(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년08월28일
(11) 등록번호 10-1977593
(24) 등록일자 2019년05월07일

(51) 국제특허분류(Int. Cl.)
H04B 7/04 (2017.01) *H04L 1/06* (2006.01)
(21) 출원번호 10-2012-0067785
(22) 출원일자 2012년06월25일
심사청구일자 2017년06월26일
(65) 공개번호 10-2014-0003706
(43) 공개일자 2014년01월10일
(56) 선행기술조사문헌
3gpp*
US20080094281 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
임종부
경기 용인시 기흥구 삼성2로 97, 기숙사 1동 508호 (농서동, 삼성종합기술원)
장경훈
경기 수원시 영통구 태장로82번길 32, 112동 1602호 (망포동, 동수원엘지빌리지1차)
허미숙
경기 수원시 영통구 청명북로 33, 435동 503호 (영통동, 청명마을4단지아파트)
(74) 대리인
특허법인 무한

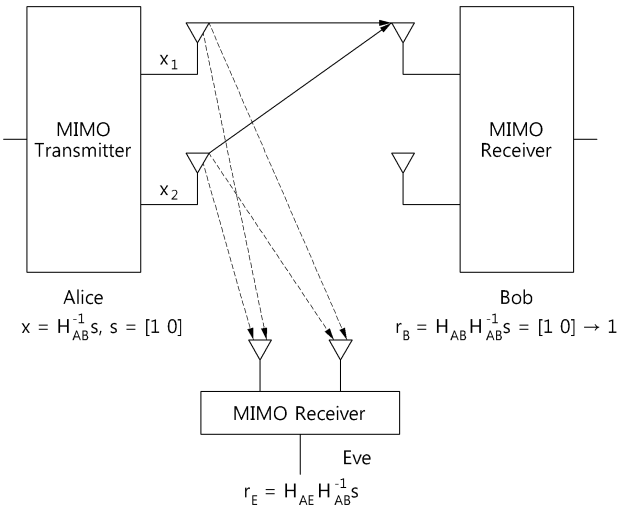
전체 청구항 수 : 총 18 항 심사관 : 황철규

(54) 발명의 명칭 **복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 전송하는 방법 및 수신단에서 시크릿 정보를 수신하는 방법**

(57) 요 약

시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하여 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하고, 채널 정보를 바탕으로 정보 벡터를 프리코딩하여 빔포밍하는 복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 전송단에서 시크릿 정보를 전송하는 방법을 제공할 수 있다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 전송단에서 시크릿 정보를 전송하는 방법에 있어서,

상기 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계;

상기 선택된 인덱스 및 나머지 인덱스를 기초로 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계;

상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 상기 정보 벡터를 프리코딩하는 단계; 및

상기 복수의 전송 안테나들을 이용하여 상기 프리코딩된 정보 벡터를 빔포밍하는 단계

를 포함하고,

상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계는

상기 정보 벡터에 포함되는 복수의 정보 심볼들 중에서 상기 선택된 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제1 값으로 설정하고, 상기 나머지 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제2 값으로 설정하는 단계

를 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 2

제1항에 있어서,

상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계는

상기 복수의 수신 안테나들의 개수를 고려하여 한 타임 슬롯에서 전송할 비트 개수를 결정하는 단계; 및

상기 비트 개수를 고려하여, 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화시키는 정보 벡터를 결정하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 3

제2항에 있어서,

상기 정보 벡터를 결정하는 단계는

상기 시크릿 정보의 길이가 상기 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우,

상기 시크릿 정보 중 상기 공배수에 해당하지 않는 나머지 정보에 아래의 수학식을 만족하는 개수에 해당하는 임의의 비트를 추가하는 단계; 및

상기 임의의 비트가 추가된 나머지 정보에 대한 정보 벡터를 결정하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

[수학식]

임의의 비트 개수= (하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수))

(여기서, %는 나머지(modular) 연산자를 의미함.)

청구항 4

제1항에 있어서, 상기 정보 벡터를 프리코딩하는 단계는

상기 복수의 수신 안테나들 중 상기 선택된 인덱스에 대응하는 수신 안테나에서의 수신 에너지가 높아지도록 상기 정보 벡터를 프리코딩하는 단계

를 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 5

제1항에 있어서,

상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 상기 시크릿 정보에 대한 채널 코딩을 수행할 것인지 여부를 결정하는 단계; 및

상기 채널 코딩을 수행할 것인지 여부를 나타내는 지시자(indicator)를 이용하여 상기 시크릿 정보에 대한 채널 코딩 여부를 표시하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 6

삭제

청구항 7

제1항에 있어서,

상기 복수의 전송 안테나들을 이용하여 해시 함수의 결과값 또는 상기 시크릿 정보에 대한 채널 코딩의 패리티 비트 중 어느 하나를 상기 복수의 수신 안테나들에게 전송하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 8

제1항에 있어서,

암호화를 위한 시크릿 정보(secret information)를 생성하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 9

제1항에 있어서,

둘 이상의 정보 벡터들이 존재하는 경우, 둘 이상의 서브 캐리어들을 이용하여 상기 정보 벡터들을 다중화하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 10

제1항에 있어서,

상기 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계는

상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계이고,

둘 이상의 정보 벡터들이 존재하는 경우, 둘 이상의 서브 캐리어들을 이용하여 상기 정보 벡터들을 다중화하는 단계

를 더 포함하는 전송단에서 시크릿 정보를 전송하는 방법.

청구항 11

복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 수신단에서 시크릿 정보를 수신하는 방법에 있어서,

복수의 수신 안테나들 각각에서 수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신 안테나를 선택하는 단계;

상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스에 기초하여 전송단에 의해 전송된 정보 벡터를 검출하는 단계;

상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스 및 나머지 인덱스를 기초로 상기 검출된 정보 벡터를 시크릿 정보로 디매핑하는 단계; 및

복수의 시크릿 정보를 결합하는 단계

를 포함하고,

상기 적어도 하나의 수신 안테나를 선택하는 단계는

복수의 수신 안테나들 중 미리 설정된 임계값보다 높은 신호의 세기를 가지는 신호를 수신한 적어도 하나의 수신 안테나를 선택하는 단계

를 포함하며,

상기 검출된 정보 벡터는

제1 값으로 설정되고 상기 선택된 수신 안테나에 매핑되는 정보 심볼; 및

제2 값으로 설정되고 상기 복수의 인덱스 중 하나 이상의 나머지 인덱스에 해당하는 상기 복수의 수신 안테나들 중 상기 선택된 수신 안테나를 제외한 나머지 수신 안테나로 매핑되는 나머지 정보 심볼

을 포함하는, 수신단에서 시크릿 정보를 수신하는 방법.

청구항 12

삭제

청구항 13

제11항에 있어서,

상기 검출된 정보 벡터를 시크릿 정보로 디매핑하는 단계는

상기 디매핑된 시크릿 정보의 길이가 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우,

상기 시크릿 정보 중 마지막에 전송된 정보에서 아래의 수학식을 만족하는 개수에 해당하는 임의의 비트를 제거하는 단계

를 포함하는 수신단에서 시크릿 정보를 수신하는 방법.

[수학식]

임의의 비트 수 = (하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수))

(여기서, %는 나머지(modular) 연산자를 의미함.)

청구항 14

제11항에 있어서,

상기 전송단에 의해 사용된 안테나 맵핑 룰(antenna mapping rule)을 결정하는 단계

를 더 포함하는 수신단에서 시크릿 정보를 수신하는 방법.

청구항 15

제11항에 있어서,

복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 코딩된 비트 정보를 디코딩하는 단계

를 더 포함하는 수신단에서 시크릿 정보를 수신하는 방법.

청구항 16

제15항에 있어서,

상기 디코딩하는 단계는

채널 코딩이 수행되었는지 여부를 나타내는 지시자를 이용하여 상기 비트 정보를 디코딩하는 단계

를 포함하는 수신단에서 시크릿 정보를 수신하는 방법.

청구항 17

제11항에 있어서,

상기 수신한 시크릿 정보에 대하여 해시 함수를 적용하는 단계;

전송단으로부터 수신한 해시 함수의 결과값 및 상기 해시 함수를 적용한 결과가 동일한지 여부를 확인하는 단계; 및

상기 확인 결과를 기초로 상기 전송단에게 상기 시크릿 정보의 재전송을 요청하는 단계

를 포함하는 수신단에서 시크릿 정보를 수신하는 방법.

청구항 18

제1항 내지 제5항, 제7항 내지 제11항, 제13항 내지 제17항 중 어느 한 항의 방법을 수행하기 위한 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

청구항 19

복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 시크릿 정보를 전송하는 전송단에 있어서,

상기 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 선택부;

상기 선택된 인덱스 및 나머지 인덱스를 기초로 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 매핑부;

상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 상기 정보 벡터를 프리코딩하는 프리코딩부; 및

상기 복수의 전송 안테나들을 이용하여 상기 프리코딩된 정보 벡터를 빔포밍하는 빔포밍부

를 포함하고,

상기 매핑부는

상기 정보 벡터에 포함되는 복수의 정보 심볼들 중에서 상기 선택된 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제1 값으로 설정하고, 상기 나머지 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제2 값으로 설정하는 시크릿 정보를 전송하는 전송단.

청구항 20

복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 시크릿 정보를 수신하는 수신단에 있어서,

복수의 수신 안테나들 각각에서 수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신

안테나를 선택하는 선택부;

상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스에 기초하여 전송단에 의해 전송된 정보 벡터를 검출하는 검출부;

상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스 및 나머지 인덱스를 기초로 상기 검출된 정보 벡터를 시크릿 정보로 디매핑하는 디매핑부; 및

복수의 시크릿 정보를 결합하는 결합부

를 포함하고,

상기 선택부는

상기 복수의 수신 안테나들 중 미리 설정된 임계값보다 높은 신호의 세기를 가지는 신호를 수신한 상기 적어도 하나의 수신 안테나를 선택하며,

상기 검출된 정보 벡터는

제1 값으로 설정되고 상기 선택된 수신 안테나에 매핑되는 정보 심볼; 및

제2 값으로 설정되고 상기 복수의 인덱스 중 하나 이상의 나머지 인덱스에 해당하는 상기 복수의 수신 안테나들 중 상기 선택된 수신 안테나를 제외한 나머지 수신 안테나로 매핑되는 나머지 정보 심볼

을 포함하는 시크릿 정보를 수신하는 수신단.

발명의 설명

기 술 분 야

[0001] 아래의 실시예들은 복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 전송단에서 시크릿 정보를 전송하는 방법 및 수신단에서 시크릿 정보를 수신하는 방법에 관한 것이다.

배 경 기 술

[0002] 일반적인 통신 시스템에서 사용하는 보안 기술은 레이어(layer)-2 혹은 레이어-3 이상에서의 암호화(encryption)를 사용하며, 공개키 혹은 비밀키 방식의 암호화 기술을 이용하여 송수신을 위한 데이터를 암호화하는 방식을 사용한다. 이러한 방식은 물리 계층(physical layer)의 특성, 다시 말해서 통신 채널(channel)의 특성과는 무관하게 수학적 논리에 의해 보안을 확보한다. 따라서, 제3의 통신 기기가 어떠한 다른 경로에 의해 해당 암호문의 해독 방법을 획득하였을 경우 해당 기기 간의 통신 보안은 무력해진다.

[0003] 특히, 무선 네트워크는 무선 채널의 브로드캐스트(broadcast) 성질로 인해 무선 통신 시스템에서 제 3자의 도청이 용이하다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0004] 일 실시예에 따르면, 복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 전송단에서 시크릿 정보를 전송하는 방법은 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계; 상기 선택된 인덱스 및 나머지 인덱스를 기초로 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계; 상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 상기 정보 벡터를 프리코딩하는 단계; 및 상기 복수의 전송 안테나들을 이용하여 상기 프리코딩된 정보 벡터를 빔포밍하는 단계를 포함할 수 있다.

[0005] 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계는 상기 복수의

수신 안테나들의 개수를 고려하여 한 타임 슬롯에서 전송할 비트 개수를 결정하는 단계; 및 상기 비트 개수를 고려하여, 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화시키는 정보 벡터를 결정하는 단계를 더 포함할 수 있다.

[0006] 상기 정보 벡터를 결정하는 단계는 상기 시크릿 정보의 길이가 상기 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우, 상기 시크릿 정보 중 상기 공배수에 해당하지 않는 나머지 정보에 아래의 수학식을 만족하는 개수에 해당하는 임의의 비트를 추가하는 단계; 및 상기 임의의 비트가 추가된 나머지 정보에 대한 정보 벡터를 결정하는 단계를 더 포함할 수 있다.

[0007] [수학식]

[0008] 임의의 비트 개수= (하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수))

[0009] (여기서, %는 나머지(modular) 연산자를 의미함.)

[0010] 상기 정보 벡터를 프리코딩하는 단계는 상기 복수의 수신 안테나들 중 상기 선택된 인덱스에 대응하는 수신 안테나에서의 수신 에너지가 높아지도록 상기 정보 벡터를 프리코딩하는 단계를 포함할 수 있다.

[0011] 상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 상기 시크릿 정보에 대한 채널 코딩을 수행할 것인지 여부를 결정하는 단계; 및 상기 채널 코딩을 수행할 것인지 여부를 나타내는 지시자(indicator)를 이용하여 상기 시크릿 정보에 대한 채널 코딩 여부를 표시하는 단계를 더 포함할 수 있다.

[0012] 상기 시크릿 정보를 상기 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑하는 단계는 상기 정보 벡터에 포함되는 복수의 정보 심볼들 중에서 상기 선택된 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제1 값으로 설정하고, 상기 나머지 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제2 값으로 설정하는 단계를 포함할 수 있다.

[0013] 상기 복수의 전송 안테나들을 이용하여 해시 함수의 결과값 또는 상기 시크릿 정보에 대한 채널 코딩의 패리티 비트 중 어느 하나를 상기 복수의 수신 안테나들에게 전송하는 단계를 더 포함할 수 있다.

[0014] 암호화를 위한 시크릿 정보(secret information)를 생성하는 단계를 더 포함할 수 있다.

[0015] 둘 이상의 정보 벡터들이 존재하는 경우, 둘 이상의 서브 캐리어들을 이용하여 상기 정보 벡터들을 다중화하는 단계를 더 포함할 수 있다.

[0016] 상기 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계는 상기 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택하는 단계이고, 둘 이상의 정보 벡터들이 존재하는 경우, 둘 이상의 서브 캐리어들을 이용하여 상기 정보 벡터들을 다중화하는 단계를 더 포함할 수 있다.

[0017] 일 실시예에 따르면, 복수의 안테나들을 이용한 MIMO 다중화(Multiplexing)에 기반하여 수신단에서 시크릿 정보를 수신하는 방법은 복수의 수신 안테나들 각각에서 수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신 안테나를 선택하는 단계; 상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스에 기초하여 전송단에 의해 전송된 정보 벡터를 검출하는 단계; 상기 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스 및 나머지 인덱스를 기초로 상기 검출된 정보 벡터를 시크릿 정보로 디매핑하는 단계; 및 복수의 시크릿 정보를 결합하는 단계를 포함할 수 있다.

[0018] 상기 적어도 하나의 수신 안테나를 선택하는 단계는 복수의 수신 안테나들 중 미리 설정된 임계값보다 높은 신호의 세기를 가지는 신호를 수신한 적어도 하나의 수신 안테나를 선택하는 단계를 포함할 수 있다.

[0019] 상기 검출된 정보 벡터를 시크릿 정보로 디매핑하는 단계는 상기 디맵핑된 시크릿 정보의 길이가 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우, 상기 시크릿 정보 중 마지막에 전송된 정보에서 아래의 수학식을 만족하는 개수에 해당하는 임의의 비트를 제거하는 단계를 포함할 수 있다.

[0020] [수학식]

[0021] 임의의 비트 수= (하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수)) (여기서, %는 나머지(modular) 연산자를 의미함.)

[0022] 상기 전송단에 의해 사용된 안테나 맵핑 룰(antenna mapping rule)을 결정하는 단계를 더 포함할 수 있다.

[0023] 상기 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 코딩된 비트 정보를 디코딩하는 단계를 더 포함할 수 있다.

[0024] 상기 디코딩하는 단계는 채널 코딩이 수행되었는지 여부를 나타내는 지시자를 이용하여 상기 비트 정보를 디코딩하는 단계를 포함할 수 있다.

[0025] 상기 획득한 시크릿 정보에 대하여 해시 함수를 적용하는 단계; 전송단으로부터 수신한 해시 함수의 결과값 및 상기 해시 함수를 적용한 결과가 동일한지 여부를 확인하는 단계; 및 상기 확인 결과를 기초로 상기 전송단에게 상기 시크릿 정보의 재전송을 요청하는 단계를 포함할 수 있다.

도면의 간단한 설명

[0026] 도 1은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송 및 수신하는 개념을 나타낸 도면이다.

도 2는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 복수의 안테나들 각각에 대응하는 인덱스를 부여하는 방법을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 각각 전송, 수신하는 전송단과 수신단의 구성도이다.

도 4는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 전송하는 방법을 나타낸 플로우차트이다.

도 5는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 수신단에서 시크릿 정보를 수신하는 방법을 나타낸 플로우차트이다.

도 6은 도 2의 방법에 따라 전송단에서 레이어 맵핑을 수행한 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

도 7은 일 실시예에 따라 시크릿 정보를 기초로 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스를 부여하는 방법을 설명하기 위한 도면이다.

도 8은 도 7의 방법에 따라 전송단에서 레이어 맵핑을 수행된 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

도 9는 일 실시예에 따라 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하기 위한 전송단 및 수신단의 구성도이다.

도 10은 도 9의 빔포밍(beamforming)에 따라 전송단에서 레이어 맵핑을 수행한 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

도 11은 다른 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 전송하는 방법을 나타낸 플로우차트이다.

도 12는 다른 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 수신단에서 시크릿 정보를 수신하는 방법을 나타낸 플로우차트이다.

도 13은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송하고, 수신하는 전송단 및 수신단의 블록도이다.

도 14는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 방법을 나타낸 플로우차트이다.

도 15는 일 실시예에 따라 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)된 시크릿 정보를 수신단에서 수신하는 방법을 나타낸 플로우차트이다.

도 16은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 기초로 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스를 부여하고, 시크릿 정보를 OFDM의 서브 캐리어

(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 방법을 나타낸 플로우차트이다.

도 17은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송하는 전송단의 블록도이다.

도 18은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 수신하는 수신단의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 이하, 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 본 발명이 일실시예들에 의해 제한되거나 한정되는 것은 아니다. 또한, 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다. 이하에서, '전송단'은 전송 노드 혹은 전송 장치와 동일한 의미로 이해될 수 있으며, '수신단'은 수신 노드 혹은 수신 장치와 동일한 의미로 이해될 수 있다.

[0028] 도 1은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송 및 수신하는 개념을 나타낸 도면이다.

[0029] 일 실시예에서는 MIMO(Multi-Input Multi-Output) 시스템에서 전송단과 수신단 사이의 채널 정보를 이용하여 전송단이 빔 포밍(beamforming)을 수행함으로써 수신단의 특정 안테나로 거의 모든 에너지가 집중되도록 할 수 있다.

[0030] 도 1을 참조하면, 상술한 MIMO 다중화(Multiplexing) 특성을 이용하여 시크릿 정보(secret information)를 전송 및 수신함으로써 전송단과 수신단 간에 안전한 통신이 가능함을 알 수 있다. 여기서, 시크릿 정보는 암호화를 위한 시크릿 키(secret key)일 수 있다.

[0031] 예를 들어, 앨리스(Alice)는 합법적인 전송단이고, 밥(Bob)은 합법적인 수신단이며, 이브(Eve)는 도청자라고 하자.

[0032] 합법적인 수신단인 밥(Bob)의 경우, 합법적인 전송단과 수신단 사이의 채널 정보($\mathbf{H}_{AB}$)를 알 수 있으며, MIMO 다중화(Multiplexing) 특성에 따라 특정 안테나(예를 들어, 첫번째)로 빔포밍(beamforming) 된 신호 $\mathbf{x}$, 즉 $\mathbf{H}_{AB}^{-1}$s를 수신할 수 있다. 따라서, 서로 다른 안테나를 통해 에너지가 수신되면, 밥(Bob)은 서로 다른 정보가 전송단인 앨리스(Alice)로부터 전송된 것으로 판단할 수 있다.

[0033] 이에 반해 도청자인 이브(Eve)의 경우, 여러 개의 안테나를 통해 에너지가 수신되기 때문에 $\mathbf{H}_{AE}$ 만을 파악할 수 있을 뿐, 합법적인 전송단과 수신단 사이의 채널 정보($\mathbf{H}_{AB}$)를 알 수 없다. 그러므로, 이브(Eve)는 합법적인 전송단과 수신단 사이의 채널 정보($\mathbf{H}_{AB}$)를 이용하여 프리코딩(precoding)된 신호(예를 들어, ($\mathbf{x} = \mathbf{H}_{AB}^{-1}$s)를 파악할 수 없다.

[0034] 결국, 이브(Eve)는 앨리스(Alice)와 밥(Bob) 사이에 어떤 정보를 주고 받는지 알 수가 없다. 뿐만 아니라, 도청자인 이브(Eve)는 합법적인 수신단인 밥(Bob)에게 에너지가 들어오는 안테나 번호에 따른 맵핑 룰(mapping rule)(예를 들어, 첫번째 안테나로 신호가 빔포밍된 경우, 수신된 신호를 [10]으로 정하자는 맵핑 룰)을 알고 있더라도 전송된 정보를 알아 낼 수 없다.

[0035] 일 실시예에서는 이러한 방식을 통해 이동 무선 네트워크, 무선 LAN, Ad-hoc 네트워크, M2M (기기간, 단말간 통신)을 포함한 모든 무선 네트워크에서 제3자에 의한 도청을 방지할 수 있다. 뿐만 아니라, 시크릿 정보가 공유되지 않은 Ad-Hoc 네트워크나 M2M 환경에서도 물리 계층(physical layer)에서 교환되는 정보를 보호하거나 제3자가 모르는 랜덤 정보(randomness information)를 공유함으로써 시크릿 정보를 송수신하거나 암호화 키를 공유할 수 있다.

[0036] 도 2는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 복수의 안테나들 각각에 대응하는 인덱스를 부여하는 방법을 설명하기 위한 도면이다.

[0037] 도 2를 참조하면, 일 실시예에 따른 전송단과 수신단은 복수의 안테나들 중 어느 안테나에 대하여 어떠한 인덱

스(즉, 비트)가 부여되었는가를 나타내는 안테나 맵핑 룰을 미리 정해서 서로 공유할 수 있다.

[0038] 이에 따라, 전송단의 4개의 안테나들(201,203,205 및 207)은 전송하고자 하는 비트가 '00'이면 첫 번째 안테나(231)로, '01'이면 두 번째 안테나(233)로, '10'이면 세 번째 안테나(235)로, '11'이면 네 번째 안테나(237)로 전송 빔포밍(transmission beamforming)을 수행할 수 있다.

[0039] 수신단에서는 도 2에서 보여 준 바와 같이 첫 번째 안테나(231)로 가장 많은 에너지가 수신되면 전송단이 비트 '00'을, 두 번째 안테나(233)로 가장 많은 에너지가 수신되면 전송단이 비트 '01'을 전송한 것으로 판단할 수 있다. 또한, 수신단에서는 세 번째 안테나(235)로 가장 많은 에너지가 수신되면 전송단이 비트 '10'을, 네 번째 안테나(237)로 가장 많은 에너지가 수신되면 전송단이 비트 '11'을 전송한 것으로 판단할 수 있다.

[0040] 도 3은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 각각 전송, 수신하는 전송단과 수신단의 구성도이다.

[0041] 도 3을 참조하면, 전송단(310)은 시크릿 정보(Secret information) 생성 블록(311), 레이어 맵핑(Layer mapping) 블록(313) 및 프리코딩 및 안테나 맵핑(Precoding/antenna mapping) 블록(315)을 포함하고, 수신단(330)은 검출 및 안테나 디맵핑(Detection/antenna demapping) 블록(331), 레이어 디맵핑(Layer demapping) 블록(333) 및 시크릿 정보(Secret information) 획득 블록(335)을 포함할 수 있다.

[0042] 전송단(310)과 수신단(330) 간에 시크릿 정보를 공유하기 위해 먼저, 전송단(310)에서는 시크릿 정보 생성 블록(311)을 통해 암호화를 위한 시크릿 정보(secret information)를 생성할 수 있다.

[0043] 이후, 전송단(310)은 수신 안테나의 수를 고려하여, 생성한 시크릿 정보를 한 타임 슬롯(time slot)에서 전송할 수 있는 비트들의 개수를 결정할 수 있다. 이때, 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터(information vector ($\mathbf{s}$)) 또한 한 타임 슬롯(time slot)에서 전송할 수 있는 비트 수를 고려하여 결정할 수 있다.

[0044] 예를 들어, 전송 안테나의 수가 4인 경우, 한 타임 슬롯(time slot)에서 전송할 수 있는 비트들의 개수에 따라 다음과 같이 정보 벡터가 결정될 수 있다.

[0045] 00→$\mathbf{s}$=[1 0 0 0], 01→$\mathbf{s}$= [0 1 0 0], 10→$\mathbf{s}$= [0 0 1 0], 11→$\mathbf{s}$= [0 0 0 1]

[0046] 이러한 과정은 '레이어 맵핑(layer mapping)'이라고 하며, 레이어 맵핑 블록(313)에서 수행될 수 있다. 레이어 맵핑(layer mapping) 과정에서 미리 공유된 안테나 맵핑 룰(mapping rule) 또한 적용될 수 있다.

[0047] 전송단(310)은 프리코딩 및 안테나 맵핑 블록(315)을 통해 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩하고, 프리코딩된 정보 벡터를 복수의 전송 안테나들 각각에 맵핑하여 빔포밍할 수 있다.

[0048] 수신단(330)은 검출 및 안테나 디맵핑 블록(331)을 통해 각 수신 안테나로 수신되는 신호들을 감지하고, 예를 들어, 가장 센 신호를 수신한 안테나를 선택하여 안테나 디맵핑 룰(antenna demapping rule)에 따라 전송된 비트(bit)를 검출할 수 있다. 수신단(330)은 레이어 디맵핑 블록(333)에 의해 검출된 정보 벡터로부터 한 타임 슬롯에 전송된 시크릿 정보를 파악할 수 있다.

[0049] 이후, 수신단(330)은 시크릿 정보 획득 블록(335)에서 연속적인 타임 슬롯(time slot)을 통해 들어오는 비트들을 결합하여 최종적인 시크릿 정보를 획득할 수 있다.

[0050] 도 4는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 전송하는 방법을 나타낸 플로우차트이다.

[0051] 도 4를 참조하면, 전송단은 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택할 수 있다(410). 이때, 복수의 전송 안테나들 각각에 대응하여 부여된 인덱스는 도 2를 참고할 수 있으며, 복수의 전송 안테나들 사이의 조합들 각각에 대응하여 부여된 인덱스는 후술하는 도 7을 참고할 수 있다.

[0052] 전송단은 410에서 선택된 인덱스 및 나머지 인덱스를 기초로 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑할 수 있다(420). 이때, 전송단은 복수의 수신 안테나들의 개수를 고려하여 한 타임

슬롯에서 전송할 비트 개수를 결정하고, 결정된 비트 개수를 고려하여 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화시키는 정보 벡터를 결정할 수 있다.

[0053] 만약, 시크릿 정보의 길이가 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우, 전송단은 시크릿 정보 중 공배수에 해당하지 않는 나머지 정보에 [하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수)]을 만족하는 개수에 해당하는 임의의 비트를 추가할 수 있다. 여기서, %는 나머지(modular) 연산자를 의미할 수 있다.

[0054] 이 후, 전송단은 임의의 비트가 추가된 나머지 정보에 대한 정보 벡터를 결정할 수 있다.

[0055] 전송단은 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩할 수 있다(430). 이때, 전송단은 복수의 수신 안테나들 중 선택된 인덱스에 대응하는 수신 안테나에서의 수신 에너지가 높아지도록 정보 벡터를 프리코딩할 수 있다.

[0056] 전송단은 복수의 전송 안테나들을 이용하여 프리코딩된 정보 벡터를 빔포밍할 수 있다(440). 전송단은 예를 들어, 정보 벡터에 포함되는 복수의 정보 심볼들 중에서 선택된 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제1 값(예를 들어, '1')으로 설정하고, 나머지 인덱스에 대응하는 전송 안테나에 매핑되는 정보 심볼을 제2 값('0')으로 설정할 수 있다.

[0057] 실시예에 따라, 전송단은 420의 과정에 앞서, 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 시크릿 정보에 대한 채널 코딩을 수행할 것인지 여부를 결정할 수 있다. 이때, 전송단은 채널 코딩을 수행할 것인지 여부를 나타내는 지시자(indicator)를 이용하여 시크릿 정보에 대한 채널 코딩 여부를 표시할 수 있다.

[0058] 도 5는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 수신단에서 시크릿 정보를 수신하는 방법을 나타낸 플로우차트이다.

[0059] 도 5를 참조하면, 수신단은 복수의 수신 안테나들 각각에서 수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신 안테나를 선택할 수 있다(510). 이때, 수신단은 복수의 수신 안테나들 중 미리 설정된 임계값보다 높은 신호의 세기를 가지는 신호(혹은 가장 센 신호)를 수신한 적어도 하나의 수신 안테나를 선택할 수 있다.

[0060] 수신단은 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스에 기초하여 전송단에 의해 전송된 정보 벡터를 검출할 수 있다(520).

[0061] 수신단은 510에서 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스 및 나머지 인덱스를 기초로 520에서 검출된 정보 벡터를 시크릿 정보로 디매핑할 수 있다(530). 이때, 시크릿 정보의 길이가 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우, 수신단은 디맵핑된 시크릿 정보 중 마지막에 전송된 비트 정보에서 [하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수)]을 만족하는 개수에 해당하는 임의의 비트를 제거할 수 있다.

[0062] 수신단은 연속적인 타임 슬롯(time slot)을 통해 들어오는 복수의 시크릿 정보들을 결합(540)하여 최종적인 스크릿 정보를 획득할 수 있다.

[0063] 이 밖에도, 수신단은 510에 앞서, 전송단에 의해 사용된 안테나 맵핑 룰(antenna mapping rule)을 결정할 수 있으며, 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 코딩된 비트 정보를 디코딩할 수도 있다. 이때, 수신단은 채널 코딩이 수행되었는지 여부를 나타내는 지시자를 이용하여 비트 정보를 디코딩할 수 있다. 여기서, '비트 정보'는 정보 벡터를 구성하는 하나의 원소로 이해될 수 있다.

[0064] 도 6은 도 2의 방법에 따라 전송단에서 레이어 맵핑을 수행한 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

[0065] 도 6을 참조하여, 전송단과 수신단 각각에 포함된 복수의 안테나들의 개수는 4개이고, 전송단이 수신단으로 전송하고자 하는 시크릿 정보가 '10 00 01 10 11 10 11 00'이라고 하자.

[0066] 이때, 시크릿 정보에 포함된 각 비트들은 도 3의 레이어 맵핑(layer mapping) 블록(313)을 통과하면 610과 같은

정보 벡터(information vector)의 형태로 매핑될 수 있다.

[0067] 따라서, 610에서와 같이 첫 번째 타임 슬롯(time slot)에서 전송되는 정보 벡터 s(0)=[0 0 1 0]이고, 마지막 타임 슬롯에서 전송되는 정보 벡터 s(7)=[1 0 0 0]일 수 있다.

[0068] 또한, 각 정보 벡터로 다중화된 시크릿 정보는 도 3의 프리코딩 및 안테나 맵핑(Precoding/Antenna mapping) 블록(315)을 통과하면, 아래의 [수학식 1]과 같은 형태로 변환될 수 있다.

수학식 1

[0069] $$\mathbf{X}_i(n) = \mathbf{H}(n)^{-1}\, \mathrm{S}(n), \text{ for the } n-th \text{ time slot}$$

[0070] 여기서, $\mathbf{X}_i(n) = [x_1(n) \quad x_2(n) \quad x_3(n) \quad x_4(n)]$ 이고, $x_i(n)$은 n번째 타임 슬롯에서 i 번째 안테나로 통해 전송되는 신호를 나타낸다. 또한, $\mathbf{H}(n)^{-1}$s(n)은 전송단과 수신단 사이의 채널 정보(H)를 이용하여 프리코딩(precoding)된 정보 벡터를 나타낸다.

[0071] 또한, 수신단은 도 3의 검출 및 안테나 디맵핑(Detection/Antenna demapping) 블록(331)을 통과한 신호로부터 630과 같이 각 안테나에 해당하는 비트를 얻을 수 있다. 이후, 수신단은 도 3의 레이어 디맵핑(Layer demapping) 블록(333)을 통해 각 안테나에 해당하는 비트 정보들을 전송단에서 전송한 시크릿 정보의 형태로 획득할 수 있다.

[0072] 도 7은 일 실시예에 따라 시크릿 정보를 기초로 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스를 부여하는 방법을 설명하기 위한 도면이다.

[0073] 도 7을 참조하면, 일 실시예에 따른 전송단과 수신단은 복수의 안테나들 사이의 조합들 각각에 대응하여 어느 안테나 조합에 대하여 어떠한 인덱스(비트)가 부여되었는가를 나타내는 안테나 맵핑 룰을 미리 정해서 서로 공유할 수 있다.

[0074] 이에 따라, 전송단의 4개의 안테나들(701,703,705 및 707)은 전송하고자 하는 비트가 '000'이면 첫 번째 안테나(731)로, '001'이면 두 번째 안테나(733)로, '010'이면 세 번째 안테나(735)로, '011'이면 네 번째 안테나(737)로 전송 빔포밍(transmission beamforming)을 수행할 수 있다. 또한, 전송하고자 하는 비트가 '100'이면 첫 번째 안테나(731)와 두 번째 안테나(733)로, '101'이면 두 번째 안테나(733)와 세 번째 안테나(735)로, '110'이면 세 번째 안테나(735)와 네 번째 안테나(737)로, '111'이면 네 번째 안테나(737)와 첫 번째 안테나(731)로 전송 빔포밍을 수행할 수 있다.

[0075] 수신단에서는 나머지 안테나들에서 수신되는 에너지 양이 일정한 임계(threshold)값을 넘지 못하는 상태에서 첫 번째 안테나(731)로 가장 많은 에너지가 수신되면 전송단에서 비트 '000'을, 두 번째 안테나(733)로 가장 많은 에너지가 수신되면 전송단에서 비트 '001'을 전송한 것으로 판단할 수 있다. 그리고, 수신단에서는 세 번째 안테나(735)로 가장 많은 에너지가 수신되면 전송단에서 비트 '010'을, 네 번째 안테나(737)로 가장 많은 에너지가 수신되면 전송단에서 비트 '011'을 전송한 것으로 판단할 수 있다.

[0076] 또한, 수신단에서는 첫 번째 안테나(731)와 두 번째 안테나(733)로 임계값보다 큰 에너지가 들어오면 비트 '100'을, 두 번째 안테나(733)와 세 번째 안테나(735)로 임계값보다 큰 에너지가 수신되면 비트 '101'을, 세 번째 안테나(735)와 네 번째 안테나(737)로 임계값보다 큰 에너지가 들어오면 비트 '110'을 네 번째 안테나(737)와 첫 번째 안테나(731)로 임계값보다 큰 에너지가 수신되면 비트 '111'을 전송단에서 전송한 것으로 판단할 수 있다.

[0077] 이 밖에도, 수신단은 각 수신 안테나로 수신되는 신호 세기를 비교하여 임계값보다 큰 신호를 수신한 안테나들을 선택하고, 안테나 디맵핑 룰에 따라 각 수신 안테나를 통해 수신된 정보 비트를 결정할 수 있다. 이후, 레이어 디맵핑(Layer demapping)을 통해 획득한 시크릿 정보를 연속적인 타임 슬롯에 따라 결합하여 최종적인 시

크릿 정보를 획득할 수 있다.

[0078] 도 8은 도 7의 방법에 따라 전송단에서 레이어 맵핑을 수행된 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

[0079] 도 8을 참조하여, 전송단과 수신단 각각에 포함된 안테나들의 개수는 4개이고, 전송단이 수신단으로 전송하고자 하는 시크릿 정보가 ''100 001 101 110 110 0'이라고 하자.

[0080] 이때, 시크릿 정보에 포함된 각 비트들은 도 3의 레이어 맵핑(layer mapping) 블록(313)을 통과 하면, 810과 같은 정보 벡터(information vector)의 형태로 매핑될 수 있다.

[0081] 따라서, 도 8과 같이 첫 번째 타임 슬롯(time slot)에서 전송되는 정보 벡터 $\mathbf{s}(0)=[1\ 1\ 0\ 0]$이고, 다섯 번째 타임 슬롯에서 전송되는 정보 벡터 $\mathbf{s}(4)=[0\ 0\ 1\ 1]$일 수 있다.

[0082] 이때, 시크릿 정보의 길이가 한 타임 슬롯에서 전송되는 비트 개수(예를 들어, 3개)의 공배수가 아닌 경우, [하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수)]만큼의 임의의 비트를 추가하여 시크릿 정보를 전송할 수 있다. 여기서, %는 나머지(modular) 연산자를 의미할 수 있다.

[0083] 즉, 시크릿 정보의 길이가 16 비트인 경우, 해당 시크릿 정보의 개수는 한 타임 슬롯에서 전송되는 비트 개수인 3개의 공배수가 되지 않는다. 따라서, 전송단은 [3- (16%3)] = [3-1]= 2 개의 임의의 비트를 시크릿 정보에 포함시켜 전송할 수 있다. 이에 따라, 전송단이 전송하는 시크릿 정보는 ''100 001 101 110 110 0(00)'일 수 있고, 000으로 인덱스된 안테나는 첫 번째 안테나이므로 전송단은 정보 벡터 $\mathbf{s}(5)=[1\ 0\ 0\ 0]$을 전송할 수 있다.

[0084] 즉, 810에서 시크릿 정보 중 공배수에 해당하지 않는 마지막 정보(0)에 위의 수학식을 만족하는 개수(2개)의 임의의 비트(00)을 추가하여 전송할 수 있다.

[0085] 도 6에서와 마찬가지로, 각 정보 벡터로 다중화된 시크릿 정보는 도 3의 프리코딩 및 안테나 맵핑(Precoding/Antenna mapping) 블록(315)을 통과하면, 전술한 [수학식 1]과 같은 형태로 변환될 수 있다.

[0086] 또한, 수신단에서 도 3의 검출 및 안테나 디맵핑(Detection/Antenna demapping) 블록(331)을 통과하면 830과 같이 각 안테나에 해당하는 비트를 얻을 수 있다. 다만, 시크릿 정보의 길이가 한 타임 슬롯에서 전송할 비트 개수의 공배수가 아닌 경우, 디맵핑된 시크릿 정보 중 마지막 타임 슬롯에 전송된 시크릿 정보에서 (하나의 타임 슬롯에 전송되는 비트의 수 - (시크릿 정보들의 총 길이)%(하나의 타임 슬롯에 전송되는 비트의 수))을 만족하는 개수(예를 들어, 2개)에 해당하는 임의의 비트를 제거(혹은 무시)할 수 있다. 따라서, 수신단에서 마지막 타임 슬롯에 수신된 신호는 0xx가 될 수 있다.

[0087] 이후, 수신단은 도 3의 레이어 디맵핑(Layer demapping) 블록(333)을 통해 각 안테나에 해당하는 비트 정보들을 전송단에서 전송한 시크릿 정보의 형태로 획득할 수 있다.

[0088] 이 밖에도, 일 실시예에서는 새로운 시크릿 정보를 교환하는 경우도 물리 계층에서 교환되는 정보를 보호하거나, 제3자가 모르는 랜덤 정보(randomness information)을 공유함으로써 시크릿 정보를 송수신하거나 암호화 키를 공유할 수 있다. 이러한 암호키는 상위 계층의 안전한 통신을 보완하는 역할로 채널 자체를 보호할 수 있으며, 이는 패킷 헤더(packet header) 및 통신 내용 자체를 보호하여 원하지 않는 정보가 제 3자에게 노출되는 것을 방지할 수 있다.

[0089] 도 9는 일 실시예에 따라 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하기 위한 전송단 및 수신단의 구성도이다.

[0090] 도 9를 참조하면, 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 경우에도 도 2와 마찬가지로 방식으로 각 안테나로 전송 빔포밍(transmission beamforming)을 수행하고, 수신단은 가장 많은 에너지가 수신된 안테나에 대응하는 인덱스에 기초하여 시크릿 정보를 파악할 수 있다.

[0091] 다만, 이때에는 정보 벡터들을 둘 이상의 서브 캐리어들을 이용하여 다중화한다는 점에 차이가 있을 뿐이다.

[0092] 즉, 도 2에서는 $00\rightarrow\mathbf{s}=[1\ 0\ 0\ 0]$, $01\rightarrow\mathbf{s}=[0\ 1\ 0\ 0]$, $10\rightarrow\mathbf{s}=[0\ 0\ 1\ 0]$, $11\rightarrow\mathbf{s}=[0\ 0\ 0\ 1]$와 같이 각 정보 벡

터들이 서브 캐리어의 구분없이, 하나의 서브 캐리어, 즉 동일한 주파수 자원에 할당될 수 있다.

[0093] 반면에, 도 9에서는 00→**s**(*n*)=[1 0 0 0], 01→**s**(*n*)= [0 1 0 0], 10→**s**(*n*)= [0 0 1 0], 11→**s**(*n*)= [0 0 0 1] (여기서, *n=1, 2, ..., N-1*이고 *N*은 사용되는 서브 캐리어(subcarrier)의 개수임)와 같이 각 정보 벡터들이 서로 다른 서브 캐리어들에 할당된다는 차이점을 가진다.

[0094] 전송단(910)은 시크릿 정보(Secret information) 생성 블록(911), 레이어 맵핑(Layer mapping) 블록(913) 및 프리코딩 및 안테나 맵핑(Precoding/antenna mapping) 블록(915) 및 리소스 맵핑(resource mapping) 블록(917)을 포함하고, 수신단(330)은 리소스 디맵핑(resource) 블록(931), 검출 및 안테나 디맵핑(Detection/antenna demapping) 블록(933), 레이어 디맵핑(Layer demapping) 블록(935) 및 시크릿 정보(Secret information) 획득 블록(937)을 포함할 수 있다.

[0095] 여기서, 리소스 맵핑(resource mapping) 블록(917) 및 리소스 디맵핑(resource) 블록(931)을 제외한 나머지 블록들의 동작은 도 3의 해당 블록들의 동작과 동일하므로 도 3의 설명을 참고하기로 한다.

[0096] 전송단(910)에서 각 정보 벡터들은 리소스 맵핑(Resource Mapping) 블록(917)을 통해 서로 다른 서브 캐리어들에 할당될 수 있다.

[0097] 수신단(930)에서는 각 서브 캐리어마다 각 안테나로 수신되는 신호 세기를 비교하여 가장 센 신호를 수신한 안테나를 선택하고, 안테나 디맵핑 룰(bit demapping rule)에 따라 전송된 비트(bit)를 검출할 수 있다.

[0098] 이후, 수신단(930)은 리소스 디맵핑(Resource Demapping) 블록(931)을 통해 각 서브 캐리어들마다에 할당된 비트들(정보 벡터)을 검출하고, 검출된 비트들에 대하여 레이어 디맵핑(layer demapping)을 수행함으로써 스크릿 정보를 생성할 수 있다.

[0099] 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 경우에도 마찬가지로 전송단과 수신단은 채널 품질(Channel Quality)이 떨어지는 경우, 채널 코딩(channel coding)을 적용하여 에러율(error rate)을 낮추거나, 해시(Hash) 함수 또는 패리티 비트(parity bit)의 전송 등을 통해 시크릿 정보가 에러 없이 제대로 전송되었는지 여부를 체크할 수 있다.

[0100] 도 10은 도 9의 빔포밍(beamforming)에 따라 전송단에서 레이어 맵핑을 수행한 결과 및 수신단에서 안테나 디맵핑을 수행한 결과를 나타낸 도면이다.

[0101] 도 10을 참조하면, 전송단과 수신단 각각에 포함된 안테나들의 개수는 4개이고, 전송단이 수신단으로 전송하고자 하는 시크릿 정보가 '10 00 01 10 11 10 11 00'이라고 하자.

[0102] 이때, 시크릿 정보에 포함된 각 비트들은 도 9의 레이어 맵핑(layer mapping) 블록(913)을 통과하면 1010과 같은 정보 벡터(information vector)의 형태로 매핑될 수 있다.

[0103] 따라서, 도 10과 같이 첫 번째 서브 캐리어(subcarrier)에서 전송되는 정보 벡터 s(0)=[0 0 1 0]이고, 마지막 서브 캐리어에서 전송되는 정보 벡터 s(7)=[1 0 0 0]일 수 있다.

[0104] 각 정보 벡터로 다중화된 시크릿 정보는 도 9의 프리코딩 및 안테나 맵핑(Precoding/Antenna mapping) 블록(915)을 통과하면, [수학식 2]과 같은 형태로 변환될 수 있다.

수학식 2

[0105] $$\mathbf{X}_i(n) = \mathbf{H}(n)^{-1}\,\mathrm{S}(n), \text{ for the } n\text{-}th \text{ subcarrier}$$

[0106] 이때, $\mathbf{X}_i(n) = [x_1(n) \quad x_2(n) \quad x_3(n) \quad x_4(n)]$ 이고, $x_i(n)$은 n번째 서브 캐리어(subcarrier)에서 i번째 안테나로 통해 전송되는 신호를 나타낸다는 점에서 차이가 있다.

[0107] 수신단에서는 도 9의 검출 및 안테나 디맵핑(Detection/Antenna demapping) 블록(933)을 통과하면 1030과 같이

각 서브 캐리어마다 각 안테나에 해당하는 정보 비트를 얻을 수 있다. 각 서브 캐리어에서 수신된 정보 비트들을 하나의 시퀀스(sequence)로 모으는 도 9의 레이어 디맵핑(Layer demapping) 블록(935)을 통과 하면 전송단에서 전송한 시크릿 정보를 수신단이 획득하게 된다.

[0108] 도 11은 다른 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 전송하는 방법을 나타낸 플로우차트이다.

[0109] 전송단은 암호화를 위한 시크릿 정보(secret information)를 생성하고(1110), 생성한 시크릿 정보에 대해 채널 코딩을 수행할 수 있다(1120). 이때, 전송단은 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 채널 코딩을 수행할 것인지 여부를 결정할 수 있다. 만약, 채널 상태(채널 품질(channel quality))가 우수한 경우, 전송단은 채널 코딩을 사용하지 않고 시크릿 정보를 전송할 수 있다. 이러한 경우, 전송단의 채널 코딩 과정과 이에 대응되는 수신단의 채널 디코딩 절차는 필요하지 않다. 하지만, 채널 품질(Channel Quality)이 떨어지는 경우, 전송단은 채널 코딩(channel coding)을 적용하여 에러율(error rate)을 낮추거나, 해시(Hash) 함수 또는 패리티 비트(parity bit)의 전송 등을 통해 시크릿 정보가 에러없이 제대로 전송되었는지 여부를 체크할 수 있다.

[0110] 전송단은 수신단으로부터 수신한 안테나 맵핑 룰을 이용하여 레이어 맵핑을 수행하여 정보 벡터를 생성할 수 있다(1130).

[0111] 이후, 전송단은 전송단 및 수신단 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩(precoding) 및 안테나 맵핑(1140)한 후, 복수의 전송 안테나들을 이용하여 프리코딩된 정보 벡터를 수신단으로 빔포밍할 수 있다(1150). 이때, 안테나 맵핑 룰은 전송단에서 결정하여 수신단으로 알려 줄 수도 있다.

[0112] 도 12는 다른 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 수신단에서 시크릿 정보를 수신하는 방법을 나타낸 플로우차트이다.

[0113] 수신단은 안테나 맵핑 룰을 결정하고, 전송단으로 결정된 안테나 맵핑 룰을 전송할 수 있다(1210). 이때, 안테나 맵핑 룰은 수신단이 직접 결정하거나, 전송단으로부터 수신할 수 있다.

[0114] 수신단은 전송단으로부터 수신한 신호를 검출(detection)한 후, 서로 공유된 안테나 맵핑 룰을 이용하여 안테나 디맵핑(antenna demapping)을 수행할 수 있다(1220). 수신단은 레이어 디맵핑(layer demapping)을 수행(1230)한 후, 채널 디코딩(channel decoding)(1240)을 통해 시크릿 정보를 획득할 수 있다.

[0115] 도 13은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송하고, 수신하는 전송단(1310) 및 수신단(1350)의 블록도이다.

[0116] 도 13을 참조하면, 전송단(1310)은 A/D(Analogue to Digital) 변환기(1311), 안테나 맵핑룰 수신부(1313), 시크릿 정보 생성부(1315), 채널 품질 판단부(1317), 채널 코더(channel coder)(1319), 레이어 맵핑부(1321), 프리코딩 및 안테나 맵핑부(1323) 및 D/A(Digital to Analogue) 변환기(1325)를 포함할 수 있다.

[0117] 채널 품질 판단부(1317)는 A/D(Analogue to Digital) 변환기(1311)를 거쳐 변환된 디지털 신호로부터 전송단과 수신단 간의 채널 품질을 판단하고, 그 판단 결과에 따라 채널 코더(1319)의 사용 여부를 결정한다.

[0118] 따라서, 채널 품질이 좋은 경우, 시크릿 정보 생성부(1315)에서 생성된 시크릿 정보는 채널 코딩하지 않고, 바로 레이어 맵핑부(1321)로 전달될 수 있다. 하지만, 채널 품질이 나쁜 경우, 시크릿 정보 생성부(1315)에서 생성된 시크릿 정보는 채널 코더(1319)를 거쳐 채널 코딩된 후, 레이어 맵핑부(1321)로 전달될 수 있다.

[0119] 레이어 맵핑부(1321)는 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑시킨다. 이때, 레이어 맵핑부(1321)는 시크릿 정보를 정보 벡터로 매핑 시에 안테나 맵핑룰 수신부(1313)로부터 수신한 안테나 맵핑룰을 적용할 수 있다. 이후, 프리코딩 및 안테나 맵핑부(1323)는 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩하고, 프리코딩된 정보 벡터를 복수의 전송 안테나들에 맵핑해 빔포밍할 수 있다. 이때, 빔포밍되는 신호는 D/A(Digital to Analogue) 변환기(1325)를 거쳐 아날로그 신호로 빔포밍될 수 있다.

[0120] 전송단(1310) 및 수신단(1350) 각각에서 동일 또는 유사한 채널 정보의 획득이 가능한 경우, 전송단 및 수신단 각각이 채널 품질을 판단할 수도 있다.

[0121] 또한, 시크릿 정보 전송 시에 채널 코더(1319)의 사용 여부는 수신단 혹은 전송단이 직접 결정하거나, 채널 코딩을 수행할 것인지 여부를 나타내는 지시자(indicator)를 이용하여 알려줄 수도 있다.

[0122] 또한, 도 13을 참조하면, 수신단(1350)은 A/D(Analogue to Digital) 변환기(1351), 채널 품질 판단부(1353), 신호 검출 및 안테나 디맵핑부(1355), 안테나 맵핑룰 결정부(1357), 레이어 디맵핑부(1359), 안테나 맵핑룰 전송부(1361), 채널 디코더(1363), 시크릿 정보 획득부(1365) 및 D/A(Digital to Analogue) 변환기(1367)를 포함할 수 있다.

[0123] 채널 품질 판단부(1353)는 A/D(Analogue to Digital) 변환기(1351)를 거쳐 수신된 디지털 신호로부터 전송단과 수신단 간의 채널 품질을 판단하고, 그 판단 결과에 따라 채널 디코더(1363)의 사용 여부를 결정한다.

[0124] 따라서, 채널 품질이 좋은 경우, 레이어 디맵핑부(1359)를 통해 디맵핑된 시크릿 정보는 채널 디코딩되지 않고, 바로 시크릿 정보 획득부(1365)로 전달될 수 있다. 하지만, 채널 품질이 나빠 전송 시에 채널 코딩된 시크릿 정보는 채널 디코더(1363)를 거쳐 채널 디코딩된 후, 시크릿 정보 획득부(1365)로 전달될 수 있다.

[0125] 또한, A/D(Analogue to Digital) 변환기(1351)를 거쳐 수신된 디지털 신호는 신호 검출 및 안테나 디맵핑부(1355)에서 수신 안테나에 대응하는 인덱스에 기초하여 정보 벡터로 검출되고, 레이어 디맵핑부(1359)를 거쳐 시크릿 정보로 디맵핑될 수 있다. 이때, 레이어 디맵핑부(1359)에서 이용되는 안테나 (디)맵핑 룰은 안테나 맵핑 룰 결정부(1357)에서 결정된 것이고, 안테나 (디)맵핑 룰은 안테나 맵핑룰 전송부(1361) 및 D/A(Digital to Analogue) 변환기(1367)를 거쳐 전송단으로 전달될 수 있다.

[0126] 또한, 도 13에서 표시되지는 않았지만, 전송단 및 수신단에서 가지고 있는 시크릿 정보가 정확한 것인지 여부를 확인하기 위하여 해시 함수를 이용할 경우, 전송단은 해시 함수를 생성하는 해시 코드 생성부(미도시)를 더 포함할 수 있으며, 수신단은 전송단에서 생성된 해시 함수의 결과값과 획득한 시크릿 정보에 전송단에서 생성된 해시 코드를 적용하여 얻은 해시 코드 값을 비교하는 해시 코드 비교부(미도시)를 더 포함할 수 있다.

[0127] 수신단은 획득한 시크릿 정보에 에러가 존재한다고 판단되면, 시크릿 정보의 재전송을 요청하거나 획득한 시크릿 정보를 보정할 수 있다.

[0128] 이 밖에도, 블록 에러 코딩을 위한 패리티 비트를 사용할 경우, 전송단 및 수신단은 이를 수행하기 위한 모듈을 더 포함할 수 있다.

[0129] 도 14는 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 방법을 나타낸 플로우차트이다.

[0130] 도 14를 참조하면, 전송단은 시크릿 정보를 생성하고(1410), 생성한 시크릿 정보에 대해 채널 코딩을 수행할 수 있다(1420).

[0131] 전송단은 수신단으로부터 받은 안테나 맵핑 룰을 이용하여 레이어 맵핑을 수행하여 정보 벡터를 생성할 수 있다(1430).

[0132] 전송단은 전송단과 수신단 간의 채널 정보를 바탕으로 프리코딩 및 안테나 맵핑을 수행(1440)한 후, 주파수 자원 맵핑을 통해 사용할 서브 캐리어로 프리코딩된 정보를 할당할 수 있다(1450).

[0133] 이후, 전송단은 서브 캐리어에 할당된 정보를 빔포밍할 수 있다(1460).

[0134] 전송단은 수신단이 획득한 시크릿 정보가 올바른 것인지 여부를 확인할 수 있도록 해시(Hash) 함수의 결과값 또한 수신단으로 전송할 수 있다(1470).

[0135] 이때, 전송단은 해시(Hash) 함수의 결과값을 대신하여 시크릿 정보에 대한 채널 코딩의 패리티 비트 중 어느 하나를 전송할 수도 있다.

[0136] 도 15는 일 실시예에 따라 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)된 시크릿 정보를 수신단에서 수신하는 방법을 나

타낸 플로우차트이다.

[0137] 도 15를 참조하면, 수신단은 안테나 맵핑 룰을 결정하여 전송할 수 있다(1510).

[0138] 수신단은 주파수 자원 디맵핑에 의해 각 서브 캐리어들마다에 할당된 비트들을 검출하고(1515), 신호 검출 및 안테나 디맵핑에 의해 각 서브 캐리어마다 각 안테나에 해당하는 정보 비트를 얻을 수 있다(1520).

[0139] 수신단은 레이어 디맵핑(Layer demapping)에 의해 각 서브 캐리어에서 수신된 정보 비트들을 하나의 시퀀스(sequence)로 모을 수 있다(1525).

[0140] 이후, 수신단은 채널 디코딩(1530)을 통해 시크릿 정보를 획득할 수 있다(1535).

[0141] 수신단은 획득한 시크릿 정보에 해시 함수를 적용하고(1540), 전송단에서 전송한 해시 함수의 결과값을 수신할 수 있다(1545).

[0142] 수신단은 1540에서 해시 함수를 적용한 시크릿 정보의 값과 1545에서 수신한 해시 함수의 결과값을 비교할 수 있다(1550).

[0143] 1550의 비교 결과, 두 값이 동일하다면 수신단은 시크릿 정보를 확정할 수 있다(1555). 하지만, 두 값이 상이하다면, 수신단은 전송단으로 시크릿 정보의 재전송을 요청하거나 또는 획득한 시크릿 정보에 대한 보정 작업을 수행할 수 있다(1560).

[0144] 도 16은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 전송단에서 시크릿 정보를 기초로 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스를 부여하고, 시크릿 정보를 OFDM의 서브 캐리어(subcarrier)마다 서로 다른 안테나로 빔포밍(beamforming)하는 방법을 나타낸 플로우차트이다.

[0145] 도 16을 참조하면, 전송단은 시크릿 정보를 기초로 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택할 수 있다(1610). 이때, 복수의 전송 안테나들 사이의 조합들 각각에 대응하여 부여된 인덱스는 후술하는 도 7을 참고할 수 있다.

[0146] 전송단은 1610에서 선택된 적어도 하나의 인덱스 및 나머지 인덱스를 기초로 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑할 수 있다(1620).

[0147] 전송단은 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩(1630)한 후, 연속적으로 프리코딩된 정보 벡터를 둘 이상의 서브 캐리어들을 이용하여 다중화할 수 있다(1640).

[0148] 전송단은 복수의 전송 안테나들을 이용하여 프리코딩된 정보 벡터를 빔포밍할 수 있다(1650). 이를 통해, 일 실시예에서는 긴 길이의 시크릿 정보를 하나의 OFDM 심볼로 전송할 수 있다.

[0149] 이에 대응하여 수신단에서는 수신한 신호를 주파수 자원 디맵핑하여 검출한 후, 전송단으로터 수신하거나, 수신단에서 생성한 안테나 맵핑 룰에 따라 안테나 디맵핑 및 레이어 디맵핑을 수행하여 시크릿 정보를 획득할 수 있다.

[0150] 도 17은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 전송하는 전송단의 블록도이다.

[0151] 도 17을 참조하면, 일 실시예에 따른 전송단(1700)은 선택부(1710), 매핑부(1730), 프리코딩부(1750) 및 빔포밍부(1770)를 포함할 수 있다.

[0152] 선택부(1710)는 시크릿 정보를 기초로 복수의 전송 안테나들 각각에 대응하는 인덱스 또는 복수의 전송 안테나들 사이의 조합들 각각에 대응하는 인덱스 중 적어도 하나를 선택할 수 있다.

[0153] 매핑부(1730)는 선택부(1710)에서 선택된 인덱스 및 나머지 인덱스를 기초로 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화되는 정보 벡터로 매핑할 수 있다. 이때, 매핑부(1730)는 복수의 수신 안테나들의 개수를 고려하여 한 타임 슬롯에서 전송할 비트 개수를 결정하고, 결정된 비트 개수를 고려하여 시크릿 정보를 복수의 전송 안테나들을 통하여 다중화시키는 정보 벡터를 결정할 수 있다.

[0154] 프리코딩부(1750)는 복수의 전송 안테나들과 복수의 수신 안테나들 간의 채널 정보를 바탕으로 정보 벡터를 프리코딩할 수 있다. 프리코딩부(1750)는 복수의 수신 안테나들 중 선택된 인덱스에 대응하는 수신 안테나에서의 수신 에너지가 높아지도록 정보 벡터를 프리코딩할 수 있다.

[0155] 빔포밍부(1770)는 복수의 전송 안테나들을 이용하여 프리코딩된 정보 벡터를 빔포밍할 수 있다.

[0156] 도 18은 일 실시예에 따른 복수의 안테나들을 이용한 MIMO 다중화에 기반하여 시크릿 정보를 수신하는 수신단의 블록도이다.

[0157] 도 18을 참조하면, 일 실시예에 따른 수신단(1800)은 선택부(1810), 검출부(1830), 디맵핑부(1850) 및 결합부(1870)를 포함할 수 있다.

[0158] 선택부(1810)는 복수의 수신 안테나들 각각에서 수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신 안테나를 선택할 수 있다.

[0159] 검출부(1830)는 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스에 기초하여 전송단에 의해 전송된 정보 벡터를 검출할 수 있다.

[0160] 디맵핑부(1850)는 선택부(1810)에서 선택된 적어도 하나의 수신 안테나에 대응하는 인덱스 및 나머지 인덱스를 기초로 검출부(1830)에서 검출된 정보 벡터를 시크릿 정보로 디매핑할 수 있다.

[0161] 결합부(1870)는 디맵핑된 복수의 시크릿 정보를 결합할 수 있다.

[0162] 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.

[0163] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0164] 310: 전송단

311: 시크릿 정보 생성 블록

313: 레이어 맵핑 블록

315: 프리코딩 및 안테나 맵핑 블록

330: 수신단

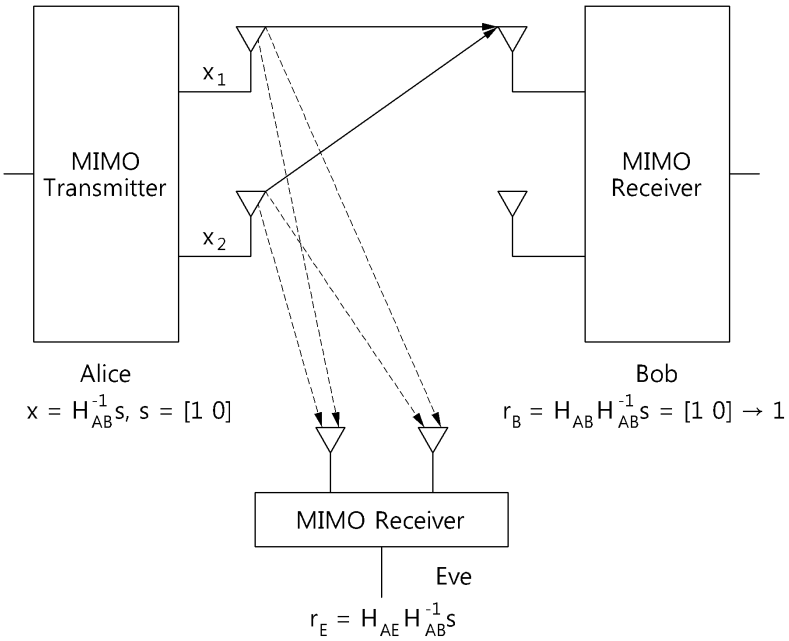
331: 검출 및 안테나 디맵핑 블록

333: 레이어 디맵핑 블록

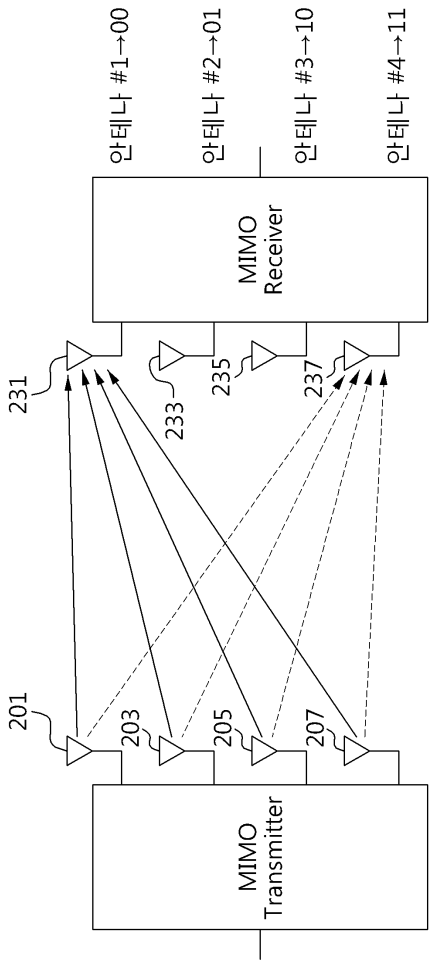
335: 시크릿 정보 획득 블록

도면

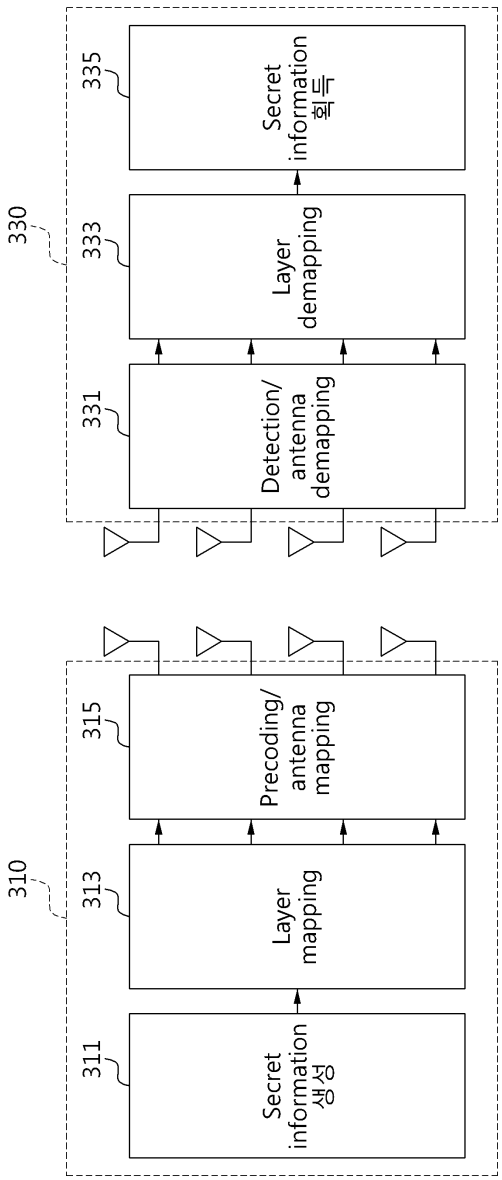
도면1


MIMO
Transmitter
x1
x2
MIMO
Receiver
Alice
x = H_AB^-1 s, s = [1 0]
Bob
r_B = H_AB H_AB^-1 s = [1 0] → 1
MIMO Receiver
Eve
r_E = H_AE H_AB^-1 s

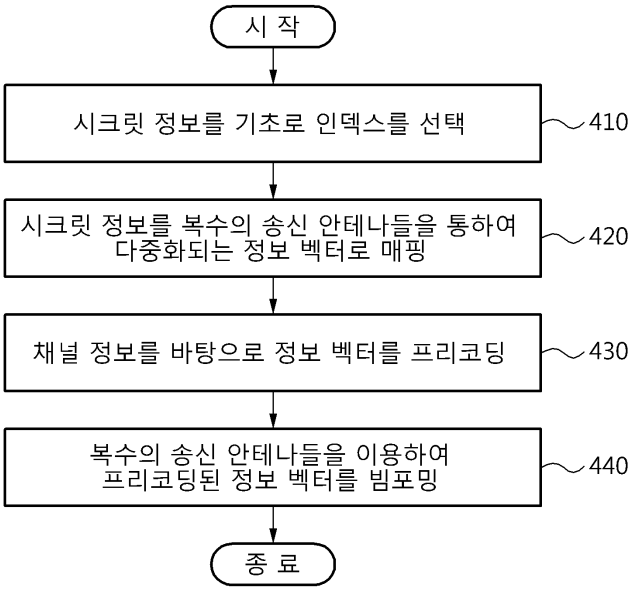
도면2


안테나 #1→00
안테나 #2→01
안테나 #3→10
안테나 #4→11
MIMO Receiver
231
233
235
237
201
203
205
207
MIMO Transmitter

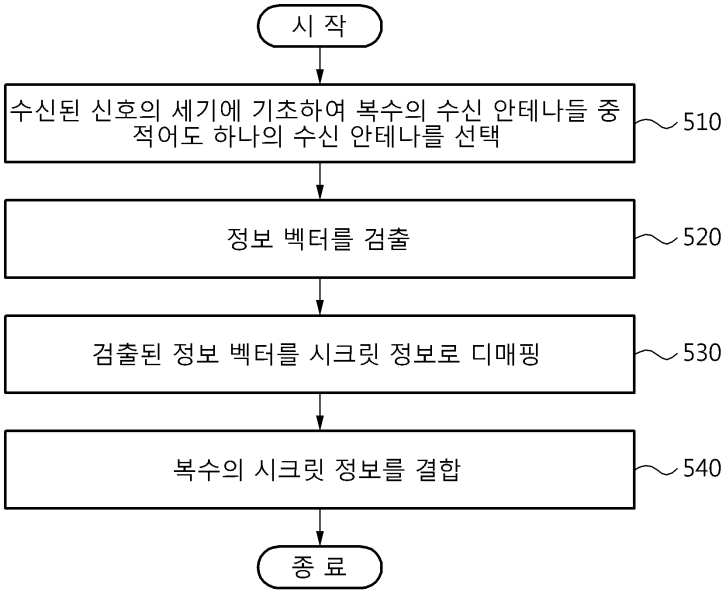
도면3


330
331
Detection/
antenna
demapping
333
Layer
demapping
335
Secret
information
획득
310
311
Secret
information
생성
313
Layer
mapping
315
Precoding/
antenna
mapping

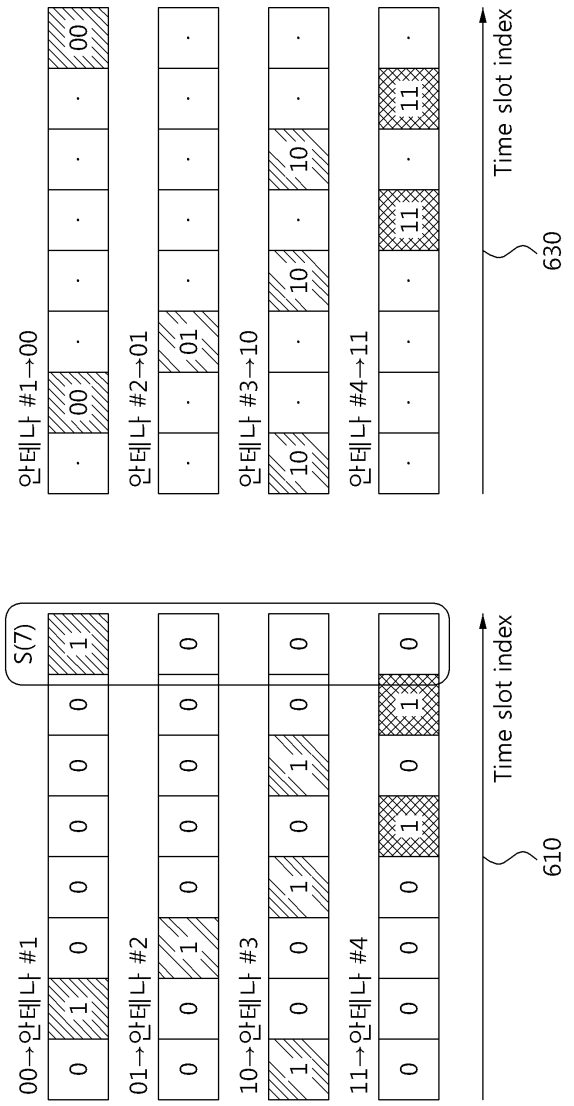
도면4


시 작
시크릿 정보를 기초로 인덱스를 선택
410
시크릿 정보를 복수의 송신 안테나들을 통하여 다중화되는 정보 벡터로 매핑
420
채널 정보를 바탕으로 정보 벡터를 프리코딩
430
복수의 송신 안테나들을 이용하여 프리코딩된 정보 벡터를 빔포밍
440
종 료

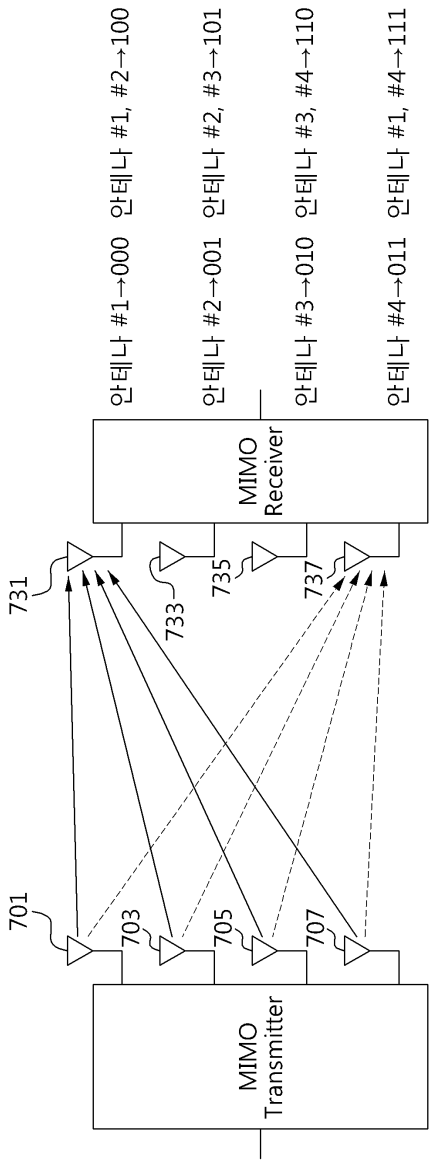
도면5


시 작
수신된 신호의 세기에 기초하여 복수의 수신 안테나들 중 적어도 하나의 수신 안테나를 선택
510
정보 벡터를 검출
520
검출된 정보 벡터를 시크릿 정보로 디매핑
530
복수의 시크릿 정보를 결합
540
종 료

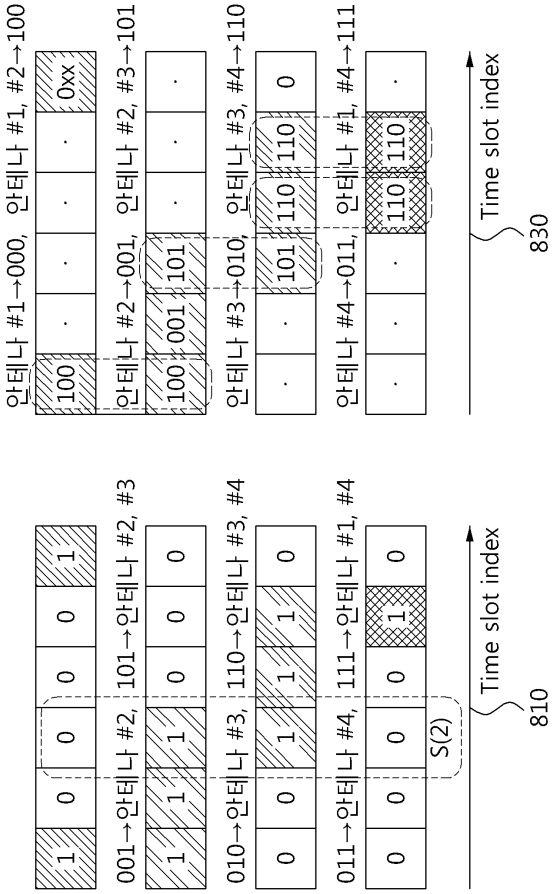
도면6


안테나 #1→00
안테나 #2→01
안테나 #3→10
안테나 #4→11
Time slot index
630
00→안테나 #1
01→안테나 #2
10→안테나 #3
11→안테나 #4
S(7)
Time slot index
610

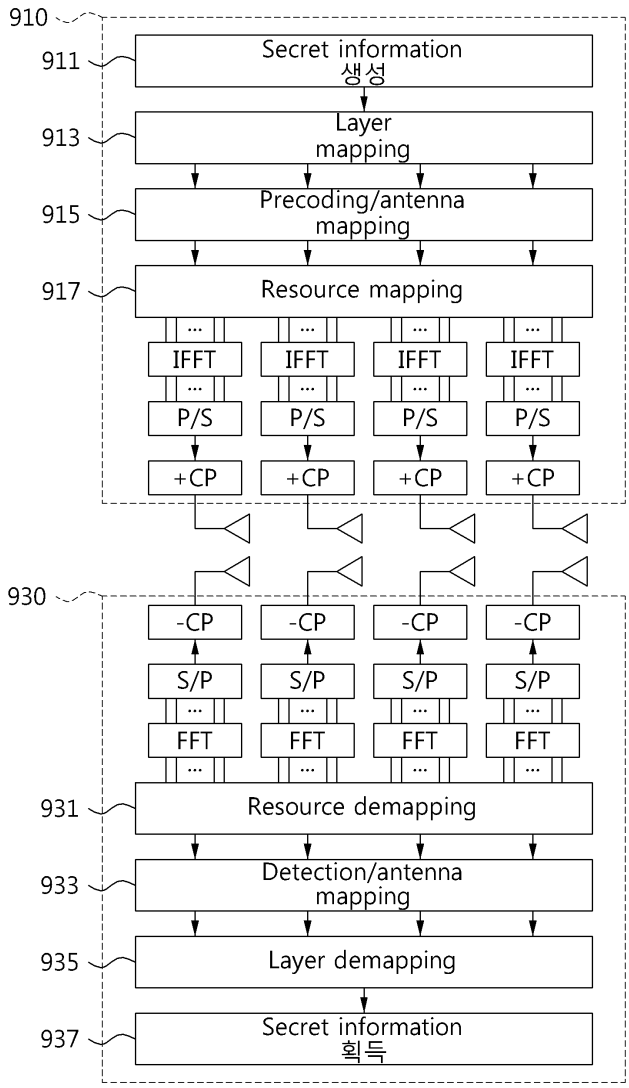
도면7


안테나 #1→000
안테나 #2→001
안테나 #3→010
안테나 #4→011
안테나 #1, #2→100
안테나 #2, #3→101
안테나 #3, #4→110
안테나 #1, #4→111
MIMO Receiver
MIMO Transmitter
731
733
735
737
701
703
705
707

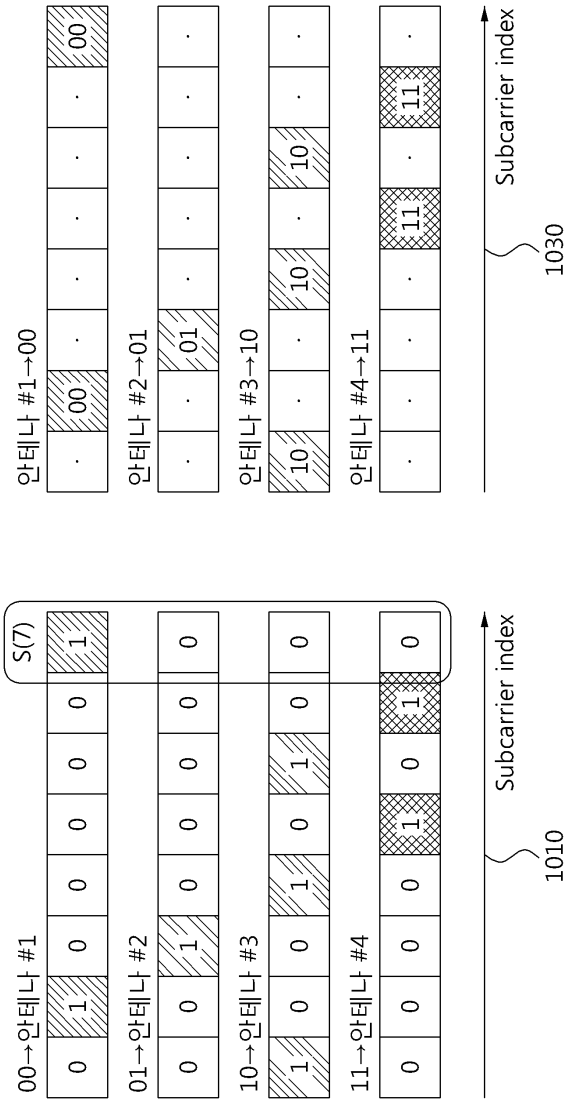
도면8


안테나 #1→000, 안테나 #1, #2→100
안테나 #2→001, 안테나 #2, #3→101
안테나 #3→010, 안테나 #3, #4→110
안테나 #4→011, 안테나 #1, #4→111
Time slot index
830
001→안테나 #2, 101→안테나 #2, #3
010→안테나 #3, 110→안테나 #3, #4
011→안테나 #4, 111→안테나 #1, #4
S(2)
Time slot index
810

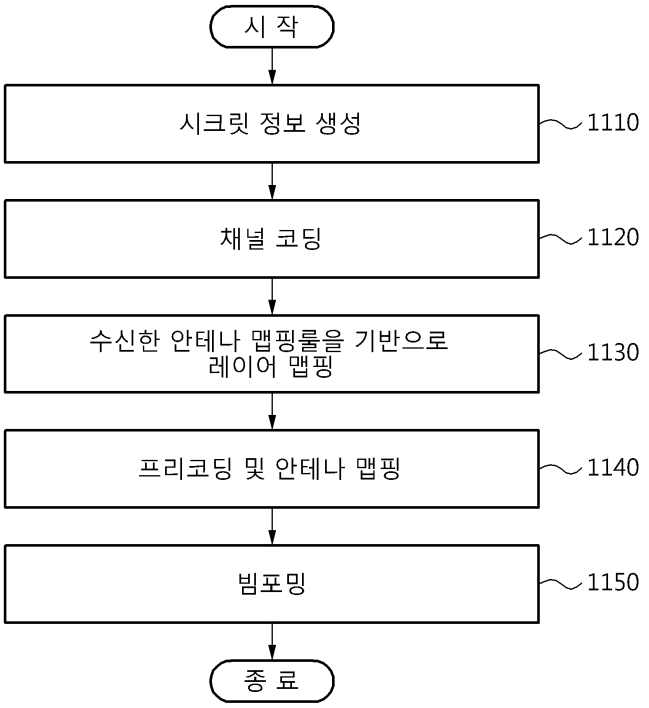
도면9


910
911
Secret information
생성
913
Layer
mapping
915
Precoding/antenna
mapping
917
Resource mapping
IFFT
P/S
+CP
930
-CP
S/P
FFT
931
Resource demapping
933
Detection/antenna
mapping
935
Layer demapping
937
Secret information
획득

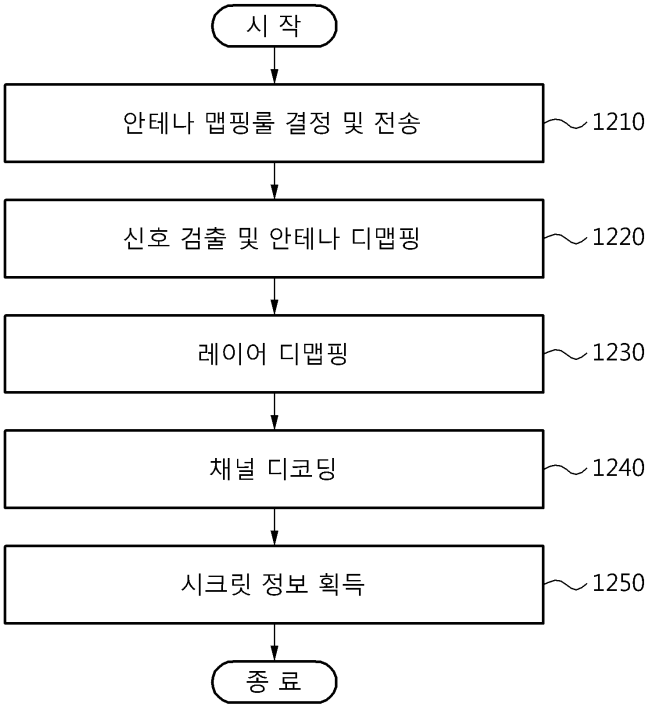
도면10


안테나 #1→00
안테나 #2→01
안테나 #3→10
안테나 #4→11
Subcarrier index
1030
00→안테나 #1
01→안테나 #2
10→안테나 #3
11→안테나 #4
S(7)
Subcarrier index
1010

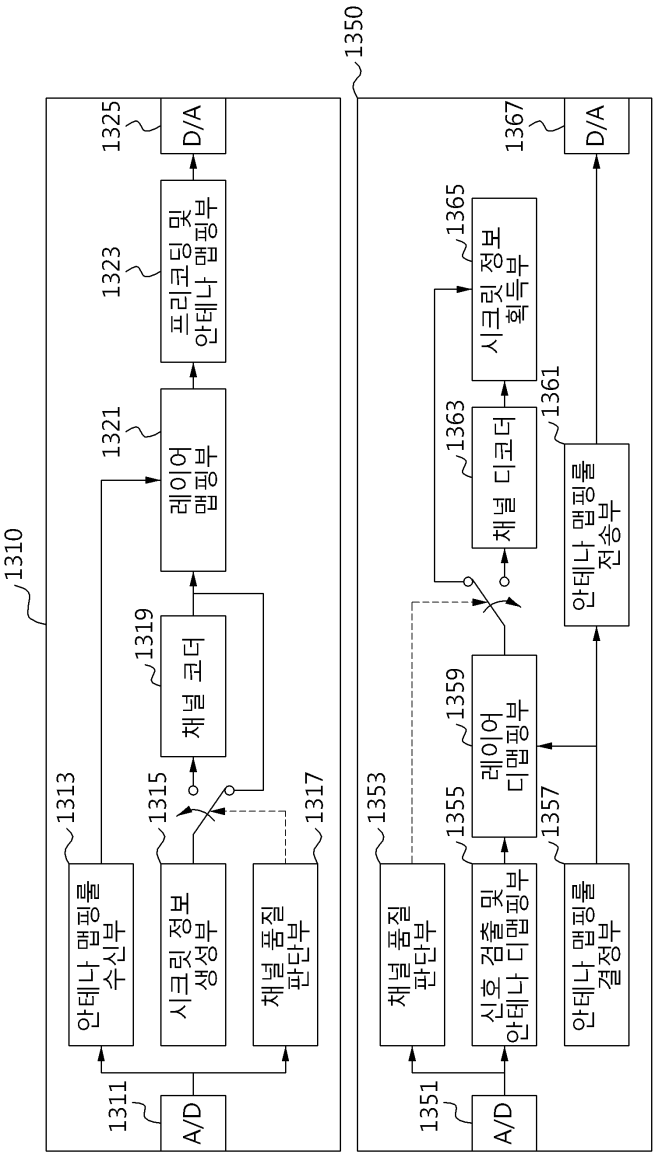
도면11


시 작
시크릿 정보 생성
1110
채널 코딩
1120
수신한 안테나 맵핑룰을 기반으로
레이어 맵핑
1130
프리코딩 및 안테나 맵핑
1140
빔포밍
1150
종 료

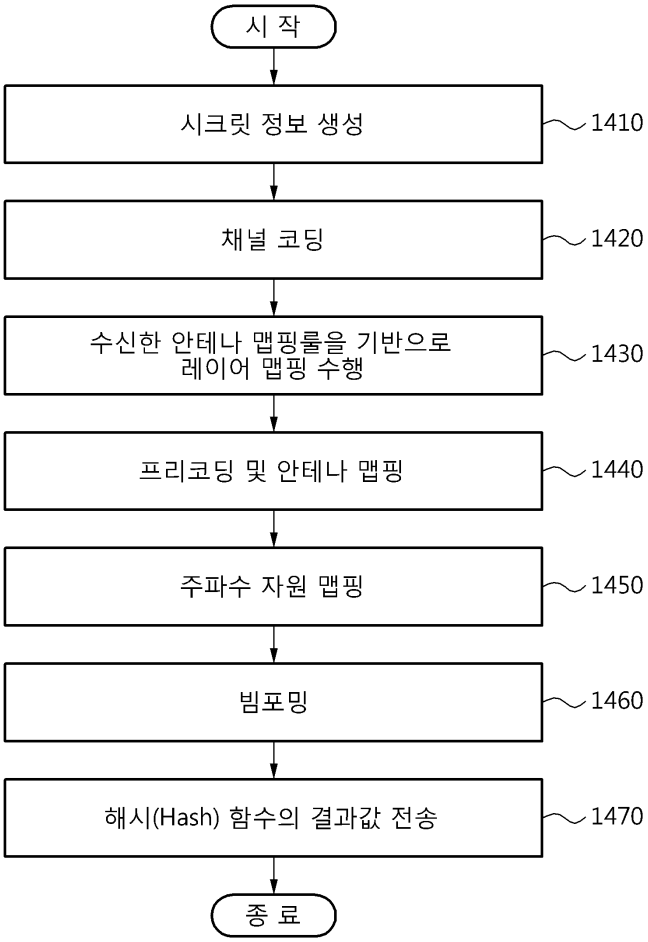
도면12


시 작
안테나 맵핑룰 결정 및 전송
1210
신호 검출 및 안테나 디맵핑
1220
레이어 디맵핑
1230
채널 디코딩
1240
시크릿 정보 획득
1250
종 료

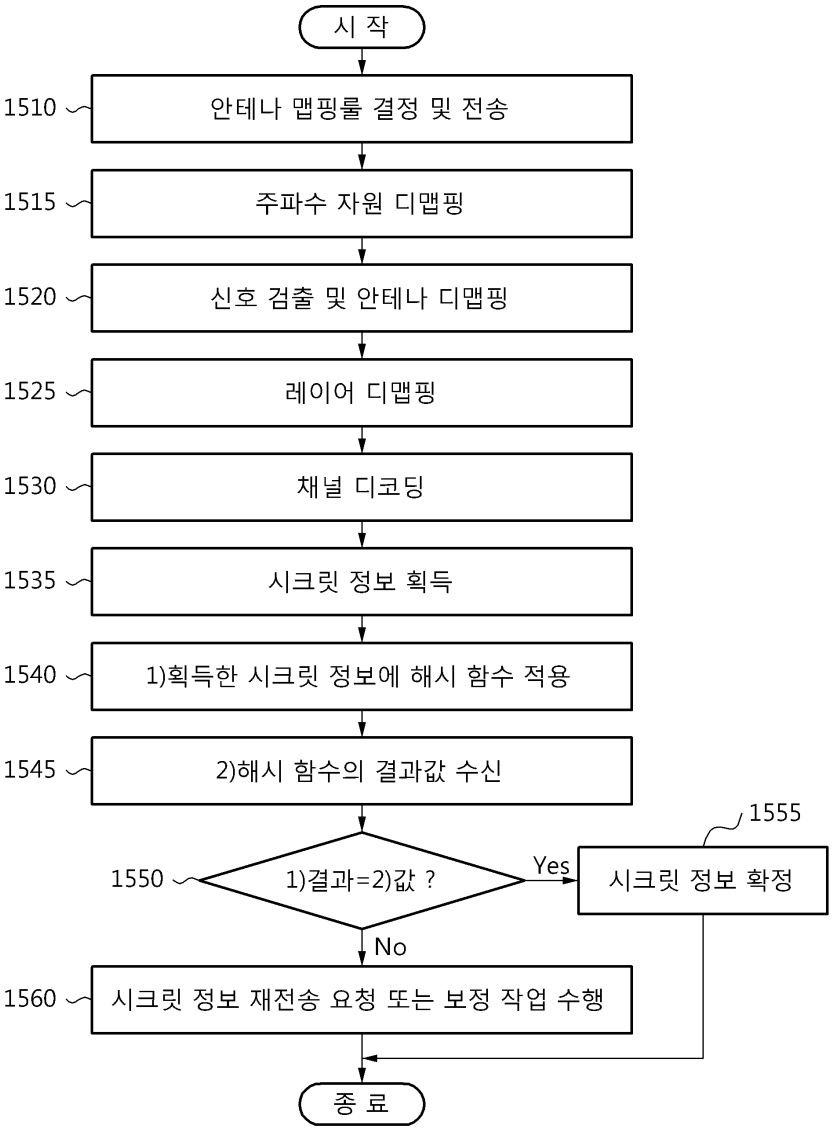
도면13


1310
1311
A/D
1313
안테나 맵핑룰 수신부
1315
시크릿 정보 생성부
1317
채널 품질 판단부
1319
채널 코더
1321
레이어 맵핑부
1323
프리코딩 및 안테나 맵핑부
1325
D/A
1350
1351
A/D
1353
채널 품질 판단부
1355
신호 검출 및 안테나 디맵핑부
1357
안테나 맵핑룰 결정부
1359
레이어 디맵핑부
1361
안테나 맵핑룰 전송부
1363
채널 디코더
1365
시크릿 정보 획득부
1367
D/A

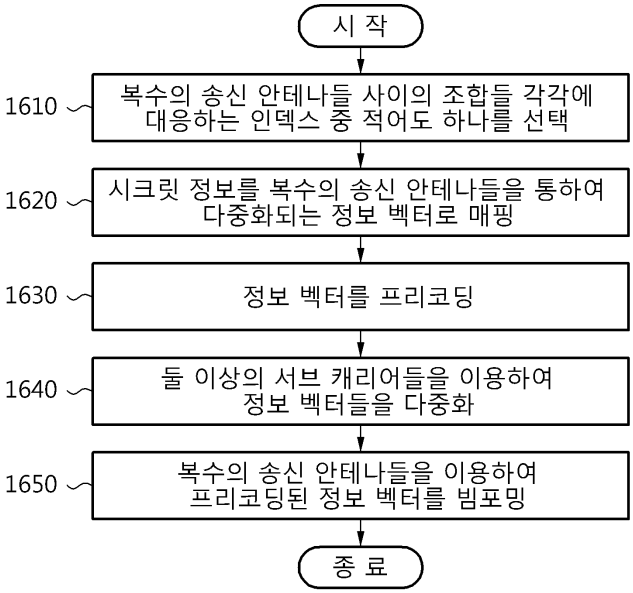
도면14


시 작
시크릿 정보 생성
1410
채널 코딩
1420
수신한 안테나 맵핑룰을 기반으로
레이어 맵핑 수행
1430
프리코딩 및 안테나 맵핑
1440
주파수 자원 맵핑
1450
빔포밍
1460
해시(Hash) 함수의 결과값 전송
1470
종 료

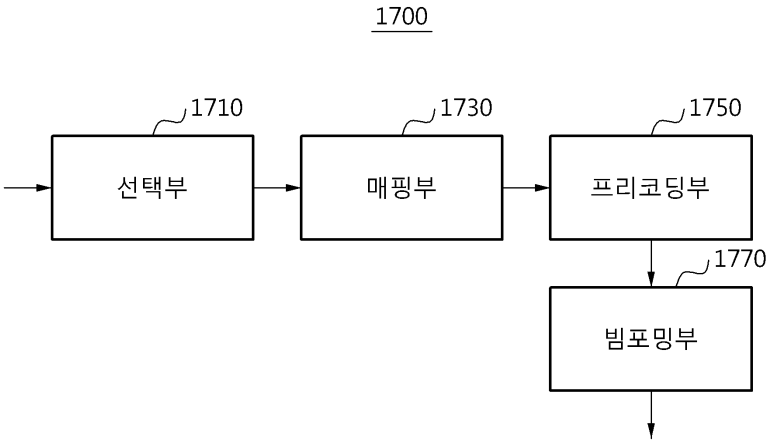
도면15


시 작
1510
안테나 맵핑룰 결정 및 전송
1515
주파수 자원 디맵핑
1520
신호 검출 및 안테나 디맵핑
1525
레이어 디맵핑
1530
채널 디코딩
1535
시크릿 정보 획득
1540
1)획득한 시크릿 정보에 해시 함수 적용
1545
2)해시 함수의 결과값 수신
1550
1)결과=2)값 ?
Yes
1555
시크릿 정보 확정
No
1560
시크릿 정보 재전송 요청 또는 보정 작업 수행
종 료

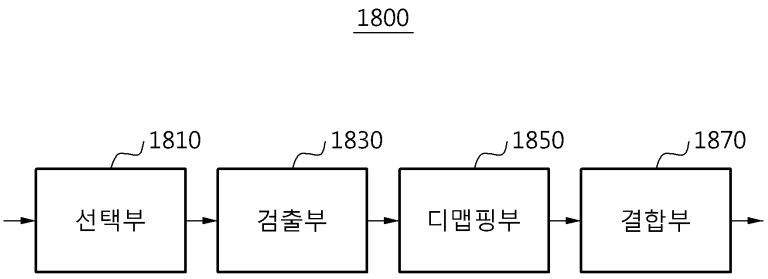
도면16



도면17



도면18



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 17

【변경전】

상기 획득한 시크릿 정보

【변경후】

상기 수신한 시크릿 정보