(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0033763
(43) 공개일자 2008년04월17일

(51) Int. Cl.
H04B 7/26 (2006.01)
(21) 출원번호 10-2006-0099900
(22) 출원일자 2006년10월13일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
손태식
경기 수원시 팔달구 인계동 1135-8 삼부오피스텔 1415
최선웅
서울 강남구 역삼2동 래미안아파트 104-1602
(뒷면에 계속)
(74) 대리인
박상수

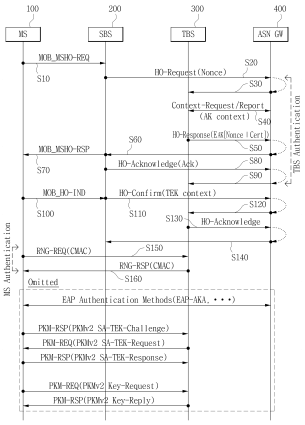
전체 청구항 수 : 총 31 항

(54) 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법및 그 시스템

(57) 요 약

본 발명은 제1 기지국에서 제2 기지국으로 핸드오버하고자 하는 무선단말이 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 과정과, 상기 제1 기지국이 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정과, 상기 제1 기지국이 상기 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정과, 상기 무선단말이 상기 제2 기지국으로부터 인증을 받기 위한 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 상기 전송된 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정으로 이루어진다.

대표도 - 도2



(72) 발명자

김선기

서울 송파구 오륜동 올림픽선수촌아파트 104-804

문강영

경기 용인시 수지구 풍덕천2동 1168번지 진산마을 삼성5차아파트510-201

특허청구의 범위

청구항 1

제1 기지국에서 제2 기지국으로 핸드오버하고자 하는 무선단말이 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 과정과,

상기 무선단말의 핸드오버 요청에 따라 제1 기지국이 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정과,

상기 제2 기지국이 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정과,

상기 제1 기지국이 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정과,

상기 무선단말이 상기 제2 기지국으로부터 인증을 받기 위한 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정과,

상기 제2 기지국이 상기 무선단말로부터 전송된 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정으로 이루어지는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 2

제 1항에 있어서,

상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서,

상기 핸드오버 요청 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 3

제 2항에 있어서,

상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값인 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 4

제 1항에 있어서,

상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서,

상기 핸드오버 응답 메시지는 상기 인증서버의 중계에 의해 상기 제1 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 5

제 4항에 있어서,

상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값이고, 상기 제2 기지국의 인증서는 상기 제2 기지국의 제조업체의 인증서 또는 ASP의 인증서인 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 6

제1항에 있어서,

상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 핸드오버 Ack 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 7

제 6항에 있어서,

상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 제1 기지국은 상기 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 해독하여 해독된 무선단말의 임시번호가 자신의 갖고 있는 무선단말의 임시번호와 일치하고, 상기 제2 기지국의 인증서가 정상인 경우 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 8

제 1항에 있어서,

상기 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 무선단말은 상기 제2 기지국과 공유하고 있는 인증키와 상기 무선단말의 임시번호로부터 생성되는 CMAC key를 이용하여 CMAC 값을 생성한 후 생성된 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 9

제 8항에 있어서,

상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정에서,

상기 제2 기지국은 무선단말의 CMAC 값과 자신의 인증키로부터 생성되는 CMAC key를 이용하여 생성되는 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 10

제 9항에 있어서,

상기 제2 기지국은 무선단말과의 CMAC 값이 동일한 경우 상기 인증키와 무선단말의 임시번호의 동일함을 증명하여 상기 무선단말을 인증하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법.

청구항 11

제1 기지국에서 제2 기지국으로 핸드오버하고자 하는 무선단말이 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 과정과,

상기 무선단말의 핸드오버 요청에 따라 제1 기지국이 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정과,

상기 제2 기지국이 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정과,

상기 제1 기지국이 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸

드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정으로 이루어지는 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 12

제 11항에 있어서,

상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서,

상기 핸드오버 요청 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 13

제 12항에 있어서,

상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값인 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 14

제 11항에 있어서,

상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서,

상기 핸드오버 응답 메시지는 상기 인증서버의 중계에 의해 상기 제1 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 15

제 14항에 있어서,

상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값이고, 상기 제2 기지국의 인증서는 상기 제2 기지국의 제조업체의 인증서 또는 ASP의 인증서인 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 16

제11항에 있어서,

상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 핸드오버 Ack 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 17

제 16항에 있어서,

상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 제1 기지국은 상기 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 해독하여 해독된 무선단말의 임시번호가 자신의 갖고 있는 무선단말의 임시번호와 일치하고, 상기 제2 기지국의 인증서가 정상인 경우 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법.

청구항 18

무선단말이 핸드오버하고자 하는 제2 기지국으로부터 인증을 받기 위한 CMAC 값이 포함된 통신초기 요청 메시지

를 상기 제2 기지국으로 전송하는 과정과,

상기 제2 기지국이 상기 무선단말로부터 전송된 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정으로 이루어지는 것을 특징으로 하는 와이브로 네트워크에서의 무선단말 인증 방법.

청구항 19

제 18항에 있어서,

상기 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정에서,

상기 무선단말은 상기 제2 기지국과 공유하고 있는 인증키와 상기 무선단말의 임시번호로부터 생성되는 CMAC key를 이용하여 CMAC 값을 생성한 후 생성된 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 무선단말 인증 방법.

청구항 20

제 19항에 있어서,

상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정에서,

상기 제2 기지국은 무선단말의 CMAC 값과 자신의 인증키로부터 생성되는 CMAC key를 이용하여 생성되는 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 하는 것을 특징으로 하는 와이브로 네트워크에서의 무선단말 인증 방법.

청구항 21

제 20항에 있어서,

상기 제2 기지국은 무선단말과의 CMAC 값이 동일한 경우 상기 인증키와 무선단말의 임시번호의 동일함을 증명하여 상기 무선단말을 인증하는 것을 특징으로 하는 와이브로 네트워크에서의 무선단말 인증 방법.

청구항 22

제1 기지국에서 제2 기지국으로 핸드오버 요청시 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 무선단말과,

상기 무선단말의 핸드오버 요청에 따라 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 제1 기지국과,

네트워크를 통해 연결된 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 제2 기지국을 포함하며,

상기 제1 기지국은 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하고,

상기 제2 기지국은 상기 무선단말로부터 CMAC 값이 포함된 통신초기 요청 메시지를 수신하는 경우 상기 수신된 무선단말의 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 23

제 22항에 있어서,

상기 핸드오버 요청 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 24

제 23항에 있어서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값인 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 25

제 22항에 있어서,

상기 핸드오버 응답 메시지는 상기 인증서버의 중계에 의해 상기 제1 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 26

제 25항에 있어서,

상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값이고, 상기 제2 기지국의 인증서는 상기 제2 기지국의 제조업체의 인증서 또는 ASP의 인증서인 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 27

제 22항에 있어서,

상기 핸드오버 Ack 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송되는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 28

제 27항에 있어서,

상기 제1 기지국은 상기 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 해독하여 해독된 무선단말의 임시번호가 자신의 갖고 있는 무선단말의 임시번호와 일치하고, 상기 제2 기지국의 인증서가 정상인 경우 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 29

제 22항에 있어서,

상기 무선단말은 상기 제2 기지국과 공유하고 있는 인증키와 상기 무선단말의 임시번호로부터 생성되는 CMAC key를 이용하여 CMAC 값을 생성한 후 생성된 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 30

제 29항에 있어서,

상기 제2 기지국은 무선단말의 CMAC 값과 자신의 인증키로부터 생성되는 CMAC key를 이용하여 생성되는 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

청구항 31

제 30항에 있어서,

상기 제2 기지국은 무선단말과의 CMAC 값이 동일한 경우 상기 인증키와 무선단말의 임시번호의 동일함을 증명하여 상기 무선단말을 인증하는 것을 특징으로 하는 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<9> 본 발명은 와이브로 네트워크에서의 상호인증(Mutual Authentication)을 통한 핸드오버 방법 및 그 시스템에 관한 것으로, 특히 모바일 와이브로 시스템에서 핸드오버 과정시 단말(Mobile Station)과 새로운 대상 기지국(Target Base Station)간의 필요한 인증 절차를 최소화시키고 효율적인 상호인증을 통해 핸드오버를 수행하는 와이브로 네트워크에서의 상호인증(Mutual Authentication)을 통한 핸드오버 방법 및 그 시스템에 관한 것이다.

<10> 컴퓨터, 전자, 통신 기술이 비약적으로 발전함에 따라 무선 통신망(Wireless Network)을 이용한 다양한 무선 통신 서비스가 제공되고 있다. 이에 따라, 무선 통신망을 이용한 이동 통신 시스템에서 제공하는 서비스는 음성 서비스뿐만이 아니라, 써킷(Circuit) 데이터, 패킷(Packet) 데이터 등과 같은 데이터를 전송하는 멀티미디어 통신 서비스로 발전해 가고 있다.

<11> 최근에는 정보통신의 발달로 ITU-R에서 표준으로 제정하고 있는 제 3 세대 이동 통신 시스템인 IMT-2000(International Mobile Telecommunication 2000)(예컨대, CDMA(Code Division Multiple Access)2000 1X, 3X, EV-DO, WCDMA(WideBand CDMA) 등)이 상용화되고 있다.

<12> IMT-2000은 개인의 이동성 및 서비스 이동성을 포함한 전세계적인 직접 로밍, 유선 전화와 동일한 수준의 통화 품질, 고속 패킷 데이터 서비스 및 유무선망의 결합에 의한 다양한 응용 서비스의 구현 등을 목표로 등장한 이동 통신 시스템으로, 기존의 음성 및 WAP 서비스 품질의 향상은 물론 각종 멀티미디어 서비스(AOD, VOD 등)를 보다 빠른 속도로 제공할 수 있다.

<13> 그러나, 이동 통신 시스템은 기지국 구축비용이 높기 때문에 무선 인터넷의 이용 요금이 높고, 이동 통신 단말기의 화면 크기가 작기 때문에 이용할 수 있는 컨텐츠에 제약이 있는 등 초고속 무선 인터넷을 제공하기에는 한계가 있다.

<14> 또한, 무선 랜(WLAN : Wireless Local Area Network) 기술은 전파 간섭 및 좁은 사용 영역(Coverage) 등의 문제로 공중 서비스의 제공에 한계가 있음으로, 휴대성과 이동성을 보장하며 저렴한 요금으로 초고속 무선 인터넷 서비스를 이용할 수 있는 초고속 휴대 인터넷 서비스인 와이브로(WiBro : Wireless Broadband Internet)가 대두되고 있다. 이러한, 와이브로는 'IEEE 802.16e'으로 정의되어 있다.

<15> 이러한 와이브로 서비스는 와이브로 단말(노트북, PDA, Handheld PC 등)을 이용하여 실내 및 실외의 정지 환경에서와 보행 속도 및 중저속 이동 수준의 이동 환경에서 인터넷에 접속하여 다양한 정보 및 컨텐츠 이용이 가능하다. 또한, 와이브로 시스템은 시속 60 km/h의 이동성을 제공하며, 하향 전송 속도는 24.8 Mbps이나 상향 전송 속도는 5.2 Mbps로 상하향 비대칭 전송 특성을 갖는 IP(Internet Protocol) 기반의 무선 데이터 시스템이다.

<16> 이러한 와이브로 단말은 단순히 무선 인터넷 기능만 지원하는 것이 아니라, 카메라 기능, 휴대 저장 기능 등과 같은 다양한 부가 기능을 지원한다.

<17> 특히, WiBro(802.16e) 단말기는 BS(Base Station)라 불리는 와이브로 기지국까지 무선으로 통신하고 그 이후는 유선으로 인터넷 망에 연결되어진다. 와이브로 기지국은 사업자의 Core망으로 연결되어 Core 망의 한쪽에는 사용자 및 기기 인증을 위한 AAA 서버가 위치하게 된다.

<18> 이러한 WiBro(802.16e) 서비스는 사용자가 한 와이브로 기지국의 영역 안에서 다른 와이브로 기지국의 영역으로 이동하는 중에도 끊김 없는 서비스(Seamless Service)를 제공해 주지만, 이러한 핸드오버 과정에서 인증 절차가 포함되는 경우 끊김 없는 서비스(Seamless Service)를 제공할 수 없다는 단점을 갖게 된다.

<19> 구체적으로, IEEE 802.16e 표준문서[1]에 정의되어 있는 기술로서 핸드오버가 필요한 경우 초기 네트워크 진입과 같은 완전한 재인증을 수행하는 방법과 HO Optimization Flag를 사용하여 인증 과정을 축약하는 방법이 있다.

<20> 초기 네트워크 진입시의 인증은 SBC-REQ/RSP의 security negotiation과정을 시작으로 PKM EAP, SA-TEK, TEK 생성 등 모든 과정을 수행하는 full-authentication을 의미한다. 반면에 HO Optimization Flag를 사용하는 경우에는 앞서 언급한 PKM EAP, SA-TEK와 같은 과정 등을 일부 생략하여 인증 과정을 단축 수행할 수 있다.

<21> 이러한 종래 기술은 본질적으로 핸드오버 과정 중에 Target BS와 MS간 부가적인 인증 메시지 교환을 필요로 한다. 즉, 핸드오버 과정시 full-authentication은 SBC Negotiation, PKM EAP Phase, SA-TEK Phase, TEK Creation Phase 등의 절차를 수행함으로써 이동간 Seamless 서비스 제공에 영향을 미친다. 하지만 이러한 HO 과정시 full-authentication 없이 효율적 인증 기능을 제공하기 위한 방법으로 HO Optimization Flag[1]를 사용하여 인증과정을 축약시키는 방법이 있다. 하지만 HO Optimization을 사용하는 방법은 아래와 같은 문제점들을 가진다.

<22> HO Optimization Flag의 Bit #1을 사용하는 경우 인증 과정 중 PKM EAP 과정이 생략되지만 Target BS와 MS간 Security Context의 정당성을 확인하는 SA-TEK 3-Way Handshake 과정이 수반되며, 또한 TEK 키 생성 과정이 필요하다. 그러므로 PKM EAP Phase가 생략될 수 있지만, 5회의 부가적 인증 메시지 교환 및 128bits 키 생성이 수반되는 성능 문제를 야기할 수 있다.

<23> 또한, HO Optimization Flag Bit #2번을 사용하는 경우에는 TEK Creation 과정까지 모두 생략할 수 있지만, 이 경우는 MS가 새로 진입하려는 Target BS에 대한 신뢰관계가 사전에 가정되어야만 가능하다. 그러므로 HO Optimization Flag 2번의 경우에는 상호 인증 과정이 생략됨으로써 MS나 BS masquerading 문제점이 발생하게 된다.

발명이 이루고자 하는 기술적 과제

<24> 따라서, 본 발명의 목적은 상기와 같은 문제점을 해결하기 위한 것으로서, 본 발명은 기존의 핸드오버 과정시 필수적으로 수반되는 인증 절차를 기본 핸드과정 절차에 포함시킴으로써, 보다 효율적인 핸드오버 기능 제공 및 상호 인증 기능을 통해 보안성을 향상시킬 수 있도록 한 네트워크에서의 상호인증(Mutual Authentication)을 통한 핸드오버 방법 및 그 시스템을 제공함에 있다.

발명의 구성 및 작용

<25> 상기한 목적을 달성하기 위한 본 발명에 따른 와이브로 네트워크에서의 상호인증을 통한 핸드오버 방법의 일 측면에 따르면, 제1 기지국에서 제2 기지국으로 핸드오버하고자 하는 무선단말이 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 과정과, 상기 무선단말의 핸드오버 요청에 따라 제1 기지국이 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정과, 상기 제1 기지국이 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정과, 상기 무선단말이 상기 제2 기지국으로부터 인증을 받기 위한 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 상기 무선단말로부터 전송된 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정으로 이루어지는 것을 특징으로 한다.

<26> 상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서, 상기 핸드오버 요청 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송된다.

<27> 상기 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정에서, 상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값이다.

<28> 상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서, 상기 핸드오버 응답 메시지는 상기 인증서버의 중계에 의해 상기 제1 기지국으로 전송된다.

<29> 상기 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정에서, 상기 무선단말의 임시번호는 상기 제2 기지국을 인증하기 위한 무선단말의 Nonce 값이고, 상기 제2 기지국의 인증서는 상기 제2 기지국의 제조업체의 인증서 또는 ASP의 인증서이다.

<30> 상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서, 상기 핸드오버 Ack 메시지는 상기 인증서버의 중계에 의해 상기 제2 기지국으로 전송된다.

<31> 상기 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정에서, 상기 제1 기지국은 상기 핸드오버 응답

메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 해독하여 해독된 무선단말의 임시번호가 자신의 갖고 있는 무선단말의 임시번호와 일치하고, 상기 제2 기지국의 인증서가 정상인 경우 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송한다.

<32> 상기 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정에서, 상기 무선단말은 상기 제2 기지국과 공유하고 있는 인증키와 상기 무선단말의 임시번호로부터 생성되는 CMAC key를 이용하여 CMAC 값을 생성한 후 생성된 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송한다.

<33> 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정에서, 상기 제2 기지국은 무선단말의 CMAC 값과 자신의 인증키로부터 생성되는 CMAC key를 이용하여 생성되는 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송한다.

<34> 특히, 상기 제2 기지국은 무선단말과의 CMAC 값이 동일한 경우 상기 인증키와 무선단말의 임시번호의 동일함을 증명하여 상기 무선단말을 인증하게 된다.

<35> 또한, 상기한 목적을 달성하기 위한 본 발명에 따른 와이브로 네트워크에서의 핸드오버 대상 기지국 인증 방법의 일 측면에 따르면, 제1 기지국에서 제2 기지국으로 핸드오버하고자 하는 무선단말이 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 과정과, 상기 무선단말의 핸드오버 요청에 따라 제1 기지국이 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 과정과, 상기 제1 기지국이 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하는 과정으로 이루어지는 것을 특징으로 한다.

<36> 또한, 상기한 목적을 달성하기 위한 본 발명에 따른 와이브로 네트워크에서의 무선단말 인증 방법의 일 측면에 따르면, 무선단말이 핸드오버하고자 하는 제2 기지국으로부터 인증을 받기 위한 CMAC 값이 포함된 통신초기 요청 메시지를 상기 제2 기지국으로 전송하는 과정과, 상기 제2 기지국이 상기 무선단말로부터 전송된 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 과정으로 이루어지는 것을 특징으로 한다.

<37> 한편, 상기한 목적을 달성하기 위한 본 발명에 따른 와이브로 네트워크에서의 상호인증을 통한 핸드오버 시스템의 일 측면에 따르면, 제1 기지국에서 제2 기지국으로 핸드오버 요청시 자신의 임시번호를 생성하여 상기 제1 기지국으로 핸드오버 요청을 하는 무선단말과, 상기 무선단말의 핸드오버 요청에 따라 상기 무선단말의 임시번호를 저장하기 위한 필드가 포함된 핸드오버 요청 메시지를 제2 기지국으로 전송하는 제1 기지국과, 네트워크를 통해 연결된 인증서버로부터 수신한 인증키를 이용하여 암호화한 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 저장하기 위한 각각의 필드가 포함된 핸드오버 응답 메시지를 상기 제1 기지국으로 전송하는 제2 기지국을 포함하며, 상기 제1 기지국은 상기 제2 기지국으로부터 전송된 핸드오버 응답 메시지내의 암호화된 상기 무선단말의 임시번호와 상기 제2 기지국의 인증서를 검증하여 상기 제2 기지국의 인증 결과를 저장하기 위한 필드가 포함된 핸드오버 Ack 메시지를 상기 제2 기지국으로 전송하고, 상기 제2 기지국은 상기 무선단말로부터 CMAC 값이 포함된 통신초기 요청 메시지를 수신하는 경우 상기 수신된 무선단말의 CMAC 값과 자신의 CMAC 값이 동일한 경우 상기 무선단말을 인증하여 상기 통신초기 요청 메시지에 대한 응답 메시지를 상기 무선단말로 전송하는 것을 특징으로 한다.

<38> 이하, 본 발명의 바람직한 실시예의 상세한 설명이 첨부된 도면들을 참조하여 설명될 것이다. 도면들 중 참조번호들 및 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 참조번호들 및 부호들로 나타내고 있음에 유의해야 한다. 하기에서 본 발명을 설명함에 있어, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략한다.

<39> 도 1은 본 발명에 따른 모바일 와이브로 네트워크 구성을 나타내는 도면이다.

<40> 도 1에 도시된 바와 같이, 본 발명의 모바일 와이브로 시스템은 MS(Mobile Station)(100)와, SBS(Serving Base Station)(200)와, TBS(Target Base Station)(300)와, ASN GW(Access Service Network Gateway)(400)로 구성된다.

<41> MS(100)는 SBS(200)에 연결되어 무선통신 서비스를 제공받고 있는 상태이며, TBS(300)로 핸드오버(Handover, 이하 'HO'라 칭함)를 시도하기 이전에 SBS(200)와 이미 상호 인증 과정을 수행하여 서로간의 인증키 등의

Security Context를 공유하고 있는 상태이다.

<42> MS(100)는 SBS(200)의 서비스 영역내에서 서비스를 받는 중에 TBS(300)로 핸드오버를 하고자 하는 경우 SBS(200)가 TBS(300)를 인증하기 위한 Challenge-Response 과정을 시작하기 위한 Nonce값을 생성하고, 생성된 Nonce값이 포함된 핸드오버 요청 메시지(MOB_MSHO-REQ)를 SBS(200)로 전송하게 된다.

<43> SBS(Serving Base Station)(200)는 해당 서비스 영역내에 위치한 MS에게 무선통신 서비스를 제공하기 위한 기지국으로서, MS(100)로부터 핸드오버 요청 메시지(MOB_MSHO-REQ)를 수신하게 되면, 핸드오버를 위한 요청 메시지{HO-Request(MSID, Nonce)}를 TBS(300)로 전송하게 된다. 이때, SBS(200)로부터 전송되는 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}는 ASN GW(Access Service Network Gateway)(400)의 중계(Relay)에 의해 TBS(300)로 전송된다.

<44> 여기서, SBS(200)가 TBS(300)로 전송하는 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}에 포함된 MSID는 MS의 ID이고, Nonce는 SBS(200)가 TBS(300)를 인증하기 위한 Challenge-Response 과정을 시작하기 위한 Nonce값을 의미한다.

<45> TBS(Target Base Station)(300)는 MS(100)가 핸드오버하기 위한 핸드오버 대상 기지국으로서, SBS(200)로부터 전송되는 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}를 수신하고, ASN GW(Access Service Network Gateway)(400)로 해당 MSID의 AK Context(Authorization Key Context of MS, 이하 'AK'라 칭함)를 요청하여 관련 정보를 수신하게 되면, SBS(200)로부터 전송된 핸드오버 요청 메시지에 대한 수정된 핸드오버 응답 메시지{HO-Reponse(E_{AK}[Nonce//Cert])}를 ASN GW(Access Service Network Gateway)(400)를 통해 SBS(200)로 중계 전송하게 된다. 이때, TBS(300)는 수정된 핸드오버 응답 메시지{HO-Reponse(E_{AK}[Nonce//Cert])}에 포함된 Nonce와 인증서(Cert)를 인증키(AK)로 암호화하여 전송하게 된다.

<46> SBS(200)는 TBS(300)로부터 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}의 암호화된 Nonce와 인증서(Cert)를 검증하여 TBS(300)에 대한 인증 결과를 전달하기 위한 수정된 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)를 통해 TBS(300)로 전송하게 된다.

<47> 즉, SBS(200)는 TBS(300)로부터 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}를 수신하는 경우, 암호화된 Nonce와 인증서(Cert)를 해독하게 되며, 자신이 갖고 있는 Nonce 값과 해독된 Nonce 값을 비교하여 만약 자신의 Nonce 값과 해독된 Nonce 값이 동일하고 해독된 인증서(Cert) 또한 정상적인 인증서인 경우, TBS(300)에 대한 인증 결과를 전달하기 위한 수정된 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)를 통해 TBS(300)로 전송하게 된다. 여기서 인증서(Cert)는 TBS의 제조업체 인증서 또는 ASP의 인증서(Manufacturer's Certification or ASP's Certification)를 의미한다.

<48> ASN GW(Access Service Network Gateway)(400)는 AAA 서버(인증 서버)의 역할을 함께 수행하게 되며, ASN GW와 AAA 서버가 분리된 경우에도 본원발명을 동일하게 적용할 수 있다.

<49> 또한, MS(100)는 TBS(300)에 대한 인증 과정이 종료됨에 따라, MOB_HO-IND 메시지를 SBS(200)로 전송하게 되고, SBS(200)는 HO_Confirm{TEK(Traffic Encription Key) Context} 메시지를 ASN GW(Access Service Network Gateway)(400)를 통해 검증된 TBS(300)로 전송하게 된다.

<50> TBS(300)는 SBS(200)로부터 전송된 HO_Confirm{TEK(Traffic Encription Key) Context} 메시지에 대한 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)를 통해 SBS(200)로 전송하게 된다.

<51> 또한, MS(100)는 TBS(300)로부터 인증을 받기 위한 RNG-REQ(Ranging Request || CMAC or HMAC) 요청 메시지를 TBS(300)로 전송하게 된다. 이때, MS(100)와 TBS(300)는 이미 같은 AK를 공유하고 있으므로, 각각 AK와 Nonce로부터 CMAC key(or HMAC key)를 생성할 수 있게 된다. 즉, Ranging 과정시 MS(100)는 Ranging 메시지에 대한 CMAC 값을 CMAC Key를 이용하여 생성한 후 TBS(300)에게 전달한다.

<52> TBS(300)는 MS(100)로부터 CMAC 값을 전달받게 되면 자신의 CMAC key를 사용한 CMAC 값을 생성하여 생성된 CMAC 값이 MS(100)로부터 전달된 CMAC 값과 동일한 경우 Ranging Message 자체 인증은 물론 AK, Nonce의 동일함을 증명함으로써 MS(100)를 인증한 후 MS(100)로부터 전송된 RNG-REQ(Ranging Request || CMAC or HMAC) 요청 메시지에 대한 RNG-RSP(Ranging Response || CMAC or HMAC) 응답 메시지를 MS(100)로 전송하게 된다.

<53> 도 2는 본 발명에 따른 와이브로 네트워크에서의 상호인증을 통한 핸드오버 과정을 나타내는 도면이고, 도 3은 도 2의 TBS 인증 과정에서의 HO-Request 메시지 포맷을 나타내는 도면이며, 도 4는 도 2의 TBS 인증 과정에서의

HO-Response 메시지 포맷을 나타내는 도면이고, 도 5는 도 2의 TBS 인증 과정에서의 HO-Acknowledge 메시지 포맷을 나타내는 도면이다.

<54> 도 2에 도시된 바와 같이, MS(100)는 SBS(200)에 연결되어 서비스를 제공받는 중이며 이후 TBS(300)로 핸드오버(Handover, 이하 'HO'라 칭함)를 시도하려는 중이다. 이때 ASN GW(400)는 AAA 서버(인증 서버)의 역할을 함께 수행하게 되며, ASN GW와 AAA 서버가 분리된 경우에도 동일하게 적용 가능하다.

<55> 특히, 본 발명에서는 MS(100)의 TBS 인증을 위해서 기존의 핸드오버 과정에서 사용되던 메시지 중 HO-Request, HO-Response, HO-Acknowledge 메시지에 인증 관련 필드를 추가한다. 또한 TBS(300)의 MS 인증을 위해 Ranging 메시지들을 검증하기 위해 HMAC/CMAC tuple을 적용한다.

<56> MS(100)와 SBS(200)는 핸드오버가 일어나기 이전에 이미 상호 인증 과정을 수행하여 서로간의 인증키 등의 Security Context를 공유하고 있는 상태에서, SBS(200)의 서비스 영역내에 위치한 MS(100)는 SBS(200)가 TBS(300)를 인증하기 위한 Challenge-Response 과정을 시작하기 위한 Nonce값을 생성하고, 생성된 Nonce값이 포함된 핸드오버 요청 메시지(MOB_MSHO-REQ)를 SBS(200)로 전송(S10)하게 된다.

<57> 이에 따라, SBS(200)는 MS(100)로부터 핸드오버 요청 메시지(MOB_MSHO-REQ)를 수신하게 되면, 핸드오버를 위한 요청 메시지{HO-Request(MSID, Nonce)}를 TBS(300)로 전송(S20)하게 된다. 이때, SBS(200)로부터 전송되는 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}는 우선 ASN GW(Access Service Network Gateway)(400)로 전송되어지고, ASN GW(Access Service Network Gateway)(400)의 중계(Relay)에 의해 TBS(300)로 전송(S30)되어진다.

<58> 여기서, 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}에 포함된 MSID는 MS의 ID이고, Nonce는 SBS(200)가 TBS(300)를 인증하기 위한 Challenge-Response 과정을 시작하기 위한 Nonce값을 의미하는 것이다.

<59> 즉, 상기 Nonce값을 전달하기 위한 수정된 HO-Request 메시지 포맷은 도 3과 같이 구성되어지며, 각 필드의 설명은 하기의 표 1과 같다.

표 1

<60>

IE(Information Element) Name	Description	M/O(Mandatory/Optional)
HO Type	Describes type of the HO(FBSS, MDHO, HHO)	M
MS Info	Contains HO-related MS context in the nested IFs.	M
MS ID	6 Octet MS ID(MAC Address)	M
...	...	...
MS Nonce	**MS generated one time random number**	**O**

<61> 즉, 상기 표 1에서와 같이 수정된 HO-Request 메시지 포맷(13 mandatory fields, 14 optional + 1 proposed field)은 MS Nonce 필드가 새롭게 추가되어 임의의 숫자(random number)가 저장될 수 있도록 한다.

<62> 이어서, 핸드오버 요청 메시지{HO-Request(MSID, Nonce)}가 ASN GW(Access Service Network Gateway)(400)의 중계(Relay)에 의해 TBS(300)로 전송되어지면, TBS(300)는 ASN GW(Access Service Network Gateway)(400)로 해당 MSID의 AK Context(Authorization Key Context of MS, 이하 'AK'라 칭함)를 요청하여 관련 정보를 수신하게 된다(Context-Request/Report)(S40).

<63> 이에 따라, SBS(200)로부터 전송된 Nonce 값이 포함된 핸드오버 요청 메시지와 ASN GW(Access Service Network Gateway)(400)로부터 전송된 MSID의 AK Context 관련 정보를 수신한 TBS(300)는 상기 SBS(200)로부터 전송된 핸드오버 요청 메시지에 대한 수정된 핸드오버 응답 메시지{HO-Reponse(E_{AK}[Nonce//Cert])}를 ASN GW(Access Service Network Gateway)(400)로 전송(S50)하게 된다.

<64> 이때, TBS(300)는 수정된 핸드오버 응답 메시지{HO-Reponse(E_{AK}[Nonce//Cert])}에 포함된 Nonce와 인증서(Cert)를 AK로 암호화하여 전송하게 된다.

<65> 이에 따라, ASN GW(Access Service Network Gateway)(400)는 TBS(300)로부터 전송된 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}를 SBS(200)로 중계 전송(S60)하게 된다.

<66> 여기서, 상기 수정된 핸드오버 응답 메시지{HO-Reponse(E_{AK}[Nonce//Cert])}의 포맷은 도 4와 같이 구성되어지며, 각 필드의 설명은 하기의 표 2와 같다.

표 2

<67>

IE(Information Element) Name	Description	M/O(Mandatory/Optional)
HO Type	Describes type of the HO(FBSS, MDHO, HHO)	M
Result Code	The result of the Requset	M
MS ID	6 Octet MS ID(MAC Address)	M
...	...	...
MS Nonce	**MS generated one time random number**	**O**
Cert	**Manufacturer's Certification or ASP's Certification**	**O**

<68> 즉, 상기 표 2에서와 같이 수정된 HO-Response 메시지 포맷(12 mandatory fields, 7 optional + 2 proposed field)은 MS Nonce 필드와 Cert 필드가 새롭게 추가되어 구성되며, MS Nonce 필드에는 임의의 숫자(random number)가 저장되어진다.

<69> 이어서, TBS(300)로부터 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}를 전송받은 SBS(200)는 MS(100)로 MOB_MSHO_RSP 메시지를 전송(S70)하게 된다.

<70> 이어서, SBS(200)는 TBS(300)로부터 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}의 암호화된 Nonce 와 인증서(Cert)를 검증하여 TBS(300)에 대한 인증 결과를 전달하기 위한 수정된 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)로 전송(S80)하게 된다.

<71> 즉, SBS(200)는 TBS(300)로부터 수정된 핸드오버 응답 메시지{HO-Request(E_{AK}[Nonce||Cert])}를 수신하는 경우, 암호화된 Nonce와 인증서(Cert)를 해독하게 되며, 여기서 인증서(Cert)는 상기 표 2에서와 같이 TBS의 제조업체 인증서 또는 ASP의 인증서(Manufacturer's Certification or ASP's Certification)를 의미하는 것이다.

<72> 이와 같이, SBS(200)는 암호화된 Nonce 와 인증서(Cert)를 해독하는 경우 먼저 자신이 갖고 있는 Nonce 값과 해독된 Nonce 값을 비교하여 만약 자신의 Nonce 값과 해독된 Nonce 값이 동일하고 해독된 인증서(Cert) 또한 정상적인 인증서인 경우, TBS(300)에 대한 인증 결과를 전달하기 위한 수정된 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)로 전송하게 되는 것이다.

<73> 이에 따라, ASN GW(Access Service Network Gateway)(400)는 상기 SBS(200)로부터 전송된 수정된 HO-Acknowledge 메시지를 TBS(300)로 중계 전송(S90)함으로써 TBS 인증과정(Challenge Response skim)을 종료하게 된다.

<74> 여기서, 상기 TBS 인증 결과를 전달하기 위한 수정된 HO-Acknowledge 메시지 포맷(2 mandatory fields, 1 proposed field)은 도 5와 같이 구성되어지며, 각 필드의 설명은 하기의 표 3과 같다.

표 3

<75>

IE(Information Element) Name	Description	M/O(Mandatory/Optional)
MS Info	Contains HO-related MS context in the nested IFs.	M
MS ID	6 Octet MS ID(MAC Address)	M
Auth Ack	**The result of TBS Authentication**	**O**

<76> 즉, 상기 표 3에서와 같이 수정된 HO-Acknowledge 메시지 포맷(2 mandatory fields, 1 proposed field)은 Auth Akc 필드가 새롭게 추가되어 구성되어진다.

<77> 이어서, TBS 인증과정(Challenge Response skim)이 종료되어지면, MS(100)는 MOB_HO-IND 메시지를 SBS(200)로

전송(S100)하게 되고, MS(100)로부터 MOB_HO-IND 메시지를 전송받은 SBS(200)는 HO_Confirm{TEK(Traffic Encription Key) Context} 메시지를 ASN GW(Access Service Network Gateway)(400)로 전송(S110)하게 된다.

<78> 이에 따라, ASN GW(Access Service Network Gateway)(400)는 SBS(20)로부터 전송된 HO_Confirm{TEK(Traffic Encription Key) Context} 메시지를 검증된 TBS(300)로 중계 전송(S120)하게 된다.

<79> 이에 따라, TBS(300)는 SBS(200)로부터 전송된 HO_Confirm{TEK(Traffic Encription Key) Context} 메시지에 대한 HO-Acknowledge 메시지를 ASN GW(Access Service Network Gateway)(400)로 전송(S130)함에 따라, ASN GW(Access Service Network Gateway)(400)는 TBS(300)로부터 전송된 HO-Acknowledge 메시지를 SBS(200)로 중계 전송(S140)하게 된다.

<80> 이어서, MS(100)는 TBS(300)로부터 단말 인증을 받기 위한 RNG-REQ(Ranging Request || CMAC or HMAC) 요청 메시지를 TBS(300)로 전송(S150)하게 되면, TBS(300)는 MS(100)로부터 전송된 RNG-REQ(Ranging Request || CMAC or HMAC) 요청 메시지에 대한 RNG-RSP(Ranging Response || CMAC or HMAC) 응답 메시지를 MS(100)로 전송(S160)하게 된다.

<81> 즉, MS(100)와 TBS(300)는 이미 같은 AK를 공유하고 있으므로 각각 AK와 Nonce로부터 하기와 같이 CMAC key(or HMAC key)를 생성할 수 있게 된다.

<82> CMAC_KEY = modified_Dot16KDF(AK, SS MAC Address || BSID || "CMAC_KEYS+KEK", 384, Nonce)

<83> HMAC_KEY = modified_Dot16KDF(AK, SS MAC Address || BSID || "HMAC_KEYS+KEK", 448, Nonce)

<84> 이에 따라, 상술한 Ranging 과정시 MS(100)는 Ranging 메시지에 대한 CMAC 값을 상기 생성된 CMAC Key를 이용하여 생성한 후 TBS(300)에게 전달하게 된다.

<85> 이에 따라, MS(100)로부터 CMAC 값을 전달받은 TBS(300) 역시 자신의 CMAC key를 이용하여 CMAC 값을 생성하고, 생성된 CMAC 값이 MS(100)로부터 전달된 CMAC 값과 동일한 경우 Ranging Message 자체 인증은 물론 AK, Nonce의 동일함을 증명함으로써 MS(100)를 인증할 수 있게 된다.

<86> 상술한 바와 같이, 본 발명에서는 와이브로 단말의 핸드오버 과정에서 필수적으로 수반되어지는 인증 절차를 기본 핸드오버 절차에 포함시킴으로써, 기존의 보안을 위한 인증 과정을 생략하여 보다 효율적으로 핸드오버를 수행할 수 있게 된다.

<87> 이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능할 것이다.

발명의 효과

<88> 본 발명에 따르면, 기존의 기존 와이브로 네트워크상에서 핸드오버 과정시 PKM Phase, TEK 관련 Phase 등 부가적인 메시지의 교환 없이 필수적으로 수반되는 인증 절차를 기본 핸드오버 절차에 포함시킴으로써, 끊김 없는 서비스(Seamless Service)로 보다 효율적인 핸드오버 기능 제공 및 상호 인증 기능을 통해 보안성을 향상시킬 수 있는 효과가 발생하게 된다.

도면의 간단한 설명

<1> 도 1은 본 발명에 따른 모바일 와이브로 네트워크 구성을 나타내는 도면.

<2> 도 2는 본 발명에 따른 와이브로 네트워크에서의 상호인증을 통한 핸드오버 과정을 나타내는 도면.

<3> 도 3은 도 2의 TBS 인증 과정에서의 HO-Request 메시지 포맷을 나타내는 도면.

<4> 도 4는 도 2의 TBS 인증 과정에서의 HO-Response 메시지 포맷을 나타내는 도면.

<5> 도 5는 도 2의 TBS 인증 과정에서의 HO-Acknowledge 메시지 포맷을 나타내는 도면.

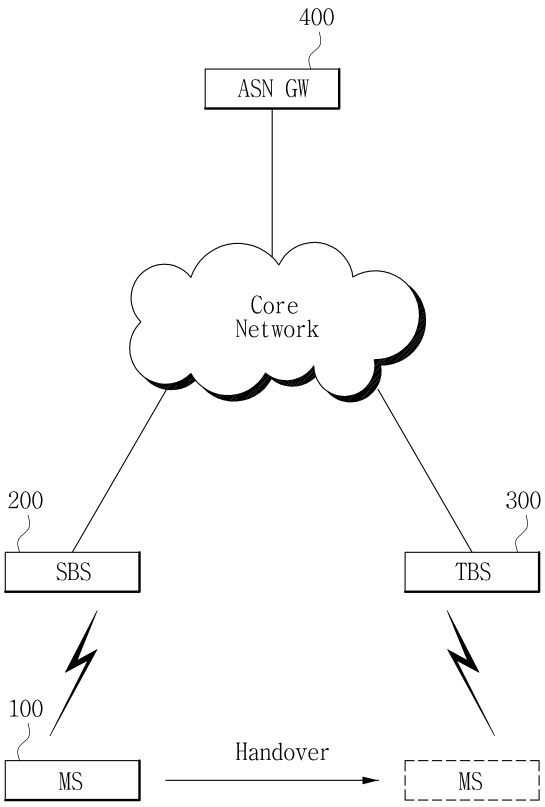
<6> * 도면의 주요 부분에 대한 부호의 설명 *

<7> 100 : 와이브로 단말 200 : 서비스 기지국(SBS)

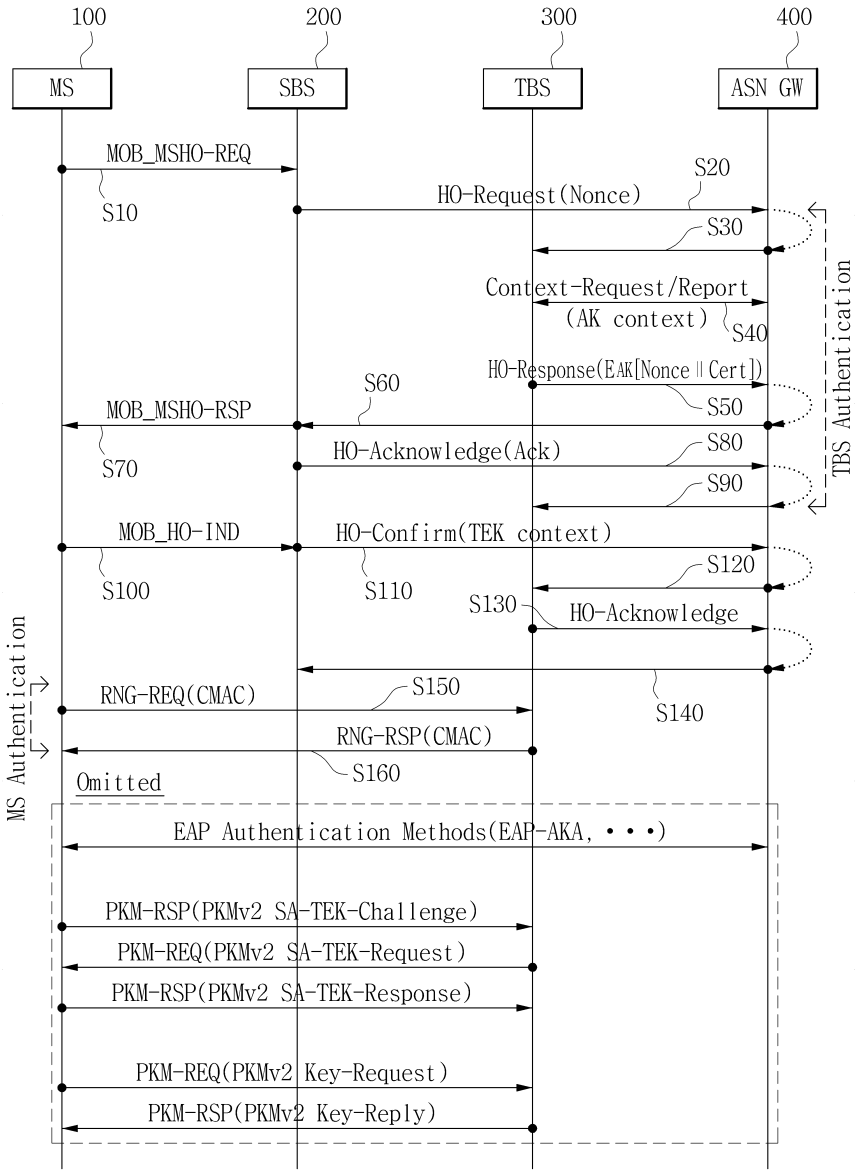
<8> 300 : 핸드오버 대상 기지국(TBS) 400 : ASN GW

도면

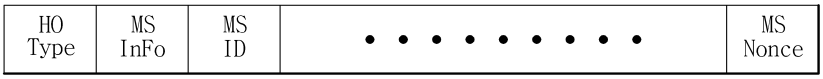
도면1



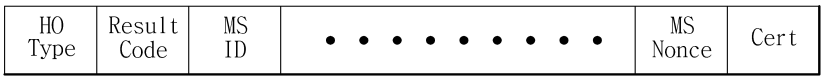
도면2


100
200
300
400
MS
SBS
TBS
ASN GW
MOB_MSHO-REQ
S10
HO-Request(Nonce)
S20
S30
Context-Request/Report
(AK context)
S40
HO-Response(EAK[Nonce ‖ Cert])
S50
TBS Authentication
S60
MOB_MSHO-RSP
S70
HO-Acknowledge(Ack)
S80
S90
MOB_HO-IND
S100
HO-Confirm(TEK context)
S110
S120
S130
HO-Acknowledge
S140
MS Authentication
RNG-REQ(CMAC)
S150
RNG-RSP(CMAC)
S160
Omitted
EAP Authentication Methods(EAP-AKA, • • •)
PKM-RSP(PKMv2 SA-TEK-Challenge)
PKM-REQ(PKMv2 SA-TEK-Request)
PKM-RSP(PKMv2 SA-TEK-Response)
PKM-REQ(PKMv2 Key-Request)
PKM-RSP(PKMv2 Key-Reply)

도면3


HO Type
MS InFo
MS ID
• • • • • • • • • •
MS Nonce

도면4


HO Type
Result Code
MS ID
• • • • • • • • • •
MS Nonce
Cert

도면5