(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년07월31일
(11) 등록번호 10-1540523
(24) 등록일자 2015년07월23일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 12/04* (2009.01)
H04W 36/12 (2009.01)
(21) 출원번호 10-2013-0157853
(22) 출원일자 2013년12월18일
심사청구일자 2013년12월18일
(65) 공개번호 10-2015-0071158
(43) 공개일자 2015년06월26일
(56) 선행기술조사문헌
KR1020080011004 A
KR1020080100746 A

(73) 특허권자
단국대학교 천안캠퍼스 산학협력단
충청남도 천안시 동남구 단대로 119, 단국대학교천안캠퍼스내(안서동)
(72) 발명자
박창섭
서울 강남구 도산대로83길 34, C동 402호 (청담동, 상지리츠빌)
강현선
충남 천안시 서북구 불당17길 14, 104동 1103호 (불당동, 현대아이파크)
(74) 대리인
특허법인이상

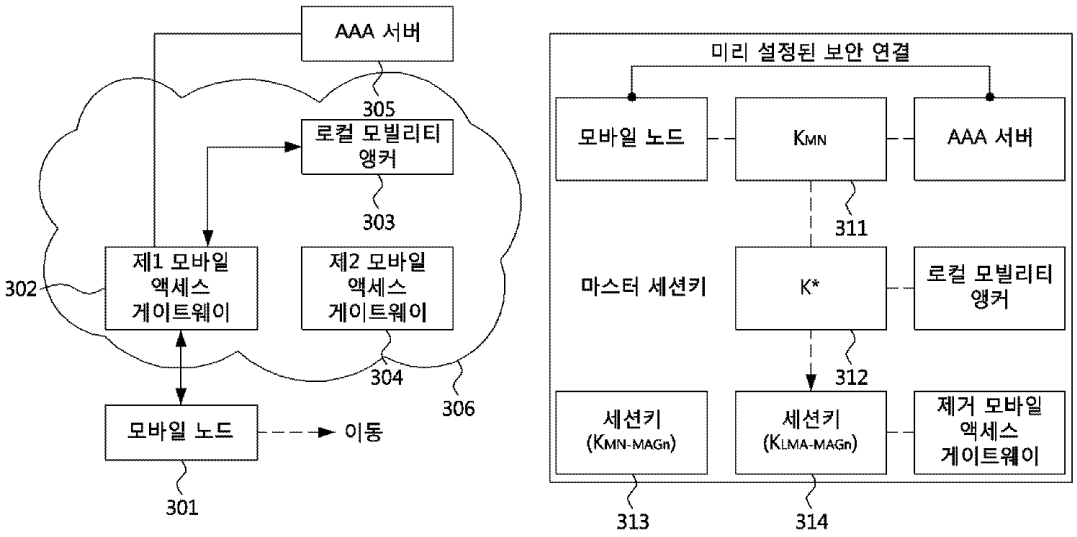
전체 청구항 수 : 총 9 항 심사관 : 손영태

(54) 발명의 명칭 **프락시 모바일 아이피를 위한 보안 연결 설정 방법 및 안전하고 빠른 핸드오버 처리 방법**

(57) 요 약

PMIPv6를 위한 보안연결 설정 방법과 핸드오버 처리 방법이 개시된다. 보안 연결들을 설정하는 방법은, 모바일 액세스 게이트웨이가 모바일 노드로부터 마스터 세션 키의 메시지 인증 코드(MAC)를 포함한 메시지를 수신하고, 마스터 세션 키의 메시지 인증 코드(MAC)가 포함된 인증요청 메시지를 AAA 서버에 전송하며, 인증요청 메시지에 대한 응답으로 모바일 노드와 모바일 액세스 게이트웨이 간에 공유될 세션 키와 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커 간에 공유될 세션 키가 포함된 인증응답 메시지를 AAA 서버로부터 수신하는 과정을 포함할 수 있다. 따라서, 새로운 비밀 키들에 의해서 시그널링 메시지들이 보호될 수 있어, 기존의 PMIPv6 및 FH-PMIPv6의 보안 문제가 해결될 수 있다.

대 표 도



명 세 서

청구범위

청구항 1

프락시 모바일 IPv6(PMIPv6)에서, 모바일 노드와 모바일 액세스 게이트웨이(MAG_A) 간 및 상기 모바일 액세스 게이트웨이(MAG_A)와 로컬 모빌리티 앵커(LMA) 간의 보안 연결들을 설정하는 방법에 있어서,

상기 모바일 액세스 게이트웨이가 상기 모바일 노드로부터 상기 모바일 노드와 AAA(Authentication, Authorization and Accounting) 서버가 공유하는 대칭키(symmetric key) K_{MN}으로부터 생성된 마스터 세션 키(K*)의 메시지 인증 코드(MAC)를 포함한 메시지(RtrSol)를 수신하는 단계;

상기 모바일 액세스 게이트웨이가 상기 마스터 세션 키(K^*)의 메시지 인증 코드(MAC)가 포함된 인증요청 메시지(Auth_Req)를 AAA 서버에 전송하는 단계; 및

상기 모바일 액세스 게이트웨이가 상기 인증요청 메시지에 대한 응답으로 상기 모바일 노드와 상기 모바일 액세스 게이트웨이(MAG_A)간에 공유될 제1 세션 키($K_{MN-MAGA}$)와 상기 모바일 액세스 게이트웨이(MAG_A)와 상기 로컬 모빌리티 앵커(LMA) 간에 공유될 제2 세션 키($K_{LMA-MAGA}$)가 포함된 인증응답 메시지(Auth_Rsp)를 상기 AAA 서버로부터 수신하는 단계를 포함하는, 프락시 모바일 IPv6의 보안 연결 설정 방법.

청구항 2

청구항 1에 있어서,

상기 모바일 액세스 게이트웨이가 상기 모바일 액세스 게이트웨이(MAG_A)와 상기 로컬 모빌리티 앵커(LMA) 간에 공유될 제2 세션 키($K_{LMA-MAGA}$)가 포함된 프락시 바인딩 업데이트(PBU) 메시지를 상기 로컬 모빌리티 앵커(LMA)에 전송하는 단계를 상기 인증응답 메시지(Auth_Rsp)를 상기 AAA 서버로부터 수신하는 단계 다음에 추가로 포함하는, 프락시 모바일 IPv6의 보안 연결 설정 방법.

청구항 3

청구항 1에 있어서,

상기 모바일 액세스 게이트웨이가 상기 모바일 노드와 상기 모바일 액세스 게이트웨이(MAG_A)간에 공유될 제1 세션 키($K_{MN-MAGA}$)가 포함한 메시지(RtrAdv)를 상기 모바일 노드로 전송하는 단계를 상기 인증응답 메시지(Auth_Rsp)를 상기 AAA 서버로부터 수신하는 단계 다음에 추가로 포함하는, 프락시 모바일 IPv6의 보안 연결 설정 방법.

청구항 4

청구항 1에 있어서,

상기 제1 세션 키($K_{MN-MAGA}$)는 상기 마스터 세션 키(K^*)와 상기 모바일 액세스 게이트웨이(MAG_A)의 식별자에 기초한 의사 랜덤 함수에 의해 생성되는, 프락시 모바일 IPv6의 보안 연결 설정 방법.

청구항 5

청구항 1에 있어서,

상기 제2 세션 키($K_{LMA-MAGA}$)는 상기 마스터 세션 키(K^*), 상기 모바일 액세스 게이트웨이(MAG_A)의 식별자 및 상기 로컬 모빌리티 앵커(LMA)의 식별자에 기초한 의사 랜덤 함수에 의해 생성되는, 프락시 모바일 IPv6의 보안 연결 설정 방법.

청구항 6

프락시 모바일 IPv6(PMIPv6)에서, 모바일 노드의 제1 모바일 액세스 게이트웨이(MAG_A)로부터 제2 모바일 액세스 게이트웨이(MAG_B)로의 핸드오버를 처리하는 방법에 있어서,

상기 제1 모바일 액세스 게이트웨이가 상기 모바일 노드가 상기 제2 모바일 액세스 게이트웨이로 핸드오버하는 것을 인지하는 단계;

상기 제1 모바일 액세스 게이트웨이가 로컬 모빌리티 앵커(LMA)에게 상기 제2 모바일 액세스 게이트웨이(MAG_B)의 식별자가 포함된 인증요청(Auth_Req) 메시지를 전송하는 단계; 및

상기 제1 모바일 액세스 게이트웨이가 상기 로컬 모빌리티 앵커로부터 상기 모바일 노드와 상기 제2 모바일 액세스 게이트웨이(MAG_B)간에 공유될 제1 세션 키($K_{MN-MAGB}$)와, 상기 로컬 모빌리티 앵커와 상기 제2 모바일 액세스 게이트웨이(MAG_B) 간에 공유될 제2 세션 키($K_{LMA-MAGB}$)가 포함된 인증응답(Auth_Rsp) 메시지를 수신하는 단계를 포함한, 프락시 모바일 IPv6의 핸드오버 처리 방법.

청구항 7

청구항 6에 있어서,

상기 제1 모바일 액세스 게이트웨이가 상기 로컬 모빌리티 앵커와 상기 제2 모바일 액세스 게이트웨이(MAG_B) 간에 공유될 제2 세션 키($K_{LMA-MAGB}$)가 포함된 메시지를 상기 제2 모바일 액세스 게이트웨이로 전송하는 단계를 상기 인증응답(Auth_Rsp) 메시지를 수신하는 단계 다음에 추가로 포함하는, 프락시 모바일 IPv6의 핸드오버 처리 방법.

청구항 8

청구항 6에 있어서,

상기 제1 세션 키($K_{MN-MAGB}$)와 상기 제2 세션 키($K_{LMA-MAGB}$)는 상기 모바일 노드와 AAA(Authentication, Authorization and Accounting) 서버가 공유하는 대칭키(symmetric key) K_{MN}으로부터 생성된 마스터 세션 키(K*)에 기초하여 생성되는, 프락시 모바일 IPv6의 핸드오버 처리 방법.

청구항 9

청구항 6에 있어서,

상기 제1 세션 키($K_{MN-MAGB}$)와 상기 제2 세션 키($K_{LMA-MAGB}$)는, AAA(Authentication, Authorization and Accounting) 서버를 거치지 않고, 상기 로컬 키 분배자의 역할을 수행하는 로컬 모빌리티 앵커(LMA)에서 생성되는, 프락시 모바일 IPv6의 핸드오버 처리 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 프락시 모바일 IP 프로토콜(Proxy Mobile IP protocol; PMIP)에 관한 것으로, 더욱 상세하게는 모바일 IPv6에서 모바일 노드(Mobile Node; MN), 모바일 액세스 게이트웨이(MAG; Mobile Access Gateway) 및 로컬 모빌리티 앵커(Local Mobility Anchor) 들간의 보안 연결(security association)을 설정하는 방법 및 안전하고 빠르게 핸드오버를 처리할 수 있는 방법에 관한 것이다.

배 경 기 술

[0002] 모바일 IPv6(MIPv6)는 모바일 노드(Mobile Node; MN)가 하나의 액세스 라우터(access router)에서 다른 액세스 라우터로의 핸드오버를 수행할 경우에 IP 이동성(IP mobility)을 지원한다. 이를 위해서, MIPv6에서는 모바일 노드의 IPv6 스택에 클라이언트 기능을 필요로 한다. 또한, 모바일 노드와 홈 에이전트(Home Agent; HA)간의 시그널링 메시지의 교환을 통해서 모바일 노드의 홈 주소(Home Address; HoA)와 보조 주소(Care-of address;

CoA) 간의 바인딩(binding)을 생성하고 유지하게 된다.

[0003] IP 이동성을 지원하기 위한 다른 방법으로서 프락시 모바일 IPv6(Proxy MIPv6; PMIPv6)가 존재한다. PMIPv6는 모바일 노드와 홈 에이전트 간의 시그널링 메시지를 확장하여 호스트의 개입 없이 IPv6 노드들의 이동성을 지원하는 것을 특징으로 한다. 즉, 프락시 모빌리티 에이전트(proxy mobility agent)가 모바일 노드를 대신하여 이동성 관리 시그널링을 네트워크에서 수행하게 된다. PMIPv6에서 정의된 핵심 기능 주체들(functional entities)은 로컬 모빌리티 앵커(Local Mobility Anchor; LMA)와 모바일 액세스 게이트웨이(Mobile Access Gateway; MAG)이다. 먼저, LMA는 MIPv6의 홈 에이전트의 역할이 확장된 주체로서 모바일 노드의 주소 바인딩 상태(binding state)를 관리한다. 다음으로, MAG는 액세스 링크에 접속된 모바일 노드의 이동성 관련된 시그널링을 관리한다. 즉, MAG는 액세스 노드로의 또는 액세스 노드로부터의 모바일 노드의 이동을 감지하고, 모바일 노드의 LMA에 초기 바인딩 등록을 수행하는 역할을 수행한다.

[0004] 그러나, PMIPv6에서도 핸드오버 지연(latency)이나 패킷 손실(packet loss) 관점에서의 기본 성능은 MIPv6와 별다른 차이가 없다. 이를 해결하기 위해서, PMIPv6에서의 빠른 핸드오버를 위한 FH-PMIPv6(Fast Handover for PMIPv6)가 제안되었다. FH-PMIPv6은 모바일 노드가 새로운 서브넷 링크를 감지하는 즉시 패킷들을 전송하도록 하고, 새로운 MAG에 의한 접속이 감지되는 즉시 패킷들을 모바일 노드로 전달한다.

[0005] 한편, PMIPv6의 시그널링 메시지에 대한 적절한 보호 체계가 없다면, PMIPv6은 MIPv6에서와 마찬가지로 흐름 변경(redirection), 서비스 거부(Denial of Service; DoS), MITM(Main In The Middle) 및 재생(replay) 공격 등과 같은 다양한 보안 공격들에 취약할 수 밖에 없다. 최근, PMIPv6의 시그널링 메시지들을 보호하기 위한 인증 체계(authentication scheme)들에 대한 연구가 진행되어왔으나, 여전히 일부 공격들에 대해서는 취약한 상황이다.

발명의 내용

해결하려는 과제

[0006] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 프락시 모바일 IPv6에 있어서, 다양한 보안 공격들에 대처할 수 있도록, 모바일 노드(MN)와 모바일 액세스 게이트웨이(MAG) 간 및 모바일 액세스 게이트웨이(MAG)와 로컬 모빌리티 앵커(LMA) 간의 보안 연결들을 효율적으로 설정하기 위한 방법을 제공하는 것이다.

[0007] 상기와 같은 문제점을 해결하기 위한 본 발명의 다른 목적은, 프락시 모바일 IPv6에 있어서, 다양한 보안 공격들에 대처할 수 있으면서 빠른 동작이 가능한, 핸드오버 처리 방법을 제공하는 것이다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위한 본 발명은, 프락시 모바일 IPv6(PMIPv6)에서, 모바일 노드와 모바일 액세스 게이트웨이(MAG_A) 간 및 상기 모바일 액세스 게이트웨이(MAG_A)와 로컬 모빌리티 앵커(LMA) 간의 보안 연결들을 설정하는 방법에 있어서, 상기 모바일 액세스 게이트웨이가 상기 모바일 노드로부터 상기 모바일 노드와 AAA(Authentication, Authorization and Accounting) 서버가 공유하는 대칭키(symmetric key) K_{MN}으로부터 생성된 마스터 세션 키(K^*)의 메시지 인증 코드(MAC)를 포함한 메시지(RtrSol)를 수신하는 단계, 상기 모바일 액세스 게이트웨이가 상기 마스터 세션 키(K^*)의 메시지 인증 코드(MAC)가 포함된 인증요청 메시지(Auth_Req)를 AAA 서버에 전송하는 단계 및 상기 모바일 액세스 게이트웨이가 상기 인증요청 메시지에 대한 응답으로 상기 모바일 노드와 상기 모바일 액세스 게이트웨이(MAG_A)간에 공유될 세션 키($K_{MN-MAGA}$)와 상기 모바일 액세스 게이트웨이(MAG_A)와 상기 로컬 모빌리티 앵커(LMA) 간에 공유될 세션 키($K_{LMA-MAGA}$)가 포함된 인증응답 메시지(Auth_Rsp)를 상기 AAA 서버로부터 수신하는 단계를 포함하는, 프락시 모바일 IPv6의 보안 연결 설정 방법을 제공한다.

[0009] 여기에서, 상기 보안연결 설정 방법은 상기 모바일 액세스 게이트웨이가 상기 모바일 액세스 게이트웨이(MAG_A)와 상기 로컬 모빌리티 앵커(LMA) 간에 공유될 세션 키($K_{LMA-MAGA}$)가 포함된 프락시 바인딩 업데이트(PBU) 메시지를 상기 로컬 모빌리티 앵커(LMA)에 전송하는 단계를 추가로 포함할 수 있다.

[0010] 여기에서, 상기 보안연결 설정 방법은 상기 모바일 액세스 게이트웨이가 상기 모바일 노드와 상기 모바일 액세스 게이트웨이(MAG_A)간에 공유될 세션 키($K_{MN-MAGA}$)가 포함한 메시지(RtrAdv)를 상기 모바일 노드로 전송하는 단계

를 추가로 포함할 수 있다.

[0011] 여기에서, 상기 인증요청(Auth_Req) 메시지에는 상기 모바일 액세스 게이트웨이의 비밀 키(SK_{MAGA})를 이용한 서명(signature)이 포함될 수 있다.

[0012] 여기에서, 상기 인증응답(Auth_Rsp) 메시지에는 상기 AAA 서버의 비밀 키(SK_{AAA})를 이용한 서명(signature)이 포함될 수 있다.

[0013] 여기에서, 상기 인증요청 메시지 전송 및 상기 인증응답 메시지 수신은 상기 모바일 노드가 PMIPv6 도메인 내에서 최초의 액세스를 수행할 때에 이루어질 수 있다.

[0014] 여기에서, 상기 마스터 세션 키(K^*)는 상기 모바일 노드가 상기 PMIPv6 도메인 내에 수행하는 세션이 종료될 때까지만 유효하도록 구성될 수 있다.

[0015] 여기에서, 상기 세션 키($K_{MN-MAGA}$)는 상기 마스터 세션 키(K^*)와 상기 모바일 액세스 게이트웨이(MAG_A)의 식별자에 기초한 의사 랜덤 함수에 의해 생성될 수 있다.

[0016] 여기에서, 상기 세션 키($K_{LMA-MAGA}$)는 상기 마스터 세션 키(K^*), 상기 모바일 액세스 게이트웨이(MAG_A)의 식별자 및 상기 로컬 모빌리티 앵커(LMA)의 식별자에 기초한 의사 랜덤 함수에 의해 생성될 수 있다.

[0017] 상기 다른 목적을 달성하기 위한 본 발명은, 프락시 모바일 IPv6(PMIPv6)에서, 모바일 노드의 제1 모바일 액세스 게이트웨이(MAG_A)로부터 제2 모바일 액세스 게이트웨이(MAG_B)로의 핸드오버를 처리하는 방법에 있어서, 상기 제1 모바일 액세스 게이트웨이가 상기 모바일 노드가 상기 제2 모바일 액세스 게이트웨이로 핸드오버하는 것을 인지하는 단계, 상기 제1 모바일 액세스 게이트웨이가 로컬 모빌리티 앵커(LMA)에게 상기 제2 모바일 액세스 게이트웨이(MAG_B)의 식별자가 포함된 인증요청(Auth_Req) 메시지를 전송하는 단계 및 상기 제1 모바일 액세스 게이트웨이가 상기 로컬 모빌리티 앵커로부터 상기 모바일 노드와 상기 제2 모바일 액세스 게이트웨이(MAG_B)간에 공유될 세션 키($K_{MN-MAGB}$)와, 상기 로컬 모빌리티 앵커와 상기 제2 모바일 액세스 게이트웨이(MAG_B) 간에 공유될 세션 키($K_{LMA-MAGB}$)가 포함된 인증응답(Auth_Rsp) 메시지를 수신하는 단계를 포함한, 프락시 모바일 IPv6의 핸드오버 처리 방법을 제공한다.

[0018] 여기에서, 상기 로컬 모빌리티 앵커(LMA)는 상기 제1 모바일 액세스 게이트웨이와 상기 제2 모바일 액세스 게이트웨이를 모두 관리한다.

[0019] 여기에서, 상기 인지하는 단계는 상기 모바일 노드로부터 상기 제2 모바일 액세스 게이트웨이의 식별자(MAG_B)가 포함된 메시지(Start_Auth)를 수신하는 것에 의해 이루어질 수 있다.

[0020] 여기에서, 상기 핸드오버 처리 방법은 상기 제1 모바일 액세스 게이트웨이가 상기 로컬 모빌리티 앵커와 상기 제2 모바일 액세스 게이트웨이(MAG_B) 간에 공유될 세션 키($K_{LMA-MAGB}$)가 포함된 메시지를 상기 제2 모바일 액세스 게이트웨이로 전송하는 단계를 추가로 포함할 수 있다.

[0021] 여기에서, 상기 세션 키($K_{MN-MAGB}$)와 상기 세션 키($K_{LMA-MAGB}$)는 상기 모바일 노드와 AAA(Authentication, Authorization and Accounting) 서버가 공유하는 대칭키(symmetric key) K_{MN}으로부터 생성된 마스터 세션 키(K^*)에 기초하여 생성될 수 있다.

[0022] 이때, 상기 마스터 세션 키(K^*)는 상기 모바일 노드가 상기 로컬 모빌리티 앵커(LMA)가 관장하는 PMIPv6 도메인 내에 머무를 경우에만 유효할 수 있다.

[0023] 이때, 상기 세션 키($K_{MN-MAGB}$)는 상기 마스터 세션 키(K*)와 상기 제2 모바일 액세스 게이트웨이(MAG_B)의 식별자에 기초한 의사 랜덤 함수에 의해 생성될 수 있다.

[0024] 이때, 상기 세션 키($K_{LMA-MAGB}$)는 상기 마스터 세션 키(K*)와 상기 로컬 모빌리티 앵커 및 제2 모바일 액세스 게이트웨이(MAG_B)의 식별자에 기초한 의사 랜덤 함수에 의해 생성될 수 있다.

[0025] 이때, 상기 세션 키($K_{MN-MAGB}$)와 상기 세션 키($K_{LMA-MAGB}$)는, AAA(Authentication, Authorization and Accounting) 서버를 거치지 않고, 상기 로컬 키 분배자의 역할을 수행하는 로컬 모빌리티 앵커(LMA)에서 생성될 수 있다.

발명의 효과

[0026] 본 발명에서는, PMIPv6을 위한 AAA 기반의 보안 메커니즘이 소개된다. 본 발명에 따른 PMIPv6를 위한 보안연결 설정 방법을 이용하면, 모바일 노드와 모바일 액세스 게이트웨이 간의 보안연결과 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커 간의 보안연결이 설정될 수 있다. 또한, 새로운 비밀 키들에 의해서 시그널링 메시지들이 보호될 수 있어, 기존의 PMIPv6 및 FH-PMIPv6의 보안 문제가 해결될 수 있다.

[0027] 또한, 본 발명에서는 종래 FH-PMIPv6의 핸드오버에서 발생되는 지연을 최소화하기 위해서 로컬 모빌리티 앵커가 로컬 키 분배 센터(local key distribution center)의 역할을 수행하도록 구성된다. 이를 통하여, 핸드오버 과정 중에서 AAA 서버와의 인증 절차가 필요하지 않으므로, 핸드오버 지연이 방지되며, 핸드오버 지연에 따른 패킷의 손실 또한 방지될 수 있다.

도면의 간단한 설명

[0028] 도 1은 프락시 모바일 IPv6(PMIPv6)의 동작 개념을 설명하기 위한 개념도이다.

도 2는 패스트 핸드오버 프락시 모바일 IPv6(FH-PMIPv6)의 동작 개념을 설명하기 위한 개념도이다.

도3은 본 발명에 따른 실시예가 적용되는 네트워크 아키텍처와 본 발명에 따른 키 계층(key hierarchy)을 설명하는 개념도이다.

도 4는 본 발명에 따른 프락시 모바일 IPv6(PMIPv6)를 위한 보안연결 설정 방법을 설명하기 위한 개념도이다.

도 5는 본 발명에 따른 프락시 모바일 IPv6(PMIPv6)를 위한 핸드오버 처리 방법을 설명하기 위한 개념도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0030] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0031] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0032] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0033] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0035] 도 1은 프락시 모바일 IPv6(PMIPv6)의 동작 개념을 설명하기 위한 개념도이다.

[0036] 도 1을 참조하면, 모바일 노드(101)가 PMIPv6 도메인(105) 내에 진입하면, 모바일 노드(101)은 모바일 액세스 게이트웨이(102)의 액세스 링크(access link)에 접속하게 되며 해당 액세스 링크의 모바일 액세스 게이트웨이(102)가 PMIPv6 동작을 수행하게 된다.

[0037] 먼저, 모바일 노드(101)는 액세스 링크에 접속된 이후에 RtrSol(Router Solicitation) 메시지(①)를 모바일 액세스 게이트웨이(102)에게 전송한다. 이때, RtrSol 메시지의 전송 시점에는 특별한 제한이 없으며, 모바일 노드(101)가 액세스 링크에 접속된 이후의 어느 시점이 될 수 있다.

[0038] 다음으로, 모바일 액세스 게이트웨이(102)는 상기 모바일 노드의 로컬 모빌리티 앵커(LMA; 103)에게 모바일 노드의 현재 위치를 업데이트해주기 위해서 프락시 바인딩 업데이트(PBU; Proxy Binding Update) 메시지(②)를 전송한다. PBU 메시지를 수신한 로컬 모빌리티 앵커는 응답으로서 프락시 바인딩 확인(PBA; Proxy Binding Acknowledge) 메시지(③)를 전송하게 된다. 이때, PAB 메시지에는 모바일 노드의 홈 네트워크 프리픽스(HNP; Home Network Prefix)가 포함될 수 있다. 이때, 로컬 모빌리티 앵커는 바인딩 캐쉬 내에 해당 모바일 노드에 대한 엔트리(Binding Cache Entry; BCE)를 생성하며 모바일 액세스 게이트웨이(102)에 대한 양방향 터널의 자신 측 엔드 포인트(end-point)를 설정한다. BCE에는 모바일 노드의 식별자(identifier), 홈 네트워크 프리픽스, 타임 스탬프 값 및 모바일 노드와 관련된 기타 정보들이 포함될 수 있다. 한편, PBA 메시지를 수신한 모바일 액세스 게이트웨이(102)는, 로컬 모빌리티 앵커(103)에 대한 양방향 터널의 자신 측 엔드 포인트를 설정한다. 즉, 생성되는 양방향 터널은 모바일 노드(101)의 트래픽을 로컬 모빌리티 앵커(103)로 포워딩하기 위한 용도로 이용된다.

[0039] 다음으로, 모바일 액세스 게이트웨이(102)는 RtrAdv(Router Advertisement) 메시지(④)를 모바일 노드(101)로 전송한다. 이때, RtrAdv 메시지에는 모바일 노드의 홈 네트워크 프리픽스(HNP)가 포함될 수 있으며, 이를 수신한 모바일 노드는 자신의 인터페이스를 HNP에 기초하여 설정할 수 있다.

[0040] 이후에, 로컬 모빌리티 앵커(103)는 PMIPv6 도메인(105) 내외에 존재하는 어떠한 노드들로부터 모바일 노드에 대해 전송되는 패킷들을 수신하는 계층상의 앵커 포인트(anchor point) 역할을 수행하게 되며, 수신된 패킷들은 설정된 양방향 터널을 통하여 모바일 액세스 게이트웨이(102)로 전달되고, 다시 모바일 액세스 게이트웨이(102)로부터 액세스 링크를 통하여 모바일 노드(101)로 전달된다.

[0041] 도 2는 패스트 핸드오버 프락시 모바일 IPv6(FH-PMIPv6)의 동작 개념을 설명하기 위한 개념도이다.

[0042] 도 2를 참조하면, 모바일 노드(201)가 제1 모바일 액세스 게이트웨이(202)로부터 제2 모바일 액세스 게이트웨이(204)로 핸드오버되는 상황이 예시된다.

[0043] FH-PMIPv6에서는, 모바일 노드가 핸드오버가 임박하였음을 감지하면 자신의 식별자와 옮겨갈 제2 모바일 액세스 게이트웨이(204)의 식별자를 제1 모바일 액세스 게이트웨이(현재 접속된 모바일 액세스 게이트웨이)에게 통보하게 된다(미도시).

[0044] 이후에, 제1 모바일 액세스 게이트웨이(202)와 제2 모바일 액세스 게이트웨이(204)는 HI(Handover Initiate) 메시지(①)와 Hack(Handover acknowledgement) 메시지(②)를 교환하는 것에 의해서, 서로간에 양방향 터널을 설정한다. 설정된 양방향 터널을 통해서 모바일 노드(201)를 향하는 패킷들이 제1 모바일 액세스 게이트웨이(202)에서 제2 모바일 액세스 게이트웨이(204)로 전달된다(핸드오버가 완료되기 전까지 일시적으로).

[0045] 로컬 모빌리티 앵커(203)와 제2 모바일 액세스 게이트웨이(204)는 앞서 설명된 바와 같은 PBU 메시지(③)와 PBA 메시지(④)를 교환하게 된다. PBU 메시지와 PBA 메시지 교환을 통해 로컬 모빌리티 앵커(203) 내의 바인딩 캐쉬가 업데이트되면, 모바일 노드(201)로의 패킷 또는 모바일 노드(201)로부터의 패킷은 제1 모바일 액세스 게이트웨이(202)를 거치지 않고, 제2 모바일 액세스 게이트웨이(204)를 직접 경유하게 된다.

[0046] 마지막으로 제2 모바일 액세스 게이트웨이(204)는 모바일 노드(201)에게 RtrAdv(Router Advertisement) 메시지(⑤)를 전송할 수 있다. 이때, RtrAdv 메시지에는 모바일 노드의 홈 네트워크 프리픽스(HNP)가 포함될 수 있으

며, 이를 수신한 모바일 노드는 자신의 인터페이스를 HNP에 기초하여 설정할 수 있다.

[0047] 이하에서, 본 발명에 따른 PMIPv6를 위한 보안연결 설정 방법 및 핸드오버 처리 방법을 설명하기 전에 몇 가지 용어를 정의한다.

[0048] MN, MAG_A, MAG_B, LMA는 각각 모바일 노드, 제1 모바일 액세스 게이트웨이(MAG_A), 제2 모바일 액세스 게이트웨이(MAG_B) 및 로컬 모빌리티 앵커(LMA)의 약어(abbreviation)이기도 하지만, 문맥에 따라서는(특히, 도 4 및 도 5에서) 대응되는 구성요소의 식별자(identifier)를 의미하는 것으로 규정한다.

[0049] PK_X와 SK_X는 각각 X의 공개 키(public key)와 비밀 키(secret key; private key)를 의미한다. SA(X, Y)는 X와 Y 간의 보안 연결(Security Association)을 의미한다. MAC(K)는 앞선 모든 필드들에 대해 K를 이용하여 계산된 메시지 인증 코드(Message Authentication Code)를 의미한다. [m]PK_X는 공개 키 PK_X를 이용한 메시지 m에 대한 암호화(encryption)을 의미하고, Sig[SK_X]는 앞선 모든 필드들에 대한 비밀 키 SK_X를 이용한 디지털 서명(digital signature)을 의미한다.

[0050] 또한, 이하에서, T_0는 초기 타임 스탬프를 의미하고, T_1은 핸드오버 시점의 타임 스탬프를 의미한다.

[0051] 도3은 본 발명에 따른 실시예가 적용되는 네트워크 아키텍처와 본 발명에 따른 키 계층(key hierarchy)를 설명하는 개념도이다.

[0052] 도 3을 참조하면, 본 발명에 따른 실시예는 모바일 노드(301)가 제1 모바일 액세스 게이트웨이(302)에 최초로 접속되고, 다시 제2 모바일 액세스 게이트웨이(304)로 핸드오버되는 네트워크 환경을 고려한다.

[0053] 이때, 모바일 노드(301)는 AAA 서버(305)와 본 발명의 범위를 벗어난 다양한 방법을 통하여 미리 설정된 장기 대칭키(long-term symmetric key; K_{MN}; 311)을 공유하고 있다고 가정된다. 즉, AAA 서버(305)와 모바일 노드(301) 간에는 보안연결이 이미 설정되어 있다는 것이 가정된다. 이는 후술될 도 4 및 도 5에서도 동일하다.

[0054] 장기 대칭키(K_{MN})으로부터 마스터 세션 키(K^*; master session key; 312)가 생성된다. 또한, 로컬 모빌리티 앵커(303)은 제1 모바일 액세스 게이트웨이(302) 및 제2 모바일 액세스 게이트웨이(304)와 연결되어, 이들 모두를 관리한다. 제1 모바일 액세스 게이트웨이(302)와 제2 모바일 액세스 게이트웨이(304)는 동일한 PMIPv6 도메인(306)에 포함되어 있다.

[0055] 한편, 도 3을 다시 참조하면, 모바일 노드(301)와 AAA 서버(305)는 키 계층(key hierarchy)내의 모든 비밀 키들에 접근할 수 있다. 반면, 모바일 액세스 게이트웨이들은 모바일 노드 또는 로컬 모빌리티 앵커와 공유하는 비밀 키에만 접근이 가능하다.

[0056] 본 발명에서, 모바일 노드와 모바일 액세스 게이트웨이 간에 공유되는 세션 키(313), 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커 간에 공유되는 세션 키(314)는 앞서 언급된 마스터 세션 키로부터 생성된다. 마스터 세션 키는 상기 단말이 PMIPv6 도메인 내에서 세션을 만료할 때까지만 유효한 키이므로, 모바일 노드와 모바일 액세스 게이트웨이 간에 공유되는 세션 키와 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커 간에 공유되는 세션 키는 마스터 세션 키에 비하여 더 짧은 유효기간을 가지게 된다. 후술되겠지만, 이러한 특징이 본 발명에 따른 보안연결 설정 방법이나 핸드오버 처리 방법이 높은 보안성을 가지도록 하는 원인이 될 수 있다.

[0057] 본 발명에서, 각각의 시그널링 메시지의 새로움을 보장하기 위해서 하나의 타임 스탬프 값이 이용된다. 모바일 노드를 위해서, 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커는 타임 스탬프에 대한 캐쉬를 유지한다. 시그널링 메시지가 수신되면, 타임 스탬프 값을 확인하여 새로운 메시지인 것이 확인되었을 경우에 메시지 인증 코드(MAC; Message Authentication Code)의 확인이 수행된다. 예를 들면, 타임 스탬프(T_1)이 기록된 메시지가 수신되면, 수신된 타임 스탬프(T_1)와 현재 타임 스탬프 캐쉬에 기록된 타임 스탬프(T_0)를 비교한다. $T_1>T_0$인 경우에만 현재 수신된 메시지가 새로운 것으로 판단하고, 수신된 메시지에 대한 프로토콜 처리를 진행한다. 만약, $T_1>T_0$이 아니라면, 수신된 메시지를 버리고 모든 프로토콜 동작을 중단한다.

[0058] 이하에서, 본 발명의 구성이 크게 두 가지 관점에서 설명된다. 첫 번째는 PMIPv6의 초기 인증 프로시저(initial authentication procedure)에서의 보안연결 설정 방법에 대한 것이며, 두 번째는 PMIPv6의 핸드오버 처리 방법에 대한 것으로, 특히 핸드오버 처리시의 인증 과정(handover authentication procedure)에 대한 것이다.

[0059] 도 4는 본 발명에 따른 프락시 모바일 IPv6(PMIPv6)를 위한 보안연결 설정 방법을 설명하기 위한 개념도이다

[0060] 도 4를 참조하면, 모바일 노드(401)가 처음으로 PMIPv6 도메인(406)에 진입하였을 때의 절차가 예시된다.

[0061] 먼저, 모바일 노드(401)는 초기 타임 스탬프(T_0)와 마스터 세션 키(K^*)를 생성한다. 이때, 마스터 세션 키(K^*)는 AAA 서버와 모바일 노드(401) 간에 이미 공유되고 있는 공유 키(K_{MN})과 상기 초기 타임 스탬프(T_0)에 기초하여 생성될 수 있다. 예컨대, 공유 키(K_{MN})와 타임 스탬프(T_0)를 입력으로 한, 의사 랜덤 함수(pseudo random function)의 출력으로 상기 마스터 세션 키(K^*)를 결정할 수 있다. 즉, $K^*=prf(K_{MN}, T_0)$로 표현될 수 있다.

[0062] 다음으로, 모바일 노드(401)는 생성된 마스터 세션 키(K^*)를 이용한 메시지 인증 코드(MAC)를 포함한 메시지(예컨대, RtrSol(Router Solicitation) 메시지(①))를 모바일 액세스 게이트웨이(402)로 전송한다. MAC에 대한 확인은 후술될 인증응답(Auth_Rsp) 메시지를 모바일 액세스 게이트웨이가 수신한 이후에 이루어진다.

[0063] 모바일 액세스 게이트웨이(402)는 모바일 노드(401)가 전송한 메시지(RtrSol 메시지)를 수신한 이후에, 수신한 메시지에 자신의 비밀 키(SK_{MAGA})를 이용한 서명($Sig(SK_{MAGA})$)을 추가한 인증요청 메시지(Auth_Req 메시지(②))를 AAA 서버(405)로 전송한다. AAA 서버는 메시지에 포함된 MAC과 디지털 서명을 확인하고, 문제가 있을 경우는 메시지를 폐기하고 절차의 진행을 중단한다. AAA서버(405)는 메시지에 포함된 MAC과 디지털 서명의 확인 결과, 문제가 없을 경우에는 세션 키($K_{MN-MAGA}$)와 세션 키($K_{LMA-MAGA}$)를 생성하고, 생성된 세션 키($K_{MN-MAGA}$)와 세션 키($K_{LMA-MAGA}$)를 인증응답 메시지(Auth_Rsp 메시지(③))에 포함하여 모바일 액세스 게이트웨이(402)로 전송한다.

[0064] 이때, 세션 키($K_{MN-MAGA}$)는 모바일 노드(401)와 모바일 액세스 게이트웨이(402) 간에 공유되는 세션 키며, 상기 마스터 세션 키(K^*)와 상기 모바일 액세스 게이트웨이의 식별자(MAG_A)에 기초한 의사 랜덤 함수에 의해 생성될 수 있다. 또한. 세션 키($K_{LMA-MAGA}$)는 로컬 모빌리티 앵커(403)과 모바일 액세스 게이트웨이(402)간에 공유되는 세션 키며, 상기 마스터 세션 키(K^*), 상기 모바일 액세스 게이트웨이(MAG_A)의 식별자 및 상기 로컬 모빌리티 앵커(LMA)의 식별자에 기초한 의사 랜덤 함수에 의해 생성될 수 있다. 앞서 언급된 바와 같이, 마스터 세션 키(K*)가 상기 모바일 노드가 상기 PMIPv6 도메인 내에 수행하는 세션이 종료될 때까지만 유효하므로, 상기 세션 키($K_{MN-MAGA}$)와 세션 키($K_{LMA-MAGA}$)들 또한 상기 모바일 노드가 상기 PMIPv6 도메인 내에 수행하는 세션이 종료될 때까지만 유효 유효하다.

[0065] 이들 세션 키들은 상기 인증응답 메시지(Auth_Rsp 메시지) 내에 모바일 액세스 게이트웨이의 공개 키(PK_{MAGA})에 의해서 암호화되어 포함된다. 인증응답 메시지(Auth_Rsp)에는 로컬 모빌리티 앵커의 공개 키(PK_{LMA})에 의해 암호화된 마스터 세션 키(K^*)와 모바일 노드의 식별자(MN) 또한 포함된다. 또한, 인증응답 메시지(Auth_Rsp)에는 AAA 서버(405)의 비밀 키(SK_{AAA})를 이용한 서명($Sig(SK_{AAA})$)이 추가된다.

[0066] 모바일 액세스 게이트웨이(402)는 인증응답 메시지(Auth_Rsp)를 수신하면, 수신된 인증응답 메시지에 포함된 세션 키($K_{MN-MAGA}$)와 세션 키($K_{LMA-MAGA}$)를 이용하여 향후 모바일 노드(401) 및 로컬 모빌리티 앵커(403)와의 시그널링 메시지를 암호화하게 된다.

[0067] 다음으로, 모바일 액세스 게이트웨이(402)는 세션 키($K_{LMA-MAGA}$)를 이용하여 계산된 MAC을 PBU 메시지(④)를 통하여 로컬 모빌리티 앵커로 전송하고, 로컬 모빌리티 앵커로부터 PBA 메시지(⑤)를 통하여 응답을 수신할 수 있다. 다음으로, 모바일 액세스 게이트웨이(402)는 세션 키($K_{MN-MAGA}$)를 이용하여 계산된 MAC을 RtrAdv 메시지(⑥)를 통하여 모바일 노드(401)로 전달할 수 있다.

[0068] 여기에서, PBU 메시지, PBA 메시지, RtrAdv 메시지 각각의 역할은 앞서 도 1 및 도 2를 통하여 설명된 바와 동일하다.

[0069] 도 5는 본 발명에 따른 프락시 모바일 IPv6(PMIPv6)를 위한 핸드오버 처리 방법을 설명하기 위한 개념도이다.

[0070] 도 5를 참조하면, 모바일 노드(501)는 제1 모바일 액세스 게이트웨이(502)의 액세스 링크에서 제2 모바일 액세스 게이트웨이(504)의 액세스 링크로 접속이 핸드오버된다.

[0071] 먼저, 모바일 노드(501)가 자신이 제1 모바일 액세스 게이트웨이(502)로부터 제2 모바일 액세스 게이트웨이(504)로의 핸드오버하는 것이 임박함을 인지하면, 자신이 옮겨갈 제2 모바일 액세스 게이트웨이(504)의 식별자(MAG_B)와 타임 스탬프(T_1)를 포함한 Start_Auth 메시지(①)를 현재 접속된 제1 모바일 액세스 게이트웨이(502)로 전송한다.

[0072] 따라서, 제1 모바일 액세스 게이트웨이(501)는 모바일 노드(501)가 제1 모바일 액세스 게이트웨이(502)로부터 제2 모바일 액세스 게이트웨이(504)로 곧 핸드오버가 될 것임을 감지하게 된다.

[0073] 이에, 제1 모바일 액세스 게이트웨이(501)는 제2 모바일 액세스 게이트웨이의 식별자(MAG_B)와 타임 스탬프(T_1)를 포함한 인증요청(Auth_Req) 메시지(②)를 로컬 모빌리티 앵커(503)로 전송하고, 로컬 모빌리티 앵커(503)로부터 모바일 노드(501)와 제2 모바일 액세스 게이트웨이(504) 간에 공유될 세션 키($K_{MN-MAGB}$)와 로컬 모빌리티 앵커(503)와 제2 모바일 액세스 게이트웨이(504) 간에 공유될 세션 키($K_{LMA-MAGB}$)를 포함한 인증응답(Auth_Rsp) 메시지(③)를 수신한다. 상기 세션 키($K_{MN-MAGB}$)와 세션 키($K_{LMA-MAGB}$)는 상기 제2 모바일 액세스 게이트웨이(504)의 비밀 키(PK_{MAGB})로 암호화되어 상기 인증응답(Auth_Rsp)에 포함될 수 있고, 인증요청(Auth_Req) 메시지에는 이를 위해 제2 모바일 액세스 게이트웨이의 키(PK_{MAGB})가 포함될 수도 있다.

[0074] 이때, 상기 로컬 모빌리티 앵커(LMA)는 상기 제1 모바일 액세스 게이트웨이와 상기 제2 모바일 액세스 게이트웨이를 모두 관리하는 구성요소일 수 있으며, 제1 모바일 액세스 게이트웨이와 제2 모바일 액세스 게이트웨이는 동일한 PMIPV6 도메인 내에 속해있다.

[0075] 한편, 상기 세션 키($K_{MN-MAGB}$)와 세션 키($K_{LMA-MAGB}$)는 앞서 도 4를 통하여 설명된 보안연결 설정방법에서의 세션 키들과 유사하게, 상기 모바일 노드와 AAA 서버(도 5에서는 생략되었음)가 공유하는 대칭키(symmetric key) K_{MN}으로부터 생성된 마스터 세션 키(K^*)에 기초하여 생성될 수 있다. 여기에서, 마스터 세션 키(K^*)는 모바일 노드(501)가 제1 모바일 액세스 게이트웨이(502)에 대해 최초의 액세스를 수행하는 과정에서 이미 생성되어 있게 된다(도 4를 통하여 설명된 initial authentication procedure).

[0076] 앞서 언급된 바와 같이, 마스터 세션 키(K^*)는 상기 모바일 노드가 상기 PMIPv6 도메인 내에 수행하는 세션이 종료될 때까지만 유효하므로, 상기 세션 키($K_{MN-MAGB}$)와 세션 키($K_{LMA-MAGB}$) 또한 마스터 세션 키가 유효한 기간 내에서만 유효할 수 있다. 상기 세션 키($K_{MN-MAGB}$)는 상기 마스터 세션 키(K*)와 상기 제2 모바일 액세스 게이트웨이의 식별자(MAG_B)에 기초한 의사 랜덤 함수에 의해 생성될 수 있고, 상기 세션 키($K_{LMA-MAGB}$)는 상기 마스터 세션 키(K*)와 상기 로컬 모빌리티 앵커 및 제2 모바일 액세스 게이트웨이의 식별자(LMA, MAG_B)에 기초한 의사 랜덤 함수에 의해 생성될 수 이다.

[0077] 다음으로, 제1 모바일 액세스 게이트웨이(501)는 HI 메시지(④)를 통하여 제2 모바일 액세스 게이트웨이에게 앞서 인증응답 메시지를 통하여 수신한 세션 키($K_{MN-MAGB}$)와 세션 키($K_{LMA-MAGB}$)를 전달하고, 제2 모바일 액세스 게이트웨이로부터 Hack 메시지(⑤)로 응답을 수신한다. 이때, 세션 키($K_{MN-MAGB}$)와 세션 키($K_{LMA-MAGB}$)는 제2 모바일 액세스 게이트웨이의 비밀 키(PK_{MAGB})로 암호화되어 상기 HI 메시지(④)에 포함될 수 있다.

[0078] 다음으로, 제2 모바일 액세스 게이트웨이(504)는 PBU 메시지(⑥)와 PBA 메시지(⑦)를 통하여 로컬 모빌리티 앵커(503)와 세션 키($K_{LMA-MAGB}$)에 대한 검증을 수행할 수 있다.

[0079] 다음으로, 제2 모바일 액세스 게이트웨이(504)는 RtrAdv 메시지(⑧)를 통하여 모바일 노드(501)에게 세션 키

($K_{MN-MAGB}$)를 이용하여 계산된 MAC을 전달 할 수 있다.

[0080] 여기에서, PBU 메시지, PBA 메시지, RtrAdv 메시지 각각의 역할은 앞서 도 1 및 도 2를 통하여 설명된 바와 동일하다.

[0081] 이상에서, 살펴본 바와 같이, 본 발명에 따른 보안 연결 설정 방법과, 핸드오버 처리 방법은 다음과 같은 특징을 가지게 된다.

[0082] 첫째로, 본 발명에 따른 보안연결 설정 방법에서는 모바일 액세스 게이트웨이와 로컬 모빌리티 앵커간의 보안 연결뿐만 아니라, 모바일 노드와 모바일 액세스 게이트웨이간의 보안 연결이 설정된다. 따라서, 이들 연결을 통한 시그널링 메시지들이 공유 키들에 의해서 보호될 수가 있다.

[0083] 둘째로, 본 발명에 따른 핸드오버 처리 방법에서는AAA 서버와의 인증절차는 초기 액세스 과정(도 4를 통해서 설명된 보안연결 설정 방법)에 의해서 1차례만 수행되며, 핸드오버 과정에서는 로컬 모빌리티 앵커가 로컬 키 분배 센터(local key distribution center)의 역할을 수행하게 되므로, AAA 서버와의 인증 절차가 수행될 필요가 없게 된다. 따라서, 핸드오버 과정에서의 지연없이 빠른 핸드오버의 수행이 가능하다.

[0084] 셋째로, 본 발명에 따른 보안 연결 설정 방법과 핸드오버 처리 방법은 세션 키는 모바일 노드가 해당 PMIPv6 도메인 내에서 수행하는 세션이 종료될 때까지만 유효하다. 또한, 핸드오버가 발생될 때마다 세션 키는 새롭게 발행된다. 이에 따라, 세션 키의 우발적인 노출이 발행될 경우에도 종래의 방법들에 비하여 보안의 우려가 상대적으로 낮다.

[0085]

[0086] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

[0087] 301: 모바일 노드 302: 제1 모바일 액세스 게이트웨이

303: 로컬 모빌리티 앵커 304: 제2 모바일 액세스 게이트웨이

305: AAA 서버 306: PMIPv6 도메인

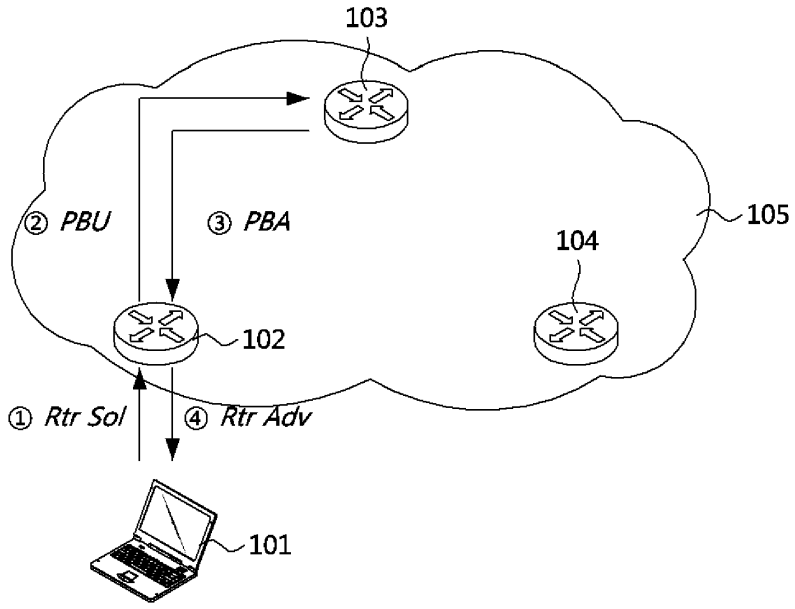
311: 모바일 노드와 AAA 서버간 공유 키

312: 마스터 세션 키

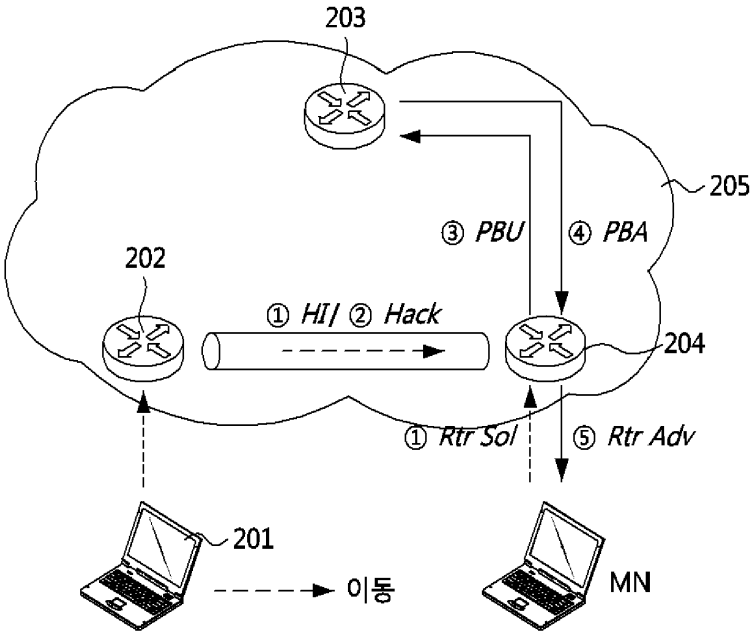
313, 314: 세션 키

도면

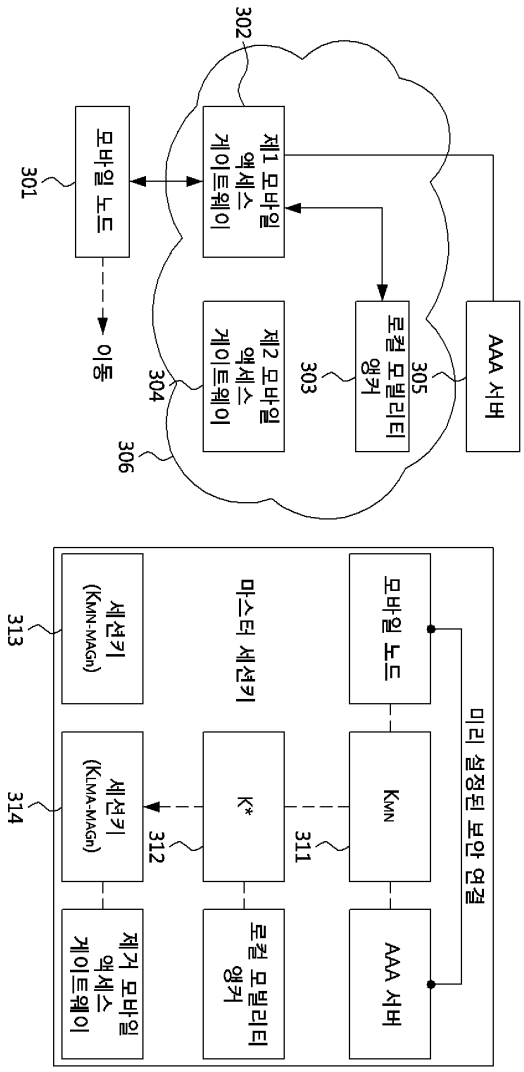
도면1


103
② PBU
③ PBA
105
104
102
① Rtr Sol
④ Rtr Adv
101

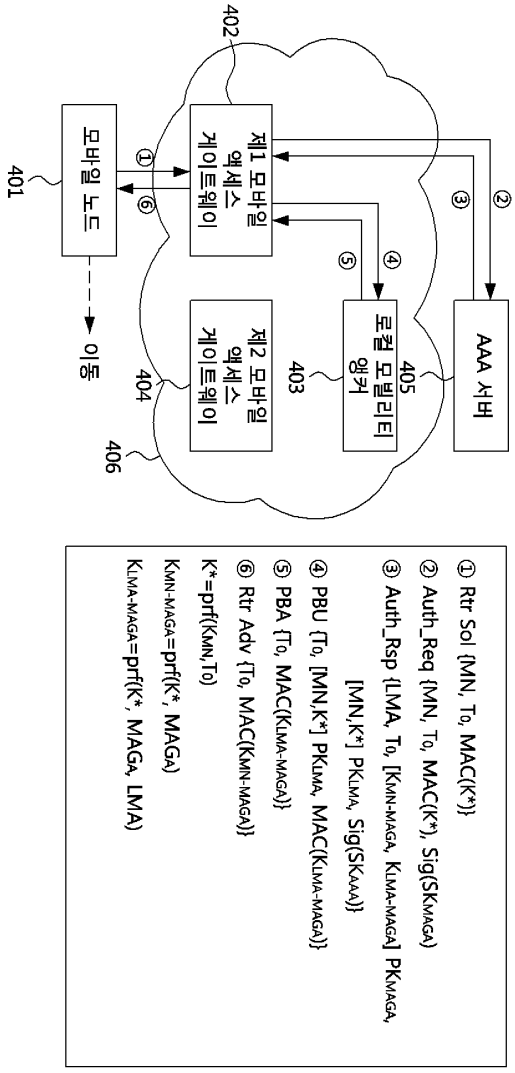
도면2


203
205
③ PBU
④ PBA
202
① HI/ ② Hack
204
① Rtr Sol
⑤ Rtr Adv
201
이동
MN

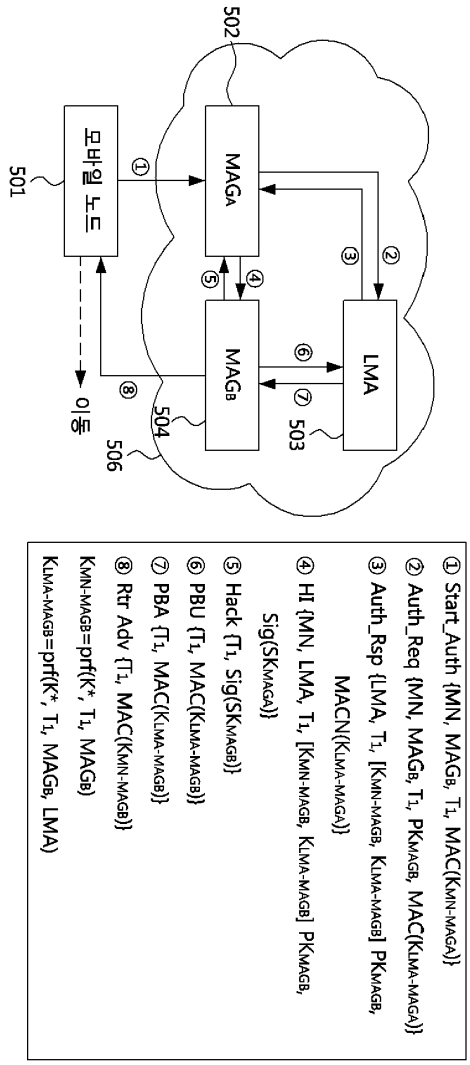
도면3


302
제1 모바일 액세스 게이트웨이
모바일 노드
301
이동
304
제2 모바일 액세스 게이트웨이
306
303
로컬 모빌리티 앵커
305
AAA 서버
미리 설정된 보안 연결
모바일 노드
KMN
AAA 서버
마스터 세션키
K*
로컬 모빌리티 앵커
311
312
세션키 (KMN-MAGn)
313
세션키 (KLMA-MAGn)
314
제거 모바일 액세스 게이트웨이

도면4


402
모바일 노드
401
제1 모바일 액세스 게이트웨이
제2 모바일 액세스 게이트웨이
404
로컬 모빌리티 앵커
405
403
AAA 서버
406
이동
① Rtr Sol {MN, T0, MAC(K*)}
② Auth_Req {MN, T0, MAC(K*), Sig(SKMAGA)
③ Auth_Rsp {LMA, T0, [KMN-MAGA, KLMA-MAGA] PKMAGA,
[MN,K*] PKLMA, Sig(SKAAA)}
④ PBU {T0, [MN,K*] PKLMA, MAC(KLMA-MAGA)}
⑤ PBA {T0, MAC(KLMA-MAGA)}
⑥ Rtr Adv {T0, MAC(KMN-MAGA)}
K*=prf(KMN,T0)
KMN-MAGA=prf(K*, MAGA)
KLMA-MAGA=prf(K*, MAGA, LMA)

도면5



① Start_Auth {MN, MAGB, T1, MAC(KMN-MAGA)}

② Auth_Req {MN, MAGB, T1, PKMAGB, MAC(KLMA-MAGA)}

③ Auth_Rsp {LMA, T1, [KMN-MAGB, KLMA-MAGB] PKMAGB, MACN(KLMA-MAGA)}

④ HI {MN, LMA, T1, [KMN-MAGB, KLMA-MAGB] PKMAGB, Sig(SKMAGA)}

⑤ Hack {T1, Sig(SKMAGB)}

⑥ PBU {T1, MAC(KLMA-MAGB)}

⑦ PBA {T1, MAC(KLMA-MAGB)}

⑧ Rtr Adv {T1, MAC(KMN-MAGB)}

KMN-MAGB=prf(K*, T1, MAGB)

KLMA-MAGB=prf(K*, T1, MAGB, LMA)