(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0015894
(43) 공개일자 2008년02월20일

(51) Int. Cl.
H04L 9/36 (2006.01) *H04L 29/08* (2006.01)
(21) 출원번호 10-2007-7031002
(22) 출원일자 2007년12월31일
심사청구일자 없음
번역문제출일자 2007년12월31일
(86) 국제출원번호 PCT/JP2006/311964
국제출원일자 2006년06월14일
(87) 국제공개번호 WO 2006/134985
국제공개일자 2006년12월21일
(30) 우선권주장
JP-P-2005-00175779 2005년06월15일 일본(JP)

(71) 출원인
가부시키가이샤 엔티티 도코모
일본 도쿄도 치요다쿠 나가타쵸 2쵸메 11반 1고
(72) 발명자
하라다 아츠시
일본 도쿄 1006150 치요다-쿠 나가타쵸 2-쵸메 11-1 산노파크타워 가부시키가이샤 엔티티 도코모 인터렉츄얼 프로퍼티디파트먼트 내
이시이 미나미
일본 도쿄 1006150 치요다-쿠 나가타쵸 2-쵸메 11-1 산노파크타워 가부시키가이샤 엔티티 도코모 인터렉츄얼 프로퍼티디파트먼트 내
(뒷면에 계속)
(74) 대리인
정홍식

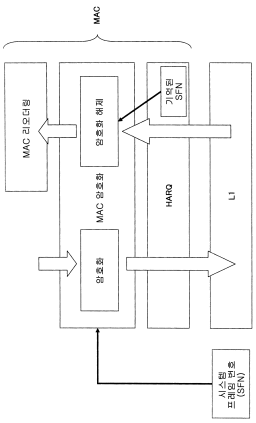
전체 청구항 수 : 총 5 항

(54) 보안처리장치 및 보안처리방법

(57) 요 약

보안처리장치는, 이동통신시스템의 MAC 레이어에서 보안처리를 수행한다. 본 장치는, 보안 시퀀스 번호를 이용하여 마스크를 작성하는 수단과, 마스크와 보안 대상 데이터를 논리연산하고, 암호화된 데이터를 출력하는 수단을 갖는다. 보안 시퀀스 번호는 하이퍼 프레임 번호 및 시스템 프레임 번호로 구성된다. 본 장치는 트랜스포트 블록(TB)을 단위로 보안처리를 수행한다. 트랜스포트 블록은, 단위시간(TTI)당 MAC층으로부터 물리층으로의 데이터 전송 단위이다. 보안 시퀀스 번호로서 HFN 및 SFN이 이용되므로, RLC의 모든 모드에서 보안 시퀀스 번호가 통일되어, HFN의 동기 불일치가 회피된다.

대표도 - 도10



(72) 발명자

아베타 사다유키

일본 도쿄 1006150 치요다-쿠 나가타쵸 2-쵸메 11-1 산노파크타워 가부시키가이샤 엔티티 도코모 인터렉츄얼 프로퍼티디파트먼트 내

나카무라 타케히로

일본 도쿄 1006150 치요다-쿠 나가타쵸 2-쵸메 11-1 산노파크타워 가부시키가이샤 엔티티 도코모 인터렉츄얼 프로퍼티디파트먼트 내

스즈키 타카시

일본 도쿄 1006150 치요다-쿠 나가타쵸 2-쵸메 11-1 산노파크타워 가부시키가이샤 엔티티 도코모 인터렉츄얼 프로퍼티디파트먼트 내

특허청구의 범위

청구항 1

이동통신시스템의 MAC 레이어에서 보안처리(security processing)를 수행하는 보안처리장치에 있어서,

보안 시퀀스 번호(security sequence number)를 이용하여 마스크(mask)를 작성하는 수단;

마스크와 보안 대상 데이터를 논리연산하여, 암호화된 데이터를 출력하는 수단;을 가지며,

상기 보안 시퀀스 번호는 하이퍼 프레임 번호(hyper frame number) 및 시스템 프레임 번호(system frame number)로 구성되는 것을 특징으로 하는 보안처리장치.

청구항 2

제 1항에 있어서,

상기 시스템 프레임 번호는, 기지국(base station)이 고유로 갖는 시퀀스 번호이며, 공통채널(common channel)로 이동국(mobile station)에 통지되는 것을 특징으로 하는 보안처리장치.

청구항 3

제 1항에 있어서,

소정의 암호화 알고리즘 입력에 보안 시퀀스 번호, 논리채널의 식별자 및 마스크 길이를 포함하는 정보가 주어지고, 상기 마스크가 상기 암호화 알고리즘에 따라 도출되는 것을 특징으로 하는 보안처리장치.

청구항 4

제 1항에 있어서

상기 논리 연산은 배타적 논리합 연산(exclusive OR operation)인 것을 특징으로 하는 보안처리장치.

청구항 5

이동통신시스템의 MAC 레이어에서 보안처리를 수행하는 보안처리방법에 있어서,

보안 시퀀스 번호를 이용하여 마스크를 작성하고,

마스크와 보안 대상 데이터를 논리 연산하고, 암호화된 데이터를 출력하며,

상기 보안 시퀀스 번호는 하이퍼 프레임 번호 및 시스템 프레임 번호로 구성되는 것을 특징으로 하는 보안처리방법.

명 세 서

기 술 분 야

<1> 본 발명은, 이동통신시스템의 보안처리를 수행하는 장치 및 방법에 관한 것이다.

배 경 기 술

<2> IMT-2000 시스템과 같은 이동통신시스템(mobile communcation system)에서는 전송되는 데이터에 보안처리가 실시된다. IMT-2000 시스템에서의 무선구간 보안처리의 개요에 대해서는, 비 특허문헌 1에 기재되어 있다.

<3> 종래의 보안처리 방식에서는 도 1에 도시된 바와 같이, 보안처리가 무선링크제어(RLC: Radio Link Control) 서브레이어(sublayer) 및 매체 액세스 제어(MAC: Medium Access Control) 서브레이어로 분산하여(separately) 배치되어 있다. 보안처리를 수행하는 프로토콜 레이어(protocol layer)는 무선 베어러(RB:Radio Bearer)에 적용되는 RLC 프로토콜의 동작 모드에 따라 정해지고 있다. 예를 들면, 음성통신에서 이용되는 트랜스페런트 모드(TM:Transparent Mode)의 경우에는 MAC층에서 보안처리가 수행되며, 패킷통신이나 제어신호의 송신에 이용되는 비 확인 모드(UM:Unacknowledgement Mode) 및 확인 모드(AM:Acknowledgement Mode)의 경우에는 RLC층에서 보안처리가 수행된다. 또, 보안 강도를 높이기 위해, 보안처리의 파라미터로서, 암호키(CK:Ciphering Key) 외에, 보

안처리를 수행하는 유닛마다 부여되는 보안 시퀀스 번호 (카운트) "COUNT"나 무선 베어러 ID "BEARER" 등이 조합된다.

<4> 도 2 및 도 3은 IMT-2000 방식에서의 무선구간(radio zone) 내의 보안처리를 나타낸다.

<5> 도 2는 RLC 동작 모드가 TM인 경우의 RB에 적용되는 보안처리이다.

<6> 보안처리는 MAC-SDU(서비스 데이터 유닛) 단위로 수행된다. 이 경우 MAC 엔티티(entity)에서 실시되는 보안처리의 파라미터로서, 암호키(CK) 이외에 커넥션 프레임 번호(CFN:Connection Frame Number)와 하이퍼 프레임 번호(HFN:Hyper Frame Number)의 조합으로부터 생성되는 보안 시퀀스 번호(COUNT) 및 논리채널의 식별자(BEARER)와 더불어, 통신의 전송방향(상향링크/하향링크의 차이)을 나타내는 식별자(DIRECTION)가 이용된다. 또, MAC 엔티티에서 실시되는 보안처리에서는 모든 논리채널에 공통된 보안 시퀀스가 설정된다.

<7> 도 3은 RLC의 동작 모드가 AM 및 UM인 경우의 RB에 적용되는 보안처리이다.

<8> 보안처리는 RLC-PDU(프로토콜 데이터 유닛) 단위로 수행된다. 이 경우 RLC 엔티티에서 실시되는 보안처리의 파라미터로서, 암호키(CK) 이외에, RLC 프로토콜 데이터 유닛(RLC-PDU)에 부여되는 시퀀스 번호(SN)와 하이퍼 프레임 번호(HFN)의 조합으로부터 생성되는 보안 시퀀스 번호(COUNT) 및 상술한 PDU가 속하는 무선 베어러 ID(BEARER)에 추가하여, 통신의 전송방향(상향링크/하향링크의 차이)을 나타내는 식별자(DIRECTION)가 이용된다. 또, RLC 엔티티에서 실시되는 보안처리에서는 각 논리 채널마다 개별 보안 시퀀스(COUNT)가 설정된다.

<9> 비특허문헌 1 : 3GPP TS33. 102, 6. 6장

<10> 비특허문헌 2 : 3GPP TR25. 858, 9. 1장

<11> 비특허문헌 3 : 3GPP TR25. 913, 6. 1장

발명의 상세한 설명

<12> 발명의 개시

<13> 발명이 해결하고자 하는 과제

<14> 일반적으로 보안처리는 처리지연을 줄이면서, 높은 강도의 보안처리를 실현하는 것이 바람직하며, 또한 장치구성의 간소화 관점에서, 트래픽이나 채널, 무선 베어러의 종별이나 RLC 동작 모드에 관계없이 통일적인 수법으로 제공할 수 있는 것이 바람직하다. 또, 보안강도를 높이기 위해서는 복잡한 보안 알고리즘을 이용할 필요가 있다. 때문에, 처리부하의 관점에서는 단위시간, 예를 들면, 송신시간간격(TTI:Transmission Time Interval)당 보안처리를 실시해야 할 처리단위(프로토콜 유닛 수(PU 수))가 적은 것이, 즉, PU는 가능한 한 페이로드 사이즈가 큰 것이 바람직하다.

<15> 또, 종래의 IMT-2000 시스템에 있어서, RLC-PDU 혹은 MAC-SDU의 PDU 사이즈는 40 바이트 정도의 일정 길이이다. 때문에 종래의 보안처리에서는, 예를 들면 HSDPA(비특허문헌 2 참조)나 Evolved UTRAN(비특허문헌 3 참조) 등의 신기술 도입에 따른 무선 베어러 전송속도의 광대역화에 수반하여, 단위시간당 보안처리를 수행할 PU 수가 증가하고, 처리부하가 증대함을 생각할 수 있다. 예를 들어, 100Mbps의 무선 전송속도가 상정되는 경우에는, TTI 길이를 HSDPA와 동일한 2msec로 하면, TTI당 약 25000bytes의 정보전송이 가능하게 된다. 따라서, 만일 HSDPA와 동일한 PDU 사이즈(42 바이트) 및 TTI 길이가 가정된다면, Evolved UTRAN에서 규정되고 있는 최대 전송속도(100Mbps)의 경우, TTI=2msec 당 약 600개의 RLC-PDU에 대한 보안처리가 필요하게 된다. 이것은 현재 HSDPA의 최대 전송속도 14.4Mbps와의 비(比)보다, 종래와 비교하여 약 7배의 처리 수가 되며 처리부하가 증대되어 버리는 것을 생각할 수 있다.

<16> 또한, 보안 파라미터로서 이용되고 있는 시퀀스 번호는 송수신에서 동기되어 있을 필요가 있다. HFN은 네트워크측(RNC)과 이동국의 커넥션 설정시에 동기된 후, 보안성을 유지하기 위해, 시퀀스 번호(SN 혹은 CFN)의 주기마다 송신측, 수신측 쌍방에서 독립적으로 카운트 업 된다. 따라서, 시퀀스 번호의 1주기분 이상의 PDU가 연속으로 손실된 경우(로스(loss)된 경우)에, 송수신측의 HFN의 동기가 어긋나는 문제가 있다. 도 4는, SN의 주기가 4이고, HFN의 주기가 8인 경우(보안 시퀀스 번호의 주기는 8×4=32)의 예를 나타낸다. 송신측의 HFN은 순차 카운트 업 되지만, 수신측에서 4개 이상의 PDU가 연속으로 로스된 경우에는, 수신측의 HFN이 1주기분 늦게 카운트 업 되어, HFN의 동기가 어긋나 버린다. 보다 구체적으로는, RLC-UM에서는 시퀀스 번호(SN)의 자릿수는 7비트이

므로, 127개의 RLC-PDU의 로스가 발생하면 보안 동기 불일치가 발생한다.

<17> 본 발명은, 상기 문제점의 적어도 하나에 대처하기 위해 이루어진 것으로, 그 과제는 보안 처리 지연 및 보안 동기 불일치의 빈도를 적어도 경감하는 보안처리장치 및 보안처리방법을 제공하는 것이다.

<18> 과제를 해결하기 위한 수단

<19> 본 발명에 따르면, 이동통신시스템의 MAC 레이어에서 보안처리를 수행하는 보안처리장치가 사용된다. 보안처리장치는, 보안 시퀀스 번호를 이용하여 마스크를 작성하는 수단과, 마스크와 보안 대상 데이터를 논리연산하고, 암호화된 데이터를 출력하는 수단을 갖는다. 보안 시퀀스 번호는 하이퍼 프레임 번호 및 시스템 프레임 번호로 구성된다.

<20> 발명의 효과

<21> 본 발명에 따르면, 이동통신시스템에서의 보안처리 지연 및 보안 동기 불일치의 빈도를 적어도 경감할 수 있다.

도면의 간단한 설명

<22> 도 1은, IMT-2000에서의 보안처리를 나타내는 도면이다.

<23> 도 2는, RLC-TM에서의 보안처리를 나타내는 도면이다.

<24> 도 3은, RLC-UM 및 RLC-AM에서의 보안처리를 나타내는 도면이다.

<25> 도 4는 동기 불일치의 설명도를 나타낸다.

<26> 도 5는, MAC 레이어 보안의 구성(송신측)을 나타내는 도면이다.

<27> 도 6은, MAC 레이어 보안의 구성(수신측)을 나타내는 도면이다.

<28> 도 7은, 본 발명의 보안처리 단위를 나타내는 도면이다.

<29> 도 8은, 본 발명의 보안처리를 나타내는 도면이다.

<30> 도 9는, 본 발명의 효과를 나타내는 도면이다.

<31> 도 10은, 본 발명의 MAC 보안 서브레이어를 나타내는 도면이다.

<32> 부호의 설명

<33> RAB : 무선 액세스 베어러(Radio Access Bearer)

<34> TM : 투과형 모드(Transparent Mode)

<35> UM : 비 확인형 모드(Unacknowledgement Mode)

<36> AM : 확인형 모드(Acknowledgement Mode)

<37> RLC : 무선링크 제어(Radio Link Control)

<38> MAC : 매체 액세스 제어(Medium Access Control)

<39> PHY : 물리 레이어(PHYsical layer)

<40> CFN : 커넥션 프레임 번호(Connection Frame Number)

<41> HFN : 하이퍼 프레임 번호(Hyper Frame Number)

<42> SFN : 시스템 프레임 번호(System frame Number)

<43> SDU : 서비스 데이터 유닛(Service Data Unit)

<44> PDU : 프로토콜 데이터 유닛(Protocol Data Unit)

<45> XOR : 배타적 논리합(eXclusive OR)

<46> LCH : 논리채널(Logical CHannel)

<47> TrCH : 트랜스포트 채널(Transport CHannel)

<48> HARQ : 하이브리드 자동 재송 요구(Hybrid Auto retransmission ReQuest)

<49> 발명을 실시하기 위한 최량의 형태

<50> 본 발명의 일 실시예에 따른 MAC 보안 서브레이어는 트랜스포트 블록(TB)을 단위로 보안처리를 수행한다. 트랜스포트 블록은, 단위시간(TTI)당 MAC층으로부터 물리층으로의 데이터 전송단위이다. 보안 시퀀스 번호로서 하이퍼 프레임 번호(HFN) 및 시스템 프레임 번호(SFN)가 이용되며, 이에 따라 RLC의 모든 모드에서 통일적인 보안 시퀀스 번호의 사용이 가능해진다. 보안 시퀀스 번호로서 HFN과 SFN을 조합함으로써, HFN의 동기 불일치가 회피된다.

<51> 보안처리부가 MAC 서브레이어에 통합됨으로써, 이동기 구성의 간소화를 실현할 수 있다. 종래는 개개의 RLC-PDU마다 보안처리가 반복되었으나, 본 발명의 일 실시예에서는, MAC층의 PDU마다 보안처리가 한꺼번에 수행되어, 그에 따라 처리부하 및 처리지연을 줄일 수 있다. RLC 모드에 관계없이, 통일된 시퀀스 번호를 이용함으로써 보안처리 시스템의 간소화를 도모할 수 있다. 또, 시스템 프레임 번호를 이용함으로써, 보안 파라미터의 동기 불일치 확률을 저감할 수 있다.

<52> 실시 예 1

<53> 이하의 실시 예에서는 하향링크 전송을 상정하여 설명이 이루어지나, 상향링크 전송의 경우에도 본 발명이 적용 가능함은 명백하다.

<54> 도 5는, 본 발명의 일 실시 예에 따른 MAC 보안 서브레이어를 포함하는 송신측 MAC 서브레이어의 구성 예를 나타낸다. 송신측 MAC 서브레이어는 논리채널(LCH:Logical Channel) 다중화부, 우선도 식별부, 우선도별 큐(queue), 스케줄링부, MAC 보안 서브레이어, 송신측 HARQ부로 구성된다. 논리채널 다중화부는, 상위 레이어로부터 전송되어 오는 복수의 다른 논리채널의 다중화 처리를 수행하며, 후단의 우선도 식별부로 데이터를 전송한다. 우선도 식별부는, 예를 들면 상위 레이어로부터의 시그널링 정보에 기초하여, 논리채널 다중화부에서 다중화된 복수의 데이터 플로우(flow)에 대하여, 플로우 간의 송신 우선도 순위 매김을 수행하며, 데이터를 각각의 우선도별 큐로 배분한다. 우선도별 큐는 전송된 데이터의 버퍼링을 수행하며, 스케줄링부로부터의 지시에 기초하여, 송신 타이밍이 할당될 수 있다. 우선도별 큐는, 송신 타이밍이 할당되면, 레이어 1에 할당된 무선리소스 양에 따라 큐로부터 상위 레이어로부터의 PDU 데이터를 추출하여 트랜스포트 블록(TB)을 구성하여, MAC 보안 서브레이어에 대하여 데이터의 전송을 수행한다. MAC 보안 서브레이어는, 데이터에 대하여 보안 처리를 실시하고, 송신측 HARQ부로 데이터를 전송한다. HARQ부는, 데이터의 송달 관리를 수행하며, 무선구간에서의 데이터 전송 오류 유무에 따라 송신 데이터의 재송을 수행한다.

<55> 도 6에 본 발명에 있어서 MAC 보안 서브레이어를 포함하는 수신측 MAC 서브레어의 구성 예를 나타낸다. 수신측 MAC 서브 레이어는 논리채널 분리부, MAC 리오더링(Reordering)부, MAC 보안 서브레이어, 수신측 HARQ부로 구성된다. 수신측 HARQ부는 하위 레이어로부터 전송되는 데이터의 복호결과를 기초로 송신측 HARQ부로 재송 요구를 수행하며, 데이터가 올바르게 수신할 수 있는 시점에 복호 데이터를 MAC 보안 서브레이어로 전송한다. MAC 보안 서브레이어는, 받은 데이터에 대하여 보안 해제 처리를 실시하고, MAC 리오더링부로 데이터를 전송한다. MAC 리오더링부는, 도착 데이터의 순서 일관성을 유지하기 위해 버퍼링을 수행하며, 순서가 보증된 데이터를 논리채널 분리부에 보고한다. 논리채널 분리부는 송신측에서 다중화된 논리채널을 분리하고, 각각의 논리채널마다 상위 레이어로 데이터를 전송한다.

<56> MAC 보안 서브레이어에는 보안처리에 이용하는 파라미터로서 보안 시퀀스 번호(SFN) 및 우선도 큐 ID(BEARER)가 통지된다. 수신측 MAC 보안 서브레이어로의 보안 파라미터 통지는, 예를 들면 공통제어 채널을 이용하여 스케줄링 할당 정보로서 해당 TB의 송신 타이밍(즉 SFN)을 통지하는 방법 등을 생각할 수 있다. 전송방향(DIRECTION)은 이미 알고 있으므로 통지가 불필요하다.

<57> 도 5, 6에 도시된 본 실시 예에 따른 MAC 서브레이어는, 도 10에 도시된 바와 같이 기능한다. 즉, 송신측의 MAC 서브레이어는 시스템 프레임 번호(SFN)를 이용하여 논리채널을 암호화하고 물리 레이어에 전달한다. 또, 수신측의 MAC 서브레이어는 시스템 프레임 번호(SFN)에 기초하여 암호화를 해제하고, 상위 레이어에 보고한다.

<58> 도 7은 보안처리 단위의 일 예를 나타낸다. 이 예에서는 동일 우선도를 갖는 복수의 다른 논리 채널에 속하는 복수의 PDU가 하나의 트랜스포트 블록에 다중화되어 단위시간(TTI)마다 하위 레이어로 전송된다. 종래의 방법에서는 개개의 PDU에 대하여 보안 처리가 실시되었다. 이에 대해 본 실시 예에서는 논리채널 다중화부에서 다중화된 복수의 PDU가 보안처리의 한 단위가 된다. 이 단위는 프로토콜 유닛(PU)이라 불러도 좋다. 복수의 PDU가 한

꺼번에 암호화됨으로써, 단위시간(TTI)당 처리해야 할 PU 수를 줄일 수 있어, 처리 부하·지연 저감을 실현할 수 있다.

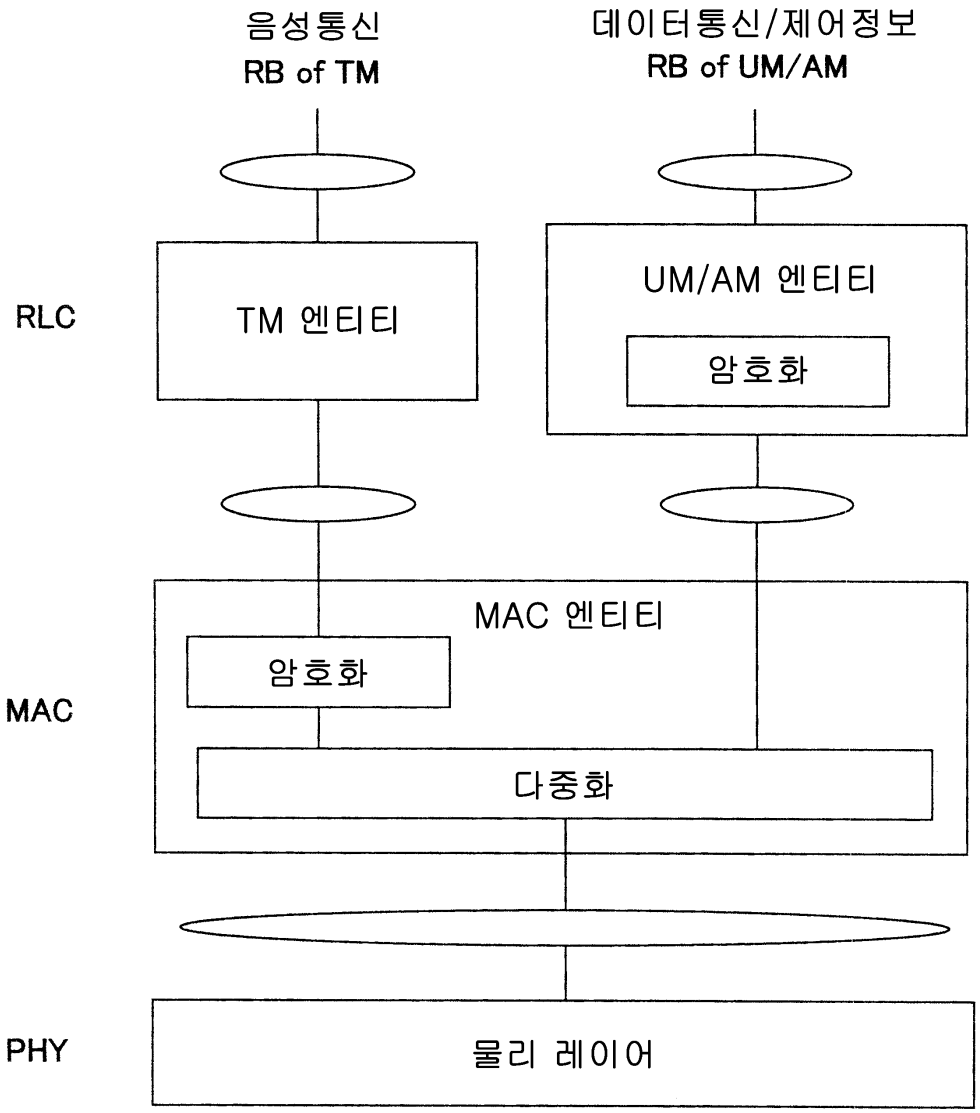
<59> 도 8은, 본 실시 예에 따른 MAC 보안 서브레이어에서의 보안처리를 나타낸다. MAC 보안 서브레이어에 도착한 PU(Transport block)의 비트계열과, 보안 알고리즘에 의해 생성된 보안 마스크(Mask)계열과의 연산처리(XOR)를 수행함으로써, 보안된 PU(Ciphered Transport block)가 생성되어, 도 4에 도시된 송신측 HARQ부로 전송된다. 보안 알고리즘은 보안 마스크 계열을 생성하기 위해 암호키(CK:Ciphering Key) 및, 보안 시퀀스 번호(카운트)"COUNT", 전송방향(디렉션) "DIRECTION", 우선도 큐 번호(베어러)"BEARER"를 파라미터로서 이용한다. 보안 시퀀스 번호(카운트)는 HFN과 SFN의 결합으로 구성된다. SFN은 기지국이 고유로 갖는 시퀀스 번호이며, 공통채널을 통해 기지국이 관리하는 이동국으로 통지되고 있으며, 기지국과 이동국 간에 동기되어 있다. SFN은 유저의 데이터 유무에 관계없이 일정한 시간주기로 카운트 업 되고 있다. 따라서, 기지국 및 이동국은, 각각의 SFN 주기에 기초하여 HFN의 카운트 업을 수행하기만 하면, 설령 카운트 업이 각각 독립적으로 수행된다 하더라도, 동기상태를 유지할 수 있다. 따라서, 개개의 PDU에 부여되는 시퀀스 번호를 이용하는 종래방식의 경우에, 1주기 이상의 패킷 로스에 기인하여 발생했던 동기 불일치 문제는 회피할 수 있다(도 9 참조). 또, 보안 파라미터(시퀀스 번호)의 불일치는 재송에 의한 트랜스포트 블록의 전송지연이 SFN 주기 이상이 되는 경우에만 발생한다. 예를 들면, 2msec의 TTI 길이에서 12비트의 SFN을 이용한 경우에는 $2\times10^{-3}\times2^{12}$=8.192초 이상의 지연이 발생한 경우에 보안 파라미터의 불일치가 발생할 수 있다. 그러나, 실제로는 그와 같은 큰 지연이 발생하지 않도록 회선품질이나 재송 횟수를 설계할 수 있으므로, 실질적으로는 파라미터의 불일치가 발생할 확률은 종래기술에 비교하여 현저하게 저감된다.

<60> 상기 실시 예에서는 하향링크 전송의 경우가 설명되었다. 그러나, 본 발명은 하향링크 전송의 경우에만 한정할 필요는 없으며, 이동기가 송신측이 되는 상향링크 전송의 경우의 보안처리에서도 적용이 가능함은 명백하다.

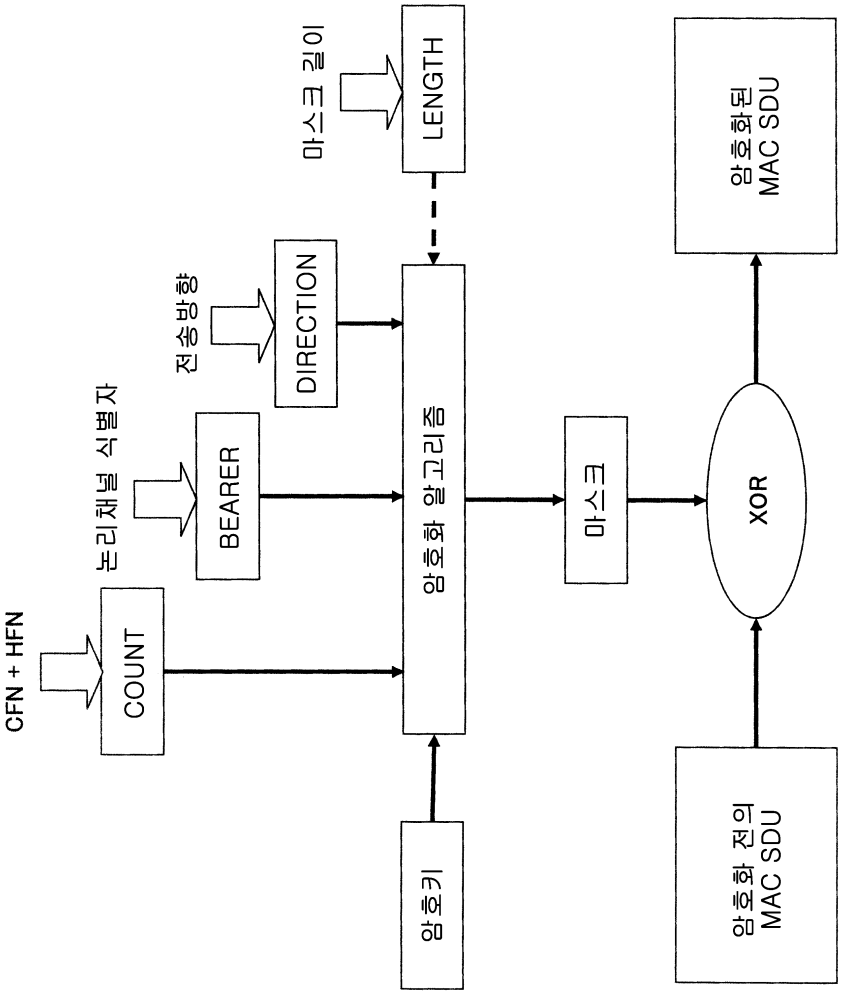
<61> 본 국제출원은 2005년 6월 15일에 출원된 일본국 특허출원 2005-175779호에 기초한 우선권을 주장하는 것이며, 2005-175779호의 전 내용을 여기 본 국제출원에 원용한다.

도면

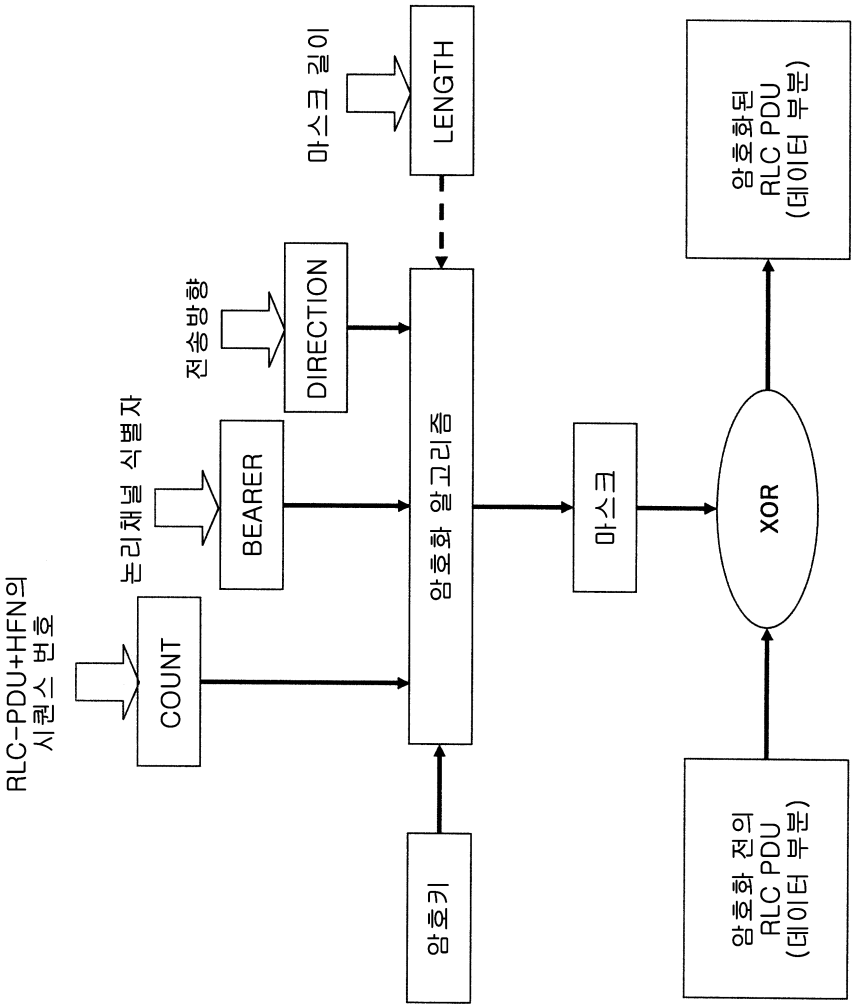
도면1


음성통신
RB of TM
데이터통신/제어정보
RB of UM/AM
RLC
TM 엔티티
UM/AM 엔티티
암호화
MAC
MAC 엔티티
암호화
다중화
PHY
물리 레이어

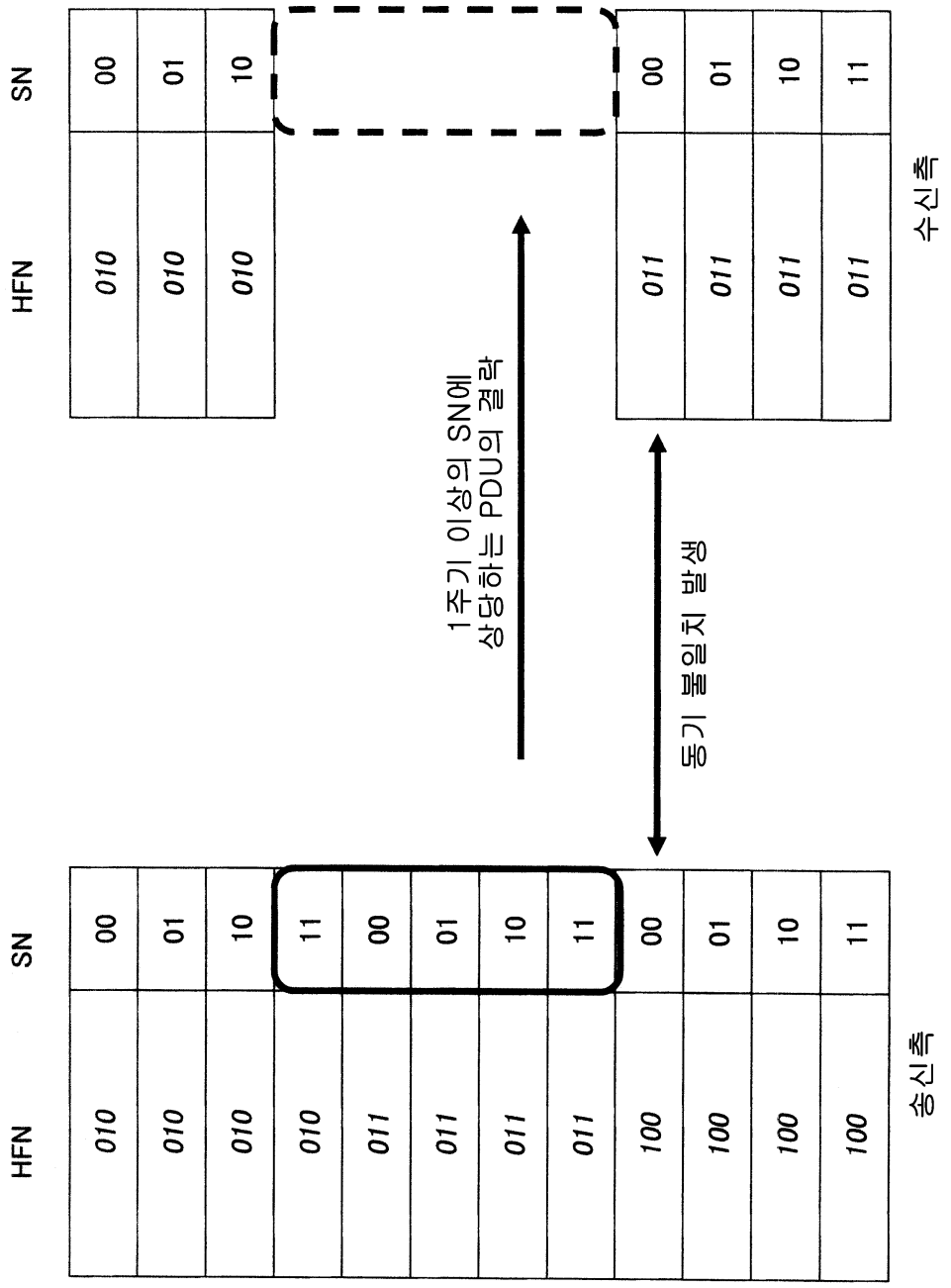
도면2


CFN + HFN
COUNT
논리채널 식별자
BEARER
전송방향
DIRECTION
마스크 길이
LENGTH
암호키
암호화 알고리즘
마스크
XOR
암호화 전의 MAC SDU
암호화된 MAC SDU

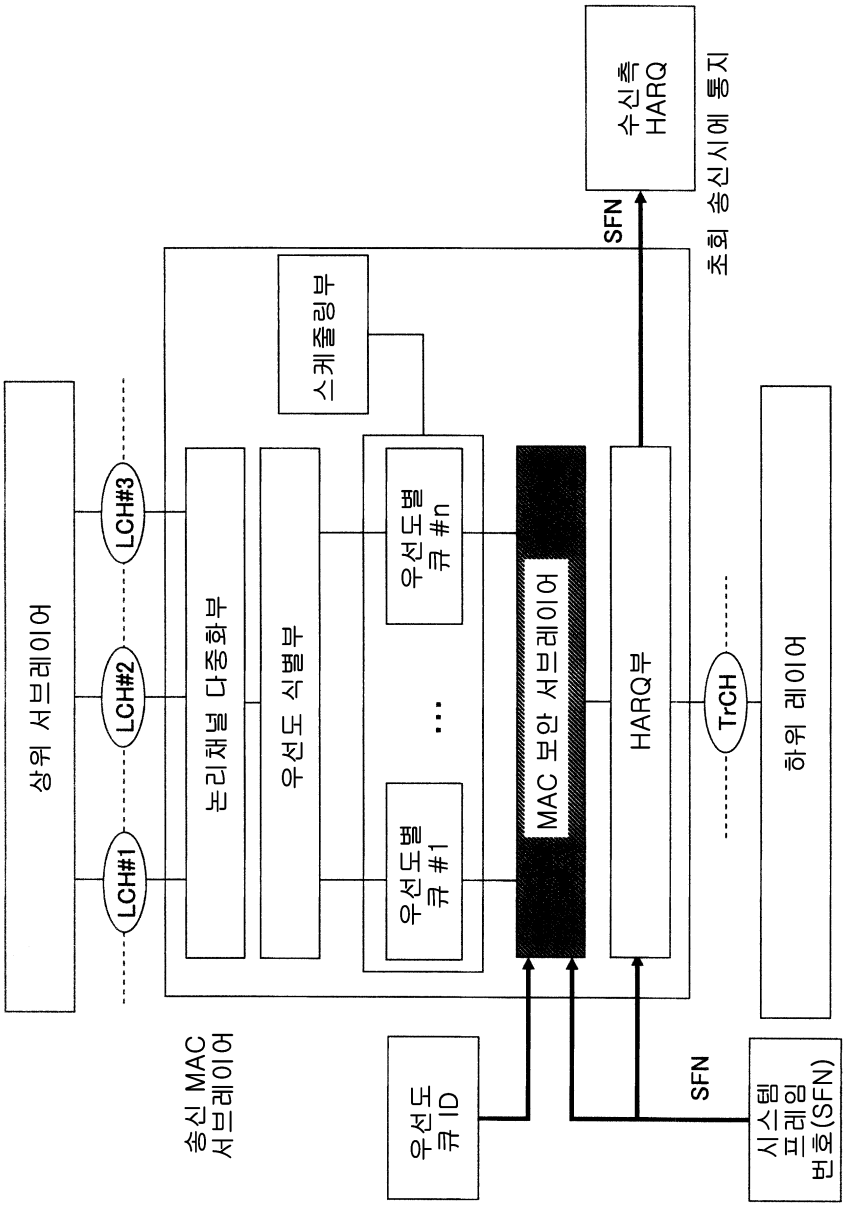
도면3


RLC-PDU+HFN의
시퀀스 번호
COUNT
논리채널 식별자
BEARER
전송방향
DIRECTION
마스크 길이
LENGTH
암호키
암호화 알고리즘
마스크
XOR
암호화 전의
RLC PDU
(데이터 부분)
암호화된
RLC PDU
(데이터 부분)

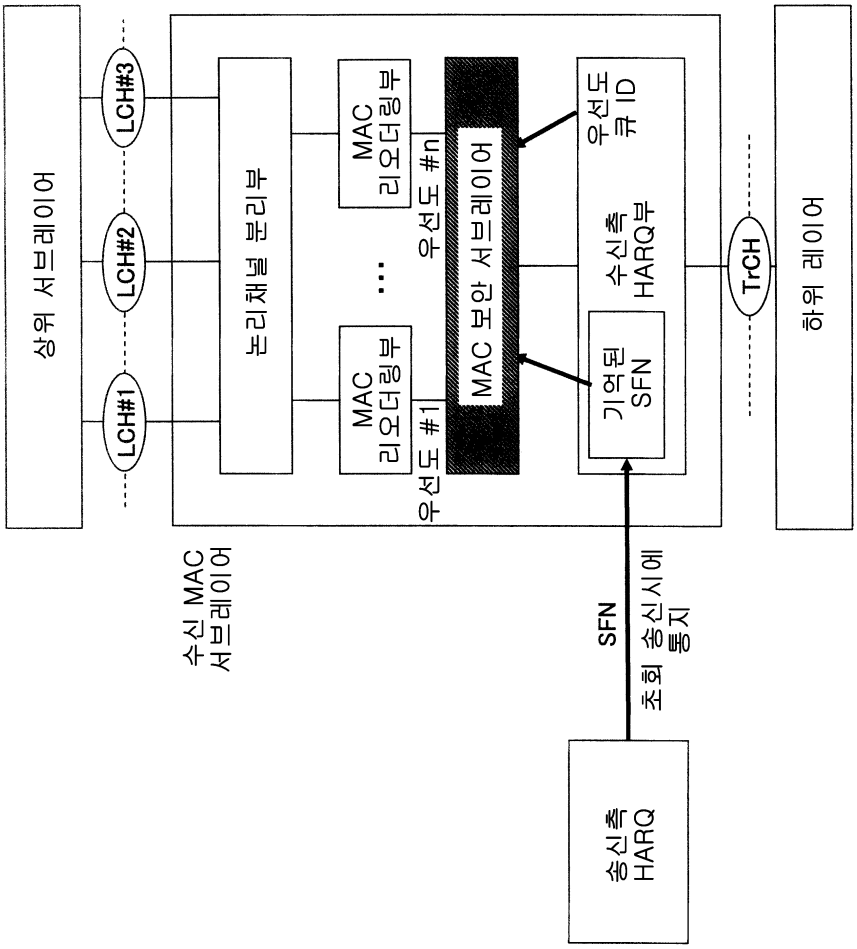
도면4


HFN
SN
010
00
010
01
010
10
011
00
011
01
011
10
011
11
수신측
1주기 이상의 SN에
상당하는 PDU의 결락
동기 불일치 발생
HFN
SN
010
00
010
01
010
10
010
11
011
00
011
01
011
10
011
11
100
00
100
01
100
10
100
11
송신측

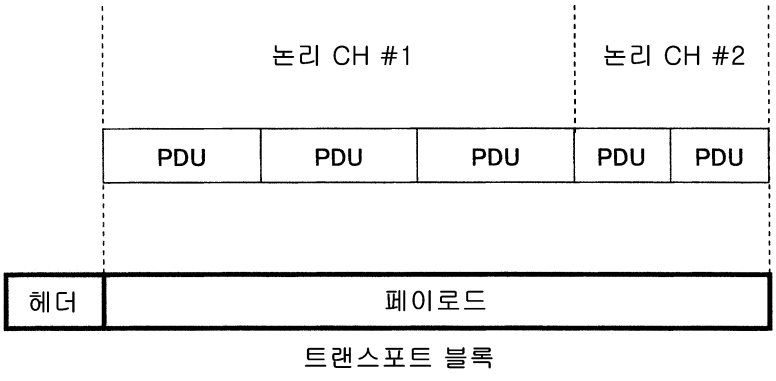
도면5


상위 서브레이어
LCH#3
LCH#2
LCH#1
논리채널 다중화부
우선도 식별부
스케줄링부
우선도별 큐 #n
우선도별 큐 #1
MAC 보안 서브레이어
HARQ부
TrCH
하위 레이어
수신측 HARQ
SFN
초회 송신시에 통지
송신 MAC 서브레이어
우선도 큐 ID
SFN
시스템 프레임 번호(SFN)

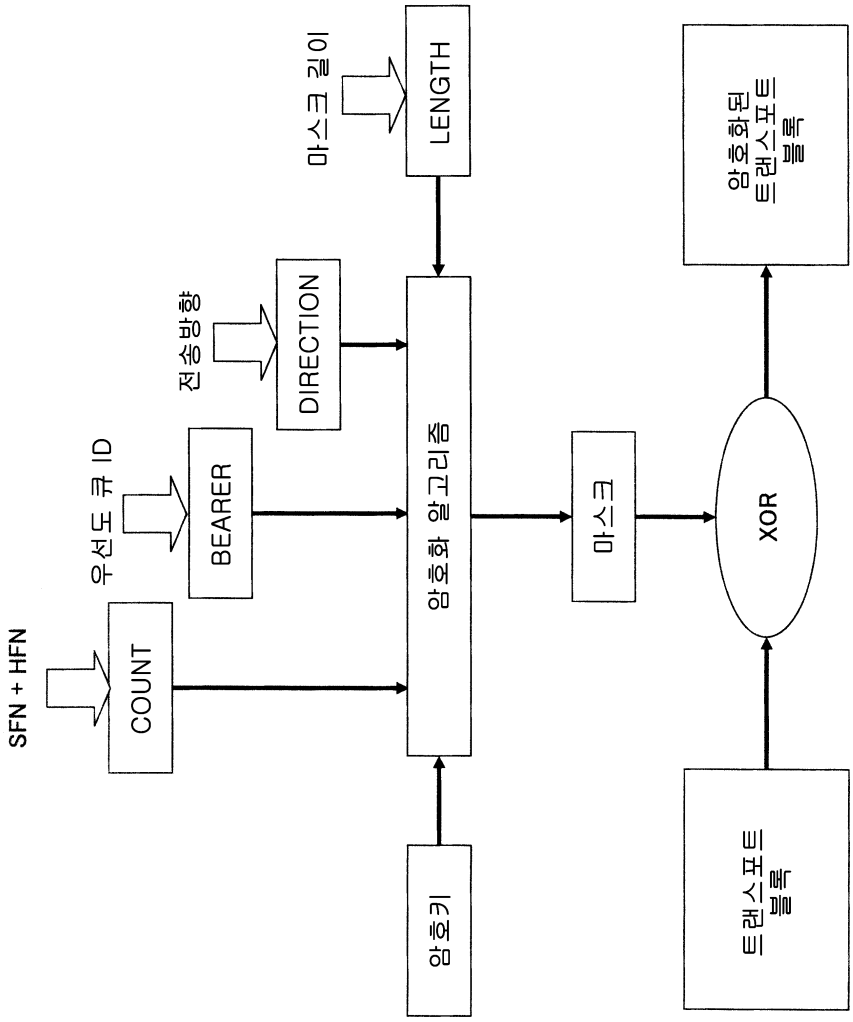
도면6


상위 서브레이어
LCH#3
LCH#2
LCH#1
논리채널 분리부
MAC 리오더링부
우선도 #n
MAC 리오더링부
우선도 #1
MAC 보안 서브레이어
우선도 큐 ID
수신측 HARQ부
기억된 SFN
TrCH
하위 레이어
수신 MAC 서브레이어
SFN 초회 송신시에 통지
송신측 HARQ

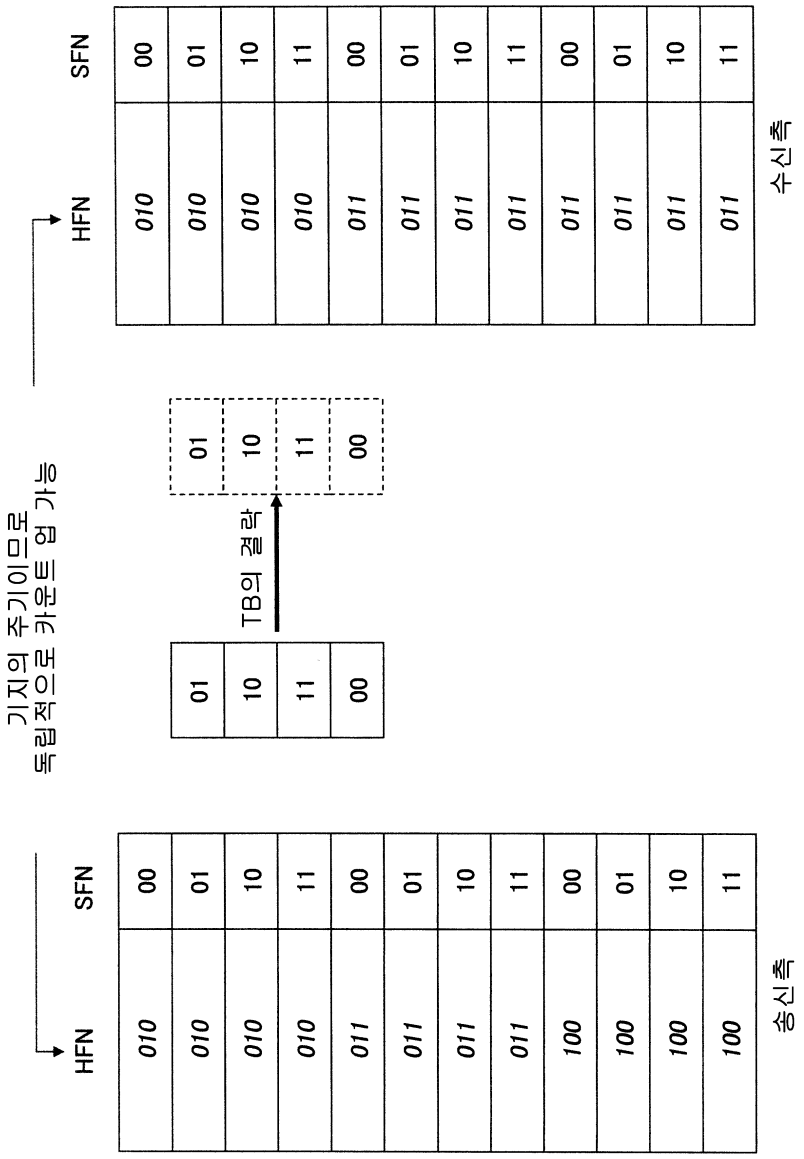
도면7


논리 CH #1
논리 CH #2
PDU
PDU
PDU
PDU
PDU
헤더
페이로드
트랜스포트 블록

도면8


SFN + HFN
COUNT
우선도 큐 ID
BEARER
전송방향
DIRECTION
마스크 길이
LENGTH
암호키
암호화 알고리즘
마스크
XOR
트랜스포트 블록
암호화된 트랜스포트 블록

도면9


송신측
HFN
SFN
010 00
010 01
010 10
010 11
011 00
011 01
011 10
011 11
100 00
100 01
100 10
100 11
기지의 주기이므로
독립적으로 카운트 업 가능
TB의 결락
01
10
11
00
수신측
HFN
SFN
010 00
010 01
010 10
010 11
011 00
011 01
011 10
011 11
011 00
011 01
011 10
011 11

도면10

