



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0059019
(43) 공개일자 2018년06월04일

(51) 국제특허분류(Int. Cl.)
H04B 7/14 (2006.01) H04L 1/00 (2006.01)
H04W 40/14 (2009.01) H04W 40/22 (2009.01)
(52) CPC특허분류
H04B 7/14 (2013.01)
H04L 1/0047 (2013.01)
(21) 출원번호 10-2016-0158100
(22) 출원일자 2016년11월25일
심사청구일자 2016년11월25일

(71) 출원인
경상대학교산학협력단
경상남도 진주시 진주대로 501 (가좌동)
(72) 발명자
반태원
부산광역시 강서구 명지오션시티12로 92 (명지동,
엘크루 블루오션)511동 803호
이병수
경상남도 창원시 마산회원구 회원동12길 22-2
(74) 대리인
김영재

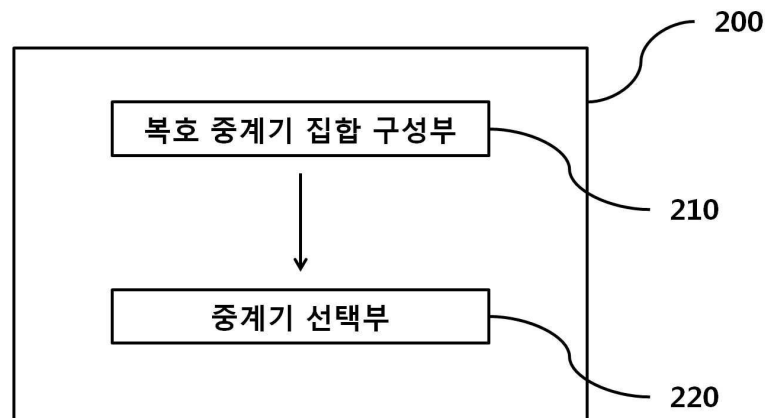
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 중계기 네트워크에서 도청 방지를 위한 중계기 선택 장치 및 방법

(57) 요약

복수의 중계기들 중에서, 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기를 선택할 수 있는 중계기 선택 장치가 개시된다. 개시된 중계기 선택 장치는 수신자를 향해 데이터를 전송할 제1 중계기 및 도청 장치의 복호 확률을 낮추면서 수신자의 복호 확률을 높일 수 있는 제2 중계기를 선택하여 데이터를 전송하도록 할 수 있다.

대표도 - 도2



(52) CPC특허분류

H04W 40/14 (2013.01)

H04W 40/22 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711035441

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 방송통신산업기술개발

연구과제명 단말 협업형 Giga급 스마트 클라우드릿 핵심 기술 개발

기 여 율 1/1

주관기관 한국과학기술원

연구기간 2016.03.01 ~ 2017.02.28

명세서

청구범위

청구항 1

전송 장치로부터 데이터를 수신하여 상기 수신한 데이터를 성공적으로 복호한 복수의 중계기들을 포함하는 복호 중계기 집합을 구성하는 복호 중계기 집합 구성부; 및

상기 복호 중계기 집합에 포함된 복수의 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기를 전송 중계기로 선택하는 중계기 선택부

를 포함하고,

상기 중계기들에서 수신된 데이터는 상기 중계기들 중에서 선택된 전송 중계기로부터 상기 수신 장치로 포워딩 되는 중계기 선택 장치.

청구항 2

제1항에 있어서,

상기 중계기 선택부는 보안 용량이 최대화 되도록 상기 전송 중계기를 선택하는 중계기 선택 장치.

청구항 3

제1항에 있어서,

상기 중계기 선택부는 하기 수학식에 따라서 상기 전송 중계기를 선택하는 중계기 선택 장치.

[수학식 1]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.

$h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.

또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

청구항 4

중계기에 있어서,

전송 장치로부터 데이터를 수신하는 수신부;

상기 수신된 데이터를 복호하는 데이터 복호부; 및

데이터 전송부

를 포함하고,

상기 데이터 복호에 성공한 경우, 상기 전송 장치로부터 데이터를 수신하여 복호에 성공한 다른 중계기들과 복호 중계기 집합에 포함되고,

상기 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률과 수신 장치의 복호 확률을 고려하여 상기 중계기가 상기 수신된 데이터를 포워딩하는 중계기로 선택된 경우,

상기 데이터 전송부는 상기 수신된 데이터를 수신 장치로 전송하는 중계기.

청구항 5

제4항에 있어서,

상기 중계기는 상기 복호 중계기 집합에 포함된 중계기들 중에서 하기 수학적 2에 따라 상기 수신된 데이터를 포워딩하는 중계기로 선택되는 중계기.

[수학적 2]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.

$h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.

또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

청구항 6

중계기를 경유하여 전송 장치로부터 데이터를 수신하는 수신 장치에 있어서,

상기 전송 장치로부터 데이터를 수신하여 상기 수신한 데이터를 성공적으로 복호한 복수의 중계기들 중에서, 도청 장치의 복호 확률을 낮추고 상기 수신 장치의 복호 확률을 높일 수 있는 전송 중계기로부터 상기 전송 중계기가 수신한 데이터를 수신하는 수신부

를 포함하는 수신 장치.

청구항 7

제6항에 있어서,

상기 전송 중계기는 상기 중계기들 중에서 하기 수학적 식 3에 따라 상기 전송 중계기로 선택되는 수신 장치.

[수학적 식 3]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.

$h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.

또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

발명의 설명

기술 분야

[0001] 하기의 실시예들은 복수의 중계기들 중에서 데이터를 포위딩할 중계기를 선택하는 기법에 관한 것으로, 구체적으로는 도청 방식을 고려하여 중계기를 선택하는 기법에 관한 것이다.

배경 기술

[0002] 고품질의 이동통신서비스에 대한 요구가 증가하고 있어 통신 사업자들은 전과 사각 지역에 기지국을 증설하기 위해 막대한 비용을 투자해야 한다. 투자 비용의 감소를 위해, 통신 사업자들은 중계기 통신(Relay Communication)에 주목하고 있다. 무선 통신의 개방성으로 인하여, 중계기 통신에서는 전송된 신호를 누구든 수신할 수 있다. 따라서, 중계기 통신의 경우 보안에 취약한 것이 일반적이다.

[0003] 중계기 통신에서의 보안 문제를 원천적으로 해결하기 위해 물리 계층 보안(Physical Layer Security)기술에 대한 연구가 활발하게 진행되고 있다. 예를 들어, 복수의 중계기와 도청 장치가 존재하는 중계기 네트워크에서 도청 장치로부터 정보를 안전하게 보호하기 위해 중계기들과 도청 장치 사이의 채널 상황을 고려하여 도청이 불가능한 중계기를 선택하여 정보를 전달하는 방식이 제안되기도 하였다.

[0004] 최근에는 복수 개의 중계기가 존재하는 협력 통신(Cooperative Communication) 네트워크에서 중계기가 의도적인 재밍(Jamming) 신호를 전송하여 도청 장치의 데이터 복호를 방해하는 중계기 선택방식들이 제안된 바 있다.

[0005] 그러나, 데이터를 전송하는 중계기 외에 재밍 신호를 전송하는 중계기를 동시에 선택하여 신호를 전송하는 기존의 중계기 선택방식들은 도청 장치의 데이터 복호 확률을 감소시키지만, 재밍 신호로 인해 수신자의 데이터 복호 확률 또한 감소시키는 문제점이 있었다.

발명의 내용

해결하려는 과제

- [0006] 하기의 실시예들의 목적은 복수의 중계기들 중에서, 데이터를 전송할 중계기를 선택하는 것이다.
- [0007] 하기의 실시예들의 목적은 중계기에서 데이터를 전송하는 경우, 수신자의 복호 확률을 높이면서도 도청 장치의 도청 확률은 낮출 수 있는 중계기를 선택하는 것이다.

과제의 해결 수단

- [0008] 예시적 실시예에 따르면, 전송 장치로부터 데이터를 수신하여 상기 수신한 데이터를 성공적으로 복호한 복수의 중계기들을 포함하는 복호 중계기 집합을 구성하는 복호 중계기 집합 구성부 및 상기 복호 중계기 집합에 포함된 복수의 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기를 전송 중계기로 선택하는 중계기 선택부를 포함하고, 상기 중계기들에서 수신된 데이터는 상기 중계기들 중에서 선택된 전송 중계기로부터 상기 수신 장치로 포워딩되는 중계기 선택 장치가 제공된다.
- [0009] 여기서, 상기 중계기 선택부는 보안 용량이 최대화 되도록 상기 전송 중계기를 선택할 수 있다.
- [0010] 그리고, 상기 중계기 선택부는 하기 수학식에 따라서 상기 전송 중계기를 선택할 수 있다.

- [0012] [수학식 1]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

- [0014]
- [0016] 여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.
- [0017] $h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.
- [0018] 또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

- [0020] 또 다른 예시적 실시예에 따르면, 중계기에 있어서, 전송 장치로부터 데이터를 수신하는 수신부, 상기 수신된 데이터를 복호하는 데이터 복호부 및 데이터 전송부를 포함하고, 상기 데이터 복호에 성공한 경우, 상기 전송 장치로부터 데이터를 수신하여 복호에 성공한 다른 중계기들과 복호 중계기 집합에 포함되고, 상기 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률과 수신 장치의 복호 확률을 고려하여 상기 중계기가 상기 수신된 데이터를 포워딩하는 중계기로 선택된 경우, 상기 데이터 전송부는 상기 수신된 데이터를 수신 장치

로 전송하는 중계기가 제공된다.

[0021] 여기서, 상기 중계기는 상기 복호 중계기 집합에 포함된 중계기들 중에서 하기 수학식 2에 따라 상기 수신된 데이터를 포워딩하는 중계기로 선택될 수 있다.

[0023] [수학식 2]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

[0025]

[0027] 여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.

[0028] $h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.

[0029] 또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

[0031] 또 다른 예시적 실시예에 따르면, 중계기를 경유하여 전송 장치로부터 데이터를 수신하는 수신 장치에 있어서, 상기 전송 장치로부터 데이터를 수신하여 상기 수신한 데이터를 성공적으로 복호한 복수의 중계기들 중에서, 도청 장치의 복호 확률을 낮추고 상기 수신 장치의 복호 확률을 높일 수 있는 전송 중계기로부터 상기 전송 중계기가 수신한 데이터를 수신하는 수신부를 포함하는 수신 장치가 제공된다.

[0032] 여기서, 상기 전송 중계기는 상기 중계기들 중에서 하기 수학식 3에 따라 상기 전송 중계기로 선택될 수 있다.

[0034] [수학식 3]

$$(R^*, H^*) = \underset{\substack{R, H \in R_N \\ R \neq H}}{\operatorname{argmax}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\}$$

[0036]

[0038] 여기서, R 은 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기이고, H

는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기이다.

[0039] $h_{R,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 수신 장치 D 사이의 채널 상태이고, $h_{H,D}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 수신 장치 D 사이의 채널 상태이다.

[0040] 또한, $h_{R,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 수신 장치를 향해 데이터를 전송할 중계기 R 과 도청 장치 E 사이의 채널 상태이고, $h_{H,E}$ 는 복호 중계기 집합에 포함된 중계기들 중에서 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기 H 와 도청 장치 E 사이의 채널 상태이다.

발명의 효과

[0041] 하기의 실시예들에 따르면, 복수의 중계기들 중에서, 데이터를 전송할 중계기를 선택할 수 있다.

[0042] 하기의 실시예들에 따르면, 중계기에서 데이터를 전송하는 경우, 수신자의 복호 확률을 높이면서도 도청 장치의 도청 확률은 낮출 수 있다.

도면의 간단한 설명

[0043] 도 1은 중계기를 경유하여 데이터를 전송하는 중계기 전송 시스템을 설명한 도면이다.

도 2는 예시적 실시예에 따른 중계기 선택 장치의 구조를 도시한 블록도이다.

도 3은 예시적 실시예에 따른 중계기의 구조를 도시한 블록도이다.

도 4는 예시적 실시예에 따른 수신 장치의 구조를 도시한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0044] 이하, 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0045] 도 1은 중계기를 경유하여 데이터를 전송하는 중계기 전송 시스템을 설명한 도면이다.

[0046] 도 1에서는 하나의 송신 장치(110, 150), K개의 중계기(141, 142, 143, 144, 181, 182, 183, 184), 도청 장치(120, 160) 및 수신 장치(130, 170)를 포함하는 중계기 전송 시스템을 가정한다.

[0047] 도 1의 (a)는 전송 장치가 데이터를 복수의 중계기들로 전송하는 제2 단계를 설명한 도면이다.

[0049] 도 1의 (a)에서, 전송 장치(110)는 복수의 중계기(141, 142, 143, 144)로 데이터를 전송한다. 일측에 따르면, 복수의 중계기(141, 142, 143, 144)들은 데이터 수신하고, 수신된 데이터를 복호할 수 있다. 일측에 따르면, 복수의 중계기(141, 142, 143, 144)들은 데이터 복호에 성공할 수도 있고, 성공하지 못할 수도 있다.

[0050] 데이터 복호에 성공하지 못한 경우, 데이터 전송은 실패한 것으로 볼 수 있다. 따라서, 데이터 복호에 성공하지 못한 중계기들은 수신 장치(130)로 데이터를 전송하지 않는 것이 바람직하다.

[0051] 따라서, 중계기 선택 장치는 데이터 복호에 성공하지 못한 중계기들은 대상에서 제외하고, 데이터 복호에 성공한 중계기 중에서 데이터를 수신 장치(130)로 전송할 전송 중계기를 선택할 수 있다.

[0052] 일측에 따르면, 중계기 선택 장치는 데이터 복호에 성공한 중계기들을 포함하는 복호 중계기 집합을 구성할 수 있다. 중계기 선택 장치는 복호 중계기 집합에 포함된 복수의 중계기들 중에서, 수신 장치(130)를 향해 데이터를 전송하는 제1 중계기 및 도청 장치의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 제2 중계기를 선택한다.

- [0054] 도 1의 (b)는 복수의 중계기들 중에서 선택된 데이터 전송 중계기가 수신 장치 및 도청 장치에게 데이터를 전송하는 제2 단계를 설명한 도면이다.
- [0055] 도 1의 (a)에서 선택된 제1 중계기(182) 및 제2 중계기(183)는 데이터를 전송하고, 수신 장치(130)와 도청 장치(120)가 모두 데이터를 수신한다.
- [0056] 제안된 방법에 따라 선택된 제1 중계기(182) 및 제2 중계기(183)가 전송한 데이터를 수신한 수신 장치(170)는 성공적으로 데이터를 복호할 수 있으나, 도청 장치(160)는 데이터를 복호하지 못한다. 일측에 따르면, 중계기 선택 장치는 도청 장치(160)로 전송되는 데이터의 신호대잡음비(SNR: Signal to Noise Ratio)가 획기적으로 낮게 설정되도록 제1 중계기(182) 및 제2 중계기(183)를 선택할 수 있다.
- [0057] 도청 장치(160)가 수신한 신호를 성공적으로 복호하지 못하므로, 도 1에 도시된 중계기 전송 시스템의 보안은 물리 계층에서 지원된다고 할 수 있다.
- [0059] 도 2는 예시적 실시예에 따른 중계기 선택 장치의 구조를 도시한 블록도이다. 예시적 실시예에 따른 중계기 선택 장치(200)는 복호 중계기 집합 구성부(210) 및 중계기 선택부(220)를 포함한다.
- [0060] 복호 중계기 집합 구성부는 전송 장치로부터 데이터를 수신하고, 수신한 데이터를 성공적으로 복호한 복수의 중계기들을 복호 중계기 집합으로 구성한다.
- [0061] 중계기 선택부(220)는 복호 중계기 집합에 포함된 복수의 중계기들 중에서 복수의 전송 중계기를 선택한다. 복호 중계기 집합에 포함된 복수의 중계기들 중에서, 전송 중계기로 선택된 중계기들만이 수신 장치로 데이터를 전송할 수 있다.
- [0062] 일측에 따르면, 중계기 선택부(220)는 수신 장치를 향해 데이터를 전송할 제1 전송 중계기를 선택한다. 또한, 중계기 선택부(220)는 도청자의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기를 제2 전송 중계기로 선택할 수 있다.
- [0063] 일측에 따르면, 도 1의 (b)에 도시한 두 번째 단계에서 수신 장치가 수신하는 신호는 하기 수학식 1과 같다.
- [0065] [수학식 1]

$$y_D = \sqrt{P}(h_{R_{T_1},D} + h_{R_{T_2},D})x + n$$

- [0067]
- [0069] 여기서, y_D 는 수신 장치가 수신하는 신호이며, P 는 중계기의 전송 전력이다. $h_{R_{T_1},D}$ 는 제1 전송 중계기로부터 수신 장치까지의 채널 상태이고, $h_{R_{T_2},D}$ 는 제2 전송 중계기로부터 수신 장치까지의 채널 상태이다. $h_{R_{T_1},D}$ 와 $h_{R_{T_2},D}$ 는 평균이 0이고 분산이 1인 복소 정규분포 $CN(0,1)$ 를 따른다. x 는 중계기가 포워딩하는 데이터의 값이고, n 은 열잡음으로서, 분산이 1인 AWGN(Additive White Gaussian Noise) 성분을 나타낸다.

[0071] 또한, 도 1의 (b)에 도시한 두 번째 단계에서 도청 장치가 수신하는 신호는 하기 수학적 식 2와 같다.

[0073] [수학적 식 2]

[0075]

$$y_E = \sqrt{P}(h_{R_{T_1},E} + h_{R_{T_2},E})x + n$$

[0077] 여기서, y_E 는 도청 장치가 수신하는 신호이며, P 는 중계기의 전송 전력이다. $h_{R_{T_1},E}$ 는 제1 전송 중계기로부터 도청 장치까지의 채널 상태이고, $h_{R_{T_2},E}$ 는 제2 전송 중계기로부터 도청 장치까지의 채널 상태이다. $h_{R_{T_1},E}$ 와 $h_{R_{T_2},E}$ 는 평균이 0이고 분산이 1인 복소 정규분포 $CN(0,1)$ 를 따른다. x 는 중계기가 포워딩 하는 데이터의 값이고, n 은 열잡음으로서, 분산이 1인 AWGN(Additive White Gaussian Noise) 성분을 나타낸다.

[0079] 이 경우에, 보안 용량은 수신자가 성공적으로 복호할 수 있는 최대 전송율과 도청자가 데이터를 복호하여 도청에 성공할 수 있는 최대 전송율의 차이를 의미하며, 아래 수학적 식 3과 같이 정의될 수 있다.

[0081] [수학적 식 3]

[0083]

$$C_{prop}(R,H) = \frac{1}{2} \log_2 \left\{ \frac{1 + P|h_{R,D} + h_{H,D}|^2}{1 + P|h_{R,E} + h_{H,E}|^2} \right\}$$

[0085] 여기서, R 은 제1 전송 중계기를 나타내고, H 는 제2 전송 중계기를 나타낸다.

[0086] 일측에 따르면, 중계기 선택부(220)는 수학적 식 3에 정의된 보안 용량 값을 최대화하기 위한 제1 전송 중계기(R), 제2 전송 중계기(H)의 조합을 다음과 같이 선택할 수 있다.

[0088] [수학적 식 4]

$$\begin{aligned} (R^*, H^*) &= \arg \max_{\substack{R, H \in R_N \\ R \neq H}} C_{prop}(R, H) \\ &= \arg \max_{\substack{R, H \in R_N \\ R \neq H}} \left\{ \frac{1 + |h_{R,D} + h_{H,D}|^2}{1 + |h_{R,E} + h_{H,E}|^2} \right\} \end{aligned}$$

[0090]

[0092] 이 경우에, 보안 오류 확률은 아래 수학적식 5와 같이 결정될 수 있다.

[0094] [수학적식 5]

[0096]

$$S_{prop} = \Pr\{C_{prop}(R^*, H^*) < \gamma_S\}$$

[0098] 여기서, γ_S 는 데이터를 도청당하지 않고 안전하게 전송할 수 있는 보안 전송률(Secrecy rate)을 나타낸다.

[0100]

제1 전송 중계기(R), 제2 전송 중계기(H)는 수학적식 3에서 정의되는 보안 용량을 최대화하도록 선택된 중계기 조합으로서, 도청자의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기들의 조합이다.

따라서, 선택된 제1 전송 중계기(R), 제2 전송 중계기(H)를 이용하여 데이터를 중계기로부터 수신 장치로 포워딩하면, 도청자의 복호 확률은 감소하고, 수신 장치의 복호 확률은 향상된다. 일측에 따르면, 선택된

제1 전송 중계기(R), 제2 전송 중계기(H)는 도청자에게 전달되는 데이터의 신호대잡음비를 획기적으로 낮춰 도청 장치가 데이터를 물리적으로 복호하지 못하도록 할 수 있다.

[0103]

도 3은 예시적 실시예에 따른 중계기의 구조를 도시한 블록도이다. 예시적 실시예에 따른 중계기(300)는 수신부(310), 데이터 복호부(320) 및 데이터 전송부(330)를 포함한다.

[0104]

수신부(310)는 전송 장치로부터 데이터를 수신한다. 일측에 따르면, 수신부(310)가 전송 장치로부터 수신한 데이터는 부호화되어있을 수 있다.

[0105]

데이터 복호부(320)는 전송 장치로부터 수신한 데이터를 복호화한다. 일측에 따르면, 데이터 복호부(320)는 데이터 복호화에 실패할 수도 있다. 데이터 복호화에 실패한 경우, 중계기(300)는 수신한 데이터를 수신 장치로 포워딩하지 않는 것이 바람직하다.

[0106]

데이터 복호부(320)가 데이터 복호화에 성공한 경우, 중계기(300)는 전송 장치로부터 데이터를 수신하여 복호에

성공한 다른 중계기들과 함께 복호 중계기 집합에 포함된다. 수신 장치로 데이터를 포워딩할 전송 중계기는 복호 중계기 집합에 포함된 중계기들 중에서 선택된다.

[0107] 일측에 따르면, 복호 중계기 집합에 포함된 중계기들 중에서 도청자의 복호 확률과 수신 장치의 복호 확률을 고려하여 전송 중계기가 선택될 수 있다. 일측에 따르면, 복호 중계기 집합에 포함된 중계기들의 조합들 중에서, 도청자의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다.

[0108] 중계기(300)가 전송 중계기 조합에 포함된 경우, 데이터 전송부(330)는 수신 장치 및 도청 장치로 데이터를 전송한다. 도청 장치가 수신한 데이터는 신호대잡음비가 획기적으로 낮아진 상태이므로, 도청 장치는 수신한 신호를 복호하지 못한다.

[0109] 일측에 따르면, 수학식 3에서 정의된 보안 용량을 최대화하는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다. 또는 수학식 4를 만족하는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다.

[0111] 도 4는 예시적 실시예에 따른 수신 장치의 구조를 도시한 블록도이다. 예시적 실시예에 따른 수신 장치(400)는 수신부(410)를 포함한다.

[0112] 도 4에 도시된 수신 장치(400)는 전송 장치가 전송한 데이터를, 중계기를 경유하여 수신한다. 전송 장치는 복수의 중계기로 부호화된 데이터를 전송한다. 각 중계기는 전송 장치로부터 부호화된 데이터를 수신하고, 부호화된 데이터를 복호한다.

[0113] 전송 장치로부터 부호화된 데이터를 수신한 복수의 중계기들 중에서, 복호에 성공한 중계기들만이 복호 중계기 집합에 포함될 수 있다. 일측에 따르면, 복호 중계기 집합에 포함된 복수의 중계기들 중에서, 도청자의 복호 확률과 수신 장치의 복호 확률을 고려하여 수신된 데이터를 포워딩할 전송 중계기가 선택될 수 있다.

[0114] 일측에 따르면, 복호 중계기 집합에 포함된 중계기들의 조합들 중에서, 도청자의 복호 확률을 낮추고 수신 장치의 복호 확률을 높일 수 있는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다. 전송 중계기 조합에 포함된 중계기들은 수신한 데이터를 수신 장치로 포워딩한다. 수신 장치로 포워딩된 데이터는 도청 장치로도 전송될 수 있다. 도청 장치가 수신한 데이터는 신호대잡음비가 획기적으로 낮아진 상태이므로, 도청 장치는 수신한 신호를 복호하지 못한다.

[0115] 일측에 따르면, 수학식 3에서 정의된 보안 용량을 최대화하는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다. 또는 수학식 4를 만족하는 중계기들의 조합이 전송 중계기 조합으로 선택될 수 있다.

[0117] 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. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0118]

[0119] 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.

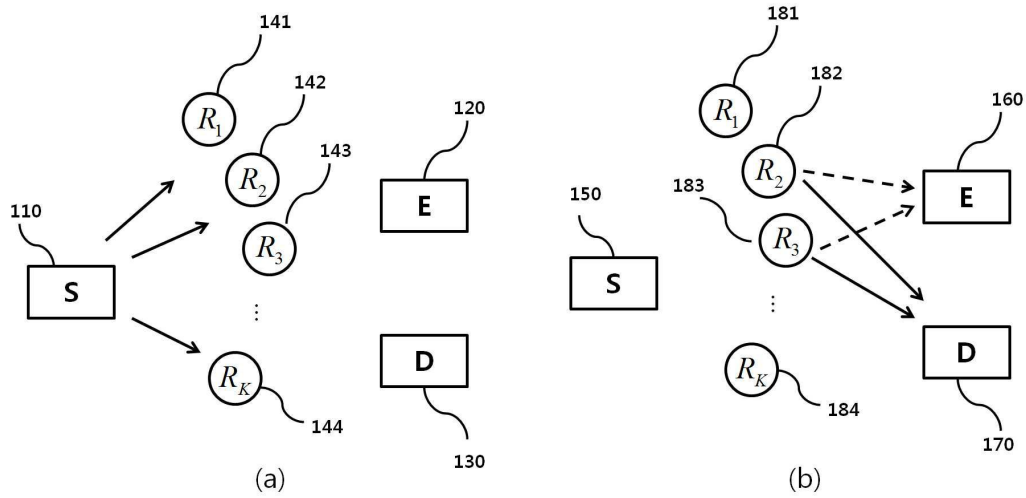
[0120] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

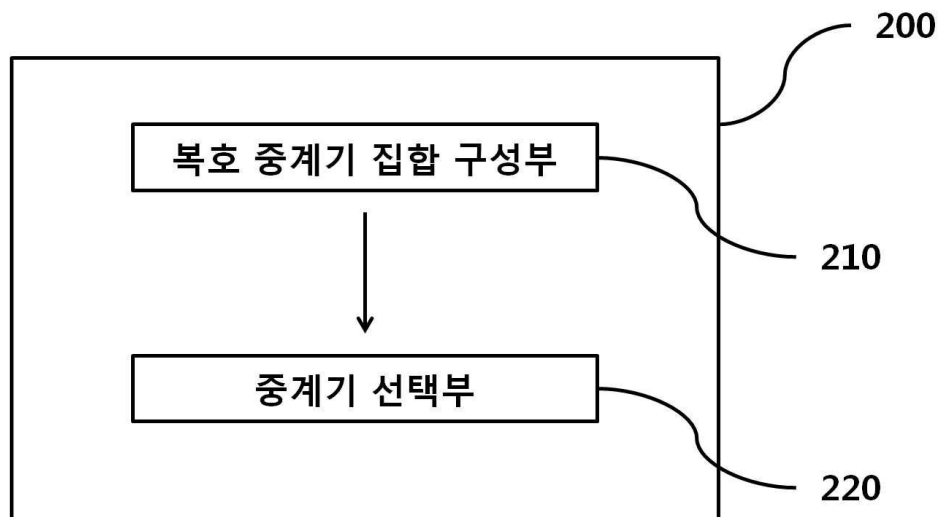
[0121] 200: 중계기 선택 장치
210: 복호 중계기 집합 구성부
220: 중계기 선택부

도면

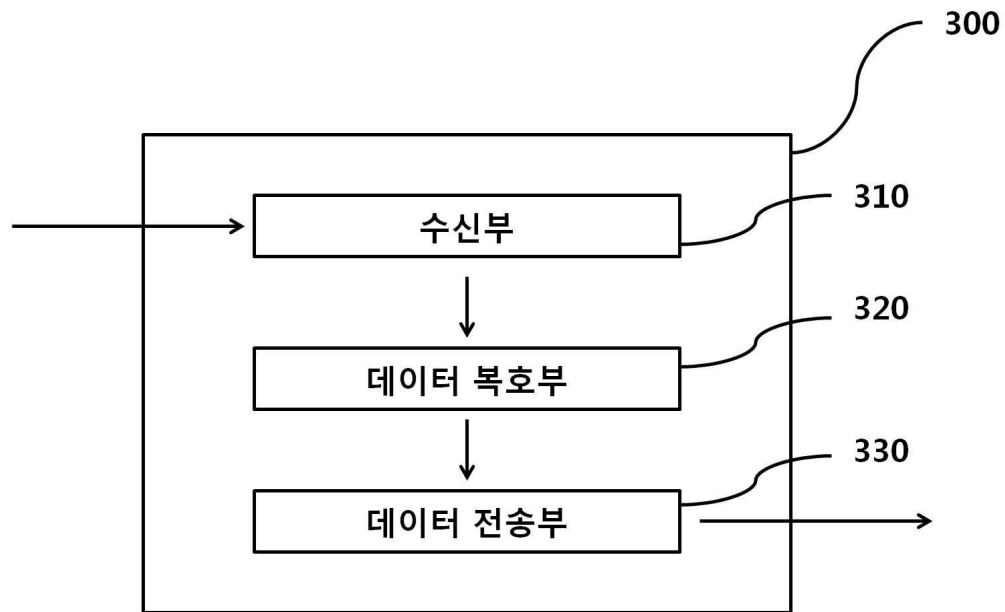
도면1



도면2



도면3



도면4

