(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년02월12일
(11) 등록번호 10-2059079
(24) 등록일자 2019년12월18일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 28/06* (2009.01)
(21) 출원번호 10-2014-7020661
(22) 출원일자(국제) 2012년12월24일
심사청구일자 2017년12월22일
(85) 번역문제출일자 2014년07월23일
(65) 공개번호 10-2014-0116144
(43) 공개일자 2014년10월01일
(86) 국제출원번호 PCT/KR2012/011349
(87) 국제공개번호 WO 2013/095074
국제공개일자 2013년06월27일
(30) 우선권주장
4551/CHE/2011 2011년12월23일 인도(IN)
(56) 선행기술조사문헌
KR1020070103707 A*
Yi-Ting Lin, etc., "Abnormal Power Down Indication Through Quick Access Procedure", IEEE C80216p-11/0236(2011.09.09.) 1부.*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
아기왈, 아닐
인도, 방갈로르 560066, 투바라할리, 바더 메인 로드, 스리람 사무르드히, 엠 101
강현정
서울특별시 강남구 논현로 209 104동 602호 (도곡동,경남아파트)
(74) 대리인
이건주, 김정훈

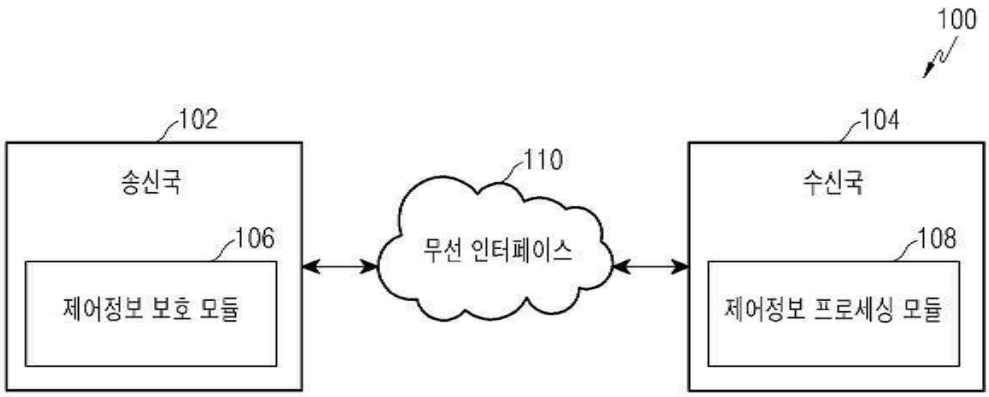
전체 청구항 수 : 총 20 항 심사관 : 최상호

(54) 발명의 명칭 **무선 네트워크 환경에서 제어정보의 보안통신을 위한 방법 및 시스템**

(57) 요 약

본 발명은 무선통신 네트워크 환경에서 제어정보를 안전하게 보안화하기 위한 방법 및 시스템을 제공한다. 송신국이 수신국에 제어정보를 전송하는 것이 필요할 때, 송신국은 제어정보가 제1 유형 또는 제2 유형에 속하는지 여부를 결정한다. 만일 제어정보가 제2 유형의 제어정보이면, 송신국은 제2 유형의 제어정보를 보호하기 위해 계산된 카운터 값, CMAC 값 및 보안키를 이용하여 제2 유형의 제어정보를 보안처리한다. 상기 제어정보를 보안처리할 시, 송신국은 수신국에 상기 보안처리된 제어정보를 전송한다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

무선 통신 시스템의 M2M(machine to machine) 디바이스에서 제어 정보를 송신하기 위한 방법에 있어서,

인증 코드에 기초하여 상기 제어 정보를 인증하기 위한 인증 키를 생성하는 과정; 및

상기 인증 키에 기초하여 보호되는 상기 제어 정보를 송신하는 과정을 포함하며,

상기 제어 정보는, 상기 제어 정보가 상기 인증 코드를 이용하여 보호되는지를 지시하는 지시자를 포함하고,

상기 인증 키는, 암호 키 (CMAC-TEK prekey) 및 상기 인증 키에 대한 기 정의된 상수 (CMACSIG)에 기반하여 생성되는 방법.

청구항 2

제1항에 있어서,

상기 보호되는 제어 정보는, 비정상 파워 다운 (abnormal power down) 시그널링 헤더에 기록되는, 방법.

청구항 3

제1항에 있어서,

상기 보호되는 제어 정보가 송신되는 프레임의 넘버(number)가 기정의된 범위에 도달하는 경우, 상기 프레임의 넘버에 대한 카운터를 증가시키고,

새로운 인증 키가 모든 기정의된 프레임의 넘버에서 생성되는 경우, 상기 카운터를 리셋(reset)하는, 방법.

청구항 4

제1항에 있어서,

모든 기정의된 프레임들의 넘버에서 새로운 인증 키를 생성하는 과정;을 더 포함하는, 방법.

청구항 5

제1항에 있어서,

상기 지시자가 상기 제어 정보가 상기 인증 코드를 이용하여 보호되고 있음을 지시하는 경우, 상기 제어 정보는, 상기 보호되는 정보가 송신되는 프레임의 넘버에 대한 카운터를 지시하는 정보 및 상기 인증 코드를 지시하는 정보 중 적어도 하나를 더 포함하는, 방법.

청구항 6

제1항에 있어서,

상기 인증 키 (CMAC_SIG_KEY_U)는,

하기의 식

CMAC_SIG_KEY_U = Dot16KDF (CMAC-TEK prekey, CMACSIG, 128)

에 따라, 암호 키 (CMAC-TEK prekey), 인증 키에 대한 기정의된 스트링 상수 (string constant) (CMACSIG), 입력 비트 스트링 (128)의 길이에 기초하는 기정이된 기정의된 함수 (Dot16KDF)를 이용하여 생성되는, 방법.

청구항 7

제1항에 있어서,

상기 인증 코드 (CMAC value)는

하기의 식

CMAC value = Truncate (CMAC (CMAC_SIG_KEY_U, AKID | 22 bits super frame number | 2 bits frame index | STID | FID | counter value | 16 bits zero padding | abnormal power down signaling header contents), 16)에 따라, 기정의된 함수 (Truncate), 인증 키(CMAC_SIG_KEY_U), 인증 키 식별자 (authorization key identifier: AKID), 플로우 식별자 (flow identifier: FID), 상기 M2M 디바이스의 스테이션 ID (station ID: STID), 상기 보호되는 제어 정보가 송신되는 카운터 값, 및 상기 인증 코드로 이용되기 위한 어드벤스드 (advanced) 암호화 표준-CMAC 계산의 결과의 LSB (least significant bit) 16 비트들인 16을 이용하여 생산되는, 방법.

청구항 8

제1항에 있어서,

상기 제어 정보는,

0b0010로 세팅된 플로우 식별자를 지시하는 제1 값, M2M 디바이스의 스테이션 ID (station ID: STID), 상기 제어 정보의 길이를 지시하는 제2 값, 상기 STID가 상기 M2M 디바이스에 유일하게 할당되는 경우, 0으로 설정된 STID 유효 오프셋을 지시하는 제3 값, 에머전시 타입 (emergency type)이 파워 아웃에이지 (power outage)인 경우, '0b1'으로 설정된 상기 에머전시 타입을 지시하는 제4 값 중 적어도 하나를 더 포함하는, 방법.

청구항 9

무선 통신 시스템에서 제어 정보를 수신하기 위한 방법에 있어서,

인증 키에 기초하여 보호되는 상기 제어 정보를 M2M(machine to machine) 디바이스로부터 수신하는 과정, 여기서, 상기 제어 정보는 상기 제어 정보가 인증 코드를 이용하여 보호되는지를 지시하는 지시자를 포함함; 및

상기 제어 정보로부터 획득되는 값들에 기초하여 생성되는 인증 키를 이용하여 상기 제어 정보를 인증하는 과정을 포함하며,

상기 인증 키는, 암호 키 (CMAC-TEK prekey) 및 상기 인증 키에 대한 기 정의된 상수 (CMACSIG)에 기반하여 생성되는 방법.

청구항 10

제9항에 있어서,

상기 보호되는 제어 정보는, 비정상 파워 다운 (abnormal power down) 시그널링 헤더에 기록되는, 방법.

청구항 11

제9항에 있어서,

상기 보호되는 제어 정보가 송신되는 프레임의 넘버(number)가 기정의된 범위에 도달하는 경우, 상기 프레임의 넘버에 대한 카운터를 증가시키고,

새로운 인증 키가 모든 기정의된 프레임의 넘버에서 생성되는 경우, 상기 카운터를 리셋(reset)하는, 방법.

청구항 12

제9항에 있어서,

모든 기정의된 프레임들의 넘버에서 새로운 인증 키를 생성하는 과정;을 더 포함하는, 방법.

청구항 13

제9항에 있어서,

상기 지시자가 상기 제어 정보가 상기 인증 코드를 이용하여 보호되고 있음을 지시하는 경우, 상기 제어 정보는, 상기 보호되는 정보가 송신되는 프레임의 넘버에 대한 카운터를 지시하는 정보 및 상기 인증 코드를 지

시하는 정보 중 적어도 하나를 더 포함하는, 방법.

청구항 14

제9항에 있어서,

상기 인증 키 (CMAC_SIG_KEY_U)는,

하기의 식

CMAC_SIG_KEY_U = Dot16KDF (CMAC-TEK prekey, CMACSIG, 128)

에 따라, 암호 키 (CMAC-TEK prekey), 인증 키에 대한 기정의된 스트링 상수 (string constant) (CMACSIG), 입력 비트 스트링 (128)의 길이에 기초하는 기정이된 기정의된 함수 (Dot16KDF)를 이용하여 생성되는, 방법.

청구항 15

제9항에 있어서,

상기 인증 코드 (CMAC value)는

하기의 식

CMAC value = Truncate (CMAC (CMAC_SIG_KEY_U, AKID | 22 bits super frame number | 2 bits frame index | STID | FID | counter value | 16 bits zero padding | abnormal power down signaling header contents), 16)

에 따라, 기정의된 함수 (Truncate), 인증 키(CMAC_SIG_KEY_U), 인증 키 식별자 (authorization key identifier: AKID), 플로우 식별자 (flow identifier: FID), 상기 M2M 디바이스의 스테이션 ID (station ID: STID), 상기 보호되는 제어 정보가 송신되는 카운터 값, 및 상기 인증 코드로 이용되기 위한 어드벤스드 (advanced) 암호화 표준-CMAC 계산의 결과의 LSB (least significant bit) 16 비트들인 16을 이용하여 생산되는, 방법.

청구항 16

제9항에 있어서,

상기 제어 정보는,

0b0010로 세팅된 플로우 식별자를 지시하는 제1 값, M2M 디바이스의 스테이션 ID (station ID: STID), 상기 제어 정보의 길이를 지시하는 제2 값, 상기 STID가 상기 M2M 디바이스에 유일하게 할당되는 경우, 0으로 설정된 STID 유효 오프셋을 지시하는 제3 값, 에머전시 타입 (emergency type)이 파워 아웃에이지 (power outage)인 경우, '0b1'으로 설정된 상기 에머전시 타입을 지시하는 제4 값 중 적어도 하나를 더 포함하는, 방법.

청구항 17

무선 통신 시스템에서 제어 정보를 송신하는 M2M(machine to machine) 디바이스에 있어서,

인증 코드에 기초하여 상기 제어 정보를 인증하기 위한 인증 키를 생성하는 제어부와; 및

상기 인증 키에 기초하여 보호되는 상기 제어 정보를 송신하는 송신부를 포함하며,

상기 제어 정보는, 상기 제어 정보가 상기 인증 코드를 이용하여 보호되는지를 지시하는 지시자를 포함하고,

상기 인증 키는, 암호 키 (CMAC-TEK prekey) 및 상기 인증 키에 대한 기 정의된 상수 (CMACSIG)에 기반하여 생성되는 M2M 디바이스.

청구항 18

제17항에 있어서,

상기 보호되는 제어 정보는, 비정상 파워 다운 (abnormal power down) 시그널링 헤더에 기록되는 M2M 디바이스.

청구항 19

무선 통신 시스템에서 제어 정보를 수신하는 기지국에 있어서,

인증 키에 기초하여 보호되는 상기 제어 정보를 M2M(machine to machine) 디바이스로부터 수신하는 수신부와,

상기 제어 정보로부터 획득되는 값들에 기초하여 생성되는 인증 키를 이용하여 상기 제어 정보를 인증하는 제어부를 포함하며,

상기 제어 정보는 상기 제어 정보가 인증 코드를 이용하여 보호되는지를 지시하는 지시자를 포함하고,

상기 인증 키는, 암호 키 (CMAC-TEK prekey) 및 상기 인증 키에 대한 기 정의된 상수 (CMACSIG)에 기반하여 생성되는 기지국.

청구항 20

제19항에 있어서,

상기 보호되는 제어 정보는, 비정상 파워 다운 (abnormal power down) 시그널링 헤더에 기록되는 기지국.

발명의 설명

기 술 분 야

[0001] 본 발명은 일반적으로 무선통신 기술분야에 관한 것으로서, 더 상세하게는, 무선 네트워크 환경에서 제어정보를 보안통신하는 것에 관한 것이다.

배 경 기 술

[0002] 다양한 통신표준들(예를 들면, WiMAX(Worldwide Interoperability for Microwave Access) 표준을 기반으로 하는 IEEE(Institute for Electronic and Electrical Engineers) 802.16e 표준 및 IEEE 802.16m에 대한 그의 발전)에 기초하는 광대역 무선 네트워크들은 음성, 패킷 데이터 등등과 같은 다양한 종류의 서비스들을 제공한다. 최근에는 IEEE 802.16m 및 IEEE 802.16e 기반의 표준들이 스마트 그리드(smart grid), 차량 추적(vehicular tracking), 헬스케어(healthcare) 등과 같은 애플리케이션들을 위한 기기간(Machine to Machine: M2M) 통신을 가능하게 하기 위해 고려되고 있다. 보안성(security)은 헬스케어 및 스마트 그리드와 같은 많은 중요한 애플리케이션들을 위해 사용될 것이기 때문에 그러한 표준들에 있어서 중요한 요건들 중의 하나이다.

[0003] 여러 가지 유형의 제어정보가 이동국 또는 M2M 장치와 기지국 사이에서 서로 간의 통신을 위하여 교환된다. 전형적으로, 제어정보는 M2M 장치와 기지국 사이에 형성되는 시그널링 접속(signalling connection)이나 흐름(flow) 시에 전송되는 제어 메시지의 형태로 교환된다. 현재, 제어 메시지들은 암호화 메시지 인증 코드(Cipher based Message Authentication Code: CMAC) 알고리즘을 이용하여 보호가 이루어지는데, 여기서 국립표준기술연구원(National Institute of Standards and Technology: NIST) 특별간행물 800-38B에 규정된 바와 같은 CMAC 구조를 이용하여 8-바이트 CMAC이 생성되고 시그널링 접속 또는 흐름 시 전송 전에 제어 메시지에 부가된다. 선택적으로는, 제어 메시지의 내용은 또한 암호화될 수도 있다. 3-바이트 카운터 또는 패킷 넘버(PN)가 또한 사용되어 재전송 공격(relay attack)에 대한 보호를 제공한다. 카운터는 매회의 제어 메시지의 전송 후에 증가된다. 튜플(tuple) <control security key, PN> 은 결코 반복되지 않는다. CMAC를 생성하기 위해 사용되는 보안키의 시퀀스 넘버(sequence number)가 또한 제어 메시지와 함께 전송된다. 제어 메시지를 보호하는 방법은 각 제어 메시지에 12-바이트의 오버헤드를 추가한다. 전형적으로, CMAC 값을 이용하여 보호되는 제어 메시지는 매체 접속 제어(medium access control: MAC) 프로토콜 데이터 유니트(protocol data unit: PDU)에 수반된다. 상기 보호된 제어 메시지를 수반하는 MAC PDU는 MAC 헤더 및 페이로드(payload)를 포함하고 있다. 페이로드는 보안키 시퀀스 넘버, 유보된 비트들, 패킷 수, 및 CMAC 값으로 이루어진 보안 정보에 의해 후속되는 제어 메시지를 포함한다.

[0004] 제어 정보는 또한 특정한 유형의 MAC 헤더들인 MAC 시그널링 헤더들의 형태로 교환된다. 상기 MAC 시그널링 헤더들은 MAC PDU들에 있는 수신국에 전송된다. MAC 시그널링 헤더를 수반하는 MAC PDU는 그 MAC 시그널링 헤더가 아닌 어떤 페이로드도 포함하지 않는다는 것이 이해될 수 있다. MAC 시그널링 헤더들은 크기에 있어 매우 짧지만(수 바이트 정도), 중요한 정보를 보유한다. 일반적으로, MAC 시그널링 헤더들은 6 내지 7 바이트의 크기이다. MAC 시그널링 헤더는 흐름 식별자(flow identifier) 필드, 유형 필드, 길이 필드 및 내용(콘텐트) 필드를 포함할 수도 있다. 흐름 식별자 필드는 MAC 시그널링 헤더와 연관되는 흐름 식별자를 나타낸다. 유형 필드

는 MAC 시그널링 헤더의 유형을 나타낸다. 길이 필드는 MAC 시그널링 헤더의 길이를 나타낸다. 내용 필드는 MAC 시그널링 헤더의 실제의 내용을 보유한다. 현재, MAC 시그널링 헤더들은 비보안형 방식으로 기지국 및 이동국 또는 M2M 장치 사이에서 교환된다.

발명의 내용

해결하려는 과제

[0005] 현재의 제어 메시지 보호 기술은 제어 정보 그 자체에 비교하면 많은 오버헤드가 MAC 시그널링 헤더의 크기에 부가될 수 있기 때문에 MAC 시그널링 헤더들에는 적용될 수가 없다.

과제의 해결 수단

[0006] 본 개시의 일 측면에 따르면, 무선통신 환경에서 제어정보를 보안처리(보안화)하는 방법이 제공되는바, 상기 방법은, 송신국에서, 제1 유형의 제어정보를 보안처리하기 위하여 하나 또는 다수의 보안키들 및 제2 유형의 제어정보를 보안처리하기 위하여 하나 또는 다수의 보안키들을 생성하는 과정; 상기 제1 유형의 제어정보에 대하여 제1 유형의 카운터를 계산하고 그리고 상기 제2 유형의 제어정보에 대하여 제2 유형의 카운터를 계산하는 과정; 상기 제1 유형의 제어정보에 대하여 제1 유형의 암호화 메시지 인증 코드(CMAC) 및 상기 제2 유형의 제어정보에 대하여 제2 유형의 암호화 메시지 인증 코드(CMAC)를 계산하는 과정; 상기 제1 유형의 CMAC, 상기 제1 유형의 카운터, 및 상기 제1 유형의 제어정보에 대하여 유도되는 상기 하나 또는 다수의 보안키들을 이용하여 상기 제1 유형의 제어정보를 보안처리하는 과정; 및 상기 제2 유형의 CMAC, 상기 제2 유형의 카운터, 및 상기 제2 유형의 제어정보에 대하여 유도되는 상기 하나 또는 다수의 보안키들을 이용하여 상기 제2 유형의 제어정보를 보안처리하는 과정을 포함한다.

[0007] 본 개시의 또 다른 측면에 따르면, 프로세서 및 상기 프로세서에 통신 가능하게 접속된 메모리를 포함하는 송신국이 제공되는바, 상기 메모리는, 제1 유형의 제어정보를 보안화하기 위하여 하나 또는 다수의 보안키들 및 제2 유형의 제어정보를 보안화하기 위하여 하나 또는 다수의 보안키들을 생성하고; 상기 제1 유형의 제어정보에 대하여 제1 유형의 카운터를 계산하고 상기 제2 유형의 제어정보에 대하여 제2 유형의 카운터를 계산하고; 상기 제1 유형의 제어정보에 대하여 제1 유형의 암호화 메시지 인증 코드(CMAC) 및 상기 제2 유형의 제어정보에 대하여 제2 유형의 CMAC를 계산하고; 상기 제1 유형의 CMAC, 상기 제1 유형의 카운터, 및 상기 제1 유형의 제어정보에 대하여 유도되는 상기 하나 또는 다수의 보안키들을 이용하여 상기 제1 유형의 제어정보를 보안처리하고; 그리고 상기 제2 유형의 CMAC, 상기 제2 유형의 카운터, 및 상기 제2 유형의 제어정보에 대하여 유도되는 상기 하나 또는 다수의 보안키들을 이용하여 상기 제2 유형의 제어정보를 보안처리하도록 구성된 제어정보 보호 모듈을 포함한다.

[0008] 본 개시의 또 다른 측면에 따르면, 무선통신 환경에서 시그널링 헤더들을 안전하게 통신하는 방법이 제공되는바, 상기 방법은, 송신국에 의해, 수신국으로 안전하게 전송될 시그널링 헤더에 대한 카운터 값을 계산하고; 상기 시그널링 헤더에 대한 암호화 메시지 인증 코드(CMAC) 값을 계산하고; 상기 CMAC 값, 상기 카운터 값 및 상기 시그널링 헤더에 대해 유도된 하나 또는 다수의 보안키들을 이용하여 상기 시그널링 헤더를 보안화하고; 그리고 상기 획득된 시그널링 헤더를 수신국으로 전송하는 과정을 포함한다.

[0009] 본 개시의 또 다른 측면에 따르면, 프로세서 및 상기 프로세서에 통신 가능하게 접속된 메모리를 포함하는 송신국이 제공되는바, 상기 메모리는, 수신국에 안전하게 전송될 시그널링 헤더에 대한 카운터 값을 계산하고; 상기 시그널링 헤더에 대한 암호화 메시지 인증 코드(CMAC) 값을 계산하고; 상기 CMAC 값, 상기 카운터 값 및 상기 시그널링 헤더에 대해 유도된 하나 또는 다수의 보안키들을 이용하여 상기 시그널링 헤더를 보안처리하고; 그리고 상기 획득된 시그널링 헤더를 수신국으로 전송하도록 구성된 제어정보 보호 모듈을 포함한다.

[0010] 본 개시의 또 다른 측면에 따르면, 송신국으로부터 수신된 시그널링 헤더를 처리하는 방법이 제공되는바, 상기 방법은, 상기 송신국으로부터 수신된 시그널링 헤더가 보호되는지 여부를 결정하는 과정; 상기 시그널링 헤더에 있는 카운터 값의 유효성(validating)을 확인하는 과정; 상기 카운터 값이 유효하다면 상기 시그널링 헤더가 상기 송신국으로부터 수신되는 프레임의 프레임 넘버를 결정하는 과정; 상기 카운터 값, 프레임 넘버, 인증키 식별자, 이동국 논리 어드레스, 흐름 식별자, 및 상기 시그널링 헤더의 내용에 기초하여 CMAC 값을 계산하는 과정; 상기 계산된 CMAC 값이 상기 시그널링 헤더에서의 상기 CMAC 값과 일치하는지 여부를 결정하는 과정; 및 상기 계산된 CMAC 값이 상기 시그널링 헤더에서의 상기 CMAC 값과 일치한다면, 상기 시그널링 헤더의 내용을 처리하는 과정을 포함한다.

[0011] 본 개시의 또 다른 하나의 측면에 따르면, 프로세서 및 상기 프로세서에 통신 가능하게 접속된 메모리를 포함하는 수신국이 제공되는바, 상기 메모리는, 송신국으로부터 수신된 시그널링 헤더가 보호되는지 여부를 결정하고; 상기 시그널링 헤더에 있는 카운터 값의 유효성을 확인하고; 상기 카운터 값이 유효하다면 상기 시그널링 헤더가 상기 송신국으로부터 수신되는 프레임의 프레임 넘버를 결정하고; 상기 카운터 값, 프레임 넘버, 인증키 식별자, 이동국 논리 어드레스, 흐름 식별자, 및 상기 시그널링 헤더의 내용에 기초하여 CMAC 값을 계산하고; 상기 계산된 CMAC 값이 상기 시그널링 헤더에서의 상기 CMAC 값과 일치하는지 여부를 결정하고; 그리고 상기 계산된 CMAC 값이 상기 시그널링 헤더에서의 상기 CMAC 값과 일치한다면, 상기 시그널링 헤더의 내용을 처리하도록 구성되는 제어정보 처리 모듈을 포함한다.

[0012] 본 개시의 또 다른 하나의 측면에 따르면, 무선 네트워크 환경에서 시그널링 헤더를 안전하게 전송하는 방법이 제공되는바, 상기 방법은, 수신국으로 전송될 시그널링 헤더를 보안화하기 위하여 보안키 정보를 생성하고; 상기 보안키 정보를 상기 시그널링 헤더의 내용과 함께 부가하고; 상기 시그널링 헤더의 내용이 부가된 상기 보안키 정보에 대한 사이클릭 리던던시 체크(CRC) 값을 생성하고; 상기 CRC 값을 상기 시그널링 헤더의 내용과 함께 부가하고; 그리고 상기 시그널링 헤더를 시그널링 헤더의 내용에 부가된 상기 CRC 값과 함께 상기 수신국에 전송하는 과정을 포함한다.

[0013] 본 개시의 또 다른 하나의 측면에 따르면, 프로세서 및 상기 프로세서에 통신 가능하게 접속된 메모리를 포함하는 송신국이 제공되는바, 상기 메모리는, 수신국으로 전송될 시그널링 헤더를 보안화하기 위하여 보안키 정보를 생성하고; 상기 보안키 정보를 상기 시그널링 헤더의 내용과 함께 부가하고; 상기 시그널링 헤더의 내용이 부가된 상기 보안키 정보에 대한 사이클릭 리던던시 체크(CRC) 값을 생성하고; 상기 CRC 값을 상기 시그널링 헤더의 내용과 함께 부가하고; 그리고 상기 시그널링 헤더를 시그널링 헤더의 내용에 부가된 상기 CRC 값과 함께 상기 수신국에 전송하도록 구성된 제어정보 보호 모듈을 포함한다.

[0014] 본 개시의 또 다른 측면에 따르면, 무선 네트워크 환경에서 보호된 시그널링 헤더를 처리하는 방법이 제공되는바, 상기 방법은, 송신국으로부터 CRC 값을 갖는 보호된 시그널링 헤더를 수신할 시 보안키 정보를 생성하고; 상기 보안키 정보를 상기 시그널링 헤더의 내용과 함께 부가하고; 상기 시그널링 헤더의 내용이 부가된 상기 보안키 정보에 기초하여 CRC 값을 생성하고; 상기 생성된 CRC 값이 상기 시그널링 헤더에 있는 CRC 값과 일치(조화)하는지 여부를 결정하고; 상기 생성된 CRC 값이 상기 시그널링 헤더에 있는 CRC 값과 일치한다면 상기 시그널링 헤더의 내용을 처리하는 과정을 포함한다.

[0015] 본 개시의 또 다른 측면에 따르면, 무선 네트워크 환경에서 보호된 시그널링 헤더를 처리하는 방법이 제공되는바, 상기 방법은, 송신국으로부터 CRC 값을 갖는 보호된 시그널링 헤더를 수신할 시 보안키 정보를 생성하고; 상기 보안키 정보를 상기 시그널링 헤더의 내용과 함께 부가하고; 상기 시그널링 헤더의 내용이 부가된 상기 보안키 정보에 기초하여 CRC 값을 생성하고; 상기 생성된 CRC 값이 상기 시그널링 헤더에 있는 CRC 값과 일치(조화)하는지 여부를 결정하고; 그리고 상기 생성된 CRC 값이 상기 시그널링 헤더에 있는 CRC 값과 일치한다면 상기 시그널링 헤더의 내용을 처리하는 과정을 포함한다.

도면의 간단한 설명

[0016] 도 1은 일 실시예에 따른, 송신국 및 수신국 사이의 제어 정보를 안전하게 통신하기 위한 무선 네트워크 시스템의 블록도를 예시한다.

도 2는 일 실시예에 따른, 수신국에 전송될 제어정보를 보안처리하는 방법을 예시하는 프로세스 흐름도이다.

도 3은 일 실시예에 따른, 시그널링 헤더를 보안처리하는 상세한 방법의 프로세스 흐름도이다.

도 4a는 일 실시예에 따른, 보호된 매체 접속 제어(MAC) 시그널링 헤더의 예시적인 포맷을 나타낸다.

도 4b는 또 다른 실시예에 따른, 보호된 매체 접속 제어(MAC) 시그널링 헤더의 예시적인 포맷을 나타낸다.

도 5a는 또 다른 실시예에 따른, 보호된 비정상 파워다운(abnormal power down) 시그널링 헤더의 예시적인 포맷을 나타낸다.

도 5b는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더의 예시적인 포맷을 나타낸다.

도 5c는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더의 또 다른 하나의 예시적인 포맷을 나타낸다.

도 5d는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더의 또 다른 하나의 예시적인 포맷을 나타낸다.

도 5e는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더의 또 다른 하나의 예시적인 포맷을 나타낸다.

도 6은 일 실시예에 따른, 송신국으로부터 수신된 시그널링 헤더를 처리하는 예시적인 방법을 나타내는 프로세스의 흐름도이다.

도 7a은 일 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도이다.

도 7b는 또 다른 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도이다.

도 7c는 또 다른 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도이다.

도 8은 선택적인 실시예에 따른 시그널링 헤더를 보안화하는 상세한 방법에 대한 프로세스 흐름도이다.

도 9는 선택적인 실시예에 따른 송신국으로부터 수신된 보호된 시그널링 헤더를 처리하는 세부적인 방법에 대한 프로세스 흐름도이다.

도 10은 본 발명의 실시예들을 구현하기 위한 여러 가지의 구성요소들을 보여주는 송신국의 블록도이다.

도 11은 본 발명의 실시예들을 구현하기 위한 여러 가지의 구성요소들을 보여주는 수신국의 블록도이다.

이상 기술된 도면들은 단지 예시의 목적을 위한 것으로서 어떤 방식으로든 본 개시의 영역을 제한하는 것을 의도하지는 않는다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명은 무선 네트워크 환경에 있어서 제어정보를 안전하게 통신하기 위한 방법 및 그 시스템을 제공한다. 후술하는 본 발명의 실시예들에 대한 설명에 있어, 그것의 일부를 형성하는 첨부된 도면들에 대해 참조가 이루어지며, 그 도면들에서는 본 발명이 실현되는 특정한 실시예들이 단지 예시적인 방식으로 도시되어 있다. 이들 실시예들은 당해 기술분야의 전문가들이 본 발명을 실시할 수 있을 정도로 충분히 상세하게 기술된다. 그리고, 또한 다른 실시예들이 활용될 수도 있으며 본 발명의 범위에서 벗어남이 없이 변경이 이루어질 수도 있음을 이해하여야 할 것이다. 따라서, 후술하는 상세한 설명은 제한적인 의미에서 이루어지는 것이 아니며, 본 발명의 영역은 단지 첨부한 특허청구범위에 의해서만 정의될 것이다.

[0018] 본 명세서 전체에 걸쳐서, "보안처리된, 안전하게 또는 안전한(secured)" 및 "보호된(protected)"이라는 표현들은 실질적으로 같은 의미를 갖는 것으로서, 서로 교환가능하게 사용되어도 좋다.

[0019] 도 1은 일 실시예에 따른, 송신국 및 수신국 사이에서 제어 정보를 안전하게 통신하기 위한 무선 네트워크 시스템(100)의 블록도를 예시한다. 도 1에서, 시스템(100)은 송신국(102), 수신국(104) 및 무선 인터페이스(106)를 포함하고 있다. 송신국(102)은 제어정보 보호 모듈(106)을 포함하며 수신국(104)은 제어정보 프로세싱 모듈(108)을 포함한다. 송신국(102)은 이동국 또는 기지국일 수 있다. 수신국(104)는 기지국 또는 이동국일 수 있다.

[0020] 송신국(102)이 수신국(104)에 제어정보를 송신할 필요가 있을 때, 제어정보 보호 모듈(106)은 그 제어정보가 보호되어야 할 것인지 여부를 판단한다. 만일 그 제어정보가 보호될 것이면, 제어정보 보호 모듈(106)은 그 제어정보가 제1 유형 또는 제2유형에 속하는지 여부를 판단한다. 예를 들면, 제1 유형의 제어정보는 기설정된 시그널링 접속/흐름 상에서 전송될 제어 메시지들(예컨대, IEEE 802.16.1 시스템에서의 관리 메시지들, LTE(Long Term Evolution) 시스템에서의 무선 리소스 접속제어 메시지 등)을 포함할 수도 있다. 제2 유형의 제어정보는 시그널링 헤더들(예컨대, IEEE 802.16.1 시스템에서의 독립형 시그널링 헤더들, LTE 시스템에 있어서의 매체접속제어(MAC) 시그널링 헤더들 등)을 포함할 수도 있다. 제2 유형의 제어정보는 크기가 7 바이트까지에 이른다. 만일 제어정보가 제1 유형의 제어정보라면, 제어정보 보호 모듈(106)은 제1 유형의 카운터, 제1 유형의 암호화 메시지 인증 코드(Cipher based Message Authentication Code: CMAC) 값 및 제1 유형의 제어정보를 보호하기 위해 계산된 보안키들을 이용하여 제1 유형의 제어정보를 보안처리한다. 만일 제어정보가 제2 유형의 제어정보

라면, 상기 제어정보 보호 모듈(106)은 제2 유형의 카운터, 제2 유형의 암호화 메시지 인증 코드(CMAC) 값 및 제2 유형의 제어정보를 보호하기 위해 계산된 보안키들을 이용하여 제2 유형의 제어정보를 보안처리한다. 제어정보를 보안처리할 시, 송신국(102)은 무선 인터페이스(110) 상에서 그 보안처리된 제어정보를 수신국(104)에 전송한다.

[0021] 상기 보안처리된 제어정보를 수신할 시, 제어정보 프로세싱 모듈(108)은 송신국(102)으로부터 수신된 제어정보의 유형을 결정한다. 따라서, 제어정보 프로세싱 모듈(108)은 그 제어정보의 유형에 기초하여 수신된 제어정보를 디코딩한다. 제어정보를 보안처리하고 그리고 그 보안처리된 제어정보를 프로세싱하는 과정은 아래의 설명에서 더 상세하게 기술된다.

[0022] 도 2는 일 실시예에 따른, 수신국에 전송될 제어정보를 확보하는 방법을 예시하는 프로세스 흐름도이다. 일반적으로 송신국(102)은 두 가지 종류의 제어정보를 수신국(104)에 전송한다. 이 두 가지 종류의 제어정보는 중요한 정보를 수반하므로, 그 제어정보들은 수신국(104)에 안전하게 전송되는 것이 필요하다. 상기 프로세스 흐름도(200)는 제1 및 제2 유형의 제어정보를 그것을 수신국(104)에 송신하기에 앞서 보안처리기 위한 방법적 과정들을 제공하고 있다.

[0023] 과정 202에서, 인증 키(authentication key: AK)로부터 프리-키(pre-key)가 생성된다. 전형적으로, 인증 키는 인증과정 중 송신국(102)(예를 들어, 기지국) 및 수신국(104)(예를 들어, 이동국)에서 서로 유도된다. 인증 키의 길이는 160 비트이다. 상기 프리-키는 제1 유형의 제어정보와 제2 유형의 제어정보를 각각 보안화하기 위한 별개의 상향(uplink) 및 하향(downlink) 보안키들을 만들기 위하여 사용될 수도 있다. 과정 204에서, 제1 유형의 제어정보를 위한 상향 및/또는 하향 보안키들과 제2 유형의 제어정보를 위한 상향 및/또는 하향 보안키들은 상기 프리-키로부터 유도된다. 예를 들면, 상향 보안키는 상향으로 전송되는 제어정보를 인증하기 위해 사용될 수 있는 반면 하향 보안키는 하향으로 전송되는 제어정보를 인증하기 위해 사용될 수도 있다. 하나의 예시적인 구현 예에 있어서, 제1 및 제2 유형의 제어정보를 위한 상향 및 하향 보안키들의 길이는 128 비트이다. 또 다른 예시적인 구현 예에 있어서는, 제1 및 제2 유형의 제어정보를 위한 상향 및 하향 보안키들의 길이는 상이한 크기로 될 수도 있다. 프리-키로부터 보안키들을 유도하는 프로세스는 당해 기술분야의 전문가에게 잘 알려져 있고 그에 대한 설명은 여기서는 생략된다는 것을 유념하여야 할 것이다. 도 7a 및 도 7c에 예시된 방법들에 따라서 새로운 보안키들이 주기적으로 생성된다.

[0024] 과정 206에서, 제1 유형의 제어정보에 대한 제1 유형의 카운터가 계산된다. 예를 들면, 제1 유형의 카운터는 제1 유형의 제어정보가 전송될 MAC PDU의 패킷 넘버(PN)일 수도 있다. 어떤 실시예들에 있어서는, 제1 유형의 제어정보에 대한 패킷 넘버가 결정된다. 이러한 실시예들에서는, 제1 유형의 카운터는 제1 유형의 제어정보에 기초하여 계산된다. 과정 208에서, 제1 유형의 제어정보에 대한 제1 유형의 CMAC가 계산된다. 상기한 제1 유형의 CMAC는 국립표준기술연구원(National Institute of Standards and Technology: NIST) 특별간행물(Special Publication 800-38B)에 규정된 것과 같은 CMAC 구성에 기초하여 계산된다. 예를 들면, 제1 유형의 CMAC는 truncate (제1 유형의 제어정보에 대한 보안키, 인증 키 식별자 | PN | 이동국 논리 어드레스 | 흐름 식별자(flow identifier) | 제로 패딩(Zero Padding) | 제1 유형의 제어정보, 64)와 같다. 과정 210에서, 제1 유형의 제어정보는 제1 유형의 CMAC, 제1 유형 카운터, 및 제1 유형의 제어정보에 대해 유도된 보안키들을 이용하여 보안화된다. 제1 유형의 제어정보를 확보하기 위해 제1 유형의 카운터 및 제1 유형의 CMAC를 계산하는 방법은 당해 기술분야의 전문가에게 잘 알려져 있으므로 그에 대한 설명은 여기서는 생략된다.

[0025] 과정 212 내지 216은 본 발명에 따른 시그널링 헤더와 같은 제2 유형의 제어정보를 보안화하기 위한 프로세스를 예시하고 있다. 과정 212에서, 제2 유형의 제어정보를 위한 제2 유형의 카운터가 계산된다. 과정 208에서, 제2 유형의 제어정보에 대한 제2 유형의 CMAC가 계산된다. 상기 제2 유형의 CMAC는 국립표준기술연구원(NIST) 특별간행물(Special Publication 800-38B)에서 규정된 것과 같은 CMAC 구성에 기초하여 계산된다. 예를 들면, 제2 유형의 CMAC는 truncate (제2 유형의 제어정보에 대한 보안키, 인증 키 식별자 | 프레임 넘버 | 이동국 논리 어드레스 | 흐름 식별자 | 제2 유형의 카운터 값 | 제로 패딩 | 제2 유형의 제어정보, 16)와 같다. 과정 210에서, 제2 유형의 제어정보는 제2 유형의 CMAC, 제2 유형 카운터, 및 제2 유형의 제어정보에 대해 유도된 보안키들을 이용하여 보안처리된다. 과정 212에서, 제2 유형의 CMAC 및 제2 유형의 카운터가 추가된 제2 유형의 정보는 수신국(104)으로 전송된다. 상기한 제2 유형의 카운터 및 제2 유형 CMAC는 제1 유형의 카운터 및 제1 유형의 CMAC와는 별개이며 제2 유형의 제어정보를 보안처리하기 위해 적합하다는 것을 유념하여야 할 것이다. 예를 들면, 제2 유형의 CMAC는 제1 유형의 CMAC에 비교해 더 짧은 길이일 수도 있고 제1 유형의 CMAC를 계산하기 위해 사용된 방법과는 다른 방법들을 사용하여 계산된다. 어떤 실시예들에 있어서는, 제2 유형의 카운터 및 제2 유형의 CMAC는 보안처리된 제2 유형의 제어정보, 제2 유형 CMAC 및 제2 유형 카운터를 포함하는 패킷의 전체 크기가 상

기 보안처리된 제2 유형의 제어정보의 허용가능한 임계치를 초과하지 않도록 계산된다. 시스널링 헤더들과 같은 제2 유형의 제어정보를 보안처리하는 상세한 과정은 도 3에서 더 상세히 설명된다.

[0026] 도 3은 일 실시예에 따른, 시그널링 헤더를 보안처리하는 상세한 방법에 대한 프로세스 흐름도이다. 송신국(102)이 수신국(104)로 전송될 시그널링 헤더를 갖고 있다고 가정한다. 과정 302에서, 그 시그널링 헤더가 수신국(104)로 안전하게(보안형으로) 전송될 것인지 여부가 결정된다. 만일 그 시그널링 헤더가 비보호 방식으로 전송될 것이면, 과정 304에서 비보안형 시그널링 헤더가 수신국(104)에 전송된다. 만일 시그널링 헤더가 보안형으로 전송될 것이면, 과정 306에서는, 그 시그널링 헤더를 보안처리하기 위한 보안키들이 이용가능한지가 결정된다. 만일 보안키들이 이용가능하지 않으면, 과정 304가 수행된다.

[0027] 만일 보안키들이 이용가능하면, 과정 308에서, 이용가능한 자원과 관련되는 프레임의 프레임 넘버가 결정된다. 선택적으로는, 만일 보안키들이 이용가능하다면, 그 시그널링 헤더를 보안형으로 전송하기 위해 충분한 자원이 이용가능한지 여부가 결정될 수도 있다. 예를 들면, 기지국은 이동국에 의한 매 전송시마다 이동국에 할당된 자원을 통신한다. 할당된 자원들에 기초하여 이동국은 시그널링 헤더의 보안형 전송을 위해 충분한 자원이 이용가능한지 여부를 결정할 수도 있다. 만일 이용가능한 어떤 자원도 없다면, 과정 304가 수행되어 시그널링 헤더가 보호 없이 전송된다. 만일 충분한 자원이 이용 가능하다면, 과정 308이 수행된다.

[0028] 과정 310에서, 프레임과 관련된 롤 오버 카운터(roll-over counter)가 결정된다. 예를 들면, 롤 오버 카운터가 매 프레임 롤 오버 후에 증가 된다. 과정 312에서, 그 시그널링 헤더와 관련된 시그널링 헤더 인덱스(제어정보 인덱스라 지칭되기도 함)가 결정된다. 매 프레임에 대하여, 각 프레임에서 전송될 각각의 시그널링 헤더에 고유의 시그널링 헤더 인덱스가 할당된다. 즉, 시그널링 헤더 인덱스는 한 프레임에서 전송될 시그널링 헤더들에 걸쳐 유일(unique)하다. 과정 314에서, 시그널링 헤더에 대한 카운터 값('제2 유형의 카운터'로서 이전에 지칭됨)이 그 프레임의 롤 오버 카운터 및 시그널링 헤더 인덱스에 기초해 계산된다. 상기 카운터 값은 재전송 공격(replay attack)에 대한 보호를 제공하기 위해 사용된다. 재전송 공격은 유효 데이터 전송이 고의적으로 또는 기만적으로 반복되거나 지연되는 네트워크 공격의 한 형태이다.

[0029] 일 실시예에 있어서, 카운터 값은 롤 오버 카운터에 해당하는 'n1' 최상위비트(most significant bits: MSB) 및 시그널링 헤더 인덱스에 해당하는 'n-n1' 최하위비트(least significant bits: LSB)를 구성한다. 롤 오버 카운터에 해당하는 상기 'n1' 최상위비트들은 프레임 롤 오버가 일어날 때 1 mod $2^{(n1)}$ 와 같은 값만큼 증분된다. 예를 들면, 만일 프레임 넘버가 24비트로 이루어져 있고 'n1'은 5 비트라면, 프레임 넘버가 0xFFFFFF에서 0x000000에 도달할 때 카운터 값의 'n1' 최상위비트는 1 mod 32만큼 증가한다. 시그널링 헤더 인덱스에 해당하는 'n-n1' 최하위비트는 같은 보안키를 이용하는 같은 프레임에서의 어떤 두 개의 시그널링 헤더들도 같은 카운터 값을 갖지 않도록 하는 방식으로 시그널링 헤더들에 할당된다. 이것은 송신국(102)으로 하여금 동일한 보안키를 이용하여 프레임당 $2^{(n-n1)}$ 시그널링 헤더들을 보안화하는 것을 가능하게 한다. 따라서, 송신국(102)은 매 $2^{(n1+n2)}$ 프레임당 새로운 보안키를 생성할 것이다. 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다.

[0030] 또 다른 실시예에 있어서, 카운터 값은 롤 오버 카운터에 해당하는 'n1' 최하위비트(LSB) 및 시그널링 헤더 인덱스에 해당하는 'n-n1' 최상위비트(MSB)를 구성한다. 롤 오버 카운터에 해당하는 상기 'n1' 최상위비트들은 프레임 롤 오버가 일어날 때 1 mod $2^{(n1)}$ 와 같은 값만큼 증분된다. 예를 들면, 만일 프레임 넘버가 24비트로 이루어져 있고 'n1'은 5 비트라면, 프레임 넘버가 0xFFFFFF에서 0x000000에 도달할 때 카운터 값의 'n1' 최하위비트는 1 mod 32만큼 증가한다. 시그널링 헤더 인덱스에 해당하는 'n-n1' 최상위비트는 같은 보안키를 이용하는 같은 프레임에서의 어떤 두 개의 시그널링 헤더들도 같은 카운터 값을 갖지 않도록 하는 방식으로 시그널링 헤더들에 할당된다. 따라서, 송신국(102)은 매 $2^{(n1+n2)}$ 프레임당 새로운 보안키를 생성할 것이며, 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다.

[0031] 또 다른 하나의 실시예에 있어서, 카운터 값은 프레임의 롤 오버 카운터를 구성한다. 롤 오버 카운터는 프레임 롤 오버가 일어날 때 1 mod $2^{(n)}$와 같은 값만큼 증분된다. 예를 들면, 만일 프레임 넘버가 24비트로 이루어져 있고 'n'은 5 비트라면, 프레임 넘버가 0xFFFFFF에서 0x000000에 도달할 때 카운터 값은 1 mod 32만큼 증분된다. 이것은 송신국(102)으로 하여금 동일한 보안키를 이용하여 프레임당 단지 하나의 시그널링 헤더를 보안처리하는 것을 가능하게 할 것이다. 따라서, 송신국(102)은 매 $2^{(n+n2)}$ 프레임당 새로운 보안키를 생성할 것이다. 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다.

[0032] 또 다른 하나의 실시예에 있어서, 카운터 값은 시그널링 헤더와 관련되는 시그널링 헤더 인덱스를 구성한다. 시그널링 헤더의 크기는 보안키를 사용하여 프레임당 보안형으로 전송될 시그널링 헤더들의 수에 기초해 계산된다. 예를 들어, 시그널링 헤더 인덱스의 크기가 'n' 비트라면, 송신국(102)은 같은 보안키를 이용하여 프레임당 2n 시그널링 헤더들을 보안처리할 수가 있다. 따라서, 송신국(102)은 매 2n2 프레임당 새로운 보안키를 생성할 것이다. 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다.

[0033] 과정 316에서, 시그널링 헤더가 보호되는 것을 나타내기 위한 표시가 시그널링 헤더에 이루어진다. 일 실시예에 있어서, 시그널링 헤더가 보호되는지 아닌지를 나타내기 위한 흐름 식별자(flow identifier)가 시그널링 헤더의 흐름 식별자 필드에 세트된다. 예를 들면, 시그널링 헤더가 보호될 때 흐름 식별자는 그 흐름 식별자 필드에서 '0b0100' 값으로 세트 된다. 또 다른 실시예에 있어서, 시그널링 헤더가 보호되는지 아닌지를 나타내기 위하여 EC 값이 시스널링 헤더의 EC 필드에 세트 된다. 예를 들면, 시그널링 헤더가 보호된다면, EC 필드는 '1' 값으로 세트 된다. 선택적으로는, 시그널링 헤더의 길이는 과정 316에서 그 시그널링 헤더의 길이 필드에 설정된다. 과정 318에서, 시그널링 헤더에 대한 CMAC 값(또는 '제2유형의 CMAC'로서 지칭됨)이 계산된다. CMAC 값은 CMAC 생성 함수를 이용해 생성된다. 하기의 파라미터들이 하나의 CMAC 값을 생성하기 위한 CMAC 생성 함수에 대한 입력으로서 제공된다: 제2유형의 제어정보에 대한 보안키, 인증키 식별자와 후속하는 프레임 넘버와 후속하는 시그널링 헤더 인덱스와 후속하는 흐름 식별자와 후속하는 카운터 값과 후속하는 시그널링 헤더의 내용. 예를 들면, CMAC 값은 truncate (제2 유형의 제어정보에 대한 보안키 | 인증 키 식별자 | 프레임 넘버 | 이동국 논리 어드레스 | 흐름 식별자 | 카운터 값 | 시그널링 헤더의 내용, 16)와 같다. 하나의 예시적인 구현 예에 있어서, 위에서 계산된 값의 16 최하위비트들이 CMAC 값으로서 사용된다. 또 다른 예시적인 구현 예에 있어서, 다른 16 비트의 상기한 계산 값이 CMAC 값으로서 사용된다.

[0034] 과정 320에서, 보안처리된 시그널링 헤더는 그 시그널링 헤더의 내용에 CMAC 값과 카운터 값을 추가함으로써 생성된다. 일 실시예에 있어서, 상기 보안화된 시그널링 헤더는 시그널링 헤더의 내용에 CMAC 값과 카운터 값의 적어도 'n-n1' 최하위비트들을 추가함으로써 생성되는데, 이때 카운터 값은 롤 오버 카운터의 'n1' 최상위비트들 및 시그널링 헤더 인덱스의 'n-n1' 최하위비트들을 구성한다. 또 다른 실시예에 있어서, 상기 보안처리된 시그널링 헤더는 CMAC 값과 카운터 값의 적어도 'n1-n1' 최상위비트들을 추가함으로써 생성되는데, 이때 카운터 값은 롤 오버 카운터의 'n1' 최하위비트들 및 시그널링 헤더 인덱스의 'n-n1' 최상위비트들을 구성한다. 또 다른 실시예에 있어서, 상기 보안처리된 시그널링 헤더는 CMAC 값과 롤 오버 카운터를 추가함으로써 생성되는데, 이때 카운터 값은 롤 오버 카운터와 같다. 또 다른 하나의 실시예에 있어서, 상기 보안처리된 시그널링 헤더는 CMAC 값 및 프레임의 롤 오버 카운터의 'n1' 최하위비트를 추가함으로써 생성되는데, 이때 카운터 값은 프레임의 롤 오버 카운터와 같다. 또 다른 하나의 실시예에 있어서, 상기 보안처리된 시그널링 헤더는 CMAC 값 및/또는 시그널링 헤더 인덱스를 추가함으로써 생성되는데, 이때 카운터 값은 시그널링 헤더 인덱스와 같다. 예를 들면, 상기 보안처리된 시그널링 헤더는 프레임당 전송이 허용되는 시그널링 헤더의 수가 '일'이라면 CMAC 값을 추가함으로써 생성된다. CMAC 값과 카운터 값은 그 시그널링 헤더의 전체 크기가 허용가능한 전체 크기(예컨대, 7 바이트)를 초과하지 않도록 시그널링 헤더의 내용에 추가된다는 것을 유념하여야 할 것이다. 과정 322에서, 상기 확보된 시그널링 헤더는 수신국(104)에 전송된다.

[0035] 다음의 기술은 IEEE 802.16.1b 시스템에 있어서 시그널링 헤더를 보호하는 예시적인 프로세스를 설명하고 있다. IEEE 802.16.1b 시스템에서의 이동국은 기지국에 시그널링 헤더를 보안형으로 전송하는 것이 필요하다고 가정한다. 또한, 업링크 및 다운링크에서 시그널링 헤더를 인증하기 위한 보안키들 CMAC_SIG_KEY_U 및 CMAC_SIG_KEY_D이 다음과 같이 유도된다고 가정한다:

[0036] CMAC_SIG_KEY_U | CMAC_SIG_KEY_D = Dot16KDF (CMAC-TEK prekey, "CMACSIG", 256).

[0037] 보안키들을 획득할 시, 이동국은 카운터 값을 영으로 리세트 한다. 카운터 값은 8 비트 크기이다. 카운터 값의 첫 번째 5 비트는 시그널링 헤더가 전송될 프레임에 대한 롤 오버 카운터를 나타낸다. 카운터 값의 다음 3 최하위비트들은 시그널링 헤더에 할당된 시그널링 헤더 인덱스를 나타낸다. 시그널링 헤더 인덱스는, 같은 보안키를 이용하여 획득된 동일 프레임에서의 어떤 두 개의 시그널링 헤더들도 같은 카운터 값을 갖지 않도록 하는 방식으로 시그널링 헤더에 할당된다는 것을 유념하여야 할 것이다. 이것은 이동국이 동일 보안키를 이용하는 5 밀리초(msec) 동안에 프레임당 8 시그널링 헤더들을 보호하는 것을 가능하게 한다. 프레임 넘버는 크기가 24 비트이고 롤 오버 카운터는 5 비트 크기이기 때문에, 이동국은 프레임 넘버가 0xFFFFFF 에서부터 0x000000 에 도달할 때 '1 mod 32' 값만큼 카운터 값을 증분한다. 더욱이, 새로운 보안키들은 매 $2^{24} * 2^{5} = 2^{29}$ 프레임들 후에 유도되는 것이 필요하다.

[0038] 다음으로 이동국은 인증키 식별자(AKID), 24비트 프레임 넘버, 시그널링 헤더의 12비트 스테이션 식별자(STID) 및 4비트 흐름 식별자(FID), 8비트 카운터 값, 16비트 제로 패딩, 시그널링 헤더의 내용으로 후속해서 이루어진 필드에 대해 CMAC 값을 계산한다. 프레임 넘버는 22비트 수퍼 프레임 및 2비트 프레임 인덱스에 기초하여 계산된다. 예를 들면, 시그널링 헤더에 대한 CMAC 값은 다음과 같이 계산된다:

[0039] CMAC 값 = Truncate (CMAC (CMAC_SIG_KEY, AKID | 22 비트 수퍼 프레임 넘버 | 2 비트 프레임 인덱스 | STID | FID | 카운터 값 | 16 비트 제로 패딩 | 시그널링 헤더 내용), 16).

[0040] CMAC 값은 NIST 특별 간행물 800-38B에 규정된 것과 같이 구성되는 것으로 이해된다. 이동국은 CMAC 값과 같은 AES-CMAC 계산 결과 중의 LSB 16비트와 카운터 값의 LSB 3비트를 이용하여 보안처리된 시그널링 헤더를 생성한다.

[0041] IEEE 802.16.1b 시스템에 있어서 비정상적인 파워다운 시그널링 헤더를 보호하는 예시적인 과정이 아래의 기술에서 설명된다. IEEE 802.16.1b에서 M2M 장치는 업링크 방향으로 비정상적인 파워다운 시그널링 헤더를 안전하게 전송하는 것이 필요하다고 가정한다. 또한, M2M 장치에 의해 업링크 방향으로 전송된 비정상적 파워다운 시그널링 헤더를 인증하기 위한 보안키 CMAC_SIG_KEY_U가 다음과 같이 유도된다고 가정한다:

[0042] CMAC_SIG_KEY_U = Dot16KDF (CMAC-TEK prekey, "CMACSIG", 128).

[0043] 보안키들을 획득할 시, 이동국은 카운터 값을 영으로 리셋한다. 카운터 값은 하나의 프레임에 대한 롤 오버 카운터와 같고 8비트 크기이다. M2M 장치는 프레임 넘버가 0xFFFFFF에서부터 0x000000에 도달할 때 값 '1 mod 8' 만큼 카운터 값을 증가한다. 따라서, M2M 장치는 동일 업링크 보안키를 이용하여 프레임당 하나의 비정상적인 파워다운 시그널링 헤더를 안전하게 전송할 수가 있다. 더욱이, 새로운 보안키들은 매 $2^{24} * 2^{8} = 2^{32}$프레임들 후에 유도되는 것이 필요하다.

[0044] 그 다음, 이동국은 인증키 식별자(AKID), 24비트 프레임 넘버, 시그널링 헤더의 12비트 스테이션 식별자(STID) 및 4비트 흐름 식별자(FID), 8비트 카운터 값, 16비트 제로 패딩, 비정상적 파워다운 시그널링 헤더의 내용으로 순차적으로 이루어진 필드에 대해 CMAC 값을 계산한다. 프레임 넘버는 22 비트 수퍼 프레임 및 2 비트 프레임 인덱스에 기초하여 계산된다. 예를 들면, 비정상적 파워다운 시그널링 헤더에 대한 CMAC 값은 다음과 같이 계산된다:

[0045] CMAC 값 = Truncate (CMAC (CMAC_SIG_KEY_U, AKID | 22 비트 수퍼 프레임 넘버 | 2 비트 프레임 인덱스 | STID |FID | 카운터 값 | 16 비트 제로 패딩 | 시그널링 헤더 내용), 16). CMAC 값은 NIST 특별 간행물 800-38B에 규정된 것과 같이 구성되는 것으로 이해된다. 이동국은 CMAC 값과 같은 AES-CMAC 계산 결과 중의 LSB 16비트와 카운터 값의 LSB 3비트를 이용하여 하나의 보안화된 비정상 파워다운 시그널링 헤더를 생성한다.

[0046] 도 4a는 일 실시예에 따른 보호된 MAC 시그널링 헤더(400)의 예시적인 포맷을 보여주고 있다. MAC 시그널링 헤더(400)는 FID 필드(402), 유형 필드(404), 길이 필드(406), 콘텐트 필드(408), 카운터 필드(410) 및 CMAC 값 필드(412)를 포함한다.

[0047] FID 필드(402)는 MAC 시그널링 헤더가 보호되는지 여부를 나타내는 MAC 시그널링 헤더(400)와 연관된 흐름 식별자를 포함한다. 예를 들면, 만일 MAC 시그널링 헤더가 보호된다면, FID 필드(401)는 값 '0b100'을 갖는다. 만일 MAC 시그널링 헤더(400)가 보호되지 않는다면, FID 필드(401)는 값 '0b0010'을 갖는다. 따라서, FID 필드(402)에 설정된 값에 기초하여 수신국(104)은 MAC 시그널링 헤더(400)가 보호되는지 또는 비보호인지의 여부를 결정한다. FID 필드(402)는 4비트 크기이다. 유형 필드(404)는 MAC 시그널링 헤더(400)의 유형을 지시하고 5비트 크기이다. 길이 필드(406)는 FID 필드(402), 유형 필드(404) 및 콘텐트 필드(406)의 길이를 지시한다. 콘텐트 필드(406)는 4비트 크기이다. 예를 들어, 만일 MAC 시그널링 헤더의 크기가 2 바이트라면, 길이 필드(406)는 값 '0b010'으로 세트 된다.

[0048] 내용(콘텐트) 필드(408)는 MAC 시그널링 헤더(400)의 내용을 보유하고 있으며 36비트 크기이다. 카운터 필드(410)는 MAC 시그널링 헤더(400)에 대해 계산된 카운터 값을 포함하고 있으며 8비트 크기이다. CMAC 필드(412)는 MAC 시그널링 헤더(400)에 대해 계산된 CMAC 값을 포함하고 있으며 16비트 크기이다. 상기한 MAC 시그널링 헤더(400)는, FID 필드(402)가 값 '0b0010'으로 세트 되어 있다면(즉, MAC 시그널링 헤더가 비보호될 경우), 카운터 필드(410)와 CMAC 필드(412)를 포함하지 않을 수도 있다는 것이 이해될 것이다.

[0049] 도 4b는 또 다른 실시예에 따른, 보호된 매체접속제어(MAC) 시그널링 헤더의 예시적인 포맷을 나타낸다. 도 4b의 MAC 시그널링 헤더(450)는 길이 필드(406)에 수반된 정보를 제외하고는 도 4c의 MAC 시그널링 헤더(400)와

유사하다는 것이 이해될 수 있을 것이다. MAC 시그널링 헤더(450)에 있어서, 길이 필드(406)는 FID 필드(402), 유형 필드(404), 콘텐트 필드(408), 카운터 필드(410) 및 CMAC 필드(412)의 길이들의 합을 나타낸다.

[0050] 도 5a는 또 다른 실시예에 따른, 보호된 비정상 파워다운(abnormal power down) 시그널링 헤더(500)에 대한 예시적인 포맷을 나타낸다. 상기 비정상 파워다운 시그널링 헤더(500)는 FID 필드(502), 유형 필드(504), 길이 필드(506), STD 필드(508), STID 유효 오프셋(510), 이머전시 유형 필드(512), EC 필드(514), 카운터 필드(516), 및 CMAC 필드(518)을 포함하고 있다.

[0051] FID 필드(502)는 다른 MAC PDU들로부터 MAC 시그널링 헤더를 구별하는 흐름 식별자를 포함하며 그리고 그 FID 필드(502)는 4비트 크기이다. 유형 필드(504)는 비정상 파워다운 시그널링 헤더(500)의 유형을 나타내며 5비트 크기이다. 길이 필드(506)는 비정상 파워다운 시그널링 헤더(500)의 전체 길이를 나타낸다. 길이 필드(506)은 4비트 크기이다. STID 필드(508)는 비정상 파워다운 시그널링 헤더(500)를 송신하는 이동국과 관련된 STID를 포함한다. STID 필드(510)는 같은 STID가 둘 이상의 이동국에 할당될 때 이동국에 할당된 STID 유효 오프셋을 나타낸다. 만일 STID가 하나의 이동국에만 유일하게 할당된다면, 그 이동국은 STID 유효 오프셋 필드(510)를 '0' 값으로 세트 한다. STID 유효 오프셋 필드(510)의 크기는 3비트이다.

[0052] 이머전시 유형 필드(512)는 비정상 파워다운 시그널링 헤더와 함께 전송되는 이머전시의 유형을 나타낸다. 이머전시 필드(512)의 크기는 1비트이다. 예를 들면, 이머전시 유형 필드(512)는 이머전시 종류가 정전이면 값 '0b0'으로 세트 된다. EC 필드(514)는 비정상 파워다운 시그널링 헤더(500)가 보호되는지 여부를 나타내고 크기는 1비트이다. 예를 들면, 만일 비정상 파워다운 시그널링 헤더(500)가 보호된다면, EC 필드(514)는 값 '1'을 포함한다. 만일 비정상 파워다운 시그널링 헤더(500)가 보호되지 않는다면, EC 필드(514)는 값 '0'을 포함한다. 따라서, EC 필드9514)에 세트 된 값에 기초하여 수신국(104)은 비정상 파워다운 시그널링 헤더(500)가 보호되는지 아니면 비보호되는지 여부를 결정한다.

[0053] 카운터 필드(516)는 비정상 파워다운 시그널링 헤더(500)에 대해 계산된 카운터 값을 포함한다. 카운터 필드(516)의 크기는 3비트이다. CMAC 필드(518)는 비정상 파워다운 시그널링 헤더(500)에 대해 계산된 CMAC 값을 포함하며 16비트 크기이다. 비정상 파워다운 시그널링 헤더(500)가 카운터 필드(516) 및 CMAC 필드(518)를 포함하지 않을 수도 있고 그리고 그것은 비정상 파워다운 시그널링 헤더가 보호되지 않을 때는 19비트 또는 3비트의 유보된 필드를 포함한다는 것이 이해될 것이다.

[0054] 도 5b는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더(550)의 또 하나의 예시적인 포맷을 나타낸다. 도 5b의 비정상 파워다운 시그널링 헤더(550)는 비정상 파워다운 시그널링 헤더(550)가 EC 필드(514)를 포함하지 않는다는 것을 제외하고는 도 5a의 비정상 파워다운 시그널링 헤더(500)와 같다는 것이 이해될 수 있을 것이다. 비정상 파워다운 시그널링 헤더(550)에 있어서, 길이 필드(506)는 비정상 파워다운 시그널링 헤더(550)가 보호되는 아닌지 여부를 나타내도록 세트 된다. 예를 들면, 만일 비정상 파워다운 시그널링 헤더(550)가 보호된다면, FID 필드는 '0b0100' 값으로 세트 된다.

[0055] 도 5c는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더(560)의 또 다른 하나의 예시적인 포맷을 나타낸다. 특히, 도 5c는 IEEE 802.16p 시스템에 따른 비정상 파워다운 시그널링 헤더(560)를 예시하고 있다. 비정상 파워다운 시그널링 헤더(560)는 HT 필드(561), EC 필드(562), 유형 필드(563), 확장 유형 필드(564), CID 필드(565), 이머전시 유형 필드(566), CMAC 인디케이터 필드(567), CMAC 값 필드(568), 카운터 필드(569), 유보 필드(570), 및 헤더 체크 시퀀스 필드(571)을 포함하고 있다.

[0056] CMAC 인디케이터 필드(567)는 비정상 파워다운 시그널링 헤더(560)가 보호되는지 여부를 나타낸다. 예를 들면, 만일 비정상 파워다운 시그널링 헤더가 보호된다면, CMAC 인디케이터 필드(567)는 값 '1'로 설정된다. 선택적으로는, 만일 비정상 파워다운 시그널링 헤더(560)가 보호되지 않는다면, CMAC 인디케이터 필드는 값 '0'으로 세트 된다. CMAC 필드(568)는 비정상 파워다운 시그널링 헤더(560)에 대해 계산된 CMAC 값을 포함하며 16비트 크기이다. 카운터 필드(569)는 비정상 파워다운 시그널링 헤더(560)에 대해 계산된 카운터 값을 포함하고 있다. 카운터 필드(569)의 크기는 2비트이다. 비정상 파워다운 시그널링 헤더(560)는, CMAC 인디케이터 필드(567)가 '0' 값으로 세트될 때 카운터 필드(569) 및 CMAC 필드(568)를 포함하지 않음이 이해될 것이다. 또한, CMAC 인디케이터 필드(567)가 '0' 값으로 세트될 때, 18비트 크기의 유보된 필드(571)가 비정상 파워다운 시그널링 헤더(560)에 포함된다. 다른 필드들(561 내지 566 및 571)은 당해 기술분야의 전문가에게 잘 알려져 있기 때문에 그에 대한 설명은 여기서는 생략된다.

[0057] 도 5d는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더(575)의 또 다른 하나의 예시적인 포맷

을 나타낸다. 도 5b의 비정상 파워다운 시그널링 헤더(575)는 그 비정상 파워다운 시그널링 헤더(575)가 확장된 유형 필드(564)를 포함하지 않는다는 것을 제외하고는 도 5c의 비정상 파워다운 시그널링 헤더(560)와 같다는 것이 이해될 수 있을 것이다. 비정상 파워다운 시그널링 헤더(575)에 있어서, 유형 필드(563)는 M2M 비정상 파워다운 시그널링 헤더(575)와 같은 유형을 나타내기 위해 사용된다. 확장된 유형 필드(564)의 제거는 송신국(102)이 비정상 파워다운 시그널링 헤더(560)에서의 2 최하위비트들과는 반대로 비정상 파워다운 시그널링 헤더(575)에서의 카운터 값의 3 최하위비트들을 포함하는 것을 가능하게 한다는 것이 이해될 수 있을 것이다.

[0058] 도 5e는 또 다른 실시예에 따른, 보호된 비정상 파워다운 시그널링 헤더(585)의 또 다른 하나의 예시적인 포맷을 나타낸다. 도 5e의 비정상 파워다운 시그널링 헤더(585)는 그 비정상 파워다운 시그널링 헤더(585)가 확장된 카운터 필드(569)를 포함하지 않는다는 것을 제외하고는 도 5c의 비정상 파워다운 시그널링 헤더(560)와 같다는 것이 이해될 수 있을 것이다.

[0059] 비정상 파워다운 시그널링 헤더의 전체 크기가 6 바이트를 초과하지 않도록 하는 방식으로 필드들이 비정상 파워다운 시그널링 헤더에 추가된다는 것이 도 5a 내지 도 5e로부터 이해될 수 있을 것이다. 이것은 송신국(102)(예컨대, M2M 장치)이 대역폭 요구(bandwidth request) 절차에 기초하는 할당된 자원(약 6 바이트의)에서의 대역폭 요구 시그널링 헤더 대신에 비정상 시그널링 헤더를 안전하게 전송하는 것을 수월하게 해준다.

[0060] 도 6은 일 실시예에 따른, 송신국(102)으로부터 수신된 시그널링 헤더를 처리하는 예시적인 방법을 나타내는 프로세스의 흐름도(600)이다. 과정 602에서, 시그널링 헤더는 송신국(102)으로부터 수신된다. 과정 604에서, 시그널링 헤더가 보호되는지 아닌지 여부가 그 시그널링 헤더에 세트 된 인디케이터에 기초하여 결정된다. 예를 들면, 만일 시그널링 헤더의 흐름 식별자 필드가 그 시그널링 헤더가 보호된다는 것을 나타내기 위해 사용된다면, 흐름 식별자 필드에 세트 된 값에 기초하여 그 시그널링 헤더가 보호되는지 아닌지의 여부가 결정된다. 선택적으로는, 만일 시그널링 헤더의 EC 필드가 그 시그널링 헤더가 보호된다는 것을 나타내기 위해 사용된다면, EC 필드에 세트 된 값에 기초하여 그 시그널링 헤더가 보호되는지 아닌지의 여부가 결정된다. 만일 인디케이터가 시그널링 헤더가 보호되지 않음을 지시한다면, 과정 606에서 시그널링 헤더는 직접 처리된다.

[0061] 만일 인디케이터가 시그널링 헤더가 보호됨을 지시한다면, 과정 608에서 시그널링 헤더의 길이 필드에 있는 정보가 읽혀진다. 시그널링 헤더가 가변적 길이의 시그널링 헤더라면 수신국(104)은 길이 필드를 읽는다. 과정 610에서 시그널링헤더의 카운터 필드에 있는 카운터 값이 읽혀진다. 과정 612에서, 시그널링 헤더가 카운터 값에 기초하여 유효한지 여부가 결정된다. 달리 설명하면, 과정 612에서, 같은 카운터 값을 갖는 임의의 시그널링 헤더가 이전에 수신되었는지 여부가 결정된다. 만일 시그널링 헤더가 유효하지 않으면, 그 시그널링 헤더는 과정 614에서 버려진다.

[0062] 과정 616에서, 시그널링 헤더가 수신되는 프레임의 프레임 넘버가 결정된다. 각각의 프레임에는 프레임 넘버가 할당된다. 시그널링 헤더를 포함하는 하나의 MAC PDU가 송신국(102)으로부터 수신될 때, 수신국(104)은 시그널링 헤더가 전송되는 프레임을 결정하고 그 다음으로는 그 프레임과 연관된 프레임 넘버를 결정한다. 과정 618에서, 시그널링 헤더에 대한 CMAC 값에 대한 CMAC 값이 프레임 넘버와 카운터 값에 기초하여 생성된다. 과정 620에서, 상기 생성된 CMAC 값이 수신된 시그널링 헤더의 CMAC 필드에서의 CMAC 값과 일치하는지 여부가 결정된다. 만일 그 결정결과 참(true)이라면, 과정 622에서 시그널링 헤더가 처리된다. 그렇지 않으면, 과정 624에서, 시그널링 헤더가 방기된다.

[0063] 도 7a은 일 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도이다. 과정 702에서, 제1 유형의 정보와 제2 유형의 정보에 대해 유도된 보안키들을 리프레싱하기 위한 소정의 조건이 충족되는지 여부가 결정된다. 일 실시예에 있어서, 상기한 소정의 조건은 프레임 넘버와 연결된(concatenated) 프레임의 롤 오버 카운터에 해당하는 카운터 값의 'n1'비트들이 임계치에 도달할 때 충족된 것으로 간주된다. 이 실시예에 있어서, 임계치는 2(n1+n2) 프레임들과 같을 수 있으며, 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다. 또 다른 실시예에 있어서, 상기한 소정의 조건은 프레임 넘버와 연결된 프레임의 롤 오버 카운터가 임계치에 도달할 때 충족된 것으로 간주된다. 본 실시예에 있어서, 임계치는 2(n+n2)프레임과 같을 수 있으며, 여기서 'n'은 프레임의 롤 오버 카운터를 나타내고 그리고 'n2'는 프레임 넘버를 나타내는 비트들의 수이다. 또 다른 실시예에 있어서, 상기한 소정의 조건은 프레임 넘버가 임계치에 도달할 때 만족되는 것으로 간주된다. 이 실시예에서, 임계치는 2n2 프레임들과 같으며, 여기서 'n2'는 프레임 넘버를 나타내는 비트들의 수이다.

[0064] 상기한 소정의 조건이 충족된다고 판단되면, 과정 704에서, 새로운 인증키 관계가 송신국(102)과 수신국(104) 사이에 설정된다. 과정 706에서, 새로운 프리-키가 새로운 인증키 상황(context)에 기초하여 생성된다. 과정

708에서, 하나 또는 다수의 새로운 보안키들이 상기 프리-키를 이용하여 제1 및 제2 유형의 제어정보를 확보하기 위해 유도된다. 과정 710에서, 카운터 값은 새로운 보안키들을 유도할 시에는 '0' 값으로 세트 되고 매번의 프레임 롤 오버 후에는 '1' 값만큼 증가한다.

[0065] 도 7b는 또 다른 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도이다. 과정 752에서, 제1 유형의 제어정보와 제2 유형의 제어정보에 대해 유도된 보안키들을 리프레싱하기 위한 상기한 소정의 조건이 만족되는지 여부가 결정된다. 만일 상기한 소정의 조건이 만족되는 것으로 결정되면, 과정 754에서, 인증키 전후관계와 관련된 인증키 카운터 값이 값 '1'만큼 증가한다. 송신국은 인증키 카운터를 유지하여 상기한 소정의 조건이 만족되는지 여부를 추적한다. 이것은 도 7a의 과정 702를 수행할 필요를 없애준다. 과정 756에서, 인증키와 연관된 인증키 카운터가 증가할 때 상기한 새로운 인증키 전후관계로부터 새로운 프리-키가 생성된다. 과정 758에서, 하나 또는 다수의 보안키들이 새로운 프리-키를 이용하여 제1 유형 및 제2 유형의 제어정보를 확보하기 위해 유도된다. 과정 760에서는 카운터 값은 새로운 보안키들을 유도할 시에는 '0' 값으로 세트 되고 그리고 매번의 프레임 롤 오버 후에는 '1' 값만큼 증가 된다.

[0066] 도 7c는 또 다른 실시예에 따른, 제1 유형의 제어정보와 제2 유형의 제어정보와 연관된 보안키들을 리프레싱하는 예시적인 방법을 나타내는 프로세스 흐름도(770)이다. 과정 772에서, 제2 유형의 정보(예를 들어, 시그널링 헤더들)에 대해 유도된 보안키들을 리프레싱하기 위한 상기한 소정의 조건이 만족되는지 여부가 결정된다. 만일 상기한 소정의 조건이 충족되는 것으로 결정되면, 과정 774에서, 제2 유형의 제어정보에 대해 유도된 보안키들과 관련된 보안키 카운터가 값 '1'만큼 증가 된다. 송신국(102)은 보안키 카운터를 유지하여 상기한 소정의 조건이 만족되는지 여부를 추적한다. 이것은 도 7a의 과정 702를 수행할 필요를 없애준다. 과정 776에서, 하나 또는 다수의 보안키들과 관련된 보안티 카운터 값이 값 '1'만큼 증가될 때 하나 또는 다수의 새로운 보안키들이 기존의 프리-키를 이용하여 제2 유형의 제어정보를 확보하기 위해 유도된다. 따라서, 송신국(102)은 제2 유형의 제어정보에 대한 보안키 카운터가 값 '1'만큼 증가될 때 양쪽 유형의 제어정보에 대한 새로운 보안키들을 유도할 필요가 없다. 당해 기술분야의 전문가라면 송신국(102)은 제1 유형의 제어정보에 대한 별개의 보안키 카운터를 유지하고 그 보안키 카운터가 증가될 때 제1 유형의 제어정보를 획득하기 위하여 프리-키로부터 새로운 보안키들을 유도할 수가 있다는 것을 상정할 수 있을 것이다. 과정 778에서, 카운터 값은 새로운 보안키들을 유도할 시 값 '0'으로 세트 되고 매번의 프레임 롤 오버 후에는 값 '1'만큼 증가한다.

[0067] 도 8은 선택적인 실시예에 따른 시그널링 헤더를 확보하는 상세한 방법에 대한 프로세스 흐름도(800)이다. 과정 802에서, 수신국(102)에 전송될 시그널링 헤더를 확보하기 위한 보안 정보가 생성된다. 보안 정보는 다음과 같이 생성된다;

[0068] 보안 정보 = 보안키 ID = Dot16KDF (보안키, 보안키 카운트 | 이동국 식별자 | 기지국 식별자 | 프레임 넘버 | 제로 패딩 (선택적) | 보안키 ID, n).

[0069] 일 실시예에 있어서, 'n'의 값은 64 비트이다. 보안 키 카운트는 매 프레임 롤 오버 시마다 업데이트 되며, 그리고 보안키는 그 보안키가 최대치에 도달하기 전에 리프레시 된다.

[0070] 과정 804에서, 보안 정보는 시그널링 헤더의 내용에 추가된다. 과정 806에서, 사이클릭 리던던시 체크(cyclic redundancy check: CRC) 값이 시그널링 헤더의 내용과 보안 정보에 기초하여 생성된다. CRC 값을 생성하는 과정은 당해 기술분야의 전문가에게 잘 알려져 있으므로 여기서는 설명이 생략된다. 과정 808에서, CRC 정보가 시그널링 헤더의 원래 내용에 부가된다. 시그널링 헤더의 EC 필드 또는 FID 필드는 그 시그널링 헤더가 보호되는지 여부를 지시하기 위해 사용될 수도 있다. 과정 810에서, CRD 정보를 갖는 시그널링 헤더는 수신국(104)에 전송된다.

[0071] 도 9는 선택적인 실시예에 따른, 송신국으로부터 수신된 보호된 시그널링 헤더를 처리하는 세부적인 방법에 대한 프로세스 흐름도(900)이다. 과정 902에서, 송신국(102)으로부터 시그널링 헤더가 수신된다. 과정 904에서, 시그널링 헤더가 보호되는지 아니면 그 시그널링 헤더에서의 흐름 식별자/EC 필드에 기초하지 않는지 여부가 결정된다. 만일 흐름 식별자/EC 필드가 시그널링 헤더가 보호되지 않음을 지시한다면, 과정 906에서, 시그널링 헤더는 직접 처리된다.

[0072] 만일 흐름 식별자가 시그널링 헤더가 보호됨을 지시한다면, 과정 908에서, 보안 정보가 생성된다. 과정 910에서, 보안 정보가 시그널링 헤더의 내용에 부가된다. 과정 912에서, CRC 값이 시그널링 헤더의 내용이 추가된 보안 정보를 이용하여 생성된다. 과정 914에서, 상기 생성된 CRC가 보호된 시그널링 헤더에 있는 CRC 값과

부합하는지 여부가 결정된다. 그 결과, 만일 부합한다면, 과정 916에서, 보호된 시그널링 헤더의 내용이 처리된다. 그러나, 부합하지 않는다면, 과정 918에서 시그널링 헤더는 방기된다.

[0073] 도 10은 본 발명의 실시예들을 구현하기 위한 여러 가지의 구성요소들을 나타내는 송신국(102)의 블록도이다. 도 10에서, 송신국(102)은 프로세서(1002), 메모리(1004), 독출전용메모리(ROM)(1006), 송신기(1008), 버스(1010), 디스플레이장치(1012), 입력장치(1014), 및 커서 제어부(1016)를 포함한다.

[0074] 본 명세서에 사용된 프로세서(1002)는 마이크로프로세서, 마이크로컨트롤러, 통합형 명령 세트(complex instruction set) 컴퓨팅 마이크로프로세서, 감축형(reduced) 명령 세트 컴퓨팅 마이크로프로세서, VLIW(very long instruction word)형 마이크로프로세서, EPIC(explicitly parallel instruction computing)형 마이크로프로세서, 그래픽 프로세서, 디지털 신호 프로세서(DSP), 또는 임의의 종류의 프로세싱 회로 등과 같은(그러나, 여기에 한정되는 것은 아님) 임의의 유형의 연산회로들을 망라하는 것으로 의도된다. 상기 프로세서(1002)는 또한 범용 또는 프로그램 가능형 논리장치들 또는 어레이들, 주문형 반도체 회로(ASIC)들, 단일-칩 컴퓨터, 스마트 카드 등등과 같은 임베디드형 컨트롤러(embedded controllers)들을 포함할 수도 있다.

[0075] 메모리(1004)는 휘발성 및 비휘발성 메모리일 수도 있다. 상기 메모리(1004)는, 전술한 실시예들 중의 어느 하나 또는 다수에 따라서, 제1 유형 및 제2 유형의 제어정보를 확보하기 위한 제어정보 보호 모듈(106)을 포함할 수도 있다. 다양한 형태의 컴퓨터로 독출 가능한 저장매체들이 메모리 요소들에 저장되고 그로부터 접속될 수도 있다. 메모리 요소들은 독출전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 소거가능형 프로그래머블 독출전용 메모리(EPROM), 전기적으로 소거가능한 프로그래머블 독출전용 메모리(EEPROM), 하드 드라이브, 컴팩트 디스크를 취급하기 위한 탈착형 매체 드라이브, 디지털 비디오 디스크, 디스켓, 자기테이프 카트리지, 메모리 카드, 메모리 스틱™ 등과 같은 데이터 및 기계로 판독가능한 명령들을 저장하기 위한 임의의 형태의 적절한 메모리 장치(들)를 포함할 수도 있다.

[0076] 본 발명의 여러 실시예들은 작업 실행, 추상적 데이터 형태의 정의, 또는 로-레벨 하드웨어 환경을 위한 기능들, 절차들, 데이터 구조들, 및 애플리케이션 프로그램들을 포함하는 모듈들과 결부하여 구현될 수도 있다. 제어정보 보호 모듈(106)은 전술한 저장매체들 중의 어느 것에 기계로 판독 가능한 명령들의 형태로 저장될 수도 있으며 프로세서(1002)에 의해 실행이 가능할 수도 있다. 예를 들면, 컴퓨터 프로그램은 본 발명의 개시된 실시예들과 그 교시에 따라서 제1 및 제2 유형의 제어정보를 획득하는 것이 가능한 기계로 판독 가능한 명령들을 포함할 수도 있다. 일 실시예에 있어서는, 상기 프로그램은 CD-ROM에 포함되고 그 CD-ROM으로부터 비휘발성 메모리에 있는 하드드라이브로 로딩 될 수도 있다.

[0077] 트랜시버(1008)는 제1 및 제2 유형의 제어정보를 수신국(104)에 안전하게 전송하는 것이 가능할 수도 있다. 버스(1010)는 송신국(102)의 여러 가지의 구성요소들 사이의 상호연결의 역할을 수행한다. 디스플레이장치(1012), 입력장치(1014) 및 커서 제어장치(1016)와 같은 구성요소들은 당해 기술분야의 전문가에게 잘 알려져 있으므로 그에 대한 설명은 여기서는 생략된다.

[0078] 도 11은 본 발명의 실시예들을 구현하기 위한 여러 가지의 구성요소들을 보여주는 수신국(104)의 블록도이다. 도 11에서, 수신국(104)은 프로세서(1102), 메모리(1104), 독출전용메모리(ROM)(1106), 수신기(1108), 버스(1110), 디스플레이장치(1112), 입력장치(1114), 및 커서 제어장치(1116)를 포함하고 있다.

[0079] 본 명세서에 사용된 프로세서(1102)는 마이크로프로세서, 마이크로컨트롤러, 통합형 명령 세트 컴퓨팅 마이크로프로세서, 감축형 명령 세트 컴퓨팅 마이크로프로세서, VLIW형 마이크로프로세서, EPIC형 마이크로프로세서, 그래픽 프로세서, 디지털 신호 프로세서(DSP), 또는 임의의 종류의 프로세싱 회로 등과 같은(그러나, 여기에 한정되는 것은 아님) 임의의 유형의 연산회로들을 망라하는 것으로 의도된다. 상기 프로세서(1002)는 또한 범용 또는 프로그램 가능형 논리장치들 또는 어레이들, 주문형 반도체 회로(ASIC)들, 단일-칩 컴퓨터, 스마트 카드 등등과 같은 임베디드형 컨트롤러들을 포함할 수도 있다.

[0080] 메모리(1104) 및 독출전용메모리(ROM)(1106)는 휘발성 및 비휘발성 메모리일 수도 있다. 상기 메모리(1104)는, 전술한 실시예들 중의 어느 하나 또는 다수에 따라서, 제1 유형 및 제2 유형의 제어정보를 확보하기 위한 제어정보 보호 모듈(108)을 포함할 수도 있다. 다양한 형태의 컴퓨터로 독출 가능한 저장매체들이 메모리 요소들에 저장되고 그로부터 접속될 수도 있다. 메모리 요소들은 독출전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 소거가능형 프로그래머블 독출전용 메모리(EPROM), 전기적으로 소거가능한 프로그래머블 독출전용 메모리(EEPROM), 하드 드라이브, 컴팩트 디스크를 취급하기 위한 탈착형 매체 드라이브, 디지털 비디오 디스크, 디스켓, 자기테이프 카트리지, 메모리 카드, 메모리 스틱™ 등과 같은 데이터 및 기계로 판독가능한 명령들을 저장하기 위한

임의의 형태의 적절한 메모리 장치(들)를 포함할 수도 있다.

[0081] 본 발명의 여러 실시예들은 작업 실행, 추상적 데이터 형태의 정의, 또는 로-레벨 하드웨어 환경을 위한 기능들, 절차들, 데이터 구조들, 및 애플리케이션 프로그램들을 포함하는 모듈들과 결부하여 구현될 수도 있다. 제어정보 보호 모듈(106)은 전술한 저장매체들 중의 어느 것에 기계로 판독 가능한 명령들의 형태로 저장될 수도 있으며 프로세서(1102)에 의해 실행이 가능할 수도 있다. 예를 들면, 컴퓨터 프로그램은 본 발명의 개시된 실시예들과 그 교시에 따라서 제1 및 제2 유형의 제어정보를 획득하는 것이 가능한 기계로 판독 가능한 명령들을 포함할 수도 있다. 일 실시예에 있어서는, 상기 프로그램은 CD-ROM에 포함되고 그 CD-ROM으로부터 비휘발성 메모리에 있는 하드드라이브로 로딩 될 수도 있다.

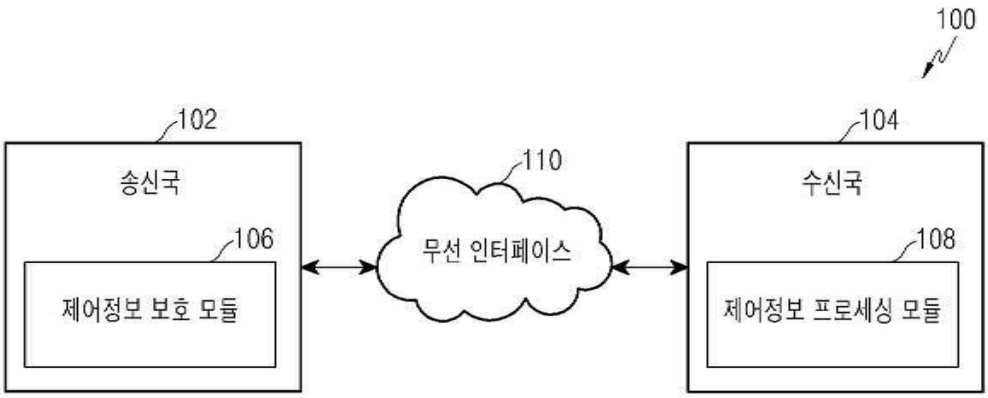
[0082] 수신기(1108)는 제1 및 제2 유형의 제어정보를 수신국(104)에 보안형으로 전송하는 것이 가능할 수도 있다. 버스(1110)는 송신국(102)의 여러 가지의 구성요소들 사이의 상호연결의 역할을 수행한다. 디스플레이장치(1112), 입력장치(1114) 및 커서 제어장치(1116)와 같은 구성요소들은 당해 기술분야의 전문가에게 잘 알려져 있으므로 그에 대한 설명은 여기서는 생략된다.

[0083] 이상 전술한 실시예들은 IEEE 802.16 시스템 및 특히 IEEE 802.16.1 시스템을 참조하여 기술되었으나, 당해 기술분야의 전문가라면 IEEE 802.16.1 시스템들에 대한 참조는 단지 예시를 위한 것으로서 개시된 여러 실시예들은 범용성을 상실하지 않고 다른 셀룰러 통신들에도 적용 가능하다는 것을 이해할 수 있을 것이다.

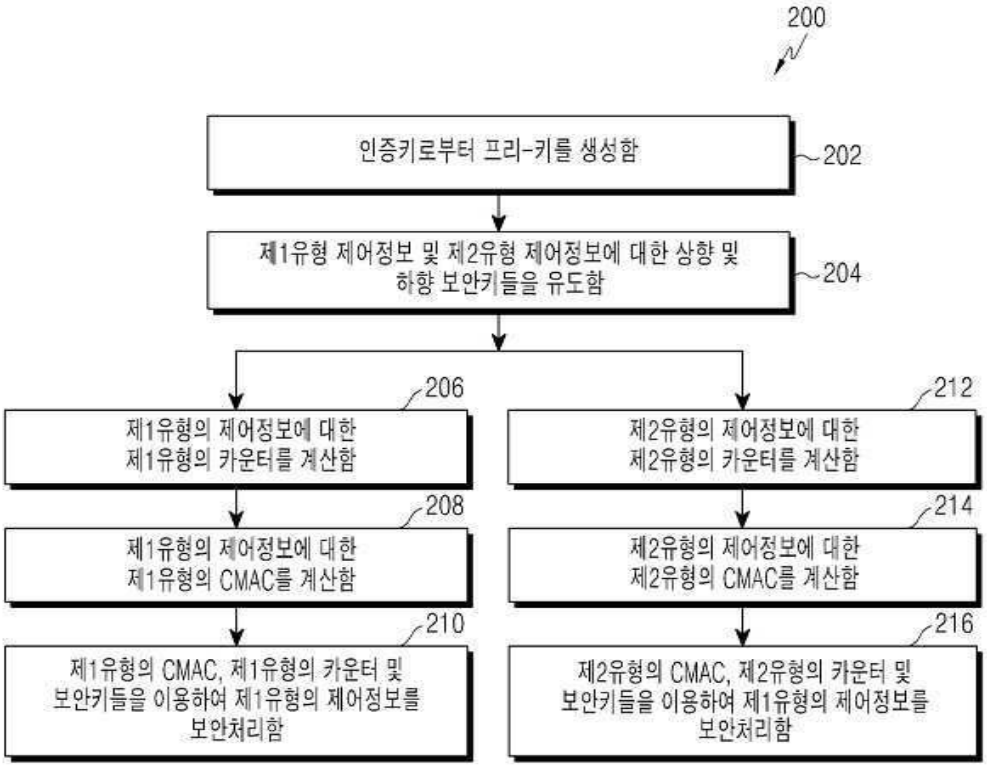
[0084] 본 발명은 특정한 예시적인 실시예들을 참조하여 이상 설명되었으나, 다양한 실시예들의 더 넓은 기본정신과 영역으로부터 벗어남이 없이 이들 실시예들에 대한 여러 가지의 변형들과 변경이 이루어질 수도 있음은 당해 기술분야의 전문가에게는 자명할 것이다. 게다가, 본 명세서에 기술된 다양한 장치들, 모듈들 등은 하드웨어 회로, 예를 들면, CMOS(complementary metal oxide)형 반도체로 된 논리회로, 펌웨어, 소프트웨어 및/또는 하드웨어, 펌웨어의 조합, 및/또는 기계로 독출이 가능한 매체에 구현된 소프트웨어를 이용하여 구현되고 동작 될 수도 있다. 예를 들면, 다양한 전기적 구성과 방법들이 트랜지스터들, 로직 게이트들, 및 주문형 집적회로(ASIC)와 같은 전기회로들을 이용하여 구현될 수도 있다.

도면

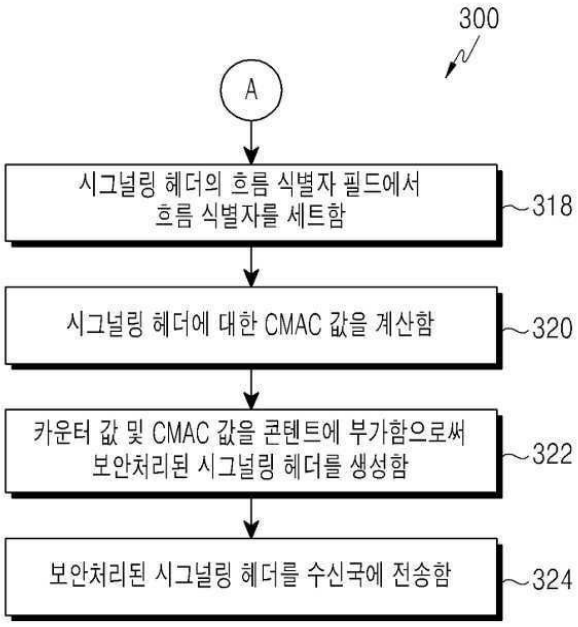
도면1



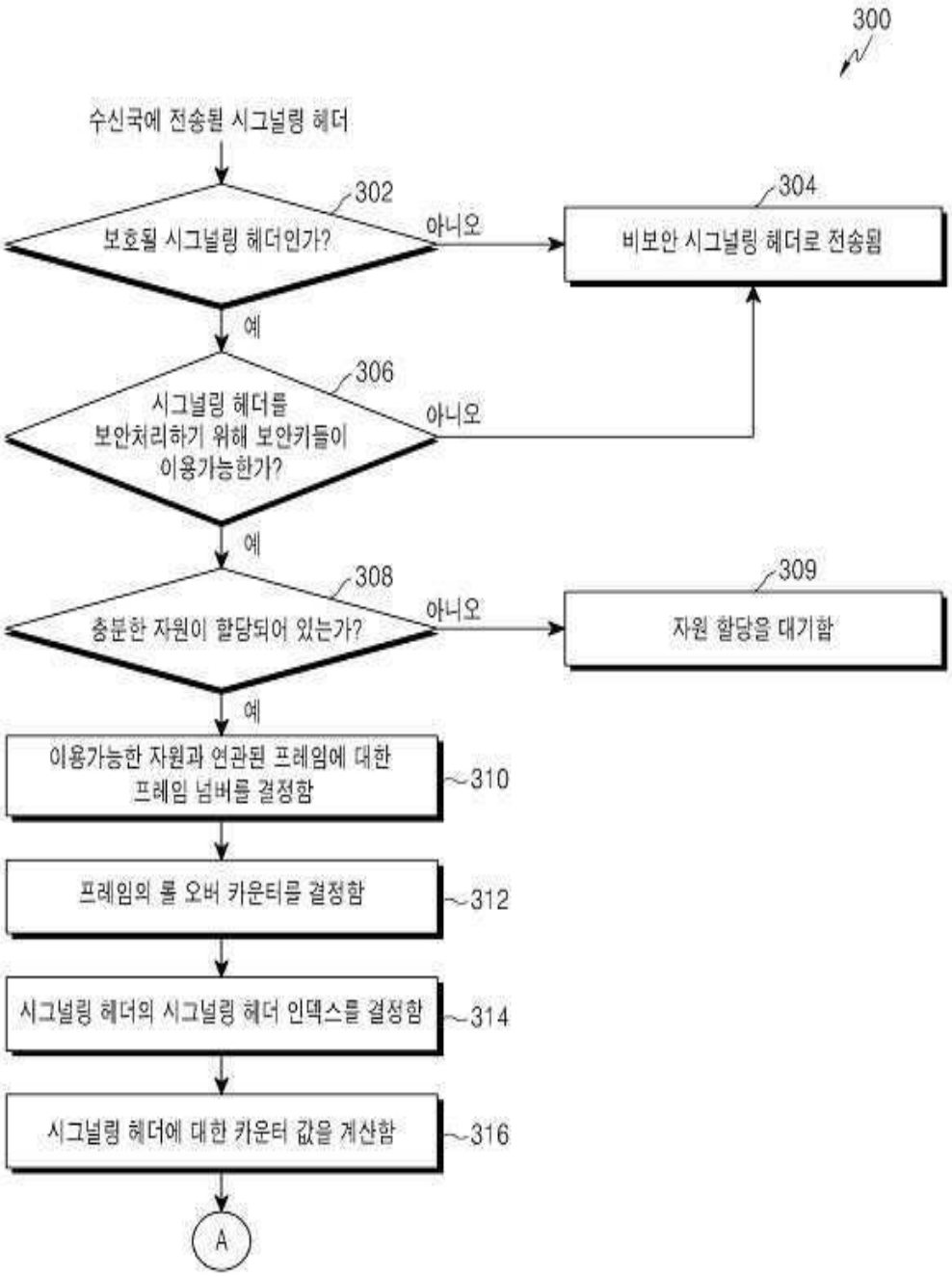
도면2


200
인증키로부터 프리-키를 생성함
202
제1유형 제어정보 및 제2유형 제어정보에 대한 상향 및 하향 보안키들을 유도함
204
206
제1유형의 제어정보에 대한 제1유형의 카운터를 계산함
208
제1유형의 제어정보에 대한 제1유형의 CMAC를 계산함
210
제1유형의 CMAC, 제1유형의 카운터 및 보안키들을 이용하여 제1유형의 제어정보를 보안처리함
212
제2유형의 제어정보에 대한 제2유형의 카운터를 계산함
214
제2유형의 제어정보에 대한 제2유형의 CMAC를 계산함
216
제2유형의 CMAC, 제2유형의 카운터 및 보안키들을 이용하여 제1유형의 제어정보를 보안처리함

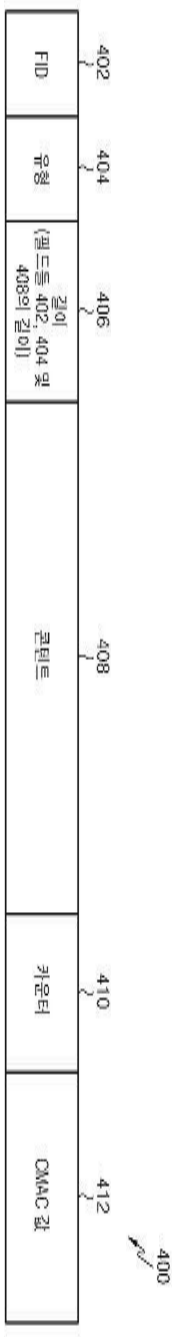
도면3a


300
A
시그널링 헤더의 흐름 식별자 필드에서 흐름 식별자를 세트함
318
시그널링 헤더에 대한 CMAC 값을 계산함
320
카운터 값 및 CMAC 값을 콘텐트에 부가함으로써 보안처리된 시그널링 헤더를 생성함
322
보안처리된 시그널링 헤더를 수신국에 전송함
324

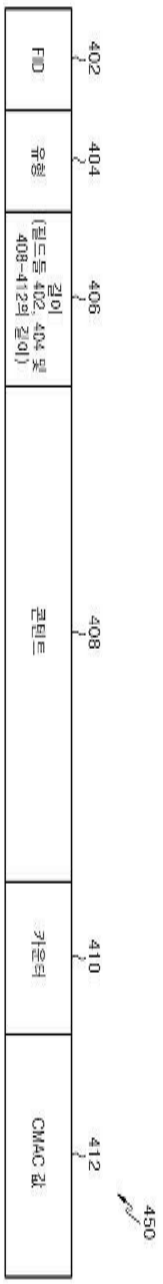
도면3b


300
수신국에 전송된 시그널링 헤더
302
보호될 시그널링 헤더인가?
아니오
304
비보안 시그널링 헤더로 전송됨
예
306
시그널링 헤더를 보안처리하기 위해 보안키들이 이용가능한가?
아니오
예
308
충분한 자원이 할당되어 있는가?
아니오
309
자원 할당을 대기함
예
이용가능한 자원과 연관된 프레임에 대한 프레임 넘버를 결정함
310
프레임의 롤 오버 카운티를 결정함
312
시그널링 헤더의 시그널링 헤더 인덱스를 결정함
314
시그널링 헤더에 대한 카운터 값을 계산함
316
A

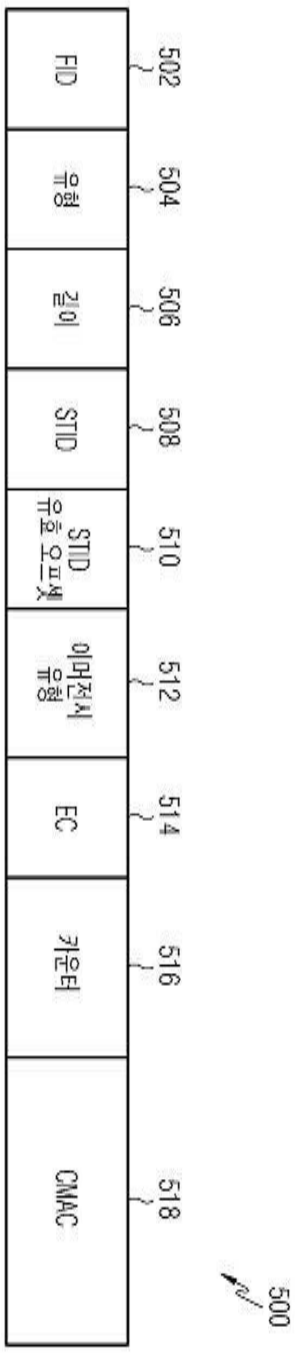
도면4a


FID
402
유형
404
길이
(필드들 402, 404 및
408의 길이)
406
콘텐트
408
카운터
410
CMAC 값
412
400

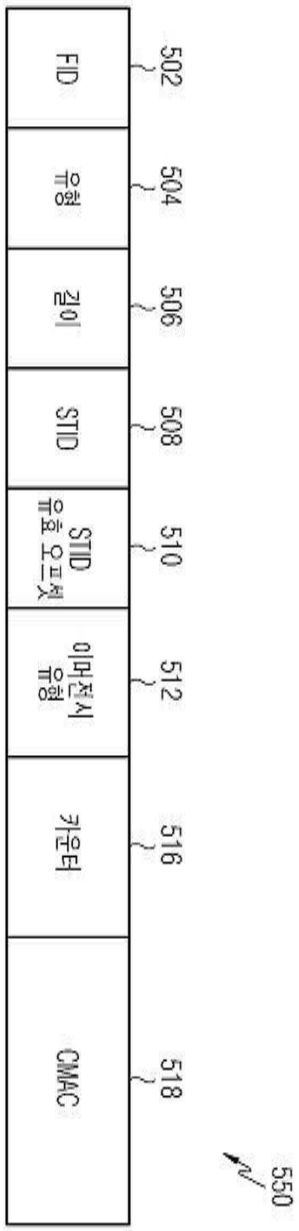
도면4b


FID
402
유형
404
길이
(필드들 402, 404 및 408-412의 길이)
406
콘텐트
408
카운터
410
CMAC 값
412
450

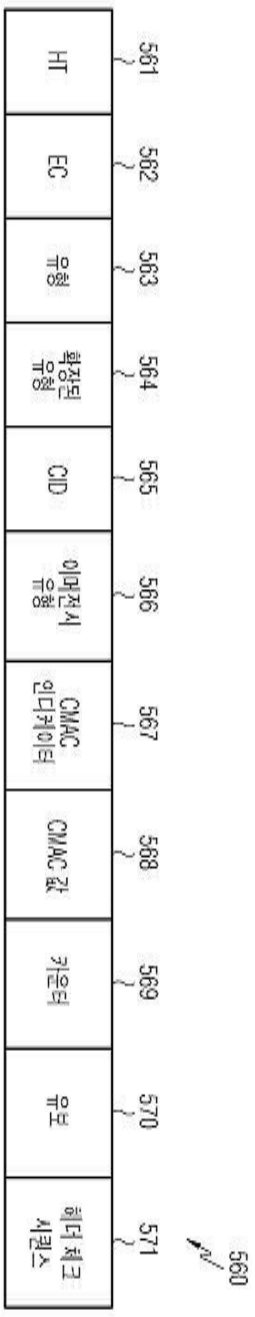
도면5a


FID
502
유형
504
길이
506
STID
508
STID 유효 오프셋
510
이머전시 유형
512
EC
514
카운터
516
CMAC
518
500

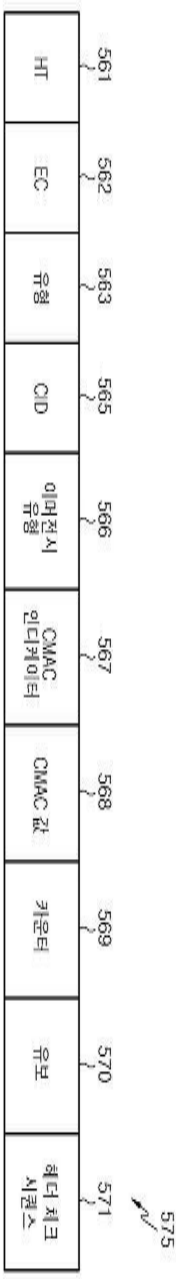
도면5b


FID
502
유형
504
길이
506
STID
508
STID 유효 오프셋
510
이머전시 유형
512
카운터
516
CMAC
518
550

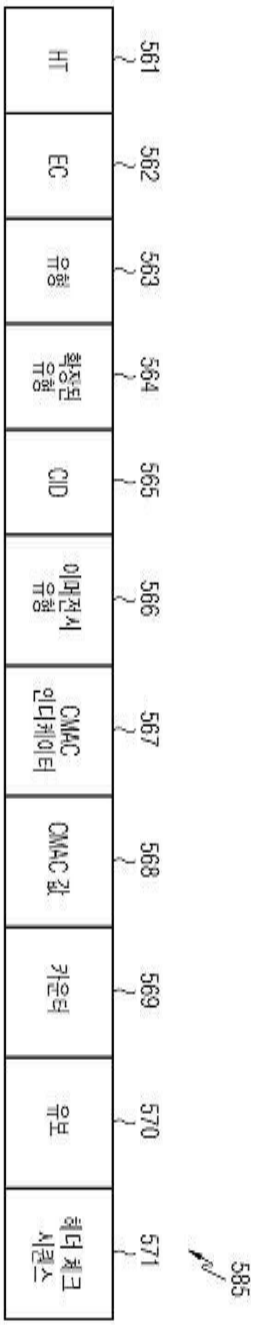
도면5c


560
561
HT
562
EC
563
유형
564
확장된 유형
565
CID
566
이미전시 유형
567
CMAC 인디케이터
568
CMAC 값
569
카운터
570
유보
571
헤더 체크 시퀀스

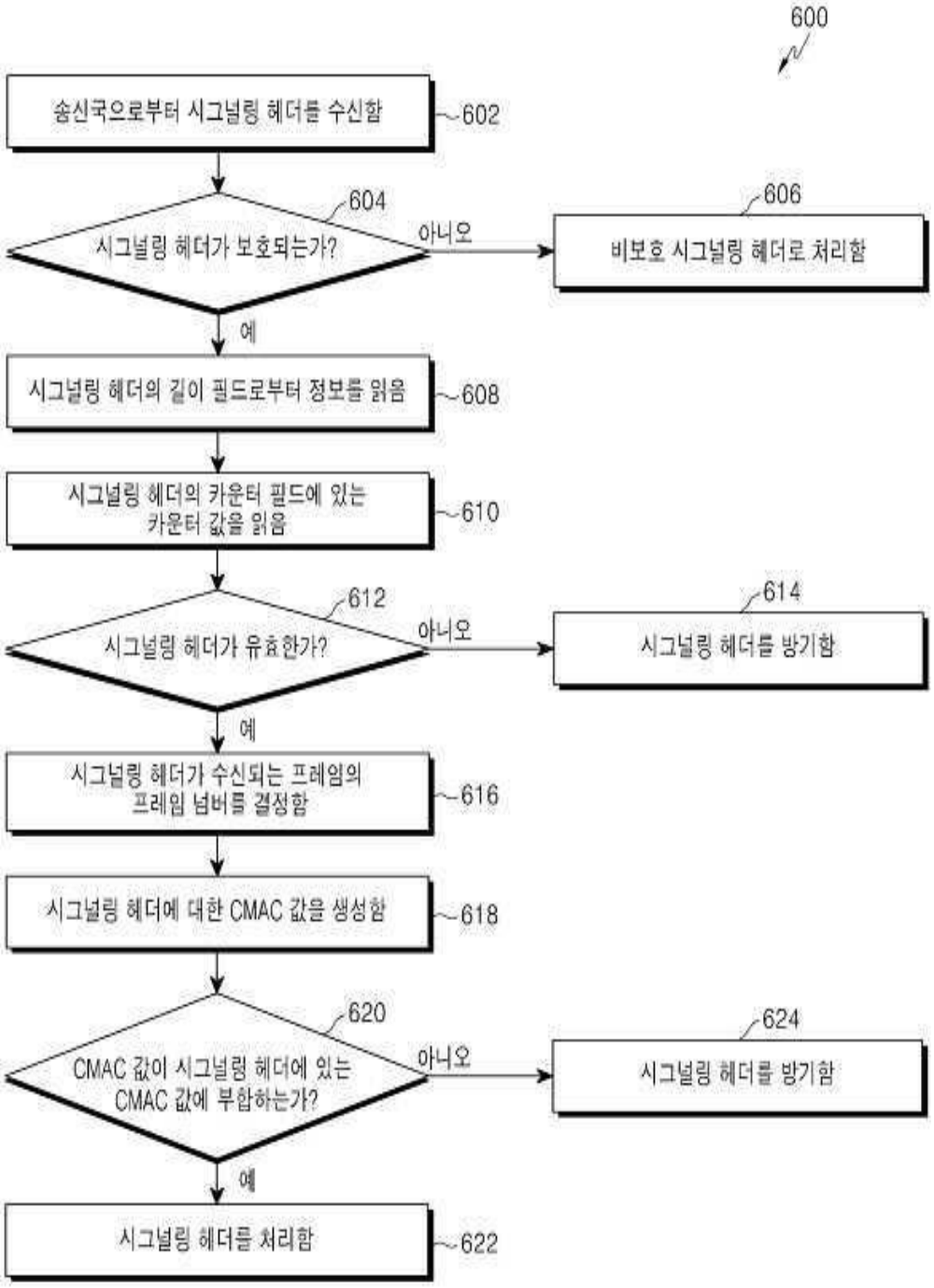
도면5d


HT
561
EC
562
유형
563
CID
565
애머전시 유형
566
CMAC 인디케이터
567
CMAC 값
568
카운터
569
유보
570
헤더 체크 시퀀스
571
575

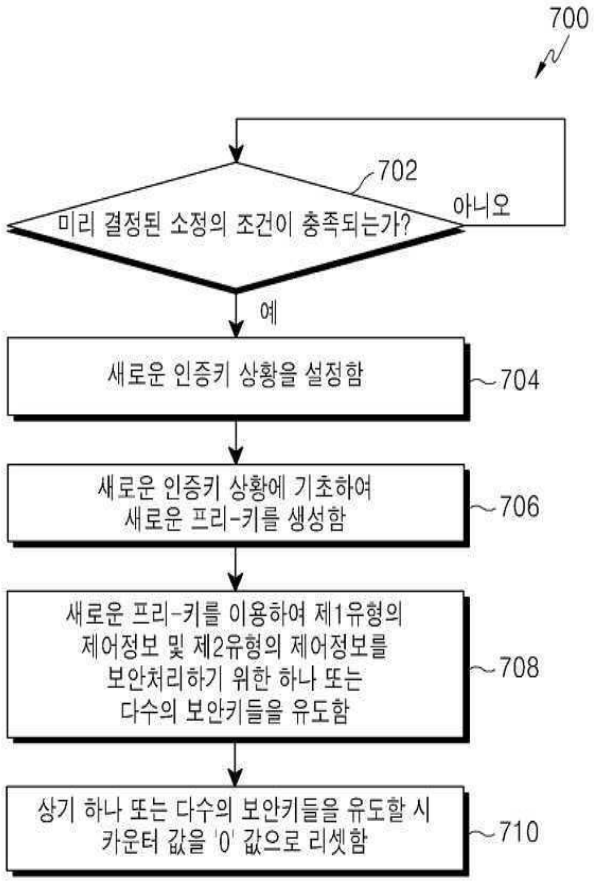
도면5e


HT
561
EC
562
유형
563
확장된 유형
564
CID
565
이머전시 유형
566
CMAC 인디케이터
567
CMAC 값
568
카운터
569
유보
570
헤더 체크 시퀀스
571
585

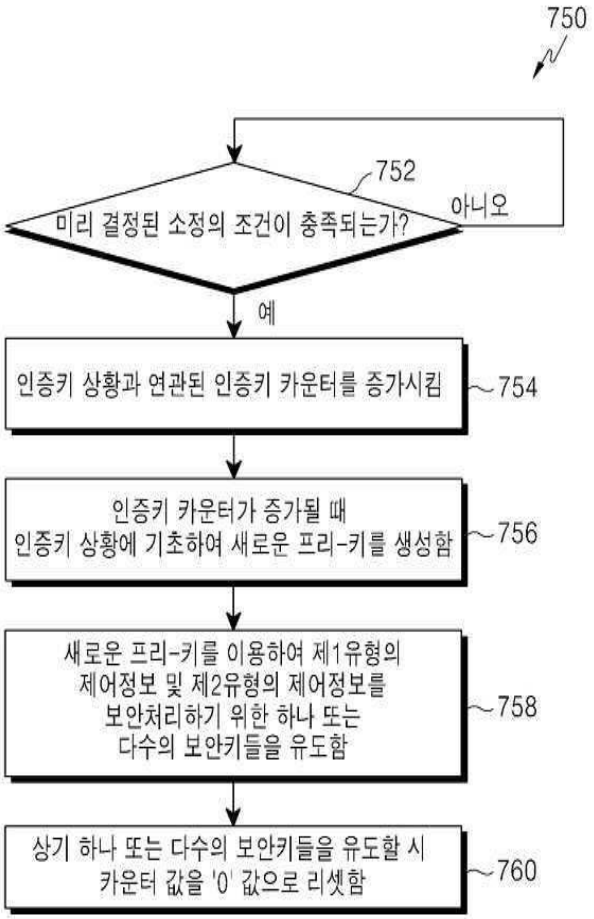
도면6


600
송신국으로부터 시그널링 헤더를 수신함
602
시그널링 헤더가 보호되는가?
604
아니오
606
비보호 시그널링 헤더로 처리함
예
시그널링 헤더의 길이 필드로부터 정보를 읽음
608
시그널링 헤더의 카운터 필드에 있는 카운터 값을 읽음
610
시그널링 헤더가 유효한가?
612
아니오
614
시그널링 헤더를 방기함
예
시그널링 헤더가 수신되는 프레임의 프레임 넘버를 결정함
616
시그널링 헤더에 대한 CMAC 값을 생성함
618
CMAC 값이 시그널링 헤더에 있는 CMAC 값에 부합하는가?
620
아니오
624
시그널링 헤더를 방기함
예
시그널링 헤더를 처리함
622

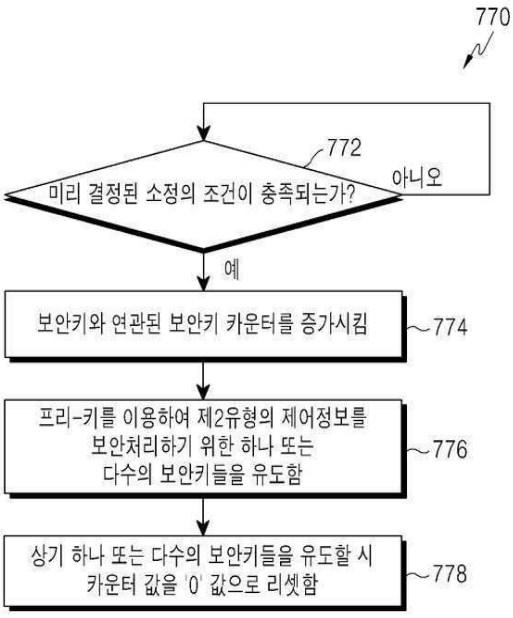
도면7a


700
702
미리 결정된 소정의 조건이 충족되는가?
아니오
예
새로운 인증키 상황을 설정함
704
새로운 인증키 상황에 기초하여
새로운 프리-키를 생성함
706
새로운 프리-키를 이용하여 제1유형의
제어정보 및 제2유형의 제어정보를
보안처리하기 위한 하나 또는
다수의 보안키들을 유도함
708
상기 하나 또는 다수의 보안키들을 유도할 시
카운터 값을 '0' 값으로 리셋함
710

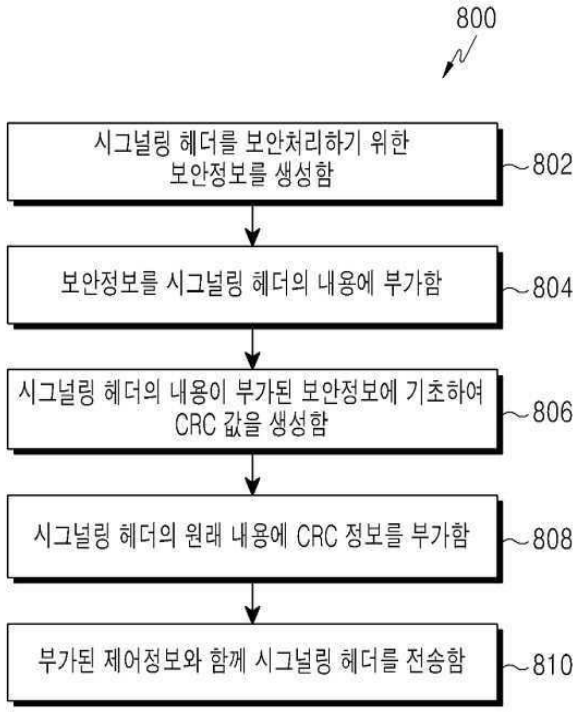
도면7b


750
752
미리 결정된 소정의 조건이 충족되는가?
아니오
예
인증키 상황과 연관된 인증키 카운터를 증가시킴
754
인증키 카운터가 증가될 때
인증키 상황에 기초하여 새로운 프리-키를 생성함
756
새로운 프리-키를 이용하여 제1유형의
제어정보 및 제2유형의 제어정보를
보안처리하기 위한 하나 또는
다수의 보안키들을 유도함
758
상기 하나 또는 다수의 보안키들을 유도할 시
카운터 값을 '0' 값으로 리셋함
760

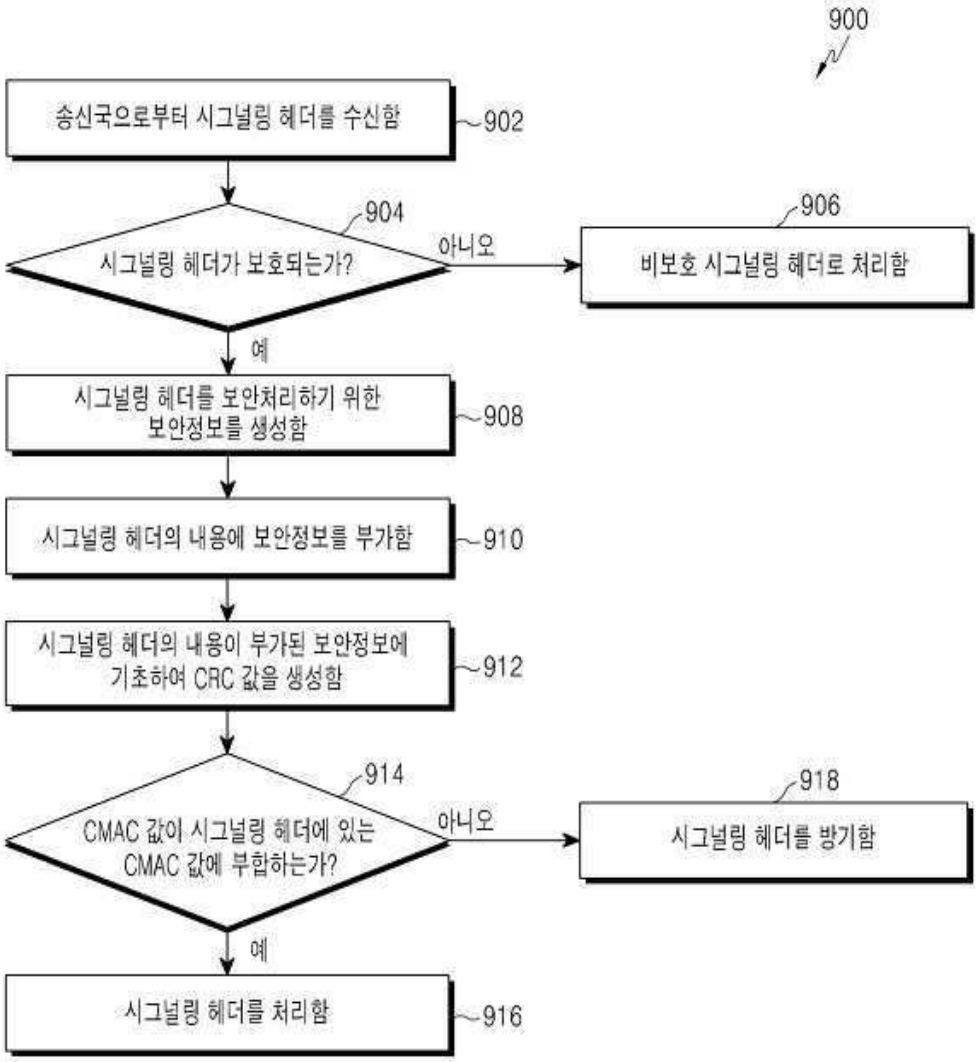
도면7c


770
772
미리 결정된 소정의 조건이 충족되는가?
아니오
예
보안키와 연관된 보안키 카운터를 증가시킴
774
프리-키를 이용하여 제2유형의 제어정보를
보안처리하기 위한 하나 또는
다수의 보안키들을 유도함
776
상기 하나 또는 다수의 보안키들을 유도할 시
카운터 값을 '0' 값으로 리셋함
778

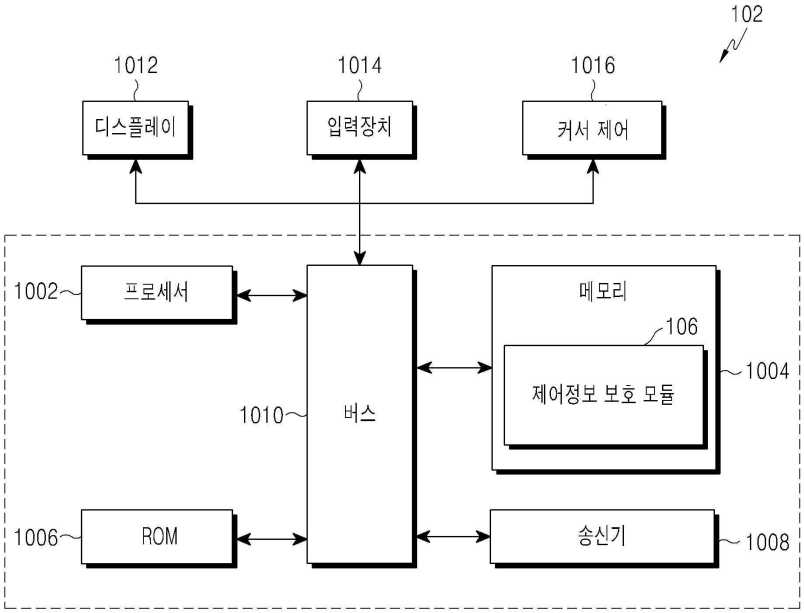
도면8


800
시그널링 헤더를 보안처리하기 위한 보안정보를 생성함
802
보안정보를 시그널링 헤더의 내용에 부가함
804
시그널링 헤더의 내용이 부가된 보안정보에 기초하여 CRC 값을 생성함
806
시그널링 헤더의 원래 내용에 CRC 정보를 부가함
808
부가된 제어정보와 함께 시그널링 헤더를 전송함
810

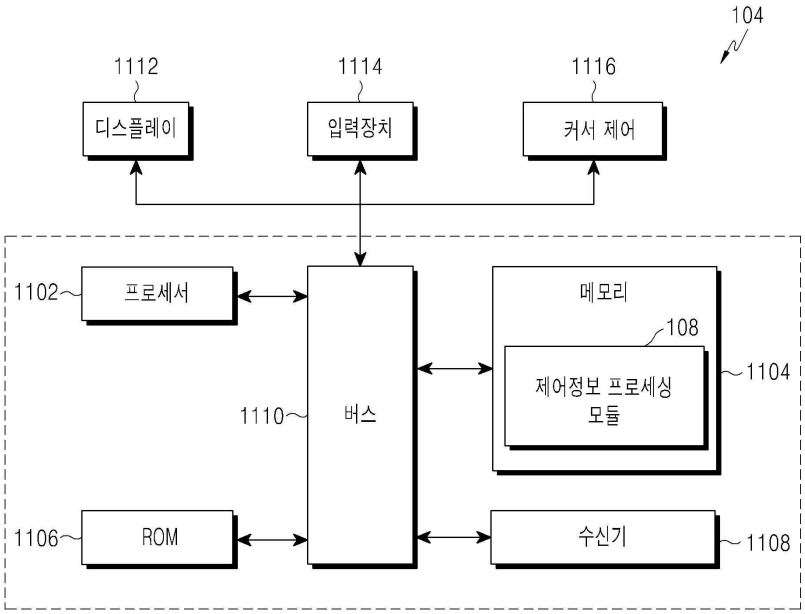
도면9


900
송신국으로부터 시그널링 헤더를 수신함
902
904
시그널링 헤더가 보호되는가?
아니오
906
비보호 시그널링 헤더로 처리함
예
시그널링 헤더를 보안처리하기 위한 보안정보를 생성함
908
시그널링 헤더의 내용에 보안정보를 부가함
910
시그널링 헤더의 내용이 부가된 보안정보에 기초하여 CRC 값을 생성함
912
914
CMAC 값이 시그널링 헤더에 있는 CMAC 값에 부합하는가?
아니오
918
시그널링 헤더를 방기함
예
시그널링 헤더를 처리함
916

도면10



도면11



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제1항 9번째줄

【변경전】

암호 키 (TEK prekey)

【변경후】

암호 키 (CMAC-TEK prekey)

【직권보정 2】

【보정항목】 청구범위
【보정세부항목】 청구항 제9항 7번째줄
【변경전】
암호 키 (TEK prekey)
【변경후】
암호 키 (CMAC-TEK prekey)

【직권보정 3】
【보정항목】 청구범위
【보정세부항목】 청구항 제17항 9번째줄
【변경전】
암호 키 (TEK prekey)
【변경후】
암호 키 (CMAC-TEK prekey)

【직권보정 4】
【보정항목】 청구범위
【보정세부항목】 청구항 제19항 6번째줄
【변경전】
상기 인증 코드를
【변경후】
인증 코드를

【직권보정 5】
【보정항목】 청구범위
【보정세부항목】 청구항 제9항 3번째줄
【변경전】
상기 인증 코드를
【변경후】
인증 코드를

【직권보정 6】
【보정항목】 청구범위
【보정세부항목】 청구항 제16항 1번째줄
【변경전】
9항에 있어서
【변경후】
제9항에 있어서

【직권보정 7】
【보정항목】 청구범위
【보정세부항목】 청구항 제19항 8번째줄
【변경전】
암호 키 (TEK prekey)
【변경후】
암호 키 (CMAC-TEK prekey)