(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0050652
(43) 공개일자 2020년05월12일

(51) 국제특허분류(Int. Cl.)
H04K 3/00 (2015.01)
(52) CPC특허분류
H04K 3/822 (2013.01)
H04K 3/825 (2013.01)
(21) 출원번호 10-2018-0133536
(22) 출원일자 2018년11월02일
심사청구일자 2018년11월02일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
문지환
경기도 용인시 수지구 죽전로193번길 35, 107동 1403호 (죽전동, 성현마을반도유보라)
이인규
서울특별시 강남구 영동대로 640, 웨스트동 3303호 (삼성동, 아이파크삼성)
(74) 대리인
윤귀상

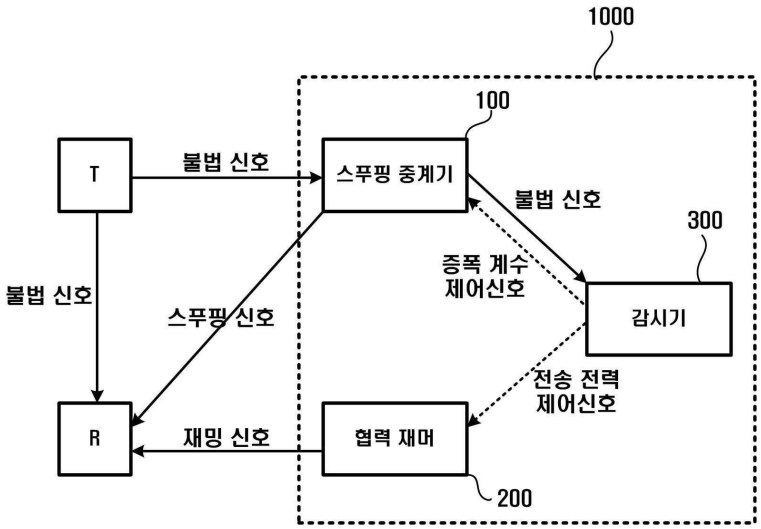
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템 및 방법**

(57) 요 약

본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템은, 불법 송신기로부터 감지되는 불법 신호를 미리 정해진 증폭 계수에 따라 증폭시켜 중계하는 스푸핑 중계기, 불법 수신기로 상기 통신 채널의 품질을 변경시키는 재밍 신호를 미리 정해진 전송 전력으로 전송하는 협력 재머 및 스푸핑 중계기로부터 수신된 불법 신호를 기초로 정보의 감시량이 최대가 되는 증폭 계수 및 전송 전력을 산출하는 감시기를 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04K 2203/34 (2013.01)

명 세 서

청구범위

청구항 1

악의적 목적으로 무선 통신을 이용하는 사용자들이 소지한 불법 송신기 및 불법 수신기간 설정된 통신 채널을 통해 송수신되는 정보를 감시하는 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템에 있어서,

상기 불법 송신기로부터 감지되는 불법 신호를 미리 정해진 증폭 계수에 따라 증폭시켜 중계하는 스푸핑 중계기;

상기 불법 수신기로 상기 통신 채널의 품질을 변경시키는 재밍 신호를 미리 정해진 전송 전력으로 전송하는 협력 재머; 및

상기 스푸핑 중계기로부터 수신된 상기 불법 신호를 기초로 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력을 산출하는 감시기를 포함하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 2

제1항에 있어서, 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은,

상기 불법 수신기로 가용한 최대 전송 전력을 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 감소시키는 증폭 계수에 따라 스푸핑 신호를 전송하는 제1 모드, 상기 불법 수신기로 상기 최대 전송 전력 이하의 전송 전력으로 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제2 모드 및 상기 불법 수신기로 상기 재밍 신호를 전송하지 않되, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제3 모드 중 어느 하나의 모드로 동작하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 3

제2항에 있어서, 상기 감시기는,

상기 불법 신호를 복구하여 획득되는 상기 정보의 감시량이 최대가 되는 모드별 증폭 계수 및 모드별 전송 전력을 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드별로 각각 산출하고,

상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 상기 정보의 감시량이 가장 큰 어느 하나의 모드를 추출하며,

추출된 어느 하나의 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 4

제3항에 있어서,

상기 감시기는, 선택된 상기 증폭 계수를 상기 스푸핑 중계기로 전송하고, 선택된 상기 전송 전력을 상기 협력 재머로 전송하고,

상기 스푸핑 중계기는, 상기 기 설정된 증폭 계수를 상기 감시기로부터 수신된 증폭 계수로 변경하며,

상기 협력 재머는, 상기 기 설정된 전송 전력을 상기 감시기로부터 수신된 전송 전력으로 변경하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 5

제2항에 있어서, 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은,

상기 스푸핑 중계기와 상기 감시기 간에 설정된 감시 채널 용량과, 상기 불법 수신기의 신호 대 잡음비에 의해 결정되는 상기 불법 송신기의 전송 속도를 비교한 결과에 따라 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 어느 하나의 모드로 동작하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 6

제5항에 있어서, 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은,

상기 감시 채널 용량이 상기 전송 속도보다 작은 것으로 확인되면, 상기 불법 송신기의 전송 속도를 감소시키기 위해 상기 불법 수신기의 신호 대 잡음비를 감소시키는 상기 제1 모드로 동작하고,

상기 감시 채널 용량이 상기 전송 속도보다 큰 것으로 확인되면, 상기 불법 송신기의 전송 속도를 상승시키기 위해 상기 불법 수신기의 신호 대 잡음비를 상승시키는 상기 제2 모드 및 상기 제3 모드 중 어느 하나로 동작하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템.

청구항 7

스푸핑 중계기, 협력 재머 및 감시기로 구성된 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템을 이용한 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법에 있어서,

상기 감시기가 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 동작 모드별로 정보의 감시량이 최대가 되는 상기 스푸핑 중계기의 모드별 증폭 계수 및 상기 협력 재머의 모드별 전송 전력을 산출하고,

상기 감시기가 정보의 감시량이 최대가 되는 어느 하나의 동작 모드를 추출하고, 추출된 상기 어느 하나의 동작 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택하며,

선택된 상기 증폭 계수를 상기 스푸핑 중계기로 전송하고, 선택된 상기 전송 전력을 상기 협력 재머로 전송하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법.

청구항 8

제7항에 있어서, 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은,

상기 불법 수신기로 가용한 최대 전송 전력을 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 감소시키는 증폭 계수에 따라 스푸핑 신호를 전송하는 제1 모드, 상기 불법 수신기로 상기 최대 전송 전력 이하의 전송 전력으로 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제2 모드 및 상기 불법 수신기로 상기 재밍 신호를 전송하지 않되, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제3 모드 중 어느 하나의 모드로 동작하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법.

청구항 9

제8항에 있어서, 상기 감시기가 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 동작 모드별로 정보의 감시량이 최대가 되는 상기 스푸핑 중계기의 모드별 증폭 계수 및 상기 협력 재머의 모드별 전송 전력을 산출하는 것은,

상기 불법 신호를 복구하여 획득되는 상기 정보의 감시량이 최대가 되는 모드별 증폭 계수 및 모드별 전송 전력

을 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드별로 각각 산출하고,

상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 상기 정보의 감시량이 가장 큰 어느 하나의 모드를 추출하며,

추출된 어느 하나의 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택하는 것인, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법.

청구항 10

제7항에 있어서,

상기 스푸핑 중계기, 상기 협력 재머 및 상기 감시기 간에 설정된 채널을 추정하고, 상기 채널 및 상기 협력 재머에서 생성된 재밍 신호를 공유하는 것을 더 포함하는, 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템 및 방법에 관한 것으로서, 더욱 상세하게는 악의적인 목적으로 무선 통신을 이용하는 사용자들 간 송수신되는 정보를 감시하는 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 무선 통신 기술 분야의 급격한 발전 및 인프라 확대로 인하여, 현재 많은 사용자들이 무선 통신을 이용하여 다른 사용자와 원격으로 정보를 주고받고 있으며, 다양한 기술 분야에서 무선 통신 기술을 접목하여 사용자의 편의를 향상시킬 수 있는 새로운 기술 및 서비스가 개발되고 있다.

[0004] 하지만, 일부 악의적인 사용자들은 특정 집단을 위한 개별 통신 네트워크 설계가 간편해진 이점을 악용하여 사이버 테러나 범죄 공모 등의 부적절한 용도로 이용하고 있으며, 이러한 악의적인 목적을 가진 사용자들간의 무선 통신 내용을 감시해야될 필요성이 증대되고 있다.

[0005] 하지만, 종래에는 정보를 감시하기 위한 감시 장치가 수신기로서의 역할만을 수행하기 때문에, 종래의 감시 시스템은 감시 채널의 품질이 좋지 않을 때는 획득된 정보를 정확하게 복구할 수 없다는 치명적인 한계가 있다.

[0006] 또한, 종래의 감시 시스템은 감시 장치와 불법 사용자 간에 직접적인 통신 채널을 형성한 상태로 정보를 획득하기 때문에 불법 사용자들은 자신이 감시를 당하고 있음을 용이하게 인지할 수 있으며, 불법 사용자들이 감시 장치로부터 멀리 떨어지거나 통신 음역 지역에서는 정보의 정확한 획득이 불가능하다는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국등록특허 제10-1403020호

(특허문헌 0002) 한국등록특허 제10-1791500호

발명의 내용

해결하려는 과제

[0009] 본 발명의 일측면은 불법 송신기와 불법 수신기 간 주고받는 불법 신호를 감시하는 과정에서, 정보의 감시량이 극대화되도록 스푸핑 중계기 및 협력 재머를 제어하는 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템 및 방법을 제공한다.

[0010] 본 발명의 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0012] 본 발명의 일 실시예에 따른 악의적 목적으로 무선 통신을 이용하는 사용자들이 소지한 불법 송신기 및 불법 수신기간 설정된 통신 채널을 통해 송수신되는 정보를 감시하는 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은, 상기 불법 송신기로부터 감지되는 불법 신호를 미리 정해진 증폭 계수에 따라 증폭시켜 중계하는 스푸핑 중계기, 상기 불법 수신기로 상기 통신 채널의 품질을 변경시키는 재밍 신호를 미리 정해진 전송 전력으로 전송하는 협력 재머 및 상기 스푸핑 중계기로부터 수신된 상기 불법 신호를 기초로 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력을 산출하는 감시기를 포함한다.

[0013] 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은, 상기 불법 수신기로 가용한 최대 전송 전력을 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 감소시키는 증폭 계수에 따라 스푸핑 신호를 전송하는 제1 모드, 상기 불법 수신기로 상기 최대 전송 전력 이하의 전송 전력으로 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제2 모드 및 상기 불법 수신기로 상기 재밍 신호를 전송하지 않되, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제3 모드 중 어느 하나의 모드로 동작할 수 있다.

[0014] 상기 감시기는, 상기 불법 신호를 복구하여 획득되는 상기 정보의 감시량이 최대가 되는 모드별 증폭 계수 및 모드별 전송 전력을 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드별로 각각 산출하고, 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 상기 정보의 감시량이 가장 큰 어느 하나의 모드를 추출하며, 추출된 어느 하나의 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택할 수 있다.

[0015] 상기 감시기는, 선택된 상기 증폭 계수를 상기 스푸핑 중계기로 전송하고, 선택된 상기 전송 전력을 상기 협력 재머로 전송하고, 상기 스푸핑 중계기는, 상기 기 설정된 증폭 계수를 상기 감시기로부터 수신된 증폭 계수로 변경하며, 상기 협력 재머는, 상기 기 설정된 전송 전력을 상기 감시기로부터 수신된 전송 전력으로 변경할 수 있다.

[0016] 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은, 상기 스푸핑 중계기와 상기 감시기 간에 설정된 감시 채널 용량과, 상기 불법 수신기의 신호 대 잡음비에 의해 결정되는 상기 불법 송신기의 전송 속도를 비교한 결과에 따라 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 어느 하나의 모드로 동작할 수 있다.

[0017] 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은, 상기 감시 채널 용량이 상기 전송 속도보다 작은 것으로 확인되면, 상기 불법 송신기의 전송 속도를 감소시키기 위해 상기 불법 수신기의 신호 대 잡음비를 감소시키는 상기 제1 모드로 동작하고, 상기 감시 채널 용량이 상기 전송 속도보다 큰 것으로 확인되면, 상기 불법 송신기의 전송 속도를 상승시키기 위해 상기 불법 수신기의 신호 대 잡음비를 상승시키는 상기 제2 모드 및 상기 제3 모드 중 어느 하나로 동작할 수 있다,

[0018] 또한, 스푸핑 중계기, 협력 재머 및 감시기로 구성된 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템을 이용한 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법은, 상기 감시기가 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 동작 모드별로 정보의 감시량이 최대가 되는 상기 스푸핑 중계기의 모드별 증폭 계수 및 상기 협력 재머의 모드별 전송 전력을 산출하고, 상기 감시기가 정보의 감시량이 최대가 되는 어느 하나의 동작 모드를 추출하고, 추출된 상기 어느 하나의 동작 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택하며, 선택된 상기 증폭 계수를 상기 스푸핑 중계기로 전송하고, 선택된 상기 전송 전력을 상기 협력 재머로 전송한다.

[0019] 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템은, 상기 불법 수신기로 가용한 최대 전송 전력을 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 감소시키는 증폭 계수에 따라 스푸핑 신호를 전송하는 제1 모드, 상기 불법 수신기로 상기 최대 전송 전력 이하의 전송 전력으로 상기 재밍 신호를 전송하면서, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제2 모드 및 상기 불법 수신기로 상기 재밍 신호를 전송하지 않되, 상기 불법 수신기의 신호 대 잡음비를 증가시키는 증폭 계수에 따라 상기 스푸핑 신호를 전송하는 제3 모드 중 어느 하나의 모드로 동작할 수 있다.

[0020] 상기 감시기가 상기 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 동작 모드별로 정보의 감시량이 최대가 되는 상기 스푸핑 중계기의 모드별 증폭 계수 및 상기 협력 재머의 모드별 전송 전력을 산출하는 것은, 상기 불법 신호를 복구하여 획득되는 상기 정보의 감시량이 최대가 되는 모드별 증폭 계수 및 모드별 전송 전력을 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드별로 각각 산출하고, 상기 제1 모드, 상기 제2 모드 및 상기 제3 모드 중 상기 정보의 감시량이 가장 큰 어느 하나의 모드를 추출하며, 추출된 어느 하나의 모드에서 산출된 상기 모드별 증폭 계수 및 상기 모드별 전송 전력을 상기 정보의 감시량이 최대가 되는 상기 증폭 계수 및 상기 전송 전력으로 선택하는 것일 수 있다.

[0021] 상기 스푸핑 중계기, 상기 협력 재머 및 상기 감시기 간에 설정된 채널을 추정하고, 상기 채널 및 상기 협력 재머에서 생성된 재밍 신호를 공유하는 것을 더 포함할 수 있다.

발명의 효과

[0023] 상술한 본 발명의 일측면에 따르면, 스푸핑 중계기 및 협력 재머를 이용하여 불법 사용자들간 주고받는 불법 신호를 주도적으로 감시할 수 있으며, 감시 채널 용량 및 불법 송신기의 전속 속도를 비교한 결과에 따라 스푸핑 중계기의 증폭 계수 및 협력 재머의 전송 전력을 실시간으로 가변시켜 감시할 수 있는 정보의 양을 극대화할 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 개략적인 구성이 도시된 개념도이다.

도 2 내지 도 4는 도 1의 감시 시스템이 불법 신호에 포함된 정보의 획득량이 최대가 되도록 불법 송신기의 전송 속도를 가변시키는 예시들이 도시된 개념도이다.

도 5는 불법 송신기와 불법 수신기 간의 거리에 따른 최대 정보 감시량의 변화를 나타내는 그래프이다.

도 6은 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 방법의 개략적인 흐름이 도시된 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0027] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0028] 도 1은 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템의 개략적인 구성이 도시된 블록도이다.

[0029] 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 사이버 테러, 범죄 공모 등과 같이 악의적인 목적을 달성하기 위해 무선 통신을 이용하는 사용자(이하, 불법 사용자)들의 목적을 사전에 차단하기 위하여, 불법 사용자들이 무선 통신망을 통해 주고받는 정보를 감시할 수 있다. 이를 위해, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 불법 사용자들측에 구비된 불법 송신기(T)와 불법 수신기(R)간 설정된 무선 통신 채널을 통해 송수신되는 정보를 획득할 수 있다.

[0030] 특히, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 불법 사용자들이 불법 송신기(T)와 불법 수신기(R)간 설정된 무선 통신 채널을 통해 송수신되는 정보가 감시되고 있음을 인지하지 못하도록, 감시기(300)는 불법 송신기(T)와 감시기(300) 사이에 직접적인 통신 채널을 형성하지 않은 상태에서 스푸핑 중계기(100)를 통해 불법 송신기(T)로부터 전송되는 불법 신호를 획득할 수 있다.

[0031] 이 과정에서, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 감시기(300)로 획득되는 불법 신호의 수신율을 최대화하기 위하여 스푸핑 중계기(100)의 불법 신호 증폭 계수 및 협력 재머(200)의 전송 전력을 실시간으로 가변시킬 수 있다.

[0032] 즉, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 스푸핑 중계기(100)의 불법 신호 증폭 계수 및 협력 재머(200)의 전송 전력을 가변하여 통신 채널 품질을 감시에 유리하게 조절함으로써, 결과적으로 불법 신호로부터 획득되는 정보량을 최대화할 수 있다.

[0033] 구체적으로, 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)은 스푸핑 중계기(100), 협력 재머(200) 및 감시기(300)를 포함할 수 있다.

[0034] 스푸핑 중계기(100)는 불법 송신기(T)와 감시기(300) 사이에 배치되어 불법 송신기(T)로부터 전송되는 불법 신호를 감지하여 감시기로(300)로 전달하는 통신 중계 장치일 수 있다.

[0035] 상술한 바와 같이, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 불법 사용자들이 불법 송신기(T)와 불법 수신기(R)간 설정된 무선 통신 채널을 통해 송수신되는 정보가 감시되고 있음을 인지하지 못하도록, 감시기(300)는 불법 송신기(T)와 감시기(300) 사이에 직접적인 통신 채널을 형성하지 않은 상태에서 스푸핑 중계기(100)를 통해 불법 송신기(T)로부터 전송되는 불법 신호를 획득할 수 있다.

[0036] 이를 위해, 스푸핑 중계기(100)는 자신의 통신 반경 내에 불법 송신기(T)가 위치하도록 배치 위치가 조절될 수 있다. 이하에서는, 설명의 편의를 위하여 불법 송신기(T)와 감시기(300) 사이에는 하나의 스푸핑 중계기(100)만 배치되어, 하나의 스푸핑 중계기(T)가 불법 송신기(T)로부터 감지된 불법 신호를 감시기(300)로 직접 중계하는 것으로 가정하여 설명하기로 한다. 하지만, 스푸핑 중계기(100)의 개수가 단일 개수로 한정되는 것은 아니며 경우에 따라서는 스푸핑 중계기(100)가 복수 개로 구비될 수도 있다. 이러한 경우, 복수의 스푸핑 중계기(100)는 릴레이 네트워크를 형성하여 어느 하나의 스푸핑 중계기(100)가 불법 송신기(T)로부터 불법 신호를 수신하면, 이를 이웃하는 다른 스푸핑 중계기(100)로 전달하여 목적 노드인 감시기(300)로 불법 신호를 전달할 수도 있다.

[0037] 스푸핑 중계기(100)는 AF(Amplify-and-Forward) 전이중(Full-Duplex, FD) 방식으로 무선 통신을 수행할 수 있다.

[0038] 구체적으로, 스푸핑 중계기(100)는 불법 송신기(T)로부터 불법 신호를 수신하면, 이를 미리 설정된 증폭 계수에 따라 증폭시킨 후 감시기(300)로 전달하는 AF(Amplify-and-Forward) 전송 방식으로 불법 신호를 전달할 수 있다.

[0039] 또한, 스푸핑 중계기(100)는 전이중(Full-Duplex, FD) 방식으로 무선 통신을 수행할 수 있으며, 이에 따라 수신된 불법 신호를 감시기(300)로 전달하는 동시에 스푸핑(spoofing) 신호를 생성하여 불법 수신기(R)로 전송할 수 있다.

[0040] 즉, 스푸핑 중계기(100)가 불법 송신기(T)로부터 수신한 신호를 감시기(300)로 중계할 때, 감시기(300) 뿐만 아니라 불법 수신기(R)도 해당 신호를 필연적으로 수신하게 된다. 스푸핑 중계기(100)는 이러한 성질을 이용하여 필요에 따라 불법 수신기(R)의 복호화 품질을 떨어뜨리거나 향상시키는 방향으로 도청된 신호를 조작하여 송신할 수 있다. 이러한 정보의 인위적 조작 및 전송 기술을 스푸핑이라고 하며, 스푸핑 중계기(100)는 상술한 스푸핑 기술을 기용하여 불법 수신기(R)의 복호화 품질을 변경시키기 위한 스푸핑 신호를 생성하여 불법 감시기(R)로 전송할 수 있다.

[0041] 협력 재머(200)는 불법 송신기(T)와 불법 수신기(R)간의 통신 채널 품질을 변경시키는 재밍(jamming) 신호를 생

성하여 불법 수신기(R)로 전송할 수 있다.

[0042] 재밍 신호는 수신측에서 수신되는 신호에 포함된 정보의 내용을 불분명하게 하기 위한 목적으로 수신측에 전송하는 일종의 노이즈 성분이 포함된 신호로, 불법 수신기(R)는 협력 재머(200)로부터 수신된 재밍 신호의 종류 및 신호 세기에 따라 신호 대 잡음비(Signal-to-Interference-plus-Noise Ratio, SINR)가 결정될 수 있다.

[0043] 후술하겠지만, 불법 송신기(T)는 불법 수신기(R)의 신호 대 잡음비에 따라 불법 신호의 전송 속도를 결정하게 되는데, 협력 재머(200)는 이러한 불법 송신기(T)의 전송 속도를 증가시키거나 감소시켜 불법 신호의 감시에 유리한 환경을 만들기 위한 재밍 신호를 불법 수신기(R)로 전송할 수 있다.

[0044] 감시기(300)는 불법 사용자를 감시하는 감시자 측에 구비된 단말로, 다른 장치와 통신이 가능하고 정보의 입출력 및 처리가 가능한 데스크탑, 스마트폰, 태블릿PC, 노트북, 서버 등과 같은 형태일 수 있다.

[0045] 감시기(300)는 스푸핑 중계기(100) 및 협력 재머(200)를 이용하여 불법 송신기(T)로부터 전송되는 불법 신호를 감시할 수 있다. 구체적으로, 감시기(300)는 스푸핑 중계기(100)로부터 중계되는 불법 신호를 수신할 수 있다. 감시기(300)는 수신된 불법 신호를 복구하여 불법 신호에 포함된 정보를 획득할 수 있다.

[0046] 이 과정에서, 감시기(300)는 불법 신호로부터 복구되어 획득되는 정보량이 최대가 되도록, 스푸핑 중계기(100) 및 협력 재머(200)를 이용하여 불법 수신기(R)의 신호 대 잡음비를 변경시킬 수 있다. 이와 관련하여, 도 2 내지 도 4를 함께 참조하여 설명하기로 한다.

[0047] 도 2 내지 도 4는 감시기(300)가 불법 신호에 포함된 정보의 획득량이 최대가 되도록 불법 수신기(R)의 신호 대 잡음비를 이용하여 불법 송신기(T)의 전송 속도를 가변시키는 예시들이 도시된 개념도이다.

[0048] 일반적으로, 불법 수신기(R)와 무선 통신을 수행하는 불법 송신기(T)는 불법 수신기(R)의 통신 채널 품질 척도에 따라 전송 속도를 조절할 수 있다. 일 예로, 불법 송신기(T)는 불법 수신기(R)의 신호 대 잡음비에 대한 정보를 수신하여, 불법 수신기(R)의 신호 대 잡음비가 낮은 것으로 확인되면 불법 신호의 전송 속도를 낮추어 불법 수신기(R)가 적은 양의 신호만 복구할 수 있도록 할 수 있다. 반면, 불법 송신기(T)는 불법 수신기(R)의 신호 대 잡음비가 높은 것으로 확인되면 불법 수신기(R)가 다량의 신호를 복구할 수 있도록 불법 신호의 전송량, 다시 말해 전송 속도를 높일 수 있다.

[0049] 즉, 감시기(300)가 수신 신호에 포함된 정보를 정확히 복구하기 위해서는 불법 송신기(T)와 감시기(300) 사이의 통신 용량이 불법 송신기(T)가 사용하는 전송 속도보다 크거나 같아야 한다. 이때, 종래의 감시 시스템의 경우 감시기(300)가 수신기로서만 작동하기 때문에 감시 채널 용량(품질)이 저하되면 불법 신호에 포함된 정보를 정확하게 복구할 수 없다는 문제점이 있다.

[0050] 이러한 문제점을 극복하기 위하여, 본 발명에 따른 감시기(300)는 스푸핑 중계기(100) 및 협력 재머(200)를 이용하여 불법 수신기(R)의 신호 대 잡음비를 변경시켜 현재의 통신 환경을 불법 신호를 감시하기 위한 유리한 환경, 다시 말해 정보의 감시량이 최대가 되는 환경으로 주도적으로 변경시킬 수 있다.

[0051] 먼저, 도 2a에 도시된 바와 같이, 감시기(300)는 감시 채널의 용량이 불법 송신기(T)의 전송 속도보다 낮아 수신된 불법 신호로부터 정보를 정확하게 복구할 수 없는 경우, 도 2b에 도시된 바와 같이 협력 재머(200)의 재밍 신호를 이용하여 불법 수신기(R)의 신호 대 잡음비를 감소시킬 수 있다. 이러한 경우, 불법 송신기(T)는 불법 수신기(R)와 설정된 통신 채널의 품질이 저하된 것으로 판단하여 불법 신호의 전송 속도를 낮추어 전송할 수 있다. 따라서, 불법 송신기(T)의 전송 속도가 감시 채널 용량보다 낮아지고 감시기(300)는 불법 신호에 포함된 정보를 정확하게 복구할 수 있다.

[0052] 다른 예로, 도 3a에 도시된 바와 같이, 감시기(300)는 감시 채널 용량이 불법 송신기(T)의 전송 속도보다 높아 불법 신호에 포함된 정보를 정확하게 복구할 수 있는 것으로 판단되면, 도 3b에 도시된 바와 같이 스푸핑 중계기(100)를 사용하여 불법 수신기(R)의 신호 대 잡음비를 의도적으로 높일 수 있다.

[0053] 이때, 스푸핑 중계기(100)가 불법 수신기(R)의 신호 대 잡음비를 상승시키는 스푸핑 신호를 전송하는 기법을 'constructive 중계' 라고 한다. 감시기(300)는 이러한 주도적인 감시 과정을 통해 종래의 수동적인 감시 방법에 비해 더 많은 양의 정보를 감시할 수 있다.

[0054] 한편, 스푸핑 중계기(100)는 도 2a에 도시된 바와 같이 도청 채널 용량이 불법 송신기의 전송 속도보다 낮아 도청된 정보를 정확하게 복구할 수 없는 경우에도 사용될 수 있다. 구체적으로, 도 4에 도시된 바와 같이 감시기(300)는 스푸핑 중계기(100)의 스푸핑 신호를 불법 수신기(R)로 전송하여 불법 수신기의 신호대 잡음비가 오히

려 감소되도록 신호를 조작할 수도 있는데 이를 'destructive 중계'라고 한다.

[0055] 이와 같이, 감시기(300)는 감시 채널 용량이 전송 속도보다 낮은 경우 협력 재머(200) 또는 스푸핑 중계기(100)의 destructive 중계를 통해 불법 송신기(T)의 전송 속도를 감소시켜 불법 신호의 누락 또는 왜곡 없이 정보가 복구되도록 하고, 감시 채널 용량이 전송 속도보다 큰 경우 스푸핑 중계기(100)의 constructive 중계를 통해 불법 송신기(T)의 전속 속도를 향상시켜 복구되는 정보량을 증가시킬 수 있다.

[0056] 이 과정에서, 감시기(300)는 수신되는 불법 신호를 복구하여 획득되는 감시 정보량이 최대가 되도록 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력 최적값을 산출할 수 있다. 다시 말해, 감시기(300)는 정보의 감시량이 최대가 되는 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 산출할 수 있다.

[0057] 이를 위해, 감시기(300)는 감시기(300)의 신호 대 잡음비 및 불법 수신기(R)의 신호 대 잡음비를 산출하고, 이를 기초로 불법 신호로부터 획득되는 정보의 감시량이 최대가 되는 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 산출할 수 있다.

[0058] 이하에서는, 감시기(300)가 정보의 감시량이 최대가 되는 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 산출하는 구체적인 과정에 대하여 설명하기로 한다.

[0059] 먼저, 불법 송신기(T)로부터 스푸핑 중계기(100)에 수신되는 불법 신호는 다음과 같다.

수학식 1

[0060] $$y_S = h_{TS}x_T + h_{SS}x_S + z_S$$

[0061] 여기서, y_S는 스푸핑 중계기(100)로 수신된 불법 신호, h_{TS}는 불법 송신기(T)와 스푸핑 중계기(100) 사이의 채널 값, x_T는 불법 송신기(T)의 송신 신호, h_{SS}는 스푸핑 중계기(100)간의 채널 값, x_S는 스푸핑 중계기(100)의 송신 신호, z_S는 스푸핑 중계기(100)의 백색 잡음을 의미한다.

[0062] 또한, 스푸핑 중계기(100)가 수신된 불법 신호(y_S)를 증폭 계수에 따라 증폭시켜 중계할 때의 신호는 다음과 같이 나타낼 수 있다.

수학식 2

[0063] $$x_S = G_S y_S = G_S\left(h_{TS}x_T + h_{SS}x_S + z_S\right)$$

[0064] $$x_S = \frac{G_S h_{TS}}{\left(1-G_S h_{SS}\right)}x_T + \frac{G_S}{\left(1-G_S h_{SS}\right)}z_S$$

[0065] 여기서, x_S는 스푸핑 중계기(100)가 중계하는 신호, G_S는 스푸핑 중계기(100)의 증폭 계수를 의미한다.

[0066] 따라서, 스푸핑 중계기(100)에 의해 중계되어 감시기(300)로 수신되는 불법 신호(y_M)는 다음과 같이 나타낼 수 있다.

수학식 3

[0067] $$y_M = h_{SM}x_S + z_M$$
$$= \underbrace{h_{SM}\frac{G_S h_{TS}}{\left(1-G_S h_{SS}\right)}x_T}_{\text{Desired}} + h_{SM}\frac{G_S}{\left(1-G_S h_{SS}\right)}z_S + z_M$$

[0068] 상술한 수학식 3에서, 첫 번째 항(Desired)에 불법 신호가 내포하는 정보가 포함되어 있다.

[0069] 한편, 불법 송신기(T)로부터 불법 수신기(R)에 수신되는 불법 신호(y_R)은 다음과 같다.

수학식 4

[0070]
$$y_R = h_{TR}x_T + h_{SR}x_S + h_{JR}x_J + z_R$$
$$= \underbrace{\left(h_{TR} + h_{SR}\frac{G_S h_{TS}}{(1-G_S h_{SS})} \right) x_T}_{\text{Desired}} + h_{SR}\frac{G_S}{(1-G_S h_{SS})} z_S + h_{JR}x_J + z_R$$

[0071] 여기서, h_{TR}은 불법 송신기(T)와 불법 수신기(R) 사이의 채널값, h_{SR}은 스푸핑 중계기(100)와 불법 수신기(R) 사이의 채널값, h_{JR}은 협력 재머(200)와 불법 수신기(R) 사이의 채널값, x_S는 스푸핑 신호, x_J는 재밍 신호, z_R는 불법 수신기(R)의 백색 잡음을 의미한다.

[0072] 상술한 수학식 3에서와 마찬가지로, 불법 신호에 포함된 정보는 첫 번째 항(Desired)에 포함되어 있다.

[0073] 따라서, 감시기(300)의 신호 대 잡음비는 아래의 수학식 5와 같고, 불법 수신기(R)의 신호 대 잡음비는 아래의 수학식 6과 같이 나타낼 수 있다.

수학식 5

[0074]
$$\gamma_M(G_S) = \frac{\left| h_{SM}\frac{G_S h_{TS}}{(1-Gh_{SS})} \right|^2 P_T}{\left| h_{SM}\frac{G_S}{(1-G_S h_{SS})} \right|^2 \sigma_S^2 + \sigma_M^2}$$

수학식 6

[0075]
$$\gamma_R(G_S, P_J) = \frac{\left| h_{TR} + h_{SR}\frac{G_S h_{TS}}{(1-G_S h_{SS})} \right|^2 P_T}{\left| h_{SR}\frac{G_S}{(1-G_S h_{SS})} \right|^2 \sigma_S^2 + |h_{JR}|^2 P_J + \sigma_R^2}$$

[0076] 이하에서는, 설명의 편의를 위해 감시기(300)의 신호 대 잡음비를 제1 신호 대 잡음비로 정의하고, 불법 수신기(R)의 신호 대 잡음비를 제2 신호 대 잡음비로 정의하여 설명하기로 한다.

[0077] 이때, 감시기(300)는 아래의 수학식을 이용하여 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전속 전력을 최적화하여 불법 신호로부터 복구되는 정보의 감시량을 최대화할 수 있다.

수학식 7

$$
\begin{aligned}
(\mathrm{P}):\ \max_{G_S,P_J}\ & W\log_2\left(1+\gamma_R\left(G_S,P_J\right)\right)\\
\text{s.t.}\ \ & \gamma_M\left(G_S\right)\geq\gamma_R\left(G_S,P_J\right)\\
& \gamma_M\left(G_S\right)\geq\bar{\gamma}_M\\
& \left|\frac{G_S h_{TS}}{\left(1-G_S h_{SS}\right)}\right|^2 P_T+\left|\frac{G_S}{\left(1-G_S h_{SS}\right)}\right|^2\sigma_S^2\leq\bar{P}_S\\
& 0\leq P_J\leq\bar{P}_J
\end{aligned}
$$

[0078]

[0079] 여기서, P_J는 협력 재머(200)의 전송 전력, $\gamma_M(G_S)$은 감시기(300)의 SINR(제1 신호 대 잡음비), $\gamma_R(G_S,P_J)$은 불법 수신기(R)의 SINR(제2 신호 대 잡음비), h_{TS}는 불법 송신기(T)와 스푸핑 중계기(100) 간의 채널 값이다.

[0080] 또한, 첫 번째 조건식은 감시 채널 용량($\gamma_M(G_S)$)이 불법 송신기(R)의 전송 속도보다 높아야 함을 뜻하는 조건식이고, 두 번째 조건식은 감시기(300)가 감시된 정보를 복구하기 위한 최소 요구 SINR 값을 표현하는 조건식이며, 세 번째와 네 번째 조건식은 각각 스푸핑 중계기(100)와 협력 재머(200)의 전송 전력 상한 값에 대한 식이다.

[0081] 수학식 7로부터 스푸핑 중계기(100)의 실질적인 증폭 계수는 $\frac{G_S}{(1-G_S h_{SS})}$ 임을 알 수 있고, 이를 $\Omega_S e^{j\theta_S}$ (여기서, Ω_S는 증폭 계수의 세기(magnitude), θ_S는 증폭 계수의 위상(phase)) 로 정의하면 제1 신호 대 잡음비 및 제2 신호 대 잡음비는 스푸핑 중계기(100)의 증폭 계수의 세기(Ω_S)와 위상(θ_S)으로 표현될 수 있다. 이를 수학식으로 나타내면 다음과 같다.

수학식 8

$$
\gamma_M\left(\Omega_S\right)=\frac{\left|h_{SM}h_{TS}\right|^2\Omega_S^2 P_T}{\left|h_{SM}\right|^2\Omega_S^2\sigma_S^2+\sigma_M^2}
$$

[0082]

수학식 9

$$
\gamma_R\left(\Omega_S,\theta_S,P_J\right)=\frac{\left(\left|h_{TR}\right|^2+2\left|h_{TR}\right|\left|h_{SR}\right|\left|h_{TS}\right|\Omega_S\cos\left(\theta_{TR}-\theta_{SR}-\theta_S-\theta_{TS}\right)+\left|h_{SR}\right|^2\left|h_{TS}\right|^2\Omega_S^2\right)P_T}{\left|h_{SR}\right|^2\Omega_S^2\sigma_S^2+\left|h_{JR}\right|^2 P_J+\sigma_R^2}
$$

[0083]

[0084] 상술한 수학식 8 및 수학식 9를 이용하면, 수학식 7은 다음과 같이 변환될 수 있다.

수학식 10

[0085]
$$
\begin{aligned}
(\mathrm{P}):\ \max_{\Omega_S,\theta_S,P_J}\ & \gamma_R\left(\Omega_S,\theta_S,P_J\right)\\
\text{s.t.}\ \ & \gamma_M\left(\Omega_S\right)\geq\gamma_R\left(\Omega_S,\theta_S,P_J\right)\\
& \gamma_M\left(\Omega_S\right)\geq\bar{\gamma}_M\\
& \left|h_{TS}\right|^2 P_T\Omega_S{}^2+\sigma_S^2\Omega_S{}^2\leq\bar{P}_S\\
& 0\leq P_J\leq\bar{P}_J
\end{aligned}
$$

[0086] 수학식 10을 참조하면, 다른 모든 값들이 고정되어 있을 때 스푸핑 중계기(100)의 증폭 계수($\frac{G_S}{(1-G_S h_{SS})}$)의 위상(θ_S)에 따라 제2 신호 대 잡음비(γ_R) 값이 변한다는 것을 알 수 있다. 그리고, 세 번째 조건식에서 알 수 있듯이, 증폭 계수의 세기(Ω_S) 및 전송 전력은 위상(θ_S)의 변화와는 관계없이 고정된 값을 가짐을 알 수 있다.

[0087] 특히, $\theta_S=\theta_{S,\max}\triangleq\theta_{TR}-\theta_{SR}-\theta_{TS}$ 일 때 γ_R 은 최대화 되고, 스푸핑 신호는 불법 신호와 건설적으로 결합하게 되며, 이는 불법 수신기(R)의 SINR, 다시 말해 제2 신호 대 잡음비를 높이는 효과를 가져온다. 따라서 이때의 경우를 constructive 중계라고 칭한다.

[0088] 반면 그 외 모든 경우인 $\theta_{S,\min}\leq\theta_S<\theta_{S,\max}$, $\theta_{S,\min}\triangleq\theta_{TR}-\theta_{SR}-\theta_{TS}-\pi$ 일 때는 불법 수신기(R)에서 스푸핑 신호는 불법 신호와 파괴적으로 결합되어 불법 수신기(R)의 SINR을 저하시키는 효과를 가져온다. 따라서 이때의 경우를 destructive 중계라고 칭한다.

[0089] 즉, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)은 증폭 계수 및 전송 전력의 크기에 따라 최대 재밍으로 불법 수신기(R)의 신호 대 잡음비를 감소시키는 제1 모드, 재밍 신호 및 스푸핑 신호를 이용하여 불법 수신기(R)의 신호 대 잡음비를 상승시키는 제2 모드 및 재밍 신호 없이 스푸핑 신호만을 이용하여 불법 수신기(R)의 신호 대 잡음비를 상승시키는 제3 모드 중 어느 하나의 동작 모드로 동작할 수 있다. 이와 관련하여, 도 5를 함께 참조하여 설명하기로 한다.

[0090] 도 5는 불법 송신기(T)와 불법 수신기(R) 간의 거리에 따른 최대 정보 감시량의 변화를 나타내는 그래프이다.

[0091] 도시된 바와 같이, 불법 송신기(T)와 불법 수신기(R)의 거리가 충분히 가까운 경우(case 1), 최대 가능한 불법 신호의 전송 속도가 감시 채널 용량보다 훨씬 높기 때문에, 이러한 상황에서는 협력 재머(200)는 재밍 신호를 최대 전력으로 전송할 뿐만 아니라 스푸핑 중계기(100)의 destructive 중계도 함께 작동해야 정보의 감시가 가능함을 알 수 있다.

[0092] 그리고, 불법 송신기(T)와 불법 수신기(R)의 거리가 다소 떨어져 있는 경우(case 2), 스푸핑 중계기(100)에서 destructive 중계를 하지 않더라도 협력 재머(200)의 재밍 신호 만으로도 충분히 불법 신호를 감시할 수 있다.

[0093] 마지막으로, 불법 송신기(T)와 불법 수신기(R)가 비교적 멀리 떨어져 있는 경우(case 3), 불법 신호의 최대 가능한 전송 속도가 도청 채널 용량보다 낮아지게 된다. 이러한 상황에서는 협력 재머(200)는 더 이상 재밍을 하지 않고 오직 스푸핑 중계기(100)의 constructive 중계만을 사용하여 불법 수신기(R)의 SINR을 감시가 가능한 정도까지 높임으로써 정보 감시량을 최대화 할 수 있다.

[0094] 이와 같이, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)은 증폭 계수의 위상이 최대값 이상 최대값 미만($\Theta_{S,\min}\leq\Theta_S^{\star}<\Theta_{S,\max}$)이고 전송 전력이 최대값($P_J^{\star}=P_J$)일 때 제1 모드로 동작하고, 증폭 계수의 위상이 최대값($\Theta_S^{\star}=\Theta_{S,\max}$)이고 재밍 신호의 전송 전력이 $0<P_J^{\star}\leq P_J$ 일 때 제2 모드로 동작하며, 증폭 계수의 위상이 최대값($\Theta_S^{\star}=\Theta_{S,\max}$)이고 전송 전력이 $0(P_J^{\star}=0)$ 일 때 제3 모드로 동작할 수 있다.

[0095] 이때, 감시기(300)는 각 동작 모드에서 정보 감시량이 최대가 되는 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 산출할 수 있다.

[0096] 먼저, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제1 모드로 동작하는 경우, 감시기(300)는 제1 모드에서의 최대 정보 감시량을 갖기 위한 스푸핑 중계기(100)의 증폭 계수를 산출할 수 있다. 이러한 경우, 수학식 10은 다음과 같이 변환될 수 있다.

수학식 11

[0097]
$$
\begin{aligned}
(\mathrm{P}.1): \ \max_{\Omega_S,\theta_S} \ & \gamma_R\left(\Omega_S,\theta_S,\bar{P}_J\right) \\
\text{s.t.} \ & \gamma_M\left(\Omega_S\right)=\gamma_R\left(\Omega_S,\theta_S,\bar{P}_J\right) \\
& \gamma_M\left(\Omega_S\right)\geq\bar{\gamma}_M \\
& \left|h_{TS}\right|^2 P_T\Omega_S{}^2+\sigma_S^2\Omega_S{}^2\leq\bar{P}_S
\end{aligned}
$$

[0098] 이때, 수학식 11의 첫 번째 조건식을 정리하면 다음과 같다

수학식 12

[0099]
$$
\begin{aligned}
\cos\left(\theta_{TR}-\theta_{SR}-\theta_S-\theta_{TS}\right) &= \frac{\dfrac{\left|h_{SM}\right|^2\Omega_S^2\left|h_{TS}\right|^2}{\left|h_{SM}\right|^2\Omega_S^2\sigma_S^2+\sigma_M^2}\left(\left|h_{SR}\right|^2\Omega_S^2\sigma_S^2+\left|h_{JR}\right|^2\bar{P}_J+\sigma_R^2\right)-\left|h_{TR}\right|^2-\left|h_{SR}\right|^2\left|h_{TS}\right|^2\Omega_S^2}{2\left|h_{TR}\right|\left|h_{SR}\right|\left|h_{TS}\right|\Omega_S} \\
&\triangleq\eta\left(\Omega_S\right)
\end{aligned}
$$

[0100] 여기서, 좌변($\cos(\cdot)$)의 범위가 $-1\leq\cos(\cdot)\leq 1$인 성질과 첫 번째 조건식의 등호에 따라 제2 신호 대 잡음비(γ_R)를 최대화 하는 것은 제1 신호 대 잡음비(γ_M)를 최대화 하는 것과 같다는 성질을 이용하면 수학식 11는 다음과 같이 간략화 될 수 있다.

수학식 13

[0101]
$$
\begin{aligned}
(\mathrm{P}.1): \ \max_{\Omega_S} \ & \Omega_S \\
\text{s.t.} \ & -1\leq\eta\left(\Omega_S\right)\leq 1 \\
& \sqrt{\frac{\bar{\gamma}_M\sigma_M^2}{\left(\left|h_{TS}\right|^2P_T-\bar{\gamma}_M\sigma_S^2\right)\left|h_{SM}\right|^2}}\leq\Omega_S\leq\sqrt{\frac{\bar{P}_S}{\left|h_{TS}\right|^2P_T+\sigma_S^2}}
\end{aligned}
$$

[0102] 수학식 13의 첫 번째 조건식을 만족하는 Ω_S의 범위는 3차 방정식의 근의 공식을 사용해 닫힌 형태(closed-form) 로 쉽게 구할 수 있기 때문에, 수학식 13의 최적해 $\Omega_S^\star$는 첫 번째 조건식을 만족하는 Ω_S의 범위와 두 번째 조건식의 범위의 교집합 중 가장 큰 Ω_S이 됨을 알 수 있다.

[0103] 그리고, 감시기(300)는 산출된 $\Omega_S^\star$를 통해 $\Theta_S^\star$의 최적해 또한 다음과 같은 닫힌 형태(closed-form)로 산출할 수 있다.

수학식 14

[0104]
$$\theta_S^{\bigstar} = \theta_{TR} - \theta_{SR} - \theta_{TS} - \cos^{-1}\left(\eta\left(\Omega_S^{\bigstar}\right)\right)$$

[0105] 결론적으로, 감시기(300)는 산출된 세기($\Omega_S^{\bigstar}$) 및 위상($\Theta_S^{\bigstar}$)을 갖는 최적의 증폭 계수($G_S^{\bigstar}$)을 산출할 수 있다. 이때, 상술한 바와 같이 제1 모드에서의 재밍 신호의 전송 전력(PJ)는 최대 전송 전력으로 고정되어 있으므로, 제1 모드에서의 최적 전송 전력은 항상 일정한 값을 가질 수 있다.

[0106] 다음으로, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제2 모드로 동작하는 경우, 감시기(300)는 제2 모드에서의 최대 정보 감시량을 갖기 위한 협력 재머(200)의 전송 전력을 산출할 수 있다. 이러한 경우, 수학식 10은 다음과 같이 변환될 수 있다.

수학식 15

[0107]
$$\begin{aligned}(\mathrm{P.2}):\ \max_{\Omega_S, P_J}\ & \gamma_R\left(\Omega_S, \theta_{S,\max}, P_J\right) \\ \text{s.t.}\ & \gamma_M\left(\Omega_S\right) = \gamma_R\left(\Omega_S, \theta_{S,\max}, P_J\right) \\ & \gamma_M\left(\Omega_S\right) \geq \bar{\gamma}_M \\ & \left|h_{TS}\right|^2 P_T \Omega_S^{\ 2} + \sigma_S^2 \Omega_S^{\ 2} \leq \bar{P}_S \\ & 0 \leq P_J \leq \bar{P}_J\end{aligned}$$

[0108] 또한, 수학식 15의 첫 번째 조건식을 정리하면 다음과 같다.

수학식 16

[0109]
$$\begin{aligned}P_J = & \left(\left|h_{TR}\right|^2 + 2\left|h_{TR}\right|\left|h_{SR}\right|\left|h_{TS}\right|\Omega_S \cos\left(\theta_{TR} - \theta_{SR} - \theta_{S,\max} - \theta_{TS}\right) + \left|h_{SR}\right|^2\left|h_{TS}\right|^2\Omega_S^2\right)\frac{\left|h_{SM}\right|^2\Omega_S^2\sigma_S^2 + \sigma_F^2}{\left|h_{SM}\Omega_S h_{TS}\right|^2\left|h_{JR}\right|^2} \\ & - \frac{\left|h_{SR}\right|^2\Omega_S^2\sigma_S^2}{\left|h_{JR}\right|^2} - \frac{\sigma_R^2}{\left|h_{JR}\right|^2} \\ \triangleq & \delta\left(\Omega_S\right)\end{aligned}$$

[0110] 한편, 협력 재밍(200)의 전송 전력(P_J)의 범위가 $0 \leq P_J \leq \bar{P}_J$인 성질과 첫 번째 조건식의 등호에 따라 제2 신호 대 잡음비(γ_R)를 최대화 하는 것은 제1 신호 대 잡음비(γ_M)를 최대화 하는 것과 같다는 성질을 이용하면 수학식 15(P.2)는 다음의 문제로 간략화 할 수 있다.

수학식 17

$$(\mathrm{P.2}):\ \max_{\Omega_S}\ \Omega_S$$
$$\text{s.t.}\quad 0 \le \delta(\Omega_S) \le \bar{P}_J$$
$$\sqrt{\frac{\bar{\gamma}_M \sigma_M^2}{\left(|h_{TS}|^2 P_T - \bar{\gamma}_M \sigma_S^2\right)|h_{SM}|^2}} \le \Omega_S \le \sqrt{\frac{\bar{P}_S}{|h_{TS}|^2 P_T + \sigma_S^2}}$$

[0111]

[0112] 수학식 17의 첫 번째 조건식을 만족하는 Ω_S의 범위는 3차 방정식의 근의 공식을 사용해 closed-form으로 쉽게 구할 수 있기 때문에 수학식 11의 최적의 해 $\Omega_S^\star$는 첫 번째 조건식을 만족하는 Ω_S의 범위와 두 번째 조건식의 범위의 교집합 중 가장 큰 Ω_S이 됨을 알 수 있다.

[0113] 그리고, 감시기(300)는 산출된 $\Omega_S^\star$를 통해 전송 전력의 최적해 또한 $P_J^\star = \delta\left(\Omega_S^\star\right)$를 통해 closed-form으로 간단하게 계산할 수 있다. 여기서, 상술한 바와 같이 제2 모드에서는 증폭 계수는 항상 최대값이므로, 제2 모드에서의 증폭 계수의 위상 최적해($\Theta_S^\star$)는 $\Theta_{S,\max}$이다.

[0114] 마지막으로, 다음으로, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제3 모드로 동작하는 경우, 감시기(300)는 제3 모드에서의 최대 정보 감시량을 갖기 위한 스푸핑 중계기(100)의 증폭 계수를 산출할 수 있다.

[0115] 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제3 모드로 동작하는 경우, 스푸핑 중계기(100)의 증폭 계수의 위상 최적해($\Theta_S^\star$)는 $\Theta_{S,\max}$로 고정되어 있고, 재밍 신호는 발생되지 않기 때문에 재밍 신호의 전송 전력은 0일 수 있으며, 이에 따라 수학식 10은 다음과 같이 변환될 수 있다.

수학식 18

$$(\mathrm{P.3}):\ \max_{\Omega_S}\ \gamma_R\left(\Omega_S, \theta_{S,\max}, 0\right)$$
$$\text{s.t.}\quad \gamma_M\left(\Omega_S\right) \ge \gamma_R\left(\Omega_S, \theta_{S,\max}, 0\right)$$
$$\gamma_M\left(\Omega_S\right) \ge \bar{\gamma}_M$$
$$|h_{TS}|^2 P_T \Omega_S^{\,2} + \sigma_S^2 \Omega_S^{\,2} \le \bar{P}_S$$

[0116]

[0117] 수학식 18을 통해 첫 번째 조건식을 만족하는 Ω_S의 범위는 3차 방정식의 근의 공식을 사용해 closed-form으로 쉽게 구할 수 있고 두 번째와 세 번째 조건식을 만족하는 Ω_S의 범위 역시 $\sqrt{\frac{\bar{\gamma}_M \sigma_M^2}{\left(|h_{TS}|^2 P_T - \bar{\gamma}_M \sigma_S^2\right)|h_{SM}|^2}} \le \Omega_S \le \sqrt{\frac{\bar{P}_S}{|h_{TS}|^2 P_T + \sigma_S^2}}$로 간단하게 closed-form으로 표현할 수 있다.

[0118] 한편, 목적 함수 γ_R은 1차 미분을 통해 $\Omega_S < |h_{TS}|\sigma_R^2 / \left(|h_{TR}||h_{SR}|\sigma_S^2\right)$ 일 때는 단조 증가 성질을 보이다

가 $\Omega_S \geq |h_{TS}|\sigma_R^2 / \left(|h_{TR}||h_{SR}|\sigma_S^2\right)$ 일 때는 단조 감소 성질을 보임을 알 수 있다.

[0119] 따라서, $\Omega_S = |h_{TS}|\sigma_R^2 / \left(|h_{TR}||h_{SR}|\sigma_S^2\right)$ 일 때 γ_R는 최대값이 되지만 수식적인 분석을 통해 해당하는 해는 수학식 18의 첫 번째 조건식에 부합하지 않고 수학식 18의 모든 조건식을 만족하는 Ω_S의 범위보다 항상 크다는 것을 알 수 있다.

[0120] 결론적으로, 수학식 18의 최적의 해 $\Omega_S^\star$는 모든 조건식을 만족하는 Ω_S의 범위 중 가장 큰 Ω_S이 됨을 알 수 있으며, 상술한 바와 같이 이 범위들은 모두 closed-form으로 계산할 수 있다.

[0121] 요약하면, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)은 불법 신호를 감시하는 과정에서 스푸핑 중계기(100)와 협력 재머(200)를 이용하여 불법 수신기의 신호 대 잡음비를 저하시키는 제1 모드, 스푸핑 중계기(100)를 이용하여 불법 수신기의 신호 대 잡음비를 상승시키는 제2 모드 및 스푸핑 중계기(100)를 이용하여 불법 수신기의 신호 대 잡음비를 상승시키는 제3 모드 중 어느 하나의 동작 모드로 동작할 수 있다.

[0122] 이때, 감시기(300)는 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제1 모드, 제2 모드 및 제3 모드에서 동작할 때, 각각의 동작 모드에서 정보 감시량이 최대가 되는 증폭 계수 또는 전송 전력을 산출할 수 있다. 이후, 감시기(300)는 제1 모드, 제2 모드 및 제3 모드 중 정보 감시량이 최대가 되는 어느 하나의 동작 모드를 선택하고, 선택된 모드에서 산출된 증폭 계수 또는 전송 전력을 정보의 감시량이 최대가 되는 증폭 계수 및 전송 전력으로 선택할 수 있다. 최종적으로, 감시기(300)는 선택된 증폭 계수를 스푸핑 중계기(100)로 전달하여 스푸핑 중계기(100)가 산출된 증폭 계수에 따라 불법 신호를 증폭시켜 중계하도록 제어하거나, 선택된 전송 전력을 협력 재머(200)로 전달하여 협력 재머(200)가 산출된 전송 전력에 따라 재밍 신호를 전송하도록 제어할 수 있다.

[0123] 따라서, 감시기(300)는 상술한 수학식 10을 통해 구한 최적의 해 $\Omega_S^\star, \theta_S^\star$로 원래의 스푸핑 중계기(100)의 증폭 계수의 최적의 값을 $$G_S^\star = \frac{\Omega_S^\star e^{j\theta_S^\star}}{\left(1+\Omega_S^\star e^{j\theta_S^\star} h_{SS}\right)}$$ 로 복구할 수 있다.

[0124] 도 6은 본 발명의 일 실시예에 따른 협력 재밍과 스푸핑을 이용한 감시 방법의 개략적인 흐름이 도시된 순서도이다.

[0125] 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 방법은 상술한 도 1에 도시된 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)에 의해 수행될 수 있으며, 협력 재밍과 스푸핑을 이용한 감시 시스템을 구성하는 각각의 구성 요소들은 후술하는 협력 재밍과 스푸핑을 이용한 감시 방법의 각 단계를 수행하기 위한 소프트웨어(애플리케이션)이 설치될 수 있다.

[0126] 먼저, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)을 구성하는 스푸핑 중계기(100), 협력 재머(200) 및 감시기(300)는 불법 송신기(T)와 불법 수신기(R) 간 주고받는 불법 신호를 감지하기 위한 감시 채널을 생성하고, 생성된 각각의 채널 상태를 추정할 수 있다(610).

[0127] 즉, 스푸핑 중계기(100) 및 협력 재머(200)는 정보의 감시를 위한 적절한 위치에 배치될 수 있다. 구체적으로, 스푸핑 중계기(100)는 불법 송신기(T)로부터 발생되는 불법 신호를 감지할 수 있으면서 불법 수신기(R)로 스푸핑 신호를 전송할 수 있는 위치에 배치될 수 있다. 그리고, 협력 재머(200)는 감시기(300)는 스푸핑 중계기(100) 및 협력 재머(200)와 통신이 가능한 위치에 배치될 수 있다. 이러한 경우, 스푸핑 중계기(100)와 감시기(300), 스푸핑 중계기(100)와 협력 재머(200), 협력 재머(200)와 감시기(300) 사이에는 각각의 통신 채널이 형성될 수 있으며, 스푸핑 중계기(100), 협력 재머(200) 및 감시기(300)는 각 통신 채널의 잡음 간섭 등과 같은 채널 품질을 추정할 수 있다.

[0128] 다음으로, 협력 재머(200)는 불법 송신기와 불법 수신기간 채널 품질을 변경시키기 위한 재밍 신호를 생성하고(620), 스푸핑 중계기(100), 협력 재머(200) 및 감시기(300)는 생성된 재밍 신호 및 서로 간에 형성된 채널 정보를 서로 공유할 수 있다(630).

[0129] 즉, 스푸핑 중계기(100), 협력 재머(200) 및 감시기(300) 사이에는 같은 재밍 신호 묶음과 재밍 신호 전송 순서

를 공유하고 있으며, 이러한 사전 협력을 통해 감시기(300)와 스푸핑 중계기(100)는 도청 중 협력 재머(200)로부터 발생하는 재밍 간섭을 상쇄할 수 있다. 또한, 효과적인 채널 측정 방법을 통해 감시기(300), 스푸핑 중계기(100) 그리고 협력 재머(200)는 모든 채널 정보를 미리 공유할 수 있다.

[0130] 이후, 감시기(300)는 본 발명에 따른 협력 재밍과 스푸핑을 이용한 감시 시스템(1000)이 제1 모드, 제2 모드 및 제3 모드로 동작할 때, 각각의 동작 모드에서 스푸핑 중계기(100)로부터 수신된 불법 신호를 복구하여 획득되는 정보의 감시량이 최대가 되는 증폭 계수 및 전송 전력을 산출할 수 있다(640).

[0131] 상술한 바와 같이, 본 발명에 따른 협력 재밍과 스푸핑을 이용한 무선 통신 채널 감시 시스템(1000)은 감시 채널 용량 및 불법 송신기(T)의 전송 속도를 비교한 결과에 따라, 협력 재머(200)가 최대 전력을 재밍 신호를 전송하면서 스푸핑 중계기(100)가 destructive 중계를 수행하는 제1 모드, 협력 재머(200)가 최대 가용 전력 이하의 재밍 신호를 전송하면서 스푸핑 중계기(100)가 constructive 중계를 수행하는 제2 모드 및 협력 재머(200)가 재밍 신호를 전송하지 않고 스푸핑 중계기(100)만 constructive 중계를 수행하는 제3 모드 중 어느 하나의 모드로 동작할 수 있다.

[0132] 이때, 감시기(300)는 각각의 동작 모드에서 정보의 감시량이 최대가 되는 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 산출할 수 있다. 이에 대한 구체적은 과정은 상술하였으므로, 반복되는 설명은 생략하기로 한다.

[0133] 감시기(300)는 정보 감시량이 최대가 되는 어느 하나의 동작 모드를 선택하고, 선택된 동작 모드에서 산출된 정보의 감시량이 최대가 되는 증폭 계수 및 전송 전력을 선택할 수 있다(650).

[0134] 최종적으로, 감시기(300)는 선택된 최적의 증폭 계수를 스푸핑 중계기(100)로 전송하고, 선택된 최적은 전송 전력을 협력 재머(200)로 전송(650)함으로써, 복구되는 정보의 감시량이 최대가 되도록 스푸핑 중계기(100)의 증폭 계수 및 협력 재머(200)의 전송 전력을 실시간으로 가변시킬 수 있다(660). 다시 말해, 스푸핑 중계기(100)는 감시기(300)로부터 설정된 증폭 계수에 따라 스푸핑 신호를 증폭시켜 불법 수신기(R)로 전송하고, 협력 재머(200)는 감시기(300)로부터 설정된 전송 전력에 따라 재밍 신호를 불법 수신기(R)로 전송함으로써, 감시기(300)에서 획득되는 정보의 감시량이 최대가 될 수 있다.

[0135] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0137] 1000: 협력 재밍과 스푸핑을 이용한 감시 시스템

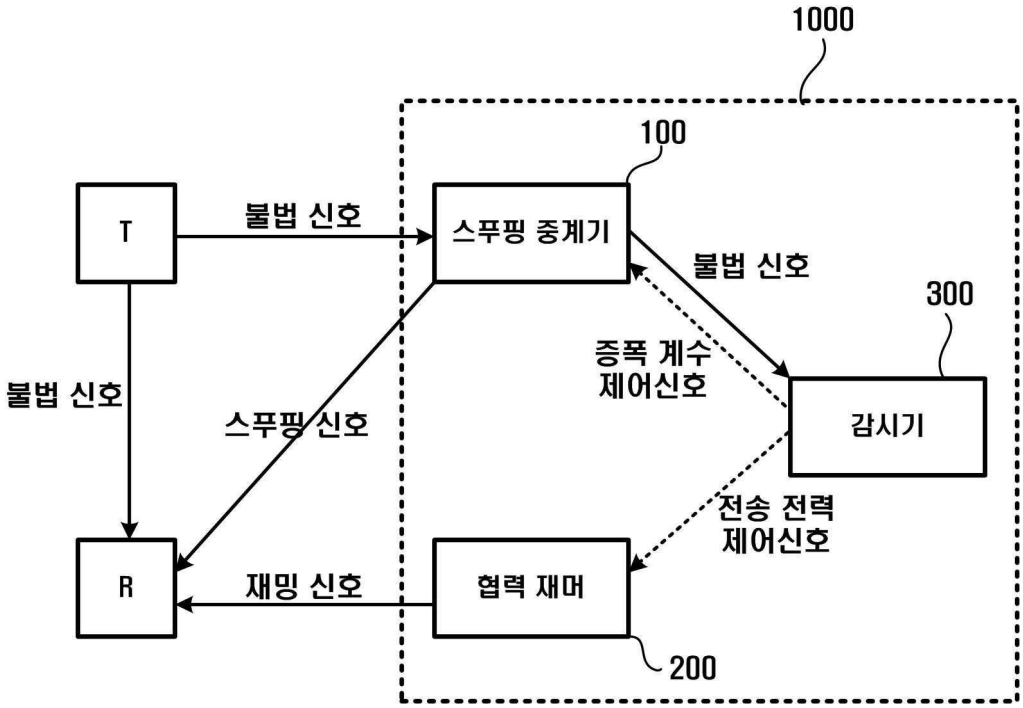
100: 스푸핑 중계기

200: 협력 재밍

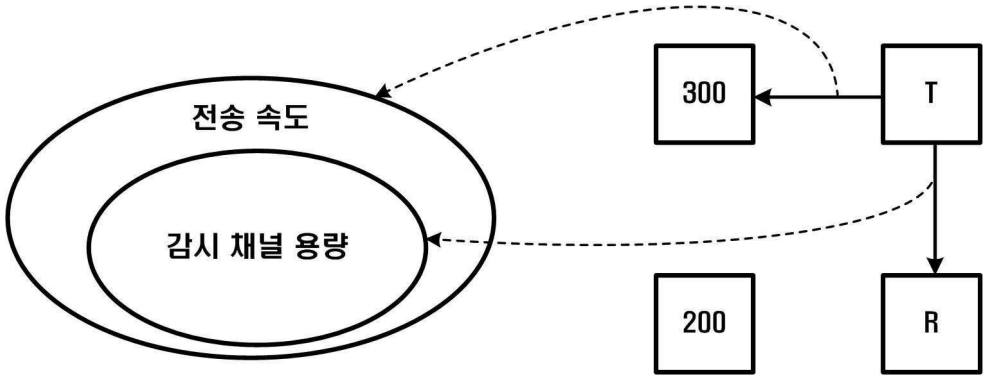
300: 감시기

도면

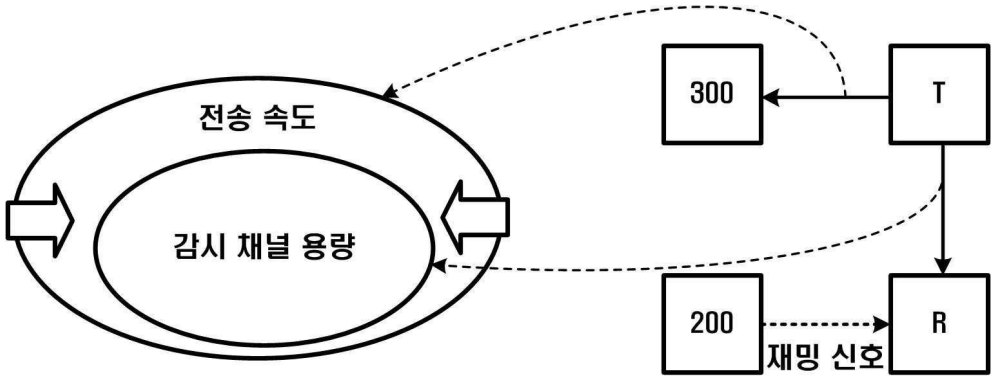
도면1



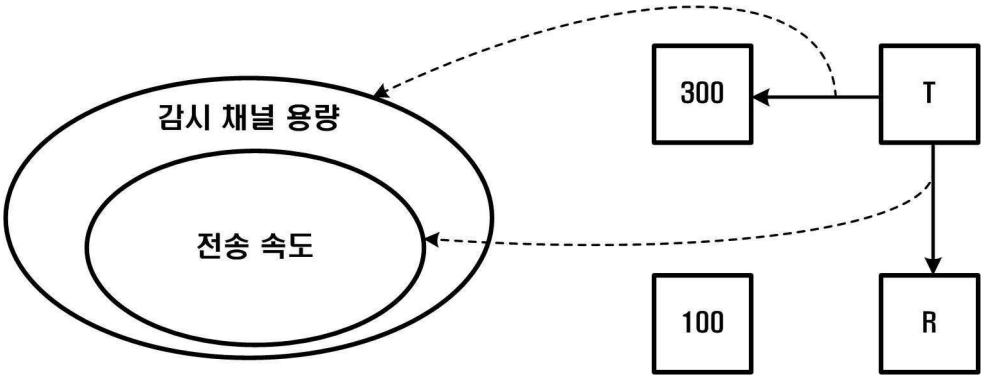
도면2a



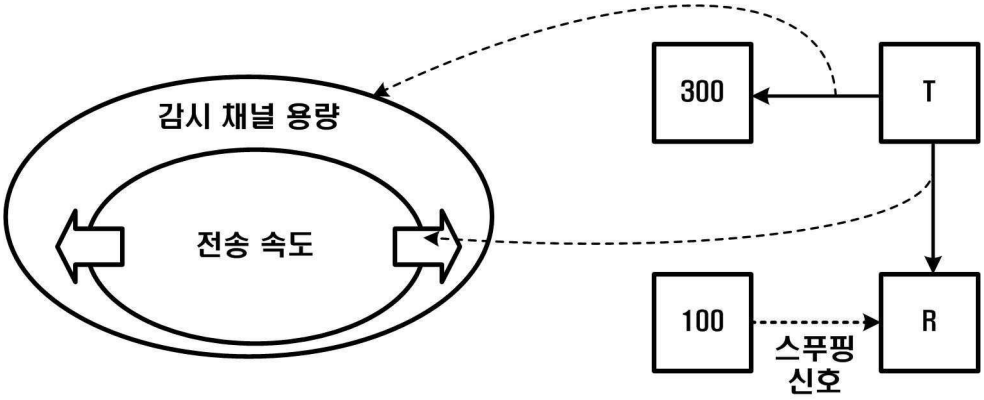
도면2b



도면3a

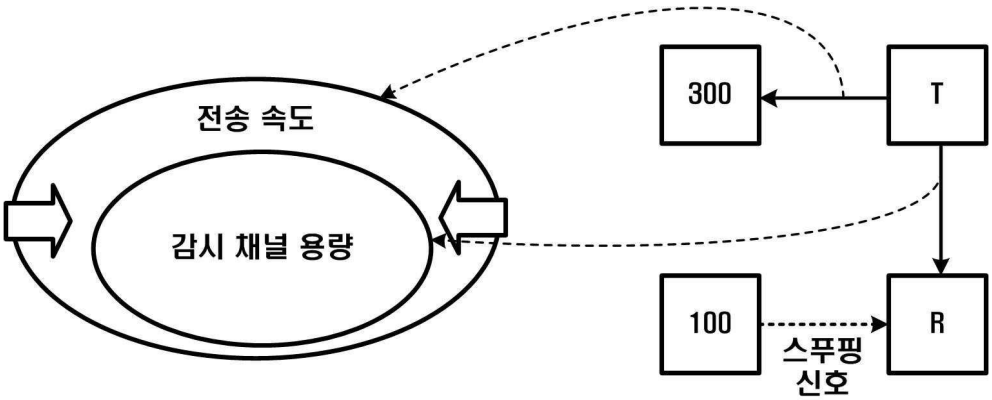


도면3b



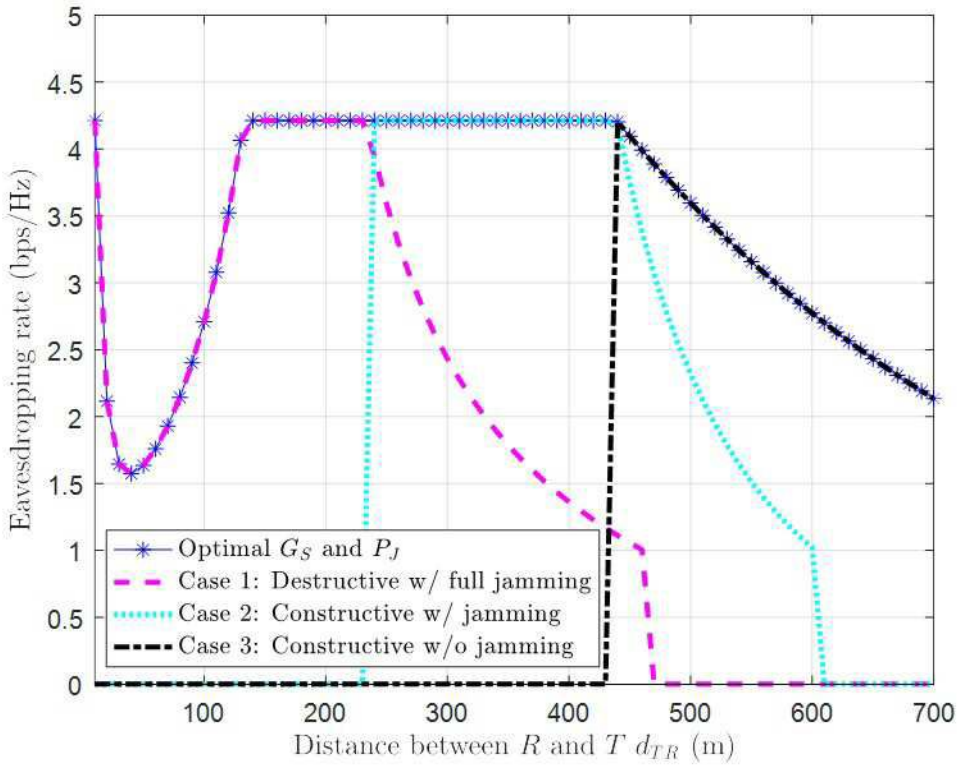
constructive relay

도면4

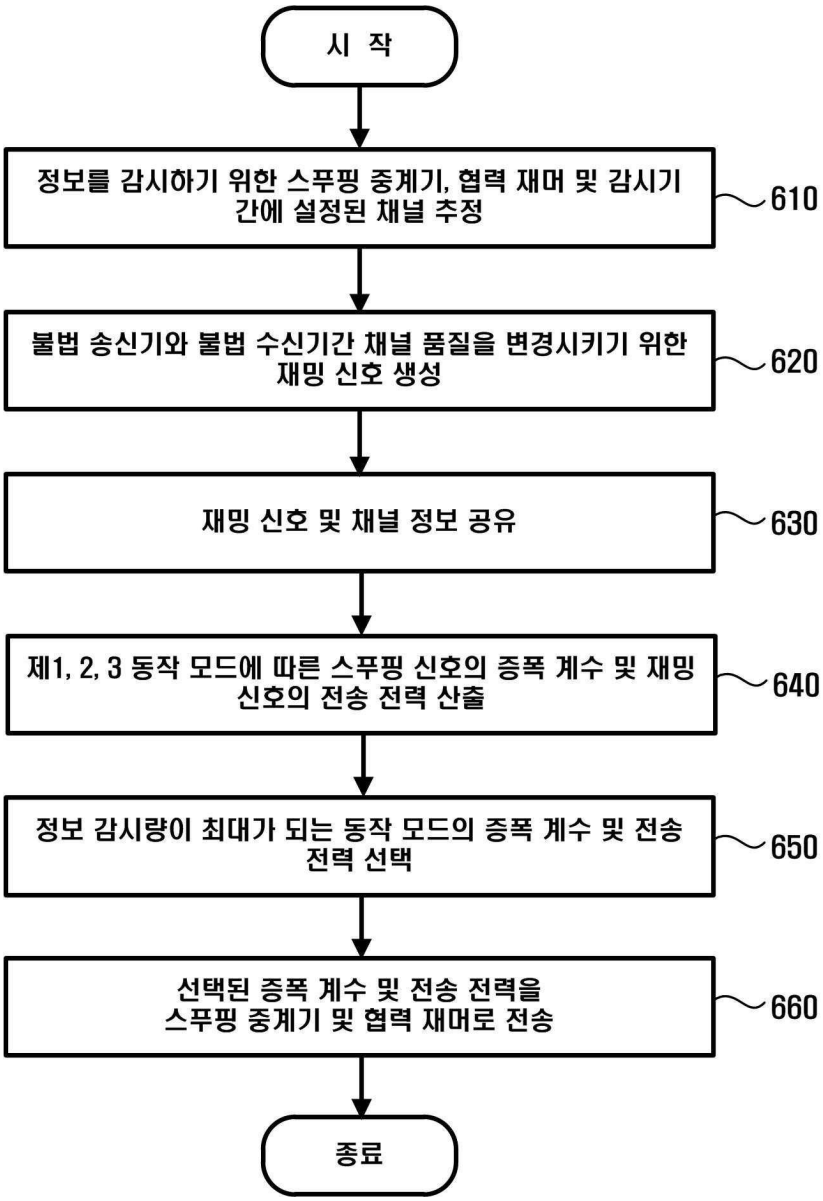


destructive relay

도면5


Eavesdropping rate (bps/Hz)
Distance between R and T d_{TR} (m)
Optimal G_S and P_J
Case 1: Destructive w/ full jamming
Case 2: Constructive w/ jamming
Case 3: Constructive w/o jamming
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
100
200
300
400
500
600
700

도면6


시 작
정보를 감시하기 위한 스푸핑 중계기, 협력 재머 및 감시기 간에 설정된 채널 추정
610
불법 송신기와 불법 수신기간 채널 품질을 변경시키기 위한 재밍 신호 생성
620
재밍 신호 및 채널 정보 공유
630
제1, 2, 3 동작 모드에 따른 스푸핑 신호의 증폭 계수 및 재밍 신호의 전송 전력 산출
640
정보 감시량이 최대가 되는 동작 모드의 증폭 계수 및 전송 전력 선택
650
선택된 증폭 계수 및 전송 전력을 스푸핑 중계기 및 협력 재머로 전송
660
종료