



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0076558
(43) 공개일자 2020년06월29일

(51) 국제특허분류(Int. Cl.)

H04L 29/06 (2006.01)

(52) CPC특허분류

H04L 69/04 (2013.01)

H04L 69/164 (2013.01)

(21) 출원번호 10-2019-0041817

(22) 출원일자 2019년04월10일

심사청구일자 없음

(30) 우선권주장

1020180165242 2018년12월19일 대한민국(KR)

(71) 출원인

삼성전자주식회사

경기도 수원시 영통구 삼성로 129 (매탄동)

(72) 발명자

김동건

서울특별시 송파구 양산로4길 8, 404동 603호

김성훈

경기도 수원시 영통구 봉영로 1620 대우월드마크
101동 1701호

(74) 대리인

윤앤리특허법인(유한)

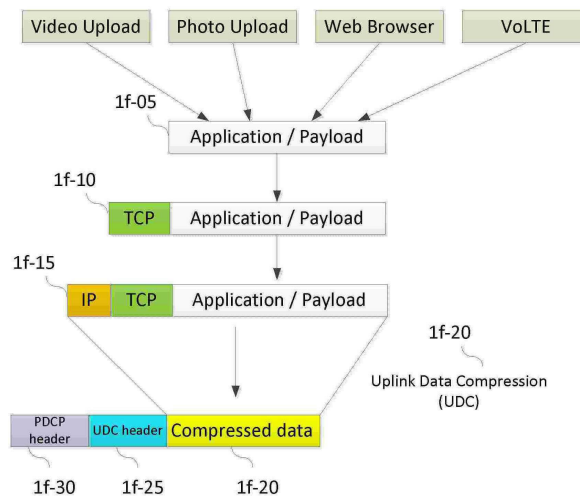
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 차세대 이동 통신 시스템에서 PDCP 계층 장치 기반 보안키 확인 방법 및 장치

(57) 요약

본 개시는 4G 시스템 이후 보다 높은 데이터 전송률을 지원하기 위한 5G 통신 시스템을 IoT 기술과 융합하는 통신 기법 및 그 시스템에 관한 것이다. 본 개시는 5G 통신 기술 및 IoT 관련 기술을 기반으로 지능형 서비스 (예를 들어, 스마트 홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 헬스케어, 디지털 교육, 소매업, 보안 및 안전 관련 서비스 등)에 적용될 수 있다. 본 발명의 한 실시 예는 차세대 이동 통신 시스템에서 암호화된 UDC 헤더를 처리하는 방법 및 장치에 관한 것이다.

대표도 - 도1f



(52) CPC특허분류

H04L 69/22 (2013.01)

명세서

청구범위

청구항 1

무선 통신 시스템에서 제어 신호 처리 방법에 있어서,

기지국으로부터 전송되는 제1 제어 신호를 수신하는 단계;

상기 수신된 제1 제어 신호를 처리하는 단계; 및

상기 처리에 기반하여 생성된 제2 제어 신호를 상기 기지국으로 전송하는 단계를 포함하는 것을 특징으로 하는 제어 신호 처리 방법.

발명의 설명

기술 분야

[0001]

본 발명은 차세대 이동 통신 시스템에서 무선 기기 간의 일대일 통신에서 PDCP 계층 장치 기반으로 보안키를 확인하는 방법 및 장치에 관한 것이다.

배경 기술

[0002]

4G 통신 시스템 상용화 이후 증가 추세에 있는 무선 데이터 트래픽 수요를 충족시키기 위해, 개선된 5G 통신 시스템 또는 pre-5G 통신 시스템을 개발하기 위한 노력이 이루어지고 있다. 이러한 이유로, 5G 통신 시스템 또는 pre-5G 통신 시스템은 4G 네트워크 이후 (Beyond 4G Network) 통신 시스템 또는 LTE 시스템 이후 (Post LTE) 이후의 시스템이라 불리어지고 있다. 높은 데이터 전송률을 달성하기 위해, 5G 통신 시스템은 초고주파(mmWave) 대역 (예를 들어, 60기가(60GHz) 대역과 같은)에서의 구현이 고려되고 있다. 초고주파 대역에서의 전파의 경로 손실 완화 및 전파의 전달 거리를 증가시키기 위해, 5G 통신 시스템에서는 빔포밍(beamforming), 거대 배열 다중 입출력(massive MIMO), 전차원 다중입출력(Full Dimensional MIMO: FD-MIMO), 어레이 안테나(array antenna), 아날로그 빔형성(analog beam-forming), 및 대규모 안테나 (large scale antenna) 기술들이 논의되고 있다. 또한 시스템의 네트워크 개선을 위해, 5G 통신 시스템에서는 진화된 소형 셀, 개선된 소형 셀 (advanced small cell), 클라우드 무선 액세스 네트워크 (cloud radio access network: cloud RAN), 초고밀도 네트워크 (ultra-dense network), 기기 간 통신 (Device to Device communication: D2D), 무선 백홀 (wireless backhaul), 이동 네트워크 (moving network), 협력 통신 (cooperative communication), CoMP (Coordinated Multi-Points), 및 수신 간섭제거 (interference cancellation) 등의 기술 개발이 이루어지고 있다. 이 밖에도, 5G 시스템에서는 진보된 코딩 변조(Advanced Coding Modulation: ACM) 방식인 FQAM (Hybrid FSK and QAM Modulation) 및 SWSC (Sliding Window Superposition Coding)과, 진보된 접속 기술인 FBMC(Filter Bank Multi Carrier), NOMA(non orthogonal multiple access), 및 SCMA(sparse code multiple access) 등이 개발되고 있다.

[0003]

한편, 인터넷은 인간이 정보를 생성하고 소비하는 인간 중심의 연결 망에서, 사물 등 분산된 구성 요소들 간에 정보를 주고 받아 처리하는 IoT(Internet of Things, 사물인터넷) 망으로 진화하고 있다. 클라우드 서버 등과의 연결을 통한 빅데이터(Big data) 처리 기술 등이 IoT 기술에 결합된 IoE (Internet of Everything) 기술도 대두되고 있다. IoT를 구현하기 위해서, 센싱 기술, 유무선 통신 및 네트워크 인프라, 서비스 인터페이스 기술, 및 보안 기술과 같은 기술 요소 들이 요구되어, 최근에는 사물간의 연결을 위한 센서 네트워크(sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 연구되고 있다. IoT 환경에서는 연결된 사물들에서 생성된 데이터를 수집, 분석하여 인간의 삶에 새로운 가치를 창출하는 지능형 IT(Internet Technology) 서비스가 제공될 수 있다. IoT는 기존의 IT(information technology)기술과 다양한 산업 간의 융합 및 복합을 통하여 스마트홈, 스마트 빌딩, 스마트 시티, 스마트 카 혹은 커넥티드 카, 스마트 그리드, 헬스 케어, 스마트 가전, 첨단의료서비스 등의 분야에 응용될 수 있다.

[0004]

이에, 5G 통신 시스템을 IoT 망에 적용하기 위한 다양한 시도들이 이루어지고 있다. 예를 들어, 센서 네트워크 (sensor network), 사물 통신(Machine to Machine, M2M), MTC(Machine Type Communication)등의 기술이 5G 통

신 기술인 빔 포밍, MIMO, 및 어레이 안테나 등의 기법에 의해 구현되고 있는 것이다. 앞서 설명한 빅데이터 처리 기술로써 클라우드 무선 액세스 네트워크(cloud RAN)가 적용되는 것도 5G 기술과 IoT 기술 융합의 일 예라고 할 수 있을 것이다.

발명의 내용

해결하려는 과제

- [0005] 무선 통신 시스템에서 하향 링크는 높은 주파수 대역의 사용과 넓은 대역폭의 사용으로 더 많은 전송 자원을 확보할 수 있다. 또한 기지국에서는 물리적으로 더 많은 안테나를 설치하여 사용할 수 있기 때문에 빔 포밍 이득과 높은 신호 세기를 얻을 수 있어서 동일한 주파수/시간 자원에 더 많은 데이터를 실어서 하향 링크로 데이터를 단말에게 전송할 수 있다. 하지만 상향 링크의 경우, 물리적으로 단말은 작은 크기를 가지고 있으며, 상향 링크 주파수는 높은 주파수 대역과 넓은 대역폭의 사용이 어려우므로 상향 링크 전송 자원이 하향 링크 전송 자원에 비해 병목 현상이 발생할 수 있다. 또한 단말의 최대 송신 파워는 기지국보다 훨씬 작기 때문에 상향 링크 데이터 전송 시에 커버리지가 작아진다는 문제 또한 가지고 있다. 따라서 상향 링크 데이터를 압축하여 전송 자원을 효율적으로 사용할 필요가 있다.
- [0006] 상향 링크 데이터를 압축하는 방법(Uplink Data Compression, UDC)은 이전의 데이터를 기반으로 다음 데이터와 중복되는 데이터 스트림을 찾아서 위치와 길이로 데이터를 표현하여 연쇄적으로 데이터 압축을 수행하는 방식이다. 상기 상향 링크 데이터를 압축하는 방법은 베어러 별로 설정될 수 있으며, 하나의 베어러에는 여러 개의 IP 플로우(flow)들이 맵핑이 될 수 있다. 따라서 IP 플로우 별 패킷에 대해서 상향 링크 데이터 압축을 수행할 수도 있고, 수행하지 않을 수도 있다. 상기에서 상향 링크 데이터 압축을 수행하지 않는 경우는 PDCP 계층 장치 위의 상위 계층 장치에서 이미 데이터 압축을 수행하였기 때문에 데이터 압축률이 떨어지는 경우일 수 있다.
- [0007] 상기에서 상향 링크 데이터를 압축하고 난 후에 PDCP 계층 장치는 UDC 헤더를 생성하고, UDC 헤더에 상위 계층 데이터에 압축 절차를 수행하였음을 지시할 수 있고, 상위 계층 데이터에 압축 절차를 수행하지 않은 경우에는 UDC 헤더에 상위 계층 데이터에 압축 절차를 수행하지 않았음을 지시할 수 있다.
- [0008] 상기와 같이 PDCP 계층 장치에서 생성하는 UDC 헤더에 대해 암호화 절차를 수행하는 경우, 차세대 이동 통신 시스템에서 적용되는 SDAP 계층 장치를 고려하면 데이터 처리 절차가 복잡해질 수 있다. 이와 같은 문제점을 해결하기 위한 방법이 고안되었다.
- [0009] 또한, 차세대 이동 통신 시스템은 공장에서 많은 무선 기기들을 제어하기 위한 용도로 설치될 수 있으며, 자동차 간 통신을 위해서 사용될 수도 있다. 상기 공장 자동화를 위한 무선 기기들 간의 통신 또는 자동차 간의 통신에서 예러 없이 무선 기기들이 동작하도록 하기 위해서는 무선 기기들(Industrial IoT) 간의 데이터 전송에서 높은 신뢰성을 지원해야 하며, 예기치 못한 공격에 대비하기 위해 보안성이 강화되어야 한다. 이와 같은 문제점을 해결하기 위한 방법이 고안되었다.

과제의 해결 수단

- [0010] 상기와 같은 문제점을 해결하기 위한 본 발명은 무선 통신 시스템에서 제어 신호 처리 방법에 있어서, 기지국으로부터 전송되는 제1 제어 신호를 수신하는 단계; 상기 수신된 제1 제어 신호를 처리하는 단계; 및 상기 처리에 기반하여 생성된 제2 제어 신호를 상기 기지국으로 전송하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

- [0011] 본 발명은 본 발명의 다양한 실시 예를 통해, 낮은 전송 지연과 높은 신뢰성을 보장하는 유선 TSN(Time Sensitive Network) 네트워크를 지원하는 공장 자동화 시설 또는 자동차 간 통신을 지원하는 차세대 이동 통신 시스템에서 무선 기기들 간의 데이터 전송에서 신뢰성 있는 일대일 무선 링크를 설정해주고, 보안성을 강화할 수 있는 방법들을 제안한다.

도면의 간단한 설명

- [0012] 도 1a는 본 발명이 적용될 수 있는 LTE 시스템의 구조를 도시하는 도면이다.
- 도 1b는 본 발명이 적용될 수 있는 LTE 시스템에서 무선 프로토콜 구조를 나타낸 도면이다.

도 1c는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 구조를 도시하는 도면이다.

도 1d는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 무선 프로토콜 구조를 나타낸 도면이다. .

도 1e는 본 발명의 다양한 실시 예에 따른 단말이 네트워크와 연결을 설정할 때 기지국이 상향 링크 데이터 압축을 수행할 지 여부를 설정하는 절차를 나타낸 도면이다.

도 1f는 본 발명 의 다양한 실시 예에 따른 상향 링크 데이터 압축(Uplink Data Compression)을 수행하는 절차와 데이터 구성을 나타낸 도면이다.

도 1g는 본 발명 의 다양한 실시 예에 따른 상향 링크 데이터 압축 방법의 한 실시 예를 나타낸 도면이다.

도 1h는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 1 실시 예를 나타낸 도면이다.

도 1i는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 2 실시 예를 나타낸 도면이다.

도 1j는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 3 실시 예를 나타낸 도면이다.

도 1k는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 4 실시 예를 나타낸 도면이다.

도 1l은 본 발명의 상기 실시 예들에서 무결성 보호 및 검증 절차가 설정된 경우, 데이터 처리 절차를 구체적으로 설명한 도면이다.

도 1m는 본 발명의 다양한 실시 예에 따른 단말 동작을 나타낸 도면이다.

도 1n에 본 발명의 실시 예가 적용될 수 있는 단말의 구조를 도시하였다.

도 1o는 본 발명의 실시 예가 적용될 수 있는 무선 통신 시스템에서 TRP의 블록 구성을 도시한다.

도 2a는 본 발명이 적용될 수 있는 LTE 시스템의 구조를 도시하는 도면이다.

도 2b는 본 발명이 적용될 수 있는 LTE 시스템에서 무선 프로토콜 구조를 나타낸 도면이다.

도 2c는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 구조를 도시하는 도면이다.

도 2d는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 무선 프로토콜 구조를 나타낸 도면이다. .

도 2e는 본 발명에서 기지국이 단말의 연결을 해제하여 단말이 RRC 연결 모드(RRC connected mode)에서 RRC 유휴 모드(RRC idle mode)로 전환하는 절차와 단말이 기지국과 연결을 설정하여 RRC 유휴 모드(RRC idle mode)에서 RRC 연결 모드(RRC connected mode)로 전환하는 절차를 설명한 도면이다.

도 2f는 본 발명의 다양한 실시 예에 따른 무선 기기 간 일대일 무선 링크를 설정하고 데이터 송수신을 가능하도록 하는 절차를 나타낸다.

도 2g는 본 발명의 다양한 실시 예에 따른 차세대 이동 통신 시스템에서 사용하는 COUNT 값의 구조를 설명하는 도면이다.

도 2h는 본 발명의 다양한 실시 예에 따른 보안 체크 (Security check) 절차를 나타낸 도면이다.

도 2i는 도 2h에서 제안한 보안 체크 절차를 데이터 베어러(DRB, Data radio bearer)에서 수행하는 구체적인 제 1 실시 예를 나타낸 도면이다.

도 2j는 도 2h에서 제안한 보안 체크 절차를 사이드 링크 베어러(SLRB, Sidelink radio bearer)에서 수행하는 구체적인 제 2 실시 예를 나타낸 도면이다.

도 2k는 본 발명의 다양한 실시 예에 따른 사이드 링크 베어러(SLRB, Sidelink radio bearer)를 통해서 송신단과 수신단이 무선 데이터 통신을 수행할 때 데이터의 유실 여부를 확인하고 무선 링크의 데이터 전송률을 체크할 수 있는 방법을 제안한다.

도 2l는 본 발명에서 제안한 보안 체크 절차의 제 1 실시 예 또는 제 2 실시 예에서 송신단 또는 수신단에서 지

시하는 COUNT 값의 비트의 크기를 줄일 수 있는 방안을 제시한다.

도 2m은 본 발명의 다양한 실시 예에 따른 보안 체크 절차를 수행하는 송신단과 수신단의 동작을 나타낸 도면이다.

도 2n에 본 발명의 실시 예가 적용될 수 있는 단말 또는 무선 노드의 구조를 도시하였다.

도 2o는 본 발명의 실시 예가 적용될 수 있는 무선 통신 시스템에서 TRP 또는 무선 노드의 블록 구성을 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0013] 이하 첨부된 도면을 참조하여 본 발명의 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명하기에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0014] 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 이하 첨부된 도면을 참조하여 본 발명의 실시 예를 설명하기로 한다.
- [0015] 이하 설명에서 사용되는 접속 노드(node)를 식별하기 위한 용어, 망 객체(network entity)들을 지칭하는 용어, 메시지들을 지칭하는 용어, 망 객체들 간 인터페이스를 지칭하는 용어, 다양한 식별 정보들을 지칭하는 용어 등은 설명의 편의를 위해 예시된 것이다. 따라서, 본 발명이 후술되는 용어들에 한정되는 것은 아니며, 동등한 기술적 의미를 가지는 대상을 지칭하는 다른 용어가 사용될 수 있다.
- [0016] 이하 설명의 편의를 위하여, 본 발명은 3GPP LTE(3rd Generation Partnership Project Long Term Evolution) 규격에서 정의하고 있는 용어 및 명칭들을 사용한다. 하지만, 본 발명이 상기 용어 및 명칭들에 의해 한정되는 것은 아니며, 다른 규격에 따르는 시스템에도 동일하게 적용될 수 있다. 본 발명에서 eNB는 설명의 편의를 위하여 gNB와 혼용되어 사용될 수 있다. 즉 eNB로 설명한 기지국은 gNB를 나타낼 수 있다. 또한 단말이라는 용어는 핸드폰, NB-IoT 기기들, 센서들뿐만 아니라 또 다른 무선 통신 기기들을 나타낼 수 있다.
- [0018] 도 1a는 본 발명이 적용될 수 있는 LTE 시스템의 구조를 도시하는 도면이다.
- [0019] 도 1a를 참조하면, 도시한 바와 같이 LTE 시스템의 무선 액세스 네트워크는 차세대 기지국(Evolved Node B, 이하 ENB, Node B 또는 기지국)(1a-05, 1a-10, 1a-15, 1a-20)과 MME (1a-25, Mobility Management Entity) 및 S-GW(1a-30, Serving-Gateway)로 구성된다. 사용자 단말(User Equipment, 이하 UE 또는 단말)(1a-35)은 ENB(1a-05 ~ 1a-20) 및 S-GW(1a-30)를 통해 외부 네트워크에 접속한다.
- [0020] 도 1a에서 ENB(1a-05 ~ 1a-20)는 UMTS 시스템의 기존 노드 B에 대응된다. ENB는 UE(1a-35)와 무선 채널로 연결되며 기존 노드 B 보다 복잡한 역할을 수행한다. LTE 시스템에서는 인터넷 프로토콜을 통한 VoIP(Voice over IP)와 같은 실시간 서비스를 비롯한 모든 사용자 트래픽이 공용 채널(shared channel)을 통해 서비스 되므로, UE들의 버퍼 상태, 가용 전송 전력 상태, 채널 상태 등의 상태 정보를 취합해서 스케줄링을 하는 장치가 필요하며, 이를 ENB(1a-05 ~ 1a-20)가 담당한다. 하나의 ENB는 통상 다수의 셀들을 제어한다. 예컨대, 100 Mbps의 전송 속도를 구현하기 위해서 LTE 시스템은 예컨대, 20 MHz 대역폭에서 직교 주파수 분할 다중 방식(Orthogonal Frequency Division Multiplexing, 이하 OFDM이라 한다)을 무선 접속 기술로 사용한다. 또한 단말의 채널 상태에 맞춰 변조 방식(modulation scheme)과 채널 코딩률(channel coding rate)을 결정하는 적응 변조 코딩(Adaptive Modulation & Coding, 이하 AMC라 한다) 방식을 적용한다. S-GW(1a-30)는 데이터 베어러를 제공하는 장치이며, MME(1a-25)의 제어에 따라서 데이터 베어러를 생성하거나 제거한다. MME는 단말에 대한 이동성 관리 기능은 물론 각종 제어 기능을 담당하는 장치로 다수의 기지국 들과 연결된다.
- [0021] 도 1b는 본 발명이 적용될 수 있는 LTE 시스템에서 무선 프로토콜 구조를 나타낸 도면이다.
- [0022] 도 1b를 참조하면, LTE 시스템의 무선 프로토콜은 단말과 ENB에서 각각 PDCP (Packet Data Convergence Protocol 1b-05, 1b-40), RLC (Radio Link Control 1b-10, 1b-35), MAC (Medium Access Control 1b-15, 1b-30)으로 이루어진다. PDCP (Packet Data Convergence Protocol)(1b-05, 1b-40)는 IP 헤더 압축/복원 등의 동작

을 담당한다. PDCP의 주요 기능은 하기와 같이 요약된다.

- [0023] - 헤더 압축 및 압축 해제 기능(Header compression and decompression: ROHC only)
- [0024] - 사용자 데이터 전송 기능 (Transfer of user data)
- [0025] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs at PDCP re-establishment procedure for RLC AM)
- [0026] - 순서 재정렬 기능(For split bearers in DC (only support for RLC AM): PDCP PDU routing for transmission and PDCP PDU reordering for reception)
- [0027] - 중복 탐지 기능(Duplicate detection of lower layer SDUs at PDCP re-establishment procedure for RLC AM)
- [0028] - 재전송 기능(Retransmission of PDCP SDUs at handover and, for split bearers in DC, of PDCP PDUs at PDCP data-recovery procedure, for RLC AM)
- [0029] - 암호화 및 복호화 기능(Ciphering and deciphering)
- [0030] - 타이머 기반 SDU 삭제 기능(Timer-based SDU discard in uplink.)

- [0032] 무선 링크 제어(Radio Link Control, 이하 RLC라고 한다)(1b-10, 1b-35)는 PDCP PDU(Packet Data Unit)를 적절한 크기로 재구성해서 ARQ 동작 등을 수행한다. RLC의 주요 기능은 하기와 같이 요약된다.
- [0033] - 데이터 전송 기능(Transfer of upper layer PDUs)
- [0034] - ARQ 기능(Error Correction through ARQ (only for AM data transfer))
- [0035] - 접합, 분할, 재조립 기능(Concatenation, segmentation and reassembly of RLC SDUs (only for UM and AM data transfer))
- [0036] - 재분할 기능(Re-segmentation of RLC data PDUs (only for AM data transfer))
- [0037] - 순서 재정렬 기능(Reordering of RLC data PDUs (only for UM and AM data transfer))
- [0038] - 중복 탐지 기능(Duplicate detection (only for UM and AM data transfer))
- [0039] - 오류 탐지 기능(Protocol error detection (only for AM data transfer))
- [0040] - RLC SDU 삭제 기능(RLC SDU discard (only for UM and AM data transfer))
- [0041] - RLC 재수립 기능(RLC re-establishment)

- [0043] MAC(1b-15, 1b-30)은 한 단말에 구성된 여러 RLC 계층 장치들과 연결되며, RLC PDU들을 MAC PDU에 다중화하고 MAC PDU로부터 RLC PDU들을 역다중화하는 동작을 수행한다. MAC의 주요 기능은 하기와 같이 요약된다.
- [0044] - 맵핑 기능(Mapping between logical channels and transport channels)
- [0045] - 다중화 및 역다중화 기능(Multiplexing/demultiplexing of MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels)
- [0046] - 스케줄링 정보 보고 기능(Scheduling information reporting)
- [0047] - HARQ 기능(Error correction through HARQ)
- [0048] - 로지컬 채널 간 우선 순위 조절 기능(Priority handling between logical channels of one UE)
- [0049] - 단말간 우선 순위 조절 기능(Priority handling between UEs by means of dynamic scheduling)
- [0050] - MBMS 서비스 확인 기능(MBMS service identification)

- [0051] - 전송 포맷 선택 기능(Transport format selection)
- [0052] - 패딩 기능(Padding)
- [0053] 물리 계층(1b-20, 1b-25)은 상위 계층 데이터를 채널 코딩 및 변조하고, OFDM 심벌로 만들어서 무선 채널로 전송하거나, 무선 채널을 통해 수신한 OFDM 심벌을 복조하고 채널 디코딩해서 상위 계층으로 전달하는 동작을 한다.
- [0054] 도 1c는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 구조를 도시하는 도면이다.
- [0055] 도 1c를 참조하면, 도시한 바와 같이 차세대 이동통신 시스템(이하 NR 혹은 5G)의 무선 액세스 네트워크는 차세대 기지국(New Radio Node B, 이하 NR gNB 혹은 NR 기지국)(1c-10) 과 NR CN (1c-05, New Radio Core Network)로 구성된다. 사용자 단말(New Radio User Equipment, 이하 NR UE 또는 단말)(1c-15)은 NR gNB(1c-10) 및 NR CN (1c-05)를 통해 외부 네트워크에 접속한다.
- [0056] 도 1c에서 NR gNB(1c-10)는 기존 LTE 시스템의 eNB (Evolved Node B)에 대응된다. NR gNB는 NR UE(1c-15)와 무선 채널로 연결되며 기존 노드 B 보다 더 월등한 서비스를 제공할 수 있다. 차세대 이동통신 시스템에서는 모든 사용자 트래픽이 공용 채널(shared channel)을 통해 서비스 되므로, UE들의 버퍼 상태, 가용 전송 전력 상태, 채널 상태 등의 상태 정보를 취합해서 스케줄링을 하는 장치가 필요하며, 이를 NR NB(1c-10)가 담당한다. 하나의 NR gNB는 통상 다수의 셀들을 제어한다. 현재 LTE 대비 초고속 데이터 전송을 구현하기 위해서 기존 최대 대역폭 이상을 가질 수 있고, 직교 주파수 분할 다중 방식(Orthogonal Frequency Division Multiplexing, 이하 OFDM이라 한다)을 무선 접속 기술로 하여 추가적으로 빔포밍 기술이 적용될 수 있다. 또한 단말의 채널 상태에 맞춰 변조 방식(modulation scheme)과 채널 코딩률(channel coding rate)을 결정하는 적응 변조 코딩(Adaptive Modulation & Coding, 이하 AMC라 한다) 방식을 적용한다. NR CN (1c-05)는 이동성 지원, 베어러 설정, QoS 설정 등의 기능을 수행한다. NR CN는 단말에 대한 이동성 관리 기능은 물론 각종 제어 기능을 담당하는 장치로 다수의 기지국 들과 연결된다. 또한 차세대 이동통신 시스템은 기존 LTE 시스템과도 연동될 수 있으며, NR CN이 MME (1c-25)와 네트워크 인터페이스를 통해 연결된다. MME는 기존 기지국인 eNB (1c-30)와 연결된다.
- [0057] 도 1d는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 무선 프로토콜 구조를 나타낸 도면이다. .
- [0058] 도 1d를 참조하면, 차세대 이동통신 시스템의 무선 프로토콜은 단말과 NR 기지국에서 각각 NR PDCP(1d-05, 1d-40), NR RLC(1d-10, 1d-35), NR MAC(1d-15, 1d-30)으로 이루어진다. NR PDCP (1d-05, 1d-40)의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0059] 헤더 압축 및 압축 해제 기능(Header compression and decompression: ROHC only)
- [0060] - 사용자 데이터 전송 기능 (Transfer of user data)
- [0061] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs)
- [0062] - 비순차적 전달 기능 (Out-of-sequence delivery of upper layer PDUs)
- [0063] - 순서 재정렬 기능(PDCP PDU reordering for reception)
- [0064] - 중복 탐지 기능(Duplicate detection of lower layer SDUs)
- [0065] - 재전송 기능(Retransmission of PDCP SDUs)
- [0066] - 암호화 및 복호화 기능(Ciphering and deciphering)
- [0067] - 타이머 기반 SDU 삭제 기능(Timer-based SDU discard in uplink.)
- [0068] 상기에서 NR PDCP 장치의 순서 재정렬 기능(reordering)은 하위 계층에서 수신한 PDCP PDU들을 PDCP SN(sequence number)을 기반으로 순서대로 재정렬하는 기능을 말하며, 재정렬된 순서대로 데이터를 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 순서를 고려하지 않고, 바로 전달하는 기능을 포함할 수 있으며, 순서를 재정렬하여 유실된 PDCP PDU들을 기록하는 기능을 포함할 수 있으며, 유실된 PDCP PDU들에 대한 상태 보고를 송신 측에 하는 기능을 포함할 수 있으며, 유실된 PDCP PDU들에 대한 재전송을 요청하는 기능을 포함할 수 있다.

- [0070] NR RLC(1d-10, 1d-35)의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0071] - 데이터 전송 기능(Transfer of upper layer PDUs)
- [0072] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs)
- [0073] - 비순차적 전달 기능(Out-of-sequence delivery of upper layer PDUs)
- [0074] - ARQ 기능(Error Correction through ARQ)
- [0075] - 접합, 분할, 재조립 기능(Concatenation, segmentation and reassembly of RLC SDUs)
- [0076] - 재분할 기능(Re-segmentation of RLC data PDUs)
- [0077] - 순서 재정렬 기능(Reordering of RLC data PDUs)
- [0078] - 중복 탐지 기능(Duplicate detection)
- [0079] - 오류 탐지 기능(Protocol error detection)
- [0080] - RLC SDU 삭제 기능(RLC SDU discard)
- [0081] - RLC 재수립 기능(RLC re-establishment)
- [0082] 상기에서 NR RLC 장치의 순차적 전달 기능(In-sequence delivery)은 하위 계층으로부터 수신한 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 말하며, 원래 하나의 RLC SDU가 여러 개의 RLC SDU들로 분할되어 수신된 경우, 이를 재조립하여 전달하는 기능을 포함할 수 있으며, 수신한 RLC PDU들을 RLC SN(sequence number) 혹은 PDCP SN(sequence number)를 기준으로 재정렬하는 기능을 포함할 수 있으며, 순서를 재정렬하여 유실된 RLC PDU들을 기록하는 기능을 포함할 수 있으며, 유실된 RLC PDU들에 대한 상태 보고를 송신 측에 하는 기능을 포함할 수 있으며, 유실된 RLC PDU들에 대한 재전송을 요청하는 기능을 포함할 수 있으며, 유실된 RLC SDU가 있을 경우, 유실된 RLC SDU 이전까지의 RLC SDU들만을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 유실된 RLC SDU가 있어도 소정의 타이머가 만료되었다면 타이머가 시작되기 전에 수신된 모든 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 유실된 RLC SDU가 있어도 소정의 타이머가 만료되었다면 현재까지 수신된 모든 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있다. 또한 상기에서 RLC PDU들을 수신하는 순서대로 (일련번호, Sequence number의 순서와 상관없이, 도착하는 순으로) 처리하여 PDCP 장치로 순서와 상관없이(Out-of sequence delivery) 전달할 수도 있으며, segment 인 경우에는 버퍼에 저장되어 있거나 추후에 수신될 segment들을 수신하여 온전한 하나의 RLC PDU로 재구성한 후, 처리하여 PDCP 장치로 전달할 수 있다. 상기 NR RLC 계층은 접합(Concatenation) 기능을 포함하지 않을 수 있고 상기 기능을 NR MAC 계층에서 수행하거나 NR MAC 계층의 다중화(multiplexing) 기능으로 대체할 수 있다.
- [0084] 상기에서 NR RLC 장치의 비순차적 전달 기능(Out-of-sequence delivery)은 하위 계층으로부터 수신한 RLC SDU들을 순서와 상관없이 바로 상위 계층으로 전달하는 기능을 말하며, 원래 하나의 RLC SDU가 여러 개의 RLC SDU들로 분할되어 수신된 경우, 이를 재조립하여 전달하는 기능을 포함할 수 있으며, 수신한 RLC PDU들의 RLC SN 혹은 PDCP SN을 저장하고 순서를 정렬하여 유실된 RLC PDU들을 기록해두는 기능을 포함할 수 있다.
- [0086] NR MAC(1d-15, 1d-30)은 한 단말에 구성된 여러 NR RLC 계층 장치들과 연결될 수 있으며, NR MAC의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0087] - 맵핑 기능(Mapping between logical channels and transport channels)
- [0088] - 다중화 및 역다중화 기능(Multiplexing/demultiplexing of MAC SDUs)
- [0089] - 스케줄링 정보 보고 기능(Scheduling information reporting)
- [0090] - HARQ 기능(Error correction through HARQ)
- [0091] - 로지컬 채널 간 우선 순위 조절 기능(Priority handling between logical channels of one UE)
- [0092] - 단말간 우선 순위 조절 기능(Priority handling between UEs by means of dynamic scheduling)

- [0093] - MBMS 서비스 확인 기능(MBMS service identification)
- [0094] - 전송 포맷 선택 기능(Transport format selection)
- [0095] - 패딩 기능(Padding)
- [0096] NR PHY 계층(1d-20, 1d-25)은 상위 계층 데이터를 채널 코딩 및 변조하고, OFDM 심벌로 만들어서 무선 채널로 전송하거나, 무선 채널을 통해 수신한 OFDM 심벌을 복조하고 채널 디코딩해서 상위 계층으로 전달하는 동작을 수행할 수 있다.
- [0098] 본 발명에서는 무선 통신 시스템에서 단말이 상향 링크로 데이터를 전송할 때에 데이터를 압축하고 기지국에서 이를 압축 해제하는 절차를 제안하고, 구체적인 헤더 포맷, 압축 해제 실패 시 해결 방법 등 송신단에서 데이터를 압축하고 전송하고 수신단에서 이를 압축해제하는 데이터 송수신 절차에 대한 지원 방법을 제안한다. 또한 본 발명에서 제안하는 방법은 기지국이 단말에게 하향 링크 데이터를 전송할 때에 데이터를 압축해서 전송하고 단말이 압축된 하향 링크 데이터를 수신하여 압축 해제하는 절차에도 적용될 수 있다. 상기와 같이 본 발명에서는 송신단에서 데이터를 압축하여 전송함으로써, 더 많은 데이터를 전송할 수 있도록 함과 동시에 커버리지를 향상시키는 효과를 가져오도록 한다.
- [0100] 도 1e는 본 발명의 다양한 실시 예에 따른 단말이 네트워크와 연결을 설정할 때 기지국이 상향 링크 데이터 압축을 수행할 지 여부를 설정하는 절차를 나타낸 도면이다.
- [0101] 도 1e는 본 발명에서 단말이 RRC 유희 모드(RRC idle mode) 혹은 RRC 비활성화 모드(RRC Inactive mode 혹은 lightly-connected mode)에서 RRC 연결 모드(RRC connected mode)로 전환하여 네트워크와 연결을 설정하는 절차를 설명하며, 상향 링크 데이터 압축(Uplink Data Compression, UDC)을 수행할 지 여부를 설정하는 절차를 설명한다.
- [0102] 도 1e에서 기지국은 RRC 연결 모드에서 데이터를 송수신하는 단말이 소정의 이유로 혹은 일정 시간 동안 데이터의 송수신이 없으면 RRCConnectionRelease 메시지를 단말에게 보내어 단말을 RRC 유희모드로 전환하도록 할 수 있다(1e-01). 추후에 현재 연결이 설정되어 있지 않은 단말 (이하 idle mode UE)은 전송할 데이터가 발생하면 기지국과 RRC connection establishment과정을 수행한다. 단말은 랜덤 액세스 과정을 통해서 기지국과 역방향 전송 동기를 수립하고 RRCConnectionRequest 메시지를 기지국으로 전송한다 (1e-05). 상기 메시지에는 단말의 식별자와 연결을 설정하고자 하는 이유(establishmentCause) 등이 수납된다. 기지국은 단말이 RRC 연결을 설정하도록 RRCConnectionSetup 메시지를 전송한다(1e-10). 상기 메시지에는 각 로지컬 채널 별(logicalchannelconfig)로 혹은 베어러 별로 혹은 각 PDCP 장치 별(PDCP-config)로 상향 링크 데이터 압축 방법(UDC)을 사용할지 말지를 지시하는 정보를 포함할 수 있다. 또한 더 구체적으로 각 로지컬 채널 혹은 베어러 혹은 각 PDCP 장치(혹은 SDAP 장치)에서 어떤 IP flow 혹은 어떤 QoS flow에 대해서만 상향 링크 데이터 압축 방법(UDC)을 사용할지를 지시할 수 있다(SDAP 장치에게 상향 링크 데이터 압축 방법을 사용하거나 사용하지 않을 IP flow 혹은 QoS flow에 대한 정보를 설정하여 SDAP 장치에게 PDCP 장치에게 상향 링크 데이터 압축 방법을 사용할 지 사용하지 않을 지를 각 QoS flow에 대해서 지시해줄 수도 있다 혹은 PDCP 장치가 각 QoS flow를 스스로 확인하고, 상향 링크 압축 방법을 적용할 지 하지 않을지를 결정할 수도 있다). 또한 상기에서 상향 링크 데이터 압축 방법을 사용할 것을 지시한다면 상향 링크 데이터 압축 방법에서 사용할 미리 정의된 라이브러리(library) 혹은 사전정보(Dictionary)에 대한 식별자 혹은 상향 링크 데이터 압축 방법에서 사용할 버퍼 사이즈 크기 등을 지시할 수 있다. 또한 상기 메시지는 상향 링크 압축 해제를 수행하도록 셋업(setup)하거나 해제(release)하는 명령을 포함할 수 있다. 또한 상기에서 상향 링크 데이터 압축 방법을 사용하도록 설정할 때는 항상 RLC AM 베어러(ARQ 기능, 재전송 기능이 있어 손실이 없는 모드)로 설정할 수 있으며, 헤더 압축 프로토콜(ROHC)와는 함께 설정하지 않을 수 있다. 또한 상기 메시지에는 RRC 연결 구성 정보 등이 수납된다. RRC 연결은 SRB (Signaling Radio Bearer)라고도 하며, 단말과 기지국 사이의 제어 메시지인 RRC 메시지 송수신에 사용된다. RRC 연결을 설정한 단말은 RRCConnexionSetupComplete 메시지를 기지국으로 전송한다 (1e-15). 만약 기지국이 현재 연결을 설정하고 있는 단말에 대한 단말 능력을 모른다면 혹은 단말 능력을 파악하고 싶다면 단말의 능력을 물어보는 메시지를 보낼 수 있다. 그리고 단말은 자신의 능력을 보고하는 메시지를 보낼 수 있다. 상기 메시지에서 단말이 상향 링크 데이터 압축 방법(Uplink Data Compression, UDC)을 사용할 수 있는 지 여부를 나타낼 수 있으며, 이를 지시하는 지시자를 포함하여 보낼 수 있다. 상기 RRCConnexionSetupComplete 메시지에

는 단말이 소정의 서비스를 위한 베어러 설정을 MME에게 요청하는 SERVICE REQUEST라는 제어 메시지가 포함되어 있다. 기지국은 RRCConnectionSetupComplete 메시지에 수납된 SERVICE REQUEST 메시지를 MME로 전송하고 (1e-20), MME는 단말이 요청한 서비스를 제공할지 여부를 판단한다. 판단 결과 단말이 요청한 서비스를 제공하기로 결정하였다면 MME는 기지국에게 INITIAL CONTEXT SETUP REQUEST라는 메시지를 전송한다(1e-25). 상기 메시지에는 DRB (Data Radio Bearer) 설정 시 적용할 QoS (Quality of Service) 정보, 그리고 DRB에 적용할 보안 관련 정보 (예를 들어 Security Key, Security Algorithm) 등의 정보가 포함된다. 기지국은 단말과 보안을 설정하기 위해서 SecurityModeCommand 메시지(1e-30)와 SecurityModeComplete 메시지(1e-35)를 교환한다. 보안 설정이 완료되면 기지국은 단말에게 RRCConnectionReconfiguration 메시지를 전송한다(1e-40). 상기 메시지에는 각 로지컬 채널 별(logicalchannelconfig)로 혹은 베어러 별로 혹은 각 PDCP 장치 별(PDCP-config)로 상향 링크 데이터 압축 방법(UDC)을 사용할지 말지를 지시하는 정보를 포함할 수 있다. 또한 더 구체적으로 각 로지컬 채널 혹은 베어러 혹은 각 PDCP 장치(혹은 SDAP 장치)에서 어떤 IP flow 혹은 어떤 QoS flow에 대해서만 상향 링크 데이터 압축 방법(UDC)을 사용할지를 지시할 수 있다(SDAP 장치에게 상향 링크 데이터 압축 방법을 사용하거나 사용하지 않을 IP flow 혹은 QoS flow에 대한 정보를 설정하여 SDAP 장치가 PDCP 장치에게 상향 링크 데이터 압축 방법을 사용할 지 사용하지 않을 지를 각 QoS flow에 대해서 지시해줄 수도 있다 혹은 PDCP 장치가 각 QoS flow를 스스로 확인하고, 상향 링크 압축 방법을 적용할 지 하지 않을지를 결정할 수도 있다). 또한 상기에서 상향 링크 데이터 압축 방법을 사용할 것을 지시한다면 상향 링크 데이터 압축 방법에서 사용할 미리 정의된 라이브러리(library) 혹은 사전정보(Dictionary)에 대한 식별자 혹은 상향 링크 데이터 압축 방법에서 사용할 버퍼 사이즈 크기 등을 지시할 수 있다. 또한 상기 메시지는 상향 링크 압축 해제를 수행하도록 셋업(setup)하거나 해제(release)하는 명령을 포함할 수 있다. 또한 상기에서 상향 링크 데이터 압축 방법을 사용하도록 설정할 때는 항상 RLC AM 베어러(ARQ 기능, 재전송 기능이 있어 손실이 없는 모드)로 설정할 수 있으며, 헤더 압축 프로토콜(ROHC)와는 함께 설정하지 않을 수 있다. 또한 상기 메시지에는 사용자 데이터가 처리될 DRB의 설정 정보가 포함되며, 단말은 상기 정보를 적용해서 DRB를 설정하고 기지국에게 RRCConnectionReconfigurationComplete 메시지를 전송한다(1e-45). 단말과 DRB 설정을 완료한 기지국은 MME에게 INITIAL CONTEXT SETUP COMPLETE 메시지를 전송하고 (1e-50), 이를 수신한 MME는 S-GW와 S1 베어러를 설정하기 위해서 S1 BEARER SETUP 메시지와 S1 BEARER SETUP RESPONSE 메시지를 교환한다(1e-055, 1e-60). S1 베어러는 S-GW와 기지국 사이에 설정되는 데이터 전송용 연결이며 DRB와 1대 1로 대응된다. 상기 과정이 모두 완료되면 단말은 기지국과 S-GW를 통해 데이터를 송수신한다(1e-65, 1e-70). 이처럼 일반적인 데이터 전송 과정은 크게 RRC 연결 설정, 보안 설정, DRB설정의 3단계로 구성된다. 또한 기지국은 소정의 이유로 단말에게 설정을 새로 해주거나 추가하거나 변경하기 위해서 RRCConnectionReconfiguration 메시지를 전송할 수 있다(1e-75). 상기 메시지에는 각 로지컬 채널 별(logicalchannelconfig)로 혹은 베어러 별로 혹은 각 PDCP 장치 별(PDCP-config)로 상향 링크 데이터 압축 방법(UDC)을 사용할지 말지를 지시하는 정보를 포함할 수 있다. 또한 더 구체적으로 각 로지컬 채널 혹은 베어러 혹은 각 PDCP 장치(혹은 SDAP 장치)에서 어떤 IP flow 혹은 어떤 QoS flow에 대해서만 상향 링크 데이터 압축 방법(UDC)을 사용할지를 지시할 수 있다(SDAP 장치에게 상향 링크 데이터 압축 방법을 사용하거나 사용하지 않을 IP flow 혹은 QoS flow에 대한 정보를 설정하여 SDAP 장치가 PDCP 장치에게 상향 링크 데이터 압축 방법을 사용할 지 사용하지 않을 지를 각 QoS flow에 대해서 지시해줄 수도 있다 혹은 PDCP 장치가 각 QoS flow를 스스로 확인하고, 상향 링크 압축 방법을 적용할 지 하지 않을지를 결정할 수도 있다). 또한 상기에서 상향 링크 데이터 압축 방법을 사용할 것을 지시한다면 상향 링크 데이터 압축 방법에서 사용할 미리 정의된 라이브러리(library) 혹은 사전정보(Dictionary)에 대한 식별자 혹은 상향 링크 데이터 압축 방법에서 사용할 버퍼 사이즈 크기 등을 지시할 수 있다. 또한 상기 메시지는 상향 링크 압축 해제를 수행하도록 셋업(setup)하거나 해제(release)하는 명령을 포함할 수 있다. 또한 상기에서 상향 링크 데이터 압축 방법을 사용하도록 설정할 때는 항상 RLC AM 베어러(ARQ 기능, 재전송 기능이 있어 손실이 없는 모드)로 설정할 수 있으며, 헤더 압축 프로토콜(ROHC)와는 함께 설정하지 않을 수 있다.

[0104] 도 1f는 본 발명의 다양한 실시 예에 따른 상향 링크 데이터 압축(Uplink Data Compression)을 수행하는 절차와 데이터 구성을 나타낸 도면이다.

[0105] 도 1f에서 상향 링크 데이터(1f-05)는 비디오 전송, 사진 전송, 웹 검색, VoLTE와 같은 서비스들에 해당하는 데이터로 생성될 수 있다. 응용 계층(application layer) 장치에서 생성된 데이터들은 네트워크 데이터 전송 계층에 해당하는 TCP/IP 혹은 UDP를 통해 처리되고, 각 헤더(1f-10, 1f-15)를 구성하고 PDCP 계층에 전달될 수 있다. 상기 PDCP 계층은 상위 계층으로부터 데이터(PDCP SDU)를 수신하면 다음과 같은 절차를 수행할 수 있다.

- [0106] 만약 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 PDCP 계층에서 상향 링크 데이터 압축 방법을 사용하도록 설정하였다면 1f-20과 같이 PDCP SDU에 대해서 상향 링크 데이터 압축(Uplink Data Compression) 방법을 수행하여 상향 링크 데이터를 압축하고, 그에 상응하는 UDC 헤더(압축된 상향 링크 데이터를 위한 헤더, 1f-25)를 구성하고, UDC 헤더를 제외하고 압축된 데이터에 대해 암호화(ciphering)을 수행하고, 설정되었다면 무결성 보호(Integrity protection)을 수행하고 PDCP 헤더(1f-30)를 구성하여 PDCP PDU를 구성할 수 있다. 상기에서 PDCP 계층 장치는 UDC 압축/압축해제 장치를 포함하고 있으며, 상기 RRC 메시지에서 설정된 대로 각 데이터에 대해서 UDC 절차를 수행할지 수행하지 않을 지 판단하고, 상기 UDC 압축/압축해제 장치를 사용한다. 송신단에서는 송신 PDCP 계층 장치에서 UDC 압축 장치를 이용하여 데이터 압축을 수행하고, 수신단에서는 수신 PDCP 계층 장치에서 UDC 압축 해제 장치를 사용하여 데이터 압축 해제를 수행한다.
- [0107] 상기에서 설명한 도 1f 절차는 단말이 상향 링크 데이터 압축할 때뿐만 아니라 하향 링크 데이터를 압축하는 데에도 적용할 수 있다. 또한 상기 상향 링크 데이터에 대한 설명은 하향 링크 데이터에 대해서도 동일하게 적용될 수 있다.
- [0109] 도 1g는 본 발명의 다양한 실시 예에 따른 적용될 수 있는 상향 링크 데이터 압축 방법의 한 실시 예를 나타낸 도면이다.
- [0110] 도 1g는 DEFLATE 기반 상향 링크 데이터 압축 알고리즘에 대한 설명을 나타낸 도면이며, DEFLATE 기반 상향 링크 데이터 압축 알고리즘은 손실이 없는 압축 알고리즘이다. 상기 DEFLATE 기반 상향 링크 데이터 압축 알고리즘은 기본적으로 LZ77 알고리즘과 호프만(Huffman) 코딩을 결합하여 상향 링크 데이터를 압축한다. 상기 LZ77 알고리즘은 데이터의 중복된 배열을 찾는 동작을 수행하고, 중복된 배열을 찾을 때 슬라이딩 윈도우를 통해 슬라이딩 윈도우 내에서 중복된 배열을 찾아서 중복된 배열이 있는 경우, 슬라이딩 윈도우 내에서 중복된 배열이 있는 위치와 중복된 정도를 길이로 나타내어 표현하여 데이터 압축을 수행한다. 상기 슬라이딩 윈도우는 상향 링크 데이터 압축 방법(UDC)에서 버퍼라고도 불리며, 8킬로바이트 혹은 32킬로바이트로 설정될 수 있다. 즉, 상기 슬라이딩 윈도우 혹은 버퍼는 8192 개 혹은 32768 개의 문자들에 대해서 기록하고 중복된 배열을 찾아서 위치와 길이로 표현하여 압축을 수행할 수 있다. 따라서 상기 LZ 알고리즘은 슬라이딩 윈도우 방식이기 때문에 즉, 이전에 코딩한 데이터들을 버퍼에 업데이트하고, 다시 바로 다음 데이터들에 코딩을 수행하기 때문에 연속되는 데이터들 간에 상관관계를 갖게 된다. 따라서 먼저 코딩한 데이터들이 정상적으로 디코딩되어야만 그 다음 데이터들이 정상적으로 디코딩이 가능하다. 상기에서 LZ77 알고리즘으로 위치와 길이로 표현되어 압축된 코드들(위치, 길이 등의 표현)은 호프만(Huffman) 코딩을 통하여 한번 더 압축이 수행된다. 상기 호프만 코딩은 다시 중복된 코드들을 찾으면서 중복된 정도가 많은 코드에는 짧은 표기를 사용하고, 중복된 정도가 적은 코드에는 긴 표기를 사용하여 다시 한번 압축을 수행한다. 상기 호프만 코딩은 접두사 코딩(prefix code)이고, 모든 코드가 뚜렷이 구분되는 특징(Uniquely decodable)을 가지고 있는 최적의 코딩 방식이다.
- [0111] 송신단에서는 상기에서 설명한 것과 같이 원래 데이터(1g-05)에 LZ77 알고리즘을 적용하여 인코딩을 수행하고(1g-10), 버퍼를 업데이트(1g-15)하고, 상기 버퍼의 콘텐츠(혹은 데이터)에 대한 체크섬(checksum) 비트들을 생성하여 UDC 헤더에 구성할 수 있다. 상기 체크섬 비트들은 수신단에서 버퍼 상태의 유효성 여부를 판단하기 위해 사용된다. 상기 LZ77 알고리즘으로 인코딩된 코드들을 호프만 코딩으로 한번 더 압축하여 상향 링크 데이터로 전송할 수 있다(1g-25). 수신단에서는 상기 수신한 압축된 데이터를 송신단의 반대로 압축 해제 절차를 수행한다. 즉, 호프만 디코딩을 수행하고(1g-30), 버퍼를 업데이트하고(1g-35), 업데이트된 버퍼의 유효성 여부를 UDC 헤더의 체크섬 비트들로 확인한다. 상기 체크섬 비트들이 오류 없다고 판단되면 LZ77 알고리즘으로 디코딩을 수행하여(1g-40) 데이터를 압축 해제하고 원래의 데이터를 복원하여 상위 계층으로 전달할 수 있다(1g-45).
- [0112] 상기에서 설명한 바와 같이 상기 LZ 알고리즘은 슬라이딩 윈도우 방식이기 때문에 즉, 이전에 코딩한 데이터들을 버퍼에 업데이트하고, 다시 바로 다음 데이터들에 코딩을 수행하기 때문에 연속되는 데이터들 간에 상관관계를 갖게 된다. 따라서 먼저 코딩한 데이터들이 정상적으로 디코딩되어야만 그 다음 데이터들이 정상적으로 디코딩이 가능하다. 따라서 수신 PDCP 계층 장치는 PDCP 헤더의 PDCP 일련번호를 확인하고 UDC 헤더를 확인(데이터 압축을 수행했는지 수행하지 않았는지를 지시하는 지시자를 확인)하여 데이터 압축 절차가 적용된 데이터들에 대해서 PDCP 일련번호의 오름차순 순으로 데이터 압축 해제 절차를 수행한다.
- [0114] 본 발명에서 제안하는 기지국이 단말에게 상향 링크 데이터 압축(Uplink data compression, UDC) 설정을 수행하

는 절차와 단말이 상향 링크 데이터 압축(UDC)을 수행하는 절차는 다음과 같다.

- [0115] 기지국은 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지로 단말에게 RLC AM 모드를 설정한 베어러 혹은 로지컬 채널에 상향 링크 데이터 압축을 수행할 것을 설정하거나 혹은 해제할 수 있다. 또한 상기 RRC 메시지를 이용하여 단말의 PDCP 계층 장치의 UDC 장치(혹은 프로토콜)를 리셋(reset)할 수 있다. 상기에서 UDC 장치(혹은 프로토콜)를 리셋한다는 것은 단말의 상향링크 데이터 압축을 위한 UDC 버퍼를 리셋한다는 의미이며, 단말의 UDC 버퍼와 기지국의 상향 링크 데이터 압축 해제를 위한 UDC 버퍼 간의 동기를 맞추기 위함이다. 상기에서 UDC 장치의 버퍼를 리셋하는 동작은 기존의 PDCP control PDU를 변형해서 정의하거나 새로운 PDCP control PDU를 정의하여 상기 RRC 메시지를 대신하여 PDCP control PDU로 송신단(기지국)이 수신단(단말)의 UDC 버퍼를 리셋하고 송수신단 간 사용자 데이터 압축 및 압축 해제를 위한 동기화를 위해 사용될 수 있다. 또한 상기 RRC 메시지를 이용하여 베어러 별 혹은 로지컬 채널 별 혹은 PDCP 계층 장치 별로 상향 링크 데이터 압축 수행 여부를 수행할 수 있으며, 더 구체적으로 하나의 베어러 혹은 로지컬 채널 혹은 PDCP 계층 장치 내에서 각 IP flow (혹은 QoS flow) 별로 상향 링크 데이터 압축 해제를 수행할 지 수행하지 않을 지를 설정해줄 수 있다.
- [0116] 또한 상기 RRC 메시지로 기지국은 단말에게 PDCP 폐기 타이머(PDCP discard timer) 값을 설정해줄 수 있다. 상기 PDCP 폐기 타이머 값은 상향 링크 데이터 압축을 수행하지 않는 데이터를 위한 PDCP 폐기 타이머 값과 상향 링크 데이터 압축을 적용하는 데이터를 위한 PDCP 폐기 타이머 값을 별도로 설정해줄 수도 있다.
- [0117] 단말은 상기 RRC 메시지로 소정의 베어러 혹은 로지컬 채널 혹은 PDCP 계층 장치에 대해서(혹은 소정의 베어러 혹은 로지컬 채널 혹은 PDCP 계층 장치의 어떤 QoS flow들에 대해서) 상향 링크 데이터 압축을 수행할 것을 설정 받았다면 상기 설정에 맞게 PDCP 계층 장치의 UDC 장치에서 버퍼를 리셋하고, 상향 링크 데이터 압축 절차를 준비한다. 그리고 상위 계층으로부터 데이터를 수신하면(PDCP SDU) 만약 PDCP 계층 장치에 대해서 상향 링크 데이터 압축을 수행하도록 설정되었다면 상기에서 수신한 데이터에 대해서 상향 링크 데이터 압축을 수행한다. 만약 PDCP 계층 장치의 특정 QoS flow들에 대해서만 상향 링크 데이터 압축을 수행하도록 설정되었다면 상위 SDAP 계층의 지시 혹은 QoS flow 식별자를 확인하여 상향 링크 데이터 압축 수행 여부를 판단하고 상향 링크 데이터 압축을 수행한다. 그리고 만약 상향 링크 데이터 압축(UDC)을 수행하고 상기 데이터 압축에 맞게 버퍼를 업데이트하였다면 UDC 버퍼를 구성한다. 상기에서 상향 링크 데이터 압축(UDC)을 수행하면 상위 계층으로부터 수신한 PDCP SDU를 더 작은 크기를 갖는 UDC 압축 데이터(UDC block)으로 압축할 수 있다. 그리고 압축한 UDC 압축 데이터에 대한 UDC 헤더를 구성한다. 상기 UDC 헤더에는 상향 링크 데이터 압축을 수행하였는지 수행하지 않았는지를 지시하는 지시자를 포함할 수 있다(예를 들어 UDC 헤더에서 1비트 지시자로 0이면 UDC 적용, 1이면 UDC 미 적용). 상기에서 상향 링크 데이터 압축을 적용하지 않은 경우는 상위 계층으로부터 수신한 PDCP SDU 데이터 구조가 반복적인 데이터 구조를 가지지 않아서 상기에서 설명한 UDC 압축 방법(DEFLATE 알고리즘)으로 데이터 압축이 수행될 수 없는 경우를 포함할 수 있다. 상기에서 상위 계층으로부터 수신한 데이터(PDCP SDU)에 대해서 상향 링크 데이터 압축(UDC)을 수행하고, UDC 버퍼를 업데이트하였다면 수신단 PDCP 계층 장치에서 상기 업데이트된 UDC 버퍼의 유효성을 확인하기 위해서 체크섬(checksum) 비트들을 계산하여 상기 UDC 버퍼에 포함하여 구성할 수 있다(상기 체크섬 비트들은 소정의 길이를 가지며 예를 들면 4비트로 구성될 수 있다).
- [0118] 단말은 상기에서 상향 링크 데이터 압축 해제를 적용한 혹은 적용하지 않은 데이터에 대해 암호화(ciphering)을 수행하고 설정되었다면 무결성 보호(Integrity protection)을 수행하고 하위 계층으로 전달한다.
- [0120] 본 발명의 다음에서는 상기 본 발명에서 제안한 사용자 데이터 압축 방법 (UDC, Uplink data compression)을 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 효과적으로 수행하는 방법을 제안한다.
- [0121] 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 1 실시 예를 다음과 같이 제안한다. 상기 제 1 실시 예에서는 사용자 데이터 압축 방법을 이용하여 SDAP 헤더를 압축하는 것을 특징으로 하며, UDC 헤더를 암호화하는 것을 특징으로 하며, 상기와 같은 특징으로 인해 상위 계층 데이터에 대해 SDAP 헤더의 유무와 상관없이 동일한 절차를 수행할 수 있기 때문에 구현의 편의성을 향상시킬 수 있으며, UDC 헤더를 암호화하여 보안성을 강화할 수 있다.
- [0122] 도 1h는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 1 실시 예를 나타낸 도면이다.
- [0123] 도 1h 에서 SDAP 계층 장치는 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 SDAP 계층 장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우 그리고 사용자 데이터 압축(Uplink

data compression, UDC)을 설정한 경우, 상위 계층으로부터 데이터를 수신하면 1h-05와 같이 SDAP 계층 장치는 SDAP 헤더를 생성하고 구성하여 PDCP 계층 장치에게 전달할 수 있다. 상기 PDCP 계층 장치는 상위 SDAP 계층 장치로부터 수신한 PDCP SDU(SDAP 헤더와 IP 패킷, 1h-06)에 대해 사용자 데이터 압축을 수행할 수 있다(1h-07). 그리고 체크섬 필드를 계산하고 UDC 적용 여부를 설정하여 UDC 헤더를 생성하고 부착할 수 있다(1h-10). 그리고 상기 UDC 헤더와 압축된 UDC block에 대해 암호화를 수행하고 PDCP 헤더(1h-20)를 생성하고 구성하여 집합한 후 하위 계층으로 전달하여 데이터 처리를 RLC 계층 장치와 MAC 계층 장치에서 진행할 수 있다.

[0124] 도 1h에서 설명한 절차는 사용자 데이터 압축 방법을 이용하여 SDAP 헤더를 압축하는 것을 특징으로 하며, UDC 헤더를 암호화하는 것을 특징으로 하며, 상기와 같은 특징으로 인해 상위 계층 데이터에 대해 SDAP 헤더의 유무와 상관없이 동일한 절차를 수행할 수 있기 때문에 구현의 편의성을 향상시킬 수 있으며, UDC 헤더를 암호화하여 보안성을 강화할 수 있다.

[0126] 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 2 실시 예를 다음과 같이 제안한다. 상기 제 2 실시 예에서는 사용자 데이터 압축 방법을 SDAP 헤더에 적용하지 않는 것을 특징으로 하며, SDAP 헤더는 암호화하지 않고, UDC 헤더를 암호화하는 것을 특징으로 하며, 상기와 같은 특징으로 인해 SDAP 헤더의 정보를 송신단 또는 수신단에서 복호화 절차 필요 없이 SDAP 헤더의 QoS 정보를 활용할 수 있다는 장점을 가진다. 예를 들면 기지국의 경우, 스케줄링에 상기 QoS 정보를 사용할 수 있고, 또한 단말 구현에서도 상위 계층 데이터를 수신할 때마다 SDAP 헤더를 생성할 필요 없이 하드웨어 가속기로 UDC 절차를 수행하고 암호화를 수행하고, SDAP 헤더는 나중에 붙일 수 있기 때문에 단말 구현에도 용이하다. 또한 UDC 헤더를 암호화하여 보안성을 강화할 수 있다.

[0127] 도 1i은 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 2 실시 예를 나타낸 도면이다.

[0128] 도 1i 에서 SDAP 계층 장치는 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 SDAP 계층 장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우 그리고 사용자 데이터 압축(Uplink data compression, UDC)을 설정한 경우, 상위 계층으로부터 데이터를 수신하면 1i-05와 같이 SDAP 헤더를 생성하고 구성하여 PDCP 계층 장치에게 전달할 수 있다. 상기 PDCP 계층 장치는 상위 SDAP 계층 장치로부터 수신한 PDCP SDU(SDAP 헤더와 IP 패킷, 1i-06)에서 SDAP 헤더를 제외한 나머지 데이터 부분에 사용자 데이터 압축 절차를 수행할 수 있다(1i-07). 그리고 체크섬 필드를 계산하고 UDC 적용 여부를 설정하여 UDC 헤더를 생성하고 SDAP 헤더 앞에 부착할 수 있다(1i-10). 그리고 무결성 보호가 설정되었다면 무결성 보호(Integrity protection)를 암호화 절차 수행 전에 상기 UDC 헤더와 압축된 UDC block 또는 PDCP 헤더에 대해 무결성 보호를 적용하고 나서 상기 UDC 헤더와 압축된 UDC block에 대해 암호화를 수행하기 위해서 UDC block에 대해서 암호화를 수행하고, UDC 헤더에도 암호화를 별도로 수행할 수 있다(1i-15, 1i-20). 만약에 한번만 암호화 절차를 수행하려면 중간에 SDAP 헤더를 떼어내고 UDC 헤더와 UDC block에 대해 암호화를 한번에 수행하고 다시 UDC 헤더와 UDC block 사이에 암호화되지 않은 SDAP 헤더를 끼워 넣고 데이터를 구성하고 PDCP 헤더(1i-20)를 생성하고 구성하여 집합한 후 하위 계층으로 전달하여 데이터 처리를 RLC 계층 장치와 MAC 계층 장치에서 진행할 수 있다.

[0130] 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 3 실시 예를 다음과 같이 제안한다. 상기 제 3 실시 예에서는 사용자 데이터 압축 방법을 SDAP 헤더에 적용하지 않는 것을 특징으로 하며, SDAP 헤더와 UDC 헤더를 암호화하는 것을 특징으로 하며, 상기와 같은 특징으로 인해 송신 PDCP 계층 장치에서 PDCP 헤더를 제외한 부분에 암호화를 수행하고 수신 PDCP 계층 장치에서는 PDCP 헤더를 제외한 부분에 복호화를 수행할 수 있기 때문에 구현이 용이해질 수 있다. 또한 상기에서 SDAP 헤더를 암호화 및 복호화하는 절차는 상향 링크 데이터 압축 절차(UDC)가 설정된 베어러에 대해서만 적용할 수 있다. 예를 들면 상향 링크 데이터 압축 절차(UDC)가 설정되지 않은 베어러에 대해서는 SDAP 헤더에 대해 암호화 및 복호화 절차를 수행하지 않고, 상향 링크 데이터 압축 절차(UDC)가 설정된 베어러에 대해서는 SDAP 헤더에 대해 암호화 및 복호화 절차를 수행할 수 있다.

[0131] 도 1j은 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 3 실시 예를 나타낸 도면이다.

[0132] 도 1j 에서 SDAP 계층 장치는 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 SDAP 계층

장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우 그리고 사용자 데이터 압축(Uplink data compression, UDC)을 설정한 경우, 상위 계층으로부터 데이터를 수신하면 1j-05와 같이 SDAP 헤더를 생성하고 구성하여 PDCP 계층 장치에게 전달할 수 있다. 상기 PDCP 계층 장치는 상위 SDAP 계층 장치로부터 수신한 PDCP SDU(SDAP 헤더와 IP 패킷, 1j-06)에서 SDAP 헤더를 제외한 나머지 데이터 부분에 사용자 데이터 압축 절차를 수행할 수 있다(1j-07). 그리고 체크섬 필드를 계산하고 UDC 적용 여부를 설정하여 UDC 헤더를 생성하고 SDAP 헤더 앞에 부착할 수 있다(1j-10). 그리고 무결성 보호가 설정되었다면 무결성 보호(Integrity protection)를 암호화 절차 수행 전에 상기 UDC 헤더와 압축된 UDC block 또는 PDCP 헤더에 대해 무결성 보호를 적용하고 나서 상기 UDC 헤더와 SDAP 헤더와 압축된 UDC block에 대해 암호화를 수행할 수 있다(1j-15, 1j-20). 그리고 상기 암호화된 데이터(PDCP SDU)에 대해 PDCP 헤더(1j-20)를 접합한 후 하위 계층으로 전달하여 데이터 처리를 RLC 계층 장치와 MAC 계층 장치에서 진행할 수 있다.

[0134] 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 4 실시 예를 다음과 같이 제안한다. 상기 제 4 실시 예에서는 사용자 데이터 압축 방법을 SDAP 헤더에 적용하지 않는 것을 특징으로 하며, SDAP 헤더는 암호화하지 않고, UDC 헤더를 암호화하는 것을 특징으로 하며, UDC 헤더를 SDAP 헤더 뒤에 부착하는 것 또는 UDC 헤더를 압축한 UDC 블록의 바로 앞에 부착하고 UDC 헤더 앞에 SDAP 헤더를 부착하는 것을 특징으로 할 수 있다. 상기와 같은 특징으로 인해 SDAP 헤더의 정보를 송신단 또는 수신단에서 복호화 절차 필요 없이 SDAP 헤더의 QoS 정보를 활용할 수 있다는 장점을 가진다. 예를 들면 기지국의 경우, 스케줄링에 상기 QoS 정보를 사용할 수 있고, 또한 단말 구현에서도 상위 계층 데이터를 수신할 때마다 SDAP 헤더를 생성할 필요 없이 하드웨어 가속기로 UDC 절차를 수행하고 UDC를 바로 생성하여 부착하고 암호화를 수행하고, SDAP 헤더는 나중에 붙일 수 있기 때문에 단말 구현에도 용이하다. 또한 UDC 헤더를 암호화하여 보안성을 강화할 수 있다. 또한 상기 실시 예에서 SDAP 헤더의 위치와 UDC 헤더의 위치를 바꿈으로써, 사용자 데이터 압축 절차를 수행할 때 SDAP 헤더를 제외하고 프로세싱하거나 SDAP 헤더를 떼고 프로세싱을 하고 다시 붙이는 불필요한 절차를 줄일 수 있게 되고, UDC 헤더와 UDC 데이터 블록에 대해서 하나의 일원화된 절차를 수행할 수 있다는 장점을 가질 수 있다.

[0135] 도 1k는 본 발명에서 RRC 메시지로 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 4 실시 예를 나타낸 도면이다.

[0136] 도 1k 에서 SDAP 계층 장치는 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 SDAP 계층 장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우 그리고 사용자 데이터 압축(Uplink data compression, UDC)을 설정한 경우, 상위 계층으로부터 데이터를 수신하면 1k-05와 같이 SDAP 헤더를 생성하고 구성하여 PDCP 계층 장치에게 전달할 수 있다. 상기 PDCP 계층 장치는 상위 SDAP 계층 장치로부터 수신한 PDCP SDU(SDAP 헤더와 IP 패킷, 1k-06)에서 SDAP 헤더를 제외한 나머지 데이터 부분에 사용자 데이터 압축 절차를 수행할 수 있다(1k-07). 그리고 체크섬 필드를 계산하고 UDC 적용 여부를 설정하여 UDC 헤더를 생성하고 압축된 UDC 데이터 블록 바로 앞에 (SDAP 헤더 뒤에) 부착할 수 있다(1k-10). 그리고 무결성 보호가 설정되었다면 무결성 보호(Integrity protection)를 암호화 절차 수행 전에 상기 SDAP 헤더와 UDC 헤더와 압축된 UDC block 과 PDCP 헤더에 대해 무결성 보호를 적용하고 나서 상기 UDC 헤더와 압축된 UDC block에 대해 암호화를 수행할 수 있다. 데이터를 구성하고 PDCP 헤더(1k-20)를 생성하고 구성하여 SDAP 헤더를 먼저 접합하고 PDCP 헤더를 접합한 후 하위 계층으로 전달하여 데이터 처리를 RLC 계층 장치와 MAC 계층 장치에서 진행할 수 있다.

[0138] 도 1l은 본 발명의 상기 실시 예들에서 무결성 보호 및 검증 절차가 설정된 경우, 데이터 처리 절차를 구체적으로 설명한 도면이다.

[0139] 도 1l 에서 SDAP 계층 장치는 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 SDAP 계층 장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우, 상위 계층으로부터 데이터를 수신하면 1l-05와 같이 SDAP 헤더를 생성하고 구성하여 PDCP 계층 장치에게 전달할 수 있다. 상기 PDCP 계층 장치는 상위 SDAP 계층 장치로부터 수신한 PDCP SDU(SDAP 헤더와 IP 패킷)에 대해 무결성 보호가 설정되었다면 무결성 보호(Integrity protection)를 암호화 절차 수행 전에 상기 SDAP 헤더와 PDCP 헤더와 데이터(PDCP SDU)에 대해 무결성 보호를 적용하고 구체적으로 MAC-I 필드값을 계산하고 소정의 길이를 갖는 MAC-I 필드(예를 들며 4바이트)를 구성하여 데이터의 맨 뒤에 붙일 수 있다(1l-10). 그리고 상기에서 PDCP 헤더와 SDAP 헤더를 제외한 데이터와 MAC-I 필드에 대해 암호화를 수행할 수 있다(1l-15). 그리고 PDCP 헤더를 접합한 후 하위 계층으로 전달하

여 데이터 처리를 RLC 계층 장치와 MAC 계층 장치에서 진행할 수 있다.

- [0140] 상기 도 11에서 제안한 무결성 보호 및 검증 절차는 상기 제안한 제 1 실시 예 또는 제 2 실시 예 또는 제 3 실시 예 또는 제 4 실시 예와 함께 적용될 수 있다.
- [0142] 도 1m는 본 발명의 다양한 실시 예에 따른 제안한 단말 동작을 나타낸 도면이다.
- [0143] 도 1m에서 단말은 도 1e에서 1e-10 혹은 1e-40 혹은 1e-75 와 같은 RRC 메시지에 의해서 사용자 데이터 압축 기능을 적용하는 것으로 설정될 수 있다(1m-05). 또한 상기 RRC 메시지에서 SDAP 계층 장치가 사용하도록 설정되었거나 혹은 SDAP 헤더를 사용하도록 설정된 경우에는(1m-10) 상기 본 발명에서 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 1 실시 예 또는 제 2 실시 예 또는 제 3 실시 예 또는 제 4 실시 예를 수행할 수 있다(1m-15). 하지만 상기 RRC 메시지에서 SDAP 계층 장치가 사용하도록 설정되지 않았거나 혹은 SDAP 헤더를 사용하지 않도록 설정된 경우에는(1m-10) 상기 본 발명에서 SDAP 계층 장치가 설정 또는 SDAP 헤더가 설정된 경우에 사용자 데이터 압축 방법을 효율적으로 수행하는 제 1 실시 예 또는 제 2 실시 예 또는 제 3 실시 예 또는 제 4 실시 예 또는 제 5 실시 예 또는 제 6 실시 예에서 SDAP 헤더에 대한 데이터 처리를 제외한 절차를 그대로 수행할 수 있다(1m-20).
- [0145] 상기 본 발명에서는 SDAP 헤더의 생성과 암호화 절차(ciphering)와 상향 링크 데이터 압축 절차(UDC, Uplink Data Compression)로 인해 발생할 수 있는 다양한 경우들과 그에 따른 구현 방법들을 설명하였고, 제안하였다.
- [0146] 상기에서 베어러 별 SDAP 헤더의 사용 여부는 도 1e에서 설명한 바와 같이 기지국이 RRC 메시지로 설정해줄 수 있으며, 베어러 별 UDC의 적용 여부 또한 상기처럼 기지국이 RRC 메시지로 설정해줄 수 있다.
- [0147] 본 발명의 다음에서는 기지국이 RRC 메시지로 베어러 별로 SDAP 헤더의 사용 여부와 UDC의 적용 여부를 설정해줄 때 하나의 베어러에 대해서 SDAP 헤더와 UDC를 동시에 사용할 수 없도록 하는 것을 제안한다(The SDAP header cannot be configured for a DRB configured with UDC or Both SDAP header and UDC cannot be configured for a DRB or Either SDAP header or UDC can be configured for a DRB, not both). 즉, 기지국이 RRC 메시지로 SDAP 헤더 사용과 UDC 적용을 하나의 베어러에 대해 동시에 설정하는 것을 금지할 수 있다. 상기에서 설명한 것처럼 UDC가 설정된 베어러에 대해서 UDC 절차를 수행할 때 SDAP 헤더의 생성과 비암호화로 인해 UDC 절차가 복잡해지고, 구현 복잡도가 증가한다. 상기 UDC는 상향 링크 데이터에 적용이 되는 것이며, SDAP 헤더는 상향 링크 데이터에 대해서 설정하는 경우는 베어러와 flow 간의 매핑을 설정하는 경우이다. 이런 경우가 UDC를 사용하는 경우에는 적합한 경우가 아닐 수 있다. UDC 절차에는 송신단과 수신단이 데이터 압축을 위한 동기화가 되어야 하므로 베어러와 flow들 간의 매핑을 UDC가 적용된 베어러에 수행하는 것은 매우 비효율적이기 때문이다. 따라서 상기와 같은 복잡도를 해결하기 위해서 SDAP 헤더의 사용과 UDC의 설정을 하나의 베어러에 대해 동시에 설정하지 않는다면 상기에서 설명한 복잡한 문제들이 발생하지 않게 된다. 따라서 본 발명에서 또 다른 실시 예로서 기지국이 단말에게 하나의 베어러에 대해서 SDAP 헤더의 사용과 UDC의 설정을 동시에 설정하는 것을 허용하지 않는 것을 제안한다.
- [0148] 상기에서 기지국이 단말에게 하나의 베어러에 대해서 SDAP 헤더의 사용과 UDC의 설정을 동시에 설정하지 않을 때 보안 강화를 위해서 UDC 헤더를 암호화할 수 있다. 즉, 상위 계층 데이터를 수신하면 UDC 절차로 데이터 압축을 수행하고 UDC 헤더를 생성한 후, 상기 UDC 헤더와 압축된 UDC 데이터 블록에 대해 암호화(ciphering)을 수행하고, 암호화된 UDC 헤더와 UDC 데이터 블록 앞에 PDCP 헤더를 생성해서 연결하고 하위 계층으로 전달할 수 있다.
- [0149] 또 다른 방법으로 상기에서 기지국이 단말에게 하나의 베어러에 대해서 SDAP 헤더의 사용과 UDC의 설정을 동시에 설정하지 않을 때 UDC 헤더의 체크섬 필드를 빠르게 확인하고 UDC 데이터의 폐기 여부를 빠르게 결정할 수 있도록 하여 복호화 절차의 헛수를 줄일 수 있다. 즉, UDC 헤더를 암호화하지 않을 수 있다. 즉, 상위 계층 데이터를 수신하면 UDC 절차로 데이터 압축을 수행하고 상기 압축된 데이터 블록에 대해 암호화를 수행하고, UDC 헤더와 PDCP 헤더를 생성하여 상기 암호화된 UDC 데이터 블록 앞에 연결하고 하위 계층으로 전달할 수 있다. 따라서 수신 PDCP 계층 장치는 복호화를 수행하기 전에 UDC 헤더를 확인하고 체크섬 필드로 UDC의 유효성을 확인하고 유효하지 않은 경우, 복호화를 수행하지 않고 상기 수신한 데이터를 바로 폐기할 수 있다. 상기 체크섬 필드로 유효함이 확인된 데이터에 대해서만 복호화를 수행하고 사용자 데이터 압축 해제 절차를 수행할 수 있다.

- [0150] 또한 무결성 검증 보호(Integrity protection) 절차도 마찬가지로 SDAP 헤더 사용 혹은 UDC 적용과 함께 하나의 베어러에 대해서 설정되었을 때 복잡한 구현 문제를 발생시킬 수 있다. 따라서 SDAP 헤더 사용과 무결성 검증 보호를 하나의 베어러에 동시에 설정하는 것을 허용하지 않을 수 있다. 또한 무결성 검증과 UDC 적용을 하나의 베어러에 대해 동시에 설정하는 것을 허용하지 않을 수 있다.
- [0152] 도 1n에 본 발명의 실시 예가 적용될 수 있는 단말의 구조를 도시하였다.
- [0153] 상기 도면을 참고하면, 상기 단말은 RF(Radio Frequency)처리부(1n-10), 기저대역(baseband)처리부(1n-20), 저장부(1n-30), 제어부(1n-40)를 포함한다.
- [0154] 상기 RF처리부(1n-10)는 신호의 대역 변환, 증폭 등 무선 채널을 통해 신호를 송수신하기 위한 기능을 수행한다. 즉, 상기 RF처리부(1n-10)는 상기 기저대역처리부(1n-20)로부터 제공되는 기저대역 신호를 RF 대역 신호로 상향 변환한 후 안테나를 통해 송신하고, 상기 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향 변환한다. 예를 들어, 상기 RF처리부(1n-10)는 송신 필터, 수신 필터, 증폭기, 믹서(mixer), 오실레이터(oscillator), DAC(digital to analog convertor), ADC(analog to digital convertor) 등을 포함할 수 있다. 상기 도면에서, 하나의 안테나만이 도시되었으나, 상기 단말은 다수의 안테나들을 구비할 수 있다. 또한, 상기 RF처리부(1n-10)는 다수의 RF 체인들을 포함할 수 있다. 나아가, 상기 RF처리부(1n-10)는 빔포밍(beamforming)을 수행할 수 있다. 상기 빔포밍을 위해, 상기 RF처리부(1n-10)는 다수의 안테나들 또는 안테나 요소(element)들을 통해 송수신되는 신호들 각각의 위상 및 크기를 조절할 수 있다. 또한 상기 RF 처리부는 MIMO를 수행할 수 있으며, MIMO 동작 수행 시 여러 개의 레이어를 수신할 수 있다. 상기 RF처리부(1n-10)는 제어부의 제어에 따라 다수의 안테나 또는 안테나 요소들을 적절하게 설정하여 수신 빔 스위핑을 수행하거나, 수신 빔이 송신 빔과 공조되도록 수신 빔의 방향과 빔 너비를 조정할 수 있다.
- [0155] 상기 기저대역처리부(1n-20)는 시스템의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 상기 기저대역처리부(1n-20)는 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(1n-20)는 상기 RF처리부(1n-10)로부터 제공되는 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 예를 들어, OFDM(orthogonal frequency division multiplexing) 방식에 따르는 경우, 데이터 송신 시, 상기 기저대역처리부(1n-20)는 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성하고, 상기 복소 심벌들을 부반송파들에 매핑한 후, IFFT(inverse fast Fourier transform) 연산 및 CP(cyclic prefix) 삽입을 통해 OFDM 심벌들을 구성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(1n-20)는 상기 RF처리부(1n-10)로부터 제공되는 기저대역 신호를 OFDM 심벌 단위로 분할하고, FFT(fast Fourier transform) 연산을 통해 부반송파들에 매핑된 신호들을 복원한 후, 복조 및 복호화를 통해 수신 비트열을 복원한다.
- [0156] 상기 기저대역처리부(1n-20) 및 상기 RF처리부(1n-10)는 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 상기 기저대역처리부(1n-20) 및 상기 RF처리부(1n-10)는 송신부, 수신부, 송수신부 또는 통신부로 지칭될 수 있다. 나아가, 상기 기저대역처리부(1n-20) 및 상기 RF처리부(1n-10) 중 적어도 하나는 서로 다른 다수의 무선 접속 기술들을 지원하기 위해 다수의 통신 모듈들을 포함할 수 있다. 또한, 상기 기저대역처리부(1n-20) 및 상기 RF처리부(1n-10) 중 적어도 하나는 서로 다른 주파수 대역의 신호들을 처리하기 위해 서로 다른 통신 모듈들을 포함할 수 있다. 예를 들어, 상기 서로 다른 무선 접속 기술들은 LTE 망, NR 망 등을 포함할 수 있다. 또한, 상기 서로 다른 주파수 대역들은 극고단파(SHF:super high frequency)(예: 2.5GHz, 5GHz) 대역, mm파(millimeter wave)(예: 60GHz) 대역을 포함할 수 있다.
- [0157] 상기 저장부(1n-30)는 상기 단말의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 상기 저장부(1n-30)는 상기 제어부(1n-40)의 요청에 따라 저장된 데이터를 제공한다.
- [0158] 상기 제어부(1n-40)는 상기 단말의 전반적인 동작들을 제어한다. 예를 들어, 상기 제어부(1n-40)는 상기 기저대역처리부(1n-20) 및 상기 RF처리부(1n-10)를 통해 신호를 송수신한다. 또한, 상기 제어부(1n-40)는 상기 저장부(1n-30)에 데이터를 기록하고, 읽는다. 이를 위해, 상기 제어부(1n-40)는 적어도 하나의 프로세서(processor)를 포함할 수 있다. 예를 들어, 상기 제어부(1n-40)는 통신을 위한 제어를 수행하는 CP(communication processor) 및 응용 프로그램 등 상위 계층을 제어하는 AP(application processor)를 포함할 수 있다.
- [0159] 도 1o는 본 발명의 실시 예가 적용될 수 있는 무선 통신 시스템에서 TRP(기지국)의 블록 구성을 도시한다.

- [0160] 상기 도면에 도시된 바와 같이, 상기 기지국은 RF처리부(10-10), 기저대역처리부(10-20), 백홀통신부(10-30), 저장부(10-40), 제어부(10-50)를 포함하여 구성된다.
- [0161] 상기 RF처리부(10-10)는 신호의 대역 변환, 증폭 등 무선 채널을 통해 신호를 송수신하기 위한 기능을 수행한다. 즉, 상기 RF처리부(10-10)는 상기 기저대역처리부(10-20)로부터 제공되는 기저대역 신호를 RF 대역 신호로 상향변환한 후 안테나를 통해 송신하고, 상기 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향변환한다. 예를 들어, 상기 RF처리부(10-10)는 송신 필터, 수신 필터, 증폭기, 믹서, 오실레이터, DAC, ADC 등을 포함할 수 있다. 상기 도면에서, 하나의 안테나만이 도시되었으나, 상기 제1접속 노드는 다수의 안테나들을 구비할 수 있다. 또한, 상기 RF처리부(10-10)는 다수의 RF 체인들을 포함할 수 있다. 나아가, 상기 RF처리부(10-10)는 빔포밍을 수행할 수 있다. 상기 빔포밍을 위해, 상기 RF처리부(10-10)는 다수의 안테나들 또는 안테나 요소들을 통해 송수신되는 신호들 각각의 위상 및 크기를 조절할 수 있다. 상기 RF 처리부는 하나 이상의 레이어를 전송함으로써 하향 MIMO 동작을 수행할 수 있다.
- [0162] 상기 기저대역처리부(10-20)는 제1무선 접속 기술의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 상기 기저대역처리부(10-20)은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(10-20)은 상기 RF처리부(10-10)로부터 제공되는 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 예를 들어, OFDM 방식에 따르는 경우, 데이터 송신 시, 상기 기저대역처리부(10-20)은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성하고, 상기 복소 심벌들을 부반송파들에 매핑한 후, IFFT 연산 및 CP 삽입을 통해 OFDM 심벌들을 구성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(10-20)은 상기 RF처리부(10-10)로부터 제공되는 기저대역 신호를 OFDM 심벌 단위로 분할하고, FFT 연산을 통해 부반송파들에 매핑된 신호들을 복원한 후, 복조 및 복호화를 통해 수신 비트열을 복원한다. 상기 기저대역처리부(10-20) 및 상기 RF처리부(10-10)는 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 상기 기저대역처리부(10-20) 및 상기 RF처리부(10-10)는 송신부, 수신부, 송수신부, 통신부 또는 무선 통신부로 지칭될 수 있다.
- [0163] 상기 통신부(10-30)는 네트워크 내 다른 노드들과 통신을 수행하기 위한 인터페이스를 제공한다.
- [0164] 상기 저장부(10-40)는 상기 주기지국의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 특히, 상기 저장부(10-40)는 접속된 단말에 할당된 베어러에 대한 정보, 접속된 단말로부터 보고된 측정 결과 등을 저장할 수 있다. 또한, 상기 저장부(10-40)는 단말에게 다중 연결을 제공하거나, 중단할지 여부의 판단 기준이 되는 정보를 저장할 수 있다. 그리고, 상기 저장부(10-40)는 상기 제어부(10-50)의 요청에 따라 저장된 데이터를 제공한다.
- [0165] 상기 제어부(10-50)는 상기 주기지국의 전반적인 동작들을 제어한다. 예를 들어, 상기 제어부(10-50)는 상기 기저대역처리부(10-20) 및 상기 RF처리부(10-10)을 통해 또는 상기 백홀통신부(10-30)을 통해 신호를 송수신한다. 또한, 상기 제어부(10-50)는 상기 저장부(10-40)에 데이터를 기록하고, 읽는다. 이를 위해, 상기 제어부(10-50)는 적어도 하나의 프로세서를 포함할 수 있다.
- [0167] 본 발명에서는 무선 기기간 일대일 통신 또는 일대다 통신에서 베어러 별로 무선 기기 간에 보안성을 강화할 수 있는 방법을 제안한다.
- [0168] 구체적으로 차세대 이동 통신 시스템에서 송신단(예를 들면 기지국)과 수신단(예를 들면 단말)은 데이터를 주고받을 때 데이터를 암호화하고 복호화하는 절차를 수행한다. 상기에서 데이터를 암호화하고 복호화할 때 암호화 키(또는 보안 키)를 이용하여 PDCP 계층 장치에서 암호화 및 복호화 알고리즘 또는 무결성 보호 및 검증 알고리즘을 적용한다. 상기에서 알고리즘에 적용되는 암호화 키는 단말과 기지국이 미리 설정한 암호화 키들(예를 들면 KgNB, K_{RRCenc} 등)과 데이터마다 바뀌는 암호화 키(COUNT 값)들을 포함한다. 그리고 상기에서 COUNT 값은 PDCP 일련번호와 HFN 값으로 구성되기 때문에 송신 PDCP 계층 장치와 수신 PDCP 계층 장치는 PDCP 일련번호의 동기화가 잘 이루어져야 한다. 왜냐하면 PDCP 일련번호는 0부터 시작해서 2ⁿ(PDCP 일련번호 길이) - 1 까지 증가하고 HFN 값을 1 증가시키고 다시 0으로 회귀하기 때문에 PDCP 일련번호가 한바퀴 이상 차이가 나게 되면 송신 PDCP 계층 장치에서 데이터에 대해서 암호화 또는 무결성 보호할 때 사용한 COUNT 값과 수신 PDCP 계층 장치에서 데이터를 복호화 또는 무결성 검증할 때 사용하는 COUNT 값이 다를 수 있고, 이런 경우, 복호화 실패 또는 무결성 검증 실패가 일어나고 HFN 비동기(HFN desynchronization) 문제가 발생하게 된다.
- [0169] 상기와 같은 복호화 실패 또는 무결성 검증 실패와 HFN 비동기 문제는 데이터의 대량 유실 또는 해커에 의한 의

도되지 않은 데이터들의 수신 때문에 발생할 수 있다. 따라서 송신단과 수신단은 필요한 경우, 예를 들면 복호화 실패 또는 무결성 검증 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 송신 PDCP 계층 장치와 수신 PDCP 계층 장치의 COUNT 값이 동기가 잘 맞춰져 있는 지 또는 보안키가 동일한지 확인해야 할 필요가 있다.

[0170] 따라서 본 발명에서는 베어러 별로 송신 PDCP 계층 장치와 수신 PDCP 계층 장치의 COUNT 값이 동기가 잘 맞춰져 있는 지 또는 보안 식별자 또는 보안키값 등이 동일한지를 확인할 수 있는 방법들을 제안한다.

[0172] 도 2a는 본 발명이 적용될 수 있는 LTE 시스템의 구조를 도시하는 도면이다.

[0173] 도 2a를 참조하면, 도시한 바와 같이 LTE 시스템의 무선 액세스 네트워크는 차세대 기지국(Evolved Node B, 이하 ENB, Node B 또는 기지국)(2a-05, 2a-10, 2a-15, 2a-20)과 MME (2a-25, Mobility Management Entity) 및 S-GW(2a-30, Serving-Gateway)로 구성된다. 사용자 단말(User Equipment, 이하 UE 또는 단말)(2a-35)은 ENB(2a-05 ~ 2a-20) 및 S-GW(2a-30)를 통해 외부 네트워크에 접속한다.

[0174] 도 2a에서 ENB(2a-05 ~ 2a-20)는 UMTS 시스템의 기존 노드 B에 대응된다. ENB는 UE(2a-35)와 무선 채널로 연결되며 기존 노드 B 보다 복잡한 역할을 수행한다. LTE 시스템에서는 인터넷 프로토콜을 통한 VoIP(Voice over IP)와 같은 실시간 서비스를 비롯한 모든 사용자 트래픽이 공용 채널(shared channel)을 통해 서비스 되므로, UE들의 버퍼 상태, 가용 전송 전력 상태, 채널 상태 등의 상태 정보를 취합해서 스케줄링을 하는 장치가 필요하며, 이를 ENB(2a-05 ~ 2a-20)가 담당한다. 하나의 ENB는 통상 다수의 셀들을 제어한다. 예컨대, 100 Mbps의 전송 속도를 구현하기 위해서 LTE 시스템은 예컨대, 20 MHz 대역폭에서 직교 주파수 분할 다중 방식(Orthogonal Frequency Division Multiplexing, 이하 OFDM이라 한다)을 무선 접속 기술로 사용한다. 또한 단말의 채널 상태에 맞춰 변조 방식(modulation scheme)과 채널 코딩률(channel coding rate)을 결정하는 적응 변조 코딩(Adaptive Modulation & Coding, 이하 AMC라 한다) 방식을 적용한다. S-GW(2a-30)는 데이터 베어러를 제공하는 장치이며, MME(2a-25)의 제어에 따라서 데이터 베어러를 생성하거나 제거한다. MME는 단말에 대한 이동성 관리 기능은 물론 각종 제어 기능을 담당하는 장치로 다수의 기지국 들과 연결된다.

[0175] 도 2b는 본 발명이 적용될 수 있는 LTE 시스템에서 무선 프로토콜 구조를 나타낸 도면이다.

[0176] 도 2b를 참조하면, LTE 시스템의 무선 프로토콜은 단말과 ENB에서 각각 PDCP (Packet Data Convergence Protocol 2b-05, 2b-40), RLC (Radio Link Control 2b-10, 2b-35), MAC (Medium Access Control 2b-15, 2b-30)으로 이루어진다. PDCP (Packet Data Convergence Protocol)(2b-05, 2b-40)는 IP 헤더 압축/복원 등의 동작을 담당한다. PDCP의 주요 기능은 하기와 같이 요약된다.

[0177] - 헤더 압축 및 압축 해제 기능(Header compression and decompression: ROHC only)

[0178] - 사용자 데이터 전송 기능 (Transfer of user data)

[0179] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs at PDCP re-establishment procedure for RLC AM)

[0180] - 순서 재정렬 기능(For split bearers in DC (only support for RLC AM): PDCP PDU routing for transmission and PDCP PDU reordering for reception)

[0181] - 중복 탐지 기능(Duplicate detection of lower layer SDUs at PDCP re-establishment procedure for RLC AM)

[0182] - 재전송 기능(Retransmission of PDCP SDUs at handover and, for split bearers in DC, of PDCP PDUs at PDCP data-recovery procedure, for RLC AM)

[0183] - 암호화 및 복호화 기능(Ciphering and deciphering)

[0184] - 타이머 기반 SDU 삭제 기능(Timer-based SDU discard in uplink.)

[0186] 무선 링크 제어(Radio Link Control, 이하 RLC라고 한다)(2b-10, 2b-35)는 PDCP PDU(Packet Data Unit)를 적절한 크기로 재구성해서 ARQ 동작 등을 수행한다. RLC의 주요 기능은 하기와 같이 요약된다.

- [0187] - 데이터 전송 기능(Transfer of upper layer PDUs)
- [0188] - ARQ 기능(Error Correction through ARQ (only for AM data transfer))
- [0189] - 접합, 분할, 재조립 기능(Concatenation, segmentation and reassembly of RLC SDUs (only for UM and AM data transfer))
- [0190] - 재분할 기능(Re-segmentation of RLC data PDUs (only for AM data transfer))
- [0191] - 순서 재정렬 기능(Reordering of RLC data PDUs (only for UM and AM data transfer))
- [0192] - 중복 탐지 기능(Duplicate detection (only for UM and AM data transfer))
- [0193] - 오류 탐지 기능(Protocol error detection (only for AM data transfer))
- [0194] - RLC SDU 삭제 기능(RLC SDU discard (only for UM and AM data transfer))
- [0195] - RLC 재수립 기능(RLC re-establishment)

- [0197] MAC(2b-15, 2b-30)은 한 단말에 구성된 여러 RLC 계층 장치들과 연결되며, RLC PDU들을 MAC PDU에 다중화하고 MAC PDU로부터 RLC PDU들을 역다중화하는 동작을 수행한다. MAC의 주요 기능은 하기와 같이 요약된다.
- [0198] - 맵핑 기능(Mapping between logical channels and transport channels)
- [0199] - 다중화 및 역다중화 기능(Multiplexing/demultiplexing of MAC SDUs belonging to one or different logical channels into/from transport blocks (TB) delivered to/from the physical layer on transport channels)
- [0200] - 스케줄링 정보 보고 기능(Scheduling information reporting)
- [0201] - HARQ 기능(Error correction through HARQ)
- [0202] - 로지컬 채널 간 우선 순위 조절 기능(Priority handling between logical channels of one UE)
- [0203] - 단말간 우선 순위 조절 기능(Priority handling between UEs by means of dynamic scheduling)
- [0204] - MBMS 서비스 확인 기능(MBMS service identification)
- [0205] - 전송 포맷 선택 기능(Transport format selection)
- [0206] - 패딩 기능(Padding)
- [0207] 물리 계층(2b-20, 2b-25)은 상위 계층 데이터를 채널 코딩 및 변조하고, OFDM 심벌로 만들어서 무선 채널로 전송하거나, 무선 채널을 통해 수신한 OFDM 심벌을 복조하고 채널 디코딩해서 상위 계층으로 전달하는 동작을 한다.
- [0208] 도 2c는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 구조를 도시하는 도면이다.
- [0209] 도 2c를 참조하면, 도시한 바와 같이 차세대 이동통신 시스템(이하 NR 혹은 5g)의 무선 액세스 네트워크는 차세대 기지국(New Radio Node B, 이하 NR gNB 혹은 NR 기지국)(2c-10)과 NR CN (2c-05, New Radio Core Network)로 구성된다. 사용자 단말(New Radio User Equipment, 이하 NR UE 또는 단말)(2c-15)은 NR gNB(2c-10) 및 NR CN (2c-05)를 통해 외부 네트워크에 접속한다.
- [0210] 도 2c에서 NR gNB(2c-10)는 기존 LTE 시스템의 eNB (Evolved Node B)에 대응된다. NR gNB는 NR UE(2c-15)와 무선 채널로 연결되며 기존 노드 B 보다 더 월등한 서비스를 제공할 수 있다. 차세대 이동통신 시스템에서는 모든 사용자 트래픽이 공용 채널(shared channel)을 통해 서비스 되므로, UE들의 버퍼 상태, 가용 전송 전력 상태, 채널 상태 등의 상태 정보를 취합해서 스케줄링을 하는 장치가 필요하며, 이를 NR NB(2c-10)가 담당한다. 하나의 NR gNB는 통상 다수의 셀들을 제어한다. 현재 LTE 대비 초고속 데이터 전송을 구현하기 위해서 기존 최대 대역폭 이상을 가질 수 있고, 직교 주파수 분할 다중 방식(Orthogonal Frequency Division Multiplexing, 이하 OFDM이라 한다)을 무선 접속 기술로 하여 추가적으로 빔포밍 기술이 적용될 수 있다. 또한 단말의 채널 상태에 맞춰 변조 방식(modulation scheme)과 채널 코딩률(channel coding rate)을 결정하는 적응 변조 코딩(Adaptive Modulation & Coding, 이하 AMC라 한다) 방식을 적용한다. NR CN (2c-05)는 이동성 지원, 베어러 설

정, QoS 설정 등의 기능을 수행한다. NR CN는 단말에 대한 이동성 관리 기능은 물론 각종 제어 기능을 담당하는 장치로 다수의 기지국들과 연결된다. 또한 차세대 이동통신 시스템은 기존 LTE 시스템과도 연동될 수 있으며, NR CN이 MME (2c-25)와 네트워크 인터페이스를 통해 연결된다. MME는 기존 기지국인 eNB (2c-30)과 연결된다.

- [0211] 도 2d는 본 발명이 적용될 수 있는 차세대 이동통신 시스템의 무선 프로토콜 구조를 나타낸 도면이다. .
- [0212] 도 2d를 참조하면, 차세대 이동통신 시스템의 무선 프로토콜은 단말과 NR 기지국에서 각각 NR SDAP(2d-01, 2d-45), NR PDCP(2d-05, 2d-40), NR RLC(2d-10, 2d-35), NR MAC(2d-15, 2d-30)으로 이루어진다.
- [0213] NR SDAP(2d-01, 2d-45)의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0214] - 사용자 데이터의 전달 기능(transfer of user plane data)
- [0215] - 상향 링크와 하향 링크에 대해서 QoS flow와 데이터 베어러의 맵핑 기능(mapping between a QoS flow and a DRB for both DL and UL)
- [0216] - 상향 링크와 하향 링크에 대해서 QoS flow ID를 마킹 기능(marking QoS flow ID in both DL and UL packets)
- [0217] - 상향 링크 SDAP PDU들에 대해서 reflective QoS flow를 데이터 베어러에 맵핑시키는 기능 (reflective QoS flow to DRB mapping for the UL SDAP PDUs).
- [0218] 상기 SDAP 계층 장치에 대해 단말은 RRC 메시지로 각 PDCP 계층 장치 별로 혹은 베어러 별로 혹은 로지컬 채널 별로 SDAP 계층 장치의 헤더를 사용할 지 여부 혹은 SDAP 계층 장치의 기능을 사용할 지 여부를 설정 받을 수 있으며, SDAP 헤더가 설정된 경우, SDAP 헤더의 NAS QoS 반영 설정 1비트 지시자(NAS reflective QoS)와 AS QoS 반영 설정 1비트 지시자(AS reflective QoS)로 단말이 상향 링크와 하향 링크의 QoS flow와 데이터 베어러에 대한 맵핑 정보를 갱신 혹은 재설정할 수 있도록 지시할 수 있다. 상기 SDAP 헤더는 QoS를 나타내는 QoS flow ID 정보를 포함할 수 있다. 상기 QoS 정보는 원할한 서비스를 지원하기 위한 데이터 처리 우선 순위, 스케줄링 정보 등으로 사용될 수 있다.
- [0220] NR PDCP (2d-05, 2d-40)의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0221] 헤더 압축 및 압축 해제 기능(Header compression and decompression: ROHC only)
- [0222] - 사용자 데이터 전송 기능 (Transfer of user data)
- [0223] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs)
- [0224] - 비순차적 전달 기능 (Out-of-sequence delivery of upper layer PDUs)
- [0225] - 순서 재정렬 기능(PDCP PDU reordering for reception)
- [0226] - 중복 탐지 기능(Duplicate detection of lower layer SDUs)
- [0227] - 재전송 기능(Retransmission of PDCP SDUs)
- [0228] - 암호화 및 복호화 기능(Ciphering and deciphering)
- [0229] - 타이머 기반 SDU 삭제 기능(Timer-based SDU discard in uplink.)
- [0230] 상기에서 NR PDCP 장치의 순서 재정렬 기능(reordering)은 하위 계층에서 수신한 PDCP PDU들을 PDCP SN(sequence number)을 기반으로 순서대로 재정렬하는 기능을 말하며, 재정렬된 순서대로 데이터를 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 순서를 고려하지 않고, 바로 전달하는 기능을 포함할 수 있으며, 순서를 재정렬하여 유실된 PDCP PDU들을 기록하는 기능을 포함할 수 있으며, 유실된 PDCP PDU들에 대한 상태 보고를 송신 측에 하는 기능을 포함할 수 있으며, 유실된 PDCP PDU들에 대한 재전송을 요청하는 기능을 포함할 수 있다.
- [0232] NR RLC(2d-10, 2d-35)의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0233] - 데이터 전송 기능(Transfer of upper layer PDUs)

- [0234] - 순차적 전달 기능(In-sequence delivery of upper layer PDUs)
- [0235] - 비순차적 전달 기능(Out-of-sequence delivery of upper layer PDUs)
- [0236] - ARQ 기능(Error Correction through ARQ)
- [0237] - 접합, 분할, 재조립 기능(Concatenation, segmentation and reassembly of RLC SDUs)
- [0238] - 재분할 기능(Re-segmentation of RLC data PDUs)
- [0239] - 순서 재정렬 기능(Reordering of RLC data PDUs)
- [0240] - 중복 탐지 기능(Duplicate detection)
- [0241] - 오류 탐지 기능(Protocol error detection)
- [0242] - RLC SDU 삭제 기능(RLC SDU discard)
- [0243] - RLC 재수립 기능(RLC re-establishment)
- [0244] 상기에서 NR RLC 장치의 순차적 전달 기능(In-sequence delivery)은 하위 계층으로부터 수신한 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 말하며, 원래 하나의 RLC SDU가 여러 개의 RLC SDU들로 분할되어 수신된 경우, 이를 재조립하여 전달하는 기능을 포함할 수 있으며, 수신한 RLC PDU들을 RLC SN(sequence number) 혹은 PDCP SN(sequence number)를 기준으로 재정렬하는 기능을 포함할 수 있으며, 순서를 재정렬하여 유실된 RLC PDU들을 기록하는 기능을 포함할 수 있으며, 유실된 RLC PDU들에 대한 상태 보고를 송신 측에 하는 기능을 포함할 수 있으며, 유실된 RLC PDU들에 대한 재전송을 요청하는 기능을 포함할 수 있으며, 유실된 RLC SDU가 있을 경우, 유실된 RLC SDU 이전까지의 RLC SDU들만을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 유실된 RLC SDU가 있어도 소정의 타이머가 만료되었다면 타이머가 시작되기 전에 수신된 모든 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있으며, 혹은 유실된 RLC SDU가 있어도 소정의 타이머가 만료되었다면 현재까지 수신된 모든 RLC SDU들을 순서대로 상위 계층에 전달하는 기능을 포함할 수 있다. 또한 상기에서 RLC PDU들을 수신하는 순서대로 (일련번호, Sequence number의 순서와 상관없이, 도착하는 순으로) 처리하여 PDCP 장치로 순서와 상관없이(Out-of sequence delivery) 전달할 수도 있으며, segment 인 경우에는 버퍼에 저장되어 있거나 추후에 수신될 segment들을 수신하여 온전한 하나의 RLC PDU로 재구성한 후, 처리하여 PDCP 장치로 전달할 수 있다. 상기 NR RLC 계층은 접합(Concatenation) 기능을 포함하지 않을 수 있고 상기 기능을 NR MAC 계층에서 수행하거나 NR MAC 계층의 다중화(multiplexing) 기능으로 대체할 수 있다.
- [0246] 상기에서 NR RLC 장치의 비순차적 전달 기능(Out-of-sequence delivery)은 하위 계층으로부터 수신한 RLC SDU들을 순서와 상관없이 바로 상위 계층으로 전달하는 기능을 말하며, 원래 하나의 RLC SDU가 여러 개의 RLC SDU들로 분할되어 수신된 경우, 이를 재조립하여 전달하는 기능을 포함할 수 있으며, 수신한 RLC PDU들의 RLC SN 혹은 PDCP SN을 저장하고 순서를 정렬하여 유실된 RLC PDU들을 기록해두는 기능을 포함할 수 있다.
- [0248] NR MAC(2d-15, 2d-30)은 한 단말에 구성된 여러 NR RLC 계층 장치들과 연결될 수 있으며, NR MAC의 주요 기능은 다음의 기능들 중 일부를 포함할 수 있다.
- [0249] - 맵핑 기능(Mapping between logical channels and transport channels)
- [0250] - 다중화 및 역다중화 기능(Multiplexing/demultiplexing of MAC SDUs)
- [0251] - 스케줄링 정보 보고 기능(Scheduling information reporting)
- [0252] - HARQ 기능(Error correction through HARQ)
- [0253] - 로지컬 채널 간 우선 순위 조절 기능(Priority handling between logical channels of one UE)
- [0254] - 단말간 우선 순위 조절 기능(Priority handling between UEs by means of dynamic scheduling)
- [0255] - MBMS 서비스 확인 기능(MBMS service identification)
- [0256] - 전송 포맷 선택 기능(Transport format selection)

- [0257] - 패딩 기능(Padding)
- [0258] NR PHY 계층(2d-20, 2d-25)은 상위 계층 데이터를 채널 코딩 및 변조하고, OFDM 심벌로 만들어서 무선 채널로 전송하거나, 무선 채널을 통해 수신한 OFDM 심벌을 복조하고 채널 디코딩해서 상위 계층으로 전달하는 동작을 수행할 수 있다.
- [0260] 도 2e는 본 발명에서 기지국이 단말의 연결을 해제하여 단말이 RRC 연결 모드(RRC connected mode)에서 RRC 유휴 모드(RRC idle mode)로 전환하는 절차와 단말이 기지국과 연결을 설정하여 RRC 유휴 모드(RRC idle mode)에서 RRC 연결 모드(RRC connected mode)로 전환하는 절차를 설명한 도면이다.
- [0261] 도 2e에서 기지국은 RRC 연결 모드에서 데이터를 송수신하는 단말이 소정의 이유로 혹은 일정 시간 동안 데이터의 송수신이 없으면 RRCConnectionRelease 메시지를 단말에게 보내어 단말을 RRC 유휴모드로 전환하도록 할 수 있다(2e-01). 추후에 현재 연결이 설정되어 있지 않은 단말(이하 idle mode UE)은 전송할 데이터가 발생하면 기지국과 RRC connection establishment 과정을 수행한다. 단말은 랜덤 액세스 과정을 통해서 기지국과 역방향 전송 동기를 수립하고 RRCConnectionRequest 메시지를 기지국으로 전송한다 (2e-05). 상기 메시지에는 단말의 식별자와 연결을 설정하고자 하는 이유(establishmentCause) 등이 수납된다. 기지국은 단말이 RRC 연결을 설정하도록 RRCConnectionSetup 메시지를 전송한다 (2e-10).
- [0262] 상기 RRCConnectionSetup 메시지에는 RRC 연결 구성 정보 등이 수납된다. 또한 상기 RRC Connection Setup 메시지는 접속한 단말에게 기지국 내에서 구별할 수 있는 단말 식별자를 할당해줄 수 있다. 또한 현재 기지국에 접속한 다른 단말 식별자들의 리스트를 보내줄 수도 있다. 상기에서 현재 기지국에 접속한 다른 단말 식별자들의 리스트는 주기적으로 업데이트될 수 있으며, 기지국이 지원하는 커버리지에 있는 단말들이 통신이 가능한 단말들의 식별자를 확인하기 위해 기지국이 시스템 정보에서 방송할 수도 있다. 또는 공장에서 무선 기기들을 설치할 때 무선 기기가 통신 가능한 다른 무선 기기들의 식별자들을 미리 설정해놓을 수도 있다. 상기에서 단말 식별자는 C-RNTI를 사용할 수도 있으며, C-RNTI의 일부를 사용할 수도 있으며, NAS 계층에서 할당해주는 고유 식별자(예를 들면 GUTI)의 일부를 사용할 수도 있다. 또한 상기 메시지에는 송신단과 수신단 사이에서 베어러 별로 PDCP 계층 장치에서 보안키(예를 들면 COUNT 값 또는 보안 식별자 또는 보안키값)들을 확인할 수 있는 기능이 설정되었는지 유무를 지시하는 지시자를 포함할 수 있다.
- [0263] RRC 연결은 SRB (Signaling Radio Bearer)라고도 하며, 단말과 기지국 사이의 제어 메시지인 RRC 메시지 송수신에 사용된다. RRC 연결을 설정한 단말은 RRCConnctionSetupComplete 메시지를 기지국으로 전송한다 (2e-15). 상기 메시지에는 단말이 소정의 서비스를 위한 베어러 설정을 MME에게 요청하는 SERVICE REQUEST라는 제어 메시지가 포함되어 있다. 기지국은 RRCConnctionSetupComplete 메시지에 수납된 SERVICE REQUEST 메시지를 MME로 전송하고 (2e-20), MME는 단말이 요청한 서비스를 제공할지 여부를 판단한다. 판단 결과 단말이 요청한 서비스를 제공하기로 결정하였다면 MME는 기지국에게 INITIAL CONTEXT SETUP REQUEST라는 메시지를 전송한다(2e-25). 상기 메시지에는 DRB (Data Radio Bearer) 설정 시 적용할 QoS (Quality of Service) 정보, 그리고 DRB에 적용할 보안 관련 정보 (예를 들어 Security Key, Security Algorithm) 등의 정보가 포함된다. 기지국은 단말과 보안을 설정하기 위해서 SecurityModeCommand 메시지(2e-30)와 SecurityModeComplete 메시지(2e-35)를 교환한다. 보안 설정이 완료되면 기지국은 단말에게 RRCConnectionReconfiguration 메시지를 전송한다(2e-40).
- [0264] 또한 상기 RRCConnectionReconfiguration 메시지에는 접속한 단말에게 기지국 내에서 구별할 수 있는 단말 식별자를 할당해줄 수 있다. 또한 현재 기지국에 접속한 다른 단말 식별자들의 리스트를 보내줄 수도 있다. 상기에서 현재 기지국에 접속한 다른 단말 식별자들의 리스트는 주기적으로 업데이트될 수 있으며, 기지국이 지원하는 커버리지에 있는 단말들이 통신이 가능한 단말들의 식별자를 확인하기 위해 기지국이 시스템 정보에서 방송할 수도 있다. 또는 공장에서 무선 기기들을 설치할 때 무선 기기가 통신 가능한 다른 무선 기기들의 식별자들을 미리 설정해놓을 수도 있다. 상기에서 단말 식별자는 C-RNTI를 사용할 수도 있으며, C-RNTI의 일부를 사용할 수도 있으며, NAS 계층에서 할당해주는 고유 식별자(예를 들면 GUTI)의 일부를 사용할 수도 있다. 또한 상기 메시지는 송신단과 수신단 사이에서 베어러 별로 PDCP 계층 장치에서 보안키(예를 들면 COUNT 값 또는 보안 식별자 또는 보안키값)들을 확인할 수 있는 기능이 설정되었는지 유무를 지시하는 지시자를 포함할 수 있다.
- [0265] 상기 메시지에는 사용자 데이터가 처리될 DRB의 설정 정보가 포함되며, 단말은 상기 정보를 적용해서 DRB를 설정하고 기지국에게 RRCConnectionReconfigurationComplete 메시지를 전송한다(2e-45). 단말과 DRB 설정을 완료한 기지국은 MME에게 INITIAL CONTEXT SETUP COMPLETE 메시지를 전송하고 (2e-50), 이를 수신한 MME는 S-GW와

S1 베어러를 설정하기 위해서 S1 BEARER SETUP 메시지와 S1 BEARER SETUP RESPONSE 메시지를 교환한다(2e-055, 2e-60). S1 베어러는 S-GW와 기지국 사이에 설정되는 데이터 전송용 연결이며 DRB와 1대 1로 대응된다. 상기 과정이 모두 완료되면 단말은 기지국과 S-GW를 통해 데이터를 송수신한다(2e-65, 2e-70). 이처럼 일반적인 데이터 전송 과정은 크게 RRC 연결 설정, 보안 설정, DRB설정의 3단계로 구성된다. 또한 기지국은 소정의 이유로 단말에게 설정을 새로 해주거나 추가하거나 변경하기 위해서 RRCConnectionReconfiguration 메시지를 전송할 수 있다(2e-75).

- [0267] 본 발명의 다음에서는 무선 기기들 간의 데이터 전송을 수행할 때에 낮은 전송 지연을 가질 수 있도록 하는 일대일 무선 연결 설정 또는 일대다 무선 연결 설정 절차를 제안한다.
- [0269] 도 2f는 본 발명의 다양한 실시 예에 따른 무선 기기 간 일대일 무선 링크를 설정하고 데이터 송수신을 가능하도록 하는 절차를 나타낸다. 상기에서 일대일 무선 링크는 무선 기기 간에 데이터를 송수신할 때 기지국을 통하지 않고, 직접 데이터를 송수신하는 것을 의미한다.
- [0270] 본 발명에서 제안하는 무선 기기 간 일대일 무선 링크(Point to Point communication)를 설정하는 절차는 크게 무선 기기들을 찾는 단계, 무선 기기간 일대일 무선 링크 또는 직접 무선 링크를 평가 및 측정하는 단계, 무선 기기간 직접 무선 링크를 설립하는 단계, 무선 기기간 직접 링크를 통해 데이터를 전송하는 단계로 구분될 수 있으며, 다음과 같은 특징들 중에 하나 혹은 복수 개의 특징을 가질 수 있다.
- [0271] 1. 기지국이 무선 데이터 송수신을 지원하는 커버리지 내의 무선 기기 간의 단말 식별자들을 공유하고, 관리할 수 있다는 것을 특징으로 한다.
- [0272] 2. 기지국이 무선 데이터 송수신을 지원하는 커버리지 내의 무선 기기들은 항상 RRC 연결 모드 또는 RRC 비활성화 모드에 있도록 설정할 수 있다는 것을 특징으로 한다.
- [0273] 3. 무선 기기가 기지국에게 일대일 통신을 위한 전송 자원 할당을 요청할 때 목적지에 해당하는 무선 기기의 식별자 또는 소스에 해당하는 무선 기기의 식별자를 포함하여 보내며, 상기 전송 자원할당을 요청한다는 것을 특징으로 한다.
- [0274] 4. 기지국은 무선 기기로부터 일대일 통신을 위한 전송 자원 할당을 요청 받으면 목적지 무선 기기의 식별자를 이용하여 목적지 무선 기기를 찾기 위한 절차(예를 들면 페이징 메시지 전송)를 수행하는 것을 특징으로 한다. 만약 목적지 무선 기기를 찾을 수 없다면 또는 기지국의 커버리지에 없다면 소스 무선 기기에게 상향 링크 전송 자원을 할당하고, 기지국이 중간에서 데이터를 전달해주는 것을 특징으로 한다.
- [0275] 5. 기지국은 일대일 통신을 위해 전송 자원을 단말의 일반적인 상향 링크 전송 자원에서 일부를 할당할 수 있다는 것을 특징으로 한다.
- [0276] 6. 기지국은 일대일 통신을 위한 전송 자원을 무선 기기들에게 할당해줄 때 소스 무선 기기의 식별자 또는 목적지 무선 기기의 식별자를 지시해주며, 일대일 무선 링크에 대한 주파수 설정 정보를 설정해주고 주파수 측정을 지시하며 또는 레퍼런스 신호를 송신하도록 하는 것을 설정 및 지시해주는 것을 특징으로 한다.
- [0277] 7. 일대일 통신을 위한 전송 자원을 할당 받은 무선 기기들이 일대일 통신을 위한 일대일 무선 링크에 대한 주파수 측정을 수행하고, 주파수 측정 결과를 기지국에게 보고하는 것을 특징으로 한다.
- [0278] 8. 기지국은 소스 무선 기기와 목적지 무선 기기로부터 주파수 측정 결과를 수신하고, 주파수 측정 결과에 따라 소스 무선 기기에게 새로 정의한 L1 신호(예를 들면 DCI) 또는 L2 신호(예를 들면 MAC CE)를 이용하여 데이터 전송을 지시할 수 있으며, 주파수 측정 결과에 따라 목적지 무선 기기에게 새로 정의한 L1 신호(예를 들면 DCI) 또는 L2 신호(예를 들면 MAC CE)를 이용하여 데이터 전송을 지시할 수 있다는 것을 특징으로 한다.
- [0279] 9. 무선 기기는 기지국으로부터 새로 정의한 L1 신호(예를 들면 DCI) 또는 L2 신호(예를 들면 MAC CE)를 통하여 데이터 전송이 지시되면 데이터 전송을 시작하는 것을 특징으로 한다.
- [0281] 본 발명에서 제안하는 무선 기기 간 일대일 무선 링크(Point to Point communication)를 설정하는 구체적인 절차는 다음과 같다.

- [0282] 기지국(2f-03)은 무선 데이터 송수신을 지원하는 커버리지 내의 무선 기기 간의 단말 식별자들을 공유하고, 관리할 수 있다. 그리고 낮은 전송 지연을 유지할 수 있도록 기지국은 무선 데이터 송수신을 지원하는 커버리지 내의 무선 기기들(2f-01 또는 2f-02)을 항상 RRC 연결 모드 또는 RRC 비활성화 모드에 있도록 설정할 수 있다.
- [0283] 만약 무선 기기(2f-01)가 기지국에게 일대일 통신을 위한 전송 자원 할당을 요청할 때 목적지에 해당하는 무선 기기의 식별자 또는 소스에 해당하는 무선 기기의 식별자를 포함하여 보내며, 상기 전송 자원할당을 요청하는 메시지를 전송할 수 있다(2f-05). 상기에서 일대일 통신을 위한 전송 자원을 요청하는 메시지에는 QoS 요구사항이 포함될 수 있다. 예를 들면 평균 패킷 크기(average packet size), 전송 비트율(bit rate), 전송 지연 요구사항(delay requirement), 신뢰도, 에러율 등을 포함하여 기지국에게 요청할 수 있다.
- [0284] 기지국은 무선 기기로부터 일대일 통신을 위한 전송 자원 할당을 요청 받으면 목적지 무선 기기(2f-02)의 식별자를 이용하여 목적지 무선 기기를 찾기 위한 절차(예를 들면 페이징 메시지 전송)를 수행할 수 있다(2f-10). 만약 목적지 무선 기기를 찾을 수 없다면 또는 기지국의 커버리지에 없다면 소스 무선 기기에게 상향 링크 전송 자원을 할당하고, 기지국이 소스 무선 기기의 데이터를 수신하고 네트워크에 전달하여 중간에서 데이터를 전달해줄 수 있다. 상기 페이징 메시지에는 소스 무선 기기의 식별자 또는 목적지 무선 기기의 식별자를 포함할 수 있다.
- [0285] 상기에서 페이징 메시지를 수신한 목적지 무선기기는 기지국으로 연결을 설정한다(2f-15). 그러면 기지국은 일대일 통신을 위해 전송 자원을 일대일 요청 응답 메시지를 소스 무선기기에게 보내고, 일대일 설정 메시지를 목적지 무선 기기에게 보내어 할당해줄 수 있다(2f-20, 2f-25). 상기에서 기지국은 일대일 통신을 위해 전송 자원을 단말의 일반적인 상향 링크 전송 자원에서 일부를 할당할 수 있다. 또한 상기에서 할당되는 전송 자원을 일정한 주기를 갖고 계속적으로 반복적으로 할당되는 전송 자원일 수 있다. 따라서 한번 설정되면 기지국의 추가 개입 없이 상기 전송 자원을 이용하여 일대일 통신을 무선 기기간에 계속 수행할 수 있다. 또한 상기 전송 자원은 기지국이 개별적으로 할당해주는 것이 아니라 시스템 정보에서 방송될 수 있으며, 기지국은 시스템 정보에서 방송되는 자원 중에 어떤 자원을 사용하라는 것을 지시해줄 수 있다. 만약 무선 기기에게 시스템 정보에서 방송되는 전송 자원과 기지국이 개별적으로 할당해준 전송 자원이 둘다 주어지면 기지국이 개별적으로 할당해준 전송 자원을 우선시할 수 있다. 또한 상기에서 기지국은 일대일 통신을 위한 전송 자원을 무선 기기들에게 할당해줄 때 소스 무선 기기의 식별자 또는 목적지 무선 기기의 식별자를 지시해주며, 일대일 무선 링크에 대한 주파수 설정 정보를 설정해주고 주파수 측정을 지시하며 또는 레퍼런스 신호를 송신하도록 하는 것을 설정 및 지시해줄 수 있다.
- [0286] 또한 상기에서 일대일 통신을 위한 전송 자원은 시간 자원, 주파수 자원, 코드 자원, 소스 무선 기기 식별자 또는 목적지 무선 기기 식별자, 변조 또는 복조 코딩 정보(MCS), 전송 블록 크기(TB size), 상기 무선 정보를 활성화할 식별자(예를 들면 RNTI) 등의 정보를 포함할 수 있다.
- [0287] 일대일 통신을 위한 전송 자원을 할당 받은 소스 무선 기기와 목적지 무선 기기들은 상기 전송 자원으로 레퍼런스 신호를 송신하며 상호 간의 일대일 통신을 위한 일대일 무선 링크에 대한 주파수 측정을 수행하고(2f-30), 주파수 측정 결과를 기지국에게 보고할 수 있다(2f-35, 2f-40).
- [0288] 상기에서 기지국은 소스 무선 기기와 목적지 무선 기기로부터 주파수 측정 결과를 수신하면, 주파수 측정 결과에 따라 소스 무선 기기에게 새로 정의한 L1 신호(예를 들면 식별자를 이용한 DCI) 또는 L2 신호(예를 들면 MAC CE)를 이용하여 데이터 전송을 지시할 수 있으며(2f-45), 주파수 측정 결과에 따라 목적지 무선 기기에게 새로 정의한 L1 신호(예를 들면 DCI) 또는 L2 신호(예를 들면 MAC CE)를 이용하여 데이터 전송을 지시할 수 있다(2f-50).
- [0289] 소스 무선 기기 또는 목적지 무선 기기는 기지국으로부터 새로 정의한 L1 신호(예를 들면 식별자를 이용한 DCI) 또는 L2 신호(예를 들면 MAC CE)를 통하여 데이터 전송이 지시되면 일대일 통신을 위한 전송 자원을 이용하여 데이터 전송을 시작할 수 있다(2f-55).
- [0291] 상기 절차에서 소스 무선 기기와 목적지 무선 기기는 송수신되는 데이터들의 신뢰도를 측정하거나 또는 직접 무선 링크의 레퍼런스 신호로 주파수를 주기적으로 측정하여 상기에서 설정된 일대일 무선 링크의 정해진 또는 설정된 일정 수준 이하가 되면 기지국에게 일대일 무선 링크를 업데이트해달라고 요청하거나 다시 2f-05 처럼 새롭게 일대일 무선 링크를 요청할 수 있다. 상기에서 소스 무선 기기와 목적지 무선 기기는 송수신되는 데이터들의 신뢰도를 측정할 때 데이터들의 일련번호를 확인하여 유실된 데이터들의 개수 또는 크기 또는 양을 확인하여

직접 무선 링크의 질을 평가할 수도 있다.

- [0292] 상기에서 소스 무선 기기 또는 목적지 무선 기기가 기지국에게 일대일 무선 링크를 업데이트해달라고 요청할 때 현재 설정된 직접 무선 링크의 평가된 또는 경험한 신뢰도 또는 전송 지연 또는 에러율을 포함하여 보고할 수 있다.
- [0293] 도 2g는 본 발명의 다양한 실시 예에 따른 차세대 이동 통신 시스템에서 사용하는 COUNT 값의 구조를 설명하는 도면이다.
- [0294] PDCP 계층 장치에서는 단말과 기지국간의 암호화(ciphering) 및 무결성 보호(integrity)를 위해 COUNT라는 값을 저장하고, PDCP 패킷의 암호화 및 무결성 보호 시에 상기 COUNT 값을 미리 설정된 암호화 및 무결성 보호 알고리즘의 파라미터로 사용하게 된다. 자세한 동작은 다음 도면 2g에서 설명된다.
- [0295] 모든 PDCP 패킷(데이터 패킷, 제어 메시지 패킷)은 PDCP 일련번호(sequence number)를 가지게 되고, 패킷의 생성시 이전 값보다 1 증가된 값을 가질 수 있다. 미리 설정된 PDCP 일련번호 사이즈를 넘어가는 경우에는 PDCP SN은 0부터 다시 카운트 되게 되며, HFN을 1씩 증가시킨다. 이 경우 이전에 보냈었던 PDCP 패킷과 같은 PDCP 일련번호를 가지는 경우가 발생할 수 있다. 만약 해커가 이전의 PDCP 일련번호에 대한 값을 가지고 있다가 이후의 단말과 기지국간의 통신시 해당 값을 이용해서 해킹을 시도한다면 해커가 전송한 PDCP 데이터로 인해 PDCP 일련번호가 계속 증가하여 송신단과 수신단의 HFN 비동기화 문제가 발생할 수 있다. 또한 해커의 공격이 아니더라도 대량의 데이터가 유실되면 상기와 같은 HFN 비동기화 문제가 발생되어 수신단에서 수신한 데이터에 대한 복호화 실패가 발생할 수 있다.
- [0296] 상기에서 COUNT 값은 32 bits 길이를 가지며, HFN(hyper frame number, 2g-05)와 PDCP 일련번호(2g-10)으로 구성된다. 상기의 COUNT 값을 단말과 기지국은 보유하고 있다가 암호화 및 무결성 보호에 사용할 수 있다. 실제 데이터 전송시 PDCP 패킷(PDCP PDU)에는 PDCP 일련번호만 포함되게 된다. 그러므로 해커 입장에서는 무선 채널에서는 PDCP 일련번호만 전송되기 때문에 정확한 COUNT 값 자체를 알기는 어렵다. 상기에서 기지국이 단말에게 RRC 메시지로 PDCP 설정정보를 설정할 때 상기의 PDCP 일련번호 길이는 12비트 또는 18비트가 설정되며, PDCP 일련번호 길이에 따라 COUNT 값의 HFN 길이는 32비트 - PDCP 일련번호 길이로 자동으로 결정될 수 있다.
- [0298] 도 2h는 본 발명의 다양한 실시 예에 따른 보안 체크(Security check) 절차를 나타낸 도면이다.
- [0299] 상기 보안 체크 절차는 송신단과 수신단 사이의 일대일 또는 일대다 무선 링크에서 해커에 의한 공격으로 과도하게 많은 패킷들 또는 변경된 패킷들이 수신되어 무선 링크가 보안 위협에 노출되는 문제를 해결하기 위해 보안키값들(보안 키 또는 보안 식별자 또는 COUNT 값)을 확인하기 위한 절차이다.
- [0300] 도 2h는 송신단이 단말의 보안키값들(예를 들면 COUNT 값)을 체크하기 위한 전체 동작을 나타내며, 제안한 절차를 통해 송신단은 설정된 베어러 별로 COUNT 값이 유효한지 여부 또는 COUNT 값의 동기화 여부를 확인할 수 있다.
- [0301] 먼저 송신단(2h-01)과 수신단(2h-02)은 일대일 또는 일대다 무선 연결을 설정할 수 있다(2h-05). 그리고 송신단은 필요한 경우, 예를 들면 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 송신 PDCP 계층 장치와 수신 PDCP 계층 장치의 보안키값들(예를 들면 COUNT 값)이 동기가 잘 맞춰져 있는 지 확인할 수 있도록 수신단에게 보안 체크 요청(Security Check Request) 메시지를 보내어 수신단에게 베어러 별 보안 체크 및 보고를 요청할 수 있다(2h-10).
- [0302] 수신단은 상기 보안 체크 요청 메시지를 수신한 뒤, 수신단의 베어러 별 보안키값들(예를 들면 COUNT)을 확인하고 보안 체크 응답(Security Check Response) 메시지를 구성하여 송신단으로 전송할 수 있다(2h-15).
- [0303] 송신단은 상기 보안 체크 응답 메시지를 수신하면, 베어러 별 보안키값들을 확인하여 HFN 비동기 문제가 확인되는 경우, 또는 해커로 인한 침입이 확인되는 경우, 연결을 끊거나 또는 연결을 재설정할 수 있다.
- [0305] 도 2i는 도 2h에서 제안한 보안 체크 절차를 데이터 베어러(DRB, Data radio bearer)에서 수행하는 구체적인 제 1 실시 예를 나타낸 도면이다.
- [0306] 본 발명에서 보안 체크 절차를 수행하는 송신단과 수신단의 구체적인 제 1-1 실시 예는 다음과 같다.

- [0307] - 송신단 : 송신단은 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 보안 체크 절차를 트리거링하기 위해서 2i-05와 같이 PDU 유형(PDU type)을 정의하여 제 1의 PDCP control PDU를 새로 정의하고 사용할 수 있다. 즉, 제 1의 PDCP control PDU는 상기 도 2h에서 보안 체크 요청(Security Check Request) 메시지로 사용될 수 있다. 상기에서 새로 정의한 제 1의 PDCP control PDU는 송신단에서 사용하고 있는 보안키값들(예를 들면 보안 식별자 또는 보안키값 또는 COUNT 값)을 포함하여 전송할 수 있다. 예를 들면 송신단은 송신 PDCP 계층 장치에서 현재까지 보낸 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값 또는 수신 PDCP 계층 장치에서 현재까지 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값을 상기 제 1의 PDCP control PDU에 포함하여 전송할 수 있다. 또 다른 방법으로 상기 송신 PDCP 계층 장치의 COUNT 값 또는 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 상기에서 보안성 강화를 위해서 전체 COUNT 값을 보내지 않고 제 1의 PDCP control PDU에서 COUNT 값을 보낼 때 상위 일부 MSB들만 전송할 수도 있다. 예를 들면 32비트 COUNT 값의 상위 20 비트 또는 25비트만을 보낼 수도 있다. 상기에서 보안성을 강화하기 위해서 상기 제 1의 PDCP control PDU는 암호화 또는 무결성 보호를 수행할 수도 있다.
- [0308] - 수신단 : 수신단은 상기 제 1의 PDCP control PDU를 통해 보안 체크 요청(Security Check Request) 메시지를 수신하면, 상기 제 1의 PDCP control PDU에 포함된 송신단의 송신 PDCP 계층 장치의 COUNT 값 또는 송신단의 수신 PDCP 계층 장치의 COUNT 값 또는 상기 COUNT 값들의 상위 일부 MSB 값을 수신단의 수신 PDCP 계층 장치의 COUNT 값 또는 수신단의 송신 PDCP 계층 장치의 COUNT 값과 비교하여 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 송신단과의 연결을 끊거나 또는 연결을 재설정할 수 있다. 상기에서 수신단은 송신단의 송신 PDCP 계층 장치의 COUNT 값을 수신단의 수신 PDCP 계층 장치에서 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT 값과 비교할 수 있다. 또한 수신단은 송신단의 수신 PDCP 계층 장치의 COUNT 값을 수신단의 송신 PDCP 계층 장치에서 전송한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT 값과 비교할 수 있다. 또 다른 방법으로 수신단은 도 2i-10과 같이 PDU 유형(PDU type)을 정의하여 제 2의 PDCP control PDU를 새로 정의하고 사용할 수 있다. 상기 제 2의 PDCP control PDU는 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 송신단에게 지시할 수 있다. 또 다른 방법으로 상기 제 2의 PDCP control PDU에 새로운 1비트 S 필드를 정의하여 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 지시하거나 또는 아무런 문제가 없다는 것을 지시할 수 있다. 또 다른 방법으로 상기에서 수신단은 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 제 2의 PDCP control PDU를 2i-15와 같이 정의하여 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값을 포함하여 전송할 수 있다. 또 다른 방법으로 상기 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 또 다른 방법으로 수신단은 2i-20과 같이 PDCP data PDU의 PDCP 헤더에 새로운 1비트 S 필드를 정의하여 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 지시하거나 또는 아무런 문제가 없다는 것을 지시할 수 있다. 상기 제 2의 PDCP control PDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 상기에서 제 2의 PDCP control PDU 또는 새로 정의한 S 필드가 포함된 PDCP 헤더가 접합된 PDCP data PDU는 도 2h의 보안 체크 응답(Security Check Response) 메시지에 해당할 수 있다.
- [0310] 본 발명에서 보안 체크 절차를 수행하는 송신단과 수신단의 구체적인 제 1-2 실시 예는 다음과 같다.
- [0311] - 송신단 : 송신단은 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 보안 체크 절차를 트리거링하기 위해서 2i-10와 같이 PDU 유형(PDU type)을 정의하여 제 3의 PDCP control PDU를 새로 정의하고 사용할 수 있으며 또는 상기 제 3의 PDCP control PDU에 새로운 1비트 S 필드를 정의할 수 있다. 또는 2i-20과 같이 PDCP data PDU의 PDCP 헤더에 새로운 1비트 S 필드를 정의할 수 있다. 즉, 제 3의 PDCP control PDU 또는 새로운 1비트 S 필드를 포함한 PDCP 헤더가 접합된 PDCP data PDU는 상기 도 2h에서 보안 체크 요청(Security Check Request) 메시지로 사용될 수 있다. 상기에서 새로 정의한 제 3의 PDCP control PDU는 송신단에서 전송되며 수신단에게 보안키값들(예를 들면 보안키값 또는 COUNT 값 또는 보안 식별자)에 대한 정보를 요청할 수 있다. 상기에서 보안성을 강화하기 위해서 상기 제 3의 PDCP control PDU는 암호화 또는 무결성 보호를 수행할 수도 있다.
- [0312] - 수신단 : 수신단은 상기 제 3의 PDCP control PDU를 통해 보안 체크 요청(Security Check Request) 메시지를

수신하면, 수신단은 2i-15와 같이 제 4의 PDCP control PDU를 정의하고 수신단에서 사용하고 있는 보안키값들(예를 들면 보안 식별자 또는 보안키값 또는 COUNT 값)을 포함하여 전송할 수 있다. 예를 들면 수신단은 송신 PDCP 계층 장치에서 현재까지 보낸 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값 또는 수신 PDCP 계층 장치에서 현재까지 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값을 상기 제 4의 PDCP control PDU에 포함하여 전송할 수 있다. 또 다른 방법으로 상기 송신 PDCP 계층 장치의 COUNT 값 또는 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 상기에서 보안성 강화를 위해서 전체 COUNT 값을 보내지 않고 제 4의 PDCP control PDU에서 COUNT 값을 보낼 때 상위 일부 MSB들만 전송할 수도 있다. 예를 들면 32비트 COUNT 값의 상위 20 비트 또는 25비트만을 보낼 수도 있다. 상기에서 보안성을 강화하기 위해서 상기 제 4의 PDCP control PDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 상기에서 제 4의 PDCP control PDU는 도 2h의 보안 체크 응답(Security Check Response) 메시지에 해당할 수 있다.

[0313] - 송신단은 상기 제 4의 PDCP control PDU를 통해 보안 체크 응답(Security Check Response) 메시지를 수신하면, 상기 제 4의 PDCP control PDU에 포함된 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값 또는 상기 COUNT 값들의 상위 일부 MSB 값을 송신단의 수신 PDCP 계층 장치의 COUNT 값 또는 송신단의 송신 PDCP 계층 장치의 COUNT 값과 비교하여 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 송신단과의 연결을 끊거나 또는 연결을 재설정할 수 있다. 상기에서 송신단은 수신단의 송신 PDCP 계층 장치의 COUNT 값을 송신단의 수신 PDCP 계층 장치에서 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT값과 비교할 수 있다. 또한 송신단은 수신단의 수신 PDCP 계층 장치의 COUNT 값을 송신단의 송신 PDCP 계층 장치에서 전송한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT값과 비교할 수 있다.

[0315] 도 2j는 도 2h에서 제안한 보안 체크 절차를 사이드 링크 베어러(SLRB, Sidelink radio bearer)에서 수행하는 구체적인 제 2 실시 예를 나타낸 도면이다.

[0316] 본 발명에서 보안 체크 절차를 수행하는 송신단과 수신단의 구체적인 제 2-1 실시 예는 다음과 같다.

[0317] - 송신단 : 송신단은 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 보안 체크 절차를 트리거링하기 위해서 2j-05와 같이 SDU 유형(SDU type)을 정의하여 제 1의 PDCP SDU를 새로 정의하고 사용할 수 있다. 즉, 제 1의 PDCP SDU는 상기 도 2h에서 보안 체크 요청(Security Check Request) 메시지로 사용될 수 있다. 상기에서 새로 정의한 제 1의 PDCP SDU는 송신단에서 사용하고 있는 보안키값들(예를 들면 보안 식별자 또는 보안키값 또는 COUNT 값)을 포함하여 전송할 수 있다. 예를 들면 송신단은 송신 PDCP 계층 장치에서 현재까지 보낸 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값 또는 수신 PDCP 계층 장치에서 현재까지 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값을 상기 제 1의 PDCP SDU에 포함하여 전송할 수 있다. 또 다른 방법으로 상기 송신 PDCP 계층 장치의 COUNT 값 또는 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 상기에서 보안성 강화를 위해서 전체 COUNT 값을 보내지 않고 제 1의 PDCP SDU에서 COUNT 값을 보낼 때 상위 일부 MSB들만 전송할 수도 있다. 예를 들면 32비트 COUNT 값의 상위 20 비트 또는 25비트만을 보낼 수도 있다. 상기에서 보안성을 강화하기 위해서 상기 제 1의 PDCP SDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 또한 상기 제 1의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다.

[0318] - 수신단 : 수신단은 상기 제 1의 PDCP SDU를 통해 보안 체크 요청(Security Check Request) 메시지를 수신하면, 상기 제 1의 PDCP SDU에 포함된 송신단의 송신 PDCP 계층 장치의 COUNT 값 또는 송신단의 수신 PDCP 계층 장치의 COUNT 값 또는 상기 COUNT 값들의 상위 일부 MSB 값을 수신단의 수신 PDCP 계층 장치의 COUNT 값 또는 수신단의 송신 PDCP 계층 장치의 COUNT 값과 비교하여 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 송신단과의 연결을 끊거나 또는 연결을 재설정할 수 있다. 상기에서 수신단은 송신단의 송신 PDCP 계층 장치의 COUNT 값을 수신단의 수신 PDCP 계층 장치에서 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT값과 비교할 수 있다. 또한 수신단은 송신단의 수신 PDCP 계층 장치의 COUNT 값을 수신단의 송신 PDCP 계층 장치에서 전송한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데

터에 상응하는 COUNT값과 비교할 수 있다. 또 다른 방법으로 수신단은 도 2j-10과 같이 SDU 유형(SDU type)을 정의하여 제 2의 PDCP SDU를 새로 정의하고 사용할 수 있다. 상기 제 2의 PDCP SDU는 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 송신단에게 지시할 수 있다. 또 다른 방법으로 상기 제 2의 PDCP SDU에 새로운 1비트 S필드를 정의하여 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 지시하거나 또는 아무런 문제가 없다는 것을 지시할 수 있다. 또 다른 방법으로 상기에서 수신단은 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 제 2의 PDCP SDU를 2j-15와 같이 정의하여 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값을 포함하여 전송할 수 있다. 또 다른 방법으로 상기 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 또 다른 방법으로 수신단은 2j-20과 같이 데이터를 전송하는 PDCP SDU의 새로운 1비트 S필드를 정의하여 HFN 비동기 문제가 발생하였거나 해커로 인한 침입이 확인되었다는 것을 지시하거나 또는 아무런 문제가 없다는 것을 지시할 수 있다. 상기 제 2의 PDCP SDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 상기에서 제 2의 PDCP SDU 또는 새로 정의한 S필드가 포함되고 데이터를 포함하는 PDCP SDU는 도 2h의 보안 체크 응답(Security Check Response) 메시지에 해당할 수 있다. 또한 상기 제 2의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다.

[0320] 본 발명에서 보안 체크 절차를 수행하는 송신단과 수신단의 구체적인 제 1-2 실시 예는 다음과 같다.

[0321] - 송신단 : 송신단은 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 보안 체크 절차를 트리거링하기 위해서 2j-10과 같이 SDU 유형(SDU type)을 정의하여 제 3의 PDCP SDU를 새로 정의하고 사용할 수 있으며 또는 상기 제 3의 PDCP SDU에 새로운 1비트 S필드를 정의할 수 있다. 또는 2j-20과 같이 데이터를 포함하는 PDCP SDU에 새로운 1비트 S필드를 정의할 수 있다. 즉, 제 3의 PDCP SDU 또는 새로운 1비트 S필드를 포함한 PDCP SDU는 상기 도 2h에서 보안 체크 요청(Security Check Request) 메시지로 사용될 수 있다. 상기에서 새로 정의한 제 3의 PDCP SDU는 송신단에서 전송되며 수신단에게 보안키값들(예를 들면 보안키값 또는 COUNT 값 또는 보안 식별자)에 대한 정보를 요청할 수 있다. 상기에서 보안성을 강화하기 위해서 상기 제 3의 PDCP SDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 또한 상기 제 3의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다.

[0322] - 수신단 : 수신단은 상기 제 3의 PDCP SDU를 통해 보안 체크 요청(Security Check Request) 메시지를 수신하면, 수신단은 2j-15와 같이 제 4의 PDCP SDU를 정의하고 수신단에서 사용하고 있는 보안키값들(예를 들면 보안 식별자 또는 보안키값 또는 COUNT 값)을 포함하여 전송할 수 있다. 예를 들면 수신단은 송신 PDCP 계층 장치에서 현재까지 보낸 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값 또는 수신 PDCP 계층 장치에서 현재까지 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 해당하는 COUNT 값을 상기 제 4의 PDCP SDU에 포함하여 전송할 수 있다. 또 다른 방법으로 상기 송신 PDCP 계층 장치의 COUNT 값 또는 수신 PDCP 계층 장치의 COUNT 값 중에 하나를 별도로 보낼 수 있도록 하기 위해서 새로운 1비트 T 필드를 정의하여 송신 PDCP 계층 장치의 COUNT 값인지 수신 PDCP 계층 장치의 COUNT 값인지를 지시할 수 있도록 할 수 있다. 상기에서 보안성 강화를 위해서 전체 COUNT 값을 보내지 않고 제 4의 PDCP SDU에서 COUNT 값을 보낼 때 상위 일부 MSB들만 전송할 수도 있다. 예를 들면 32비트 COUNT 값의 상위 20 비트 또는 25비트만을 보낼 수도 있다. 상기에서 보안성을 강화하기 위해서 상기 제 4의 PDCP SDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 상기에서 제 4의 PDCP SDU는 도 2h의 보안 체크 응답(Security Check Response) 메시지에 해당할 수 있다. 또한 상기 제 4의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다.

[0323] - 송신단은 상기 제 4의 PDCP SDU를 통해 보안 체크 응답(Security Check Response) 메시지를 수신하면, 상기 제 4의 PDCP SDU에 포함된 수신단의 송신 PDCP 계층 장치의 COUNT 값 또는 수신단의 수신 PDCP 계층 장치의 COUNT 값 또는 상기 COUNT 값들의 상위 일부 MSB 값을 송신단의 수신 PDCP 계층 장치의 COUNT 값 또는 송신단의 송신 PDCP 계층 장치의 COUNT 값과 비교하여 HFN 비동기 문제가 발생한 경우, 또는 해커로 인한 침입이 확인된 경우, 송신단과의 연결을 끊거나 또는 연결을 재설정할 수 있다. 상기에서 송신단은 수신단의 송신 PDCP 계층 장치의 COUNT 값을 송신단의 수신 PDCP 계층 장치에서 수신한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT값과 비교할 수 있다. 또한 송신단은 수신단의 수신 PDCP 계층 장치의 COUNT 값을 송신단의 송신 PDCP 계층 장치에서 전송한 데이터들 중에서 가장 높은 PDCP 일련번호를 가지는 데이터에 상응하는 COUNT값과 비교할 수 있다.

- [0325] 도 2k는 본 발명의 다양한 실시 예에 따른 사이드 링크 베어러(SLRB, Sidelink radio bearer)를 통해서 송신단과 수신단이 무선 데이터 통신을 수행할 때 데이터의 유실 여부를 확인하고 무선 링크의 데이터 전송률을 체크할 수 있는 방법을 제안한다.
- [0326] 본 발명에서 사이드 링크 베어러(SLRB, Sidelink radio bearer)를 통해서 송신단과 수신단이 무선 데이터 통신을 수행할 때 데이터의 유실 여부를 확인하고 무선 링크의 데이터 전송률을 체크할 수 있는 방법의 구체적인 제 3 실시 예는 다음과 같다.
- [0327] - 송신단 : 송신단은 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우, 또는 데이터의 전송률을 확인하기 위해서 또는 유실이 있는 경우 재전송을 수행하기 위해서 2j-10와 같이 SDU 유형(SDU type)을 정의하여 제 5의 PDCP SDU를 새로 정의하고 사용할 수 있으며 또는 상기 제 5의 PDCP SDU에 새로운 1비트 P필드를 정의할 수 있다. 또는 2k-05와 같이 데이터를 포함하는 PDCP SDU에 새로운 1비트 P필드를 정의할 수 있다. 상기에서 새로 정의한 제 5의 PDCP SDU 또는 상기 새로 정의된 1비트 P필드는 송신단에서 전송되며 수신단에게 수신한 데이터들의 성공적인 데이터 수신 여부에 대한 정보를 요청할 수 있다. 상기에서 보안성을 강화하기 위해서 상기 제 5의 PDCP SDU는 암호화 또는 무결성 보호를 수행할 수도 있다. 또한 상기 제 5의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다.
- [0328] - 수신단 : 수신단은 상기 제 5의 PDCP SDU 또는 새로 정의된 1비트 P필드를 통해 수신한 데이터들에 대한 성공적인 수신 여부에 대한 요청을 수신하면, 수신단은 2k-10와 같이 제 6의 PDCP SDU를 정의하고 수신단에서 현재까지 수신한 데이터들의 PDCP 일련번호 또는 COUNT값을 오름차순으로 정렬하고 처음으로 유실된 또는 유실된 데이터들 중에서 가장 작은 PDCP 일련번호 또는 COUNT값을 확인하여 상기 제 6의 PDCP SDU에 새로운 FMS(First Missing SN 또는 First MisSing COUNT) 필드에 포함시키고, 상기 FMS 필드값보다 큰 PDCP 일련번호 또는 COUNT 값들에 대해서는 오름차순으로 1비트 지시자로 성공적인 수신 여부를 지시할 수 있는 비트맵을 구성하여 포함시킬 수 있다. 또 다른 방법으로 수신단은 2k-15와 같이 제 7의 PDCP SDU를 정의하고 수신단에서 현재까지 수신한 데이터들의 PDCP 일련번호 또는 COUNT값을 오름차순으로 정렬하고 처음으로 유실된 또는 유실된 데이터들 중에서 가장 작은 PDCP 일련번호 또는 COUNT값을 확인하여 상기 제 7의 PDCP SDU에 새로운 FMS(First Missing SN 또는 First MisSing COUNT) 필드에 포함시키고, 현재까지 수신한 데이터들 중에서 가장 큰 PDCP 일련번호 또는 COUNT 값을 상기 제 7의 PDCP SDU에 새로운 HRS(Highest Received SN 또는 Highest Received COUNT) 필드에 포함시킬 수 있다. 그리고 상기 현재까지 수신된 가장 작은 PDCP 일련번호 또는 COUNT값을 지시하는 FMS 필드값과 상기 현재까지 수신된 가장 큰 PDCP 일련번호 또는 COUNT값을 지시하는 HRS 필드값 사이의 PDCP 일련번호 또는 COUNT 값에 해당하는 데이터들 중에서 성공적으로 수신되지 않은 데이터들의 개수를 상기 제 7의 PDCP SDU에 새로운 NMS(Number of missing SN 또는 Number of missing COUNT) 필드에 포함시킬 수 있다. 상기와 같이 제 7의 PDCP SDU를 구성하여 송신단으로 전송하여 응답할 수 있다. 상기에서 제 6의 PDCP SDU 또는 제 7의 PDCP SDU에서 보안 식별자 값은 생략될 수도 있다. 또 다른 방법으로 제 8의 PDCP SDU를 정의하여 유실된 데이터의 수 또는 데이터 유실 정도(예를 들면 유실률 또는 유실 확률 또는 유실 통계)만 보고할 수도 있다.
- [0329] - 송신단은 상기 제 6의 PDCP SDU 또는 제 7의 PDCP SDU를 수신단으로부터 수신하면 전송한 데이터들의 성공적인 수신 여부를 확인할 수 있고, 유실된 데이터들에 대해서는 재전송을 수행할 수도 있다. 또한 제 7의 PDCP SDU를 수신한 경우, 전송한 데이터의 개수 대비 유실된 데이터의 개수를 확인할 수 있기 때문에 현재 무선 링크의 데이터 전송률 또는 데이터 유실률 또는 무선 링크 품질을 계산해내는데 사용될 수 있다.
- [0331] 상기 본 발명의 제 1-1 실시 예 또는 제 1-2 실시 예 또는 제 2-1 실시 예 또는 제 2-2 실시 예 또는 제 3 실시 예는 SDAP 계층 장치에서 정의되고 확장되어 또는 응용되어 적용될 수 있다.
- [0332] 본 발명에서 설명한 상향 링크 데이터 압축 절차(Uplink data compression, UDC)는 사이드 링크 베어러에서 확장되어 적용될 수 있으며, 2j-20와 같은 데이터 PDCP SDU에 적용될 때 데이터의 첫 6바이트(즉, SDU 헤더)에는 상향 링크 데이터 압축 절차를 적용하지 않고, 뒷 부분(즉, 상위 계층 데이터)에만 상향 링크 데이터 압축 절차를 적용하고, UDC 헤더를 생성하여 접합하여 상기 SDU 헤더와 UDC 헤더와 압축된 데이터 순으로 데이터를 구성하여 전송할 수 있다. 또 다른 방법으로 2j-20와 같은 데이터 PDCP SDU에 적용될 때 데이터의 첫 6바이트(즉, SDU 헤더)와 뒷부분(상위 계층 데이터)에 모두 상향 링크 데이터 압축 절차를 적용하고, UDC 헤더를 생성하여 접합하여 UDC 헤더와 압축된 데이터 순으로 데이터를 구성하여 전송할 수 있다. 수신단은 상기 절차의 반대로

데이터 압축해제를 수행할 수 있다.

- [0334] 도 21는 본 발명에서 제안한 보안 체크 절차의 제 1 실시 예 또는 제 2 실시 예에서 송신단 또는 수신단에서 지시하는 COUNT 값의 비트의 크기를 줄일 수 있는 방안을 제시한다.
- [0335] 상기 본 발명에서 제안한 보안 체크(Security check) 절차는 각 베어러별로 COUNT 값의 HFN 값을 확인하기 위한 목적이다. 따라서 설정할 수 있는 PDCP 일련번호의 길이에 따라서 송신단이 지시하는 COUNT 값의 상위 비트의 크기를 줄일 수 있다. 차세대 이동 통신 시스템에서는 지원하는 PDCP 일련번호의 길이의 종류에 따라서 줄일 수 있는 비트의 크기가 결정될 수 있다. 예를 들어 21-10과 21-15와 같이 PDCP 일련번호의 길이가 12비트라면 상기 베어러에 대해서 HFN 값을 비교할 때 도 21-15와 같이 상위 20비트면 충분하다. 따라서 상기에서 제안한 보안 체크 절차에서 각 베어러 별로 상위 20비트를 사용한다면 5비트x베어러 수 만큼 오버헤드를 줄일 수 있다. 또한 상기 상위 비트 수를 (32비트 - 각 베어러의 PDCP 일련번호 길이)로 설정하면 오버헤드를 줄일 수 있다.
- [0336] 만약 RLC 계층 장치에서 6비트 RLC 일련번호를 지원하기 때문에 PDCP 계층 장치에서도 헤더 오버헤드를 줄이기 위해서 새로운 PDCP 일련번호 길이로 6비트가 도입이 된다면 상기 보안 체크 절차에서 HFN의 정확한 비교를 위해서 COUNT 값의 상위 26비트로 사용될 수 있다.
- [0338] 본 발명의 다음에서는 상기와 같이 일대일 통신 또는 일대다 통신에서 또는 구체적으로 단말과 기지국 간의 데이터 송수신이 이루어질 때 무결성 보호 및 검증 절차와 데이터 중복 탐지 방법을 악용하여 데이터 유실을 발생시키는 해커의 공격을 방지하기 위한 수신단의 데이터 처리 방법을 제안한다.
- [0339] 상기에서 언급한 데이터 유실을 발생시키는 해커의 공격은 PDCP 계층 장치의 수신 동작을 악용하여 수행할 수 있다.
- [0340] 상기에서 해커가 악용할 수 있는 수신 PDCP 계층 장치의 동작에 대한 제 1 실시 예는 다음과 같다.
- [0341] 수신 PDCP 계층 장치는 수신한 데이터를 프로세싱할 때 3개의 COUNT 변수를 유지하고 관리한다. 상기 수신 PDCP 계층 장치는 수신한 데이터를 프로세싱할 때 다음에 수신할 것이라고 예상되는 데이터(예를 들면 PDCP SDU)의 COUNT 값을 유지하는 제 2의 COUNT 변수를 사용하며, 상기 제 2의 COUNT 변수는 RX_NEXT로 명명될 수 있다. 그리고 상기 수신 PDCP 계층 장치는 수신한 데이터를 프로세싱할 때 상위 계층으로 전달되지 않은 첫 번째 데이터(예를 들면 PDCP SDU)의 COUNT 값을 유지하는 제 3의 COUNT 변수를 사용하며, 상기 제 3의 COUNT 변수는 RX_DELIV로 명명될 수 있다. 그리고 상기 수신 PDCP 계층 장치는 수신한 데이터를 프로세싱할 때 PDCP 재정렬 타이머(t-Reordering)를 트리거링하게 했던 데이터(예를 들면 PDCP SDU)의 COUNT 값을 유지하는 제 4의 COUNT 변수를 사용하며, 상기 제 4의 COUNT 변수는 RX_REORD로 명명될 수 있다. 그리고 상기 수신 PDCP 계층 장치는 수신한 데이터를 프로세싱할 때 현재 수신한 데이터(예를 들면 PDCP SDU)의 COUNT 값을 유지하는 제 5의 COUNT 변수를 사용하며, 상기 제 5의 COUNT 변수는 RCVD_COUNT로 명명될 수 있다. 상기에서 PDCP 재정렬 타이머는 상위 계층(RRC 계층)에서 도 1e에서와 같이 RRC 메시지로 설정된 타이머 값 혹은 구간을 사용하며, 상기 타이머는 유실된 PDCP PDU를 탐지하기 위해서 사용되고, 오로지 한번에 하나의 타이머만 구동된다.
- [0342] 또한 수신 PDCP 계층 장치의 동작에서 단말은 다음과 같은 변수들을 정의하고 사용할 수 있다.
- [0343] - HFN : 윈도우 상태 변수의 HFN(Hyper Frame Number) 부분을 나타낸다.
- [0344] - SN : 윈도우 상태 변수의 일련번호(SN, Sequence Number) 부분을 나타낸다.
- [0345] - RCVD_SN : 수신한 PDCP PDU의 헤더에 포함되어 있는 PDCP 일련번호
- [0346] - RCVD_HFN : 수신 PDCP 계층 장치가 계산한 수신한 PDCP PDU의 HFN 값
- [0347] 본 발명에서 제안하는 단말 또는 기지국의 수신 PDCP 계층 장치의 동작은 다음과 같다.
- [0348] 하위 계층으로부터 PDCP PDU를 수신하였을 때 수신 PDCP 계층 장치는 수신한 PDCP PDU의 COUNT 값을 다음과 같이 결정한다.
- [0349] - 만약 수신한 RCVD_SN이 $RCVD_SN \leq SN(RX_DELIV) - Window_Size$ 이라면
- [0350] $RCVD_HFN = HFN(RX_DELIV) + 1$ 로 업데이트 한다.

- [0351] - 그렇지 않고 만약 RCVD_SN이 $RCVD_SN > SN(RX_DELIV) + Window_Size$ 이라면
- [0352] $RCVD_HFN = HFN(RX_DELIV) - 1$ 로 업데이트 한다.
- [0353] - 상기의 경우가 아니라면
- [0354] $RCVD_HFN = HFN(RX_DELIV)$ 로 업데이트 한다.
- [0355] - RCVD_COUNT 은 $RCVD_COUNT = [RCVD_HFN, RCVD_SN]$ 와 같이 결정된다.
- [0357] 수신한 PDCP PDU의 COUNT 값을 결정하고 나면 수신 PDCP 계층 장치는 다음과 같이 윈도우 상태 변수들을 업데이트하고 PDCP PDU를 처리한다.
- [0358] - 상기 RCVD_COUNT 값을 사용하여 상기 PDCP PDU에 대해서 복호화를 수행하고, 무결성 검증을 수행한다.
- [0359] 만약 무결성 검증에 실패했다면
- [0360] 상위 계층에 무결성 검증 실패를 지시하고 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0361] - 만약 $RCVD_COUNT < RX_DELIV$ 이거나 혹은 RCVD_COUNT의 값을 갖는 PDCP PDU가 이전에 수신된 적이 있다면(만료한 혹은 기간이 지난 혹은 윈도우 밖에 패킷의 경우 혹은 중복된 패킷의 경우)
- [0362] 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0363] 만약 상기에서 수신한 PDCP PDU가 버려지지 않았다면 수신 PDCP 계층 장치는 다음과 같이 동작한다.
- [0364] - 상기에서 처리된 PDCP SDU를 수신 버퍼에 저장한다.
- [0365] - 만약 $RCVD_COUNT \geq RX_NEXT$ 라면
- [0366] RX_NEXT 를 $RCVD_COUNT + 1$ 로 업데이트한다.
- [0367] - 만약 비순서 전달 지시자(outOfOrderDelivery)가 설정되었다면(비순서 전달 동작을 지시하였다면),
- [0368] 상기 PDCP SDU를 상위 계층으로 전달한다.
- [0369] - 만약 RCVD_COUNT가 RX_DELIV와 같다면
- [0370] 상기에 데이터들에 대해 COUNT 값 순서대로 상위 계층에 전달한다.
- [0371] $COUNT = RX_DELIV$ 값부터 시작해서 연속적인 PDCP SDU들을 모두 상위 계층으로 전달한다.
- [0372] RX_DELIV 값을 현재 RX_DELIV 보다 크거나 같은 COUNT 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 COUNT 값으로 업데이트한다.
- [0373] - 만약 t-Reordering 타이머가 구동되고 있고, RX_DELIV 값이 RX_REORD 보다 크거나 같다면,
- [0374] t-Reordering 타이머를 중지하고 리셋한다.
- [0375] - 만약 t-Reordering 타이머가 구동되고 있지 않고(상기 조건에서 중지된 경우도 포함하여) RX_DELIV 가 RX_NEXT 보다 작다면,
- [0376] RX_REORD 값을 RX_NEXT 로 업데이트 한다.
- [0377] t-Reordering 타이머를 시작한다.
- [0379] PDCP 재정렬 타이머(t-Reordering)가 만료하였을 때 수신 PDCP 계층 장치는 다음과 같이 동작한다.
- [0380] - 이전에 헤더 압축 해제 절차가 적용되지 않았다면 (즉 상위 계층 헤더에 대해 아직 데이터 처리가 되지 않았다면) 헤더 압축 해제 절차를 저장된 데이터들에 대해 수행하고, 상기 데이터들에 대해 COUNT 값의 순서대로 상위 계층으로 전달한다.
- [0381] RX_REORD 값보다 작은 COUNT 값들을 가지는 모든 PDCP SDU들을 전달한다.

- [0382] RX_REORD 값부터 시작해서 연속적인 COUNT 값들을 가지는 모든 PDCP SDU들을 전달한다.
- [0383] - RX_DELIV 값을 RX_REORD보다 크거나 같은 COUNT 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 COUNT 값으로 업데이트한다.
- [0384] - 만약 RX_DELIV 값이 RX_NEXT 값보다 작다면,
- [0385] RX_REORD 값을 RX_NEXT 값으로 업데이트한다.
- [0386] t-Reordering 타이머를 시작한다.
- [0387] 상기 수신 PDCP 계층 장치의 동작 제 1 실시 예에서 무결성 보호 및 검증 절차는 SRB(Signalling Radio Bearer) 또는 DRB(Data Radio Bearer)에 설정될 수 있다. 만약 SRB에 무결성 보호 및 검증 절차가 설정되었는데 수신한 데이터에 대해 무결성 검증 실패가 발생한다면 무결성 검증 실패를 상위 계층 장치(예를 들면 RRC 계층 장치)에 보고하고 상위 계층 장치는 RRC 연결 재수립 절차를 트리거링할 수 있다. 즉, 단말의 연결을 재설정하기 때문에 상기 베어러를 해제하고 다시 설정할 수 있다. 상기와 같이 SRB는 단말과 기지국 간의 설정을 송수신하는 RRC 메시지와 같이 중요한 메시지들을 주고 받기 때문에 무결성 실패가 발생한 경우, 해커의 공격으로 간주하고 새롭게 RRC 연결을 설정하여 상기 해커에 의한 공격을 피할 수 있도록 하기 위함이다.
- [0388] 하지만 DRB에 대해 무결성 보호 및 검증 절차가 설정된 경우, 수신 PDCP 계층 장치는 만약 수신한 데이터에 대해 무결성 검증 절차에 실패한다면, 무결성 검증 실패를 상위 계층 장치에 보고를 수행하고, 상기 무결성 검증 실패가 발생한 데이터를 폐기하지만 데이터 송수신을 계속 수행할 수 있다. 여기서 주의할 점은 상기 무결성 검증 절차 이후에 수행하는 중복 탐지 절차이다. 상기 본 발명의 수신 PDCP 계층 장치의 동작 제 1 실시 예에서 수신 PDCP 계층 장치는 어떤 COUNT 값에 해당하는 데이터를 수신하면 상기 COUNT값으로 무결성 검증 절차를 수행하여 실패가 발생한 데이터를 버리게 되어 있으며, 중복 탐지 절차에서는 현재 수신한 데이터에 해당하는 COUNT값을 이전에도 수신한 적이 있다면 즉, 이전에 상기 COUNT 값에 해당하는 데이터를 수신한 적이 있다면 데이터를 폐기하게 되어 있다.
- [0389] 따라서 상기와 같은 수신 PDCP 계층 장치의 동작 제 1 실시 예를 악용하여 또는 허점을 이용하여, 해커가 서로 다른 COUNT 값을 갖는 굉장히 많은 데이터를 수신 PDCP 계층 장치에게 송신할 수 있다. 그러면 수신 PDCP 계층 장치는 무결성 보호 및 검증 절차가 설정된 경우, 상기 해커에 의해 전송된 데이터들에 무결성 검증 실패를 확인하고 상기 공격에 해당하는 데이터들을 폐기할 수 있다. 하지만 문제는 상기 공격에 의한 데이터들에 해당하는 COUNT 값을 수신한 적이 있다고 수신 PDCP 계층 장치는 간주하게 된다. 따라서 공격에 의한 데이터들이 아닌 송신단이 전송한 정상적인 데이터들을 수신할 지라도 만약 상기 정상적인 데이터들에 해당하는 COUNT 값이 상기 공격에 의한 데이터들과 동일한 COUNT 값을 갖는다면, 수신 PDCP 계층 장치는 중복 탐지 절차에 의해 상기 정상적인 데이터들을 중복 수신한 것으로 간주하고 폐기하게 된다. 따라서 결국 해커에 의한 공격으로 인해 수신 PDCP 계층 장치가 정상적인 데이터들을 중복 탐지 절차에 의해 폐기하게 되어 데이터 유실이 발생하게 된다.
- [0390] 따라서 본 발명에서는 상기와 같이 해커가 무결성 보호 및 검증 절차와 중복 탐지 절차를 악용하여 데이터 유실을 발생시키는 공격을 방어하기 위한 수신 PDCP 계층 장치의 제 2 실시 예를 다음과 같이 제안한다. 구체적으로 수신 PDCP 계층 장치는 중복 탐지 절차에서 현재 수신한 데이터에 해당하는 COUNT 값을 이전에 수신한 적이 있고, 그 COUNT 값에 해당하는 데이터를 이전에 단순히 수신만 한 것이 아니라 성공적으로 수신한 적이 있다면 중복 탐지가 발생하였다고 판단하고 상기 수신한 데이터를 폐기하도록 하여 중복 탐지 절차를 향상시켜 해커의 공격을 방지할 수 있다. 상기에서 데이터를 성공적으로 수신하였다는 것은 상기 COUNT 값에 해당하는 데이터를 처리하여 버퍼에 저장한 적이 있거나 또는 수신 처리하고 상위 계층 장치로 전달한 적이 있거나 또는 무결성 보호 및 검증 절차가 설정된 경우, 상기 COUNT 값에 해당하는 데이터에 대해 무결성 검증을 성공적으로 수행했다는 것을 지시할 수 있다. 즉, 해커에 의한 공격으로 수신된 데이터들이 무결성 검증에 실패한 경우를 성공적으로 데이터가 수신하지 않았다고 판단할 수 있기 때문에 중복 탐지 절차에서 정상적인 데이터를 폐기하지 않을 수 있는 것이다. 본 발명에서 제안하는 수신 PDCP 계층 장치의 제 2 실시 예의 구체적인 절차는 다음과 같다.
- [0391] 하위 계층으로부터 PDCP PDU를 수신하였을 때 수신 PDCP 계층 장치는 수신한 PDCP PDU의 COUNT 값을 다음과 같이 결정한다.
- [0392] - 만약 수신한 RCVD_SN이 $RCVD_SN \leq SN(RX_DELIV) - Window_Size$ 이라면
- [0393] $RCVD_HFN = HFN(RX_DELIV) + 1$ 로 업데이트 한다.

- [0394] - 그렇지 않고 만약 $RCVD_SN < RCVD_SN > SN(RX_DELIV) + Window_Size$ 이라면
- [0395] $RCVD_HFN = HFN(RX_DELIV) - 1$ 로 업데이트 한다.
- [0396] - 상기의 경우가 아니라면
- [0397] $RCVD_HFN = HFN(RX_DELIV)$ 로 업데이트 한다.
- [0398] - $RCVD_COUNT$ 은 $RCVD_COUNT = [RCVD_HFN, RCVD_SN]$ 와 같이 결정된다.
- [0400] 수신한 PDCP PDU의 COUNT 값을 결정하고 나면 수신 PDCP 계층 장치는 다음과 같이 윈도우 상태 변수들을 업데이트하고 PDCP PDU를 처리한다.
- [0401] - 상기 $RCVD_COUNT$ 값을 사용하여 상기 PDCP PDU에 대해서 복호화를 수행하고, 무결성 검증을 수행한다.
- [0402] 만약 무결성 검증에 실패했다면
- [0403] 상위 계층에 무결성 검증 실패를 지시하고 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0404] - 만약 $RCVD_COUNT < RX_DELIV$ 이거나
- [0405] - 또는 $RCVD_COUNT$ 의 값을 갖는 PDCP PDU가 이전에 성공적으로 수신된 적이 있다면
- [0406] 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0407] 만약 상기에서 수신한 PDCP PDU가 버려지지 않았다면 수신 PDCP 계층 장치는 다음과 같이 동작한다.
- [0408] - 상기에서 처리된 PDCP SDU를 수신 버퍼에 저장한다.
- [0409] - 만약 $RCVD_COUNT \geq RX_NEXT$ 라면
- [0410] RX_NEXT 를 $RCVD_COUNT + 1$ 로 업데이트한다.
- [0411] - 만약 비순서 전달 지시자(outOfOrderDelivery)가 설정되었다면(비순서 전달 동작을 지시하였다면),
- [0412] 상기 PDCP SDU를 상위 계층으로 전달한다.
- [0413] - 만약 $RCVD_COUNT$ 가 RX_DELIV 와 같다면
- [0414] 상기에 데이터들에 대해 COUNT 값 순서대로 상위 계층에 전달한다.
- [0415] $COUNT = RX_DELIV$ 값부터 시작해서 연속적인 PDCP SDU들을 모두 상위 계층으로 전달한다.
- [0416] RX_DELIV 값을 현재 RX_DELIV 보다 크거나 같은 COUNT 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 COUNT 값으로 업데이트한다.
- [0417] - 만약 t-Reordering 타이머가 구동되고 있고, RX_DELIV 값이 RX_REORD 보다 크거나 같다면,
- [0418] t-Reordering 타이머를 중지하고 리셋한다.
- [0419] - 만약 t-Reordering 타이머가 구동되고 있지 않고(상기 조건에서 중지된 경우도 포함하여) RX_DELIV 가 RX_NEXT 보다 작다면,
- [0420] RX_REORD 값을 RX_NEXT 로 업데이트 한다.
- [0421] t-Reordering 타이머를 시작한다.
- [0423] PDCP 재정렬 타이머(t-Reordering)가 만료하였을 때 수신 PDCP 계층 장치는 다음과 같이 동작한다.
- [0424] - 이전에 헤더 압축 해제 절차가 적용되지 않았다면(즉 상위 계층 헤더에 대해 아직 데이터 처리가 되지 않았다면) 헤더 압축 해제 절차를 저장된 데이터들에 대해 수행하고, 상기 데이터들에 대해 COUNT 값의 순서대로 상위 계층으로 전달한다.
- [0425] RX_REORD 값보다 작은 COUNT 값들을 가지는 모든 PDCP SDU들을 전달한다.

- [0426] RX_REORD 값부터 시작해서 연속적인 COUNT 값들을 가지는 모든 PDCP SDU들을 전달한다.
- [0427] - RX_DELIV 값을 RX_REORD보다 크거나 같은 COUNT 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 COUNT 값으로 업데이트한다.
- [0428] - 만약 RX_DELIV 값이 RX_NEXT 값보다 작다면,
- [0429] RX_REORD 값을 RX_NEXT 값으로 업데이트한다.
- [0430] t-Reordering 타이머를 시작한다.
- [0432] 또한 본 발명에서는 상기와 같이 해커가 무결성 보호 및 검증 절차와 중복 탐지 절차를 악용하여 데이터 유실을 발생시키는 공격을 방어하기 위한 수신 PDCP 계층 장치의 제 3 실시 예를 다음과 같이 제안한다. 구체적으로 수신 PDCP 계층 장치는 중복 탐지 절차에서 현재 수신한 데이터에 해당하는 COUNT 값을 이전에 수신한 적이 있고, 그 COUNT 값에 해당하는 데이터를 이전에 성공적으로 수신한 적이 있다면(만약 무결성 보호 및 검증 절차가 설정된 경우, 상기 COUNT 값에 해당하는 데이터를 이전에 수신하였고, 무결성 검증 절차가 성공적으로 수행된 적이 있다면) 중복 탐지가 발생하였다고 판단하고 상기 수신한 데이터를 폐기하도록 하여 중복 탐지 절차를 항상 시켜 해커의 공격을 방지할 수 있다. 상기에서 데이터를 성공적으로 수신하였다는 것은 상기 COUNT 값에 해당하는 데이터를 처리하여 버퍼에 저장한 적이 있거나 또는 수신 처리하고 상위 계층 장치로 전달한 적이 있거나 또는 무결성 보호 및 검증 절차가 설정된 경우, 상기 COUNT 값에 해당하는 데이터에 대해 무결성 검증을 성공적으로 수행했다는 것을 지시할 수 있다. 즉, 해커에 의한 공격으로 수신된 데이터들이 무결성 검증에 실패한 경우를 성공적으로 데이터가 수신하지 않았다고 판단할 수 있기 때문에 중복 탐지 절차에서 정상적인 데이터를 폐기하지 않을 수 있는 것이다. 본 발명에서 제안하는 수신 PDCP 계층 장치의 제 2 실시 예의 구체적인 절차는 다음과 같다.
- [0433] 하위 계층으로부터 PDCP PDU를 수신하였을 때 수신 PDCP 계층 장치는 수신한 PDCP PDU의 COUNT 값을 다음과 같이 결정한다.
- [0434] - 만약 수신한 RCVD_SN이 $RCVD_SN \leq SN(RX_DELIV) - Window_Size$ 이라면
- [0435] $RCVD_HFN = HFN(RX_DELIV) + 1$ 로 업데이트 한다.
- [0436] - 그렇지 않고 만약 RCVD_SN이 $RCVD_SN > SN(RX_DELIV) + Window_Size$ 이라면
- [0437] $RCVD_HFN = HFN(RX_DELIV) - 1$ 로 업데이트 한다.
- [0438] - 상기의 경우가 아니라면
- [0439] $RCVD_HFN = HFN(RX_DELIV)$ 로 업데이트 한다.
- [0440] - $RCVD_COUNT$ 은 $RCVD_COUNT = [RCVD_HFN, RCVD_SN]$ 와 같이 결정된다.
- [0442] 수신한 PDCP PDU의 COUNT 값을 결정하고 나면 수신 PDCP 계층 장치는 다음과 같이 윈도우 상태 변수들을 업데이트하고 PDCP PDU를 처리한다.
- [0443] - 상기 $RCVD_COUNT$ 값을 사용하여 상기 PDCP PDU에 대해서 복호화를 수행하고, 무결성 검증을 수행한다.
- [0444] 만약 무결성 검증에 실패했다면
- [0445] 상위 계층에 무결성 검증 실패를 지시하고 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0446] - 만약 $RCVD_COUNT < RX_DELIV$ 이거나
- [0447] - 또는 $RCVD_COUNT$ 의 값을 갖는 PDCP PDU가 이전에 성공적으로 수신된 적이 있다면 그리고 만약 무결성 보호 및 검증 절차가 설정된 경우에 상기 $RCVD_COUNT$ 값에 해당하는 PDCP PDU에 대해 무결성 검증 절차를 이전에 성공적으로 수행한 적이 있다면,
- [0448] 상기 수신한 PDCP Data PDU(PDCP PDU의 데이터 부분)를 폐기한다.
- [0449] 만약 상기에서 수신한 PDCP PDU가 버려지지 않았다면 수신 PDCP 계층 장치는 다음과 같이 동작한다.

- [0450] - 상기에서 처리된 PDCP SDU를 수신 버퍼에 저장한다.
- [0451] - 만약 $RCVD_COUNT \geq RX_NEXT$ 라면
- [0452] RX_NEXT 를 $RCVD_COUNT + 1$ 로 업데이트한다.
- [0453] - 만약 비순서 전달 지시자(outOfOrderDelivery)가 설정되었다면(비순서 전달 동작을 지시하였다면),
- [0454] 상기 PDCP SDU를 상위 계층으로 전달한다.
- [0455] - 만약 $RCVD_COUNT$ 가 RX_DELIV 와 같다면
- [0456] 상기에 데이터들에 대해 $COUNT$ 값 순서대로 상위 계층에 전달한다.
- [0457] $COUNT = RX_DELIV$ 값부터 시작해서 연속적인 PDCP SDU들을 모두 상위 계층으로 전달한다.
- [0458] RX_DELIV 값을 현재 RX_DELIV 보다 크거나 같은 $COUNT$ 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 $COUNT$ 값으로 업데이트한다.
- [0459] - 만약 t-Reordering 타이머가 구동되고 있고, RX_DELIV 값이 RX_REORD 보다 크거나 같다면,
- [0460] t-Reordering 타이머를 중지하고 리셋한다.
- [0461] - 만약 t-Reordering 타이머가 구동되고 있지 않고(상기 조건에서 중지된 경우도 포함하여) RX_DELIV 가 RX_NEXT 보다 작다면,
- [0462] RX_REORD 값을 RX_NEXT 로 업데이트 한다.
- [0463] t-Reordering 타이머를 시작한다.
- [0465] PDCP 재정렬 타이머(t-Reordering)가 만료하였을 때 수신 PDCP 계층 장치는 다음과 같이 동작한다.
- [0466] - 이전에 헤더 압축 해제 절차가 적용되지 않았다면 (즉 상위 계층 헤더에 대해 아직 데이터 처리가 되지 않았다면) 헤더 압축 해제 절차를 저장된 데이터들에 대해 수행하고, 상기 데이터들에 대해 $COUNT$ 값의 순서대로 상위 계층으로 전달한다.
- [0467] RX_REORD 값보다 작은 $COUNT$ 값들을 가지는 모든 PDCP SDU들을 전달한다.
- [0468] RX_REORD 값부터 시작해서 연속적인 $COUNT$ 값들을 가지는 모든 PDCP SDU들을 전달한다.
- [0469] - RX_DELIV 값을 RX_REORD 보다 크거나 같은 $COUNT$ 값이면서 상위 계층으로 전달하지 않은 첫 번째 PDCP SDU의 $COUNT$ 값으로 업데이트한다.
- [0470] - 만약 RX_DELIV 값이 RX_NEXT 값보다 작다면,
- [0471] RX_REORD 값을 RX_NEXT 값으로 업데이트한다.
- [0472] t-Reordering 타이머를 시작한다.
- [0474] 도 2m은 본 발명의 다양한 실시 예에 따른 보안 체크 절차를 수행하는 송신단과 수신단의 동작을 나타낸 도면이다.
- [0475] 먼저 송신단(2m-01)과 수신단(2m-02)은 일대일 또는 일대다 무선 연결을 설정할 수 있다. 그리고 송신단은 필요한 경우, 예를 들면 무결성 검증 실패 또는 복호화 실패가 발생하거나 HFN 비동기 문제가 의심되는 경우, 또는 해커로 인한 침입이 의심되는 경우(2m-05), 송신 PDCP 계층 장치와 수신 PDCP 계층 장치의 보안키값들(예를 들면 $COUNT$ 값)이 동기가 잘 맞춰져 있는 지 확인할 수 있도록 상기 본 발명에서 제안한 제 1-1 실시 예 또는 제 1-2 실시 예 또는 제 2-1 실시 예 또는 제 2-2 실시 예에 따라서 수신단에게 보안 체크 요청(Security Check Request) 메시지를 보내어 수신단에게 베어러 별 보안 체크 및 보고를 요청할 수 있다(2m-10, 2m-15).
- [0476] 수신단은 상기 보안 체크 요청 메시지를 수신한 뒤(2m-30), 수신단의 베어러 별 보안키값들(예를 들면 $COUNT$)을 확인하고(2m-35) 상기 본 발명에서 제안한 제 1-1 실시 예 또는 제 1-2 실시 예 또는 제 2-1 실시 예 또는 제 2-2 실시 예에 따라서 보안 체크 응답(Security Check Response) 메시지를 구성하여 송신단으로 전송할 수 있다

(2m-40, 2m-45). 만약 상기에서 보안 체크 요청 메시지를 수신한 뒤 수신단은 HFN 비동기 문제가 확인되는 경우, 또는 해커로 인한 침입이 확인되는 경우, 연결을 끊거나 또는 연결을 재설정할 수 있다.

[0477] 송신단은 상기 보안 체크 응답 메시지를 수신하면, 베어러 별 보안키값들을 확인하여 HFN 비동기 문제가 확인되는 경우, 또는 해커로 인한 침입이 확인되는 경우, 연결을 끊거나 또는 연결을 재설정할 수 있다(2m-25).

[0479] 도 2n에 본 발명의 실시 예가 적용될 수 있는 단말 또는 무선 노드의 구조를 도시하였다.

[0480] 상기 도면을 참고하면, 상기 단말은 RF(Radio Frequency)처리부(2n-10), 기저대역(baseband)처리부(2n-20), 저장부(2n-30), 제어부(2n-40)를 포함한다.

[0481] 상기 RF처리부(2n-10)는 신호의 대역 변환, 증폭 등 무선 채널을 통해 신호를 송수신하기 위한 기능을 수행한다. 즉, 상기 RF처리부(2n-10)는 상기 기저대역처리부(2n-20)로부터 제공되는 기저대역 신호를 RF 대역 신호로 상향 변환한 후 안테나를 통해 송신하고, 상기 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향 변환한다. 예를 들어, 상기 RF처리부(2n-10)는 송신 필터, 수신 필터, 증폭기, 믹서(mixer), 오실레이터(oscillator), DAC(digital to analog convertor), ADC(analog to digital convertor) 등을 포함할 수 있다. 상기 도면에서, 하나의 안테나만이 도시되었으나, 상기 단말은 다수의 안테나들을 구비할 수 있다. 또한, 상기 RF처리부(2n-10)는 다수의 RF 체인들을 포함할 수 있다. 나아가, 상기 RF처리부(2n-10)는 빔포밍(beamforming)을 수행할 수 있다. 상기 빔포밍을 위해, 상기 RF처리부(2n-10)는 다수의 안테나들 또는 안테나 요소(element)들을 통해 송수신되는 신호들 각각의 위상 및 크기를 조절할 수 있다. 또한 상기 RF 처리부는 MIMO를 수행할 수 있으며, MIMO 동작 수행 시 여러 개의 레이어를 수신할 수 있다. 상기 RF처리부(2n-10)는 제어부의 제어에 따라 다수의 안테나 또는 안테나 요소들을 적절하게 설정하여 수신 빔 스위핑을 수행하거나, 수신 빔이 송신 빔과 공조되도록 수신 빔의 방향과 빔 너비를 조정할 수 있다.

[0482] 상기 기저대역처리부(2n-20)은 시스템의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 상기 기저대역처리부(2n-20)은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(2n-20)은 상기 RF처리부(2n-10)로부터 제공되는 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 예를 들어, OFDM(orthogonal frequency division multiplexing) 방식에 따르는 경우, 데이터 송신 시, 상기 기저대역처리부(2n-20)는 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성하고, 상기 복소 심벌들을 부반송파들에 매핑한 후, IFFT(inverse fast Fourier transform) 연산 및 CP(cyclic prefix) 삽입을 통해 OFDM 심벌들을 구성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(2n-20)은 상기 RF처리부(2n-10)로부터 제공되는 기저대역 신호를 OFDM 심벌 단위로 분할하고, FFT(fast Fourier transform) 연산을 통해 부반송파들에 매핑된 신호들을 복원한 후, 복조 및 복호화를 통해 수신 비트열을 복원한다.

[0483] 상기 기저대역처리부(2n-20) 및 상기 RF처리부(2n-10)는 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 상기 기저대역처리부(2n-20) 및 상기 RF처리부(2n-10)는 송신부, 수신부, 송수신부 또는 통신부로 지칭될 수 있다. 나아가, 상기 기저대역처리부(2n-20) 및 상기 RF처리부(2n-10) 중 적어도 하나는 서로 다른 다수의 무선 접속 기술들을 지원하기 위해 다수의 통신 모듈들을 포함할 수 있다. 또한, 상기 기저대역처리부(2n-20) 및 상기 RF처리부(2n-10) 중 적어도 하나는 서로 다른 주파수 대역의 신호들을 처리하기 위해 서로 다른 통신 모듈들을 포함할 수 있다. 예를 들어, 상기 서로 다른 무선 접속 기술들은 LTE 망, NR 망 등을 포함할 수 있다. 또한, 상기 서로 다른 주파수 대역들은 극고단파(SHF:super high frequency)(예: 2.2GHz, 2ghz) 대역, mm파(millimeter wave)(예: 60GHz) 대역을 포함할 수 있다.

[0484] 상기 저장부(2n-30)는 상기 단말의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 상기 저장부(2n-30)는 상기 제어부(2n-40)의 요청에 따라 저장된 데이터를 제공한다.

[0485] 상기 제어부(2n-40)는 상기 단말의 전반적인 동작들을 제어한다. 예를 들어, 상기 제어부(2n-40)는 상기 기저대역처리부(2n-20) 및 상기 RF처리부(2n-10)을 통해 신호를 송수신한다. 또한, 상기 제어부(2n-40)는 상기 저장부(2n-40)에 데이터를 기록하고, 읽는다. 이를 위해, 상기 제어부(2n-40)는 적어도 하나의 프로세서(processor)를 포함할 수 있다. 예를 들어, 상기 제어부(2n-40)는 통신을 위한 제어를 수행하는 CP(communication processor) 및 응용 프로그램 등 상위 계층을 제어하는 AP(application processor)를 포함할 수 있다.

- [0487] 도 2o는 본 발명의 실시 예가 적용될 수 있는 무선 통신 시스템에서 TRP (기지국)또는 무선 노드의 블록 구성을 도시한다.
- [0488] 상기 도면에 도시된 바와 같이, 상기 기지국은 RF처리부(2o-10), 기저대역처리부(2o-20), 백홀통신부(2o-30), 저장부(2o-40), 제어부(2o-50)를 포함하여 구성된다.
- [0489] 상기 RF처리부(2o-10)는 신호의 대역 변환, 증폭 등 무선 채널을 통해 신호를 송수신하기 위한 기능을 수행한다. 즉, 상기 RF처리부(2o-10)는 상기 기저대역처리부(2o-20)로부터 제공되는 기저대역 신호를 RF 대역 신호로 상향변환한 후 안테나를 통해 송신하고, 상기 안테나를 통해 수신되는 RF 대역 신호를 기저대역 신호로 하향변환한다. 예를 들어, 상기 RF처리부(2o-10)는 송신 필터, 수신 필터, 증폭기, 믹서, 오실레이터, DAC, ADC 등을 포함할 수 있다. 상기 도면에서, 하나의 안테나만이 도시되었으나, 상기 제1접속 노드는 다수의 안테나들을 구비할 수 있다. 또한, 상기 RF처리부(2o-10)는 다수의 RF 채널들을 포함할 수 있다. 나아가, 상기 RF처리부(2o-10)는 빔포밍을 수행할 수 있다. 상기 빔포밍을 위해, 상기 RF처리부(2o-10)는 다수의 안테나들 또는 안테나 요소들을 통해 송수신되는 신호들 각각의 위상 및 크기를 조절할 수 있다. 상기 RF 처리부는 하나 이상의 레이어를 전송함으로써 하향 MIMO 동작을 수행할 수 있다.
- [0490] 상기 기저대역처리부(2o-20)는 제1무선 접속 기술의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행한다. 예를 들어, 데이터 송신 시, 상기 기저대역처리부(2o-20)은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(2o-20)은 상기 RF처리부(2o-10)로부터 제공되는 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 예를 들어, OFDM 방식에 따르는 경우, 데이터 송신 시, 상기 기저대역처리부(2o-20)은 송신 비트열을 부호화 및 변조함으로써 복소 심벌들을 생성하고, 상기 복소 심벌들을 부반송파들에 매핑한 후, IFFT 연산 및 CP 삽입을 통해 OFDM 심벌들을 구성한다. 또한, 데이터 수신 시, 상기 기저대역처리부(2o-20)은 상기 RF처리부(2o-10)로부터 제공되는 기저대역 신호를 OFDM 심벌 단위로 분할하고, FFT 연산을 통해 부반송파들에 매핑된 신호들을 복원한 후, 복조 및 복호화를 통해 수신 비트열을 복원한다. 상기 기저대역처리부(2o-20) 및 상기 RF처리부(2o-10)는 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 상기 기저대역처리부(2o-20) 및 상기 RF처리부(2o-10)는 송신부, 수신부, 송수신부, 통신부 또는 무선 통신부로 지칭될 수 있다.
- [0491] 상기 통신부(2o-30)는 네트워크 내 다른 노드들과 통신을 수행하기 위한 인터페이스를 제공한다.
- [0492] 상기 저장부(2o-40)는 상기 주기지국의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 특히, 상기 저장부(2o-40)는 접속된 단말에 할당된 베어러에 대한 정보, 접속된 단말로부터 보고된 측정 결과 등을 저장할 수 있다. 또한, 상기 저장부(2o-40)는 단말에게 다중 연결을 제공하거나, 중단할지 여부의 판단 기준이 되는 정보를 저장할 수 있다. 그리고, 상기 저장부(2o-40)는 상기 제어부(2o-50)의 요청에 따라 저장된 데이터를 제공한다.
- [0493] 상기 제어부(2o-50)는 상기 주기지국의 전반적인 동작들을 제어한다. 예를 들어, 상기 제어부(2o-50)는 상기 기저대역처리부(2o-20) 및 상기 RF처리부(2o-10)을 통해 또는 상기 백홀통신부(2o-30)을 통해 신호를 송수신한다. 또한, 상기 제어부(2o-50)는 상기 저장부(2o-40)에 데이터를 기록하고, 읽는다. 이를 위해, 상기 제어부(2o-50)는 적어도 하나의 프로세서를 포함할 수 있다.
- [0495] 본 발명의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들은 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합의 형태로 구현될(implemented) 수 있다.
- [0496] 소프트웨어로 구현하는 경우, 하나 이상의 프로그램(소프트웨어 모듈)을 저장하는 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체에 저장되는 하나 이상의 프로그램은, 전자 장치(device) 내의 하나 이상의 프로세서에 의해 실행 가능하도록 구성된다(configured for execution). 하나 이상의 프로그램은, 전자 장치로 하여금 본 발명의 청구항 또는 명세서에 기재된 실시 예들에 따른 방법들을 실행하게 하는 명령어(instructions)를 포함한다.
- [0497] 이러한 프로그램(소프트웨어 모듈, 소프트웨어)은 랜덤 액세스 메모리(random access memory), 플래시(flash) 메모리를 포함하는 불휘발성(non-volatile) 메모리, 롬(ROM: Read Only Memory), 전기적 삭제가능 프로그램가능 롬(EEPROM: Electrically Erasable Programmable Read Only Memory), 자기 디스크 저장 장치(magnetic disc storage device), 콤팩트 디스크 롬(CD-ROM: Compact Disc-ROM), 디지털 다목적 디스크(DVDs: Digital

Versatile Discs) 또는 다른 형태의 광학 저장 장치, 마그네틱 카세트(magnetic cassette)에 저장될 수 있다. 또는, 이들의 일부 또는 전부의 조합으로 구성된 메모리에 저장될 수 있다. 또한, 각각의 구성 메모리는 다수 개 포함될 수도 있다.

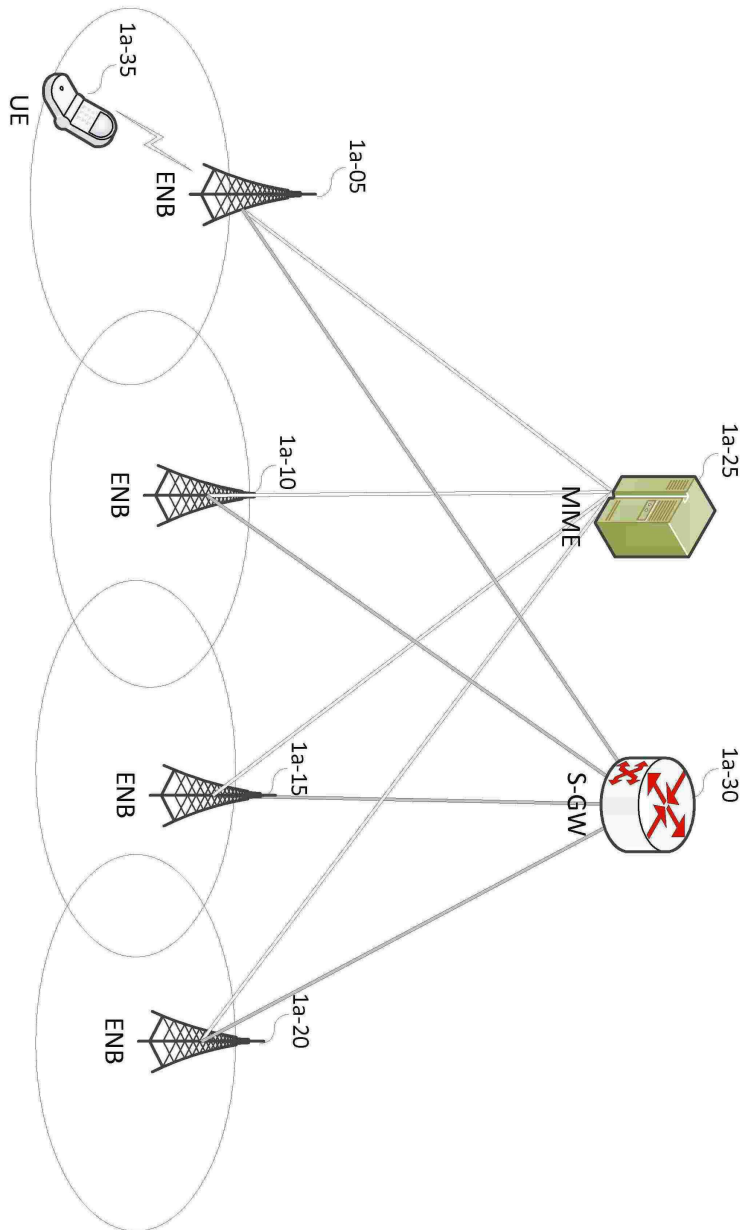
[0498] 또한, 상기 프로그램은 인터넷(Internet), 인트라넷(Intranet), LAN(Local Area Network), WLAN(Wide LAN), 또는 SAN(Storage Area Network)과 같은 통신 네트워크, 또는 이들의 조합으로 구성된 통신 네트워크를 통하여 접근(access)할 수 있는 부착 가능한(attachable) 저장 장치(storage device)에 저장될 수 있다. 이러한 저장 장치는 외부 포트를 통하여 본 발명의 실시 예를 수행하는 장치에 접속할 수 있다. 또한, 통신 네트워크상의 별도의 저장장치가 본 발명의 실시 예를 수행하는 장치에 접속할 수도 있다.

[0500] 상술한 본 발명의 구체적인 실시 예들에서, 발명에 포함되는 구성 요소는 제시된 구체적인 실시 예에 따라 단수 또는 복수로 표현되었다. 그러나, 단수 또는 복수의 표현은 설명의 편의를 위해 제시한 상황에 적합하게 선택된 것으로서, 본 발명이 단수 또는 복수의 구성 요소에 제한되는 것은 아니며, 복수로 표현된 구성 요소라 하더라도 단수로 구성되거나, 단수로 표현된 구성 요소라 하더라도 복수로 구성될 수 있다.

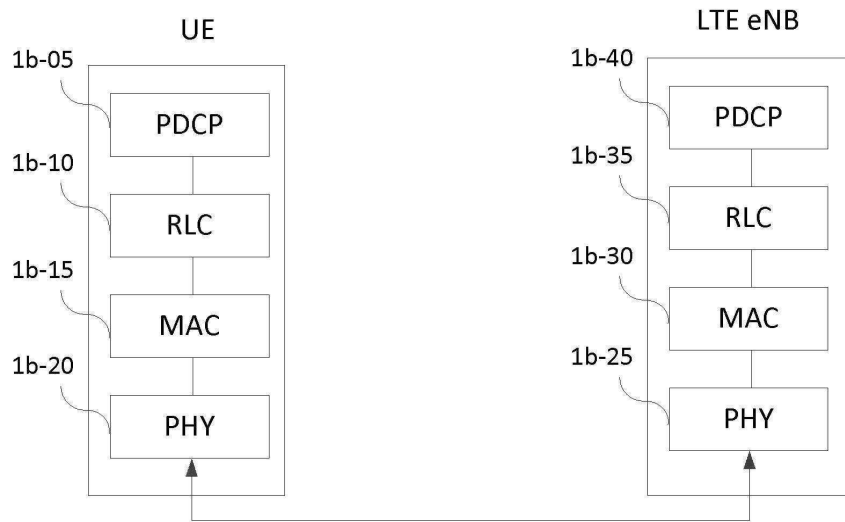
[0501] 한편 본 발명의 상세한 설명에서는 구체적인 실시 예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시 예에 국한되어 정해져서는 아니 되며 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

도면

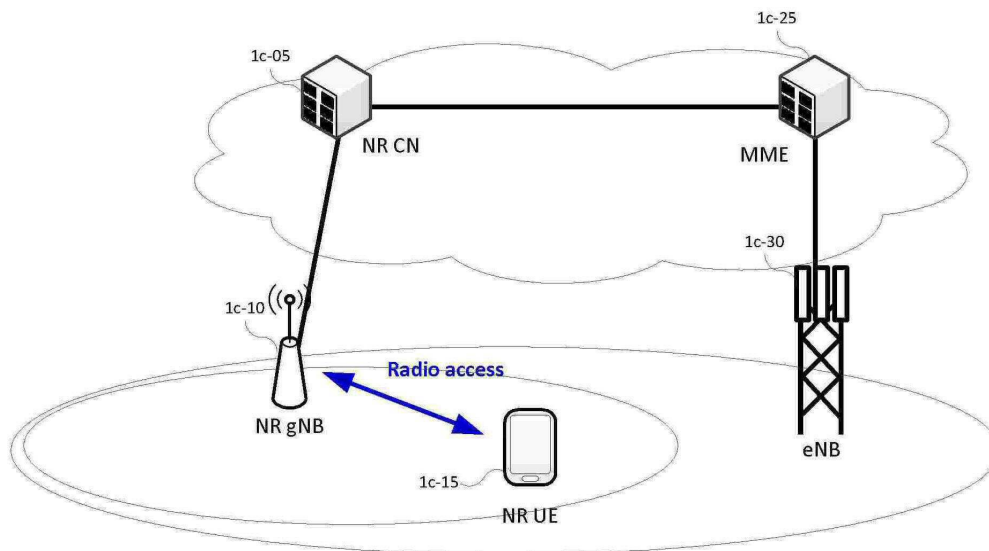
도면1a



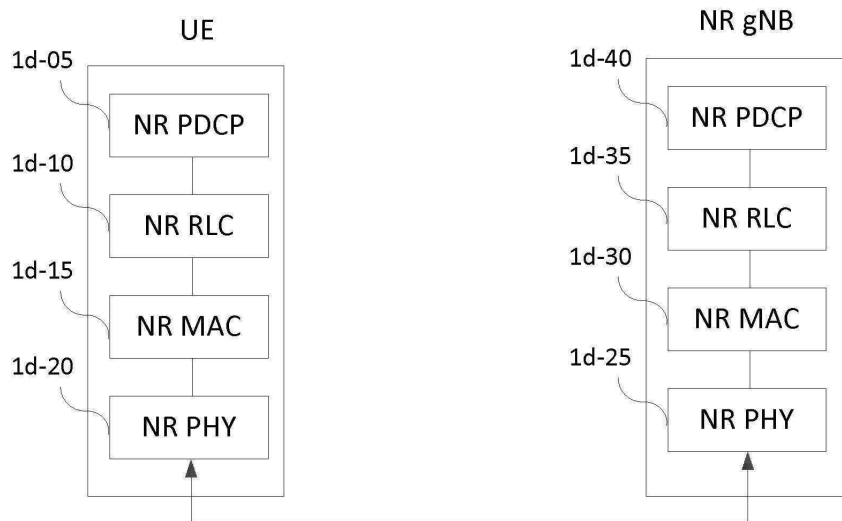
도면1b



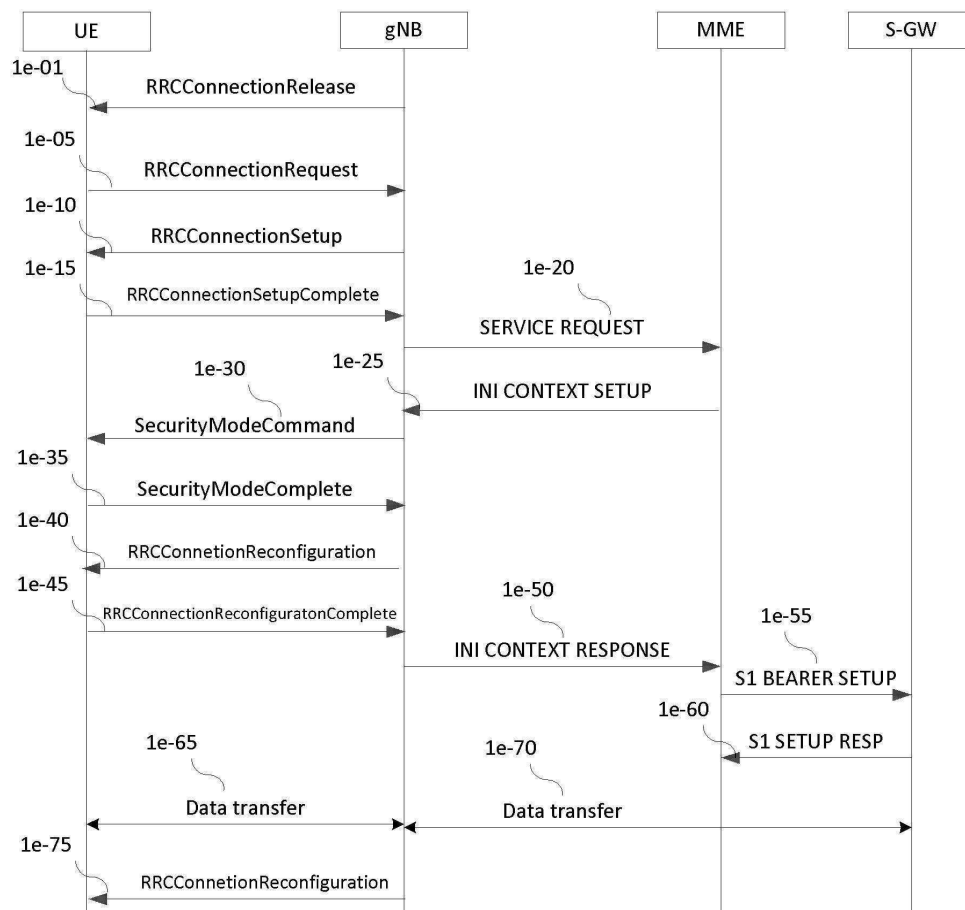
도면1c



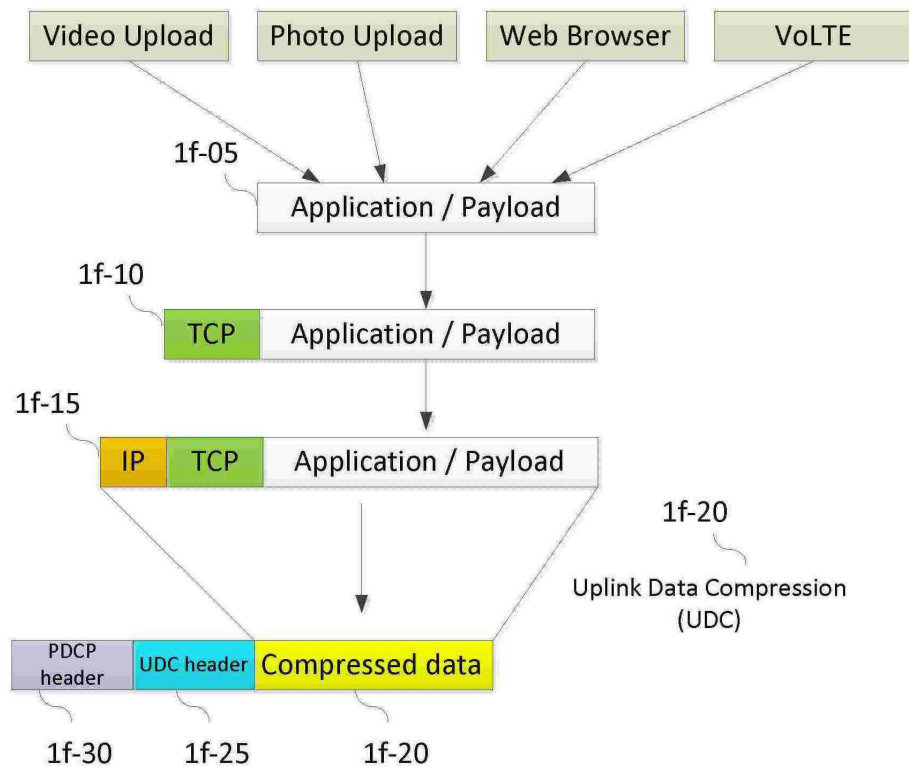
도면1d



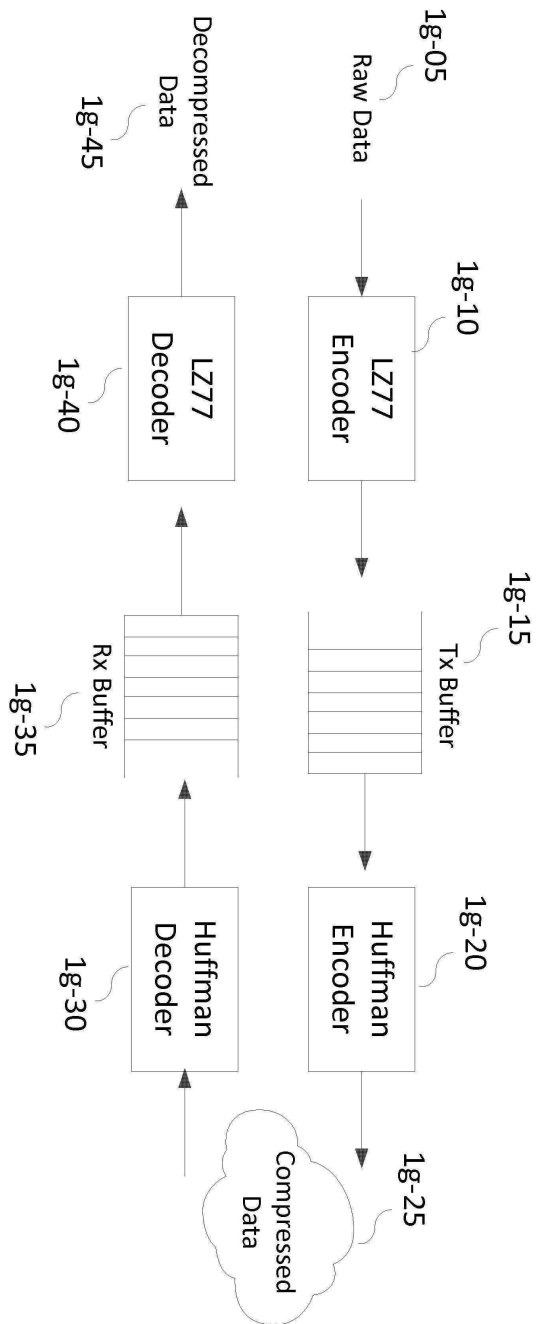
도면1e



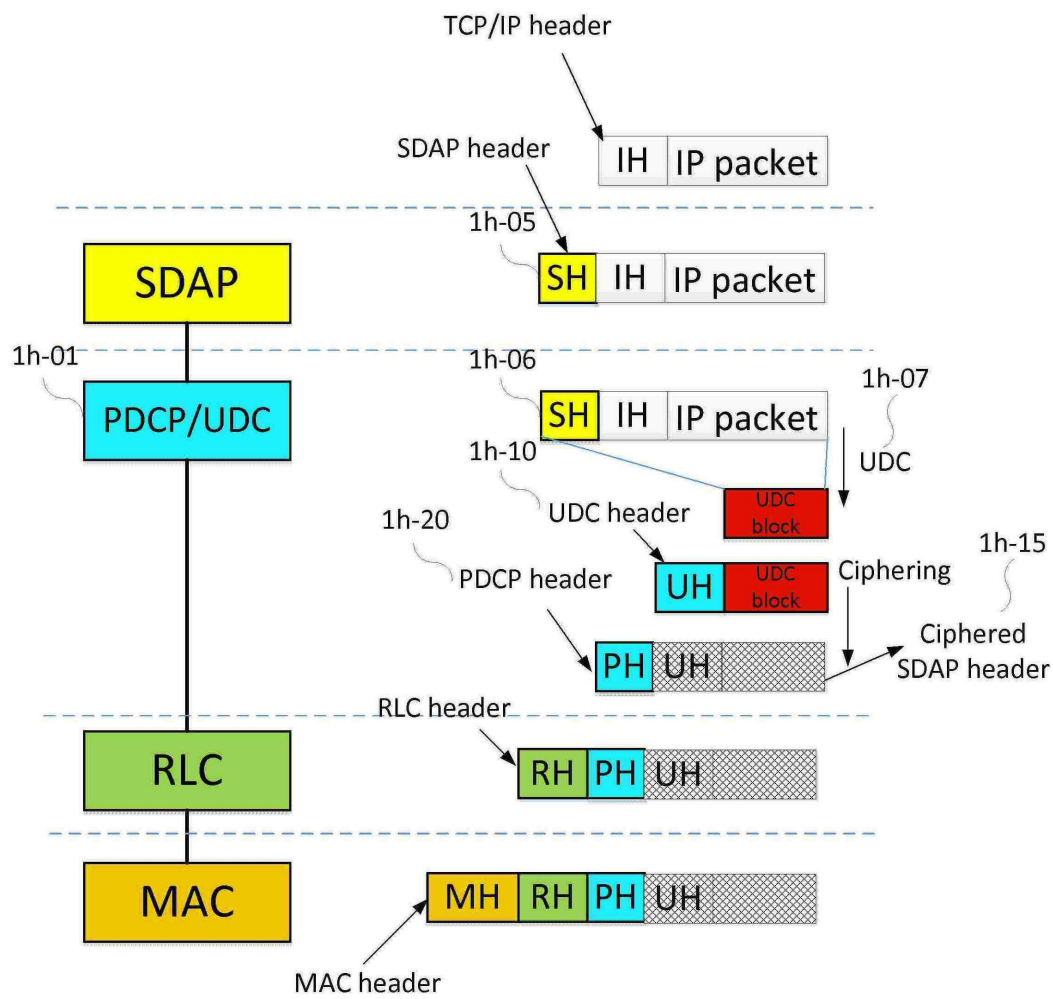
도면1f



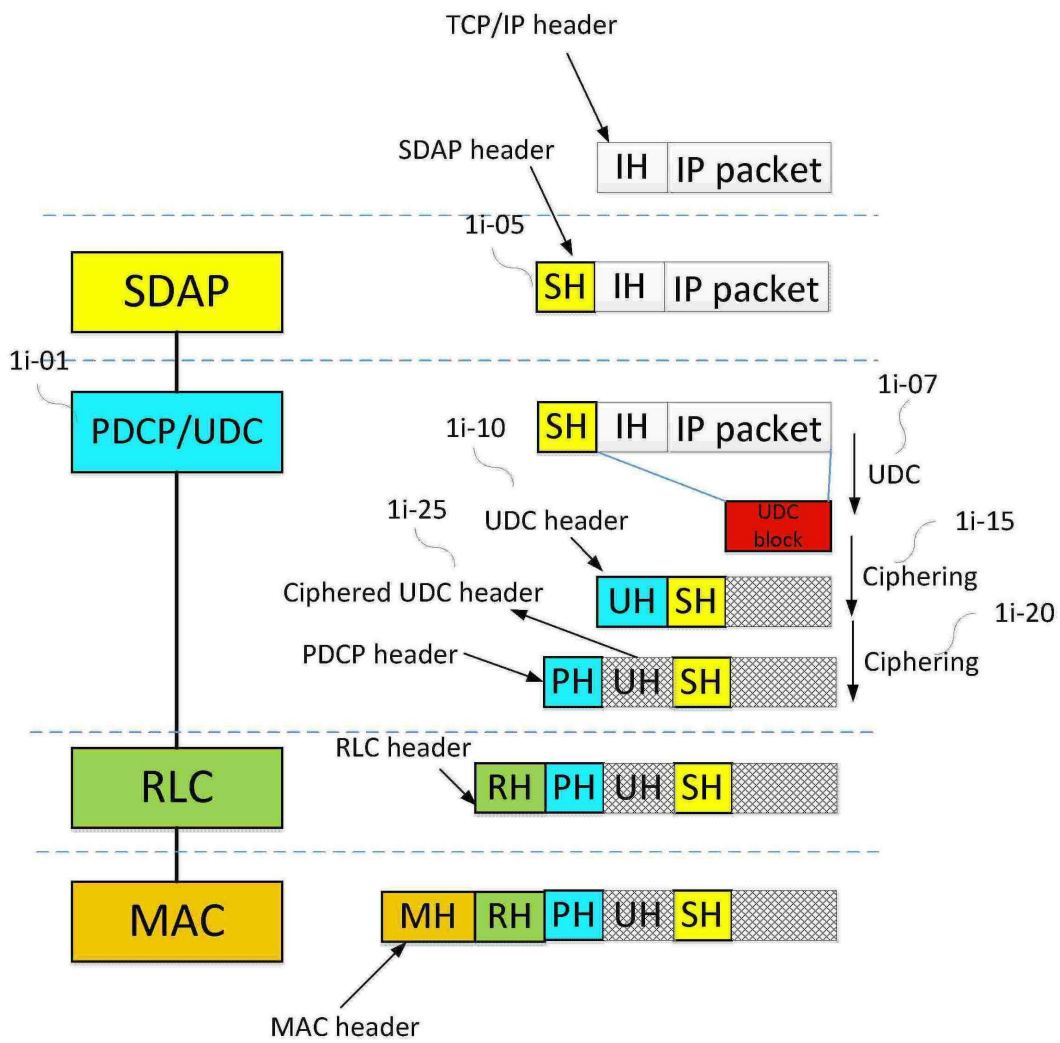
도면 1g



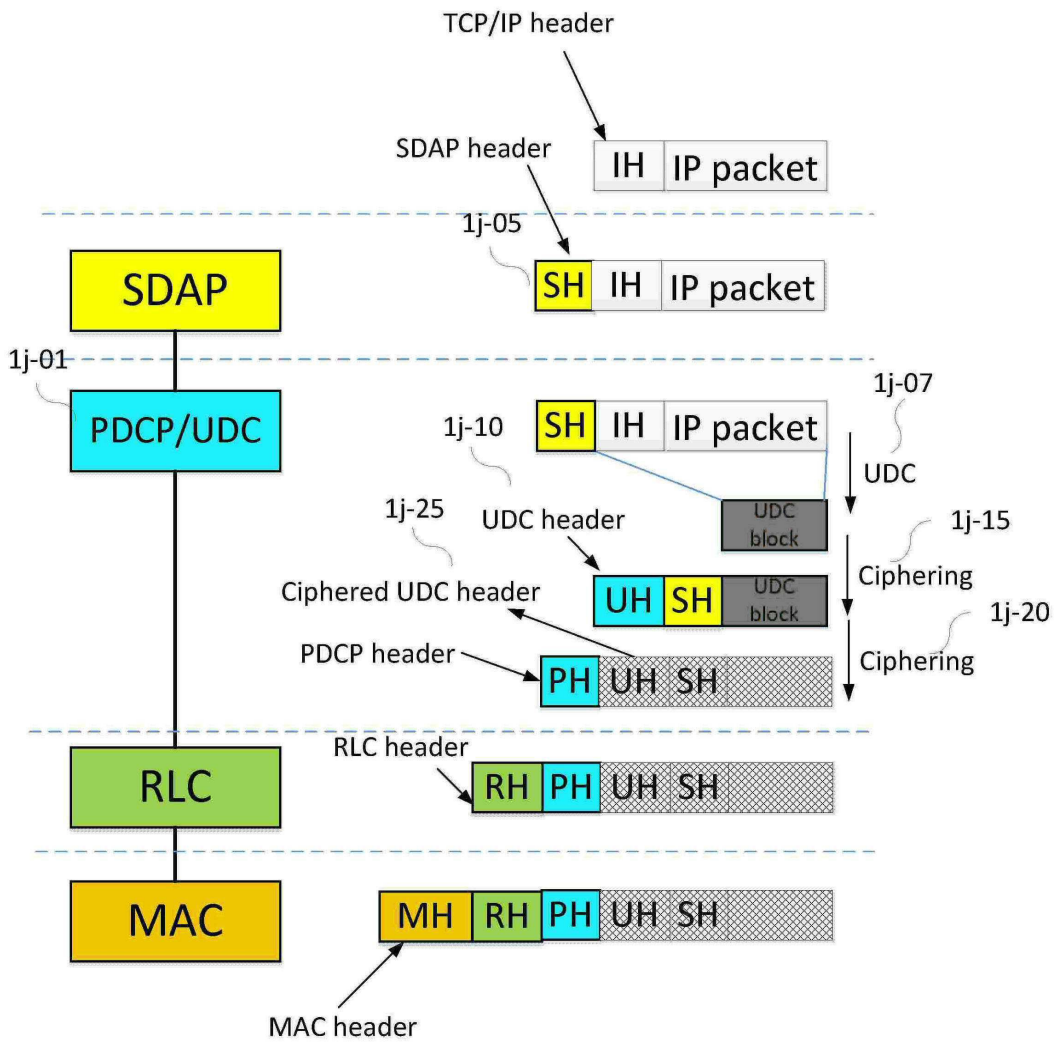
도면 1h



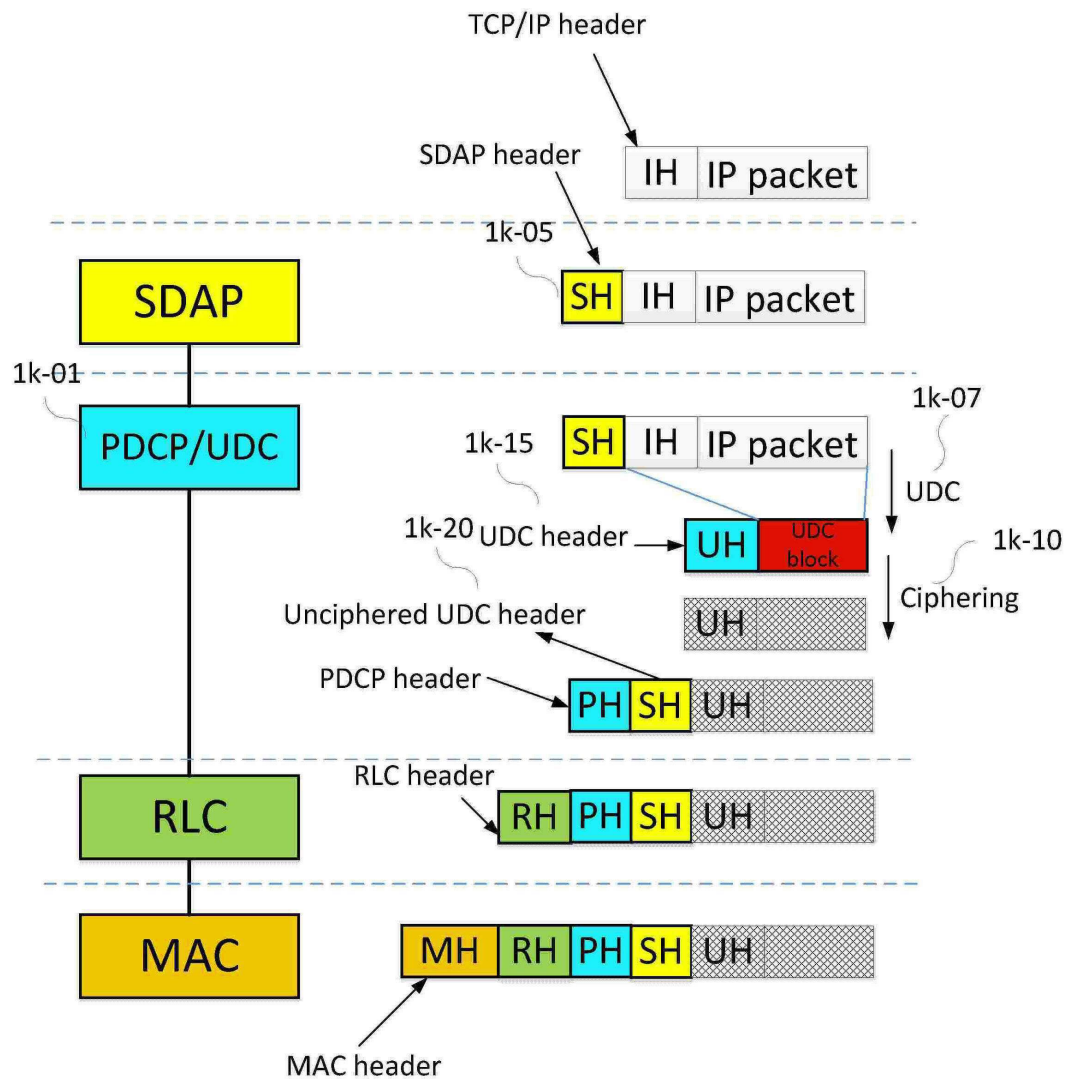
도면1i



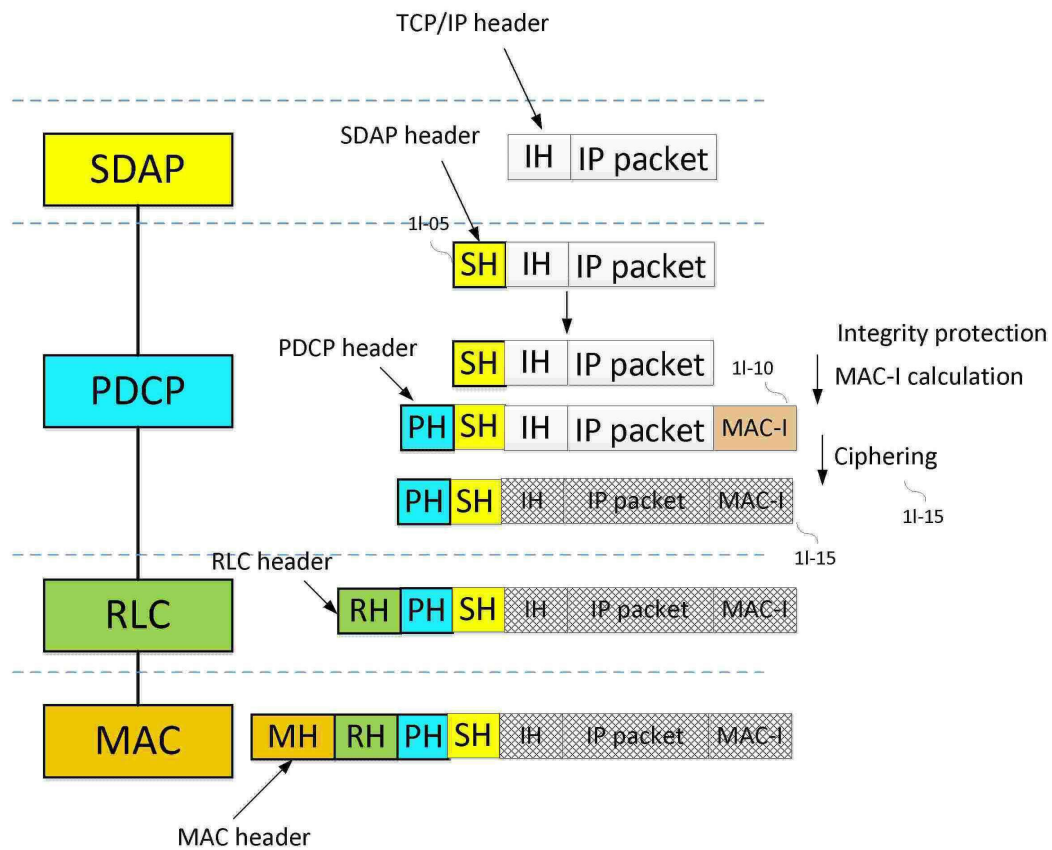
도면1j



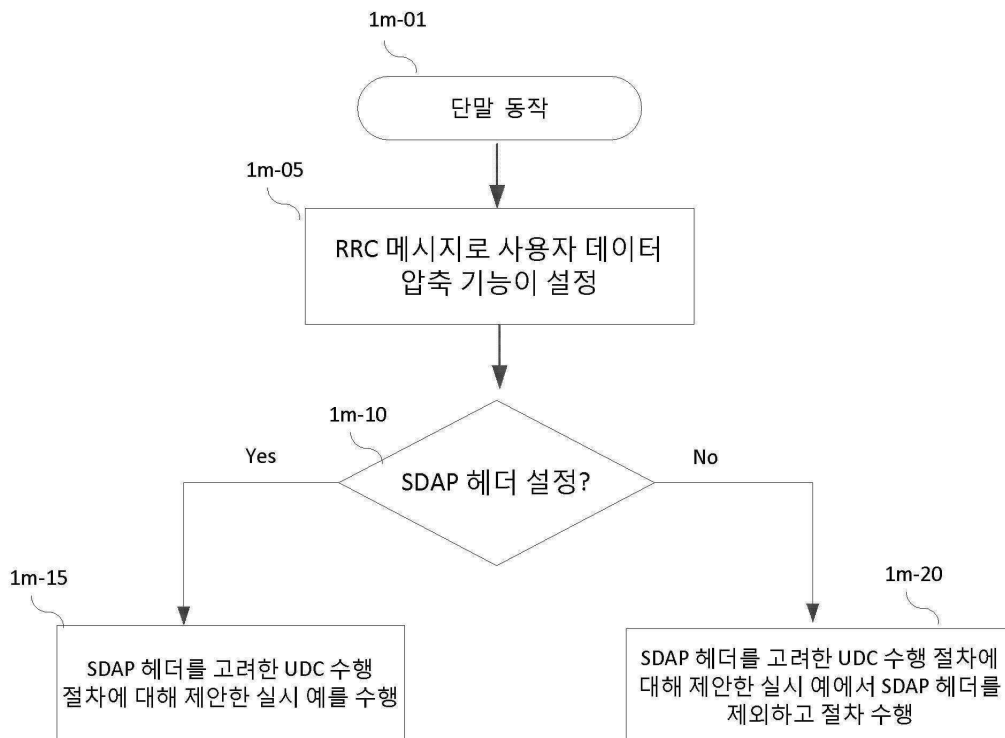
도면 1k



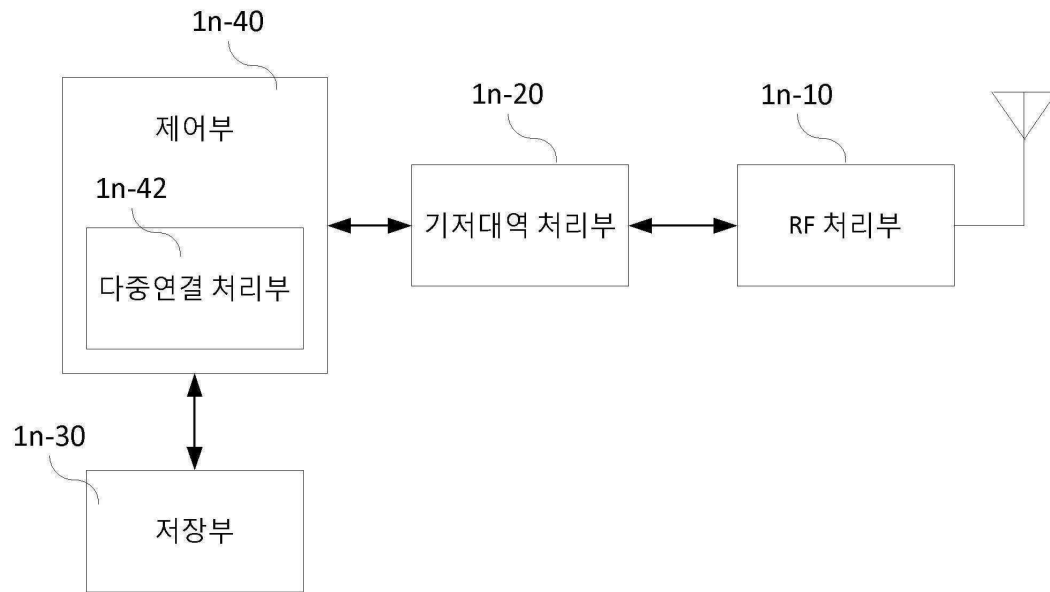
도면11



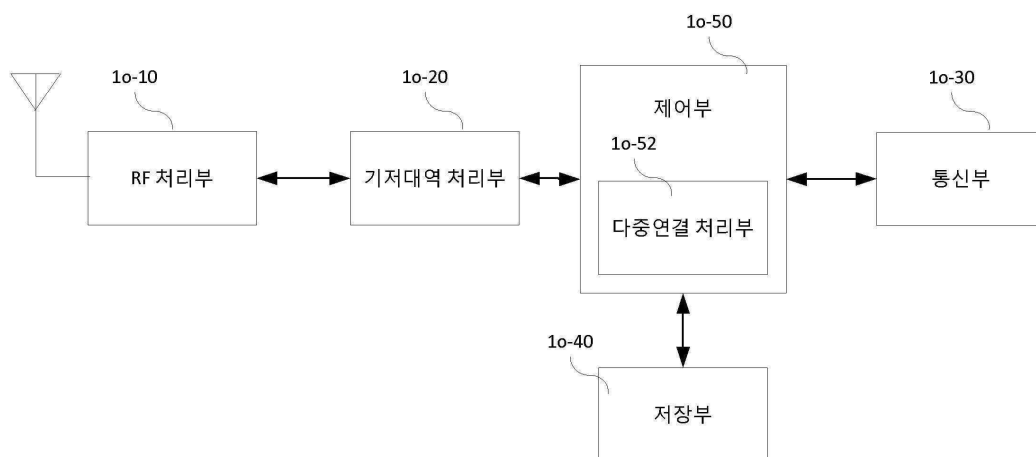
도면1m



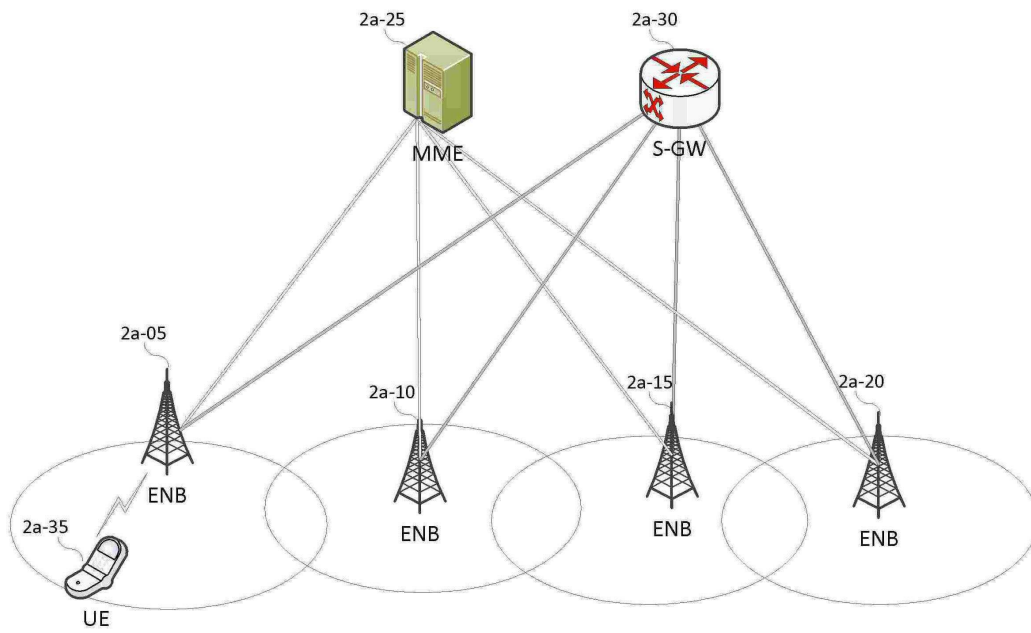
도면1n



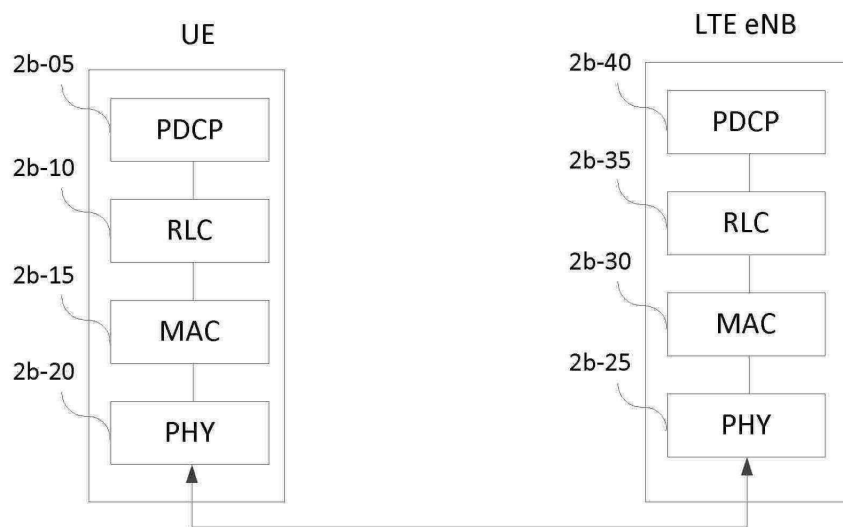
도면1o



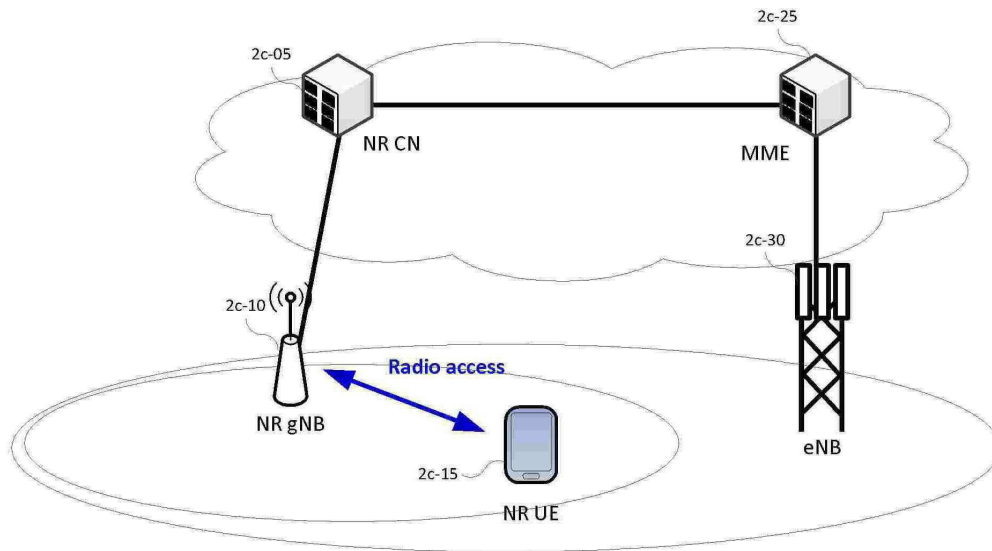
도면2a



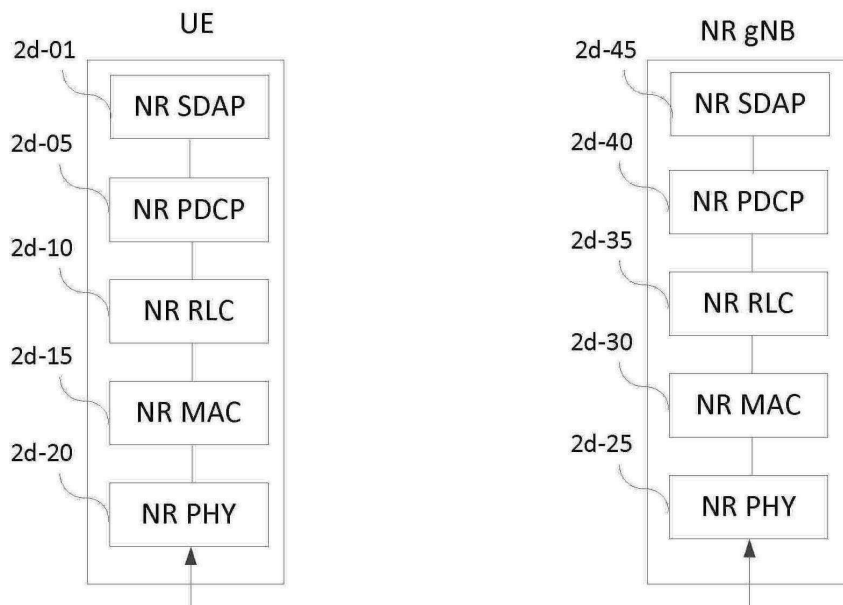
도면2b



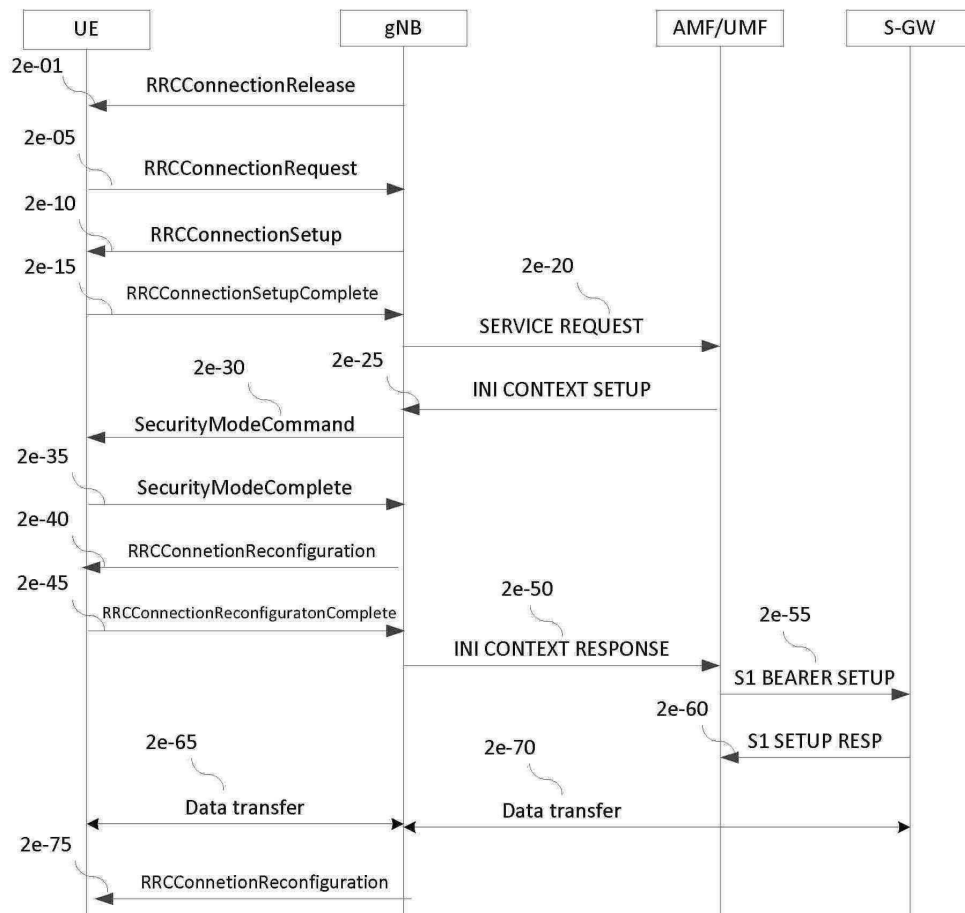
도면2c



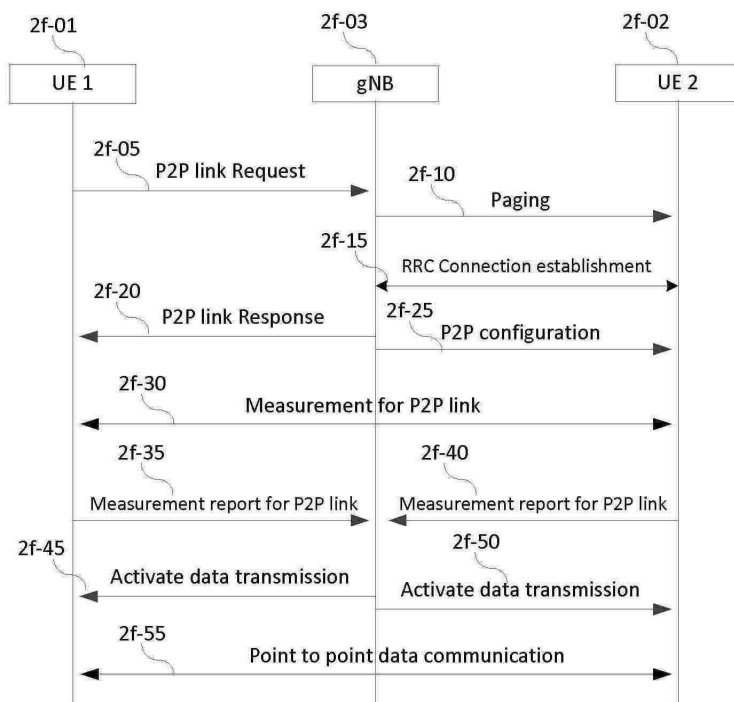
도면2d



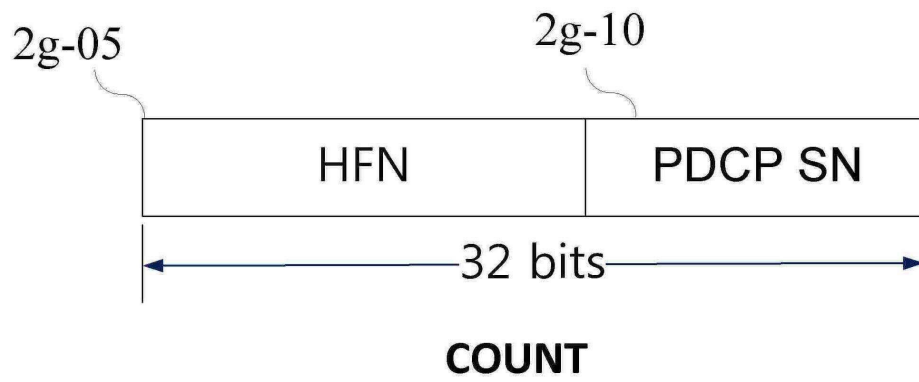
도면2e



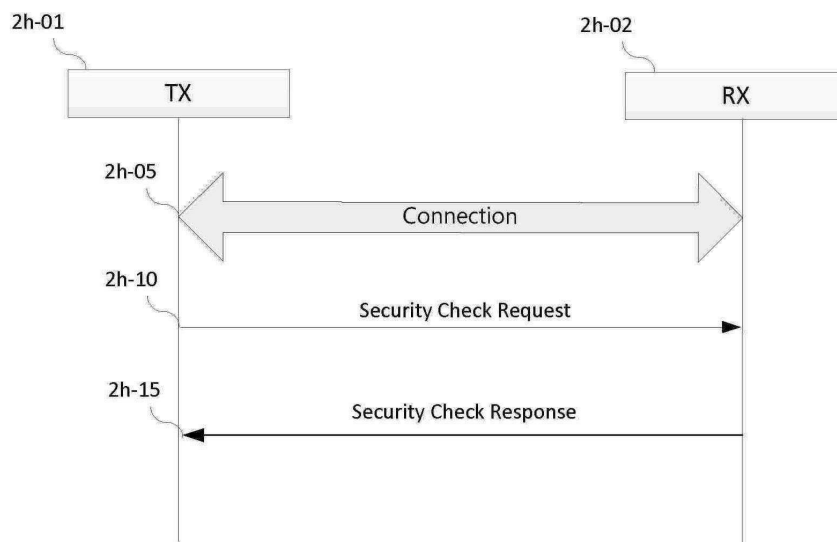
도면2f



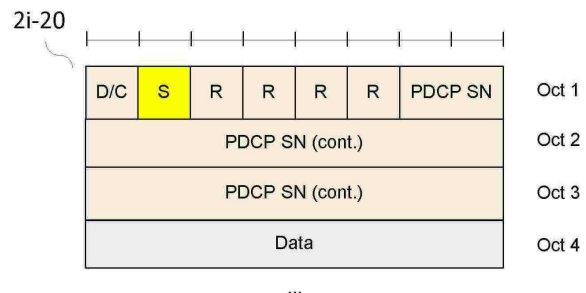
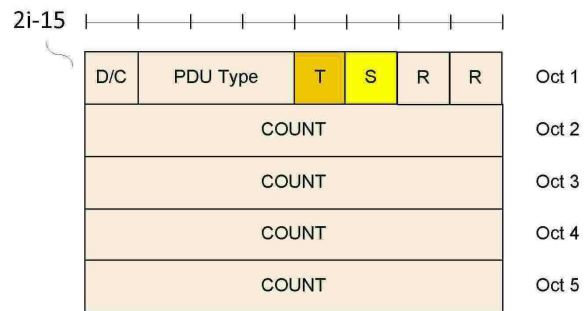
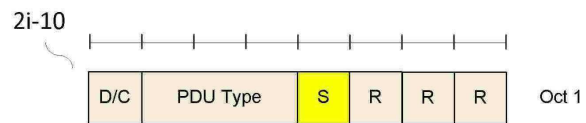
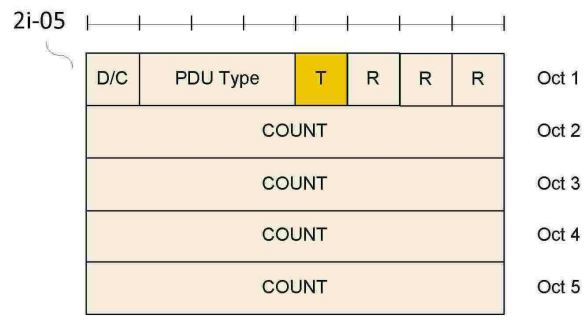
도면2g



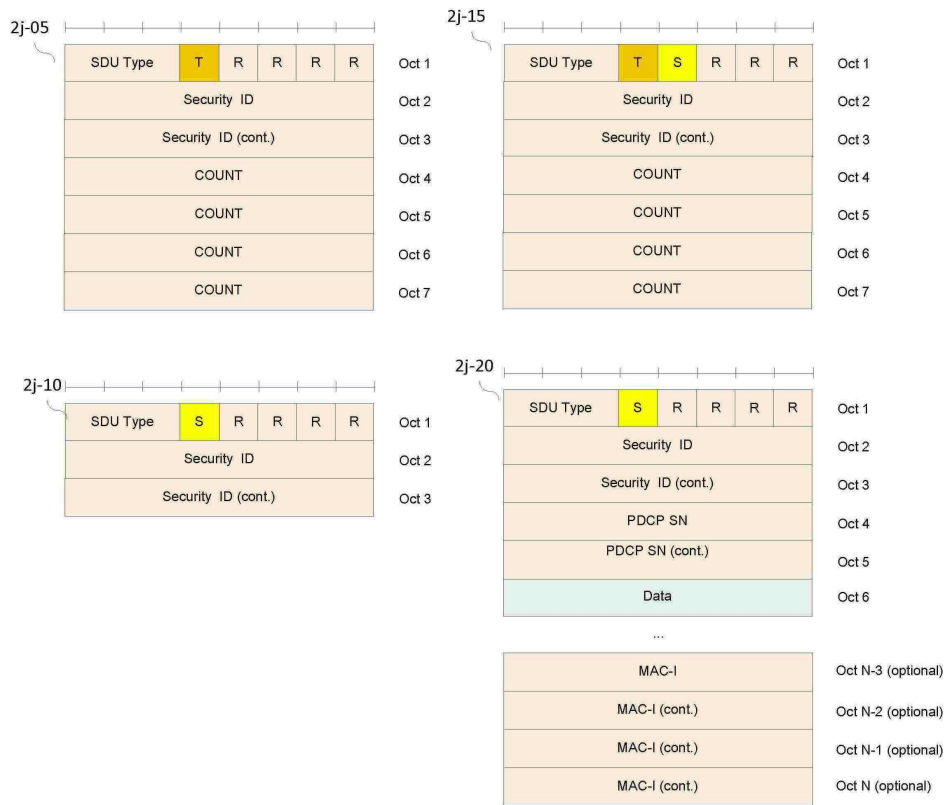
도면2h



도면2i



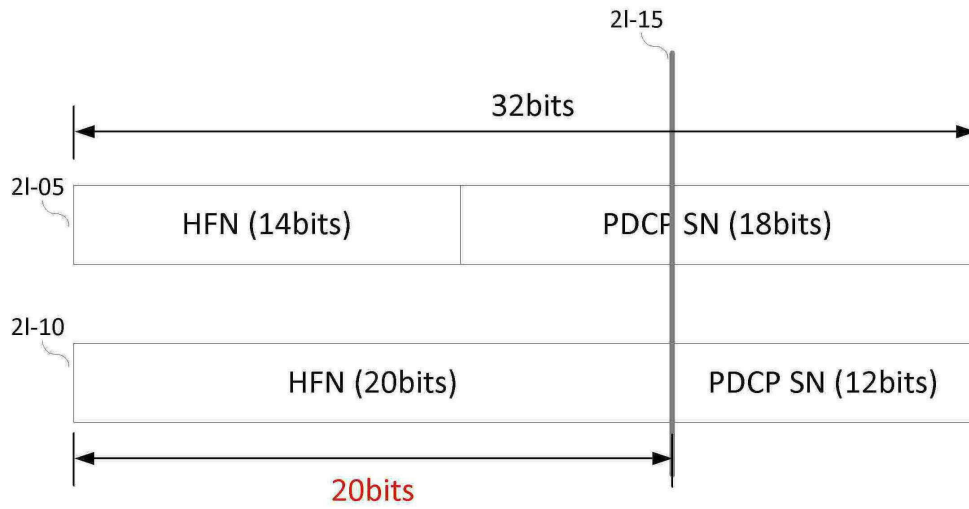
도면2j



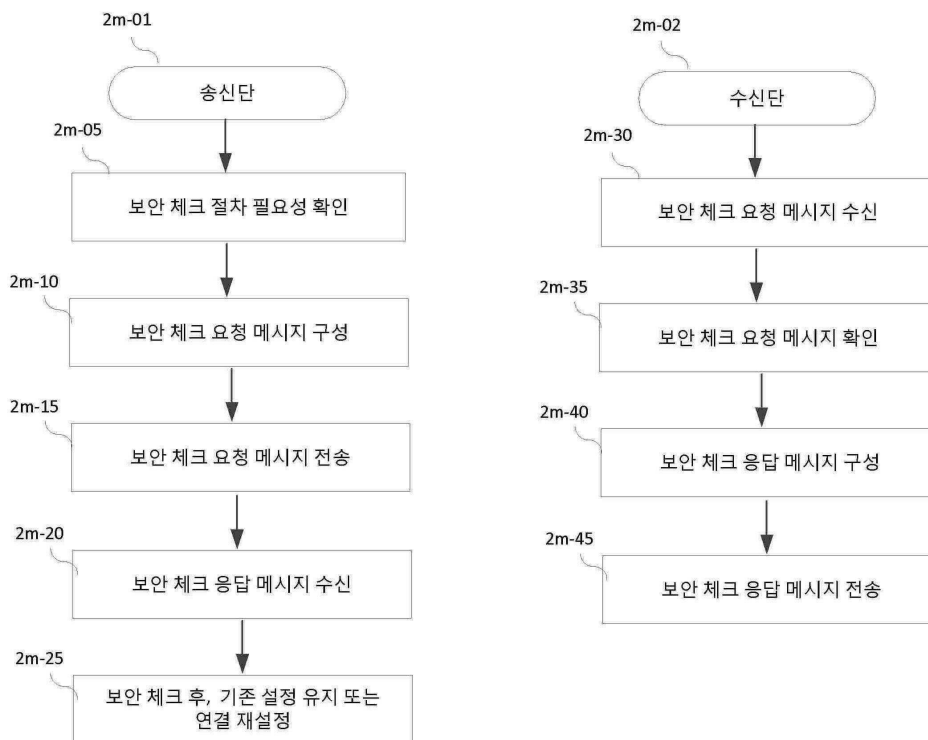
도면2k



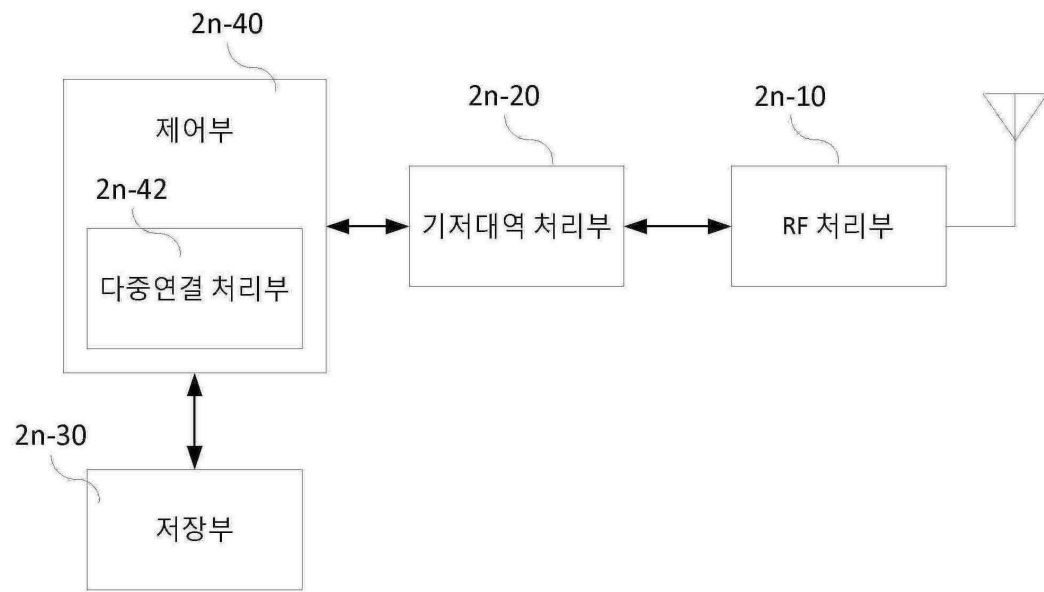
도면21



도면2m



도면 2n



도면 2o

