(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2025 년 7 월 10 일 (10.07.2025)

WIPO | PCT

(10) 국제공개번호
WO 2025/147145 A1

(51) 국제특허분류:
H04W 12/106 (2021.01) *H04W 12/0471* (2021.01)
H04L 1/1607 (2023.01) *H04W 84/12* (2009.01)

(21) 국제출원번호: PCT/KR2025/000145

(22) 국제출원일: 2025 년 1 월 3 일 (03.01.2025)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2024-0001748 2024 년 1 월 4 일 (04.01.2024) KR

(71) 출원인: 엘지전자 주식회사 (**LG ELECTRONICS INC.**) [KR/KR]; 07336 서울특별시 영등포구 여의대로 128 (KR).

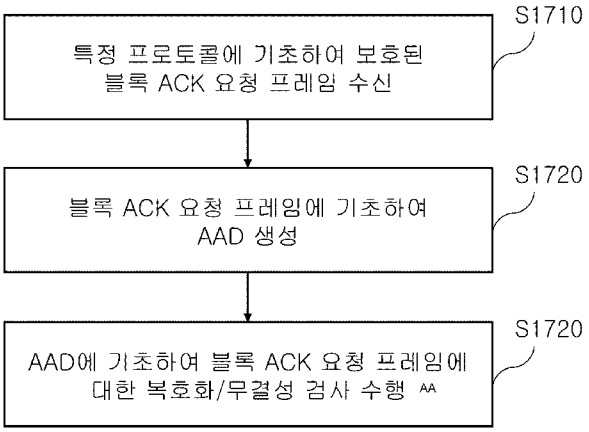
(72) 발명자: **백선희 (BAEK, Sunhee)**; 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터 (KR). **최진수 (CHOI, Jinsoo)**; 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터 (KR). **장인선 (JANG, Insun)**; 06772 서울특별시 서초구 양재대로 11길 19 LG전자 특허센터 (KR). **김건환 (KIM, Geonhwan)**; 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터 (KR). **윤예린 (YOON, Yelin)**; 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터 (KR). **차동주 (CHA, Dongju)**; 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터 (KR).

(74) 대리인: **최윤서 등 (CHOE, Yun Seo** et al.); 06253 서울특별시 강남구 강남대로 318, 7층 윤특허법률사무소 (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ,

(54) Title: METHOD AND DEVICE FOR TRANSMITTING OR RECEIVING PROTECTED CONTROL FRAME IN WIRELESS LAN SYSTEM

(54) 발명의 명칭: 무선랜 시스템에서 보호된 제어 프레임 송신 또는 수신 방법 및 장치



S1710 ... Receive block ACK request frame protected on basis of specific protocol
S1720 ... Generate AAD on basis of block ACK request frame
AA ... Perform decoding/integrity checking for block ACK request frame on basis of AAD

(57) Abstract: A method and a device for transmitting or receiving a protected control frame in a wireless LAN system are disclosed. A method according to one embodiment of the present disclosure may comprise the steps of: receiving, by a first station (STA), a block ACK request frame protected on the basis of a specific protocol from a second STA; generating, by the first STA, an AAD on the basis of the block ACK request frame; and performing, by the first STA, at least one of decoding or integrity checking for the block ACK request frame on the basis of the AAD. The AAD may be based on one or more fields included in a MAC header of the block ACK request frame, or based on one or more subfields included in the MAC header and one or more subfields included in a block ACK request control field or a block ACK request information field of the block ACK request frame.

WO 2025/147145 A1

[다음 쪽 계속]

EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 무선랜 시스템에서 보호된 제어 프레임 송신 또는 수신 방법 및 장치가 개시된다. 본 개시의 일 실시예에 따른 방법은, 제1 스테이션(STA)에 의해서, 특정 프로토콜에 기초하여 보호된 블록 ACK 요청 프레임을 제2 STA으로부터 수신하는 단계; 상기 제1 STA에 의해서, 상기 블록 ACK 요청 프레임에 기초하여 AAD를 생성하는 단계; 및 상기 제1 STA에 의해서, 상기 AAD에 기초하여 상기 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행하는 단계를 포함할 수 있다. 상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초할 수 있다.

발명의 설명

발명의 명칭: 무선랜 시스템에서 보호된 제어 프레임 송신 또는 수신 방법 및 장치

기술분야

[1] 본 개시는 무선랜(Wireless Local Area Network, WLAN) 시스템에서 보호된 제어 프레임을 송신 또는 수신하는 방법 및 장치에 관한 것이다.

배경기술

[2] 무선랜(WLAN)에 대해서 송신 레이트 향상, 대역폭 증가, 신뢰성 향상, 에러 감소, 레이턴시 감소 등을 위한 새로운 기술이 도입되어 왔다. 무선랜 기술 중에서, IEEE(Institute of Electrical and Electronics Engineers) 802.11 계열의 표준을 Wi-Fi 라고 칭할 수 있다. 예를 들어, 최근에 무선랜에 도입된 기술은, 802.11ac 표준의 VHT(Very High-Throughput)를 위한 개선사항(enhancement), IEEE 802.11ax 표준의 HE(High Efficiency)를 위한 개선사항 등을 포함한다.

[3] 보다 향상된 무선 통신 환경을 제공하기 위해서, EHT(Extremely High Throughput)를 위한 개선 기술이 논의되고 있다. 예를 들어, 증가된 대역폭, 다중 대역의 효율적 활용, 증가된 공간 스트림을 지원하는 MIMO(Multiple Input Multiple Output), 다중 액세스 포인트(AP) 조정을 위한 기술이 연구되고 있으며, 특히 낮은 레이턴시(low latency) 또는 실시간(real time) 특성의 트래픽을 지원하기 위한 다양한 기술이 연구되고 있다. 나아가, EHT 기술의 개선 또는 확장을 포함하여, 극히 높은 신뢰성(ultra high reliability, UHR)을 지원하기 위한 새로운 기술이 논의되고 있다.

발명의 내용

기술적 과제

[4] 본본 개시의 기술적 과제는 무선랜 시스템에서 보호된 제어 프레임을 송신 또는 수신하는 방법 및 장치를 제공하는 것이다.

[5] 본 개시의 기술적 과제는 무선랜 시스템에서 블록 ACK(acknowledgement) 요청 프레임에 대해서 추가 인증 데이터(additional authentication data, AAD)에 기반하는 암호화(encryption)/복호화(decryption)/무결성 검사(integrity check)를 지원하는 방법 및 장치를 제공하는 것이다.

[6] 본 개시에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[7] 본 개시의 일 양상에 따른 방법은, 제1 스테이션(STA)에 의해서, 특정 프로토콜에 기초하여 보호된 블록 ACK(acknowledgement) 요청 프레임을 제2 STA으로부

터 수신하는 단계; 상기 제1 STA에 의해서, 상기 블록 ACK 요청 프레임에 기초하여 AAD(additional authentication data)를 생성하는 단계; 및 상기 제1 STA에 의해서, 상기 AAD에 기초하여 상기 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행하는 단계를 포함할 수 있다. 여기서, 상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초할 수 있다.

[8] 본 개시의 추가적인 양상에 따른 방법은, 제2 스테이션(STA)에 의해서, 특정 프로토콜에 기초하여 블록 ACK(acknowledgement) 요청 프레임에 대한 AAD(additional authentication data)를 생성하는 단계; 및 상기 제2 STA에 의해서, 상기 AAD에 기초하여 보호된 블록 ACK 요청 프레임을 제1 STA에게 송신하는 단계를 포함할 수 있다. 여기서, 상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드, 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초할 수 있다.

발명의 효과

[9] 본 개시에 따르면, 무선랜 시스템에서 보호된 제어 프레임을 송신 또는 수신하는 방법 및 장치가 제공될 수 있다.

[10] 본 개시에 따르면, 무선랜 시스템에서 블록 ACK(acknowledgement) 요청 프레임에 대해서 추가 인증 데이터(additional authentication data, AAD)에 기반하는 암호화(encryption)/복호화(decryption)/무결성 검사(integrity check)를 지원하는 방법 및 장치가 제공될 수 있다.

[11] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[12] 본 개시에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면은 본 개시에 대한 실시예를 제공하고, 상세한 설명과 함께 본 개시의 기술적 특징을 설명한다.

[13] 도 1은 본 개시의 일 실시예에 따른 무선 통신 장치의 블록 구성도를 예시한다.

[14] 도 2는 본 개시가 적용될 수 있는 무선랜 시스템의 예시적인 구조를 나타내는 도면이다.

[15] 도 3은 본 개시가 적용될 수 있는 링크 셋업(link setup) 과정을 설명하기 위한 도면이다.

[16] 도 4는 본 개시가 적용될 수 있는 백오프 과정을 설명하기 위한 도면이다.

[17] 도 5는 본 개시가 적용될 수 있는 CSMA/CA 기반 프레임 송신 동작을 설명하기 위한 도면이다.

[18] 도 6은 본 개시가 적용될 수 있는 무선랜 시스템에서 사용되는 프레임 구조의 예시를 설명하기 위한 도면이다.

[19] 도 7은 본 개시가 적용될 수 있는 IEEE 802.11 표준에서 정의되는 PPDU의 예시들을 도시한 도면이다.

[20] 도 8은 본 개시가 적용될 수 있는 4-웨이 핸드셰이킹 절차를 설명하기 위한 도면이다.

[21] 도 9는 본 개시가 적용될 수 있는 확대된(expanded) CCMP MPDU의 일 예시를 나타내는 도면이다.

[22] 도 10은 본 개시가 적용될 수 있는 CCMP 인캡슐레이션 블록 다이어그램을 나타낸다.

[23] 도 11은 기존(conventional) AAD의 포맷의 일 예시를 나타낸다.

[24] 도 12는 본 개시가 적용될 수 있는 CCMP 디캡슐레이션 블록 다이어그램을 나타낸다.

[25] 도 13은 본 개시가 적용될 수 있는 확대된(expanded) GCMP MPDU의 일 예시를 나타내는 도면이다.

[26] 도 14는 본 개시가 적용될 수 있는 GCMP 인캡슐레이션 블록 다이어그램을 나타낸다.

[27] 도 15는 본 개시가 적용될 수 있는 GCMP 디캡슐레이션 블록 다이어그램을 나타낸다.

[28] 도 16은 본 개시가 적용될 수 있는 블록-ACK 요청 프레임의 예시적인 포맷을 나타내는 도면이다.

[29] 도 17은 본 개시에 따른 제 1 STA의 동작을 설명하기 위한 도면이다.

[30] 도 18은 본 개시에 따른 제 2 STA의 동작을 설명하기 위한 도면이다.

[31] 도 19는 본 개시의 실시예에 따른 블록 ACK 요청 프레임의 보호를 위한 AAD 구성의 예시들을 나타낸다.

[32] 도 20은 본 개시에 따른 블록 ACK 요청 프레임에 대한 보호를 지원하는 송신 STA의 동작을 예시한다.

[33] 도 21은 본 개시에 따른 블록 ACK 요청 프레임에 대한 보호를 지원하는 수신 STA의 동작을 예시한다.

발명의 실시를 위한 최선의 형태

[34] 이하, 본 개시에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 개시의 예시적인 실시형태를 설명하고자 하는 것이며, 본 개시가 실시될 수 있는 유일한 실시형태를 나타내고자 하는 것이 아니다. 이하의 상세한 설명은 본 개시의 완전한 이해

를 제공하기 위해서 구체적 세부사항을 포함한다. 그러나, 당업자는 본 개시가 이러한 구체적 세부사항 없이도 실시될 수 있음을 안다.

[35] 몇몇 경우, 본 개시의 개념이 모호해지는 것을 피하기 위하여 공지의 구조 및 장치는 생략되거나, 각 구조 및 장치의 핵심기능을 중심으로 한 블록도 형식으로 도시될 수 있다.

[36] 본 개시에 있어서, 어떤 구성요소가 다른 구성요소와 "연결", "결합" 또는 "접속"되어 있다고 할 때, 이는 직접적인 연결관계 뿐만 아니라, 그 사이에 또 다른 구성요소가 존재하는 간접적인 연결관계도 포함할 수 있다. 또한 본 개시에서 용어 "포함한다" 또는 "가진다"는 언급된 특징, 단계, 동작, 요소 및/또는 구성요소의 존재를 특정하지만, 하나 이상의 다른 특징, 단계, 동작, 요소, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는다.

[37] 본 개시에 있어서, "제 1", "제 2" 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용되고 구성요소들을 제한하기 위해서 사용되지 않으며, 특별히 언급되지 않는 한 구성요소들 간의 순서 또는 중요도 등을 한정하지 않는다. 따라서, 본 개시의 범위 내에서 일 실시예에서의 제 1 구성요소는 다른 실시예에서 제 2 구성요소라고 칭할 수도 있고, 마찬가지로 일 실시예에서의 제 2 구성요소를 다른 실시예에서 제 1 구성요소라고 칭할 수도 있다.

[38] 본 개시에서 사용된 용어는 특정 실시예에 대한 설명을 위한 것이며 청구범위를 제한하려는 것이 아니다. 실시예의 설명 및 첨부된 청구범위에서 사용되는 바와 같이, 단수 형태는 문맥상 명백하게 다르게 나타내지 않는 한 복수 형태도 포함하도록 의도한 것이다. 본 개시에 사용된 용어 "및/또는"은 관련된 열거 항목 중의 하나를 지칭할 수도 있고, 또는 그 중의 둘 이상의 임의의 및 모든 가능한 조합을 지칭하고 포함하는 것을 의미한다. 또한, 본 개시에서 단어들 사이의 "/"는 달리 설명되지 않는 한 "및/또는"과 동일한 의미를 가진다.

[39] 본 개시의 예시들은 다양한 무선 통신 시스템에 적용될 수 있다. 예를 들어, 본 개시의 예시들은 무선랜 시스템에 적용될 수 있다. 예를 들어, 본 개시의 예시들은 IEEE 802.11a/g/n/ac/ax/be 표준 기반 무선랜에 적용될 수 있다. 나아가, 본 개시의 예시들은 새롭게 제안되는 IEEE 802.11bn (또는 UHR) 표준 기반 무선랜에 적용될 수도 있다. 추가적으로, 본 개시의 예시들은 IEEE 802.11bn 후의 차세대 표준 기반 무선랜에 적용될 수도 있다. 또한, 본 개시의 예시들은 셀룰러 무선 통신 시스템에 적용될 수도 있다. 예를 들어, 3GPP(3rd Generation Partnership Project) 표준의 LTE(Long Term Evolution) 계열의 기술 및 5G NR(New Radio) 계열의 기술에 기반하는 셀룰러 무선 통신 시스템에 적용될 수 있다.

[40] 이하 본 개시의 예시들이 적용될 수 있는 기술적 특징에 대해서 설명한다.

[41] 도 1은 본 개시의 일 실시예에 따른 무선 통신 장치의 블록 구성도를 예시한다.

[42] 도 1에 예시된 제 1 디바이스(100)와 제 2 디바이스(200)는, 단말(Terminal), 무선 기기(wireless device), WTRU(Wireless Transmit Receive Unit), UE(User Equipment), MS(Mobile Station), UT(user terminal), MSS(Mobile Subscriber Station),

MSS(Mobile Subscriber Unit), SS(Subscriber Station), AMS(Advanced Mobile Station), WT(Wireless terminal), 또는 단순히 사용자(user) 등의 다양한 용어로 대체될 수 있다. 또한, 제 1 디바이스(100)와 제 2 디바이스(200)는, 액세스 포인트(Access Point, AP), BS(Base Station), 고정국(fixed station), Node B, BTS(base transceiver system), 네트워크, AI(Artificial Intelligence) 시스템, RSU(road side unit), 리피터, 라우터, 릴레이(relay), 게이트웨이 등의 다양한 용어로 대체될 수 있다.

[43] 도 1에 예시된 디바이스(100, 200)는 스테이션(station, STA)이라 칭할 수도 있다. 예를 들어, 도 1에 예시된 디바이스(100, 200)는 송신 디바이스, 수신 디바이스, 송신 STA, 수신 STA 등의 다양한 용어로 칭할 수 있다. 예를 들어, STA(110, 200)은 AP(access Point) 역할을 수행하거나 non-AP 역할을 수행할 수 있다. 즉, 본 개시에서 STA(110, 200)은 AP 및/또는 non-AP의 기능을 수행할 수 있다. STA(110, 200)이 AP 기능을 수행하는 경우 단순히 AP라고 칭할 수도 있고, STA(110, 200)이 non-AP 기능을 수행하는 경우 단순히 STA라고 칭할 수도 있다. 또한, 본 개시에서 AP는 AP STA으로도 표시될 수 있다.

[44] 도 1을 참조하면, 제 1 디바이스(100)와 제 2 디바이스(200)는 다양한 무선랜 기술(예를 들어, IEEE 802.11 계열)을 통해 무선 신호를 송수신할 수 있다. 제 1 디바이스(100)와 제 2 디바이스(200)는 IEEE 802.11 표준의 규정을 따르는 매체 접속 제어(medium access control, MAC) 계층 및 물리 계층(physical layer, PHY)에 대한 인터페이스를 포함할 수 있다.

[45] 또한, 제 1 디바이스(100)와 제 2 디바이스(200)는 무선랜 기술 이외의 다양한 통신 표준(예를 들어, 3GPP LTE 계열, 5G NR 계열의 표준 등) 기술을 추가적으로 지원할 수도 있다. 또한 본 개시의 디바이스는 휴대 전화, 차량(vehicle), 개인용 컴퓨터, AR(Augmented Reality) 장비, VR(Virtual Reality) 장비 등의 다양한 장치로 구현될 수 있다. 또한, 본 명세서의 STA은 음성 통화, 영상 통화, 데이터 통신, 자율 주행(Autonomous-Driving), MTC(Machine-Type Communication), M2M(Machine-to-Machine), D2D(Device-to-Device), IoT(Internet-of-Things) 등의 다양한 통신 서비스를 지원할 수 있다.

[46] 제 1 디바이스(100)는 하나 이상의 프로세서(102) 및 하나 이상의 메모리(104)를 포함하며, 추가적으로 하나 이상의 송수신기(transceiver)(106) 및/또는 하나 이상의 안테나(108)을 더 포함할 수 있다. 프로세서(102)는 메모리(104) 및/또는 송수신기(106)를 제어하며, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 구현하도록 구성될 수 있다. 예를 들어, 프로세서(102)는 메모리(104) 내의 정보를 처리하여 제 1 정보/신호를 생성한 뒤, 송수신기(106)을 통해 제 1 정보/신호를 포함하는 무선 신호를 송신할 수 있다. 또한, 프로세서(102)는 송수신기(106)를 통해 제 2 정보/신호를 포함하는 무선 신호를 수신한 뒤, 제 2 정보/신호의 신호 처리로부터 얻은 정보를 메모리(104)에 저장할 수 있다. 메모리(104)는 프로세서(102)와 연결될 수 있고, 프로세서(102)의 동작과 관련한 다양

한 정보를 저장할 수 있다. 예를 들어, 메모리(104)는 프로세서(102)에 의해 제어되는 프로세스들 중 일부 또는 전부를 수행하거나, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 수행하기 위한 명령어(instruction)들을 포함하는 소프트웨어 코드를 저장할 수 있다. 여기서, 프로세서(102)와 메모리(104)는 무선랜 기술(예를 들어, IEEE 802.11 계열)을 구현하도록 설계된 통신 모뎀/회로/칩의 일부일 수 있다. 송수신기(106)는 프로세서(102)와 연결될 수 있고, 하나 이상의 안테나(108)를 통해 무선 신호를 송신 및/또는 수신할 수 있다. 송수신기(106)는 송신기 및/또는 수신기를 포함할 수 있다. 송수신기(106)는 RF(Radio Frequency) 유닛과 혼용될 수 있다. 본 개시에서 디바이스는 통신 모뎀/회로/칩을 의미할 수도 있다.

[47] 제 2 디바이스(200)는 하나 이상의 프로세서(202), 하나 이상의 메모리(204)를 포함하며, 추가적으로 하나 이상의 송수신기(206) 및/또는 하나 이상의 안테나(208)를 더 포함할 수 있다. 프로세서(202)는 메모리(204) 및/또는 송수신기(206)를 제어하며, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 구현하도록 구성될 수 있다. 예를 들어, 프로세서(202)는 메모리(204) 내의 정보를 처리하여 제 3 정보/신호를 생성한 뒤, 송수신기(206)를 통해 제 3 정보/신호를 포함하는 무선 신호를 송신할 수 있다. 또한, 프로세서(202)는 송수신기(206)를 통해 제 4 정보/신호를 포함하는 무선 신호를 수신한 뒤, 제 4 정보/신호의 신호 처리로부터 얻은 정보를 메모리(204)에 저장할 수 있다. 메모리(204)는 프로세서(202)와 연결될 수 있고, 프로세서(202)의 동작과 관련한 다양한 정보를 저장할 수 있다. 예를 들어, 메모리(204)는 프로세서(202)에 의해 제어되는 프로세스들 중 일부 또는 전부를 수행하거나, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 수행하기 위한 명령어들을 포함하는 소프트웨어 코드를 저장할 수 있다. 여기서, 프로세서(202)와 메모리(204)는 무선랜 기술(예를 들어, IEEE 802.11 계열)을 구현하도록 설계된 통신 모뎀/회로/칩의 일부일 수 있다. 송수신기(206)는 프로세서(202)와 연결될 수 있고, 하나 이상의 안테나(208)를 통해 무선 신호를 송신 및/또는 수신할 수 있다. 송수신기(206)는 송신기 및/또는 수신기를 포함할 수 있다 송수신기(206)는 RF 유닛과 혼용될 수 있다. 본 개시에서 디바이스는 통신 모뎀/회로/칩을 의미할 수도 있다.

[48] 이하, 디바이스(100, 200)의 하드웨어 요소에 대해 보다 구체적으로 설명한다. 이로 제한되는 것은 아니지만, 하나 이상의 프로토콜 계층이 하나 이상의 프로세서(102, 202)에 의해 구현될 수 있다. 예를 들어, 하나 이상의 프로세서(102, 202)는 하나 이상의 계층(예를 들어, PHY, MAC과 같은 기능적 계층)을 구현할 수 있다. 하나 이상의 프로세서(102, 202)는 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 하나 이상의 PDU(Protocol Data Unit) 및/또는 하나 이상의 SDU(Service Data Unit)를 생성할 수 있다. 하나 이상의 프로세서(102, 202)는 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 메시지, 제어정보, 데이터 또는 정보를 생성할 수 있다. 하나 이상의 프

로세서(102, 202)는 본 개시에 개시된 기능, 절차, 제안 및/또는 방법에 따라 PDU, SDU, 메시지, 제어정보, 데이터 또는 정보를 포함하는 신호(예를 들어, 베이스밴드 신호)를 생성하여, 하나 이상의 송수신기(106, 206)에게 제공할 수 있다. 하나 이상의 프로세서(102, 202)는 하나 이상의 송수신기(106, 206)로부터 신호(예를 들어, 베이스밴드 신호)를 수신할 수 있고, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 PDU, SDU, 메시지, 제어정보, 데이터 또는 정보를 획득할 수 있다.

[49] 하나 이상의 프로세서(102, 202)는 컨트롤러, 마이크로 컨트롤러, 마이크로 프로세서 또는 마이크로 컴퓨터로 지칭될 수 있다. 하나 이상의 프로세서(102, 202)는 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 조합에 의해 구현될 수 있다. 일 예로, 하나 이상의 ASIC(Application Specific Integrated Circuit), 하나 이상의 DSP(Digital Signal Processor), 하나 이상의 DSPD(Digital Signal Processing Device), 하나 이상의 PLD(Programmable Logic Device) 또는 하나 이상의 FPGA(Field Programmable Gate Arrays)가 하나 이상의 프로세서(102, 202)에 포함될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 펌웨어 또는 소프트웨어를 사용하여 구현될 수 있고, 펌웨어 또는 소프트웨어는 모듈, 절차, 기능 등을 포함하도록 구현될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 수행하도록 설정된 펌웨어 또는 소프트웨어는 하나 이상의 프로세서(102, 202)에 포함되거나, 하나 이상의 메모리(104, 204)에 저장되어 하나 이상의 프로세서(102, 202)에 의해 구동될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 코드, 명령어 및/또는 명령어의 집합 형태로 펌웨어 또는 소프트웨어를 사용하여 구현될 수 있다.

[50] 하나 이상의 메모리(104, 204)는 하나 이상의 프로세서(102, 202)와 연결될 수 있고, 다양한 형태의 데이터, 신호, 메시지, 정보, 프로그램, 코드, 지시 및/또는 명령어를 저장할 수 있다. 하나 이상의 메모리(104, 204)는 ROM, RAM, EPROM, 플래시 메모리, 하드 드라이브, 레지스터, 캐쉬 메모리, 컴퓨터 판독 저장 매체 및/또는 이들의 조합으로 구성될 수 있다. 하나 이상의 메모리(104, 204)는 하나 이상의 프로세서(102, 202)의 내부 및/또는 외부에 위치할 수 있다. 또한, 하나 이상의 메모리(104, 204)는 유선 또는 무선 연결과 같은 다양한 기술을 통해 하나 이상의 프로세서(102, 202)와 연결될 수 있다.

[51] 하나 이상의 송수신기(106, 206)는 하나 이상의 다른 장치에게 본 개시의 방법들 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 송신할 수 있다. 하나 이상의 송수신기(106, 206)는 하나 이상의 다른 장치로부터 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 수신할 수 있다. 예를 들어, 하나 이상의 송수신기(106, 206)는 하나 이상의 프로세서(102, 202)와 연결될 수 있고, 무선 신호를 송수신할 수 있다. 예를 들어, 하나 이상의 프로세서(102, 202)는 하나 이상의 송수신기(106, 206)가 하나 이상의 다른 장치에게 사용

자 데이터, 제어 정보 또는 무선 신호를 송신하도록 제어할 수 있다. 또한, 하나 이상의 프로세서(102, 202)는 하나 이상의 송수신기(106, 206)가 하나 이상의 다른 장치로부터 사용자 데이터, 제어 정보 또는 무선 신호를 수신하도록 제어할 수 있다. 또한, 하나 이상의 송수신기(106, 206)는 하나 이상의 안테나(108, 208)와 연결될 수 있고, 하나 이상의 송수신기(106, 206)는 하나 이상의 안테나(108, 208)를 통해 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 송수신하도록 설정될 수 있다. 본 개시에서, 하나 이상의 안테나는 복수의 물리 안테나이거나, 복수의 논리 안테나(예를 들어, 안테나 포트)일 수 있다. 하나 이상의 송수신기(106, 206)는 수신된 사용자 데이터, 제어 정보, 무선 신호/채널 등을 하나 이상의 프로세서(102, 202)를 이용하여 처리하기 위해, 수신된 무선 신호/채널 등을 RF 밴드 신호에서 베이스밴드 신호로 변환(Convert)할 수 있다. 하나 이상의 송수신기(106, 206)는 하나 이상의 프로세서(102, 202)를 이용하여 처리된 사용자 데이터, 제어 정보, 무선 신호/채널 등을 베이스밴드 신호에서 RF 밴드 신호로 변환할 수 있다. 이를 위하여, 하나 이상의 송수신기(106, 206)는 (아날로그) 오실레이터 및/또는 필터를 포함할 수 있다.

[52] 예를 들어, STA(100, 200)의 하나는 AP의 의도된 동작을 수행하고, STA(100, 200)의 다른 하나는 non-AP STA의 의도된 동작을 수행할 수 있다. 예를 들어, 도 1의 송수신기(106, 206)는 신호(예를 들어, IEEE 802.11a/b/g/n/ac/ax/be/bn 등에 따르는 패킷 또는 PPDU(Physical layer Protocol Data Unit))의 송수신 동작을 수행할 수 있다. 또한, 본 개시에서 다양한 STA이 송수신 신호를 생성하거나 송수신 신호를 위해 사전에 데이터 처리나 연산을 수행하는 동작은 도 1의 프로세서(102, 202)에서 수행될 수 있다. 예를 들어, 송수신 신호를 생성하거나 송수신 신호를 위해 사전에 데이터 처리나 연산을 수행하는 동작의 일례는, 1) PPDU 내에 포함되는 필드(SIG(signal), STF(short training field), LTF(long training field), Data 등)의 비트 정보를 결정/획득/구성/연산/디코딩/인코딩하는 동작, 2) PPDU 내에 포함되는 필드(SIG, STF, LTF, Data 등)를 위해 사용되는 시간 자원이나 주파수 자원(예를 들어, 서브캐리어 자원) 등을 결정/구성/획득하는 동작, 3) PPDU 내에 포함되는 필드(SIG, STF, LTF, Data 등)를 위해 사용되는 특정한 시퀀스(예를 들어, 파일럿 시퀀스, STF/LTF 시퀀스, SIG에 적용되는 엑스트라 시퀀스) 등을 결정/구성/획득하는 동작, 4) STA에 대해 적용되는 전력 제어 동작 및/또는 파워 세이빙 동작, 5) ACK 신호의 결정/획득/구성/연산/디코딩/인코딩 등에 관련된 동작을 포함할 수 있다. 또한, 이하의 일례에서 다양한 STA이 송수신 신호의 결정/획득/구성/연산/디코딩/인코딩을 위해 사용하는 다양한 정보(예를 들어, 필드/서브필드/제어필드/파라미터/파워 등에 관련된 정보)는 도 1의 메모리(104, 204)에 저장될 수 있다.

[53] 이하에서, 하향링크(downlink, DL)는 AP STA로부터 non-AP STA로의 통신을 위한 링크를 의미하며, 하향링크를 통해 하향링크 PPDU/패킷/신호 등의 송수신

될 수 있다. 하향링크 통신에서 송신기는 AP STA의 일부이고, 수신기는 non-AP STA의 일부일 수 있다. 상향링크(uplink, UL)는 non-AP STA로부터 AP STA로의 통신을 위한 링크를 의미하며, 상향링크를 통해 상향링크 PPDU/패킷/신호 등의 송수신될 수 있다. 상향링크 통신에서 송신기는 non-AP STA의 일부이고, 수신기는 AP STA의 일부일 수 있다.

[54] 도 2는 본 개시가 적용될 수 있는 무선랜 시스템의 예시적인 구조를 나타내는 도면이다.

[55] 무선랜 시스템의 구조는 복수개의 구성요소(component)들로 구성될 수 있다. 복수의 구성요소들의 상호작용에 의해 상위계층에 대해 트랜스패런트한 STA 이동성을 지원하는 무선랜이 제공될 수 있다. BSS(Basic Service Set)는 무선랜의 기본적인 구성 블록에 해당한다. 도 2에서는 2 개의 BSS(BSS1 및 BSS2)가 존재하고, 각각의 BSS의 멤버로서 2 개의 STA이 포함되는 것(STA1 및 STA2는 BSS1에 포함되고, STA3 및 STA4는 BSS2에 포함됨)을 예시적으로 도시한다. 도 2에서 BSS를 나타내는 타원은 해당 BSS에 포함된 STA들이 통신을 유지하는 커버리지 영역을 나타내는 것으로도 이해될 수 있다. 이 영역을 BSA(Basic Service Area)라고 칭할 수 있다. STA이 BSA 밖으로 이동하게 되면 해당 BSA 내의 다른 STA들과 직접적으로 통신할 수 없게 된다.

[56] 도 2에서 도시하는 DS를 고려하지 않는다면, 무선랜에서 가장 기본적인 타입의 BSS는 독립적인 BSS(Independent BSS, IBSS)이다. 예를 들어, IBSS는 2 개의 STA만으로 구성된 최소의 형태를 가질 수 있다. 예를 들어, 다른 구성요소들이 생략된 것을 가정하여, STA1 및 STA2만으로 구성된 BSS1 또는 STA3 및 STA4만으로 구성된 BSS2는 각각 IBSS의 대표적인 예시에 해당할 수 있다. 이러한 구성은 STA들이 AP 없이 직접 통신할 수 있는 경우에 가능하다. 또한, 이러한 형태의 무선랜에서 미리 계획되어서 구성되는 것이 아니라 LAN이 필요한 경우에 구성될 수 있으며, 이를 애드-혹(ad-hoc) 네트워크라고 칭할 수도 있다. IBSS는 AP를 포함하지 않기 때문에 중앙에서 관리 기능을 수행하는 개체(centralized management entity)가 없다. 즉, IBSS에서 STA들은 분산된 방식(distributed manner)으로 관리된다. IBSS에서는 모든 STA들이 이동 STA으로 이루어질 수 있으며, 분산 시스템(DS)으로의 접속이 허용되지 않아서 자기 완비적 네트워크(self-contained network)를 이룬다.

[57] STA의 켜지거나 꺼짐, STA이 BSS 영역에 들어오거나 나감 등에 의해서, BSS에서의 STA의 멤버십이 동적으로 변경될 수 있다. BSS의 멤버가 되기 위해서는, STA은 동기화 과정을 이용하여 BSS에 조인할 수 있다. BSS 기반구조의 모든 서비스에 액세스하기 위해서는, STA은 BSS에 결합(associated)되어야 한다. 이러한 결합(association)은 동적으로 설정될 수 있고, 분산 시스템 서비스(Distribution System Service, DSS)의 이용을 포함할 수 있다.

[58] 무선랜에서 직접적인 STA-대-STA의 거리는 PHY 성능에 의해서 제한될 수 있다. 어떠한 경우에는 이러한 거리의 한계가 충분할 수도 있지만, 경우에 따라서

는 보다 먼 거리의 STA 간의 통신이 필요할 수도 있다. 확장된 커버리지를 지원하기 위해서 분산 시스템(DS)이 구성될 수 있다.

[59] DS는 BSS들이 상호 연결되는 구조를 의미한다. 구체적으로, 도 2와 같이 복수개의 BSS들로 구성된 네트워크의 확장된 형태의 구성요소로서 BSS가 존재할 수도 있다. DS는 논리적인 개념이며 분산 시스템 매체(DSM)의 특성에 의해서 특정될 수 있다. 이와 관련하여, 무선 매체(Wireless Medium, WM)와 DSM는 논리적으로 구분될 수 있다. 각각의 논리적 매체는 상이한 목적을 위해서 사용되며, 상이한 구성요소에 의해서 사용된다. 이러한 매체들이 동일한 것으로 제한되지도 않고 상이한 것으로 제한되지도 않는다. 이와 같이 복수개의 매체들이 논리적으로 상이하다는 점에서, 무선랜 구조(DS 구조 또는 다른 네트워크 구조)의 유연성이 설명될 수 있다. 즉, 무선랜 구조는 다양하게 구현될 수 있으며, 각각의 구현예의 물리적인 특성에 의해서 독립적으로 해당 무선랜 구조가 특정될 수 있다.

[60] DS는 복수개의 BSS들의 끊김없는(seamless) 통합을 제공하고 목적지로의 어드레스를 다루는 데에 필요한 논리적 서비스들을 제공함으로써 이동 디바이스를 지원할 수 있다. 또한, DS는 무선랜과 다른 네트워크(예를 들어, IEEE 802.X)와의 연결을 위한 브리지 역할을 수행하는 포털(portal)이라는 구성요소를 더 포함할 수 있다.

[61] AP는 결합된 non-AP STA들에 대해서 WM을 통해서 DS 로의 액세스를 가능하게 하고, STA의 기능성 또한 가지는 엔티티(entity)를 의미한다. AP를 통해서 BSS 및 DS 간의 데이터 이동이 수행될 수 있다. 예를 들어, 도 2에서 도시하는 STA2 및 STA3은 STA의 기능성을 가지면서, 결합된 non-AP STA(STA1 및 STA4)이 DS로 액세스하도록 하는 기능을 제공한다. 또한, 모든 AP는 기본적으로 STA에 해당하므로, 모든 AP는 어드레스 가능한 엔티티이다. WM 상에서의 통신을 위해 AP에 의해서 사용되는 어드레스와, DSM 상에서의 통신을 위해 AP에 의해서 사용되는 어드레스는 반드시 동일할 필요는 없다. AP와 하나 이상의 STA으로 구성되는 BSS를 인프라스트럭처(infrastructure BSS)라고 칭할 수 있다.

[62] AP에 결합된 STA(들) 중의 하나로부터 해당 AP의 STA 어드레스로 송신되는 데이터는, 항상 비제어 포트(uncontrolled port)에서 수신되고 IEEE 802.1X 포트 액세스 엔티티에 의해서 처리될 수 있다. 또한, 제어 포트(controlled port)가 인증되면 송신 데이터(또는 프레임)는 DS로 전달될 수 있다.

[63] 전술한 DS의 구조에 추가적으로 넓은 커버리지를 제공하기 위한 확장된 서비스 세트(Extended Service Set, ESS)가 설정될 수도 있다.

[64] ESS는 임의의(arbitrary) 크기 및 복잡도를 가지는 네트워크가 DS 및 BSS들로 구성된 네트워크를 의미한다. ESS는 하나의 DS에 연결된 BSS들의 집합에 해당할 수 있다. 그러나, ESS는 DS를 포함하지는 않는다. ESS 네트워크는 LLC(Logical Link Control) 계층에서 IBSS로 보이는 점이 특징이다. ESS에 포함되는 STA들은 서로 통신할 수 있고, 이동 STA들은 LLC에 트랜스패런트하게 하나의 BSS에서 다른 BSS로(동일한 ESS 내에서) 이동할 수 있다. 하나의 ESS에 포함

되는 AP들은 동일한 SSID(service set identification)을 가질 수 있다. SSID는 BSS의 식별자인 BSSID와 구별된다.

[65] 무선랜 시스템에서는 BSS들의 상대적인 물리적 위치에 대해서 아무것도 가정하지 않으며, 다음과 같은 형태가 모두 가능하다. BSS들은 부분적으로 중첩될 수 있고, 이는 연속적인 커버리지를 제공하기 위해서 일반적으로 이용되는 형태이다. 또한, BSS들은 물리적으로 연결되어 있지 않을 수 있고, 논리적으로는 BSS들 간의 거리에 제한은 없다. 또한, BSS들은 물리적으로 동일한 위치에 위치할 수 있고, 이는 리던던시를 제공하기 위해서 이용될 수 있다. 또한, 하나 (또는 하나 이상의) IBSS 또는 ESS 네트워크들이 하나 (또는 하나 이상의) ESS 네트워크로서 동일한 공간에 물리적으로 존재할 수 있다. 이는 ESS 네트워크가 존재하는 위치에 애드-혹 네트워크가 동작하는 경우나, 상이한 기관(organizations)에 의해서 물리적으로 중첩되는 무선 네트워크들이 구성되는 경우나, 동일한 위치에서 2 이상의 상이한 액세스 및 보안 정책이 필요한 경우 등에서의 ESS 네트워크 형태에 해당할 수 있다.

[66] 도 3은 본 개시가 적용될 수 있는 링크 셋업(link setup) 과정을 설명하기 위한 도면이다.

[67] STA이 네트워크에 대해서 링크를 셋업하고 데이터를 송수신하기 위해서는, 먼저 네트워크를 발견(discovery)하고, 인증(authentication)을 수행하고, 결합(association)을 맺고(establish), 보안(security)을 위한 인증 절차 등을 거쳐야 한다. 링크 셋업 과정을 세션 개시 과정, 세션 셋업 과정이라고도 칭할 수 있다. 또한, 링크 셋업 과정의 발견, 인증, 결합, 보안 설정의 과정을 통칭하여 결합 과정이라고 칭할 수도 있다.

[68] 단계 S310에서 STA은 네트워크 발견 동작을 수행할 수 있다. 네트워크 발견 동작은 STA의 스캐닝(scanning) 동작을 포함할 수 있다. 즉, STA이 네트워크에 액세스하기 위해서는 참여 가능한 네트워크를 찾아야 한다. STA은 무선 네트워크에 참여하기 전에 호환 가능한 네트워크를 식별하여야 하는데, 특정 영역에 존재하는 네트워크 식별과정을 스캐닝이라고 한다.

[69] 스캐닝 방식에는 능동적 스캐닝(active scanning)과 수동적 스캐닝(passive scanning)이 있다. 도 3에서는 예시적으로 능동적 스캐닝 과정을 포함하는 네트워크 발견 동작을 도시한다. 능동적 스캐닝에서 스캐닝을 수행하는 STA은 채널들을 옮기면서 주변에 어떤 AP가 존재하는지 탐색하기 위해 프로브 요청 프레임(probe request frame)을 송신하고 이에 대한 응답을 기다린다. 응답자(responder)는 프로브 요청 프레임을 송신한 STA에게 프로브 요청 프레임에 대한 응답으로 프로브 응답 프레임(probe response frame)을 송신한다. 여기에서, 응답자는 스캐닝되고 있는 채널의 BSS에서 마지막으로 비콘 프레임(beacon frame)을 송신한 STA일 수 있다. BSS에서는 AP가 비콘 프레임을 송신하므로 AP가 응답자가 되며, IBSS에서는 IBSS 내의 STA들이 돌아가면서 비콘 프레임을 송신하므로 응답자가 일정하지 않다. 예를 들어, 1번 채널에서 프로브 요청 프레임을 송신하고 1

번 채널에서 프로브 응답 프레임을 수신한 STA은, 수신한 프로브 응답 프레임에 포함된 BSS 관련 정보를 저장하고 다음 채널(예를 들어, 2번 채널)로 이동하여 동일한 방법으로 스캐닝(즉, 2번 채널 상에서 프로브 요청/응답 송수신)을 수행할 수 있다.

[70] 도 3에서 도시하고 있지 않지만, 스캐닝 동작은 수동적 스캐닝 방식으로 수행될 수도 있다. 수동적 스캐닝에서 스캐닝을 수행하는 STA은 채널들을 옮기면서 비콘 프레임을 기다린다. 비콘 프레임은 IEEE 802.11에서 정의되는 관리 프레임(management frame) 중 하나로서, 무선 네트워크의 존재를 알리고, 스캐닝을 수행하는 STA으로 하여금 무선 네트워크를 찾아서, 무선 네트워크에 참여할 수 있도록 주기적으로 송신된다. BSS에서 AP가 비콘 프레임을 주기적으로 송신하는 역할을 수행하고, IBSS에서는 IBSS 내의 STA들이 돌아가면서 비콘 프레임을 송신한다. 스캐닝을 수행하는 STA은 비콘 프레임을 수신하면 비콘 프레임에 포함된 BSS에 대한 정보를 저장하고 다른 채널로 이동하면서 각 채널에서 비콘 프레임 정보를 기록한다. 비콘 프레임을 수신한 STA은, 수신한 비콘 프레임에 포함된 BSS 관련 정보를 저장하고 다음 채널로 이동하여 동일한 방법으로 다음 채널에서 스캐닝을 수행할 수 있다. 능동적 스캐닝과 수동적 스캐닝을 비교하면, 능동적 스캐닝이 수동적 스캐닝보다 딜레이(delay) 및 전력 소모가 작은 장점이 있다.

[71] STA이 네트워크를 발견한 후에, 단계 S320에서 인증 과정이 수행될 수 있다. 이러한 인증 과정은 후술하는 단계 S340의 보안 셋업 동작과 명확하게 구분하기 위해서 첫 번째 인증(first authentication) 과정이라고 칭할 수 있다.

[72] 인증 과정은 STA이 인증 요청 프레임(authentication request frame)을 AP에게 송신하고, 이에 응답하여 AP가 인증 응답 프레임(authentication response frame)을 STA에게 송신하는 과정을 포함한다. 인증 요청/응답에 사용되는 인증 프레임(authentication frame)은 관리 프레임에 해당한다.

[73] 인증 프레임은 인증 알고리즘 번호(authentication algorithm number), 인증 트랜잭션 시퀀스 번호(authentication transaction sequence number), 상태 코드(status code), 검문 텍스트(challenge text), RSN(Robust Security Network), 유한 순환 그룹(Finite Cyclic Group) 등에 대한 정보를 포함할 수 있다. 이는 인증 요청/응답 프레임에 포함될 수 있는 정보들의 일부 예시에 해당하며, 다른 정보로 대체되거나, 추가적인 정보가 더 포함될 수 있다.

[74] STA은 인증 요청 프레임을 AP에게 송신할 수 있다. AP는 수신된 인증 요청 프레임에 포함된 정보에 기초하여, 해당 STA에 대한 인증을 허용할지 여부를 결정할 수 있다. AP는 인증 처리의 결과를 인증 응답 프레임을 통하여 STA에게 제공할 수 있다.

[75] STA이 성공적으로 인증된 후에, 단계 S330에서 결합 과정이 수행될 수 있다. 결합 과정은 STA이 결합 요청 프레임(association request frame)을 AP에게 송신하고, 이에 응답하여 AP가 결합 응답 프레임(association response frame)을 STA에게 송신하는 과정을 포함한다.

[76] 예를 들어, 결합 요청 프레임은 다양한 캐퍼빌리티(capability)에 관련된 정보, 비콘 청취 간격(listen interval), SSID(service set identifier), 지원 레이트(supported rates), 지원 채널(supported channels), RSN, 이동성 도메인, 지원 오퍼레이팅 클래스(supported operating classes), TIM 브로드캐스트 요청(Traffic Indication Map Broadcast request), 상호동작(interworking) 서비스 캐퍼빌리티 등에 대한 정보를 포함할 수 있다. 예를 들어, 결합 응답 프레임은 다양한 캐퍼빌리티에 관련된 정보, 상태 코드, AID(Association ID), 지원 레이트, EDCA(Enhanced Distributed Channel Access) 파라미터 세트, RCPI(Received Channel Power Indicator), RSNI(Received Signal to Noise Indicator), 이동성 도메인, 타임아웃 간격(예를 들어, 결합 컴백 시간(association comeback time)), 중첩(overlapping) BSS 스캔 파라미터, TIM 브로드캐스트 응답, QoS(Quality of Service) 맵 등의 정보를 포함할 수 있다. 이는 결합 요청/응답 프레임에 포함될 수 있는 정보들의 일부 예시에 해당하며, 다른 정보로 대체되거나, 추가적인 정보가 더 포함될 수 있다.

[77] STA이 네트워크에 성공적으로 결합된 후에, 단계 S340에서 보안 셋업 과정이 수행될 수 있다. 단계 S340의 보안 셋업 과정은 RSNA(Robust Security Network Association) 요청/응답을 통한 인증 과정이라고 할 수도 있고, 상기 단계 S320의 인증 과정을 첫 번째 인증(first authentication) 과정이라고 하고, 단계 S340의 보안 셋업 과정을 단순히 인증 과정이라고도 칭할 수도 있다.

[78] 단계 S340의 보안 셋업 과정은, 예를 들어, EAPOL(Extensible Authentication Protocol over LAN) 프레임을 통한 4-웨이(way) 핸드쉐이킹을 통해서, 프라이빗 키 셋업(private key setup)을 하는 과정을 포함할 수 있다. 또한, 보안 셋업 과정은 IEEE 802.11 표준에서 정의하지 않는 보안 방식에 따라 수행될 수도 있다.

[79] 도 4는 본 개시가 적용될 수 있는 백오프 과정을 설명하기 위한 도면이다.

[80] 무선랜 시스템에서, MAC(Medium Access Control)의 기본 액세스 메커니즘은 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance) 메커니즘이다. CSMA/CA 메커니즘은 IEEE 802.11 MAC의 분배 조정 기능(Distributed Coordination Function, DCF)이라고도 불리는데, 기본적으로 "말하기 전에 듣기(listen before talk)" 액세스 메커니즘을 채용하고 있다. 이러한 유형의 액세스 메커니즘 따르면, AP 및/또는 STA은 송신을 시작하기에 앞서, 소정의 시간구간(예를 들어, DIFS(DCF Inter-Frame Space) 동안 무선 채널 또는 매체(medium)를 센싱(sensing)하는 CCA(Clear Channel Assessment)를 수행할 수 있다. 센싱 결과, 만일 매체가 유휴 상태(idle status)인 것으로 판단되면, 해당 매체를 통하여 프레임 송신을 시작한다. 반면, 매체가 점유된(occupied) 또는 비지(busy) 상태인 것으로 감지되면, 해당 AP 및/또는 STA은 자기 자신의 송신을 시작하지 않고 매체 액세스를 위한 지연 기간(예를 들어, 랜덤 백오프 기간(random backoff period))을 설정하여 기다린 후에 프레임 송신을 시도할 수 있다. 랜덤 백오프 기간의 적용으로, 여러 STA들은 서로 다른 시간 동안 대기한 후에 프레임 송신을 시도할 것이 기대되므로, 충돌(collision)을 최소화시킬 수 있다.

[81] 또한, IEEE 802.11 MAC 프로토콜은 HCF(Hybrid Coordination Function)를 제공한다. HCF는 상기 DCF와 PCF(Point Coordination Function)를 기반으로 한다. PCF는 폴링(polling) 기반의 동기식 액세스 방식으로 모든 수신 AP 및/또는 STA이 데이터 프레임을 수신할 수 있도록 주기적으로 폴링하는 방식을 일컫는다. 또한, HCF는 EDCA(Enhanced Distributed Channel Access)와 HCCA(HCF Controlled Channel Access)를 가진다. EDCA는 제공자가 다수의 사용자에게 데이터 프레임을 제공하기 위한 액세스 방식을 경쟁 기반으로 하는 것이고, HCCA는 폴링(polling) 메커니즘을 이용한 비경쟁 기반의 채널 액세스 방식을 사용하는 것이다. 또한, HCF는 무선랜의 QoS(Quality of Service)를 향상시키기 위한 매체 액세스 메커니즘을 포함하며, 경쟁 기간(Contention Period, CP)와 비경쟁 기간(Contention Free Period, CFP) 모두에서 QoS 데이터를 송신할 수 있다.

[82] 도 4를 참조하여 랜덤 백오프 주기에 기반한 동작에 대해서 설명한다. 점유된/비지 상태이던 매체가 유휴 상태로 변경되면, 여러 STA들은 데이터(또는 프레임) 송신을 시도할 수 있다. 충돌을 최소화하기 위한 방안으로서, STA들은 각각 랜덤 백오프 카운트를 선택하고 그에 해당하는 슬롯 시간만큼 대기한 후에, 송신을 시도할 수 있다. 랜덤 백오프 카운트는 의사-랜덤 정수(pseudo-random integer) 값을 가지며, 0 내지 CW 범위의 값 중에서 하나로 결정될 수 있다. 여기서, CW는 경쟁 윈도우(Contention Window) 파라미터 값이다. CW 파라미터는 초기값으로 CWmin이 주어지지만, 송신 실패의 경우(예를 들어, 송신된 프레임에 대한 ACK을 수신하지 못한 경우)에 2 배의 값을 취할 수 있다. CW 파라미터 값이 CWmax가 되면 데이터 송신이 성공할 때까지 CWmax 값을 유지하면서 데이터 송신을 시도할 수 있고, 데이터 송신이 성공하는 경우에는 CWmin 값으로 리셋된다. CW, CWmin 및 CWmax 값은 2^n-1 (n=0, 1, 2, ...)로 설정되는 것이 바람직하다.

[83] 랜덤 백오프 과정이 시작되면 STA은 결정된 백오프 카운트 값에 따라서 백오프 슬롯을 카운트 다운하는 동안에 계속하여 매체를 모니터링한다. 매체가 점유 상태로 모니터링되면 카운트 다운을 멈추고 대기하고, 매체가 유휴 상태가 되면 나머지 카운트 다운을 재개한다.

[84] 도 4의 예시에서 STA3의 MAC에 송신할 패킷이 도달한 경우에, STA3는 DIFS만큼 매체가 유휴 상태인 것을 확인하고 바로 프레임을 송신할 수 있다. 나머지 STA들은 매체가 점유/비지 상태인 것을 모니터링하고 대기한다. 그 동안 STA1, STA2 및 STA5의 각각에서도 송신할 데이터가 발생할 수 있고, 각각의 STA은 매체가 유휴상태로 모니터링되면 DIFS만큼 대기한 후에, 각자가 선택한 랜덤 백오프 카운트 값에 따라 백오프 슬롯의 카운트 다운을 수행할 수 있다. STA2가 가장 작은 백오프 카운트 값을 선택하고, STA1이 가장 큰 백오프 카운트 값을 선택한 경우를 가정한다. 즉, STA2가 백오프 카운트를 마치고 프레임 송신을 시작하는 시점에서 STA5의 잔여 백오프 시간은 STA1의 잔여 백오프 시간보다 짧은 경우를 예시한다. STA1 및 STA5는 STA2가 매체를 점유하는 동안에 잠시 카운트 다운을 멈추고 대기한다. STA2의 점유가 종료되어 매체가 다시 유휴 상태가 되면,

STA1 및 STA5는 DIFS만큼 대기한 후에, 멈추었던 백오프 카운트를 재개한다. 즉, 잔여 백오프 시간만큼의 나머지 백오프 슬롯을 카운트 다운한 후에 프레임 송신을 시작할 수 있다. STA5의 잔여 백오프 시간이 STA1보다 짧았으므로 STA5이 프레임 송신을 시작하게 된다. STA2가 매체를 점유하는 동안에 STA4에서도 송신할 데이터가 발생할 수 있다. STA4의 입장에서는 매체가 유휴 상태가 되면 DIFS만큼 대기한 후, 자신이 선택한 랜덤 백오프 카운트 값에 따른 카운트 다운을 수행하고 프레임 송신을 시작할 수 있다. 도 4의 예시에서는 STA5의 잔여 백오프 시간이 STA4의 랜덤 백오프 카운트 값과 우연히 일치하는 경우를 나타내며, 이 경우, STA4와 STA5 간에 충돌이 발생할 수 있다. 충돌이 발생하는 경우에는 STA4와 STA5 모두 ACK을 받지 못하여, 데이터 송신을 실패하게 된다. 이 경우, STA4와 STA5는 CW 값을 2배로 늘린 후에 랜덤 백오프 카운트 값을 선택하고 카운트 다운을 수행할 수 있다. STA1은 STA4와 STA5의 송신으로 인해 매체가 점유 상태인 동안에 대기하고 있다가, 매체가 유휴 상태가 되면 DIFS만큼 대기한 후, 잔여 백오프 시간이 지나면 프레임 송신을 시작할 수 있다.

[85] 도 4의 예시에서와 같이, 데이터 프레임은 상위 레이어로 포워드되는 데이터의 송신을 위해 사용되는 프레임이며, 매체가 유휴 상태가 된 때로부터 DIFS 경과 후 수행되는 백오프 후 송신될 수 있다. 추가적으로, 관리 프레임은 상위 레이어에 포워드되지 않는 관리 정보의 교환을 위해 사용되는 프레임으로서, DIFS 또는 PIFS (Point coordination function IFS)와 같은 IFS 경과 후 수행되는 백오프 후 송신된다. 관리 프레임의 서브타입 프레임으로 비콘(Beacon), 결합 요청/응답(Association request/response), 재(re)-결합 요청/응답, 프로브 요청/응답(probe request/response), 인증 요청/응답(authentication request/response) 등이 있다. 제어 프레임은 매체에 액세스를 제어하기 위하여 사용되는 프레임이다. 제어 프레임의 서브 타입 프레임으로 RTS(Request-To-Send), CTS(Clear-To-Send), ACK(Acknowledgment), PS-Poll(Power Save-Poll), 블록 ACK(BlockAck), 블록 ACK 요청(BlockACKReq), NDP 공지(null data packet announcement), 트리거(Trigger) 등이 있다. 제어 프레임은 이전 프레임의 응답 프레임이 아닌 경우 DIFS 경과 후 수행되는 백오프 후 송신되고, 이전 프레임의 응답 프레임인 경우 SIFS(short IFS) 경과 후 백오프 수행 없이 송신된다. 프레임의 타입과 서브 타입은 프레임 제어(FC) 필드 내의 타입(type) 필드와 서브타입(subtype) 필드에 의해 식별될 수 있다.

[86] QoS(Quality of Service) STA은 프레임이 속하는 액세스 카테고리(access category, AC)를 위한 AIFS(arbitration IFS), 즉 AIFS[i] (여기서, i는 AC에 의해 결정되는 값) 경과 후 수행되는 백오프 후 프레임을 송신할 수 있다. 여기서, AIFS[i]가 사용될 수 있는 프레임은 데이터 프레임, 관리 프레임이 될 수 있고, 또한 응답 프레임이 아닌 제어 프레임이 될 수 있다.

[87] 도 5는 본 개시가 적용될 수 있는 CSMA/CA 기반 프레임 송신 동작을 설명하기 위한 도면이다.

[88] 전술한 바와 같이 CSMA/CA 메커니즘은 STA이 매체를 직접 센싱하는 물리적 캐리어 센싱(physical carrier sensing) 외에 가상 캐리어 센싱(virtual carrier sensing)도 포함한다. 가상 캐리어 센싱은 숨겨진 노드 문제(hidden node problem) 등과 같이 매체 액세스에서 발생할 수 있는 문제를 보완하기 위한 것이다. 가상 캐리어 센싱을 위하여, STA의 MAC은 NAV(Network Allocation Vector)를 이용할 수 있다. NAV는 현재 매체를 사용하고 있거나 또는 사용할 권한이 있는 STA이, 매체가 이용 가능한 상태로 되기까지 남아 있는 시간을 다른 STA에게 지시(indicate)하는 값이다. 따라서 NAV로 설정된 값은 해당 프레임을 송신하는 STA에 의하여 매체의 사용이 예정되어 있는 기간에 해당하고, NAV 값을 수신하는 STA은 해당 기간동안 매체 액세스가 금지된다. 예를 들어, NAV는 프레임의 MAC 헤더(header)의 "duration" 필드의 값에 기초하여 설정될 수 있다.

[89] 도 5의 예시에서, STA1은 STA2로 데이터를 송신하고자 하고, STA3는 STA1과 STA2 간에 송수신되는 프레임의 일부 또는 전부를 오버히어링(overhearing)할 수 있는 위치에 있는 것으로 가정한다.

[90] CSMA/CA 기반 프레임 송신 동작에서 다수의 STA의 송신의 충돌 가능성을 감소시키기 위해서, RTS/CTS 프레임을 이용하는 메커니즘이 적용될 수 있다. 도 5의 예시에서 STA1의 송신이 수행되는 동안 STA3의 캐리어 센싱 결과 매체가 유휴 상태라고 결정할 수도 있다. 즉, STA1은 STA3에게 히든 노드에 해당할 수 있다. 또는, 도 5의 예시에서 STA2의 송신이 수행되는 동안 STA3의 캐리어 센싱 결과 매체가 유휴 상태라고 결정할 수도 있다. 즉, STA2는 STA3에게 히든 노드에 해당할 수 있다. STA1과 STA2 간의 데이터 송수신을 수행하기 전에 RTS/CTS 프레임의 교환을 통해, STA1 또는 STA2 중의 하나의 송신 범위 밖의 STA, 또는 STA1 또는 STA3로부터의 송신에 대한 캐리어 센싱 범위 밖의 STA이, STA1과 STA2 간의 데이터 송수신 동안 채널 점유를 시도하지 않도록 할 수 있다.

[91] 구체적으로, STA1은 캐리어 센싱(carrier sensing)을 통해 채널이 사용되고 있는지를 결정할 수 있다. 물리적 캐리어 센싱의 측면에서, STA1은 채널에서 검출되는 에너지 크기 또는 신호 상관도(correlation)에 기초하여 채널 점유 유휴 상태를 결정할 수 있다. 또한, 가상 캐리어 센싱 측면에서, STA1은 NAV(network allocation vector) 타이머(timer)를 사용하여 채널의 점유 상태를 판단할 수 있다.

[92] STA1은 DIFS 동안 채널이 유휴 상태인 경우 백오프 수행 후 RTS 프레임을 STA2에게 송신할 수 있다. STA2은 RTS 프레임을 수신한 경우 SIFS 후에 RTS 프레임에 대한 응답인 CTS 프레임을 STA1에게 송신할 수 있다.

[93] STA3가 STA2으로부터의 CTS 프레임을 오버히어링할 수는 없지만 STA1으로부터의 RTS 프레임을 오버히어링할 수 있다면, STA3은 RTS 프레임에 포함된 듀레이션(duration) 정보를 사용하여 이후에 연속적으로 송신되는 프레임 송신 기간(예를 들어, SIFS + CTS 프레임 + SIFS + 데이터 프레임 + SIFS + ACK 프레임)에 대한 NAV 타이머를 설정할 수 있다. 또는, STA3가 STA3가 STA1으로부터의 RTS 프레임을 오버히어링할 수는 없지만 STA2로부터의 CTS 프레임을 오버히

어링할 수 있다면, STA3는 CTS 프레임에 포함된 듀레이션 정보를 사용하여 이후에 연속적으로 송신되는 프레임 송신 기간(예를 들어, SIFS + 데이터 프레임 + SIFS + ACK 프레임)에 대한 NAV 타이머를 설정할 수 있다. 즉, STA3는 STA1 또는 STA2 중의 하나 이상으로부터의 RTS 또는 CTS 프레임 중의 하나 이상을 오버히어링할 수 있다면, 그에 따라 NAV를 설정할 수 있다. STA3은 NAV 타이머가 만료되기 전에 새로운 프레임을 수신한 경우 새로운 프레임에 포함된 듀레이션 정보를 사용하여 NAV 타이머를 갱신할 수 있다. STA3은 NAV 타이머가 만료되기 전까지 채널 액세스를 시도하지 않는다.

[94] STA1은 STA2로부터 CTS 프레임을 수신한 경우 CTS 프레임의 수신이 완료된 시점부터 SIFS 후에 데이터 프레임을 STA2에게 송신할 수 있다. STA2는 데이터 프레임을 성공적으로 수신한 경우 SIFS 후에 데이터 프레임에 대한 응답인 ACK 프레임을 STA1에 송신할 수 있다. STA3는 NAV 타이머가 만료된 경우 캐리어 센싱을 통해 채널이 사용되고 있는지를 결정할 수 있다. STA3은 NAV 타이머의 만료 후부터 DIFS 동안 채널이 다른 단말에 의해 사용되지 않은 것으로 결정한 경우 랜덤 백오프에 따른 경쟁 윈도우(CW)가 지난 후에 채널 액세스를 시도할 수 있다.

[95] 도 6은 본 개시가 적용될 수 있는 무선랜 시스템에서 사용되는 프레임 구조의 예시를 설명하기 위한 도면이다.

[96] MAC 계층으로부터의 명령어(instruction) 또는 프리머티브(primitive)(명령어들 또는 파라미터들의 세트를 의미함)에 의해서, PHY 계층은 송신될 MPDU(MAC PDU)를 준비할 수 있다. 예를 들어, PHY 계층의 송신 시작을 요청하는 명령어를 MAC 계층으로부터 받으면, PHY 계층에서는 송신 모드로 스위치하고 MAC 계층으로부터 제공되는 정보(예를 들어, 데이터)를 프레임의 형태로 구성하여 송신할 수 있다. 또한, PHY 계층에서는 수신되는 프레임의 유효한 프리앰블(preamble)을 검출하게 되면, 프리앰블의 헤더를 모니터링하여 PHY 계층의 수신 시작을 알려주는 명령어를 MAC 계층으로 보낸다.

[97] 이와 같이, 무선랜 시스템에서의 정보 송신/수신은 프레임의 형태로 이루어지며, 이를 위해서 PHY 계층 프로토콜 데이터 유닛(Physical layer Protocol Data Unit, PPDU) 포맷이 정의된다.

[98] 기본적인 PPDU는 STF(Short Training Field), LTF(Long Training Field), SIG(SIGNAL) 필드, 및 데이터(Data) 필드를 포함할 수 있다. 가장 기본적인(예를 들어, 도 7에서 도시하는 non-HT(High Throughput)) PPDU 포맷은 L-STF(Legacy-STF), L-LTF(Legacy-LTF), L-SIG(Legacy-SIG) 필드 및 데이터 필드만으로 구성될 수 있다. 또한, PPDU 포맷의 종류(예를 들어, HT-mixed 포맷 PPDU, HT-greenfield 포맷 PPDU, VHT(Very High Throughput) PPDU 등)에 따라서, L-SIG 필드와 데이터 필드 사이에 추가적인 (또는 다른 종류의) RL-SIG, U-SIG, 비-레거시 SIG 필드, 비-레거시 STF, 비-레거시 LTF, (즉, xx-SIG, xx-STF, xx-LTF (예를 들어, xx는

HT, VHT, HE, EHT 등)) 등이 포함될 수도 있다. 보다 구체적인 사항에 대해서는 도 7을 참조하여 후술한다.

[99] STF는 신호 검출, AGC(Automatic Gain Control), 다이버시티 선택, 정밀한 시간 동기 등을 위한 신호이고, LTF는 채널 추정, 주파수 오차 추정 등을 위한 신호이다. STF와 LTF는 OFDM 물리계층의 동기화 및 채널 추정을 위한 신호라고 할 수 있다.

[100] SIG 필드는 PPDU 송신 및 수신에 관련되는 다양한 정보를 포함할 수 있다. 예를 들어, L-SIG 필드는 24 비트로 구성되고, L-SIG 필드는 4-비트 레이트(Rate) 필드, 1-비트 유보(Reserved) 비트, 12-비트 길이(Length) 필드, 1-비트 패리티(Parity) 필드, 및 6-비트 테일(Tail) 필드를 포함할 수 있다. RATE 필드는 데이터의 변조 및 코딩 레이트에 대한 정보를 포함할 수 있다. 예를 들어, 12-비트 Length 필드는 PPDU의 길이 또는 시간 듀레이션에 관한 정보를 포함할 수 있다. 예를 들어, 12-비트 Length 필드의 값은 PPDU의 타입을 기초로 결정될 수 있다. 예를 들어, non-HT, HT, VHT, 또는 EHT PPDU에 대해서, Length 필드의 값은 3의 배수로 결정될 수 있다. 예를 들어, HE PPDU에 대해서, Length 필드의 값은 3의 배수 + 1 또는 3의 배수 + 2로 결정될 수 있다.

[101] 데이터 필드는 SERVICE 필드, PSDU(Physical layer Service Data Unit), PPDU TAIL 비트를 포함할 수 있고, 필요한 경우에는 패딩 비트도 포함할 수 있다. SERVICE 필드의 일부 비트는 수신단에서의 디스크램블러의 동기화를 위해 사용될 수 있다. PSDU는 MAC 계층에서 정의되는 MAC PDU에 대응하며, 상위 계층에서 생성/이용되는 데이터를 포함할 수 있다. PPDU TAIL 비트는 인코더를 0 상태로 리턴하기 위해서 이용될 수 있다. 패딩 비트는 데이터 필드의 길이를 소정의 단위로 맞추기 위해서 이용될 수 있다.

[102] MAC PDU는 다양한 MAC 프레임 포맷에 따라서 정의되며, 기본적인 MAC 프레임은 MAC 헤더, 프레임 바디, 및 FCS(Frame Check Sequence)로 구성된다. MAC 프레임은 MAC PDU로 구성되어 PPDU 포맷의 데이터 부분의 PSDU를 통하여 송신/수신될 수 있다.

[103] MAC 헤더는 프레임 제어(Frame Control) 필드, 듀레이션(Duration)/ID 필드, 주소(Address) 필드 등을 포함한다. 프레임 제어 필드는 프레임 송신/수신에 필요한 제어 정보들을 포함할 수 있다. 듀레이션/ID 필드는 해당 프레임 등을 송신하기 위한 시간으로 설정될 수 있다. 주소 서브필드들은 프레임의 수신자(receiver) 주소, 송신자(transmitter) 주소, 목적지(destination) 주소, 소스(source) 주소를 나타낼 수 있으며, 일부 주소 서브필드는 생략될 수도 있다. 시퀀스 제어(Sequence Control), QoS 제어(QoS Control), HT 제어(HT Control) 서브필드들을 포함하여, MAC 헤더의 각각의 서브필드들의 구체적인 내용은 IEEE 802.11 표준 문서를 참조할 수 있다.

[104] 널-데이터 PPDU(NDP) 포맷은 데이터 필드를 포함하지 않는 형태의 PPDU 포맷을 의미한다. 즉, NDP은, 일반적인 PPDU 포맷에서 PPDU 프리앰블(즉, L-STF,

L-LTF, L-SIG 필드, 및 추가적으로 존재한다면 비-레거시 SIG, 비-레거시 STF, 비-레거시 LTF)을 포함하고, 나머지 부분(즉, 데이터 필드)은 포함하지 않는 프레임 포맷을 의미한다.

[105] 도 7은 본 개시가 적용될 수 있는 IEEE 802.11 표준에서 정의되는 PPDU의 예시들을 도시한 도면이다.

[106] IEEE 802.11a/g/n/ac/ax 등의 표준에서는 다양한 형태의 PPDU가 사용되었다. 기본적인 PPDU 포맷(IEEE 802.11a/g)은 L-LTF, L-STF, L-SIG 및 Data 필드를 포함한다. 기본적인 PPDU 포맷을 non-HT PPDU 포맷이라 칭할 수도 있다(도 7(a)).

[107] HT PPDU 포맷(IEEE 802.11n)은 HT-SIG, HT-STF, HT-LFT(s) 필드를 기본적인 PPDU 포맷에 추가적으로 포함한다. 도 7(b)에 도시된 HT PPDU 포맷은 HT-mixed 포맷이라고 칭할 수 있다. 추가적으로 HT-greenfield 포맷 PPDU가 정의될 수 있으며, 이는 L-STF, L-LTF, L-SIG를 포함하지 않고, HT-GF-STF, HT-LTF1, HT-SIG, 하나 이상의 HT-LTF, Data 필드로 구성되는 포맷에 해당한다 (미도시).

[108] VHT PPDU 포맷(IEEE 802.11ac)의 일례는 VHT SIG-A, VHT-STF, VHT-LTF, VHT-SIG-B 필드를, 기본적인 PPDU 포맷에 추가적으로 포함한다(도 7(c)).

[109] HE PPDU 포맷(IEEE 802.11ax)의 일례는 RL-SIG(Repeated L-SIG), HE-SIG-A, HE-SIG-B, HE-STF, HE-LTF(s), PE(Packet Extension) 필드를, 기본적인 PPDU 포맷에 추가적으로 포함한다(도 7(d)). HE PPDU 포맷의 세부 예시들에 따라 일부 필드가 제외되거나 그 길이가 달라질 수도 있다. 예를 들어, HE-SIG-B 필드는 다중 사용자(MU)를 위한 HE PPDU 포맷에 포함되고, 단일 사용자(SU)를 위한 HE PPDU 포맷에는 HE-SIG-B가 포함되지 않는다. 또한, HE 트리거-기반(trigger-based, TB) PPDU 포맷은 HE-SIG-B를 포함하지 않고, HE-STF 필드의 길이가 8 마이크로초(us)로 달라질 수 있다. HE ER(Extended Range) SU PPDU 포맷은 HE-SIG-B 필드를 포함하지 않고, HE-SIG-A 필드의 길이가 16us로 달라질 수 있다. 예를 들어, RL-SIG는 L-SIG와 동일하게 구성될 수 있다. 수신 STA은 RL-SIG의 존재를 기초로 수신 PPDU가 HE PPDU 또는 후술하는 EHT PPDU임을 알 수 있다.

[110] EHT PPDU 포맷은 도 7(e)의 EHT MU(multi-user) 및 도 7(f)의 EHT TB(trigger-based) PPDU를 포함할 수 있다. EHT PPDU 포맷은 L-SIG에 후속하여 RL-SIG를 포함하는 것은 HE PPDU 포맷과 유사하지만, RL-SIG에 후속하여 U(universal)-SIG, EHT-SIG, EHT-STF, EHT-LTF를 포함할 수 있다.

[111] 도 7(e)의 EHT MU PPDU는 하나 이상의 사용자에 대한 하나 이상의 데이터(또는 PSDU)를 나르는(carry) PPDU에 해당한다. 즉, EHT MU PPDU는 SU 송신 및 MU 송신 모두를 위해서 사용될 수 있다. 예를 들어, EHT MU PPDU는 하나의 수신 STA 또는 복수의 수신 STA을 위한 PPDU에 해당할 수 있다.

[112] 도 7(f)의 EHT TB PPDU는 EHT MU PPDU에 비하여 EHT-SIG가 생략된다. UL MU 송신을 위한 트리거(예를 들어, 트리거 프레임 또는 TRS(triggered response

scheduling))를 수신한 STA은, EHT TB PPDU 포맷에 기초하여 UL 송신을 수행할 수 있다.

[113] L-STF, L-LTF, L-SIG, RL-SIG, U-SIG(Universal SIGNAL), EHT-SIG 필드들은, 레거시 STA에서도 복조 및 디코딩을 시도할 수 있도록 인코딩 및 변조되어 정해진 서브캐리어 주파수 간격(예를 들어, 312.5kHz)에 기반하여 매핑될 수 있다. 이들을 프리-EHT 변조(pre-EHT modulated) 필드들이라고 칭할 수 있다. 다음으로, EHT-STF, EHT-LTF, Data, PE 필드들은, 비-레거시 SIG(예를 들어, U-SIG 및/또는 EHT-SIG)를 성공적으로 디코딩하여 해당 필드에 포함된 정보를 획득한 STA에 의해서 복조 및 디코딩될 수 있도록 인코딩 및 변조되어 정해진 서브캐리어 주파수 간격(예를 들어, 78.125kHz)에 기반하여 매핑될 수 있다. 이들을 EHT 변조(EHT modulated) 필드들이라고 칭할 수 있다.

[114] 이와 유사하게, HE PPDU 포맷에서 L-STF, L-LTF, L-SIG, RL-SIG, HE-SIG-A, HE-SIG-B 필드들을 프리-HE 변조 필드라 칭하고, HE-STF, HE-LTF, Data, PE 필드들을 HE 변조 필드라고 칭할 수 있다. 또한, VHT PPDU 포맷에서 L-STF, L-LTF, L-SIG, VHT-SIG-A 필드들을 프리 VHT 변조 필드라고 칭하고, VHT STF, VHT-LTF, VHT-SIG-B, Data 필드들을 VHT 변조 필드라고 칭할 수 있다.

[115] 도 7의 EHT PPDU 포맷에 포함되는 U-SIG는, 예를 들어, 2개의 심볼(예를 들어, 연속하는 2 개의 OFDM 심볼)을 기초로 구성될 수 있다. U-SIG를 위한 각 심볼(예를 들어, OFDM 심볼)은 4us의 듀레이션을 가질 수 있고, U-SIG는 전체 8us의 듀레이션을 가질 수 있다. U-SIG의 각 심볼은 26 비트 정보를 송신하기 위해 사용될 수 있다. 예를 들어 U-SIG의 각 심볼은 52개의 데이터 톤과 4 개의 파일럿 톤을 기초로 송수신될 수 있다.

[116] U-SIG는 20MHz 단위로 구성될 수 있다. 예를 들어, 80MHz PPDU가 구성되는 경우, 20MHz 단위로 동일한 U-SIG가 복제될 수 있다. 즉, 80MHz PPDU 내에 동일한 4개의 U-SIG가 포함될 수 있다. 80 MHz 대역폭을 초과하는 경우, 예를 들어, 160MHz PPDU에 대해서는 첫 번째 80MHz 단위의 U-SIG와 두 번째 80MHz 단위의 U-SIG는 상이할 수 있다.

[117] U-SIG를 통해서는 예를 들어 A 개의 코딩되지 않은 비트(un-coded bit)가 송신될 수 있고, U-SIG의 제 1 심볼(예를 들어, U-SIG-1 심볼)은 총 A 비트 정보 중 처음 X 비트 정보를 송신하고, U-SIG의 제 2 심볼(예를 들어, U-SIG-2 심볼)은 총 A 비트 정보 중 나머지 Y 비트 정보를 송신할 수 있다. A 비트 정보(예를 들어, 52 코딩되지 않은 비트)에는 CRC 필드(예를 들어 4 비트 길이의 필드) 및 테일 필드(예를 들어 6 비트 길이의 필드)가 포함될 수 있다. 테일 필드는 컨볼루션 디코더의 트렐리스(trellis)를 종료(terminate)하기 위해 사용될 수 있고, 예를 들어 0으로 설정될 수 있다.

[118] U-SIG에 의해 송신되는 A 비트 정보는 버전-독립적(version-independent) 비트들과 버전-종속적(version-dependent) 비트들로 구분될 수 있다. 예를 들어, 도 7에 도시하지 않은 새로운 PPDU 포맷(예를 들어, UHR PPDU 포맷)에 U-SIG가 포함

될 수 있으며, EHT PPDU 포맷에 포함되는 U-SIG 필드의 포맷과, UHR PPDU 포맷에 포함되는 U-SIG 필드의 포맷에서, 버전-독립적 비트들은 동일할 수 있고, 버전-종속적 비트들은 일부 또는 전부가 상이할 수 있다.

[119] 예를 들어, U-SIG의 버전-독립적 비트들의 크기는 고정적이거나 가변적일 수 있다. 버전-독립적 비트들은 U-SIG-1 심볼에만 할당되거나, U-SIG-1 심볼 U-SIG-2 심볼 모두에 할당될 수 있다. 버전-독립적 비트들과 버전-종속적 비트들은 제 1 제어 비트 및 제 2 제어 비트 등의 다양한 명칭으로 불릴 수 있다.

[120] 예를 들어, U-SIG의 버전-독립적 비트들은 3 비트의 물리계층 버전 식별자(PHY version identifier)를 포함할 수 있으며, 이 정보는 송수신 PPDU의 PHY 버전(예를 들어, EHT, UHR 등)을 지시할 수 있다. U-SIG의 버전-독립적 비트들은 1 비트의 UL/DL 플래그(flag) 필드를 포함할 수 있다. 1-비트 UL/DL flag 필드의 제 1 값은 UL 통신에 관련되고, UL/DL flag 필드의 제 2 값은 DL 통신에 관련된다. U-SIG의 버전-독립적 비트들은 TXOP(transmission opportunity)의 길이에 관한 정보, BSS 컬러(color) ID에 관한 정보를 포함할 수 있다.

[121] 예를 들어, U-SIG의 버전-종속적 비트들은 PPDU의 타입(예를 들어, SU PPDU, MU PPDU, TB PPDU 등)을 직접적 또는 간접적으로 지시하는 정보를 포함할 수 있다.

[122] PPDU 송수신을 위해서 필요한 정보가 U-SIG에 포함될 수 있다. 예를 들어, U-SIG는, 대역폭에 관한 정보, 비-레거시 SIG(예를 들어, EHT-SIG 또는 UHR-SIG 등)에 적용되는 MCS 기법에 대한 정보, 비-레거시 SIG에 DCM(dual carrier modulation) 기법(예를 들어, 동일한 신호를 두 개의 서브캐리어 상에서 재사용(reuse)하여 주파수 다이버시티와 유사한 효과를 달성하기 위한 기법)이 적용되는지 여부를 지시하는 정보, 비-레거시 SIG를 위해 사용되는 심볼의 개수에 대한 정보, 비-레거시 SIG가 전 대역에 걸쳐 생성되는지 여부에 대한 정보 등을 더 포함할 수 있다.

[123] PPDU 송수신을 위해서 필요한 정보 중 일부는 U-SIG 및/또는 비-레거시 SIG(예를 들어, EHT-SIG 또는 UHR-SIG 등)에 포함될 수도 있다. 예를 들어, 비-레거시 LTF/STF(예를 들어, EHT-LTF/EHT-STF 또는 UHR-LTF/UHR-STF 등)의 타입에 대한 정보, 비-레거시 LTF의 길이 및 CP(cyclic prefix) 길이에 대한 정보, 비-레거시 LTF에 적용되는 GI(guard interval)에 대한 정보, PPDU에 적용가능한 프리앰블 펑처링(puncturing)에 대한 정보, RU(resource unit) 할당에 대한 정보 등은, U-SIG에만 포함될 수도 있고, 비-레거시 SIG에만 포함될 수도 있고, U-SIG에 포함된 정보와 비-레거시 SIG에 포함되는 정보의 조합에 의해서 지시될 수도 있다.

[124] 프리앰블 펑처링은 PPDU의 대역폭 중에서 하나 이상의 주파수 유닛에 신호가 존재(present)하지 않는 PPDU의 송신을 의미할 수 있다. 예를 들어, 주파수 유닛의 크기(또는 프리앰블 펑처링의 분해도(resolution))는 20MHz, 40MHz 등으로 정

의될 수도 있다. 예를 들어, 소정의 크기 이상의 PPDU 대역폭에 대해서 프리앰블 펑처링이 적용될 수 있다.

[125] 도 7의 예시에서 HE-SIG-B, EHT-SIG 등의 비-레거시 SIG는 수신 STA을 위한 제어 정보를 포함할 수 있다. 비-레거시 SIG는 적어도 하나의 심볼을 통해 송신될 수 있고, 하나의 심볼은 4us의 길이를 가질 수 있다. EHT-SIG를 위해 사용되는 심볼의 개수에 관한 정보는 이전의 SIG(예를 들어, HE-SIG-A, U-SIG 등)에 포함될 수 있다.

[126] HE-SIG-B, EHT-SIG 등의 비-레거시 SIG는, 공통필드(common field) 및 사용자-특정 필드(user-specific field)를 포함할 수 있다. 공통 필드 및 사용자-특정 필드는 개별적으로 코딩될 수 있다.

[127] 일부 경우에서, 공통 필드는 생략될 수도 있다. 예를 들어, 비-OFDMA(orthogonal frequency multiple access)가 적용되는 압축 모드에서 공통 필드가 생략될 수 있고, 복수의 STA은 동일한 주파수 대역을 통해 PPDU(예를 들어, PPDU의 데이터 필드)를 수신할 수 있다. OFDMA가 적용되는 비-압축 모드에서는 복수의 사용자는 상이한 주파수 대역을 통해 PPDU(예를 들어, PPDU의 데이터 필드)를 수신할 수 있다.

[128] 사용자-특정 필드의 개수는 사용자(user)의 개수를 기초로 결정될 수 있다. 하나의 사용자 블록 필드는 최대 2개의 사용자 필드(user field)를 포함할 수 있다. 각 사용자 필드(user field)는 MU-MIMO 할당에 관련되거나, 비-MU-MIMO 할당에 관련될 수 있다.

[129] 공통 필드는 CRC 비트와 Tail 비트를 포함할 수 있고, CRC 비트의 길이는 4 비트로 결정될 수 있고, Tail 비트의 길이는 6 비트로 결정되고 000000으로 설정될 수 있다. 공통 필드는 RU 할당 정보(RU allocation information)를 포함할 수 있다. RU 할당 정보는 복수의 사용자(즉, 복수의 수신 STA)이 할당되는 RU의 위치(location)에 관한 정보를 포함할 수 있다.

[130] RU는 복수 개의 서브캐리어(또는 톤)을 포함할 수 있다. RU는 OFDMA 기법을 기초로 다수의 STA에게 신호를 송신하는 경우 사용될 수 있다. 또한 하나의 STA에게 신호를 송신하는 경우에도 RU가 정의될 수 있다. 비-레거시 STF, 비-레거시 LTF, Data 필드에 대해 RU 단위로 자원이 할당될 수 있다.

[131] PPDU 대역폭에 따라서 적용가능한 크기의 RU가 정의될 수 있다. RU는 적용되는 PPDU 포맷(예를 들어, HE PPDU, EHT PPDU, UHR PPDU 등)에 대해서 동일하게 또는 상이하게 정의될 수도 있다. 예를 들어, 80MHz PPDU의 경우 HE PPDU와 EHT PPDU의 RU 배치가 상이할 수 있다. PPDU 대역폭 별로 적용가능한 RU의 크기, RU 개수, RU 위치, DC(direct current) 서브캐리어 위치 및 개수, 널(null) 서브캐리어 위치 및 개수, 가드 서브캐리어 위치 및 개수 등을 톤-플랜(tone-plan)이라 할 수 있다. 예를 들어, 넓은 대역폭에 대한 톤-플랜은 낮은 대역폭의 톤-플랜의 다수 반복의 형태로 정의될 수도 있다.

[132] 다양한 크기의 RU는 26-톤 RU, 52-톤 RU, 106-톤 RU, 242-톤 RU, 484-톤 RU, 996-톤 RU, 2X996-톤 RU, 4X996-톤 RU 등과 같이 정의될 수 있다. MRU(multiple RU)는 복수의 개별적인 RU와 구별되며, 복수의 RU로 구성되는 서브캐리어들의 그룹에 해당한다. 예를 들어, 하나의 MRU는, 52+26-톤, 106+26-톤, 484+242-톤, 996+484-톤, 996+484+242-톤, 2X996+484-톤, 3X996-톤, 또는 3X996+484-톤으로 정의될 수 있다. 또한, 하나의 MRU를 구성하는 복수의 RU는 주파수 도메인에서 연속적일 수도 있고, 연속적이지 않을 수도 있다.

[133] RU의 구체적인 크기는 축소 또는 확장될 수도 있다. 따라서, 본 개시에서 각 RU의 구체적인 크기(즉, 상응하는 톤의 개수)는 제한적이지 않으며 예시적이다. 또한, 본 개시에서 소정의 대역폭(예를 들어, 20, 40, 80, 160, 320MHz, ...) 내에서, RU의 개수는 RU 크기에 따라서 달라질 수 있다.

[134] 도 7의 PPDU 포맷들에서 각각의 필드의 명칭은 예시적인 것이며, 그 명칭에 의해서 본 개시의 범위가 제한되지 않는다. 또한, 본 개시의 예시들은, 도 7에서 예시하는 PPDU 포맷은 물론, 도 7의 PPDU 포맷들을 기반으로 일부 필드가 제외되거나 및/또는 일부 필드가 추가되는 형태의 새로운 PPDU 포맷에도 적용될 수 있다.

[135] 다중 액세스 포인트(MAP) 동작

[136] 이하에서는 다중 액세스 포인트(MAP) 동작에 대한 본 개시의 예시들에 대해서 설명한다.

[137] MAP 동작은 마스터 AP(또는 공유하는(sharing) AP) 및 슬레이브 AP(또는 공유받는(shared) AP) 간의 동작으로 정의될 수 있다.

[138] 마스터 AP는 다수의 AP 간의 송수신을 위한 MAP 동작을 개시(initiate)하고 제어(control)하는 역할을 한다. 마스터 AP는 슬레이브 AP를 그룹화하고, 슬레이브 AP들 간 정보를 공유할 수 있도록 슬레이브 AP들과의 링크를 관리한다. 마스터 AP는 슬레이브 AP들이 구성하고 있는 BSS의 정보와, 해당 BSS에 결합(association)을 맺은 STA들의 정보를 관리한다.

[139] 슬레이브 AP는 마스터 AP와 결합을 맺고, 서로 제어 정보, 관리 정보, 데이터 트래픽을 공유할 수 있다. 슬레이브 AP는 무선랜에서의 BSS를 수립(establish)할 수 있는 AP의 기본적인 기능을 동일하게 수행한다.

[140] MAP 동작에서의 STA은 슬레이브 AP 또는 마스터 AP와 결합을 맺고 BSS를 구성할 수 있다.

[141] MAP 환경에서, 마스터 AP와 슬레이브 AP는 서로 직접적인 송수신을 수행할 수 있다. 마스터 AP와 STA은 서로 직접적인 송수신을 수행하지 못할 수도 있다. 슬레이브 AP(예를 들어, STA과 결합을 맺은 슬레이브 AP)는 STA과 직접적인 송수신을 수행할 수 있다. 슬레이브 AP들 중의 하나가 마스터 AP가 될 수 있다.

[142] MAP 동작은, 하나 이상의 AP들이 하나 이상의 STA에게 정보를 전송 및 수신하는 기법이다. 예를 들어, AP 간 할당을 시간축으로 나누는 C-TDMA (coordinated-time division multiple access), 주파수축으로 나누는 C-

OFDMA(coordinated-orthogonal frequency division multiple access), 공간 재사용을 이용하는 C-SR(coordinated-spatial reuse) 기법 등이 MAP 동작을 위해 적용될 수 있다. 또는, MAP 동작은 협력하여 동시에 송수신을 수행하는 협력 빔포밍(coordinated beamforming, C-BF) 또는 조인트 빔포밍(joint beamforming) 기법도 적용될 수 있다.

[143] 도 8은 본 개시가 적용될 수 있는 MAP 환경에서의 다양한 송수신 기법을 설명하기 위한 도면이다.

[144] 기존 방식과 같이 BSS AP가 BSS STA에게 송신을 수행하는 것을 STX(single transmission)이라고 칭할 수 있다. STX에서는 인접 AP와의 간섭(interference)으로 인해 셀 에지(edge)에 위치한 사용자/STA들에 대한 송수신의 성능이 떨어지는 문제가 있다. 예를 들어, 도 8(a)와 같이 AP1과 AP2가 동일한 주파수 대역폭에서 동일한 시간에 각각 STA1 및 STA2에 대한 송신을 수행하는 경우 무선 매체 상에서 충돌이 발생할 수 있다.

[145] MAP 기법에서는 이웃 AP들간의 협력을 통해서 심볼간 간섭(ISI)을 줄이거나, 함께 송신을 수행하는 방법 등을 통해 성능을 개선할 수 있다. 예를 들어, 도 8(b)의 C-OFDMA 방식에서는 동일한 시간에 AP1은 제 1 대역폭에서 STA1에게 송신을 수행하고, AP2는 제 2 대역폭에서 STA2에게 송신을 수행함으로써 간섭을 회피할 수 있다. 도 8(c)의 예시에서는 AP1이 STA1으로의 송신을 수행하면서 AP2 및/또는 STA2에게 미치는 간섭을 널링(nulling)하고, AP2가 STA2로의 송신을 수행하면서 AP1 및/또는 STA1에게 미치는 간섭을 널링하는 협력 빔포밍 또는 널링 기법을 나타낸다. 도 8(d)에서는 인접한 AP들 중에서 채널 상태가 좋은 AP가 송신을 수행하는 AP 선택 방식을 나타낸다. 도 8(e)의 예시와 같이 다수의 AP가 협력하여 동시에 송신 또는 수신하는 조인트 송신(JTX) 또는 조인트 수신(JRX)이 적용될 수도 있으며, 나아가 조인트 MU-MIMO가 지원될 수도 있다.

[146] RSN 동작

[147] 도 3을 참조하여 설명한 바와 같이, STA과 AP 간의 발견(discovery) 과정 이후 인증(authentication) 과정은 오픈 시스템 방식으로 수행될 수 있고, 결합(association) 과정이 수행될 수 있다. 이러한 과정은 RSN(robust security network) 지원 여부를 탐색하고 인증 및 결합을 맺는 단계 0라고 할 수 있다.

[148] 단계 0이 성공적으로 완료되면, IEEE 802.1X/EAP(extensible authentication protocol) 또는 PSK(pre-shared key)에 의한 사용자 인증 및 PMK(pairwise master key)를 확보하는 단계 1이 수행될 수 있다. 여기서 적용되는 상호 인증 방식은 802.1X/EAP, PSK, 또는 SAE(simultaneous authentication of equals) 등을 포함할 수 있다. 예를 들어, 802.1X/EAP 인증 방식의 경우에는 STA과 RADIUS(remote authentication dial-in user service) 간의 인증 후, MSK(master session key)로부터 PMK가 생성될 수 있다. PSK에 의한 사용자 인증 방식의 경우, AP와 STA은 PSK와 동일하게 PMK를 직접 설정할 수 있다. SAE에 의한 사용자 인증 방식의 경우,

AP와 STA은 SAE 인증 과정을 통해서 상호 인증 및 인증 과정의 연산 값을 이용하여 PMK를 직접 설정할 수 있다.

[149] 단계 1에 후속하여 EAPoL-Key 프레임을 사용하여 상대방이 동일한 PMK를 보유하는지 확인하고, 암호키를 생성 및 공유하는 단계 2가 수행될 수 있다. 단계 2는 4-웨이 핸드셰이킹(4-way handshaking)을 통해서, PMK 생성을 상호 확인하고, 그룹 키(예를 들어, GTK(group temporal key))를 생성 및 전달하는 과정을 포함할 수 있다. 4-웨이 핸드셰이킹을 통하여 PTK(pairwise transient key), KCK(key confirmation key), KEK(key encryption key), TK(temporal key)가 생성될 수 있다.

[150] 구체적으로, 단계 1에서 MSK로부터 PMK가 생성되고, 단계 2에서 PMK로부터 PTK가 생성될 수 있다. 여기서, PTK는 KCK, KEK, TK로 분리되어 설정된다. GTK는 AP로부터 생성되어 STA에게 전달될 수 있다. AP가 새로운 GTK를 생성하고자 하는 경우 STA과의 핸드셰이킹을 수행하고 STA에게 새로운 GTK를 전달할 수도 있다.

[151] STA과 AP가 상호 동일한 PMK를 보유하는지 확인하기 위해서, 802.1X/EAP의 경우에는 STA과 인증 서버(AS) 간의 사용자 인증 결과에 의해서 STA과 AS 간에 동일한 MSK가 설정되고, AS는 AP에게 해당 MSK를 전달한다. STA과 AP는 MSK로부터 생성되는 대칭키인 PMK의 보유 여부를 4-웨이 핸드셰이킹을 통해 서로 확인할 수 있다. PSK의 경우, AP와 STA 간에 사전에 설정된 PSK로부터 생성되는 PMK의 확보 여부를 4-웨이 핸드셰이킹을 통해 상호 검증함으로써 인증 절차를 대신할 수 있다. SAE의 경우 AP와 STA 간에 사전에 설정된 PMK를 4-웨이 핸드셰이킹을 통해 상호 검증할 수 있다.

[152] 동일한 PTK를 생성했음을 STA과 AP가 상호 검증함으로써 동일한 PMK를 보유하는지 확인할 수도 있다. 예를 들어, 4-웨이 핸드셰이킹의 메시지 2 및 메시지 3을 통해서 PMK 확보 여부를 확인할 수도 있다. 구체적으로, 메시지 2에서 STA은 자신이 생성한 PTK의 KCK를 키 MIC 필드(Key MIC field(에 포함해서 AP에게 송신할 수 있다. 메시지 3에서 AP는 자신이 생성한 PTK의 KCK의 키 MIC 필드에 포함해서 STA에게 송신할 수 있다. 이를 통해서 STA(AP)은 AP(STA)가 자신의 PTK와 동일한 PTK를 생성했음을 검증하여 AP(STA)가 자신과 동일한 PMK를 보유하는 것을 확인할 수 있다. 한편, 메시지 1에서는 키 MIC 필드의 값이 0으로 설정될 수 있고, 메시지 4에서는 키 MIC 필드에 KCK 값이 포함될 수 있다.

[153] 이와 같이, 단계 2에서 STA과 AP 간에 송수신될 데이터를 암호화하기 위한 비밀키가 생성될 수 있다. RSN에서는 AP에게 결합된 STA마다 다른 비밀키가 생성되고, STA이 다른 AP와 재-결합되는 경우 또 다른 비밀키가 생성된다.

[154] 단계 2의 4-웨이 핸드셰이킹의 결과로서 생성된 TK에 기초하여, TKIP(temporal key integrity protocol), CCMP(cipher-block chaining message authentication code protocol), GCMP(Galois/Counter Mode protocol) 등을 이용하여 데이터에 대한 암호화가 수행될 수 있으며, 이를 단계 3이라고 칭할 수 있다.

[155] 전술한 MSK, PSK, PMK, PTK, KCK, KEK, TK는 페어와이즈(pairwise), 즉, AP와 STA 간에 쌍을 이루는 키에 해당한다. 페어와이즈 키와 달리 그룹 키는, 비콘 프레임과 같이 AP가 그룹-어드레시된 프레임에 대한 비밀키 생성을 위해서 GMK(group master key)에 기초하여 생성될 수 있다. GMK는 AP가 랜덤하게 설정한다. GTK(group temporal key)는 GMK로부터 PRF(pseudorandom function) 함수에 의해서 생성되며, AP로부터 STA으로의 단방향 그룹 키에 해당한다.

[156] 도 9는 본 개시가 적용될 수 있는 4-웨이 핸드셰이킹 절차를 설명하기 위한 도면이다.

[157] STA은 인증을 요청하는 측(supplicant)에 해당하고, AP는 인증을 하는 측(authenticator)에 해당한다. 4-웨이 핸드셰이킹은, STA이 PMK를 보유 또는 알고 있고, AP가 PMK 및 GMK를 보유 또는 알고 있는 경우에, AP 및 STA 간에 PTK 및 GTK를 생성 및 확인하기 위해서 수행될 수 있다.

[158] ANonce 및 SNonce는 PTK 생성을 위해서 사용되는 PRF 함수에서 사용되는 인자에 해당한다. ANonce는 액세스 포인트(즉, authenticator)에 의해서 생성되는 난수(random number)에 해당할 수 있다. SNonce는 STA(즉, supplicant)에 의해서 생성되는 난수에 해당할 수 있다. PRF 함수는, 예를 들어, PMK, ANonce, SNonce, supplicant의 MAC 어드레스, authenticator의 MAC 어드레스에 기초하여 PTK를 생성하는 함수에 해당할 수 있다.

[159] 단계 S810의 메시지 1은 AP로부터 STA에게 유니캐스트 방식으로 송신되며, EAPOL-key 프레임은 ANonce 정보를 포함할 수 있다. AP가 PMK를 생성한 경우, EAPOL-key 프레임의 키 데이터 필드에 PMKID가 포함될 수 있다. STA은 AP로부터 수신한 정보에 기초하여 PTK를 생성할 수 있고, PTK에 기초하여 KCK, KEK, TK를 생성할 수 있다.

[160] 단계 S820의 메시지 2는 STA으로부터 AP에게 유니캐스트 방식으로 송신되며, EAPOL-key 프레임은 SNonce 정보 및 키 MIC(message integrity code)를 포함할 수 있다. 예를 들어, 메시지 2의 키 MIC는 STA이 생성한 KCK에 기초하는 값을 가질 수 있다. AP는 STA로부터 수신한 정보에 기초하여 PTK를 생성할 수 있고, PTK에 기초하여 KCK, KEK, TK를 생성할 수 있다. AP는 메시지 2에 포함된 값에 기초하여 생성한 PTK의 KCK 값과, 메시지 2에 포함된 키 MIC 값에 관련된 KCK 값이 동일한지 여부에 따라서, AP와 STA이 동일한 PTK를 생성한 것인지 검증할 수 있다. 또한, AP는 필요한 경우 GTK를 생성할 수 있다. GTK의 생성은 STA의 관여 없이 AP에 의해서 GMK로부터 생성될 수 있다.

[161] 단계 S830의 메시지 3는 AP로부터 STA에게 유니캐스트 방식으로 송신되며, EAPOL-key 프레임은 MIC(즉, AP가 생성한 PTK의 KCK 값에 해당), 암호화된 GTK 정보를 포함할 수 있다. 메시지 3의 암호화된 GTK는 AP가 생성한 KEK에 기초하여 암호화되어 키 데이터 필드에 포함될 수 있다. STA은 PTK를 PTK-SA(PTK-Security Association)에 저장하고, GTK를 GTK-SA에 저장할 수 있다.

[162] 단계 S840의 메시지 4는 STA으로부터 AP에게 유니캐스트 방식으로 송신되며, EAPOL-key 프레임은 MIC 정보를 포함할 수 있다. MIC를 통하여 검증 완료되면, AP는 PTK를 PTK-SA에 저장하고, GTK를 GTK-SA에 저장할 수 있다.

[163] 이와 같이 4-웨이 핸드셰이킹이 성공적으로 완료되면, 모든 트래픽을 블락(block)하는 가상 제어 포트가 언블락(ubblock)되고 암호화된 트래픽이 송수신될 수 있다. 이후 모든 유니캐스트 트래픽은 PTK에 의해서 암호화되고, 모든 멀티캐스트/브로드캐스트 트래픽은 GTK에 의해서 암호화될 수 있다.

[164] RSNA 기밀성(confidentiality) 및 무결성(integrity) 프로토콜

[165] RSNA에 대해서, STA들에 대한 인증 메커니즘, 키 관리 알고리즘, 암호 키 수립(cryptographic key establishment), 암호 메커니즘, FT(fast BSS transition), 강인한(robust) 관리 프레임에 대한 암호 인캡슐레이션 등이 정의될 수 있다. 예를 들어, 암호 메커니즘은, CCMP(counter mode(CTR) with cipher-block chaining message authentication code(CBC-MAC) protocol), GCMP(Galois/Counter Mode protocol) 등을 포함할 수 있다.

[166] RSNA 보안은 TKIP(temporal key integrity protocol), CCMP, GCMP, BIP(broadcast/multicast integrity protocol), RSNA 수립 및 종료(termination) 절차, 키 관리 절차(예를 들어, 키 분배) 등의 알고리즘 및 절차를 포함할 수 있다. 예를 들어, RSNA 수립 및 종료 절차는, IEEE 802.1X 인증, SAE(simultaneous authentication of equals) 인증, IETF(internet engineering task force) RFC(request for comments) 8110에서 정의되는 OWE(opportunistic wireless encryption) 등을 포함할 수 있다.

[167] 이하에서는 CCMP(counter mode(CTR) with cipher-block chaining message authentication code(CBC-MAC) protocol)에 대해서 설명한다.

[168] CCMP는 데이터 기밀성(confidentiality), 인증, 무결성(integrity), 및 리플레이 보호(replay protection) 등을 제공하는 프로토콜이다. CCMP는 AES(advanced encryption standard) 암호화 알고리즘의 CCM에 기초한다. CCM은 데이터 기밀성에 대한 CTR 및 인증 및 무결성에 대한 CBC-MAC를 조합한다. CCM은 MPDU 데이터 필드 및 MPDU 헤더(MAC 헤더)의 선택된 부분 양자 모두에 대한 무결성을 보호할 수 있다.

[169] 도 9는 본 개시가 적용될 수 있는 확대된(expanded) CCMP MPDU의 일 예시를 나타내는 도면이다.

[170] 보안 PV0(protocol version 0) MPDU에 대해서, CCMP-128 프로세싱은 원래의 MPDU 크기를 16 옥텟(즉, CCMP 헤더 필드에 대한 8 옥텟 및 MIC 필드에 대한 8 옥텟)만큼 확대시킨다. CCMP-256 프로세싱은 원래의 MPDU 크기를 24 옥텟(즉, CCMP 헤더 필드에 대한 8 옥텟, MIC 필드에 대한 16 옥텟)만큼 확대시킨다. CCMP 헤더 필드는 PN(packet number), ExtIV (extended initialization vector), 및 키 ID 서브필드로부터 구성(construct)된다. PN은 6 옥텟의 어레이로서 표현되는 48-비트 PN이다. PN5는 PN의 최상위(most significant) 옥텟이고, PN0은 최하위

(least significant) 옥텟이다. CCMP 헤더의 세 번째 옥텟은 유보된다. 키 ID 옥텟의 ExtIV 서브필드(비트 5(B5))는 CCMP에 대해서 항상 1로 세팅되고, 비트 6(B6) 및 비트 7(B7)은 키 ID 서브필드이고, 키 ID 옥텟의 나머지 비트들은 유보된다.

[171] 도 10은 본 개시가 적용될 수 있는 CCMP 인캡슐레이션 블록 다이어그램을 나타낸다.

[172] 평문(plaintext) MPDU의 MAC 헤더로부터 AAD(additional authentication data)가 구성(construct)될 수 있다. 평문 MPDU의 A2(address 2) 및 우선순위(priority)와, 증가(increment)된 PN에 기초하여 Nonce가 구성될 수 있다. AAD 및 Nonce는, 데이터 및 TK와 함께 CCM 암호화(encryption)에 사용될 수 있다. 증가된 PN 및 키 ID에 기초하여 CCMP 헤더가 구성될 수 있다. CCM 암호화의 결과물인 데이터 및 MIC는, MAC 헤더 및 CCMP 헤더와 함께, 도 9의 예시와 같은 암호화된 MPDU를 구성할 수 있다.

[173] 도 11은 기존(conventional) AAD의 포맷의 일 예시를 나타낸다.

[174] 도 11(a)의 예시는 PV0 MPDU에 대한 기존 AAD 구성(construction)의 예시에 해당할 수 있다. FC(frame control), A1(address 1), A2(address 2), A3(address 3), SC(sequence control) 필드들은, MAC 헤더에 포함되다면, 기존 AAD에 항상 포함될 수 있다. AAD의 길이는 QC(QoS Control) 필드 및 A4(address 4) 필드의 존재(present) 또는 부재(absent)에 따라서 달라질 수 있다. 기존 AAD에 대해서, 예를 들어, QC 및 A4가 모두 부재하면 AAD 길이는 22 옥텟이고, QC가 존재하고 A4가 부재하면 AAD 길이는 24 옥텟이고, QC가 부재하고 A4가 존재하면 AAD 길이는 28 옥텟이고, QC 및 A4가 모두 존재하면 AAD 길이는 30 옥텟일 수 있다.

[175] AAD는 MPDU 헤더로부터 구성된다. 도 11(b)를 참조하여, 기존 AAD는 MAC 헤더의 듀레이션/ID 필드를 포함하지 않고, MAC 헤더의 HT 제어 필드도 포함하지 않는다. 이는, 재전송과 같은 동작 동안 내용이 변경되거나 삽입/삭제될 수 있는 필드가 기존 AAD에 포함되지 않도록 하기 위함이다.

[176] 또한, MAC 헤더의 프레임 제어(FC) 필드의 일부 서브필드들은 마스크 아웃될(masked-out) 수 있다. 마스크-아웃은 MAC 헤더의 해당 서브필드/필드의 값을 0으로 변경하여 AAD에 포함됨을 의미한다.

[177] 예를 들어, 기존 AAD의 FC 필드에서 마스크-아웃되는 서브필드들은 다음과 같다:

[178] 데이터 프레임의 서브타입(subtype) 서브필드의 3 LSB (즉, 비트 4, 5 및 6)는 마스크-아웃되고, 비트 7은 수정되지 않고;

[179] 리트라이(retry) 서브필드는 마스크-아웃되고;

[180] 전력 관리(power management) 서브필드(즉, 비트 12)는 마스크 아웃되고;

[181] 모어 데이터(more data) 서브필드(즉, 비트 13)는 마스크-아웃 되고;

[182] 보호되는 프레임(protected frame) 서브필드(즉, 비트 14)는 수정되지 않고(즉, 1로서 남겨짐(left));

[183] +HTC 서브필드(즉, 비트 15)는, QoS 제어 필드를 포함하는 모든 데이터 프레임에서 마스크-아웃되고, 그 외의 경우에는 수정되지 않으며;

[184] FC 필드의 다른 서브필드들은 수정되지 않는다.

[185] 예를 들어, 기존 AAD의 시퀀스 제어(SC) 필드에서 시퀀스 번호(sequence number) 서브필드는 마스크-아웃될 수 있다.

[186] 도 11의 예시에서 도시하지는 않지만, 기존 AAD에 QoS 제어(QC) 필드가 포함되는 경우, QC 필드는 MSDU 우선순위(priority) 서브필드, QC TID(traffic identifier) 서브필드, A-MSDU 캐퍼블(capable) 서브필드, A-MSDU 존재(present) 서브필드, A-MSDU 타입 서브필드 중의 하나 이상이 MAC 헤더에 존재하는 경우, 기존 AAD에 포함될 수 있다. 기존 AAD의 QC 필드에서 그 외의 서브필드들은 마스크-아웃될 수 있다. 즉, EOSP(end of service period) 서브필드, ACK 정책 지시자(ACK policy indicator) 서브필드, TXOP 제한(limit) 서브필드, 큐 크기(queue size) 서브필드, TXOP 듀레이션 요청됨(duration requested) 서브필드, 및 AP PS 버퍼 상태(power save buffer state) 서브필드는 마스크-아웃되고 기존 AAD 구성에 사용되지 않을 수 있다.

[187] 도 12는 본 개시가 적용될 수 있는 CCMP 디캡슐레이션 블록 다이어그램을 나타낸다.

[188] 암호화된 MPDU의 MAC 헤더로부터 AAD가 구성될 수 있다. 암호화된 MPDU의 A2 및 우선순위와, PN에 기초하여 Nonce가 구성될 수 있다. AAD 및 Nonce는, MIC, 데이터 및 키와 함께 CCM 복호화(decryption)에 사용될 수 있다. CCM 복호화의 결과물인 데이터는, MAC 헤더와 함께 리플레이 체크(replay check)를 거쳐 평문 MPDU가 획득될 수 있다. 리플레이 체크는 PN 및 리플레이 카운터(replay counter)에 기초할 수 있다.

[189] 이하에서는 BIP(broadcast/multicast integrity protocol)에 대해서 설명한다.

[190] BIP는 IGTKSA(integrity group temporal key security association) 수립 후 그룹 어드레스된 강인한 관리 프레임에 대한 데이터 무결성 및 리플레이 보호를 제공한다. 예를 들어, BIP는 BIGTKSA(beacon IGTKSA) 수립 후 비콘 프레임에 대한 데이터 무결성 및 리플레이 보호를 제공한다. BIP는 IGTK 또는 BIGTK를 사용하여 MMPDU(MAC management PDU) MIC를 계산할 수 있다. MME(management MIC element)는 관리 프레임 바디의 다른 모든 요소 뒤 및 FCS 앞에 위치할 수 있다. 즉, MME는 관리 프레임 바디의 마지막 요소로서 포함될 수 있다. MME는 요소 ID 필드, 길이 필드, 키 ID 필드, IPN(IGTK packet number)/BIPN(BIGTK packet number) 필드, 및 MIC 필드를 포함할 수 있다.

[191] BIP에 대한 기존 AAD는 FC, A1, A2, A3에 기반하여 구성될 수 있으며, FC 내의 리트라이 서브필드(비트 11), 전력 관리 서브필드(비트 12), 및 모어 데이터 서브필드(비트 13)은 마스크-아웃되고, 다른 서브필드들은 수정되지 않을 수 있다.

[192] 이하에서는 GCMP(Galois/Counter Mode protocol)에 대해서 설명한다.

[193] GCMP는 데이터 기밀성(confidentiality), 인증, 무결성(integrity), 및 리플레이 보호(replay protection) 등을 제공하는 프로토콜이다. EHT RSNA STA는 GCMP-256을 지원할 수 있다. GCMP는 AES(advanced encryption standard) 암호화 알고리즘의 GCM에 기초한다. GCM은 MPDU 데이터 필드 및 MPDU 헤더(MAC 헤더)의 선택된 부분 양자 모두에 대한 무결성을 보호할 수 있다.

[194] 도 13은 본 개시가 적용될 수 있는 확대된(expanded) GCMP MPDU의 일 예시를 나타내는 도면이다.

[195] GCMP 프로세싱은 원래의 MPDU 크기를 24 옥텟(즉, GCMP 헤더 필드에 대한 8 옥텟 및 MIC 필드에 대한 16 옥텟)만큼 확대시킨다. CCMP 헤더 필드는 PN(packet number) 및 키 ID 서브필드로부터 구성(construct)된다. PN은 6 옥텟의 어레이로서 표현되는 48-비트 PN이다. PN5는 PN의 최상위(most significant) 옥텟이고, PN0은 최하위(least significant) 옥텟이다. GCMP 헤더의 세 번째 옥텟은 유보된다. 키 ID 옥텟의 ExtIV 서브필드(비트 5(B5))는 GCMP에 대해서 항상 1로 세팅되고, 비트 6(B6) 및 비트 7(B7)은 키 ID 서브필드이고, 키 ID 옥텟의 나머지 비트들은 유보된다.

[196] 도 14는 본 개시가 적용될 수 있는 GCMP 인캡슐레이션 블록 다이어그램을 나타낸다.

[197] 평문(plaintext) MPDU의 MAC 헤더로부터 AAD(additional authentication data)가 구성(construct)될 수 있다. 평문 MPDU의 A2(address 2)와, 증가(increment)된 PN에 기초하여 Nonce가 구성될 수 있다. AAD 및 Nonce는, 데이터 및 TK와 함께 GCM 암호화(encryption)에 사용될 수 있다. 증가된 PN 및 키 ID에 기초하여 GCMP 헤더가 구성될 수 있다. CCM 암호화의 결과물인 데이터는, MAC 헤더 및 CCMP 헤더와 함께, 도 13의 예시와 같은 암호화된 MPDU를 구성할 수 있다.

[198] GCMP에 적용되는 기존 AAD의 구성은 도 11을 참조하여 설명한 바와 동일하므로, 중복되는 설명은 생략한다.

[199] 도 15는 본 개시가 적용될 수 있는 GCMP 디캡슐레이션 블록 다이어그램을 나타낸다.

[200] 암호화된 MPDU의 MAC 헤더로부터 AAD가 구성될 수 있다. 암호화된 MPDU의 A2와, PN에 기초하여 Nonce가 구성될 수 있다. AAD 및 Nonce는, 데이터 및 키와 함께 GCM 복호화(decryption)에 사용될 수 있다. GCM 복호화의 결과물인 데이터는, MAC 헤더와 함께 리플레이 체크(replay check)를 거쳐 평문 MPDU가 획득될 수 있다. 리플레이 체크는 PN 및 리플레이 카운터(replay counter)에 기초할 수 있다.

[201] 블록-ACK 요청(Block ACK Request, BAR) 프레임

[202] 도 16은 본 개시가 적용될 수 있는 블록-ACK 요청 프레임의 예시적인 포맷을 나타내는 도면이다.

[203] 블록-ACK 요청 프레임은 하나의 프레임에 복수의 확인 응답이 포함된 블록-ACK 프레임의 전송을 요청하기 위한 것일 수 있으며, 이를 통해 채널 효율성이

증대될 수 있다. 예를 들어, 제1 STA(예를 들어, AP)는 블록-ACK 요청 프레임을 통해 다수의 MPDU에 대한 수신 결과를 요청할 수 있으며, 블록-ACK 요청 프레임을 수신한 제2 STA(들)은 해당 요청에 기초하여 다수의 MPDU에 대한 확인 응답을 포함하는 블록-ACK 프레임을 송신할 수 있다.

[204] 도 16에 도시된 바와 같이, 블록-ACK 요청(BAR) 프레임은 프레임 바디에 BAR 제어(BAR control) 필드 및 BAR 정보(BAR information) 필드를 포함할 수 있다.

[205] BAR 제어 필드는 블록-ACK 요청 프레임의 유형(예를 들어, 압축된(compressed), 다중 TID(multi-TID), GCR(groupcast with retries) 등)을 지시하는 BAR 유형(BAR type), TID 정보(TID_INFO) 등을 포함할 수 있다.

[206] BAR 정보 필드는 BAR 제어 정보 내 BAR 유형 필드/서브필드에 의해 지시되는 블록-ACK 요청 프레임의 유형(예를 들어, 블록-ACK 요청 프레임 배리언트 유형)에 기초할 수 있다.

[207] 예를 들어, 압축된 블록-ACK 요청 프레임 유형(예를 들어, 압축된 블록-ACK 프레임 유형 또는 확장된 압축된 블록-ACK 프레임 유형)이 지시되는 경우, 압축된 블록-ACK 요청에 상응하는 BAR정보 필드 포맷은 블록-ACK 시작 시퀀스 제어(Block Ack Starting Sequence Control) 서브필드를 포함할 수 있다.

[208] 예를 들어, 블록-ACK 시작 시퀀스 제어 서브필드는 조각 번호(fragment number) 서브필드, 시작 시퀀스 번호(starting sequence number) 서브필드를 포함할 수 있다. 여기서, 조각 번호 서브필드는 0으로 세팅되며, 시작 시퀀스 번호 서브필드는 해당 블록-ACK 요청 프레임이 송신되는 첫번째 MSDU 또는 A-MSDU의 시퀀스 번호를 포함할 수 있다.

[209] 다른 예를 들어, 다중 TID(multi-STA) 블록-ACK 요청 프레임 유형이 지시되는 경우, 다중 TID 블록-ACK 요청에 상응하는 BAR 정보 필드 포맷은 각 TID에 대하여, 각 TID 정보(Per TID Info) 서브필드 및 블록-ACK 시작 시퀀스 제어 서브필드를 포함할 수 있다.

[210] 예를 들어, 각 TID 정보 서브필드는 4-비트의 TID 값 서브필드를 포함할 수 있다. 또한, 블록-ACK 시작 시퀀스 제어 서브필드는 조각 번호 서브필드, 시작 시퀀스 번호 서브필드를 포함할 수 있다. 여기서, 조각 번호 서브필드는 0으로 세팅되며, 시작 시퀀스 번호 서브필드는 해당 블록-ACK 요청 프레임이 송신되는 첫번째 MSDU 또는 A-MSDU의 시퀀스 번호를 포함할 수 있다.

[211] 이와 관련하여, 다중 TID 블록-ACK 요청 프레임의 BAR 제어 필드의 TID_INFO 서브필드는 TID_INFO + 1로 주어진 다중 TID 블록-ACK 요청 프레임에 존재하는 TID의 수를 결정할 수 있다. 예를 들어, TID_INFO 서브필드가 2로 세팅됨은 다중 TID 블록-ACK 요청 프레임의 BAR 정보 필드에 3개의 TID 값이 있다는 것을 의미할 수 있다.

[212] 또 다른 예를 들어, GCR 블록-ACK 요청 프레임 유형이 지시되는 경우, GCR 블록-ACK 요청에 상응하는 BAR 정보 필드 포맷은 GCR 그룹 어드레스 서브필드 및 블록-ACK 시작 시퀀스 제어 서브필드를 포함할 수 있다. 여기서, GCR 그룹

어드레스 서브필드는 수신 상태가 요청되는 그룹의 MAC 어드레스를 포함할 수 있다. 또한, 블록-ACK 시작 시퀀스 제어 서브필드는 조각 번호 서브필드, 시작 시퀀스 번호 서브필드를 포함할 수 있다. 여기서, 조각 번호 서브필드는 0으로 세팅되며, 시작 시퀀스 번호 서브필드는 해당 블록-ACK 요청 프레임이 송신되는 첫번째 MSDU 또는 A-MSDU의 시퀀스 번호를 포함할 수 있다.

[213] 또 다른 예를 들어, GLK-GCR 블록-ACK 요청 프레임 유형이 지시되는 경우, GCR-GCR 블록-ACK 요청에 상응하는 BAR 정보 필드 포맷은 블록-ACK 시작 시퀀스 제어 서브필드를 포함할 수 있다. 여기서, 블록-ACK 시작 시퀀스 제어 서브필드는 조각 번호 서브필드, 시작 시퀀스 번호 서브필드를 포함할 수 있다. 여기서, 조각 번호 서브필드는 0으로 세팅되며, 시작 시퀀스 번호 서브필드는 해당 블록-ACK 요청 프레임이 송신되는 첫번째 MSDU 또는 A-MSDU의 시퀀스 번호를 포함할 수 있다.

[214] 블록-ACK 요청(Block Ack Request, BAR) 프레임에 대한 AAD(additional authentication data) 구성

[215] 기존 무선랜 시스템의 경우, 개별 어드레스된 데이터 프레임(예를 들어, 유니캐스트 기반 데이터 프레임) 및 관리 프레임(들)에 대해, PTK(pairwise transient key)를 이용하여 TKIP(Temporal Key Integrity Protocol)/CCMP/GCMP에 기초하는 암호화/복호화가 수행/적용될 수 있다. 또한, 그룹 어드레스된 프레임(예를 들어, 브로드캐스트 기반 데이터 프레임)에 대해, GTK(group temporal key)를 이용하여 TKIP/CCMP/GCMP에 기초하는 암호화/복호화가 수행/적용될 수 있다. 즉, CCMP/GCMP는 암호화/복호화를 수행하는 보안 프로토콜로서, SU(single-user)의 경우 PTK를 기반으로 하는 TK가 사용되며, MU(multi-user)의 경우에는 GTK를 기반으로 하는 TK가 사용될 수 있다. CCMP/GCMP는 데이터 프레임 및 관리 프레임(들)에 대한 기밀성(confidentiality) 및 무결성(integrity)을 보장할 수 있다.

[216] 또한, 그룹 어드레스된 관리 프레임(들)에 대하여, IGTK(integrity group temporal key)를 이용하여 BIP 기반의 무결성 검사가 수행될 수 있다. 특히, 비콘 프레임의 경우, BIGTK(beacon integrity group temporal key)를 이용하여 BIP 기반의 무결성 검사가 수행될 수 있다. BIP의 경우, IGTK/BIGTK을 기반으로 한 TK을 사용하여 해당 데이터 프레임의 프레임 바디(frame body)에 대한 MIC(message integrity code)을 생성하며, 이에 기초하는 무결성 검사가 수행될 수 있다. 즉, BIP는, CCMP/GCMP와 달리, 데이터 프레임 및 관리 프레임(들)에 대한 무결성만 보장할 수 있다.

[217] CCMP 및 GCMP에 기반하는 MPDU를 구성하는 방식과 BIP에 기반하는 MMPDU(management MPDU)를 구성하는 방식은 다음과 같은 차이점을 가진다.

[218] 먼저, CCMP/GCMP의 경우, 송신 STA은 CCM/GCM으로 데이터 부분에 대한 암호화를 진행하며, 암호화된 데이터를 송신하고, 수신 STA은 수신한 암호화된 데이터를 복호화할 수 있다. 이와 달리, BIP의 경우, 송신 STA은 데이터 부분의

암호화를 진행하지 않으며, 프레임 바디(frame body)의 데이터의 무결성 검사를 위한 MIC을 생성하기 위해 해당 프로토콜을 수행할 수 있다.

[219] 다음으로, CCMP/GCMP의 경우, MPDU는 MAC 헤더, CCMP/GCMP 헤더, 암호화된 데이터, MIC (CCMP의 경우 암호화된 MIC), 및 FCS의 순서로 구성 및 송수신될 수 있다. 이와 달리, BIP의 경우, MAC 헤더, MME(management MIC element)를 포함하는 관리 프레임 바디, 및 FCS의 순서로 구성 및 송수신될 수 있다. 여기서, MME는 CCMP/GCMP 헤더의 역할을 대신하기 때문에, 키 ID 필드(Key ID field), IPN/BIPN, MIC의 정보를 포함할 수 있다.

[220] 전술한 바와 같이, 그룹 어드레스된 프레임 중 데이터 프레임 및 비콘 프레임을 포함한 관리 프레임에 대해서는 보호(protection)가 지원된다. 다만, 제어 프레임(control frame)에 대해서는 보호가 지원되지 않으며, 이에 따라 제어 프레임은 어떠한 암호화/복호화 및/또는 무결성 검사를 위한 프로토콜이 적용되지 않은 상태로 송수신된다.

[221] 예를 들어, ACK 프레임, 블록-ACK(BlockAck, Block Ack, BA) 프레임, 및 블록-ACK 요청 프레임은 제어 프레임의 한 유형에 해당한다. 송신 STA가 데이터를 송신하면, 수신 STA은 해당 데이터에 대한 ACK을 송신 STA에게 송신할 수 있다. 이때, A(aggregated)-MPDU를 지원하는 STA(들)은 해당 ACK을 A-MPDU로 구성하여 블록-ACK 형태로 송신할 수 있다.

[222] 블록-ACK 요청 프레임은 송신 STA이 수신 STA으로부터 블록-ACK을 수신하기 위해 송신될 수 있다. 즉, 송신 STA이 수신 STA에게 블록-ACK 요청 프레임을 송신하면, 수신 STA은 해당 송신 STA에게 블록-ACK 프레임을 송신할 수 있다. 이를 기반으로, 블록-ACK 요청 프레임은 TXOP에서 송신된 이전 프레임에 대한 ACK 정보를 획득하기 위해, 또는 수신 STA의 수신 재-오더 버퍼(receive re-order buffer)를 초기화(예를 들어, 클리어(clear))하기 위해 사용될 수 있다.

[223] 이와 관련하여, 블록-ACK 요청 프레임의 정보가 제3의 STA(예를 들어, 공격(attack) STA)에게 노출이 된다면, 송신 STA과 수신 STA 간의 데이터 송수신 여부를 확인시켜주는 역할인 ACK 정보를 취득하여 송신 STA 및 수신 STA 간의 송수신 여부를 교란시킬 수 있다. 그 결과, 블록-ACK 요청 프레임에 대한 공격은 데이터 송수신 능력의 저하 및 이로 인한 전력(power)/매체(medium)의 낭비가 발생할 수 있다.

[224] 이러한 점을 고려하여, 본 개시에서는 송신 STA과 수신 STA 간에 송수신되는 블록-ACK 요청 프레임의 기밀성 및 무결성을 확보하기 위한 보안 기술을 제안한다.

[225] 또한, 본 개시의 설명에서, 본 개시에 따른 블록-ACK 요청 프레임을 송수신하는 STA(들)은 UHR STA(및/또는 beyond UHR STA)임이 가정된다. 일 예로, 본 개시에 따른 블록-ACK 요청 프레임을 활용하는 경우, 송신 STA인 AP가 송신한 블록-ACK 요청 프레임을 수신하는 수신 STA들은 모두 UHR STA임을 가정할 수 있다. 즉, 만일 본 개시의 제안 방법에 따라 구성된 블록-ACK 요청 프레임을

UHR 이전 STA(pre-UHR STA)(예를 들어, EHT/HE STA 등)이 수신한 경우, 해당 블록-ACK 요청 프레임에 대한 디코딩 시 오류가 발생할 수 있다.

[226] 추가적으로, 본 개시에서는 제어 프레임 중 블록-ACK 요청 프레임에 대한 보안 기술을 대표적인 예시로 하여 설명하지만, 본 개시의 제안 방법은 블록-ACK 요청 프레임 이외의 다른 유형의 제어 프레임에 대해서도 확장하여 적용될 수 있다.

[227] 본 개시에서, 블록 ACK 요청 프레임에 대해 기밀성 및 무결성 검사를 수행한다는 것은 블록 ACK 요청 프레임에 대해 BIP/CCMP/GCMP를 확장하여 적용하는 것으로 해석될 수 있다. 이와 관련하여, 기존에 정의된 BIP/CCMP/GCMP에 대하여 제어 프레임을 위한 사항이 추가적으로 정의되거나, 제어 프레임의 기밀성 및 무결성 검사를 위한 BIP/CCMP/GCMP를 기반으로 하는 별도의 프로토콜이 새롭게 정의될 수도 있다.

[228] 이하에서는 블록-ACK 요청 프레임에 대한 보호(예를 들어, 기밀성 및 무결성 검사)를 지원/수행하는 본 개시의 구체적인 예시들에 대해서 설명한다. 본 개시에서 제안하는 필드, 서브필드, 요소, 파라미터, 키 등의 명칭 및 값들은 예시적인 것이며 그 명칭 및 값으로 제한되지 않는다. 또한, 별도로 구분하지 않는 한, STA은 AP STA일 수도 있고 non-AP STA일 수도 있다.

[229] 도 17은 본 개시에 따른 제1 STA의 동작을 설명하기 위한 도면이다.

[230] 단계 S1710에서 제1 STA은 특정 프로토콜에 기초하여 보호된 블록 ACK 요청 프레임을 제2 STA으로부터 수신할 수 있다.

[231] 단계 S1720에서 제1 STA은 블록 ACK 요청 프레임에 기초하여 AAD를 생성할 수 있다.

[232] 여기서, AAD는 수신된 블록 ACK 요청 프레임의 평문(plain text)에 기초하여 생성될 수 있다. 예를 들어, 보호된 블록 ACK 요청 프레임 내의, 보호 정보가 위치하거나, MIC의 계산 범위에 해당하거나, 암호화된 부분을 제외하고, 평문 상태의 정보에 기초하여 AAD가 생성될 수 있다.

[233] 또한, AAD는, 블록 ACK 요청 프레임의 MAC 헤더에 포함되는 하나 이상의 필드에 기초할 수 있다. 대안적으로, AAD는 블록 ACK 요청 프레임의 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 서브필드에 기초할 수 있다. 대안적으로, AAD는 블록 ACK 요청 프레임의 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 프레임의 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초할 수 있다.

[234] 본 개시에 따라, 블록 ACK 요청 프레임의 보호에 적용되는 특정 프로토콜이 BIP 등의 무결성 프로토콜인 경우, 블록 ACK 요청 프레임의 MAC 헤더, 블록 ACK 요청 제어 필드, 및 블록 ACK 요청 정보 필드 중에서 보호 정보 필드(또는 서브필드)가 위치하는 필드를 제외한 나머지 필드 중의 하나 이상의 서브필드에

기초하여 AAD가 구성될 수 있다. 예를 들어, 보호 정보 (서브)필드는, 키 ID, 패킷 번호(PN), 또는 MIC(message integrity code) 중의 하나 이상을 포함할 수 있다.

[235] 추가적으로 또는 대안적으로, 본 개시에 따라, 블록 ACK 요청 프레임의 보호에 적용되는 특정 프로토콜이 BIP 등의 무결성 프로토콜인 경우, 블록 ACK 요청 프레임의 MAC 헤더, 블록 ACK 요청 제어 필드, 및 블록 ACK 요청 정보 필드 중에서 MIC 계산 범위에 해당하는 하나 이상의 필드를 제외한 나머지 필드 중의 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다. 예를 들어, 보호 정보 (서브)필드가 위치하는 필드는 MIC 계산 범위에 해당할 수 있다.

[236] 예를 들어, 보호 정보 (서브)필드가 위치하는 또는 MIC 계산 범위에 해당하는 필드가 블록 ACK 요청 제어 필드인 경우, 블록 ACK 요청 제어 필드를 제외한 나머지 필드들 중에서, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성되거나, 또는 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다. 예를 들어, 보호 정보 (서브)필드가 위치하는 또는 MIC 계산 범위에 해당하는 필드가 블록 ACK 요청 정보 필드인 경우, 블록 ACK 요청 정보 필드를 제외한 나머지 필드들 중에서, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성되거나, 또는 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다. 예를 들어, 보호 정보 (서브)필드가 위치하는 또는 MIC 계산 범위에 해당하는 필드가 블록 ACK 요청 제어 필드도 아니고 블록 ACK 요청 정보 필드도 아닌 (예를 들어, 블록 ACK 요청 정보 필드와 FCS 필드 사이의 특정 필드인) 경우, 블록 ACK 요청 제어 필드 및 블록 ACK 요청 정보 필드를 제외한 나머지 필드인, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다.

[237] 또한, 본 개시에 따라, 블록 ACK 요청 프레임의 보호에 적용되는 특정 프로토콜이 CCMP, GCMP 등의 암호화 프로토콜인 경우, 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드 중의 하나 이상에 대한 암호화 적용 여부에 기반하여 AAD가 구성될 수 있다.

[238] 예를 들어, 블록 ACK 요청 제어 필드 및 블록 ACK 요청 정보 필드에 암호화가 적용되는 경우, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다. 다른 예를 들어, 블록 ACK 요청 제어 필드에 암호화가 적용되는 경우, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성되거나, 또는 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다. 또 다른 예를 들어, 블록 ACK 요청 정보 필드에 암호화가 적용되는 경우, MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성되거나, 또는 MAC 헤더에 포함되는 하나 이상의 서브필드 및 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 서브필드에 기초하여 AAD가 구성될 수 있다.

[239] 또한, 본 개시에 따라, 블록 ACK 요청 프레임의 상기 MAC 헤더, 블록 ACK 요청 제어 필드, 또는 블록 ACK 요청 정보 필드 중의 하나 이상의 각각에 포함되는 하나 이상의 서브필드는, AAD에 모두 동일하게 포함될 수 있다. 대안적으로, 그 중의 일부 서브필드(들)은 AAD에 동일하게 포함될 수도 있고, 특정 서브필드(들)은 그 비트 값의 일부 또는 전부가 0으로 변경/세팅되어(예를 들어, 마스크-아웃되어) AAD에 포함될 수도 있다.

[240] 이와 관련하여, MAC 헤더에 포함되는 서브필드들 중 AAD 구성에 이용되는 서브필드는, 프레임 제어 서브필드, 듀레이션 서브필드, 수신자 어드레스(RA) 서브필드, 또는 송신자 어드레스(TA) 서브필드 중 하나 이상일 수 있다. 추가적으로, 프레임 제어 서브필드의 하위 서브필드들인, 프로토콜 버전(protocol version) 서브필드, 타입(type) 서브필드, 서브타입(subtype) 서브필드, to DS(distribution system) 서브필드, from DS 서브필드, 모어 프래그먼트(more fragments) 서브필드, 재시도(retry) 서브필드, 전력 관리(power management) 서브필드, 모어 데이터(more data) 서브필드, 보호 프레임(protection frame) 서브필드, 또는 +HTC 서브필드 중의 하나 이상이 AAD 구성에 이용될 수도 있다.

[241] 또한, 블록 ACK 요청 제어 필드에 포함되는 서브필드들 중 AAD 구성에 이용되는 서브필드는, 블록 ACK 요청 타입 서브필드, TID_INFO 서브필드, 또는 비트 위치 0(B0) 및 B5-B11 중의 하나 이상의 비트 위치에 대응하는 서브필드(들) 중의 하나 이상일 수 있다.

[242] 또한, 압축 블록 ACK 요청 배리언트, 확장된 압축 블록 ACK 요청 배리언트, 또는 GLK-GCR 블록 ACK 요청 배리언트의 블록 ACK 요청 정보 필드에 포함되는 서브필드들 중 AAD 구성에 이용되는 서브필드는, 블록 ACK 시작 시퀀스 제어(Block Ack starting sequence control) 서브필드를 포함할 수 있다.

[243] 또한, 다중 TID(traffic identifier) 블록 ACK 요청 배리언트의 블록 ACK 요청 정보 필드에 포함되는 서브필드들 중 AAD 구성에 이용되는 서브필드는, 각 TID 정보(per TID info) 서브필드 또는 블록 ACK 시작 시퀀스 제어 서브필드 중의 하나 이상일 수 있다.

[244] 또한, GCR 블록 ACK 요청 배리언트의 블록 ACK 요청 정보 필드에 포함되는 서브필드들 중 AAD 구성에 이용되는 서브필드는, 블록 ACK 시작 시퀀스 제어 서브필드 또는 GCR 그룹 어드레스 서브필드 중의 하나 이상일 수 있다.

[245] 단계 S1730에서 제1 STA은 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행할 수 있다.

[246] 이와 관련하여, 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상은, 블록 ACK 요청 프레임에 대한 보호와 관련된 키 정보 및 전술한 AAD에 기초하여 수행될 수 있다. 예를 들어, 블록 ACK 요청 프레임은 제2 STA에 의해 수신될 데이터에 대한 블록 ACK의 요청과 관련된 정보를 포함할 수 있다. 여기서, 블록 ACK 요청 프레임에 대한 보호와 관련된 키 정보는, 해당 데이터에 대한 보호를 위한 키 정보와 구별되는 키 정보일 수 있다.

[247] 추가적으로 또는 대안적으로, (전술한 단계 S1710 전에) 제1 STA와 제2 STA 간에, 블록 ACK 요청 프레임에 대한 보호의 지원 여부, 보호된 블록 ACK 요청 프레임의 MPDU 포맷, 또는 블록 ACK 요청 AAD 타입 중의 하나 이상을 지시하는 지시 정보가 교환될 수 있다. 이러한 지시 정보는, 예를 들어, 비콘 프레임, 프로브 요청 프레임, 프로브 응답 프레임, 결합 요청 프레임, 결합 응답 프레임, 재-결합 요청 프레임, 재-결합 응답 프레임 중의 하나 이상에 포함될 수도 있고; 또는 특정 프로토콜이 무결성 프로토콜인 경우 블록 ACK 요청 제어 필드에 포함되거나; 또는 특정 프로토콜이 암호화 프로토콜이고 암호화에서 블록 ACK 요청 제어 필드가 제외되는 경우에는 블록 ACK 요청 제어 필드에 포함될 수도 있고; 또는, 특정 프로토콜이 암호화 프로토콜인 경우에는 블록 ACK 요청 프레임 내 암호화 프로토콜 헤더(예를 들어, CCMP 헤더, GCMP 헤더)에 포함될 수도 있다.

[248] 예를 들어, 블록 ACK 요청 AAD 타입은, AAD가 MAC 헤더에 포함되는 하나 이상의 필드에 기초하여 구성되는 경우인 제1 타입을 지시하거나; 또는 AAD가 MAC 헤더에 포함되는 하나 이상의 필드 및 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 필드에 기초하여 구성되는 경우인 제2 타입을 지시하거나; 또는 AAD가 MAC 헤더에 포함되는 하나 이상의 필드 및 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 필드에 기초하여 구성되는 경우인 제3 타입을 지시할 수 있다.

[249] 예를 들어, 블록 ACK 요청 프레임에 대해 특정 프로토콜이 적용되는 경우, 블록 ACK 요청 프레임의 MAC 헤더의 프레임 제어 서브필드 내 보호된 프레임 (protected frame) 서브필드는 미리 정의된 특정 값으로 세팅될 수 있다. 이에 따라, 제1 STA은 블록 ACK 요청 프레임이 보호된 블록 ACK 요청 프레임임을 확인할 수도 있다.

[250] 도 17의 예시에서 설명하는 방법은 도 1의 제1 디바이스(100)에 의해서 수행될 수 있다. 예를 들어, 도 1의 제1 디바이스(100)의 하나 이상의 프로세서(102)는 특정 프로토콜에 기초하여 보호된 블록 ACK 요청 프레임을 하나 이상의 송수신기(106)를 통하여 수신하고; 블록 ACK 요청 프레임에 기초하여 AAD를 생성하고; 및 AAD에 기초하여 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행하도록 설정될 수 있다. 나아가, 제1 디바이스(100)의 하나 이상의 메모리(104)는 하나 이상의 프로세서(102)에 의해서 실행되는 경우 도 17의 예시 또는 후술하는 예시들에서 설명하는 방법을 수행하기 위한 명령들을 저장할 수 있다.

[251] 도 18은 본 개시에 따른 제2 STA의 동작을 설명하기 위한 도면이다.

[252] 단계 S1810에서 제2 STA은 특정 프로토콜에 기초하여, 블록 ACK 요청 프레임에 대한 AAD를 생성할 수 있다.

[253] 송신 STA인 제2 STA의 블록 ACK 요청 프레임에 대한 AAD의 생성은 도 17의 수신 STA인 제1 STA의 블록 ACK 요청 프레임에 대한 AAD의 생성과 동일하므로, 중복되는 설명은 생략한다. 예를 들어, 블록 ACK 요청 프레임에 대해서 특

정 프로토콜에 기초한 보호가 적용되는 경우, 보호된 블록 ACK 요청 프레임에서, 보호 정보가 위치하거나, MIC의 계산 범위에 해당하거나, 암호화된 부분을 제외하고, 수신 STA측에서 평문 상태의 정보를 획득할 수 있는 부분에 기초하여 AAD가 생성될 수 있다.

[254] 단계 S1820에서 제2 STA은 AAD에 기초하여 보호된 블록 ACK 요청 프레임을 제1 STA에게 송신할 수 있다.

[255] 보호된 블록 ACK 요청 프레임의 구성 및 이를 위하여 제1 STA과 제2 STA 간에 송신 또는 수신되는 정보 등에 대해서는 도 17의 예시에서 설명한 내용과 동일하므로, 중복되는 설명은 생략한다.

[256] 도 18의 예시에서 설명하는 방법은 도 1의 제2 디바이스(200)에 의해서 수행될 수 있다. 예를 들어, 도 1의 제2 디바이스(200)의 하나 이상의 프로세서(202)는 특정 프로토콜에 기초하여, 블록 ACK 요청 프레임에 대한 AAD를 생성하고; 및 AAD에 기초하여 보호된 블록 ACK 요청 프레임을 하나 이상의 송수신기(206)를 통하여 송신하도록 설정될 수 있다. 나아가, 제2 디바이스(200)의 하나 이상의 메모리(204)는 하나 이상의 프로세서(202)에 의해서 실행되는 경우 도 18의 예시 또는 후술하는 예시들에서 설명하는 방법을 수행하기 위한 명령들을 저장할 수 있다.

[257] 도 17 및 도 18의 예시들은 본 개시의 다양한 예시들 중의 일부에 대응할 수 있다. 이하에서는 도 17 및 도 18의 예시를 포함하는 본 개시의 다양한 예시들에 대해서 보다 구체적으로 설명한다.

[258] 실시예 1

[259] 본 실시예는 블록 ACK 요청 프레임에 대한 보호를 위한 AAD 구성 방안에 대한 것이다.

[260] 전술한 BIP, CCMP, 및 GCMP의 경우, 송신되는 프레임의 MAC 헤더(MAC header)에 포함되는 정보에 기반하여 AAD가 구성될 수 있다.

[261] 이와 관련하여, 일반 프레임의 MAC 헤더와 달리, 블록 ACK 요청 프레임의 MAC 헤더는 프레임 제어(frame control) 필드, 듀레이션(duration) 필드, RA(receiver address) 필드, 및 TA(transmitter address) 필드로 구성된다(예를 들어, 도 16 참조).

[262] 이하에서는, 전술한 블록 ACK 요청 프레임의 MAC 헤더에 기초하여, 블록 ACK 요청 프레임에 대해 BIP, CCMP, 및/또는 GCMP를 적용할 때 AAD를 구성하는 구체적인 방식들을 설명한다. 본 개시에 따른 AAD를 구성함에 있어, 이하 제안되는 방식들 중 최소한 하나의 방식 또는 하나 이상의 방식들이 사용될 수 있다.

[263] 실시예 1-1

[264] 블록 ACK 요청 프레임에 대한 보호를 위한 AAD는, 해당 블록 ACK 요청 프레임 내 BAR 제어 필드 전에 위치하는 필드들을 활용하여 구성될 수 있다.

[265] 구체적으로, AAD는 해당 블록 ACK 요청 프레임 내 프레임 제어 필드, 듀레이션 필드, RA 필드, 및/또는 TA 필드를 활용하여 구성될 수 있다.

[266] 도 19는 본 개시의 실시예에 따른 블록 ACK 요청 프레임의 보호를 위한 AAD 구성의 예시들을 나타낸다.

[267] 도 19(a)를 참조하면, AAD가 4가지 필드들, 즉, 프레임 제어 필드, 듀레이션 필드, RA 필드, 및 TA 필드를 모두 포함하여 구성되는 경우가 예시되지만, 이에 한정되지 않는다. 예를 들어, 블록 ACK 요청 프레임을 위한 AAD는 프레임 제어 필드, RA 필드, 및 TA 필드만으로 구성될 수도 있다.

[268] 이와 관련하여, 프레임 제어 필드의 경우, 하위 서브필드들의 값이 모두 AAD에 포함되거나, 특정 서브필드(들)은 0으로 변경/세팅(예를 들어, 마스크-아웃)되어 포함될 수도 있다. 일 예로, 프레임 제어 필드의 하위 서브필드는 프로토콜 버전(protocol version) 서브필드, 타입(type) 서브필드, 서브타입(subtype) 서브필드, 분산 시스템에게로(to DS) 서브필드, 분산 시스템으로부터(from DS) 서브필드, 모어 프래그먼트(more fragments) 서브필드, 재시도(retry) 서브필드, 전력 관리(power management) 서브필드, 모어 데이터(more data) 서브필드, 보호 프레임(protection frame) 서브필드, +HTC 서브필드 등을 포함할 수 있다.

[269] 실시예 1-2

[270] 블록 ACK 요청 프레임에 대한 보호를 위한 AAD는, 해당 블록 ACK 요청 프레임 내 BAR 정보 필드 전에 위치하는 필드들을 활용하여 구성될 수 있다.

[271] 구체적으로, AAD는 해당 블록 ACK 요청 프레임 내 프레임 제어 필드, 듀레이션 필드, RA 필드, 및/또는 TA 필드 뿐만 아니라, BAR 제어 필드를 추가적으로 활용하여 구성될 수 있다.

[272] 도 19(b)를 참조하면, AAD가 블록 ACK 요청 프레임 내 프레임 제어 필드 전에 위치하는 필드들을 모두 포함하여 구성되는 경우가 예시되지만, 이에 한정되지 않는다. 예를 들어, 블록 ACK 요청 프레임을 위한 AAD는 프레임 제어 필드, RA 필드, TA 필드, 및 BAR 제어 필드만으로 구성될 수도 있다.

[273] 이하에서는 블록 ACK 요청 프레임을 위한 AAD에 포함되는 BAR 제어 필드의 예시들을 설명하며, 이하의 예시들 중의 하나가 적용되거나, 또는 복수의 예시들의 조합이 적용될 수도 있다.

[274] 예를 들어, BAR 제어 필드 내의 모든 필드들의 값들이 변경 없이 AAD에 포함될 수 있다.

[275] 다른 예를 들어, BAR 제어 필드 내 일부 (서브)필드(들)의 값(들)은 변경 없이 AAD에 포함되고, 다른 특정 (서브)필드(들)의 값(들)의 전부 또는 일부 비트(들)이 0으로 변경/세팅(예를 들어, 마스크-아웃)되어 AAD에 포함될 수 있다. 0 값으로 변경/세팅될 수 있는 BAR 제어 필드 내 특정 비트/(서브)필드(들)는, 아래의 항목들 중 하나 또는 복수를 포함할 수 있다. 이하에서, BX는 X 번째 비트 위치를 의미한다.

[276] - B0 (유보된 비트)

[277] - B1 부터 B4 까지의 BAR 타입 서브필드

[278] - B5 부터 B11 까지의 (유보된 비트)

[279] - B12 부터 B15 까지의 TID_INFO 서브필드

[280] 실시예 1-3

[281] 블록 ACK 요청 프레임에 대한 보호를 위한 AAD는, 해당 블록 ACK 요청 프레임 내 BAR 제어 필드 전에 위치하는 필드들 및 BAR 정보 필드를 활용하여 구성될 수 있다. 예를 들어, 블록 ACK 요청 프레임 내 BAR 제어 필드를 제외한 모든 필드들을 기반으로 AAD가 구성될 수 있다.

[282] 구체적으로, AAD는 해당 블록 ACK 요청 프레임 내 프레임 제어 필드, 듀레이션 필드, RA 필드, 및/또는 TA 필드 뿐만 아니라, BAR 정보 필드를 추가적으로 활용하여 구성될 수 있다.

[283] 도 19(c)를 참조하면, AAD가 블록 ACK 요청 프레임 내 BAR 제어 필드 전에 위치하는 필드들, 및 BAR 정보 필드를 모두 포함하여 구성되는 경우가 예시되지만, 이에 한정되지 않는다. 예를 들어, 블록 ACK 요청 프레임을 위한 AAD는 프레임 제어 필드, RA 필드, TA 필드, 및 BAR 정보 필드만으로 구성될 수도 있다.

[284] BAR 제어 필드에 포함되는 BAR 타입 서브필드에 의해서 식별되는 다양한 블록 ACK 요청 배리언트(또는 유형)가 정의될 수 있다. 예를 들어, 확장된 압축(extended compressed) 블록 ACK 요청 배리언트, 압축(compressed) 블록 ACK 요청 배리언트, 다중 TID(traffic identifier) 블록 ACK 요청 배리언트, GCR(groupcast with retries) 블록 ACK 요청 배리언트, GLK-GCR(general link-groupcast with retries) 블록 ACK 요청 배리언트에 따라서 정의되는 블록 ACK 요청 프레임에 포함되는 서브필드들이 달라질 수 있다. 본 개시에서는 블록 ACK 요청 배리언트(또는 유형)에 따라서 블록 ACK 요청 프레임에 포함되는 서브필드들 중에서 하나 또는 복수의 서브필드들이 AAD에 포함될 수 있다.

[285] 이하에서는 본 개시에 따른 블록 ACK 요청 프레임을 위한 AAD에 포함되는 BAR 정보 필드를 구성하는 방식들을 설명하며, 이하의 방식들 중의 하나가 적용되거나, 또는 복수의 방식들의 조합이 적용될 수도 있다.

[286] (방식 1)

[287] 블록 ACK 요청 프레임 내의 BAR 정보 필드에 포함되는 모든 (서브)필드들의 값들이 변경 없이, 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[288] 압축 블록 ACK 요청 배리언트의 BAR 정보 필드에 포함되는 모든 서브필드(예를 들어, 2-옥텟의 블록 ACK 시작 시퀀스 제어(Block Ack starting sequence control) 서브필드)의 값들이 변경 없이 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[289] 확장된 압축 블록 ACK 요청 배리언트의 BAR 정보 필드에 포함되는 모든 서브필드(예를 들어, 2-옥텟의 블록 ACK 시작 시퀀스 제어 서브필드)의 값들이 변경 없이 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[290] 다중 TID 블록 ACK 요청 베리언트의 BAR 정보 필드에 포함되는 모든 서브필드(예를 들어, 각각의 TID에 대해서 반복되는 단위(하나의 단위에 포함되는 2-옥텟의 각 TID 정보(per TID info) 서브필드, 2-옥텟의 블록 ACK 시작 시퀀스 제어 서브필드))의 값들이 변경 없이 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[291] GCR 블록 ACK 요청 베리언트의 BAR 정보 필드에 포함되는 모든 서브필드(예를 들어, 2-옥텟의 블록 ACK 시작 시퀀스 제어 서브필드, 6-옥텟의 GCR 그룹 어드레스 서브필드)의 값들이 변경 없이 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[292] GLK-GCR 블록 ACK 요청 베리언트의 BAR 정보 필드에 포함되는 모든 서브필드(예를 들어, 2-옥텟의 블록 ACK 시작 시퀀스 제어 서브필드)의 값들이 변경 없이 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[293] (방식 2)

[294] 블록 ACK 요청 프레임 내의 BAR 정보 필드의 일부 (서브)필드(들)의 값(들)은 변경 없이 AAD에 포함되고, 다른 특정 (서브)필드(들)의 값(들)의 전부 또는 일부 비트(들)이 0으로 변경/세팅(예를 들어, 마스크-아웃)되어 AAD에 포함될 수 있다. 0 값으로 변경/세팅될 수 있는 BAR 정보 필드 내 특정 비트/(서브)필드(들)는, 아래의 항목들 중 하나 또는 복수를 포함할 수 있다.

[295] 압축 블록 ACK 요청 베리언트, 확장된 압축 블록 ACK 요청 베리언트, 또는 GLK-GCR 블록 ACK 요청 베리언트의 경우, BAR 정보 필드에 포함되는 블록 ACK 시작 시퀀스 제어(Block Ack starting sequence control) 서브필드 내 조각 번호(fragment number) 서브필드 및 시작 시퀀스 번호(starting sequence number) 서브필드 중 하나 이상은, 그 일부/전부 비트의 값이 0으로 변경/세팅되어 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[296] 다중 TID 블록 ACK 요청 베리언트의 경우, BAR 정보 필드에 포함되는 각각의 TID에 대해서 반복되는 단위(하나의 단위에 포함되는 2-옥텟 TID 당 정보(per TID info) 서브필드, 2-옥텟 블록 ACK 시작 시퀀스 제어 서브필드 내 조각 번호 서브필드 및 시작 시퀀스 번호 서브필드) 중 하나 이상은, 그 일부/전부 비트의 값이 0으로 변경/세팅되어 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[297] GCR 블록 ACK 요청 베리언트의 경우, BAR 정보 필드에 포함되는 2-옥텟 블록 ACK 시작 시퀀스 제어 서브필드 내 조각 번호 서브필드 및 시작 시퀀스 번호 서브필드, 6-옥텟 GCR 그룹 어드레스 서브필드 중 하나 이상은, 그 일부/전부 비트의 값이 0으로 변경/세팅되어 블록 ACK 요청 프레임을 위한 AAD에 포함될 수 있다.

[298] 실시예 1-4

[299] 본 실시예는 블록 ACK 요청 프레임에 대한 보호(예를 들어, BIP, CCMP, 또는 GCMP)의 지원 여부에 대한 시그널링 방안에 대한 것이다.

[300] 본 개시에 따른 블록 ACK 요청 프레임에 대한 보호의 적용과 관련하여, 송신 STA과 수신 STA(들)은 블록 ACK 요청 프레임에 대한 보호의 지원 여부에 대한 정보를 서로 공유할 수 있다. 해당 정보는 디스커버리 과정(예를 들어, 비콘 프레임, 프로브 응답 프레임 등) 및/또는 (재)결합 과정(예를 들어, (재)결합 요청 프레임, (재)결합 응답 프레임 등)에서 특정 요소(예를 들어, RSNXE(Extended RSN element))를 통해 공유될 수 있다.

[301] 이와 관련하여, 기존 요소(element)(예를 들어, RSNXE) 내 유보된 비트를 활용하거나, 신규 요소 내 신규 (서브)필드를 정의하여, 블록 ACK 요청 프레임에 대한 보호 적용의 지원 여부가 공유될 수 있다. 예를 들어, 1-비트의 보호된 블록 ACK 요청 지원 (서브)필드(protected BlockAck request support (sub)field)가 새롭게 정의될 수 있으며, 1 값은 블록 ACK 요청 프레임에 대한 보호 적용을 지원함을 의미/지시하고, 0 값은 블록 ACK 요청 프레임에 대한 보호 적용을 지원하지 않음을 의미/지시하도록 정의될 수 있다.

[302] 만일 송신 STA 및 수신 STA이 모두 보호를 지원하고 블록 ACK 요청 프레임에 대한 보호 적용을 지원하는 경우, 2개의 STA들은 블록 ACK 요청 프레임에 대한 보호 적용을 수행할 수도 있다. 이와 달리, 송신 STA 및 수신 STA이 보호를 지원하지만 블록 ACK 요청 프레임에 대한 보호 적용을 지원하지 않는 경우, 2개의 STA들은 블록 ACK 요청 프레임에 대한 보호 적용을 수행하지 않을 수 있다. 추가적으로, 블록 ACK 요청 프레임에 대한 보호를 적용하는 경우, 송신 STA과 수신 STA이 협상(negotiation) 과정에서 협의한 암호 스위트(cipher suite)(예를 들어, CCMP-128, CCMP-256, GCMP-128, GCMP-256, BIP-GMAC-128, BIP-GMAC-256, 또는 BIP-CMAC-256 등)가 동일하게 사용될 수 있다. 또는, 블록 ACK 요청 프레임에 대한 보호를 적용하기 위하여, 송신 STA과 수신 STA은 해당 블록 ACK 요청 프레임을 위한 추가적인/별도의 암호 스위트를 협상할 수도 있다. 또는, 송신 STA 및 수신 STA이 모두 블록 ACK 요청 프레임에 대한 보호 적용을 지원함을 명시하는 경우는 물론, 명시하지 않고 암시하는 경우(예를 들어, 보호에 관련된 정보가 구성되는 방식에 따라서 블록 ACK 요청 프레임에 대한 보호 적용이 지원됨이 간접적으로 지시되는 경우)에도, 블록 ACK 요청 프레임에 대한 보호 적용이 수행될 수도 있다. 또는, 블록 ACK 요청 프레임의 수신 STA이 다수인 경우, 그 중의 일부 STA이 블록 ACK 요청 프레임에 대한 보호 적용을 지원하지만 다른 일부 STA이 블록 ACK 요청 프레임에 대한 보호 적용을 지원하지 않는 경우에도, 송신 STA은 블록 ACK 요청 프레임에 대한 보호를 적용할 수도 있다.

[303] 추가적으로 또는 대안적으로, 기존 무선랜 시스템의 경우, 제어 프레임의 한 타입인 블록 ACK 요청 프레임에 대하여, 송신 STA 및 수신 STA은 BIP, CCMP, 또는 GCMP을 기반으로 하는 보호 동작을 수행하지 않는다. 이러한 점에서, MAC 헤더 내 프레임 제어 필드의 보호된 프레임 서브필드(protected frame subfield)는 제어 프레임의 경우 유보됨(reserved)으로 세팅된다.

[304] 이와 달리, 본 개시에서 제안하는 방법에 따라 블록 ACK 요청 프레임에 대하여 BIP, CCMP, 또는 GCMP을 적용하여 BAR 제어 필드 및/또는 BAR 정보 필드가 보호되는 경우, 해당 블록 ACK 요청 프레임의 프레임 제어 필드 내 보호된 프레임 서브필드의 값은 1로 세팅된다. 이에 기초하여, 수신 STA은 보호된 프레임 서브필드의 값을 통해 해당 블록 ACK 요청 프레임 내 BAR 제어 필드 및/또는 BAR 정보 필드가 보호되어 있음을 인지할 수 있다. 이와 관련하여, 블록 ACK 요청 프레임을 보호하는 경우, 송신 STA과 수신 STA이 협상 과정에서 협의한 암호 스위트(cipher suite)(예를 들어, CCMP-128, CCMP-256, GCMP-128, GCMP-256, BIP-GMAC-128, BIP-GMAC-256, 또는 BIP-CMAC-256 등)가 동일하게 사용될 수 있다. 또는, 블록 ACK 요청 프레임을 보호하기 위하여, 송신 STA과 수신 STA은 해당 블록 ACK 요청 프레임을 위한 추가적인/별도의 암호 스위트(예를 들어, 제어 프레임을 위한 별도의 무결성 프로토콜과 관련된 CIP(control integrity protocol)-GMAC-128, CIP-GMAC-256, CIP-CMAC-128, CIP-CMAC-256 등)를 협상할 수도 있다.

[305] 추가적으로 또는 대안적으로, 송신 STA와 수신 STA 간에, 블록 ACK 요청 프레임에 대한 보호(예를 들어, BIP, CCPM, 또는 GCMP) 적용의 지원 여부 및 BIP/CCMP/GCMP MPDU 포맷과 관련된 AAD 구성 방식(예를 들어, 도 19의 예시들)과 관련된 정보가 공유될 수 있다. 예를 들어, AAD 구성 방식과 관련된 정보는 AAD 구성을 명시적으로 지시하는 정보(예를 들어, 도 19의 예시들 중 하나를 지시하는 정보)이거나, AAD 구성을 암시적으로 지시하는 정보일 수 있다.

[306] 이와 관련하여, AAD 구성을 암시적으로 지시하는 정보는, BIP/CCMP/GCMP MPDU 포맷의 구조에 대한 정보일 수 있다. 일 예로, BIP의 경우, AAD 구성을 암시적으로 지시하는 정보는, 키 ID, PN 관련 정보, 및/또는 MIC를 포함하는 보호-관련 정보가 블록 ACK 요청 프레임 내에서 포함되는 위치에 대한 정보일 수 있다. 다른 예로, CCMP/GCMP의 경우, AAD 구성을 암시적으로 지시하는 정보는, 블록 ACK 요청 프레임 내 암호화가 적용되는 위치(예를 들어, BAR 제어 필드 및/또는 BAR 정보 필드)에 대한 정보일 수 있다.

[307] 전술한 정보의 공유를 위하여, 기존 요소(예를 들어, RSNXE) 내 유보된 비트, BAR 제어 필드 내 유보된 비트, 및/또는 신규 요소 내 신규 (서브)필드(예를 들어, 블록 ACK 요청 AAD 타입 (서브)필드(BlockAck request AAD type (sub)field) 또는 보호된 블록 ACK 요청 모드 (서브)필드)(protected BlockAck request mode (sub)field, 이하 설명의 명료성을 위해 블록 ACK 요청 AAD 타입 (서브)필드로 통칭함)가 정의될 수도 있다. 해당 (서브)필드는 (재)결합 과정 뿐만 아니라, 데이터 송수신 과정에서 송신 STA에 의해 비콘 프레임에 포함되거나, 수신 STA에 의해 데이터 프레임에 포함될 수 있다.

[308] 예를 들어, 블록 ACK 요청 AAD 타입 (서브)필드의 값이 0으로 세팅됨은, 해당 블록 ACK 요청 프레임에 대한 보호(예를 들어, BIP, CCMP, 또는 GCMP)가 적용되지 않는 것을 의미/지시할 수 있다. 이와 달리, 블록 ACK 요청 AAD 타입 (서

브)필드의 값이 1 이상으로 세팅됨은, 블록 ACK 요청 프레임에 대한 보호가 적용되는 것을 의미/지시할 수 있다.

[309] 구체적인 예로, 해당 블록 ACK 요청 AAD 타입 (서브)필드가 1 이상의 값으로 설정되는 경우, 해당 블록 ACK 요청 AAD 타입 (서브)필드의 값은 하기 표 2와 같이 정의될 수 있다. 표 1은 예시적인 것으로, 표 1에서 설명되는 값들 중 적어도 하나의 값이 적용/정의될 수 있으며, 구체적인 값은 해당 예시와 다르게 세팅/정의될 수도 있다.

[310] [표1]

블록 ACI 요청 AAD 타입 (서브)필드의 값	의미
0	블록 ACK 요청 프레임에 보호 적용되지 않음
1	실시예 1-1에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
2	실시예 1-2에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
3	실시예 1-3에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
...	...

[311] 추가적으로 또는 대안적으로, CCMP 헤더 및/또는 GCMP 헤더 내 키 ID 정보 (즉, 키 ID 옥텟) 앞 부분에 존재하는 유보된 비트(reserved bit)를 블록 ACK 요청 AAD 타입 (서브)필드로서 활용하여, 블록 ACK 요청 프레임에 대한 보호(예를 들어, CCMP, 또는 GCMP) 적용의 지원 여부 및 BIP/CCMP/GCMP MPDU 포맷과 관련된 AAD 구성 방식(예를 들어, 도 19의 예시들 참고)과 관련된 정보가 공유될 수 있다. 예를 들어, AAD 구성 방식과 관련된 정보는 AAD 구성을 명시적으로 지시하는 정보(예를 들어, 도 19의 예시들 중 하나를 지시하는 정보)이거나, AAD 구성을 암시적으로 지시하는 정보일 수 있다.

[312] 이와 관련하여, AAD 구성을 암시적으로 지시하는 정보는, CCMP/GCMP MPDU 포맷의 구조에 대한 정보일 수 있다. 일 예로, AAD 구성을 암시적으로 지시하는 정보는, 블록 ACK 요청 프레임 내 암호화가 적용되는 위치(예를 들어, BAR 제어 필드 및/또는 BAR 정보 필드)에 대한 정보일 수 있다.

[313] 여기서, 블록 ACK 요청 프레임을 암호화/복호화하는 방식은, 송신 STA과 수신 STA이 협상 과정에서 협의한 암호 스위트(cipher suite)(예를 들어, CCMP-128, CCMP-256, GCMP-128, GCMP-256, BIP-GMAC-128, BIP-GMAC-256, 또는 BIP-CMAC-256등)를 동일하게 사용하거나, 블록 ACK 요청 프레임을 위한 추가적인/별도의 암호 스위트를 협상할 수도 있다.

[314] 해당 (서브)필드는 데이터 송수신 과정에서 송신 STA에 의해 수신 STA에게 송신되는 데이터 프레임에 포함될 수 있다.

[315] 구체적인 예로, 해당 블록 ACK 요청 AAD 타입 (서브)필드가 1 이상의 값으로 설정되는 경우, 해당 블록 ACK 요청 AAD 타입 (서브)필드의 값은 하기 표 2와 같이 정의될 수 있다. 표 2는 예시적인 것으로, 표 2에서 설명되는 값들 중 적어도 하나의 값이 적용/정의될 수 있으며, 구체적인 값은 해당 예시와 다르게 세팅/정의될 수도 있다.

[316] [표2]

블록 ACK 요청 AAD 타입 (서브)필드의 값	의미
1	실시예 1-1에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
2	실시예 1-2에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
3	실시예 1-3에 기초하여 블록 ACK 요청 프레임을 위한 AAD 구성
...	...

[317] 실시예 2

[318] 본 실시예는 전술한 블록 ACK 요청 프레임에 대한 보호 적용과 관련하여, 해당 블록 ACK 요청 프레임을 위한 AAD를 구성하는 구체적인 방안에 대한 것이다.

[319] 먼저, 블록 ACK 요청 프레임에 대한 보호를 위하여 BIP를 적용하는 경우에서의 AAD 구성 방식에 대해 설명한다.

[320] 이와 관련하여, 블록 ACK 요청 프레임을 위한 AAD는 키 ID, PN(예를 들어, IPN/BIPN 등), MIC 등의 정보를 포함하는 보호 정보 (서브)필드가 블록 ACK 요청 프레임 내에서 포함되는 위치에 기초하여 구성될 수 있다.

[321] 예를 들어, 보호 정보 (서브)필드가 블록 ACK 요청 프레임의 BAR 정보 필드 내에 위치하는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-2의 방식에 기반하여 구성될 수 있다.

[322] 다른 예를 들어, 보호 정보 (서브)필드가 블록 ACK 요청 프레임의 BAR 제어 필드 내에 위치하는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-3의 방식에 기반하여 구성될 수 있다.

[323] 또 다른 예를 들어, 보호 정보 (서브)필드가 블록 ACK 요청 프레임의 BAR 제어 필드 및 BAR 정보 필드 외에 위치하는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1의 방식에 기반하여 구성될 수 있다.

[324] 전술한 예시들을 참조하면, 블록 ACK 요청 프레임을 위한 AAD는 BIP와 관련된 보호 정보 (서브)필드가 위치하는 필드 또는 보호 정보 (서브)필드 내 MIC의

계산 범위에 해당하는 필드(들)을 제외한 나머지 필드(들)에 기초하여 구성되는 것이 효율적일/바람직할 수 있다.

[325] 다음으로, 블록 ACK 요청 프레임에 대한 보호를 위하여 CCMP를 적용하는 경우에서의 AAD 구성 방식에 대해 설명한다.

[326] 이와 관련하여, 블록 ACK 요청 프레임을 위한 AAD는 BAR 제어 필드 및/또는 BAR 정보 필드의 암호화 여부에 기초하여 구성될 수 있다.

[327] 예를 들어, CCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 제어 필드 및 BAR 정보 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1의 방식에 기반하여 구성될 수 있다.

[328] 다른 예를 들어, CCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 제어 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-3의 방식에 기반하여 구성될 수 있다.

[329] 또 다른 예를 들어, CCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 정보 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-2의 방식에 기반하여 구성될 수 있다.

[330] 전술한 예시들을 참조하면, 블록 ACK 요청 프레임을 위한 AAD는 CCMP 기반의 암호화가 적용되는 필드(들)을 제외한 나머지 필드(들)에 기초하여 구성되는 것이 효율적일/바람직할 수 있다.

[331] 다음으로, 블록 ACK 요청 프레임에 대한 보호를 위하여 GCMP를 적용하는 경우에서의 AAD 구성 방식에 대해 설명한다.

[332] 이와 관련하여, 블록 ACK 요청 프레임을 위한 AAD는 BAR 제어 필드 및/또는 BAR 정보 필드의 암호화 여부에 기초하여 구성될 수 있다.

[333] 예를 들어, GCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 제어 필드 및 BAR 정보 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1의 방식에 기반하여 구성될 수 있다.

[334] 다른 예를 들어, GCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 제어 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-3의 방식에 기반하여 구성될 수 있다.

[335] 또 다른 예를 들어, GCMP 기반의 암호화가 블록 ACK 요청 프레임 내 BAR 정보 필드에 적용되는 경우, 블록 ACK 요청 프레임을 위한 AAD는 본 개시의 실시예 1-1 또는 실시예 1-2의 방식에 기반하여 구성될 수 있다.

[336] 전술한 예시들을 참조하면, 블록 ACK 요청 프레임을 위한 AAD는 GCMP 기반의 암호화가 적용되는 필드(들)을 제외한 나머지 필드(들)에 기초하여 구성되는 것이 효율적일/바람직할 수 있다.

[337] 실시예 3

[338] 본 실시예는 본 개시에서 제안하는 블록 ACK 요청 프레임 구성에 기초하여 블록 ACK 요청 프레임에 대한 보호를 수행하는 구체적인 방안에 대한 것이다.

[339] 후술하는 예시 상황들에 대하여, 모든 송신 STA 및 수신 STA(들)이 보호된 블록 Ack 지원 (서브)필드를 통해 BIP, CCMP, 또는 GCMP 상에서 블록 ACK 요청 프레임의 활용을 지원하는 경우 및/또는 보호된 블록 ACK 요청 모드 (서브)필드를 통해 블록 ACK 요청 프레임 내 BIP, CCMP/GCMP MPDU 포맷의 구성 방식을 공유하는 경우가 가정된다.

[340] 먼저, 모든 송신 STA 및 수신 STA(들)이 보호된 블록 ACK 요청 지원 (서브)필드를 통해 블록 ACK 요청 프레임에 대한 BIP 기반의 보호 적용을 지원하는 상황에서의 STA 동작을 설명한다.

[341] 예를 들어, 수신 STA은 송신 STA으로부터 수신한 블록 ACK 요청 프레임의 정보에 기반하여 해당 블록 ACK 요청 프레임을 위한 AAD를 구성할 수 있다. 이후, 수신 STA은 해당 AAD를 이용하여 해당 MPDU를 기반으로 MIC 값을 산출할 수 있다. 이때, 수신 STA은 송신 STA이 해당 MPDU를 기반으로 MIC 값을 산출할 때 수행했던 과정을 동일하게 수행하여 MIC 값을 도출할 수 있다.

[342] 이후, 수신 STA은 도출된 MIC 값과 송신 STA에 의해 송신된 MIC 값(예를 들어, 보호 정보 (서브)필드에 포함되는 MIC 정보)을 비교할 수 있다. 만일 두 개의 MIC 값이 동일하다면, 수신 STA은 획득한 MPDU의 정보를 따를 수 있다. 이와 달리, 두 개의 MIC 값이 동일하지 않다면, 수신 STA이 획득한 MPDU 내 적어도 하나의 정보가 제3의 다른 STA(예를 들어, 공격 STA)에 의해 변경되거나, 송수신 중에 손상되었음을 인지할 수 있으며, 이를 폐기(discard)할 수 있다.

[343] 다음으로, 모든 송신 STA 및 수신 STA(들)이 보호된 블록 ACK 요청 지원 (서브)필드를 통해 블록 ACK 요청 프레임에 대한 CCMP/GCMP 기반의 보호 적용을 지원하는 상황에서의 STA 동작을 설명한다.

[344] 예를 들어, 수신 STA은 송신 STA으로부터 수신한 MPDU의 MAC 헤더의 정보(예를 들어, 프레임 제어 필드, 듀레이션 필드, RA 필드, TA 필드 등)에 기초하여 블록 ACK 요청 프레임을 위한 AAD를 구성할 수 있다. 이후, 수신 STA은 해당 AAD를 사용하여, MSDU에 대한 복호화를 진행할 수 있다.

[345] 수신 STA은 블록 ACK 요청 프레임을 위해 자신이 구성한 AAD와 CCMP를 기반으로 복호화를 수행한 결과인 평문 형태의 MPDU 및 해당 MPDU를 기반으로 하는 MIC 값을 획득할 수 있다. 이때, 수신 STA은 송신 STA이 해당 MPDU를 암호화할 때 수행했던 과정을 동일하게 수행하여 MIC 값을 도출할 수 있다.

[346] 수신 STA은 도출된 MIC 값과 송신 STA에 의해 송신된 MIC 값(예를 들어, CCMP MPDU 포맷 또는 GCMP MPDU 포맷에 포함되는 MIC 정보)을 비교할 수 있다. 만일 두 개의 MIC 값이 동일하다면, 수신 STA은 획득한 평문 형태의 MPDU의 정보를 따를 수 있다. 이와 달리, 두 개의 MIC 값이 동일하지 않다면, 수신 STA이 획득한 평문 형태의 MPDU 내 적어도 하나의 정보가 제3의 다른 STA(예를 들어, 공격 STA)에 의해 변경되거나, 송수신 중에 손상되었음을 인지할 수 있으며, 이를 폐기(discard)할 수 있다.

[347] MIC 필드가 암호화되는 CCMP의 경우, 수신 STA은 MPDU에 대한 복호화를 수행하여 도출된 평문 기반으로 생성/계산된 MIC를 이용하여 무결성 검사를 수행할 수 있다. MIC 필드가 암호화되지 않는 GCMP의 경우, 수신 STA은 MPDU의 MIC 필드의 값을 이용하여 먼저 무결성 검사를 수행하고, MIC 값이 일치하는 경우에 MPDU에 대한 복호화를 수행할 수 있다.

[348] 본 개시의 실시예에 따른 블록-ACK 요청 프레임에 대한 보호를 지원/수행하는 STA의 동작은 도 20 및 도 21과 같을 수 있다.

[349] 도 20은 본 개시에 따른 블록 ACK 요청 프레임에 대한 보호를 지원하는 송신 STA의 동작을 예시한다.

[350] 도 20을 참조하면, 송신 STA은 블록 ACK 요청 프레임에 대한 보호(예를 들어, 기밀성 및 무결성 검사)를 지원하는지에 대한 정보를 포함하여 수신 STA와 공유할 수 있다(S2010).

[351] 이때, 송신 STA과 수신 STA(들)이 모두 블록 ACK 요청 프레임에 대한 보안을 적용하는 경우에, 송신 STA은 블록 ACK 요청 프레임의 기밀성 및 무결성 검사를 위해 사용되는 키(들)을 생성 및 공유할 수 있다(S2020). 이와 관련하여, 송신 STA과 수신 STA은 키 생성 과정을 통해 상호 간 동일한 키 정보를 생성/협의/공유하거나, 송신 STA에 의해 생성된 키 정보가 수신 STA에게 전달될 수도 있다.

[352] 예를 들어, 블록 ACK 요청 프레임의 무결성 검사 및/또는 암호화/복호화와 관련하여, 개별적 어드레스된 프레임(individually addressed frame)을 위한 키(들)(예를 들어, PTK 또는 BAPTK, 설명의 명료성을 위해 PTK로 통칭함) 및/또는 그룹 어드레스된 프레임(group addressed frame)을 위한 키(들)(예를 들어, GTK, IGTK, BIGTK, 또는 BAGTK, 설명의 명료성을 위해 GTK로 통칭함)이 생성 및 공유될 수 있다.

[353] 송신 STA은 수신 STA(들)에게 공유할 정보를 포함하는 블록 ACK 요청 프레임을 구성할 수 있다. 여기서, 해당 블록 ACK 요청 프레임은 평문 형태에 해당할 수 있다.

[354] 이에 기초하여, 송신 STA은 블록 ACK 요청 프레임을 위한 AAD를 구성하며, 수신 STA과 공유한 (블록 ACK 요청 프레임을 위한) 보안 키(들)에 기초하여 해당 블록 ACK 요청 프레임에 대해 보호(예를 들어, BIP, CCMP, 또는 GCMP)를 적용할 수 있다(S2030). 이와 관련하여, 송신 STA은 수신 STA와 사전에 공유된 키(들)을 사용하여 블록 ACK 요청 프레임에 대한 MIC 값을 도출할 수 있다.

[355] 송신 STA은 BIP, CCMP, 또는 GCMP 적용에 대한 결과 값/정보를 포함하는 블록 ACK 요청 프레임을 송신할 수 있다(S2140).

[356] 전술한 과정과 관련하여, 송신 STA은 송신되는 블록 ACK 요청 프레임에서의 CCMP/GCMP MPDU 포맷을 어떤 형식으로 구성하는지, 블록 ACK 요청 프레임에 대한 AAD를 어떻게 구성할 것인지 등에 대한 정보를 수신 STA과 사전에 공유/협의하거나, 블록 ACK 요청 프레임에 해당 정보를 포함하여 송신할 수도 있다.

[357] 도 21은 본 개시에 따른 블록 ACK 요청 프레임에 대한 보호를 지원하는 수신 STA의 동작을 예시한다.

[358] 도 21을 참조하면, 수신 STA은 블록 ACK 요청 프레임에 대한 보호(예를 들어, 기밀성 및 무결성 검사)를 지원하는지에 대한 정보를 포함하여 송신 STA에게 공유할 수 있다(S2110).

[359] 이때, 송신 STA과 블록 ACK 요청 프레임의 보호(예를 들어, 기밀성 및 무결성 검사)를 위해 사용되는 키(들)을 공유하는 경우, 수신 STA은 송신 STA에 의해 송신된 블록 ACK 요청 프레임에 보호 방식이 적용되었음을 가정할 수 있다(S2120).

[360] 이와 관련하여, 송신 STA과 수신 STA은 키 생성 과정을 통해 상호 간 동일한 키 정보(예를 들어, PTK/GTK 등)를 생성/협의/공유하거나, 송신 STA에 의해 생성된 키 정보가 수신 STA에게 전달될 수도 있다.

[361] 예를 들어, 수신 STA은 송신 STA으로부터 송신된 블록 ACK 요청 프레임을 수신하여, 사전에 공유된 키(들), 블록 ACK 요청 프레임 내 무결성 검사를 위한 정보의 구성 방식에 관련된 정보, CCMP/GCMP MPDU 포맷의 구성 방식, 및/또는 블록 ACK 요청 프레임에 대한 AAD의 구성 방식에 대한 정보를 기반으로 해당 블록 ACK 요청 프레임에 보호가 적용되었음을 인지할 수 있다.

[362] 블록 ACK 요청 프레임을 수신하였을 때, 수신 STA은 해당 블록 ACK 요청 프레임에 기초하여 블록 ACK 요청 프레임을 위한 AAD를 구성할 수 있다. 해당 AAD는 복호화 및 무결성 검사를 위해 활용될 수 있다. 이후, 수신 STA은 구성된 AAD 및 (사전에) 공유/생성/협의된 키(들)(예를 들어, PTK/GTK 등) 등을 사용하여 해당 블록 ACK 요청 프레임에 대한 복호화 및/또는 무결성 검사를 수행할 수 있다(S2130).

[363] 이후, 수신 STA은 복호화한 블록 ACK 요청 프레임을 기반으로 도출한 MIC 값과 송신 STA에 의해 송신된 MIC 값(예를 들어, 블록 ACK 요청 프레임 내에 포함되는 MIC 정보/값) 간의 비교를 통해, 무결성 검사를 수행할 수 있다(S2140).

[364] 기존의 무선랜 시스템에서 활용되는 BIP/CCMP/GCMP 등의 프로토콜은 블록 ACK 프레임과 같은 제어 프레임에 대한 보호를 제공할 수 없다. 본 개시에서는 블록 ACK 프레임과 같은 제어 프레임에 대해서 BIP/CCMP/GCMP 등의 프로토콜이 적용되는 경우 보호된 제어 프레임의 송신 또는 수신에 이용되는 AAD를 구성하는 새로운 방안을 제공할 수 있다.

[365] 이상에서 설명된 실시예들은 본 개시의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 개시의 실시예를 구성하는 것도 가능하다. 본 개시의 실시예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과

교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.

[366] 본 개시는 본 개시의 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다. 따라서, 상술한 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니 되고 예시적인 것으로 고려되어야 한다. 본 개시의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 개시의 등가적 범위 내에서의 모든 변경은 본 개시의 범위에 포함된다.

[367] 본 개시의 범위는 다양한 실시예의 방법에 따른 동작이 장치 또는 컴퓨터 상에서 실행되도록 하는 소프트웨어 또는 머신-실행가능한 명령들(예를 들어, 운영체제, 애플리케이션, 펌웨어(firmware), 프로그램 등), 및 이러한 소프트웨어 또는 명령 등이 저장되어 장치 또는 컴퓨터 상에서 실행 가능한 비-일시적 컴퓨터-판독가능 매체(non-transitory computer-readable medium)를 포함한다. 본 개시에서 설명하는 특징을 수행하는 프로세싱 시스템을 프로그래밍하기 위해 사용될 수 있는 명령은 저장 매체 또는 컴퓨터 판독가능 저장 매체 상에/내에 저장될 수 있고, 이러한 저장 매체를 포함하는 컴퓨터 프로그램 제품을 이용하여 본 개시에서 설명하는 특징이 구현될 수 있다. 저장 매체는 DRAM, SRAM, DDR RAM 또는 다른 랜덤 액세스 솔리드 스테이트 메모리 디바이스와 같은 고속 랜덤 액세스 메모리를 포함할 수 있지만, 이에 제한되지 않으며, 하나 이상의 자기 디스크 저장 디바이스, 광 디스크 저장 장치, 플래시 메모리 디바이스 또는 다른 비-휘발성 솔리드 스테이트 저장 디바이스와 같은 비-휘발성 메모리를 포함할 수 있다. 메모리는 선택적으로 프로세서(들)로부터 원격에 위치한 하나 이상의 저장 디바이스를 포함한다. 메모리 또는 대안적으로 메모리 내의 비-휘발성 메모리 디바이스(들)는 비-일시적 컴퓨터 판독가능 저장 매체를 포함한다. 본 개시에서 설명하는 특징은, 머신 판독가능 매체 중 임의의 하나에 저장되어 프로세싱 시스템의 하드웨어를 제어할 수 있고, 프로세싱 시스템이 본 개시의 실시예에 따른 결과를 활용하는 다른 메커니즘과 상호작용하도록 하는 소프트웨어 및/또는 펌웨어에 통합될 수 있다. 이러한 소프트웨어 또는 펌웨어는 애플리케이션 코드, 디바이스 드라이버, 운영 체제 및 실행 환경/컨테이너를 포함할 수 있지만 이에 제한되지 않는다.

산업상 이용가능성

[368] 본 개시에서 제안하는 방법은 IEEE 802.11 기반 시스템에 적용되는 예를 중심으로 설명하였으나, IEEE 802.11 기반 시스템 이외에도 다양한 무선랜 또는 무선통신 시스템에 적용하는 것이 가능하다.

청구범위

[청구항 1] 제1 스테이션(STA)에 의해서, 특정 프로토콜에 기초하여 보호된 블록 ACK(acknowledgement) 요청 프레임을 제2 STA으로부터 수신하는 단계;
상기 제1 STA에 의해서, 상기 블록 ACK 요청 프레임에 기초하여 AAD(additional authentication data)를 생성하는 단계; 및
상기 제1 STA에 의해서, 상기 AAD에 기초하여 상기 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행하는 단계를 포함하고,
상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하는, 방법.

[청구항 2] 제1항에 있어서,
상기 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상은 상기 블록 ACK 요청 프레임에 대한 보호와 관련된 키 정보 및 상기 AAD에 기초하여 수행되는, 방법.

[청구항 3] 제1항에 있어서,
상기 특정 프로토콜이 무결성 프로토콜임에 기초하여,
상기 AAD는, 상기 MAC 헤더, 상기 블록 ACK 요청 제어 필드, 및 상기 블록 ACK 요청 정보 필드 중에서, 보호 정보 필드가 위치하는 필드를 제외한 나머지 필드 중의 하나 이상의 서브필드에 기초하여 구성되는, 방법.

[청구항 4] 제3항에 있어서,
상기 보호 정보 필드는, 키 ID(identifier), 패킷 번호(PN), 또는 MIC(message integrity code) 중의 하나 이상을 포함하는, 방법.

[청구항 5] 제1항에 있어서,
상기 특정 프로토콜이 암호화 프로토콜임에 기초하여:
상기 AAD는 상기 블록 ACK 요청 제어 필드 또는 상기 블록 ACK 요청 정보 필드 중의 하나 이상에 대한 암호화 적용 여부에 기반하여 구성되는, 방법.

[청구항 6] 제5항에 있어서,
상기 블록 ACK 요청 제어 필드 및 상기 블록 ACK 요청 정보 필드에 암호화가 적용됨에 기초하여, 상기 AAD는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 구성되는, 방법.

[청구항 7] 제5항에 있어서,
상기 블록 ACK 요청 제어 필드에 암호화가 적용됨에 기초하여, 상기 AAD는, 상기 MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여

구성되거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드 및 상기 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하여 구성되는, 방법.

[청구항 8] 제5항에 있어서,
상기 블록 ACK 요청 정보 필드에 암호화가 적용됨에 기초하여, 상기 AAD는, 상기 MAC 헤더에 포함되는 하나 이상의 서브필드에 기초하여 구성되거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드 및 상기 블록 ACK 제어 필드에 포함되는 하나 이상의 서브필드에 기초하여 구성되는, 방법.

[청구항 9] 제1항에 있어서,
상기 MAC 헤더, 상기 블록 ACK 요청 제어 필드, 또는 상기 블록 ACK 요청 정보 필드 중의 하나 이상의 각각에 포함되는 하나 이상의 서브필드는, 상기 AAD에 동일하게 포함되는, 방법.

[청구항 10] 제1항에 있어서,
상기 MAC 헤더, 상기 블록 ACK 요청 제어 필드, 또는 상기 블록 ACK 요청 정보 필드 중의 하나 이상의 각각에 포함되는 하나 이상의 서브필드 중, 특정 하나 이상의 서브필드의 일부 또는 전부 비트 값이 0으로 세팅되어 상기 AAD에 포함되는, 방법.

[청구항 11] 제1항에 있어서,
상기 MAC 헤더에 포함되는 하나 이상의 서브필드는, 프레임 제어 서브필드, 듀레이션 서브필드, 수신자 어드레스(RA) 서브필드, 또는 송신자 어드레스(TA) 서브필드 중의 하나 이상을 포함하는, 방법.

[청구항 12] 제1항에 있어서,
상기 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 서브필드는, 블록 ACK 요청 타입 서브필드, TID_INFO 서브필드, 또는 비트 위치 0(B0) 및 B5-B11 중의 하나 이상의 비트 위치에 대응하는 하나 이상의 서브필드 중의 하나 이상을 포함하는, 방법.

[청구항 13] 제1항에 있어서,
상기 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드는:
압축 블록 ACK 요청 배리언트, 확장된 압축 블록 ACK 요청 배리언트, 또는 GLK-GCR(general link-groupcast with retries) 블록 ACK 요청 배리언트에 관련되는, 블록 ACK 시작 시퀀스 제어(Block Ack starting sequence control) 서브필드;
다중 TID(traffic identifier) 블록 ACK 요청 배리언트에 관련되는, 각 TID 정보(per TID info) 서브필드, 블록 ACK 시작 시퀀스 제어 서브필드;
GCR 블록 ACK 요청 배리언트에 관련되는, 블록 ACK 시작 시퀀스 제어 서브필드, GCR 그룹 어드레스 서브필드
중의 하나 이상을 포함하는, 방법.

[청구항 14] 제1항에 있어서,
상기 제1 STA와 상기제 2 STA 간에, 상기 블록 ACK 요청 프레임에 대한 보호의 지원 여부, 상기 보호된 블록 ACK 요청 프레임의 MPDU(MAC protocol data unit) 포맷, 또는 블록 ACK 요청 AAD 타입 중의 하나 이상에 대한 정보가 교환되는, 방법.

[청구항 15] 제14항에 있어서,
상기 정보는,
비콘 프레임, 프로브 요청 프레임, 프로브 응답 프레임, 결합 요청 프레임, 결합 응답 프레임, 재-결합 요청 프레임, 재-결합 응답 프레임 중의 하나 이상에 포함되거나, 또는
상기 특정 프로토콜이 무결성 프로토콜임에 기초하여, 상기 블록 ACK 요청 제어 필드에 포함되거나, 또는
상기 특정 프로토콜이 암호화 프로토콜이고, 암호화에서 상기 블록 ACK 요청 제어 필드가 제외됨에 기초하여, 상기 블록 ACK 요청 제어 필드에 포함되거나, 또는
상기 특정 프로토콜이 암호화 프로토콜임에 기초하여, 상기 블록 ACK 요청 프레임 내 암호화 프로토콜 헤더에 포함되는, 방법.

[청구항 16] 제14항에 있어서,
상기 블록 ACK 요청 AAD 타입은:
상기 MAC 헤더에 포함되는 하나 이상의 필드에 기초하여 구성되는 제1 타입;
상기 MAC 헤더에 포함되는 하나 이상의 필드 및 상기 블록 ACK 요청 제어 필드에 포함되는 하나 이상의 필드에 기초하여 구성되는 제2 타입; 또는
상기 MAC 헤더에 포함되는 하나 이상의 필드 및 상기 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 필드에 기초하여 구성되는 제3 타입
중의 하나를 지시하는, 방법.

[청구항 17] 제1항에 있어서,
상기 블록 ACK 요청 프레임에 대해 상기 특정 프로토콜이 적용됨에 기초하여, 상기 MAC 헤더의 프레임 제어(frame control) 서브필드 내 보호된 프레임(protected frame) 서브필드는 미리 정의된 특정 값으로 세팅되는, 방법.

[청구항 18] 제1항에 있어서,
상기 블록 ACK 요청 프레임은 상기 제2 STA에 의해 수신될 데이터에 대한 블록 ACK의 요청과 관련된 정보를 포함하고,
상기 블록 ACK 요청 프레임에 대한 보호와 관련된 키 정보는, 상기 데이터에 대한 보호를 위한 키 정보와 구별되는, 방법.

[청구항 19] 하나 이상의 송수신기; 및

상기 하나 이상의 송수신기와 연결된 하나 이상의 프로세서를 포함하고,
상기 하나 이상의 프로세서는:
특정 프로토콜에 기초하여 보호된 블록 ACK(acknowledgement) 요청 프레임을 상기 하나 이상의 송수신기를 통하여 수신하고;
상기 블록 ACK 요청 프레임에 기초하여 AAD(additional authentication data)를 생성하고; 및
상기 AAD에 기초하여 상기 블록 ACK 요청 프레임에 대한 복호화 또는 무결성 검사 중의 하나 이상을 수행하도록 설정되며,
상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드, 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하는, 장치.

[청구항 20] 제2 스테이션(STA)에 의해서, 특정 프로토콜에 기초하여 블록 ACK(acknowledgement) 요청 프레임에 대한 AAD(additional authentication data)를 생성하는 단계; 및
상기 제2 STA에 의해서, 상기 AAD에 기초하여 보호된 블록 ACK 요청 프레임을 제1 STA에게 송신하는 단계를 포함하고,
상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드, 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하는, 방법.

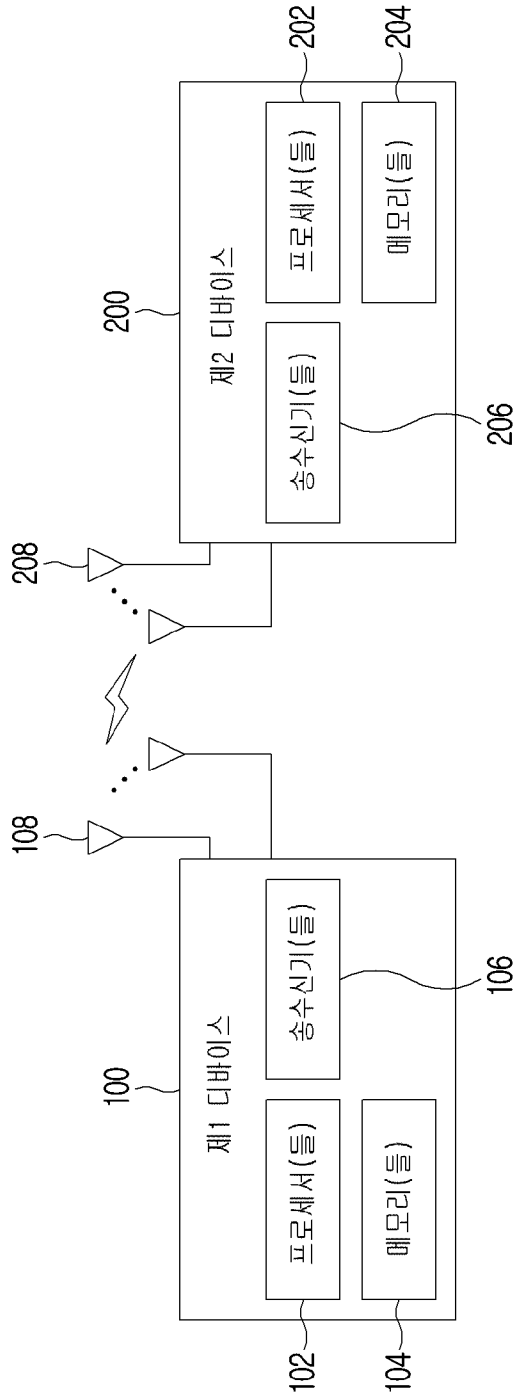
[청구항 21] 하나 이상의 송수신기; 및
상기 하나 이상의 송수신기와 연결된 하나 이상의 프로세서를 포함하고,
상기 하나 이상의 프로세서는:
특정 프로토콜에 기초하여, 블록 ACK(acknowledgement) 요청 프레임에 대한 AAD(additional authentication data)를 생성하고; 및
상기 AAD에 기초하여 보호된 블록 ACK 요청 프레임을, 상기 하나 이상의 송수신기를 통하여 송신하도록 설정되며,
상기 AAD는, 상기 블록 ACK 요청 프레임의 MAC(medium access control) 헤더에 포함되는 하나 이상의 필드에 기초하거나, 또는 상기 MAC 헤더에 포함되는 하나 이상의 서브필드, 및 상기 블록 ACK 요청 프레임의 블록 ACK 요청 제어 필드 또는 블록 ACK 요청 정보 필드에 포함되는 하나 이상의 서브필드에 기초하는, 장치.

[청구항 22] 하나 이상의 프로세서; 및
상기 하나 이상의 프로세서에 동작 가능하게 연결되고, 상기 하나 이상의 프로세서에 의해 실행됨에 기반하여, 제1항 내지 제18항 중 어느 한 항에

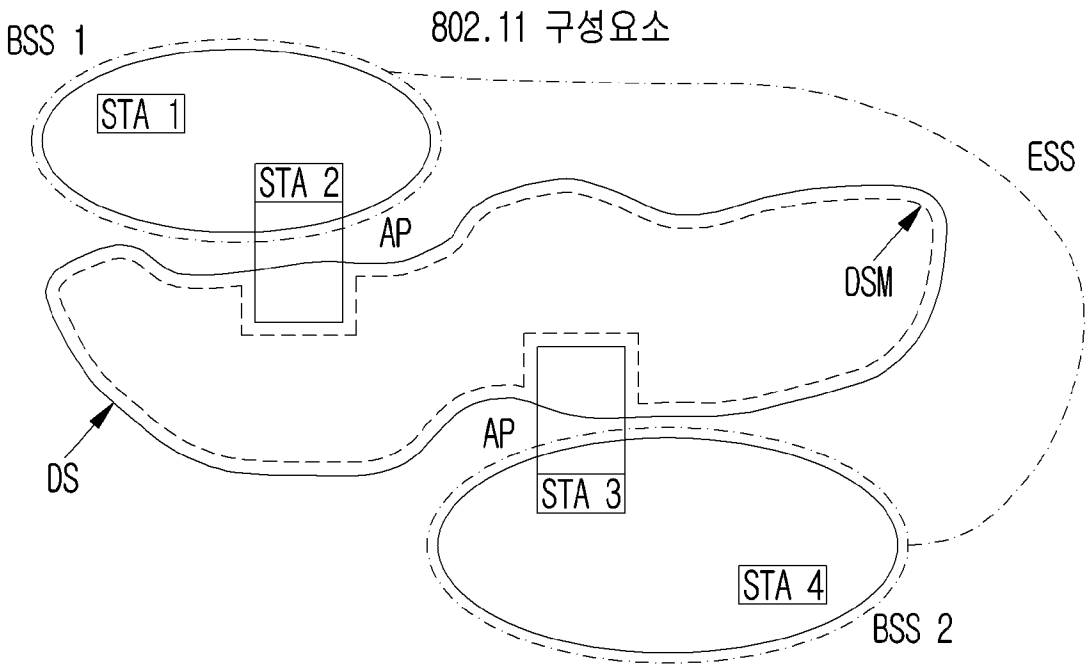
따른 방법을 수행하기 위한 명령들을 저장하는 하나 이상의 컴퓨터 메모리를 포함하는, 프로세싱 장치.

[청구항 23] 하나 이상의 프로세서에 의해서 실행되어 제1항 내지 제18항 중 어느 한 항에 따른 방법을 수행하도록 제어하는 하나 이상의 명령을 저장하는 하나 이상의 비-일시적(non-transitory) 컴퓨터 판독가능 매체.

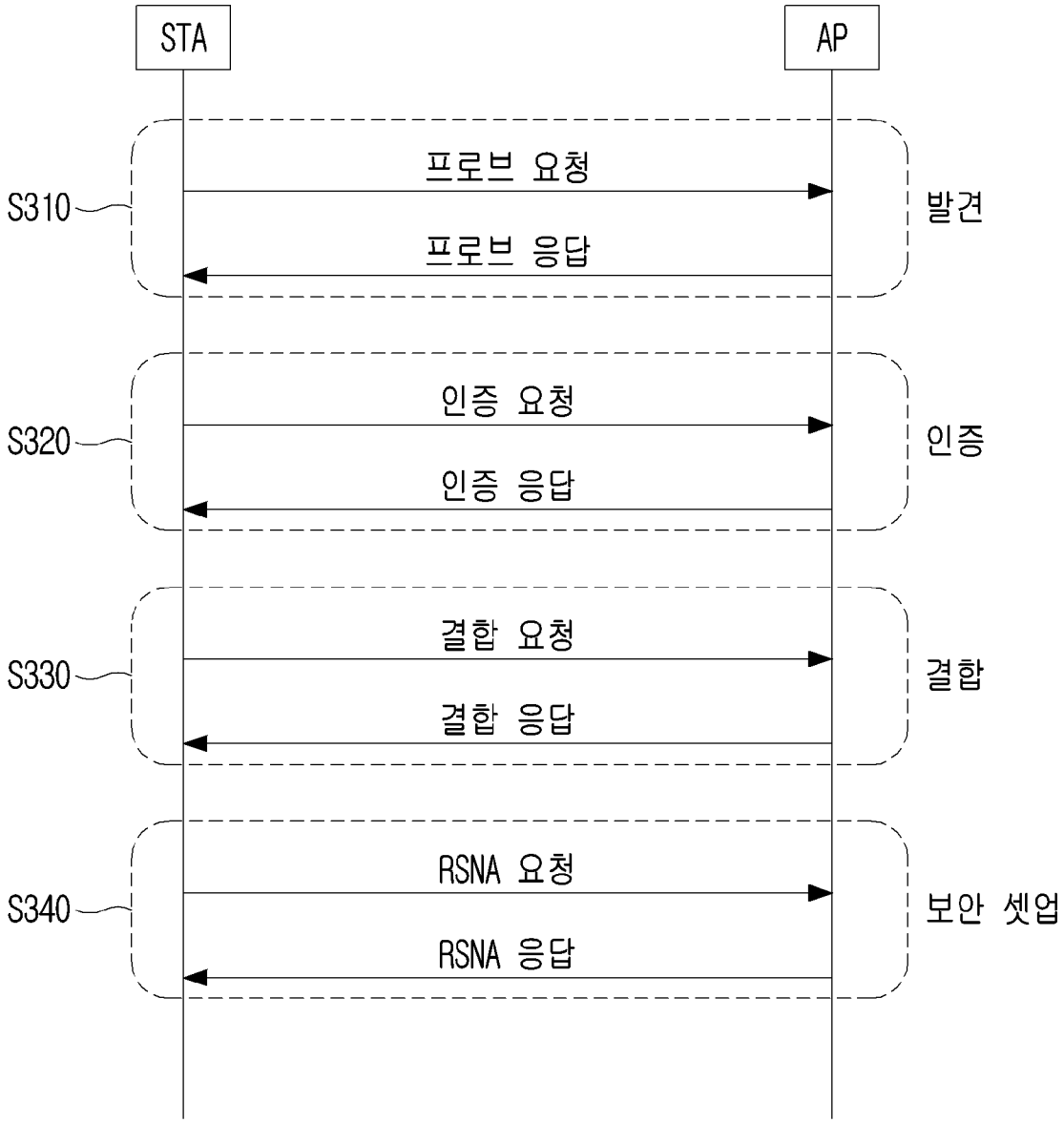
[도1]


202
204
200
제2 디바이스
프로세서(들)
메모리(들)
송수신기(들)
206
208
108
100
제1 디바이스
송수신기(들)
106
프로세서(들)
메모리(들)
102
104

[도2]



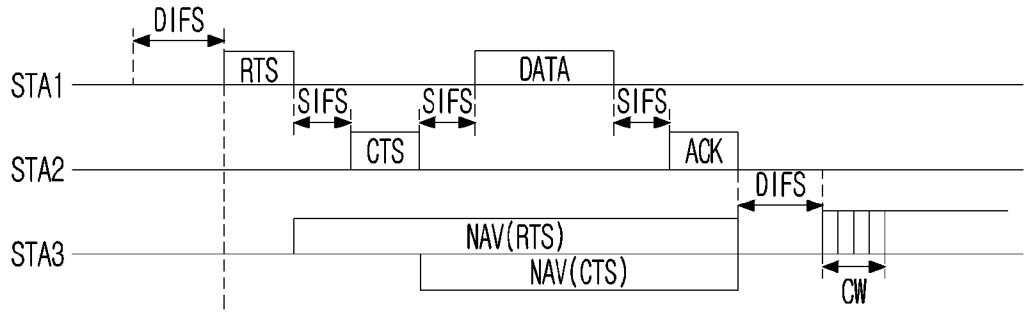
[도3]


STA
AP
S310
프로브 요청
프로브 응답
발견
S320
인증 요청
인증 응답
인증
S330
결합 요청
결합 응답
결합
S340
RSNA 요청
RSNA 응답
보안 셋업

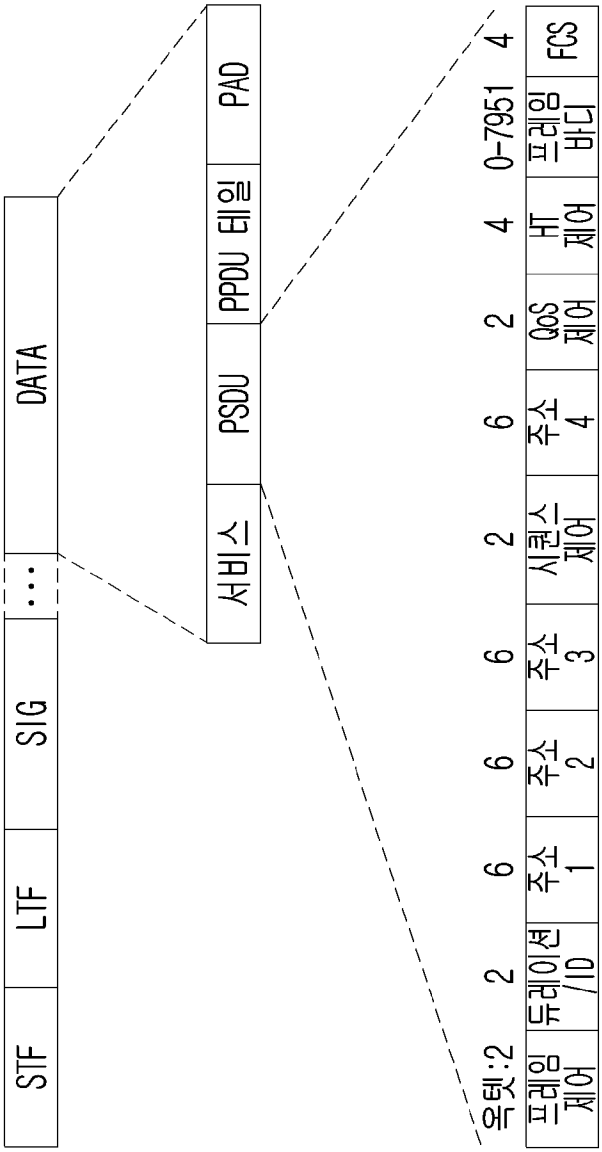
[도4]


DIFS
station1
station2
station3
station4
station5
busy
t
busy 점유된 매체
MAC에서 패킷 도착
경과된 백오프 시간
잔여 백오프 시간

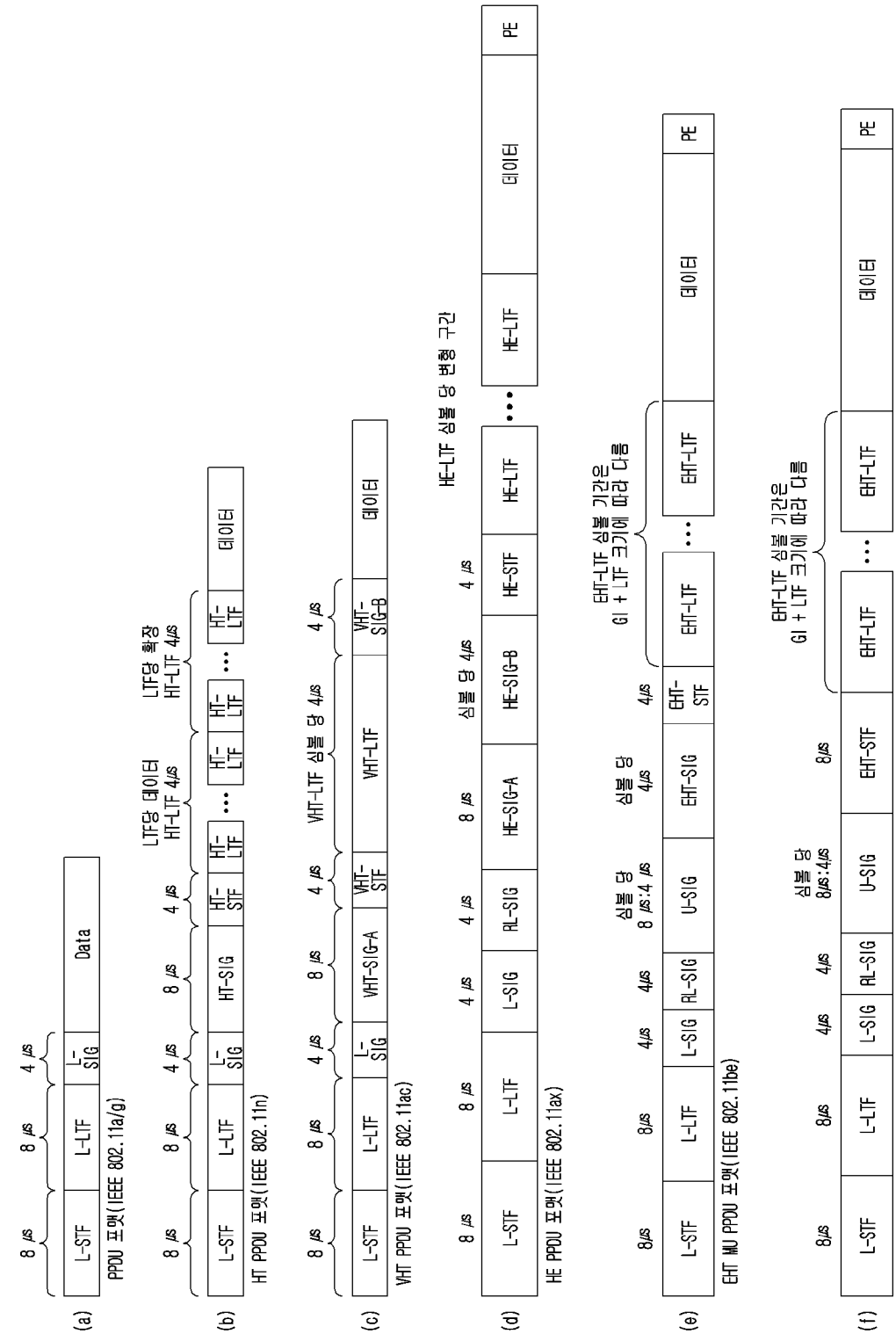
[도5]


DIFS
STA1
STA2
STA3
RTS
SIFS
CTS
DATA
ACK
NAV(RTS)
NAV(CTS)
CW

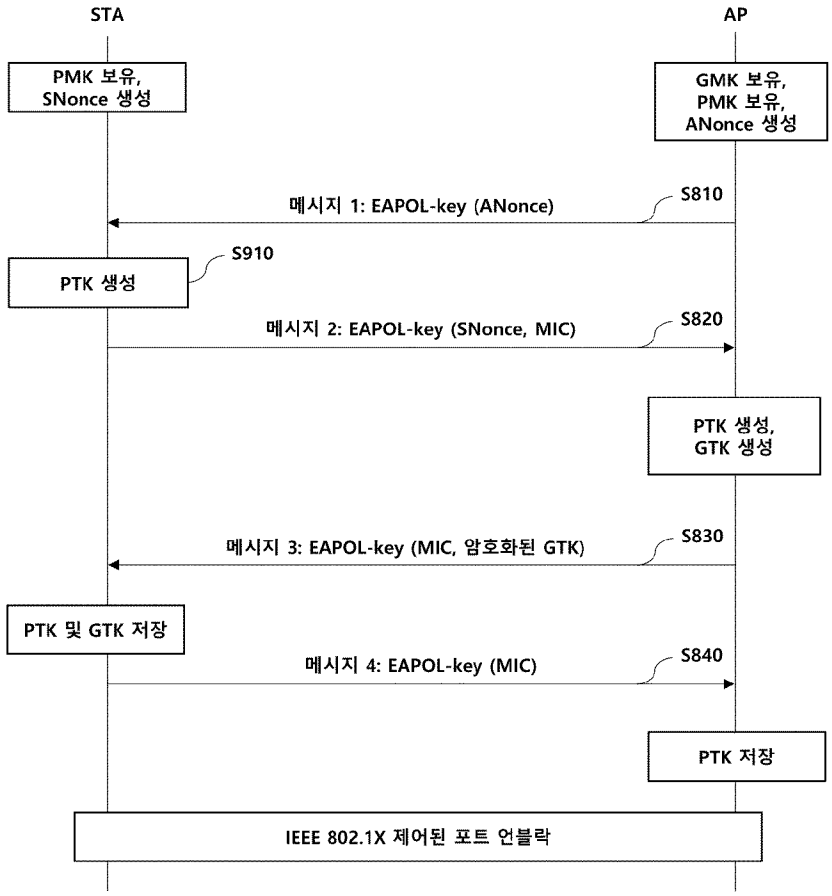
[도6]


STF
LTF
SIG
...
DATA
서비스
PSDU
PPDU 테일
PAD
옥텟:2
2
6
6
6
6
2
6
2
4
0-7951
4
프레임 제어
듀레이션 /ID
주소 1
주소 2
주소 3
시퀀스 제어
주소 4
QoS 제어
HT 제어
프레임 바디
FCS

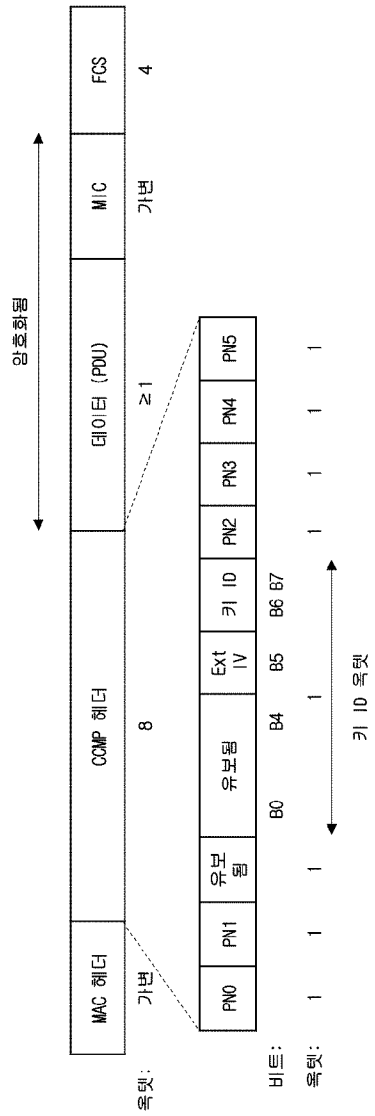
[도7]


(a)
8 μs
8 μs
4 μs
L-STF
L-LTF
L-SIG
Data
PPDU 포맷(IEEE 802.11a/g)
(b)
LTF당 데이터 HT-LTF 4μs
LTF당 확장 HT-LTF 4μs
L-STF
L-LTF
L-SIG
HT-SIG
HT-STF
HT-LTF
HT-LTF
데이터
HT PPDU 포맷(IEEE 802.11n)
(c)
VHT-LTF 심볼 당 4μs
L-STF
L-LTF
L-SIG
VHT-SIG-A
VHT-STF
VHT-LTF
VHT-SIG-B
데이터
VHT PPDU 포맷(IEEE 802.11ac)
(d)
HE-LTF 심볼 당 변형 구간
심볼 당 4μs
L-STF
L-LTF
L-SIG
RL-SIG
HE-SIG-A
HE-SIG-B
HE-STF
HE-LTF
HE-LTF
데이터
PE
HE PPDU 포맷(IEEE 802.11ax)
(e)
심볼 당 8 μs:4 μs
심볼 당 4μs
EHT-LTF 심볼 기간은 GI + LTF 크기에 따라 다름
L-STF
L-LTF
L-SIG
RL-SIG
U-SIG
EHT-SIG
EHT-STF
EHT-LTF
EHT-LTF
데이터
PE
EHT MU PPDU 포맷(IEEE 802.11be)
(f)
심볼 당 8μs:4μs
EHT-LTF 심볼 기간은 GI + LTF 크기에 따라 다름
L-STF
L-LTF
L-SIG
RL-SIG
U-SIG
EHT-STF
EHT-LTF
EHT-LTF
데이터
PE
EHT TB PPDU 포맷(IEEE 802.11be)

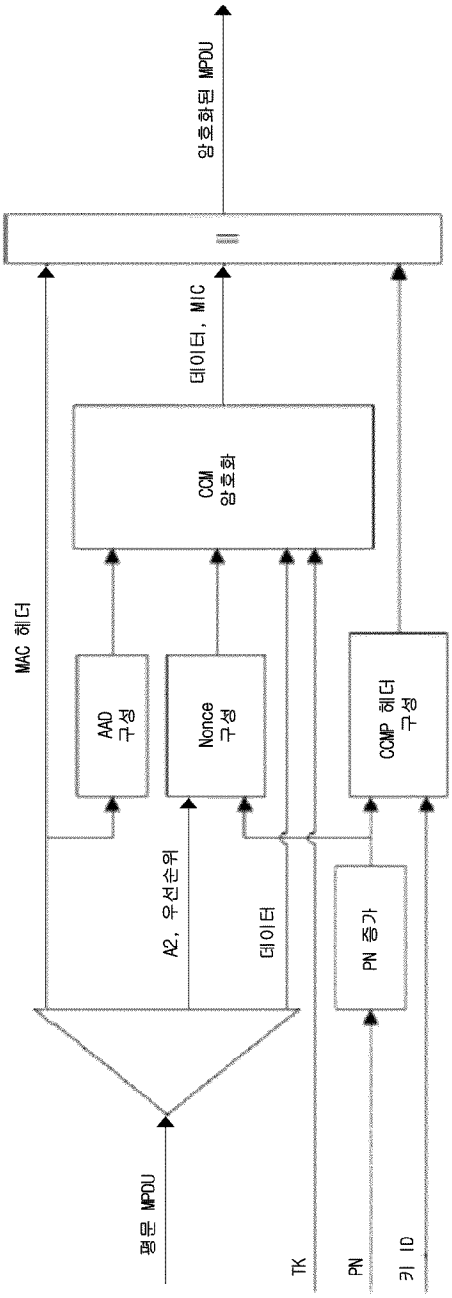
[도8]


STA
AP
PMK 보유,
SNonce 생성
GMK 보유,
PMK 보유,
ANonce 생성
메시지 1: EAPOL-key (ANonce)
S810
S910
PTK 생성
메시지 2: EAPOL-key (SNonce, MIC)
S820
PTK 생성,
GTK 생성
메시지 3: EAPOL-key (MIC, 암호화된 GTK)
S830
PTK 및 GTK 저장
메시지 4: EAPOL-key (MIC)
S840
PTK 저장
IEEE 802.1X 제어된 포트 언블락

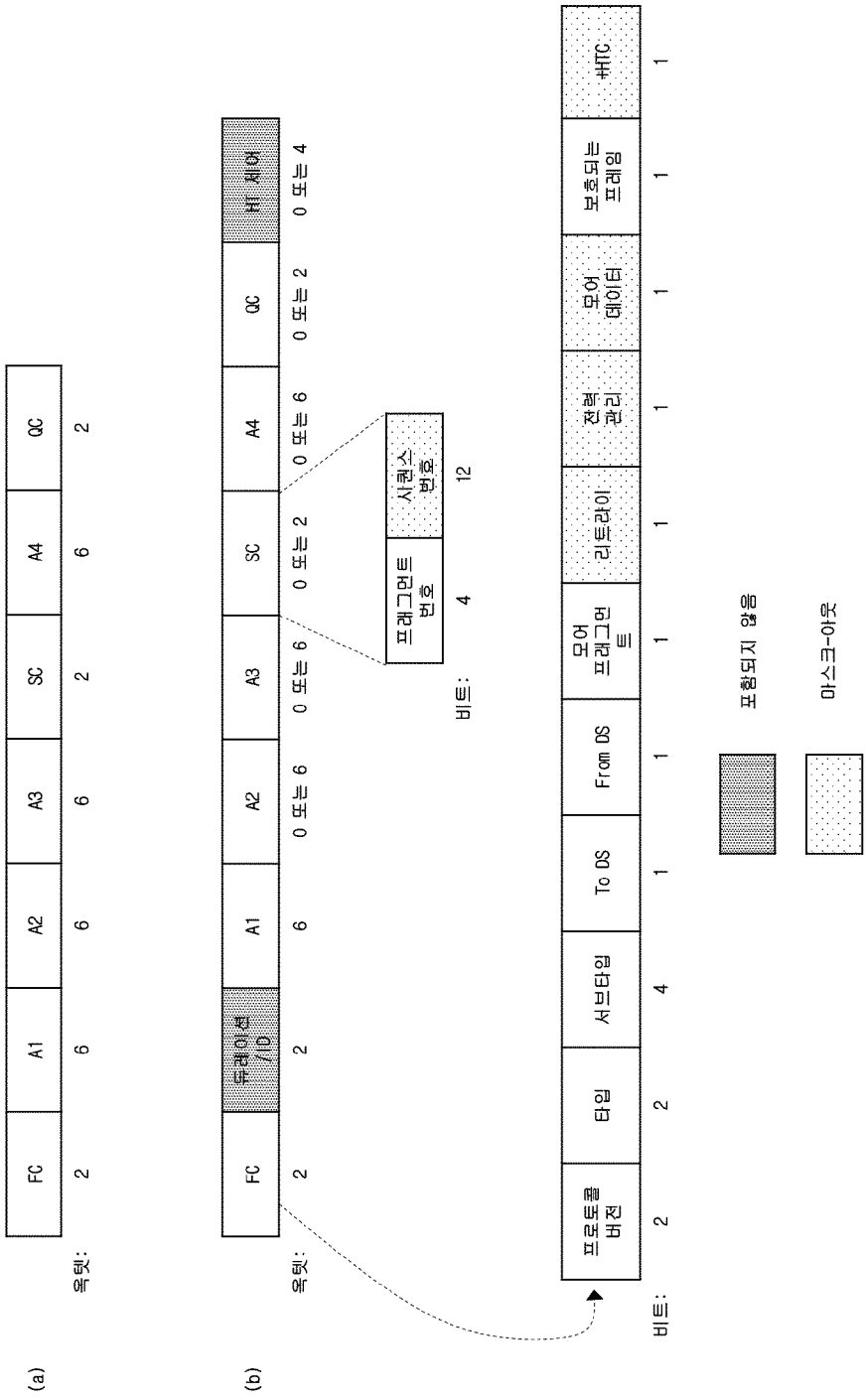
[도9]


암호화됨
MAC 헤더
COMP 헤더
데이터 (PDU)
MIC
FCS
옥텟:
가변
8
≥1
가변
4
PN0
PN1
유보됨
유보됨
Ext IV
키 ID
PN2
PN3
PN4
PN5
비트:
B0
B4
B5
B6 B7
옥텟:
1
1
1
1
1
1
1
1
키 ID 옥텟

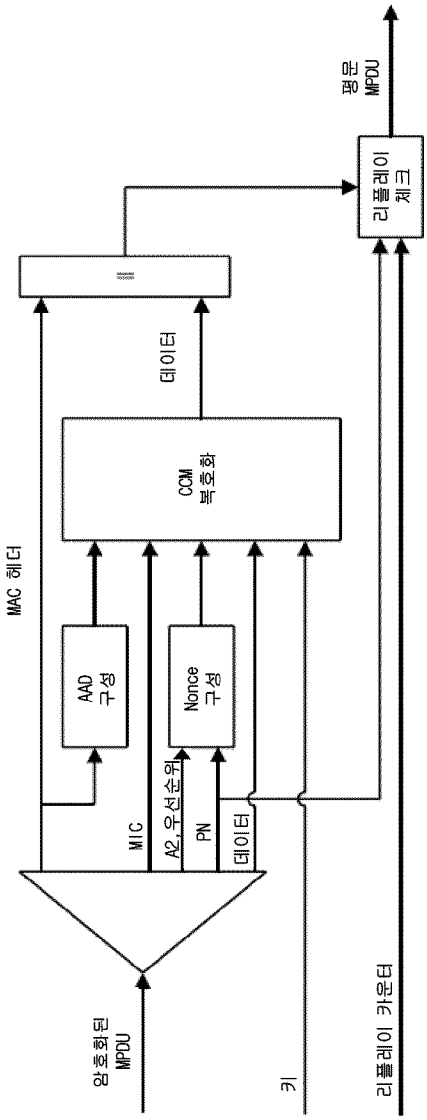
[도10]


암호화된 MPDU
데이터, MIC
CCM 암호화
MAC 헤더
AAD 구성
Nonce 구성
CCMP 헤더 구성
A2, 우선순위
데이터
PN 증가
평문 MPDU
TK
PN
키 ID

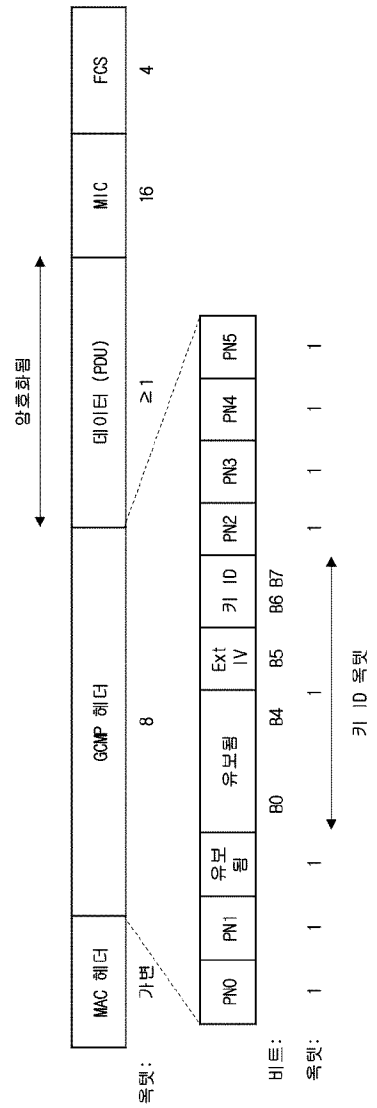
[도11]


(a)
옥텟:
FC
A1
A2
A3
SC
A4
QC
2
6
6
6
2
6
2
(b)
옥텟:
FC
듀레이션 /ID
A1
A2
A3
SC
A4
QC
HT 제어
2
2
6
6
6
2
6
2
0 또는 2
0 또는 6
0 또는 2
0 또는 4
프래그먼트 번호
시퀀스 번호
비트:
4
12
비트:
프로토콜 버전
타입
서브타입
To DS
From DS
모어 프래그먼트
리트라이
전력 관리
모어 데이터
보호되는 프레임
+HTC
2
2
4
1
1
1
1
1
1
1
1
포함되지 않음
마스크-아웃

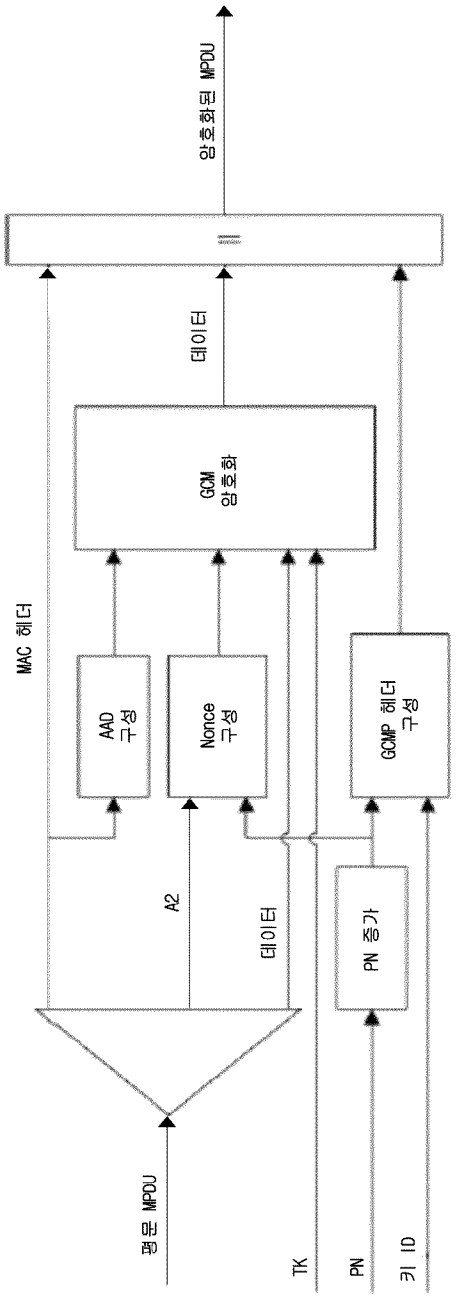
[도12]


평문 MPDU
리플레이 체크
데이터
CCM 복호화
MAC 헤더
AAD 구성
Nonce 구성
MIC
A2, 우선순위
PN
데이터
암호화된 MPDU
키
리플레이 카운터

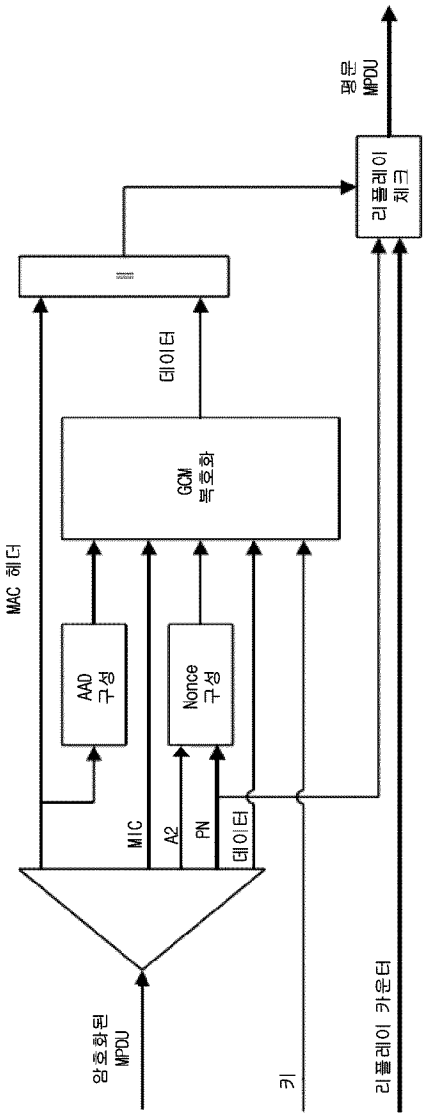
[도13]


MAC 헤더
GCMP 헤더
데이터 (PDU)
MIC
FCS
암호화됨
옥텟:
가변
8
≥1
16
4
PN0
PN1
유보됨
유보됨
Ext IV
키 ID
PN2
PN3
PN4
PN5
비트:
B0
B4
B5
B6 B7
옥텟:
1
1
1
1
1
1
1
1
1
1
키 ID 옥텟

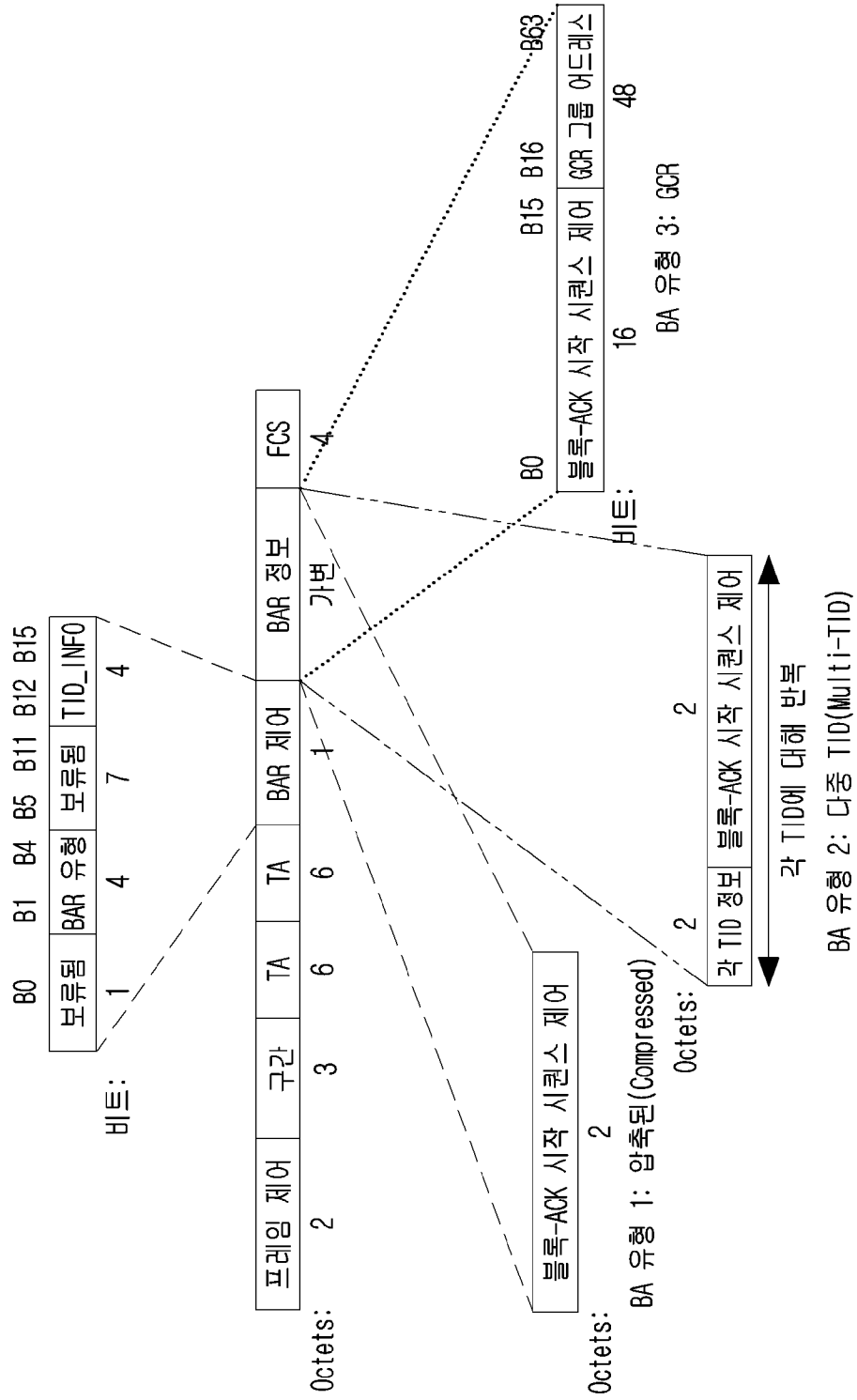
[도14]


암호화된 MPDU
데이터
GCM 암호화
MAC 헤더
AAD 구성
Nonce 구성
GCMP 헤더 구성
A2
데이터
PN 증가
평문 MPDU
TK
PN
키 ID

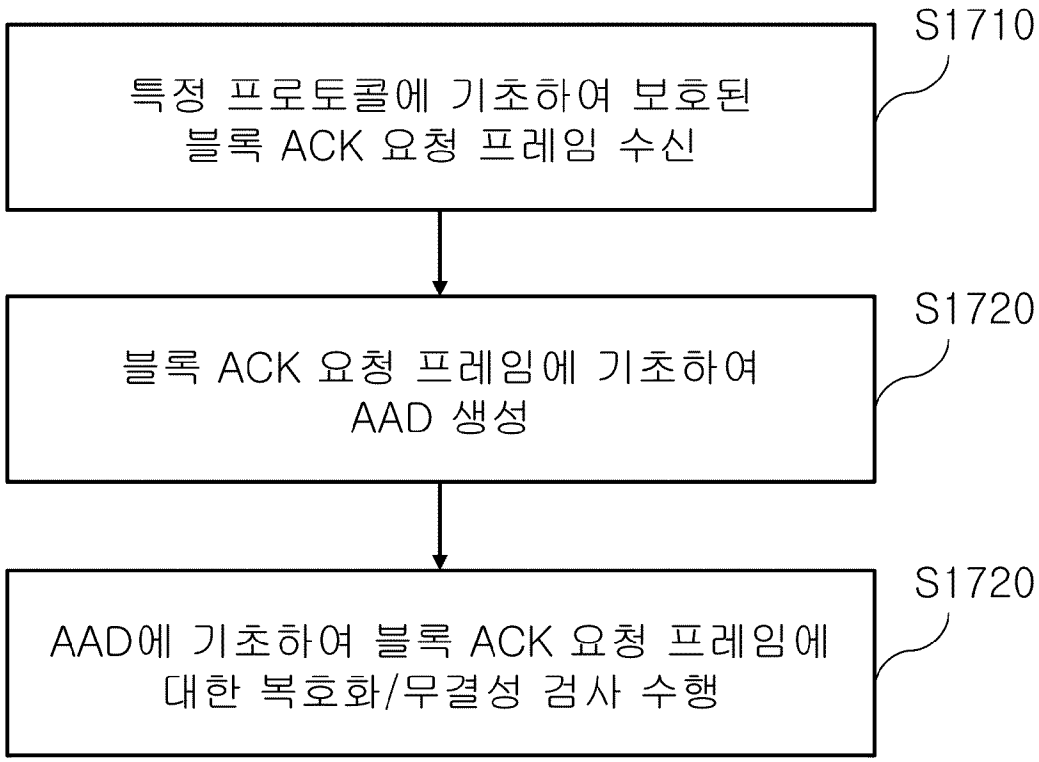
[도15]


평문 MPDU
리플레이 체크
데이터
GCM 복호화
MAC 헤더
AAD 구성
Nonce 구성
MIC
A2
PN
데이터
암호화된 MPDU
키
리플레이 카운터

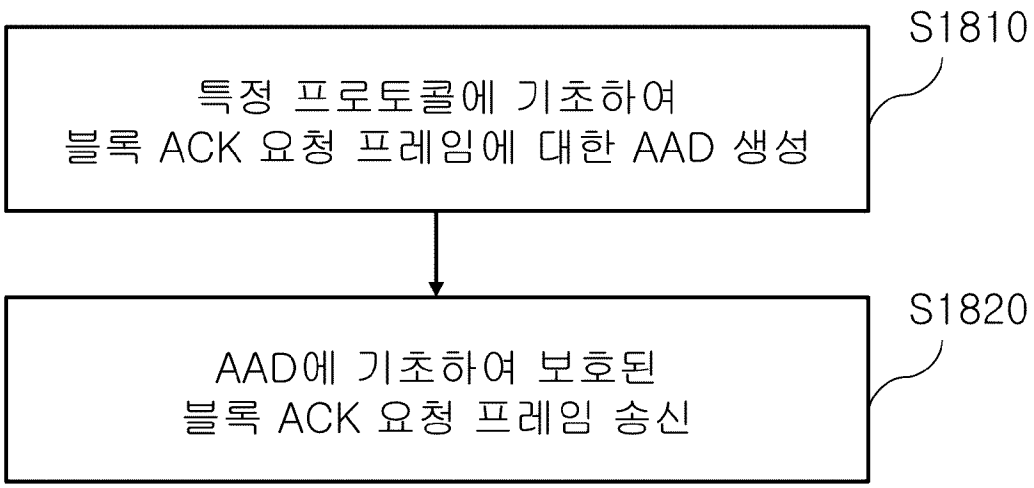
[도16]


B0 B1 B4 B5 B11 B12 B15
보류됨 BAR 유형 보류됨 TID_INFO
비트: 1 4 7 4
프레임 제어 구간 TA TA BAR 제어 BAR 정보 FCS
Octets: 2 3 6 6 1 가변 4
블록-ACK 시작 시퀀스 제어
Octets: 2
BA 유형 1: 압축된(Compressed)
각 TID 정보 블록-ACK 시작 시퀀스 제어
Octets: 2 2
각 TID에 대해 반복
BA 유형 2: 다중 TID(Multi-TID)
B0 B15 B16 B63
비트: 16 48
블록-ACK 시작 시퀀스 제어 GCR 그룹 어드레스
BA 유형 3: GCR

[도17]


S1710
특정 프로토콜에 기초하여 보호된 블록 ACK 요청 프레임 수신
S1720
블록 ACK 요청 프레임에 기초하여 AAD 생성
S1720
AAD에 기초하여 블록 ACK 요청 프레임에 대한 복호화/무결성 검사 수행

[도18]


S1810
특정 프로토콜에 기초하여 블록 ACK 요청 프레임에 대한 AAD 생성
S1820
AAD에 기초하여 보호된 블록 ACK 요청 프레임 송신

[도19]

(a)

프레임 제어	듀레이션	RA	TA
옥텟: 2	6	6	6

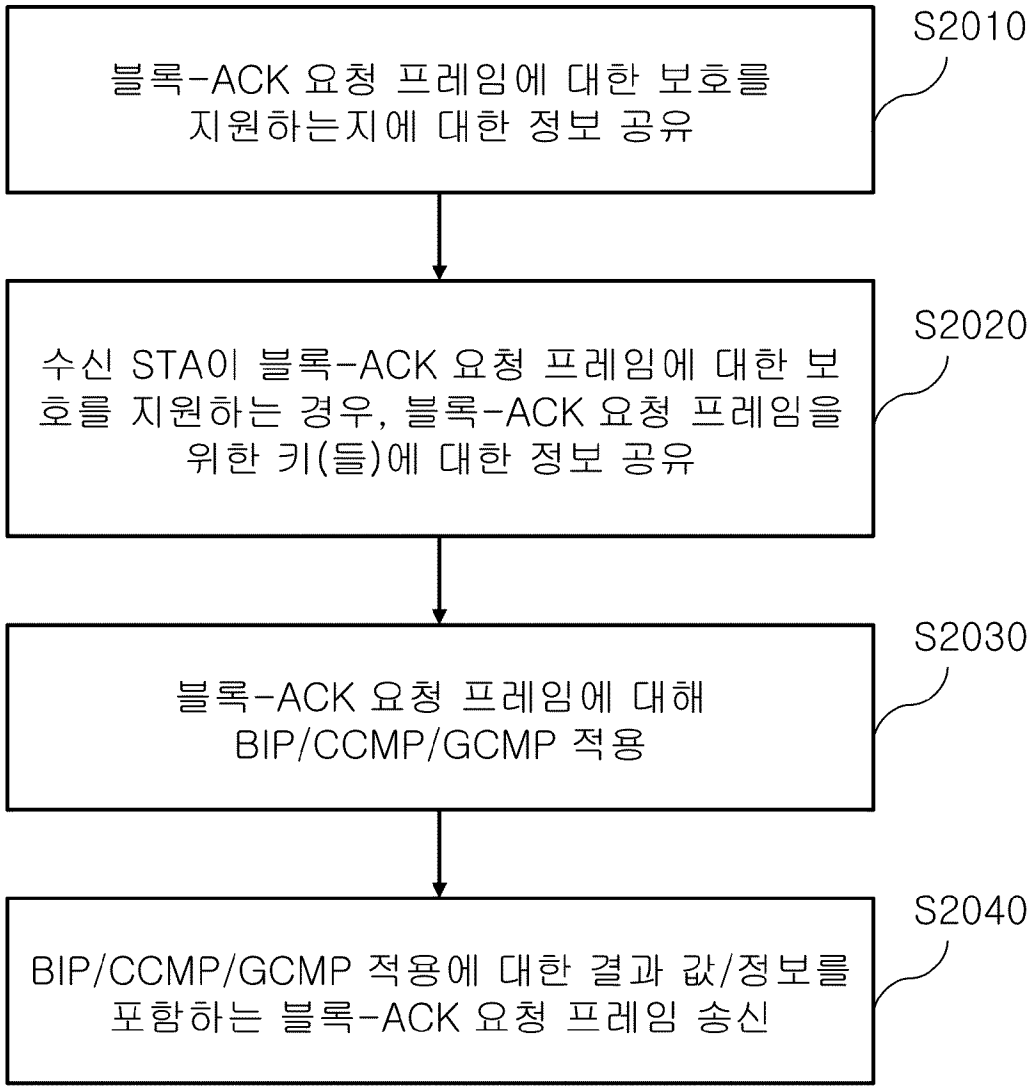
(b)

프레임 제어	듀레이션	RA	TA	BAR 제어
옥텟: 2	6	6	6	2

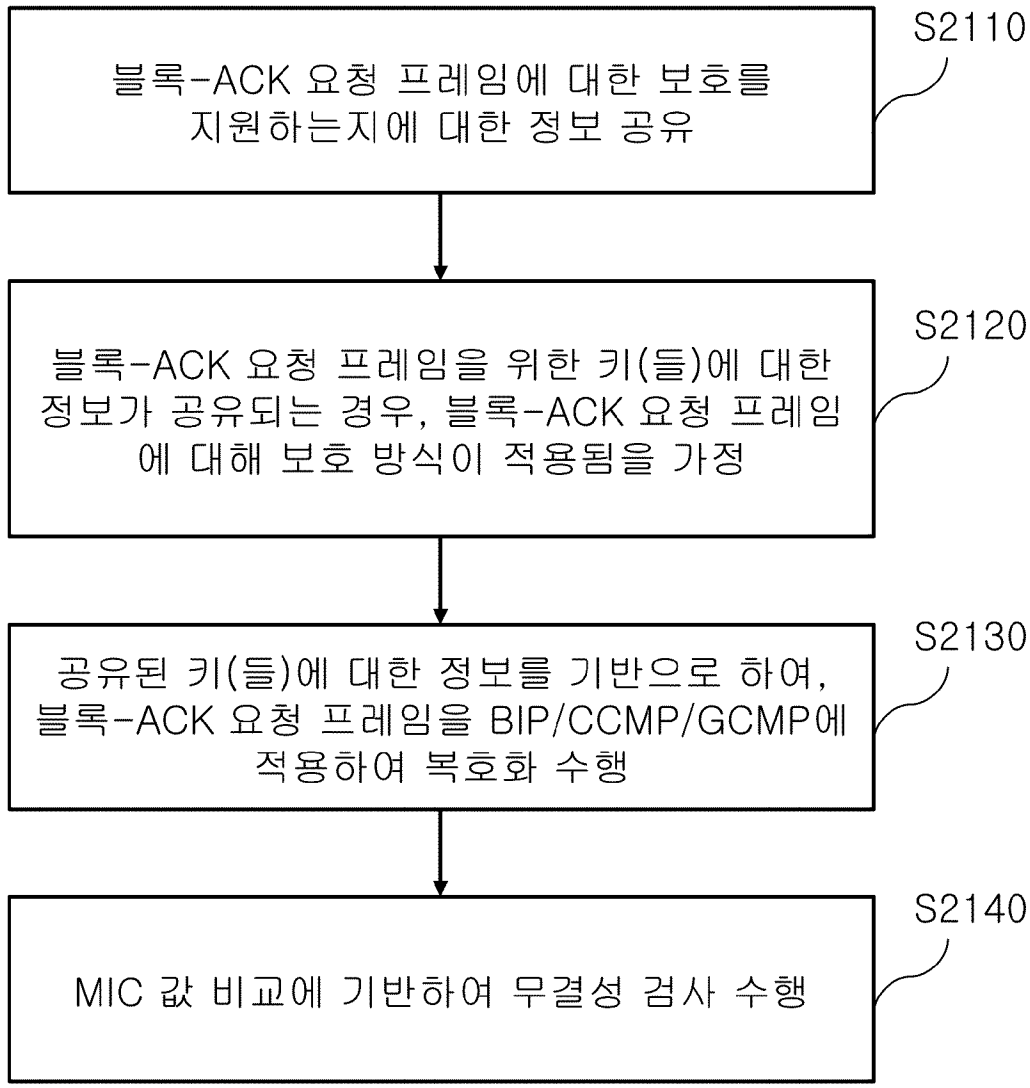
(c)

프레임 제어	듀레이션	RA	TA	BAR 정보
옥텟: 2	6	6	6	가변

[도20]



[도21]


블록-ACK 요청 프레임에 대한 보호를 지원하는지에 대한 정보 공유
S2110
블록-ACK 요청 프레임을 위한 키(들)에 대한 정보가 공유되는 경우, 블록-ACK 요청 프레임에 대해 보호 방식이 적용됨을 가정
S2120
공유된 키(들)에 대한 정보를 기반으로 하여, 블록-ACK 요청 프레임을 BIP/CCMP/GCMP에 적용하여 복호화 수행
S2130
MIC 값 비교에 기반하여 무결성 검사 수행
S2140

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2025/000145

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/106(2021.01)i; **H04L 1/1607**(2023.01)i; **H04W 12/0471**(2021.01)i; **H04W 84/12**(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/106(2021.01); H04L 1/16(2006.01); H04L 1/1607(2023.01); H04L 9/32(2006.01); H04W 72/0446(2023.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 블록 ACK, 요청(request), AAD, 무결성(integrity), 인증(authentication)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2023-0125787 A1 (HUANG, Po-Kai et al.) 27 April 2023 (2023-04-27) See paragraphs [0018], [0032], [0082], [0096] and [0098]; and claims 1-20.	1-8,11,14,19-23
A		9-10,12-13,15-18
Y	WO 2023-200572 A1 (QUALCOMM INCORPORATED) 19 October 2023 (2023-10-19) See paragraphs [0066], [0079], [0081] and [0084]; and claims 1-18.	1-8,11,14,19-23
Y	WO 2018-031750 A1 (QUALCOMM INCORPORATED) 15 February 2018 (2018-02-15) See paragraphs [0056]-[0068]; and claims 1-30.	5-8
Y	QIAN, Luke et al. A Simplifed Solution For Critical A-MPDU DoS Issues. IEEE 802.11-08/1021r1. 04 September 2008. See slides 3 and 7.	14
A	CHITRAKAR, Rojan. Comment Resolutions for 11be D1.0 AAD and Nonce CIDs. IEEE 802.11-21/1279r0. 06 December 2021. See page 2.	1-23

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2025	**15 April 2025**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208**	
Facsimile No. **+82-42-481-8578**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2025/000145

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2023-0125787 A1	27 April 2023	None	
WO 2023-200572 A1	19 October 2023	CN 118975172 A	15 November 2024
		KR 10-2025-0002158 A	07 January 2025
		TW 202345564 A	16 November 2023
WO 2018-031750 A1	15 February 2018	US 2018-0049027 A1	15 February 2018

국 제 조 사 보 고 서

국제출원번호
PCT/KR2025/000145

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 12/106(2021.01)i; **H04L 1/1607**(2023.01)i; **H04W 12/0471**(2021.01)i; **H04W 84/12**(2009.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 12/106(2021.01); H04L 1/16(2006.01); H04L 1/1607(2023.01); H04L 9/32(2006.01); H04W 72/0446(2023.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 블록 ACK, 요청(request), AAD, 무결성(integrity), 인증(authentication)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2023-0125787 A1 (PO-KAI HUANG 등) 2023.04.27 단락 [0018], [0032], [0082], [0096], [0098]; 및 청구항 1-20	1-8,11,14,19-23
A		9-10,12-13,15-18
Y	WO 2023-200572 A1 (QUALCOMM INCORPORATED) 2023.10.19 단락 [0066], [0079], [0081], [0084]; 및 청구항 1-18	1-8,11,14,19-23
Y	WO 2018-031750 A1 (QUALCOMM INCORPORATED) 2018.02.15 단락 [0056]-[0068]; 및 청구항 1-30	5-8
Y	LUKE QIAN 등, 'A Simplifed Solution For Critical A-MPDU DoS Issues', IEEE 802.11-08/1021r1, 2008.09.04 슬라이드 3, 7	14
A	ROJAN CHITRAKAR, 'Comment Resolutions for 11be D1.0 AAD and Nonce CIDs', IEEE 802.11-21/1279r0, 2021.12.06 페이지 2	1-23

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☑ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌
"D" 본 국제출원에서 출원인이 인용한 문헌
"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌
"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌
"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌
"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌
"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌
"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.
"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.
"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2025년04월14일(14.04.2025)	**2025년04월15일(15.04.2025)**

ISA/KR의 명칭 및 우편주소	심사관
대한민국 특허청 **(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)**	**양정록**
팩스 번호 **+82-42-481-8578**	전화번호 **+82-42-481-5709**

서식 PCT/ISA/210 (두 번째 용지) (2022년 7월)

국 제 조 사 보 고 서
대응특허에 관한 정보

국제출원번호
PCT/KR2025/000145

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2023-0125787 A1	2023/04/27	없음	
WO 2023-200572 A1	2023/10/19	CN 118975172 A	2024/11/15
		KR 10-2025-0002158 A	2025/01/07
		TW 202345564 A	2023/11/16
WO 2018-031750 A1	2018/02/15	US 2018-0049027 A1	2018/02/15