



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0078092
(43) 공개일자 2020년07월01일

(51) 국제특허분류(Int. Cl.)
H04W 12/12 (2009.01) H04B 7/0417 (2017.01)
H04B 7/0452 (2017.01) H04B 7/06 (2017.01)
H04W 12/00 (2019.01) H04W 84/12 (2009.01)
(52) CPC특허분류
H04W 12/1204 (2019.01)
H04B 7/0421 (2013.01)
(21) 출원번호 10-2018-0167672
(22) 출원일자 2018년12월21일
심사청구일자 없음

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이원준
서울특별시 강남구 선릉로 221, 104동 2005호 (도곡동, 도곡렉슬아파트)
김영기
서울특별시 성북구 안암로9가길 25, 101호 (안암동4가)
샤오 첸 룡
서울특별시 동대문구 제기로4길 17, 104호 (제기동)
(74) 대리인
특허법인엠에이피에스

전체 청구항 수 : 총 1 항

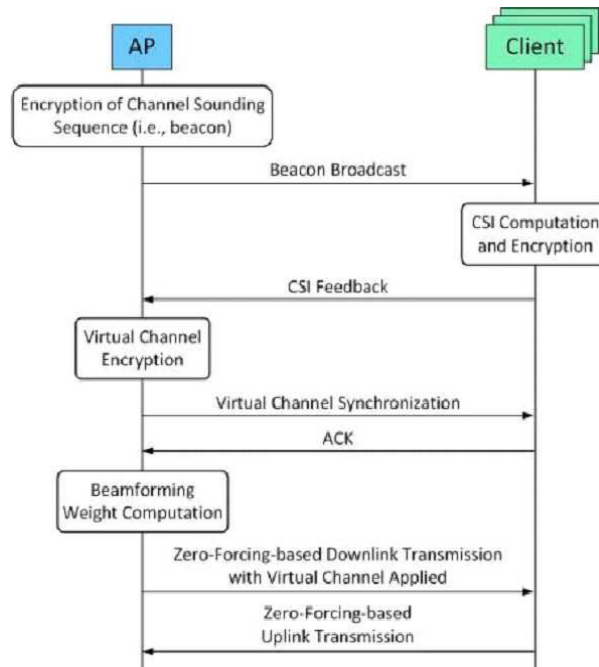
(54) 발명의 명칭 무선 랜에서의 선택적 재밍 공격 억제 방법

(57) 요약

본 발명은 무선랜에서의 선택적 재밍 공격 억제 방법에 관한 것으로서, MU-MIMO 시스템에 의해 수행되는 무선랜에서의 선택적 재밍 공격 억제 방법에 있어서, a) AP와 클라이언트 단말간 통신시, AP는 암호화된 채널 사운드링 시퀀스를 비콘(beacon) 신호로 브로드캐스트 하는 단계; b) 각 클라이언트 단말이 상기 비콘 신호에 기초하여 하

(뒷면에 계속)

대표도 - 도3



양 전송의 채널 상태 정보(CSI)를 계산한 후, 상기 계산된 CSI를 암호화하여 상기 AP에 피드백 하는 단계; c) 상
 $N \times 1$
 기 AP는 자신에게 연결된 모든 클라이언트 단말로부터 피드백된 CSI에 기초하여 데이터 스트림 행렬(백
 터)에 가상 채널(H_V)을 설정하고, 상기 가상 채널이 설정된 데이터 스트림 행렬을 암호화하여 각 클라이언트 단
 말에 전송하는 단계; d) 상기 가상 채널이 설정된 데이터 스트림 행렬을 전송받은 클라이언트 단말은 가상 채널
 의 동기화를 위해 상기 AP에게 확인응답(acknowledgement) 메시지를 전송하는 단계; 및 e) 상기 AP가 모든 클라
 이언트 단말로부터 확인응답 메시지를 수신하면 상기 가상 채널 사용을 위한 메시지 교환을 종료하는 단계를 포
 함하는 것이다.

(52) CPC특허분류

H04B 7/0452 (2013.01)

H04B 7/0626 (2013.01)

H04W 12/001 (2019.01)

H04W 84/12 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711070433

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 대학ICT연구센터육성지원사업

연구과제명 세이프 웰빙을 위한 IoT 기반 스마트 웨어러블 SW 기술개발

기 여 율 1/1

주관기관 단국대학교 산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

MU-MIMO 시스템에 의해 수행되는 무선랜에서의 선택적 재밍 공격 억제 방법에 있어서,

- a) AP와 클라이언트 단말간 통신시, AP는 암호화된 채널 사운딩 시퀀스를 비콘(beacon) 신호로 브로드캐스트 하는 단계;
- b) 각 클라이언트 단말이 상기 비콘 신호에 기초하여 하향 전송의 채널 상태 정보(CSI)를 계산한 후, 상기 계산된 CSI를 암호화하여 상기 AP에 피드백 하는 단계;

N × 1

- c) AP는 자신에게 연결된 모든 클라이언트 단말로부터 피드백된 CSI에 기초하여 데이터 스트림 행렬(벡터)에 가상 채널(H_v)을 설정하고, 상기 가상 채널이 설정된 데이터 스트림 행렬을 암호화하여 각 클라이언트 단말에 전송하는 단계;
- d) 상기 가상 채널이 설정된 데이터 스트림 행렬을 전송받은 클라이언트 단말은 가상 채널의 동기화를 위해 상기 AP에게 확인응답(acknowledgement) 메시지를 전송하는 단계; 및
- e) 상기 AP가 모든 클라이언트 단말로부터 확인응답 메시지를 수신하면 상기 가상 채널 사용을 위한 메시지 교환을 종료하는 단계를 포함하는 것인, 무선 랜에서의 선택적 재밍 공격 억제 방법.

발명의 설명

기술 분야

- [0001] 본 발명은 중 사용자의 공동 통신을 지원하는 무선 랜에서 상향 전송에서 특정한 사용자에게 선택적 재밍(jamming) 공격을 억제하는 방법에 관한 것이다.

배경 기술

- [0002] MU-MIMO(Multi-user multiple input multiple output) 기술을 적용한 무선랜(Wireless Local Area Network, WLAN)에서는 AP가 하향 전송의 총 스루풋(aggregate throughput)을 향상시키기 위하여 공간 다중화(spatial multiplexing)를 활용해 자신에게 연결된 클라이언트 단말에 데이터 스트림을 동시에 제공할 수 있다.
- [0003] 이러한 성능 향상을 완전히 달성하기 위해, 각 클라이언트 단말이 AP와 자신 사이에 형성된 채널 정보를 포함하는 채널 상태 정보(channel state information, CSI)를 전송해야 하는데, CSI 는 MU-MIMO 기술뿐만 아니라 다른 보안 쟁점에도 적용할 수 있다. 예를 들어, CSI는 시간 및 공간적 특성으로 인해 패킷(packet)의 출발지(source)를 인증하는 서명으로 활용되거나, 의도된 수신자에게는 영향을 주지 않으면서 도청자들의 채널 환경을 저하시키는 인공 잡음(artificial noise)에 도입될 수 있다.
- [0004] 이와 같은 CSI의 중요성으로 인해 IEEE 802.11ac와 같이 MU-MIMO 기술이 도입된 무선랜 표준에서는 채널 사운딩 시퀀스(channel sounding sequence)에 따라 AP와 클라이언트 단말 사이에 전송되는 CSI 관련 피드백(feedback)들을 암호화할 것을 권고하고 있다.
- [0005] 최근, 단순히 CSI 관련 피드백을 암호화하는 방법만으로는 MU-MIMO 기술을 활용하는 무선랜에서 CSI의 노출을 방지할 수 없음이 발견되었다. 구체적으로, 공격자는 클라이언트 단말과 AP 간 하향 전송에서 실제로 전송되는 데이터 스트림을 지속해서 도청하는 것만으로도 전송하는 신호의 MAC 계층의 헤더 등에 대해 알고 있는 지식을 활용하여 AP가 MU-MIMO를 활용하여 하향 전송시 사용하는 빔포밍 가중치(beamforming weight)를 계산하고 이를 통해 최종적으로 암호화된 CSI를 추론할 수 있다.
- [0006] 일단 CSI가 공격자에게 노출되면, 공격자는 이를 활용하여 다양한 종류의 공격을 수행할 수 있다. 그중 가장 주요한 공격으로, 공격자는 호혜성(reciprocity)을 기반으로 모든 클라이언트 단말의 상향 전송 채널의 CSI를

추론할 수 있으며, 결국 특정 클라이언트 단말의 상향 전송에 선택적으로 재밍 공격을 수행할 수 있다.

[0007] 선택적 재밍(selective jamming)이라 불리는 이런 공격은 특정 클라이언트 단말뿐만 아니라 공격자의 전송 범위 내 다른 모든 기기까지 같이 공격하는 기존의 재밍 공격과는 다르게 훨씬 정교하게(fine-grained) 공격을 수행할 수 있는 등 다양한 차별성을 갖는다.

[0008] 클라이언트 단말의 주도로 ZFBF(zero-forcing beamforming)을 통해 모든 신호에 대하여 특정 신호와 해당 신호를 제외한 신호들의 부분 공간(sub-space)이 직교(orthogonal)하도록 하여 스트림 간 간섭(interference)을 제거해야 한다.

[0009] 그러나, 이러한 특성은 공격자가 수집한 하향 전송 채널의 CSI를 활용하여 상향 MU-MIMO에 선택적 재밍 공격을 수행하는데 활용할 수 있다는 문제점이 있다.

[0010] 수학적으로, 추론된 상향 채널의 CSI를 나타내는 $H_{AC_i}^u$ 는 와 수학식 1과 같이 표현된다.

[0011] [수학식 1]

$$H_{AC_i}^u = Q_{AP} (H_{AC_i}^d)^T \alpha_{C_i}$$

[0012] 수학식 1에서, $H_{AC_i}^d$ 는 AP에서 클라이언트 단말로의 하향 전송 채널에서의 CSI이고, α_{C_i} 는 클라이언트 단말(C_i)의 데이터 스트림의 송신 및 수신과정 차이에 의한 교정 계수(calibration coefficient)이며, Q_{AP} 는 AP의 송신 및 수신과정에서 특정 안테나에 국한된 교정 계수를 말한다. 만일, 공격자가 자신의 상향 MU-MIMO 재밍 신호에 가중치($Q_E^{-1}((H_{AE}^d)^T)^{-1}(H_{AC_i}^d)^T$)를 곱하면, AP에 최종적으로 도달하게 되는 신호의 계수는 $(1/\alpha_{C_i})H_{AC_i}^u$ 가 된다.

[0013] 이러한 신호는 클라이언트 단말(C_i)이 전송하는 신호의 부분 공간에 속하게 되므로 공격자의 재밍 공격으로 발생하는 간섭 현상은 다른 어떠한 클라이언트 단말들보다도 클라이언트 단말(C_i)에 미치는 영향(약 20 dB)이 크다. 따라서, 선택적 재밍 공격은 기존의 재밍 공격에 비해 높은 공격 정밀도와 효율성을 가지게 되므로, 이러한 선택적 재밍 공격을 억제해야 한다.

발명의 내용

해결하려는 과제

[0014] 본 발명은 전술한 문제점을 해결하기 위하여, 본 발명의 일 실시예에 따라 AP가 하향 전송을 수행하기 전에 추가적인 가상 채널(virtual channel)을 도입하고 이를 정당한 클라이언트 단말에게 전송하여 실제 데이터 전송 과정에서 CSI가 기밀성을 유지할 수 있도록 하는 것에 목적이 있다.

[0015] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0016] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서 본 발명의 일 실시예에 따른, 무선랜에서의 선택적 재밍 공격 억제 방법은, MU-MIMO 시스템에 의해 수행되는 무선랜에서의 선택적 재밍 공격 억제 방법에 있어서, a) AP와 클라이언트 단말간 통신시, AP는 암호화된 채널 사운딩 시퀀스를 비콘(beacon) 신호로 브로드캐스트 하는 단계; b) 각 클라이언트 단말이 상기 비콘 신호에 기초하여 하향 전송의 채널 상태 정보(CSI)를 계산한 후, 상기 계산된 CSI를 암호화하여 상기 AP에 피드백 하는 단계; c) 상기 AP는 자신에게 연결된 모든 클라이언트 단

$N \times 1$

말로부터 피드백된 CSI에 기초하여 데이터 스트림 행렬(벡터)에 가상 채널(H_v)을 설정하고, 상기 가상 채널이 설정된 데이터 스트림 행렬을 암호화하여 각 클라이언트 단말에 전송하는 단계; d) 상기 가상 채널이 설정

된 데이터 스트림 행렬을 전송받은 클라이언트 단말은 가상 채널의 동기화를 위해 상기 AP에게 확인응답(acknowledgement) 메시지를 전송하는 단계; 및 e) 상기 AP가 모든 클라이언트 단말로부터 확인응답 메시지를 수신하면 상기 가상 채널 사용을 위한 메시지 교환을 종료하는 단계를 포함하는 것이다.

발명의 효과

[0018] 진술한 본 발명의 과제 해결 수단에 의하면, MU-MIMO를 활용하는 무선 랜의 전송 과정에서 실제 CSI가 AP와 이에 연결된 클라이언트 단말에게만 알려지도록 하여 기밀성을 유지할 수 있다.

[0019] 또한, 본 발명은 AP와 클라이언트 그룹 간의 CSI가 공격자에게 알려진다고 하더라도 실제로 MU-MIMO 기술에 활용하는 CSI와 달라지게 하여 선택적 제밍 공격이 실패하도록 할 수 있다.

도면의 간단한 설명

[0020] 도 1은 AP에서 N개의 클라이언트 단말에 데이터 스트림을 동시에 하향 전송하는 상황을 설명하는 도면이다.

도 2는 클라이언트 단말로부터 AP의 상향 MU-MIMO 전송이 이루어지는 상황에서 공격자로부터 선택적 제밍 공격이 수행되는 상황을 설명하는 도면이다.

도 3은 본 발명의 일 실시예에 따른 무선 랜에서의 선택적 제밍 공격 억제 방법의 AP와 클라이언트 단말과의 메시지 절차를 나타내는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0021] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0022] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미하며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0023] 이하의 실시예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아니다. 따라서 본 발명과 동일한 기능을 수행하는 동일 범위의 발명 역시 본 발명의 권리 범위에 속할 것이다.

[0025] 이하 첨부된 도면을 참고하여 본 발명의 일 실시예를 상세히 설명하기로 한다.

[0026] 도 1은 AP에서 N개의 클라이언트 단말에 데이터 스트림을 동시에 하향 전송하는 상황을 설명하는 도면이고, 도 2는 클라이언트 단말로부터 AP의 상향 MU-MIMO 전송이 이루어지는 상황에서 공격자로부터 선택적 제밍 공격이 수행되는 상황을 설명하는 도면이다.

[0027] 도 1을 참조하면, AP와 공격자는 K개의 안테나를 장착하고 있으며, 동시 하향 전송을 위해 $K \geq N$ 임을 가정한다.

[0028] 가상 채널의 도입이 없는 경우, 기존의 하향 빔포밍 과정에서 AP는 전송될 N개의 데이터 스트림, 즉 각 클라이언트 단말에게 전송될 데이터가 행으로 구분된 벡터)에 $W_A P$ 를 곱하여 스트림 간 간섭을 제거한다.

$N \times 1$

[0029] 여기에서 W_A 는 빔포밍 가중치 행렬이며, P 는 전송 출력 크기 조정(transmit power scaling) 행렬이다.

[0030] X. Zhang and E. W. Knightly가 2017년 7월에 발표한 "CSIsnoop: Attacker Inference of Channel State Information in Multi-User WLANs," 에 의하면, 공격자는 AP와 동일한 수의 안테나와 MAC 헤더로 알려진 신호의 심볼(symbol)을 활용한 공개된 전송 심볼 공격(known-transmitted-symbol attack)으로 실제로 전송된 하향 전송을 도청한 후 $W_A P$ 를 도출할 수 있으며, 결국 AP와 각 클라이언트 단말 간 하향 전송의 CSI를 계산할 수 있

다.

- [0031] CSI의 노출을 막기 위하여, 본 발명의 무선 랜에서의 선택적 재밍 공격 억제 방법에서는 가상 채널로 추가적인 $N \times 1$ 가중치 행렬(H_V)을 전송된 데이터 스트림 행렬(벡터)에 곱하도록 한다. 이러한 가상 채널(H_V)의 도입으로 인해, 공격자가 실제 하향 전송을 도청하여 도출하는 CSI는 W_{AP} 에서 $W_{AP}H_V$ 로 변하게 되어 실제 하향 전송의 CSI와 다르게 된다.
- [0032] 그러나, 가상 채널(H_V)의 도입은 이미 CSI를 통해 구해진 최적의 빔포밍 가중치를 재조정하는 것이기 때문에 데이터 스트림 간 간섭문제를 야기할 수 있으므로 AP와 클라이언트 단말의 빔포밍 가중치 모두 신중하게 조정해야 한다.
- [0033] 도 2를 참조하면, 클라이언트 단말로부터 AP의 상향 MU-MIMO 전송이 이루어지는 상황에서 공격자로부터 선택적 재밍 공격이 수행되면, 공격자가 이미 하향 전송에서의 CSI $H_{A_i}^d$ 를 Q_{AP} 계산했다고 가정하고, 공격자는 자신의 재밍 신호에 $Q_{Eve}^{-1}((H_{AE}^d)^T)^{-1}(H_{A_i}^d)^T$ 를 곱하여 클라이언트 단말(C_i)의 상향 전송 신호에만 선택적으로 재밍 공격을 수행할 수 있다.
- [0034] 그러나, 가상 채널(H_V)을 도입함에 따라, AP에 도달하게 되는 재밍 공격 신호의 계수 $(1/\alpha_{C_i})H_{A_i}^u$ 는 클라이언트 단말의 부분 공간에 속하지 않게 되고, 공격자는 효율적으로 공격을 수행하지 못하게 된다.
- [0036] 도 3은 본 발명의 일 실시예에 따른 무선 랜에서의 선택적 재밍 공격 억제 방법의 AP와 클라이언트 단말과의 메시지 절차를 나타내는 흐름도이다.
- [0037] 도 3을 참조하면, AP와 클라이언트 단말간 통신에 가상 채널을 도입하기 위하여 AP는 암호화된 채널 사운딩 시퀀스를 비콘(beacon)의 형태로 브로드캐스트한다.
- [0038] 각 클라이언트 단말은 알려진 비콘 신호를 바탕으로 하향 전송의 CSI를 계산하고 이를 암호화하여 AP에 피드백한다.
- [0039] AP는 모든 클라이언트 단말로부터 전달받은 CSI를 바탕으로 가상 채널 행렬을 설정하고, 이를 암호화하여 해당하는 각 클라이언트 단말에게 부분 행렬을 전송한다.
- [0040] 각 부분 행렬을 전송받은 클라이언트 단말들은 가상 채널 동기화를 위해 AP에게 확인응답(acknowledgement) 메시지를 보내며, AP가 모든 클라이언트 단말로부터 확인응답 메시지를 수신하면 가상 채널 도입을 위한 메시지 교환 절차가 종료된다.
- [0041] 메시지 교환 절차가 종료되면, 모든 클라이언트 단말은 자신과 AP가 공유한 가상 채널(H_V)를 보유하게 되며, 다른 클라이언트 단말의 가상 채널에 대한 정보는 보유하지 못하기 때문에 공격자는 물론 정당한 클라이언트 단말 내부적으로도 서로의 CSI에 대해 전혀 알지 못하게 된다. 이후에 빔포밍을 기반으로 한 하향, 상향 전송이 AP와 클라이언트 단말간에 진행된다.
- [0043] 이상에서 설명한 본 발명의 실시예에 따른 무선 랜에서의 선택적 재밍 공격 억제 방법은, 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 이러한 기록 매체는 컴퓨터 판독 가능 매체를 포함하며, 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체를 포함하며, 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.
- [0044] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명

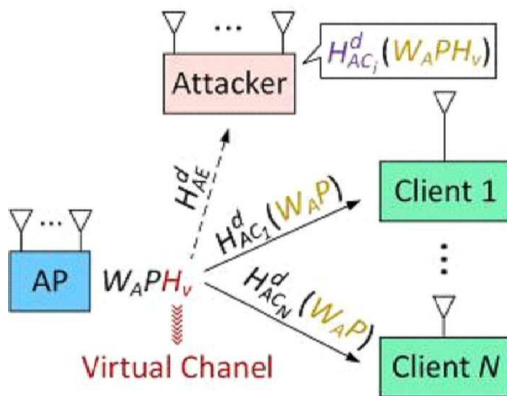
의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0045]

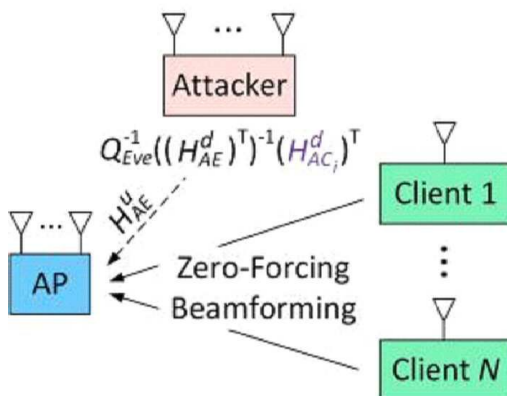
본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

도면1



도면2



도면3

