



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0109948
(43) 공개일자 2017년10월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 27/34 (2006.01)
H04L 29/06 (2006.01) H04L 9/12 (2006.01)
(52) CPC특허분류
H04L 9/08 (2013.01)
H04L 27/34 (2013.01)
(21) 출원번호 10-2016-0034207
(22) 출원일자 2016년03월22일
심사청구일자 없음

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
명정호
대전광역시 유성구 도안동로 523, 212동 1902호
(봉명동, 호반베르디움)
(74) 대리인
성병기, 최윤서

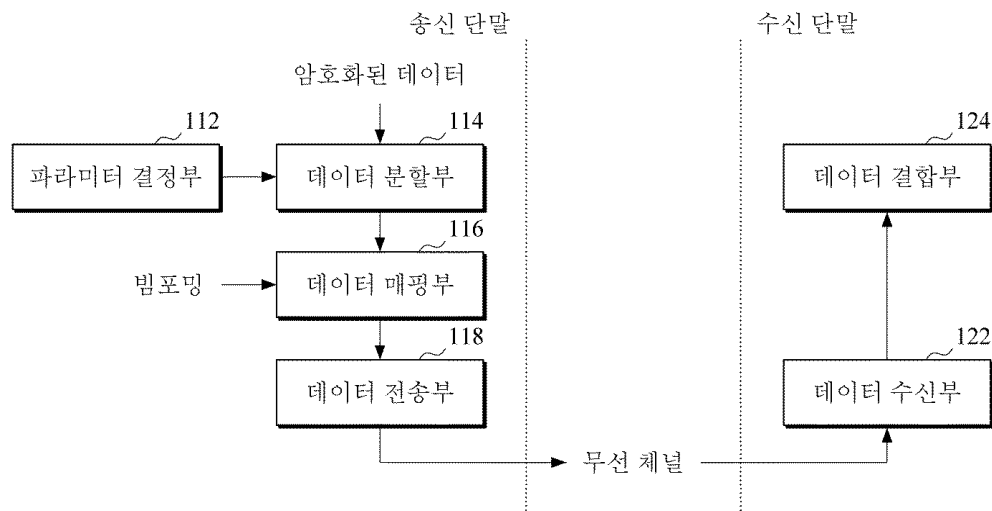
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 데이터 전송 보안이 강화된 데이터 전송 방법 및 이를 위한 무선 장치

(57) 요약

콘텐츠 적응적 임계치를 적용한 영상 콘텐츠의 샷 분할 기술이 개시된다. 본 발명에 따른 샷 분할 기술은 영상 콘텐츠에 대하여 샷을 분할하고자 할 때 샷 분할의 기준이 되는 임계치(threshold)를 콘텐츠에 적응적으로 구한 이후에 적용하는 과정을 포함한다. 일례로, 영상 콘텐츠에 대한 영상정보의 분석 및 가공 결과에 미리 설정되어 있는 고정 임계치를 적용하여 대상 영상 콘텐츠를 복수의 샷으로 분할한다. 그리고 분할의 결과로 얻어진 복수의 샷 각각에 대한 영상정보의 분석 및 가공을 통하여 변동 임계치를 구한 다음 이를 적용하여 복수의 샷 중에서 일부를 다시 복수의 샷으로 분할한다.

대표도 - 도2b



(52) CPC특허분류

H04L 63/04 (2013.01)

H04L 9/12 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711026593

부처명 미래창조과학부

연구관리전문기관 정보통신기술진흥센터

연구사업명 방송통신산업기술개발

연구과제명 SDN 기반 동적 네트워크 은닉 핵심 기술 개발

기 여 율 1/1

주관기관 한국전자통신연구원

연구기간 2015.03.01 ~ 2016.02.29

명세서

청구범위

청구항 1

무선 통신 시스템에서의 보안 데이터의 전송 방법에 있어서,

상기 보안 데이터의 분할에 적용할 복수 개의 파라미터를 결정하는 파라미터 결정 단계;

결정된 상기 파라미터에 기초하여 상기 보안 데이터를 T개의 조각 데이터들로 분할하는 단계; 및

상기 분할된 T개의 조각 데이터들을 변조한 다음 빔포밍 방식으로 전송하는 단계를 포함하고,

상기 복수 개의 파라미터는 크기 조절용 소수값(p), 상기 조각 데이터들의 개수(T), 필요 조각 데이터의 개수(K) 및 데이터 분할 과정에서 사용하는 (K-1)개의 랜덤 변수를 포함하는 것을 특징으로 하는 데이터 전송 방법.

발명의 설명

기술 분야

[0001] 본 발명은 무선 통신 기술에 관한 것으로, 보다 구체적으로 데이터 전송 보안이 강화된 데이터 전송 기술에 관한 것이다.

배경 기술

[0002] 무선 통신 시스템에서는 많은 암호화 기술이 적용되어 사용되고 있다. 이것은 기존 무선통신 채널의 보안은 암호화 기반으로 구성되어 있다는 것을 의미한다. 보다 구체적으로, 송신 단에서는 사전에 공유된 키(key)를 기반으로 데이터를 암호화하여 전송하고, 수신 단에서는 공유 키를 사용하여 수신된 암호화된 데이터를 복호화한다.

[0003] 하지만, 이러한 기존의 방법에 의하면 공유되고 있는 암호화/복호화 키가 노출된 상황에서는 더 이상 통신 보안이 보장되지 않는다. 이것은 기존의 기술들은 도청자가 적법한 사용자들이 사용하고 있는 암호화/복호화 키를 획득하는 것이 현실적으로 어렵거나 또는 쉽지 않다 등과 같은 사실에 의존하고 있을 뿐이고, 수학적으로나 현실적으로 불가능하다는 사실에 의존하고 있는 것은 아니기 때문이다. 일례로, 도청자가 이용 가능한 연산 능력이 증가할수록 기존의 방법이 갖는 보안 효과는 감소할 수 밖에 없으며, 현실적으로 도청자에 의하여 암호화/복호화 키가 탈취되거나 편취될 가능성도 높아진다.

[0004] 이러한 기존 암호화 방식의 한계를 극복하기 위하여 여러 가지 방식이 제안되고 있다. 일례로, 한국공개특허 제2011-0073563호, "무선 통신 네트워크에서 완벽한 비밀키의 생성"에서는 2개 또는 그 이상의 트랜스미버 사이에서 완벽한 랜덤 비밀키를 생성하는 기술이 개시되어 있는데, 이에 의하면 수신된 무선 신호에 기초하여 추정되는 채널 임펄스 응답(CIR)을 활용하여 랜덤 비밀키가 생성된다. 다른 예로, 한국공개특허 제2007-0055557호, "무선 통신 시스템에서의 OTA 통신의 암호화를 위한 방법 및 장치"에서는 물리 계층에서 심볼들을 암호화하는 기술이 개시되어 있는데, 이에 의하면 심볼들 각각에 위상 시프트 및 진폭 조정 중에서 적어도 하나를 적용하여 심볼들을 암호화하여 전송한다. 또 다른 예로, 한국등록특허 제1446629호, "무선 통신 시스템에서 보안 데이터 전송 장치 및 방법"에서는 무선 채널 상태로부터 물리계층 암호키 스트림을 생성하여 평문 데이터를 암호화하고 암호화된 데이터를 송신하는 기술이 개시되어 있는데, 이에 의하면 수신된 파일럿 신호에서 획득한 무선 채널 상태 정보를 활용한다.

[0005] 그러나 전술한 한국공개특허 제2011-0073563호와 한국등록특허 제1446629호는 기본적으로 암호화 기반으로 무선 통신 채널의 보안을 강화하고자 한다는 점에서, 기존의 방식과 동일한 한계가 있다. 그리고 한국공개특허 제2007-0055557호는 암호화를 위하여 추가로 비트스트림을 심볼로 나누고 또한 나누어진 심볼들에 대하여 위상 및/또는 진폭 변조를 수행하므로, 적용될 수 있는 무선 통신 시스템 등에 제한이 따른다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 한국공개특허 제2011-0073563호
(특허문헌 0002) 한국공개특허 제2007-0055557호
(특허문헌 0003) 한국등록특허 제1446629호

발명의 내용

해결하려는 과제

- [0007] 본 발명이 해결하고자 하는 하나의 과제는 기존의 암호화 기반 방식보다 데이터 전송 보안이 강화된 데이터 전송 방법 및 이를 위한 무선 장치를 제공하는 것이다.
- [0008] 본 발명이 해결하고자 하는 다른 하나의 과제는 기존의 암호화 기반 방식과 병행하여 사용할 수 있는 데이터 전송 방법 및 이를 위한 무선 장치를 제공하는 것이다.

과제의 해결 수단

- [0009] 상기한 과제를 해결하기 위한 본 발명의 일 실시예에 따른 무선 통신 시스템에서의 보안 데이터의 전송 방법은 상기 보안 데이터의 분할에 적용할 복수 개의 파라미터를 결정하는 파라미터 결정 단계, 결정된 상기 파라미터에 기초하여 상기 보안 데이터를 T개의 조각 데이터들로 분할하는 단계 및 상기 분할된 T개의 조각 데이터들을 변조한 다음 빔포밍 방식으로 전송하는 단계를 포함하고, 상기 복수 개의 파라미터는 크기 조절용 소수값(p), 상기 조각 데이터들의 개수(T), 필요 조각 데이터의 개수(K) 및 데이터 분할 과정에서 사용하는 (K-1)개의 랜덤 변수를 포함한다.

발명의 효과

- [0010] 전술한 본 발명의 실시예에 의하면, 무선 송수신기 사이의 무선 채널 정보를 활용하여 송신기는 데이터를 분할하여 전송하고 또한 수신기는 수신된 분할 데이터를 조립하여 복호화한다. 따라서 비록 도청자가 암호화 키를 알고 있더라도 전송되는 데이터에 관한 정보를 얻기 어렵게 함으로써, 도청 방지 등과 같은 무선 채널의 보안을 강화할 수 있다.

도면의 간단한 설명

- [0011] 도 1은 본 발명의 일 실시예에 따른 무선 데이터 전송 방법이 적용될 수 있는 무선 통신 시스템의 구성을 보여주는 도면이다.
- 도 2a는 본 발명의 일 실시예에 따른 무선 단말의 구성으로서 송수신 모듈을 모두 구비한 무선 단말의 구성을 보여주는 블록도이다.
- 도 2b는 도 2a에 도시된 무선 단말의 구성을 송신 단말과 수신 단말로 구분하여 도시한 것이다.
- 도 3은 동일한 무선 통신 환경에서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우와 기존의 데이터 전송 방법을 이용할 경우의 에러-확률(error-probability)을 비교하여 시뮬레이션한 결과의 일례이다.
- 도 4는 동일한 무선 통신 환경에서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우와 기존의 데이터 전송 방법을 이용할 경우의 에러-확률(error-probability)을 비교하여 시뮬레이션한 결과의 다른 예이다.

발명을 실시하기 위한 구체적인 내용

- [0012] 이하 첨부된 도면을 참조하여 실시예들을 보다 상세히 설명한다. 그러나 이러한 도면은 기술적 사상의 내용과 범위를 쉽게 설명하기 위한 예시일 뿐, 이에 의해 기술적 범위가 한정되거나 변경되는 것은 아니다. 그리고 이러한 예시에 기초하여 기술적 사상의 범위 안에서 다양한 변형과 변경이 가능함은 통상의 기술자에게는 당연할 것이다. 또한, 본 명세서에서 사용되는 용어 및 단어들은 실시예에서의 기능을 고려하여 선택된 용어들로서,

그 용어의 의미는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 따라서 후술하는 실시예들에서 사용된 용어는, 본 명세서에 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우는 통상의 기술자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.

[0013] 도 1은 본 발명의 일 실시예에 따른 무선 데이터 전송 방법이 적용될 수 있는 무선 통신 시스템의 구성을 보여주는 도면이다. 도 1에 도시된 무선 통신 시스템에는 송신 단말(transmitter)과 수신 단말(receiver) 외에 도청 단말(eavesdropper)도 존재한다. 그리고 송신 단말, 수신 단말 및 도청 단말은 모두 복수 개의 안테나를 구비하는 멀티안테나 장치이다. 보다 구체적으로, 도 1에서 송신 단말은 N_t 개의 안테나를 가지며, 수신 단말은 N_r 개 그리고 도청 단말은 N_e 개의 안테나를 가지고 있는 것으로 가정한 경우이다. 이 경우에, H 로 표시되어 있는 송신 단말과 수신 단말 사이의 무선 채널 정보는 $N_t \times N_r$ 크기의 매트릭스 정보로 구성되고, G 로 표시되어 있는 송신 단말과 도청 단말 사이의 무선 채널 정보는 $N_t \times N_e$ 크기의 매트릭스 정보로 구성된다. 이러한 무선 통신 시스템에 의하면, 송신 단말이 H 채널을 통해 수신 단말로 암호화된 데이터를 전송할 때, 그 암호화된 데이터는 무선 채널의 특성상 G 채널을 통해서 도청 단말에게도 전달될 수 있다.

[0014] 도 2a 및 도 2b는 본 발명의 일 실시예에 따른 무선 단말의 구성을 보여주는 블록도로서, 도 2a는 송수신 모듈을 모두 구비한 무선 단말을 도시한 것이며, 도 2b는 이해의 편의를 위하여 도 2a에 도시된 무선 단말의 구성을 송신 단말(즉, 송신 모듈을 구비한 무선 단말)과 수신 단말(즉, 수신 모듈을 구비한 무선 단말)로 구분하여 도시한 것이다. 도 2a 및 도 2b를 참조하면, 무선 단말(100)은 송신 모듈(110)과 수신 모듈(120)을 포함한다. 그리고 송신 모듈(110)은 파라미터 결정부(parameter determining unit, 112), 데이터 분할부(data dividing unit, 114), 데이터 맵핑부(data mapping unit, 116) 및 데이터 전송부(data transmitting unit, 118)를 포함하며, 수신 모듈(120)은 데이터 수신부(data receiving unit, 122) 및 데이터 결합부(data integrating unit, 124)를 포함한다.

[0015] 파라미터 결정부(112)는 송신 모듈(110)을 통해서 전송하고자 하는 데이터의 분할에 활용하는 변수 값을 설정 또는 결정하는 기능을 수행한다. 보다 구체적으로, 파라미터 결정부(112)는 분할된 데이터의 크기 조절에 필요한 임의의 소수값인 크기 조절용 소수값(p), 전송하고자 하는 데이터가 몇 개의 조각 데이터로 분할되는지를 나타내기 위한 분할 데이터의 전체 개수(T), T 개의 조각 데이터 중에서 수신 단말이 복호화에 성공하기 위하여 필요한 조각 데이터의 개수(K), 그리고 데이터의 분할 과정에 사용되는 $(K-1)$ 개의 임의의 랜덤 변수를 결정한다.

[0016] 파라미터 결정부(112)는 이러한 변수들을 다음과 같은 조건을 고려하여 결정할 수 있으며, 후술하는 조건을 만족한다면 파라미터 결정부(112)는 분할에 활용하는 변수 값을 시스템이나 사용자가 지정하는 값 및/또는 랜덤 변수로 결정할 수 있다. 다만, 상기 변수들 중에서 크기 조절용 소수값(p)은 송신 단말과 수신 단말 사이에서 약속한 패턴에 의하여 공유되어야 한다.

[0017] 우선, 전체 조각 데이터의 개수(T)와 필요 조각 데이터의 개수(K) 각각은 무선 채널 환경에 영향을 받는 변수이다. 보다 구체적으로, T 와 K 는 각각 송수신 단말 각각의 안테나의 개수, 전송시에 사용할 수 있는 독립적인 주파수의 개수, 안테나별 무선 채널의 상관 관계 등에 영향을 받을 수 있는데, 사용자나 무선 통신 시스템에서 특정값 또는 임의의 값으로 설정할 수 있다. 예를 들어, 전체 조각 데이터의 개수(T)의 최대값은 멀티 안테나 환경에서는 랭크(rank)값과 같거나 작아야 한다. 일례로, 상관 관계가 0인 경우에, 랭크값은 $\min(N_t, N_r)$ 으로 결정될 수 있다. 그리고 전체 조각 데이터의 개수(T)는 무선 통신 시스템의 송신 단말과 수신 단말 사이에 독립적으로 사용할 수 있는 채널 정보에 따라서 결정되는 변수인데, 무선 통신 시스템에서 송신 단말과 수신 단말 사이에서 독립적으로 사용할 수 있는 주파수의 개수(P) 보다 작거나 같다. 또한, 필요 조각 데이터의 개수(K)의 값 역시 전체 조각 데이터의 개수(T) 보다 작거나 같다는 것은 자명하다.

[0018] 데이터 분할부(114)는 파라미터 결정부(112)에 의하여 결정된 변수값들을 이용하여 전송하고자 하는 데이터를 T 개의 데이터로 분할하는 역할을 수행한다. 본 명세서에서 T 개를 구성하는 하나의 조각 데이터를 셰어(share)라고도 칭하기로 한다. i ($i \leq T$)번째 셰어(S_i)는 아래의 수학적 식 1과 같은 다항형 함수(polynomial function)의 수식을 통하여 구할 수 있다.

수학식 1

$$S_i = (a_0 + a_1i + \dots + a_{K-1}i^{K-1}) \bmod p$$

[0019]

[0020] 여기서, 변수 a_1 내지 a_{K-1} 은 파라미터 결정부(112)가 임의로 생성한 (T-1)개의 랜덤 변수에 해당하며, a_0 는 전송하고자 하는 데이터, 즉 보안 데이터(secret data)를 의미한다. 변수 p 또한 파라미터 결정부(112)가 결정한 임의의 소수값으로서, 전송한 바와 같이 수신 단말과 미리 공유된 값이다. 그리고 수학식 1에서 수식 'mod'는 모듈로(modulo) 연산을 의미한다.

[0021] 수학식 1과 같은 다항식 연산은 파라미터 결정부(112)에 의하여 결정되는 변수값에 따라서 다양하게 정의될 수 있는데, 예컨대 다음의 수학식 2에서 예시된 것과 같이 정의될 수 있다.

수학식 2

$a_0 = 1234$ (secret data), $T = 5$, $K = 3$, $p = 9839$ $a_1 = 166$, $a_2 = 94$ 일 경우,

$$S_1 = (1234 + 166*1 + 94*1) \bmod p = 1494$$

$$S_2 = (1234 + 166*2 + 94*2^2) \bmod p = 1942$$

$$S_3 = (1234 + 166*3 + 94*3^2) \bmod p = 2578$$

$$S_4 = (1234 + 166*4 + 94*4^2) \bmod p = 3402$$

$$S_5 = (1234 + 166*5 + 94*5^2) \bmod p = 4414$$

[0022]

[0023] 그리고 데이터 맵핑부(116)는 데이터 분할부(114)에 의하여 생성된 세어들($S_i \sim S_T$)에 대하여 변조(modulation) 과정을 수행한다. 그리고 데이터 전송부(118)는 사전에 송수신 단말 사이에 설정된 빔포밍(beamforming)을 통하여 변조된 데이터를 수신 단말로 전송한다. 이러한 과정을 거쳐서 송신 단말과 수신 단말 사이에서 데이터가 전송되는 과정을 수식으로 표현하면, 수학식 3과 같다.

수학식 3

$$y = H \cdot V \cdot x + n$$

[0024]

[0025] 여기서, y 는 수신 단말의 데이터 수신부(122)에서 수신되는 데이터를 표시하는 벡터이고, H 는 송신 단말과 수신 단말 사이의 무선 채널을 나타내는 벡터, V 는 빔 포밍 벡터, x 는 변조 과정을 거친 세어 정보로 구성된 벡터, n 은 노이즈 벡터를 가리킨다. 만약, 멀티 안테나가 아닌 주파수를 여러 개 사용하는 경우라면, 각 주파수 별로 변조된 세어 정보가 1:1로 매핑되어 전송된다.

[0026] 계속해서 도 2a 및 도 2b를 참조하면, 데이터 수신부(122)는 수신된 y 값을 이용하여 수신 빔포밍과 필터링을 통해 변조된 세어 정보를 추정(estimation)한다. 그리고 데이터 결합부(124)는 추정된 세어 정보를 이용하여 송신 단말이 송신한 데이터, 예컨대 보안 데이터(secret data)를 복원한다. 일례로, 데이터 결합부(124)는 수학식 4에 표시된 것과 같은 라그랑주 보간 다항식(Lagrange interpolating polynomial)을 계산하여 보안 데이터를 복원할 수 있다. 그리고 이러한 수학식 4는 수학식 1로 표시된 다항 함수에 따라서 달라질 수 있다는 것은 자명하다.

수학식 4

$$\sum_{j=1}^K \hat{S}_j \cdot \left[\prod_{k=1, k \neq j}^K \frac{i - i_k}{i_j - i_k} \right] \bmod p$$

[0027]

[0028]

예를 들어, 데이터 수신부(122)에서 추정된 세어의 값이 $S_2 = 1942$, $S_4 = 3402$ 그리고 $S_5 = 4144$ 인 경우라고 하자. 이 경우에, 데이터 결합부(124)는 추정된 S_2 , S_4 및 S_5 를 수학식 5에 적용하여 다항식을 전개하면 $1234 + 166i + 94i^2$ 가 되므로, 보안 데이터는 1234를 얻을 수 있다.

[0029]

이상에서 설명한 바와 같이, 본 발명의 실시예에 의하면, 송신 단말은 전송하고자 하는 데이터(예컨대, 보안 데이터)를 T개로 분할하여 전송을 하며, 수신 단말에서는 전송되는 T개의 조각 데이터 중에서 K개만 받아도 보안 데이터를 복원하는 것이 가능하다.

[0030]

도 3은 동일한 무선 통신 환경에서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우와 기존의 데이터 전송 방법을 이용할 경우의 에러-확률(error-probability)을 비교하여 시뮬레이션한 결과의 일례이다. 본 시뮬레이션에서 에러-확률이 낮으면 수신 단말 또는 도청 단말에서의 수신율이 좋은 것을 가리키며 또한 에러-확률이 높으면 수신 단말 또는 도청 단말에서의 수신율이 좋지 않은 것을 가리킨다. 따라서 우수한 전송 보안을 위해서는 수신 단말에서는 에러-확률이 낮고 도청 단말에서는 에러-확률이 높은 것이 바람직하다. 본 시뮬레이션에서 사용한 무선 통신 환경은 다음과 같다.

[0031]

- 채널 환경: 레일레이 플랫 페이딩 채널(Rayleigh flat fading channel)

[0032]

- 안테나 환경: 송신 단말의 안테나 개수(N_t)=8, 수신 단말의 안테나 개수(N_r)=8, 도청 단말의 안테나 개수(N_e)=8

[0033]

- 변조 방식: 직교 진폭 변조(Quadrature Amplitude Modulation, QAM)

[0034]

- 데이터 분할을 위한 파라미터: 하나의 보안 데이터를 8개의 세어로 분할하여 전송함(전체 조각 데이터의 개수(T)=8, 필요 조각 데이터의 개수(K)=4)

[0035]

- 비교 대상이 되는 기존의 데이터 전송 방법: 공간 다중화(Spatial Multiplexing, SM) 기법으로 8개의 보안 데이터를 생성하여 동시에 전송하는 방법과 하나의 보안 데이터를 다이버시티(Diversity) 기법으로 전송함

[0036]

도 3을 참조하면, 비교 대상이 되는 기존의 방법들 중에서, SM 기법을 사용하여 보안 데이터를 전송하는 경우에도 도청 단말(SM-8-QAM(eavesdropper))의 에러-확률이 높지만 수신 단말(SM-8-QAM(receiver))의 에러-확률도 역시 높다는 것을 알 수 있다. 이것은 수신 단말은 물론 도청 단말도 모두 보안 데이터를 수신하지 못하는 수신 불능의 상태가 되는 것을 의미한다. 그리고 다이버시티 기법을 사용하여 보안 데이터를 전송하는 경우에 수신 단말(Diversity-8-QAM(receiver))과 도청 단말(Diversity-8-QAM(eavesdropper)) 모두의 에러-확률이 낮다는 것을 알 수 있는데, 이것은 보안 데이터를 수신 단말은 물론 도청 단말도 잘 수신하고 있다는 것을 의미하므로, 도청이 용이하게 이루어질 수 있다는 것을 의미한다. 따라서 기존의 데이터 전송 방법의 경우에는 모두 일정한 한계가 있다는 것을 알 수 있다.

[0037]

반면, 본 발명의 실시예에 따른 방법을 이용하여 보안 데이터를 전송하는 경우에, 수신 단말(Sharing-8,4 QAM(receiver))의 에러-확률은 낮은 반면에 도청 단말(Sharing-8,4 QAM(eavesdropper))의 에러-확률이 높다는 것을 알 수 있다. 이것은 수신 단말의 경우에는 보안 데이터에 대한 수신율이 높아서 데이터 수신이 원활하게 이루어지는 반면에, 도청 단말의 경우에는 보안 데이터를 잘 수신하지 못하므로 도청이 잘 되지 않는다는 것을 의미한다. 따라서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우에 기존의 데이터 전송 방법에 비하여 무선 데이터 전송 효율이 우수한 것은 물론 데이터 전송 보안도 우수하다는 것을 알 수 있다.

[0038]

도 4는 동일한 무선 통신 환경에서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우와 기존의 데이터 전송 방법을 이용할 경우의 에러-확률(error-probability)을 비교하여 시뮬레이션한 결과의 다른 예이다. 도 4에 도시된 시뮬레이션 결과는 필요 조각 데이터의 개수(K)=5인 점에서 도 3에 도시된 시뮬레이션 결과(K=4)와

차이가 있으며, 나머지 무선 통신 환경은 도 3의 그것과 완전히 동일하다.

[0039] 도 4를 참조하면, 비교 대상이 되는 기존의 방법들, 즉 SM 기법을 사용하여 보안 데이터를 전송하는 경우(SM-8-QAM(receiver) 및 SM-8-QAM(eavesdropper))와 다이버시티 기법을 사용하여 보안 데이터를 전송하는 경우(Diversity-8-QAM(receiver) 및 Diversity-8-QAM(eavesdropper)) 모두 도 3을 참조하여 설명한 것과 동일한 한계가 있는 반면에 본 발명에 따른 데이터 전송 방법을 이용하는 경우(Sharing-8,4-QAM(receiver) 및 Sharing-8,4-QAM(eavesdropper))에는 무선 데이터 전송 효율이 우수한 것은 물론 데이터 전송 보안이 우수하다는 것을 알 수 있다. 또한, 도 3과 대비하면, 필요 조각 데이터의 개수(K)가 증가함에 따라서 수신 단말의 에러-확률이 증가하였으나 도청 단말의 에러 확률도 역시 증가한다는 것을 알 수 있다.

[0040] 이러한 도 3 및 도 4 각각에 개시되어 있는 시뮬레이션 결과를 비교하면, 본 발명의 실시예에서 도청 방지율과 수신 단말에 의한 수신율을 결정하는 중요한 파라미터가 필요 조각 데이터의 개수(K)라는 사실을 알 수 있다. 따라서 본 발명의 실시예에 따른 데이터 전송 방법을 이용할 경우에는 필요 조각 데이터의 개수(K)를 적절하게 설정 또는 조정함으로써 원하는 수신율과 도청 방지율을 얻을 수 있다.

[0041] 이상에서 설명한 바와 같이, 본 발명의 실시예에 의하면 송수신 단말 사이에 미리 공유된 소수값(p)을 적용하여 송신 단말은 보안 데이터를 소정의 개수로 분할한 다음 전송하며 수신 단말은 수신된 조각 데이터의 일부를 수신하여 조립함으로써 비밀 데이터를 복원한다. 따라서 본 발명의 실시예에 의하면, 비록 암호화 키가 유출된 상황이라고 하더라도 데이터의 분할 및 조립 과정을 통하여 물리계층에서 데이터를 보호할 수가 있다. 그리고 기존의 전송 방법과 비교하여, 수신 단말은 높은 수신율로 보안 데이터를 수신할 수 있으며 도청 단말의 도청율은 낮추는 것이 가능할 뿐만 아니라 파라미터 값의 조정을 통하여 사용자가 원하는 수신율과 도청율을 선택할 수가 있다. 뿐만 아니라, 설정된 조각 데이터의 개수(K) 이상으로 조각 데이터(세어)가 도청되지 않으면, 도청 단말은 보안 데이터를 수신하여 복호화하는 것이 불가능하므로 보안이 강화되는 효과가 있다.

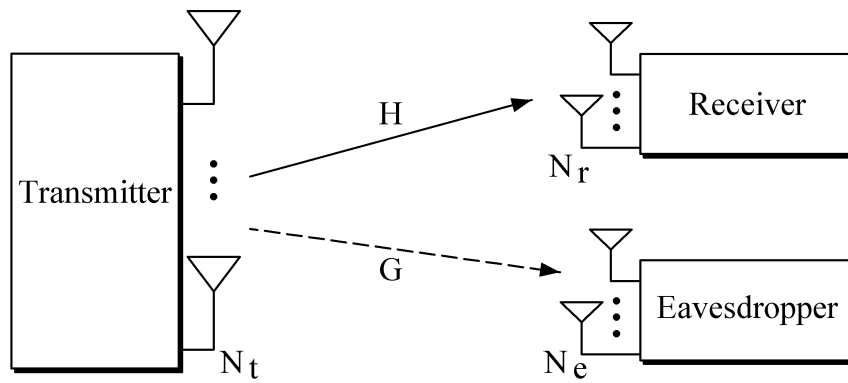
[0042] 이상의 설명은 실시예에 불과할 뿐, 이에 의하여 한정되는 것으로 해석되어서는 안된다. 본 발명의 기술 사상은 특허청구범위에 기재된 발명에 의해서만 특정되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다. 따라서 전술한 실시예가 다양한 형태로 변형되어 구현될 수 있다는 것은 통상의 기술자에게 자명하다.

부호의 설명

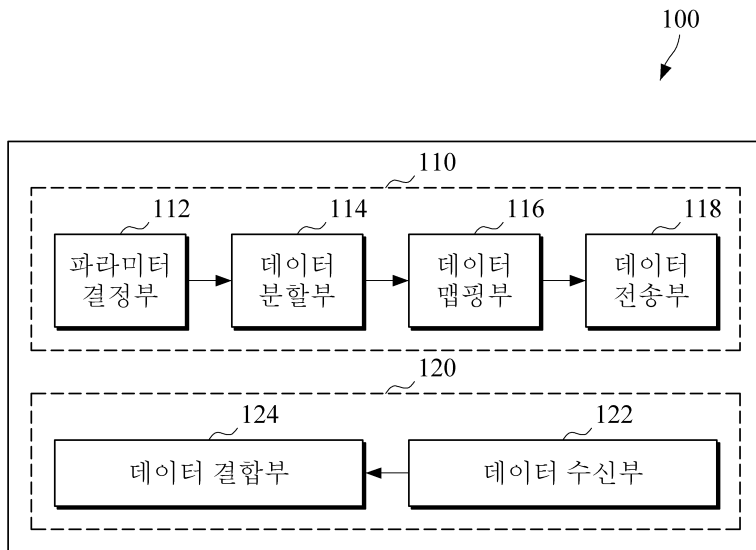
[0043] 110: 송신 모듈
112: 파라미터 결정부
114: 데이터 분할부
116: 데이터 맵핑부
118: 데이터 전송부
120: 수신 모듈
122: 데이터 수신부
124: 데이터 결정부

도면

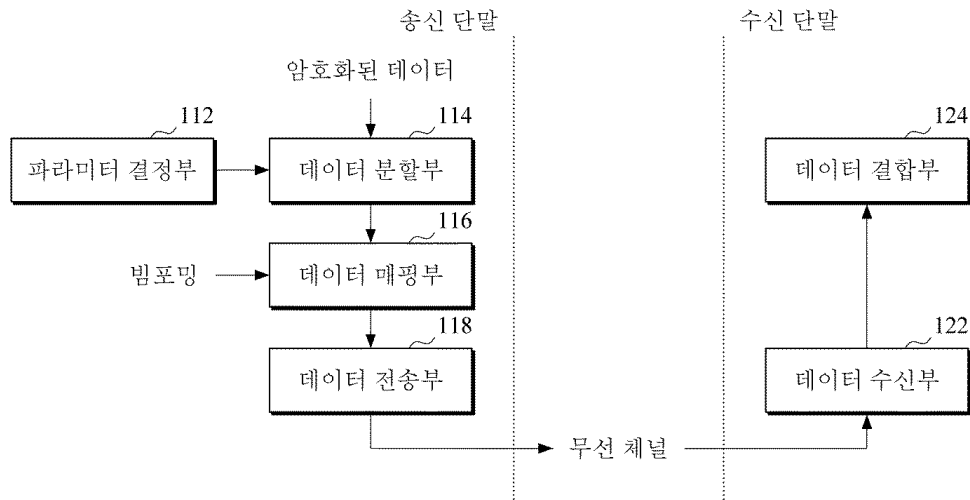
도면1



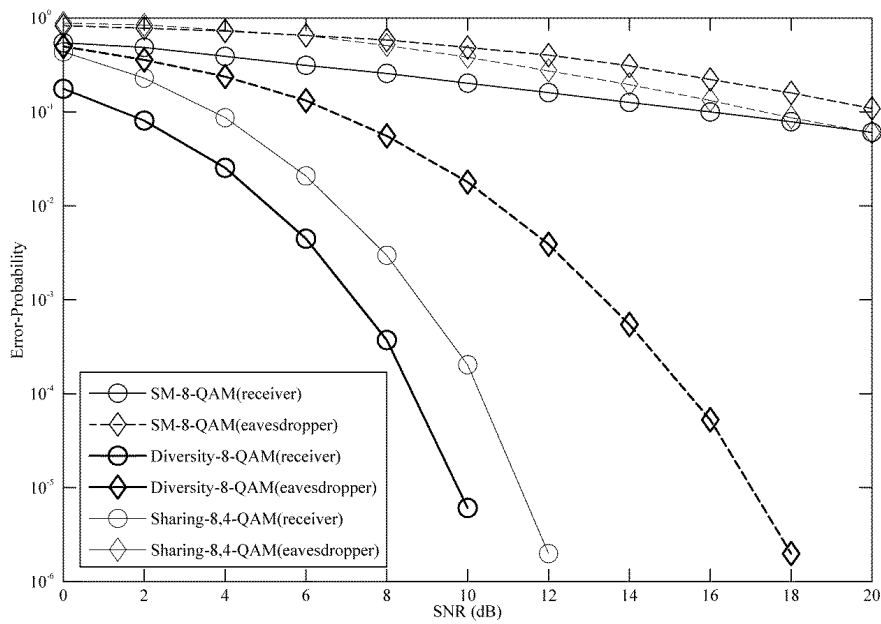
도면2a



도면2b



도면3



도면4

