

특허청구의 범위

청구항 1

위치기반 시스템과 프라이버시 체크 시스템을 포함하여 사용자 단말로부터의 요청에 따라 개인 단말기 사용자의 위치정보를 전송하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템에 있어서,

상기 위치기반 시스템은

사용자단말로부터 위치정보 서비스 설정/제공요청을 접수하는 위치 응용서버와,

위치 정보를 사용자 단말에 전달하는 위치 데이터 서버와,

상기 위치 응용서버 및 위치 데이터 서버와 연결되어 서비스 설정/제공요청을 접수하고 저장된 위치정보를 제공하는 위치서버와,

상기 사용자 단말로부터 요청된 접근허가 리스트, 접근 허가시간 정보 리스트, 접근허가 지역 리스트를 기반으로 PSP(Privacy Self- control Protocol) 프로토콜을 통해 접근권한 정보 등록 및 변경을 위한 기능을 담당하는 자기제어 관리(Self_Control Manager) 모듈을 포함하여 이루어지고,

상기 PSP(Privacy Self- control Protocol) 프로토콜을 통해 접근권한 정보 등록 및 변경을 위한 요청신호를 접수하여 처리하는 Privacy Profile Registry 모듈을 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템.

청구항 2

제 1 항에 있어서,

상기 Privacy Profile Registry 모듈은 사용자가 설정한 접근 설정규칙(Access Rule)을 이용하여 기본 PSP 정보(Basic PSP Info)를 PSP 메시지 형식 분석(PSP Message Format Analyzer)모듈에게, 접근 규칙(Access Rule)을 접근 제어형식 분석(Access Control Format Analyzer)모듈에게 각각 분배하는 Access Rule Format 모듈과,

상기 접근 설정규칙(Access)을 형식확인(Loader&Format Checker)모듈로 넘겨주는 PSP 메시지 형식 분석(PSP Message Format Analyzer)모듈과,

상기 PSP 메시지 형식분석모듈을 적용하여 PSP 접근 규칙(PSP Access Rule)을 생성하는 상기 형식확인 모듈과,

상기 PSP 접근 규칙(PSP Access Rule)과 Formal Rule 정보를 나뉘어진 정보를 합하여 임시로 프라이버시 프로파일을 만드는 접근 제어형식 분석(Access Control Format Analyzer)모듈과,

상기 프라이버시 자기제어 프로파일을 생성 및 갱신을 하고 PSP기반의 임시 자기제어 정보데이터를 생성하는 개인 프로파일 프리프로세서를 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템.

청구항 3

제 1 항에 있어서,

상기 프라이버시 체크시스템은 접근 권한이 확인된 사용자가 위치정보를 요청한 경우 사용자에게 필요한 위치정보를 획득하되, 상기 Privacy Profile Registry 모듈에게 받은 PSP기반의 자기제어 메시지(PSP Access Control Message)를 접수하는 PSP 액세스 제어 데이터 분석(PSP Access Control Data Analyzer)모듈과,

상기 PSP기반의 접근제어 메시지(PSP Access Control Message)는 상기 분석모듈을 거쳐 Privacy Checking모듈을 통해 사용자 권한을 체크하는 프라이버시 체크모듈과,

상기 프라이버시 체크모듈을 거친 데이터를 저장하는 데이터 저장소(Data Storage)를 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템.

청구항 4

제 2 항에 있어서, 상기 데이터 저장소(Data Storage)에 저장된 데이터의 쿼리 분석을 수행하여 저장하는 쿼리 분석(Query Analyer)과 쿼리 실행 모듈(Executive Query Module)을 포함하는 쿼리 처리기(Query Processor) 및 승인된 사용자의 요청에 따라 필요한 데이터를 추가, 수정, 삭제하여 필요한 데이터를 갱신하고 각 사용자의 요청에 따라 처리를 하는 Data Processor(29)를 더 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템.

청구항 5

프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 방법에 있어서,

사용자가 사용자 위치정보 접근 설정을 LBS 시스템에 요청하는 제1 단계;

LBS시스템의 자기제어관리모듈을 통해 접근 권한을 확인하는 제2 단계;

상기 자기제어관리모듈은 접근 설정규칙을 이용하여 접근권한을 체크하고 임시로 프라이버시 프로파일을 만드는 제3 단계;

Privacy Checking Entity를 통해 프라이버시 프로파일을 체크하는 제4 단계;

PSP기반 임시 자기제어 정보데이터를 생성하고 저장하는 제5 단계;를 포함하여 이루어진 것을 특징으로 하는 제 1 항 내지 제 4 항 중 어느 한 항에 따른 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 방법.

청구항 6

프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 사용자 위치정보요청 처리방법에 있어서,

사용자로 부터 Location Application Server에 위치요청이 있는 경우, 위치서버는 프라이버시 체크 Entity를 통해 접근권한과 프로파일을 확인하는 제 6 단계;

프라이버시 프로파일 레지스트리에 프라이버시 권한 확인을 하고 프라이버시 권한을 승인하는 제 7 단계;

승인완료된 경우 위치서버를 통해 위치 데이터 서버에 사용자가 요청했었던 위치정보에 대한 제공을 요청하는 제 8 단계;를 포함하여 이루어진 것을 특징으로 하는 제 1 항 내지 제 4 항 중 어느 한 항에 따른 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 사용자 위치정보요청 처리방법.

명 세 서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 위치기반서비스(Location Based Service:LBS)인 개인 위치 정보를 사용하는 사용자들의 개인 위치정보를 사용자 스스로 제어 하고, 정보유출 및 악용을 방지 할 수 있는 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 위치정보기반서비스와 관련한 OMA(Open Mobile Alliance) 표준화 동향을 살펴보면 다음과 같다. OMA LOC WG은 Location Interoperability Forum(LIF) 기구와 통합되어, MLP(Mobile Location Protocol), RLP(Roaming

Location Protocol), SUPL(Secure User Plane Location) 및 PCP(Privacy Check Protocol) 등에 대한 표준화를 진행하고 있다. OMA의 프로토콜을 소개하면, 먼저, MLP(Mobile Location Protocol)로서 위치 추적을 실시하는 망 구조와 측위 방법에 상관없이 위치서버(location server)와 위치 클라이언트(LCS client)간에 사용자 이동단말 등의 위치를 요청하고 전달하는 응용 레벨 프로토콜이고, 위치서버와 위치클라이언트간의 프로토콜이 있다. 둘째, RLP(Roaming Location Protocol)로서 이는 서로 다른 통신망에 존재하는 위치서버간 프로토콜이며, MLP의 DTD element 및 attribute를 근간으로 하고 있으며 roaming과 관련된 부분들이 특화되어 있는 프로토콜이다. 또한 PCP(Privacy Checking Protocol)은 사용자가 미리 설정한 위치 정보와 관련된 privacy 설정 정보를 기반으로 위치서버가 위치정보를 요청하는 위치 클라이언트에 대한 privacy 보호를 목적으로 하는 프로토콜이다.

[0003] OMA PCP 표준 현황 분석에서 먼저 PCP(Privacy Checking Protocol)에 살펴보면 이는 위치정보 보호 및 인증 기술에 대한 규격이며, 위치정보를 수집 및 제공하는 위치 서버와 외부 프라이버시 인증부간의 프로토콜이고, 여기서, PCE(Privacy Checking Entity) : privacy 설정 정보를 갖고 있는 서버로 PCP는 PCE와 위치서버간의 프로토콜을 정의한다. PCP(Privacy Checking Protocol) 세부 모듈 구성은 위치 서버, 프라이버시 인증부, 위치 응용 클라이언트 등 3가지 주요 모듈로 구성된다.

[0004] 최근 사용자들은 조금 더 편리한 생활을 위치기반 서비스를 많이 이용하는 실정이다. 예를 들면, 다양한 생활 밀착형 서비스로서 친구 찾기, 교통안내 서비스, 긴급구조 요청 등의 서비스가 제공되고 있다. 또한 국외에서는 재난 발생에 대처하기 위한 서비스를 지원하고 있으며, 핸드폰에 GPS 모듈이 탑재된 예도 있다. 또한, 다양한 생활정보 제공 서비스도 제공되고 있는데, 예를 들면, 대중교통을 이용한 최단거리 계산 및 안내 서비스, 안전 운행 서비스를 위한 운행 정보 제공, 주유소, 식당 등의 사용자 요청에 따른 정보 이용 및 안내 서비스 제공등을 들 수 있다.

[0005] 다시말하면, 최근 이동통신의 기술 발달과 휴대폰, 노트북, PDA 등의 휴대용 단말기의 진화를 통해 사용자는 이동 중에도 자신이 원하는 작업을 언제 어디서나 처리할 수 있다. 특히, 사용자의 휴대용 단말기 사용은 점차 일반화되고 있으며, 무선망은 사용자의 이동성(mobility)을 지원할 수 있어 이러한 특성을 반영한 무선인터넷 서비스가 점차 늘어나고 있는 추세다.

[0006] 그러나, 이러한 위치기반 서비스에 있어서, 먼저 개인정보 유출에 대한 정부 대책이 미흡한 문제점 있고, 이를 해결하기 위하여 가칭 위치정보보호법이 준비되고 있는데, 그 내용은 개인위치정보 보호의 범위, 정보이용의 법적 근거를 마련하는 데 초점을 두어 위치기반서비스(location-based service: LBS) 활성화의 순기능을 유도하고, 개인정보 노출과 사생활 침해 등 개인위치정보 서비스에 따른 부작용을 방지하고자 하는 것이다. 그러나, 정부 기술정책 추진의 정부 대책 및 지원이 부족한 실정이다.

[0007] 또한, 종래 위치기반 서비스는 개인위치정보의 보호기술 및 대책이 미흡한 문제점이 있는데, 예를 들어, 정당한 사용자가 아닌 비정상적인 사용자의 정보 악이용에 대한 개인 사생활 침해 문제에 대한 대책이 미흡하고, 개인 신상정보, 개인 위치정보등의 정보 누출로 개인 위치 추적이 가능하며 사회적인 큰 문제가 발생하며, 개인정보 오남용의 여지인 프라이버시 침해에 대한 인권 침해요소를 제거할 수 있는 대책이 필요한 실정이다. 즉, 정보 프라이버시 : 신용정보와 의료기록과 같이 지극히 개인적인 정보들의 취급과 수집을 통한 사생활 침해, 영역 프라이버시 : 가정과 직장, 기타 공공장소에서의 침해의 제한, 통신 프라이버시 : 통신상태의 프라이버시 침해문제가 있다.

[0008] 종래의 위치기반 서비스는 이동통신 사업자에 의해 무분별한 개인위치정보 검색/모니터링 문제 발생, 제 3 자에 의한 불법적인 개인위치정보 검색으로 인한 문제점 발생, 공공분야에 위치정보 서비스를 도입하고자 할 경우 사회적 저항 문제 발생, 위치정보에 대한 개인별 시간대 및 영역 설정 방식 부재로 인한 프라이버시 침해, 위치정보에 대한 도청/가로채기, 불법 정보수집, DoS 공격 등 취약점 발생과 같은 문제점이 있다.

[0009] 상기와 같은 종래의 문제점 중 먼저, 공격자의 여부 파악이 불가능한 문제점을 살펴보면, 자동화 시스템 상의 위치정보 시스템 공격자의 여부 파악이 미흡하고, 인증된 공격자에 대한 대책 미비하다.

[0010] 또한, 도청 또는 가로채기 위협이 존재하는 문제점을 살펴보면, 위치결정시스템과 위치정보 타겟 디바이스간 전송 내용에 대한 도청/가로채기 문제, 위치 프라이버시 규칙 서버에 전송되는 내용에 대한 도청/가로채기 등 수행등의 문제점이 있다.

[0011] 또한, 신분 위장(Identify Spoofing) 공격의 문제점을 살펴보면, 공격자는 위치결정시스템으로부터 위치정보서버까지 네트워크 트래픽을 위장하도록 시도하고, 개인의 프라이버시를 침해 받을 수 있는 사진들이 공개(Google Earth)되고, 개인의 위치정보가 모바일 마케팅이나 개인감시에 사용될 경우 심각한 문제 발생하며, 너

무 자세한 위치추적이 개인적인 사생활 침해가 될 수 있다.

- [0012] 또한, 정보 수집 공격 및 DoS 공격분야에서의 문제점은 트래픽 분석은 도청자가 특정한 위치에서 표적들의 신분이나 특징을 확인하도록 허용하고, 전송되는 메시지에 대한 암호문 분석 및 평문 형태의 메시지 내용 분석하는 문제점이 있다.
- [0013] 또한, 위치정보 규칙의 위변조 공격의 문제점에 있어서는 악의적인 사용자에게 의한 상대방 사용자의 위치정보 위·변조 문제 대두되고 있으며, 국가적인 차원에서 사용자의 동의 없는 정보조작 가능한 문제점이 있다.
- [0014] 또한, 위치정보의 기밀성 문제 및 이동통신사에 의한 개인위치정보 누출 공격의 문제점을 살펴보면, 개인의 프라이버시뿐만 아니라 국가 안보에 치명적 영향을 줄 수 있으며, 사용자 개개인의 위치가 24시간 실시간으로 노출될 수 있으며, 이동통신사에 의해 개인의 위치정보가 누출될 수 있는 문제점이 있다.
- [0015] 이러한 위치기반서비스(LBS)를 사용하는 사용자들은 자신의 위치정보를 보호 받고 통제 할 수 있는 방법이 절실한 상황이다.

발명의 내용

해결 하고자하는 과제

- [0016] 본 발명의 목적은 위치기반서비스(Location Based Service:LBS)인 개인 위치 정보를 사용하는 사용자들의 개인 위치정보를 사용자 스스로 제어 하고, 정보유출 및 악용을 방지 할 수 있는 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템 및 방법을 제공하는데 있다.

과제 해결수단

- [0017] 상기한 바와 같은 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따르면, 위치기반 시스템과 프라이버시 체크 시스템을 포함하여 사용자 단말로부터의 요청에 따라 개인 단말기 사용자의 위치정보를 전송하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템에 있어서,
- [0018] 상기 위치기반 시스템은
- [0019] 사용자단말로부터 위치정보 서비스 설정/제공요청을 접수하는 위치 응용서버와,
- [0020] 위치 정보를 사용자 단말에 전달하는 위치 데이터 서버와,
- [0021] 상기 위치 응용서버 및 위치 데이터 서버와 연결되어 서비스 설정/제공요청을 접수하고 저장된 위치정보를 제공하는 위치서버와,
- [0022] 상기 사용자 단말로부터 요청된 접근허가 리스트, 접근 허가시간 정보 리스트, 접근허가 지역 리스트를 기반으로 PSP(Privacy Self-control Protocol) 프로토콜을 통해 접근권한 정보 등록 및 변경을 위한 기능을 담당하는 자기제어 관리(Self-Control Manager) 모듈을 포함하여 이루어지고,
- [0023] 상기 PSP(Privacy Self-control Protocol) 프로토콜을 통해 접근권한 정보 등록 및 변경을 위한 요청신호를 접수하여 처리하는 Privacy Profile Registry 모듈을 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템이 제공된다.
- [0024] 또한, 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 방법에 있어서, 사용자가 사용자 위치정보 접근 설정을 LBS 시스템에 요청하는 제1 단계;
- [0025] LBS시스템의 자기제어관리모듈은 접근 권한을 확인하는 제2 단계;
- [0026] 상기 자기제어관리모듈은 접근 설정규칙을 이용하여 접근권한을 체크하고 임시로 프라이버시 프로파일을 만드는 제3 단계;
- [0027] Privacy Checking Entity를 통해 프라이버시 프로파일을 체크하는 제4 단계;
- [0028] PSP기반 임시 자기제어 정보데이터를 생성하고 저장하는 제5 단계;를 포함하여 이루어진 것을 특징으로 하는

프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 방법이 제공된다.

- [0029] 또한, 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 사용자 위치정보요청 처리방법에 있어서, 사용자로 부터 Location Application Server에 위치요청이 있는 경우, 위치서버는 프라이버시 체크 Entity를 통해 접근권한과 프로파일을 확인하는 제 6 단계;
- [0030] 프라이버시 프로파일 레지스트리에 프라이버시 권한 확인을 하고 프라이버시 권한을 승인하는 제 7 단계;
- [0031] 승인완료된 경우 위치서버를 통해 위치 데이터 서버에 사용자가 요청했었던 위치정보에 대한 제공을 요청하는 제 8 단계;를 포함하여 이루어진 것을 특징으로 하는 프라이버시 자기 제어 프로토콜 기반의 개인위치정보 설정 시스템을 이용한 사용자 위치정보요청 처리방법이 제공된다.

효 과

- [0032] 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템 및 방법에 의하면, 프라이버시 자기제어 프로토콜(PSP)을 기존의 프로토콜들을 연동하여 사용자 개인이 자신의 위치정보에 대한 프라이버시 설정기능을 제공하여 기존의 해결하지 못하고 심각한 사회문제로 야기될 수 있는 사생활 침해에 대한 문제와 종래의 문제점을 해결 할 수 있다.
- [0033] LBS 제품 개발시 안정성을 확보한 개인위치정보 방식을 제안하여 개인위치정보의 안전성 및 신뢰성 확보에 기여할 수 있다.
- [0034] 정보보호 기술에 대한 안정성 및 성능에 대한 비교/분석이 가능하게 되어, 기술적으로 우수한 제품 개발을 지원할 수 있는 토대를 제공한다.
- [0035] 또한, 종래의 문제점을 해결하고 본인 이외의 개인정보 유출로 문제가 생기는 문제를 방지할 수 있다.

발명의 실시를 위한 구체적인 내용

- [0036] 이하 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템 및 방법에 대하여 첨부도면을 참조하여 상세히 설명한다.
- [0037] 도 1은 본 발명에서 제시하는 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템의 개략적인 도면이다. 이 시스템은 기존의 위치 추적을 실시하는 망 구조와 측위 방법에 상관없이 위치서버(location server)(16)와 위치 클라이언트(LCS client)(2)간에 사용자 이동단말(11) 등의 위치를 요청하고 전달하는 응용 레벨 프로토콜인 MLP(Mobile Location Protocol)와 사용자가 미리 설정한 위치 정보와 관련된 privacy 설정 정보를 기반으로 위치서버가 위치정보를 요청하는 위치 클라이언트에 대한 privacy 보호를 목적으로 하는 프로토콜인 PCP(Privacy Checking Protocol)를 기반으로 하는 LBS 시스템에 PSP 프로토콜을 추가하는 방식이다. 본 발명에서는 도 1과 같은 방식으로 기존 시스템에 최소한의 변화로 사용자가 직접 자신의 위치정보를 제어 할 수 있는 시스템을 제안하였다.
- [0038] 개인 모바일 단말(11)로부터 수집된 위치정보에 대해 본 발명에서 제안하는 개인위치정보 프라이버시 설정 프로토콜(PSP : Privacy Self-Control Protocol)을 이용하여 프라이버시 프로파일(Privacy Profile)을 생성/갱신하도록 하고, 접근권한을 부여받은 응용 서비스 사용자(2)에게만 개인위치정보를 제공할 수 있도록 하여 프라이버시 보호 기능을 제공함으로써 사용자의 개인 위치정보가 보장될 수 있도록하고 또한 본인이 그 정보를 제어할 수 있는 서비스를 제공한다.
- [0039] 도 2는 본 발명에서 제안하는 위치정보 프라이버시 설정 프로토콜의 간단한 단계를 구별하여 설명하는 개념도이다.
- [0040] 도 2를 참조하면, 본 발명에서 제안하는 위치정보 프라이버시 설정 프로토콜의 간단한 단계를 구별하자면 간략히 3단계로 표현될 수 있다.

- [0041] - 1단계 : 1단계에서는 위치정보 자기제어 정보 설정 주체 및 정보 형태를 제시하여 사용자로 하여금 자신의 위치정보 접근 설정을 한다.(주체 : 가입자/사용자)
- [0042] - 2단계 : 이는 1단계에서 사용자로부터 얻은 접근 설정 정보를 통해 사용자의 위치정보 접근권한을 Null로 설정하고 정보를 저장/관리를 하는 단계이다.(주체 : 정부기관(공공기관), LBS 산업체/서비스 제공자)
- [0043] - 3단계 : 이 단계에서는 이동통신사에 의해 새로운 위치정보 수집/전송을 하는 단계이다.(주체 : 이동통신사)
- [0044] 실질적인 PSP프로토콜이 적용된 단계는 1,2단계라고 말할 수 있다.
- [0045] 도 3은 본 발명에 따른 개인의 위치정보에 대한 프라이버시 설정 기능을 제공하는 단계 및 작동방식에 대한 설명도이다.
- [0046] 도 3을 참조하면, 위치정보 프라이버시 설정 프로토콜 작동 방식에 있어서, 본 발명에서 제안하는 시스템은 프라이버시 자기제어 프로토콜(PSP)을 이용하여 기존의 MLP, PCP 프로토콜과 연동하여 사용자 개인이 자신의 위치정보에 대한 프라이버시 설정 기능을 제공하는 단계 및 작동방식에 대해 설계하고 이를 보완하는 시스템이다. 도 3은 본 발명에서 제안하는 시스템의 작동 방식이다. 이는 제안한 프로토콜(MLS PCP/PSP with HTTP)을 통한 송수신 메시지 포맷 및 내용 설정하고 관리하는 방식의 모듈들로 구성이 되어있다.
- [0047] 세부적인 작동방식은 총 6단계로 구성될 수 있다.
- [0048] - 1단계 : 첫 단계에서 사용자는 자신의 단말(11 또는 11-1)로 자신의 위치정보를 자기제어 하기 위해 LBS시스템(10)에 요청을 하는 단계이다.
- [0049] - 2단계 : 2단계에서는 PCP 프로토콜을 통해 Privacy Checking Entity모듈(20)를 통해 프라이버시 권한 확인을 요청하는 단계이다.
- [0050] - 3단계 : Privacy Checking Entity모듈(20)에서는 프라이버시 권한 확인을 위해 Privacy Profile Registry(30)에게 프라이버시 프로파일을 요청하여 정당한 권한을 가진 사용자인지를 확인요청을 한다.
- [0051] - 4단계 : Privacy Profile Registry(30)에서는 3단계에서 요청한 프라이버시 프로파일을 제공하는 단계이다.
- [0052] - 5단계 : 3,4단계에서의 수행이 이루어지고 이 단계에서는 PCP 프로토콜을 통해 사용자의 권한 승인여부를 결정하게 된다.
- [0053] - 6단계 : 이 단계에서는 5단계의 PCP 프로토콜을 통해 권한이 승인된 경우 다시 Privacy Profile Registry(30)에 프라이버시 자기제어 프로파일을 생성 및 갱신을 하는 단계이다.
- [0054] 도 4는 본 발명에 따른 개인의 위치정보에 대한 프라이버시 설정 및 위치정보 제공요청 프로토콜에 대한 설명도이다.
- [0055] 도 4를 참조하면, 위치정보 프라이버시 설정 및 위치정보 제공 요청 프로토콜에 있어서, 프라이버시 자기제어 프로토콜(PSP)을 이용하여 Privacy Profile을 참조하여 접근권한 등에 대한 검증/확인 과정을 거쳐 접근권한을 획득한 후 응용 서비스 이용자에게 원하는 개인 사용자에게 위치정보를 제공하는 과정에 대해 설명한다.
- [0056] 도 4는 도 3 작동방식과는 반대로 MLP 프로토콜을 통해 위치정보를 요청해서 확인하는 작동방식을 나타내는 그림이다. 이는 LBS 시스템을 조금 더 세분화해서 나타낼 수 있다.
- [0057] - 1단계 : 사용자(11)가 MLP 프로토콜을 통해 위치정보를 LBS 시스템(10)에 요청을 하는 단계이다.
- [0058] - 2단계 : 1단계에서 요청한 위치정보는 MLP 프로토콜을 통해 LBS 시스템(10)의 Location application server(12)를 거쳐 Location Server(16)에 위치정보를 요청하게 된다.
- [0059] - 3단계 : 3단계는 도 3과 같은 방식으로 PCP 프로토콜을 통해 사용자의 프라이버시 권한 확인을 한다.
- [0060] - 4,5단계 : 3단계의 확인을 위해 4,5단계에서는 Privacy Profile Registry(30)에 프라이버시 프로파일을 요청하고 받는다.
- [0061] - 6단계 : 이 단계에서는 Privacy Profile Registry(30)에서 승인하여 얻은 프라이버시 프로파일과 PCP 프로토콜을 통해 프라이버시 권한 승인을 한다.
- [0062] - 7단계 : 모든 승인 단계가 문제 없이 진행되었을 경우 LBS시스템(10)의 Location Server(16)를 통해 Location Data Server(14)에 사용자가 요청했었던 위치정보에 대한 제공을 요청한다.

- [0063] - 8단계 : 요청받은 위치정보를 MLP 프로토콜을 통해 각각의 사용자에게 재분배하여 나누어주는 최종단계이다.
- [0064] 도 5는 본 발명에 따른 프라이버시 자기제어 프로토콜(PSP) 기반 OMA MLS 표준 스펙을 지원하는 개인위치정보 자기제어 방식을 설명하는 개념도이다.
- [0065] 도 5를 참조하면, 본 발명에 따른 프라이버시 자기제어 프로토콜(PSP) 기반 OMA MLS 표준 스펙을 지원하는 개인위치정보 자기제어 방법은 OMA MLS 표준을 준용하고 PCP와 연동하는 PSP 프로토콜 지원 방식이다.
- [0066] 도 5는 사용자가 자신의 위치정보 접근 설정하여 자신의 위치정보를 제어하기 위해 요청을 하는 도면이다. 세부 모듈에서 설명 했듯이 이는 LBS시스템(10)의 Self-Control Manager(18)를 통해 Privacy Profile Registry 모듈(30)에 사용자 프라이버시 권한을 요청하고 이를 등록하고 자기제어 프로파일 생성 및 갱신을 하여 사용자가 자신의 위치정보를 스스로 제어할 수 있도록 해준다.
- [0067] 도 6은 도 5의 전체적인 구성도 및 세부모듈을 나타낸 도면이다.
- [0068] 이하, 도 6을 참조하여 단계별로 개인위치정보 자기제어방법을 설명한다.
- [0069] 1단계 : 사용자가 자신의 위치정보 접근을 설정하기 위해 LBS 시스템(10)에 요청을 하는 단계이다. 주목적은 프라이버시 자기제어이다. 이를 위해 접근허가 리스트, 접근 허가시간 정보 리스트, 접근허가 지역 리스트를 사용자가 설정하여 요청한다.
- [0070] 2단계 : LBS시스템(10)의 추가된 자기제어 관리(Self-Control Manager) 모듈(18)은 PSP(Privacy Self-control Protocol) 프로토콜을 통해 접근권한 정보 등록 및 변경을 위해 Privacy Profile Registry 모듈(30)에 요청을 한다.
- [0071] 2-1단계 : 사용자가 설정한 접근 설정규칙(Access Rule)(31)을 이용하여 Access Rule Format 모듈(33)을 통해 분리하여 기본 PSP 정보(Basic PSP Info)(33a)를 PSP 메시지 형식 분석(PSP Message Format Analyzer)모듈(35)에게, 접근 규칙(Access Rule)(31)을 접근 제어형식 분석(Access Control Format Analyzer)모듈(37)에게 각각 분배한다.
- [0072] 2-2단계 : 접근 설정규칙(Access)(31)을 형식확인(Loader&Format Checker)모듈(34)로 넘겨주고 PSP 메시지 형식 분석(PSP Message Format Analyzer)모듈(35)을 적용하여 PSP 접근 규칙(PSP Access Rule)(36)을 생성한다.
- [0073] 2-3단계 : PSP 접근 규칙(PSP Access Rule)(36)과 Formal Rule 정보를 받아온 접근 제어형식 분석(Access Control Format Analyzer)모듈(37)을 적용하여 나뉘어진 정보를 합하여 임시로 프라이버시 프로파일을 만든다.
- [0074] 2-4단계 : 프라이버시 자기제어 프로파일을 생성 및 갱신을 하고 PSP기반의 임시 자기제어 정보데이터를 생성한다.
- [0075] 3단계 : 접근권한의 여부를 최종적으로 확인을 하는 모듈이다. 접근 권한이 확인된 사용자가 위치정보를 요청한 경우 Privacy Checking Entity(20)를 통해 사용자에게 필요한 위치정보를 얻을 수 있게 된다.
- [0076] 3-1단계 : Privacy Profile Registry 모듈(30)에게 받은 PSP기반의 자기제어 메시지(PSP Access Control Message)를 분석(PSP Access Control Data Analyzer)모듈(26)로 넘긴다.
- [0077] 3-2단계 : PSP기반의 접근제어 메시지(PSP Access Control Message)는 상기 분석모듈(26)을 거쳐 Privacy Checking모듈(28)을 통해 프라이버시 사용자 권한을 체크하고 저장소(Data Storage)(25)에 저장을 한다.
- [0078] 3-3단계 : 저장소(Data Storage)(25)에 저장된 데이터는 쿼리 처리기(Query Processor)(27)안에서 쿼리 분석(Query Analyer)과 쿼리 실행 모듈(Executive Query Module)(27-2)을 통해 다시 데이터를 저장하고, 승인된 사용자는 Data Processor(29)로 필요한 데이터를 추가, 수정, 삭제하여 필요한 데이터를 갱신하고 각 사용자의 요청에 따라 처리를 하는 단계이다.
- [0079] 4단계 : 모든 작업이 종료되면 PCP프로토콜을 통해 Location server(16)로 데이터를 보내고 저장한다. 허가된 사용자로 하여금 위치정보 요청이 필요하다면 자기 제어 할 수 있는 환경 및 단계를 구축한다.
- [0080] 도 7은 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템을 이용한 사용자 개인정보 접근권한 설정 요청과정을 나타낸 흐름도이다.

- [0081] 도 7을 참조하면, 먼저 사용자가 사용자 위치정보 접근 설정을 LBS 시스템에 요청한다(S1).
- [0082] 이후 LBS시스템(10)의 자기제어관리모듈(18)은 접근 권한을 확인한다(S3).
- [0083] 이후 상기 자기제어관리모듈(18)은 접근 설정규칙(31)을 이용하여 접근권한을 체크한다(S5). 이때 임시로 프라이버시 프로파일을 만들게 된다(위 설명 2-3단계 참조).
- [0084] 이후 Privacy Checking Entity를 통해 프라이버시 프로파일을 체크한다(S7).
- [0085] 이후 PSP기반 임시 자기제어 정보데이터를 생성하게 된다(S9).
- [0086] 이후 프라이버시 자기제어 정보데이터를 데이터 저장소(25)에 저장하게 된다(S10)(위 설명 3-2단계 참조).
- [0087] 도 8은 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템을 이용한 사용자 위치정보요청 처리과정을 나타낸 흐름도이다.
- [0088] 도 8을 참조하면, 사용자가 Location Application Server(12)에 위치요청을 하게 되면(S2), 위치서버(16)는 프라이버시 체크 Entity(20)을 통해 접근권한과 프로파일을 확인한다(S4,S6).
- [0089] 이후 프라이버시 프로파일 레지스트리(30)에 프라이버시 권한 확인을 하고 프라이버시 권한을 승인하게된다(S8). 모든 승인단계가 문제없이 진행된 경우 위치서버(16)를 통해 위치 데이터 서버(14)에 사용자가 요청했던 위치정보에 대한 제공을 요청한다(S10).

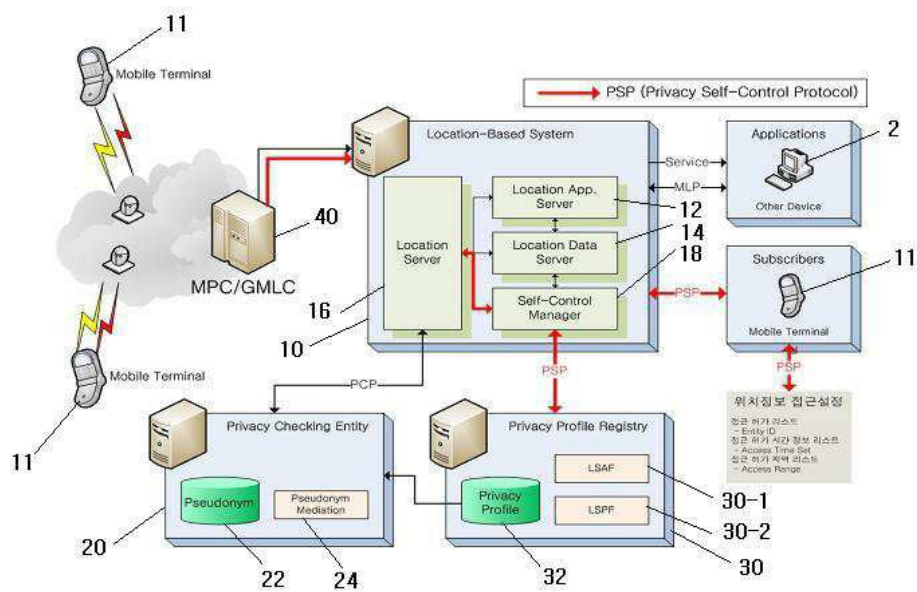
도면의 간단한 설명

- [0090] 도 1은 본 발명에서 제시하는 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템의 개략적인 도면이다.
- [0091] 도 2는 본 발명에서 제안하는 위치정보 프라이버시 설정 프로토콜의 간단한 단계를 구별하여 설명하는 개념도이다.
- [0092] 도 3은 본 발명에 따른 개인의 위치정보에 대한 프라이버시 설정 기능을 제공하는 단계 및 작동방식에 대한 설명도이다.
- [0093] 도 4는 도 3 작동방식과는 반대로 MLP 프로토콜을 통해 위치정보를 요청해서 확인하는 작동방식을 나타내는 그림이다.
- [0094] 도 5는 본 발명에 따른 프라이버시 자기제어 프로토콜(PSP) 기반 OMA MLS 표준 스펙을 지원하는 개인위치정보 자기제어 방식을 설명하는 개념도이다.
- [0095] 도 6은 도 5의 전체적인 구성도 및 세부모듈을 나타낸 도면이다.
- [0096] 도 7은 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템을 이용한 사용자 개인정보 접근권한 설정 요청과정을 나타낸 흐름도이다.
- [0097] 도 8은 본 발명에 따른 PSP(Privacy Self-Control Protocol)기반의 개인위치정보 설정시스템을 이용한 사용자 위치정보요청 처리과정을 나타낸 흐름도이다.
- [0098] * 도면의 주요부분에 대한 부호의 설명 *
- [0099] 10: 위치기반시스템
- [0100] 18: 자기제어 관리(Self-Control Manager)모듈
- [0101] 20: 프라이버시 체크시스템(Privacy Checking Entity)
- [0102] 26: PSP 접근 제어 데이터 분석(PSP Access Control Data Analyzer)모듈
- [0103] 28: Privacy Checking모듈
- [0104] 25: 데이터 저장소(Data Storage)
- [0105] 27: 쿼리처리기
- [0106] 29: 데이터 처리기

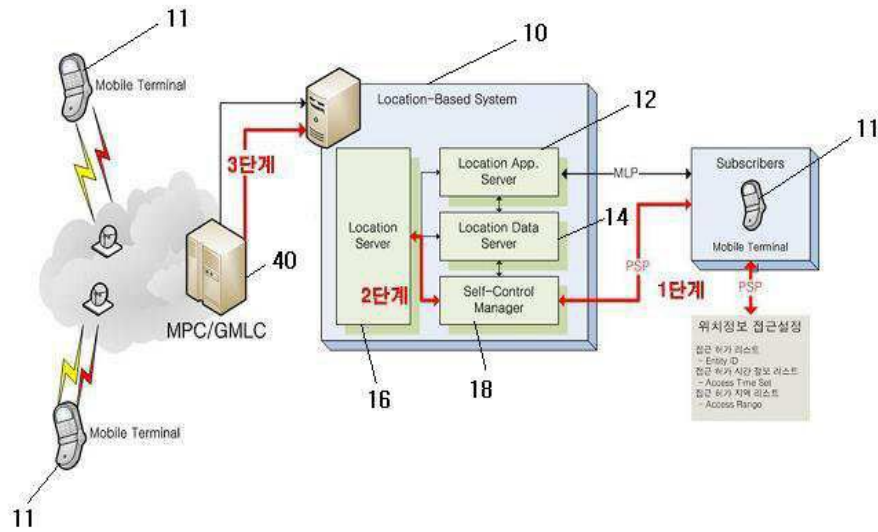
- [0107] 30: 프라이버시 프로파일 레지스트리 모듈
- [0108] 31: 접근 설정규칙(Access Rule)
- [0109] 33: Access Rule Format 모듈
- [0110] 33a: PSP 정보(Basic PSP Info)
- [0111] 35: PSP 메시지 형식 분석(PSP Message Format Analyzer)모듈
- [0112] 37: 접근 제어형식 분석(Access Control Format Analyzer)모듈
- [0113] 34: 형식확인(Loader&Format Checker)모듈
- [0114] 36: PSP 접근 규칙(PSP Access Rule)

도면

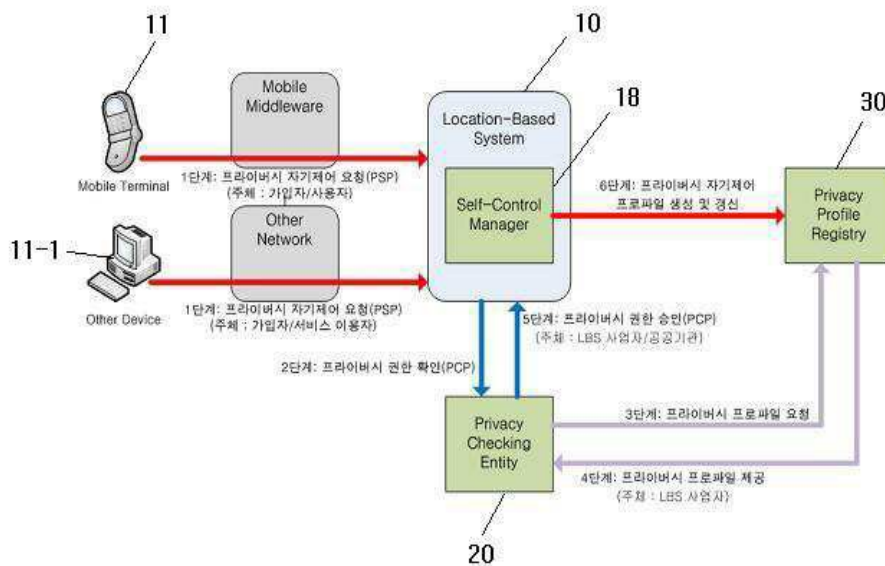
도면1



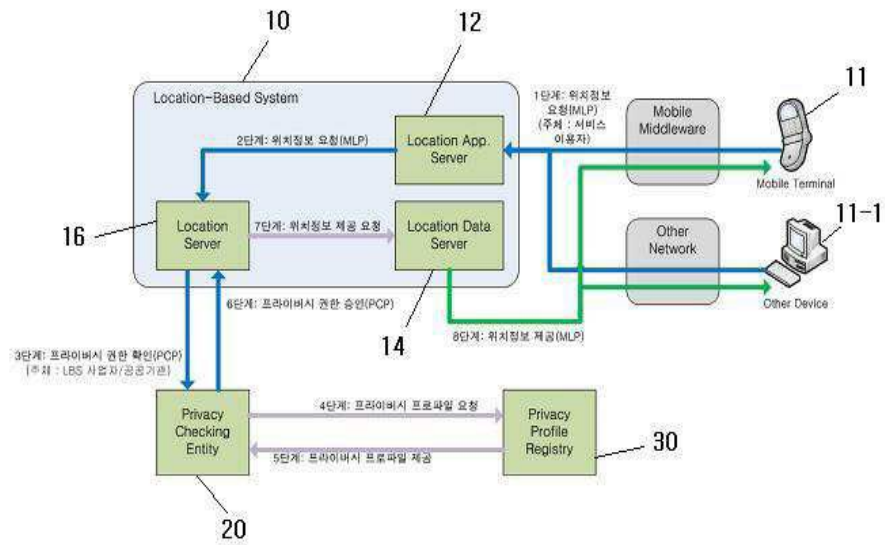
도면2



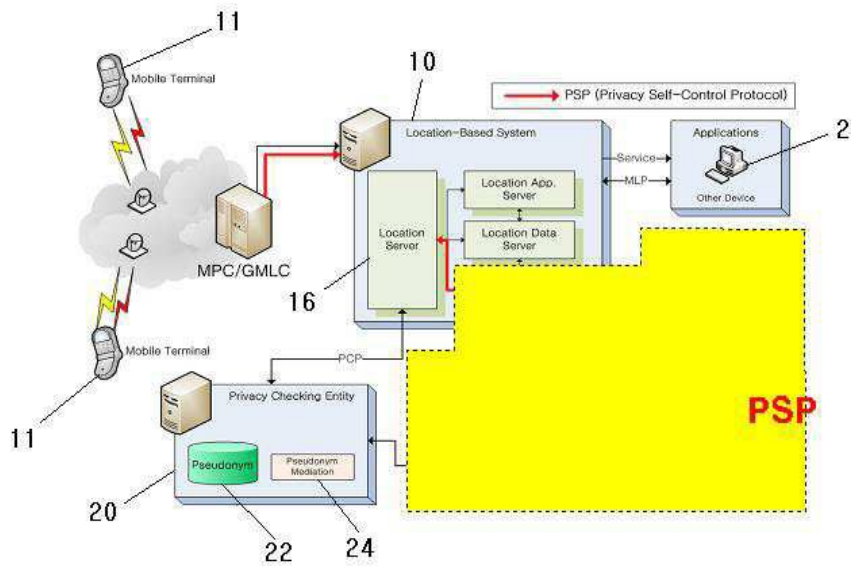
도면3



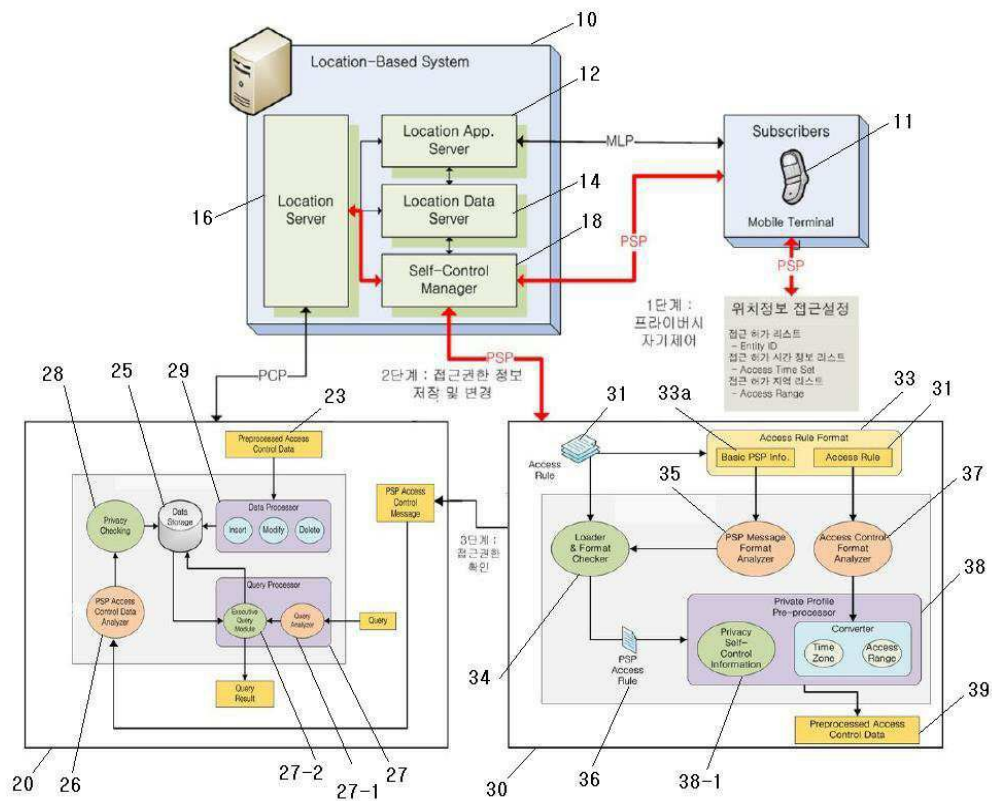
도면4



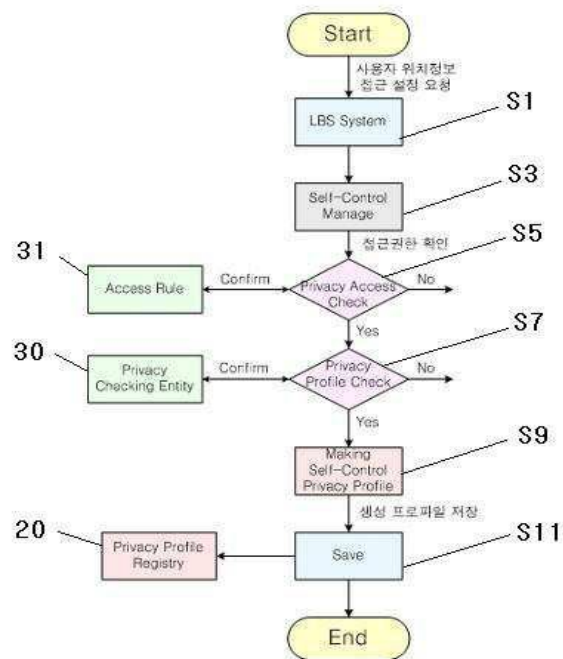
도면5



도면6



도면7



도면8

