(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0103721
(43) 공개일자 2010년09월27일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)
H04L 12/28 (2006.01)
(21) 출원번호 10-2010-7018865
(22) 출원일자(국제출원일자) 2009년02월16일
심사청구일자 2010년08월25일
(85) 번역문제출일자 2010년08월25일
(86) 국제출원번호 PCT/US2009/034184
(87) 국제공개번호 WO 2009/108523
국제공개일자 2009년09월03일
(30) 우선권주장
12/037,516 2008년02월26일 미국(US)

(71) 출원인
모토로라 인코포레이티드
미국, 일리노이 60196, 샤움버그, 이스트 앨공퀸 로드 1303
(72) 발명자
메트케, 안소니, 알.
미국 60563 일리노이주 네이퍼빌 터트힐 로드 1108
루이스, 아담, 씨.
미국 60089 일리노이주 버팔로 그로브 채담 써클 477
포포비치, 조지
미국 60067 일리노이주 팔라틴 사우쓰 켄싱톤 코트 347
(74) 대리인
양영준, 백만기, 정은진

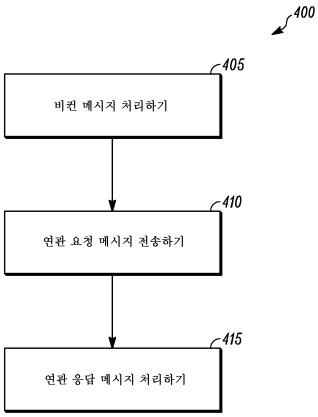
전체 청구항 수 : 총 20 항

(54) 무선 통신 네트워크에서 노드들의 상호 인증을 위한 방법 및 시스템

(57) 요 약

제공되는 방법은 무선 통신 네트워크에서 노드의 상호 인증을 가능하게 한다. 본 방법은 제1 노드에서 제2 노드로부터 수신되는 비컨 메시지를 처리하는 단계(단계 405)를 포함하는데, 이 경우 비컨 메시지는 제1 난스값을 구비한다. 다음으로는, 제1 노드의 인증서, 제1 인증 데이터 서명 블록, 및 제2 난스값을 구비하는 연관 요청 메시지가 제1 노드로부터 제2 노드쪽으로 전송된다(단계 410). 그 다음, 제2 노드는 제1 노드의 인증서에 대한 서명을 확인할 수 있고 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있다. 다음으로는, 제2 노드로부터 수신되는 연관 응답 메시지가 제1 노드에서 처리되는데(단계 415), 그에 의해 제1 노드는 제2 노드의 인증서에 대한 서명을 확인하고 제2 인증 데이터 서명 블록에 대한 서명을 확인한다.

대 표 도 - 도4



특허청구의 범위

청구항 1

무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하는 방법으로서,

상기 제1 노드에서 상기 제2 노드로부터 수신되는 비컨 메시지를 처리하는 단계 - 상기 비컨 메시지는 제1 난스값(nonce value)을 포함함 -;

상기 제1 노드에서 상기 제2 노드로 상기 제1 노드의 인증서, 제1 인증 데이터 서명 블록, 및 제2 난스값을 포함하는 연관 요청 메시지를 전송하는 단계 - 그에 의해 상기 제2 노드는 상기 제1 노드의 인증서에 대한 서명을 확인할 수 있고 상기 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있음 -; 및

상기 제1 노드에서, 상기 제2 노드로부터 수신되는 연관 응답 메시지를 처리하는 단계 - 상기 연관 응답 메시지는 상기 제2 노드의 인증서, 제2 인증 데이터 서명 블록, 및 상기 제1 노드의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터(radom keying data)를 구비하고, 그에 의해 상기 제1 노드는 상기 제2 노드의 인증서에 대한 서명을 확인하고 상기 제2 인증 데이터 서명 블록에 대한 서명을 확인함 -

를 포함하는 상호 인증 방법.

청구항 2

제1항에 있어서,

상기 제1 인증 데이터 서명 블록은, 상기 제1 노드의 MAC(medium access control) 어드레스, 상기 제2 노드의 MAC 어드레스, 상기 제2 노드에 의해 발생되는 난스값, 또는 텍스트 스트링 중 적어도 하나를 포함하는 상호 인증 방법.

청구항 3

제1항에 있어서,

상기 연관 요청 메시지는, 상기 제2 노드가 신뢰 앵커 리스트(trust anchor list) 또는 AP(access point) 인증서 중 적어도 하나를 상기 연관 응답 메시지에 포함해야 한다는 요청을 포함하는 상호 인증 방법.

청구항 4

제1항에 있어서,

상기 비컨 메시지는 또한, 공개 키를 포함하는 상호 인증 방법.

청구항 5

제1항에 있어서,

상기 연관 요청 메시지는 또한, 상기 제2 노드의 공개 키를 사용해 암호화된 임시 변조 데이터(provisional keying data)를 포함하는 상호 인증 방법.

청구항 6

제5항에 있어서,

상기 연관 응답 메시지를 처리하는 단계는, 임시 변조 데이터를 발생시키는 단계, 및 원격 변조 데이터(remote keying data) 및 상기 임시 변조 데이터 양자로부터 공유 비밀을 유도하는 단계를 더 포함하는 상호 인증 방법.

청구항 7

제6항에 있어서,

상기 임시 변조 데이터 및 상기 원격 변조 데이터는 DH(Diffie-Hellman) 파라미터들을 포함하는 상호 인증

방법.

청구항 8

제1항에 있어서,

상기 제1 무작위 변조 데이터는 상기 제2 노드의 비밀 키에 의해 서명되는 상호 인증 방법.

청구항 9

제1항에 있어서,

상기 제1 무작위 변조 데이터는 상기 제2 노드의 PMK(pairwise master key)를 포함하는 상호 인증 방법.

청구항 10

제9항에 있어서,

상기 연관 요청 메시지는 제3 난스값을 포함하고, 상기 연관 응답 메시지는 제4 난스값을 포함하는 상호 인증 방법.

청구항 11

제1항에 있어서,

상기 비컨 메시지는 또한, 상기 제2 노드(AP)의 공개 키 인증서를 포함하는 상호 인증 방법.

청구항 12

무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 시스템으로서,

상기 제1 노드에서, 상기 제2 노드로부터 수신되는 비컨 메시지를 처리하기 위한 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들을 갖는 컴퓨터 판독 가능 매체 - 상기 비컨 메시지는 제1 난스값을 포함함 -;

상기 제1 노드에서 상기 제2 노드로 상기 제1 노드의 인증서, 제1 인증 데이터 서명 블록, 및 제2 난스값을 포함하는 연관 요청 메시지를 전송하기 위한 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들을 갖는 컴퓨터 판독 가능 매체 - 그에 의해 상기 제2 노드는 상기 제1 노드의 인증서에 대한 서명을 확인할 수 있고 상기 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있음 -; 및

상기 제1 노드에서, 상기 제2 노드로부터 수신되는 연관 응답 메시지를 처리하기 위한 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들을 갖는 컴퓨터 판독 가능 매체 - 상기 연관 응답 메시지는 상기 제2 노드의 인증서, 제2 인증 데이터 서명 블록, 및 상기 제1 노드의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터를 구비하고, 그에 의해 상기 제1 노드는 상기 제2 노드의 인증서에 대한 서명을 확인하고 상기 제2 인증 데이터 서명 블록에 대한 서명을 확인함 -

를 포함하는 상호 인증 시스템.

청구항 13

제12항에 있어서,

상기 제1 인증 데이터 서명 블록은 상기 제1 노드의 MAC(medium access control) 어드레스, 상기 제2 노드의 MAC 어드레스, 상기 제2 노드에 의해 발생되는 난스값, 또는 텍스트 스트링 중 적어도 하나를 포함하는 상호 인증 시스템.

청구항 14

제12항에 있어서,

상기 비컨 메시지는 또한, 상기 제2 노드에 의해 신뢰되는 상기 무선 통신 네트워크에서의 노드들에 대한 ID(identifications)를 포함하는 상호 인증 시스템.

청구항 15

제12항에 있어서,

상기 비컨 메시지는 또한, 공개 키를 포함하는 상호 인증 시스템.

청구항 16

제12항에 있어서,

상기 연관 응답 메시지는 또한, 상기 제2 노드의 공개 키를 이용하여 암호화된 임시 변조 데이터를 포함하는 상호 인증 시스템.

청구항 17

제16항에 있어서,

상기 연관 응답 메시지를 처리하는 것은, 임시 변조 데이터를 발생시키는 것, 및 원격 변조 데이터 및 상기 임시 변조 데이터 양자로부터 공유 비밀을 유도하는 것을 더 포함하는 상호 인증 시스템.

청구항 18

제12항에 있어서,

상기 제1 무작위 변조 데이터는 상기 제2 노드의 비밀 키에 의해 서명되는 상호 인증 시스템.

청구항 19

제12항에 있어서,

상기 제1 무작위 변조 데이터는 상기 제2 노드의 PMK(pairwise master key)를 포함하는 상호 인증 시스템.

청구항 20

제12항에 있어서,

상기 연관 요청 메시지는 제3 난스값을 포함하고, 상기 연관 응답 메시지는 제4 난스값을 포함하는 상호 인증 시스템.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 무선 통신 네트워크에 관한 것으로서, 좀더 구체적으로는, 네트워크 노드 사이에서 빠른 상호 인증을 제공하는 것에 관한 것이다.

배 경 기 술

[0002] 대다수 무선 통신 시스템은 사용자 노드들 사이의 안정적인 통신 뿐만 아니라 독립적인 모바일 사용자의 빠른 전개(rapid deployment)를 요구한다. MANET(Mobile Ad Hoc Network)들과 같은, 메쉬 네트워크들은 제한된 대역폭들을 가진 무선 링크들을 통해 서로 통신하는 휴대용 장치들의 자기 구성 자동 수집(self-configuring autonomous collection)들에 기초한다. 메쉬 네트워크는 여러개의 홉을 가로질러 노드들에 도달될 수 있게 하는 것에 의해 범위 확장을 제공하도록 분산 방식으로 조직된 무선 노드들 또는 장치들의 수집이다. 그에 따라, 메쉬 네트워크에서는, 소스 노드에 의해 송신되는 통신 패킷들이 목적지 노드에 도달하기 전에 하나 이상의 중개 노드를 통해 중계될 수 있다. 메쉬 네트워크들은, 만약에 있다고 하더라도, 중요한 지원 인프라스트럭처를 포함하지 않는 임시적인 패킷 라디오 네트워크들로서 활용될 수 있다. 일부 메쉬 네트워크에서는, 고정된 기지국들을 이용하는 대신에, 각각의 사용자 노드가 다른 사용자 노드들을 위한 라우터로서 동작함으로써, 저렴한 비용으로 신속하게 설정될 수 있고 상당히 내고장성인(highly fault tolerant), 확장된 네트워크 커버리지를 가능하게 할 수 있다. 일부 메쉬 네트워크에서는, 특수한 무선 라우터들이 중개 인프라스트럭처 노드들로서 사용될 수도 있다. 이와 같이, 무선 노드에 유선 백홀 또는 WAN(wide area network)으로의 액세스를 제공하는, 게이트웨이들 또는 포털들로도 공지된, IAP(intelligent access point)들을 사용해 거대 네트워크들이 실현될 수 있다.

[0003] 메쉬 네트워크들은, 예를 들어, 경찰과 소방 인력, 군사 애플리케이션들, 산업 시설 및 건설 현장을 지원하는 응급 서비스들을 포함하는 다양한 환경에서 중요한 통신 서비스를 제공할 수 있다. 또한, 메쉬 네트워크들은 가정에서, 기본적인 전기 통신 또는 광대역 인프라스트럭처가 거의 없거나 전혀 없는 지역에서, 그리고 고속 서비스들을 위한 수요를 갖춘 다른 지역들(예를 들어, 대학, 통합업무단지, 및 빽빽한 도시 지역)에서 통신 서비스들을 제공하는데 사용된다.

[0004] 그러나, 메쉬 통신 네트워크에서 노드들 사이의 안전한 통신들을 확립하는 것은 복잡할 수 있다. 셀룰러폰들과 같은 기존의 모바일 장치들은 대체로 인프라스트럭처 기반의 인증 프로세스들을 사용해 통신 보안을 획득한다. 장치들은 일반적으로 인증 서버에 접속되는, 기지국과 같은, AP(Access Point)를 통해 인증된다. 인증 요청은, 예를 들어, EAPOL(EAP Over Local Area Network) 패킷들을 구비하는 EAP(Extensible Authentication Protocol)를 사용해 전송될 수 있다. 인증 프로세스는, EAP Start 패킷으로 시작해 EAP Success 메시지 패킷이나 EAP Failure 메시지 패킷으로 종료하는, 전송되고 수신되는 몇가지 EAPOL 패킷을 포함한다. 인증 서버는 인증되고 있는 (통상적으로 탄원자라고 하는) 모바일 장치의 인증 자격 증명들을 저장한다. 또한, 인증 서버는 국지적으로 저장되지 않는 탄원자 인증 자격 증명들을 획득하기 위해 다른 인증 서버들에도 접속될 수 있다.

[0005] 인프라스트럭처 기반의 모바일 네트워크들에서는, 대체로 단일 AP가 AP 범위내의 모든 탄원자들을 위한 인증 프로세스를 핸들링하는 집중 절차(centralized procedure)가 수반된다. 예를 들어, ANSI/IEEE(American National Standards Institute/Institute of Electrical and Electronics Engineers) 802.1X 또는 ANSI/IEEE 802.11i 표준을 준수하는 종래 시스템은 그러한 집중 절차를 이용한다(http://standards.ieee.org/getieee802/index.html를 참고하거나 IEEE, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855-1331, USA의 IEEE에 연락하기). 그러나, 모든 탄원자가 AP를 통해서만 인증될 수 있기 때문에, 흔히 IAP(Intelligent AP)의 무선 범위 밖에서 동작하는 노드들을 갖는 무선 메쉬 통신 네트워크들에서 그러한 집중 절차는 비실용적이다. 이와 같이, 무선 메쉬 통신 네트워크들은 대체로 인접한 모든 네트워크 노드들 사이에서 수행되는 복잡한 상호 인증 방법을 포함하고, 이는 네트워크 노드들의 상당한 시간 및 프로세서 리소스들을 소비할 수 있다.

[0006] 따라서, 무선 통신 네트워크에서 노드들을 상호 인증하기 위한 개선된 방법 및 시스템이 필요하다.

발명의 내용

도면의 간단한 설명

[0007] 유사한 참조 번호가 별도 도면 전체에 걸쳐 동일하거나 기능적으로 유사한 구성 요소를 참조하는 첨부 도면은, 다음의 상세한 설명과 함께, 본 명세서에 통합되어 명세서의 일부를 형성하고, 청구된 발명을 포함하는 개념의 실시예를 추가 예시하며 그러한 실시예의 다양한 원리와 이점을 설명하는 기능을 한다.

도 1은, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 방법을 예시하는 메시지 순서도(message sequence chart)이다.

도 2는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 추가 방법을 예시하는 메시지 순서도이다.

도 3은, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 다른 방법을 예시하는 메시지 순서도이다.

도 4는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 방법을 예시하는 일반적인 흐름도이다.

도 5는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드 또는 제2 노드로서 기능할 수 있는 무선 통신 장치의 컴포넌트를 예시하는 블록도이다.

당업자라면, 도면들의 구성 요소들이 간략화와 명료화를 위해 예시되며, 반드시 실제 비율대로 도시되는 것은 아니라는 점을 알 수 있을 것이다. 예를 들어, 도면의 구성 요소 중 일부의 치수는 본 발명의 실시예에 대한 이해 증진을 돕기 위해 다른 구성 요소들에 비해 강조될 수 있다.

장치 및 방법 컴포넌트들은, 여기에서의 설명 이점을 갖춘 당업자라면 쉽게 알 수 있을 세부 사항으로써 본 명세서를 불명료하게 하지 않기 위해 본 발명의 실시예를 이해하는 것과 관련된 특정 세부 사항들만을

나타내면서, 통상의 심볼들에 의해 도면에 적절하게 표현되었다.

발명을 실시하기 위한 구체적인 내용

[0008] 본 발명의 일부 실시예에 따르면, 본 발명은 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 방법이다. 본 방법은 제2 노드로부터 수신되는 비컨 메시지를 제1 노드에서 처리하는 단계를 포함하는데, 이 경우 비컨 메시지는 제1 난스값(nonce value)을 구비한다. 다음으로는, 제1 노드의 인증서, 제1 인증 데이터 서명 블록(first signed block of authentication data), 및 제2 난스값을 구비하는 연관 요청 메시지가 제1 노드로부터 제2 노드쪽으로 전송된다. 그 다음, 제2 노드는 제1 노드의 인증서에 대한 서명을 확인할 수 있고 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있다. 다음으로는, 제1 노드에서 제2 노드로부터 수신되는 연관 응답 메시지가 처리된다. 연관 응답 메시지는 제2 노드의 인증서, 제2 인증 데이터 서명 블록, 및 제1 노드의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터(first random keying data)를 구비하고, 그에 의해 제1 노드는 제2 노드의 인증서에 대한 서명을 확인하고 제2 인증 데이터 서명 블록에 대한 서명을 확인한다.

[0009] 이와 같이, 앞서 설명된 방법에 따르면, 본 발명의 일부 실시예는 네트워크 노드들 사이의 빠른 상호 인증 및 키 교환을 가능하게 한다. 무선 통신 네트워크에서의 2개 노드가 서로를 발견하는 시점과 그들이 안전하게 통신할 수 있는 시점 사이의 "첨부 시주기(attachment time period)"는 대체로 최소화되어야 한다. 예를 들어, 제한된 셀 크기들을 가진 고도의 모바일 동적 네트워크들과 같은 일부 환경에서, 그러한 첨부 시주기는 100밀리초 미만일 것이 요구될 수 있다. 그러나, 종래 기술에 따른 2-당사자 인증 처리(two-party authentication processes)는 간혹 당사자들 사이에서 11개만큼이나 많은 메시지가 교환될 것을 요구한다. 예를 들어, 그러한 메시지들은 1개의 비컨 메시지, 2개의 연관 메시지, 4개의 TLS(Transport Layer Security) 메시지, 및 4단계 핸드쉐이크(four-way handshake)에서의 4개 메시지를 포함할 수 있다. 그렇게 많은 수의 메시지를 교환하는 것은 시간 소모적일 수 있고, 지나치게 긴 첨부 시기를 초래할 수 있다.

[0010] 도 1을 참조하면, 메시지 순서도는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크(100)에서 제1 노드(105)와 제2 노드(110)를 상호 인증하기 위한 방법을 예시한다. 예를 들어, 무선 통신 네트워크(100)는 무선 메쉬 네트워크이고, 제1 노드(105) 및 제2 노드(110)는 서로를 발견하여 2-당사자 인증 처리를 완료해야 한다고 하자. 예시를 위해, 제1 노드(105)가 연관 요청을 개시하며 그에 따라 STA(station)를 표현하고, 제2 노드(115)가 연관 요청을 수신하며 그에 따라 AP(access point)를 표현한다고 하자. 먼저, 제1 노드(105) 또는 제2 노드(110) 중 어느 하나가 비컨 메시지를 전송할 수 있지만, 제1 난스값(ANonce)을 포함하는 비컨 메시지(115)는 제2 노드(110)로부터 제1 노드(105)쪽으로 전송된다.

[0011] 당업자라면 알 수 있는 바와 같이, 난스값은 이전 통신이 재생 공격들(replay attacks)에 재사용될 수 없다는 것을 보장하는데 사용되는 난수 또는 의사 난수(pseudo-random number)이다. 난스값을 구현하는 통상적인 방법들은 (프로토콜의 각각의 반복을 위해 증분되는 단조 증가 수인) 시퀀스 번호, (재사용 확률이 충분히 작도록 선택되는) 임의의 큰 수, 또는 타임스탬프 값을 사용하는 단계를 포함한다.

[0012] 더 나아가, "비컨"이라는 용어는 다른 노드들에게, 예를 들어, 동작 파라미터들, 다른 상태 정보, 설정들, 또는 제1 노드의 존재를 알리기 위해 제1 노드에 의해 전송되는 주기적인 자발적 메시지(periodic unsolicited message)를 지시하는데 사용된다. 또한, "비컨"이라는 용어는 동작 파라미터들, 다른 상태 정보, 설정들, 또는 노드의 존재와 같은 정보를 위한 요청에 대한, 폴 응답(poll response)과 같은, 요청 응답(solicited response)을 포함한다.

[0013] 제1 노드(105)가 제2 노드(110)와 결합하고자 한다면, 제1 노드(105)는 제2 노드(110)쪽으로 연관 요청 메시지(120)를 전송하는 것에 의해 응답한다. 연관 요청 메시지(120)는 제1 노드(105)의 인증서, 제1 인증 데이터 서명 블록, 및 제2 난스값(SNonce)을 구비한다. 그 다음, 제2 노드(110)는 제1 노드(105)의 인증서에 대한 서명을 확인할 수 있고 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있다.

[0014] 그 다음, 제2 노드(110)는 연관 응답 메시지(125)를 제1 노드(105)쪽으로 전송하는 것에 의해 응답한다. 연관 응답 메시지는 제2 노드(110)의 인증서, 제2 인증 데이터 서명 블록, 및 제1 노드(105)의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터를 구비한다. 예를 들어, 제2 노드(110)는 제2 난스값(SNonce) 및 다른 데이터를 서명할 수 있고, 연관 응답 메시지(125)에 제1 노드(105)의 공개 키(Pb1)를 사용해 암호화된 세션 키(SK)를 포함하는데, 여기에서 Pb1은 연관 요청 메시지(120)의 제1 노드(105)의 인증서에 포함되어 있었다. 제1 노드(105)가 연관 응답 메시지(125)를 수신하지 않으면, 제1 노드(105)는 연관 요청 메시지(120)를 재전송한다. 그

전체가 여기에 참고 문헌으로써 포함되어 있는, *D. Eastlake, 3rd, J. Schiller, and S. Crocker. Randomness Requirements for Security. Request for Comments(Proposed Standard) 4086, Internet Engineering Task Force, June 2005*에서 설명된 것과 같은, 다양한 방법이 충분히 무작위적인 세션 키(SK: session key)를 발생시키는데 필요한 엔트로피가 이용 가능하다는 것을 보장하는데 사용될 수 있다.

[0015] 연관 응답 메시지(125)를 수신한 후, 제1 노드(105)는 제2 노드(110)가 제2 노드(110)의 인증서와 연관된 비밀 키를 보유한다는 것을 확인할 수 있다. 또한, 제1 노드(105)는 제1 노드(105)의 비밀 키를 사용해 세션 키(SK)를 복호화할 수 있다. 그 다음, 세션 키(SK)는 제1 노드(105)와 제2 노드(110) 사이의 보안 연관을 위한 PMK(pairwise master key)로서 사용될 수 있다. 그 다음, 암호화된 데이터가 제1 노드(105)와 제2 노드(110) 사이에서 어느 한 방향으로 교환될 수 있다.

[0016] 이와 같이, 연관 요청 메시지(120)가 STA와 AP를 완전하게 인증하는데 사용될 수 있다. 그것은 연관 요청 메시지(120) 또한, 선행 비컨 메시지(115)로부터의, STA의 인증서, 제1 난스값(ANonce), 및 다른 데이터를 포함하기 때문이다. 연관 요청 메시지(120)를 수신한 후, AP가 인증서를 서명한 CA(certification authority)의 공개 키를 가진다고 가정하면, AP(제2 노드(110)는 STA(제1 노드(105)의 인증서를 평가할 수 있다. STA의 인증서가 유효한 것으로 판정되면, AP는, 연관 요청 메시지(120)에 포함된 서명을 확인하는 것에 의해 STA가 연관된 비밀 키를 가지고 있는지를 판정할 수 있고, 그에 따라 STA의 진위를 증명할 수 있다. 그 다음, AP는 STA가 무선 통신 네트워크(100)를 사용하도록 인증되는지를 판정할 수 있다. 또한, 연관 요청 메시지(120)는 STA가 AP에 대해 자신의 정체를 증명하는데 사용하는 제2 난스값(SNonce)을 포함한다.

[0017] 연관 응답 메시지(125)의 악의적 인터셉션(malicious interception)은, 제1 노드(105)의 공개 키가 비밀이 아니므로, 세션 키(SK)를 제2 세션 키(SK')로 대체하는 결과를 초래할 수 있다. 그러나, 악의적 인터셉터가 제2 난스값(SNonce)을 서명할 수는 없을 것인데, 그것은 제2 노드(110)의 비밀 키에 대한 지식을 요구하기 때문이다.

[0018] 다른 방법으로, 연관 요청 메시지에 한 쌍의 추가 난스값(예를 들어, SNonce1 및 SNonce2)을 그리고 연관 응답 메시지에 한 쌍의 추가 난스값(예를 들어, ANonce1 및 ANonce2)을 포함하는 것에 의해 가상의 4단계 핸드쉐이크를 완료할 수 있다. 제1 난스값 및 제2 난스값(각각, SNonce1 및 ANonce1)은 앞서 설명된 바와 같이 인증을 완료하는데 사용되고, 제3 난스값 및 제4 난스값(각각, SNonce2 및 ANonce2)은 가상의 4단계 핸드쉐이크를 완료하고 PMK로부터 PTK(pairwise transient key)를 유도하는데 사용된다. 예를 들어, 그러한 PTK는, 그 전체가 여기에 참고 문헌으로써 포함되어 있는, IEEE(Institute of Electrical and Electronics Engineers) 표준 802.11i에서 정의된 방법에 따라 발생될 수 있다. (여기에서 참조되는 어떠한 IEEE 표준 또는 스펙도 http://standards.ieee.org/getieee802/index.html에서 또는 IEEE, 445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855-1331, USA의 IEEE에 연락하는 것에 의해 획득될 수 있다.) 구체적으로, PTK는 다음의 수학식 1을 사용해 발생될 수 있는데,

수학식 1

$$PTK = PRF\text{-}X(PMK, \text{“Pairwise key expansion”}, Min(AA,SPA) \| Max(AA,SPA) \| Min(ANonce2, SNonce2) \| Max(ANonce2, SNonce2))$$

[0019]

[0020] 여기에서, SK의 값이 PMK에 사용되고, Max(x,y)는 x 및 y의 최대값이며, Min(x,y)는 x 및 y의 최소값이고, AA는 인증자 어드레스(Authenticator Address;즉, 제2 노드)이며, SPA는 탄원자 어드레스(Supplicant Address;즉, 제1 노드)이고, "‖"는 합성(concatenation)을 지시한다.

[0021] PRF-X는 다양한 입력들을 해싱하여 겉보기 무작위(seemingly random)(또는 의사-무작위) 값을 리턴하는 PRF(pseudo-random function)이다. 흔히 사용되는 한가지 PRF가 IEEE 표준 802.11i에 의해 정의되고, 이 PRF의 간략화된 버전이 다음에서 설명된다.

[0022] PRF는 가변 갯수의 출력 비트를 제공하는데 사용될 수 있다. IEEE 표준 802.11은 5개의 PRF: 128개 비트를 출력하는 PRF-128; 192개 비트를 출력하는 PRF-192; 256개 비트를 출력하는 PRF-256; 384개 비트를 출력하는 PRF-384; 및 512개 비트를 출력하는 PRF-512를 정의한다. 간략화를 위해, 다음에서는 PRF-128만이 정의된다.

[0023] PRF-128은 다음과 같이 정의되는데,

[0024] PRF-128(K, A, B) /* 함수 PRF-128은 입력 K, A, 및 B를 가짐 */

[0025] R <- HMAC-SHA-1(K, A‖Y‖B‖Y) /* R을 K와 A‖Y‖B‖Y의 해시로 설정함 */

[0026] return L(R, 0, 128) /* 해시의 첫번째 128개 비트를 리턴함 */

[0027] 여기에서, Y는 0을 포함하는 단일 옥텟이고, HMAC-SHA-1은 IETF(Internet Engineering Task Force) 문서 "RFC 2104"에 의해 정의되는 바와 같은 HMAC(keyed-Hash Message Authentication Code)이며, L(R, 0, 128)은 R의 첫 번째 128개 비트를 리턴한다. 여기에서 설명되는 실례에서, K는 PMK(즉, SK)의 값과 동일하게 설정되고, A의 값은 스트링 "Pairwise key expansion"과 동일하며, B의 값은 [Min(AA,SPA)‖Max(AA,SPA)‖Min(ANonce2,SNonce2)‖Max(ANonce2,SNonce2)]와 동일하다.

[0028] 도 2를 참조하면, 메시지 순서도는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크(100)에서 제1 노드(105)와 제2 노드(110)를 상호 인증하기 위한 추가 방법을 예시한다. 제2 노드(110)가 제2 비컨 메시지(210)를 제1 노드(105)쪽으로 전송하는 것과 거의 동일한 시점에 제1 노드(105)가 제1 비컨 메시지(205)를 제2 노드(110)쪽으로 전송한다고 하자. 그에 따라, 제1 노드(105)는 제1 연관 요청 메시지(215)를 전송하는 것에 의해 제2 비컨 메시지(210)에 응답하고, 제2 노드(110))는 제2 연관 요청 메시지(220)를 전송하는 것에 의해 제1 비컨 메시지(205)에 응답한다.

[0029] 다음으로, 제1 노드(105) 및 제2 노드(110) 양자는, 그들이 비컨 메시지(각각, 210 또는 205) 및 연관 응답 메시지(각각, 220 또는 215) 모두를 수신했다는 것을 인지한다. 따라서, 상호 인증을 위해 어떤 노드가 AP로서 기능할 것이고 어떤 노드가 STA로서 기능할 것인지에 관한 판정이 내려져야 한다. 예를 들어, 제1 노드(105) 및 제2 노드(110)는 간단하게 어떤 노드가 좀더 작은 MAC(medium access control) 어드레스를 갖는지를 식별할 수 있다. 제2 노드(110)가 제1 노드(105)보다 좀더 작은 MAC 어드레스를 가진다고 제2 노드(110)가 판정하면, 제2 노드(110)는 연관 응답 메시지(225)를 제1 노드(105)쪽으로 전송한다. 더 나아가, 제1 노드(105)가 제2 노드(110)보다 좀더 큰 MAC 어드레스를 가진다고 제1 노드(105)가 판정하면, 제1 노드(105)는 연관 요청 메시지(215)에 의해 개시되는 인증 메커니즘을 종료한다. 그 다음, 연관 응답 메시지(225)의 처리는 앞서 설명된 연관 응답 메시지(125)의 처리와 유사하게 진행한다.

[0030] 도 3을 참조하면, 메시지 순서도는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크(100)에서 제1 노드(105)와 제2 노드(110)를 상호 인증하기 위한 추가 방법을 예시한다. 이번에도, 제1 노드(105)가 연관 요청을 개시하며 그에 따라 STA를 표현하고, 제2 노드(110)가 연관 요청을 수신하며 그에 따라 AP를 표현한다고 하자.

[0031] 먼저, 제1 난스값(ANonce) 및 제2 노드(110)의 공개 키(Pb2)를 포함하는 비컨 메시지(315)가 제2 노드(110)로부터 제1 노드(105)쪽으로 전송된다. 제1 노드(105)가 제2 노드(110)와 결합하고자 한다면, 제1 노드(105)는 제2 노드(110)쪽으로 연관 요청 메시지(320)를 전송하는 것에 의해 응답한다. 연관 요청 메시지(320)는 제1 노드(105)의 인증서, 제2 난스값(SNonce), 및 제1 인증 데이터 서명 블록을 구비한다. 제1 인증 데이터 서명 블록은 ANonce 및 SNonce 양자의 서명, 어떠한 소정의 애플리케이션 특정 텍스트, 및 제2 노드(110)의 공개 키(Pb2)를 사용해 암호화된 임시 변조 데이터(provisional keying data;(SK1)를 구비한다. SK1은, 제1 노드(105)가 제2 노드(110)를 인증하기 이전에 제1 노드(105)가 SK1을 제2 노드(110)쪽으로 송신하기 때문에 임시적인 것으로 간주된다. 그 다음, 제2 노드(110)는, 제1 노드(105)가 제1 노드(105)의 인증서에 공개 키와 연관된 비밀 키를 보유하는지를 확인할 수 있다.

[0032] 그 다음, 제2 노드(110)는 제1 노드(105)쪽으로 연관 응답 메시지(325)를 전송하는 것에 의해 응답한다. 연관 응답 메시지는 제2 노드(110)의 인증서, 제2 인증 데이터 서명 블록, 및 제1 노드(105)의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터를 구비한다. 예를 들어, 제2 노드(110)는 제2 난스값(SNonce) 및 다른 데이터를 서명할 수 있고, 연관 응답 메시지(125)에 제1 노드(105)의 공개 키(Pb1)를 사용해 암호화된 원격 변조 데이터(remote keying data;SK2)를 포함할 수 있다.

[0033] 그 다음, 제1 노드(105)는, 제2 노드(110)가 제2 노드(110)의 인증서와 연관된 비밀 키를 보유하는지를 확인할 수 있다. 그러한 확인이 실패일 경우(예를 들어, 제2 노드(110)의 인증서가 유효하지 않거나 연관 응답 메시지(325)에서의 서명이 유효하지 않은 경우), 제1 노드(105)는 인증 세션을 종료할 것이다.

[0034] 본 발명의 일부 실시예에 따르면, 세션 키(SK1 및 SK2)는, 각각, D-H(Diffie-Hellman) 파라미터 $g^a \bmod p$ 및 $g^b \bmod p$일 수 있는데, 여기에서, p는 선택된 소수(prime number)이고, g는 (Diffie-Hellman "베이스(base)"라고도 하는) "mod p의 원시근(primitive root)"이다. 변수(a 및 b)는, 비밀 정수(secret integers)로서 공지된

정수인데, 제1 노드(105)만이 a를 알고 제2 노드(110)만이 b를 안다. 당업자라면 알 수 있는 바와 같이, 그러한 Diffie-Hellman 파라미터는, 서로에 대한 선행 지식이 없는 2 당사자가 불안정한 통신 채널을 통해 공동으로 공유 비밀 키를 확립할 수 있게 하는 주지의 암호화 프로토콜과 관련이 있다. 예를 들어, 그 전체가 여기에 참고 문헌으로써 포함되어 있는, Hellman 등에게 부여된 "Cryptographic Apparatus and Method"라는 명칭의 US Patent No. 4,200,770과 W. Diffie 및 M.E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, IT-22, 6, 1976, pp.644-654를 참고한다. 변수(a 및 b)는, 각각, 제2 노드(110;AP) 및 제1 노드(105;STA)에서 무작위로 선택될 수 있다. 변수(g 및 p)는 미리 구성되거나 비컨 메시지(315)에 포함될 수 있다. 다른 방법으로는, 비컨 메시지(315)에서의 새로운 필드가 g 및 p 변수의 미리 구성된 집합 중 하나를 사용할 것을 지시할 수 있다. 그러한 경우, 세션 키(SK1)는, 제2 노드(110)의 공개 키로써 암호화되기 보다는, 제1 노드(105)의 비밀 키에 의해 서명된다. 마찬가지로, 세션 키(SK2)는, 제1 노드(105)의 공개 키로써 암호화되기 보다는, 제2 노드(110)의 비밀 키에 의해 서명된다.

[0035] 본 발명의 또 다른 실시예에 따르면, 연관 응답 메시지들(125, 225, 또는 325)이 데이터를 포함할 수 있다. 또한, 제2 노드(110;AP)도 비컨 메시지들(115, 210 또는 315)에 또는 연관 응답 메시지들(125, 225, 또는 325)에 신뢰 앵커의 리스트를 포함할 수 있다. 더 나아가, 제2 노드(110;AP)는 그것의 공개 키 인증서를 비컨 메시지들(115, 210, 또는 315) 또는 연관 응답 메시지들(125, 225, 또는 325)에 포함할 수 있다. 제1 노드(105;STA) 또한 제2 노드(AP)가, 각각, 신뢰 앵커 리스트나 AP 인증서, 또는 양자를 연관 응답 메시지들(125, 225, 또는 325)에 포함해야 한다는 요청을 연관 요청 메시지들(120, 215, 또는 320)에 포함할 수 있다. 더 나아가, 본 발명의 일부 실시예에 따르면, 연관 요청 메시지들(120, 215, 또는 320) 및 연관 응답 메시지들(125, 225, 또는 325)에 포함된 서명은 추가적으로 제1 노드(105) 및 제2 노드(110)의 MAC 어드레스를 포함한다. 예를 들어, 그러한 메시지는 다음과 같이 나타날 수 있다: 연관 요청(노드 1의 인증서 + SNonce + [ANonce ‖ SNonce ‖ MAC 1 ‖ MAC 2 ‖ SK1 ‖ "text 2"]의 서명 + {SK1}Pb2); 및 연관 요청(노드 2의 인증서 + [ANonce ‖ SNonce ‖ MAC 1 ‖ MAC 2 ‖ SK2 ‖ "text 3"]의 서명 + {SK2}Pb1).

[0036] 당업자라면 알 수 있는 바와 같이, 본 도면들에 예시된 텍스트가 아니라, 좀더 서술적인 텍스트(more descriptive text)가 서명된 데이터에 사용될 수 있다. 예를 들어, "Fast authentication message 2"가 "text 2"에 사용될 수 있고, "Fast authentication message 3"이 "text 3"에 사용될 수 있다.

[0037] 도 4를 참조하면, 일반적인 흐름도가, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크에서 제1 노드와 제2 노드를 상호 인증하기 위한 방법(400)을 예시한다. 단계 405에서는, 제1 노드가 제2 노드로부터 수신되는 비컨 메시지를 처리하는데, 비컨 메시지는 제1 난스값을 구비한다. 예를 들어, 도 1에 표시된 바와 같이, 제1 노드(105;STA)는 제2 노드(110;AP)로부터 수신되는 비컨 메시지(115)를 처리한다.

[0038] 단계 410에서는, 제1 노드가 제1 노드의 인증서, 제1 인증 데이터 서명 블록, 및 제2 난스값을 구비하는 연관 요청 메시지를 제2 노드쪽으로 전송하고, 그에 의해 제2 노드는 제1 노드의 인증서에 대한 서명을 확인할 수 있고 제1 인증 데이터 서명 블록에 대한 서명을 확인할 수 있다. 예를 들어, 도 1에 표시된 바와 같이, 제1 노드(105;STA)는 제2 노드(110;AP)쪽으로 연관 요청 메시지(120)를 전송한다.

[0039] 단계 415에서는, 제1 노드가 제2 노드로부터 수신되는 연관 응답 메시지를 처리하는데, 연관 응답 메시지는 제2 노드의 인증서, 제2 인증 데이터 서명 블록, 및 제1 노드의 공개 키를 사용해 암호화된 제1 무작위 변조 데이터를 구비하고, 그에 의해 제1 노드는 제2 노드의 인증서에 대한 서명을 확인하고 제2 인증 데이터 서명 블록에 대한 서명을 확인한다. 예를 들어, 도 1에 표시된 바와 같이, 제1 노드(105;STA)는 제2 노드(110;AP)로부터 수신되는 연관 응답 메시지(125)를 처리한다.

[0040] 도 5를 참조하면, 블록도는, 본 발명의 일부 실시예에 따른, 무선 통신 네트워크(100)에서 제1 노드(105) 또는 제2 노드(110)로서 기능할 수 있는 무선 통신 장치의 컴포넌트를 예시한다. 제1 노드(105) 또는 제2 노드(110)는, 예를 들어, 양방향 라디오, 휴대 전화, 노트북 컴퓨터, 또는 WiMAX(Worldwide Interoperability for Microwave Access) 차량 모뎀, IEEE(Institute of Electrical and Electronics Engineers) 802.11i 모뎀, 메쉬 네트워크 차량 모뎀, 또는 네트워크 노드의 다른 유형으로서 동작하는 다른 장치 유형일 수 있다. 제1 노드(105) 또는 제2 노드(110)는 적어도 하나의 프로세서(510)에 동작 가능하게 결합되는 사용자 인터페이스(505)를 구비할 수 있다. 적어도 하나의 메모리(515) 또한 프로세서(510)에 동작 가능하게 결합된다. 메모리(515)는 OS(520), 애플리케이션(525), 및 범용 파일 저장(530)을 위한 충분한 저장 공간을 가진다. 범용 파일 저장(530)은, 예를 들어, 본 발명의 구현과 연관된 데이터를 저장할 수 있다. 사용자 인터페이스들(505)은, 예를 들어, 키패드, 터치 스크린, 마이크로폰, 및 통신 스피커를 포함하지만 그것으로 제한되는 것은 아닌, 사용자

인터페이스들의 조합일 수 있다. 이 또한 전용 프로세서 및/또는 메모리, 드라이버 등을 가질 수 있는 그래픽 디스플레이(535)가 프로세서(510)에 동작 가능하게 결합된다. 제1 트랜시버(540) 및 제2 트랜시버(545)와 같은, 다수 트랜시버 또한 프로세서(510)에 동작 가능하게 결합된다. 제1 트랜시버(540) 및 제2 트랜시버(545)는 E-UTRA(Evolved Universal Mobile Telecommunications Service Terrestrial Radio Access), UMTS(Universal Mobile Telecommunications System), E-UMTS(Enhanced UMTS), E-HRPD(Enhanced High Rate Packet Data), CDMA2000(Code Division Multiple Access 2000), IEEE(Institute of Electrical and Electronics Engineers) 802.11, IEEE 802.16, 및 다른 표준들과 같은, 그러나 그것으로 제한되는 것은 아닌, 다양한 표준을 사용해, 무선 통신 네트워크(100)와 같은, 다양한 무선 통신 네트워크와 통신한다.

[0041] 도 5는 예시적인 목적을 위한 것일 뿐이라는 것과, 본 발명의 일부 실시예에 따라, 제1 노드(105) 또는 제2 노드(110)의 일부 컴포넌트만을 포함한다는 것을 이해할 수 있어야 하며, 도 5는 본 발명의 다양한 실시예를 구현할 수 있는 모든 장치를 위해 요구되는 다양한 컴포넌트 및 컴포넌트 사이의 접속에 대한 완전한 개략도가 아니라는 것을 이해할 수 있어야 한다.

[0042] 메모리(515)는 OS(520), 애플리케이션들(525), 및 범용 파일 저장(530)을 기록하는 컴퓨터 판독 가능 매체를 구비한다. 또한, 컴퓨터 판독 가능 매체는 상호 인증에 관한 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들(550)을 구비한다. 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들(550)이 프로세서(510)에 의해 처리될 때, 컴퓨터 판독 가능한 프로그램 코드 컴포넌트들(550)은, 앞서 설명된 바와 같이, 본 발명의 일부 실시예에 따른, 상호 인증을 위한 방법(400)을 실행하도록 구성될 수 있다.

[0043] 이와 같이, 본 발명의 이점은 무선 통신 네트워크에서 서로를 발견하는 2개 노드 사이의 빠른 상호 인증 처리를 가능하게 하는 것을 포함한다. 본 발명의 일부 실시예에 따르면, 요구되는 "첨부 시주기"를 크게 감소시키면서, 연관, 인증 및 키 유도 처리가 하나의 처리로 조합될 수 있다. 그 다음, 빠른 첨부 시주기는 효과적이고, 이동성이 높으며, 동적인 무선 통신 네트워크를 가능하게 한다.

[0044] 상기 명세서에서는, 특정 실시예가 설명되었다. 그러나, 당업자라면, 다음의 청구항에서 기술되는 본 발명의 범위를 벗어나지 않으면서, 다양한 변경 및 변화가 이루어질 수 있다는 것을 알 수 있을 것이다. 따라서, 명세서 및 도면들은 한정적인 의미가 아니라 예시적인 것으로 간주되어야 하고, 그러한 모든 변경은 본 교수의 범위 내에 포함되어야 한다. 어떠한 이점, 이익, 또는 해결책을 발생시키거나 두드러지게 할 수 있는 이점, 이익, 문제에 대한 해결책, 및 임의 구성 요소(들)가 어떤 한 청구항 또는 모든 청구항의 결정적이거나, 요구되거나, 필수적인 사양들 또는 구성 요소들로서 해석되어서는 안된다. 본 발명은, 이 출원의 계류 중에 행해지는 모든 정정 및 발행되는 청구항의 모든 등가물들을 포함하는, 첨부된 청구항에 의해서만 정의된다.

[0045] 더 나아가, 이 문서에서, 제1 및 제2, 상단 및 하단 등과 같은 관계 용어는, 그러한 엔티티들 또는 액션들 사이의 어떠한 실질적 그런 관계 또는 순서를 반드시 요구하거나 내포할 필요없이, 단지 1개 엔티티 또는 액션을 다른 엔티티 또는 액션으로부터 구분하는데 사용될 수 있다. "구비하다", "구비하는", "갖다", "갖는", "포함하다", "포함하는", "함유하다", "함유하는", 또는 그것에 관한 다른 어떤 변형 용어도 비-배타적인 포함을 커버하기 위한 것이고, 그에 따라, 일련의 구성 요소들을 구비하고, 갖고, 포함하고, 함유하는 프로세스, 방법, 제품, 또는 장치가 그 구성 요소만을 포함하는 것은 아니며, 명시적으로 열거되지 않았거나 그러한 프로세스, 방법, 제품, 또는 장치에 본질적인 다른 구성 요소들을 포함할 수도 있다. "하나의 ~를 구비하다", "하나의 ~를 갖다", "하나의 ~를 포함한다", "하나의 ~를 함유하다"가 수반되는 구성 요소는, 추가 제약 사항들 없이, 그 구성 요소를 구비하고, 갖고, 포함하고, 함유하는 프로세스, 방법, 제품, 또는 장치에서 추가적인 동일 구성 요소의 존재를 배제하지 않는다. "하나의(a 및 an)"라는 용어는, 여기에서 명백하게 다르게 기술되지 않는 한, 하나 이상으로 정의된다. "사실상", "본질적으로, "대략적으로", "약", 또는 그것에 관한 다른 어떤 버전의 용어도 당업자에 의해 이해되는 바에 근접한 것으로 정의되고, 비한정적인 일 실시예에서, 그 용어는 10% 이내인 것으로 정의되고, 다른 실시예에서는, 5% 이내인 것으로 정의되며, 또 다른 실시예에서는, 1% 이내인 것으로 정의되고, 또 다른 실시예에서는, 0.5% 이내인 것으로 정의된다. 여기에서 사용되는 "결합되는"이라는 용어는, 반드시 직접적이거나 기계적일 필요는 없지만, 접속되는 것으로 정의된다. 소정 방법으로 "구성되는" 장치 또는 구조는 적어도 그 방법으로 구성되지만, 열거되지 않은 방법으로 구성될 수도 있다.

[0046] 일부 실시예는, 마이크로프로세서들, DSP들(digital signal processors), 맞춤형 프로세서들(customized processors), 및 FPGA들(field programmable gate arrays)과 같은, 하나 이상의 범용 또는 특수 목적 프로세서들(또는 "처리 장치들") 및 하나 이상의 프로세서를, 특정한 비-프로세서 회로들과 관련하여, 여기에서 기술되는 방법 및/또는 시스템의 기능 중 일부, 대다수, 또는 전부를 구현하도록 제어하는 (소프트웨어 및 펌웨어 양

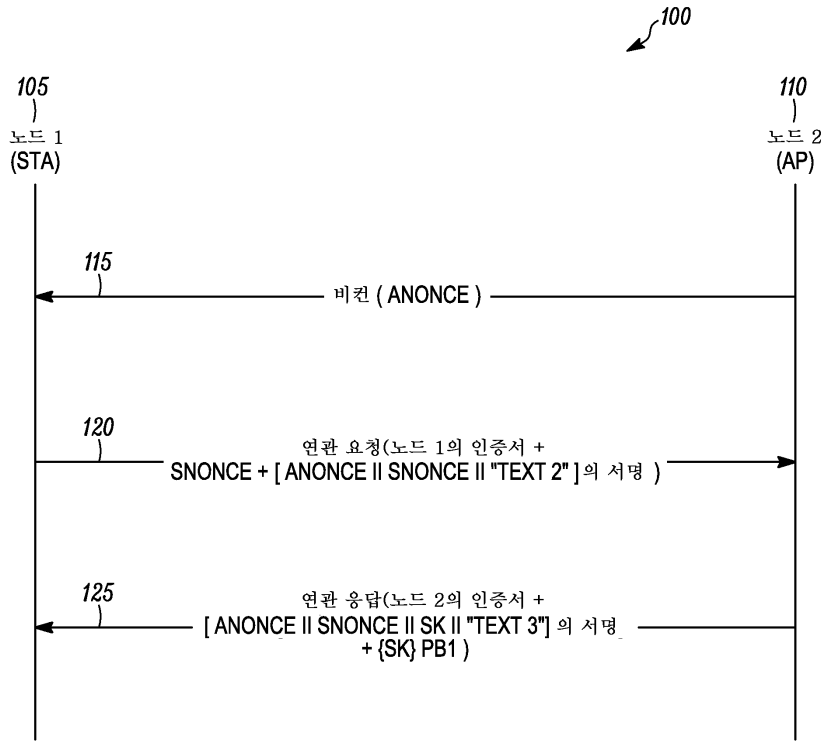
자를 포함하는) 고유한 저장 프로그램 명령어로 이루어질 수 있다는 것을 알 수 있을 것이다. 다른 방법으로, 일부 또는 모든 기능은 프로그램 명령어가 저장되지 않는 상태 머신에 의해 또는 하나 이상의 ASIC(application specific integrated circuits)으로 구현될 수 있는데, 이 경우, 각각의 기능 또는 특정 기능의 소정 조합은 사용자 정의 로직(custom logic)으로서 구현된다. 물론, 2가지 접근 방법의 조합도 사용될 수 있다.

[0047] 더 나아가, 일 실시예는 여기에서 기술되고 청구되는 방법을 수행하도록 (예를 들어, 프로세서를 구비하는) 컴퓨터를 프로그래밍하기 위한 컴퓨터 판독 가능 코드가 저장되는 컴퓨터-판독 가능 저장 매체로서 구현될 수 있다. 그러한 컴퓨터-판독 가능 저장 매체의 실례로는 하드 디스크, CD-ROM, 광학 저장 장치, 자기 저장 장치, ROM(Read Only Memory), PROM(Programmable Read Only Memory), EPROM(Erasable Programmable Read Only Memory), EEPROM(Electrically Erasable Programmable Read Only Memory), 및 플래시 메모리를 들 수 있지만, 그것으로 제한되는 것은 아니다. 더 나아가, 당업자라면, 어쩌면 상당할 수 있는 노력 및, 예를 들어, 이용 가능한 시간, 현재의 기술, 및 경제적 고려에 의해 동기 부여되는 다수 설계 선택에도 불구하고, 여기에서 개시되는 개념 및 원리에 의해 안내되는 경우, 최소한의 실험으로써 그러한 소프트웨어 명령어와 프로그램 및 IC를 쉽게 생성할 수 있을 것이다.

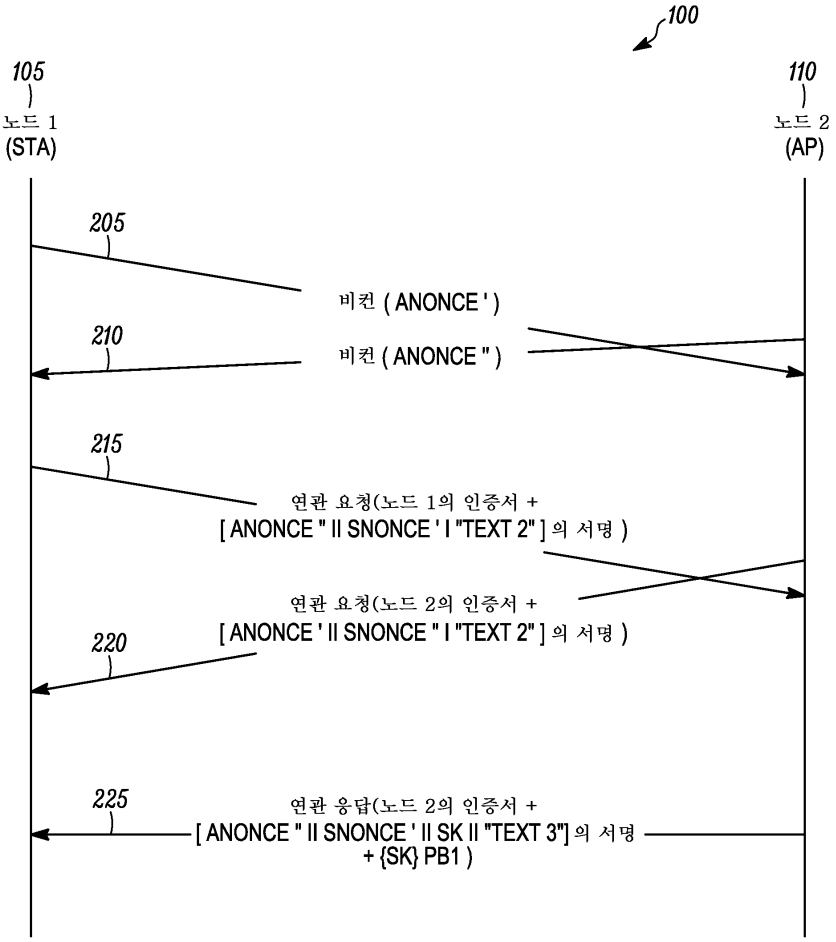
[0048] 명세서의 요약은 판독자가 기술 명세서의 특징을 쉽게 확인할 수 있도록 하기 위해 제공된다. 명세서의 요약이 청구항의 범위 또는 의미를 해석하거나 제한하는데 사용되지 않을 것이 이해된 상태에서 명세서의 요약이 제출된다. 또한, 상기한 상세한 설명에서는, 다양한 사양들이 명세서를 능률화할 목적으로 다양한 실시예에서 다같이 그룹화된다는 것을 알 수 있다. 명세서의 이 방법이, 청구된 실시예가 각 청구항에서 명시적으로 언급되는 것보다 많은 사양을 요구한다는 것을 반영하는 것으로 해석되어서는 안된다. 오히려, 다음 청구항이 반영하는 바와 같이, 발명 주제는 개시된 단일 실시예의 모든 사양보다 적은 것에 존재한다. 그에 따라, 다음 청구항은, 각각의 청구항이 별도로 청구된 주제로서 자립하는 상태로, 상세한 설명에 통합된다.

도면

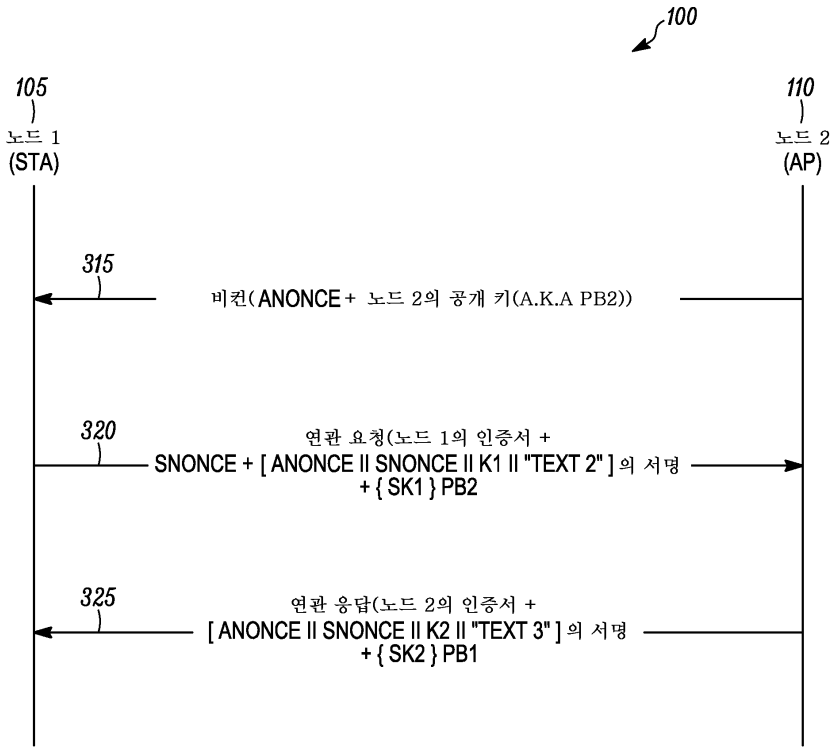
도면1



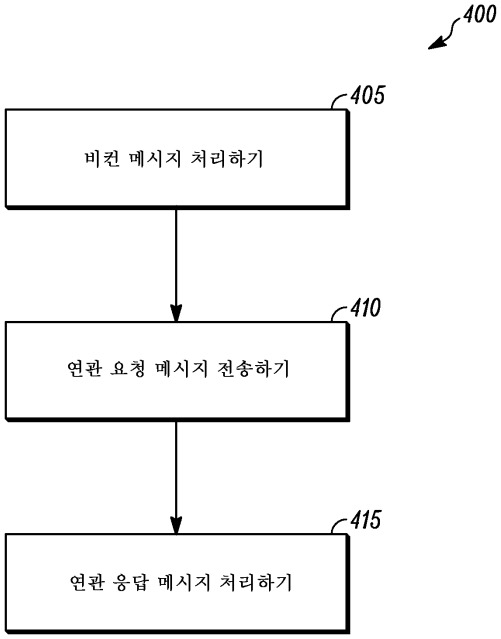
도면2


100
105
노드 1
(STA)
110
노드 2
(AP)
205
비컨 (ANONCE ')
210
비컨 (ANONCE ")
215
연관 요청(노드 1의 인증서 +
[ANONCE " II SNONCE ' I "TEXT 2"] 의 서명)
연관 요청(노드 2의 인증서 +
[ANONCE ' II SNONCE " I "TEXT 2"] 의 서명)
220
225
연관 응답(노드 2의 인증서 +
[ANONCE " II SNONCE ' II SK II "TEXT 3"] 의 서명
+ {SK} PB1)

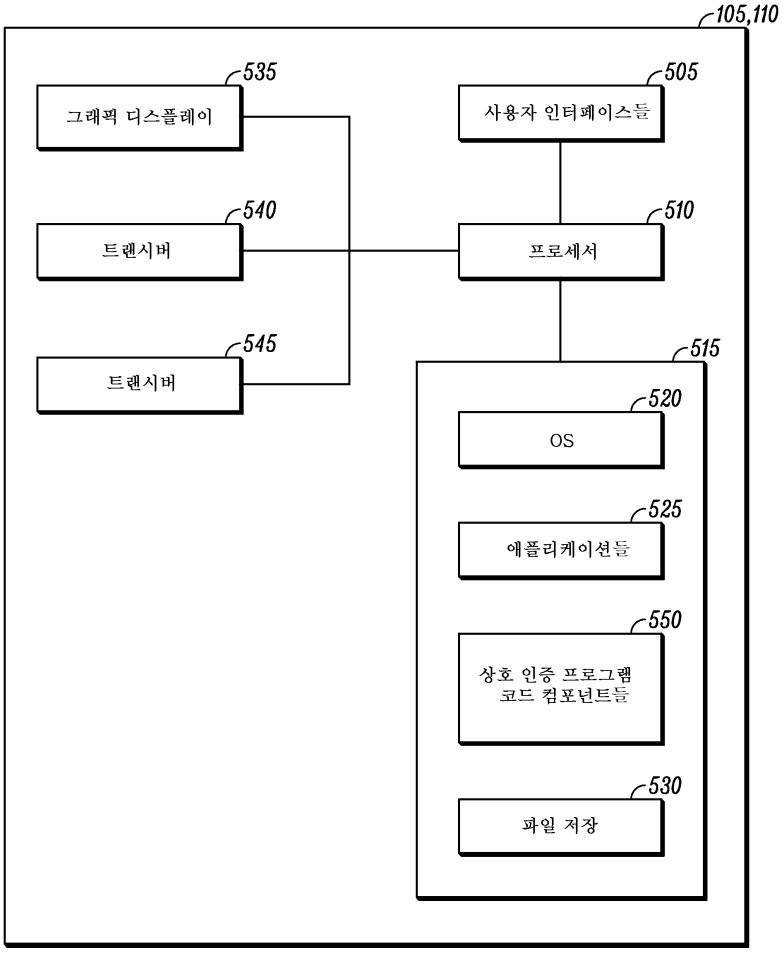
도면3


100
105
노드 1
(STA)
110
노드 2
(AP)
315
비컨(ANONCE + 노드 2의 공개 키(A.K.A PB2))
320
연관 요청(노드 1의 인증서 +
SNONCE + [ANONCE || SNONCE || K1 || "TEXT 2"]의 서명
+ { SK1 } PB2
325
연관 응답(노드 2의 인증서 +
[ANONCE || SNONCE || K2 || "TEXT 3"]의 서명
+ { SK2 } PB1

도면4


400
405
비컨 메시지 처리하기
410
연관 요청 메시지 전송하기
415
연관 응답 메시지 처리하기

도면5


105,110
535
그래픽 디스플레이
505
사용자 인터페이스들
540
트랜시버
510
프로세서
545
트랜시버
515
520
OS
525
애플리케이션들
550
상호 인증 프로그램
코드 컴포넌트들
530
파일 저장