(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년12월11일
(11) 등록번호 10-2054715
(24) 등록일자 2019년12월05일

(51) 국제특허분류(Int. Cl.)
H04W 12/00 (2019.01) *H04W 40/12* (2009.01)
H04W 40/22 (2009.01) *H04W 84/18* (2009.01)
(52) CPC특허분류
H04W 12/009 (2019.01)
H04W 12/00506 (2019.01)
(21) 출원번호 10-2019-0047123
(22) 출원일자 2019년04월23일
심사청구일자 2019년04월23일
(56) 선행기술조사문헌
KR1020090037719 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 미추홀구 인하로 100(용현동, 인하대학교)
(72) 발명자
곽경섭
인천광역시 연수구 해돋이로84번길 10(송도동, 송도풍림아이원6단지아파트)
아니쉬
인천광역시 미추홀구 경인남길102번길 95(용현동, 경기주택)
(74) 대리인
양성보

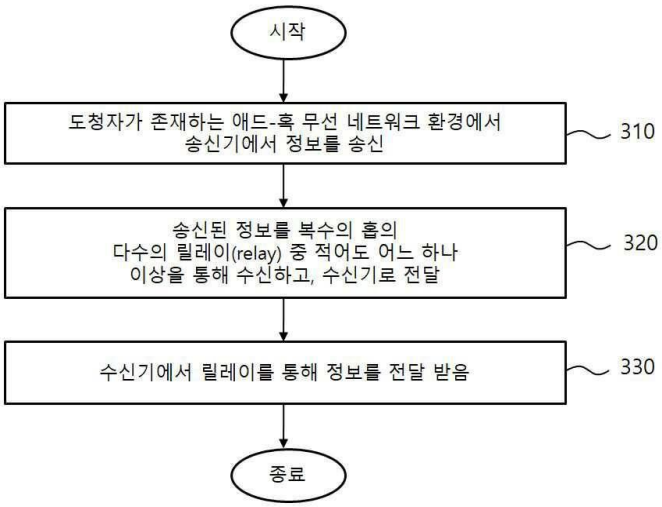
전체 청구항 수 : 총 7 항 심사관 : 이준석

(54) 발명의 명칭 **애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템**

(57) 요 약

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템이 제시된다. 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법은, 도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계; 송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계; 및 상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계를 포함하고, 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달할 수 있다.

대 표 도



(52) CPC특허분류
H04W 40/12 (2013.01)
H04W 40/22 (2013.01)
H04W 84/18 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711093227 (세부과제번호 2014-1-00729-006)
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 IT연구센터 육성·지원
연구과제명 [IITP-ezbaro][정부] 스마트한 주파수 이용을 위한 스펙트럼 및 전파기술(6차년도)
기 여 율 1/2
주관기관 인하대학교 산학협력단
연구기간 2019.01.01 ~ 2019.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711086535 (세부과제번호 2017R1A2B2012337)
부처명 과학기술정보통신부
연구관리전문기관 한국연구재단
연구사업명 중견연구
연구과제명 [Ezbaro] 나노 인체영역네트워크 핵심기술 연구: 분자-전자파 나노통신 하이브리드 메카니즘 규명
기 여 율 1/2
주관기관 인하대학교 산학협력단
연구기간 2019.03.01 ~ 2020.02.29
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계; 및

상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계

를 포함하고,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며, 각 홉에서 상기 수신기와 상기 도청자의 순간 채널 조건에 기초하여 상기 각 릴레이 클러스터에서 홉간(hop-by-hop) 최적의 보안 릴레이를 선택하여 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송하는 것

을 특징으로 하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 2

삭제

청구항 3

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계; 및

상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계

를 포함하고,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며,

상기 릴레이는,

디코드 및 포워드(Decode and Forward, DF) 릴레이이고, 메인 채널이라고 불리는 무선 페이딩 채널을 통해 재전송하기 이전에, 앞의 노드에서 디지털 방식으로 수신된 신호를 디코딩하고 다시 인코딩하여 도청을 방지하는 것

을 특징으로 하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 4

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로

전달하는 단계; 및

상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계

를 포함하고,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

각 홉에서의 메인 채널의 순간 신호대잡음비(Signal to Noise Ratio, SNR)와 도청자 채널의 순간 신호대잡음비(SNR)를 기반으로 메인 채널의 순간 용량에서 도청 채널의 순간 용량을 차감하여 비밀유지 용량 확률(secrecy capacity probability)을 도출하는 단계

를 포함하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 5

제4항에 있어서,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

상기 각 홉에서 비밀유지 신호대잡음비(SNR)의 누적분포함수(CDF)를 산정하는 단계; 및

상기 각 홉에서 최대의 상기 비밀유지 신호대잡음비(SNR)를 갖는 릴레이를 선택하는 단계

를 더 포함하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 6

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계; 및

상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계

를 포함하고,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

비밀유지 성과를 정량화하도록 순간 엔드 투 엔드 전송 속도가 주어진 임계 비밀유지 속도(Rs) 아래로 떨어질 확률인 비밀유지 아웃티지 확률(probability of secrecy outage)을 도출하는 단계

를 포함하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 7

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로

전달하는 단계; 및

상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계

를 포함하고,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며,

상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는,

알고리즘을 이용하여 보안 다중홉 라우팅 정책을 수행하는 단계

를 포함하고,

상기 알고리즘을 이용하여 보안 다중홉 라우팅 정책을 수행하는 단계는,

상기 홉의 수 및 각 릴레이 클러스터 릴레이 수를 설정하는 단계;

각 홉에서 선택된 릴레이 노드의 인덱스 r_k^* 를 정의하는 단계;

$r_0^* = A$ 및 $r_K^* = B$로 초기화하는 단계;

각각의 홉 k = 1, ... , K-2에서 선택된 최대 보안유지 릴레이를 구하는 단계;

홉 K-1에서, 가장 큰 $\gamma_{S,r_{k-2}^*,r}^{(K-1)}$ 을 경로로 선택하는 대신 $r_{k-1}^* = \max_{r=1,\ldots,N} min(\gamma_{S,r_{k-2}^*,r}^{(K-1)}, \gamma_{S,r,r_k^*}^{(K)})$ 로 조인트 릴레이를 선택하는 단계; 및

최적의 비밀유지 릴레이 $\{r_k^*\}$를 결정하는 단계

를 포함하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법.

청구항 8

애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템에 있어서,

도청자가 존재하는 애드-혹 무선 네트워크 환경에서 정보를 송신하는 송신기;

송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 중간 클러스터; 및

상기 릴레이를 통해 정보를 전달 받는 수신기

를 포함하고,

상기 중간 클러스터는,

복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달하며, 각 홉에서 상기 수신기와 상기 도청자의 순간 채널 조건에 기초하여 상기 각 릴레이 클러스터에서 홉간(hop-by-hop) 최적의 보안 릴레이를 선택하여 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송하는 것

을 특징으로 하는, 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템.

발명의 설명

기 술 분 야

[0001] 아래의 실시예들은 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 무선 네트워크 보안을 위하여 전통적인 암호화 기술(cryptographic technique)의 대안으로 정보 이론적 비밀 기반의 물리계층(physical layer, PHY) 보안이 최근 대두되고 있다.

[0003] 기존에 무선 다중홉 링크에 대한 포인트 투 포인트 에러 프리 링크를 기반으로 다양한 라우팅 프로토콜이 제안되었다. 그러나 이러한 프로토콜은 무선 채널의 확률론적 행동과 방송 특성을 염두에 두고 모델링한 것이 아니다. 이 한계를 극복하기 위해, 채널 인식 라우팅 전략을 조사하고 라우팅 아웃티지의 가능성을 성능 평가 지표로 고려할 수 있다. 특히, 각 홉에서 복수의 릴레이로 구성된 다중홉 네트워크에 대한 라우팅 전략을 제공하여 릴레이들 간의 협력에 의해 제공되는 다양성 이득을 달성할 수 있다. 협력적 네트워크는 그에 의해 제공되는 다양성 이득으로 꽤 인기 있다. 그러나 이러한 작업들 중 어느 것도 물리계층(PHY) 보안에서 분석을 고려하지 않았다. 정보-이론적 제약에 기초한 무조건적 보안으로 무선 네트워크를 보호하는 것에 대한 합의가 점점 높아지고 있기 때문에, 오늘날 많은 연구 작업들은 물리계층 보안을 조사의 필수적인 기준으로 간주하고 있다.

[0004] 기존의 암호 접근법은 큰 숫자의 소인수분해 및 조건부 보안을 초래하는 이산 대수 문제와 같은 특정 수학적 함수의 난해성에 기초한다. 암호 접근법과 달리, 물리계층 보안은 간섭, 잡음, 페이딩 채널의 시간 변동 특성 등과 같은 무선 채널의 불확실한 속성을 이용함으로써 정보 이론적으로 완벽한 비밀유지를 달성하는 다른 패러다임이다. 더욱이 적절한 채널 코딩 기법과 신호 처리 설계는 비밀키 없이도 기밀 메시지를 전송할 수 있게 한다. 완벽한 비밀유지는 모든 비밀 메시지 X와 비밀 메시지에 대한 도청자의 관찰 Y에 대하여, 확률(Pr)을 정의할 때에 Pr(XIY) = Pr(X)이다. 기존의 연구에서는 도청자가 도청 채널을 저하시켰을 때에 비밀 메시지가 양의 속도로 전송될 수 있기 때문에 완벽한 비밀유지가 가능하다는 것을 제시하였다. 도청 채널이 메인 채널에 비해 평균 신호대잡음비(Signal to Noise Ratio, SNR)가 더 우수함에도 불구하고 완벽한 비밀유지의 존재는 페이딩 채널 하에서 보여졌다.

[0005] 물리계층 보안을 개선하기 위한 대표적인 방법은 다중 입력 다중 출력(Multiple Input Multiple Output, MIMO), 다중 사용자 다양성 및 협력적 다양성과 같은 몇 가지 다양성 기법의 이용을 포함한다. 이들 작업의 대부분은 단일 송신기와 단일 또는 복수의 합법적인 수신기와 도청자로 구성된 작은 네트워크와 2개의 홉 릴레이 시스템을 생성하는 릴레이 노드로 구성된다. 게임 이론과 확률론적 기하학적 구조를 사용하여 정보 보안 제약이 있는 다중홉 네트워크에서 몇 가지 작업이 수행되었다. 물리계층 보안이 가능한 다중홉 시스템은 각 홉에서 단일 디코드 및 포워드(Decode and Forward, DF) 릴레이를 지원하여 제안된다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) Royer E M, Toh C K. A review of current routing protocols for ad hoc mobile wireless networks[J]. IEEE Personal Communications, 1999, 6(2):46-55.

발명의 내용

해결하려는 과제

[0007] 실시예들은 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템에 관하여 기술하며, 보다 구체적으로 다중홉(multi-hop) 무선 네트워크에서 라우팅 기법과 연계한 물리계층 보안 방법을 제공하는 기술을 제공한다.

[0008] 실시예들은 도청자(eavesdropper)가 존재하는 애드-혹 무선 네트워크 환경에서 각 홉에 다수의 릴레이(relay)를 설치하여 홉간 최적의 릴레이를 선택함으로써, 송수신기 간의 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송할 수 있는 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템을 제공하는데 있다.

과제의 해결 수단

[0009] 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법은, 도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계; 송신된 상기 정보를 복수의 홉의 다

수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계; 및 상기 수신기에서 상기 릴레이를 통해 정보를 전달 받는 단계를 포함하고, 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달할 수 있다.

[0010] 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 각 홉에서 상기 수신기와 상기 도청자의 순간 채널 조건에 기초하여 상기 각 릴레이 클러스터에서 홉간(hop-by-hop) 최적의 보안 릴레이를 선택하여 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송할 수 있다.

[0011] 상기 릴레이는, 디코드 및 포워드(Decode and Forward, DF) 릴레이이고, 메인 채널이라고 불리는 무선 페이딩 채널을 통해 재전송하기 이전에, 앞의 노드에서 디지털 방식으로 수신된 신호를 디코딩하고 다시 인코딩하여 도청을 방지할 수 있다.

[0012] 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 각 홉에서의 메인 채널의 순간 신호대잡음비(Signal to Noise Ratio, SNR)와 도청자 채널의 순간 신호대잡음비(SNR)를 기반으로 메인 채널의 순간 용량에서 도청 채널의 순간 용량을 차감하여 비밀유지 용량 확률(secrecy capacity probability)을 도출하는 단계를 포함할 수 있다.

[0013] 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 상기 각 홉에서 비밀유지 신호대잡음비(SNR)의 누적분포함수(CDF)를 산정하는 단계; 및 상기 각 홉에서 최대의 상기 비밀유지 신호대잡음비(SNR)를 갖는 릴레이를 선택하는 단계를 더 포함할 수 있다.

[0014] 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 비밀유지 성과를 정량화하도록 순간 엔드 투 엔드 전송 속도가 주어진 임계 비밀유지 속도(Rs) 아래로 떨어질 확률인 비밀유지 아웃티지 확률(probability of secrecy outage)을 도출할 수 있다.

[0015] 상기 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계는, 알고리즘을 이용하여 보안 다중홉 라우팅 정책을 수행하는 단계를 포함하고, 상기 알고리즘을 이용하여 보안 다중홉 라우팅 정책을 수행하는 단계는, 상기 홉의 수 및 각 릴레이 클러스터 릴레이 수를 설정하는 단계; 각 홉에서 선택된 릴레이 노드의 인덱스 r_k^* 를 정의하는 단계; $r_0^* = A$ 및 $r_K^* = B$로 초기화하는 단계; 각각의 홉 k = 1, ... , K-2에서 선택된 최대 보안유지 릴레이를 구하는 단계; 홉 K-1에서, 가장 큰 $\gamma_{S,r_{k-2}^*,r}^{(K-1)}$을 경로로 선택하는 대신 $r_{k-1}^* = \max_{r=1,\ldots,N} min(\gamma_{S,r_{k-2}^*,r}^{(K-1)}, \gamma_{S,r,r_k^*}^{(K)})$로 조인트 릴레이를 선택하는 단계; 및 최적의 비밀유지 릴레이 $\{r_k^*\}$를 결정하는 단계를 포함할 수 있다.

[0016] 다른 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템은, 도청자가 존재하는 애드-혹 무선 네트워크 환경에서 정보를 송신하는 송신기; 송신된 상기 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 중간 클러스터; 및 상기 릴레이를 통해 정보를 전달 받는 수신기를 포함하고, 상기 중간 클러스터는, 복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 상기 정보를 전달할 수 있다.

발명의 효과

[0017] 실시예들에 따르면 도청자(eavesdropper)가 존재하는 애드-혹 무선 네트워크 환경에서 각 홉에 다수의 릴레이(relay)를 설치하여 홉간 최적의 릴레이를 선택함으로써, 송수신기 간의 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송할 수 있는 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법 및 시스템을 제공할 수 있다.

도면의 간단한 설명

[0018] 도 1는 일 실시예에 따른 키가 없는 물리계층(PHY) 보안 전송을 설명하기 위한 도면이다.

도 2는 일 실시예에 따른 비밀유지 용량을 설명하기 위한 도면이다.

도 3은 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법을 나타내는 흐름도이다.

도 4는 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템을 개략적으로 나타내는 도면이다.

도 5a는 일 실시예에 따른 non-zero 비밀유지 용량 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다.

도 5b는 일 실시예에 따른 비밀유지 아웃티지 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다.

도 6a는 일 실시예에 따른 비밀유지 아웃티지 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다.

도 6b는 일 실시예에 따른 임계 비밀유지 속도(Rs)에 따른 비밀유지 아웃티지 확률을 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0019] 이하, 첨부된 도면을 참조하여 실시예들을 설명한다. 그러나, 기술되는 실시예들은 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 이하 설명되는 실시예들에 의하여 한정되는 것은 아니다. 또한, 여러 실시예들은 당해 기술분야에서 평균적인 지식을 가진 자에게 본 발명을 더욱 완전하게 설명하기 위해서 제공되는 것이다. 도면에서 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[0021] 아래의 실시예에서는 협력적 다양성을 가지는 다중홉 무선 네트워크의 라우팅 정책과 물리계층 보안을 결합하는 문제에 초점을 맞추고 있다. 여러 개의(다중) 디코드 및 포워드(Decode and Forward, DF) 릴레이와 도청자로 구성된 일련의 중간 클러스터(intermediate clusters)를 통해 연결된 단일 송신기와 수신기로 구성된 시스템을 고려할 수 있다.

[0022] 여기에서는 각 홉에서 수신기와 도청자의 순간 채널 조건에 기초하여 완전한 다양성을 얻기 위해, 각 클러스터에서 홉간(hop-by-hop) 최적의 보안 릴레이를 선택할 수 있다. 신호 처리 기법은 특히 자유 공간의 정도를 고려할 수 있는 다양성을 이용하는 시스템 모델에서 채널 코딩 작업의 복잡성을 줄이는 데 도움이 되기 때문에 채널 코딩보다는 신호 처리 측면에 초점을 맞춘다.

[0023] 주요 기술로 협력적 무선 네트워크에서 애드혹 라우팅 아키텍처 및 알고리즘 제안할 수 있으며, 또한 주요 결과로 비밀유지 아웃티지 확률(secrecy outage probability) 및 비밀유지 용량 확률(secrecy capacity probability)을 도출할 수 있다.

[0024] 도 1는 일 실시예에 따른 키가 없는 물리계층(PHY) 보안 전송을 설명하기 위한 도면이다.

[0025] 도 1을 참조하면, 일 실시예들은 다중홉(multi-hop) 무선 네트워크에서 라우팅 기법과 연계한 물리계층 보안 방법 및 시스템을 제공할 수 있으며, 특히 협력적 라우팅 기법을 적용함으로써 각 홉간 최대 다이버시티(full diversity) 효과를 달성할 수 있다.

[0026] 일 실시예들은 도청자(eavesdropper, 120)가 존재하는 애드-혹 무선 네트워크 환경에서 각 홉에 다수의 릴레이(relay, 110, 130)를 설치하여 홉간 최적의 릴레이를 선택함으로써 송신기(101) 및 수신기(103) 간의 보안 라우팅 기법을 적용하여 채널(120)을 통해 기밀 메시지(confidential message)를 전송할 수 있다. 이 때 도청자(120) 및 릴레이(110, 130)의 실시간 채널 상태를 고려하여 최적의 릴레이를 선택할 수 있다.

[0027] 기밀 메시지는 상대방에게 신뢰할 수 있는 디코딩을 유지하면서 도청자(120)에게 상당한 혼란을 가하는 채널 코딩 방식을 사용하여 전송될 수 있다. 이에 따라 오류 확률이 낮고 엔트로피가 높은 채널 코드를 설계할 수 있다. 그리고 다중 경로 페이딩, 간섭, 잡음 등과 같은 무선 채널의 물리계층 특성을 활용할 수 있다.

[0028] 도 2는 일 실시예에 따른 비밀유지 용량을 설명하기 위한 도면이다.

[0029] 도 2를 참조하면, 송신기(210)가 인코딩 후 메인 채널을 통해 수신기(230)로 정보를 전달함에 따라 수신기(230)에서 디코딩하여 정보를 획득할 수 있다. 이 때 도청자(220)가 도청 정보 채널(wiretap channel)을 통해 송신기(210)에서 송신되는 정보를 도청할 수 있으며, 도청자(220) 또한 디코딩을 통해 정보를 획득할 수 있다.

[0030] 여기서, 비밀유지 용량(secrecy capacity) $C_S = [C_{Bob} - C_{Eve}]^+$이다. 이는 아래에서 보다 상세히 설명하기로 한다.

[0031] 도 3은 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법을 나타내는 흐름도이다.

[0032] 도 3을 참조하면, 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법은, 도청자가 존재하는 애드-혹 무선 네트워크 환경에서 송신기에서 정보를 송신하는 단계(310), 송신된 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계(320), 및 수신기에서 릴레이를 통해 정보를 전달 받는 단계(330)를 포함하여 이루어질 수 있다.

[0033] 여기서, 정보를 복수의 홉의 다수의 릴레이 중 적어도 어느 하나 이상을 통해 수신하고, 수신기로 전달하는 단계(320)는, 복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 정보를 전달할 수 있다.

[0034] 아래에서는 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법을 하나의 예를 들어 설명한다.

[0035] 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 방법은 도 4를 참조하여 후술하는 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템(400)을 통해 보다 구체적으로 설명할 수 있다. 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템(400)은 송신기(410), 중간 클러스터(420) 및 수신기(430)를 포함할 수 있다.

[0036] 단계(310)에서, 송신기(410)는 도청자(440)가 존재하는 애드-혹 무선 네트워크 환경에서 정보를 송신할 수 있다.

[0037] 단계(320)에서, 중간 클러스터(420)는 송신된 정보를 복수의 홉의 다수의 릴레이(relay) 중 적어도 어느 하나 이상을 통해 수신하고, 수신기(430)로 전달할 수 있다.

[0038] 중간 클러스터(420)는 복수의 홉의 각 릴레이 클러스터에서 적어도 어느 하나 이상의 릴레이를 선택하여 정보를 전달할 수 있다. 보다 구체적으로, 각 홉에서 수신기(430)와 도청자(440)의 순간 채널 조건에 기초하여 각 릴레이 클러스터에서 홉간(hop-by-hop) 최적의 보안 릴레이를 선택하여 보안 라우팅 기법을 적용하여 기밀 메시지(confidential message)를 전송할 수 있다. 여기서, 릴레이는 디코드 및 포워드(Decode and Forward, DF) 릴레이이고, 메인 채널이라고 불리는 무선 페이딩 채널을 통해 재전송하기 이전에, 앞의 노드에서 디지털 방식으로 수신된 신호를 디코딩하고 다시 인코딩하여 도청을 방지할 수 있다.

[0039] 중간 클러스터(420)는 각 홉에서의 메인 채널의 순간 신호대잡음비(Signal to Noise Ratio, SNR)와 도청자(440) 채널의 순간 신호대잡음비(SNR)를 기반으로 메인 채널의 순간 용량에서 도청 채널의 순간 용량을 차감하여 비밀유지 용량 확률(secrecy capacity probability)을 도출할 수 있다. 그리고, 중간 클러스터(420)는 각 홉에서 비밀유지 신호대잡음비(SNR)의 누적분포함수(CDF)를 산정하고, 각 홉에서 최대의 비밀유지 신호대잡음비(SNR)를 갖는 릴레이를 선택할 수 있다.

[0040] 또한, 중간 클러스터(420)는 비밀유지 성과를 정량화하도록 순간 엔드 투 엔드 전송 속도가 주어진 임계 비밀유지 속도(Rs) 아래로 떨어질 확률인 비밀유지 아웃티지 확률(probability of secrecy outage)을 도출할 수 있다.

[0041] 더욱이, 중간 클러스터(420)는 알고리즘(표 1)을 이용하여 보안 다중홉 라우팅 정책을 수행할 수 있다. 알고리즘은 홉의 수 및 각 릴레이 클러스터 릴레이 수를 설정하고, 각 홉에서 선택된 릴레이 노드의 인덱스 r_k^*를 정의하며, $r_0^* = A$ 및 $r_K^* = B$로 초기화한 후, 각각의 홉 k = 1, ... , K-2에서 선택된 최대 보안유지 릴레이를 구하고, 홉 K-1에서, 가장 큰 $\gamma_{S,r_{k-2}^*,r}^{(K-1)}$을 경로로 선택하는 대신 $r_{k-1}^* = \max_{r=1,\ldots,N} min(\gamma_{S,r_{k-2}^*,r}^{(K-1)}, \gamma_{S,r,r_k^*}^{(K)})$로 조인트 릴레이를 선택하며, 최적의 비밀유지 릴레이 $\{r_k^*\}$를 결정할 수 있다.

[0042] 단계(330)에서, 수신기(430)는 릴레이를 통해 정보를 전달 받을 수 있다. 이 때 수신기(430)는 도청자(440)에

의해 도청을 최소화시킨 비밀 메시지를 전달 받을 수 있다. 이와 같이 협력적 라우팅 기법을 적용함으로써 각 홉간 최대 다이버시티(full diversity) 효과를 달성할 수 있다.

[0043] 도 4는 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템을 개략적으로 나타내는 도면이다.

[0044] 도 4를 참조하면, 각 클러스터에서 K 개의 홉과 N 개의 신뢰할 수 있는 릴레이(R1~RN)가 있는 선형 네트워크 모델을 나타내며, K-1 릴레이 클러스터와 함께 Alice(A)라 불리는 송신기(410)(소스 노드), Bob(B)이라 불리는 합법적인 수신기(430), 그리고 Eve(E)라 불리는 도청자(440)로 구성된 일반적인 K-홉 선형 네트워크 모델을 나타낸다. 즉, 일 실시예에 따른 애드-혹 무선 네트워크에서 협력적 다중홉 라우팅을 위한 물리계층 보안 시스템은 송신기(410), 중간 클러스터(420) 및 수신기(430)를 포함할 수 있다. 여기서, 중간 클러스터(420)는 복수의 릴레이 클러스터로 구성되며, 각 릴레이 클러스터는 복수의 릴레이(릴레이 노드)로 구성될 수 있다.

[0045] 선형 네트워크 모델은 센서와 차량 네트워크를 포함하는 무선 통신에서 일반적으로 사용된다. 각 릴레이 클러스터는 N 개의 DF 릴레이 노드(R1~RN)로 구성될 수 있다. 송신기(Alice, 410)와 수신기(Bob, 430)는 다이렉트 링크가 없으며 각 클러스터에서 신뢰할 수 있는 릴레이의 도움을 받아 통신을 수행할 수 있다. 각각의 중간 릴레이는 메인 채널이라고 불리는 무선 페이딩 채널을 통해 재전송하기 이전에, 바로 앞의 노드에서 디지털 방식으로 수신된 신호를 디코딩하고 다시 인코딩할 수 있다.

[0046] 한편, 도청자(440)는 각 홉마다 도청 채널을 통해 메시지를 디코딩하려고 할 수 있다. 도청자(440)를 혼란시키기 위해 각 홉에서 무작위 코드북을 사용한다고 가정하여, 도청자(440)가 조인트 디코딩을 할 수 없다고 가정할 수 있다. 이 선형 네트워크 모델은 서로 공모하지 않는 각 클러스터에 도청자(440)가 존재하는 것과 동일하다. 각 홉에서, 기밀 메시지를 전달하기 위해 최고의 보안 릴레이를 선택할 수 있다. 모든 노드는 하나의 안테나가 장착된 것으로 간주될 수 있다. 또한 각 클러스터 간의 거리가 어느 클러스터에서의 릴레이 노드 간의 거리보다 상당히 크다고 가정할 수 있다.

[0047] 이와 같이, 홉의 채널 이득은 동일 분포뿐만 아니라 독립적으로 분포할 수 있다. 또한 송신기(410)가 메인 채널과 도청 채널의 전체 채널 상태 정보(Channel State Information, CSI)를 가지고 있다고 가정할 수 있다. 이는 비밀유지 제약이 있는 통신 시스템에 대한 기존 문헌에서 널리 채택된 가정이다. 이러한 시나리오에서, 일부 릴레이는 완전히 신뢰되지만 다른 일부는 낮은 인증 허가 및 QoS 설정으로 인해 신뢰할 수 없는 이종 네트워크(heterogeneous network)에서 흔히 볼 수 있다. 두 종류의 릴레이가 모두 적극적으로 통신에 참여하지만, 송신기(410)는 특정 합법적인 수신기(430)에게 예정된 기밀 메시지를 전송하기 위하여 신뢰할 수 없는 릴레이를 선호하지 않을 수 있으며, 신뢰할 수 없는 릴레이는 도청자(440)로 간주될 수 있다. 따라서 송신기(410)는 신뢰할 수 있는 릴레이(메인 채널)와 신뢰할 수 없는 릴레이(도청 채널)의 채널 상태 정보(CSI)를 모두 가질 수 있다.

[0048] 모든 채널이 준정적 레일리 페이딩(quasi-static Rayleigh fading)이라고 간주한다. 홉 k에서 릴레이 r1부터 릴레이 r2까지의 메인 채널의 채널 계수를 $h_{M,r1,r2}^{(k)}$ 로 나타낼 수 있다. 여기서, r1, r2 $\in$ {1, 2, ..., N}이고 k $\in$ {1, 2, ..., K}이다. 첫 번째 홉에는 송신기(410)가 하나만 있고, 이는 k = 1일 때에 r1 = A인 송신기(Alice, 410)이다. 마찬가지로 마지막 홉에서도 수신기(430)는 오직 한 개이며, 이는 k = K일 때에 r2 = B인 수신기(Bob, 430)이다. 반면, $h_{W,r1,E}^{(k)}$ 를 홉 k에서 릴레이 r1부터 도청자(Eve, 440)까지의 도청 채널의 채널 계수로 정의할 수 있다. 이 경우에도, 첫 번째 홉에는 송신기(410)가 하나만 있고, 그 결과 k = 1일 때에 r1 = A이다.

[0049] 각 노드가 수신 측에서 같은 레벨의 전송 전력 P_t와 N_0인 부가 백색 가우스 잡음(Additive White Gaussian Noise, AWGN)의 분산을 가진다고 가정하고, 홉 k에서의 메인 링크의 순간 신호대잡음비(Signal to Noise Ratio, SNR)는 다음과 같이 정의할 수 있다.

[0050] [수학식 1]

[0051]
$$\gamma_{M,r1,r2}^{(k)} = \frac{P_t |h_{M,r1,r2}^{(k)}|^2}{\mathcal{N}_0}$$

[0052] 또한, 도청자(440) 링크의 순간 신호대잡음비(SNR)는 다음과 같이 정의할 수 있다.

[0053] [수학식 2]

[0054] $$\gamma_{W,r1,E}^{(k)} = \frac{P_t |h_{W,r1,E}^{(k)}|^2}{\mathcal{N}_0}$$

[0055] 홉 k에서 달성할 수 있는 순간 비밀유지 용량(secrecy capacity)은 다음과 같이 나타낼 수 있다.

[0056] [수학식 3]

[0057] $$C_{s,r1,r2}^{(k)} = \begin{cases} C_{M,r1,r2}^{(k)} - C_{W,,r1,E}^{(k)}, & \text{if } \gamma_{M,r1,r2}^{(k)} > \gamma_{W,r1,E}^{(k)} \\ 0, & \text{otherwise} \end{cases}$$

[0058] 여기서, $C_{M,r1,r2}^{(k)}$ 은 다음에 의해 주어진 홉 k에서의 메인 채널의 순간 용량이다.

[0059] [수학식 4]

[0060] $$C_{M,r1,r2}^{(k)} = \log(1 + \gamma_{M,r1,r2}^{(k)})$$

[0061] 그리고, $C_{W,r1,E}^{(k)}$ 는 홉 k에서 주어진 도청 채널의 순간 용량이다.

[0062] [수학식 5]

[0063] $$C_{W,r1,E}^{(k)} = \log(1 + \gamma_{W,r1,E}^{(k)})$$

[0064] 여기에서 명시되지 않은 한 기본 2 척도로 로그를 가정할 수 있다. 분석을 용이하게 하기 위해 비밀유지 신호대잡음비(SNR)를 다음과 같이 정의할 수 있다.

[0065] [수학식 6]

[0066] $$\gamma_{S,r1,r2}^{(k)} = \frac{1 + \gamma_{M,r1,r2}^{(k)}}{1 + \gamma_{W,r1,E}^{(k)}}$$

[0067] 일반 표기법 Z ∈ {M, W}을 도입함으로써, $\gamma_{Z,r1,r2}^{(k)}$ 의 확률밀도함수(Probability Density Function, PDF)와 누적분포함수(Cumulative Distribution Function, CDF)를 각각 다음 식과 같이 표현할 수 있다.

[0068] [수학식 7]

[0069] $$f_{\gamma_{Z,r1,r2}^{(k)}}(x) = \frac{1}{\bar{\gamma}_Z^{(k)}} e^{-\frac{x}{\bar{\gamma}_Z^{(k)}}}$$

[0070] [수학식 8]

[0071] $$F_{\gamma_{Z_{r1,r2}^{(k)}}}(x) = 1 - e^{-\frac{x}{\bar{\gamma}_Z^{(k)}}}$$

[0072] 여기서, $\bar{\gamma}_Z^{(k)}$ 은 홉 k의 모든 링크에 대한 평균 신호대잡음비(SNR)다. 수학식6 내지 수학식 8로부터, 홉 k에서의 비밀유지 신호대잡음비(SNR)의 누적분포함수(CDF)는 다음과 같이 얻을 수 있다.

[0073] [수학식 9]

$$F_{\gamma_{S,r1,r2}^{(k)}}(x) = \int_0^{\infty} f_{\gamma_{W,r1,E}^{(k)}}(y) F_{\gamma_{M,r1,r2}^{(k)}}(x(1+y)-1)dy$$
$$= 1 - e^{-\frac{x-1}{\bar{\gamma}_M^{(k)}}} \left(\frac{\bar{\gamma}_M^{(k)}}{x\bar{\gamma}_W^{(k)} + \bar{\gamma}_M^{(k)}} \right).$$

[0074]

[0075] 아래에서는 보안 다중홉 라우팅에 대해 보다 상세히 설명한다.

[0076] 여기에서 제안한 라우팅 정책은 애드-혹(ad-hoc) 특성을 가지며, 각 홉에서 최대 비밀유지 신호대잡음비(SNR)를 갖는 릴레이를 선택할 수 있다. 직관으로, 각 홉에서의 기회 선택이 릴레이 N의 다양성 이득에 기여할 수 있다는 것을 알 수 있다. 그러나 마지막 홉 K에는 하나의 수신기(430)가 있다. 마지막 홉에서 동일한 릴레이 선택 접근은 다양성 이득을 제공하지 않는다. 이와 같이, 마지막 홉에서도 완전한 다양성을 달성하기 위해, 마지막 두 홉에서 비밀유지 신호대잡음비(SNR)에 기반한 조인트 릴레이 선택을 수행할 수 있다.

[0077] 홉 k = 1, ... , K-2에서 선택된 최대 보안유지 릴레이는 $r_{k-1}^* = \max_{r=1,\dots,N}\{\gamma_{S,r_{k-1}^*,r}^{(K)}\}$ 이며, 여기서 r_{k-1}^*는 홉 k-1에서 선택된 릴레이가 된다. 홉 K-1에서는, 가장 큰 $\gamma_{S,r_{k-2}^*,r_0}^{(K-1)}$을 경로로 선택하는 대신 $r_{k-1}^* = \max_{r=1,\dots,N} min(\gamma_{S,r_{k-2}^*,r}^{(K-1)}, \gamma_{S,r,r_k^*}^{(K)})$로 조인트 선택을 수행할 수 있다. $r_0^* = A$이고 $r_K^* = B$인 것은 명백하다. 라우팅 정책은 표 1의 알고리즘 1과 같이 요약될 수 있다.

[0078] [표 1]

1. Set K and N
2. Define r_k^* as the index of selected relay node at k-th hop, k=1,…,K-1
3. Initialization r_0^*=A and r_K^*=B
4. For k=1:K-2 do
   $$r_k^* = \max_{r=1,\dots,N} \{\gamma_{s_{r^*k-1,r}^{(k)}}\}$$
   End for
5. $$r_{K-1}^* = \max_{r=1,\dots,N} \{\gamma_{s_{r^*k-2,r}^{(K-1)}} \gamma_{s_{r,B}^{(K)}}\}$$
6. Result best secure relay $\{r_k^*\}$

[0079]

[0080] 가능한 모든 경로 중에서 최소 엔드 투 엔드(end to end) 아웃티지(outage) 확률로 경로를 식별하는 것이 최적의 정책이지만, 모든 경로의 공동 최적화와 함께 모든 링크의 채널 상태 정보(CSI)가 필요하므로 높은 복잡도 수준과 상당한 피드백이 필요하다. 제안된 라우팅 정책의 애드-혹(ad-hoc) 특성은 피드백과 복잡성을 획기적으로 감소시킬 수 있다.

[0081] 제안된 정책은 각 홉에서 N 링크의 채널 상태 정보(CSI)를 요구하는 반면에, 마지막 두 홉에서 조인트 선택을 위한 2N 링크가 필요하다. 반면, 첫 번째 K-2 홉에서는 (N - 1) 비교들이 필요하고, 마지막 홉에서는 (2N-1) 비교가 필요하다. 이와 같이 이 정책에 필요한 총 비교 수는 K(N -1)+1이다.

[0082] 성능 평가를 위해 수신기(Bob, 430)에서 엔드 투 엔드 비밀유지 신호대잡음비(SNR)의 배포를 얻어야 한다. DF 릴레이를 가정하기 때문에, 순간 엔드 투 엔드 비밀유지 속도는 병목현상의 역할을 하는 K 홉들 사이의 최소 비밀 신호대잡음비(SNR)에 의존한다. 따라서 수신기(Bob, 430)의 엔드 투 엔드 비밀 신호대잡음비(SNR)는 다음과 같이 얻을 수 있다.

[0083] [수학식 10]

[0084] $$\gamma_{e2e} = \min_{k=1,..,K} \gamma_S^{(k)}$$

[0085] 여기서, $\gamma_S^{(k)}$ 는 k = 1,...,K-2의 경우 $\gamma_{S^1}^{(k)}$ 로, k = K-1의 경우 $\gamma_{S^2}^{(k)}$ 로 표시된다. 또한, 이는 다음과 같이 표현할 수 있다.

[0086] [수학식 11]

[0087] $$\gamma_{S^1}^{(k)} = \max_{r=1,\ldots,N} \left(\gamma_{S,r_{k-1}^*,r}^{(k)} \right)$$

[0088] [수학식 12]

[0089] $$\gamma_{S^2}^{(k)} = \max_{r=1,\ldots,N} \min \left(\gamma_{S,r_{K-2}^*,r}^{(K-1)}, \gamma_{S,r,B}^{(K)} \right)$$

[0090] 순서 통계량을 사용하여 수학식 9 및 수학식 11에서 다음과 같이 $\gamma_{S^1}^{(k)}$ 의 누적분포함수(CDF)을 구할 수 있다.

[0091] [수학식 13]

[0092] $$\begin{aligned} F_{\gamma_{S^1}^{(k)}}(x) &= \left[1 - e^{-\frac{x-1}{\bar{\gamma}_M^{(k)}}} \left(\frac{\bar{\gamma}_M^{(k)}}{x\bar{\gamma}_W^{(k)} + \bar{\gamma}_M^{(k)}} \right) \right]^N \\ &= \sum_{j=0}^{N} \binom{N}{j} (-1)^j e^{-\frac{(x-1)j}{\bar{\gamma}_M^{()k}}} \left(\frac{\bar{\gamma}_M^{(k)}}{x\bar{\gamma}_W^{(k)+\bar{\gamma}_M^{(k)}}} \right)^j \end{aligned}$$

[0093] 홉 K-1의 경우 릴레이 선택은 다음 K^{th} 홉에 따라서도 달라진다. 따라서, $\gamma_{S^2}^{(k)}$ 에 대한 누적분포함수(CDF)는 다음과 같이 계산될 수 있다.

[0094] [수학식 14]

[0095] $$\begin{aligned} F_{\gamma_{S^2}^{(k)}}(x) &= Pr\left[\max_{r=1,\ldots,N} \min\{\gamma_{M,r_{K-2}^*,r}^{(K-1)}, \gamma_{M,r,B}^{(K)}\} < x \right] \\ &= \prod_{r=1}^{N} Pr\left[\gamma_{(r)}^{min} < x \right], \end{aligned}$$

[0096] 여기서, $\gamma_{(r)}^{min} = \min\{\gamma_{M,r_{K-2}^*,r}^{(K-1)}, \gamma_{M,r,B}^{(K)}\}, r = 1, 2, ..., N$ 이다. 여기에서는 다음과 같이 알고 있다.

[0097] [수학식 15]

[0098] $$\begin{aligned} Pr\left[\gamma_{(r)}^{min} > x \right] &= Pr\left(\gamma_{M,r_{K-2}^*,r}^{(K-1)} > x \right) Pr\left(\gamma_{M,r,B}^{(K)} > x \right) \\ &= \left(1 - F_{\gamma_{M,r_{K-2}^*,r}^{(K-1)}}(x) \right) \left(1 - F_{\gamma_{M,r,B}^{(K)}}(x) \right) \end{aligned}$$

[0099] 그리고, 수학식 8, 수학식 12, 수학식 14 및 수학식 15로부터 다음을 얻을 수 있다.

[0100] [수학식 16]

[0101] $$F_{\gamma_{S^2}^{(k)}}(x) = \left[1 - \left(1 - F_{\gamma_{M,r^*_{K-2},r}^{(K-1)}}(x)\right)\left(1 - F_{\gamma_{M,r,B}^{(K)}}(x)\right)\right]^N$$

[0102] 간단한 수학적 조작을 한 후, 마침내 $\gamma_{S^2}^{(k)}$ 의 누적분포함수(CDF)를 얻을 수 있다.

[0103] [수학식 17]

[0104] $$\begin{aligned} F_{\gamma_{S^2}^{(k)}}(x) &= \left(1 - e^{-(x-1)\left(\frac{1}{\bar{\gamma}_M^{(K-1)}} + \frac{1}{\bar{\gamma}_M^{(K)}}\right)}\right. \\ &\quad \left. \times \frac{\gamma_M^{K-1}\gamma_M^K}{(x\gamma_W^{K-1} + \gamma_M^{K-1})(x\gamma_W^K + \gamma_M^K)}\right)^N \\ &= \sum_{j=0}^{N} \binom{N}{j} (-1)^j e^{-j(x-1)\left(\frac{\bar{\gamma}_M^{(K)} + \bar{\gamma}_M^{(K-1)}}{\bar{\gamma}_M^{(K)}\bar{\gamma}_M^{(K-1)}}\right)} \\ &\quad \times \left(\frac{\bar{\gamma}_M^{(K)} + \bar{\gamma}_M^{(K-1)}}{(x\bar{\gamma}_W^{(K)} + \bar{\gamma}_M^{(K)})(x\bar{\gamma}_W^{(K-1)} + \bar{\gamma}_M^{(K-1)})}\right)^j \end{aligned}$$

[0105] 순서통계량을 사용하여 수학식 10에서의 엔드 투 엔드 비밀유지 신호대잡음비(SNR)의 누적분포함수(CDF)를 다음과 같이 구할 수 있다.

[0106] [수학식 18]

[0107] $$F_{\gamma_{e2e}}(x) = 1 - \prod_{k=1}^{K-1}\left(1 - F_{\gamma_S^{(k)}}(x)\right)$$

[0108] 엔드 투 엔드 비밀유지 신호대잡음비(SNR)의 분포가 첫 번째 K-2 홉과 마지막 두 홉에서 다르기 때문에 수학식 18은 다음과 같이 다시 나타낼 수 있다.

[0109] [수학식 19]

[0110] $$F_{\gamma_{e2e}}(x) = 1 - \prod_{k=1}^{K-2}\left(1 - F_{\gamma_{S^1}^{(k)}}(x)\right)\left(1 - F_{\gamma_{S^2}^{(K-1)}}(x)\right)$$

[0111] 수학식 13과 수학식 17를 사용하여 단순화될 수 있다.

[0113] 아래에서는 성능 평가를 수행할 수 있다.

[0114] 먼저, Non-zero 비밀유지 용량 확률을 확인할 수 있다. 순간 엔드 투 엔드 비밀유지 용량은 다음과 같이 표현된다.

[0115] [수학식 20]

[0116] $$C_S = \frac{1}{K}\log(\gamma_{e2e})$$

[0117] 인자 1/K는 전체 전송이 K 단계에서 일어난다는 사실을 설명한다. 메인 채널의 순간 신호대잡음비(SNR)가 도청

채널의 순간 신호대잡음비(SNR)보다 클 때만 비밀유지 용량이 존재하기 때문에, non-zero 비밀유지 용량의 존재 가능성을 조사할 필요가 있다. 수학식 20으로부터 다음과 같이 얻을 수 있다.

[0118] [수학식 21]

$$Pr(C_S > 0) = Pr(\gamma_{e2e} > 1)$$
$$= 1 - F_{\gamma_{e2e}(1)}.$$

[0119]

[0120] non-zero 비밀유지 용량 확률을 위한 폐쇄형 표현식은 아래와 같이 수학식 13, 수학식 17, 수학식 19 및 수학식 21을 조합하여 x를 1로 대체하여 얻을 수 있다.

[0121] [수학식 22]

$$Pr(C_S > 0) = \prod_{k=1}^{K-1}\left(1 - \sum_{i=0}^{N}\binom{N}{i}(-1)^i {a_k}^i\right)$$

[0122]

[0123] 여기서, a_k 는 다음과 같이 정의될 수 있다.

[0124] [수학식 23]

$$a_k = \begin{cases} \frac{\bar{\gamma}_M^{(k)}}{\bar{\gamma}_W^{(k)}+\bar{\gamma}_M^{(k)}} & \text{if } k < K-1 \\ \frac{\bar{\gamma}_M^{(K)}\bar{\gamma}_M^{(K-1)}}{(\bar{\gamma}_W^{(K-1)}+\bar{\gamma}_M^{(K-1)})(\bar{\gamma}_W^{(K)}+\bar{\gamma}_M^{(K)})} & \text{if } k = K-1 \end{cases}$$

[0125]

[0126] 또한, 비밀유지 아웃티지 확률(probability of secrecy outage)을 확인할 수 있다.

[0127] 폐쇄형 표현식에서 정확한 비밀유지 아웃티지 확률을 도출함으로써 제안된 정책에 의해 달성된 비밀유지 성과를 정량화할 수 있다. 비밀유지 아웃티지 확률은 순간 엔드 투 엔드 전송 속도가 주어진 임계 비밀유지 속도(Rs) 아래로 떨어질 확률이라고 정의할 수 있다. 이렇게 하면 $C_s > R_s$ 인 경우에만 안전한 전송이 보장된다. 따라서, 비밀유지 아웃티지 확률은 다음과 같이 나타낼 수 있다.

[0128] [수학식 24]

$$P_{out} = Pr(C_S < R_S)$$
$$= F_{\gamma_{e2e}}(2^{R_S K}).$$

[0129]

[0130] 이와 같이 비밀유지 아웃티지 확률에 대한 폐쇄형 표현식은 x를 $2^{R_S K}$ 로 대체하여 수학식 3, 수학식 17 및 수학식 19에서 다음과 같이 쉽게 얻을 수 있다. 즉, 비밀유지 아웃티지 확률을 다음과 같이 나타낼 수 있다.

[0131] [수학식 25]

$$P_{out} = 1 - \prod_{k=1}^{K-1}\left(1 - \sum_{j=0}^{N}\binom{N}{j}(-1)^j \Gamma_k^j e^{-\frac{(2^{R_s K}-1)j}{b_k}}\right)$$

[0132]

[0133] 여기서,

[0134] [수학식 26]

$$b_k = \begin{cases} \bar{\gamma}_M^{(k)} & \text{if } k < K-1 \\ \frac{\bar{\gamma}_M^{(K)}\bar{\gamma}_M^{(K-1)}}{\bar{\gamma}_M^{(K)}+\bar{\gamma}_M^{(K-1)}} & \text{if } k = K-1 \end{cases}$$

[0135]

[0136] [수학식 27]

$$\Gamma_k = \begin{cases} \frac{\bar{\gamma}_M^{(k)}}{p\bar{\gamma}_W^{(k)}+\bar{\gamma}_M^{(k)}} & \text{if } k < K-1 \\ \frac{\bar{\gamma}_M^{(K)}\bar{\gamma}_M^{(K-1)}}{(p\bar{\gamma}_W^{(K)}+\bar{\gamma}_M^{(K)})(p\bar{\gamma}_W^{(K-1)}+\bar{\gamma}_M^{(K-1)})} & \text{if } k = K-1 \end{cases}$$

[0137]

[0138] 이고, $p = 2^{R_S K}$ 이다.

[0139] 비록 이 폐쇄형 표현식으로 제안된 정책의 성능을 평가할 수 있지만, 이 복잡한 표현은 다양성 이득이 어떻게 영향을 받는지에 대한 유용한 통찰력을 얻을 수 없다. 따라서, 높은 비밀유지 신호대잡음비(SNR) 근사치, 즉 다음의 $\gamma_{e2e} \to \infty$로 점근적 분석을 연구할 수 있다.

[0140] 이론 1. $\gamma_{e2e} \to \infty$일 때 점근적 아웃티지 확률은 다음과 같이 나타낼 수 있다.

[0141] [수학식 28]

$$P_{out}^{a} \approx (2^{KR_S}-1)^N \times \left[\sum_{k=1}^{K-2}\left(\frac{1}{\bar{\gamma}_M^{(k)}}\right)^N + \left(\frac{1}{\bar{\gamma}_M^{(K-1)}}+\frac{1}{\bar{\gamma}_M^{(K)}}\right)^N\right]$$

[0142]

[0143] 증명. 비밀유지 신호대잡음비(SNR)의 엔드 투 엔드 누적분포함수(CDF)는 다음과 같이 단순화할 수 있다.

[0144] [수학식 29]

$$F_{\gamma_{e2e}}^{a}(x) \approx \sum_{k=1}^{K-1} F_{\gamma_S^{(k)}}(x)$$

[0145]

[0146] $F_{\gamma_S^{(k1)}} \times F_{\gamma_S^{(k2)}}, k1 \neq k2$의 곱이 $F_{\gamma_S^{(k1)}}$에 비해 작다는 사실에서 근사치를 구할 수 있다. 여기에서는 $\bar{\gamma}_M^{(k)} >> \bar{\gamma}_W^{(k)}$ 일 때 $\gamma_{e2e} \to \infty$인 것을 안다. 또한 수학식 13 및 수학식 17의 익스퍼넨셜 텀을 확장하고 상위 차수 항을 무시하면 누적분포함수(CDF)를 다음과 같이 다시 나타낼 수 있다.

[0147] [수학식 30]

$$F_{\gamma_{S1}^{(k)}}(x) = \left(\frac{x-1}{\bar{\gamma}_M^{(k)}}\right)^N$$

[0148]

[0149] [수학식 31]

$$F_{\gamma_{S2}^{(k)}}(x) = \left(\frac{(x-1)(\bar{\gamma}_M^{(K-1)}+\bar{\gamma}_M^{(K)})}{\bar{\gamma}_M^{(K-1)}\bar{\gamma}_M^{(K)}}\right)^N$$

[0150]

[0151] 수학식 29 내지 수학식 31에서, 결국 다음을 구할 수 있다.

[0152] [수학식 32]

$$F^{a}_{\gamma_{e2e}}(x) = (x-1)^{N} \times \left[\sum_{k=1}^{K-2}\left(\frac{1}{\gamma_M^{(k)}}\right)^{N} + \left(\frac{1}{\bar{\gamma}_M^{(K-1)}} + \frac{1}{\bar{\gamma}_M^{(K)}}\right)^{N}\right]$$

[0153]

[0154] 여기서, x를 $2^{R_s K}$ 로 대체하면, 수학식 28을 얻을 수 있다.

[0155] 메인 채널의 모든 링크에서 평균 신호대잡음비(SNR)가 동일한 균형된 링크의 특별한 경우(예: $\bar{\gamma}_M^1 = \bar{\gamma}_M^2 = \ldots = \bar{\gamma}_M^K = \bar{\gamma}_M$), 점근적 아웃티지 표현이 다음과 같이 감소할 수 있다.

[0156] [수학식 33]

[0157] $$P^{a}_{out} = (\psi\bar{\gamma}_M)^{-\Delta}$$

[0158] 여기서, 비밀유지 다양성 차수는 Δ=N 이고, 동등 비밀유지 아웃티지 신호대잡음비(SNR) 이득은 $\psi = \left((2^{KR_S}-1)^N \times (K-2+2^N)\right)^{-\frac{1}{\Delta}}$ 이다. 비밀유지 다양성 차수 Δ는 점근적 비밀유지 아웃티지 확률 곡선의 기울기를 구하기 쉽게 한다. 비슷하게, 비밀유지 아웃티지 신호대잡음비(SNR) 이득은 기준 곡선 $\bar{\gamma}_M^{-\Delta}$ 에 관련된 점근적 비밀유지 아웃티지 확률의 신호대잡음비(SNR) 장점을 결정할 수 있다.

[0159] 도 5a는 일 실시예에 따른 non-zero 비밀유지 용량 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다. 도 5a에 도시된 바와 같이, $\bar{\gamma}_M$ 및 N이 커지고 K가 작아질수록 non-zero 비밀유지 용량 확률이 커지는 것을 확인할 수 있다.

[0160] 그리고 도 5b는 일 실시예에 따른 비밀유지 아웃티지 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다. 도 5b에 도시된 바와 같이, K 및 $\bar{\gamma}_M$가 커질수록 비밀유지 아웃티지 확률이 커지는 것을 확인할 수 있다.

[0161] 도 6a는 일 실시예에 따른 비밀유지 아웃티지 확률과 평균 메인 채널 신호대잡음비(SNR)를 비교한 결과를 나타낸다. 도 6a에 도시된 바와 같이, N이 커질수록 비밀유지 아웃티지 확률이 작아지는 것을 확인할 수 있다.

[0162] 또한 도 6b는 일 실시예에 따른 임계 비밀유지 속도(Rs)에 따른 비밀유지 아웃티지 확률을 나타낸다. 도 6b에 도시된 바와 같이, Rs가 커질수록 비밀유지 아웃티지 확률이 커지는 것을 확인할 수 있다.

[0163] 이와 같이 점근선 곡선은 높은 신호대잡음비(SNR)에서 정확한 곡선과 병합되고, 다이버시티 이득은 기울기가 변경되는 것에 의해 알 수 있듯이 N에 의해 영향을 받는다. 또한, 다중홉은 Rs가 작을수록 우후하며, 각 홉은 여러 개의 신뢰할 수 있는 릴레이에 의해 제공되는 공간적 다양성을 활용할 수 있다.

[0165] 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, 컨트롤러, 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 컨트롤러를 포함할 수 있다. 또한, 병렬 프로세서

(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0166] 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(embody)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.

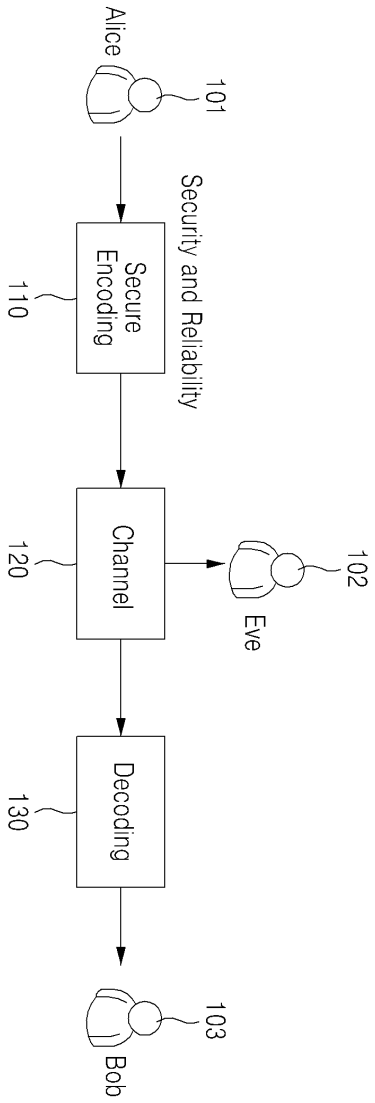
[0167] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic 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.

[0168] 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.

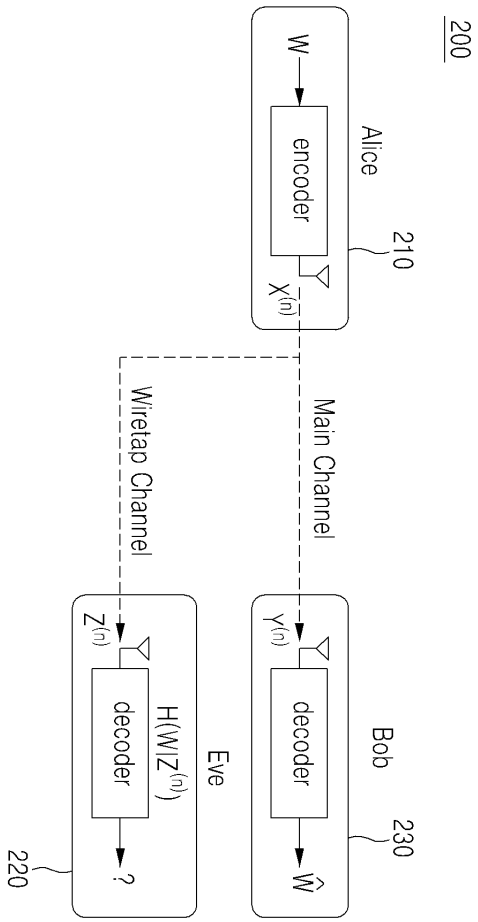
[0169] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

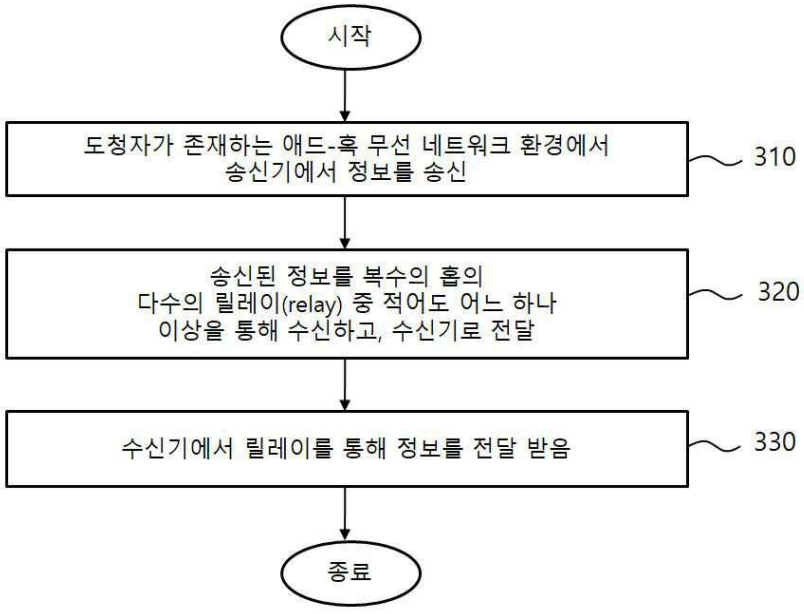
도면1


Alice
101
Security and Reliability
Secure Encoding
110
Channel
120
102
Eve
Decoding
130
103
Bob

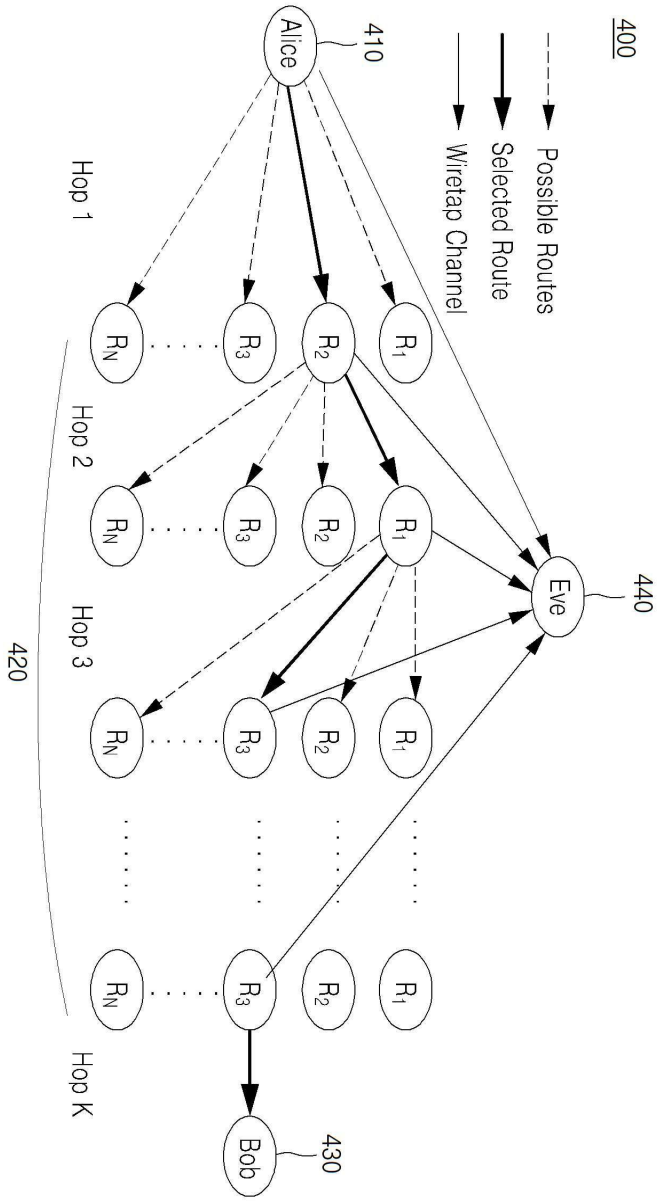
도면2


200
W
encoder
Alice
210
$X^{(n)}$
Wiretap Channel
Main Channel
$Z^{(n)}$
H(W|Z$^{(n)}$)
decoder
Eve
220
?
$Y^{(n)}$
decoder
Bob
230
$\hat{W}$

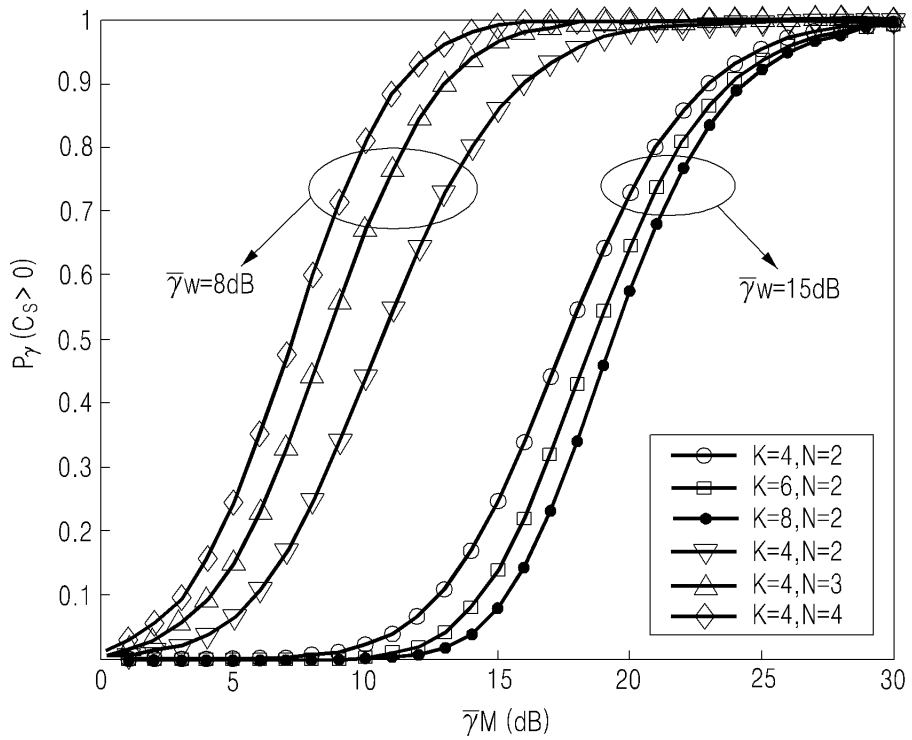
도면3


시작
도청자가 존재하는 애드-혹 무선 네트워크 환경에서
송신기에서 정보를 송신
310
송신된 정보를 복수의 홉의
다수의 릴레이(relay) 중 적어도 어느 하나
이상을 통해 수신하고, 수신기로 전달
320
수신기에서 릴레이를 통해 정보를 전달 받음
330
종료

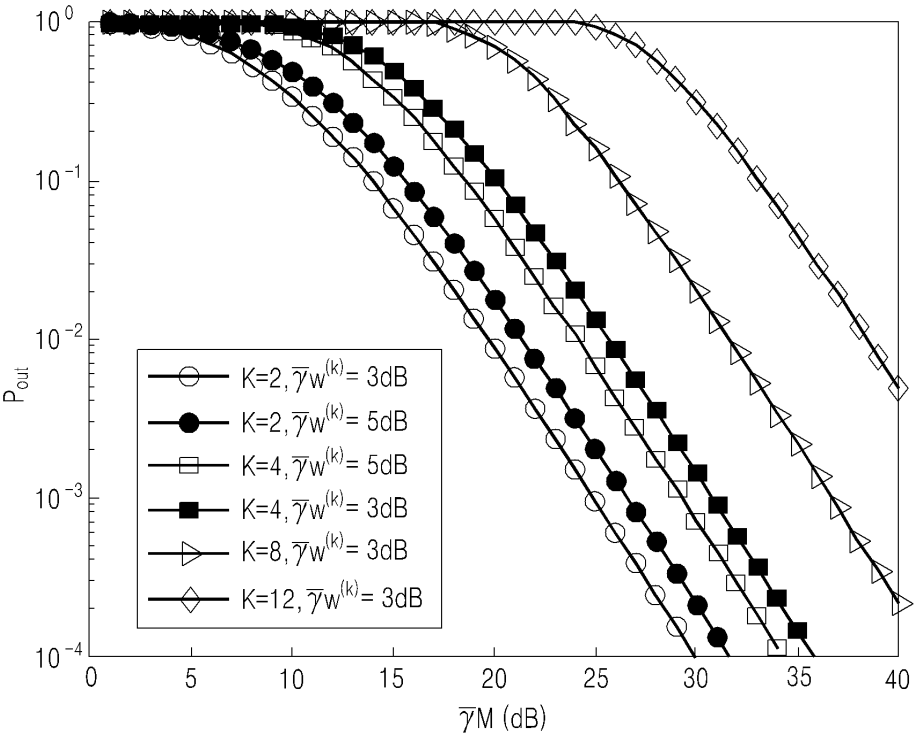
도면4


400
Possible Routes
Selected Route
Wiretap Channel
Alice
410
Hop 1
Hop 2
Hop 3
Hop K
420
Eve
440
Bob
430
R_N
R_3
R_2
R_1

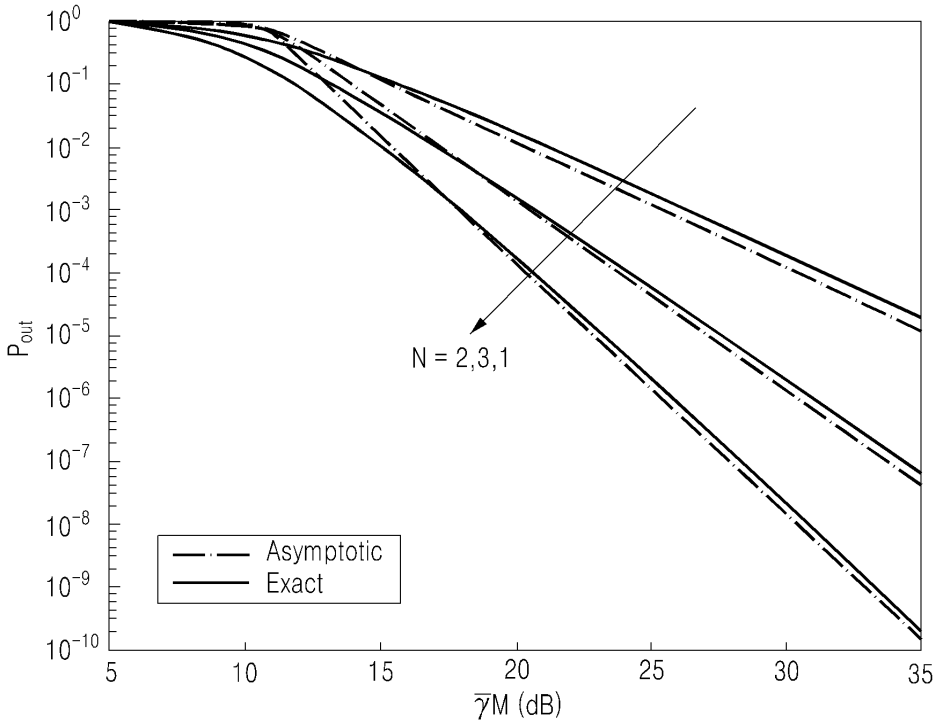
도면5a


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
$P_\gamma(C_S>0)$
$\overline{\gamma}$w=8dB
$\overline{\gamma}$w=15dB
K=4,N=2
K=6,N=2
K=8,N=2
K=4,N=2
K=4,N=3
K=4,N=4
0
5
10
15
20
25
30
$\overline{\gamma}$M (dB)

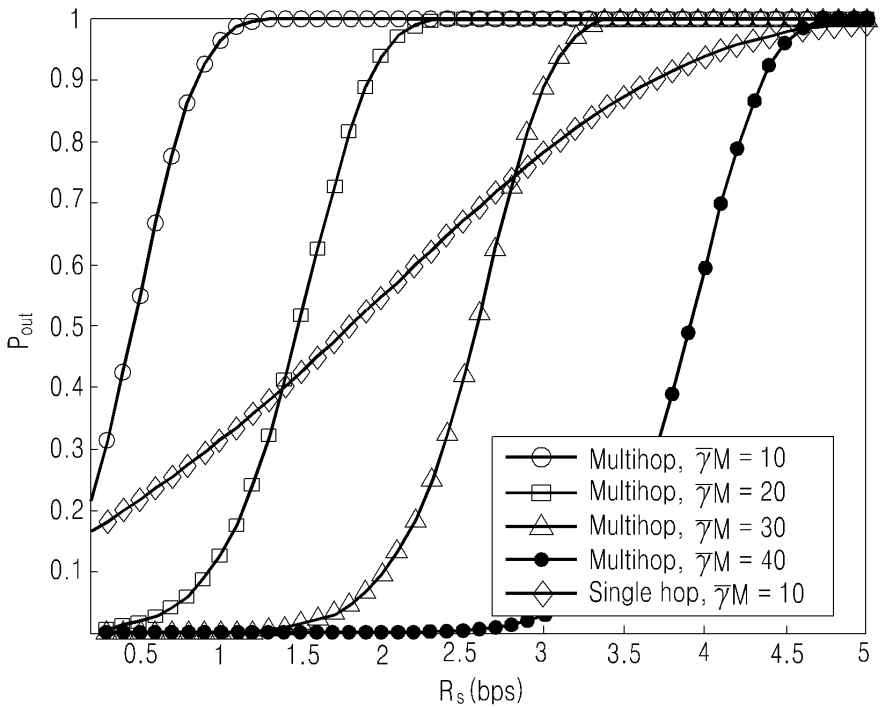
도면5b


10^0
10^{-1}
10^{-2}
10^{-3}
10^{-4}
P_{out}
K=2, $\overline{\gamma}w^{(k)}$= 3dB
K=2, $\overline{\gamma}w^{(k)}$= 5dB
K=4, $\overline{\gamma}w^{(k)}$= 5dB
K=4, $\overline{\gamma}w^{(k)}$= 3dB
K=8, $\overline{\gamma}w^{(k)}$= 3dB
K=12, $\overline{\gamma}w^{(k)}$= 3dB
0
5
10
15
20
25
30
35
40
$\overline{\gamma}$M (dB)

도면6a


10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
P_{out}
N = 2,3,1
Asymptotic
Exact
5
10
15
20
25
30
35
$\overline{\gamma}$M (dB)

도면6b


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
P_{out}
Multihop, $\overline{\gamma}$M = 10
Multihop, $\overline{\gamma}$M = 20
Multihop, $\overline{\gamma}$M = 30
Multihop, $\overline{\gamma}$M = 40
Single hop, $\overline{\gamma}$M = 10
0.5
1
1.5
2
2.5
3
3.5
4
4.5
5
R_s (bps)