(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0081355
(43) 공개일자 2010년07월14일

(51) Int. Cl.
H04W 36/02 (2009.01) *H04W 36/08* (2009.01)
(21) 출원번호 10-2010-7011373
(22) 출원일자(국제출원일자) 2008년10월29일
심사청구일자 2010년05월25일
(85) 번역문제출일자 2010년05월25일
(86) 국제출원번호 PCT/US2008/081639
(87) 국제공개번호 WO 2009/058903
국제공개일자 2009년05월07일
(30) 우선권주장
12/259,825 2008년10월28일 미국(US)
60/983,838 2007년10월30일 미국(US)

(71) 출원인
콸콤 인코포레이티드
미국 캘리포니아 샌디에고 모어하우스 드라이브5775 (우 92121-1714)
(72) 발명자
기타조에, 마사토
미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775
호, 사이 이유 던칸
미국 92121 캘리포니아 샌디에고 모어하우스 드라이브 5775
(74) 대리인
남상선

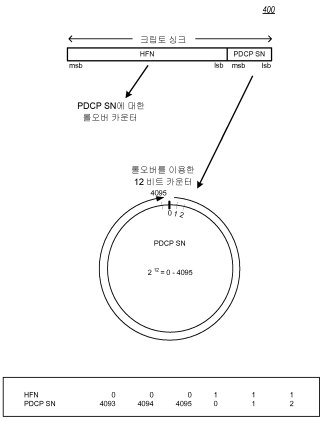
전체 청구항 수 : 총 20 항

(54) 모바일 통신 네트워크들에서의 기지국-간 핸드오버시 HFN 취급을 위한 방법들 및 시스템들

(57) 요 약

이동성에서 발생할 수 있는 네트워크와 이동국들(eNB) 간의 크립토싱크의 동기화-해제를 어드레싱하기 위한 시스템들 및 방법들이 제시된다. 동기화-해제는 HFN과 PDCP 시퀀스 번호(들)를 소스 eNB로부터 타겟 eNB로 포워딩함으로써 해결된다. 주어진 키에 대한 크립토싱크의 재-사용을 회피하기 위해, 초기 카운트(COUNT) 값으로부터의 역방향 오프셋이 타겟 eNB에 의해 이용된다. 이러한 방안들은 네트워크에서의 무선 시그널링 및 카운트 값 취급이 이동국에 투명할 것을 요구하지 않는다.

대 표 도 - 도4



특허청구의 범위

청구항 1

무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(Hyper-Frame Number, HFN) 관련 동기화에 이용되는 방법으로서:

적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(packet data convergence protocol, PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키는 단계; 및

이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키는 단계를 포함하며,

상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호의 정보가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는, HFN 관련 동기화에 이용되는 방법.

청구항 2

제 1 항에 있어서,

상기 소스 및 타겟 기지국들은 eNB들인, HFN 관련 동기화에 이용되는 방법.

청구항 3

제 1 항에 있어서,

상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향(backward) 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하는 단계를 더 포함하는, HFN 관련 동기화에 이용되는 방법.

청구항 4

제 3 항에 있어서,

상기 HFN과 PDCP 값들은 핸드오프시 리셋될 것이 요구되지 않는, HFN 관련 동기화에 이용되는 방법.

청구항 5

제 3 항에 있어서,

새로운 키가 핸드오프시 발생되는, HFN 관련 동기화에 이용되는 방법.

청구항 6

제 3 항에 있어서,

무선(over the air) 시그널링이 핸드오프시 요구되지 않는, HFN 관련 동기화에 이용되는 방법.

청구항 7

제 3 항에 있어서,

키 수명 기간(key life time) 유지는 상기 단말에 투명한, HFN 관련 동기화에 이용되는 방법.

청구항 8

무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(Hyper-Frame Number, HFN) 관련 동기화를 위한 장치로서:

소스 기지국;

타겟 기지국;

상기 소스 기지국과 상기 타겟 기지국 간의 통신 링크; 및

상기 소스 기지국으로부터 상기 타겟 기지국으로 핸드오프되는 단말을 포함하며, 상기 소스 기지국은 상기 통신 링크를 통해 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 상기 타겟 기지국으로 이전시키고, 상기 통신 링크를 통해 이용할 다음 PDCP SN을 상기 타겟 기지국으로 이전시키며,

상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호의 정보가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는, HFN 관련 동기화를 위한 장치.

청구항 9

제 8 항에 있어서,

상기 소스 및 타겟 기지국들은 eNB들인, HFN 관련 동기화를 위한 장치.

청구항 10

제 8 항에 있어서,

카운트 유지는 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 수행되는, HFN 관련 동기화를 위한 장치.

청구항 11

제 8 항에 있어서,

상기 HFN 및 PDCP 값들은 핸드오프시 리셋될 것이 요구되지 않는, HFN 관련 동기화를 위한 장치.

청구항 12

제 10 항에 있어서,

새로운 키가 핸드오프시 발생되는, HFN 관련 동기화를 위한 장치.

청구항 13

제 10 항에 있어서,

무선 시그널링이 핸드오프시 요구되지 않는, HFN 관련 동기화를 위한 장치.

청구항 14

제 10 항에 있어서,

키 수명 시간 유지는 상기 단말에 투명한, HFN 관련 동기화를 위한 장치.

청구항 15

무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(HFN) 관련 동기화에 이용되는 장치로서:

적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키고; 그리고

이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위해 구성되는 처리기; 및

데이터를 저장하기 위해 상기 처리기에 접속되는 메모리를 포함하며,

상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과

PDCP 시퀀스 번호의 정보가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는, HFN 관련 동기화에 이용되는 장치.

청구항 16

제 15 항에 있어서,

상기 처리기는 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하기 위해 추가로 구성되는, HFN 관련 동기화에 이용되는 장치.

청구항 17

무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(HFN) 관련 동기화에 이용되는 장치로서:

적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키기 위한 수단; 및

이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위한 수단을 포함하며,

상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호의 정보가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는, HFN 관련 동기화에 이용되는 장치.

청구항 18

적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키기 위한 코드; 및

이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위한 코드를 포함하는, 컴퓨터로-읽을 수 있는 매체를 포함하는 컴퓨터 프로그램 물건으로서, 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호의 정보가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는, 컴퓨터 프로그램 물건.

청구항 19

제 18 항에 있어서,

상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하기 위한 코드를 더 포함하는, 컴퓨터 프로그램 물건.

청구항 20

제 18 항에 있어서,

상기 HFN 및 PDCP 값들이 핸드오프시 리셋되지 않도록 하기 위한 코드를 더 포함하는, 컴퓨터 프로그램 물건.

명 세 서

기 술 분 야

[0001] 본 개시물은 일반적으로 무선 통신의 암호화 무결성, 그리고 더 특정하게는 모바일 시스템들에서의 기지국들 간의 핸드오프 동안 하이퍼-프레임 번호(Hyper-frame Number, HFN) 관련 취급에 관련된다.

배 경 기 술

[0002] 무선 통신 시스템들이 널리 구축되어 음성, 데이터 등과 같은 다양한 통신 컨텐트를 제공한다. 이러한 시스템들은 가용 시스템 자원들(예컨대, 대역폭 및 송신 전력)을 공유함으로써 다수의 사용자들과의 통신을 지원할 수 있는 다중-접속 시스템들일 수 있다. 그러한 다중-접속 시스템들의 예들은 코드 분할 다중 접속(CDMA) 시스템들, 시 분할 다중 접속(TDMA) 시스템들, 주파수 분할 다중 접속(FMDA) 시스템들, 3GPP 롱 텀 에볼루션(LTE) 시스템들, 및 직교 주파수 분할 다중 접속(OFDMA) 시스템들을 포함한다.

[0003] 일반적으로, 무선 다중-접속 통신 시스템은 다수의 무선 단말들에 대한 통신을 동시에 지원할 수 있다. 각 단말은 순방향 및 역방향 링크들 상에서의 송신들을 통해 하나 이상의 기지국들과 통신한다. 순방향 링크(또는 다운링크)는 기지국들로부터 단말들로의 통신 링크를 지칭하고, 역방향 링크(또는 업링크)는 단말들로부터 기지국들로의 통신 링크를 지칭한다. 본 통신 링크는 단일-입력-단일-출력, 다중-입력-단일-출력 또는 다중-입력-다중-출력(MIMO) 시스템을 통해 수립될 수 있다.

[0004] MIMO 시스템은 다수의(N_T) 송신 안테나들 및 다수의(N_R) 수신 안테나들을 데이터 송신에 채택한다. 상기 N_T개의 송신 및 N_R개의 수신 안테나들에 의해 형성되는 MIMO 채널은 N_S개의 독립 채널들로 분해될 수 있으며, 이들은 또한 공간 채널들로 지칭되고, 여기서 $N_S \leq \min\{N_T, N_R\}$이다. N_S개의 독립 채널들 각각은 차원(dimension)에 대응한다. MIMO 시스템은 상기 다수의 송신 및 수신 안테나들에 의해 생성되는 추가적인 차원성들이 활용된다면 개선된 성능(예컨대, 더 높은 스루풋 및/또는 더 나은 신뢰도)을 제공할 수 있다.

[0005] MIMO 시스템은 시 분할 이중화(TDD) 및 주파수 분할 이중화(FDD) 시스템들을 지원한다. TDD 시스템에서, 순방향 및 역방향 링크 송신들은 동일 주파수 영역 상에 존재하여 가역성 원리가 역방향 링크 채널로부터 순방향 링크 채널의 추정을 허용한다. 이는 액세스 포인트로 하여금 다수의 안테나들이 상기 액세스 포인트에서 이용가능할 때 순방향 링크 상에서의 송신 빔포밍 이득을 추출할 수 있게 한다.

발명의 내용

[0006] 본 개시물은 모바일 시스템에서 기지국들 간의 핸드오프 동안 암호화/복호화 파라미터들을 관리하기 위한 시스템들 및 방법들, 및 이들의 변형들에 관한 것이다.

[0007] 본 개시물의 다양한 양상들 중 하나로, 무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(Hyper-Frame Number, HFN) 관련 동기화에 이용되는 방법이 제시되며, 상기 방법은: 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(packet data convergence protocol, PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키는 단계; 및 이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키는 단계를 포함하며, 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 한다.

[0008] 상기 개시물의 다양한 양상들 중 하나로, 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향(backward) 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하는 단계를 더 포함하는, 상기 개시된 방법이 제시된다.

[0009] 본 개시물의 다양한 양상들 중 하나로, 무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(Hyper-Frame Number, HFN) 관련 동기화를 위한 장치로서: 소스 기지국; 타겟 기지국; 상기 소스 기지국과 상기 타겟 기지국 간의 통신 링크; 및 상기 소스 기지국으로부터 상기 타겟 기지국으로 핸드오프되는 단말을 포함하며, 상기 소스 기지국은 상기 통신 링크를 통해 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 상기 타겟 기지국으로 이전시키고, 상기 통신 링크를 통해 이용할 다음 PDCP SN을 상기 타겟 기지국으로 이전시키며, 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하는 무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(Hyper-Frame Number, HFN) 관련 동기화를 위한 장치가 제시된다.

[0010] 본 개시물의 다양한 양상들 중 하나로, 상기 개시된 장치가 제시되며, 여기서 카운트 유지는 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및

최종 복호화 HFN과 PDCP에 기초하여 수행된다.

[0011] 본 개시물의 다양한 양상들 중 하나로, 무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(HFN) 관련 동기화에 이용되는 장치가 제시되며, 상기 장치는: 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키고; 이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위해 구성되는 처리기를 포함하며, 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 하고; 및 데이터를 저장하기 위해 상기 처리기에 접속되는 메모리를 포함한다.

[0012] 본 개시물의 다양한 양상들 중 하나로, 상기 기재된 장치가 제시되며, 여기서 상기 처리기는 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하기 위해 추가로 구성된다.

[0013] 본 개시물의 다양한 양상들 중 하나로, 무선 통신 시스템에서 핸드오프 동안 기지국들 간의 하이퍼-프레임 번호(HFN) 관련 동기화에 이용되는 장치가 제시되며, 상기 장치는: 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키기 위한 수단; 이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위한 수단을 포함하며, 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 한다.

[0014] 본 개시물의 다양한 양상들 중 하나로, 적어도 최종 암호화 HFN과 패킷 데이터 컨버전스 프로토콜(PDCP) 시퀀스 번호(SN) 및 최종 복호화 HFN과 PDCP 시퀀스 번호를 소스 기지국으로부터 타겟 기지국으로 이전시키기 위한 코드; 및 이용할 다음 PDCP SN을 상기 소스 기지국으로부터 상기 타겟 기지국으로 이전시키기 위한 코드를 포함하는, 컴퓨터로-읽을 수 있는 매체를 포함하는 컴퓨터 프로그램 물건이 제시되며, 여기서 상기 이전되는 정보는 상기 소스 기지국에 의해 전송되는 상기 최종 HFN과 PDCP 시퀀스 번호의 이후의 HFN과 PDCP 시퀀스 번호가 상기 타겟 기지국에 의해 수신되지 않는다면 상기 타겟 기지국으로 하여금 상기 소스 기지국으로부터 핸드 오프되는 단말에 대한 상기 HFN과 PDCP 시퀀스 번호(들)의 실질적인 연속성을 제공할 수 있도록 한다.

[0015] 본 개시물의 다양한 양상들 중 하나로, 상기 타겟 기지국에 의해 이용되는 카운트 값으로부터의 역방향 오프셋을 이용함으로써 적어도 상기 최종 암호화 HFN과 PDCP 및 최종 복호화 HFN과 PDCP에 기초하여 카운트 유지를 수행하기 위한 코드를 더 포함하는, 상기 기재된 컴퓨터 프로그램 물건이 제시된다.

도면의 간단한 설명

[0016] 도 1은 일 실시예에 따른 다중 접속 무선 통신 시스템을 나타낸다.

도 2는 통신 시스템의 블록도이다.

도 3은 모바일 시스템용 암호화 및 복호화 방식의 블록도이다.

도 4는 HFN 대 PDCP SN 관계의 도시이다.

도 5는 두 개의 eNB들 간의 핸드오프 파라미터들의 도시이다.

도 6A-B는 HFN/PDCP SN 제어를 위한 오프셋 방식들의 도시들이다.

도 7은 예시적인 프로세스를 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 다양한 실시예들이 도면들을 참조로 이제 기재되며, 여기서 동일한 참조 번호들은 전반적으로 동일한 구성요소들을 지칭하는데 이용된다. 다음의 기재에서, 설명 목적들을 위해, 다수의 특정 세부사항들이 하나 이상의 실시예들의 총괄적 이해를 제공하기 위해 제시된다. 그러나, 그러한 실시예(들)가 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 수 있다. 다른 보기들로, 기지의 구조들 및 장치들은 하나 이상의 실시예들을 기재하

는 것을 용이하기 하기 위해 블록도 형태로 도시된다.

[0018] 본 출원에서 이용되는 바로서, 용어들 "컴포넌트", "모듈", "시스템" 등은 컴퓨터-관련 엔티티, 하드웨어, 펌웨어, 하드웨어와 소프트웨어의 조합, 소프트웨어, 또는 실행 소프트웨어를 지칭하고자 하는 것이다. 예를 들어, 컴포넌트는 처리기 상에서 실행하는 프로세스, 처리기, 객체, 실행가능, 실행 스레드, 프로그램, 및/또는 컴퓨터일 수 있지만, 이에 한정되는 것은 아니다. 설명으로써, 컴퓨팅 장치 상에서 실행하는 애플리케이션과 컴퓨팅 장치 모두가 컴포넌트일 수 있다. 하나 이상의 컴포넌트들이 프로세스 및/또는 실행 스레드 내부에 상주할 수 있으며 컴포넌트는 하나의 컴퓨터 상에서 국부화되고 그리고/또는 둘 이상의 컴퓨터들 사이에서 분산될 수 있다. 추가로, 이러한 컴포넌트들은 저장된 다양한 데이터 구조들을 갖는 다양한 컴퓨터로 읽을 수 있는 매체로부터 실행할 수 있다. 상기 컴포넌트들은 하나 이상의 데이터 패킷들(예컨대, 신호를 통해 다른 시스템과 로컬 시스템, 분산 시스템에서, 및/또는 인터넷과 같은 네트워크를 통해 다른 컴포넌트와 상호작용하는 하나의 컴포넌트로부터의 데이터)을 갖는 신호에 따라서와 같이 국부 및/또는 원격 프로세스들을 통해 통신할 수 있다.

[0019] 또한, 다양한 실시예들이 액세스 단말과 관련하여 기재된다. 액세스 단말은 시스템, 가입자 유닛, 가입자국, 이동국, 모바일, 원격국, 원격 단말, 모바일 장치, 사용자 단말, 단말, 무선 통신 장치, 사용자 에이전트, 사용자 장치 또는 사용자 장비(UE)로 지칭될 수 있다. 액세스 단말은 셀룰러 전화, 무선 전화, 세션 개시 프로토콜(SIP) 전화, 무선 로컬 루프(WLL) 스테이션, 개인 휴대 단말기(PDA), 무선 접속 능력을 구비한 휴대용 장치, 컴퓨팅 장치, 또는 무선 모뎀을 활용하거나 무선 모뎀에 접속되는 다른 처리 장치일 수 있다. 또한, 다양한 실시예들이 여기서 기지국과 관련하여 기재된다. 기지국은 액세스 단말(들)과 통신하는데 활용될 수 있으며 또한 액세스 포인트, 노드 B, eNode B(eNB), 또는 다른 어떠한 용어로 지칭될 수 있다. 이하에 제공되는 발명을 실시하기 위한 구체적인 내용의 정황에 따라, 채택되는 관련 통신 시스템에 따라서 용어 노드 B는 eNB로 대체되고 그리고/또는 그 역도 성립할 수 있다.

[0020] 또한, 여기서 제시된 다양한 양상들은 표준 프로그래밍 및/또는 엔지니어링 기술을 이용하여 방법, 장치, 또는 제품(article)으로 구현될 수 있다. 여기서 이용되는 바로서 용어 "제품"은 임의의 컴퓨터 판독가능한 장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터 판독가능한 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, 컴팩트 디스크(CD), 디지털 다기능 디스크(DVD), 등), 스마트 카드들, 및 플래쉬 메모리 장치들(예를 들면, 소거가능 프로그램가능 읽기 전용 메모리(EEPROM), 카드, 스틱, 키 드라이브, 등)를 포함할 수 있지만, 이들로 제한되는 것은 아니다. 또한, 여기서 제시되는 다양한 저장 매체는 정보를 저장하기 위한 하나 이상의 장치 및/또는 다른 기계-판독가능한 매체를 포함한다. 용어 "기계-판독가능한 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

[0021] 여기에 기재된 기술들은 코드 분할 다중 접속(CDMA), 다중-반송파 CDMA(MC-CDMA), 광대역 CDMA(W-CDMA), 고-속 패킷 접속(HSPA, HSPA+), 시 분할 다중 접속(TDMA), 주파수 분할 다중 접속(FDMA), 직교 주파수 분할 다중 접속(OFDMA), 단일 반송파 주파수 영역 다중화(SC-FDMA) 및 다른 다중 접속 시스템들/기술들과 같은 다양한 무선 통신 시스템들에 이용될 수 있다. 용어 "시스템"과 "네트워크"는 상호교환적으로 이용될 수 있다. CDMA 네트워크는 Universal Terrestrial Radio Access(UTRA), cdma2000 등과 같은 무선 기술을 구현할 수 있다. UTRA는 광대역-CDMA(W-CDMA) 및 Low Chip Rate (LCR)를 포함할 수 있다. cdma2000은 IS-2000, IS-95 및 IS-856 표준들을 망라한다. TDMA 네트워크는 Global SYstem for Mobile Communications (GSM)과 같은 무선 기술을 구현할 수 있다. OFDMA 네트워크는 Evolved UTRA(E-UTRA), IEEE 802.11, IEEE 802.16, IEEE 802.20, Flash-OFDM® 등과 같은 무선 기술을 구현할 수 있다. UTRA 및 E-UTRA는 Universal Mobile Telecommunication System (UMTS)의 일부이다. 3GPP 롱 텀 에볼루션(LTE)은 E-UTRA를 이용하는 UMTS의 대두되는 릴리즈이다. UTRA, E-UTRA, UMTS, LTE 및 GSM은 "제 3 세대 파트너십 프로젝트"(3GPP)로 명명되는 조직으로부터의 문헌들에 기재된다. cdma2000은 "제 3 세대 파트너십 프로젝트 2"(3GPP2)로 명명되는 조직으로부터의 문헌들에 기재된다. 이러한 다양한 무선 기술들 및 표준들은 당해 기술분야에 공지되어 있다. 명확화를 위해, 상기 기술들의 어떠한 양상들은 이하에서 LTE에 대해 기재되며, LTE 용어가 이하의 기재의 대부분에서 이용된다.

[0022] 단일 반송파 변조 및 주파수 영역 등화를 활용하는, 단일 반송파 주파수 분할 다중 접속(SC-FDMA)는 통신 기술이다. SC-FDMA는 OFDMA 시스템들과 유사한 성능 및 본질적으로 동일한 총괄적 복잡도를 갖는다. SC-FDMA 신호는 본질적인 단일 반송파 구조 때문에 더 낮은 첨두치-대평균 전력 비(PAPR)를 갖는다. SC-FDMA는, 특히 더 낮은 PAPR이 송신 전력 효율성에 관련하여 모바일 단말에 매우 유익한 업링크 통신에 있어서, 큰 관심을 끌어왔다. 이는 3GPP 롱 텀 에볼루션(LTE), 또는 Evolved UTRA에서의 업링크 다중 접속 방식에 대한 현재 적용

되는 전제이다.

[0023] 도 1을 참조하면, 일 실시예에 따른 다중 접속 무선 통신 시스템이 도시된다. e-NodeB 또는 eNB로도 지칭되는, 액세스 포인트(100)(AP)는 다수의 안테나 그룹들을 포함하며, 하나는 104 및 106을 포함하고, 다른 것은 108 및 110을 포함하며, 추가적인 것은 112 및 114를 포함한다. 도 1에서, 단 두 개의 안테나들이 각 안테나 그룹에 대해 도시되지만, 그러나, 더 많거나 적은 안테나들이 각 안테나 그룹에 활용될 수 있다. 사용자 장비(UE)로도 지칭되는, 액세스 단말(116)(AT)은 안테나들(112 및 114)과 통신하며, 여기서 안테나들(112 및 114)은 정보를 액세스 단말(116)로 순방향 링크(120) 상으로 송신하고 정보를 액세스 단말(116)로부터 역방향 링크(118) 상으로 수신한다. 액세스 단말(122)은 안테나들(106 및 108)과 통신하며, 여기서 안테나들(106 및 108)은 정보를 액세스 단말(122)로 순방향 링크(126)를 통해 송신하고 정보를 액세스 단말(122)로부터 역방향 링크(124)를 통해 수신한다. FDD 시스템에서, 통신 링크들(118, 120, 124 및 126)은 통신을 위해 상이한 주파수를 이용할 수 있다. 예를 들어, 순방향 링크(120)는 역방향 링크(118)에 의해 이용되는 것과 상이한 주파수를 이용할 수 있다.

[0024] 통신하도록 설계되는 지역 및/또는 안테나들의 각 그룹은 종종 액세스 포인트의 섹터로 지칭된다. 본 실시예에서, 안테나 그룹들 각각은 액세스 포인트(100)에 의해 커버되는 지역들의, 섹터 내의 액세스 단말들로 통신하도록 설계된다.

[0025] 순방향 링크들(120 및 126)을 통한 통신에서, 액세스 포인트(100)의 송신 안테나들은 상이한 액세스 단말들(116 및 124)에 대한 순방향 링크들의 신호-대-잡음 비를 개선하기 위해 빔포밍을 활용한다. 또한, 그 커버리지를 통틀어 무작위로 산재된 액세스 단말들로 송신하기 위해 빔포밍을 이용하는 액세스 포인트는 단일 안테나를 통해 모든 그 액세스 단말들로 송신하는 액세스 포인트보다 인접 셀들의 액세스 단말들에 간섭을 덜 야기한다.

[0026] 액세스 포인트는 단말들과 통신하는데 이용되는 고정국일 수 있으며 또한 액세스 포인트, 노드 B, 또는 어떠한 다른 용어로 지칭될 수도 있다. 또한 액세스 단말은 액세스 단말, 사용자 장비(UE), 무선 통신 장치, 단말, 액세스 단말 또는 다른 어떠한 용어로 호칭될 수도 있다.

[0027] 도 2는 MIMO 시스템(200)에서의 송신기 시스템(210)(액세스 포인트로도 알려짐) 및 수신기 시스템(250)(액세스 단말로도 알려짐)의 실시예의 블록도이다. 송신기 시스템(210)에서, 다수의 데이터 스트림들에 대한 트래픽 데이터가 데이터 소스(212)로부터 송신(TX) 데이터 처리기(214)로 제공된다.

[0028] 일 실시예로, 각 데이터 스트림은 각각의 송신 안테나를 통해 송신된다. TX 데이터 처리기(214)는 각 데이터 스트림에 대해 선택되는 특정 코딩 방식에 기초하여 상기 데이터 스트림에 대한 트래픽 데이터를 포맷, 코딩, 및 인터리빙하여 코딩된 데이터를 제공한다.

[0029] 각 데이터 스트림에 대한 코딩된 데이터는 OFDM 기술들을 이용하여 파일럿 데이터와 다중화될 수 있다. 상기 파일럿 데이터는 기지의 방식으로 처리되는 일반적으로 기지의 데이터 패턴이며 수신기 시스템에서 이용되어 채널 응답을 추정할 수 있다. 각 데이터 스트림에 대한 다중화된 파일럿 및 코딩된 데이터는 상기 데이터 스트림에 대해 선택된 특정 변조 방식(예컨대, BPSK, QPSK, M-PSK, 또는 M-QAM)에 기초하여 변조(즉, 심볼 매핑)되어 변조 심볼들을 제공한다. 각 데이터 스트림에 대한 데이터 레이트, 코딩, 및 변조는 처리기(230)에 의해 수행되는 명령들에 의해 결정될 수 있다. 메모리(232)는 처리기(230)에 접속될 수 있다.

[0030] 그리고 나서 모든 데이터 스트림들에 대한 변조 심볼들이 TX MIMO 처리기(22)에 제공되며, 이는 상기 변조 심볼들을 추가로 처리할 수 있다(예컨대, OFDM을 위해). 그리고 나서 TX MIMO 처리기(220)는 N_T개의 변조 심볼 스트림들을 N_T개의 송신기들(TMTR)(222a 내지 222t)에 제공한다. 어떠한 실시예들에서, TX MIMO 처리기(220)는 빔포밍 가중치들을 상기 데이터 스트림들의 심볼들에 그리고 상기 심볼이 송신되는 안테나에 적용한다.

[0031] 각 송신기(222a-t)는 각각의 심볼 스트림을 수신 및 처리하여 하나 이상의 아날로그 신호들을 제공하며, 추가로 상기 아날로그 신호들을 컨디셔닝(예컨대, 증폭, 필터링, 및 상향변환)하여 MIMO 채널을 통한 송신에 적합한 변조된 신호를 제공한다. 그리고 나서 송신기들(222a 내지 222t)로부터의 N_T개의 변조된 신호들이, 각각, N_T개의 안테나들(224a 내지 224t)로부터 송신된다.

[0032] 수신기 시스템(250)에서, 송신된 변조된 신호들은 N_R개의 안테나들(252a 내지 252r)에 의해 수신되고 각 안테나(252a-r)로부터의 수신된 신호는 각각의 수신기(RCVR)(254a 내지 254r)에 제공된다. 각 수신기(254a-r)는 각각의 수신된 신호를 컨디셔닝(예컨대, 필터링, 증폭, 및 하향변환)하고, 상기 컨디셔닝된 신호를 디지털화하여 샘

플들을 제공하며, 상기 샘플들을 추가로 처리하여 대응하는 "수신된" 심볼 스트림을 제공한다.

[0033] 그리고 나서 RX 데이터 처리기(260)는 상기 N_R개의 수신기들(254a-r)로부터의 N_R개의 수신된 심볼 스트림들을 수신하고 특정한 수신 처리 기술에 기초하여 처리하여 N_T개의 "검출된" 심볼 스트림들을 제공한다. 그리고 나서 RX 데이터 처리기(260)가 각각의 검출된 심볼 스트림을 복조, 디인터리빙, 및 디코딩하여 상기 데이터 스트림에 대한 트래픽 데이터를 복원한다. RX 데이터 처리기(260)에 의한 처리는 송신기 시스템(210)에서의 TX MIMO 처리기(220) 및 TX 데이터 처리기(214)에 의해 수행되는 것과 상보적이다.

[0034] 처리기(270)는 어느 사전-코딩(pre-coding) 행렬을 이용할 것인지를 주기적으로 결정한다(이하에서 논의됨). 처리기(270)는 행렬 인덱스 부분 및 랭크(rank) 값 부분을 포함하는 역방향 링크 메시지를 작성한다. 메모리(272)는 처리기(270)에 접속될 수 있다.

[0035] 상기 역방향 링크 메시지는 통신 링크 및/또는 수신된 데이터 스트림에 대한 다양한 종류의 정보를 포함할 수 있다. 그리고 나서 역방향 링크 메시지는 TX 데이터 처리기(238)에 의해 처리되며, 이는 또한 변조기(280)에 의해 변조되고, 송신기들(254a 내지 254r)에 의해 컨디셔닝되며, 다시 송신기 시스템(210)으로 송신되는, 데이터 소스(236)로부터의 다수의 데이터 스트림들에 대한 트래픽 데이터를 수신한다.

[0036] 송신기 시스템(210)에서, 수신기 시스템(250)으로부터의 변조된 신호들은 안테나들(224a-t)에 의해 수신되고, 수신기들(222a-t)에 의해 컨디셔닝되고, 복조기(240)에 의해 복조되며, RX 데이터 처리기(242)에 의해 처리되어 수신기 시스템(250)에 의해 송신된 역방향 링크 메시지를 추출한다. 그리고 나서 처리기(230)는 빔포밍 가중치들을 결정하기 위해 어느 사전-코딩 행렬을 이용할 것인지를 결정하여 상기 추출된 메시지를 처리한다.

[0037] 일 양상으로, 논리 채널들은 제어 채널들과 트래픽 채널들로 분류된다. 논리 채널들은 시스템 제어 정보를 동보하기 위한 DL 채널인 동보 제어 채널(BCCH)을 포함한다. 페이징 정보를 전달하는 DL 채널인 페이징 제어 채널(PCCH). 하나 또는 수개의 MTCH들에 대한 멀티미디어 브로드캐스트 및 멀티캐스트 서비스(MBMS) 스케쥴링 및 제어 정보를 송신하는데 이용되는 포인트-투-멀티포인트 DL 채널인 멀티캐스트 제어 채널(MCCH). 일반적으로, RRC 접속을 수립한 후 이 채널은 MBMS를 수신하는 UE들에 의해서만 이용된다(주목: 구 MCCH+MSCH). 전용 제어 채널(DCCH)은 전용 제어 정보를 송신하며 RRC 접속을 갖는 UE들에 의해 이용되는 포인트-투-포인트 양-방향 채널이다. 일 양상으로, 논리 트래픽 채널들은 사용자 정보의 전달을 위해, 하나의 UE에 전용되는, 포인트-투-포인트 양-방향 채널인 전용 트래픽 채널(DTCH)을 포함한다. 또한, 트래픽 데이터를 송신하기 위한 포인트-투-멀티포인트 DL 채널에 대한 멀티캐스트 트래픽 채널(MTCH).

[0038] 일 양상으로, 전송 채널들은 DL과 UL로 분류된다. DL 전송 채널들은 브로드캐스트 채널(BCH), 다운링크 공용 데이터 채널(DL-SDCH) 및 페이징 채널(PCH)을 포함하고, 상기 PCH는 UE 전력 절감의 지원을 위한 것이고(DRX 사이클은 UE에 대해 네트워크에 의해 표시된다), 전체 셀에 걸쳐 동보되며 다른 제어/트래픽 채널들에 이용될 수 있는 PHY 자원들로 매핑된다. UL 전송 채널들은 랜덤 액세스 채널(RACH), 요청 채널(REQCH), 업링크 공용 데이터 채널(UL-SDCH) 및 복수의 PHY 채널들을 포함한다. PHY 채널들은 DL 채널들과 UL 채널들의 세트를 포함한다.

[0039] DL PHY 채널들은:

[0040] 공통 파일럿 채널 (CPICH)

[0041] 동기화 채널 (SCH)

[0042] 공통 제어 채널 (CCCH)

[0043] 공용 DL 제어 채널 (SDCCH)

[0044] 멀티캐스트 제어 채널 (MCCH)

[0045] 공용 UL 할당 채널 (SUACH)

[0046] 확인응답 채널 (ACKCH)

[0047] DL 물리 공용 데이터 채널 (DL-PSDCH)

[0048] UL 전력 제어 채널 (UPCCH)

[0049] 페이징 표시자 채널 (PICH)

[0050] 부하 표시자 채널 (LICH)을 포함한다.

[0051] UL PHY 채널들은:

[0052] 물리 랜덤 액세스 채널 (PRACH)

[0053] 채널 품질 표시자 채널 (CQICH)

[0054] 확인응답 채널 (ACKCH)

[0055] 안테나 서브셋 표시자 채널 (ASICH)

[0056] 공용 요청 채널 (SREQCH)

[0057] UL 물리 공용 데이터 채널 (UL-PSDCH)

[0058] 동보 파일럿 채널 (BPICH)을 포함한다.

[0059] 일 양상으로, 단일 반송파 파형의 낮은 PAR(임의의 주어진 시간에서, 채널은 주파수에서 연속적 또는 균일하게 이격됨) 속성들을 보존하는 채널 구조가 제공된다.

부호의 설명

[0060] 본 문헌의 목적들을 위해, 다음의 약어가 적용된다:

AM 확인응답된 모드

AMD 확인응답된 모드 데이터

ARQ 자동 반복 요청

BCCH 동보 제어 채널

BCH 동보 채널

C- 제어-

CCCH 공통 제어 채널

CCH 제어 채널

CCTrCH 코딩된 복합 전송 채널

CP 순환 프리픽스

CRC 순환 중복 검사

CTCH 공통 트래픽 채널

DCCH 전용 제어 채널

DCH 전용 채널

DL 다운링크

DSCH 다운링크 공용 채널

DTCH 전용 트래픽 채널

FACH 순방향 링크 액세스 채널

FDD 주파수 분할 이중화

L1 계층 1 (물리 계층)

L2 계층 2 (데이터 링크 계층)

L3 계층 3 (네트워크 계층)

LI 길이 표시자

LSB 최하위 비트

MAC 매체 액세스 제어

MBMS 멀티미디어 브로드캐스트 멀티캐스트 서비스

MCCH MBMS 포인트-투-멀티포인트 제어 채널

MRW 수신 윈도우를 이동

MSB 최상위 비트

MSCH MBMS 포인트-투-멀티포인트 스케쥴링 채널

MTCH MBMS 포인트-투-멀티포인트 트래픽 채널

PCCH 페이징 제어 채널

PCH 페이징 채널

PDU 프로토콜 데이터 유닛

PHY 물리 계층

PhyCH 물리 채널들

RACH 랜댐 액세스 채널

RLC 무선 링크 제어

RRC 무선 자원 제어

SAP 서비스 액세스 포인트

SDU 서비스 데이터 유닛

SHCCH 공용 채널 제어 채널

SN 시퀀스 번호

SUFI 수퍼 필드

TCH 트래픽 채널

TDD 시 분할 이중화

TFI 전송 포맷 표시자

TM 투명 모드(Transparent Mode)

TMD 투명 모드 데이터

TTI 전송 시간 간격

U- 사용자-

UE 사용자 장비

UL 업링크

UM 확인응답되지않은 모드

UMD 확인응답되지않은 모드 데이터

UMTS Universal Mobile Telecommunications System

UTRA UMTS Terrestrial Radio Access

UTRAN UMTS Terrestrial Radio Access Network

MBSFN 멀티캐스트 브로드캐스트 단일 주파수 네트워크

MCE MBMS 조정 엔티티

MCH 멀티캐스트 채널

DL-SCH 다운링크 공용 채널

MSCH MBMS 제어 채널

PDCCH 물리 다운링크 제어 채널

PDSCH 물리 다운링크 공용 채널

eNB 기지국 또는 기지 송시신기 국

PDCP 패킷 데이터 컨버전스 프로토콜

HFN 하이퍼 프레임 번호

도 3은 모바일 시스템에서의 이용에 적합한 암호화 및 복호화 방식을 나타내는 블록도(300)이다. 상부 다이어그램은 eNB에서의 암호화 절차의 일반적인 방책들을 나타낸다. 여기서, 데이터(310)는 HFN(320) 및 패킷 데이터 컨버전스 프로토콜(PDCP) 계층 시퀀스 번호(SN)(330)을 포함하는 크립토싱크(cryptosync) 표현(expression)과 조합되고, 암호화 알고리듬(350)을 이용하여 암호화 키(340)로써 코딩되어, UE로 포워딩되는 암화화된 데이터(360)를 발생시킨다.

하부 다이어그램은 UE에서의 일반적인 복호화 절차를 나타낸다. 여기서, 수신된 암화화된 데이터(360)는 PDCP SN(330) 및 HFN(320)(이는 초기화/셋업시 UE에서 획득 또는 발생될 수 있음)과 조합되고, 암호화 키(340)(때때로 무결성 키로 호칭됨) 및 복호화 알고리듬(370)을 이용하여 디코딩되어 본래의 데이터(310)를 재생시킨다. 도 3은 암호화/복호화를 위한 HFN(320) 및 PDCP SN(330)의 이용의 일반적인 요약을 제공한다. 암화화/복호화에 관한 추가적인 요소들 및 구성요소들은 이들이 여기에 개시되는 다양한 실시예들을 이해하는 목적들에 적합하지 않으므로 추가로 설명되지 않는다.

암호학에서 증가된 보안 레벨이 가능한 조합들의 개수를 증가시키기 위해 큰 세트(set)로써 데이터를 조합함에 의해 도달될 수 있다는 점에 이해된다. 모바일 커뮤니티에서, 본 큰 세트는, HFN 및 PDCP SN을 갖는, PDCP SN의 값을 증분시킴으로써 순차적으로 정렬될 수 있는, 크립토싱크(cryptosync)로서 지칭된다. 본 증분은 HFN/PDCP SN 값들에 대한 순서 또는 시퀀싱을 제공하여 상기 크립토싱크가 각각의 암화화된/복호화된 패킷들의 세트에 대해 변화할 것을 보장한다. 크립토싱크가 큰 값을 나타낼 수 있기 때문에, 그리고 이 값이 변화하기 때문에(PDCP SN 시퀀싱을 통해), 어떠한 정도의 무작위성이 유입되어 더 견고한 암호화 방식으로 귀결된다. 그러나, 이러한 견고성은 동일한 HFN/PDCP SN 시퀀스가 주어진 키에 대해 두번 이상 이용되지 않을 것을 가정한다. 이는 반복적인 "코딩 엘리먼트들"을 이용한 암호화 방법들이 더 깨지기 쉬운 것으로 알려져 있기 때문이다.

도 4는 HFN 대 PDCP SN 관계를 도시하는 도면(400)이다. PDCP SN은 12 비트 카운터로서 도 4에 도시되는, 고정 비트 카운터이다. 다양한 구현들에서, PDCP SN은 5, 7, 또는 12 비트 카운터 또는 다른-크기 카운터일 수 있으며 따라서 PDCP SN이 여기서 도시되는 12 비트 구현에 한정되는 것이 아님에 유의하여야 한다. PDCP SN은 스스로 "리셋"하며 이전 시작 값으로 롤 오버(roll over)하는 순환 카운터로서 동작한다. 예를 들어, PDCP SN(12개의 비트들을 이용하는)은 1 내지 4096(또는 0 내지 4095)의 십진 범위를 갖는다. 0 내지 4095를 이용하면, 값 4096은 0과 동등하며, 값 4097은 1과 동등하고, 4098은 2와 동등하다. 따라서, 1인 PDCP SN 값들은 4097, 8193, 12,289 등의 롤오버 값들과 동등하다. PDCP SN의 "롤오버들"의 개수를 추적하기 위해, HFN이 카운터로서 이용될 수 있다. 따라서, PDCP SN이 4번 롤오버 하였다면, HFN은 우측 편에서 4의 값을 나타낼 것이다(HFN은, 일부 보기들에서, 다른 정보를 위해 상위 비트들을 유보할 수 있다). 명백하게도, HFN/PDCP SN 조합에 의해 획득될 수 있는 대단히 많은 수의 값들이 존재할 수 있다.

도 3에 도시된 바와 같이, 복호화 알고리듬(370)은 PDCP SN과 HFN 값들이 암호화 알고리듬(360)에서 이용되는 동일한 값들일 것을 요구한다. 그러므로, 복호화 엔티티(수신 단말)가 암호화 엔티티(송신국)에서 이용되는 동일한 PDCP SN과 HFN 값(들)을 정확하게 획득하는 것이 중요하다. 두 개의 송신국들 간의 핸드오프 동안, 타겟 송신국이 소스 송신국으로부터 정확한 시퀀스 PDCP SN/HFN 값들을 수신하지 못할 가능성이 존재한다. 이를 회피하기 위해, 타겟 송신국에 의해 이용되는 HFN이 핸드오버시 영으로 리셋되고, PDCP 시퀀스가 보존되며, 핸드오버시 키 변경을 요구할 것이 제안되었다. 그러나, 이 방안은 HFN 값들이 "조급히" 리셋될 수 있는 가능성을

야기한다. 즉, HFN 값들의 전 범위가 핸드오프시 영으로 리셋되기 전에 완전히 활용되지 않을 수 있으며, 따라서 암호화 알고리듬에 대한 "큰" 크립토싱크 기여를 본질적으로 좌절시킨다. 바람직한 것은 큰 범위의 HFN/PDCP SN 값들을 활용하고 PDCP SN의 롤오버로부터의 모호성들을 회피하는 방식일 것이다.

도 5는 예시적인 방안에 따른 두 개의 eNB들 간의 핸드오프 파라미터들의 도시(500)이며 여기서 HFN도 이동성에 유지된다. 본 실시예에서, HFN은 리셋될 필요가 없다(그러므로, 키가 핸드오버시 변경될 필요가 없다). 소스 송신기(510)가 암호화된 데이터를 링크(515)를 통해 전송 중이며 수신기(520)(UE)가 타겟 송신기(530)로 핸드오프될 때, "이용할 다음 PSCP SN" 및 이하사항이 소스 eNB(510)로부터 타겟 eNB(530)로 통신 회선 X2(540)를 통해 전달된다:

· 소스 eNB(510)에서의 암호화를 위해 이용되는 최종 HFN 및 PDCP SN

· 소스 eNB(510)에서의 복호화를 위해 이용되는 최종 HFN 및 PDCP SN

DL 암호화를 위해, 타겟 eNB(530)는 송신될 PDCP SDU의 SN 및 암호화를 위한 전송된 최종 HFN과 PDCP SN에 기초하여 암호화를 위한 통상(normal) 카운트(COUNT) 유지를 수행할 수 있다. 용어 카운트(COUNT)는 HFN과 PDCP SN의 취합을 나타낼 수 있다. 다음은 도 5에 도시되는 바와 같은 예시적인 실시예에 따른 DL 암호화에 대한 예시를 도시한다:

소스 eNB(510)는 핸드오버 전의 암호화를 위해 HFN 값 = x를 이용 중이며 PDCP SN 값=4093이다. 본 조합은 표현 x‖4093으로 기호화될 수 있다. 핸드오버 동안, 소스 eNB(510)는 현재의 HFN 값 = x 및 현재의 PDCP SN 값 4093(즉, x‖4093)을 타겟 eNB(530)로 전달하고 "이용할 다음 PDCP SN = 2"도 타겟 eNB(530)로 전달한다. 또한 소스 eNB(530)는 SN들 4094, 4095, 0, 1과 함께 PDCP PDU들을 타겟 eNB(530)로 전달한다.

핸드오버시, 타겟 eNB(530)는 UE(520)에 다음을 전송한다: x‖4094, x‖4095, (x+1)‖0 (카운트 유지는 HFN의 증분을 요구한다), (x+1)‖1, 및 (x+1)‖2.

시작 PDCP SN 값 = 4093 및 이용할 다음 PDCP SN = 2 를 소스 eNB(510)로부터 수신하였다면, PDCP SN = 4094 및 PDCP SN = 4095가 타겟 eNB(530)로의 데이터 링크 X2(540)에서 손실되었을지라도, 타겟 eNB(530)는 여전히 언제 HFN을 증분시킬 것인지를 알 것인데 이는 그것이 소스 eNB(510)에 의해 보고된 최종 PDCP SN이 4093이었음을 알기 때문이다. 따라서, 링크(535)에서 보여지는 바와 같이, 타겟 eNB(530)는 암호화/복호화 HFN/PDCP SN 값들의 정확한 시퀀스를 UE(520)로 포워딩할 수 있다.

그러므로, 소스 및 타겟 eNB들이 핸드오프 동안 탈동기(out of sync)될 수 있는 가능성 때문에 핸드오프시 HFN 및/또는 PDCP SN 값들의 리셋을 강제할 필요성이 방지될 수 있다. 또한, 본 방식에 의해, 더 큰 범위의 HFN 및/또는 PDCP SN 값들이 활용될 수 있다.

상기 기재에 기초하여, UL 복호화 절차는, 적절한 적응을 이용하여, 유사하게 따른다. 이것이 당해 기술분야에서 통상의 지식을 가진 자의 시계 이내이기 때문에, UL 절차의 세부사항들은 일반적으로 중복되는 것으로서 설명되지 않는다.

도 6A-B는 HFN/PDCP SN 제어의 오프셋 방식들의 도시이다. UE가 긴 시간 기간 동안 기지국과 단지 통신 중이라면, HFN/PDCP SN 조합이 완전(full) 사이클을 돌 수 있다. 즉, 크립토싱크(또는 일부 보기들에서 카운트로 지칭됨)가 오버플로(overflow)하고 영에서 시작할 수 있다. 또는 특정 구현은 영으로의 리셋을 실시할 수 있다. 카운트=0 값을 재사용하는 것을 회피하기 위해, 전형적인 시스템들에서, 카운트가 임계(THRESHOLD)에 도달하거나 초과할 때 키가 변경되는 임계 값이 이용될 수 있다. 이 시나리오는 도 6A에 도시된다.

그러나, 상기 예시적인 실시예(들)에 기재된 바와 같이, 일단 우리가 HFN이 eNB-간(inter-eNB) 핸드오버에서 유지된다고 가정하면 임계 트리거(trigger)에 대한 필요성은 덜 분명하다. 특히, 카운트의 랩어라운드(wraparound)가 반드시 키 수명 시간(life time)의 만료를 의미하는 것은 아니다. 이는 eNB 키가 eNB-간 핸드오버시 변경되며 카운트 값이 임의의 값으로부터 시작하기 때문이다.

도 6B는 상기 설명에 기초한 예시적인 방안을 도시한다. 초기화 또는 첫 핸드오프시 제 1 키 또는 새로운 키가 생성되었다고 전제하면, 카운트 값은 다음의 또는 다음-제공되는 시퀀스로 계속할 수 있으며(상기 기재된 실시예(들)에 따라) 과거 카운트 = 0 값을 증분시키고 이로써 계속할 수 있다. 핸드오프 포인트로부터의 역방향 오프셋(OFFSET)(또는, 구현 선호도에 따라, 순방향 오프셋)에 의해 지정되는, 핸드오프 값 전의 일부 트리거링 값에서, 키가 만료될 것이며 새로운 키가 발생될 것이다. 만일 요구된다면, 오프셋은 일부 네트워크 파라미터에

의존할 수 있다.

네트워크가 도 6B에 도시되는 바와 같이 초기 카운트 값으로부터의 역방향 오프셋을 적용할 수 있음에 유념하여야 한다. 상기 키 수명 시간 취급이 네트워크에서 RLC-AM을 이용하여 무선 베어러(bearer)마다 필요하며, E-UTRAN에서 적용가능성을 발견할 수 있음에 유의하여야 한다. 카운트의 예시적인 취급은 표준화를 요구하지 않으며 UE에 완전히 투명할 수 있다. UE 명세(specification)는 카운트 값의 랩어라운드를 허용하여야 하지만, UE는 가능한 카운트 값 재사용을 알 필요는 없다. 동일한 키에 대해 카운트 값의 재사용을 회피하기 위해 적절한 동작(즉, 재-키잉(re-keying))을 취할 것인지는 네트워크에 달려 있을 수 있다. 이 방안은 다음의 이점들을 제공한다:

· 네트워크 동작의 표준화를 요구하지 않는다.

· 무선 시그널링 없음

· 키 수명 기간 유지가 완전히 UE에 투명하다.

본 해법이 다음의 일부 네트워크 내부 동작들 또는 이들의 수정들을 요구할 수 있음에 유념하여야 한다. 그러나, 여기에 개시되는 예시적인 방법들 및 시스템들은 네트워크 복잡도를 변경하는 것을 정당화할 것으로 여겨지는 이점들을 제시한다.

도 7은 본 개시물의 실시예에 따른 예시적인 프로세스(700)를 나타내는 순서도이다. 개시(710) 후, 예시적인 프로세스(700)는 핸드오프가 임박하다는 어떠한 통지로써 시작한다(720). 핸드오프에 앞서, 소스 스테이션은 필요한 HFN 및 다음 PDCP SN 번호들을 타겟 스테이션(730)으로 전송한다. 적절한 정보를 수신한, 타겟 스테이션은 UE에 대한 복호화/암호화의 제어를 인계받는다-단계(740). 핸드오프 후, 예시적인 프로세스(700)는 도 6에 기재된 방식(들)에 따라 카운트에 대한 역방향 오프셋들을 선택적으로 개시할 수 있다(750). 단계(740) 또는 선택적 단계(750)의 완료시, 예시적인 프로세스는 종료한다(760).

개시된 프로세스들에서의 단계들의 특정한 순서 또는 체계는 예시적인 방안들의 예시임에 유념하여야 한다. 설계 선호들에 기초하여, 상기 프로세스들에서의 단계들의 특정 순서 또는 계층은 본 개시물의 범위 내에 잔류하면서 재배열될 수 있음에 유념하여야 한다. 첨부된 방법 청구항들은 표본적인 순서로 다양한 단계들의 구성요소들을 제시하며, 제시되는 특정한 순서나 계층에 한정됨을 의미하는것은 아니다.

또한 당해 기술분야에서 통상의 지식을 가진 자는 여기 개시된 상기 실시예들에 관련된 다양한 도식적인 논리 블록, 모듈, 회로, 및 알고리듬 단계들이 전자 하드웨어, 컴퓨터로-읽을 수 있는 매체의 형태의 컴퓨터 프로그램을 포함하는, 컴퓨터 소프트웨어, 또는 양자의 조합으로서 구현될 수 있음을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 교환성을 명확하게 나타내기 위해, 다양한 도식적인 컴포넌트, 블록, 모듈, 회로, 및 단계들이 기능성의 관점에서 일반적으로 앞서 기술되었다. 그러한 기능성이 하드웨어 또는 소프트웨어로서 구현될 것인지 여부는 특정한 애플리케이션 및 전체 시스템에 부과되는 설계 제약들에 달려 있다. 당업자는 각각의 특정한 애플리케이션에 대해서 다양한 방법으로 상기 기술된 기능성을 구현할 수 있지만, 그러한 구현 결정들이 본 발명의 범위를 벗어나도록 하는 것으로 해석되어서는 안 된다.

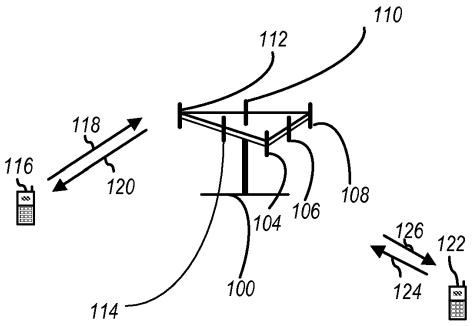
여기 개시된 실시예들과 관련하여 기재된 상기 다양한 도식적인 논리 블록, 모듈, 그리고 회로는 범용 처리기, 디지털 신호 처리기(DSP), 주문형 반도체(ASIC), 필드 프로그래머블 게이트 어레이(FGPA) 또는 다른 프로그래머블 논리 장치, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트, 또는 상기 기술된 기능들을 수행하도록 설계된 이들의 임의의 조합으로써 구현되거나 수행될 수 있다. 범용 처리기는 마이크로프로세서일 수 있지만, 대안으로, 상기 처리기는 임의의 종래의 처리기, 제어기, 마이크로제어기, 또는 상태 머신일 수 있다. 또한 처리기는 컴퓨팅 장치들의 조합, 예컨대, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 함께 하나 이상의 마이크로프로세서들, 또는 임의의 다른 그러한 구성으로서 구현될 수 있다.

상기 기재된 것들은 하나 이상의 실시예들의 예시들을 포함한다. 물론, 전술한 실시예들을 기술하기 위한 목적들을 위해 컴포넌트들 또는 방법론들의 모든 고안가능한 조합을 기재하는 것은 불가능하지만, 당해 기술분야에서 통상의 지식을 가진 자는 다양한 실시예들의 많은 추가적인 조합들 및 치환들이 가능함을 알 것이다. 따라서, 기재된 실시예들은 첨부된 청구항들의 사상 및 범위 내에 속하는 모든 그러한 변형들, 수정들 및 변형들을 포괄하고자 하는 것이다. 또한, 용어 "포함하는"이 발명을 실시하기 위한 구체적인 내용 또는 청구항들에서 이용되는 한도에서, 그러한 용어는 "포함하는"이 청구항의 전이구에서 채택될 때 해석되는 바와 같이 용어 "포함하는"과 유사한 방식으로 포함적인 것이다.

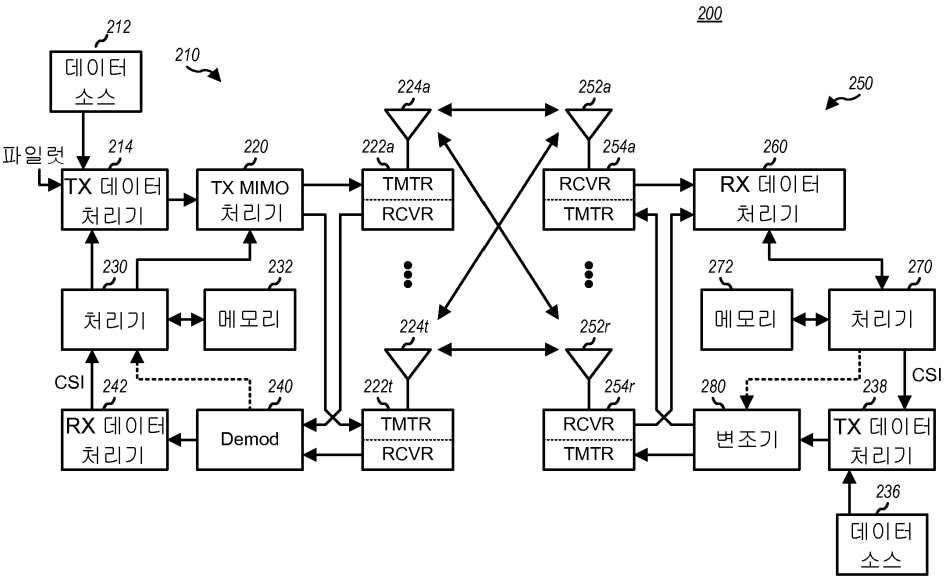
상기 개시된 예시들의 이전 기재는 임의의 당업자로 하여금 본 발명을 생산 또는 이용하게 하기 위하여 제시된다. 이러한 개시사항들에 대하여 다양한 변형들이 당업자에게 용이하게 명백할 것이며, 여기 정의된 일반 원리들은 본 개시사항의 사상과 범위를 벗어나지 않고도 다른 변형들에 적용될 수 있다. 따라서, 본 개시사항은 여기 제시된 예시들 및 설계들에 제한되어야 하는 것이 아니라 여기 개시된 원리들과 신규한 특징들에 따라서 가장 광범위하게 해석되어야 한다.

도면

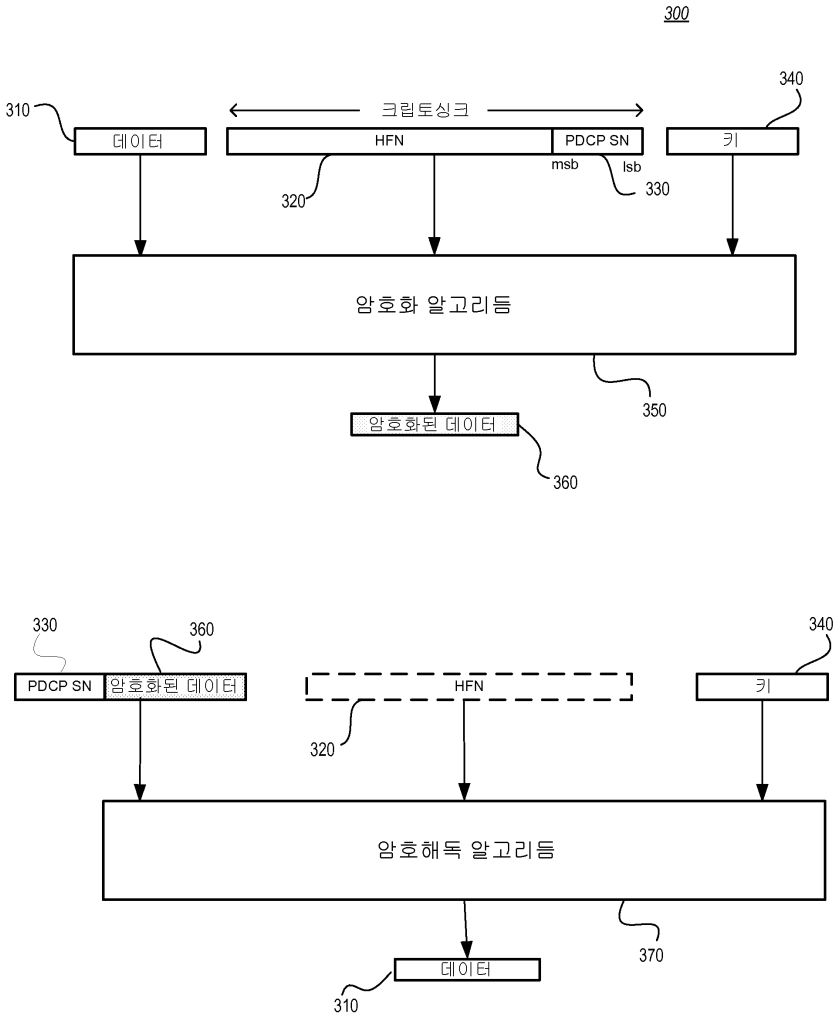
도면1



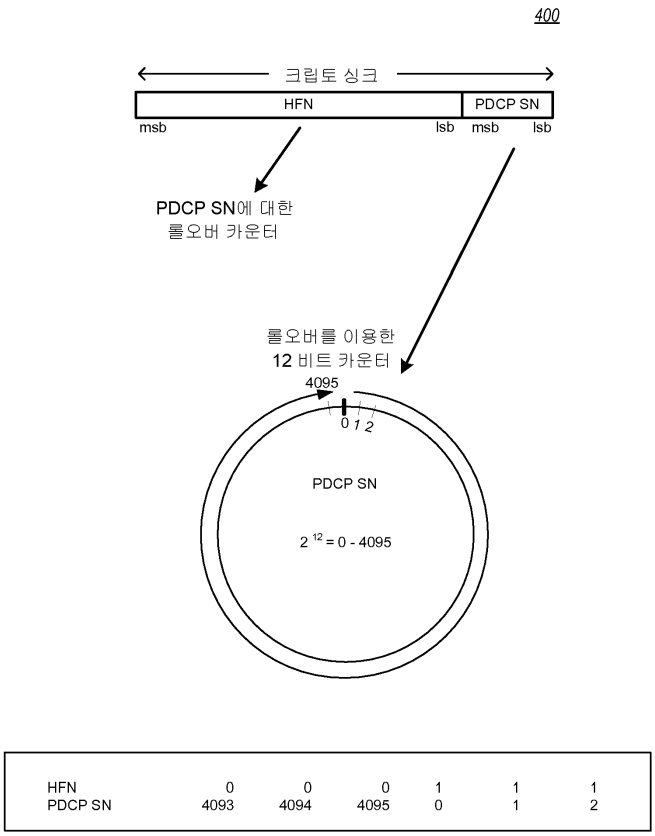
도면2



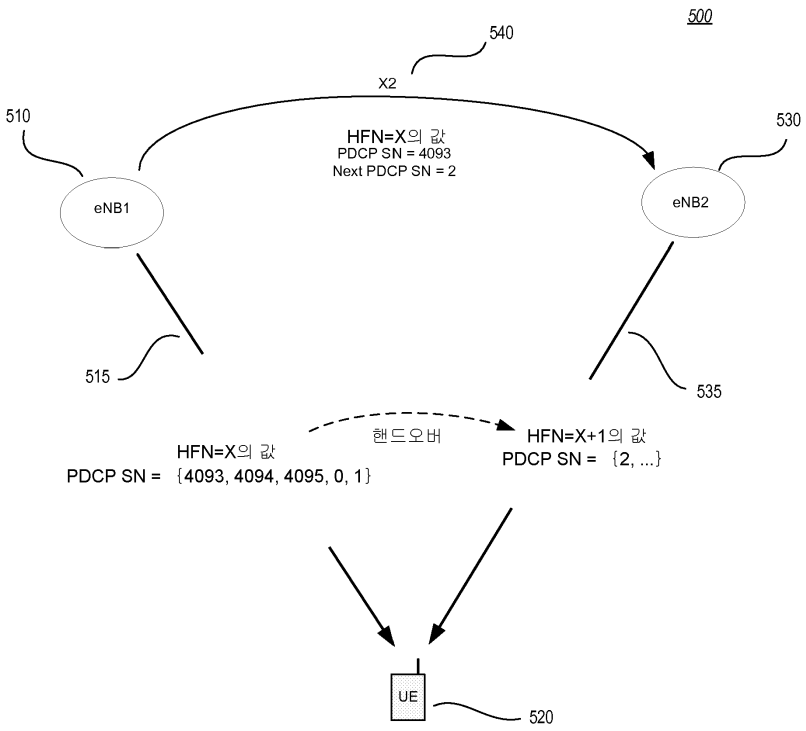
도면3


300
310
데이터
크립토싱크
HFN
PDCP SN
msb
lsb
320
330
340
키
암호화 알고리듬
350
암호화된 데이터
360
330
PDCP SN
360
암호화된 데이터
HFN
320
340
키
암호해독 알고리듬
370
데이터
310

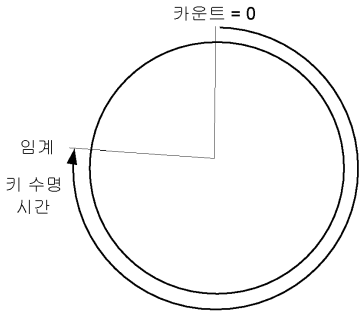
도면4


400
크립토 싱크
HFN
PDCP SN
msb
lsb
msb
lsb
PDCP SN에 대한
롤오버 카운터
롤오버를 이용한
12 비트 카운터
4095
0 1 2
PDCP SN
2 12 = 0 - 4095
HFN 0 0 0 1 1 1
PDCP SN 4093 4094 4095 0 1 2

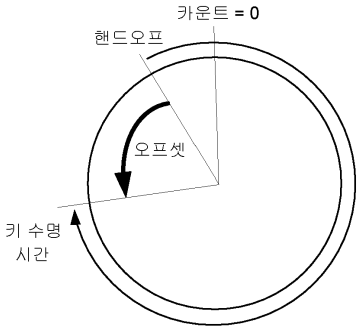
도면5


500
540
X2
510
HFN=X의 값
PDCP SN = 4093
Next PDCP SN = 2
530
eNB1
eNB2
515
535
핸드오버
HFN=X의 값
PDCP SN = {4093, 4094, 4095, 0, 1}
HFN=X+1의 값
PDCP SN = {2, ...}
UE
520

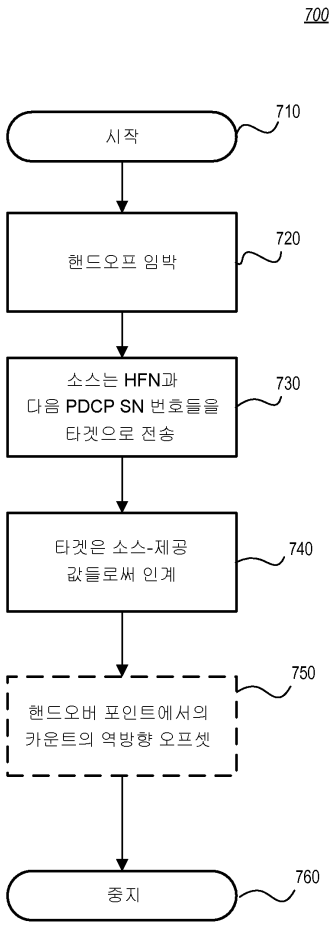
도면6a



도면6b



도면7


700
710
시작
720
핸드오프 임박
730
소스는 HFN과
다음 PDCP SN 번호들을
타겟으로 전송
740
타겟은 소스-제공
값들로써 인계
750
핸드오버 포인트에서의
카운트의 역방향 오프셋
760
중지