(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0044692
(43) 공개일자 2015년04월27일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01)
(21) 출원번호 10-2013-0124056
(22) 출원일자 2013년10월17일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준
서울특별시 강남구 광평로10길 6 한솔마을아파트 206동 103호
권경훈
경기도 성남시 분당구 정자로 143 한솔마을LG아파트 203동 204호
(74) 대리인
이건주, 김정훈

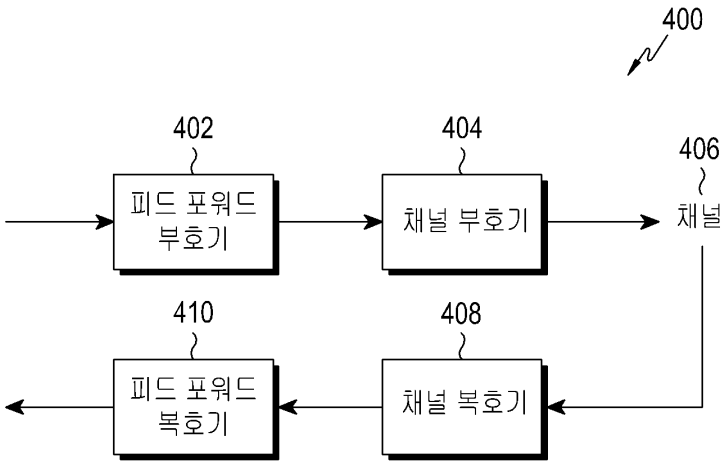
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **근거리 무선 통신 시스템에서 데이터를 암호화하는 장치 및 방법**

(57) 요 약

본 발명은 근거리 무선 통신 시스템에서 데이터를 암호화하는 방법에 있어서, 송신 단말이 현재 스테이트에서 송신할 데이터를, 미리 정해진 수신 단말은 상기 데이터 복원에 성공하고 미리 정해지지 않은 도청 단말은 상기 데이터 복원에 실패하도록 암호화하고, 암호화된 데이터를 오류 정정 부호를 통해 부호화하여 상기 미리 정해진 수신 단말에게 전송한다.

대 표 도 - 도4



명 세 서

청구범위

청구항 1

근거리 무선 통신 시스템에서 데이터를 암호화하는 방법에 있어서,

송신 단말이 현재 스테이트에서 송신할 데이터를, 미리 정해진 수신 단말은 상기 데이터 복원에 성공하고 미리 정해지지 않은 도청 단말은 상기 데이터 복원에 실패하도록 암호화하는 과정과,

암호화된 데이터를 오류 정정 부호를 통해 부호화하여 전송하는 과정을 포함하는 데이터 암호화 방법.

청구항 2

제1항에 있어서,

상기 암호화하는 과정은,

상기 현재 스테이트에서 송신할 데이터를 지연시켜 상기 현재 스테이트의 바로 이전 스테이트의 데이터를 생성하는 과정과,

상기 현재 스테이트에서 송신할 데이터를 코드 레이트 1을 갖도록 피드 포워드하고, 상기 피드포워드된 데이터와 상기 이전 스테이트의 데이터를 모듈로 연산하는 과정을 포함함을 특징으로 하는 데이터 암호화 방법.

청구항 3

제1항에 있어서,

상기 송신 단말과 상기 수신 단말 간에 송수신되는 데이터의 보안성을 보장하는 보안 채널의 용량은, 상기 송신 단말과 상기 수신 단말 간의 메인 채널 용량과 상기 메인 채널을 도청하는 상기 도청 단말의 도청 채널 용량의 차로 계산됨을 특징으로 하는 데이터 암호화 방법.

청구항 4

제3항에 있어서,

상기 보안 채널의 용량을 확보하기 위해서는, 상기 송수신되는 데이터의 신뢰성을 보장하기 위한 하기의 제1조건과 상기 송수신되는 데이터의 보안성을 보장하기 위한 하기의 제2조건이 만족되어야 함을 특징으로 하는 데이터 암호화 방법.

$\Pr\{M \neq M_B\} < \epsilon, \epsilon \approx 0$ (제1조건)

$I(M;M_E) = H(M) - H(M|M_E) = 0$ (제2조건)

여기서 M은 상기 현재 스테이트에서 송신할 데이터를 의미하고, M_B는 상기 수신 단말이 수신한 데이터를 의미하고, $\Pr\{M \neq M_B\}$는 상기 M과 상기 M_B가 동일하지 않을 확률을 의미하고, M_E는 상기 도청 단말이 수신한 데이터를 의미하고, H(M)은 상기 M의 불확정성을 의미하고, $H(M|M_E)$는 상기 M_E의 불확정성을 의미함.

청구항 5

근거리 무선 통신 시스템에서 암호화된 데이터를 복원하는 방법에 있어서,

현재 스테이트에서 수신된 데이터를 오류 정정 부호를 통해 암호화된 데이터로 복호하는 과정과,

상기 암호화된 데이터와 상기 현재 스테이트의 바로 이전 스테이트에서 복호된 데이터를 고려하여, 상기 현재 스테이트에서 수신된 데이터를 복원하는 과정을 포함하는 데이터 복원 방법.

청구항 6

제5항에 있어서

상기 데이터를 복원하는 과정은,

상기 현재 스테이트에서 수신된 데이터의 복호 데이터를 지연시켜 상기 현재 스테이트의 바로 이전 스테이트의 복호 데이터를 생성하는 과정과,

상기 암호화된 데이터의 연판정 값과 상기 이전 스테이트의 복호 데이터를 모듈로 연산하여 상기 암호화된 데이터를 복호하는 과정과,

상기 암호화된 데이터를 복호하는 과정을 미리 정해진 횟수만큼 반복하는 과정을 포함함을 특징으로 하는 데이터 복원 방법.

청구항 7

제6항에 있어서

상기 암호화된 데이터를 복호하는 과정이 상기 미리 정해진 횟수만큼 반복되면, 상기 암호화된 데이터의 연판정 값을 경판정 값으로 결정하는 과정을 더 포함함을 특징으로 하는 데이터 복원 방법.

청구항 8

근거리 무선 통신 시스템에서 데이터를 암호화하는 장치에 있어서,

송신 단말이 현재 스테이트에서 송신할 데이터를, 미리 정해진 수신 단말은 상기 데이터 복원에 성공하고 미리 정해지지 않은 도청 단말은 상기 데이터 복원에 실패하도록 암호화하는 제1부호기와,

암호화된 데이터를 오류 정정 부호를 통해 부호화하여 전송하는 제2부호기를 포함하는 데이터 암호화 장치.

청구항 9

제8항에 있어서,

상기 제1부호기는, 상기 현재 스테이트에서 송신할 데이터를 지연시켜 상기 현재 스테이트의 바로 이전 스테이트의 데이터를 생성하는 지연기와, 상기 현재 스테이트에서 송신할 데이터를 코드 레이트 1을 갖도록 피드 포워드하고, 상기 피드포워드된 데이터와 상기 이전 스테이트의 데이터를 모듈로 연산하는 연산기를 포함함을 특징으로 하는 데이터 암호화 장치.

청구항 10

제8항에 있어서,

상기 송신 단말과 상기 수신 단말 간에 송수신되는 데이터의 보안성을 보장하는 보안 채널의 용량은, 상기 송신 단말과 상기 수신 단말 간의 메인 채널 용량과 상기 메인 채널을 도청하는 상기 도청 단말의 도청 채널 용량의 차로 계산됨을 특징으로 하는 데이터 암호화 장치.

청구항 11

제10항에 있어서,

상기 보안 채널의 용량을 확보하기 위해서는, 상기 송수신되는 데이터의 신뢰성을 보장하기 위한 하기의 제1조건과 상기 송수신되는 데이터의 보안성을 보장하기 위한 하기의 제2조건이 만족되어야 함을 특징으로 하는 데이터 암호화 장치.

$\Pr\{M \neq M_B\} < \epsilon, \epsilon \approx 0$ (제1조건)

$I(M;M_E) = H(M) - H(M|M_E) = 0$ (제2조건)

여기서 M은 상기 현재 스테이트에서 송신할 데이터를 의미하고, M_B는 상기 수신 단말이 수신한 데이터를 의미하고, $\Pr\{M \neq M_B\}$는 상기 M과 상기 M_B가 동일하지 않을 확률을 의미하고, M_E는 상기 도청 단말이 수신한 데이터를 의미하고, H(M)은 상기 M의 불확정성을 의미하고, $H(M|M_E)$는 상기 M_E의 불확정성을 의미함.

청구항 12

근거리 무선 통신 시스템에서 암호화된 데이터를 복원하는 장치에 있어서,

현재 스테이트에서 수신된 데이터를 오류 정정 부호를 통해 암호화된 데이터로 복호하는 제1복호기와,

상기 암호화된 데이터와 상기 현재 스테이트의 바로 이전 스테이트에서 복호된 데이터를 고려하여, 상기 현재 스테이트에서 수신된 데이터를 복원하는 제2복호기를 포함하는 데이터 복원 장치.

청구항 13

제12항에 있어서

상기 제2복호기는, 상기 현재 스테이트에서 수신된 데이터의 복호 데이터를 지연시켜 상기 현재 스테이트의 바로 이전 스테이트의 복호 데이터를 생성하는 지연기와, 상기 암호화된 데이터의 연판정 값과 상기 이전 스테이트의 복호 데이터를 모듈로 연산하여 상기 암호화된 데이터를 복호하는 연산기를 포함하며,

상기 연산기는 상기 암호화된 데이터의 복호를 미리 정해진 횟수만큼 반복함을 특징으로 하는 데이터 복원 장치.

청구항 14

제13항에 있어서

상기 연산기는 상기 암호화된 데이터의 복호를 상기 미리 정해진 횟수만큼 반복하면, 상기 암호화된 데이터의 연판정 값을 경판정 값으로 결정함을 특징으로 하는 데이터 복원 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 장치간 직접 통신을 수행하는 근거리 무선 통신 시스템에서 데이터를 암호화하는 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 아주 가까운 거리의 무선 통신을 위한 기술을 근거리 무선 통신(NFC: Near Field Communication)이

라 칭하며, 대표적으로 중계기 없이 장치간 직접 통신을 수행하는 장치 대 장치(D2D: Device to Device) 통신이 상기 근거리 무선 통신에 포함된다.

[0003] 한편 물리 계층(Physical Layer)에서 오류 정정 부호에 관한 연구는 송신자와 수신자간에 전송된 데이터의 신뢰성을 높이면서 상기 데이터를 빠르게 전송하고 또한 상기 데이터가 빠르게 처리될 수 있는 방향으로 발전되어 왔다. 상기 오류 정정 부호에는 일례로 터보(turbo) 부호가 포함되며, 상기 터보 부호는 낮은 복잡도의 부호화 및 복호화 알고리즘으로 부가 백색 가우시안 잡음(AWGN: Additive White Gaussian Noise) 환경에서 비교적 적은 횟수의 반복 복호만으로 섀넌(Shannon)의 이론적 한계에 근접하는 매우 우수한 오류 정정 성능을 제공한다.

발명의 내용

해결하려는 과제

[0004] 그러나 장치 대 장치 통신에서 송신자와 수신자간의 무선 통신 채널은 누구에게나 개방되어 있기 때문에 무엇보다도 보안성이 취약할 수 밖에 없으며, 누구나 무선 통신 채널로 전송되는 데이터를 획득할 수 있기 때문에 보안성을 위협하는 존재를 검출하여 이러한 문제를 해결하는 데에는 큰 어려움이 있다.

[0005] 본 발명은 근거리 무선 통신 시스템에서 데이터를 암호화하는 장치 및 방법을 제안한다.

[0006] 또한 본 발명은 근거리 무선 통신 시스템에서 미리 정해진 수신 단말만이 데이터 복원에 성공하도록 상기 데이터를 암호화하는 장치 및 방법을 제안한다.

[0007] 또한 본 발명은 근거리 무선 통신 시스템에서 암호화된 데이터를 복원하는 장치 및 방법을 제안한다.

과제의 해결 수단

[0008] 본 발명에서 제안하는 방법은; 근거리 무선 통신 시스템에서 데이터를 암호화하는 방법에 있어서, 송신 단말이 현재 스테이트에서 송신할 데이터를, 미리 정해진 수신 단말은 상기 데이터 복원에 성공하고 미리 정해지지 않은 도청 단말은 상기 데이터 복원에 실패하도록 암호화하는 과정과, 암호화된 데이터를 오류 정정 부호를 통해 부호화하여 전송하는 과정을 포함한다.

[0009] 본 발명에서 제안하는 다른 방법은; 근거리 무선 통신 시스템에서 암호화된 데이터를 복원하는 방법에 있어서, 현재 스테이트에서 수신된 데이터를 오류 정정 부호를 통해 암호화된 데이터로 복호하는 과정과, 상기 암호화된 데이터와 상기 현재 스테이트의 바로 이전 스테이트에서 복호된 데이터를 고려하여, 상기 현재 스테이트에서 수신된 데이터를 복원하는 과정을 포함한다.

[0010] 본 발명에서 제안하는 장치는; 근거리 무선 통신 시스템에서 데이터를 암호화하는 장치에 있어서, 송신 단말이 현재 스테이트에서 송신할 데이터를, 미리 정해진 수신 단말은 상기 데이터 복원에 성공하고 미리 정해지지 않은 도청 단말은 상기 데이터 복원에 실패하도록 암호화하는 제1부호기와, 암호화된 데이터를 오류 정정 부호를 통해 부호화하여 전송하는 제2부호기를 포함한다.

[0011] 본 발명에서 제안하는 다른 장치는; 근거리 무선 통신 시스템에서 암호화된 데이터를 복원하는 장치에 있어서, 현재 스테이트에서 수신된 데이터를 오류 정정 부호를 통해 암호화된 데이터로 복호하는 제1복호기와, 상기 암호화된 데이터와 상기 현재 스테이트의 바로 이전 스테이트에서 복호된 데이터를 고려하여, 상기 현재 스테이트에서 수신된 데이터를 복원하는 제2복호기를 포함한다.

발명의 효과

[0012] 본 발명은 근거리 무선 통신 시스템에서 미리 정해진 적법한 수신 단말 이외의 도청 단말이 존재할 경우, 도청 단말의 도청에 대한 피해를 줄일 수 있는 물리 계층 보안 기술이 적용된 부호기를 제안하며, 이를 통해 상기 부호기의 처리 속도를 향상시키고 높은 신뢰도와 더불어 보안성을 최대화시킬 수 있는 장점이 있다.

도면의 간단한 설명

[0013] 도 1은 단말간 직접 통신이 적용되는 셀룰러 통신 시스템을 모델링한 도면,

도 2 본 발명의 일실시예에 따른 D2D 통신 시스템에서 송신 단말, 수신 단말 및 도청 단말 간의 채널들을 도시한 도면,

도 3은 본 발명의 일실시예에 따른 D2D 통신 시스템에서의 BER 성능 곡선과 보안 갭을 표시한 그래프,

도 4는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 구조를 도시한 도면,

도 5는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 피드포워드 부호기를 도시한 도면,

도 6은 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 피드포워드 복호기를 도시한 도면,

도 7는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 코드 레이트 1의 피드포워드 부호의 트랠리스 다이어그램을 도시한 도면,

도 8는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 부호화 동작을 도시한 순서도,

도 9는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 복호화 동작을 도시한 순서도,

도 10a는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 2364bits일 경우, 이진 위상 편의 변조 방식, 스크램블링 방식, 코드 레이트 1의 피드포워드 부호 방식의 BER/FER 성능 비교를 도시한 그래프,

도 10b는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 2364bits일 경우, 이진 위상 편의 변조 방식, 스크램블링 방식, 코드 레이트 1의 피드포워드 부호 방식의 보안 갭 성능 비교를 도시한 그래프,

도 11a는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 6144bits일 경우, 이진 위상 편의 변조 및 터보 부호 방식, 스크램블링 및 터보 부호 방식 방식, 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식의 BER/FER 성능 비교를 도시한 그래프,

도 11b는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 6144bits일 경우, 이진 위상 편의 변조 및 터보 부호 방식, 스크램블링 및 터보 부호 방식 방식, 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식의 보안 갭 성능 비교를 도시한 그래프.

발명을 실시하기 위한 구체적인 내용

[0014] 이하, 본 발명의 바람직한 실시예를 첨부된 도면을 참조하여 상세히 설명한다. 하기의 설명에서는 본 발명의 동작을 이해하는데 필요한 부분만을 설명하며 그 이외의 배경 기술은 본 발명의 요지를 흩트리지 않도록 생략한다.

[0015] 본 명세서에서는 설명의 편의를 위해 단말간 직접 통신을 수행할 시 수신 측으로 동작하는 단말을 '수신 단말'이라 칭하고, 송신 측으로 동작하는 단말을 '송신 단말'이라 칭한다.

[0016] 도 1은 단말간 직접 통신이 적용되는 셀룰러 통신 시스템을 모델링한 도면이다.

[0017] 도 1을 참조하면, 도시된 통신 시스템은 기지국(108)과, 상기 기지국(108)과 데이터를 송수신하는 중계국(110) 및 단말(112)과, 상기 중계국(110)과 데이터를 송수신하는 송신 단말(102)과, 상기 송신 단말(102)과 데이터를 송수신하는 수신 단말(104)과, 상기 송신 단말(102)과 상기 수신 단말(104)이 송수신하는 데이터를 도청하는 도청 단말(106)을 포함한다. 여기서는 도청 단말(106)을 특정 하나의 단말로 예를 들어 설명하나, 도청 단말(106)은 송신 단말(102)의 주변 단말들 중 어느 단말도 될 수 있다.

[0018] 송신 단말(102)은 미리 정해진 적법한 단말, 즉 수신 단말(104)에게 데이터를 전송한다. 그러나 상기 수신 단말(104)의 주변 단말인 도청 단말(106)이 도청을 시도할 경우, 상기 데이터는 상기 수신 단말(104)뿐만이 아닌 상기 도청 단말(106)에게도 수신될 수 있으며, 이 경우 데이터의 보안성에 대한 문제가 발생될 수 있다.

[0019] 후술할 본 발명의 실시예에서는 이러한 데이터의 보안성 문제를 해결하기 위해, 즉 데이터의 보안성을 확보하기

위해 수신 단말(104)은 데이터 복원에 성공하고 도청 단말(106)은 데이터 복원에 실패하게 만드는 오류 정정 부호를 제안한다.

[0020] 도 2는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 송신 단말, 수신 단말 및 도청 단말 간의 채널들을 도시한 도면이다.

[0021] 도 2에서는 송신 단말(200), 수신 단말(204) 및 도청 단말(208)로 구성되는 D2D 통신 시스템을 가정하며, 송신 단말(200)과 수신 단말(204)간의 채널을 메인 채널(main channel)(202)이라 정의하고, 상기 메인 채널(202)을 도청하는 도청 단말(208)의 채널을 도청 채널(wiretap channel)(206)이라 정의한다. 이때 메인 채널(202)은 도청 채널(206)보다 채널 상태가 양호함을 가정하며, 송신 단말(200)과 도청 단말(208) 사이에서의 보안 채널 용량(secrecy channel capacity) C는 하기 수학식 1과 같이 계산될 수 있다. 여기서 보안 채널이란 송수신되는 데이터의 보안성을 보장하는 채널을 의미한다.

수학식 1

[0022] $$C = \left\{\frac{1}{2}\log\left(1+\frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_E^2}\right)\right\}^+$$

[0023] 즉 보안 채널 용량 C는 메인 채널 용량과 도청 채널 용량의 차로 계산된다. 수학식 1에서 P는 수신 신호 전력을 의미하고, σ_B^2는 수신 단말의 잡음 변화량(noise variance)을 의미하고, σ_E^2는 도청 단말의 잡음 변화량을 의미한다.

[0024] 보안 채널 용량 C를 확보하기 위해서는 완벽 보안 상황, 즉 송수신되는 데이터의 보안성과 신뢰성 모두가 만족되는 상황을 가정해야 한다. 완벽 보안 상황을 가정하기 위해 도청 채널(206)의 혼란(confusion)의 정도를 결정하기 위한 기준으로 도청 채널(206)의 모호 정도(equivocation)를 나타내는 $\Delta = \frac{1}{k}H(M|M_E)$정보가 필요하다. 또한 완벽 보안 상황을 가정하기 위해서는 하기의 두 가지 조건이 고려되어야 한다. 즉 해당 데이터의 신뢰성이 보장되기 위해서는 제1조건이 만족되어야 하고, 해당 데이터의 보안성이 보장되기 위해서는 제2조건이 만족되어야 한다.

[0025] $\Pr\{M \neq M_B\} < \epsilon, \epsilon \approx 0$: 신뢰성 보장 (제1조건)

[0026] $I(M;M_E) = H(M) - H(M|M_E) = 0$: 보안성 보장 (제2조건)

[0027] 또한 제1 및 제2조건을 통해 완벽 보안이 보장되기 위해서는 수신 단말(204)의 수신 신호 대 잡음비(SNR: Signal-to-Noise Ratio)가 도청 단말(208)의 수신 SNR보다 커야 한다. 즉 도청 단말(208)의 수신 SNR이 수신 단말(204)의 수신 SNR보다 낮을 경우에만 물리계층의 보안성 유지가 가능하다. 그러나 만약 도청 단말(208)의 수신 SNR이 수신 단말(204)의 수신 SNR보다 높을 경우에는 상위계층의 암호학을 기반으로 보안성을 유지시켜야 한다.

[0028] 생성된 데이터 M의 비트 정보 0과 1의 생성 확률이 서로 동일한 확률임을 가정하면, 상기 생성된 데이터 M의 불확정성 H(M)의 값은 1이 된다. 또한 도청 단말(208)이 수신한 데이터 M_E가 0.5의 비트 에러율(BER: Bit Error Rate)을 가지게 되면, 상기 수신한 데이터 M_E의 불확정성 $H(M|M_E)$의 값도 1이 된다. 즉 앞서 설명한 완벽 보안이 보장되기 위한 제2조건, 즉 보안성 보장의 조건이 만족되며, 이는 낮은 수신 SNR값을 가지는 영역에서의 BER이 0.5인 것과 동일한 의미를 갖는다.

[0029] 또한 수신 단말(204)이 수신한 데이터 M_B의 높은 신뢰성을 보장하기 위해 상기 수신한 데이터 M_B의 BER $\Pr\{M \neq M_B\}$이 0에 근접하게 된다면, 앞서 설명한 완벽 보안이 보장되기 위한 제1조건, 즉 신뢰성 보장의 조건이 만족된다. 이는 마찬가지로 높은 수신 SNR 값을 가지는 영역에서의 BER이 0에 근접한 값을 가진다는 것을 의미한다.

[0030] 도시된 도면에서 M은 송신 단말(200)이 생성한 데이터를 의미하고, X는 데이터 M을 부호화한 데이터를

의미하고, 부호화된 데이터 X는 메인 채널(202)를 통과한다. Y는 부호화된 데이터 X가 메인 채널(202)을 통과한 뒤 수신 단말(204)에 의해 복호된 데이터를 의미하고, Z는 부호화된 데이터 X가 도청 채널(206)을 통과한 뒤 도청 단말(208)에 의해 복호된 데이터를 의미한다. 여기서 상기 복호된 데이터 Y,Z 각각은 M_B, M_E 각각과 동일한 의미로 사용되었다.

[0031] 이하에서는 본 발명의 일실시예에 따른 보안성을 위한 오류 정정 부호에 대해 보다 상세히 설명하도록 한다.

[0032] 송신 단말(200)은 생성한 데이터 M을 전송하기 이전에 먼저 암호화를 수행한다. 일례로 생성한 데이터의 시퀀스를 벡터 u로 정의하고, 암호화된 데이터의 시퀀스를 벡터 m으로 정의하면, 상기 생성한 데이터와 암호화된 데이터 사이에는 하기와 같은 수학식이 성립된다.

수학식 2

[0033] $$m = u \cdot S$$

[0034] S는 벡터 u암호화시키기 위한 행렬로서 역(inverse) 행렬이 존재하는 비특이(non-singular) 행렬로 구성이 가능하다. 본 발명의 일실시예에서는 암호화 행렬 S로서 하기와 같은 이중 대각(dual diagonal) 행렬을 사용한다.

수학식 3

[0035] $$S = \begin{bmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{bmatrix}$$

[0036] 상기와 같은 이중 대각 행렬 S를 통해 암호화된 메시지 m은 행렬식을 통해 현재 스테이트(state)에서의 비트(bit)와 바로 이전 스테이트에서의 비트 간의 모듈로(modulo) 연산을 통한 값으로 암호화가 진행됨을 알 수 있다.

수학식 4

[0037] $$\begin{aligned} m_1 &= u_1 \\ m_2 &= u_1 + u_2 \\ m_3 &= u_2 + u_3 \\ &\vdots \\ m_n &= u_{n-1} + u_n \end{aligned}$$

[0038] 수학식 4의 규칙성으로 볼 때, 암호화 행렬 S의 생성 다항식(generator polynomial)은 하기 수학식 5과 같이 정의될 수 있다.

수학식 5

[0039] $$g(D) = 1 + D$$

[0040] 즉 수학식 5의 생성 다항식을 통해서 레지스터(regigster) 한 개를 가지는 길쌈 부호기(convolution encoder)의 구성이 가능하게 된다. 상기 생성 다항식에서 1의 의미는 레지스터 이전에 비트에 대해서 에지(edge)가 형성되어 있음을 의미하고, D의 의미는 레지스터 이후의 비트에 대해서 에지가 형성되어 있음을 의미한다. 여기서 에

지라 함은 레지스터 이전 비트가 레지스터 이후로 피드포워드 되어 입력되는 것을 의미하며, 결과적으로 본 발명의 일실시예에 따른 보안성을 위한 오류 정정 부호는 레지스터를 기준으로 레지스터 이전 비트와 레지스터 이후 비트의 모듈로 연산을 통해서 정해진다.

[0041] 도 3은 본 발명의 일실시예에 따른 D2D 통신 시스템에서의 BER 성능 곡선과 보안 갭을 표시한 그래프이다

[0042] 도 3을 참조하면, 물리계층 기반의 보안 시스템에서 보안성 및 신뢰성에 대한 성능은 BER 기준의 성능을 지표로 삼는다. 도시한 그래프의 가로축은 수신 단말 및 도청 단말 각각에 대한 수신 SNR을 나타내고, 세로축은 수신 단말 및 도청 단말 각각에 대한 BER을 나타낸다. 또한 $P^{B}_{e,max}$ 는 수신 단말의 오류 확률의 최대값을 나타내고, $P^{E}_{e,min}$ 은 도청 단말의 오류 확률의 최소값을 나타낸다.

[0043] 데이터의 신뢰성이 보장되는 신뢰성 영역(302)은 BER 기준으로 10^{-5}의 오류율을 가지는 구간이고, 데이터의 보안성이 보장되는 보안성 영역(300)은 BER 기준으로 0.5의 오류율을 가지는 구간이다.

[0044] 또한 보안 갭(security gap)(304)은 신뢰성 영역(302)의 SNR 값, 즉 BER 10^{-5}을 가지는 SNR 값($SNR_{B,min}$)와 BER 0.5를 가지는 SNR 값($SNR_{E,max}$)의 차이로 정의된다.

[0045] 도 4는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 구조를 도시한 도면이다.

[0046] 도 4를 참조하면, 단말(400)은 피드포워드 부호기(402)와, 채널 부호기(404)와, 채널 복호기(408)와, 피드포워드 복호기(410)를 포함한다. 여기서 상기 채널 부호기(404) 및 채널 복호기(408) 각각은 일례로 터보 부호기 및 터보 복호기가 될 수 있다.

[0047] 단말(400)은 피드포워드(feed-forward) 부호기(402)에 데이터가 입력되면, 입력된 데이터에 앞서 설명한 암호화 행렬 S를 적용하여 암호화하고 암호화된 데이터를 채널 부호기(404)로 출력한다. 채널 부호기(404)는 암호화된 데이터를 오류 정정 부호를 통해 부호화한 최종 데이터를 채널(406)상으로 출력한다. 여기서 상기 채널은 메인 채널 또는 도청 채널 등이 될 수 있다.

[0048] 채널 복호기(408)은 메인 채널을 통해 수신되는 최종 데이터를 입력하고 오류 정정 부호를 통해 복호하여 피드포워드 복호기(410)로 출력한다. 피드포워드 복호기(410)는 복호된 데이터의 암호를 해독하고 최초 데이터를 복원하여 출력한다.

[0049] 이하에서는 도 5를 통해 상기 피드포워드 부호기(402)의 상세 동작을 설명하고, 도 6을 통해 상기 피드포워드 복호기(410)의 상세 동작을 설명하도록 한다.

[0050] 도 5는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 피드포워드 부호기를 도시한 도면이다.

[0051] 도 5를 참조하면, 피드포워드 부호기는 송신 단말이 생성한 데이터 벡터 u_n이 입력되면, 데이터 벡터 u_n을 암호화하고 암호화된 데이터 벡터 m_n을 출력한다. 이때 피드포워드 부호기는 데이터 벡터 u_n을 수학식 5의 생성 다항식에 따라, 미리 정해진 수신 단말인 적법한 단말은 데이터 복원에 성공하고 미리 정해진 수신 단말이 아닌 도청 단말은 데이터 복원에 실패하도록 암호화한다. 여기서 n은 데이터 인덱스를 나타낸다.

[0052] 상기 암호화 과정을 보다 상세히 설명하면, 피드포워드 부호기는 현재 스테이트에서 입력된 데이터 벡터 u_n을 지연기(500) 이후로 피드포워드하고, 피드포워드 부호기의 연산부(502)는 피드포워드된 데이터 벡터 u_n과 상기 지연기(500)를 통과한 데이터 벡터 u_{n-1}을 모듈로 연산하여 암호화된 데이터 벡터 m_n을 생성한 뒤 출력한다. 본 발명에서는 일례로 코드 레이트(code rate) 1의 피드포워드 부호기를 고려하며, 여기서 코드 레이트 1이라 함은 입력된 데이터 벡터 u_n을 구성하는 정보 비트들의 수가 피드포워드된 데이터 벡터 u_n을 구성하는 정보 비트들의 수와 동일함을 나타낸다. 또한 지연기(500)를 통과한 데이터 벡터 u_{n-1}은 현재 스테이트의 바로 이전 스테이트에

서 입력된 데이터 벡터와 동일하다.

[0053] 피드포워드 부호기를 통해 출력된 암호화된 데이터 벡터 m_n은 이후 채널 부호기에 입력되고, 상기 채널 부호기는 오류 정정 부호를 통해 상기 암호화된 데이터 벡터m_n으로부터 최종 코드워드(codeword)를 생성하여 출력한다. 상기 코드워드는 채널을 통해 전송되며, 수신 단말과 도청 단말은 각각 메인 채널과 도청 채널을 통해 상기 코드워드를 수신한다.

[0054] 피드포워드 부호기는 지연기(500)를 이용한 일종의 터보 부호기이므로 비터비(viterbi) 알고리즘을 사용할 수 있다. 또한 비터비 알고리즘에서 사용되는 복호 알고리즘들 중에서 BCJR(Bahl, Cocke, Jelinel Raviv) 알고리즘이 트랠리스(trellis) 부호로 정의된 오류 정정 부호를 위한 MAP(maximum a posteriori) 복호이기 때문에 가장 우수한 성능을 가진다. 따라서 피드포워드 부호기는 상기 BCJR 알고리즘을 피드포워드 부호의 복호 알고리즘으로 사용한다.

[0055] 도 6은 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 피드포워드 복호기를 도시한 도면이다.

[0056] 도 6을 참조하면, 채널 복호기(도시하지 않음)는 송신 단말로부터 수신되는 코드워드를 수신하여 복호한다. 이때 수신 단말은 메인 채널을 통해 상기 코드워드를 수신하고, 도청 단말은 도청 채널을 통해 상기 코드워드를 수신한다.

[0057] 상기 복호 과정을 보다 상세히 설명하면, 먼저 내부부호로 사용된 오류 정정 부호의 복호 과정을 통해 채널에서 발생된 오류를 정정한다. 보안성이란 오류 정정 과정을 모두 완료한 다음의 잔여 오류에 대해서 암호화 메시지에 대한 해독을 불가능하게 만드는 것이기 때문에, 오류 정정 후의 잔여 오류가 도청 단말의 복호 실패율이 최대가 될 수 있도록 조절해야 한다.

[0058] 피드포워드 복호기는 오류 정정 부호를 통해 복호된 데이터의 최종 확률 정보를 이용해 수신된 데이터 벡터 m_n에 대한 복호를 수행한다. 즉 피드포워드 복호기의 연산부(602)는 현재 스테이트의 바로 이전 스테이트에서 복호된 데이터 벡터 $\hat{u}_{n-1}$을 현재 스테이트에서 수신된 데이터 벡터 m_n과 모듈러 연산하여 최종적으로 현재 스테이트에서 복호된 데이터 벡터 $\hat{u}_n$을 생성한다. 본 발명에서는 일례로 코드 레이트 1의 피드포워드 복호기를 고려하며, 여기서 코드 레이트 1이라 함은 입력된 데이터 벡터 u_n을 구성하는 정보 비트들의 수가 피드포워드된 데이터 벡터 u_n을 구성하는 정보 비트들의 수와 동일함을 나타낸다.

[0059] 상기 연산부(602)의 복호 동작은 하기 수학식 6과 같이 나타낼 수 있다.

수학식 6

[0060] $$\hat{u}_n = m_n + \hat{u}_{n-1}$$

[0061] 수학식 5에서의 생성 다항식과 복호 다항식과의 곱은 $g(D)\cdot g^{-1}(D)=1$ 을 만족해야 하므로, 복호 다항식 $g^{-1}(D)$ 은 하기 수학식 7과 같이 정의될 수 있다.

수학식 7

[0062] $$g^{-1}(D)=\frac{1}{1+D}$$

[0063] 피드포워드 복호기 구조는 반복적으로 이전 복호 데이터 벡터가 계속해서 누적되는 형태이기 때문에, 어느 한곳에서 오류가 발생하게 되면 오류가 계속적으로 누적되어서 최종적으로는 오류 전파(error propagation) 현상이

발생하게 되는 것을 알 수 있다. 그러나 미리 정해진 적법한 수신 단말 역시 한 개의 잔여오류가 발생하게 되면 오류가 계속적으로 누적되어 오류 전파 현상이 발생하게 된다.

[0064] 따라서 피드포워드 복호기는 이러한 오류 전파 현상을 줄이기 위해 경판정(hard decision) 복호 방식이 아닌 연판정(soft decision) 복호 방식을 사용한다. 즉 피드포워드 복호기는 연판정 복호 방식에 따른 값을 코드 레이트 1의 피드 포워드 복호기를 통해 복호한다.

[0065] 도 7는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 코드 레이트 1의 피드포워드 부호의 트랠리스 다이어그램을 도시한 도면이다.

[0066] 도 7을 참조하면, 이전 스테이트의 값이 0인지 또는 1인지에 따라, 피드포워드 복호기에 입력되는 신호는 상기 이전 스테이트의 다음 스테이트에서 0 또는 1의 값을 가지는 스테이트로 이동한다. BCJR 알고리즘은 모든 심볼들에 대해 심볼 검출을 이용한다. 즉 현재 스테이트에서의 심볼의 확률값만을 이용하는 것이 아니라 이전 스테이트까지 누적된 심볼의 확률값과 현재 스테이트에서의 심볼의 확률값, 그리고 마지막 스테이트에서부터 현재 스테이트까지 저장된 확률값 모두를 이용하게 된다. 세가지 확률값들을 통해 현재 스테이트에서의 확률값이 최대가 되는 확률을 선택하여 최종값을 결정한다.

[0067] 도 8는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 부호화 동작을 도시한 순서도이다.

[0068] 도 8을 참조하면, 단말은 802단계에서 송신할 데이터를 생성하고, 804단계로 진행하여 생성된 데이터를 코드 레이트 1의 피드포워드 부호기를 통해 암호화한다. 상기 코드 레이트 1의 피드포워드 부호기는 미리 정해진 수신 단말인 적법한 단말은 데이터 복원에 성공하고 미리 정해진 수신 단말이 아닌 도청 단말은 데이터 복원에 실패하도록 암호화한다. 상기 코드 레이트 1의 피드포워드 부호기의 암호화 과정은 앞서 도 5를 통해 상세히 설명하였으므로 여기서는 그 상세한 설명을 생략하도록 한다.

[0069] 806단계에서 단말은 암호화된 데이터를 채널 부호기를 통해 부호화하여 최종 데이터를 생성하고, 상기 생성한 최종 데이터를 전송한다. 여기서 상기 채널 부호기는 일례로 터보 부호기가 될 수 있다.

[0070] 도 9는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말의 복호화 동작을 도시한 순서도이다.

[0071] 도 9를 참조하면, 단말은 902단계에서 데이터를 수신하고, 수신된 데이터를 채널 복호기를 통해 복호한다. 904단계에서 단말은 복호된 데이터의 연판정 값을 코드 레이트 1의 피드포워드 복호기를 통해 복호한 다음 906단계로 진행한다.

[0072] 906단계에서 단말은 미리 정해진 반복 횟수만큼 복호가 진행되었는지 여부를 확인하고, 미리 정해진 반복 횟수만큼 복호가 진행되지 않은 경우 902단계로 진행한다. 한편 미리 정해진 반복 횟수만큼 복호가 진행된 경우에는 908단계로 진행하여 복호된 데이터의 연판정 값을 경판정 값으로 결정한다.

[0073] 도 10a는 본 발명의 일실시예에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 2364bits일 경우, 이진 위상 편의 변조 방식, 스크램블링 방식, 코드 레이트 1의 피드포워드 부호 방식의 BER/FER 성능 비교를 도시한 그래프이다.

[0074] 도 10a에서 가로축은 SNR을 나타내고 세로축은 BER/프레임 에러율(FER: Frame Error Rate)을 나타낸다. 성능 곡선을 살펴보면 낮은 SNR 영역에서 코드 레이트 1의 피드포워드 부호 방식과 스크램블링(scrambling) 방식은 모두 보안성이 확보되는 BER 0.5의 값을 가지게 된다. 또한 높은 SNR 영역으로 갈수록 코드 레이트 1의 피드포워드 부호 방식은 이진 위상 편의(BPSK: Binary Phase Shift Keying) 변조 방식과 BER 성능이 수렴하게 된다.

[0075] 즉 코드 레이트 1의 피드포워드 부호 방식은 낮은 SNR 영역에서 보안성을 확보하는 동시에 높은 SNR 영역에서 신뢰성을 동시에 만족하게 되는 결과를 나타낸다. 또한 코드 레이트 1의 피드포워드 부호 방식은 스크램블링 방식에 비해 BER 기준으로 약 1dB 정도의 성능 향상을 보이며, FER 측면에서는 스크램블링 방식이나 BPSK 변조 방식에 비해 월등히 좋은 FER 성능을 가지는 것을 확인할 수 있다.

[0076] 도 10b는 본 발명의 일실시에에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 2364bits일 경우, 이진 위상 편의 변조 방식, 스크램블링 방식, 코드 레이트 1의 피드포워드 부호 방식의 보안 갭 성능 비교를 도시한 그래프이다.

[0077] 도 10b에서 가로축은 보안 갭을 나타내고 세로축은 도청 단말의 BER을 나타낸다. 성능 곡선을 살펴보면 도청 단말의 BER 0.4를 기준으로 코드 레이트 1의 피드포워드 부호 방식의 성능은 스크램블링 방식에 비해 약 0.8dB 가량의 보안 갭 이득(gain)을 갖는다.

[0078] 또한 도청 단말의 BER 0.4를 기준으로 코드 레이트 1의 피드포워드 부호 방식은 4.2dB 가량의 보안 갭을 가지고 있고, 스크램블링 방식은 5dB 가량의 보안 갭을 가지고 있음을 확인할 수 있다. 이는 코드 레이트 1의 피드포워드 부호 방식을 사용할 경우에는 수신 단말과 도청 단말의 채널 상태가 수신 SNR 대비 4.2dB 가량의 차이가 있어야 완벽 보안이 가능하고, 스크램블링 방식을 사용할 경우 수신 단말과 도청 단말의 채널 상태가 수신 SNR 대비 5dB 가량의 차이가 있어야 완벽 보안이 가능함을 나타낸다.

[0079] 도 11a는 본 발명의 일실시에에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 6144bits일 경우, 이진 위상 편의 변조 및 터보 부호 방식, 스크램블링 및 터보 부호 방식 방식, 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식의 BER/FER 성능 비교를 도시한 그래프이다.

[0080] 도 11a는 내부부호로 터보 부호를 사용하고 반복 복호 횟수를 8번으로 설정한 경우를 가정하였고, 펑처링하여 부호율의 변화에 따른 성능 정도를 코드 레이트(R) 1/3인 경우와 1/2인 경우를 구분하여 도시하였다. 또한 도 11a에서 가로축은 SNR을 나타내고 세로축은 BER/FER을 나타낸다.

[0081] 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식, 즉 코드 레이트 1의 피드포워드 부호에 터보 부호가 연접된 오류 정정 부호가 스크램블링 및 터보 부호 방식, 즉 스크램블링 부호에 터보 부호가 연접된 오류 정정 부호에 비해 약 0.05-0.1dB 가량의 성능 이득을 가지는 것을 확인할 수 있다.

[0082] 도 11b는 본 발명의 일실시에에 따른 D2D 통신 시스템에서 적용되는 단말이 전송하는 데이터가 6144bits일 경우, 이진 위상 편의 변조 및 터보 부호 방식, 스크램블링 및 터보 부호 방식 방식, 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식의 보안 갭 성능 비교를 도시한 그래프이다.

[0083] 도 11b에서 가로축은 보안 갭을 나타내고 세로축은 도청 단말의 BER을 나타낸다. 또한 도 11b는 해당 방식의 보안 갭 성능 정도를 코드 레이트(R) 1/3인 경우와 1/2인 경우를 구분하여 도시하였다.

[0084] 코드 레이트 1/2을 가정했을 때, 코드 레이트 1의 피드포워드 부호 및 터보 부호 방식, 즉 코드 레이트 1의 피드포워드 부호에 터보 부호가 연접된 오류 정정 부호의 보안 갭이 스크램블링 및 터보 부호 방식, 즉 스크램블링 부호에 터보 부호가 연접된 오류 정정 부호의 보안 갭에 비해 약 0.1dB 가량의 보안 갭 이득을 가지는 것을 확인할 수 있다.

[0085] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 안되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

[0086] 또한 본 발명의 실시예에 따른 보안성을 위한 오류 정정 부호를 생성하는 장치 및 방법은 하드웨어, 소프트웨어 또는 하드웨어 및 소프트웨어의 조합의 형태로 실현 가능하다는 것을 알 수 있을 것이다. 이러한 임의의 소프트웨어는 예를 들어, 삭제 가능 또는 재기록 가능 여부와 상관없이, ROM 등의 저장 장치와 같은 휘발성 또는 비휘발성 저장 장치, 또는 예를 들어, RAM, 메모리 칩, 장치 또는 집적 회로와 같은 메모리, 또는 예를 들어 CD, DVD, 자기 디스크 또는 자기 테이프 등과 같은 광학 또는 자기적으로 기록 가능함과 동시에 기계(예를 들어, 컴퓨터)로 읽을 수 있는 저장 매체에 저장될 수 있다. 본 발명의 그래픽 화면 갱신 방법은 제어부 및 메모리를 포함하는 컴퓨터 또는 휴대 단말에 의해 구현될 수 있고, 상기 메모리는 본 발명의 실시 예들을 구현하는 지시들을 포함하는 프로그램 또는 프로그램들을 저장하기에 적합한 기계로 읽을 수 있는 저장 매체의 한 예임을 알 수

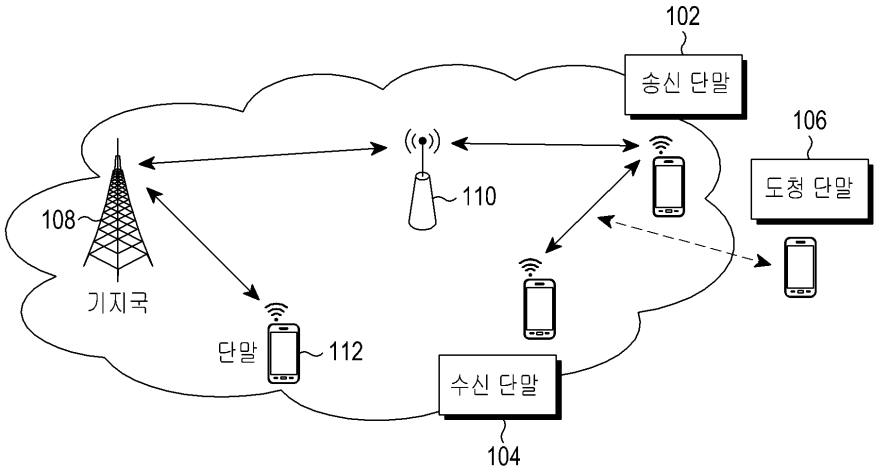
있을 것이다.

[0087] 따라서, 본 발명은 본 명세서의 임의의 청구항에 기재된 장치 또는 방법을 구현하기 위한 코드를 포함하는 프로그램 및 이러한 프로그램을 저장하는 기계(컴퓨터 등)로 읽을 수 있는 저장 매체를 포함한다. 또한, 이러한 프로그램은 유선 또는 무선 연결을 통해 전달되는 통신 신호와 같은 임의의 매체를 통해 전자적으로 이송될 수 있고, 본 발명은 이와 균등한 것을 적절하게 포함한다

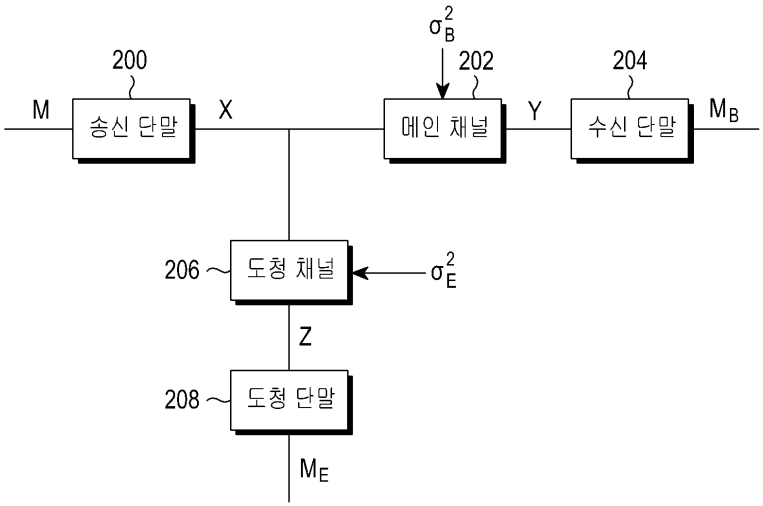
[0088] 또한 본 발명의 실시예에 따른 보안성을 위한 오류 정정 부호를 생성하는 장치는 유선 또는 무선으로 연결되는 프로그램 제공 장치로부터 상기 프로그램을 수신하여 저장할 수 있다. 상기 프로그램 제공 장치는 그래픽 처리 장치가 기설정된 컨텐츠 보호 방법을 수행하도록 하는 지시들을 포함하는 프로그램, 컨텐츠 보호 방법에 필요한 정보 등을 저장하기 위한 메모리와, 상기 그래픽 처리 장치와의 유선 또는 무선 통신을 수행하기 위한 통신부와, 상기 그래픽 처리 장치의 요청 또는 자동으로 해당 프로그램을 상기 송수신 장치로 전송하는 제어부를 포함할 수 있다.

도면

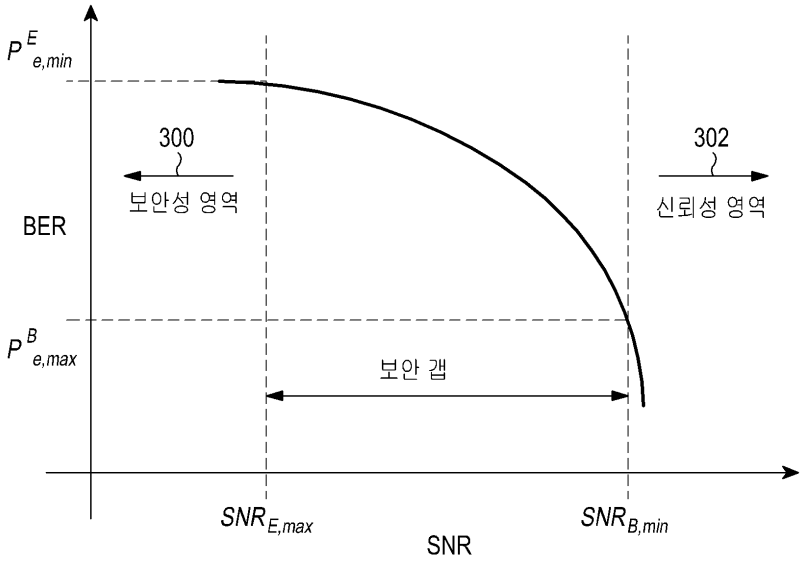
도면1



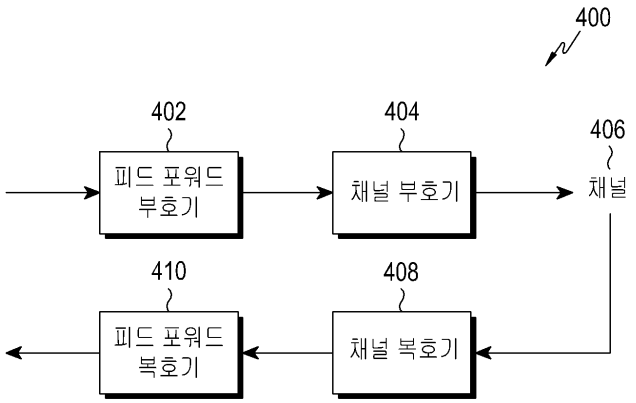
도면2



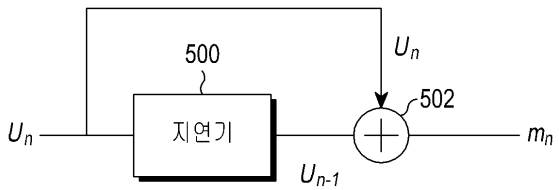
도면3


$P^{E}_{e,min}$
300
보안성 영역
302
신뢰성 영역
BER
$P^{B}_{e,max}$
보안 갭
$SNR_{E,max}$
$SNR_{B,min}$
SNR

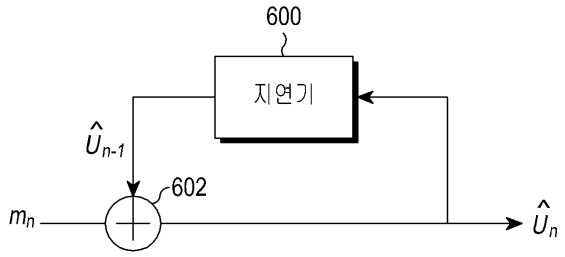
도면4


400
402
피드 포워드 부호기
404
채널 부호기
406
채널
410
피드 포워드 복호기
408
채널 복호기

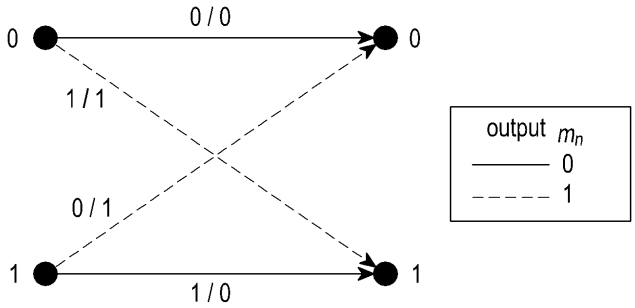
도면5


500
지연기
U_n
U_{n-1}
502
m_n

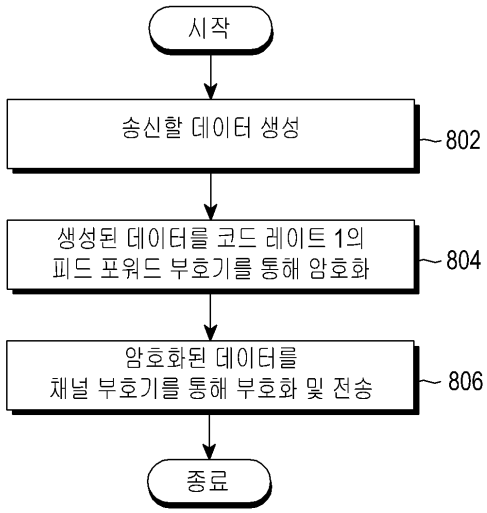
도면6


600
지연기
$\hat{U}_{n-1}$
602
m_n
$\hat{U}_n$

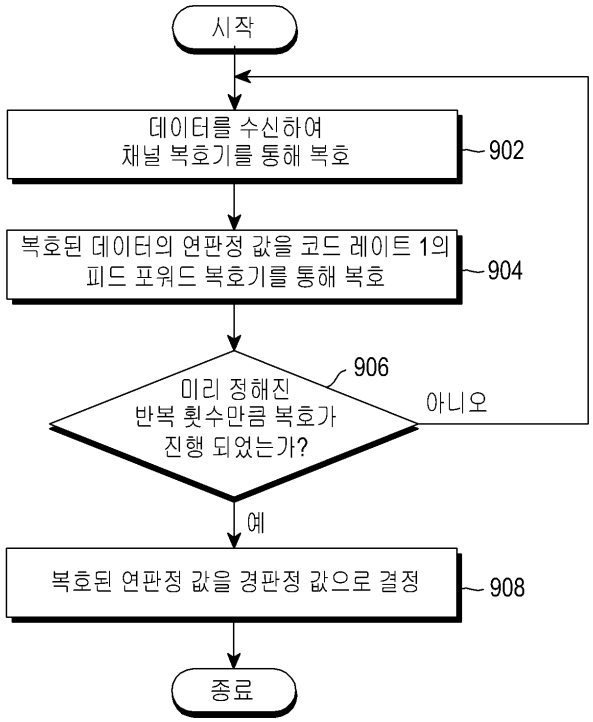
도면7


0
0 / 0
0
1 / 1
0 / 1
1
1 / 0
1
output m_n
0
1

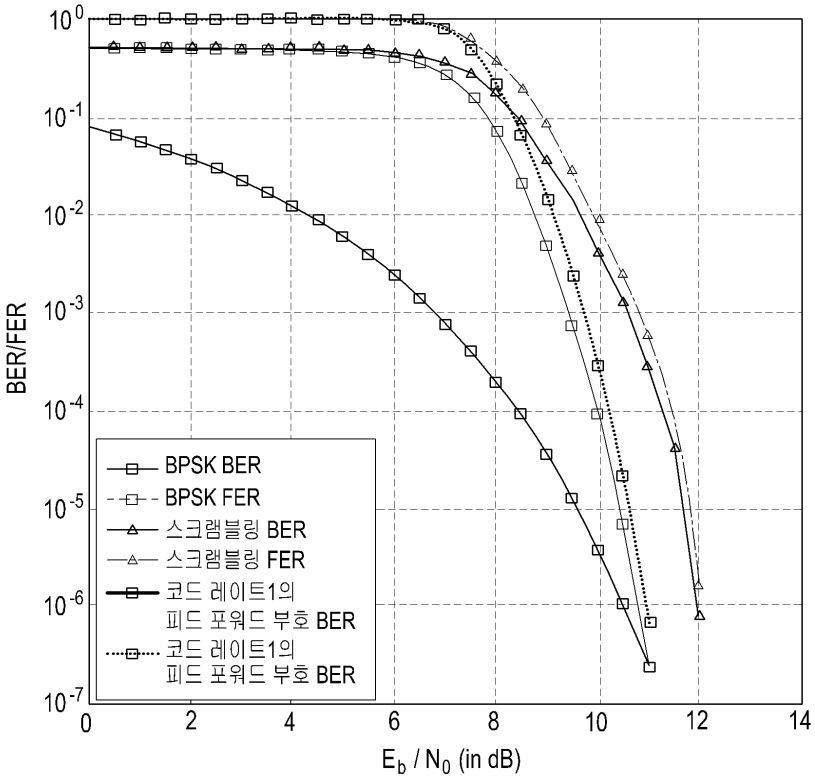
도면8


시작
송신할 데이터 생성
802
생성된 데이터를 코드 레이트 1의
피드 포워드 부호기를 통해 암호화
804
암호화된 데이터를
채널 부호기를 통해 부호화 및 전송
806
종료

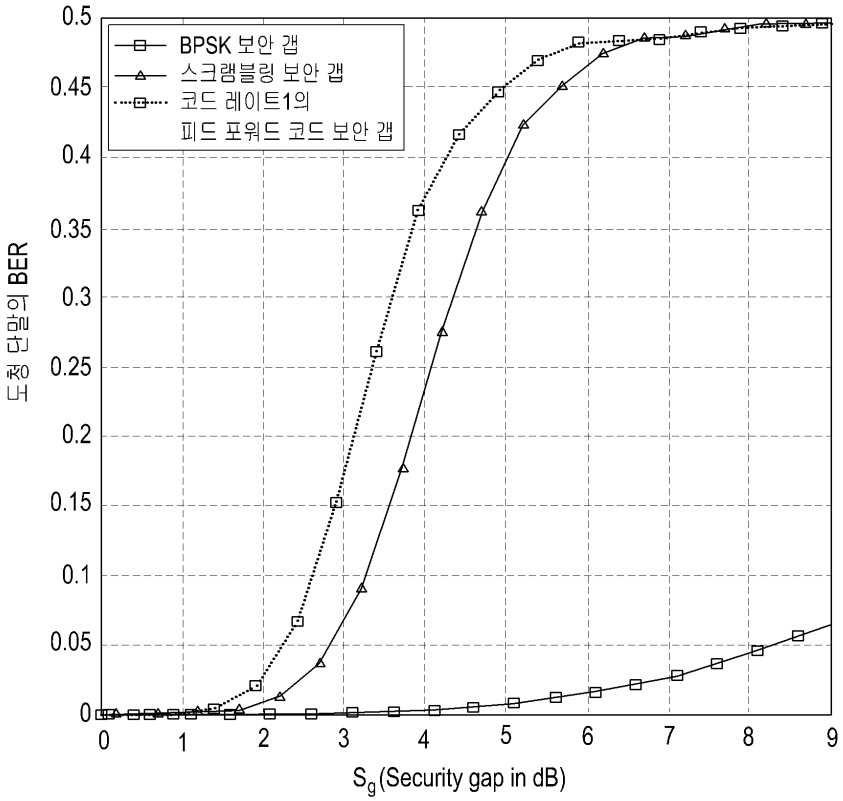
도면9


시작
데이터를 수신하여
채널 복호기를 통해 복호
902
복호된 데이터의 연판정 값을 코드 레이트 1의
피드 포워드 복호기를 통해 복호
904
906
미리 정해진
반복 횟수만큼 복호가
진행 되었는가?
아니오
예
복호된 연판정 값을 경판정 값으로 결정
908
종료

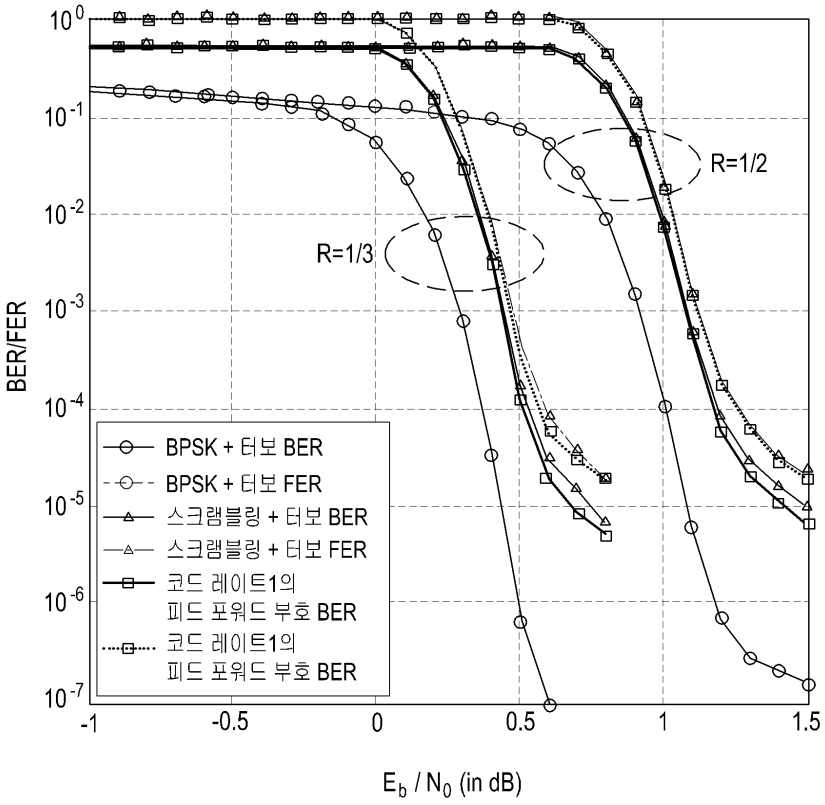
도면10a


BER/FER
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
0
2
4
6
8
10
12
14
E_b / N_0 (in dB)
BPSK BER
BPSK FER
스크램블링 BER
스크램블링 FER
코드 레이트1의
피드 포워드 부호 BER
코드 레이트1의
피드 포워드 부호 BER

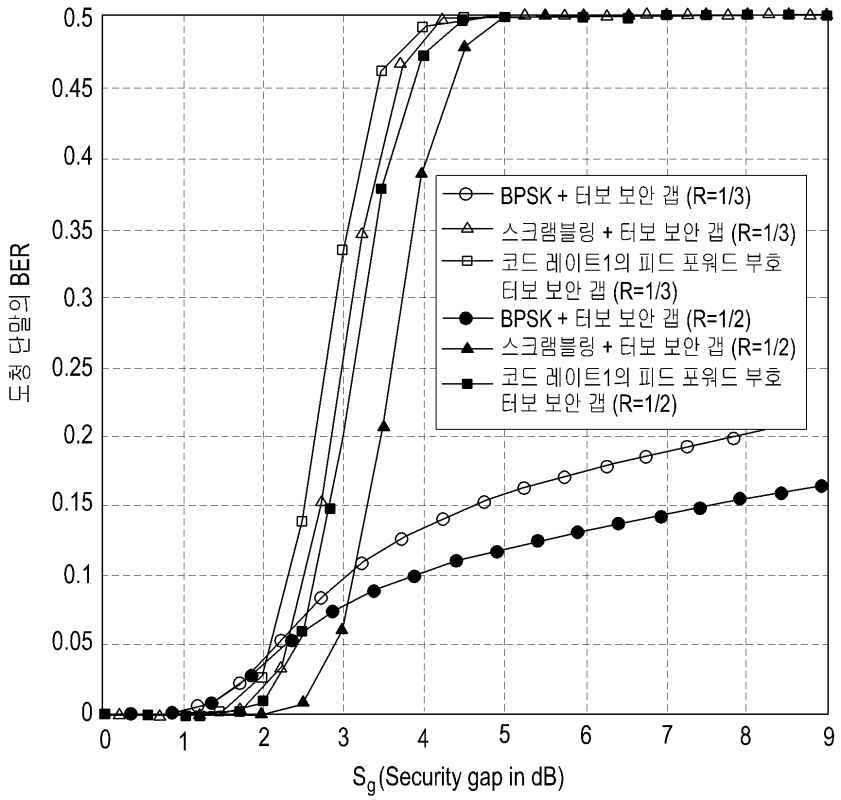
도면10b


BPSK 보안 갭
스크램블링 보안 갭
코드 레이트1의
피드 포워드 코드 보안 갭
도청 단말의 BER
0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
1
2
3
4
5
6
7
8
9
S_g(Security gap in dB)

도면11a


BER/FER
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
-1
-0.5
0
0.5
1
1.5
E_b / N_0 (in dB)
R=1/2
R=1/3
BPSK + 터보 BER
BPSK + 터보 FER
스크램블링 + 터보 BER
스크램블링 + 터보 FER
코드 레이트1의 피드 포워드 부호 BER
코드 레이트1의 피드 포워드 부호 BER

도면11b


0.5
0.45
0.4
0.35
0.3
0.25
0.2
0.15
0.1
0.05
0
0
1
2
3
4
5
6
7
8
9
도청 단말의 BER
S_g(Security gap in dB)
BPSK + 터보 보안 갭 (R=1/3)
스크램블링 + 터보 보안 갭 (R=1/3)
코드 레이트1의 피드 포워드 부호 터보 보안 갭 (R=1/3)
BPSK + 터보 보안 갭 (R=1/2)
스크램블링 + 터보 보안 갭 (R=1/2)
코드 레이트1의 피드 포워드 부호 터보 보안 갭 (R=1/2)