



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0086497
(43) 공개일자 2012년08월03일

(51) 국제특허분류(Int. Cl.)

H04B 7/04 (2006.01) *H04W 12/00* (2009.01)

H04W 52/24 (2009.01)

(21) 출원번호 10-2011-0007761

(22) 출원일자 2011년01월26일

심사청구일자 2011년01월26일

(71) 출원인

경희대학교 산학협력단

경기도 용인시 기흥구 덕영대로 1732, 국제캠퍼스 내 (서천동, 경희대학교)

(72) 발명자

신현동

경기도 수원시 영통구 청명북로 81, 청명마을 주공아파트 404동 901호 (영통동)

정영민

경기도 성남시 분당구 양현로 537, 313동 305호 (야탑동, 매화마을)

(74) 대리인

특허법인 신지

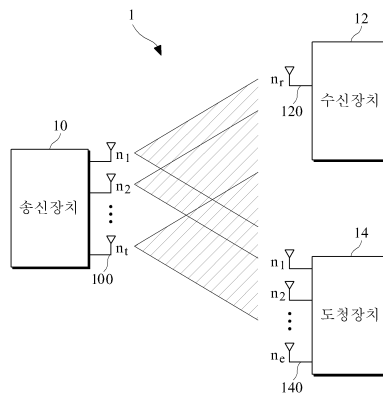
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 보안 데이터 송신장치와 그 방법 및 다중채널 무선통신 시스템

(57) 요약

보안 데이터 송신장치와 그 방법 및 다중채널 무선통신 시스템이 개시된다. 본 발명의 일 실시예에 따르면 다중 입력 다중 출력 다중 도청장치(MISOME)의 페이딩 도청 채널 존재 하에서 전송채널의 송신전력을 온-오프로 할당하고 할당 결과에 따라 수신장치에 보안 데이터 신호를 빔포밍함에 따라 보안 전송률을 최대화할 수 있다.

대표도 - 도1



특허청구의 범위

청구항 1

송신장치가 다중 채널을 통해 데이터를 보안 전송하는 방법에 있어서,
 상기 다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화하여 보안 용량을 최대화하는 단계;
 상기 최대화된 보안 용량 조건 하에서 보안 전송률을 최대화하도록 상기 다중 채널의 송신전력을 온-오프(on-off)로 할당하는 단계; 및
 상기 송신전력 할당 결과에 따라 데이터 신호를 빔포밍(beamforming)하는 단계;
 를 포함하는 것을 특징으로 하는 데이터 보안전송 방법.

청구항 2

제 1 항에 있어서, 상기 송신전력을 온-오프로 할당하는 단계는,
 안테나 수와 수신신호 대 잡음비를 기초로 하여 상기 송신전력을 할당하는 것을 특징으로 하는 데이터 보안전송 방법.

청구항 3

제 2 항에 있어서, 상기 송신전력을 온-오프로 할당하는 단계는,
 전송 채널의 채널 이득 파라미터 크기가 기설정된 문턱값보다 크거나 동일하면 상기 송신전력 파라미터를 1로 할당하고, 상기 문턱값보다 작으면 상기 송신전력 파라미터를 0으로 할당하는 것을 특징으로 하는 데이터 보안 전송 방법.

청구항 4

제 3 항에 있어서,
 상기 문턱값은 송신장치의 안테나 수와 도청장치의 안테나 수와 수신장치의 신호 대 잡음비와 도청장치의 신호 대 잡음비를 이용하여 설정되는 것을 특징으로 하는 데이터 보안전송 방법.

청구항 5

제 1 항에 있어서, 상기 송신전력 할당 결과에 따라 데이터 신호를 빔포밍하는 단계는,
 상기 온-오프 송신전력 할당을 통해 수신장치 전송채널의 채널 이득 파라미터의 결레전치 방향으로 상기 데이터 신호를 빔포밍하는 것을 특징으로 하는 데이터 보안전송 방법.

청구항 6

제 1 항에 있어서,
 상기 다중 채널은 합법 채널 및 도청 채널을 포함하며,
 상기 보안 용량을 최대화하는 단계는,
 상기 합법 채널을 통해 전 채널 상태정보에 대해 접근하고 상기 도청 채널을 통해 부분 채널 상태정보에 대해 접근하는 단계; 및
 상기 합법 채널에 대한 채널 용량은 증가시키고 상기 도청 채널에 대한 채널 용량은 감소시켜 상기 보안 용량을 최대화하는 단계;
 를 포함하는 것을 특징으로 하는 데이터 보안전송 방법.

청구항 7

다중 입력 단일 출력 다중 도청장치(MISOME);

단일 수신 안테나를 갖는 수신장치;

다수의 송신 안테나를 갖으며, 상기 MISOME의 페이딩 도청 채널 존재 하에서 보안 전송물을 최대화하도록 채널의 송신전력을 온-오프로 할당하고 상기 할당 결과에 따라 상기 수신장치에 보안 데이터 신호를 빔포밍하는 송신장치;

를 포함하는 것을 특징으로 하는 다중채널 무선통신 시스템.

청구항 8

다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화하여 보안 용량을 최대화하는 보안 용량 설정부; 및

상기 최대화된 보안 용량 조건 하에서 보안 전송물을 최대화하도록 상기 다중 채널의 송신전력을 온-오프로 할당하는 전력 설정부; 및

상기 송신전력 할당 결과에 따라 데이터 신호를 빔포밍하는 전송부;

를 포함하는 것을 특징으로 하는 보안 데이터 송신장치.

청구항 9

제 8 항에 있어서, 상기 전력 설정부는,

안테나 수와 수신신호 대 잡음비를 기초로 하여 상기 송신전력을 할당하는 것을 특징으로 하는 보안 데이터 송신장치.

청구항 10

제 9 항에 있어서, 상기 전력 설정부는,

전송 채널의 채널 이득 파라미터 크기의 크기가 기설정된 문턱값보다 크거나 동일하면 상기 송신전력 파라미터를 1로 할당하고, 상기 문턱값보다 작으면 상기 송신전력 파라미터를 0으로 할당하는 것을 특징으로 하는 보안 데이터 송신장치.

청구항 11

제 10 항에 있어서,

상기 문턱값은 송신장치의 안테나 수와 도청장치의 안테나 수와 수신장치의 신호 대 잡음비와 도청장치의 신호 대 잡음비를 이용하여 설정되는 것을 특징으로 하는 보안 데이터 송신장치.

명 세 서

기술 분야

[0001] 본 발명의 일 양상은 무선통신 기술에 관한 것으로, 보다 상세하게는 다중채널 무선통신 환경에서 보안 전송물을 최적화하기 위한 전력 제어 및 보안 데이터 전송 기술에 관한 것이다.

배경 기술

[0002] 무선통신은 대기(air)로 신호를 송출하거나 대기 중의 신호를 수신하여 통신을 수행하는 방식으로 대기라는 공개된 매체를 이용한다. 따라서 허락받지 않은 제3자가 수신자와 근접하여 위치하고 수신자로 송신되는 신호의 부호화 방식을 알고 있다면, 송신 신호를 도청하여 수신자와 송신자 사이의 비밀 정보를 쉽게 빼낼 수 있는 위험을 가진다.

[0003] 송신자와 수신자가 통신을 수행하는 과정에서, 허락받지 않은 제3자가 송신자와 수신자 사이에서 송수신되는 데이터를 도청하는 통신 모델은 와이너(Wyner)에 의해 처음으로 제안되었다. 그 후로도 무선통신의 브로드캐스팅(broadcasting) 특성 때문에 무선통신에서의 보안 전송물을 높이기 위한 방안들이 연구되고 있다.

발명의 내용

해결하려는 과제

[0004] 일 양상에 따라, 다중채널 무선통신 환경에서 보안 전송률을 최적화하기 위한 전력 제어 및 보안 데이터 전송 기술을 제안한다.

과제의 해결 수단

[0005] 일 양상에 따른 송신장치가 다중 채널을 통해 데이터를 보안 전송하는 방법은, 다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화하여 보안 용량을 최대화하는 단계와, 최대화된 보안 용량 조건 하에서 보안 전송률을 최대화하도록 다중 채널의 송신전력을 온-오프(on-off)로 할당하는 단계와, 송신전력 할당 결과에 따라 데이터 신호를 빔포밍(beamforming)하는 단계를 포함한다.

[0006] 다른 양상에 따른 다중채널 무선통신 시스템은, 다중 입력 단일 출력 다중 도청장치(MISOME)와, 단일 수신 안테나를 갖는 수신장치와, 다수의 송신 안테나를 갖으며 MISOME의 페이딩 도청 채널 존재 하에서 보안 전송률을 최대화하도록 채널의 송신전력을 온-오프로 할당하고 할당 결과에 따라 수신장치에 보안 데이터 신호를 빔포밍하는 송신장치를 포함한다.

[0007] 또 다른 양상에 따른 보안 데이터 송신장치는, 다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화하여 보안 용량을 최대화하는 보안 용량 설정부와, 최대화된 보안 용량 조건 하에서 보안 전송률을 최대화하도록 다중 채널의 송신전력을 온-오프로 할당하는 전력 설정부와, 송신전력 할당 결과에 따라 데이터 신호를 빔포밍하는 전송부를 포함한다.

발명의 효과

[0008] 일 실시예에 따르면, 다중채널 무선통신 환경에서 보안 전송률을 최대화하여 데이터를 전송할 수 있다. 즉, 다중 입력 다중 출력 다중 도청장치(MISOME)의 페이딩 도청 채널 존재 하에서 전송채널의 송신전력을 온-오프로 할당하고 할당 결과에 따라 수신장치에 보안 데이터 신호를 빔포밍함에 따라 보안 전송률을 최대화한다.

도면의 간단한 설명

[0009] 도 1은 본 발명의 일 실시예에 따른 다중채널 무선통신 시스템을 도시한 구성도,
 도 2는 본 발명의 일 실시예에 따른 송신장치의 세부 구성도,
 도 3은 본 발명의 일 실시예에 따른 송신장치의 데이터 전송방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0010] 이하에서는 첨부한 도면을 참조하여 본 발명의 실시예들을 상세히 설명한다. 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0011] 도 1은 본 발명의 일 실시예에 따른 다중채널 무선통신 시스템(1)을 도시한 구성도이다.

[0012] 도 1을 참조하면, 본 발명의 다중채널 무선통신 시스템(1)은 송신장치(10), 수신장치(12) 및 도청장치(14)를 포함한다.

[0013] 송신장치(transmitter)(10)는 송신 안테나(100)를 구비하고, 송신 안테나(100)를 이용하여 데이터 신호를 무선 채널을 통해 수신장치(receiver)(12)에 송신한다. 송신된 데이터 신호는 송신장치(10)와 수신장치(12) 사이에 존재하는 방해 대상에 의해 반사되어 서로 다른 경로로 페이딩되어 수신 안테나(120)에 의해 수신된다.

[0014] 수신장치(12)는 서로 다른 경로로 페이딩되는 데이터 신호를 수신 안테나(120)를 이용하여 수신한다. 한편, 송신장치(10)의 데이터 신호 송신 범위에 위치하는 도청장치(eavesdropper)(14)는 송신장치(10)로부터 송신되는 데이터 신호를 도청 안테나(140)를 이용하여 도청한다.

- [0015] 도청 통신 모델을 보다 구체적으로 살펴보면, 송신장치(10)는 데이터 신호를 합법 채널(legitimate channel)을 통해 수신장치(12)로 송신한다. 수신장치(12)는 합법 채널을 통해 데이터 신호를 수신한다. 한편, 수신장치(12)에서 수신한 데이터 신호는 도청 채널(eavesdropper channel)을 통해 허락받지 않은 도청장치(14)에 의해 도청된다.
- [0016] 무선 통신에서 사용자의 가장 중요한 관심 중에 하나는 송신장치(10)와 수신장치(12) 사이에서 송수신되는 데이터를 허락받지 않은 도청장치(14)가 도청하지 못하도록 하는 것이다. 따라서 각각 정해진 채널 용량을 가지는 합법 채널과 도청 채널에서 수신장치(12)가 데이터 신호를 도청장치(14)에 의해 도청되지 않고 수신할 수 있는 조건에 대해 관심을 가지게 된다.
- [0017] 채널 용량이란 데이터가 오류 없이 채널을 통해 상대방으로 송신되는 최대 데이터 전송률, 즉 사용된 전송 매체가 수용할 수 있는 정보 송신 능력을 의미한다. 보안 용량이란 데이터가 도청장치(14)의 도청 없이 합법 채널을 통해 허락된 수신장치(12)로 송신되는 최대 데이터 전송률을 의미한다. 즉, 보안 용량이란 도청 채널의 채널 용량에 대한 합법 채널의 채널 용량비로 계산된다.
- [0018] 일 실시예에 따르면, 본 발명의 다중채널 무선통신 시스템(1)은 도 1에 도시된 바와 같이 송신장치(10)가 다수의 송신 안테나($n_1, n_2, \dots, n_t$)를 갖고, 수신장치(12)가 단일의 수신 안테나(n_r)를 갖는다. 그리고, 도청장치(14)는 다중 입력 다중 출력 방식을 따르는 다수 개의 도청기(multiple-input single-output multiple-eavesdropper: 이하 MISOME이라 칭함)이다. 이하 도청장치(14)를 MISOME과 혼용하여 사용한다.
- [0019] 도 2는 본 발명의 일 실시예에 따른 송신장치(10)의 세부 구성도이다.
- [0020] 도 1 및 도 2를 참조하면, 송신장치(10)는 채널의 송신전력 할당 최적화 및 보안 전송률 최대화를 위해 보안 용량 설정부(200), 전력 설정부(210) 및 전송부(220)를 포함한다.
- [0021] 보안 용량 설정부(200)는 다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화하여 보안 용량을 최대화한다. 다중 채널은 합법 채널(legitimate channel) 및 도청 채널(eavesdropper channel)을 포함한다. 송신장치(10)는 합법 채널을 통해 전 채널 상태정보(full channel state information: full CSI)에 대한 접근 권한을 갖고, 도청 채널을 통해 부분 채널 상태정보(partial channel state information: partial CSI)에 대해 접근 권한을 갖는다. 채널 상태정보는 채널의 특성을 기술한 것이다. 송신장치(10)는 도청장치(14)의 위치는 안다고 가정한다. 송신장치(10)의 CSI에 대한 접근 권한은 평균 수신 신호 대 잡음비(Average received signal-to-noise ratio: SNR)에 따라 결정될 수 있다.
- [0022] 전술한 위치 인식 시나리오에 기반하여 본 발명은 완전 보안(perfect secrecy)으로 달성가능 보안 전송률(achievable secrecy rate)을 최대화할 수 있는 전력 할당 최적화 기법(optimal power allocation strategy)을 제안한다.
- [0023] 구체적으로, 전력 설정부(210)는 MISOME의 레일리 페이딩 도청 채널(Rayleigh-fading wiretap channels) 하에서 달성가능 보안 전송률을 최대화하도록 채널의 송신전력을 온-오프(on-off)로 할당한다. 전송부(200)는 전력 설정부(210)에서의 할당 결과에 따라 수신장치(12)에 보안 데이터(confidential data) 신호를 빔포밍한다.
- [0024] 전력 설정부(210)는 안테나 수(the numbers of antennas)와 평균 수신신호 대 잡음비(the average received SNRs)를 기초로 하여 송신전력을 할당할 수 있다. 일 실시예를 들면, 채널 이득 파라미터의 크기가 기설정된 문턱값(threshold)보다 크거나 동일하면 송신전력 파라미터를 1로 할당하고, 문턱값 보다 작으면 송신전력파라미터를 0으로 할당한다. 이때, 문턱값은 송신장치(10)의 안테나 수와 도청장치(14)의 안테나 수와 수신장치(12)의 신호 대 잡음비와 도청장치(14)의 신호 대 잡음비를 이용하여 설정된다.
- [0025] 이하 수식들을 참조로 하여, 달성가능 보안 전송률(achievable secrecy rate)을 최대화할 수 있는 전력 할당 최적화 기법(optimal power allocation strategy)을 설명한다.
- [0026] 우선, 본 발명은 도청 채널(MISOME wiretap channel)을 통해 n_e 개의 안테나(140)로 신호를 도청하는 도청장치(14)의 존재 하에서 n_r 개의 안테나(100)를 갖는 송신장치(10)가 합법적인 단일 개의 안테나(120)를 갖는 수신장치(12)에 보안 데이터를 전송한다고 가정한다. 이때, 수신장치(12)와 도청장치(14)에 수신되는 신호는 각각 식 1 및 식 2와 같다.

수학식 1

[0027]

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

[0028]

식 1에 있어서, y_r 은 수신장치(12)가 합법 채널을 통해 수신하는 신호를 나타낸다. $\mathbf{x} \in \mathbb{C}^{n_t}$ 은 $\mathbf{\Sigma} \in \mathbb{C}^{n_t \times n_t}$ 이 전력 제한 $\text{tr}(\mathbf{\Sigma}) \leq 1$ 을 만족하는 공분산 행렬(covariance matrix)을 따른다. $\text{tr}(\cdot)$ 은 트레이스 연산자(trace operator)이다. $\mathbf{h}_r \sim \tilde{\mathcal{N}}_{1,n_t}$ 은 합법 채널의 레일리 페이딩 채널 이득 파라미터(Rayleigh-fading channel gains)이다. $\mathbf{z}_r \sim \tilde{\mathcal{N}}_{1,1}$ 는 수신장치(12)가 수신한 신호에 첨가된 잡음신호(additive white Gaussian noises)이다. snr_r 은 수신장치(12)에 대한 평균 신호 대 잡음비(the average received signal-to-noise ratios(SNRs) per antenna at the receiver)를, n_t 는 송신장치(10)의 송신 안테나 수를 나타낸다.

수학식 2

[0029]

$$y_e = \sqrt{\text{snr}_e/n_t} \mathbf{H}_e \mathbf{x} + z_e$$

[0030]

식 2에 있어서, y_e 은 도청장치(14)가 도청 채널을 통해 수신하는 신호를 나타낸다. $\mathbf{x} \in \mathbb{C}^{n_t}$ 은 $\mathbf{\Sigma} \in \mathbb{C}^{n_t \times n_t}$ 이 전력 제한 $\text{tr}(\mathbf{\Sigma}) \leq 1$ 을 만족하는 공분산 행렬(covariance matrix)을 따른다. $\text{tr}(\cdot)$ 은 트레이스 연산자(trace operator)이다. $\mathbf{H}_e \sim \tilde{\mathcal{N}}_{n_e, n_t}$ 은 도청 채널의 레일리 페이딩 채널 이득 파라미터(Rayleigh-fading channel gains)이다. $\mathbf{z}_e \sim \tilde{\mathcal{N}}_{n_e, 1}$ 는 도청장치(14)가 수신한 신호에 첨가된 잡음신호(additive white Gaussian noises)이다. snr_e 은 도청장치(14)에 대한 평균 신호 대 잡음비(the average received signal-to-noise ratios(SNRs) per antenna at the eavesdropper)를, n_t 는 송신장치(10)의 송신 안테나 수를 나타낸다.

[0031]

송신장치(10)가 수신장치(12)에 대해 완전 채널 상태정보(perfect CSI)에 대해 접근 가능하다고 가정하면, MISOME 도청 채널 하에서 순간 완전 보안 용량(the instantaneous perfect secrecy capacity)(nat/s/Hz)은 식 3과 같다.

수학식 3

[0032]

$$C_s = \max_{\substack{\mathbf{\Sigma} \succeq 0 \\ \text{tr}(\mathbf{\Sigma}) \leq 1}} \ln \left(\frac{1 + \frac{\text{snr}_r}{n_t} \mathbf{h}_r \mathbf{\Sigma} \mathbf{h}_r^\dagger}{\det \left(\mathbf{I} + \frac{\text{snr}_e}{n_t} \mathbf{H}_e \mathbf{\Sigma} \mathbf{H}_e^\dagger \right)} \right)$$

[0033]

상첨자(superscript) $(\cdot)^\dagger$ 는 켤레전치(conjugate transpose)를, $\mathbf{I}$ 는 단위 행렬(identity matrix)을, $\mathbf{A} \succeq 0$ 는 행렬 $\mathbf{A}$ (matrix $\mathbf{A}$)가 양의 준정부호 행렬(positive semidefinite)임을 각각 나타낸다.

[0034]

식 3에 있어서, 보안 용량 최대화를 위한 입력 공분산(the input covariance for secrecy capacity maximization)을 최적화하기 위해서, 송신장치(10)는 합법 채널(legitimate channel)과 도청 채널

(eavesdropper channel) 모두에 대한 전 채널 상태 정보(full CSI) 접근이 요구되나, 이는 현실적으로 불가능하다.

[0035] 전술한 문제를 해결하기 위해서, 본 발명은 송신장치(10)가 합법 채널에 대해서는 전 채널 상태정보(full CSI)에 대한 접근 권한을 갖고, 도청 채널에 대해서는 위치 인식 기반 하에서 부분 채널 상태정보(partial CSI)에 대한 접근 권한을 갖는다고 가정한다. 전술한 가정 하에 보안 용량(C_s)은 식 4와 같다.

수학식 4

$$C_s = \max_{\substack{\Sigma \succeq 0 \\ \text{tr}(\Sigma) \leq 1}} \mathbb{E}_{H_e} \left\{ \left[\ln \left(\frac{1 + \frac{\text{snr}_r}{n_t} \mathbf{h}_r \Sigma \mathbf{h}_r^\dagger}{\det \left(\mathbf{I} + \frac{\text{snr}_e}{n_t} \mathbf{H}_e \Sigma \mathbf{H}_e^\dagger \right)} \right) \right]^+ \right\}$$

$$\geq \underbrace{\max_{\substack{\Sigma \succeq 0 \\ \text{tr}(\Sigma) \leq 1}} \mathbb{E}_{H_e} \left\{ \ln \left(\frac{1 + \frac{\text{snr}_r}{n_t} \mathbf{h}_r \Sigma \mathbf{h}_r^\dagger}{\det \left(\mathbf{I} + \frac{\text{snr}_e}{n_t} \mathbf{H}_e \Sigma \mathbf{H}_e^\dagger \right)} \right) \right\}}_{R_s^*}$$

[0036]

[0037] 식 4에 있어서 $[x]^+ = \max\{0, x\}$ 이다. $W \sim \text{Erl}(n_e, 1)$ 이면, 식 5 및 식 6과 같다. $\text{Erl}(n, \lambda)$ 는 평균값 λ 을 갖는 n 차 Erlang 분포이다.

수학식 5

$$\ln \left(1 + \frac{\text{snr}_r}{n_t} \mathbf{h}_r \Sigma \mathbf{h}_r^\dagger \right) \leq \ln \left(1 + \text{tr}(\Sigma) \frac{\text{snr}_r}{n_t} \|\mathbf{h}_r\|^2 \right)$$

[0038]

수학식 6

$$\mathbb{E}_{H_e} \left\{ \ln \det \left(\mathbf{I} + \frac{\text{snr}_e}{n_t} \mathbf{H}_e \Sigma \mathbf{H}_e^\dagger \right) \right\}$$

$$\geq \mathbb{E}_W \left\{ \ln \left(1 + \text{tr}(\Sigma) \frac{\text{snr}_e}{n_t} W \right) \right\}$$

[0039]

[0040] 식 5는 $\mathbf{h}_r^\dagger$ 의 방향으로 데이터 신호를 빔포밍하는 경우(예:rank-one Σ with a nonzero eigenvector $\mathbf{h}_r^\dagger / \|\mathbf{h}_r\|$)이고, 식 6은 어느 방향(any direction)으로 데이터 신호를 빔포밍하는 경우(예:any rank-one Σ)이다. 따라서 최대의 달성가능 보안 전송률(achievable secrecy rate) R_s^* 은 식 7과 같다.

수학식 7

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

[0041]

[0042] 본 발명은 식 7에서의 달성 가능 보안 전송률을 최대화할 수 있는 최적의 전력 할당 방식을 식 8에서와 같이 제안한다. 또한 최적의 전력 할당 방식을 통해 MISOME 보안 채널 하에서의 에르고딕 보안 전송률(ergodic secrecy rate)을 얻을 수 있다. $\lambda \in [0, 1]$ 인 조건에서 보안 전송률(secrecy rate) $R_s(\lambda)$ 을 최대화할 수 있는 최적의 λ 인 λ^* 는 식 8과 같다.

수학식 8

[0043]
$$\lambda^* = \arg \max_{0 \leq \lambda \leq 1} R_s(\lambda)$$

[0044] 그러면, 최적의 λ^* 는 식 9와 같이 기설정된 문턱값(threshold) ζ 에 따른 온-오프(on-off) 전력 할당 값이다.

수학식 9

[0045]
$$\lambda^* = \begin{cases} 1, & \text{if } \|h_r\|^2 \geq \zeta \\ 0, & \text{otherwise} \end{cases}$$

[0046] 식 9에 따르면, 송신장치(10)는 수신장치(12)의 합법 채널의 채널 이득 파라미터 크기 $\|h_r\|^2$ 가 기설정된 문턱값 ζ 보다 크거나 동일하면 송신전력을 1로 할당하고, 문턱값 ζ 보다 작으면 송신전력을 0으로 할당한다. 이때 문턱값 ζ 은 식 10과 같다.

수학식 10

[0047]
$$\zeta = \frac{\exp \left\{ e^{\frac{n_t}{\text{snr}_e}} \sum_{n=1}^{n_e} E_n \left(\frac{n_t}{\text{snr}_e} \right) \right\} - 1}{\text{snr}_r / n_t}$$

[0048] 식 10에서 $E_n(z) = \int_1^\infty e^{-zt} t^{-n} dt, n = 0, 1, \dots, \Re\{z\} > 0$ 이다. 문턱값 ζ 은 n_e 에 따라 증가하고 snr_e 에 따라 점근적 선형 형태(asymptotically linearly)로 증가하지만, snr_r 에 역으로 감소(decrease inversely)한다.

[0049] 전송부(220)는 달성 가능 보안 전송률을 최대화하기 위해 온-오프 전력 할당 방식을 통해 $h_r^\dagger$ 의 방향으로 데이터 신호를 빔포밍한다.

수학식 11

[0050]
$$\lambda^* \sim \text{Bern} \left(1 - F_{\|h_r\|^2}(\zeta) \right)$$

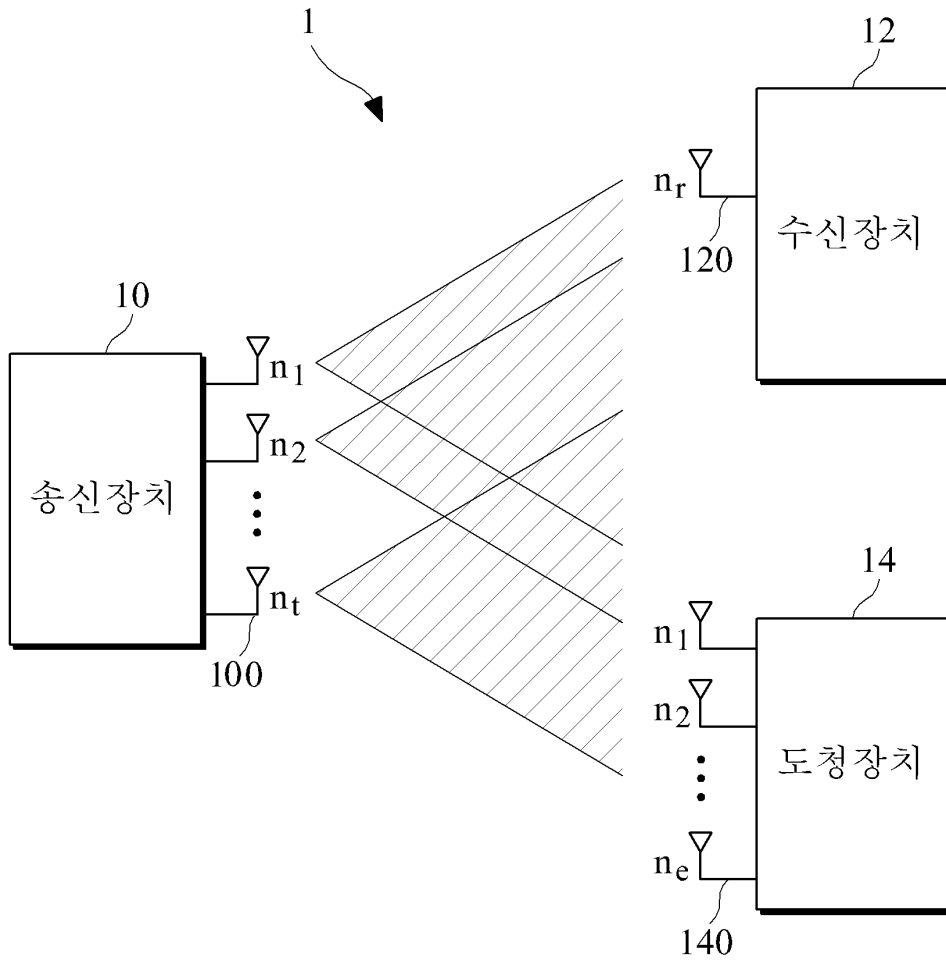
- [0051] 식 11에 있어서, $F_{\|h_r\|^2}(x)$ 는 $\|h_r\|^2 \sim \text{Erl}(n_r, 1)$ 의 분포이다. Bern(p)는 평균(mean) p를 갖는 베르누이 분포(Bernoulli distribution)이다.
- [0052] 도 3은 본 발명의 일 실시예에 따른 송신장치의 데이터 전송방법을 도시한 흐름도이다.
- [0053] 도 1 및 도 3을 참조하면, 송신장치(10)는 다중 채널에 대한 채널 상태정보 접근 정도를 도청 여부에 따라 차별화(300)하여 보안 용량을 최대화한다(310). 다중 채널은 합법 채널 및 도청 채널을 포함한다. 일 실시예에 따르면 송신장치(10)는 합법 채널을 통해 전 채널 상태정보에 대해 접근하고, 도청 채널을 통해 부분 채널 상태정보에 대해 접근한다. 그리고, 합법 채널에 대한 채널 용량은 증가시키고 도청 채널에 대한 채널 용량은 감소시켜 보안 용량을 최대화한다.
- [0054] 이어서, 송신장치(10)는 최대화된 보안 용량 조건 하에서 보안 전송률을 최대화하도록 다중채널의 송신전력을 온-오프(on-off)로 할당한다(320). 일 실시예에 따르면 안테나 수와 수신신호 대 잡음비를 기조로 하여 송신전력을 할당한다. 즉, 전송 채널의 채널 이득 파라미터 크기가 기설정된 문턱값보다 크거나 동일하면 송신전력을 1로 할당하고, 문턱값보다 작으면 송신전력을 0으로 할당할 수 있다. 이때 문턱값은 송신장치의 안테나 수와 도청장치의 안테나 수와 수신장치의 신호 대 잡음비와 도청장치의 신호 대 잡음비를 이용하여 설정된다.
- [0055] 이어서, 송신장치(10)는 송신전력 할당 결과에 따라 데이터 신호를 빔포밍한다(330).
- [0056] 이제까지 본 발명에 대하여 그 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

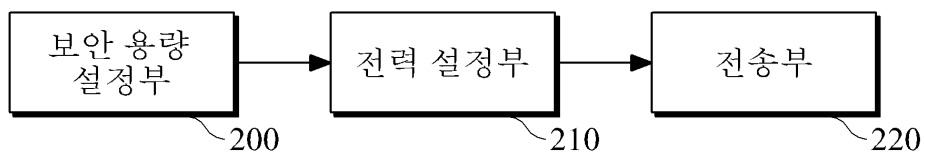
- [0057]
- | | |
|-------------------|--------------|
| 1 : 다중채널 무선통신 시스템 | 10 : 송신장치 |
| 12 : 수신장치 | 14 : 도청장치 |
| 200 : 보안 용량 설정부 | 210 : 전력 설정부 |
| 220 : 전송부 | |

도면

도면1



도면2



도면3

