(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년12월22일
(11) 등록번호 10-1097635
(24) 등록일자 2011년12월15일

(51) Int. Cl.
H04L 12/28 (2006.01) *H04B 7/26* (2006.01)
H04L 29/02 (2006.01) *H04L 29/10* (2006.01)
(21) 출원번호 10-2006-7011570
(22) 출원일자(국제출원일자) 2004년10월26일
심사청구일자 2009년10월26일
(85) 번역문제출일자 2006년06월12일
(65) 공개번호 10-2006-0123309
(43) 공개일자 2006년12월01일
(86) 국제출원번호 PCT/EP2004/012083
(87) 국제공개번호 WO 2005/051026
국제공개일자 2005년06월02일
(30) 우선권주장
03026069.9 2003년11월12일
유럽특허청(EPO)(EP)
(56) 선행기술조사문헌
WO2003079700 A1
US20030103496 A1
전체 청구항 수 : 총 24 항

(73) 특허권자
파나소닉 주식회사
일본 오오사카후 가도마시 오오아자 가도마 1006 반치
(72) 발명자
바흐만 옌스
독일 61440 오베루르셀 레이펜베르게르 스트라세 6
보게트 알렉산더
독일 64283 담스타트 에르바체르 스트라세 2
(74) 대리인
제일특허법인

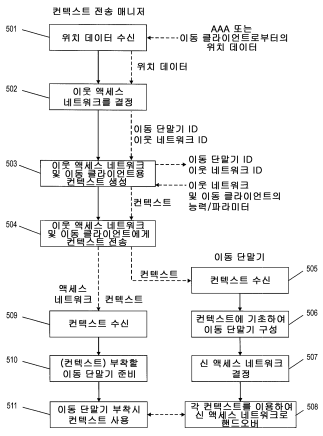
심사관 : 이상웅

(54) 복수의 이종 액세스 네트워크를 포함하는 통신네트워크에서의 컨텍스트 전송

(57) 요 약

본 발명은 복수의 이종 액세스 네트워크(220, 221, 222)를 포함하는 통신 네트워크에서의 컨텍스트 전송 방법에 관한 것으로서, 이동 단말기가 액세스 네트워크 중 하나에 접속된다. 또한, 본 발명은 그 방법을 수행하는 컨텍스트 전송 매니저에 관한 것이다(220, 600). 게다가, 본 발명은 컨텍스트 전송용으로 제공되는 방법을 수행하는 데 특히 적합한 이동 단말기에 관한 것이다. 이종 액세스 네트워크 간의 컨텍스트 전송이 용이하도록, 본 발명은, 이동 단말기와 관련된 능력과 파라미터 및 인접하는 액세스 네트워크의 능력과 파라미터에 기초하여 적어도 하나의 컨텍스트를 각 액세스 기술을 고려하여 생성하는 컨텍스트 전송 매니저를 도입하고 있다(도 5 참조). 게다가, 컨텍스트 전송 매니저는 통신 네트워크의 이종 액세스 네트워크에 대하여 공통이며 특정한 이동 단말기에 관한 컨텍스트 전송을 수행한다.

대 표 도 - 도5



특허청구의 범위

청구항 1

복수의 이종 액세스 네트워크(220, 221, 222, 620, 621, 622) - 상기 액세스 네트워크 중 하나에 이동 단말기(207)가 접속됨 - 를 포함하는 통신 네트워크에서의 컨텍스트 전송 방법으로서,

컨텍스트 전송 매니저(200, 600)에서 위치 정보를 수신하는 단계(501)와,

상기 컨텍스트 전송 매니저(200, 600)에 의해, 상기 위치 정보에 기초하여 상기 이동 단말기(207)에 대한 인접 액세스 네트워크를 결정하는 단계(502)와,

상기 컨텍스트 전송 매니저(200, 600)에 의해, 상기 인접 액세스 네트워크와 상기 이동 단말기(207)에 대한 적어도 하나의 컨텍스트를 생성하는 단계(503)와,

상기 컨텍스트 전송 매니저(200, 600)에 의해, 컨텍스트를 상기 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)의 각각 및 상기 이동 단말기(207)에 송신하는 단계(504)

를 포함하고,

상기 적어도 하나의 컨텍스트(304)의 생성은, 상기 이동 단말기(207)와 관련된 능력(capabilities)과 파라미터, 및 각 액세스 기술을 고려한 상기 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)의 능력과 파라미터에 기초하며,

상기 통신 네트워크에서의 복수의 이종 액세스 네트워크(220, 221, 222, 620, 621, 622)에 공통인 상기 컨텍스트 전송 매니저(200, 600)는 상기 이동 단말기(207)에 관련된 컨텍스트 전송을 수행하는 컨텍스트 전송 방법.

청구항 2

제 1 항에 있어서,

상기 이동 단말기(207)에서, 다른 액세스 네트워크의 존재를 표시하는 비콘 신호를 수신하여, 현재의 액세스 네트워크로부터 상기 비콘 신호를 수신한 새로운 액세스 네트워크로의 핸드오버를 수행하는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)의 각각 및 상기 이동 단말기(207)에 대해 생성된 컨텍스트(304)는 상기 이동 단말기(207)의 정적 식별자 또는 임시 식별자를 포함하는 컨텍스트 전송 방법.

청구항 4

제 3 항에 있어서,

상기 정적 식별자 또는 임시 식별자는 상기 새로운 액세스 네트워크 내의 컨텍스트 매니저(209, 210, 211, 609, 610, 611)에 의해 상기 이동 단말기(207)를 상기 컨텍스트 전송 매니저(200, 600)로부터 수신된 상기 이동 단말기의 컨텍스트와 연관시키는데 사용되는 컨텍스트 전송 방법.

청구항 5

제 3 항에 있어서,

상기 이동 단말기(207)는 상기 새로운 액세스 네트워크로 송신된 데이터에 정적 식별자 또는 임시 식별자를 포함하는 컨텍스트 전송 방법.

청구항 6

제 1 항 또는 제 2 항에 있어서,

상기 컨텍스트 전송 매니저(200, 600)로부터 수신한 컨텍스트에 기초하여 상기 이동 단말기(207)를 사전 구성하

는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 7

제 1 항 또는 제 2 항에 있어서,

상기 컨텍스트 전송 매니저(200, 600)에서 상기 이동 단말기(207)로부터의 상태 정보를 수신하는 단계를 더 포함하고,

상기 상태 정보는, 현재의 액세스 네트워크에서 얻은 서비스 품질과 상기 현재의 액세스 네트워크가 아닌 적어도 하나의 다른 액세스 네트워크로의 실패한 액세스 시도 중 적어도 하나를 표시하는 컨텍스트 전송 방법.

청구항 8

제 7 항에 있어서,

상기 인접 액세스 네트워크를 결정하는 단계는, 상기 이동 단말기(207)로부터의 상태 정보에 기초하여 상기 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)를 결정하는데 사용되는 선택 알고리즘을 적응시키는 단계를 포함하는 컨텍스트 전송 방법.

청구항 9

제 1 항 또는 제 2 항에 있어서,

상기 이동 단말기(207)에 의해 보고되는 액세스 네트워크로의 실패한 액세스 시도에 대한 정보를 상기 컨텍스트 전송 매니저(200, 600)에 저장하는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 10

제 1 항 또는 제 2 항에 있어서,

상기 이동 클라이언트와 연관된 능력 및 파라미터는,

정적 또는 임시 단말기 식별자를 포함하는 인증, 허가 및 과금 파라미터와,

단말기의 통신에 대한 요구 조건, 보장된 서비스 품질 파라미터 및 서비스에 대한 액세스 허가 중 적어도 하나를 포함하는 사용자 선호도(preferences)와,

암호화 키, 시드, 암호 및 헤더 압축 정보 중 적어도 하나를 포함하는 세션 데이터와,

디스플레이, 네트워크 인터페이스, 처리 전력, 지원 애플리케이션 및 비디오/오디오 코덱 중 적어도 하나에 대한 정보를 포함하는 단말기 능력

중 적어도 하나를 포함하는

컨텍스트 전송 방법.

청구항 11

제 1 항 또는 제 2 항에 있어서,

상기 인접 액세스 네트워크의 능력 및 파라미터는, 무선 주파수, 데이터 속도, 채널 및 코딩 방식 중 적어도 하나를 포함하는 액세스 기술 특정 속성과, 각 액세스 네트워크의 암호화 능력, 액세스 네트워크 식별자, 지원되는 서비스 품질 메카니즘, 이용가능 트래픽 클래스, 로컬 서비스, 정보 포탈 및 대중 교통 정보 중 적어도 하나를 포함하는 액세스 네트워크 특정 속성 중 적어도 하나를 포함하는 컨텍스트 전송 방법.

청구항 12

제 1 항 또는 제 2 항에 있어서,

상기 컨텍스트 전송 매니저(200, 600)에 의해 수신된 위치 정보는, 상기 이동 단말기(207)와 상기 인증 서버(206) 간에 수행된 인증 절차 후에 상기 컨텍스트 전송 매니저(200)의 홈 도메인의 인증 서버(206)로부터의 시그널링 메시지에 의해 또는 상기 이동 단말기(207)에 의해 송신되는 페이징 메시지에서 수신되는 컨텍스트 전송

방법.

청구항 13

제 1 항 또는 제 2 항에 있어서,

상기 위치 정보는, 위치 결정 장치로부터 얻은 지리적 위치, 또는 네트워크 어드레스 및 네트워크 프리픽스 중 적어도 하나에 기초하여 결정된 네트워크 관련 위치에 기초하는 컨텍스트 전송 방법.

청구항 14

제 2 항에 있어서,

상기 새로운 액세스 네트워크에 관한 컨텍스트 정보를 상기 컨텍스트 전송 매니저(200, 600)로부터 수신시 핸드오버를 수행하는 컨텍스트 전송 방법.

청구항 15

제 1 항 또는 제 2 항에 있어서,

상기 컨텍스트 전송 매니저(200, 600)로부터 상기 복수의 액세스 네트워크(220, 221, 222, 620, 621, 622) 및 상기 이동 단말기(207)에 전송된 컨텍스트를 설명하는데 마크업 언어 기반 데이터 포맷이 사용되는 컨텍스트 전송 방법.

청구항 16

제 1 항 또는 제 2 항에 있어서,

인접 액세스 네트워크의 인증 서버(206, 606)가 상기 컨텍스트 전송 매니저(200, 600)로부터 상기 컨텍스트를 수신하고, 상기 수신된 컨텍스트 정보를 이용하여 상기 이동 단말기(207)의 상기 인접 액세스 네트워크로의 등록 및 인증 절차 중 적어도 하나를 수행하는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 17

제 16 항에 있어서,

상기 등록 및 인증 절차 중 적어도 하나는 상기 이동 단말기(207)의 보안 키를 등록하는 단계를 포함하는 컨텍스트 전송 방법.

청구항 18

제 17 항에 있어서,

상기 이동 단말기(207)가, 상기 보안 키가 등록되어 있는 인접 액세스 네트워크에 접속시에, 통신을 위해서 상기 등록된 보안 키를 이용하는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 19

제 1 항 또는 제 2 항에 있어서,

상기 컨텍스트 전송 매니저(600)는 방문 통신 네트워크에 상주하는 컨텍스트 전송 방법.

청구항 20

제 19 항에 있어서,

상기 이동 단말기(207)의 홈 통신 네트워크의 컨텍스트 전송 매니저(200)에 의해, 상기 적어도 하나의 컨텍스트의 생성에 관련된 데이터를 상기 방문 통신 네트워크의 컨텍스트 전송 매니저(600)에 송신하는 단계를 더 포함하는 컨텍스트 전송 방법.

청구항 21

제 1 항 또는 제 2 항에 있어서,

액세스 네트워크의 컨텍스트 매니저(209, 210, 211, 609, 610, 611)에서, 상기 컨텍스트 전송 매니저(200, 600)로부터의 컨텍스트를 수신하는 단계를 더 포함하고,

상기 컨텍스트 매니저는 다른 액세스 네트워크의 다른 컨텍스트 매니저와의 접속을 유지하지 않는 컨텍스트 전송 방법.

청구항 22

복수의 이종 액세스 네트워크(220, 221, 222, 620, 621, 622)- 상기 액세스 네트워크 중 하나에 이동 단말기(207)가 접속됨 - 를 포함하는 통신 네트워크에서의 컨텍스트 전송 매니저(200, 600)로서,

상기 컨텍스트 전송 매니저(200, 600)는,

위치 정보를 수신하는 수신 수단과,

상기 위치 정보에 기초하여 상기 이동 단말기(207)의 인접 액세스 네트워크를 결정하는 처리 수단(202, 602)과,

상기 인접 액세스 네트워크 및 상기 이동 단말기(207)에 대해 적어도 하나의 컨텍스트(304)를 생성하는 컨텍스트 생성 수단(201, 601)과,

상기 인접 액세스 네트워크의 각각 및 상기 이동 단말기(207)에 각각의 컨텍스트를 송신하는 송신 수단

을 포함하고,

상기 컨텍스트 생성 수단(201, 601)은, 상기 이동 단말기(207)에 관련된 능력과 파라미터, 및 상기 인접 액세스 네트워크의 각 액세스 기술을 고려한 능력과 파라미터에 기초하여 상기 적어도 하나의 컨텍스트(304)를 생성하도록 구성되며,

상기 통신 네트워크 내의 복수의 이종 액세스 네트워크(220, 221, 222, 620, 621, 622)에 공통인 상기 컨텍스트 전송 매니저(200, 600)는 상기 이동 단말기(207)에 관련된 컨텍스트 전송을 수행하는 컨텍스트 전송 매니저.

청구항 23

제 22 항에 있어서,

상기 컨텍스트 전송 매니저(200, 600)는 청구항 1 또는 청구항 2에 개시된 방법을 수행하도록 구성되는 컨텍스트 전송 매니저.

청구항 24

복수의 이종 액세스 네트워크(220, 221, 222, 620, 621, 622)를 포함하는 통신 네트워크의 이동 단말기(207)로서,

상기 이동 단말기(207)는, 상기 액세스 네트워크중 하나에 접속되고, 청구항 1 또는 청구항 2에 개시된 방법을 수행하도록 구성되는 이동 단말기.

명 세 서

기 술 분 야

[0001] 본 발명은 복수의 이종 액세스 네트워크를 포함하는 통신 네트워크에서의 컨텍스트 전송 방법에 관한 것으로서, 여기서 이동 단말기는 액세스 네트워크 중 하나에 접속(attach)된다. 또한, 본 발명은 그 방법을 수행하는 컨텍스트 전송 매니저에 관한 것이다. 게다가, 본 발명은 컨텍스트 전송용으로 제공되는 방법을 수행하는데 특히 적합한 이동 단말기에 관한 것이다.

배 경 기 술

[0002] 네트워크에 접속되어 있는 모든 이동 노드는, 접속성을 유지하기 위하여 구 네트워크의 커버리지 영역을 벗어날 때 새로운 네트워크로의 핸드오버를 수행할 수 있다. 이동 노드가 그 접속중에 진행하는 데이터 세션을 갖고 있다면, 이 접속은 적어도 핸드오버 프로세스의 시간동안 중단된다. MobileIP와 같은 추가 메카니즘에 의해 그 세션을 재개할 수 있도록 트래픽을 새로운 접속점으로 리라우팅(rerouting)할 수 있다. 그러나, 핸드오버 지속시간은 세션 불연속성의 최소 시간 리미트(limit)이다.

[0003] 따라서, 핸드오버 지속시간을 가능한 한 짧게 하는 것이 바람직하다. 이를 유지하는 메카니즘이 프로액티브(proactive) 컨텍스트 전송이다. 프로액티브 컨텍스트 전송으로 인해, 이동 노드(이동 단말기)가 새로운 네트워크로 핸드오버를 시작하기 전에 액세스 라우터(AR) 또는 액세스 포인트(AP)에서 세션 상태를 확립할 수 있다. 액세스 라우터 또는 액세스 포인트가 접속되어 있는 백본 네트워크를 통해 전송을 행한다. 이것은 예를 들어 인터넷일 수 있다.

[0004] 전송된 데이터의 기점은 컨텍스트에 대한 지식을 이미 갖고 있는 엔티티이다. 프로액티브 컨텍스트 전송을 위한 다른 해결책으로는, 소위 반응성 컨텍스트 전송으로서, 핸드오버가 이미 시작되었다면 컨텍스트 전송을 개시한다.

[0005] 프로액티브 컨텍스트 전송을 실현하는 주요 기능은, 핸드오버를 수행하기 전에 컨텍스트가 전송되는 후보들을 선택하는 것이다. 일반적으로 이동 노드의 이동 패턴이 알려져 있지 않기 때문에 어느 액세스 라우터 또는 액세스 포인트가 다음 접속점인지를 예측할 수 없다. 일반적으로, 핸드오버를 수행할 수 있도록 액세스 포인트의 셀 커버리지 영역들이 중첩된다고 가정한다. 그러나, 도달 범위 내의 새로운 액세스 포인트가 많이 존재하는 경우, 이것은 더해져야 할 새로운 네트워크의 선택 프로세스에 별로 도움을 주지 못한다.

[0006] Seamoby CTP 및 CARD

[0007] IETF (인터넷 엔지니어링 태스크 포스) 작업 그룹 Seamoby는 컨텍스트 전송에 관한 2개의 프로토콜을 개발하였다. 이것은 컨텍스트 전송 프로토콜 (CTP; Loughney 등의 "Context Transfer Protocol", 인터넷 초안, 2003년 10월, 모든 인터넷 초안 및 RFC는 http://www. ietf. org 참조) 및 후보 액세스 라우터 디스커버리(CARD; Liebsch 등의 "Candidate Access Router Discovery" 인터넷 초안, 2003년 9월)이다. CTP는 프로토콜로서 기능하여 컨텍스트 전송을 개시하고 컨텍스트 데이터를 전달한다. CTP 통신에는 3개의 당사자들이 관련되며, 즉, 이동 노드(모바일 노드), 이전 액세스 라우터(pAR), 및 다음 액세스 라우터(nAR)이다. 이들 모두는, 상이한 메시지 유형을 갖고, 프로토콜 교환을 개시할 수 있다. 이동 노드가 자신의 네트워크 액세스 포인트를 교환하길 원하거나 교환해야 한다면, 이미 이전 액세스 라우터로부터 비접속되어 있는 경우, 적어도 다음 액세스 라우터에 요청을 송신한다. 이동 노드가 만약 CARD를 통해 다음 액세스 라우터 예측의 일부를 대략 이용하면, 이동 노드는 다음 액세스 라우터 자체에 접속하기 전에 예측되는 다음 액세스 라우터에 컨텍스트 전송을 시작하도록 하는 취지의 메시지를 이전 액세스 라우터에 송신한다. 이것은 다음 액세스 라우터의 IP 어드레스, 이전 액세스 라우터상의 이동 노드의 구 IP 어드레스, 전송할 컨텍스트 데이터 리스트, 다음 액세스 라우터상의 가능성있는 것으로 알려져 있는 IP 어드레스, 및 안전하고 신뢰성있는 컨텍스트 전송을 요청하는 플래그를 포함한다. 이후, "피쳐(feature) 컨텍스트"라 칭하는 컨텍스트 데이터가 추가 메시지에서 송신된다.

[0008] CARD 프로토콜은 2개 메시지, 즉, CARD 요청 및 CARD 응답으로만 구성된다. 이들은 2개의 액세스 라우터, 예를 들어, 다음 액세스 라우터(nAR)와 이전 액세스 라우터(pAR)라 칭하는 현재 액세스 라우터 간에, 또는 이동 노드와 이전 액세스 라우터 또는 다음 액세스 라우터 간에 사용될 수도 있다. 액세스 라우터 간에, CARD는 컨텍스트 전송 및 차후의 이동 노드 핸드오버를 위해 가장 적합한 후보를 선택하는데 필요한 다음 액세스 라우터 후보들의 능력 정보를 얻는데 기여한다. 이동 노드와 이전 액세스 라우터 간에, CARD 요청을 발생하여 다음 액세스 라우터 후보들의 리스트를 요구한다. 이 요청에서, 이동 노드는 일부 메카니즘에 의해 검출하였을 수 있는 임의의 다음 액세스 라우터 데이터 링크층(Layer2) 식별자들을 송신할 수 있으며, 이에 따라 이전 액세스 라우터는 어느 액세스 라우터가 이동 노드의 범위내에 있는지에 대한 힌트를 갖는다. 이전 액세스 라우터가 다음 액세스 라우터를 Layer 2 식별자에 의해 식별하는 방식은 CARD 초안에 특정되어 있지 않다. 이동 노드에 대한 응답에서, 이전 액세스 라우터는 이동 노드가 후보로써 처리해야 하는 다음 액세스 라우터의 수를 감축하기 위해서, 이전 액세스 라우터 결정 기준에 의해 사전필터링(pre-filtered)되었을 수도 있는 다음 액세스 라우터 능력과 함께 다음 액세스 라우터 리스트를 송신한다.

[0009] 무선랜에서의 컨텍스트 전송 (IEEE 802.11f)

[0010] 무선랜(WLAN)에서, 새로운 액세스 포인트에서의 재연관(re-association) 프로세스를 허용하는 핸드오버에 관련된 액세스 포인트(AP) 간의 클라이언트 또는 스테이션(STA)에 관한 정보가 교환된다. 이 재연관 프로세스를 가속하는 컨텍스트 전송 방식이 사용된다. 2개의 기능 엔티티, 즉, 액세스 포인트 및 RADIUS 서버가 컨텍스트 전송에 관련된다. 스테이션(STA)에 대해서는, 관리 프로세스가 투명하다. RADIUS 서버는 전달된 BSSID(Basic Service Set Identifier)를 액세스 포인트의 FQDN(Fully Qualified Domain Name) 또는 IP 어드레스로 매핑하는 태스크를 수행한다. 이 매핑은 액세스 포인트가 동일한 연장 서비스 세트(ESS)에 RADIUS 서버로서 속하는지 여부를 암시적으로 보여준다. 또한, 이것은 요청 암호 키를 액세스 포인트에 분산하여 2개의 액세스 포인트 간에 암호화된 통신을 가능하게 한다. 이 통신은, 노드간의 클라이언트의 이동을 허용하며 클라이언트의 한번에 하나만의 액세스 포인트와의 연관을 강화하는 모든 관리 데이터를 포함한다. 관리 메시지는, 컨텍스트 데이터를 포함할 수 있다. 후속하는 ESS에서의 각 액세스 포인트는 자신의 인접 액세스 포인트의 동적 표현을 유지한다. 이 표현을 인접 그룹이라고도 칭한다.

[0011] 2002년 1월, IEEE 초안 IEEE 802.11f-D3 "Recommended Practice for Multi-Vendor Access Point;Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation"에서의 부록 B, 섹션 B.3.1에서 언급하고 있는, 상이한 서비스 모델들을 갖는 매체간의 컨텍스트 전송은 성공적일 것으로 예측될 수 없다는 점은 주목해야할 중요한 점이다. IEEE 802.11 컨텍스트 전송 매커니즘에 따른 IEEE 802.11 액세스 포인트 및 셀룰러 장치들간에 컨텍스트를 전송하려는 시도는, 셀룰러 액세스 포인트가 802.11 액세스 포인트와 동일한 세트의 서비스를 구현하지 못하면 실패한다. 결론적으로, 이 문헌은 이종 기술간의 컨텍스트 전송이 실패한다는 것을 개시하고 있다.

[0012] 다른 메카니즘

[0013] CTP 시나리오의 이동 노드 및 액세스 라우터에 더하여, 미국 특허 출원 공개번호 제2003/0,103,496 A1호에 개시된 메카니즘은, (CARD 메카니즘에 비교할 때) 인접 액세스 네트워크(AN)를 검색하는 태스크를 수행하는 폴리시 서버(PS), 및 컨텍스트를 전송할 수 있는 액세스 라우터를 포함하고 있다. 액세스 네트워크는 이동 노드에 의해 수신된 비콘 신호에서 레이어 2 정보에 의해 표시되고, PS에 의해 로컬 데이터베이스에서 탐색된다. PS는, 이동 노드를 서빙할 수 있으며 이동 노드를 인접 폴리시 서버들로 사전 인증할 수 있다면, 인접 폴리시 서버들과 통신한다. 이러한 메카니즘의 한가지 단점은 CTP 시나리오보다 더 많은 안전 접속(또는 다른 면에서 보안 연계)을 필요로 한다는 것이다. 다음으로, 이것은 새로운 액세스 네트워크로 컨텍스트를 송신하기 전에 동적 및 정적 부분으로부터 컨텍스트를 구축하지만, 타겟 네트워크의 임의의 특징들 또는 능력을 고려하지 않는다.

[0014] 미국 특허출원 공개번호 제2003/0,092,444 A1호는 인접 후보들을 선택시 현재의 트래픽 부하 및 사용자 권한과 같은 동적 파라미터를 고려하는 메카니즘을 개시하고 있다. 따라서, 후보들의 리스트는 각 이동 노드마다 상이할 수 있다. 전송 프로세스 자체는 액세스 네트워크의 액세스 라우터간에 수행된다.

[0015] 인접 액세스 라우터를 발견하고 컨텍스트 전송 메카니즘용으로 사용가능한 메카니즘이 미국 특허출원 공개번호 제2003/0,087,646 A1호에 개시되어 있으며, GAARD로 약칭한다. 이것은 인접 액세스 네트워크가 예를 들어 IP 어드레스를 고려할 때 위상적으로 인접하지 아니하더라도 인접 액세스 네트워크를 지리적으로 검출할 수 있다. 이 문헌에서는, 이동 노드가, 레이어 2 (데이터 링크층) 어드레스 및 레이어 3 (네트워크층) 어드레스의 로컬 캐시를 구비한다. 이동 노드가 레이어 2를 갖는 비콘 신호를 수신하고 이 노드로의 컨텍스트 전송을 개시하려면, 이동 노드는 자신의 캐시에서 대응 레이어 3 어드레스를 탐색한다. 캐시 탐색이 실패하면, 이동 노드는 서빙 액세스 라우터에게 대응 레이어 3 어드레스를 탐색할 것을 요청한다. 액세스 라우터는 자신의 캐시를 탐색한다. 그 어드레스가 발견되지 않으면, 액세스 라우터는 동적 발견 프로세스를 개시하여 요청한 레이어 3 어드레스를 도출한다. 액세스 라우터는 그 어드레스를 이동 노드로 리턴하고 이에 따라 이동 노드는 그 어드레스를 이용하여 식별된 액세스 라우터로 컨텍스트 전송 또는 다른 핸드오버 메카니즘을 개시한다. 이 시스템의 기능은, 이 시스템을 사용하거나 지원하려는 이동 노드 및 모든 액세스 라우터에 존재해야 한다. 메카니즘은 CARD 프로세스의 구현으로서 기능할 수 있다.

[0016] 일반적인 컨텍스트 전송 시나리오와 대조적으로, 모든 인접 액세스 라우터가 이동 노드용 액세스 포인트로 가능한 경우, 후자의 가정은 계약을 기초로 함께 동작하는 네트워크 시나리오에서 맞지 않다. 인접 액세스 라우터는 이동 노드의 홈 운영자와의 로밍 협정이 없는 네트워크 운영자에게 속할 수 있다. 따라서, 이동 노드는 외

래 네트워크의 비콘을 수신하지만 인증 프로세스가 실패하면, 외래 네트워크의 인증 기관은 이동 노드의 홈 AAA(인증, 인가, 및 과금) 서버에 액세스할 수 없거나 알려져 있지 않은 이 서버를 신뢰하지 않는다. 이러한 네트워크로의 컨텍스트 전송도 동일한 이유로 실패한다.

[0017] 직접적 로밍 협약이 없는 네트워크를 이동 노드의 홈 운영자와 통합하는 방식은 프록시 AAA 서버들을 이용하는 것이다. 액세스 네트워크 운영자는, 이동 노드의 홈 운영자를 신뢰하는 운영자의 프록시 AAA 서버를 신뢰한다. 이러한 방식으로, 이 외래 네트워크에서도 이동 노드를 허가할 수 있다.

[0018] WLAN에서의 컨텍스트 전송과 같은 메카니즘을 다른 랜 기술용으로 개발할 수 있다. 위상적으로 인접하는 엔티티간의 컨텍스트 전송은 짧은 거리라는 이점을 갖고, 이러한 방식으로 낮은 대기 시간 전송이 이루어진다.

[0019] 이종 액세스 네트워크 구조는 이전 문제점과 연관된다. 이동하는 이동 노드의 컨텍스트를 정적 데이터로 간주될 수 없을 가능성이 높다. 이것은 새로운 액세스 포인트의 액세스 네트워크 인프라스트럭쳐가 이전과 상이할 때 변경된다. 새로운 액세스 네트워크로의 컨텍스트 데이터를 간단히 전달하는 것은 이 문제점을 해결하지 못한다.

[0020] 컨텍스트 전송의 일반적인 문제점은 컨텍스트 전송 프로세스에서 관련된 엔티티간의 신뢰 관계이다. n개의 인접 액세스 라우터를 포함하는 영역의 시나리오에서, 컨텍스트 데이터를 서로 전송하게 되면, 모든 액세스 라우터간에 n(n-1)/2 신뢰 관계라는 상한이 발생한다. 이 관계가 피어들(peers)간의 일부 암호 키 교환에 의해 기술적으로 표현되어 암호화된 통신을 허용할 때, 큰 수(n)는, 액세스 라우터당 n-1 데이터 세트인 예에서 데이터 세트용 많은 저장 공간을 의미한다. 또한, 이 관계는 피어들간에 컨텍스트 전송이 가능하기 전에 확립되어야 하며, 관리 기능을 필요로 한다. 따라서, 신뢰 관계들의 수를 줄이는 방법은 저장 공간 및 관리 노력을 절약한다. 안전한 데이터 전달을 위한 기존의 기술은 신뢰 관계 보안 연계(SA)를 가리키는 IPSec이다.

[0021] 이동 노드는, 대부분의 경우, 무선 링크에 의해 자신의 액세스 포인트에 접속된다. 이들 링크는 일반적으로 액세스 네트워크의 백본 부분에서 유선 링크들보다 저 대역폭 및 상이한 액세스 네트워크의 상호접속을 갖는다. 이것은 무선 도메인에서 데이터 양당 높은 전송 비용을 야기한다.

[0022] 다른 관점은 이동 노드의 전력 소모이다. 이 소모는 무선 링크에 대한 송신 패킷들의 수와 직접적으로 상관된다. 양측 관점으로 인해 사용자 페이로드 트래픽에 비교할 때 관리 트래픽의 양을 가능한 적게 유지할 필요가 있다.

발명의 상세한 설명

[0023] 본 발명의 목적은 상술한 문제점들중 적어도 하나를 해결하는 것이다.

[0024] 이 목적은 독립항들의 청구 대상에 의해 해결된다. 본 발명의 바람직한 실시예들은 종속항들의 청구 대상이다.

[0025] 본 발명의 제 1 실시예에 따르면, 복수의 이종 액세스 네트워크를 포함하는 통신 네트워크에서의 컨텍스트 전송 방법을 제공한다. 이동 단말기가 액세스 네트워크중 하나에 접속될 수 있다.

[0026] 본 발명의 방법에 따르면, 컨텍스트 전송 매니저는 위치 정보를 수신할 수 있고 위치 정보에 기초하여 이동 단말기에 대한 인접 액세스 네트워크를 결정할 수 있다. 게다가, 컨텍스트 전송 매니저는 인접 액세스 네트워크에 대하여 적어도 하나의 컨텍스트를 생성할 수 있고 이동 단말기 및 인접 액세스 네트워크의 각각에 그 컨텍스트를 송신할 수 있다.

[0027] 적어도 하나의 컨텍스트의 생성은, 이동 클라이언트와 관련된 능력 및 파라미터 그리고 각 액세스 기술을 고려하는 인접 액세스 네트워크의 능력 및 파라미터에 기초할 수 있고, 컨텍스트 전송 매니저는 통신 네트워크에서 복수의 이종 액세스 네트워크에 대하여 공통일 수 있으며, 이동국에 관련된 컨텍스트 전송을 수행한다.

[0028] 따라서, 제 1 실시예에 따른 본 발명은 2개의 상이한 액세스 기술을 이용하는 액세스 네트워크간에 이동 단말기가 핸드오버를 수행하는 경우에도 컨텍스트 전송을 허용한다. 또한, 이동 단말기가 이동할 수 있는 후보 액세스 네트워크, 즉, 인접 액세스 네트워크에서 사용되는 액세스 기술을 고려할 때, 상이한 액세스 기술에 의해 사용되는 각 프로토콜에 대하여 구성될 수 있는 동적 컨텍스트를 생성할 수 있다. 또한, 이것은, 공통 컨텍스트 전송 매니저만이 통신 네트워크에서 보안 연계를 훨씬 덜 요구하는 상이한 후보 액세스 네트워크의 컨텍스트 매니저에게 컨텍스트를 전송할 수 있기 때문에, 그 통신 네트워크에서의 공통 컨텍스트 전송 매니저를 이용함으로

써 용이해진다. 본 발명이 제안한 아키텍처의 이점을 상세히 후술한다.

[0029] 추가 실시예에 따르면, 이동 단말기는 다른 액세스 네트워크의 존재를 가리키는 비콘 신호를 수신하고, 현재의 액세스 네트워크로부터 비콘 신호를 송신한 새로운 액세스 네트워크로 핸드오버를 수행한다.

[0030] 이동 단말기 및 인접 액세스 네트워크 각각에 대하여 생성된 컨텍스트는 이동 단말기의 정적 식별자 또는 임시 식별자를 포함할 수 있다. 정적 식별자 또는 임시 식별자는, 예를 들어, 새로운 액세스 네트워크의 컨텍스트 매니저에 의해 사용되어 이동 단말기를 컨텍스트 전송 매니저로부터 수신한 이동 단말기의 컨텍스트와 관련지을 수 있다. 후자는, 이동 단말기가 새로운 액세스 네트워크로 송신된 데이터에 정적 식별자 또는 임시 식별자를 포함하는 경우 용이해질 수 있다. 따라서, 새로운 액세스 네트워크의 컨텍스트 매니저에 송신된 메시지에 식별자를 포함함으로써, 제안하는 방법은 컨텍스트 전송 매니저로부터 (이전에) 수신한 컨텍스트의 이동 단말기로의 매핑을 용이하게 할 수 있다.

[0031] 이동 단말기에 의해 수신되는 컨텍스트는 이동 단말기에 의해 컨텍스트 전송 매니저로부터 수신한 컨텍스트에 기초하여 이동 단말기를 사전 구성(pre-configure)하는데 사용될 수 있다. 따라서, 예를 들어, 네트워크 인터페이스의 사전 구성에 의해, 이 프로세스는, 이동 단말기가 새로운 액세스 네트워크에 접속시, 수행될 필요가 없다.

[0032] 컨텍스트 전송 매니저는, 이동 단말기로부터 상태 정보를 추가로 수신할 수 있으며, 이 상태 정보는, 현재의 액세스 네트워크에서 얻은 서비스 품질과 현재의 액세스 네트워크가 아닌 적어도 하나의 다른 액세스 네트워크에 대한 실패한 액세스 시도 중 적어도 하나를 가리킨다.

[0033] 따라서, 컨텍스트 전송 매니저에 의해 수집된 이 정보를 컨텍스트 전송 매니저가 이용함으로써 이 정보에 기초하여 컨텍스트 전송 매니저에서 여러 결정 프로세스를 구성할 수 있으며, 예를 들어, 인접 액세스 네트워크의 결정에는 이동 단말기로부터의 상태 정보에 기초하여 구성될 수 있는 선택 알고리즘을 이용할 수도 있다.

[0034] 또한, 클라이언트가 특정 액세스 네트워크에 대한 접속 실패를 보고하면, 후자는 인접 액세스 네트워크의 결정 프로세스에 있어서 더 이상 고려될 필요가 없고 액세스 네트워크의 운영자 또는 컨텍스트 전송 매니저의 운영자에 의해 어드레싱되고 핸들링될 수 있는 적합한 에러 메시지를 생성할 수 있다. 후자의 경우, 컨텍스트 전송 매니저는 이동 단말기에 의해 보고된 액세스 네트워크로의 실패한 액세스 시도에 대한 정보를 저장할 수 있다.

[0035] 컨텍스트 생성동안 고려된 이동 클라이언트와 연관되는 능력 및 파라미터는, 정적 단말기 식별자 또는 임시 단말기 식별자를 포함하는 인증, 허가 및 과금 파라미터와, 단말기의 통신에 대한 요구 조건, 보장된 서비스 품질 파라미터 및 서비스에 대한 액세스 허가 중 적어도 하나를 포함하는 사용자 선호도(preferences)와, 암호화 키, 시드, 암호 및 헤더 압축 정보 중 적어도 하나를 포함하는 세션 데이터와, 디스플레이, 네트워크 인터페이스, 처리 전력, 지원 애플리케이션 및 비디오/오디오 코덱 중 적어도 하나에 대한 정보를 포함하는 단말기 능력 중 적어도 하나를 포함할 수 있다. 명백한 바와 같이, 액세스 네트워크에서 상이한 액세스 기술을 어드레싱할 수 있는 여러 액세스 네트워크 특정 파라미터를 이용하여 동적 컨텍스트를 생성할 수 있다. 이것은 인접 액세스 네트워크의 능력 및 파라미터에도 동일하게 적용되며, 이 능력 및 파라미터는, 무선 주파수, 데이터 속도, 채널 및 코딩 방식 중 적어도 하나를 포함하는 액세스 기술 특정 속성과, 각 액세스 네트워크의 암호화 능력, 액세스 네트워크 식별자, 지원되는 서비스 품질 메카니즘, 이용가능 트래픽 클래스, 로컬 서비스, 정보 포탈, 및 대중 교통 정보 중 적어도 하나를 포함하는 액세스 네트워크 특정 속성 중 적어도 하나를 포함할 수 있다.

[0036] 컨텍스트 전송 매니저에 의해 수신되는 위치 정보는, 이동 단말기와 인증 서버간에 수행되는 또는 이동 단말기가 접속된 액세스 네트워크에 위치하는 엔티티에 의해 수행되는 인증 절차로부터 이동 단말기에 의해 송신되는 페이징 메시지에서 수신될 수 있다. 두 번째 예에서, 액세스 네트워크가 예를 들어 연관된 AAA 서버에 결합하도록 초기 인증 절차를 수행하는 이동 단말기는 위치 정보를 AAA 서버에 제공할 수 있다. 이 정보는, 컨텍스트 전송 매니저가 인증 절차로부터의 위치 정보를 이용하여 인접 액세스 네트워크를 결정하도록 컨텍스트 전송 매니저에 대하여 이용가능할 수도 있다. 게다가, 컨텍스트 전송 매니저는 이동 단말기의 인증 절차에 응답하여 컨텍스트 전송을 개시할 수도 있다.

[0037] 게다가, 위치 정보는 위치 결정 장치, 예를 들어, GPS 수신기로부터 얻은 지리적 위치, 또는 네트워크 어드레스 및 네트워크 프리픽스 중 적어도 하나에 기초하여 결정된 네트워크 연관 위치에 기초할 수 있다. 예를 들어, IP 프로토콜을 사용함으로써, 네트워크 어드레스는 IP 어드레스에 대응하고, 네트워크 프리픽스는 서브네트 마스크가 될 것이다.

[0038] 본 발명의 추가 실시예에 따르면, 컨텍스트 전송 매니저로부터 새로운 액세스 네트워크에 관한 컨텍스트 정보를

수신시 이동 단말기의 핸드오버를 수행할 수 있다. 따라서, 본 발명에 따라 프로액티브 컨텍스트 전송도 실현될 수 있다.

[0039] 생성된 컨텍스트를 설명하고자, 마크업 언어 기반 데이터 포맷이 이용될 수 있다. 게다가, 이 포맷을 이용하여 컨텍스트 전송 매니저로부터 복수의 액세스 네트워크 및 이동 단말기로 전송되는 컨텍스트를 설명할 수도 있다.

[0040] 본 발명의 다른 실시예에서, 컨텍스트 전송 매니저로부터 컨텍스트를 수신하는 인접 액세스 네트워크의 인증 서버는 수신한 컨텍스트 정보를 이용하여 액세스 네트워크에 이동 단말의 등록 및 인증 절차 중 적어도 하나를 수행할 수 있다. 게다가, 이동 단말기의 등록 및 인증 중 적어도 하나는 이동 단말기의 보안 키의 등록을 포함할 수 있다.

[0041] 이동 단말기는, 보안 키가 등록된 인접 액세스 네트워크에 접속시 통신용으로 등록된 보안을 이용할 수 있다.

[0042] 본 발명의 또다른 실시예는, 이동 단말기가 외부 통신 네트워크, 즉, 소위 방문 통신 네트워크에 접속되는 상황을 고려한다. 본 실시예에서, 컨텍스트 전송 매니저는 방문 통신 네트워크에 상주할 수 있다. 본 발명에서, 통신 네트워크는, 관리 도메인으로서, 즉, 운영자의 또는 운영자와의 서비스 레벨 협약을 갖는 제공자들의 액세스 네트워크의 적어도 하나의 코어 네트워크 및 복수의 액세스 네트워크를 포함하는 네트워크로서 해석될 수 있다. 따라서, 본 실시예는 이동 단말기가 홈 도메인이 아닌 다른 관리 도메인에 상주하는 상황에 관한 것일 수 있다.

[0043] 방문 컨텍스트 전송 매니저, 즉, 방문 통신 네트워크의 컨텍스트 전송 매니저가 컨텍스트 전송용으로 적절한 컨텍스트를 생성하기 위해, 이동 단말기의 홈 네트워크에 있는 컨텍스트 전송 매니저는, 적어도 하나의 컨텍스트의 생성에 관한 데이터를 방문 통신 네트워크의 컨텍스트 전송 매니저에게 송신할 수 있다.

[0044] 게다가, 액세스 네트워크의 컨텍스트 매니저는 컨텍스트 전송 매니저로부터 컨텍스트를 수신할 수 있으며, 여기서 컨텍스트 매니저는 다른 액세스 네트워크의 다른 컨텍스트 매니저와 어떠한 접속도 유지하지 않는다는 점에 주목하길 바란다. 따라서, 상이한 액세스 네트워크의 컨텍스트 매니저는 서로에 대한 접속을 유지할 필요가 없으며 컨텍스트를 가능하다면 서로 직접 전송하거나 전달할 필요가 없고, 컨텍스트 전송 매니저는 엔티티나 상위 계층 레벨로부터 컨텍스트를 수신할 수 있다.

[0045] 본 발명의 또다른 실시예는 복수의 이종 액세스 네트워크를 포함하는 통신 네트워크의 컨텍스트 전송 매니저를 제공하고, 여기서 이동 단말기는 액세스 네트워크중 하나에 접속된다. 컨텍스트 전송 매니저는, 위치 정보를 수신하는 수신 수단과, 위치 정보에 기초하여 이동 단말기에 대한 인접 액세스 네트워크를 결정하는 처리 수단과, 인접 액세스 네트워크 및 이동 단말기에 대한 적어도 하나의 컨텍스트를 생성하는 컨텍스트 생성 수단과, 인접 액세스 네트워크의 각각 및 이동 단말기에 각 컨텍스트를 송신하는 송신 수단을 포함할 수 있다. 게다가, 컨텍스트 생성 수단은 이동 단말기에 관련된 능력 및 파라미터 그리고 인접 액세스 네트워크의 각 액세스 기술을 고려하는 능력 및 파라미터에 기초하여 적어도 하나의 컨텍스트를 생성하도록 구성될 수 있다. 게다가, 통신 네트워크에서 복수의 이종 액세스 네트워크에 공통인 컨텍스트 전송 매니저는 이동 단말기에 관한 컨텍스트 전송을 수행할 수 있다.

[0046] 컨텍스트 전송 매니저는 상술한 방법 중 임의의 방법을 수행하도록 구성될 수 있다.

[0047] 본 발명의 다른 실시예에 따르면, 상술한 방법 중 하나를 수행하도록 구성된 이동 단말기를 제공한다. 이 단말기는, 액세스 네트워크에 대하여 실패한 액세스 시도를 컨텍스트 전송 매니저에 시그널링하거나 마크업 언어 포맷으로 제공되는 컨텍스트 정보를 수신할 수 있도록 구성될 수 있다.

실 시 예

[0055] 본 발명의 일실시예에 따라 이동 노드에 대한 컨텍스트 전송을 관리하는 통신 네트워크의 아키텍처 개략도를 도2에 도시한다. 아키텍처는 이동 노드의 홈 도메인의 네트워크, 이동 노드(207) 자체, 및 액세스 네트워크에 걸쳐서 분포된다.

[0056] 컨텍스트 전송 매니저(CTM; 200)는 홈 도메인의 AAA 서버(206)와 나란히 배열될 수 있다. 컨텍스트 전송 매니저(200)는 적합하면서 동적으로 생성된 컨텍스트 데이터를 이동 노드의 현재 위치의 인접 액세스 네트워크에 송신할 수 있다. 이 인접들은 컨텍스트 전송 매니저(200)로부터 이동 노드(207)의 현재 위치(예를 들어, IP 어드레스 또는 네트워크 프리픽스)를 갖는 인접 로케이터(202) 기능에 의해 검출되며 인접 리스트에서 리턴된다.

이동 노드(207)의 사용자에 관한 정보와 함께 이 인접 리스트는 컨텍스트 생성기(201)에 제공될 수 있다. 컨텍스트 생성기(201)는, 액세스 네트워크 및 이동 노드들의 능력에 대한 그리고 컨텍스트 포맷에 대한 데이터베이스를 유지할 수 있다(사용자 프로파일 데이터베이스(203), 액세스 네트워크 컨텍스트 데이터베이스(204), 인접 능력 데이터베이스(205) 참조). 이 정보에 기초하여, 적합한 컨텍스트를, 예를 들어, 구별되는 단말기 식별자들, 가입 정보, 사용자 선호, 단말기 능력, 서비스 파라미터 품질, 암호화 및 압축 정보, 액세스 기술 특정 속성 또는 액세스 네트워크 특정 속성을, 각 인접 액세스 네트워크에 대하여 생성할 수 있다. 이후, 그 컨텍스트를 프로액티브 방식으로 액세스 네트워크에 전송할 수 있으며, 이 네트워크에서 컨텍스트는 액세스 네트워크(AN)의 컨텍스트 매니저(CM; 209, 210, 211)에 의해 예시된다. 이동 노드(207)상의 모빌리티 매니저(208) 기능은, 컨텍스트 전송을 이용하여 인접 네트워크로의 가속 핸드오버를 수행하는데 필요한 정보를 포함하여 인접 네트워크(220, 221, 222)를 통보받을 수 있다. 컨텍스트 전송 매니저(200)로부터 수신한 컨텍스트에 기초하여, 이동 노드(207)는 다음 액세스 포인트용에 대해 자신의 네트워크 인터페이스를 (사전)구성할 수 있다. 이동 노드(207) 자체는, 범위 내의 인접 네트워크의 비콘 신호들을 수신할 때, 핸드오버 결정을 내릴 수 있다.

[0057] 이동 노드(207)가 외부 도메인으로 로밍할 때, 방문 운영자의 컨텍스트 전송 매니저(600)에 의해 컨텍스트 전송 관리를 행할 수 있다(도 6 참조). 컨텍스트 전송 프로세스는 비로밍(non-roaming)의 경우와 유사하며, 단지 관리 핸드오버를 홈 컨텍스트 전송 매니저(200)로부터 방문 컨텍스트 전송 매니저(600)로 추가하는 것이다.

[0058] 다음으로, 컨텍스트 전송 매니저(200, 600)를 상세히 설명한다. 컨텍스트 핸들링을 위한 주요 예는 컨텍스트 전송 매니저(CTM; 200, 600)일 수 있다. 이것은 필요한 컨텍스트 정보에 액세스하는 기능을 제어할 수 있다. 제어에 대한 아키텍처 기능으로는, 컨텍스트 생성기(201), 인접 로케이터(202), 액세스 네트워크(AN) 컨텍스트 매니저(209, 210, 211, 609, 610, 611), 및 모빌리티 매니저(208) 기능이 있다. 먼저, 컨텍스트 전송 매니저(200, 600)는, 예를 들어, 이동 단말기(207)가 작동되어 액세스 네트워크에 접속될 때 모빌리티 매니저(208)와의 통신을 통해 또는 표준 인증 절차에 의해 이동 노드(207)의 현재 위치를 수신할 수 있다.

[0059] 이후, 컨텍스트 전송 매니저(200, 600)는 인접 로케이터(202, 602)를 이용하여 이동 노드(207)의 모든 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)를 결정할 수 있다. 다음으로, 컨텍스트 전송 매니저(200, 600)는 컨텍스트 생성 기능(201, 601)을 시그널링하여 이동 노드(207)의 인접 액세스 네트워크(220, 221, 222, 620, 621, 622)에 의해 사용되는 컨텍스트에 관한 사용자 정보를 검색할 수 있다. 시그널링은, 사용자 ID, 및 네트워크 프리픽스와 같이 인접 네트워크(220, 221, 222, 620, 621, 622)에 대한 적용가능 네트워크 ID를 포함할 수 있다. 컨텍스트에 포함되는 다른 파라미터는, 액세스 네트워크가 차후에 온라인 또는 오프라인 전달 서비스 요금 부과용으로 이용할 수 있는 사용자를 위한 추가 고유 정적 또는 임시 식별자일 수 있다. 정적 또는 임시 식별자로서 각각 사용되는 GSM 또는 UMTS 혹은 익명의 가능성있는 NAI(네트워크 액세스 식별자의 약어)의 IMSI(국제 모바일 가입자 아이덴티티; Aboba등의 1999년 1월, RFC 2486 "Network Access Identifier" 참조)를 고려할 수 있다.

[0060] 이 정보를 컨텍스트 데이터내로 집적한 후, 컨텍스트 전송 매니저(200, 600)는 컨텍스트 데이터를 액세스 네트워크 컨텍스트 매니저(209, 210, 211, 609, 610, 611)에 송신할 수 있고 생성된 컨텍스트 정보의 일부를 이동 클라이언트(이동 단말기; 207)의 모빌리티 매니저(208)에 송신할 수 있다. 이러한 정보의 일부로 인해 이동 노드(207)는 자신의 네트워크 인터페이스를 구성할 수 있으며 다음의 인접 네트워크 액세스 시도에 대한 정확한 식별자를 이용할 수 있다.

[0061] 이동 노드(207)의 추적 정보에 더하여, 컨텍스트 전송 매니저(200, 600)는, 모빌리티 매니저(208)로부터의 상태 정보를 수락할 수도 있다. 상태 정보에서, 이동 노드(207)는 현재 네트워크에 도달된 서비스 품질(QoS) 또는 완전한 액세스 실패를 다른 액세스 네트워크에 시그널링할 수 있다. 이것은 인접 리스트에서 최적의 액세스 네트워크를 위한 선택 알고리즘의 동적 구성을 허용할 수 있어, 동일 영역에서 이동중인 다른 이동 노드들이 적합한 새로운 액세스 네트워크를 선택하는데 기여한다. 이러한 방식으로, 이동 노드(207)는 네트워크 상태에 대한 정보를 수집하는 네트워크 프로브로서 기능할 수 있다. 많은 모빌리티 매니저가 단일 액세스 네트워크에서 컨텍스트 지원 핸드오버의 실패를 시그널링하면, 컨텍스트 전송 매니저(200, 600)는 자신의 고유 네트워크에게 관리 및 동작 기능을 통보하여 이 에러를 추가로 조사하거나 운영자에게 그 액세스 네트워크를 통보할 수 있다.

[0062] 이하, 컨텍스트 생성기(201)의 컨텍스트 생성 기능을 상세히 설명한다. 상술한 바와 같이, 기본적인 Seamoby CTP 방식은, 이종 네트워크 또는 상이한 관리 도메인의 네트워크에서 구현될 때 제한을 갖는다. 이것은 컨텍스트 생성에 속한다. 컨텍스트는 아이덴티티, 패스워드 또는 암호화 키처럼 단지 순수한 사용자 관련 데이터의 세트가 아닐 수 있다. 특히, 이 컨텍스트는 클라이언트의 관점에서 볼 때 네트워크 상태를 더 설명할 수 있다.

네트워크 상태 정보는, 예를 들어, 네트워크 서비스에 대한 액세스 권한, 송신 데이터용 암호화 알고리즘, 사용자 데이터용 라우팅 폴리시, 사용자 세션 트래픽 또는 액세스가능한 네트워크 엔티티(DNS 서버, 디폴트 게이트웨이 등)에 할당된 트래픽 클래스를 포함할 수 있다. 단일 관리 도메인에서, 사용자가 요구하면, 이 데이터 상태를 전체 네트워크를 통해 유지할 수 있다. 다른 도메인으로의 경계를 지나면, 이 데이터는 변경될 수 있으며, 말하자면, 동적일 수 있다. 이것을 방지하기 위해 가능하다면 운영자간의 매우 밀접한 결합이 필요할 수 있다. 따라서, 본 발명이 제안하는 컨텍스트 전송을 이러한 동적 상황에 적응시키는 방안은 이점을 가지며 상술한 문제점들을 해결한다.

[0063] 본 발명의 일실시예에 따른 컨텍스트 생성을 도 3에 도시하고 있다. 컨텍스트 생성 프로세스는 4부분으로 분리될 수 있는데, 즉, 2개의 소스 데이터 오브젝트, 하나의 처리 기능, 및 하나의 결과 데이터 오브젝트이다. 2개의 정적 데이터 오브젝트는 (단말기 파라미터 및 능력을 포함하는) 사용자 파라미터(301) 및 네트워크 파라미터(302) 그리고 능력을 나타낸다. 이 2개 파라미터 세트에 기초하여, 처리 기능(303)은 결과 데이터 오브젝트, 즉, 동적 컨텍스트(304)를 도출할 수 있다. 네트워크 관련 파라미터가 각 액세스 네트워크에서 사용되는 액세스 기술에도 의존하기 때문에, 상이한 액세스 기술을 갖는 액세스 네트워크를 위한 컨텍스트는 가변할 수 있다. 일예로, 세션 암호화 키들, 상태 플래그 또는 사용자 ID 핸들을 생성하는 처리 기능내의 여러 알고리즘을 고려해 본다. 사용자 파라미터용 데이터 오브젝트는, 임시 아이덴티티, QoS 요건 또는 허용되는 세션 종류(예를 들어, 비디오, 보이스)와 같은 사용자 선호, 암호화 키 또는 시드 및 설치된 암호화 및 스크린 해상도와 같은 단말기 능력, 처리 전력, 오디오/비디오 코덱, 및 이용가능한 응용, 네트워크 인터페이스 등을 포함하는 사용자 아이덴티티의 설명을 포함할 수 있다.

[0064] 컨텍스트 관련 데이터도 데이터 오브젝트에 포함될 수 있다. 이것은 결국 다른 용도(3GPP의 일반적인 사용자 프로파일(GUP))로 존재하는 일반적인 사용자 데이터 저장을 사용하는 이점을 갖는다. 네트워크 파라미터용 데이터 오브젝트는 결과 컨텍스트가 추후에 전송될 수 있는 특정 액세스 네트워크에 대한 정보를 포함할 수 있다.

[0065] 다음 액세스 네트워크의 액세스 기술에 의존하는 파라미터뿐만 아니라 사용자 특정 파라미터 및 단말기 특정 파라미터 중 적어도 하나를 고려할 때, 이동 단말기(207)가 새로운 네트워크에 액세스하는 경우 컨텍스트 전송 실패를 방지할 수 있는 동적 컨텍스트를 생성할 수 있다. 이 동적 컨텍스트는, 네트워크 비콘에 포함되는 WLANSSID(서비스 세트 식별자) 또는 지원되는 암호화 알고리즘과 같은 데이터일 수 있으며, 이동 노드(207)가 선택할 WLAN을 식별하는데 기여한다. 또한, 데이터 오브젝트(304; 컨텍스트)에 컨텍스트 관련 데이터뿐만 아니라 그 오브젝트를 이용하는 다른 응용에 속하는 데이터 세트도 포함될 수 있다. 일반적으로, XML 도출 언어를 이용하여 컨텍스트 데이터를 설명할 수 있으며, 예를 들어, GUP 또는 복합 능력/선호 프로파일(CC/PP)용으로 이용할 수 있다. XML 다큐먼트 및 XSL내의 데이터 탐색 및 선택용 W3C 언어 Xpath 및 XQuery를 이용할 수 있다. XSL을 이용하여 XML 다큐먼트를 변환하고 이들을 임의의 출력 포맷으로 후처리(post-process)할 수 있다. 또한, 마크업 언어를 이용하여 컨텍스트 정보를 설명함으로써 데이터 설명을 안전하고도 쉬운 방식으로 연장할 수 있고, 구 설명과의 호환성도 유지할 수 있다. 온 디맨드(on-demand) 컨텍스트 생성은 비간섭성 네트워크로의 컨텍스트 전송 문제점을 해결할 수 있으며, 또한 네트워크 파라미터의 일부 또는 전체를 동적으로 유지하는 능력을 제공할 수 있다. 사용자는 자신의 사용자 선호를 변경할 수 있으며, 통신 네트워크에서의 다음 도래하는 컨텍스트 전송을 새로운 선호(고 세션 QoS, 새로운 암호화 모드 등)에 즉시 적합화할 수 있다.

[0066] 그 외에, 이동 단말기(207)의 모빌리티 매니저(208)는, 네트워크 인터페이스를 제어할 수 있으며 이동 노드(207)의 이동을 추적할 수 있다. 따라서, 최고의 위치가 이동 노드(207)일 수 있다. 다른 방법으로, 액세스 네트워크는 단말기가 하나의 액세스 포인트로부터 다른 액세스 포인트로 이동할 때 단말기의 이동에 기초하여 이동 노드의 위치를 추적할 수도 있다. 이동 노드(207)에 위치하는 모빌리티 매니저(208)의 경우, 상태 정보는 이동 클라이언트(207)로부터 컨텍스트 전송 매니저(200)로 송신되는 페이징 메시지에 포함될 수 있다. 모빌리티 매니저(208)는 이동 노드(207)의 이동 및 위치를 컨텍스트 전송 매니저(200)에 시그널링할 수 있다. 따라서, 모빌리티 매니저는, GPS(위치 확인 시스템) 수신기와 같은 내장 위치 결정 장치에 의해 또는 수신한 네트워크 비콘 또는 수신한 라우터 광고들을 평가함으로써 수집된 정보를 이용할 수 있다.

[0067] 지리적 또는 가상 네트워크 관련 위치에 의해 위치를 표현할 수 있다. 이동 단말기(207) 위치를 설명하기 위한 다중 포맷을 지원하여 상이한 기술을 이동 노드(207)에서 구현할 수 있으며 다양한 위치 표현들로부터 상이한 정보를 얻을 수 있다. 이것은 단일 기술이 모든 필요를 충족하지 못한다는 사실에 의해 동기 부여된다. 예를 들어, GPS는 단말기의 위치에 대하여 매우 정밀한 위치 정보를 제공할 수 있지만 위치 계산을 위해 GPS 위성에 대한 직접적인 관찰 라인을 필요로 한다. 특히, 높은 건물 지평선이 있는 도시에서는, 이것을 얻는다는 것이 불가능할 수 있다. 예를 들어, 이동 노드(207)의 네트워크 관련 위치(예를 들어, 네트워크 어드레스 및 프리픽

스)는 이동 노드(207)가 접속되어 있는 네트워크에 대한 정보를 수집하는데 (예를 들어, 액세스 서버의 어드레스를 얻는데) 기여할 수 있다. 그러나, 이동 노드(207)의 단일 네트워크 어드레스는 지리적으로 인접하는 네트워크의 어드레스와 유사하지 않아야 한다. 따라서, 추가 메카니즘을 이용하여 주어진 네트워크 어드레스에 대한 인접들을 계산할 수 있다(예를 들어, 인접 그래프).

[0068] 모빌리티 매니저(208)의 네트워크 제어부를 활성화하여 컨텍스트 전송 매니저(200)로부터 수신한 컨텍스트내의 정보를 이용하여 이동 노드(207)의 네트워크 인터페이스(들)를 사전 구성할 수 있다. 네트워크 제어부는 로컬 캐시내의 시그널링받은 인접 액세스 네트워크중 임의의 네트워크에 대하여 상이한 구성 프리세트를 유지할 수 있으며, 핸드오버 상황을 검출시 적합한 하나를 예시할 수 있다. 예를 들어, 어떤 응용이 높은 대역폭을 필요로 하거나, 현재 접속이 페이딩 중인 경우와 같이, 모빌리티 매니저가 스위칭이 필요하다고 판정하면, 모빌리티 매니저(208)에 의해 핸드오버를 능동적으로 개시할 수 있다.

[0069] 모빌리티 매니저(208)는, 네트워크 접속 또는 QoS 요건에 대한 사용자 선호 변경을 컨텍스트 전송 매니저(200)와 통신하는 태스크를 추가로 해결할 수 있다. 이러한 선호는 적절한 네트워크 인접들의 선택 및 컨텍스트 생성 프로세스에 영향을 끼친다.

[0070] 액세스 네트워크 컨텍스트 매니저(209, 210, 211, 609, 610, 611)(AN 컨텍스트 매니저)는 수신한 컨텍스트 데이터를 처리할 수 있다. 이 프로세스에서, 액세스 제어 엔티티, 즉, 액세스 네트워크(220, 221, 222, 620, 621, 622)의 액세스 서버(212, 213, 214, 612, 613, 614)를 예를 들어 이동하는 이동 노드(207)용으로 구성할 수 있다(도 2 및 6 참조). 구성 프로세스는 외부 네트워크에 대하여 그리고 그 컨텍스트를 송신한 컨텍스트 전달 엔티티에 대하여 투명할 수 있다. 유일한 요건은, 컨텍스트 전송 매니저(200, 600)의 컨텍스트 생성기(201, 601)가 만족시킬 수 있고, 액세스 네트워크 컨텍스트 매니저(209, 210, 211, 609, 610, 611)가 이해하고 예시할 수 있는 컨텍스트 포맷을 설명하는 규정된 템플릿을 사용하는 것일 수 있다. 네트워크와 관련된 내부 정보는, 양측이 신뢰 관계를 갖고 컨텍스트 전송 데이터의 남용을 방지하는 것으로서, 포함될 수 있다. 액세스 네트워크 컨텍스트 매니저(209, 210, 211, 609, 610, 611)에 의한 내부 액세스 네트워크 구성은 액세스 네트워크 와이드 컨텍스트 전송 메카니즘을 포함하여 인트라 도메인 핸드오버를 가속할 수 있다.

[0071] 인접 로케이터(202, 602)는 이동 노드(207)의 인접 액세스 네트워크를 검색할 수 있다. 인접 로케이터(202, 602)는 컨텍스트 전송 매니저(200, 600)로부터 이동 노드의 위치를 미리 얻을 수 있다. 이 위치 정보를 이용함으로써, 인접 관계를 저장하는 네트워크 표현을 탐색할 수 있다(도 2의 데이터베이스(203, 204, 205) 또는 도 6의 데이터베이스(603, 604, 605) 참조). 이 표현은 동적 또는 정적일 수 있다.

[0072] WLAN을 공공 영역 및 회사 영역에서 무선 광대역 액세스용으로 각광받는 기술로 볼 때, 3GPP는 WLAN과 3GPP 셀룰러 네트워크 간의 상호동작 메카니즘의 요건을 식별하였다. 따라서, 3GPP는 3GPP 네트워크와 상호동작하는 WLAN에 의해 지원되는 서비스 레벨들을 설명하는 6개의 상이한 시나리오를 규정하였다.

[0073] 3G-WLAN 상호동작 시나리오에서는, 다이아미터(diameter) 서버를 갖는 중앙 집중 AAA 구조가 존재한다. 이 구조는, 컨텍스트 전송의 보안을 위해, 여기서는, 방문 공공 랜드 이동 네트워크(VPLMN), 홈 공공 랜드 이동 네트워크(HPLMN), WLAN 액세스 네트워크간에 재사용될 수 있는 보안 연계(SA)도 구비한다. 본 발명은 외래 네트워크로의 성공적인 컨텍스트 전송이 가능하도록 홈 및 방문 컨텍스트 전송 매니저 간에 체인형 신뢰 관계를 제공할 수 있다. 따라서, 이 시나리오에 대한 컨텍스트 전송 해결책은 컨텍스트 전송을 위한 프록시 기능을 구현하여, 계층적 컨텍스트 전송을 위한 시스템을 구축할 수 있다. 도 1은, 홈 도메인(예를 들어, HPLMN)으로부터 방문 도메인(예를 들어, VPLMN)의 프록시를 통해 컨텍스트가 처리되고 예시되는 WLAN으로의 컨텍스트 전송의 간략한 구조를 도시한다.

[0074] 따라서, 액세스 라우터 대 액세스 라우터 컨텍스트 전송 시나리오, 즉, 이전 액세스 라우터(pAR)로부터 다음 액세스 라우터(nAR)로의 컨텍스트 전송이 변경될 수 있다.

[0075] 본 발명에 따른 3개의 관련 엔티티는 이동 노드(207), 다음 액세스 라우터, 및 AAA 서버(206)일 수 있다. 이동 노드(207)는 컨텍스트 전송 요청을 AAA 서버(206)에 송신할 수 있다. 이에 따라, AAA 서버(206)는 이동 노드(207)의 컨텍스트를 다음 액세스 라우터에 전송할 수 있다. 이것은 다음 액세스 라우터 및 AAA 서버(206)간에 신뢰 관계를 제시할 수 있으며, WLAN AR 운영자가 AAA 서버(206) 운영자와의 로밍 협약을 갖고 있다면, 이미 존재한다. 로밍 파트너의 수가 m개로 주어지면, 이것은 n개의 액세스 라우터의 각각마다 m개의 보안 연계 및 전체에 걸친 n*m개의 보안 연계를 야기한다.

[0076] 이 수는 실질적으로 액세스 라우터 대 액세스 라우터 컨텍스트 전송 시나리오에서의 수보다 작아야 한다. 다른

이점으로는, 액세스 라우터에서의 AAA 서버(206)가 인접 발견을 행하기 때문에 CARD형 기능이 더이상 필요없다는 것이다. 단지 액세스 라우터에 컨텍스트 전송 에이전트가 존재할 수 있다. 일반적으로, 인접 발견 기능은 네트워크에게 구분되지 않을 수 있으며 이에 따라 벤더 특정 방식으로 구현될 수 있다. 상이한 관리 도메인간의 적어도 수직 핸드오버에서 예상되는 2개의 액세스 라우터간의 호환불가 컨텍스트 데이터라는 문제점도, 이전 액세스 라우터를 모조하는 AAA 서버(206)를 이용함으로써 더 효율적으로 될 수 있다.

[0077] AAA 서버(206)가 인접 발견 프로세스를 통해 다음 액세스 라우터 능력의 정확한 지식을 갖고 있는 경우, AAA 서버는 컨텍스트를 다음의 타겟 액세스 라우터의 능력에 동적으로 적응시킬 수 있다. 완전한 사용자 프로파일로의 액세스를 가지면, 감소된 정보 세트만을 갖는 인터 액세스 라우터 컨텍스트 전송과 반대되는 적절한 특징 컨텍스트를 생성할 수 있다.

[0078] 컨텍스트 전송 매니저(600)는 외래 도메인의 액세스 네트워크(621, 622)에 대한 충분한 정보를 갖지 않거나 정보를 갖지 않을 수 있기 때문에, 외래 도메인 또는 방문 도메인(예를 들어, VPLMN)에서 로밍하는 이동 노드(207)는 홈 컨텍스트 전송 매니저(200)에 의해 직접적으로 지원되지 않을 수 있다. 홈 컨텍스트 전송 매니저(200), 즉, 이동 클라이언트(207)의 홈 도메인의 컨텍스트 전송 매니저(200)는 액세스 네트워크에 있어서의 컨텍스트 데이터를 생성하지 못할 수 있다. 따라서, 이동 노드(207)는 외래 도메인의 컨텍스트 전송 매니저(600), 즉, 방문 컨텍스트 전송 매니저(600; VCTM)에 의해 지원될 수 있다. VCTM(600)이 지원할 수 있도록, 홈 컨텍스트 전송 매니저(200; HCTM)는 이동 노드의 또는 사용자의 프로파일의 필요한 부분들을 VCTM(600)에 전달할 수 있다.

[0079] 도 6은 개별적인 액세스 네트워크를 제어하는 홈 및 방문 도메인의 네트워크의 아키텍처를 도시한다. 방문 도메인(VPLMN)의 컨텍스트 전송 매니저(600)는 수신 데이터를 타겟 액세스 포인트 또는 액세스 네트워크에 맞도록 만들 가능성을 가질 수 있다. 홈 운영자의 컨텍스트 전송 매니저(200)처럼, VCTM(600)은 고유의 운영자를 갖는 서비스 레벨 협약(SLA)을 구비하는 액세스 네트워크(621, 622)에 대한, 이들의 능력에 대한, 그리고 이들의 필요한 컨텍스트 포맷에 대한 데이터베이스(603, 604, 605)를 유지할 수 있다. 게다가, 방문 컨텍스트 전송 매니저(600)는 AAA 서버(606)로부터 정보를 검색할 수도 있다. 이동 노드(207)를 서빙하는 VPLMN(VCTM)에서의 컨텍스트 전송 매니저(600)와 모빌리티 매니저(208)간의 차이는 로밍 이동 노드(207)의 영구적이지 않도록 저장된 사용자 프로파일일 수 있다.

[0080] 이 프로파일에 대한 대체는 컨텍스트 전송 매니저간에 전송되는 것일 수 있다. 일반적 사용자 프로파일(GUP) 또는 CC/PP의 파생물의 사용이 시그널링에 유용할 수 있다. 그럼에도 불구하고, 전송되는 데이터는 홈 컨텍스트 전송 매니저(200)의 데이터베이스에 위치하는 원래의 사용자 프로파일의 직접적인 복제본이 아닐 수 있다.

[0081] 적어도 사용자의 아이덴티티는, 사용자의 세션을 식별할 수 있고 의사용으로(pseudonym) 전달된 서비스를 고려할 수 있지만 다중 세션들에 걸친 이동 패턴 또는 사용자의 습관에 대한 정보를 수집하는 것을 허용하지 않는 임시 의사로 대체될 수 있다. 게다가, 컨텍스트 생성 프로세스에 영향을 끼치지 않는 모든 데이터는, 홈 컨텍스트 전송 매니저(200)로부터 방문 컨텍스트 전송 매니저(600)로 전송되는 임시 프로파일로부터 분리될 수 있다.

[0082] 임시 사용자 프로파일의 전송은 암호화로 인해 안전할 수 있다. 암호화 프로세스는 무결성 보호뿐만 아니라 비밀성을 공급할 수 있다. 비밀성만으로 공격자가 사용자 프로파일에 가짜 데이터를 삽입할 수 있으며, 이것은 서비스 거부(DoS) 공격으로 기능할 수 있다. 2개의 운영자간에 존재하는 보안 연계를 이용하여 안전한 접속 자체를 확립할 수 있다. 그 데이터를 위한 특정 응용 프로토콜은 필요하지 않을 수 있다.

[0083] 컨텍스트 전송용 추천 모드는 프로액티브 모드일 수 있으며, 이것은 시간 제한이 보다 덜 엄하다. 그러나, 리액티브 모드를 이용할 수도 있다. 이 경우, 이동 노드(207)는 핸드오버 프로세스의 시작 후에 컨텍스트 전송을 요청한다. 컨텍스트 전송 매니저(200, 600)는 새로운 액세스 네트워크(221, 621)를 통해 요청을 수신할 수 있고 이동 노드(207)의 컨텍스트를 액세스 네트워크 컨텍스트 매니저(209, 210, 211, 609, 610, 611)로 리턴할 수 있다. 컨텍스트 전송 매니저(200, 600)는 이동 노드(207)의 이동을 추적함으로써 그리고 인접에 대한 컨텍스트를 사전 처리 및 캐싱함으로써 응답 시간을 짧게 유지할 수 있다.

[0084] 컨텍스트 전송 기능들(CTM, 컨텍스트 생성기(201) 등)을 갖는 외부 AAA 서버로부터 WLAN의 액세스 라우터 또는 인증 서버(AS)로의 컨텍스트 전송 프로세스의 예를 도 4를 참조하여 설명한다.

[0085] 그 예를, 이동 노드가 WLAN 및 3GPP 운영자 간의 협약에 의해 WLAN을 이용하도록 허용된다고 가정한다. 이동 노드의 홈 운영자는, 데이터베이스에 저장된 WLAN의 능력에 대한 충분한 정보를 갖고 있고 필요한 암호화 데이

터를 도출하기 위한 기술적 능력을 갖고 있다. 이동 노드는 액세스 네트워크에 접속되어 있으며 새로운 액세스 네트워크로의 핸드오버를 아직 시작하지 않은 상태에 있다. 게다가, WLAN의 인증 서버(AAA)를 활성화하여 IAPP를 송신한다. 액세스 포인트에 대한 CACHE-NOTIFY 메시지는, 캐시에 이동 노드용 컨텍스트 엔트리를 삽입하도록 AP에게 요청하며, 메시지는 IEEE 초안, 2003년 1월, 2개 액세스 포인트간의 네트워크, IEEE 802.11f-D5 "Recommended Practice for Multi-Vendor Access Point; Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation"에서 정상적으로 교환된다.

[0086] AAA 서버는 인접 선택 프로세스에 의해 인접으로서 검출된 WLAN의 인증 서버에 적절한 컨텍스트를 전송(401)할 수 있다. 다음으로, AAA 서버는, 현재 링크를 통해 UE(즉, 이동 단말기의 모빌리티 매니저)에게 다른 액세스 네트워크에 대하여 가능성있는 다음 접속을 위한 컨텍스트 파라미터(예를 들어, 페어와이즈(Pairwise) 마스터 키, WLAN의 SSID 등)를 통지(402)할 수 있다. 컨텍스트 파라미터는 인트라 WLAN 특징 컨텍스트용으로도 사용할 수 있다. 다른 독립적인 컨텍스트 분야들도 포함할 수 있다.

[0087] 유효 데이터를 갖는 컨텍스트를 수신한 모든 인접 인증 서버는, 수신한 컨텍스트를 포함하는 모든 관련된 액세스 포인트에 대한 IAPP.CACHE-NOTIFY를 개시(403)할 수 있다. 모든 WLAN 액세스 포인트는 IAPP.CACHE-NOTIFY에서 전달된 컨텍스트를 판독하고 그 컨텍스트를 삽입하는 응용을 가질 수 있고, 이것은, 이 경우, PMK SA 테이블 내로의 페어와이즈 마스터 키(PMK) 보안 연계(SA)일 수 있다. 액세스 포인트에 대해서는, 이 시점에서는 일반적으로 이동 노드는 액세스 네트워크에 액세스하는 새로운 클라이언트에 대해 통상적으로 수행되는 키 확립 프로세스를 완료한 것으로 보인다.

[0088] 이동 노드 또는 클라이언트가 이전의 접속을 통해 컨텍스트 데이터를 수신하였던 액세스 포인트와의 연관(404)을 행할 때, 이것은 로버스트 보안 네트워크(RSN) 정보 소자 내부의 KID를 직접 송신할 수 있고, 이것은 연관 요청의 STA에 의해 지원되는 리스팅 키 암호, 인증 및 키 관리 알고리즘이다(IEEE 802.11i-D5 "Medium Access Control (MAC) Security Enhancements", 2003년 8월, IEEE 초안, 섹션 7.3 2.9 참조).

[0089] 이후, 액세스 포인트는 PMKID에 의해 참조된 PMK를 식별할 수 있고, 초기 EAPOL 프로세스를 교묘히 회피하는 클라이언트와의 4방향 핸드셰이크(405)를 바로 개시한다. 이것은 액세스 포인트 및 액세스 서버간의 인증 핸드셰이크 및 WLAN 액세스 서버 및 AAA 서버간의 인증 핸드셰이크 모두를 생략한다.

[0090] 클라이언트 및 액세스 포인트간의 4방향 핸드셰이크는 프레시 임시 페어와이즈 및 그룹 키(PTK, GTK)를 생성하여 다음에 따르는 유니캐스트 및 멀티캐스트 사용자 데이터 전송을 안전하게 한다. 클라이언트가 연장된 서비스 세트(ESS) 내부에서 더 로밍하면(406), WLAN에서 진행중인 컨텍스트 전송은 떨어져 있는 AAA 서버의 상호작용없이 내부 메카니즘에 의해 달성될 수 있다.

[0091] WLAN의 인증 서버 및 AAA 서버간의 컨텍스트 전송 프로세스는 HPLMN 및 VPLMN AAA 서버들에 대하여 일치한다. 이것은 홈 및 방문 도메인에서의 컨텍스트 전송 매니저간의 컨텍스트 전송 관리의 핸드오프에 의해 달성될 수 있다. WLAN 인증 서버는 프록시 컨텍스트 전송 매니저로부터 후 처리된 컨텍스트 및 원래의 컨텍스트간을 구별하지 못할 수 있다. 이것은 미신뢰 소스 또는 신뢰 소스로부터의 컨텍스트 데이터간을 구별할 수 있다.

[0092] 액세스 포인트의 PMK 보안 연계 캐시에서의 보안 연계의 타임아웃 때문에 또는 완전히 실패한 WLAN으로의 컨텍스트 전송으로 인해 리스트 프로세스가 실패할 수 있다. 이 경우, 4방향 핸드셰이크가 실패하고, 예를 들어 연장가능 인증 프로토콜(EAP) 핸드셰이크를 이용하는 정상적인 인증 절차를 개시한다. 이 핸드셰이크를 위해, 상호 인증을 허용하는 EAP 메카니즘을 이용할 수 있다. 일예로, IETF 초안 EAP-SIM 및 EAP-AKA에 개시한 바와 같은 메카니즘을 이용하여 상호 인증을 제공할 수 있다(2003년 10월 IETF 인터넷 초안에서 Haverinen 등의 "EAP SIM Authentication", 및 2003년 10월 IETF 인터넷 초안에서 Arkko 등의 "EAP AKA Authentication" 참조). 이들은, 사용자 식별 및 키 생성을 위해 SIM(가입자 아이덴티티 모듈) 또는 USIM(UMTS SIM) 카드에서 암호화 기능을 사용한다.

[0093] 다음으로, PMK 보안 연계 데이터의 생성을 상세히 설명한다. 표준 메카니즘은 해시 함수(HMAC-SHA1-128)를 이용하여 PMKID를 생성한다. 해시 함수는 단방향 함수이고, 이에 따라 해시 알고리즘을 위한 소스 정보를 직접적으로 검색하는데 사용될 수 없다. 해시 함수는, 미지의 입력 파라미터를 갖는 해시 함수가 알려져 있는 입력 파라미터를 갖는 기준 해시 함수와 동일한 결과에 도달하였는지 여부에 대한 체크만을 허용한다. 그 결과가 일치하면, 입력 파라미터는 일치하였음에 틀림없다. PMKID 생성을 위해, 값(PMK, PMK 이름, BSSID(기본 서비스 세트 식별)) 및 클라이언트의 MAC 어드레스를 해시 함수용 입력 값들로서 취급할 수 있다. 이 값들은 클라이언트가 액세스 포인트에 접속될 때 액세스 포인트에 대하여 이용가능하다. 따라서, 액세스 포인트는 완전한 PMK

보안 연계 엔트리를 생성할 수 있다. 본 예에서, 이 엔트리는 로컬 액세스 포인트에 의해 생성되지 않을 수 있지만 컨텍스트 전송 매니저(200)는 엔트리를 생성할 수 있다. 컨텍스트 전송 매니저(200)는 자신의 액세스 네트워크 능력 데이터베이스를 통해 WLAN의 SSID에 대한 지식을 갖고 있을 수 있지만, 클라이언트가 로밍하는 액세스 네트워크에서 액세스 포인트, 특히, 액세스 포인트의 ESSID에 대한 지식은 전혀 없다. 이것은 HMAC-SHA1 알고리즘으로 PMKID의 계산시 컨텍스트 전송 매니저(200)가 BSSID를 사용하지 않을 수 있다는 것을 의미한다.

[0094] 한 가지 해결책은, PMKID 계산을 연기하고 이에 따라 비콘 메시지를 통해 클라이언트가 BSSID 및 SSID를 검출하였을 때까지 그리고 액세스 네트워크로 이미 스위칭되기 전에 그 액세스 네트워크로의 컨텍스트 전송을 연기하는 것이다. 이후, 모빌리티 매니저(208)는, 검출한 BSSID 및 SSID를, SSID에 의해 액세스 네트워크를 결정하는 컨텍스트 전송 매니저(200)로 다시 송신할 수 있다.

[0095] 본 발명의 또 다른 실시예에 따르면, 컨텍스트 전송 매니저(200)는 PMKID를 계산할 수 있고, 액세스 네트워크의 컨텍스트 전송 매니저(200)에 대한 컨텍스트 전송을 행하고 이를 통해 검출한 BSSID를 갖는 액세스 포인트로 컨텍스트 전송을 행한다. 컨텍스트가 액세스 포인트에 도달하지 못할 수도 있으며 이에 따라 반응성 컨텍스트 전송이 다시 발생할 수 있다. 액세스 네트워크에서의 모든 액세스 포인트를 위한 단일 컨텍스트 메시지를 송신할 수 있다. 이것은 컨텍스트 전송 매니저(200)에 대하여 WLAN 인프라스트럭쳐의 완전한 지식을 요구할 수 있으며, 이것은 예상할 수 없다.

[0096] PMK 보안 연계를 생성하는 문제점에 대한 또다른 해결책은 PMKID의 처리를 WLAN의 컨텍스트 매니저(209, 210, 211)에게 위임하는 것이다. 컨텍스트 매니저(209, 210, 211)는 컨텍스트 전송 매니저(200)로부터 수신한 클라이언트의 추가 컨텍스트와 함께 계산된 PMKID를 액세스 포인트에 송신할 수 있다. 클라이언트는, 컨텍스트 전송 매니저(200)로부터 모빌리티 매니저(208)를 통해 수신한 액세스 네트워크상의 정보를 갖는 동일한 PMKID 및 WLAN 비콘에서의 검출된 BSSID를 계산했을 수 있다. 이 해결책은 컨텍스트 전송 매니저(200)로부터 PMKID 계산 부하를 취하고 이것을 WLAN 컨텍스트 매니저(209, 210, 211)와 이동 클라이언트(207)에게 분배하며, 이것은 성능 문제점만을 야기할 수 있다. 클라이언트는 컨텍스트 전송이 실패하는 경우 그 계산을 수행할 수 있어야 한다.

[0097] WLAN에 대하여, PMKID는 캐시로부터 PMK 보안 연계를 선택하도록 고유하고도 예측불가능한 식별자로서 기능한다. 피어들간에 전혀 교환되지 않는 PMK를 이용하는 도전/응답 기술에 의해 4방향 핸드셰이크내에서 보안 연계 자체의 유효성을 체크할 수 있다(도 4 참조). 따라서, 악의가 있는 클라이언트의 PMKID의 권한 예측은 페어와이즈 마스터 키를 여전히 위험에 노출시킬 수 없다. 이것에 의하여 정확한 PMKID를 계산하지 못하는 문제점에 대한 손쉬운 방법이 실현될 수 있다. 컨텍스트 전송 매니저(200)는 해시 함수를 이용하지 않고서 랜덤 128비트 수를 PMKID로서 생성할 수 있다. 이 손쉬운 방법은 2가지 문제점을 갖고 있다. 첫번째로, PMKID는 WLAN 컨텍스트 매니저(209, 210, 211)로부터 액세스 포인트로 지연될 수 있고, 두번째로 액세스 포인트의 로컬 PMK 보안 연계에서 랜덤하게 생성된 PMKID 및 엔트리들간의 충돌 확률이 있다. 이하, 충돌 확률의 추정을 설명한다.

[0098] HMAC-SHA1 알고리즘이 분산된 해시값들을 균등하게 생성한다고 가정할 수 있다. PMKID는 128비트를 갖고, 이것은 $3.4 \cdot 10^{38}$개의 가능성있는 값들을 야기하고 공급받은 구별되는 값에 대하여 $P(x) = 2.9 \cdot 10^{-39}$의 확률을 제공한다. 이 경우, 이것은, 하나의 엔트리를 포함하는 캐시에서 랜덤하게 계산된 PMKID가 PMKID 엔트리와 매칭되는 확률이 ($P(충돌) = P(x) = 2.9 \cdot 10^{-39}$)이 된다는 것을 의미한다. n개의 PMKID 엔트리들의 캐시 크기를 가정하면, 충돌 확률은 $P(충돌) = n \cdot P(x) = n \cdot 2.9 \cdot 10^{-39}$이다. 1000개 캐시 엔트리들에 대해서는, $P(충돌) = 2.9 \cdot 10^{-36}$의 확률이 발생하며, 이것은 매우 작은 확률이다.

[0099] 이점으로는, 컨텍스트 전송 매니저(200)는, PMKID를 미리 분배할 수 있고, 클라이언트나 WLAN 컨텍스트 매니저(209, 210, 211)는 PMKID 자체를 계산하지 않을 수 있으며 이것은 처리 시간과 전력을 절약하고 클라이언트로부터의 연관 요청이 액세스 포인트로 송신될 준비 상태로 될 때까지의 시간을 줄일 수 있다. WLAN 컨텍스트 매니저(209, 210, 211)에 대해서는, 동일한 컨텍스트 데이터 세트를 모든 필요한 액세스 포인트에 송신하여 임의의 액세스 포인트를 위한 특정 컨텍스트를 계산한다는 것을 의미할 수 있다.

[0100] 다음으로, 본 발명의 또 다른 실시예에 따라 제안하는 컨텍스트 전송 메카니즘에 대한 개요를 도 5의 흐름도를 참조하여 설명한다. 컨텍스트 전송 매니저(200)는 이동 노드(207) 또는 컨텍스트 전송 매니저(200)에 의해 액세스가능한 AAA로부터 평가할 위치 정보를 수신할 수 있다(501). 전달 소스로부터 그 위치 정보를 수신하게 되

면, 컨텍스트 전송 매니저(200)는, 이동 노드의 위치에 기초하여 인접 액세트 네트워크를 결정하며 이동 노드(207)가 핸드오버시 접속될 수 있는 기능부 또는 수단에 그 정보를 전달할 수 있다(502). 이 기능부는 예를 들어 도 2와 6에 도시한 바와 같이 인접 로케이터(202)에 의해 실현될 수 있다.

[0101] 이동 노드(207)가 접속할 수 있는 인접 액세스 네트워크는 예를 들어 개략적으로 상술한 바와 같이 식별자에 의해 식별된다. 게다가, 이동 노드의 식별자도 다음 처리 단계로 전달된 정보에 포함될 수 있다. 이후, 인접 네트워크 및 이동 노드(207)를 식별하는 ID에 기초하여, 컨텍스트 전송 매니저(200)는 컨텍스트 생성 기능 또는 수단을 이용하여 인접 액세스 네트워크 및 이동 노드(207)용으로 적절한 컨텍스트를 동적 생성할 수 있다(503). 인접 네트워크의 액세스 기술에 따라, 컨텍스트 전송 매니저(200)에 의해 생성되는 컨텍스트가 상이한 파라미터를 가질 수 있다는 점에 주목하길 바란다. 이동 노드(207)는 개략적으로 상술한 바와 같이 핸드오버용으로 필요한 정보에 대하여 특화된 컨텍스트를 수신할 수도 있다.

[0102] 인접 네트워크 및 이동 노드(207)용으로 상이한 컨텍스트를 생성하면, 컨텍스트 전송 매니저(200)는 모든 컨텍스트를 각 액세스 네트워크 및 이동 노드(207)에 전송(504)할 수 있다.

[0103] 이동 노드(207)에서 컨텍스트를 수신(505)하면 그리고 예시용으로 다음 액세스 네트워크로의 핸드오버가 아직 수행되지 않았다고 가정하면, 이동 노드(207)는, 컨텍스트 전송 매니저(200)로부터 수신된 컨텍스트에 포함된 정보에 기초하여 자신의 네트워크 장치를 사전 구성(506)할 수 있고, 예를 들어, IPv6 네트워크의 WLAN 인터페이스를 이용하는 경우, 이동 단말기(207)는, 액세스 네트워크를 결정(507)하여 다음 액세스 네트워크를 결합(join)하고 그것에 핸드오버시 처럼, 새로운 IP 어드레스, 새로운 디폴트 게이트웨이 등을 갖는 네트워크 인터페이스의 사전 구성을 생성할 수 있고, 사전 구성 설정을 인계받아 네트워크 인터페이스의 새로운 구성을 이용하여 새로운 액세스 네트워크로의 통신을 즉시 개시(508)할 수 있다.

[0104] 컨텍스트 전송 매니저(200)로부터 컨텍스트를 수신(509)하는 액세스 네트워크는, 그 컨텍스트 내의 정보를 이용하여 가능성있는 접속 이동 클라이언트(207)를 위한 액세스 네트워크를 준비(510)하여도 된다. 접속 이동 클라이언트(207)에 대하여 특정 구성을 관련짓기 위해, 이동 노드가 네트워크에 접속시 컨텍스트 매니저가 이동 노드(207)를 식별할 수 있게 하며 통신용 컨텍스트 정보를 이용(511)할 수 있게 하는 인접 액세스 네트워크의 컨텍스트 매니저(209, 210, 211)에 송신되는 컨텍스트에 식별자를 포함할 수 있다.

도면의 간단한 설명

[0048] 이하, 첨부 도면을 참조하여 본 발명을 보다 상세히 설명한다. 도면에서 유사하거나 대응하는 부분은 동일한 부재 번호로 표시되어 있다.

[0049] 도 1은 본 발명의 일실시예에 따라 홈 도메인으로부터 방문 도메인의 프록시를 통해 WLAN으로 컨텍스트를 전송하는 간략한 구조를 나타내는 도면,

[0050] 도 2는 본 발명의 일실시예에 따라 이동 노드에 대한 컨텍스트 전송을 관리하는 통신 네트워크의 아키텍처 개략도,

[0051] 도 3은 본 발명의 일실시예에 따라 컨텍스트 생성 프로세스를 나타내는 도면,

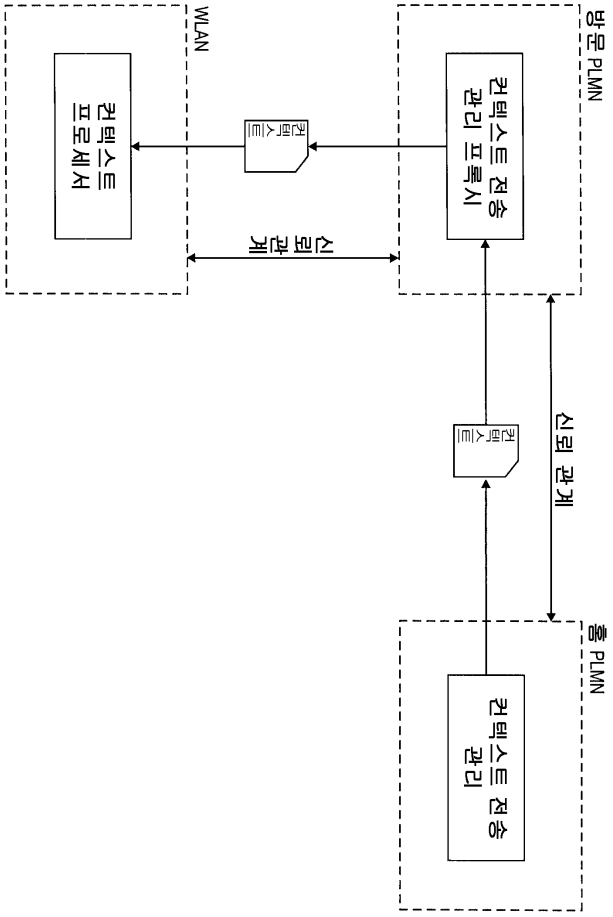
[0052] 도 4는 본 발명의 일실시예에 따라 컨텍스트 전송 기능들을 갖는 외부 AAA 서버로부터 WLAN의 액세스 라우터 또는 인증 서버(AS)로의 컨텍스트 전송 프로세스를 나타내는 도면,

[0053] 도 5는 본 발명의 일실시예에 따라 컨텍스트 전송 프로세스의 흐름도,

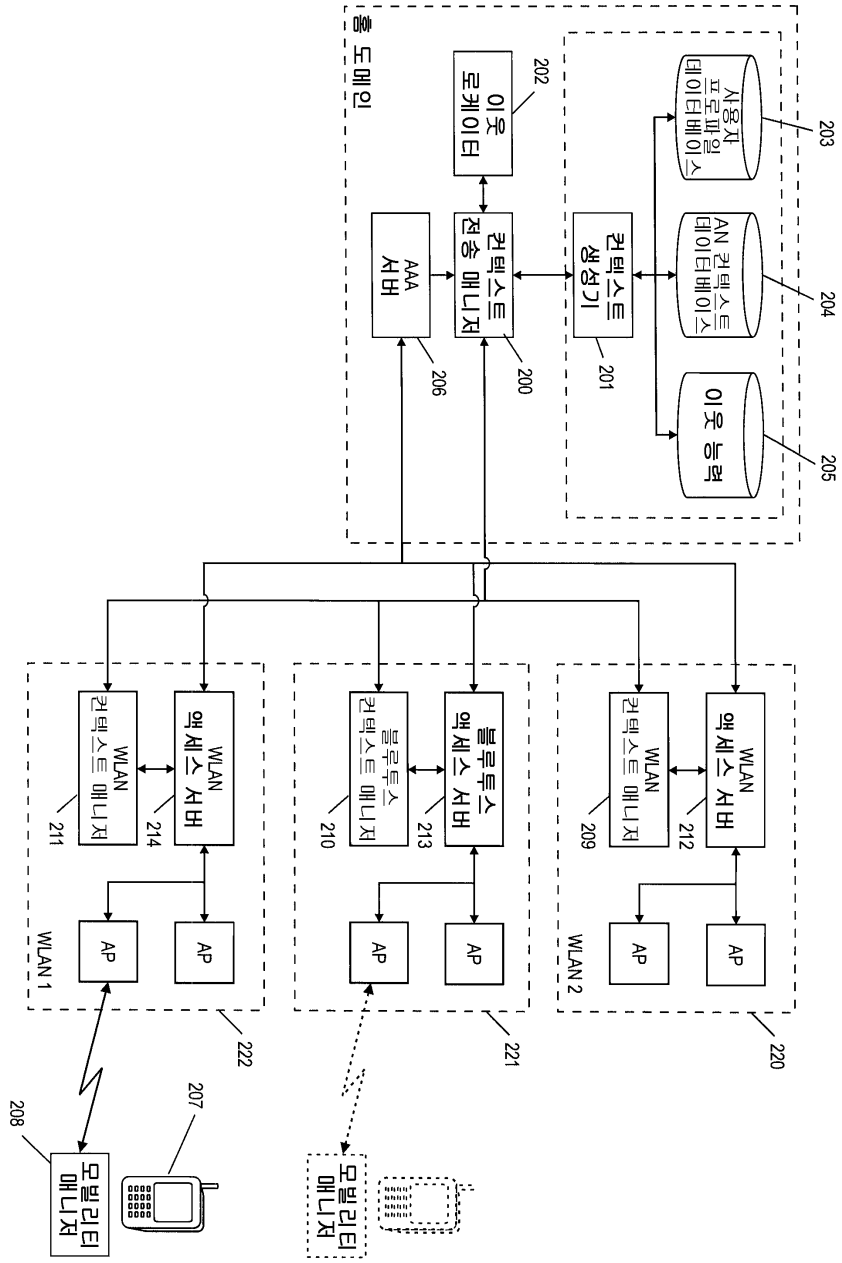
[0054] 도 6은 본 발명의 일실시예에 따라 방문 네트워크에 접속된 이동 노드에 대한 컨텍스트 전송을 관리하는 통신 네트워크의 아키텍처 개략도.

도면

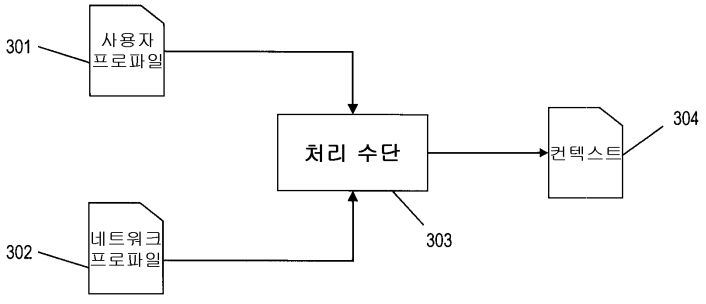
도면1


방문 PLMN
WLAN
컨텍스트 전송 관리 프록시
컨텍스트 프로세서
컨텍스트
신뢰 관계
신뢰 관계
컨텍스트
홈 PLMN
컨텍스트 전송 관리

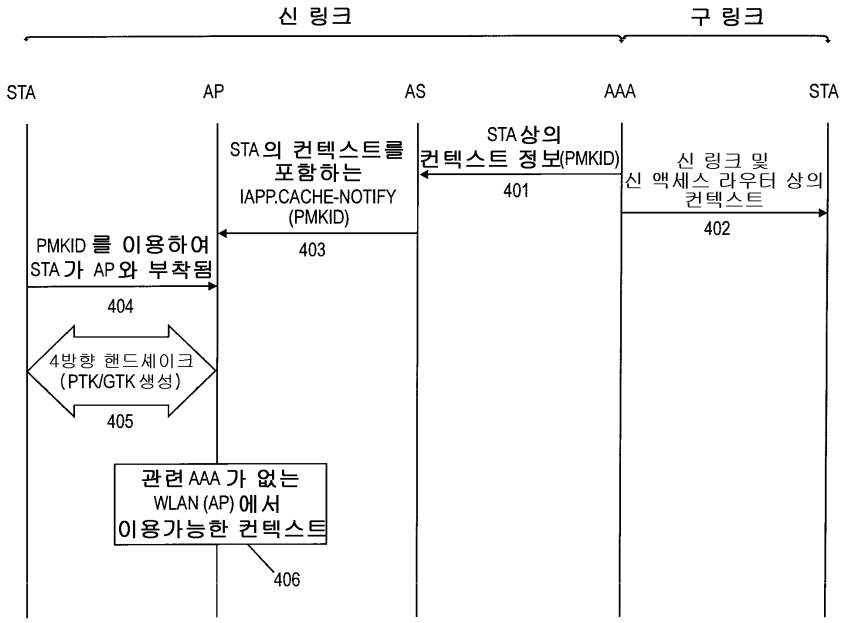
도면2


홈 도메인
이웃 로케이터
202
사용자 프로파일 데이터베이스
203
AN 컨텍스트 데이터베이스
204
이웃 능력
205
AAA 서버
206
컨텍스트 전송 매니저
200
컨텍스트 생성기
201
WLAN 컨텍스트 매니저
211
WLAN 액세스 서버
214
블루투스 컨텍스트 매니저
210
블루투스 액세스 서버
213
WLAN 컨텍스트 매니저
209
WLAN 액세스 서버
212
AP
WLAN 1
222
WLAN 2
220
221
모빌리티 매니저
208
207

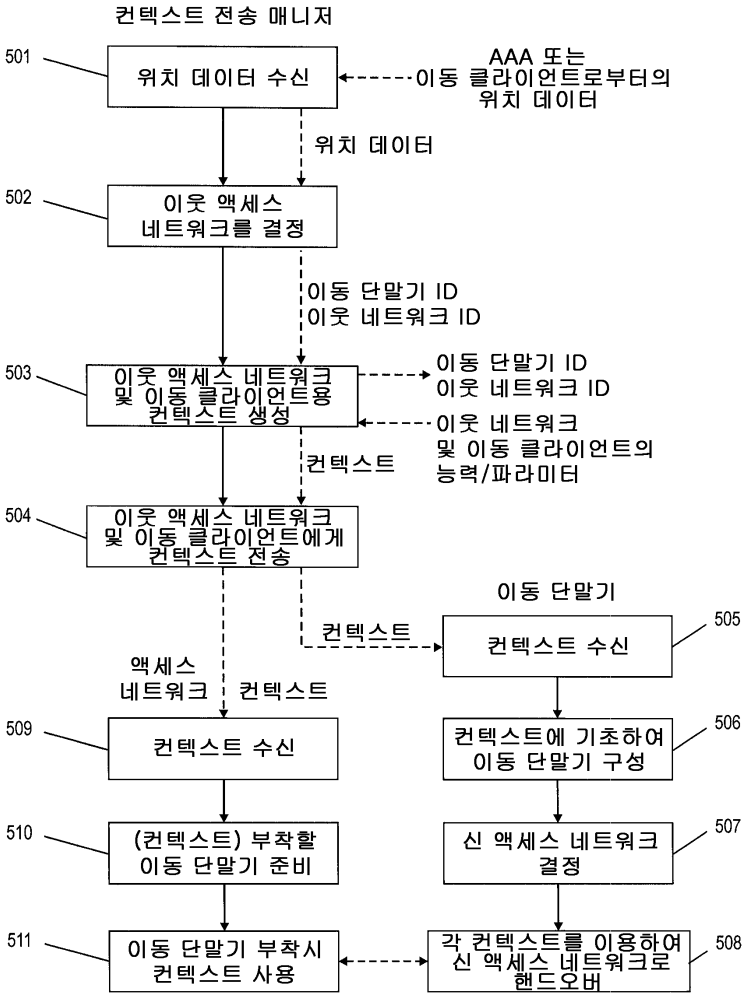
도면3


301
사용자 프로파일
처리 수단
303
컨텍스트
304
302
네트워크 프로파일

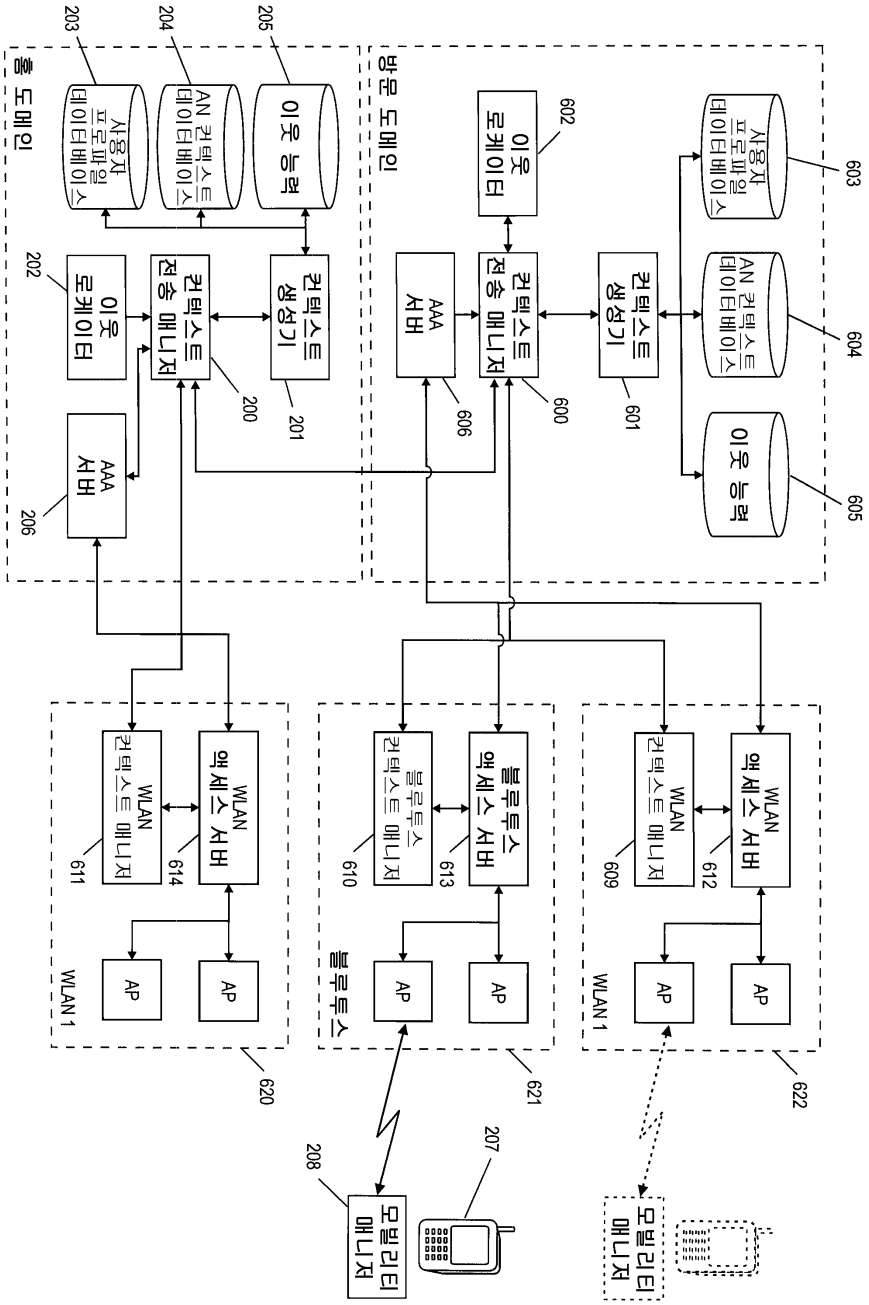
도면4


신 링크
구 링크
STA
AP
AS
AAA
STA
STA의 컨텍스트를 포함하는 IAPP.CACHE-NOTIFY (PMKID)
403
STA상의 컨텍스트 정보(PMKID)
401
신 링크 및 신 액세스 라우터 상의 컨텍스트
402
PMKID를 이용하여 STA가 AP와 부착됨
404
4방향 핸드셰이크 (PTK/GTK 생성)
405
관련 AAA가 없는 WLAN (AP)에서 이용가능한 컨텍스트
406

도면5


컨텍스트 전송 매니저
501
위치 데이터 수신
AAA 또는 이동 클라이언트로부터의 위치 데이터
위치 데이터
502
이웃 액세스 네트워크를 결정
이동 단말기 ID
이웃 네트워크 ID
503
이웃 액세스 네트워크 및 이동 클라이언트용 컨텍스트 생성
이동 단말기 ID
이웃 네트워크 ID
이웃 네트워크 및 이동 클라이언트의 능력/파라미터
컨텍스트
504
이웃 액세스 네트워크 및 이동 클라이언트에게 컨텍스트 전송
이동 단말기
컨텍스트
505
컨텍스트 수신
액세스 네트워크
컨텍스트
509
컨텍스트 수신
506
컨텍스트에 기초하여 이동 단말기 구성
510
(컨텍스트) 부착할 이동 단말기 준비
507
신 액세스 네트워크 결정
511
이동 단말기 부착시 컨텍스트 사용
508
각 컨텍스트를 이용하여 신 액세스 네트워크로 핸드오버

도면6


홈 도메인
방문 도메인
이웃 능력
AN 컨텍스트 데이터베이스
사용자 프로파일 데이터베이스
컨텍스트 생성기
컨텍스트 전송 매니저
이웃 로케이터
AAA 서버
WLAN 액세스 서버
WLAN 컨텍스트 매니저
블루투스 액세스 서버
블루투스 컨텍스트 매니저
블루투스
WLAN 1
AP
모빌리티 매니저
200
201
202
203
204
205
206
207
208
600
601
602
603
604
605
606
609
610
611
612
613
614
620
621
622