



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2011-0122708  
 (43) 공개일자 2011년11월10일

- (51) Int. Cl.  
     H04L 9/00 (2006.01) H04L 12/56 (2006.01)  
     H04B 7/26 (2006.01)
- (21) 출원번호 10-2011-7020378
- (22) 출원일자(국제출원일자) 2010년03월01일  
     심사청구일자 2011년09월01일
- (85) 번역문제출일자 2011년09월01일
- (86) 국제출원번호 PCT/US2010/025762
- (87) 국제공개번호 WO 2010/101825  
     국제공개일자 2010년09월10일
- (30) 우선권주장  
     12/587,166 2009년09월30일 미국(US)  
     61/156,882 2009년03월03일 미국(US)

- (71) 출원인  
     인텔 코오퍼레이션  
     미합중국 캘리포니아 산타클라라 미션 칼리지 블러바드 2200
- (72) 발명자  
     존스톤, 데이비드  
     미국 97006 오레곤주 비버튼 노쓰웨스트 보네빌 루프 14675
- (74) 대리인  
     양영준, 백만기

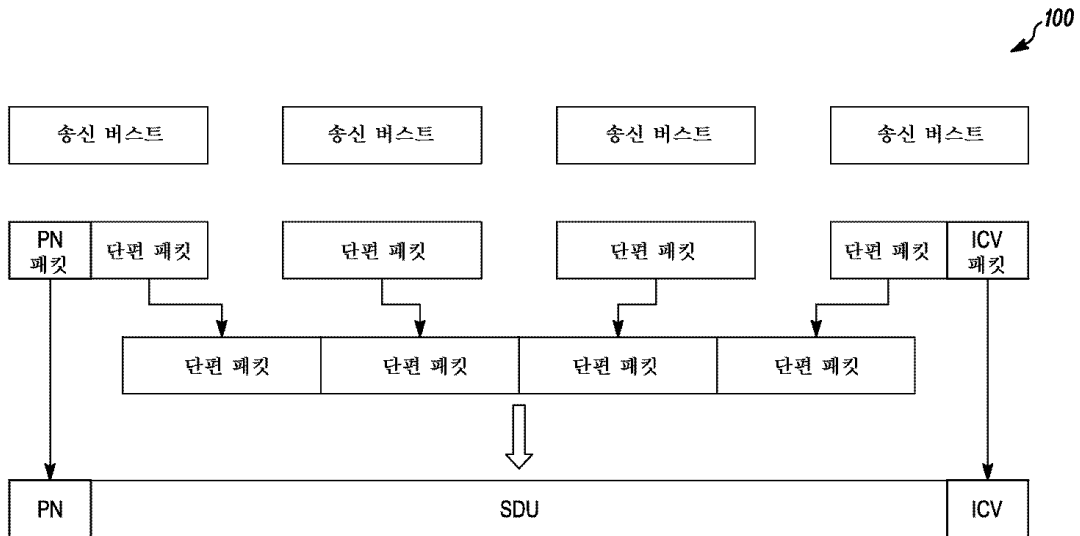
전체 청구항 수 : 총 12 항

**(54) 적응 패킷 암호화**

**(57) 요약**

본 발명의 실시예들은 적응 패킷 암호화를 위한 방법들 및 장치를 제공한다.

**대표도**



## 특허청구의 범위

### 청구항 1

무선 네트워크에서 통신 가능하며, PN(Packet Number) 및 ICV(Integrity Check Value)를 PDU(packet data unit)들의 스트림 내의 개별 PDU들로서 지정 가능한 트랜스미터 - PN-PDU와 ICV-PDU 사이의 모든 데이터는 연결된 PDU들의 단일 페이로드(payload)로서 암호화될 것임 - 를 포함하는 장치.

### 청구항 2

제1항에 있어서,  
상기 PN 및 ICV는 하나 또는 그 이상의 프레임들에 걸칠 수 있는 장치.

### 청구항 3

제1항에 있어서,  
상기 트랜스미터는 전송되는 트래픽의 종류에 대해 효율적인 방식으로 그것이 암호화하는 필드의 크기를 선택하도록 적응되는 장치.

### 청구항 4

제3항에 있어서,  
보호된 트래픽은 항상 PN 및 ICV 쌍 사이에 있으며, 평문(plaintext) 트래픽이 ICV의 뒤를 이을 것인 장치.

### 청구항 5

적용 패킷 암호화의 방법으로서,  
PN 및 ICV를 PDU들의 스트림 내의 개별 PDU들로서 지정하는 단계 - PN-PDU와 ICV-PDU 사이의 모든 데이터는 연결된 PDU들의 단일 페이로드로서 암호화될 것임 - 를 포함하는 적용 패킷 암호화 방법.

### 청구항 6

제5항에 있어서,  
상기 PN 및 ICV에 의해 하나 또는 그 이상의 프레임들에 걸치게 하는 단계를 더 포함하는 적용 패킷 암호화 방법.

### 청구항 7

제5항에 있어서,  
송신기는 전송되는 트래픽의 종류에 대해 효율적인 방식으로 그것이 암호화하는 필드의 크기를 선택하도록 적응되는 적용 패킷 암호화 방법.

### 청구항 8

제7항에 있어서,  
보호된 트래픽을 PN 및 ICV 쌍 사이에 배치하는 단계를 더 포함하며, 평문 트래픽이 ICV의 뒤를 이을 것인 적용 패킷 암호화 방법.

### 청구항 9

컴퓨터 실행 가능한 명령어들로 인코딩된 컴퓨터 판독 가능 매체로서,  
액세스될 때 기계로 하여금,

적용 패킷 암호화를 사용하며, PN 및 ICV를 PDU들의 스트림 내의 개별 PDU들로서 지정하는 단계 - PN-PDU 및 ICV-PDU 사이의 모든 데이터는 연결된 PDU들의 단일 페이로드로서 암호화될 것임 -

를 포함하는 동작을 수행하도록 하는 컴퓨터 판독 가능 매체.

**청구항 10**

제9항에 있어서,

상기 PN 및 ICV에 의해 하나 또는 그 이상의 프레임들에 걸쳐서 하는 것을 제공하는 추가적인 명령어들을 더 포함하는 컴퓨터 판독 가능 매체.

**청구항 11**

제9항에 있어서,

송신기는 전송되는 트래픽의 종류에 대해 효율적인 방식으로 그것이 암호화하는 필드의 크기를 결정하도록 적응되는 컴퓨터 판독 가능 매체.

**청구항 12**

제11항에 있어서,

보호된 트래픽을 PN 및 ICV 사이에 배치하는 것을 제공하는 추가적인 명령어들을 더 포함하며, 평문 트래픽이 ICV의 뒤를 이을 것인 컴퓨터 판독 가능 매체.

**명세서**

**배경기술**

[0001] 무선 통신에서, 보안 요구는 데이터를 암호화하는 것을 요구할 수 있다. 그러나, PN(Packet Number) 및 ICV(Integrity Check Value)를 추가해야 하는 필요 때문에 일부 데이터를 암호화하는 것은 오버헤드를 요구할 수 있다. 예컨대, IEEE(Institute for Electrical and Electronic Engineering) 802.16e(WiMAX)에서 오버헤드는 12바이트이나, 이에 제한되지 않는다.

[0002] 패킷 통신 시스템에서, 퍼센티지 오버헤드는 큰 패킷들보다 작은 패킷들에서 더 크다. 그러나, 패킷들이 단편화되는 WiMAX와 같은 시스템에서, 패킷당 다수의 암호 오버헤드(crypto overhead)들이 존재할 것이기 때문에 이익이 감소한다. 예컨대, 큰 패킷들이 각각이 암호 오버헤드를 갖는 다수의 작은 단편(fragment)들로서 전송되는 셀-에지 시나리오에서 효율은 매우 떨어진다.

[0003] 작고 큰 패킷들을 갖는 작고 큰 버스트(burst)들에 대해 효율적인 암호화 적용 방법이 요구된다.

**도면의 간단한 설명**

[0004] 도 1은 작은 단편 크기를 갖는 큰 단편 패킷들에 대한 PN 및 ICV 배치를 도시한다.

도 2는 실시예에 따라 패킹된(packed) 버스트들의 마지막 및 제1 PDU들이 단편화되어 있는 전형적인 대량 데이터 시나리오를 도시한다.

도 3은 실시예에 따른 하나의 보호된 PDU.

도 4는 본 발명의 실시예의 ICV를 뒤를 잇는 평문(plaintext) 관리 패킷을 도시한다.

**발명을 실시하기 위한 구체적인 내용**

[0005] 상세한 설명에서, 본 발명의 실시예들에 대한 완전한 이해를 제공하기 위해 다수의 특정한 세부 사항들이 진술된다. 그러나, 본 기술분야의 기술자들은 본 발명의 실시예들이 이러한 특정한 세부 사항들 없이 실행될 수 있다는 것을 이해할 것이다. 다른 경우들에서, 앞서 말한 실시예들을 모호하게 하지 않기 위해 잘 알려진 방법들, 절차들, 및 기법들은 설명되지 않는다.

[0006] 뒤따르는 상세한 설명의 일부 부분들은 컴퓨터 메모리 내의 데이터 비트들 또는 2진(binary) 디지털 신호들에 대한 연산들의 알고리즘, 및 기호적 표현으로서 제시된다. 이러한 알고리즘적 설명 및 표현들은 데이터 프로세

싱 기술분야의 기술자들이 그들의 연구 내용을 그 기술분야의 다른 기술자들에게 전달하기 위해 사용되는 기법 들일 수 있다.

- [0007] 여기서 일반적으로, 알고리즘은 요구되는 결과로 연결되는 행위 또는 동작들의 일관성 있는 시퀀스로 간주된다. 이들은 물리량들의 물리적 조작들을 포함한다. 보통 이러한 양들은 저장, 이동, 조합, 비교, 및 달리 조작될 수 있는 전기적 또는 자기적 신호의 형태를 갖지만, 반드시 그런 것은 아니다. 주로 일반적인 사용의 이유로 이러한 신호들을 비트, 값, 요소, 기호, 문자, 용어, 숫자, 또는 유사한 것들로서 명명하는 것이 때때로 편리하다는 것이 증명되었다. 그러나, 이러한 및 유사한 모든 용어들은 적당한 물리량과 연관될 것이며, 단지 이 양(quantity)들에 적용된 편리한 라벨임을 이해해야 한다.
- [0008] 특히 다르게 진술되지 않는다면, 하기 논의로부터 명백한 것과 같이, 본 명세를 통틀어 "처리(processing)" 또는 "컴퓨팅(computing)" 또는 "계산(calculating)" 또는 "결정(determining)" 등과 같은 용어들을 이용한 논의는 컴퓨팅 시스템의 레지스터 또는 메모리 내의 전자적 양과 같은 물리량으로서 표시된 데이터를 조작하고, 컴퓨팅 시스템의 메모리, 레지스터 또는 다른 그러한 정보 저장, 송신, 또는 디스플레이 장치들 내의 물리량으로서 유사하게 표시되는 다른 데이터로 변환하는 컴퓨터 또는 컴퓨팅 시스템, 또는 유사한 전자 컴퓨팅 장치의 액션 및 프로세스에 관한 것임을 인식한다.
- [0009] 본 발명의 실시예들은 본원의 동작들을 수행하기 위한 장치들을 포함할 수 있다. 이 장치는 요구되는 목적들을 위해 특별히 구축될 수 있거나, 또는 컴퓨팅 장치 내에 저장된 프로그램에 의해 선택적으로 활성화 또는 재구성되는 범용 컴퓨팅 장치를 포함할 수 있다. 그러한 프로그램은 플로피 디스크, 광디스크, CD-ROM, 자기-광 디스크를 포함하는 임의의 종류의 디스크, 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), EPROM, EEPROM, 플래시 메모리, 자기 또는 광학 카드, 또는 전자적 명령을 저장하기 적합하며 컴퓨팅 장치를 위한 시스템 버스에 연결될 수 있는 임의의 다른 종류의 매체를 포함하지만 이들에 제한되지 않는 저장 매체에 저장될 수 있다.
- [0010] 본원에 소개된 프로세스 및 디스플레이는 본질적으로 임의의 특정 컴퓨팅 장치 또는 다른 장치와 연관되지 않는다. 본원의 가르침에 따라 다양한 범용 시스템들이 프로그램들과 함께 사용될 수 있으며, 또는 요구되는 방법을 수행하기 위해 더 특화된 장치를 구성하는 것이 편리하다는 것이 증명될 수 있다. 이러한 다양한 시스템들을 위해 요구되는 구조는 아래의 설명으로부터 분명해질 것이다. 게다가, 본 발명의 실시예들은 임의의 특정 프로그래밍 언어에 관련하여 설명되지 않는다. 본원에서 설명한 것과 같은 본 발명의 가르침을 구현하기 위해 다양한 프로그래밍 언어들이 사용될 수 있다는 것을 인식할 것이다.
- [0011] 하기 설명 및 청구항들에서, 용어 결합된(coupled) 및 연결된(connected)이 그들의 파생어들과 함께 사용될 수 있다. 특정 실시예들에서, 연결된(connected)은 둘 또는 그 이상의 요소들이 서로 직접적인 물리적 또는 전기적 접촉 상태임을 나타내기 위해 사용될 수 있다. 결합된(coupled)은 둘 또는 그 이상의 요소들이 직접적인 물리적 또는 전기적 접촉 상태임을 나타낼 수 있다. 그러나, 결합된(coupled)은 둘 또는 그 이상의 요소들이 서로 직접적으로 접촉하지 않지만, 여전히 서로 협동 또는 상호 작용할 수 있다는 것을 또한 의미할 수 있다.
- [0012] 본 명세서에서의 "일 실시예" 또는 "실시예"의 참조는, 그 실시예와 관련하여 설명한 특정한 특징, 구조, 또는 특성이 본 발명의 적어도 하나의 실시예에 포함될 수 있다는 것을 의미한다는 것에 주목할 만 하다. 본 명세서의 다양한 곳들에서의 어구 "일 실시예" 또는 "실시예"가 나온다고 해서 반드시 동일한 실시예를 참조하는 것은 아니며, 서로 다른 실시예들을 참조할 수 있다.
- [0013] 본 발명의 실시예들은 다양한 어플리케이션들에서 사용될 수 있다는 것을 이해해야 한다. 본원에 개시된 회로들은 라디오 시스템의 송신기 및 수신기와 같은 많은 장치들에서 사용될 수 있으나, 본 발명은 이에 제한되지 않는다. 본 발명의 범위 내에 포함되도록 의도되는 라디오 시스템들은, 단지 예로서 무선 네트워크 인터페이스 장치 및 네트워크 인터페이스 카드들(NICs), 기지국, 액세스 포인트(APs), 게이트웨이, 브리지, 허브, 셀룰러 라디오 전화 통신 시스템, 위성 통신 시스템, 양방향 라디오 통신 시스템, 단방향 페이지, 양방향 페이지, 개인 통신 시스템(PCS), PC, PDA 등을 포함하는 WLAN 장치 및 WWAN 장치를 포함하나, 본 발명의 범위는 이에 제한되지 않는다.
- [0014] 본원에 사용된 용어 패킷은 노드들 또는 스테이션들 사이에서 또는 네트워크를 통해 라우팅되거나 송신될 수 있는 데이터의 단위를 포함할 수 있다. 본원에 사용된 용어 패킷은 프레임, 프로토콜 데이터 단위들 또는 데이터의 다른 단위들을 포함할 수 있다. 패킷은 비트들의 그룹을 포함할 수 있으며, 이는 예컨대 하나 또는 그 이상의 어드레스 필드, 컨트롤 필드 및 데이터를 포함할 수 있다. 데이터 블록은 데이터 또는 정보 비트의 임의의 단위일 수 있다.

- [0015] 같은 숫자들이 같은 요소들을 나타내는 도면들을 참조하여, 도 1a는 본 발명의 일 실시예에 따른 무선 통신 시스템의 예를 도시한 도면이다. 도 1a에 도시된 통신 시스템(100a)에서, 사용자 무선 시스템(116)은 안테나(117) 및 프로세서(112)에 연결된 무선 트랜스미터(110)를 포함할 수 있다. 일 실시예에서, 프로세서(112)는 하나의 프로세서를 포함할 수 있거나, 또는 대안적으로 베이스밴드 프로세서 및 어플리케이션 프로세서를 포함할 수 있으나, 본 발명의 범위는 이에 제한되지 않는다. 일 실시예에 따라, 프로세서(112)는 베이스밴드 프로세서 및 MAC(Medium Access Control)을 포함할 수 있다.
- [0016] 프로세서(112)는 DRAM과 같은 휘발성 메모리, 플래시 메모리와 같은 비휘발성 메모리를 포함할 수 있으며, 또는 대안적으로 하드 디스크 드라이브와 같은 다른 종류의 저장 장치를 포함할 수 있는 메모리(114)에 연결될 수 있으나, 본 발명의 범위는 이에 제한되지 않는다. 메모리(114)의 일부 또는 전부는 프로세서(112)와 동일한 집적 회로에 포함될 수 있거나, 또는 대안적으로 메모리(114)의 일부 또는 전부는 프로세서(112)의 집적 회로 외부에 있는, 집적 회로 또는 예컨대 하드 디스크 드라이브와 같은 다른 매체 위에 배치될 수 있으나, 본 발명의 범위는 이에 제한되지 않는다. 일 실시예에 따라, 무선 시스템(116)이 다양한 태스크들(이들 중 일부는 본원에서 설명됨)을 수행하는 것을 허용하도록 프로세서(112)에 의해 실행될 소프트웨어가 메모리(114)에 제공될 수 있다.
- [0017] 무선 시스템(116)은 무선 통신 링크(134)를 통해 액세스 포인트(AP)(128)(또는 다른 무선 시스템)와 통신할 수 있으며, 액세스 포인트(128)는 적어도 하나의 안테나(118)를 포함할 수 있다. 안테나들(117 및 118)은 각각, 예컨대 지향성(directional) 안테나 또는 전방향(omni directional) 안테나일 수 있으나, 본 발명은 그에 제한되지 않는다. 도 1에 도시되지 않았지만, AP(128)는 예컨대 무선 트랜스미터, 프로세서, 메모리, 및 AP(128)가 다양한 기능들을 수행하는 것을 허용하도록 메모리 내에 제공된 소프트웨어를 포함하는 무선 시스템(116)과 유사한 구조를 포함할 수 있다. 실시예에서, 무선 시스템(116) 및 AP(128)는 WLAN 시스템과 같은 무선 통신 시스템에서 스테이션들로 간주될 수 있다.
- [0018] 무선 통신 링크(134)를 통해 액세스 포인트(128)와 통신함으로써 무선 시스템(116)이 (네트워크(130)에 연결된 장치들을 포함하는) 네트워크(130)와 통신할 수 있도록, 액세스 포인트(128)는 네트워크(130)에 연결될 수 있다. 네트워크(130)는 전화 네트워크 또는 인터넷과 같은 공중 네트워크를 포함할 수 있거나, 또는 대안적으로 네트워크(130)는 인트라넷과 같은 사설 네트워크, 또는 공중 및 사설 네트워크의 조합을 포함할 수 있으나, 본 발명의 범위는 이에 제한되지 않는다.
- [0019] 무선 시스템(116)과 액세스 포인트(128) 사이의 통신은 무선 근거리 통신망(WLAN), 예컨대 IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.15, IEEE 802.16 등과 같은 IEEE 표준에 따를 수 있는 네트워크를 통해 구현될 수 있으나, 본 발명의 범위는 이에 제한되지 않는다.
- [0020] 다른 실시예에서, 무선 시스템(116)과 액세스 포인트(128) 사이의 통신은 3GPP 또는 IEEE 802.16 표준에 따르는 셀룰러 통신 네트워크를 통해 구현될 수 있으나, 본 발명의 범위는 이에 제한되지 않는다.
- [0021] 단일 반송파를 통해 정보가 송신될 수 있는 단일 반송파 시스템들에 본 발명의 하나 또는 그 이상의 양태들이 적용될 수 있다. 대안적으로, 예컨대 OFDM(Orthogonal Frequency Division Multiplexing) 시스템과 같은, 다수의 반송파들 또는 부반송파들을 통해 정보가 송신될 수 있는 다중반송파 시스템들에 본 발명의 하나 또는 그 이상의 양태들이 적용될 수 있으나, 본 발명은 이에 제한되지 않는다.
- [0022] 상기 진술한 것과 같이, 이전의 통신 암호 포맷들은 예컨대 PDU 또는 SDU 또는 송신 버스트와 같은 일부 데이터 유닛에 대해 작용했다. 본 발명의 실시예들은 암호 정보를 데이터 정보로부터 분리하며, 이는 PDU, SDU, 또는 송신 버스트 경계들에 상관없는 PN 및 ICV들의 배치를 허용한다. 본 발명은 PDU, SDU, 또는 버스트 경계의 한계가 없는 암호화의 시작 및 끝점을 자유롭게 지정하는 능력을 제공한다. 특별한 PDU 포맷 없이 PN 및 ICV, 및 또다른 PDU의 인코딩. 본 발명의 실시예들은 페이로드(payload)에 더하여, PN(Packet Number) 및 ICV(Integrity Check Value)를 포함하는 프로토콜 데이터 단위(PDU) 또는 서비스 데이터 단위(SDU)들을 정의하는 대신, PN 및 ICV를 PDU들의 스트림에서 개별 PDU들로 지정한다.
- [0023] 본 발명의 실시예들은 PN-PDU 및 ICV-PDU 사이의 모든 데이터가 연결된 PDU들의 단일 페이로드로서 암호화되는 것을 제공한다. PN 및 ICV가 그들 자신의 PDU 내에 있으며 데이터 PDU들로부터 독립적이므로 그들은 하나 또는 그 이상의 프레임들에 걸쳐질 수 있다.
- [0024] 이는 송신기가 그것이 암호화하는 필드의 크기를 전송되는 트래픽의 종류에 대해 효율적인 방식으로 자유롭게 결정하도록 한다. 예컨대, 작은 격리된 패킷들은 그들 자신의 PN 및 ICV를 얻을 것이다. 약한 신호 상태에서,

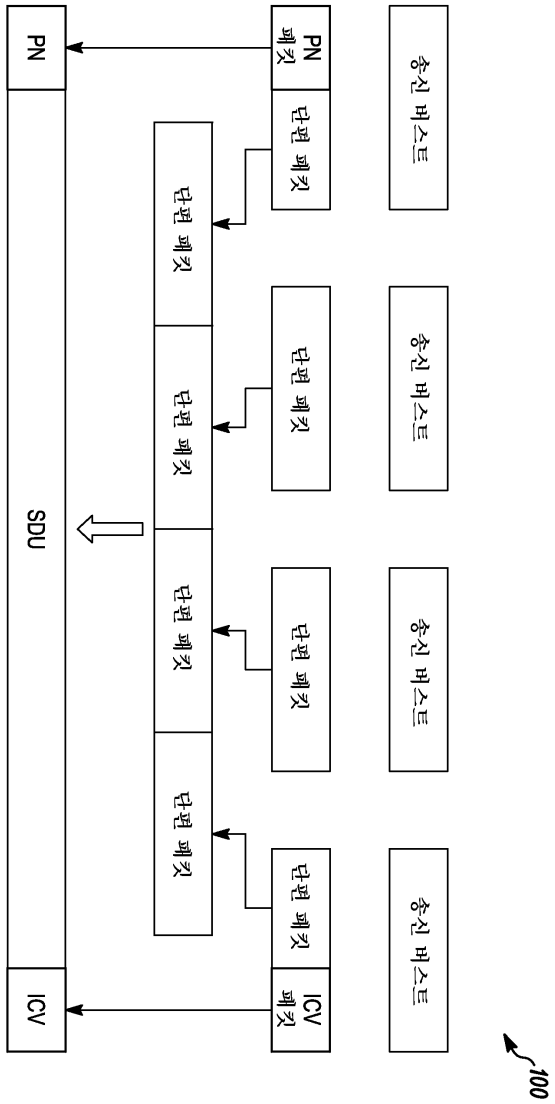
다수의 송신들에 걸쳐 확산된 큰 단편화된 패킷들은 하나의 PN 및 ICV를 공유할 것이다. 좋은 신호 상태에서, 다수의 패킹된(packed) PDU들을 보유하는 큰 버스트들은 버스트를 보호하기 위해 하나의 PN 및 ICV를 사용할 것이다. 보호된 트래픽은 항상 PN 및 ICV 쌍 사이에 있을 것이다. 평문(plaintext) 트래픽(예컨대, PKM 관리 메시지)은 ICV의 뒤를 이을 것이다.

[0025] 도 1은, 100에서, 본 발명의 일 실시예에 따라 작은 단편 크기를 갖는 큰 단편 패킷에 대한 PN 및 ICV 배치를 도시한다. (일반적으로 200으로 도시된) 도 2는 실시예에 따라 마지막 및 제1 PDU들이 단편화되어 있는 전형적인 대량 데이터 시나리오를 도시한다. 도 2에서, 패킹된 SDU들에 대한 통상의 거동을 볼 수 있으며, 마지막 단편화된 PDU 전에 ICV+PN이 삽입된다. 그러므로, 가운데 버스트의 모든 완료된 PDU들은 해독되고 전달될 수 있는 한편, 나머지 단편들이 수신될 때까지 전달될 수 없는 새로운 단편은 후속 버스트에서의 ICV의 수신에 이어 해독된다. 이 예에서, 버스트당 암호화(per-burst encryption)의 경우에 비하여 PN+ICV의 하나 더 적은 인스턴스가 존재한다.

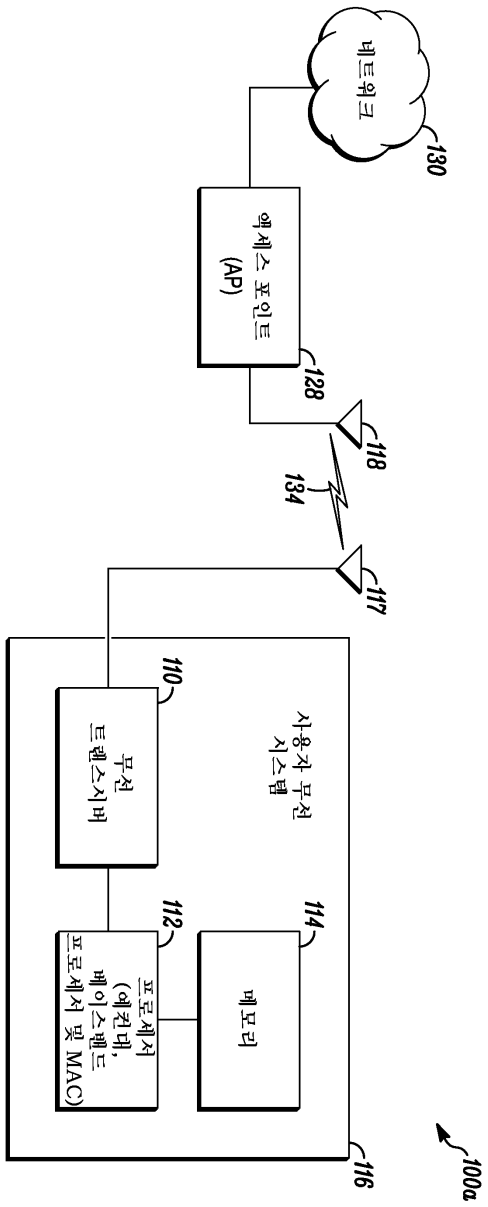
[0026] 도 3은 300에서 실시예에 따른 하나의 보호된 PDU를 도시한다. 도 4는 400에서 본 발명의 실시예들의 ICV의 뒤를 잇는 평문 관리 패킷을 도시한다.

[0027] 본 발명의 실시예들의 특정한 특징들이 본원에 설명한 것과 같이 예시되었으나, 다양한 변형, 대응, 변경 및 동등물들이 본 기술분야의 기술자들의 뇌리에 이제 떠오를 것이다. 그러므로, 첨부된 청구항들은 본 발명의 실시예들의 진의 내에 포함되는 모든 그러한 변형들 및 변경들을 포함하는 것으로 의도됨을 이해할 것이다.

도면  
도면1

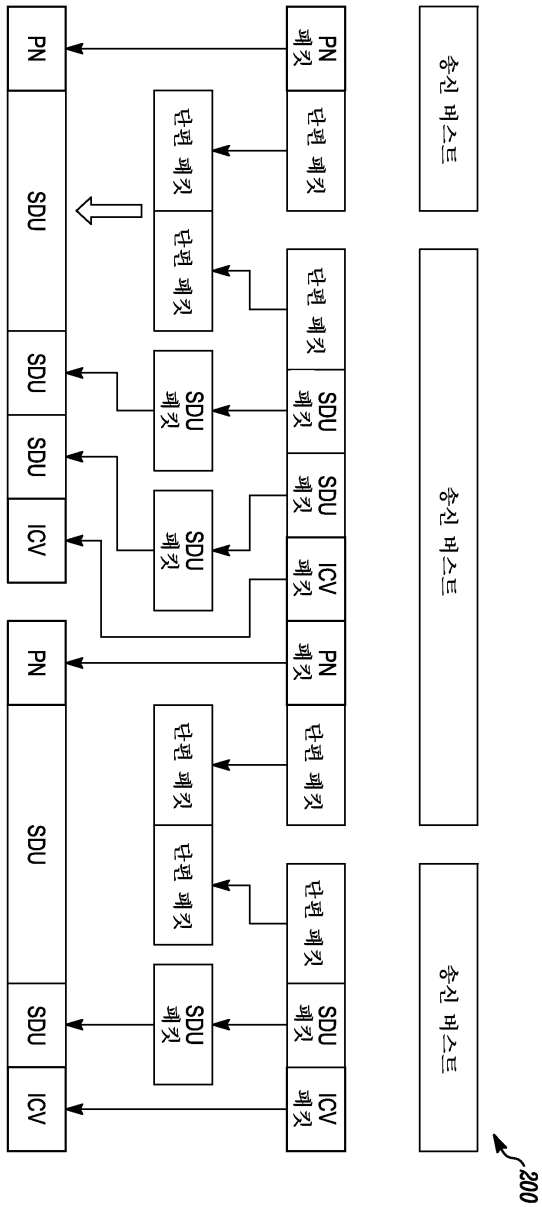


도면1a





도면2

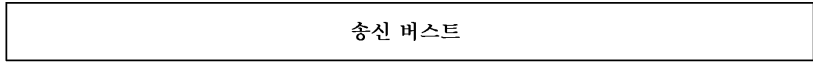


도면3



도면4

400



단편 패킷	SDU 패킷	SDU 패킷	ICV 패킷	평문 관리 패킷	PN 패킷	단편 패킷
-------	-----------	-----------	-----------	-------------	----------	-------