|^2 \geq \zeta_{\downarrow\uparrow} \\ \lambda_{\uparrow}^*, & \text{if } \zeta_{\uparrow} < \|h_r\|^2 < \zeta_{\downarrow\uparrow} \\ 0, & \text{otherwise} \end{cases}$$

[0076]

[0077] 식 23에 따르면, 송신장치는 수신장치의 합법 채널의 채널 이득 파라미터 크기 $\|h_r\|^2$ 가 설정된 변환 전력 할당의 문턱값 $\zeta_{\downarrow\uparrow}$ 보다 크거나 동일하면 송신전력을 1로 할당한다. $\|h_r\|^2$ 가 변환 전력 할당의 문턱값 $\zeta_{\downarrow\uparrow}$ 보다 작고, 강한 도청장치의 문턱값 $\zeta_{\uparrow}$ 보다 크면 송신전력을 강한 도청장치를 위한 최적 전력 할당비 $\lambda_{\uparrow}^*$ 로 설정한다. 그리고 전술한 경우 이외에는 모두 송신전력을 0으로 할당한다.

[0078] 약한 도청장치, 강한 도청장치 및 변환 전력 할당의 문턱값 각각이 $\zeta_{\uparrow} < \zeta_{\downarrow} < \zeta_{\downarrow\uparrow}$ 을 만족하지 않는 경우, 변환 전력 할당의 전력 할당비 λ_s 는 식 24와 같다.

수학식 24

$$\lambda_s = \begin{cases} \frac{\zeta_{\min} - \zeta_{\downarrow}}{\zeta_{\uparrow} - \zeta_{\downarrow}} \lambda_{\uparrow}^* + \frac{\zeta_{\uparrow} - \zeta_{\min}}{\zeta_{\uparrow} - \zeta_{\downarrow}}, & \text{if } \|h_r\|^2 \geq \zeta_{\min} \\ 0, & \text{otherwise} \end{cases}$$

[0079]

[0080] 식 22에서 $\zeta_{\min}$ 는 $\zeta_{\min} = \min \{\zeta_{\downarrow}, \zeta_{\uparrow}\}$ 를 만족한다.

[0081] $\zeta_{\uparrow} < \zeta_{\downarrow} < \zeta_{\downarrow\uparrow}$ 를 만족하는 경우, 변환 전력 할당비 λ_s 를 위한 인공 잡음을 포함하는 보안 빔포밍을 얻을 수 있는 MISOME 레일리 페이딩 도청 채널의 에르고딕(Ergodic) 보안 전송률(nats/s/Hz)은 식 25와 같다.

수학식 25

$$\langle R_s \rangle = \mathcal{J}_{\zeta_{\uparrow}}^{\zeta_{\uparrow}} \left(\lambda_{\uparrow}^* \frac{\text{snr}_r}{n_t} \right) - \mathcal{J}_{\zeta_{\uparrow}}^{\zeta_{\downarrow}} \left(\lambda_{\uparrow}^* \frac{\text{snr}_r}{n_t} \right) + \mathcal{J}_{\zeta_{\downarrow\uparrow}}^{\zeta_{\downarrow}} \left(\frac{\text{snr}_r}{n_t} \right)$$

[0082]

[0083] 정보 이론적 관점에서 보면, 보안 통신에서 순간(Instantaneous) 보안 전송률은 목표 보안 전송률보다 낮다. 그러나 이러한 측정치는 합법 연결의 통신 신뢰도와 도청 연결과 반대되는 기밀성 사이에서 통찰력을 제공하지 못한다. 따라서 합법 통신에서 보안성과 신뢰성을 가지는 비밀 정보의 에러 확률에 대한 새로운 개념을 정의하였다. 그리고 보안 에러 확률에서 인공 잡음이 포함된 보안 빔포밍의 다이버시티 효과(Diversity Effect)를 분석한다.

[0084] 식 26의 Γ_r 는 합법 수신장치의 순간 SNR이고, 식 27의 Γ_e 는 도청장치의 순간 SINR이다.

수학식 26

[0085]
$$\Gamma_r = \lambda \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2$$

수학식 27

[0086]
$$\Gamma_r = \lambda \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2$$

[0087] 보안 점수(Secrecy Score) Δ_s 는 식 28과 같이 정의 된다.

수학식 28

[0088]
$$\Delta_s = \frac{1 + \Gamma_r}{1 + \Gamma_e}$$

[0089] 순간 보안 전송률은 $[\ln \Delta_s]^+$ 로 표현할 수 있기 때문에, 가우시안 신호에서 보안 점수는 완벽한 보안을 반영한다. M-PSK 또는 M-ary 구상 진폭 변조(Quadrature Amplitude modulation)와 같은 이산(Discrete) 신호에서, 보안 점수 Δ_s 는 도청 장치가 존재하는 환경에서 합법 통신을 보호하기 위한 보안 제약을 제공한다.

수학식 29

[0090]
$$\mathcal{SP}_e(\delta) = \mathbb{P} \left\{ \Delta_s < \delta \cup \{ \hat{s}_I \neq s_I, \Delta_s \geq \delta \} \right\}$$

[0091] 식 29의 델타 보안 심볼 오류 확률(δ -secrecy Symbol Error Probability, SEP) $\mathcal{SP}_e(\delta)$ 는 보안 점수 Δ_s 가 δ 보다 작을 경우 또는 Δ_s 가 δ 보다 클 때 합법 수신장치는 비밀 정보를 부정확하게 해독하는 경우의 두 가지 경우 중에 어느 하나의 경우에 대한 확률로 정의된다. $\hat{s}_I$ 는 합법 수신장치에서 해독된 정보, δ 는 비밀의 단계가 드러나는 파라미터이다.

[0092] 어떤 신호에서든, Δ_s 가 1보다 작다면 보안 제약은 보장할 수 없다. 따라서 δ 가 1보다 크거나 같은 경우만 고려한다. δ 보안 SEP을 최소화 할 수 있는 λ 의 최적값을 결정한다. 그러나 비밀 신호와 인공 잡음 사이의 전력 할당은 높은 δ 보안 SEP 곡선의 SNR 경사에 영향을 미치지 못한다. 이런 이유로, λ 의 값을(0,1)로 결정하

였다. 예를 들어 전력 할당 비율 $\lambda = \lambda_{\uparrow}^*$ 로 설계한다.

[0093] 인공 잡음이 포함된 보안 빔포빙에서 M-PSK의 δ 보안 SEP는 식 30과 같이 주어진다.

수학식 30

$$\mathcal{SP}_e(\delta) = P_1 + (1 - P_1) P_2$$

[0094]

[0095] 식 30에서 P_1 은 식 31과 같다.

수학식 31

$$P_1 = F_{\Gamma_r}(\delta - 1) + \frac{e^{\frac{(1-\delta)n_t}{\lambda \text{snr}_r}}}{(n_t - 1)!} \left(\frac{n_t}{\lambda \text{snr}_r} \right)^{n_t} \sum_{i=0}^{n_e-1} \sum_{j=0}^{n_e-1-i} \sum_{k=0}^{n_t-1} \left\{ \binom{n_t-1}{j} \binom{n_t-1}{k} \frac{a_{\lambda}^{j-1}}{i!} \right. \\ \left. \times (\delta - 1)^{n_t-1-k} \left(\frac{n_t}{\lambda \delta \text{snr}_e} \right)^{-k-1} \left(1 + \delta \frac{\text{snr}_e}{\text{snr}_r} \right)^{-i-j-k} \mathcal{I}_{n_t-2}^{i+j+k} \left(0, \frac{a_{\lambda}}{1 + \delta \frac{\text{snr}_e}{\text{snr}_r}}, \frac{a_{\lambda}}{1 + \delta \frac{\text{snr}_e}{\text{snr}_r}} \right) \right\}$$

[0096]

[0097] 식 31에서 P_2 은 식 32와 같다.

수학식 32

$$P_2 = \frac{1}{\pi} \int_0^{\Theta} \left(1 + \frac{\lambda \text{snr}_r}{n_t} \frac{g_{\text{PSK}}}{\sin^2 \theta} \right)^{-n_t} \left[1 - F_{\Gamma_r} \left(\left(1 + \frac{\lambda \text{snr}_r}{n_t} \frac{g_{\text{PSK}}}{\sin^2 \theta} \right) (\delta - 1) \right) \right] d\theta \\ - \frac{e^{\frac{(\delta-1)n_t}{\lambda \delta \text{snr}_e}}}{\pi (n_t - 1)!} \left(\frac{n_t}{\lambda \text{snr}_r} \right)^{n_t} \left(1 + \frac{(1-\delta)n_t a_{\lambda}}{\lambda \delta \text{snr}_e} \right)^{2-n_t} \sum_{i=0}^{n_e-1} \sum_{j=0}^{n_e-1-i} \sum_{k=0}^{i+j} \left\{ \binom{n_t-1}{j} \binom{i+j}{k} \right. \\ \left. \times \frac{a_{\lambda}^{j-1}}{i!} \left(\frac{n_t}{\lambda \delta \text{snr}_e} \right)^{i+j-1} \int_0^{\Theta} \chi_{\theta}^{n_t+k-1} \mathcal{I}_{n_t-2}^{n_t+k-1} \left(\frac{\delta-1}{\chi_{\theta}}, \frac{\chi_{\theta}}{1 - \delta + \frac{\lambda \delta \text{snr}_e}{n_t a_{\lambda}}}, \frac{\chi_{\theta}}{1 - \delta + \frac{\lambda \delta \text{snr}_e}{n_t a_{\lambda}}} \right) d\theta \right\}$$

[0098]

[0099] 식 32에서, $g_{\text{PSK}} = \sin^2 \frac{\pi}{M}$ 및 $\Theta = \pi - \frac{\pi}{M}$ 를 만족하며 F_{Γ_r} 과 χ_{θ} 는 식 33 및 식34와 같다.

수학식 33

$$F_{\Gamma_r}(x) = 1 - \sum_{k=0}^{n_t-1} \frac{1}{k!} \left(\frac{n_t}{\lambda \text{snr}_r} x \right)^k e^{-\frac{n_t}{\lambda \text{snr}_r} x}, \quad x \geq 0,$$

[0100]

수학식 34

$$\chi_{\theta} \triangleq \left(\frac{n_t}{\lambda \text{snr}_r} + \frac{n_t}{\lambda \delta \text{snr}_e} + \frac{g_{\text{PSK}}}{\sin^2 \theta} \right)^{-1}$$

[0101]

δ 보안 SEP 경사의 높은 SNR 경사에서 인공 잡음이 포함된 보안 빔포밍의 다이버시티 영향(Impact)을 수량화한다.

수학식 35

$$d_s \triangleq \lim_{\substack{\text{snr}_r, \text{snr}_e \rightarrow \infty \\ \frac{\text{snr}_e}{\text{snr}_r} \rightarrow \alpha}} \frac{-\log \mathcal{SP}_e(\delta)}{\log \text{snr}_r}$$

[0103]

δ 보안 SEP의 보안 다이버시티 오더(Secrecy Diversity Order)는 식 35와 같다.

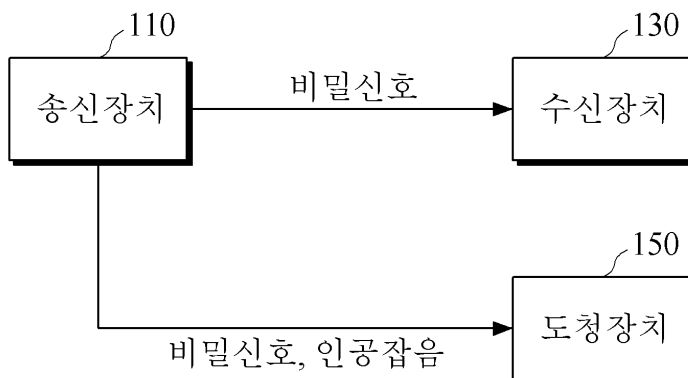
이상 바람직한 실시 예를 들어 본 발명을 상세하게 설명하였으나, 본 발명은 전술한 실시 예에 한정되지 않고, 본 발명의 기술적 사상의 범위 내에서 당 분야에서 통상의 지식을 가진 자에 의하여 여러 가지 변형이 가능하다.

부호의 설명

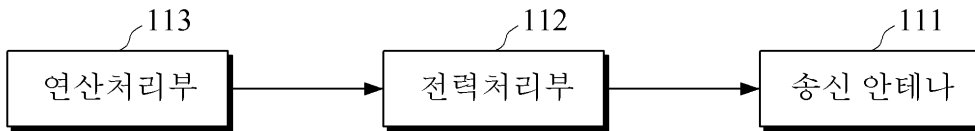
- 110: 송신장치
- 130: 수신장치
- 150: 도청장치
- 111: 송신 안테나
- 112: 전력처리부
- 113: 연산처리부

도면

도면1



도면2



도면3

