(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년06월17일
(11) 등록번호 10-2675382
(24) 등록일자 2024년06월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 25/02* (2006.01)
(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 25/0202 (2013.01)
(21) 출원번호 10-2022-0007063
(22) 출원일자 2022년01월18일
심사청구일자 2022년01월18일
(65) 공개번호 10-2023-0111348
(43) 공개일자 2023년07월25일
(56) 선행기술조사문헌
KR101446629 B1*
KR101253370 B1*
US20170338956 A1*
1.오토인코더(AutoEncoder), 네이버 블로그 (2021.09.11.)
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
광주과학기술원
광주광역시 북구 첨단과기로 123 (오룡동)
(72) 발명자
황의석
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 전기전자컴퓨터공학부
송준호
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 기계공학부
한승남
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 전기전자컴퓨터공학부
(74) 대리인
특허법인지담

전체 청구항 수 : 총 4 항 심사관 : 양종필

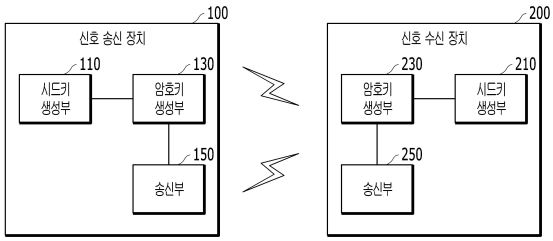
(54) 발명의 명칭 **오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치, 신호 수신 장치, 신호 송신 방법 및 신호 수신 방법**

(57) 요 약

본 발명은 오토인코더 기반 암호키 생성 기술에 관한 것으로, 더욱 상세하게는 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치, 신호 수신 장치, 신호 송신 방법 및 신호 수신 방법에 관한 것이다.

본 발명의 실시 예에 따르면, 오토인코더를 기반으로 보안성을 강화한 암호키를 생성할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0838 (2013.01)
H04L 9/0858 (2013.01)
Z01T 30/00 (2019.06)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711139241
과제번호 2021-0-01835-001
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성(R&D)
연구과제명 영지식 센싱, 암호인증, 블록체인 기반 클라우드 서비스 융합 기술 개발
기 여 율 1/2
과제수행기관명 광주과학기술원
연구기간 2021.07.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711103315
과제번호 2017-0-00413-004
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 방송통신산업기술개발(R&D)
연구과제명 Cellular IoT 환경에서 물리계층 장치 인식 기반 간결한 보안 통신 연구
기 여 율 1/2
과제수행기관명 광주과학기술원
연구기간 2020.01.01 ~ 2021.06.30

명 세 서

청구범위

청구항 1

오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치에 있어서,

수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정하고,

상기 추정된 채널 정보의 특징값을 추출하며,

상기 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성하고,

상기 생성된 시드키값에 대해 오류값을 제거하는 레컨실리에이션(reconciliation)을 수행하는 시드키 생성부;

상기 생성된 시드값을 이용하여 암호키를 생성하되,

상기 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성하고,

학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성하는 암호키 생성부; 및

인코더로 구성되어 상기 생성된 암호키에 대한 메시지 신호를 압축하고, 암호화된 신호로 변환하여 신호 수신 장치로 송신하는 송신부를 포함하는 신호 송신 장치.

청구항 2

삭제

청구항 3

오토인코더 기반 암호키 생성 시스템에서 신호 수신 장치에 있어서,

수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정하고,

상기 추정된 채널 정보의 특징값을 추출하며,

상기 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성하고,

상기 생성된 시드키값에 대해 오류값을 제거하는 레컨실리에이션(reconciliation)을 수행하는 시드키 생성부;

상기 생성된 시드값을 이용하여 암호키를 생성하되,

상기 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성하고,

학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성하는 암호키 생성부; 및

디코더로 구성되어 신호 송신 장치로부터 수신한 암호화된 신호를 원래 메시지 신호로 복원하는 수신부를 포함하는 신호 수신 장치.

청구항 4

삭제

청구항 5

오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치가 오토인코더 기반 암호키 생성 시스템에서 신호를 송신하는 방법에 있어서,

수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정하고,

상기 추정된 채널 정보의 특징값을 추출하며,

상기 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성하고,

상기 생성된 시드키값에 대해 오류값을 제거하는 레컨실리에이션(reconciliation)을 수행하는 단계;

상기 생성된 시드값을 이용하여 암호키를 생성하되,

상기 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성하고,

학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성하는 단계; 및

인코더로 구성되어 상기 생성된 암호키에 대한 메시지 신호를 압축하고, 암호화된 신호로 변환하여 신호 수신 장치로 송신하는 단계를 포함하는 신호 송신 방법.

청구항 6

삭제

청구항 7

오토인코더 기반 암호키 생성 시스템에서 신호 수신 장치가 오토인코더 기반 암호키 생성 시스템에서 신호를 수신하는 방법에 있어서,

수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정하고,

상기 추정된 채널 정보의 특징값을 추출하며,

상기 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성하고,

상기 생성된 시드키값에 대해 오류값을 제거하는 레컨실리에이션(reconciliation)을 수행하는 단계;

상기 생성된 시드값을 이용하여 암호키를 생성하되,

상기 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성하고,

학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성하는 단계; 및

디코더로 구성되어 신호 송신 장치로부터 수신한 암호화된 신호를 원래 메시지 신호로 복원하는 단계를 포함하는 신호 수신 방법.

청구항 8

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 오토인코더 기반 암호키 생성 기술에 관한 것으로, 더욱 상세하게는 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치, 신호 수신 장치, 신호 송신 방법 및 신호 수신 방법에 관한 것이다.

배 경 기 술

[0003] 최근, 안전한 무선 통신 시스템을 위한 다양한 방식의 물리 계층 보안 기술이 개발 및 연구되고 있다.

[0004] 일반적으로, 무선 통신 시스템은 물리적으로 비밀키를 직접 공유하거나, 키분배 센터(Key Distribution Center, KDC) 또는 공개키 인프라구조(Public Key Infrastructure, PKI)를 이용한 물리 계층 보안 기술을 적용하여 암호키를 분배 및 관리한다.

[0005] 공개키 인프라구조를 이용한 물리 계층 보안 기술은 송신자와 수신자가 동일한 암호키를 공유하는 것을 특징으로 한다. 그러나, 공개키 인프라구조를 이용한 물리 계층 보안 기술은 악의적인 공격자의 계산 능력이 뛰어날 경우, 보안성을 보장하기 어려운 문제점이 있다.

[0006] 본 발명의 배경기술은 대한민국 등록특허 제10-1912443 호에 게시되어 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 오토인코더를 기반으로 보안성을 강화한 암호키를 생성할 수 있는 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치, 신호 수신 장치, 신호 송신 방법 및 신호 수신 방법을 제공한다.

[0009] 본 발명이 이루고자 하는 기술적 과제는 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 본 발명의 일 측면에 따르면, 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치가 제공된다.

[0012] 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치는 수신한 메시지에서 통신 네트워크의 무선 채널 정보를 추정하여 오토인코더의 시드값을 생성하는 시드키 생성부, 생성된 시드값을 이용하여 암호키를 생성하는 암호키 생성부 및 인코더로 구성되어 생성된 암호키에 대한 메시지 신호를 압축하고, 암호화된 신호로 변환하여 신호 수신 장치로 송신하는 송신부를 포함할 수 있다.

[0013] 본 발명의 다른 일 측면에 따르면, 오토인코더 기반 암호키 생성 시스템에서 신호 송신 방법이 제공된다.

[0014] 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 방법은 수신한 메시지에서 통신 네트워크의 무선 채널 정보를 추정하여 오토인코더의 시드값을 생성하는 단계, 생성된 시드값을 이용하여 암호키를 생성하는 단계 및 인코더로 구성되어 생성된 암호키에 대한 메시지 신호를 압축하고, 암호화된 신호로 변환하여 신호 수신 장치로 송신하는 단계를 포함할 수 있다.

발명의 효과

[0016] 본 발명의 실시 예에 따르면, 오토인코더를 기반으로 보안성을 강화한 암호키를 생성할 수 있다.

[0017] 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 설명 또는 청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

[0019] 도 1 내지 도 7은 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치 및 신호 수신 장치를 설명하기 위한 도면들.

도 8은 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 방법 및 신호 수신 방법을 설명하기 위한 도면.

도 9 내지 도 15는 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치 및 신호 수신 장치의 성능을 설명하기 위한 도면들.

발명을 실시하기 위한 구체적인 내용

[0020] 이하에서는 첨부한 도면을 참조하여 본 발명을 설명하기로 한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 따라서 여기에서 설명하는 실시예로 한정되는 것은 아니다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0021] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결(접속, 접촉, 결합)"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 부재를 사이에 두고 "간접적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 구비할 수 있다는 것을 의미한다.

[0022] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0023] 도 1 내지 도 7은 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치 및 신호 수신 장치를 설명하기 위한 도면들이다.

[0024] 도 1을 참조하면, 오토인코더 기반 암호키 생성 시스템(10)은 암호화된 신호를 송신하는 신호 송신 장치(100) 및 암호화된 신호를 수신하는 신호 수신 장치(200)를 포함한다.

[0025] 신호 송신 장치(100) 및 신호 수신 장치(200)는 각각 오토인코더를 기반으로 무선 채널의 특징(latent variable)을 추출하고, 시드값을 입력으로 하여 암호키인 가중치(weight) 및 편향(bias)을 생성하여 동일한 물리계층 암호키를 송수신한다.

[0026] 신호 송신 장치(100)는 시드키 생성부(110), 암호키 생성부(130) 및 송신부(150)를 포함한다.

[0027] 시드키 생성부(110)는 수신한 메시지에서 통신 네트워크의 무선 채널 정보를 추정하여 특징을 추출하고, 추출된 특징을 양자화(quantization)하여 오토인코더의 시드값을 생성한다. 시드키 생성부(110)의 구성은 추후 상세히 설명하기로 한다.

[0028] 암호키 생성부(130)는 생성된 시드값을 이용하여 암호키를 생성한다.

[0029] 송신부(150)는 인코더로 구성되어 생성된 암호키에 대한 메시지 신호를 압축하고 암호화된 신호로 변환한다. 송신부(150)는 암호화된 신호를 신호 수신 장치(200)로 송신한다.

[0030] 신호 수신 장치(200)는 시드키 생성부(210), 암호키 생성부(230) 및 수신부(250)를 포함한다.

[0031] 시드키 생성부(210)는 수신한 메시지에서 통신 네트워크의 무선 채널 정보를 추정하여 특징을 추출하고, 추출된 특징을 양자화하여 오토인코더의 시드값을 생성한다.

[0032] 암호키 생성부(230)는 생성된 시드값을 이용하여 암호키를 생성한다.

[0033] 수신부(250)는 디코더로 구성되어 신호 송신 장치(100)로부터 수신한 암호화된 신호를 원래 메시지 신호로 복원한다.

[0034] 도 2를 참조하면, 시드키 생성부(110)는 채널 추정부(111), 특징 추출부(113), 양자화부(115) 및 레컨실리에이션부(117)를 포함한다. 여기서, 신호 송신 장치(100) 및 신호 수신 장치(200)의 시드키 생성부(110) 및 암호키 생성부(230)에 대한 설명은 동일하므로, 신호 송신 장치(100)의 구성을 대표로 설명하도록 한다.

[0035] 채널 추정부(111)는 수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정한다.

[0036] 특징 추출부(113)는 오토인코더를 이용하여 추정된 채널 정보의 특징값(latent variable)을 추출한다.

[0037] 여기서, 오토인코더는 채널의 특징을 추출하기 위해 사용되는 비지도 방식의 신경망으로, 입력 받은 데이터를 압축시키는 트랜스미터(transmitter) 및 압축시킨 데이터를 입력 데이터 형태로 복구하는 리시버(receiver)로 구성된다.

[0038] 도 3을 참조하면, 오토인코더는 트랜스미터(Input layer, connected Layer 및 Normalized Layer), 채널(Latent space Representation) 및 리시버(Fully connected Layer, Fully connected Layer with softmax 및 Output Layer)를 포함한다. 이 때, 오토인코더의 배치 사이즈(Batch size)는 50, 에포크(Epoch)는 100, 학습률(Learning rate)은 0.001이며, 옵티마이저(Optimizer)는 SGD의 변형 함수인 Adam일 수 있다.

[0039] 신호 송신 장치(100)의 특징 추출부(113) 및 신호 수신 장치(200)의 특징 추출부(113)에서 오코인코더는 도 4와 같이 추정된 채널 정보를 입력으로 하여 채널 정보의 특징값을 각각 추출한다.

[0040] 도 5를 참조하면, 양자화부(115)는 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성한다.

[0041] 다시 도 2를 참조하면, 레컨실리에이션부(117)는 양자화를 통해 생성된 시드키값을 레컨실리에이션(reconciliation)한다. 여기서, 레컨실리에이션부(117)는 송신자와 수신자 사이에 생성된 시드키값의 동일성을 유지하기 위해 오류값을 제거한다.

[0042] 도 6 및 도 7을 참조하면, 암호키 생성부(130)는 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성한다. 이 때, 암호키 생성부(130)는 학습 데이터를 저장하는 저장부를 포함할 수 있으며, 저장부에 저장된 학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성할 수 있다.

[0043] 도 8은 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 방법 및 신호 수신 방법을 설명하기 위한 도면이다.

[0044] 도 8을 참조하면, S810에서 신호 송신 장치(100) 및 신호 수신 장치(200)는 채널 정보를 추정한다. 이 때, 신호 송신 장치(100) 및 신호 수신 장치(200)는 수신한 메시지에서 채널 이득(channel gain), 채널 위상(channel phase) 중 적어도 하나 이상의 채널 정보를 추정한다.

[0045] S820에서 신호 송신 장치(100) 및 신호 수신 장치(200)는 오토인코더를 이용하여 추정된 채널 정보의 특징값(latent variable)을 추출한다.

[0046] S830에서 신호 송신 장치(100) 및 신호 수신 장치(200)는 추출된 채널 정보의 특징값에 대한 양자화 수행을 통해 채널 정보 특징값을 이진화(binary)하여 시드(seed)키값을 생성한다.

[0047] S840에서 신호 송신 장치(100) 및 신호 수신 장치(200)는 양자화를 통해 생성된 시드키값을 레컨실리에이션(reconciliation)한다. 신호 송신 장치(100) 및 신호 수신 장치(200)는 송신자와 수신자 사이에 생성된 시드키값의 동일성을 유지하기 위해 오류값을 제거한다.

[0048] S850에서 신호 송신 장치(100) 및 신호 수신 장치(200)는 생성된 시드값을 오토인코더에 입력으로 하는 프라이버시 앰플리피케이션을 수행하여 암호키인 가중치(weight) 및 편향(bias)을 생성한다. 이 때, 신호 송신 장치(100) 및 신호 수신 장치(200)는 학습 데이터를 통해 학습된 오토인코더를 사용하여 암호키를 생성할 수 있다.

[0049] S860에서 신호 송신 장치(100)는 암호키를 이용하여 메시지 신호를 압축하고 암호화된 신호로 변환한다. 신호 송신 장치(100)는 암호화된 신호를 신호 수신 장치(200)로 송신한다. 또한, 신호 수신 장치(200)는 신호 송신 장치(100)로부터 암호화된 신호를 수신하여 원래 메시지 신호로 복원한다.

[0050] 도 9 내지 도 15는 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치 및 신호 수신 장치의 성능을 설명하기 위한 도면들이다.

[0051] 도 9 내지 도 11을 참조하면, 30개 위치에서 측정된 채널 이득 정보를 이용하여 기존의 채널 특징 추출 방법(DCT)을 통해 생성된 시드키와 본 발명의 일 실시 예에 따른 오토인코더 기반 특징 추출 방법(AE, AAE)을 통해 생성된 시드키의 특징 추출 성능을 비교한 결과, 오토인코더 기반 특징 추출 방법에 의해 생성된 시드키가 기존의 특징 추출 방법에 의해 생성된 시드키에 비하여 키 동의율(key agreement rate)이 더 높은 것을 확인할 수 있다. 이를 통해, 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치(100) 및 신호 수신 장치(200)의 특징 추출 성능이 우수함을 확인할 수 있다.

[0052] 도 12 및 도 13을 참조하면, 기존의 채널 특징 추출 방법(DCT)을 통해 생성된 시드키와 본 발명의 일 실시 예에 따른 오토인코더 기반 특징 추출 방법(AE, AAE)을 통해 생성된 시드키의 보안 성능을 비교한 결과, 오토인코더 기반 특징 추출 방법을 통해 생성된 시드키가 기존의 의해 생성된 시드키에 비하여 키 비동의율(key disagreement rate)이 0.5에 가까움을 알 수 있다. 이를 통해, 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치(100) 및 신호 수신 장치(200)의 시드키 보안 성능이 우수함을 확인할 수 있다.

[0053] 도 14 및 도 15를 참조하면, 본 발명의 일 실시 예에 따른 오토인코더 기반 특징 추출 방법(AE, AAE)에 대해 공격자(Eve)가 시드키를 생성하는 공격 시나리오를 수행한 결과, 신호대잡음비(SNR) 및 압축률(CR)에 따라 암호키를 생성하고 통신시스템에 적용하였을 때의 메시지 신호에 대한 블록 오류율(block error rate)은 공격자(Eve)가 수신자(Bob)보다 높은 것을 확인할 수 있다. 이를 통해, 본 발명의 일 실시 예에 따른 오토인코더 기반 암호키 생성 시스템에서 신호 송신 장치(100) 및 신호 수신 장치(200)의 암호키 보안 성능이 우수함을 확인할 수 있다.

[0054] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0055] 본 발명의 범위는 후술하는 청구범위에 의하여 나타내어지며, 청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

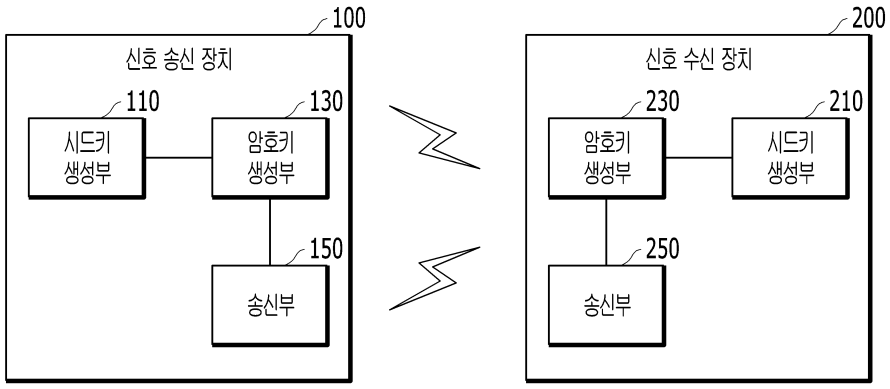
[0057] 100: 신호 송신 장치

110: 시드키 생성부

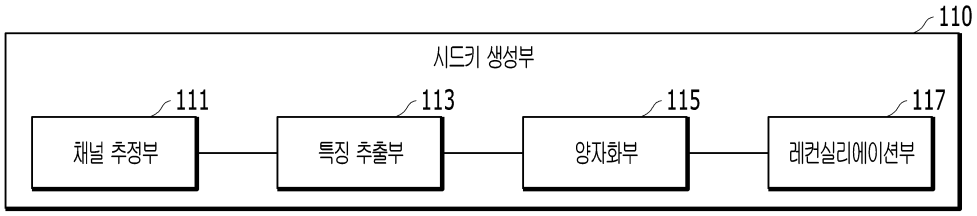
200: 신호 수신 장치

도면

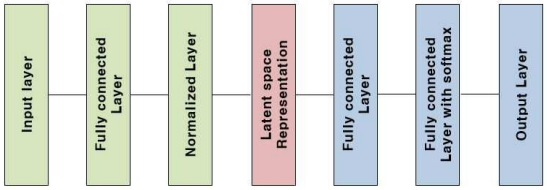
도면1



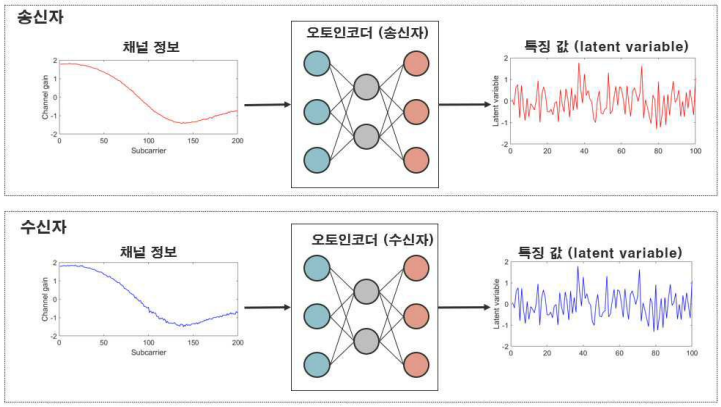
도면2



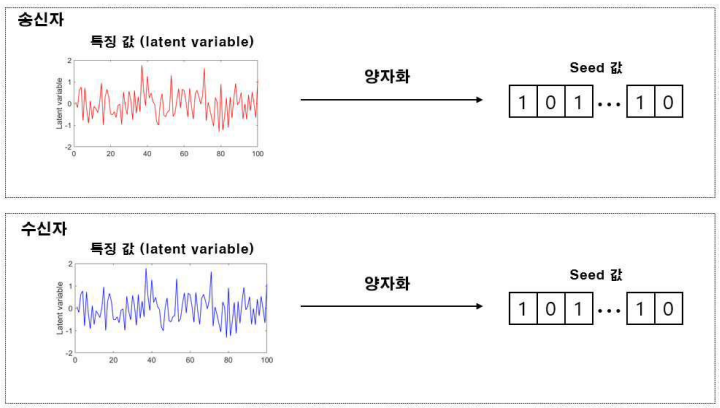
도면3



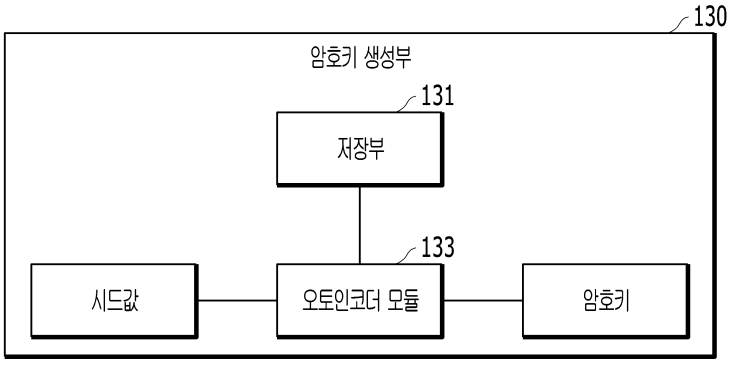
도면4



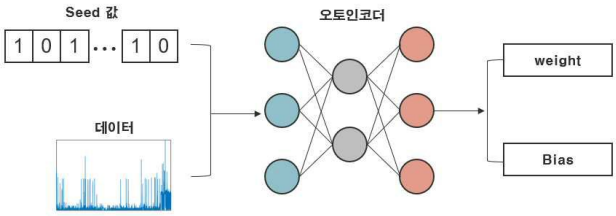
도면5



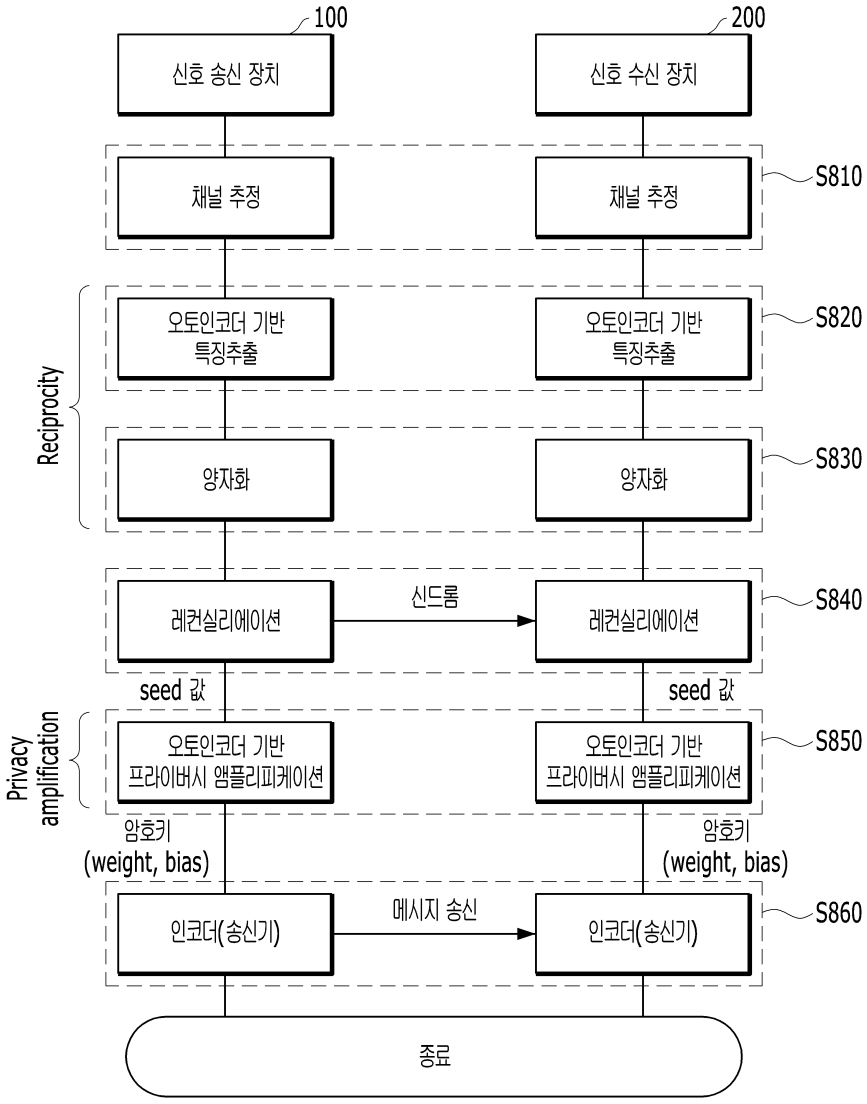
도면6


130
암호키 생성부
131
저장부
133
시드값
오토인코더 모듈
암호키

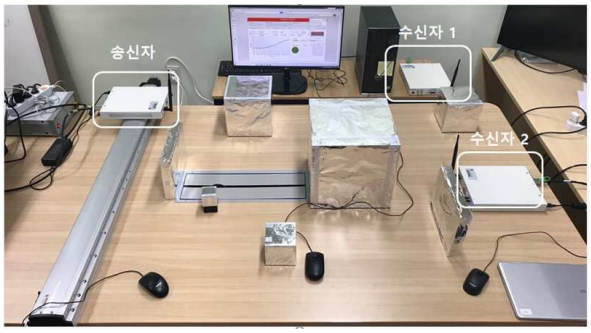
도면7


Seed 값
1 0 1 ... 1 0
데이터
오토인코더
weight
Bias

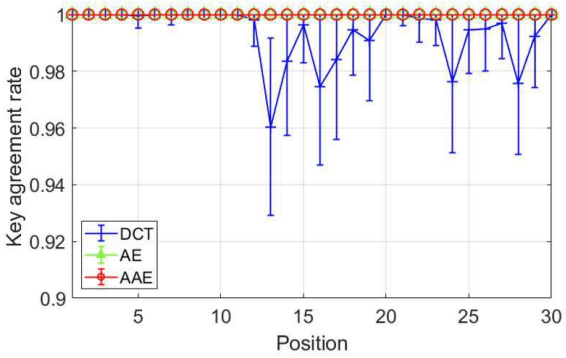
도면8


100
200
신호 송신 장치
신호 수신 장치
채널 추정
채널 추정
S810
오토인코더 기반 특징추출
오토인코더 기반 특징추출
S820
Reciprocity
양자화
양자화
S830
레컨실리에이션
신드롬
레컨실리에이션
S840
seed 값
seed 값
Privacy amplification
오토인코더 기반 프라이버시 앰플리피케이션
오토인코더 기반 프라이버시 앰플리피케이션
S850
암호키 (weight, bias)
암호키 (weight, bias)
인코더(송신기)
메시지 송신
인코더(송신기)
S860
종료

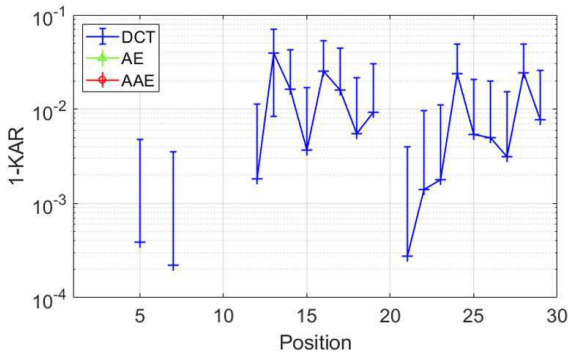
도면9


송신자
수신자 1
수신자 2

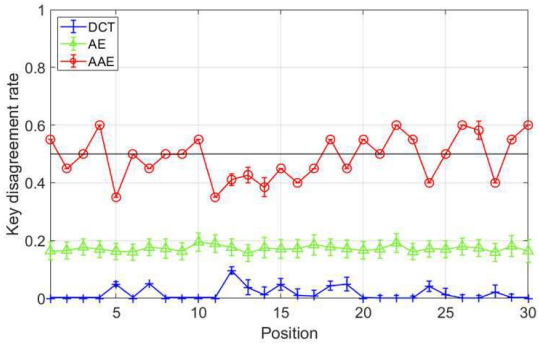
도면10



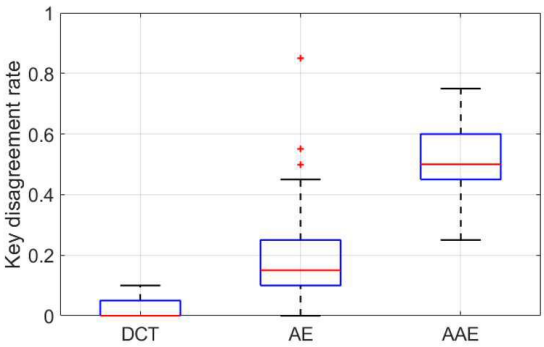
도면11



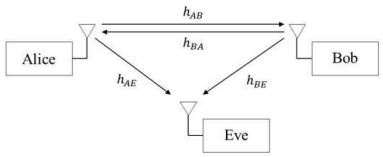
도면12



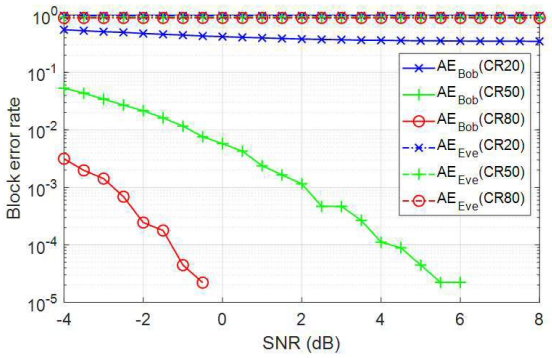
도면13



도면14


h_{AB}
h_{BA}
Alice
Bob
h_{AE}
h_{BE}
Eve

도면15


Block error rate
SNR (dB)
AE_Bob(CR20)
AE_Bob(CR50)
AE_Bob(CR80)
AE_Eve(CR20)
AE_Eve(CR50)
AE_Eve(CR80)