



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0144528
(43) 공개일자 2022년10월27일

(51) 국제특허분류(Int. Cl.)
H04B 7/0413 (2017.01) H01Q 15/14 (2006.01)
H04B 7/06 (2017.01)
(52) CPC특허분류
H04B 7/0413 (2013.01)
H01Q 15/14 (2018.05)
(21) 출원번호 10-2021-0050952
(22) 출원일자 2021년04월20일
심사청구일자 2021년04월20일

(71) 출원인
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대 학교)
(72) 발명자
박대영
인천광역시 연수구 송도문화로84번길 24, 208동 3104호(송도동, 송도 에듀포레 푸르지오)
김민식
경기도 수원시 영통구 동수원로 448, 105동 402호(매탄동, 현대아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 8 항

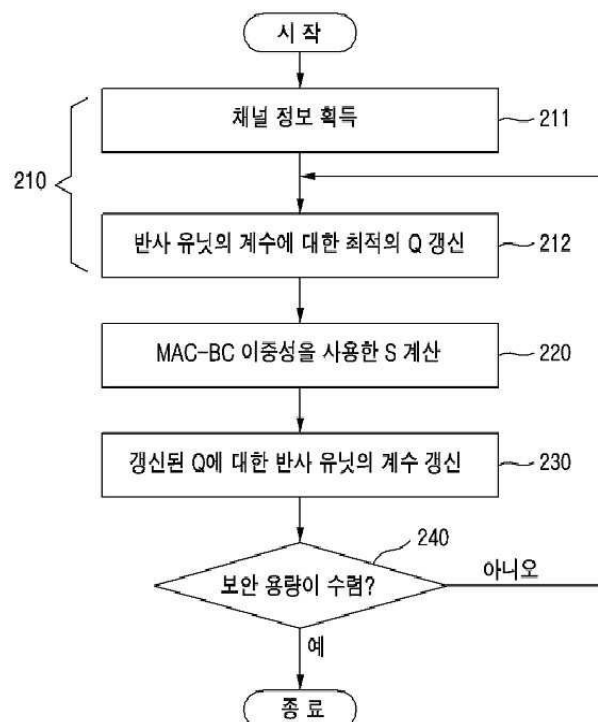
(54) 발명의 명칭 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 방법 및 장치

(57) 요약

지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 방법 및 장치가 제시된다. 본 발명에서 제안하는 합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 방법은 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포

(뒷면에 계속)

대표도 - 도2



함하는 대각 행렬은 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계, 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계, 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계 및 MIMO 시스템의 보안 용량이 수렴할 때까지 상기 공분산 행렬을 계산하여 채널을 갱신하는 단계 및 상기 대각 행렬을 계산하여 채널을 갱신하는 단계를 반복하는 단계를 포함한다.

(52) CPC특허분류

H04B 7/0634 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711109488
과제번호	2019R1A2C1005512
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	중견연구
연구과제명	[Ezbaro] 딥러닝을 이용한 차세대 통신 시스템 설계
기 여 율	90/100
과제수행기관명	인하대학교
연구기간	2021.03.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116910
과제번호	2020-0-01389-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	인공지능융합연구센터지원사업(국고)
연구과제명	[Ezbaro][정부] 인공지능융합연구센터지원(2차년도)
기 여 율	10/100
과제수행기관명	인하대학교 산학협력단
연구기간	2021.01.01 ~ 2021.12.31

명세서

청구범위

청구항 1

합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 방법에 있어서,

합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계;

브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계;

갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계; 및

MIMO 시스템의 보안 용량이 수렴할 때까지 상기 공분산 행렬을 계산하여 채널을 갱신하는 단계 및 상기 대각 행렬을 계산하여 채널을 갱신하는 단계를 반복하는 단계

를 포함하는 MIMO 시스템의 보안 용량 최적화 방법.

청구항 2

제1항에 있어서,

합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계는,

동일한 해를 갖는 문제로 변형하여 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고,

IRS를 구성하는 각각의 반사 유닛의 계수에 대하여 닫힌 형태(closed form)의 해를 제공하는

MIMO 시스템의 보안 용량 최적화 방법.

청구항 3

제1항에 있어서,

브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계는,

MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 문제를 다중 접속 채널의 문제로 변환하는

MIMO 시스템의 보안 용량 최적화 방법.

청구항 4

제1항에 있어서,

갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계는,

최적의 대각 행렬을 구하기 위해 각각 독립적인 IRS 반사 유닛의 계수에 좌표하강법(coordinate descent methods)을 적용하여 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하는

MIMO 시스템의 보안 용량 최적화 방법.

청구항 5

합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 장치에 있어서,

계산부에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신하는 업데이트부;

합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고, 업데이트부를 통해 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하는 계산부;

브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 공분산 행렬 변환부; 및

MIMO 시스템의 보안 용량이 수렴할 때까지 계산부가 공분산 행렬을 계산하고, 대각 행렬을 계산하고, 업데이트부가 계산부에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신하는 과정을 반복하도록 제어하는 제어부

를 포함하는 MIMO 시스템의 보안 용량 최적화 장치.

청구항 6

제5항에 있어서,

계산부는,

동일한 해를 갖는 문제로 변형하여 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고,

IRS를 구성하는 각각의 반사 유닛의 계수에 대하여 닫힌 형태(closed form)의 해를 제공하는

MIMO 시스템의 보안 용량 최적화 장치.

청구항 7

제5항에 있어서,

공분산 행렬 변환부는,

MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 문제를 다중 접속 채널의 문제로 변환하는

MIMO 시스템의 보안 용량 최적화 장치.

청구항 8

제5항에 있어서,

계산부는,

최적의 대각 행렬을 구하기 위해 각각 독립적인 IRS 반사 유닛의 계수에 좌표하강법(coordinate descent methods)을 적용하여 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하는

MIMO 시스템의 보안 용량 최적화 장치.

발명의 설명

기술 분야

[0001] 본 발명은 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 방법 및 장치에 관한 것이다.

배경 기술

[0002] 지능형 반사 표면(Intelligent Reflecting Surface; IRS)은 무선 통신 용량을 향상시키거나 소모 전력을 최소화할 수 있는 유망한 솔루션으로 주목 받고 있다. IRS는 독립적으로 위상 및 진폭 조절이 가능한 값싼 수동 소자 요소들로 구현되어 있으며 각각의 수동 소자 요소들을 조절하여 방향성 신호를 강화하거나 감소시키는 수동 빔포밍을 설계할 수 있다. 따라서 IRS를 이용하면 정보 전달율을 높이거나 소모 전력을 최소화하는 등, 저 비용

으로 무선 통신 채널을 원하는 대로 바꿀 수 있다.

- [0003] 최근 다중 안테나를 가지는 송수신기가 있는 시스템(MISO/MIMO)에서 다중 안테나를 가지는 도청자가 있는 경우에 IRS를 도입하여 통신 성능을 향상시키는 기술이 등장하였다. 사용자와 도청자 근처에 배치된 IRS는 먼저 요소의 위상 변이를 조정하여 비밀 율을 높인다. 다음으로 송신 신호의 전력을 합법적 유저에게는 강하게 도청자에게는 약하도록 신호를 설계한다. 따라서 송신 신호와 IRS 반사 유닛의 위상을 공동으로 최적화함으로써 사용자의 보안 용량을 극대화할 수 있다. 그러나 이 두 가지를 최적화하는 문제는 변수가 결합되어 있고 비볼록 최적화 문제이기 때문에 해결하기 어렵다.

발명의 내용

해결하려는 과제

- [0004] 본 발명이 이루고자 하는 기술적 과제는 IRS가 있는 MIMO 시스템의 보안용량을 최대화하기 위해 공분산 행렬과 IRS 유닛의 계수를 교대로 최적화하여 해를 구하는 방법 및 장치를 제공하는데 있다. 또한, 기존의 알고리즘에서 제안하는 실험적으로 최적의 값을 찾는 수치 최적화(numerical optimization) 기법과 다르게 닫힌 형태의 해를 제공함으로써 항상 최적의 해에 빠르게 수렴하는 것을 보장하고자 한다. 또한, 단일 사용자의 보안 용량을 증가시키는 방법을 확장함으로써 다중 사용자의 보안 합 용량을 최대화하고자 한다.

과제의 해결 수단

- [0005] 일 측면에 있어서, 본 발명에서 제안하는 합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 방법은 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계, 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계, 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계 및 MIMO 시스템의 보안 용량이 수렴할 때까지 상기 공분산 행렬을 계산하여 채널을 갱신하는 단계 및 상기 대각 행렬을 계산하여 채널을 갱신하는 단계를 반복하는 단계를 포함한다.

- [0006] 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계는 동일한 해를 갖는 문제로 변형하여 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고, IRS를 구성하는 각각의 반사 유닛의 계수에 대하여 닫힌 형태(closed form)의 해를 제공한다.

- [0007] 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계는 MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 문제를 다중 접속 채널의 문제로 변환한다.

- [0008] 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계는 최적의 대각 행렬을 구하기 위해 각각 독립적인 IRS 반사 유닛의 계수에 좌표하강법(coordinate descent methods)을 적용하여 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산한다.

- [0009] 또 다른 일 측면에 있어서, 본 발명에서 제안하는 합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 장치는 계산부에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신하는 업데이트부, 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고, 업데이트부를 통해 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하는 계산부, 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 공분산 행렬 변환부 및 MIMO 시스템의 보안 용량이 수렴할 때까지 계산부가 공분산 행렬을 계산하고, 대각 행렬을 계산하고, 업데이트부가 계산부에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신하는 과정을 반복하도록 제어하는 제어부를 포함한다.

발명의 효과

- [0010] 본 발명의 실시예들에 따르면 IRS가 있는 MIMO 시스템의 보안용량을 최대화하기 위해 공분산 행렬과 IRS 유닛의

계수를 교대로 최적화하여 해를 구하고, 기존의 알고리즘에서 제안하는 실험적으로 최적의 값을 찾는 수치 최적화(numerical optimization) 기법과 다르게 닫힌 형태의 해를 제공하므로 항상 최적의 해에 빠르게 수렴하는 것을 보장할 수 있다. 또한, 단일 사용자의 보안 용량을 증가시키는 방법을 확장함으로써 다중 사용자의 보안 용량을 최대화할 수 있다.

도면의 간단한 설명

- [0011] 도 1은 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 모델을 설명하기 위한 도면이다.
- 도 2는 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 방법을 설명하기 위한 흐름도이다.
- 도 3은 본 발명의 일 실시예에 따른 단일 합법적 사용자, 단일 도청자 및 IRS가 있는 MIMO 시스템에서의 보안 용량 최적화 알고리즘을 나타내는 도면이다.
- 도 4는 본 발명의 일 실시예에 따른 복수의 합법적 사용자, 단일 도청자 및 IRS가 있는 MIMO 시스템에서의 보안 용량 최적화 알고리즘을 나타내는 도면이다.
- 도 5는 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 장치의 구성을 나타내는 도면이다.
- 도 6은 본 발명의 일 실시예에 따른 보안 용량 최적화 알고리즘의 반복 횟수에 따른 수렴성에 대한 그래프이다.
- 도 7은 본 발명의 일 실시예에 따른 단일 사용자가 있는 MISO 시스템에서 반사 유닛 수에 따른 보안 용량에 대한 그래프이다.
- 도 8은 본 발명의 일 실시예에 따른 단일 사용자가 있는 MIMO 시스템에서 SNR에 따른 보안 용량에 대한 그래프이다.
- 도 9는 본 발명의 일 실시예에 따른 다중 사용자가 있는 브로드캐스트 채널에서 사용자의 안테나 수에 따른 보안 용량에 대한 그래프이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 이하, 본 발명의 실시 예를 첨부된 도면을 참조하여 상세하게 설명한다.
- [0014] 도 1은 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 모델을 설명하기 위한 도면이다.
- [0015] 도 1을 참조하면, 지능형 반사 표면(Intelligent Reflecting Surface; IRS)을 포함하는 MIMO 도청 채널의 시스템 모델을 나타내었다. 여기서 사용자1은 합법적 사용자(110)를 나타내고, 사용자2는 도청자(120)를 나타낸다. 송신기(130)는 안테나(N_t)를 갖고, 사용자 i (여기서, $i = 1, 2$)는 안테나($N_{r,i}$)를 갖는다. $\mathbf{H}_i \in \mathbb{C}^{N_{r,i} \times N_t}$ 는 송신기에서 수신기 i 로의 직접 채널을 나타낸다.
- [0016] IRS에는 조정 가능한 진폭 및/또는 위상으로 신호를 재분산 할 수 있는 M 수동 반사 장치가 장착되어 있다. IRS 컨트롤러는 반사 계수 $\alpha_m \in \mathbb{C}$, i.e., $|\alpha_m| = 1$, $m = 1, 2, \dots, M$ 의 위상을 조정한다고 가정한다.
- [0017] $\mathbf{T} \in \mathbb{C}^{N_t \times M}$ 는 IRS로부터 송신기로의 채널이고, $\mathbf{R}_i \in \mathbb{C}^{N_{r,i} \times M}$ 는 IRS로부터 수신기 i 로의 채널을 나타낸다. 채널 상호성으로 인해, 송신기로부터 IRS로의 채널은 $\mathbf{T}^H \in \mathbb{C}^{M \times N_t}$ 이다. $\Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ 은 IRS 각각의 반사 유닛의 계수로 구성된 대각 행렬을 나타낸다. 송신기에서 수신기 i 로의 유효 채널은 $\tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H$ 로 주어진다.

- [0019] 도 2는 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 방법을 설명하기 위한 흐름도이다.
- [0020] 제안하는 합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 방법은 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신하는 단계(210), 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환하는 단계(220), 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신하는 단계(230) 및 MIMO 시스템의 보안 용량이 수렴할 때까지 상기 공분산 행렬을 계산하여 채널을 갱신하는 단계 및 상기 대각 행렬을 계산하여 채널을 갱신하는 단계를 반복하는 단계(240)를 포함한다.
- [0021] 단계(210)에서, 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신한다.
- [0022] 먼저, 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득(211)한다. 획득된 채널 정보에 대하여 반사 유닛의 계수에 대한 최적의 브로드캐스트 채널의 공분산 행렬을 계산하여 채널을 갱신한다(212).
- [0023] 동일한 해를 갖는 문제로 변형하여 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고, IRS를 구성하는 각각의 반사 유닛의 계수에 대하여 닫힌 형태(closed form)의 해를 제공한다.
- [0024] 단계(220)에서, 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환한다. 이때, MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 문제를 다중 접속 채널의 문제로 변환한다.
- [0025] 단계(230)에서, 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산하여 채널을 갱신한다.
- [0026] 최적의 대각 행렬을 구하기 위해 각각 독립적인 IRS 반사 유닛의 계수에 좌표하강법(coordinate descent methods)을 적용하여 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산한다.
- [0027] 단계(240)에서, MIMO 시스템의 보안 용량이 수렴할 때까지 상기 공분산 행렬을 계산하여 채널을 갱신하는 단계 및 상기 대각 행렬을 계산하여 채널을 갱신하는 단계를 반복한다.
- [0028] 제안하는 교대 최적화 알고리즘에서는 먼저 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고 브로드캐스트 채널의 공분산 행렬을 최적화한 뒤, 최적화된 브로드캐스트 채널의 공분산 행렬을 고정하고 대각 행렬을 최적화하며 이 과정을 보안 용량이 수렴할 때까지 반복한다. 도 3 내지 도 4의 알고리즘을 참조하여 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 과정에 관해 아래에서 더욱 상세히 설명한다.
- [0030] 도 3은 본 발명의 일 실시예에 따른 단일 합법적 사용자, 단일 도청자 및 IRS가 있는 MIMO 시스템에서의 보안 용량 최적화 알고리즘을 나타내는 도면이다.
- [0031] 본 발명의 실시예에 따른 다중 안테나를 가지는 1명의 합법적 사용자, 1명의 도청자 그리고 IRS가 있는 MIMO 시스템에서 수신된 신호는 다음과 같이 나타낼 수 있다:
- [0032]
$$\mathbf{y}_i = (\mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H) \mathbf{x} + \mathbf{z}_i, \quad i = 1, 2,$$
 수식 1
- [0033] 이때 $\mathbf{y}_i \in \mathbb{C}^{N_{r,i}}$ 는 수신 신호 벡터, $\mathbf{x} \in \mathbb{C}^{N_t}$ 는 송신 신호 벡터, $\mathbf{z}_i \in \mathbb{C}^{N_{r,i}}$ 는 가산 백색 가우스 잡음 벡터이다. $\mathbf{H}_i \in \mathbb{C}^{N_{r,i} \times N_t}$ 는 합법적 사용자 및 도청자와 송신기 사이의 채널 행렬, $\mathbf{R}_i \in \mathbb{C}^{N_{r,i} \times M}$ 는 합법적 사용자 및 도청자와 IRS사이의 채널 행렬, $\mathbf{T} \in \mathbb{C}^{N_t \times M}$ 는 송신기와 IRS사이의 채널행렬, $\Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ 는 IRS를 구성하는 각각의 반사 유닛의 계수 $|\alpha_m| = 1$ 로 구성된 대각 행렬이며, 송신신호의 전송 전력 제한은 $\text{tr}(\mathbf{Q}) \leq P$, $\mathbf{Q} = \mathbf{E}[\mathbf{x}\mathbf{x}^H] \in \mathbb{C}^{N_t \times N_t}$ 이다. 도청자와 IRS가 있는 MIMO 채널에서 송신 신호와 반사 유닛을 조절하여

보안 용량(secretcy capacity)의 최대값을 찾는 문제는 다음과 같이 나타낼 수 있다:

$$\begin{aligned} & \max_{\mathbf{Q}, \Phi} \log \det(\mathbf{I} + \tilde{\mathbf{H}}_1 \mathbf{Q} \tilde{\mathbf{H}}_1^H) - \log \det(\mathbf{I} + \tilde{\mathbf{H}}_2 \mathbf{Q} \tilde{\mathbf{H}}_2^H) \\ & \text{s. t. } \tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}_i^H, i = 1, 2 \quad \leftarrow \\ & \quad \Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\} \quad \leftarrow \\ & \quad |\alpha_m| = 1, \forall m \quad \leftarrow \\ & \quad \text{tr}(\mathbf{Q}) \leq P \quad \leftarrow \\ & \quad \mathbf{Q} \succeq \mathbf{0}. \end{aligned}$$

[0034] 수식2

[0035] 수식 2는 비볼록 최적화 문제로 풀기 어려운 문제가 있다. 본 발명에서는 교대 최적화 방법으로 이 문제를 해결하였다.

[0036] 제안하는 교대 최적화 알고리즘에서는 먼저 Φ 를 고정하고 $\mathbf{Q}$ 를 최적화한 뒤 $\mathbf{Q}$ 를 고정하고 Φ 를 최적화하며 이 과정을 수렴할 때까지 반복한다.

[0037] IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬 Φ 가 고정되었다면 이 문제는 MIMO 시스템에서 보안 용량을 최대화하는 전통적인 문제와 같다. 따라서 KKT에 수렴하는 교대 최적화[1], barrier method[2] 등으로 전역 최적해를 구할 수 있다.

[0038] 다음으로 앞서 구한 $\mathbf{Q}$ 를 사용하여 Φ 를 최적화한다. 하지만 Φ 에 대해서 비볼록(concave) 함수가 아니기 때문에 최적의 Φ 를 구하기 어렵다. 각각의 IRS 반사 유닛의 계수 α_m 은 독립적이므로 최적의 $\{\alpha_m\}_{m=1}^M$ 을 구하기 위해 좌표하강법(coordinate descent methods)을 적용하였다. 따라서 $\{\alpha_j\}_{j=1, j \neq m}^M$ 와 $\mathbf{Q}$ 가 주어졌을 때 각각의 α_m 에 대한 하위 문제들이 수렴할 때까지 최적화를 진행한다. 각각의 α_m 에 대한 유효 MIMO 채널을 다시 작성하면 다음과 같다:

$$\tilde{\mathbf{H}}_i = \mathbf{H}_i + (\sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H) + \alpha_m \mathbf{r}_{im} \mathbf{t}_m^H, \quad \text{수식 3}$$

[0040] 여기서 $\mathbf{R}_i = [\mathbf{r}_{i1}, \mathbf{r}_{i2}, \dots, \mathbf{r}_{iM}]$, $\mathbf{T}_i = [\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_M]$ 이다. 수식 3을 수식 2에 대입하고 정리하면 다음과 같다:

$$\max_{\alpha_m \in \mathbb{C}} \log \det(\mathbf{I} + \alpha_m \mathbf{p}_{1m} \mathbf{q}_{1m}^H + \alpha_m^* \mathbf{q}_{1m} \mathbf{p}_{1m}^H) - \log \det(\mathbf{I} + \alpha_m \mathbf{p}_{2m} \mathbf{q}_{2m}^H + \alpha_m^* \mathbf{q}_{2m} \mathbf{p}_{2m}^H)$$

$$\text{s. t. } |\alpha_m| = 1, \quad \text{수식 4}$$

[0043] 수식 4를 구성하는 변수는 다음과 같다:

$$\mathbf{p}_{im} = \mathbf{A}_{im}^{-\frac{1}{2}} \mathbf{r}_{im}$$

$$\mathbf{q}_{im} = \mathbf{A}_{im}^{-\frac{1}{2}} (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H) \mathbf{Q} \mathbf{t}_m$$

$$\mathbf{A}_{im} = \mathbf{I} + \mathbf{r}_{im} \mathbf{t}_m^H \mathbf{Q} \mathbf{t}_m \mathbf{r}_{im}^H + (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H) \mathbf{Q} (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H)^H$$

$$\mathbf{B}_{im} = \mathbf{r}_{im} \mathbf{t}_m^H \mathbf{Q} (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H). \quad \text{수식 5}$$

[0048] 본 발명에서는 수식 4를 직접 푸는 것 대신 다음과 같이 동일한 해를 갖는 문제로 변형하여 해결하였다:

$$\max_{\alpha_m \in \mathbb{C}} \frac{1 + \text{Re}\{a_{1m}^* \alpha_m\}}{1 + \text{Re}\{a_{2m}^* \alpha_m\}}$$

$$\text{s. t. } |\alpha_m| = 1. \quad \text{수식 6}$$

[0051] 여기서 $a_{im} = \frac{2(\mathbf{q}_{im}^H \mathbf{p}_{im})^*}{1 - (\|\mathbf{p}_{im}\|^2 \|\mathbf{q}_{im}\|^2 - |\mathbf{q}_{im}^H \mathbf{p}_{im}|^2)}$ 이다. 수식 6에 대한 해는 다음과 같이 닫힌 형태(closed form)로 구할 수

있다:

$$\alpha_m = (a_{1m} - \lambda a_{2m}) / |a_{1m} - \lambda a_{2m}|,$$

수식 7

여기서

λ 는

다음과

같다:

$$\lambda = (1 - \text{Re}\{a_{1m}^* a_{2m}\} + \sqrt{(1 - \text{Re}\{a_{1m}^* a_{2m}\})^2 - (1 - |a_{1m}|^2)(1 - |a_{2m}|^2)}) / (1 - |a_{2m}|^2).$$

수식 8

수식 7을 사용하여 모든 α_m 을 계산한 후에 MIMO 채널의 보안 용량을 구하고 보안 용량이 수렴할 때까지 α_m 을 업데이트 하면 고정된 Q에 대한 최적의 Φ 를 구할 수 있다.

최종적으로 단일 사용자가 있는 시스템에서 $\mathbf{Q}, \Phi$ 를 교대로 업데이트하여 최적의 보안 용량을 구하는 알고리즘은 도 3과 같다.

도 4는 본 발명의 일 실시예에 따른 복수의 합법적 사용자, 단일 도청자 및 IRS가 있는 MIMO 시스템에서의 보안 용량 최적화 알고리즘을 나타내는 도면이다.

본 발명에서는 앞서 다중 안테나를 가지는 1명의 합법적 사용자, 1명의 도청자 그리고 IRS가 있는 MIMO 시스템을 복수의 합법적 사용자를 가지는 MIMO 브로드캐스트 채널(broadcast channel; BC)에서의 문제로 확장하였다.

본 발명의 실시예에 따른 K명의 합법적 사용자, 1명의 도청자 그리고 IRS가 있는 MIMO 브로드캐스트 채널에서 사용자들과 도청자에게 수신된 신호는 다음과 같다:

$$\mathbf{y}_i = (\mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H) \mathbf{x} + \mathbf{z}_i, i = 1, 2, \dots, K$$

$$\mathbf{y}_e = (\mathbf{G} + \mathbf{U} \Phi \mathbf{T}^H) \mathbf{x} + \mathbf{z}_e,$$

수식 9

이때 $\mathbf{y}_i \in \mathbb{C}^{N_{r,i}}$ 는 합법적 사용자의 수신 신호 벡터, $\mathbf{y}_e \in \mathbb{C}^{N_{r,e}}$ 는 도청자의 수신신호 벡터, $\mathbf{x} \in \mathbb{C}^{N_s}$ 는 송신 신호 벡터, $\mathbf{z}_i \in \mathbb{C}^{N_{r,i}}$ 와 $\mathbf{z}_e \in \mathbb{C}^{N_{r,e}}$ 는 가산 백색 가우스 잡음 벡터이다. $\mathbf{H}_i \in \mathbb{C}^{N_{r,i} \times N_t}$ 는 합법적 사용자와 송신기 사이의 채널 행렬, $\mathbf{R}_i \in \mathbb{C}^{N_{r,i} \times M}$ 은 합법적 사용자와 IRS사이의 채널 행렬, $\mathbf{G} \in \mathbb{C}^{N_{r,e} \times N_t}$ 는 도청자와 송신기 사이의 채널 행렬, $\mathbf{U} \in \mathbb{C}^{N_{r,e} \times M}$ 는 도청자와 IRS 사이의 채널 행렬, $\mathbf{T} \in \mathbb{C}^{N_t \times M}$ 는 송신기와 IRS사이의 채널행렬, $\Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ 는 IRS를 구성하는 각각의 반사 유닛의 계수 $|\alpha_m| = 1$ 로 구성된 행렬이다.

본 발명에서는 MIMO 브로드캐스트 채널에서 최대 보안 합 용량을 구하기 위해서 더티 페이퍼 코딩(dirty paper coding; DPC)을 도입하였다. 이 때 i 번째 합법적 사용자의 달성 가능한 보안용량[3]은 다음과 같다:

$$R_i = \log \frac{\det(\mathbf{I} + \tilde{\mathbf{H}}_i (\sum_{j=i}^K \mathbf{Q}_j) \tilde{\mathbf{H}}_i^H)}{\det(\mathbf{I} + \tilde{\mathbf{H}}_i (\sum_{j=i+1}^K \mathbf{Q}_j) \tilde{\mathbf{H}}_i^H)} - \log \frac{\det(\mathbf{I} + \tilde{\mathbf{G}} (\sum_{j=i}^K \mathbf{Q}_j) \tilde{\mathbf{G}}^H)}{\det(\mathbf{I} + \tilde{\mathbf{G}} (\sum_{j=i+1}^K \mathbf{Q}_j) \tilde{\mathbf{G}}^H)},$$

수식 10

여기서 합법적 사용자와 도청자의 유효 채널은 각각 $\tilde{\mathbf{H}} = \mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H, \tilde{\mathbf{G}} = \mathbf{G} + \mathbf{U} \Phi \mathbf{T}^H$ 이다.

다중 사용자와 도청자 그리고 IRS가 있는 MIMO 채널에서 송신 신호와 반사 유닛을 조절하여 보안 합 용량의 최대값을 찾는 문제는 다음과 같이 나타낼 수 있다.

$$\max_{\{\mathbf{Q}_i\}} \sum_{i=1}^K R_i$$

$$\text{s. t. } \Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$$

$$|\alpha_m| = 1, \forall m$$

$$\sum_{i=1}^K \text{tr}(\mathbf{Q}_i) \leq P$$

$$\mathbf{Q}_i \succeq \mathbf{0}, \forall i,$$

수식 11

이 문제는 비볼록 최적화 문제로 풀기 어려운 문제가 있다. 사용자가 한 명일 때와 마찬가지로 교대 최적화 방법을 적용하였다. 먼저 Φ 를 고정하고 $\{\mathbf{Q}_i\}$ 를 최적화한 뒤 $\{\mathbf{Q}_i\}$ 를 고정하고 Φ 를 최적화하며 이 과정을 수렴할 때까지 반복한다.

먼저 Φ 가 고정되었다면 이 문제는 MIMO 브로드캐스트 채널에서 보안 합 용량을 최대화하는 전통적인 문제와 같다. 본 발명에서는 MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널에서의 문제를 다중 접속 채널(multiple access channel, MAC) 문제로 변환한 뒤 교대 최적화 알고리즘으로 $\{\mathbf{Q}_i\}$ 를 최적화하였다 [4].

다음으로 앞서 구한 $\{\mathbf{Q}_i\}$ 를 사용하여 Φ 를 최적화한다. 먼저 MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 공분산 행렬 $\{\mathbf{Q}_i\}$ 을 다중 접속 채널의 공분산 행렬 $\{\mathbf{S}_i\}$ 로 바꾸면 수식 11에서 Φ 를 최적화하는 문제는 다음과 같이 작성할 수 있다[5]:

$$\max_{\Phi} \log \det(\mathbf{I} + \sum_{i=1}^K \tilde{\mathbf{H}}_i^H \mathbf{S}_i \tilde{\mathbf{H}}_i) - \log \det(\mathbf{I} + \tilde{\mathbf{G}}^H \mathbf{S}_i^e \tilde{\mathbf{G}})$$

$$\text{s. t. } \Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$$

$$|\alpha_m| = 1, \forall m$$

수식 12

수식 12는 Φ 에 대해서 비볼록 함수가 아니기 때문에 최적의 Φ 를 구하기 어렵다. 각각의 IRS 반사 유닛의 계수 α_m 은 독립적이므로 최적의 $\{\alpha_m\}_{m=1}^M$ 을 구하기 위해 좌표하강법을 적용하였다. 따라서 $\{\alpha_j\}_{j=1, j \neq m}^M$ 과 $\{\mathbf{S}_i\}$ 가 주어졌을 때 각각의 α_m 에 대한 하위 문제들이 수렴할 때까지 최적화를 진행한다. 각각의 α_m 에 대한 합법적 사용자의 유효 채널 $\tilde{\mathbf{H}}_i = \mathbf{H}_i + (\sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H) + \alpha_m \mathbf{r}_{im} \mathbf{t}_m^H$ 과 도청자의 유효 채널 $\tilde{\mathbf{G}} = \mathbf{G} + (\sum_{j=1, j \neq m}^M \alpha_j \mathbf{u}_j \mathbf{t}_j^H) + \alpha_m \mathbf{r}_m \mathbf{t}_m^H$ 을 사용하여 수식 12의 목적함수를 다시 정리하면 다음과 같다:

$$\max_{\alpha_m \in \mathbb{C}} \log \det(\mathbf{I} + \alpha_m \mathbf{p}_{1m} \mathbf{q}_{1m}^H + \alpha_m^* \mathbf{q}_{1m} \mathbf{p}_{1m}^H) - \log \det(\mathbf{I} + \alpha_m \mathbf{p}_{2m} \mathbf{q}_{2m}^H + \alpha_m^* \mathbf{q}_{2m} \mathbf{p}_{2m}^H)$$

$$\text{s. t. } |\alpha_m| = 1, \text{ s. t. } |\alpha_m| = 1,$$

수식 13

수식 13을 구성하는 변수는 다음과 같다:

$$\mathbf{p}_{1m} = \mathbf{A}_m^{-\frac{1}{2}} \sum_{i=1}^K (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H)^H \mathbf{S}_i \mathbf{r}_{im}$$

$$\mathbf{q}_{1m} = \mathbf{A}_m^{-\frac{1}{2}} \mathbf{t}_m \mathbf{q}_{1m} = \mathbf{A}_m^{-\frac{1}{2}} \mathbf{t}_m$$

$$\mathbf{p}_{2m} = \mathbf{C}_m^{-\frac{1}{2}} (\mathbf{G} + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{u}_j \mathbf{t}_j^H)^H \mathbf{S}^e \mathbf{u}_m$$

$$\mathbf{q}_{2m} = \mathbf{C}_m^{-\frac{1}{2}} \mathbf{t}_m \mathbf{q}_{2m} = \mathbf{C}_m^{-\frac{1}{2}} \mathbf{t}_m$$

$$\mathbf{A}_m = \mathbf{I} + \sum_{i=1}^K \mathbf{t}_m \mathbf{r}_{im}^H \mathbf{S}_i \mathbf{r}_{im} \mathbf{t}_m^H + \sum_{i=1}^K (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H)^H \mathbf{Q} (\mathbf{H}_i + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{r}_{ij} \mathbf{t}_j^H)$$

$$\mathbf{C}_m = \mathbf{I} + \mathbf{t}_m \mathbf{u}_m^H \mathbf{S}^e \mathbf{u}_m \mathbf{t}_m^H + (\mathbf{G} + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{u}_j \mathbf{t}_j^H)^H \mathbf{S}^e (\mathbf{G} + \sum_{j=1, j \neq m}^M \alpha_j \mathbf{u}_j \mathbf{t}_j^H)$$

수식 14

- [0089] 여기서 $\mathbf{R}_i = [\mathbf{r}_{i1}, \mathbf{r}_{i2}, \dots, \mathbf{r}_{iM}]$, $\mathbf{T}_i = [\mathbf{t}_1, \mathbf{t}_2, \dots, \mathbf{t}_M]$, $\mathbf{U}_i = [\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_M]$ 이다.
- [0090] 수식 13은 단일 사용자에서의 α_m 을 구하는 문제와 같으므로 수식 7과 수식 14를 사용하여 α_m 을 구할 수 있다. 보안 용량이 수렴할 때까지 α_m 을 업데이트 하면 고정된 공분산 행렬에 대한 최적의 Φ 를 구할 수 있다.
- [0091] 최종적으로 다중 사용자가 있는 시스템에서 $\{\mathbf{Q}_i\}, \Phi$ 를 교대로 업데이트하여 최적의 보안용량을 구하는 알고리즘은 도 4와 같다.
- [0093] 도 5는 본 발명의 일 실시예에 따른 지능형 반사 표면을 포함하는 MIMO 시스템의 보안 용량 최적화 장치의 구성을 나타내는 도면이다.
- [0094] 제안하는 합법적 사용자, 도청자 및 IRS(Intelligent Reflecting Surface)가 있는 MIMO 시스템의 보안 용량 최적화 장치(500)는 계산부(510), 업데이트부(520), 공분산 행렬 변환부(530) 및 제어부(540)를 포함한다.
- [0095] 업데이트부(520)는 계산부(510)에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신한다.
- [0096] 계산부(510)는 합법적 사용자, 도청자 및 송신기 간의 채널 정보를 획득하여 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고, 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산한다. 이후, 업데이트부(520)를 통해 갱신된 브로드캐스트 채널의 공분산 행렬을 고정하고, 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산한다.
- [0097] 계산부(510)는 먼저, 합법적 사용자, 도청자 및 송신기 간의 획득된 채널 정보에 대하여 반사 유닛의 계수에 대한 최적의 브로드캐스트 채널의 공분산 행렬을 계산한다. 이때, 동일한 해를 갖는 문제로 변형하여 고정된 대각 행렬에 대한 브로드캐스트 채널의 공분산 행렬을 계산하고, IRS를 구성하는 각각의 반사 유닛의 계수에 대하여 닫힌 형태(closed form)의 해를 제공한다.
- [0098] 계산부(510)는 최적의 대각 행렬을 구하기 위해 각각 독립적인 IRS 반사 유닛의 계수에 좌표하강법(coordinate descent methods)을 적용하여 고정된 공분산 행렬에 대한 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 계산한다.
- [0099] 공분산 행렬 변환부(530)는 브로드캐스트 채널의 공분산 행렬을 다중 접속 채널의 공분산 행렬로 변환한다. 이때, MIMO MAC-BC 이중성을 사용하여 브로드캐스트 채널의 문제를 다중 접속 채널의 문제로 변환한다.
- [0100] 제어부(540)는 MIMO 시스템의 보안 용량이 수렴할 때까지 계산부가 공분산 행렬을 계산하고, 대각 행렬을 계산하고, 업데이트부가 계산부에서 계산된 공분산 행렬 및 대각 행렬을 이용하여 채널을 갱신하는 과정을 반복하도록 제어한다.
- [0101] 제안하는 교대 최적화 알고리즘에서는 먼저 IRS를 구성하는 각각의 반사 유닛의 계수를 포함하는 대각 행렬을 고정하고 브로드캐스트 채널의 공분산 행렬을 최적화한 뒤, 최적화된 브로드캐스트 채널의 공분산 행렬을 고정하고 대각 행렬을 최적화하며 이 과정을 보안 용량이 수렴할 때까지 반복한다.
- [0102] 본 발명의 실시예들에 따르면 IRS가 있는 MIMO 시스템의 보안용량을 최대화하기 위해 공분산 행렬과 IRS 유닛의 계수를 교대로 최적화하여 해를 구하고, 기존의 알고리즘에서 제안하는 실험적으로 최적의 값을 찾는 수치 최적화(numerical optimization) 기법과 다르게 닫힌 형태의 해를 제공하므로 항상 최적의 해에 빠르게 수렴하는 것을 보장할 수 있다. 또한, 단일 사용자의 보안 용량을 증가시키는 방법을 확장함으로써 다중 사용자의 보안 합용량을 최대화할 수 있다.
- [0103] 제안하는 기법의 성능 검증하기 위해서 IRS가 존재하지 않는(without IRS), 단일 사용자를 가지는 MISO 시스템에서 가우시안 무선헌당(Gaussian randomization)을 사용한 SDR(Gauss randomization)[6], 단일 사용자를 가지는 MIMO 시스템에서 이분법(bisection search)을 적용하여 최적의 솔루션을 가지는 OBO(Bisection)[7] 그리고 제안하는 기법 CD(Exact)에 대한 성능을 비교하였다.
- [0105] 도 6은 본 발명의 일 실시예에 따른 보안 용량 최적화 알고리즘의 반복 횟수에 따른 수렴성에 대한 그래프이다.
- [0106] 도 6을 참조하면, IRS 반사 유닛 개수가 16, 32 그리고 64일 때의 결과로 모든 경우 6번 이내의 반복에서 수렴

하는 것을 확인할 수 있다. 또한 IRS 반사 유닛의 계수의 초기 값을 무작위로 정하는 것과 0으로 했을 때의 결과가 거의 동일하므로 제안하는 방법이 초기 값에 상관없이 잘 수렴하는 것을 알 수 있다.

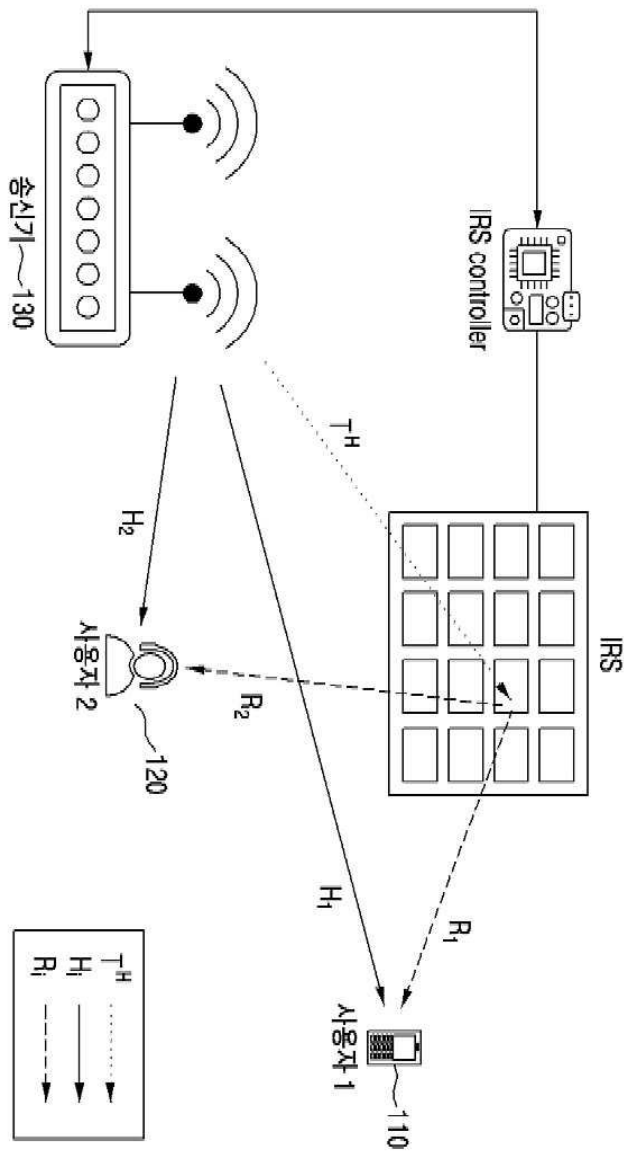
- [0108] 도 7은 본 발명의 일 실시예에 따른 단일 사용자가 있는 MISO 시스템에서 반사 유닛 수에 따른 보안 용량에 대한 그래프이다.
- [0109] 도 7은 1개의 안테나를 가지는 단일 사용자가 있는 상황에서 제한된 전력이 10 dBm일 때 IRS 반사 유닛의 개수에 따른 보안 용량을 보여주는 그래프이다. IRS가 없는 시스템의 성능은 IRS의 수와 상관없이 성능이 일정하며 IRS를 고려한 기법들은 반사 유닛의 개수가 증가함에 따라 보안 용량이 크게 증가하는 것을 확인할 수 있다. 따라서 IRS가 보안 용량을 증가시키는데 효과가 있는 것을 알 수 있다. 또한 반사 유닛의 개수가 많은 경우 CD와 OBO의 성능은 SDR의 성능보다 우수한 것을 확인할 수 있다.
- [0111] 도 8은 본 발명의 일 실시예에 따른 단일 사용자가 있는 MIMO 시스템에서 SNR에 따른 보안 용량에 대한 그래프이다.
- [0112] 도 8을 참조하면, SDR은 단일 수신 안테나만 고려하므로 성능을 비교할 수 있으며, IRS가 없는 경우 반사 유닛의 개수 M 과 상관없이 같은 성능을 가진다. CD와 OBO가 찾은 최적의 해가 같은 것을 확인할 수 있으며 SNR이 증가할수록 IRS가 없는 경우와의 성능 차이가 커지는 것을 확인할 수 있다.
- [0114] 도 9는 본 발명의 일 실시예에 따른 다중 사용자가 있는 브로드캐스트 채널에서 사용자의 안테나 수에 따른 보안 용량에 대한 그래프이다.
- [0115] 도 9를 참조하면, 보안 용량은 합법적인 사용자의 안테나 수에 따라 단조 증가하는 것을 확인할 수 있다. 또한 합법적인 사용자가 증가할수록 달성 가능한 보안 합 용량이 더 높은 것을 확인할 수 있다.
- [0117] 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.
- [0118] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0119] 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 판

독 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.

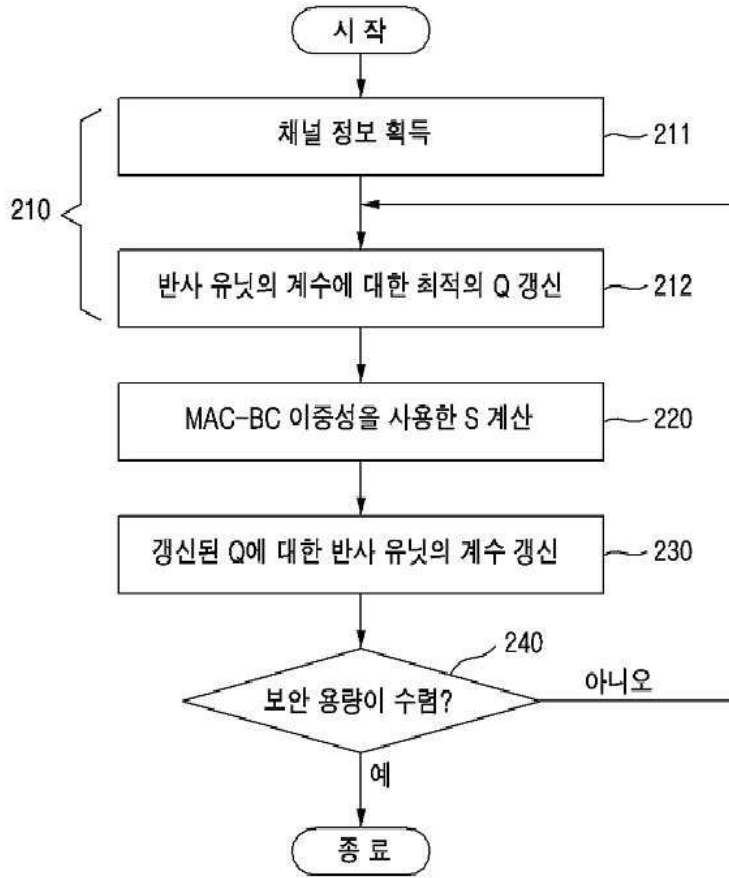
- [0120] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.
- [0121] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.
- [0123] <참고문헌>
- [0124] [1] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714-1727, Sep. 2013.
- [0125] [2] S. Loyka and C. D. Charalambous, "An algorithm for global maximization of secrecy rates in Gaussian MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 6, pp. 2288-2299, June 2015.
- [0126] [3] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083-2114, Apr. 2011.
- [0127] [4] D. Park, "Secrecy sum rates of MIMO multi-receiver wiretap channels," *IEEE Commun. Lett.*, vol. 20, no. 9, pp. 1804-1807, Sept. 2016.
- [0128] [5] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2658-2668, Oct. 2003.
- [0129] [6] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410-1414, Oct. 2019.
- [0130] [7] L. Dong and H.-M. Wang, "Enhancing secure MIMO transmission via intelligent reflecting surface," *IEEE Trans. Wireless Commun.*, vol. 19, no. 11, pp. 7543-7556, Nov. 2020.

도면

도면1



도면2



도면3

Algorithm 1 Secrecy Rate Maximization Algorithm for IRS-aided MIMO Wiretap Channels.

- 1: Input: $\{\mathbf{H}_i\}, \{\mathbf{R}_i\}, \mathbf{T}, P$
- 2: Initialize Φ
- 3: Repeat until convergence
- 4: $\tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H, i = 1, 2$
- 5: $\mathbf{Q} = \arg \max_{\mathbf{Q} \succeq 0: \text{tr}(\mathbf{Q}) \leq P} \log \det (\mathbf{I} + \tilde{\mathbf{H}}_1 \mathbf{Q} \tilde{\mathbf{H}}_1^H) - \log \det (\mathbf{I} + \tilde{\mathbf{H}}_2 \mathbf{Q} \tilde{\mathbf{H}}_2^H)$
- 6: Repeat until convergence
- 7: for $m = 1 : M$
- 8: Compute $a_{im}, i = 1, 2$
- 9: Compute λ
- 10: $\alpha_m = (a_{1m} - \lambda a_{2m}) / |a_{1m} - \lambda a_{2m}|$
- 11: end for
- 12: end
- 13: $\Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$
- 14: end

도면4

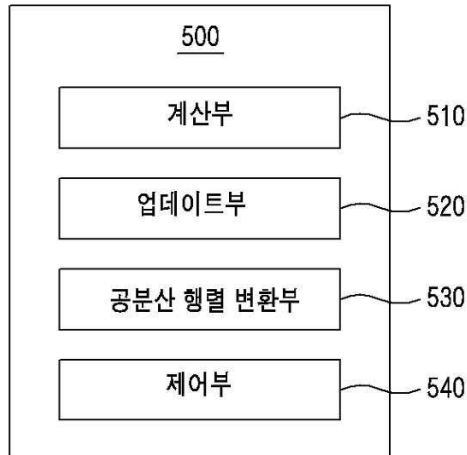
Algorithm 2 Sum Rate Maximization Algorithm for IRS-aided MIMO Broadcast Channels with an External Eavesdropper.

```

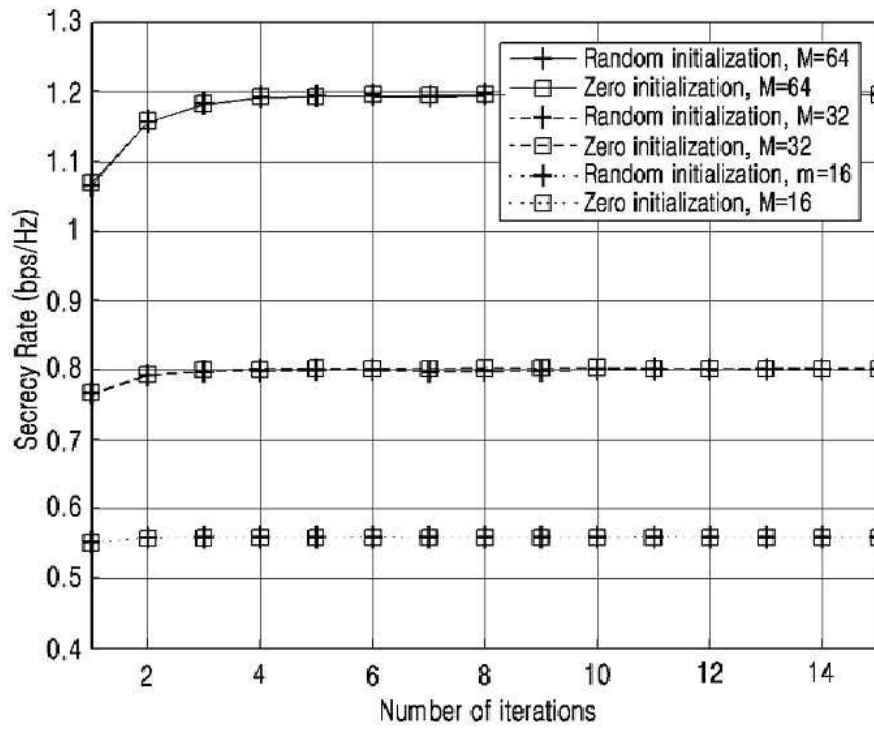
1: Input:  $\{\mathbf{H}_i\}, \{\mathbf{R}_i\}, \mathbf{T}, \mathbf{G}, \mathbf{U}, P$ 
2: Initialize  $\Phi$ 
3: Repeat until convergence
4:    $\tilde{\mathbf{H}}_i = \mathbf{H}_i + \mathbf{R}_i \Phi \mathbf{T}^H, \forall i$ 
5:    $\tilde{\mathbf{G}} = \mathbf{G} + \mathbf{U} \Phi \mathbf{T}^H$ 
6:   Find  $\{\mathbf{Q}_i\}_{i=1}^K$  that maximizes  $\sum_{i=1}^K R_i^{\text{BC}}(\{\tilde{\mathbf{H}}_i\}, \{\mathbf{Q}_i\}) - R_i^{\text{BC}}(\tilde{\mathbf{G}}, \{\mathbf{Q}_i\})$ 
      such that  $\sum_{i=1}^K \text{tr}(\mathbf{Q}_i) \leq P$  and  $\mathbf{Q}_i \succeq 0, \forall i$ 
7:   Compute  $\{\mathbf{S}_i\}_{i=1}^K$  and  $\mathbf{S}^e$  using the MIMO MAC-BC duality
8:   Repeat until convergence
9:     for  $m = 1 : M$ 
10:       Compute  $a_{im}, i = 1, 2$ 
11:       Compute  $\lambda$ 
12:        $\alpha_m = (a_{1m} - \lambda a_{2m}) / |a_{1m} - \lambda a_{2m}|$ 
13:     end for
14:   end
15:    $\Phi = \text{diag}\{\alpha_1, \alpha_2, \dots, \alpha_M\}$ 
16: end

```

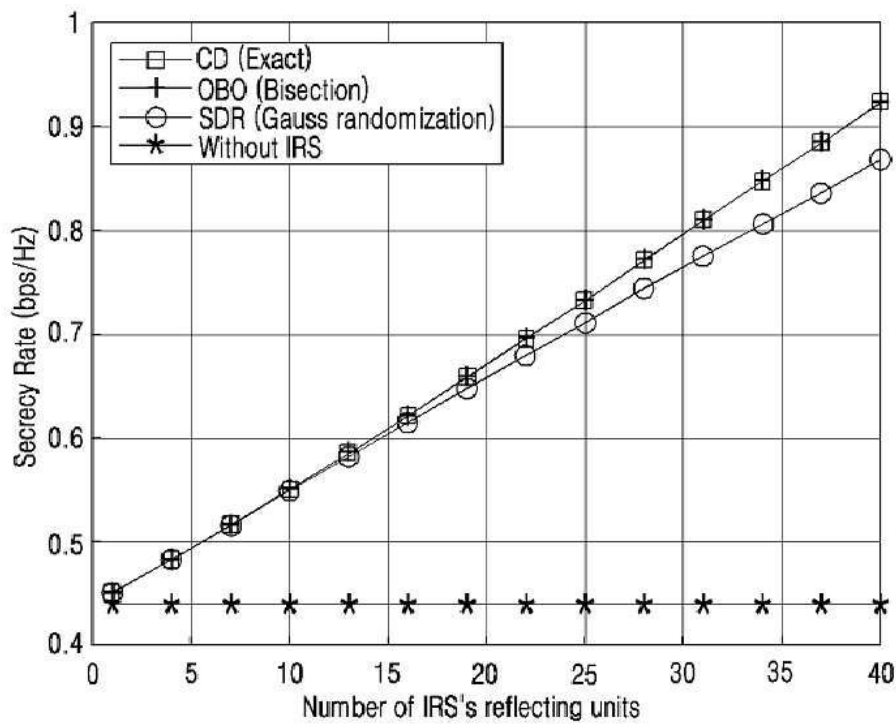
도면5



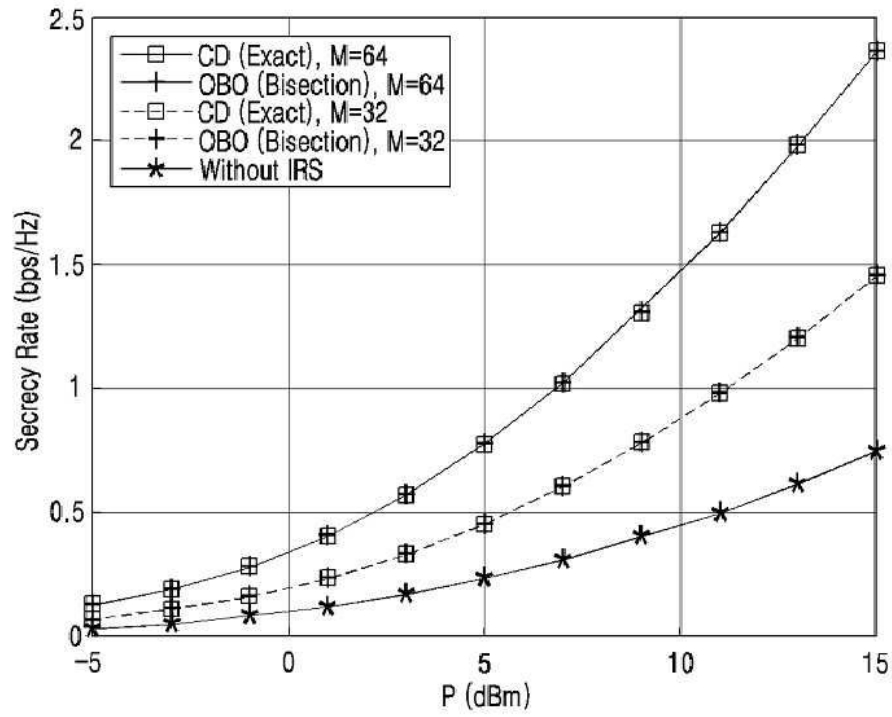
도면6



도면7



도면8



도면9

