(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년10월26일
(11) 등록번호 10-0989769
(24) 등록일자 2010년10월18일

(51) Int. Cl.
H04B 7/26 (2006.01) *H04L 12/28* (2006.01)
H04L 9/16 (2006.01)
(21) 출원번호 10-2008-7018063
(22) 출원일자(국제출원일자) 2006년12월15일
심사청구일자 2008년07월23일
(85) 번역문제출일자 2008년07월23일
(65) 공개번호 10-2008-0087863
(43) 공개일자 2008년10월01일
(86) 국제출원번호 PCT/US2006/062138
(87) 국제공개번호 WO 2007/079349
국제공개일자 2007년07월12일
(30) 우선권주장
11/323,727 2005년12월30일 미국(US)
(56) 선행기술조사문헌
US20040240412 A1
US6922728 B2
US20040143842 A1
전체 청구항 수 : 총 7 항

(73) 특허권자
모토로라 인코포레이티드
미국, 일리노이 60196, 샤움버그, 이스트 앨공퀸 로드 1303
(72) 발명자
정, 혜윤
미국 32713 플로리다주 드베리 소더비 웨이 509
(74) 대리인
양영준, 정은진, 백만기

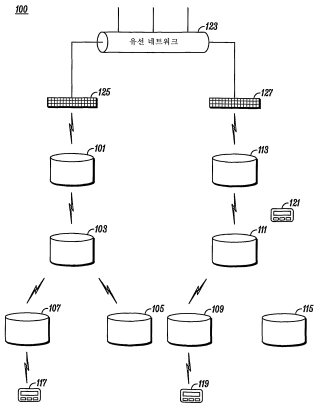
심사관 : 박성웅

(54) 멀티-홉 무선 네트워크에서의 무선 라우터 보조 보안핸드오프(WRASH)

(57) 요 약

무선 라우터 보조 보안 핸드오프 방법(300)은 인프라스트럭처-기반 이동 멀티-홉 무선 네트워크를 위한 효율적인 층 2 보안 핸드오프를 포함한다. 핸드오프는, 이동국(301)으로부터 신 액세스 포인트(307)로의 제1 홉인 무선 라우터(311)의 보조를 받는다. 구 액세스 포인트(303)로부터의 보안 문맥은 먼저 안전한 방식으로 이동국(301)에 전달된다. 이동국(301)으로부터 신 액세스 포인트(307)로의 제1 핸드오프 메시지(309)는 3가지 역할들, 즉, 재연계 요청, 보안 문맥 전달 및 신 세션 키 생성 핸드셰이킹을 갖는다. 제1 홉 무선 라우터(311)는 메시지 콘텐츠의 신규성을 보증하고, 메시지를 신 액세스 포인트(307)에 안전하게 터널링한다. 신 액세스 포인트(307)로부터 이동국(301)으로의 제2 메시지(315)는 핸드오프 프로세스를 완료한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

멀티-홉 통신 네트워크에서의 무선 라우터 보조 보안 핸드오프(wireless router assisted security handoff)의 방법으로서,

이동국에서,

보안 핸드오프를 보조하기 위해 액세스 포인트에 대한 제1 홉(hop)인 무선 라우터를 선택하는 단계와,

상기 무선 라우터로부터 수신된 헬로우(hello) 메시지로부터 상기 무선 라우터의 SN(sequence number)과, 상기 액세스 포인트의 액세스 포인트 MAC(media access control) 어드레스(AA)를 검색하는 단계와,

상기 SN 및 상기 AA를 사용해서 PTK(pairwise transient key)를 생성하는 단계와,

재연계 요청(re-association request)을 포함하는 제1 핸드오프 메시지를 상기 이동국으로부터 상기 무선 라우터로 송신하는 단계를 포함하고,

상기 무선 라우터에서,

상기 제1 핸드오프 메시지를 안전하게(securely) 상기 액세스 포인트에게 터널링하는 단계를 포함하며,

상기 액세스 포인트에서,

상기 무선 라우터로부터 상기 제1 핸드오프 메시지를 수신하는 단계와,

상기 SN 및 상기 AA를 사용해서 상기 PTK를 생성하는 단계와,

상기 PTK를 사용해서 상기 제1 핸드오프 메시지의 메시지 무결성(integrity)을 검증(validating)하는 단계와,

상기 PTK를 사용해서 재연계 응답을 포함하는 제2 핸드오프 메시지를 생성하는 단계와,

상기 무선 라우터에게 상기 제2 핸드오프 메시지를 송신하는 단계를 포함하고,

상기 무선 라우터에서,

상기 제2 핸드오프 메시지를 안전하게 상기 이동국에 터널링하는 단계를 포함하며,

상기 이동국에서,

상기 PTK를 사용해서 상기 제2 핸드오프 메시지의 메시지 무결성을 검증하는 단계와,

상기 이동국과 상기 액세스 포인트 사이의 통신을 설정하는 단계를 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 2

제1항에 있어서,

상기 제1 핸드오프 메시지는 MID(message identification), 상기 이동국의 PSC(protected security context), 상기 무선 라우터의 SN(sequence number), MS_Nonce(mobile station-generated random number), 상기 액세스 포인트의 AA, 상기 이동국의 MAC(media access control) 어드레스(SPA), WRA(wireless router address) 및 MIC(message integrity code) 중 하나 또는 그 이상을 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 3

제1항에 있어서,

상기 액세스 포인트를 포함하는 모든 네트워크 액세스 포인트들에서 SCEK(security context encryption key)를 구성하는 단계와,

SCEK를 사용해서 상기 액세스 포인트에서 수신된 상기 제1 핸드오프 메시지를 해독하는 단계를 더 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 4

제1항에 있어서,

상기 선택 단계 전에,

상기 무선 라우터가 상기 네트워크에 합류(join)할 때 상기 무선 라우터와 상기 액세스 포인트 사이에서 보안 연계(security association)를 제공하는 단계를 더 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 5

제1항에 있어서,

상기 선택 단계 전에,

초기 이동국 인증 중에 제1 액세스 포인트와 상기 이동국 둘 모두에서 핸드오프 PMK(pairwise master key)를 생성하는 단계와,

상기 이동국의 상기 핸드오프 PMK와 MAC 어드레스를 암호화함으로써 상기 제1 액세스 포인트에서 PSC(protected security context) 데이터를 생성하는 단계와,

상기 초기 이동국 인증 중에 상기 제1 액세스 포인트로부터 상기 이동국으로 상기 PSC를 전송하는 단계와,

상기 이동국과 상기 액세스 포인트 간의 통신을 설정한 후, 상기 이동국을 경유해서 상기 제1 액세스 포인트로부터 상기 액세스 포인트로 상기 PSC 데이터의 핸드오프 PMK를 전송하는 단계를 더 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 6

제1항에 있어서,

상기 무선 라우터에 의해 메시지의 나이(age)를 검증한 후, 상기 재연계 요청 메시지가 터널링되는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 7

제2항에 있어서,

상기 무선 라우터에서, 상기 제1 핸드오프 메시지를 터널링하기 전에,

상기 제1 핸드오프 메시지의 SN, SPA 및 AA를 체크하는 단계와,

동일한 SPA를 갖는 이전 SN을 구비한 상기 제1 핸드오프 메시지를 폐기하는 단계와,

체크가 통과될 때, 상기 제1 핸드오프 메시지를 상기 액세스 포인트에게 안전하게 터널링하고 현재의 SN값을 1만큼 증가시키는 단계

를 더 포함하는 무선 라우터 보조 보안 핸드오프의 방법.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

명 세 서

기 술 분 야

[0001] 본 발명은, 일반적으로, 무선 멀티-홉 네트워크에 관한 것으로, 특히, 멀티-홉 무선 네트워크에서 이동국과 액세스 노드 간의 안전한 핸드오프(secure handoff)에 관한 것이다.

배 경 기 술

[0002] 보이스 오버 인터넷 프로토콜(IP)과 라이브 스트림 비디오와 같은 이동 무선 네트워크 실시간 애플리케이션에서, 무선 메시 네트워크와 같은 최신 어드밴스(emerging advanced) 멀티-홉 무선 네트워크의 최종 사용자 수용을 용이하게 하기 위해 고속 핸드오프가 바람직하다. 하나의 액세스 포인트(AP)로부터 다른 AP로 이동하는 이동국을 위한 심리스(seamless) 핸드오프는 애플리케이션 성능 및 유용성(usability)을 향상시킨다.

[0003] 액세스 포인트들 간의 이동국 핸드오프는 링크층 핸드오프와 네트워크층 핸드오프 중 하나 또는 둘 다를 포함할 수 있다. 서브넷이 다수의 액세스 포인트들을 통상 커버한다는 사실 때문에, 대부분의 핸드오프는 링크층에서만 발생한다. 따라서, 안전한 고속 링크층 핸드오프는 전체 네트워크 성능을 강화한다. 이동국이 먼저 네트워크에 참여할 때, 이동국과 AP 간의 보안 연계(security association)을 위한 초기 인증 및 키 관리에 대체로, 수 초 정도의 비교적 긴 시간이 걸릴 수도 있다. 이동국이 AP들 사이에서 이동하기 때문에, 전체 인증 및 키 관리 프로토콜을 재개시하는 것은 핸드오프 성능에 불가피하게 영향을 준다. 현 무선 LAN(local area network) 토폴로지(topologies)에서, 고속 핸드오프를 위한 2 부류의 방식이 제안되었다: 즉, "선-인증(pre-authentication)" 핸드오프와 "보안 문맥 전송(security context transfer)" 핸드오프를 포함한다.

[0004] 선-인증 핸드오프 방식과 관련해서, 이동 장치는, 구(old) AP를 통해 또는 신(new) AP를 통해, 구 액세스 포인트와의 연결을 끊기 전에 신 액세스 포인트에 대해 인증할 수 있다. 이러한 핸드오프는, 신 보안 세션 키가 이동 장치가 신 액세스 포인트로 이동할 때 사용될 준비가 되어 있기 때문에, 비교적 고속이다. 선-인증 방식에서 해결해야 할 한가지 문제점은 정확한 신 AP의 위치를 정하는 것과 선-인증을 위한 적합한 시간을 할당하는 것 사이에서 균형을 맞추는 것이다. 핸드오프가 전체 인증 및 키 관리 프로세스에 필요한 시간 지연을 효율적으로 야기할 수 없는 고속 환경으로 인해 어려움이 증가된다.

[0005] 보안 문맥 전송 핸드오프 방식과 관련해서 다양한 방식들이 제안되었다. 한 방식은 현 AP와 신 AP 간의 이동 장치의 보안 문맥의 인터 액세스 포인트 프로토콜(IAPP; Inter Access-Point Prtocol) 교환이다. 상기 방식에서, 보안 문맥은 이웃 AP 그래프를 사용해서 미리(proactively) 분산될 수 있으며, 또는, 구 AP로부터 신 AP에 의해 반응적으로(reactively) 앞당겨질 수 있다. 새롭게 제안된 IEEE 802.11(r) 표준에서, 보안 문맥은 키 홀더 계층에 분산된다. 따라서, 이러한 타입의 핸드오프 방식에서, 신 PTK(pairwise transient key)를 유도하기 위한 포웨이 핸드셰이크(four-way handsahke)의 지연은 감소되지 않으며, 메모리 및 계산 요구에 대한 오버헤드가 클 수 있다. IEEE 802.11(r)에서, 탑 키 홀더를 위한 추가 하드웨어가 요구될 수 있다.

[0006] 따라서, 보안 방식의 핸드오프에 필요한 메시지의 수를 감소시키는 방법을 제공하는 것이 유익하다.

실 시 예

[0012] 본 발명에 따른 실시예들을 상세하게 설명하기에 앞서, 실시예들은 주로 멀티-홉 무선 네트워크에서의 무선 라우터 보조 보안 핸드오프와 관련된 방법 단계 및 시스템 컴포넌트에 대한 조합에 속한다는 것을 알아야 한다. 따라서, 시스템 컴포넌트 및 방법 단계들은 도면에서 종래의 심볼에 의해 적절하게 표현되었고, 도면은 본 설명의 이점을 가지며 본 기술분야에 숙련된 자에게 명백한 세부사항으로 본 명세서를 모호하게 하지 않도록 본 발명의 실시예들의 이해에 관련된 특정 세부사항들만을 도시하고 있다.

[0013] 본 문서에서, 제1(first) 및 제2(second), 상부(top) 및 하부(bottom) 등과 같은 관계 용어(relational terms)는 임의의 실제적인 관계 또는 엔티티들 또는 액션들 간의 순서를 반드시 요구하거나 의미하지 않고 하나의 엔티티 또는 액션을 다른 엔티티 또는 액션과 구별하는 데에만 사용될 수 있다. 용어 "포함한다(comprises)", "포함하는(comprising)" 또는 임의의 어미 변화는 비-배타적 포함(non-exclusive inclusion)을 커버하려는 것으로서, 구성요소의 리스트를 포함하는 프로세스, 방법, 제품 또는 장치는 단지 상기 구성요소들만을 포함하는 것이 아니라 명백하게 리스트되지 않거나 상기 프로세스, 방법, 제품 또는 장치에 속한 다른 구성요소들을 포함할 수 있다. "...를 포함한다(comprises ... a)"에 이어지는 구성요소는, 어떠한 제한도 없이, 상기 구성요소를 포함하는 프로세스, 방법, 제품 또는 장치에 추가의 동일한 구성요소의 존재를 배제하지 않는다.

[0014] 본 명세서에 기재되는 본 발명의 실시예들은 하나 이상의 종래의 프로세서들과, 하나 이상의 프로세서들이 특정 비-프로세서 회로(non-processor circuit)와 결합하여 본 명세서에 기재된 멀티-홉 무선 네트워크에서의 무선

라우터 보조 보안 핸드오프의 기능의 일부, 대부분 또는 모두를 구현하도록 제어하는 고유 저장 프로그램 명령을 포함할 수 있음을 알 것이다. 비-프로세서 회로는 무선 수신기, 무선 송신기, 신호 구동기, 클럭 회로, 전원 회로 및 사용자 입력 디바이스를 포함할 수 있지만, 이들로 제한되지는 않는다. 상기 기능들은 멀티-홉 무선 네트워크에서의 무선 라우터 보조 보안 핸드오프를 실행하는 방법의 단계들로서 해석될 수 있다. 대안으로, 일부 또는 모든 기능들은 저장된 프로그램 명령이 없는 상태 머신에 의해 또는 하나 이상의 애플리케이션 특정 집적 회로(ASIC)로 구현될 수 있으며, 특정 기능들 중 각 기능 또는 일부 조합들이 커스텀 로직(custom logic)으로서 구현된다. 물론, 두 방법들의 조합도 사용될 수 있다. 따라서, 상기 기능을 위한 방법 및 수단이 본 명세서에 기재되었다. 또한, 본 기술분야에 숙련된 자라면, 예를 들면, 가용시간, 현재 기술 및 경제적인 고려사항으로 인한 상당한 노력 및 다수의 설계 선택에도 불구하고, 본 명세서에 기술된 개념 및 원리를 지표 삼아, 최소의 실험으로 소프트웨어 명령 및 프로그램과 IC를 용이하게 생성할 수 있을 것으로 예상된다.

[0015] 최근 몇년간, 이동 무선 네트워크는 산업 애플리케이션 관점에서 볼 때 공공 안전성(public safety) 및 지능형 수송(intelligent transportation) 분야에서 중대한 주의를 받아왔다. 대부분의 애플리케이션 전개에서, 하나 이상의 유선 네트워크에 대한 액세스가 요구된다. 무선 이동국이 다른 이동국과 통신하는 피어-투-피어 애플리케이션에서 조차도, 유선 인프라스트럭처는 비교적 멀리 떨어져서 통신하는 두개의 무선 이동국들의 무선 홉들을 감소시킴으로써 성능을 향상시키기 위해 여전히 필요할 수 있다. 이러한 멀티-홉 무선 네트워크의 설계에서, 이동국은 하나 이상의 무선 라우터들을 통해 액세스 포인트와의 연속적인 연결성(connectivity)을 유지할 수 있다. 따라서, 유선 네트워크와 이동국 간의 통신 성능, 또는, 하나의 이동국 및 먼 거리에 있는 이동국 간의 통신 성능이 상당히 향상될 수 있다.

[0016] 도 1은 인프라스트럭처-기반 멀티-홉 무선 네트워크(100)를 도시한 블록도이다. 무선 라우터(101, 103, 105, 107, 109, 111, 115)는 이동국(117, 119, 121)을 위한 패킷들을 라우트하는데 사용된다. 본 기술 분야에 숙련된 자들이 알 수 있는 바와 같이, 무선 라우터는 TDMA(time-division multiple access) 포맷, CDMA(code-division multiple access) 포맷, 또는 FDMA(frequecny-division multiple access) 포맷과 같은 멀티플렉스 포맷의 데이터 패킷 통신을 송수신할 수 있다. 일례의 이동국으로부터 유선 네트워크까지의 경로만이 도시되어 있다. 예를 들어, 유선 네트워크는 다른 애드-혹 네트워크, PSTN(public switched telephone network) 및 인터넷과 같은 다른 네트워크에 대한 액세스를 네트워크 노드에 제공하기 위해, 코어 LAN(local access network)과, 다수의 서버 및 게이트웨이 라우터를 포함할 수 있다.

[0017] 본 기술 분야에 숙련된 자들은, 메시 커넥션 또는 네트워크 커넥션이 무선 라우터들 또는 다른 유사 장치들 간에 설정되었음을 알 것이다. 무선 라우터들(101, 103, 105, 107, 109, 111, 113, 115) 간의 메시 커넥션은 두 개의 이웃 장치들이 서로 통신할 수 있는 경우라면 언제든지 설정될 수 있다. 링크층의 단말간(end-to-end) 보안 모델이 멀티-홉 무선 네트워크(100)에서 사용될 때, 보안 연계는 링크층의 무선 도메인 내의 두 통신 노드들 간에 설정된다. 예를 들어, 이동국(119, 121)은, 두 장치들이 무선 라우터들(109, 111, 113)을 통해 서로 통신할 때 보안 연계를 설정할 수 있다. 유선 네트워크(123)와의 모든 트래픽은 액세스 포인트(125, 127)를 통과한다. 따라서, 이동국(119, 121)은 액세스 포인트(125, 127) 중 하나와 링크층 연계 및 보안 연계를 둘 다 계속해서 유지한다. 소정의 이동국과 액세스 포인트 간에 임의의 수의 무선 라우터들이 있을 수 있다. 본 기술 분야에 숙련된 자들은, 각 통신 홉에서의 고유 지연으로 인해, 보안 문맥 전송 방식에서 선-인증, 포웨이 핸드셰이킹 및 키 재료 분배 각각은 핸드오프 중에 보다 더 긴 시간이 걸릴 수도 있음을 알 것이다.

[0018] 본 발명은 무선 라우터 보조 보안 핸드오프(WRASH)로서 기술될 수 있는 보안 문맥 캐싱 핸드오프 방식과 관련된 고속 핸드오프 방식을 제공한다. 무선 라우터는, 가능한 재생 침해(replay attack)를 방지하기 위해, "Anonce"의 "신규성(freshness)"을 보증함으로써 핸드오프를 촉진시킨다. 본 기술 분야에 숙련된 자들은, Anonce가 포웨이 핸드셰이킹 중에 인증 장치(authenticator)로부터 요청자(supplicant)에게 송신된 난수(random number)임을 알 것이다. 보안 문맥은 핸드오프시 이동국을 통해 전송된다. 재연계(re-association) 및 포웨이 핸드셰이크 메시지는 오직 두개의 메시지들로 조합된다.

[0019] 이하는 본 발명에 의해 사용되는 방식의 상세한 설명이다. 본 발명은, 모든 액세스 포인트들이 보안 문맥 암호키(SCEK; security context encryption key)로 선-구성될 것을 요구하는 방법을 사용한다. SCEK는 모든 액세스 노드들 또는 포인트들 간에 동적으로 협상될 수도 있다. 이러한 요구 사항은, 일반적으로, 모든 보안 문맥 캐싱 고속 핸드오프 방식에 필요하다. IAPP에서, RADIUS(Remote Authentication Dial In User Service) 서버는 액세스 포인트들 간의 공유 키들을 제공하도록 추천된다. 예를 들어, SCEK는 적어도 128 비트 길이일 수 있으며, 임의의 암호문(cipher text)에서 임의의 암호 침해(cryptographic attack)를 저항할만큼 충분히 견고할

수 있다.

[0020] 이동국에 대한 보안 문맥과 관련해서, 이동국이 초기에 네트워크에 합류할 때, 선택된 액세스 포인트에 따라 전체 인증 및 키 관리 프로토콜을 실행한다. 이는 WLAN(wireless local area network)를 위한 IEEE 802.11(i)(Institute for Electrical and Electronics Engineers) 표준에 기술된 보안 프레임워크와 유사하다. 초기 트랜잭션 중에, PMK(pairwise master key) 및 PTK가 이동국과 액세스 포인트 둘 다에서 생성될 수 있다. WLAN 관점에서의 차이점은, 인증 및 키 관리 메시지들이 멀티-홉 무선 네트워크에서 메시 라우팅 포워딩 기구를 경유해서 다수의 무선 라우터들을 통해 운송된다는 점이다.

[0021] 따라서, PMK 외에, 이동국 및 액세스 포인트는 PRF(Pseudo-Random Function)-256비트(PMK, "핸드오프 PMK 도출(Derivation)", Supplicant Address(SPA))와 등가인 핸드오프 PMK(PMK_H)를 생성한다. PRF는 IEEE 802.11(i) 표준에서 정의되는데, 지정 "PRF-256"은 PRF의 출력 비트 길이를 지정한다. "SPA"는 이동국의 MAC(media access control) 어드레스이다. 본 기술 분야에 숙련된 자들은, MAC 층이 OSI(open systems interconnection) 모델의 데이터 링크층을 구성하는 두개의 서브-층들 중 하나임을 알 것이다. MAC 층은 공유 채널을 가로 질로 하나의 NIC(Network Interface Card)로부터 다른 NIC로 데이터 패킷을 이동시킬 책임이 있다. MAC 서브층은 동일한 채널을 통해 상이한 국들로부터 송신된 신호들은 충돌하지 않음을 보장하기 위해 MAC 프로토콜을 사용한다.

[0022] 핸드오프의 보안 문맥은 개시/종료 시간 및 SPA를 갖는 PMK 핸드오프(PMK_H), PMK_H 라이프타임을 포함한다. 보안 문맥은 SCEK로 현 액세스 포인트에서 암호화되며, 암호화된 데이터는 PSC(protected security context)로서 명명된다. 그 후, 액세스 포인트는 초기 보안 세션 셋업 타임 중에 PSC를 이동국에 전달한다. 이는, IEEE 802.11(i) 표준 프레임워크에서 정의된 바와 같이 액세스 포인트로부터 이동국으로의 GTK(group temporal key) 전달과 동일한 방식을 실행될 수 있다. 이동국이 PSC를 수신할 때, PSC는 만료(expiration)시까지 재사용될 수 있다.

[0023] 본 발명에서, 무선 라우터는 SN(sequence number)를 생성하고 액세스 포인트에 대한 타당성(validity)을 보증하는데 있어 중요한 역할을 한다. 멀티-홉 무선 네트워크에서, 무선 라우터가 작동할 때, 액세스 포인트와의 보안 연계를 설정하고, 보안 채널은 무선 라우터와 액세스 포인트 사이에서 셋업된다. 네트워크의 각각의 무선 라우터는 SN을 유지한다. 무선 라우터는 SN을 SN과, "hello" 메시지의 연계된 액세스 포인트 MAC 어드레스(AA)를 브로드캐스트한다. SN은, 무선 라우터가 이동국으로부터 유효 재연계 요청을 수신할 때만 증가된다.

[0024] 도 2는 이동국(MS), 무선 라우터(WR) 및 액세스 포인트(AP) 간의 통신을 도시한 흐름도(200)이다. 이동국이 신 액세스 포인트로 핸드오프하기 위해 제1 홉 무선 라우터를 선택할 때, 제1 홉 무선 라우터의 hello 메시지로부터 SN과 AA를 검색하고, 신 PTK(201)를 생성한다. 신 PTK는 PRF-X(PMK_H, "Pairwise Key Expansion," AA‖SPA‖SN‖MS_Nonce)와 동일하며, X는 PRF 출력의 길이이고, MS_Nonce(Mobile Station Nonce)는 이동국에 의해 생성된 난수이다. PTK 도출에서 사용된 SN은 이동국에 의해 수신된 최종 비콘 프레임("hello" 메시지)(203)로부터 다시 검색되고, SN은 IEEE 802.11(i) 표준의 포웨이 핸드세이크에서처럼 Anonce로서 사용된다. 무선 라우터와 액세스 포인트 간에 신뢰 관계가 있기 때문에, 액세스 포인트는 Anonce로서 사용되도록 유효 SN을 유지하기 위해 무선 라우터를 신뢰한다. 무선 라우터는 재생 침해를 방지하기 위해 SN을 근거로 재연계 요청의 나이(age)와 "신규성"을 체크한다. 이동국으로부터의 핸드오프 요청은 재연계 요청(205)과 조합된다. 요청 내의 정보는 메시지 식별(MID), PSC, SN, MS_Nonce, AA, SPA, WRA(wireless router address) 및 MIC(message integrity code)를 포함할 수 있다. WRA는 선택된 무선 라우터의 MAC 어드레스이고, SN을 무선 라우터에 결합시키는데 사용된다. MIC는 재연계 메시지 콘텐츠에 따라 이동국의 새롭게 도출된 PTK로 생성된 "메시지 무결성 체크" 코드이다. 상술된 바와 같이 재연계 메시지를 생성한 후에, 이동국은 선택된 무선 라우터에 메시지를 송신한다.

[0025] 무선 라우터가 재연계 요청(205)을 수신할 때, 메시지의 SN, SPA 및 AA를 체크한다. 무선 라우터는 동일한 SPA를 가진 이전 SN을 구비한 재연계 요청을 폐기한다. 체크가 통과되면, 메시지를 액세스 포인트에 안전하게 터널링(tunnel)하고 현 SN 값을 1 증가시킨다. 본 기술 분야에 숙련된 자들은, 용어 "터널링(tunnel or tunneling)"이 이동국 또는 다른 최종 행선으로의 진로(way)에서 무선 라우터를 통과하는 데이터와 관련됨을 알 것이다.

[0026] 신 액세스 포인트가 무선 라우터로부터 재연계 요청을 수신할 때(207), SCEK로 PSC(protect security context)를 해독한다. 그 후, PTK_H, SN, MS_Nonce, AA, SPA로부터 PTK를 생성하는데, 이는 이동국에 의해 실행된다. 그 후, 수신된 메시지의 MIC는 신 PTK에 의해 체크된다. PTK를 획득한 후, 신 AP는 GTK, MID,

WRA, AA, SPA, MIC를 포함하는 재연계 응답을 생성한다. 응답 메시지의 MIC는 응답 메시지 콘텐츠에 걸쳐 신 PTK로 생성된다. 응답이 생성된 후에, 메시지를 송신 WR로 안전하게 터널링한다(209). 응답 메시지가 무선 라우터에 의해 수신될 때, 터널링된 재연계 응답을 이동국에 송신한다(211). 이동국은 응답을 수신한 후, 신 PTK로 응답 메시지의 MIC를 체크한다. 체크 비교가 통과되면, 보안 핸드오프 프로세스가 완료된다(213). 이 때, 이동국 및 신 액세스 포인트는 둘 다 두 장치들 간의 데이터 흐름을 안전하게 하는데 사용될 수 있는 공통 PTK를 공유한다. 그 다음, 무선 라우터는 비콘 프레임의 메시지를 이동국에 송신하고(215), 보안 연계가 설정되었음을 나타내는 메시지에 포함된 AA에 따라 SN이 모두 1씩 증가한다(SN+1).

[0027] 본 발명의 방법이 일례가 도 3에 도시된다. 도 3에서, 두 핸드셰이킹 메시지들은, 도 1에 상술된 바와 같이 참여 장치들(300) 사이에서 전달된다. 본 일례에서, 이동국(301)은 먼저 구 액세스 포인트(303)와 연계되어서, PSC 데이터(305)를 수신한다. 이동국(301)이 신 액세스 포인트(307)로 이동하기로 결심할 때, 도시된 선택된 무선 라우터(311)로 재연계 메시지(309)를 송신한다. 무선 라우터(311)는 재연계 메시지의 나이를 검증(validates)한 후에 재연계 메시지(313)를 신 액세스 포인트(305)로 터널링한다. 그 후, 신 액세스 포인트(305)는 PTK를 생성하고, 신 PTK로 재연계 메시지를 검증한다. 그 후, 신 액세스 포인트(305)는 무선 라우터들(317, 319)을 통해 재연계 응답 메시지(315)를 무선 라우터(311)에 송신한다. 무선 라우터(311)는 이어서 메시지(321)를 이동국(301)에 송신한다.

[0028] 따라서, 본 발명의 보안 핸드오프 방식은, 무선 라우터가 액세스 포인트에 의해 인증될 때 설정된 무선 라우터와 액세스 포인트 간의 신뢰 관계를 사용한다. 무선 라우터는 핸드오프 프로세스에서 사용되는 SN 형태로 Anonce를 생성한다. 본 방법의 한가지 장점은, 전체 보안 핸드오프 프로세스를 위해 두개의 메시지들만이 요구된다는 점이다. 본 방식은 현존 핸드오프 방식에 비해 핸드오프 지연 시간 기간을 상당히 감소한다. 또한, 재연계 요청은 신 PTK로 인증된다. 새로운 방식은 연계된 국들과 액세스 포인트들에서의 서버 침해의 거부 위험성을 감소시키기 위해 통신 네트워크에서의 재연계 메카니즘의 보안성(security)을 증가시킨다. 최종적으로, 본 발명의 방법은, 추가의 보안 문맥 분배 프로토콜이 필요하지 않기 때문에, 다른 현 보안 문맥 전송 기반 방법들보다 훨씬 더 간단하다.

[0029] 상술된 명세서에서, 본 발명의 특정 실시예들이 기재되었다. 그러나, 본 기술분야에 숙련된 자라면, 이하의 청구의 범위에 제시된 본 발명의 범위에서 벗어나지 않고서도 다양한 변형 및 변경이 이루어질 수 있음을 잘 알 것이다. 따라서, 명세서 및 제한적 의미라기 보다는 예시적인 것으로 간주되어야 하고, 모든 변형은 본 발명의 범위 내에 포함된다고 생각된다. 이점, 장점, 문제에 대한 솔루션, 및 임의의 이점, 장점 또는 솔루션이 발생하거나 더욱 명백하게 되도록 야기하는 임의의 구성요소(들)는 임의의 또는 모든 청구의 범위의 핵심적이고, 요구되거나 필수적인 특징 또는 구성요소들로서 해석돼서는 안 된다. 본 발명은 본 출원의 계류중에 만들어지는 임의의 보정을 포함하는 첨부된 청구의 범위 및 발행된 청구의 범위의 모든 동등물에 의해서만 정의된다.

도면의 간단한 설명

[0007] 유사한 참조부호는 개별적인 도면 전체에 걸쳐 동일하거나 기능적으로 유사한 구성요소를 지칭하고, 이하의 상세한 설명과 함께 명세서의 일부에 포함되며, 또한, 그 일부를 형성하는 첨부된 도면들은, 다양한 실시예들을 추가적으로 설명하고, 본 발명에 따른 다양한 원리들 및 장점들을 모두 설명하는 기능을 한다.

[0008] 도 1은 본 발명의 실시예에 따른 인프라스트럭처-기반 멀티-홉 무선 네트워크를 도시한 블록도이다.

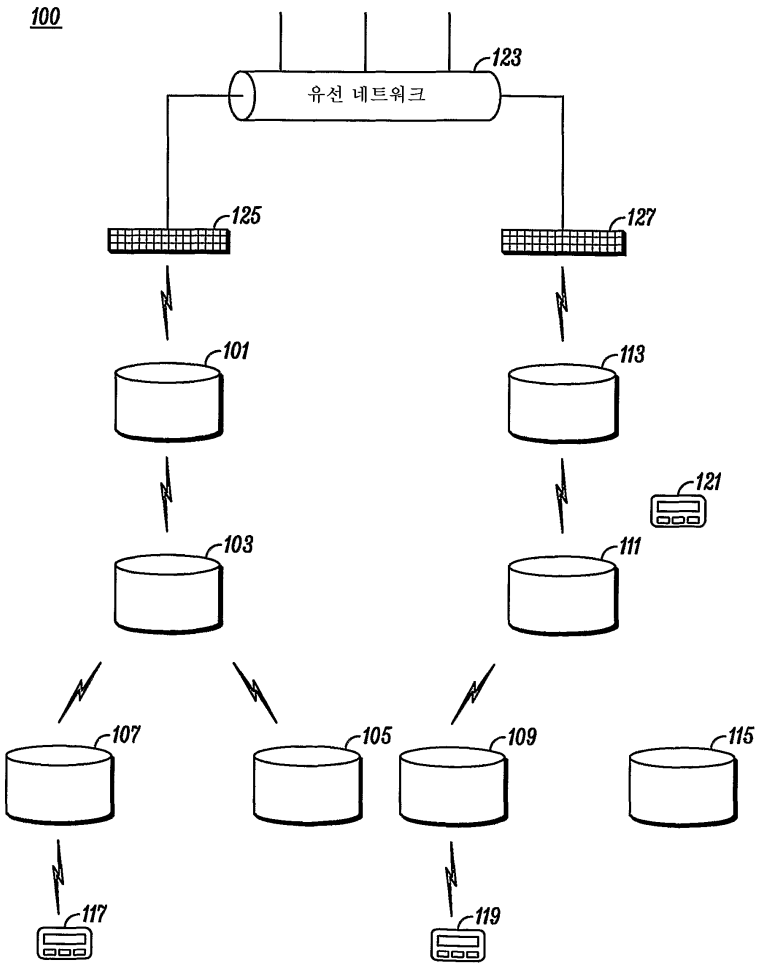
[0009] 도 2는 이동국(MS), 무선 라우터(WR) 및 액세스 포인트(AP) 간의 통신을 도시한 흐름도이다.

[0010] 도 3은 도 1의 멀티-홉 무선 네트워크에서의 두 참여 장치들(participating devices) 간의 메시지 흐름을 도시한 블록도이다.

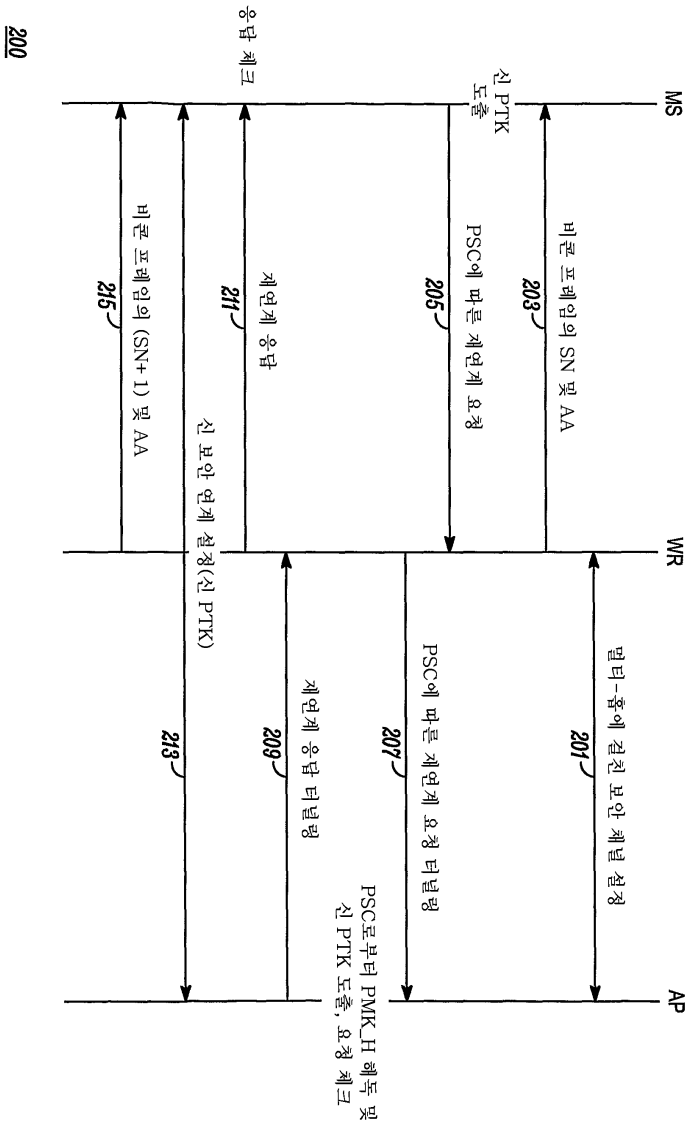
[0011] 당업자는, 도면의 구성요소가 단순화 및 명료함을 위해 도시된 것으로, 반드시 일정한 비율로 그려질 필요는 없음을 잘 알고 있을 것이다. 예를 들어, 도면의 일부 구성요소의 치수는 다른 구성요소에 비해 과장되게 그려져서, 본 발명의 실시예들의 이해를 도울 수 있다.

도면

도면1


100
123
유선 네트워크
125
127
101
113
121
103
111
107
105
109
115
117
119

도면2


200
MS
WR
AP
멀티-홉에 걸친 보안 채널 설정
201
비콘 프레임의 SN 및 AA
203
PSC에 따른 재연계 요청
205
PSC에 따른 재연계 요청 터널링
207
PSC로부터 PMK_H 해독 및
신 PTK 도출, 요청 체크
재연계 응답 터널링
209
재연계 응답
211
신 보안 연계 설정(신 PTK)
213
비콘 프레임의 (SN+ 1) 및 AA
215
신 PTK
도출
응답 체크

도면3