고려대학교 KOREA UNIVERSITY

노광석 교수 (고려대학교 초신뢰양자인터넷센터)

보안이 강화된 데이터 전송 방법
(기술분류-차세대통신-5G·6G 위성통신)

기술성 분석

기술 개요

- 데이터를 전송할 때 양자키분배 프로토콜을 이용하는 보안이 강화된 데이터 전송 방법에 관한 것임
- 도청자는 탈취한 데이터에 대하여 무차별 대입 방식(brute-force)으로만 복호화를 수행함으로써 도청자 단말의 성능을 열화시킴으로써 높은 보안성을 제공함

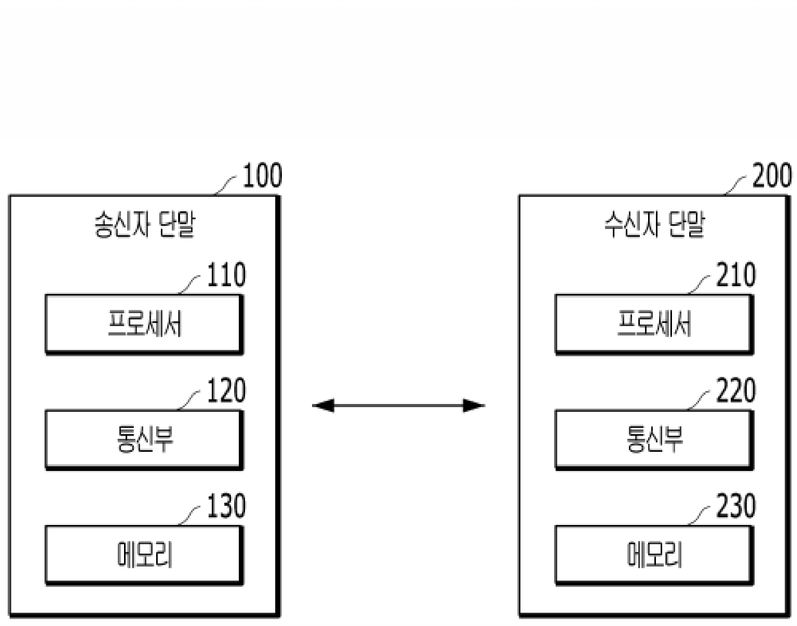
미해결 과제(Unmet needs)

- 기존 오류정정부호 보안 방법의 한계
  - 오류정정부호(FEC, Forward Error Correction)는 전송 채널에서 발생하는 전송 신호의 오류 등을 정정하는 기능을 제공함
  - 디지털 통신에서 오류정정부호는 도청을 효과적으로 막기 위하여 무결성, 인증 등을 위한 Secure Forward Error Correction(secure FEC) 등 추가적인 암호화 기능을 이용할 뿐 오류정정부호 자체는 도청을 막는 기능을 제공하지 않으므로 이에 대하여 완벽한 보안을 제공하는 오류정정부호를 처리하기 위한 방법 및 장치가 필요한 실정임
  - 한편, 양자키분배 프로토콜(Quantum Key Distribution(QKD) protocol)은 도청자의 무한한 계산 능력, 저장공간을 가정하더라도, 양자역학적 특성으로 인해 도청 불가능한 random 키를 송/수신자가 공유함으로써 보안을 제공하는 프로토콜임

기술적 해결수단(발명의 구성)

- 1) 본 기술에 따른 송신자 단말 및 수신자 단말의 구성
  - 송신자 단말 및 수신자 단말은 프로세서, 통신부 및 메모리로 구성됨
  - 프로세서는 송신자 단말 및 수신자 단말의 전반적인 동작을 제어하며, 메모리에 저장된 응용 프로그램을 구동하기 위하여 단말의 구성요소들 중 일부를 제어하거나 서로 조합하여 동작시킬 수 있음
  - 또한, 송신자 단말의 프로세서는 부호화된 특정 데이터 및 페이크 심볼(도청을 방해하기 위한 심볼)을 수신자 단말로 전송하고, QKD를 통해 페이크 심볼의 개수 및 위치에 대한 정보를 확인할 수 있는 정보를 전송하도록 통신부를 제어하며, 수신자 단말의 프로세서는 페이크 심볼의 개수 및 위치에 대한 정보를 획득하고 부호화된 특정 데이터에서 페이크 심볼을 제거한 후 복호화를 수행함
  - 통신부는 송신자 단말과 수신자 단말 사이의 통신을 가능하게 하는 모듈과 네트워크에 연결하는 모듈을 포함함
  - 메모리는 프로세서의 동작을 위한 프로그램을 저장하고, 입/출력되는 데이터들을 임시 또는 영구 저장함

본 기술에 따른 송신자 단말 및 수신자 단말의 구성

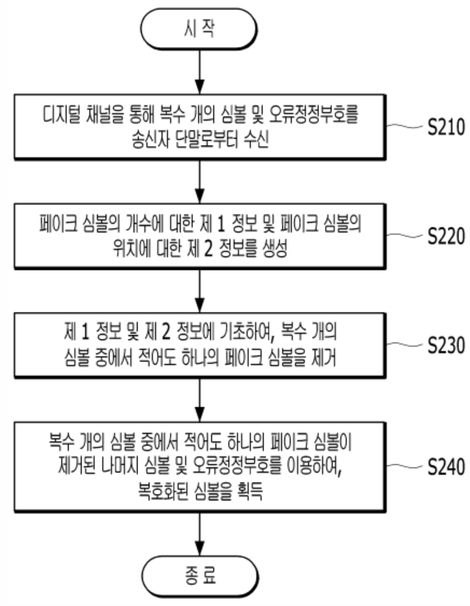


본 기술의 우수성 및 파급 효과

본 기술의 우수성(효과)

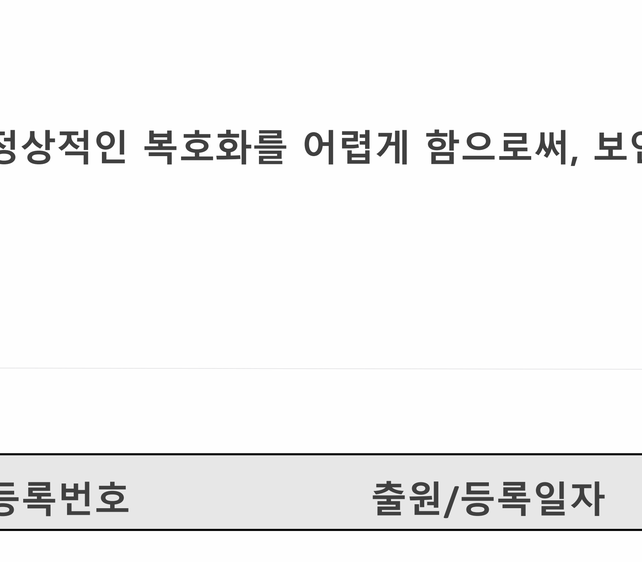
- 보안이 강화된 데이터 전송 방법
  - 수신자 단말의 프로세서는 송신자 단말로부터 디지털 채널을 통해 복수 개의 심볼 및 오류정정부호를 수신함
  - 송신자 단말로부터 퀀텀 채널을 통해 사전에 수신된 키 시퀀스 및 복수 개의 심볼의 개수를 이용하여, 페이크 심볼의 개수에 대한 제 1 정보 및 페이크 심볼의 위치에 대한 제 2 정보를 생성함
  - 이후 제 1 정보 및 제 2 정보에 기초하여 복수 개의 심볼 중에서 페이크 심볼을 제거하고, 나머지 심볼 및 오류정정부호를 이용하여 복호화된 심볼을 획득함

보안이 강화된 데이터 전송 방법



- 도청자 단말의 성능 열화로 인한 도청 불가능
  - 페이크 심볼의 위치를 QKD를 통해 전송된 random key를 이용하여 설정함으로써, 즉 도청자 단말이 알아낼 수 없는 정보를 이용하여 페이크 심볼의 개수 및 위치를 설정하여 도청자 단말은 페이크 심볼의 정확한 위치를 알 수 없게 됨
  - 따라서 도청자 단말이 정확하게 페이크 심볼을 제거하지 못하고, 페이크 심볼의 위치가 정확하게 일치할 때까지 복호화를 수행하는 과정을 반복하게 되므로 도청자 단말의 성능 열화가 발생하고 사실상 페이크 심볼의 위치를 찾는 것이 불가능해짐

도청자 단말이 페이크 심볼이 포함된 심볼을 복호화하는 방법의 일례



적용 제품 및 파급 효과

- 데이터 전송 장치
- 본 기술을 통해 도청자 단말이 페이크 심볼의 개수 및 위치를 알아내는 것을 막고 정상적인 복호화를 어렵게 함으로써, 보안성이 높은 데이터 전송 방법을 제공할 수 있음

지식재산권 현황

발명의 명칭	출원/등록번호	출원/등록일자
보안이 강화된 데이터 전송 방법	10-2702344	2024.08.29.
패밀리 특허 현황	**패밀리 국가**	
-	-	

문 의 | 고려대학교 산학협력단 기술사업화센터 권성진 02-3290-5832, giannie77@korea.ac.kr