(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2021-0127095
(43) 공개일자 2021년10월21일

(51) 국제특허분류(Int. Cl.)
H04L 29/08 (2006.01) *H04L 12/24* (2006.01)
H04W 4/70 (2018.01)
(52) CPC특허분류
H04L 67/16 (2013.01)
H04L 41/0893 (2013.01)
(21) 출원번호 10-2021-0045407
(22) 출원일자 2021년04월07일
심사청구일자 없음
(30) 우선권주장
63/009,035 2020년04월13일 미국(US)

(71) 출원인
현대자동차주식회사
서울특별시 서초구 헌릉로 12 (양재동)
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
기아 주식회사
서울특별시 서초구 헌릉로 12 (양재동)
(72) 발명자
송재승
서울특별시 광진구 능동로 209
(74) 대리인
성병기

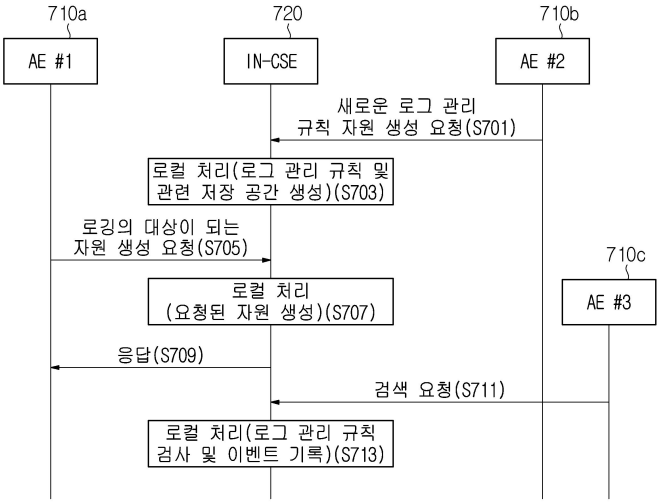
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **M2M 시스템에서 로그 정보를 관리하기 위한 방법 및 장치**

(57) 요 약

본 발명은 M2M(Machine-to-Machine) 시스템에서 로그(log) 정보를 관리하기 위한 방법 및 장치에 대한 것으로, MM2M(Machine-to-Machine) 시스템에서 M2M 장치의 동작 방법은, 로그 관리 규칙(log management rule)의 생성을 요청하는 제1 메시지를 수신하는 단계, 상기 로그 관리 규칙 및 상기 로그 관리 규칙에 따라 생성될 로그 정보를 저장하기 위한 저장 공간을 생성하는 단계, 및 상기 로그 관리 규칙 및 상기 저장 공간의 참조 관계를 설정하는 단계를 포함할 수 있다.

대 표 도 - 도7



(52) CPC특허분류
H04L 67/12 (2013.01)
H04W 4/70 (2018.02)

명 세 서

청구범위

청구항 1

M2M(Machine-to-Machine) 시스템에서 M2M 장치의 동작 방법에 있어서,

로그 관리 규칙(log management rule)의 생성을 요청하는 제1 메시지를 수신하는 단계;

상기 로그 관리 규칙 및 상기 로그 관리 규칙에 따라 생성될 로그 정보를 저장하기 위한 저장 공간을 생성하는 단계; 및

상기 로그 관리 규칙 및 상기 저장 공간의 참조 관계를 설정하는 단계를 포함하는 방법.

청구항 2

청구항 1에 있어서,

상기 로그 관리 규칙은, 상기 로그 관리를 위한 자원의 형태로 생성되며,

상기 로그 관리를 위한 자원은, 로깅(logging) 동작의 시기를 지시하는 정보, 로깅의 대상이 되는 정보 또는 동작을 특정하는 정보, 로그 정보의 포맷을 정의하는 정보, 로그 정보의 생성 조건, 로깅될 대상 자원에 대한 정보, 로그 정보를 저장할 저장 공간을 지시하는 정보 중 적어도 하나를 포함하는 방법.

청구항 3

청구항 1에 있어서,

상기 참조 관계는, 상기 로그 관리 규칙에 상기 저장 공간을 지시하는 어트리뷰트를 포함시킴으로써 설정되는 방법.

청구항 4

청구항 1에 있어서,

상기 로그 관리 규칙에 따르는 자원의 생성을 요청하는 제2 메시지를 수신하는 단계;

상기 제2 메시지에 포함된 정보에 기반하여 상기 자원을 생성하는 단계;

상기 자원 및 상기 로그 관리 규칙의 참조 관계를 설정하는 단계를 더 포함하는 방법.

청구항 5

청구항 4에 있어서,

상기 제2 메시지는, 상기 자원이 로깅의 대상이 됨을 지시하는 정보 및 상기 자원의 로깅에 적용될 로그 관리 규칙을 지시하는 정보 중 적어도 하나를 포함하는 방법.

청구항 6

청구항 4에 있어서,

상기 참조 관계는, 상기 자원에 상기 로그 관리 규칙을 지시하는 어트리뷰트를 포함시킴으로써 설정되는 방법.

청구항 7

청구항 4에 있어서,

상기 자원에 대한 동작(operation)을 요청하는 제3 메시지를 수신하는 단계;

상기 제3 메시지에 의해 요청된 동작을 수행하는 단계;

상기 로그 관리 규칙에 기반하여 상기 동작에 관한 로그 정보를 생성하는 단계; 및

상기 로그 정보를 저장하는 단계를 더 포함하는 방법.

청구항 8

청구항 7에 있어서,

상기 로그 정보를 생성하는 단계는,

상기 로그 관리 규칙에 기반하여, 상기 요청된 동작이 로깅의 대상인지 판단하는 단계를 포함하는 방법.

청구항 9

청구항 7에 있어서,

상기 로그 정보를 생성하는 단계는,

상기 로그 관리 규칙에 기반하여, 상기 요청이 발생한 시각이 로깅 동작의 시기 내에 포함되는지 판단하는 단계를 포함하는 방법.

청구항 10

M2M(Machine-to-Machine) 시스템에서 M2M 장치에 있어서,

신호를 송수신하는 송수신부; 및

상기 송수신부를 제어하는 프로세서를 포함하며,

상기 프로세서는,

로그 관리 규칙(log management rule)의 생성을 요청하는 제1 메시지를 수신하고,

상기 로그 관리 규칙 및 상기 로그 관리 규칙에 따라 생성될 로그 정보를 저장하기 위한 저장 공간을 생성하고,

상기 로그 관리 규칙 및 상기 저장 공간의 참조 관계를 설정하도록 제어하는 M2M 장치.

청구항 11

청구항 10에 있어서,

상기 로그 관리 규칙은, 상기 로그 관리를 위한 자원의 형태로 생성되며,

상기 로그 관리를 위한 자원은, 로깅(logging) 동작의 시기를 지시하는 정보, 로깅의 대상이 되는 정보 또는 동작을 특정하는 정보, 로그 정보의 포맷을 정의하는 정보, 로그 정보의 생성 조건, 로깅될 대상 자원에 대한 정보, 로그 정보를 저장할 저장 공간을 지시하는 정보 중 적어도 하나를 포함하는 M2M 장치.

청구항 12

청구항 10에 있어서,

상기 프로세서는,

상기 로그 관리 규칙에 따르는 자원의 생성을 요청하는 제2 메시지를 수신하고,

상기 제2 메시지에 포함된 정보에 기반하여 상기 자원을 생성하고,

상기 자원 및 상기 로그 관리 규칙의 참조 관계를 설정하도록 제어하는 M2M 장치.

청구항 13

청구항 12에 있어서,

상기 프로세서는,

상기 자원에 대한 동작(operation)을 요청하는 제3 메시지를 수신하고,

상기 제3 메시지에 의해 요청된 동작을 수행하고,

상기 로그 관리 규칙에 기반하여 상기 동작에 관한 로그 정보를 생성하고,

상기 로그 정보를 저장하도록 제어하는 M2M 장치.

청구항 14

M2M(Machine-to-Machine) 시스템에서 M2M 장치에 있어서,

신호를 송수신하는 송수신부; 및

상기 송수신부를 제어하는 프로세서를 포함하며,

상기 프로세서는,

로그 관리 규칙(log management rule)에 기반하여 로깅(logging)의 대상이 되는 자원의 생성을 요청하는 제1 메시지를 송신하고,

상기 자원의 생성을 완료하였음을 알리는 제2 메시지를 수신하도록 제어하며,

상기 제1 메시지는, 상기 로깅의 대상이 됨을 지시하는 제1 정보 및 상기 로그 관리 규칙을 지시하는 제2 정보를 포함하는 M2M 장치.

청구항 15

청구항 14에 있어서,

상기 로그 관리 규칙은, 로깅(logging) 동작의 시기를 지시하는 정보, 로깅의 대상이 되는 정보 또는 동작을 특정하는 정보, 로그 정보의 포맷을 정의하는 정보, 로그 정보의 생성 조건, 로깅될 대상 자원에 대한 정보, 로그 정보를 저장할 저장 공간을 지시하는 정보 중 적어도 하나를 정의하는 M2M 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 M2M(Machine-to-Machine) 시스템에서 로그(log) 정보를 관리하기 위한 방법 및 장치에 대한 것이다. 보다 구체적으로, 본 발명은 M2M 시스템에서 자원(resource)에 대한 활동에 관련된 정보를 로깅(logging)하기

위한 방법 및 장치에 대한 것이다.

배 경 기 술

[0002] 최근 M2M(Machine-to-Machine) 시스템에 대한 도입이 활발해지고 있다. M2M 통신은 사람의 개입 없이 기계(machine)와 기계 사이에 수행되는 통신을 의미할 수 있다. M2M은 MTC(Machine Type Communication), IoT(Internet of Things) 또는 D2D(Device-to-Device)를 지칭할 수 있다. 다만, 하기에서는 설명의 편의를 위해 M2M로 통일하게 지칭하지만, 이에 한정되지 않는다. M2M 통신에 사용되는 단말은 M2M 단말(M2M device)일 수 있다. M2M 단말은 일반적으로 적은 데이터를 전송하면서 낮은 이동성을 갖는 디바이스일 수 있다. 이때, M2M 단말은 기계 간 통신 정보를 중앙에서 저장하고 관리하는 M2M 서버와 연결되어 사용될 수 있다. 또한, M2M 단말은 사물 추적, 자동차 연동, 전력 계량 등과 같이 다양한 시스템에서 적용될 수 있다.

[0003] 한편, M2M 단말과 관련하여, oneM2M 표준화 기구는 M2M 통신, 사물통신, IoT 기술을 위한 요구사항, 아키텍처, API(Application Program Interface) 사양, 보안 솔루션, 상호 운용성에 대한 기술을 제공하고 있다. oneM2M 표준화 기구의 사양은 스마트 시티, 스마트 그리드, 커넥티드 카, 홈 오토메이션, 치안, 건강과 같은 다양한 어플리케이션과 서비스를 지원하는 프레임워크를 제공하고 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명은 M2M(Machine-to-Machine) 시스템에서 로그(log) 정보를 관리하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0005] 본 발명은 M2M 시스템에서 자원(resource)에 대한 활동에 관련된 정보를 로깅(logging)하기 위한 방법 및 장치를 제공하는데 목적이 있다.

[0006] 본 발명은 M2M 시스템에서 로그 정보의 관리에 관련된 규칙을 설정하기 위한 방법 및 장치를 제공하는데 목적이 있다.

과제의 해결 수단

[0007] 본 발명의 일 실시 예에 따르면, M2M(Machine-to-Machine) 시스템에서 M2M 장치의 동작 방법은, 로그 관리 규칙(log management rule)의 생성을 요청하는 제1 메시지를 수신하는 단계, 상기 로그 관리 규칙 및 상기 로그 관리 규칙에 따라 생성될 로그 정보를 저장하기 위한 저장 공간을 생성하는 단계, 및 상기 로그 관리 규칙 및 상기 저장 공간의 참조 관계를 설정하는 단계를 포함할 수 있다.

[0008] 본 발명의 일 실시 예에 따르면, M2M(Machine-to-Machine) 시스템에서 M2M 장치는, 신호를 송수신하는 송수신부, 및 상기 송수신부를 제어하는 프로세서를 포함하며, 상기 프로세서는, 로그 관리 규칙(log management rule)의 생성을 요청하는 제1 메시지를 수신하고, 상기 로그 관리 규칙 및 상기 로그 관리 규칙에 따라 생성될 로그 정보를 저장하기 위한 저장 공간을 생성하고, 상기 로그 관리 규칙 및 상기 저장 공간의 참조 관계를 설정하도록 제어할 수 있다.

[0009] 본 발명의 일 실시 예에 따르면, M2M(Machine-to-Machine) 시스템에서 M2M 장치는, 신호를 송수신하는 송수신부, 및 상기 송수신부를 제어하는 프로세서를 포함하며, 상기 프로세서는, 로그 관리 규칙(log management rule)에 기반하여 로깅(logging)의 대상이 되는 자원의 생성을 요청하는 제1 메시지를 송신하고, 상기 자원의 생성을 완료하였음을 알리는 제2 메시지를 수신하도록 제어하며, 상기 제1 메시지는, 상기 로깅의 대상이 됨을 지시하는 제1 정보 및 상기 로그 관리 규칙을 지시하는 제2 정보를 포함할 수 있다.

발명의 효과

[0010] 본 개시에 따르면, M2M(Machine-to-Machine) 시스템에서 로그(log) 정보가 효과적으로 관리될 수 있다.

[0011] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0012] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조를 도시한다.

도 2는 본 개시에 따른 M2M 시스템에서 기준점(reference point)을 도시한다.

도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 도시한다.

도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 평션을 도시한다.

도 5는 본 개시에 따른 M2M 시스템에서 송신자 및 수신자가 메시지를 교환하는 방법을 도시한다.

도 6은 본 개시에 따른 M2M 시스템에서 로그(log) 관리의 개념을 도시한다.

도 7은 본 개시에 따른 M2M 시스템에서 로그 정보를 관리하기 위한 신호 교환의 예를 도시한다.

도 8은 본 개시에 따른 M2M 시스템에서 로그 관리 규칙을 생성하기 위한 절차의 예를 도시한다.

도 9는 본 개시에 따른 M2M 시스템에서 로그 관리 대상이 되는 자원을 생성하기 위한 절차의 예를 도시한다.

도 10은 본 개시에 따른 M2M 시스템에서 로그 정보를 생성하기 위한 절차의 예를 도시한다.

도 11은 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하에서는 첨부한 도면을 참고로 하여 본 개시의 실시 예에 대하여 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나, 본 개시는 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다.

[0014] 본 개시에 있어서, 제1, 제2 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용되며, 특별히 언급되지 않는 한 구성요소들간의 순서 또는 중요도 등을 한정하지 않는다. 따라서, 본 개시의 범위 내에서 일 실시 예에서의 제1 구성요소는 다른 실시 예에서 제2 구성요소라고 칭할 수도 있고, 마찬가지로 일 실시 예에서의 제2 구성요소를 다른 실시 예에서 제1 구성요소라고 칭할 수도 있다.

[0015] 본 개시에 있어서, 어떤 구성요소가 다른 구성요소와 "연결", "결합" 또는 "접속"되어 있다고 할 때, 이는 직접적인 연결관계뿐만 아니라, 그 중간에 또 다른 구성요소가 존재하는 간접적인 연결관계도 포함할 수 있다. 또한 어떤 구성요소가 다른 구성요소를 "포함한다" 또는 "가진다"고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 배제하는 것이 아니라 또 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0016] 본 개시에 있어서, 서로 구별되는 구성요소들은 각각의 특징을 명확하게 설명하기 위함이며, 구성요소들이 반드시 분리되는 것을 의미하지는 않는다. 즉, 복수의 구성요소가 통합되어 하나의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있고, 하나의 구성요소가 분산되어 복수의 하드웨어 또는 소프트웨어 단위로 이루어질 수도 있다. 따라서, 별도로 언급하지 않더라도 이와 같이 통합된 또는 분산된 실시 예도 본 개시의 범위에 포함된다.

[0017] 본 개시에 있어서, 다양한 실시 예에서 설명하는 구성요소들이 반드시 필수적인 구성요소들은 의미하는 것은 아니며, 일부는 선택적인 구성요소일 수 있다. 따라서, 일 실시 예에서 설명하는 구성요소들의 부분집합으로 구성되는 실시 예도 본 개시의 범위에 포함된다. 또한, 다양한 실시 예에서 설명하는 구성요소들에 추가적으로 다른 구성요소를 포함하는 실시 예도 본 개시의 범위에 포함된다.

[0018] 본 개시의 실시 예를 설명함에 있어서 공지 구성 또는 기능에 대한 구체적인 설명이 본 개시의 요지를 흐릴 수 있다고 판단되는 경우에는 그에 대한 상세한 설명은 생략한다. 그리고, 도면에서 본 개시에 대한 설명과 관계없는 부분은 생략하였으며, 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0019] 또한 본 명세서는 M2M(Machine-to-Machine) 통신에 기초한 네트워크에 대해 설명하며, M2M 통신 네트워크에서 이루어지는 작업은 해당 통신 네트워크를 관할하는 시스템에서 네트워크를 제어하고 데이터를 송신하는 과정에서 이루어질 수 있다.

[0020] 또한, 본 명세서에서 M2M 단말은 M2M 통신을 수행하는 단말일 수 있으나, 호환성(Backward Compatibility)을 고려하여 무선 통신 시스템에서 동작하는 단말일 수 있다. 즉, M2M 단말은 M2M 통신 네트워크에 기초하여 동작될 수 있는 단말을 의미할 수 있으나, M2M 통신 네트워크로 한정되는 것은 아니다. M2M 단말은 다른 무선 통신 네트워크에 기초하여 동작하는 것도 가능할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0021] 또한, M2M 단말은 고정되거나 이동성을 가질 수 있다. 또한, M2M 서버는 M2M 통신을 위한 서버를 지칭하며 고정

국(fixed station) 또는 이동국(mobile station)일 수 있다.

[0022] 또한, 본 명세서에서 엔티티는 M2M 디바이스, M2M 게이트웨이, M2M 서버와 같은 하드웨어를 지칭할 수 있다. 또한, 일 예로, 엔티티는 M2M 시스템의 계층 구조에서 소프트웨어적인 구성을 지칭하는데 사용할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0023] 또한, 일 예로, 본 발명은 M2M 시스템을 중심으로 설명되지만 본 발명은 M2M 시스템에만 제한적으로 적용되는 것은 아니다.

[0024] 또한, M2M 서버는 M2M 단말 또는 다른 M2M 서버와 통신을 수행하는 서버일 수 있다. 또한, M2M 게이트웨이는 M2M 단말과 M2M 서버를 연결하는 연결점 역할을 수행할 수 있다. 일 예로, M2M 단말과 M2M 서버의 네트워크가 상이한 경우, M2M 게이트웨이를 통해 서로 연결될 수 있다. 이때, 일 예로, M2M 게이트웨이, M2M 서버 모두 M2M 단말일 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0026] 본 발명은 M2M(Machine-to-Machine) 시스템에서 개인 데이터(personal data)를 취급하기 위한 방법 및 장치에 대한 것이다. 보다 구체적으로, 본 발명은 M2M 시스템에서 개인 데이터의 취급에 대한 동의(consent)를 확인하기 위한 기술에 대해 설명한다.

[0028] oneM2M은 에너지, 교통, 국방, 공공서비스 등 산업별로 종속적이고 폐쇄적으로 운영되는, 파편 화된 서비스 플랫폼 개발 구조를 벗어나 응용서비스 인프라(플랫폼) 환경을 통합하고 공유하기 위한 사물인터넷 공동서비스 플랫폼 개발을 위해 발족된 사실상 표준화 단체이다. oneM2M은 사물통신, IoT(Internet of Things) 기술을 위한 요구사항, 아키텍처, API(Application Program Interface) 사양, 보안 솔루션, 상호 운용성을 제공하고자 한다. 예를 들어, oneM2M의 사양은 스마트 시티, 스마트 그리드, 커넥티드 카, 홈 오토메이션, 치안, 건강과 같은 다양한 어플리케이션과 서비스를 지원하는 프레임워크를 제공한다. 이를 위해, oneM2M은 모든 어플리케이션들 사이에 데이터의 교환 및 공유를 위한 단일 수평 플랫폼을 정의하는 표준들의 집합을 개발해왔다. oneM2M에서 고려하는 어플리케이션들은 상이한 산업 부문들에 걸친 어플리케이션들도 포함할 수 있다. oneM2M은, 운영체제처럼, 상이한 기술들과 연동하기 위한 프레임워크를 제공함으로써, 단일화를 촉진하는 분산된 소프트웨어 레이어를 생성하고 있다. 분산된 소프트웨어 레이어는 M2M 어플리케이션들과 데이터 전송을 제공하는 통신 HW(Hardware)/SW(Software) 사이에 위치하는 공통 서비스 계층에서 구현된다. 예를 들어, 공통 서비스 계층은 도 1과 같은 계층 구조의 일부를 차지할 수 있다.

[0030] 도 1은 본 개시에 따른 M2M(Machine-to-Machine) 시스템의 계층 구조(layered structure)를 도시한다.

[0031] 도 1를 참조하면, M2M 시스템의 계층 구조는 어플리케이션 계층(110), 공통 서비스 계층(120), 네트워크 서비스 계층(120)으로 구성될 수 있다. 이때, 어플리케이션 계층(110)은 구체적인 어플리케이션에 기초하여 동작하는 계층일 수 있다. 일 예로, 어플리케이션은 차량 추적 어플리케이션(fleet tracking application), 원거리 혈당 모니터링 어플리케이션(remote blood sugar monitoring application), 전력 계량 어플리케이션(power metering application) 또는 제어 어플리케이션(controlling application) 등일 수 있다. 즉, 어플리케이션 계층은 구체적인 어플리케이션에 대한 계층일 수 있다. 이때, 어플리케이션 계층에 기초하여 동작하는 엔티티는 어플리케이션 엔티티(Application Entity, AE)일 수 있다.

[0032] 공통 서비스 계층(120)은 공통 서비스 평션(Common Service Function, CSF)에 대한 계층일 수 있다. 일 예로, 공통 서비스 계층(120)은 데이터 관리(data management), 단말 관리(device management), M2M 서비스 구독 관리(M2M service subscription management), 위치 서비스(location Services) 등과 같이 공통 서비스 제공에 대한 계층일 수 있다. 일 예로, 공통 서비스 계층(120)에 기초하여 동작하는 엔티티는 공통 서비스 엔티티(Common Service Entity, CSE)일 수 있다.

[0033] 공통 서비스 계층(120)은 기능에 의해 CSF로 그룹화되는 서비스들의 집합을 제공할 수 있다. 다수의 인스턴스화된 CSF들은 CSE들을 형성한다. CSE들은 어플리케이션들(예: oneM2M 명명법에서 어플리케이션 엔티티들 또는 AE들), 다른 CSE들 및 기저 네트워크들(예: oneM2M 명명법에서 네트워크 서비스 엔티티 또는 NSE)과 인터페이스할 수 있다.

[0034] 네트워크 서비스 계층(120)은 장치 관리(device management), 위치 서비스(location service) 및 장치 트리거링(device triggering)과 같은 서비스들을 공통 서비스 계층(120)에 제공할 수 있다. 이때, 네트워크 계층(120)에 기초하여 동작하는 엔티티는 네트워크 서비스 엔티티(Network Service Entity, NSE)일 수 있다.

[0036] 도 2는 본 개시에 따른 M2M 시스템에서 기준점(reference point)을 도시한다.

[0037] 도 2를 참조하면, M2M 시스템 구조는 필드 도메인(Field Domain) 및 인프라스트럭쳐 도메인(Infrastructure Domain)으로 구별될 수 있다. 이때, 각각의 도메인에서 각각의 엔티티들은 기준점(예: Mca 또는 Mcc)을 통해 통신을 수행할 수 있다. 일 예로, 기준점(reference point)은 각각의 엔티티들 간의 통신 흐름을 나타낼 수 있다. 이때, 도 2를 참조하면, AE(210 또는 240)와 CSE(220 또는 250) 사이의 기준점인 Mca 기준점, 서로 다른 CSE 사이의 기준점인 Mcc 기준점 및 CSE(220 또는 250)와 NSE(230 또는 260) 사이의 기준점인 Mcn 기준점이 설정될 수 있다.

[0039] 도 3은 본 개시에 따른 M2M 시스템에서 각각의 노드를 도시한다.

[0040] 도 3을 참조하면, 특정 M2M 서비스 제공자의 인프라스트럭쳐 도메인은 특정 인프라스트럭쳐 노드(310, Infrastructure Node, IN)를 제공할 수 있다. 이때, IN의 CSE는 다른 인프라스트럭쳐 노드의 AE와 Mca 기준점에 기초하여 통신을 수행할 수 있다. 이때, 하나의 M2M 서비스 제공자마다 하나의 IN이 설정될 수 있다. 즉, IN은 인프라스트럭쳐 구조에 기초하여 다른 인프라스트럭쳐의 M2M 단말과 통신을 수행하는 노드일 수 있다. 또한, 일 예로, 노드의 개념은 논리적 엔티티일 수 있으며, 소프트웨어적인 구성일 수 있다.

[0041] 다음으로, 어플리케이션 지정 노드(320, Application Dedicated Node, ADN)는 적어도 하나의 AE를 포함하고, CSE를 포함하지 않는 노드일 수 있다. 이때, ADN은 필드 도메인에서 설정될 수 있다. 즉, ADN은 AE에 대한 전용 노드일 수 있다. 일 예로, ADN은 하드웨어적으로 M2M 단말에 설정되는 노드일 수 있다. 또한, 어플리케이션 서비스 노드(330, Application Service Node, ASN)는 하나의 CSE와 적어도 하나의 AE를 포함하는 노드일 수 있다. ASN은 필드 도메인에서 설정될 수 있다. 즉, AE 및 CSE를 포함하는 노드일 수 있다. 이때, ASN은 IN과 연결되는 노드일 수 있다. 일 예로, ASN은 하드웨어적으로 M2M 단말에 설정되는 노드일 수 있다.

[0042] 또한, 미들 노드(340, Middle Node, MN)은 CSE를 포함하고, 0개 또는 그 이상의 AE를 포함하는 노드일 수 있다. 이때, MN은 필드 도메인에서 설정될 수 있다. MN은 다른 MN 또는 IN과 기준점에 기초하여 연결될 수 있다. 또한 일 예로, MN은 하드웨어적으로 M2M 게이트웨이에 설정될 수 있다.

[0043] 또한, 일 예로, 논-M2M 단말 노드(350, Non-M2M device node, NoDN)은 M2M 엔티티들을 포함하지 않은 노드로서 M2M 시스템과 관리나 협업 등을 수행하는 노드일 수 있다.

[0045] 도 4는 본 개시에 따른 M2M 시스템에서 공통 서비스 평션을 도시한다.

[0046] 도 4를 참조하면, 공통 서비스 평션들이 제공될 수 있다. 일 예로, 공통 서비스 엔티티는 어플리케이션 및 서비스 계층 관리(402, Application and Service Layer Management), 통신 관리 및 전달 처리(404, Communication Management and Delivery Handling), 데이터 관리 및 저장(406, Data Management and Repository), 장치 관리(408, Device Management), 발견(410, Discovery), 그룹 관리(412, Group Management), 위치(414, Location), 네트워크 서비스 노출/서비스 실행 및 트리거링(416, Network Service Exposure/ Service Execution and Triggering), 등록(418, Registration), 보안(420, Security), 서비스 과금 및 계산(422, Service Charging and Accounting), 서비스 세션 관리 기능(Service Session Management) 및 구독/통지(424, Subscription/Notification) 중 적어도 어느 하나 이상의 CSF을 제공할 수 있다. 이때, 공통 서비스 평션에 기초하여 M2M 단말들이 동작할 수 있다. 또한, 공통 서비스 평션은 다른 실시 예도 가능할 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0047] 어플리케이션 및 서비스 계층 관리(402) CSF는 AE들 및 CSE들의 관리를 제공한다. 어플리케이션 및 서비스 계층 관리(402) CSF는 CSE의 기능들을 구성하고, 문제 해결하고, 및 업그레이드하는 것뿐만 아니라, AE들을 업그레이드하는 능력들을 포함한다.

[0048] 통신 관리 및 전달 처리(404) CSF는 다른 CSE들, AE들, 및 NSE들과의 통신들을 제공한다. 통신 관리 및 전달 처

리(404) CSF는 어떤 시간 및 어느 통신 연결로 통신들을 전달할지를 결정하고, 필요하고 허용되는 경우 그것들이 나중에 전달될 수 있도록 통신들 요청을 버퍼링하기로 결정한다.

[0049] 데이터 관리 및 저장(406) CSF는 데이터 저장 및 중재 기능들(예: 집결을 위한 데이터 수집, 데이터 리포맷팅, 및 분석 및 시멘틱 처리를 위한 데이터 저장)을 제공한다.

[0050] 장치 관리(408) CSF는 M2M 게이트웨이들 및 M2M 디바이스들 상에서 디바이스 능력들의 관리를 제공한다.

[0051] 발견(410) CSF는 필터 기준들에 기초하여 어플리케이션들 및 서비스들에 대한 정보를 검색하는 기능을 제공한다.

[0052] 그룹 관리(412) CSF는 그룹 관련 요청들의 처리를 제공한다. 그룹 관리(412) CSF는 M2M 시스템이 여러 디바이스들, 어플리케이션들 등에 대한 대량 작업들(bulk operations)을 지원하는 것을 가능하게 한다.

[0053] 위치(414) CSF는 AE들이 지리적 장소 정보를 획득하는 것을 가능하게 하는 기능을 제공한다.

[0054] 네트워크 서비스 노출/서비스 실행 및 트리거링(416) CSF는 네트워크 서비스 기능들에 액세스하기 위한 기저 네트워크들과의 통신들을 관리한다.

[0055] 등록(418) CSF는 AE들(또는 다른 원격 CSE들)이 CSE에 등록하기 위한 기능을 제공한다. 등록(418) CSF는 AE들(또는 원격 CSE)이 CSE의 서비스들을 사용하는 것을 허용한다.

[0056] 보안(420) CSF는 식별, 인증, 및 허가를 포함하는 액세스 제어와 같은 서비스 레이어에 대한 보안 기능들을 제공한다.

[0057] 서비스 과금 및 계산(422) CSF는 서비스 레이어에 대한 과금 기능들을 제공한다.

[0058] 구독/통지(424) CSF는 이벤트에 가입하는 것을 허용하고, 해당 이벤트가 발생할 때 통지되는 기능을 제공한다.

[0060] 도 5는 본 개시에 따른 M2M 시스템에서 송신자 및 수신자가 메시지를 교환하는 방법을 도시한다.

[0061] 도 5를 참조하면, 송신자(originator, 510)는 요청 메시지를 수신자(receiver, 520)로 전송할 수 있다. 이때, 송신자(510)와 수신자(520)는 상술한 M2M 단말일 수 있다. 다만, M2M 단말에 한정되지 않고, 송신자(510)와 수신자(520)는 다른 단말일 수 있으며, 상술한 실시 예로 한정되지 않는다. 또한, 일 예로, 송신자(510) 및 수신자(520)는 상술한 노드, 엔티티, 서버 또는 게이트웨이일 수 있다. 즉, 송신자(510) 및 수신자(520)는 하드웨어적인 구성 또는 소프트웨어적인 구성일 수 있으며, 상술한 실시 예로 한정되지 않는다.

[0062] 이때, 일 예로, 송신자(510)가 전송하는 요청 메시지에는 적어도 하나의 파라미터가 포함될 수 있다. 이때, 일 예로, 파라미터는 필수 파라미터 또는 선택 파라미터가 있을 수 있다. 일 예로, 송신단과 관련된 파라미터, 수신단과 관련된 파라미터, 식별 파라미터 및 동작 파라미터 등은 필수적인 파라미터일 수 있다. 또한, 그 밖에 다른 정보에 대해서는 선택 파라미터일 수 있다. 이때, 송신단 관련 파라미터는 송신자(510)에 대한 파라미터일 수 있다. 또한, 수신단 관련 파라미터는 수신자(520)에 대한 파라미터일 수 있다. 또한, 식별 파라미터는 상호간의 식별을 위해 요구되는 파라미터일 수 있다.

[0063] 또한, 동작 파라미터는 동작을 구분하기 위한 파라미터일 수 있다. 일 예로, 동작 파라미터는 생성(Create), 조회(Retrieve), 갱신(Update), 삭제(Delete) 및 통지(Notify) 중 적어도 어느 하나로 설정될 수 있다. 즉, 동작을 구별하기 위한 파라미터일 수 있다.

[0064] 이때, 수신자(520)는 송신자(510)로부터 요청 메시지를 수신하면 해당 요청 메시지를 처리할 수 있다. 일 예로, 수신자(520)는 요청 메시지에 포함된 동작을 수행할 수 있으며, 이를 위해 파라미터가 유효한지 여부 및 권한이 있는지 여부 등을 판단할 수 있다. 이때, 수신자(520)는 파라미터가 유효하고, 권한이 있다면 요청 대상이 되는 자원 존재하는지 여부를 확인하고, 이에 기초하여 프로세싱을 수행할 수 있다.

[0065] 일 예로, 이벤트가 발생하는 경우, 송신자(510)는 수신자(520)에게 통지에 대한 파라미터를 포함하는 요청 메시지를 전송할 수 있다. 수신자(520)는 요청 메시지에 포함된 통지에 대한 파라미터를 확인하고, 이에 기초하여 동작을 수행할 수 있으며, 응답 메시지를 송신자(510)로 다시 전송할 수 있다.

[0066] 도 5와 같은 요청 메시지 및 응답 메시지를 이용한 메시지 교환 절차는 Mca 기준점에 기반하여 AE 및 CSE 간 또는 Mcc 기준점에 기반하여 CSE들 간 수행될 수 있다. 즉, 송신자(510)는 AE 또는 CSE이고, 수신자(520)는 AE 또

는 CSE일 수 있다. 요청 메시지 내의 동작에 따라, 도 5와 같은 메시지 교환 절차는 AE 또는 CSE에 의해 시작될(initiated) 수 있다.

[0068] 기준점 Mca 및 Mcc를 통한 요청자로부터 수신자로의 요청은 적어도 하나의 필수적인(mandatory) 파라미터를 포함하고, 적어도 하나의 선택적인(optional) 파라미터를 포함할 수 있다. 즉, 정의된 각 파라미터는 요청되는 동작(operation)에 따라 필수적이거나 선택적일 수 있다. 예를 들어, 응답 메시지는 이하 [표 1]에 나열된 파라미터들 중 적어도 하나를 포함할 수 있다.

표 1

[0069]

Response message parameter/success or not
Response Status Code - successful, unsuccessful, ack
Request Identifier - uniquely identifies a Request message
Content - to be transferred
To - the identifier of the Originator or the Transit CSE that sent the corresponding non-blocking request
From - the identifier of the Receiver
Originating Timestamp - when the message was built
Result Expiration Timestamp - when the message expires
Event Category - what event category shall be used for the response message
Content Status
Content Offset
Token Request Information
Assigned Token Identifiers
Authorization Signature Request Information
Release Version Indicator - the oneM2M release version that this response message conforms to

[0070] 요청 메시지 또는 응답 메시지에서 사용될 수 있는 필터 기준 조건(filter criteria condition)은 이하 [표 2] 및 [표 3]과 같이 정의될 수 있다.

표 2

[0071]

Condition tag	Multiplicity	Description
Matching Conditions		
createdBefore	0..1	The creationTime attribute of the matched resource is chronologically before the specified value.
createdAfter	0..1	The creationTime attribute of the matched resource is chronologically after the specified value.
modifiedSince	0..1	The lastModifiedTime attribute of the matched resource is chronologically after the specified value.
unmodifiedSince	0..1	The lastModifiedTime attribute of the matched resource is chronologically before the specified value.
stateTagSmaller	0..1	The stateTag attribute of the matched resource is smaller than the specified value.
stateTagBigger	0..1	The stateTag attribute of the matched resource is bigger than the specified value.
expireBefore	0..1	The expirationTime attribute of the matched resource is chronologically before the specified value.
expireAfter	0..1	The expirationTime attribute of the matched resource is chronologically after the specified value.
labels	0..1	The labels attribute of the matched resource matches the specified value.
labelsQuery	0..1	The value is an expression for the filtering of labels attribute of resource when it is of key-value pair format. The expression is about the relationship between label-key and label-value which may include equal to or not equal to, within or not within a specified set etc. For example, label-key equals to label value, or label-key within {label-value1, label-value2}. Details are defined in [3]

childLabels	0..1	A child of the matched resource has labels attributes matching the specified value. The evaluation is the same as for the labels attribute above. Details are defined in [3].
parentLabels	0..1	The parent of the matched resource has labels attributes matching the specified value. The evaluation is the same as for the labels attribute above. Details are defined in [3].
resourceType	0..n	The resourceType attribute of the matched resource is the same as the specified value. It also allows differentiating between normal and announced resources.
childResourceType	0..n	A child of the matched resource has the resourceType attribute the same as the specified value.
parentResourceType	0..1	The parent of the matched resource has the resourceType attribute the same as the specified value.
sizeAbove	0..1	The contentSize attribute of the <contentInstance> matched resource is equal to or greater than the specified value.
sizeBelow	0..1	The contentSize attribute of the <contentInstance> matched resource is smaller than the specified value.
contentType	0..n	The contentInfo attribute of the <contentInstance> matched resource matches the specified value.
attribute	0..n	This is an attribute of resource types (clause 9.6). Therefore, a real tag name is variable and depends on its usage and the value of the attribute can have wild card *. E.g. creator of container resource type can be used as a filter criteria tag as "creator=Sam", "creator=Sam*", "creator=*Sam".
childAttribute	0..n	A child of the matched resource meets the condition provided. The evaluation of this condition is similar to the attribute matching condition above.
parentAttribute	0..n	The parent of the matched resource meets the condition provided. The evaluation of this condition is similar to the attribute matching condition above.
semanticsFilter	0..n	Both semantic resource discovery and semantic query use semanticsFilter to specify a query statement that shall be specified in the SPARQL query language [5]. When a CSE receives a RETRIEVE request including a semanticsFilter, and the Semantic Query Indicator parameter is also present in the request, the request shall be processed as a semantic query; otherwise, the request shall be processed as a semantic resource discovery. In the case of semantic resource discovery targeting a specific resource, if the semantic description contained in the <semanticDescriptor> of a child resource matches the semanticFilter, the URI of this child resource will be included in the semantic resource discovery result. In the case of semantic query, given a received semantic query request and its query scope, the SPARQL query statement shall be executed over aggregated semantic information collected from the semantic resource(s) in the query scope and the produced output will be the result of this semantic query. Examples for matching semantic filters in SPARQL to semantic descriptions can be found in [i.28].
filterOperation	0..1	Indicates the logical operation (AND/OR) to be used for different condition tags. The default value is logical AND.
contentFilterSyntax	0..1	Indicates the Identifier for syntax to be applied for content-based discovery.
contentFilterQuery	0..1	The query string shall be specified when contentFilterSyntax parameter is present.

표 3

[0072]

Condition tag	Multip-l icity	Description
Filter Handling Conditions		

filterUsage	0..1	Indicates how the filter criteria is used. If provided, possible values are 'discovery' and 'IPEOnDemandDiscovery'. If this parameter is not provided, the Retrieve operation is a generic retrieve operation and the content of the child resources fitting the filter criteria is returned. If filterUsage is 'discovery', the Retrieve operation is for resource discovery (clause 10.2.6), i.e. only the addresses of the child resources are returned. If filterUsage is 'IPEOnDemandDiscovery', the other filter conditions are sent to the IPE as well as the discovery Originator ID. When the IPE successfully generates new resources matching with the conditions, then the resource address(es) shall be returned. This value shall only be valid for the Retrieve request targeting an <AE> resource that represents the IPE.
limit	0..1	The maximum number of resources to be included in the filtering result. This may be modified by the Hosting CSE. When it is modified, then the new value shall be smaller than the suggested value by the Originator.
level	0..1	The maximum level of resource tree that the Hosting CSE shall perform the operation starting from the target resource (i.e. To parameter). This shall only be applied for Retrieve operation. The level of the target resource itself is zero and the level of the direct children of the target is one.
offset	0..1	The number of direct child and descendant resources that a Hosting CSE shall skip over and not include within a Retrieve response when processing a Retrieve request to a targeted resource.
applyRelativePath	0..1	This attribute contains a resource tree relative path (e.g. ../tempContainer/LATEST). This condition applies after all the matching conditions have been used (i.e. a matching result has been obtained). The attribute determines the set of resource(s) in the final filtering result. The filtering result is computed by appending the relative path to the path(s) in the matching result. All resources whose Resource-IDs match that combined path(s) shall be returned in the filtering result. If the relative path does not represent a valid resource, the outcome is the same as if no match was found, i.e. there is no corresponding entry in the filtering result.

[0073] 기준점 Mca 및 Mcc를 통한 자원으로의 접근(accessing)에 대한 요청에 대응한 응답은 적어도 하나의 필수적인(mandatory) 파라미터를 포함하고, 적어도 하나의 선택적인(optional) 파라미터를 포함할 수 있다. 즉, 정의된 각 파라미터는 요청되는 동작(operation) 또는 필수 응답 코드(mandatory response code)에 따라 필수적이거나 선택적일 수 있다. 예를 들어, 요청 메시지는 이하 [표 4]에 나열된 파라미터들 중 적어도 하나를 포함할 수 있다.

표 4

[0074]

Request message parameter	
Mandatory	Operation - operation to be executed / CREAT, Retrieve, Update, Delete, Notify
	To - the address of the target resource on the target CSE
	From - the identifier of the message Originator
	Request Identifier - uniquely identifies a Request message
Operation dependent	Content - to be transferred
	Resource Type - of resource to be created

Optional	Originating Timestamp - when the message was built
	Request Expiration Timestamp - when the request message expires
	Result Expiration Timestamp - when the result message expires
	Operational Execution Time - the time when the specified operation is to be executed by the target CSE
	Response Type - type of response that shall be sent to the Originator
	Result Persistence - the duration for which the reference containing the responses is to persist
	Result Content - the expected components of the result
	Event Category - indicates how and when the system should deliver the message
	Delivery Aggregation - aggregation of requests to the same target CSE is to be used
	Group Request Identifier - Identifier added to the group request that is to be fanned out to each member of the group
	Group Request Target Members-indicates subset of members of a group
	Filter Criteria - conditions for filtered retrieve operation
	Desired Identifier Result Type - format of resource identifiers returned
	Token Request Indicator - indicating that the Originator may attempt Token Request procedure (for Dynamic Authorization) if initiated by the Receiver
	Tokens - for use in dynamic authorization
	Token IDs - for use in dynamic authorization
	Role IDs - for use in role based access control
	Local Token IDs - for use in dynamic authorization
	Authorization Signature Indicator - for use in Authorization Relationship Mapping
	Authorization Signature - for use in Authorization Relationship Mapping
	Authorization Relationship Indicator - for use in Authorization Relationship Mapping
	Semantic Query Indicator - for use in semantic queries
	Release Version Indicator - the oneM2M release version that this request message conforms to.
	Vendor Information

[0075] 일반 자원(normal resource)은 관리될 정보의 기저(base)를 구성하는 데이터의 표현(representation)의 완전한 집합을 포함한다. 가상(virtual) 또는 선언된(announced)이 아닌 한, 본 문서에서 자원 종류(type)는 일반 자원으로 이해될 수 있다.

[0076] 가상 자원(virtual resource)은 처리(processing) 및/또는 검색 결과(retrieve result)를 트리거링하기 위해 사용된다. 하지만, 가상 자원은 CSE 내에서 영구적인(permanent) 표현을 가지지 아니한다.

[0077] 선언된 자원(announced resource)은 오리지널(original) 자원의 어트리뷰트들(attributes)의 집합을 포함한다. 오리지널 자원이 변화할 때, 선언된 자원은 오리지널 자원의 호스팅(hosting) CSE에 의해 자동적으로 갱신된다. 선언된 자원은 오리지널 자원으로의 링크(link)를 포함한다.

[0078] 자원 선언(resource announcement)은 자원 발견(resource discovery)을 가능하게 한다. 원격(remote) CSE에서의 선언된 자원은 원격 CSE에서, 오리지널 자원의 자식(children)으로서 존재하지(present) 아니하거나 선언된 자식이 아닌, 자식 자원(child resource)을 생성하기 위해 사용될 수 있다.

[0079] 자원의 선언을 지원하기 위해, 자원 템플릿(template) 내의 추가적인 열(column)이 관련된 선언된 자원 타입 내의 포함을 위해 선언될 속성을 특정할 수 있다. 각 선언된 <resourceType>에 대하여, 오리지널 <resourceType>으로의 접미사 'Annc'의 추가가 관련된 선언된 자원 종류를 지시하기 위해 사용될 수 있다. 예를 들어, 자원 <containerAnnc>는 <container> 자원을 위한 선언된 자원 종류를 지시할 수 있고, <groupAnnc>는 <group>을 위한 선언된 자원 종류를 지시할 수 있다.

[0081] GDPR(general data protection regulation)는 유럽 연합(European Union, EU) 및 유럽 경제 지역(European economic area, EEA)의 개인(individual citizens)에 대한 프라이버시(privacy) 및 데이터 보호에 관련된 유럽 연합 법 내의 규정이다. 개인 데이터를 다루는 비즈니스 절차는 원칙의 고려와 함께 설계 및 구현되어야 하며, 데이터를 보호하기 위한 보호 장치를 제공한다. 그리고, 개인 데이터를 다루는 비즈니스 절차는, 데이터가 명백하게 알려진 허락없이 공개적으로 활용되지 아니하고, 분리되어 저장된 부가 정보 없이 대상을 식별하기 위해

사용될 수 없도록, 기본적으로 가장 높은 가능한 프라이버시 설정(highest-possible privacy setting)을 이용한다. GDPR에 따르면, 개인 데이터를 처리하는 것은 원칙적으로 금지되나, 법에 의해 특별히 허용되거나 또는 데이터 주체가 동의한 경우에 허용된다.

[0082] 프로세서(processor)가 다양한 목적을 위해 데이터에 대한 활동을 모니터링해야 한다는 몇몇 문헌들(articles)이 존재한다. 예를 들어, 프로세서는 개인적인 데이터에 대한 위반(breach)을 인지하면, 과도한 지연(undue delay) 없이 제어자(controller)에게 통지해야 한다. 그러므로, IoT 시스템에서 적절한 로깅(logging) 메커니즘을 가질 것인지가 매우 중요하다.

[0084] 로깅 메커니즘을 정의하는데 있어서, 몇몇 주요 이슈가 존재한다. oneM2M 시스템과 같은 IoT 시스템은 다음과 같은 측면에서 정보를 로깅하는 것을 지원할 수 있다.

[0085] · 자원으로의 접근: 누가 해당 자원에 접근하였는가?

[0086] · 접근의 종류: 어떤 종류의 접근(동작)이 이루어졌는가?

[0087] · 시간/날짜: 이벤트가 언제 발생했는가?

[0088] · 위치: 이벤트가 어디서 발생했는가?

[0089] · 레벨: 무엇이 중요하고 무엇이 그렇지 아니한지 어떻게 특정할 것인가?

[0090] · 목적: 로깅의 목적이 무엇인가? (예: 과금, 보안 등)

[0091] · 저장 위치: 로그 정보를 어디에 저장할 것인가?

[0092] 또한, 로깅 메커니즘에 있어서, 자원은 정보를 로깅하는 것에 대한 지시(indication)에 관련된 속성들(properties)을 가질 수 있다. 예를 들어, 속성들은 로깅의 토글(toggle), 무엇을 로깅할지, 언제 로깅할지, 로깅의 종류(예: 사용자, 시스템) 등을 지정할 수 있다.

[0093] 로깅 메커니즘에 따라, oneM2M 시스템은 다음과 같은 동작을 수행할 수 있다. oneM2M 시스템은 주어진 자원이 시스템 로깅의 대상인지 여부를 확인한다. 시스템 로깅의 대상이면, oneM2M 시스템은 주어진 동작(operation)이 로깅의 대상인지 확인한다. 로깅의 대상이면, oneM2M 시스템은 어떤 종류의 로그가 어디로 제공되어야 하는지 판단한다. 또한, oneM2M 시스템은 침임 방지 및 검출 시스템(intrusion prevention and detection system)에 의해 사용될 수단(means) 또는 정보(예: 로그 정보)를 지원할 수 있다.

[0094] 로깅에 관련된 속성이 존재하는 자원에 추가될 수 있다. 예를 들어, 제1 속성은 해당 속성을 가지는 자원이 시스템 로깅의 대상인지를 지시한다. 제1 속성은 어떠한 자원 하에서도 생성될 수 있다. 제1 속성은 'logIndication'이라 지칭될 수 있다. 예를 들어, 제2 속성은 어느 로그 규칙에 따르는지 지시할 수 있다. 로그 관리 규칙에 관련된 자원을 참조하는 URI(uniform resource identifier)가 추가될 수 있다. 제2 속성은 'eventLogID'라 지칭될 수 있다.

[0095] 로그 관리 규칙을 설정하기 위한 자원 타입이 정의될 수 있다. 로그 관리 규칙을 설정하기 위한 자원(이하 '로그 관리 규칙 자원' 또는 '로그 관리 자원'이라 칭함)입은 <logMgtRule>이라 지칭될 수 있다. 로그 관리 규칙 자원은 시스템에 로깅되어야 하는 이벤트들을 정의하기 위해 사용될 수 있다. 로그 관리 규칙 자원은 로깅에 관련된 규칙과 로깅을 트리거링하는 이벤트를 정의하기 위해 사용될 수 있다. 로그 관리 규칙 자원은 이하 [표 5]에 특정된 자식 자원들 중 적어도 하나를 포함할 수 있다. 다시 말해, 로그 관리 규칙 자원은 이하 [표 5]에 나열된 속성들 중 적어도 하나를 포함할 수 있다.

표 5

[0096]

어트리뷰트 이름	설명
logStart	해당 로그 기록의 시작 시점(When to start this log record).
logEnd	해당 로그 기록의 종료 시점(When to end this log record).
logCriteria	본 어트리뷰트는 어떤 정보가 로깅되어야하는지를 제공하는 속성임(This is a property to provide which information should be logged). 예를 들어, 자원에 관련된 모든 동작들이 로깅되어야 하면, 이 속성에 CRUDN가 언급됨(For example, if all the operations on the resource have to be logged, CRUDN have to be mentioned in this property).

logFormat	본 어트리뷰트는 어느 종류의 로그 정보가 어느 포맷으로 저장되어야 하는지를 제공하는 속성임(This is a property to provide what kinds of log information have to be stored under which format). 기본 포맷은 <이벤트 시간, 출처, 동작, 목표 자원, 결과>로 정의될 수 있음(Default format could be <event time, Origin, operation, target resource, results>). 추가적으로, 출처의 IP 주소, 바인딩 프로토콜 등이 로깅될 수 있음(Additionally, ip address of Origin, binding protocols, etc. can be logged). 각 항목은 ';'와 같은 구분자를 이용하여 분리될 수 있음(Each item can be separated using a delimiter such as ';').
logLevel	로그 정보의 레벨(Level of log information). 예를 들어, 모든 정보를 저장하는 것, 성공한 이벤트만 저장하는 것, 실패한 이벤트만 저장하는 것 등으로 정의될 수 있음(For example, store all information, store only successful events, store only failed events).
logResourceIDs	로깅될 자원 식별자들의 목록(A list of resource IDs to be logged)
logStorage	실제로 로그 기록이 저장될 자원에 대한 참조(a reference to a resource that actual log records are stored).

[0098] 도 6은 본 개시에 따른 M2M 시스템에서 로그(log) 관리의 개념을 도시한다. 도 6은 자원 <AE-1>(602), 로그 관리 규칙 <logMgtRule-1>(604), 저장 공간 <logStorage-1>(606) 간 참조 관계를 예시한다.

[0099] 도 6을 참고하면, IoT 플랫폼(620)은 로그-AE(log-AE)(610a)의 요청에 따라 로그 관리 규칙(예: <logMgtRule-1>(604))을 생성한다. 또한, IoT 플랫폼(620)은 AE-1(610b)의 요청에 따라 자원 <AE-1>(602)를 생성한다. 이때, 자원 <AE-1>(602)는 자원 <AE-1>(602)에 적용되는 로그 관리 규칙(예: <logMgtRule-1>(604))을 지시하는 속성(예: eventLogID)을 포함할 수 있다.

[0100] <logMgtRule-1>(604)은 해당 규칙에 따르는 자원을 지시하는 어트리뷰트(예: logResourceIDs)를 포함할 수 있으며, 해당 어트리뷰트는 자원 <AE-1>(602)을 참조(refer)할 수 있다. <logMgtRule-1>(604)의 생성 시, 로그 정보를 저장할 공간으로 사용될 자원(이하 '로그 저장 자원' 또는 '로그 자원'으로 칭함)으로서 <log-Storage-1>(606)이 생성될 수 있다. 이 경우, <logMgtRule-1>(604)은 해당 규칙에 따라 생성된 로그 정보를 저장하는 자원을 지시하는 어트리뷰트(예: logStorage)를 포함할 수 있으며, 해당 어트리뷰트는 <log-Storage-1>(606)을 참조할 수 있다.

[0101] <logMgtRule-1>(604) 및 Storage-1(606)가 생성된 후, 로그-AE-1(610a)에 의해 자원 <AE-1>(602)의 갱신(update)가 요청될 수 있다. 이 경우, eventLogID에 의해 지시되는 <logMgtRule-1>(604)에 따라 로그 정보가 생성하고, 생성된 로그 정보는 logStorage에 의해 참조되는 <logStorage-1>(606)에 저장될 수 있다.

[0103] 도 7은 본 개시에 따른 M2M 시스템에서 로그 정보를 관리하기 위한 신호 교환의 예를 도시한다. 도 7은 AE#1(710a), AE#2(710b), AE#3(710c), IN-CSE(730) 간 신호 교환을 예시한다.

[0104] 도 7을 참고하면, S701 단계에서, AE#2(710b)는 새로운 로그 관리 규칙 자원의 생성을 요청하는 메시지를 IN-CSE(720)에게 송신한다. 예를 들어, AE#2(710b)는 로깅을 위한 새로운 logMgtRule 자원의 생성(create)을 요청할 수 있다. 일 실시 예에 따라, 메시지는 logMgtRule 자원의 생성을 위해 필요한 정보를 포함할 수 있다. 예를 들어, 메시지는 <표 5>에 나열된 어트리뷰트들 중 적어도 하나의 값을 포함할 수 있다.

[0105] S703 단계에서, IN-CSE(720)는 로그 관리 규칙 및 관련 저장 공간(storage)을 생성하기 위한 로컬 처리(local processing)를 수행한다. 예를 들어, IN-CSE(720)는 로그 관리 규칙으로서 자원 <logMgtRule1>을 생성하고, 저장 공간으로서 <logStorage1>을 생성할 수 있다. 일 실시 예에 따라, 자원 <logMgtRule1>은 복수의 어트리뷰트들을 포함하며, 어트리뷰트들 중 적어도 하나의 값은 S701 단계에서 수신된 메시지에 포함된 정보에 기반하여 설정될 수 있다.

[0106] S705 단계에서, AE#1(710a)은 로깅의 대상이 되는 자원의 생성을 요청하는 메시지를 IN-CSE(720)에게 송신한다. 여기서, 메시지는 해당 자원이 로깅의 대상이 됨을 지시하는 제1 정보(예: logIndication), 해당 자원의 로깅에 적용될 로그 관리 규칙(예: logMgtRule 자원)을 지시하는 제2 정보(예: eventLogID)을 포함할 수 있다. 예를 들어, AE#1(710a)은 로깅 대상임을 지시하는 속성 및 따라야 하는 로그 관리 규칙을 참조하는 속성을 가지는 자원의 생성을 요청할 수 있다. 이를 위해, AE#1(710a)는 별도의 절차를 통해 S703 단계에서 생성된 자원

<logMgtRule1>에 대한 정보를 획득할 수 있다. 예를 들어, AE#1(710a)는 IN-CSE(720)과 연결을 설정하는 과정에서 자원 <logMgtRule1>에 대한 정보를 획득하거나, AE#2(710b)로부터 자원 <logMgtRule1>에 대한 정보를 획득할 수 있다.

[0107] S707 단계에서, IN-CSE(720)는 요청된 자원을 생성하기 위한 로컬 처리를 수행한다. 예를 들어, IN-CSE(720)는 AE#1(710a)에 의해 요청된 자원을 로깅 정보와 함께 생성하고, 해당 자원에 해당 자원이 로깅의 대상이 됨을 지시하는 제1 정보(예: logIndication), 해당 자원의 로깅에 적용될 로그 관리 규칙을 지시하는 제2 정보(예: eventLogID)를 포함시킬 수 있다. 이때, 제1 정보는 긍정의 값(예: 1)으로, 제2 정보는 자원 <logMgtRule1>을 지시하는 값으로 설정될 수 있다.

[0108] S709 단계에서, IN-CSE(720)는 응답 메시지를 송신한다. 즉, IN-CSE(720)는 요청된 자원이 성공적으로 생성되었음을 알리는 응답을 AE#1(710a)에게 송신한다.

[0109] S711 단계에서, AE#3(710c)은 AE#1(710a)의 요청에 의해 생성된 자원(예: AE#1)의 검색(retrieve)을 위한 메시지를 IN-CSE(720)에게 송신한다. 즉, AE#3(710c)은 AE#1(710a)의 요청에 의해 생성된 자원(예: AE#1)에 관련된 동작을 요청한다.

[0110] S713 단계에서, IN-CSE(720)는 로그 관리 규칙 검사 및 이벤트 기록을 위한 로컬 처리를 수행한다. 구체적으로, IN-CSE(720)는 AE#3(710c)에 의해 요청된 동작(예: 검색(RETRIEVE))을 수행하고, 수행된 동작에 대한 정보를 로깅한다. 이를 위해, IN-CSE(720)는 요청된 동작에 관련된 자원 및 동작이 로깅 대상인지를 판단하고, 로그 정보를 생성하고, 지정된 저장 공간에 로그 정보를 저장할 수 있다.

[0112] 도 7을 참고하여 설명한 바와 같이, 로그 관리 규칙이 활용될 수 있다. 즉, AE#2(710b)의 요청에 로그 관리 규칙에 따라, AE#1(710a)에 의해 생성된 자원에 대한 AE#3(730c)의 활동에 관련된 로그 정보가 기록될 수 있다.

[0113] 일 실시 예에 따라, 로그 관리 자원 <logMgtRule1>는 로그 관리 어플리케이션에 의해 IN-CSE(720) 내에 생성될 수 있다. 이때, logMgtRule 자원이 제공될 수 있다. 자원이 생성될 때, 로그 관리 어플리케이션은 실제 로그 기록들을 저장하기 위한 자원을 생성할 수 있다. 즉, <logStorage1>이 생성될 수 있다. 본 실시 예와 같은 사례(use case)에서, <logMgtRule1>은, logStorage 어트리뷰트가 <logMgtRule1> 자원의 주소를 참조하도록, 'logFormat' 어트리뷰트가 '시간(time);출처(originator);동작(operation);타겟(target);상태(status)'로 설정되도록, 설정될 수 있다. logResourceIDs 어트리뷰트는 AE#1로 설정될 수 있다. logLevel 어트리뷰트는 모든 요청 메시지들로 설정될 수 있다. logCriteria 어트리뷰트는 CRUDN으로 설정될 수 있다.

[0114] 예를 들어, 인체 센서(human body sensor) 어플리케이션이 IN-CSE(720)에게 logIndication을 가지는 AE#1의 생성을 요청할 수 있다. 인체 센서 어플리케이션은 따를 로깅 규칙으로서 <logMgtRule1>을 참조할 수 있다. IN-CSE(720)는 AE#1에 대한 로깅을 시작하기 위해 <logMgtRule1>의 logResourceID에 AE#1를 추가할 수 있다.

[0115] AE#2(710b)는 AE#2(710b)의 사용자에게 값을 보여주기 위해 AE#1 자원의 읽기를 시도한다. IN-CSE(720)가 요청을 수신하면, IN-CSE(720)가 동작을 수행한다. IN-CSE(720)는 해당 메시지가 로그 자원에 기록되어야 하는지 여부를 검사한다. AE#1이 로깅될 대상이면, IN-CSE(720)는, 어느 객체(entity)가 읽기를 시도했는지, 언제 메시지가 수신되었는지, 바인딩이 사용되는지, 요청의 결과가 무엇인지 등 필요한 정보를 획득하고, 적절한 자원에 수집된 정보를 저장할 수 있다. 이 경우, <logStorage1>/<AE#1>이 처리된 요청을 기록하기 위한 공간(place)이다.

[0117] 도 8은 본 개시에 따른 M2M 시스템에서 로그 관리 규칙을 생성하기 위한 절차의 예를 도시한다. 도 8은 로그 관리 규칙을 생성하는 장치(예: IN-CSE)의 동작 방법을 예시한다. 도 8을 참고한 설명에서, 동작 주체는 '장치'라 지칭된다.

[0118] 도 8을 참고하면, S801 단계에서, 장치는 로그 관리 규칙의 생성 요청을 수신한다. 다시 말해, 장치는 새로운 로그 관리 규칙 자원의 생성을 요청하는 메시지를 수신한다. 일 실시 예에 따라, 메시지는 logMgtRule 자원의 생성을 위해 필요한 정보를 포함할 수 있다. 예를 들어, logMgtRule 자원의 생성을 위해 필요한 정보는 로그 관리 규칙의 내용을 나타내는 정보를 포함할 수 있다.

[0119] S803 단계에서, 장치는 로그 관리 규칙을 생성한다. 로그 관리 규칙은 logMgtRule 자원의 형태로 생성될 수 있다. 로그 관리 규칙은 복수의 어트리뷰트들을 포함한다. 예를 들어, 복수의 어트리뷰트들은 로깅 동작의 시기를

지시하는 정보(예: 시작 시점, 종료 시점), 로깅의 대상이 되는 정보 또는 동작을 특정하는 정보, 로그 정보의 포맷을 정의하는 정보, 로그 정보의 생성 조건, 로깅될 대상 자원에 대한 정보, 로그 정보를 저장할 저장 공간을 지시하는 정보 중 적어도 하나를 포함할 수 있다.

[0120] S805 단계에서, 장치는 로그 정보의 저장 공간을 생성한다. 장치는 S803 단계에서 생성된 로그 관리 규칙에 따라 추후 생성될 로그 정보를 저장하기 위한 저장 공간을 함께 생성할 수 있다. 저장 공간은 logStorage 자원의 형태로 생성될 수 있다. 저장 공간은 관련된 자원들 각각을 위한 하위 공간들을 포함할 수 있다. 여기서, 하위 공간은 대응하는 자원이 생성된 후 생성될 수 있다.

[0121] S807 단계에서, 장치는 참조 관계를 설정한다. 참조 관계는 자원들 간 상호 연동되는 연관성을 의미한다. 참조 관계는 제1 자원의 특정 어트리뷰트에 제2 자원을 지시하는 정보를 저장함으로써 설정될 수 있다. 로깅에 있어서, 로그 관리 규칙, 로그 정보를 저장하기 위한 저장 공간, 로그 관리 규칙이 적용되는 자원은 3자 간 참조 관계에 있다. 아직 로그 관리 규칙이 적용되는 자원이 존재하지 아니하므로, 장치는 로그 관리 규칙 및 저장 공간 간 참조 관계를 설정한다. 구체적으로, 장치는 로그 관리 규칙의 어트리뷰트들 중 하나(예: logStorage)의 값을 저장 공간을 지시하는 정보를 설정한다.

[0122] 도 8을 참고하여 설명한 실시 예에 따라, 장치(예: IN-CSE)는 로그 관리 규칙을 생성함으로써, 로그 관리 규칙의 적용을 요구하는 자원을 생성하기 위한 준비를 완료한다. 이에 따라, 이후 새로운 자원이 생성되는 경우, 장치는 생성된 자원에 로그 관리 규칙을 적용할 수 있다.

[0124] 도 9는 본 개시에 따른 M2M 시스템에서 로그 관리 대상이 되는 자원을 생성하기 위한 절차의 예를 도시한다. 도 9는 로그 정보를 생성하는 장치(예: IN-CSE)의 동작 방법을 예시한다. 도 9를 참고한 설명에서, 동작 주체는 '장치'라 지칭된다.

[0125] 도 9를 참고하면, S901 단계에서, 장치는 자원 생성 요청을 수신한다. 다시 말해, 장치는 AE로부터 자원의 생성을 요청하는 메시지를 수신한다.

[0126] S903 단계에서, 장치는 자원을 생성한다. 장치는 S901 단계에서 요청된 자원을 생성한다. 이후, 도 9에 도시되지 아니하였으나, 자원은 AE와 관련된 정보를 저장하기 위해 사용될 수 있다.

[0127] S905 단계에서, 장치는 로그 관리가 필요한지 여부를 판단한다. 다시 말해, 장치는 S903 단계에서 생성된 자원에 대한 로그 정보의 생성 및 기록이 요구되는지 확인한다. 로그 관리가 필요한지 여부는 S901 단계에서 수신된 메시지에 기반하여 판단될 수 있다. 즉, 수신된 메시지가 해당 자원이 로깅의 대상이 됨을 지시하는 정보, 해당 자원의 로깅에 적용될 로그 관리 규칙을 지시하는 정보를 포함하는 경우, 장치는 로그 관리가 필요함을 판단한다. 만일, 로그 관리가 필요하지 아니하면, 장치는 본 절차를 종료한다.

[0128] 반면, 로그 관리가 필요하면, 907 단계에서, 장치는 로그 관리 규칙 및 자원 간 참조 관계를 설정한다. 생성된 자원이 로그 관리의 대상이므로, 장치는 해당 자원을 로그 관리 규칙과 연관시킨다. 구체적으로, 장치는 해당 자원이 로깅의 대상이 됨을 지시하는 정보로 설정된 어트리뷰트(예: logIndication), 해당 자원의 로깅에 적용될 로그 관리 규칙을 지시하는 정보로 설정된 어트리뷰트(예: eventLogID)를 자원에 포함시킨다.

[0130] 도 10은 본 개시에 따른 M2M 시스템에서 로그 정보를 생성하기 위한 절차의 예를 도시한다. 도 10은 로그 정보를 생성하는 장치(예: IN-CSE)의 동작 방법을 예시한다. 도 10을 참고한 설명에서, 동작 주체는 '장치'라 지칭된다.

[0131] 도 10을 참고하면, S1001 단계에서, 장치는 자원에 대한 동작 요청을 수신한다. 동작은 제1 AE에 의해 생성된 자원에 대하여 제2 AE에 의해 요청된 것으로, 생성, 검색, 삭제, 갱신, 통지 중 적어도 하나일 수 있다.

[0132] S1003 단계에서, 장치는 요청된 동작을 처리한다. 예를 들어, 검색이 요청된 경우, 장치는 자원에서 정보를 읽고, 읽어진 정보를 제2 AE에게 송신한다. 단, 도 10에 도시되지 아니하였으나, 제2 AE가 요청된 동작에 대한 권한을 가지지 아니한 경우, 장치는 요청된 동작을 처리하지 아니하고, 본 절차를 종료할 수 있다.

[0133] S1005 단계에서, 장치는 동작에 관련된 자원이 로그 관리 대상인지 확인한다. 장치는 자원에 포함된 어트리뷰트들 중 적어도 하나의 값을 확인함으로써 해당 자원이 로그 관리 대상인지 확인할 수 있다. 예를 들어, 자원은 해당 자원이 로깅의 대상이 됨을 지시하는 정보로 설정된 어트리뷰트(예: logIndication)를 포함하며, 장치는

해당 어트리뷰트가 긍정의 값으로 설정되어 있는지 확인함으로써 해당 자원이 로그 관리 대상인지 확인할 수 있다. 만일, 자원이 로그 관리 대상이 아니면, 장치는 본 절차를 종료한다.

[0134] 반면, 자원이 로그 관리 대상이면, S1007 단계에서, 장치는 로그 정보를 생성 및 저장한다. 로그 정보는 로그 관리 규칙에 따라 생성되고, 로그 설정 규칙에서 지정된 자원에 저장된다. 이때, 적용되는 로그 관리 규칙은 동작 요청의 대상이 되는 자원에 포함되 어트리뷰트에 의해 지시된다. 즉, 장치는 자원에 포함된 어트리뷰트에 기반하여 적용되는 로그 관리 규칙을 확인하고, 확인된 로그 관리 규칙에 기반하여 로그 정보를 생성하고, 로그 관리 규칙에 포함된 어트리뷰트에 의해 지시되는 저장 공간에 로그 정보를 생성한다. 단, 로그 관리 규칙에 의해 판단한 결과, 로깅의 조건이 만족되지 아니하면, 장치는 본 단계를 생략할 수 있다.

[0135] 도 10을 참고하여 설명한 실시 예와 같이, 로그 정보가 생성 및 저장될 수 있다. 전술한 바와 같이, 제2 AE가 요청된 동작에 대한 권한을 가지지 아니한 경우, 장치는 요청된 동작을 처리하지 아니할 수 있다. 이때, 다른 실시 예에 따라, 장치는 실패한 이벤트에 대한 로그 정보를 생성하고, 저장할 수 있다. 예를 들어, 로그 관리 규칙이 실패한 이벤트, 즉, 거절된 요청을 로깅하도록 설정된 경우, 장치는 거절된 동작에 대한 로그 정보를 생성 및 저장할 수 있다.

[0137] 도 11은 본 개시에 따른 M2M 시스템에서 M2M 장치의 구성을 도시한다. 도 11에 도시된 M2M 장치(1110) 또는 M2M 장치(1120)는 전술한 AE, CSE, NSE 중 적어도 하나의 기능을 수행하는 하드웨어로 이해될 수 있다.

[0138] 도 11를 참고하면, M2M 장치(1110)는 장치를 제어하는 프로세서(1112) 및 신호를 송수신하는 송수신부(1114)를 포함할 수 있다. 이때, 프로세서(1112)는 송수신부(1114)를 제어할 수 있다. 또한, M2M 장치(1110)는 다른 M2M 장치(1120)와 통신을 수행할 수 있다. 다른 M2M 장치(1120)도 프로세서(1122) 및 송수신부(1124)를 포함할 수 있으며, 프로세서(1122) 및 송수신부(1124)는 프로세서(1112) 및 송수신부(1114)와 동일한 기능을 수행할 수 있다.

[0139] 일 예로, 상술한 송신자, 수신자, AE, CSE는 각각 도 11의 M2M 장치들(1110 및 1120) 중 하나일 수 있다. 또한, 도 11의 장치들(1110 및 1120)은 다른 장치일 수 있다. 일 예로, 도 11의 장치들(1110 및 1120)은 통신을 수행하는 장치, 자동차 또는 기지국 등과 같은 장치일 수 있다. 즉, 도 11의 장치들(1110 및 1120)은 통신을 수행할 수 있는 장치를 지칭하는 것으로 상술한 실시 예로 한정되지 않는다.

[0141] 상술한 본 발명의 실시 예들은 다양한 수단을 통해 구현될 수 있다. 일 예로, 본 발명의 실시 예들은 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다.

[0142] 상술한 바와 같이 개시된 본 발명의 바람직한 실시형태에 대한 상세한 설명은 당업자가 본 발명을 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 발명의 바람직한 실시 형태를 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. 따라서, 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다. 또한, 이상에서는 본 명세서의 바람직한 실시 예에 대하여 도시하고 설명하였지만, 본 명세서는 상술한 특정의 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 명세서의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형 실시들은 본 명세서의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안될 것이다.

[0143] 그리고 당해 명세서에서는 물건 발명과 방법 발명이 모두 설명되고 있으며, 필요에 따라 양 발명의 설명은 보충적으로 적용될 수 있다.

[0144] 또한, 본 발명에 대하여 그 바람직한 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0145] 1110: M2M 장치

1112: 송수신부

1114: 프로세서

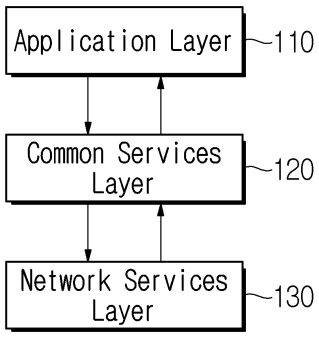
1120: M2M 장치

1122: 송수신부

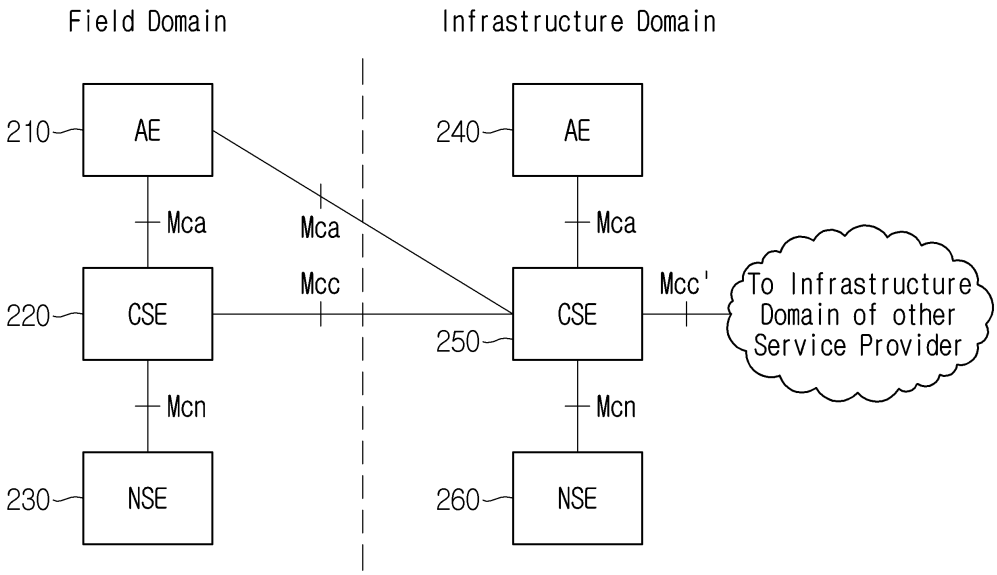
1124: 프로세서

도면

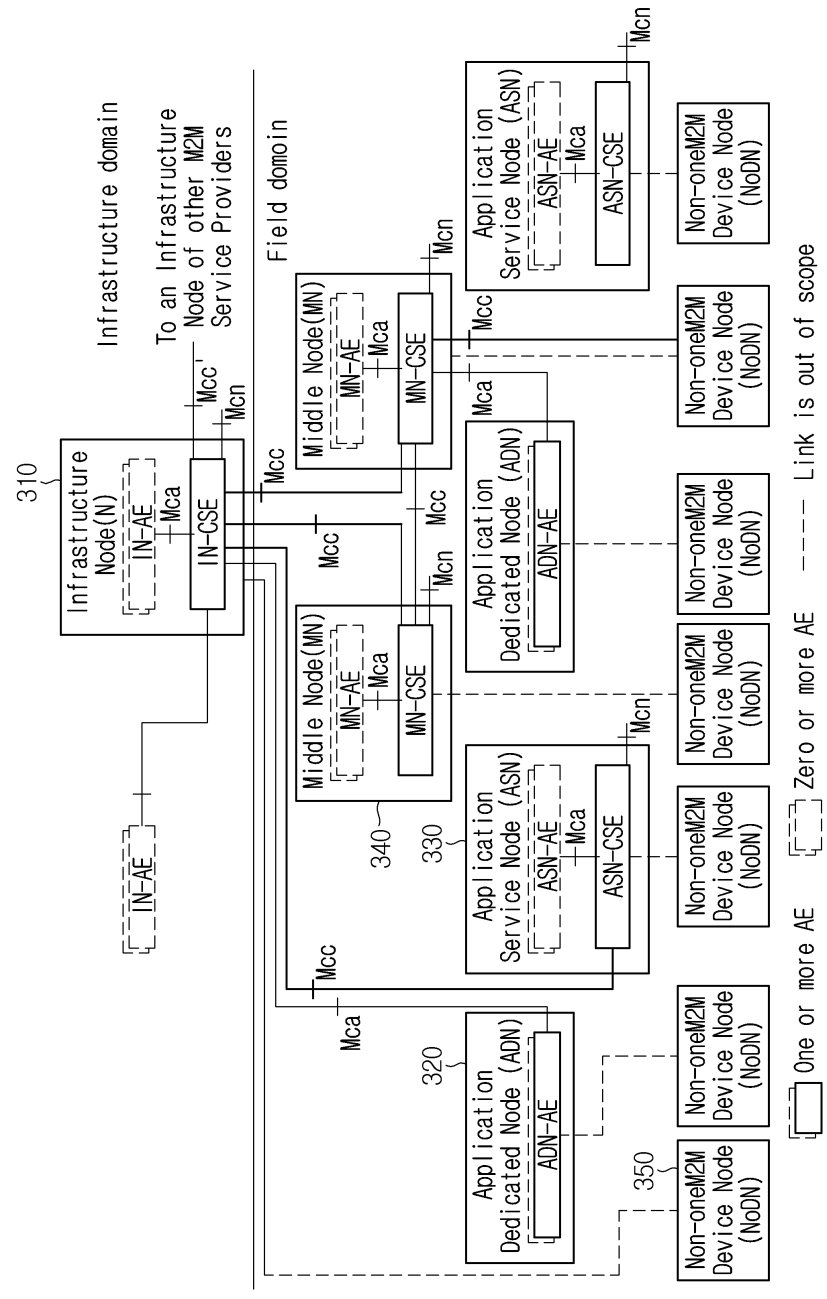
도면1



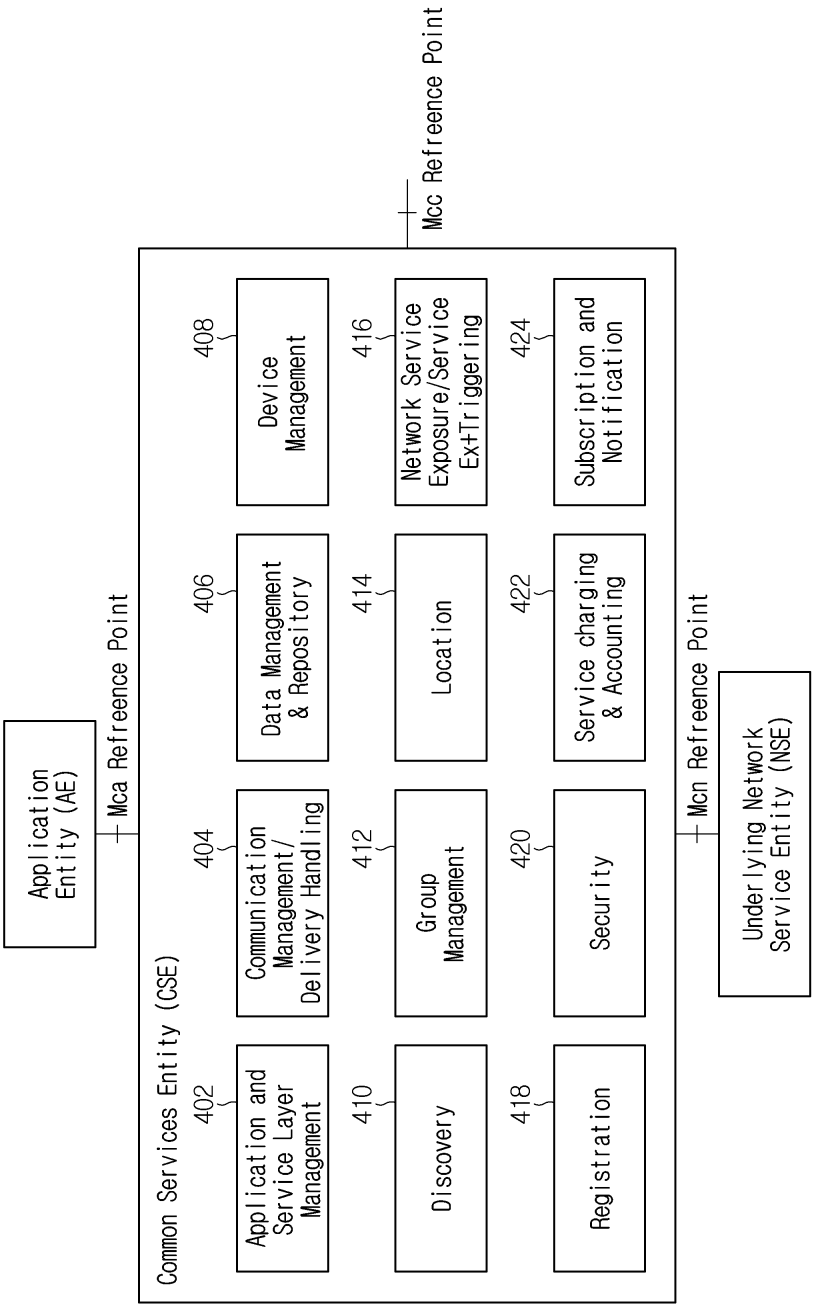
도면2



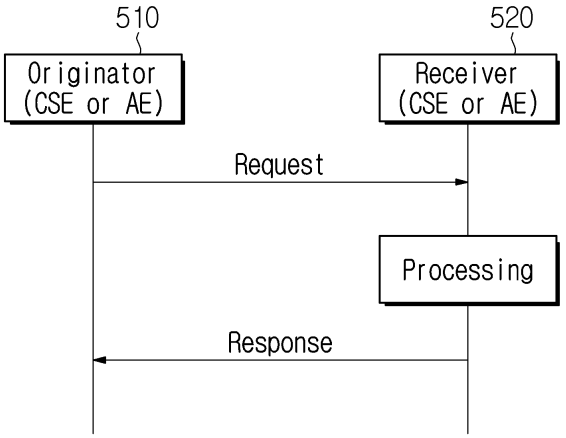
도면3


Infrastructure domain
To an Infrastructure Node of other M2M Service Providers
Field domoin
Infrastructure Node(N)
IN-AE
IN-CSE
Mca
Mcc
Mcc'
Mcn
Middle Node(MN)
MN-AE
MN-CSE
Application Dedicated Node (ADN)
ADN-AE
Application Service Node (ASN)
ASN-AE
ASN-CSE
Non-oneM2M Device Node (NoDN)
310
320
330
340
350
One or more AE
Zero or more AE
Link is out of scope

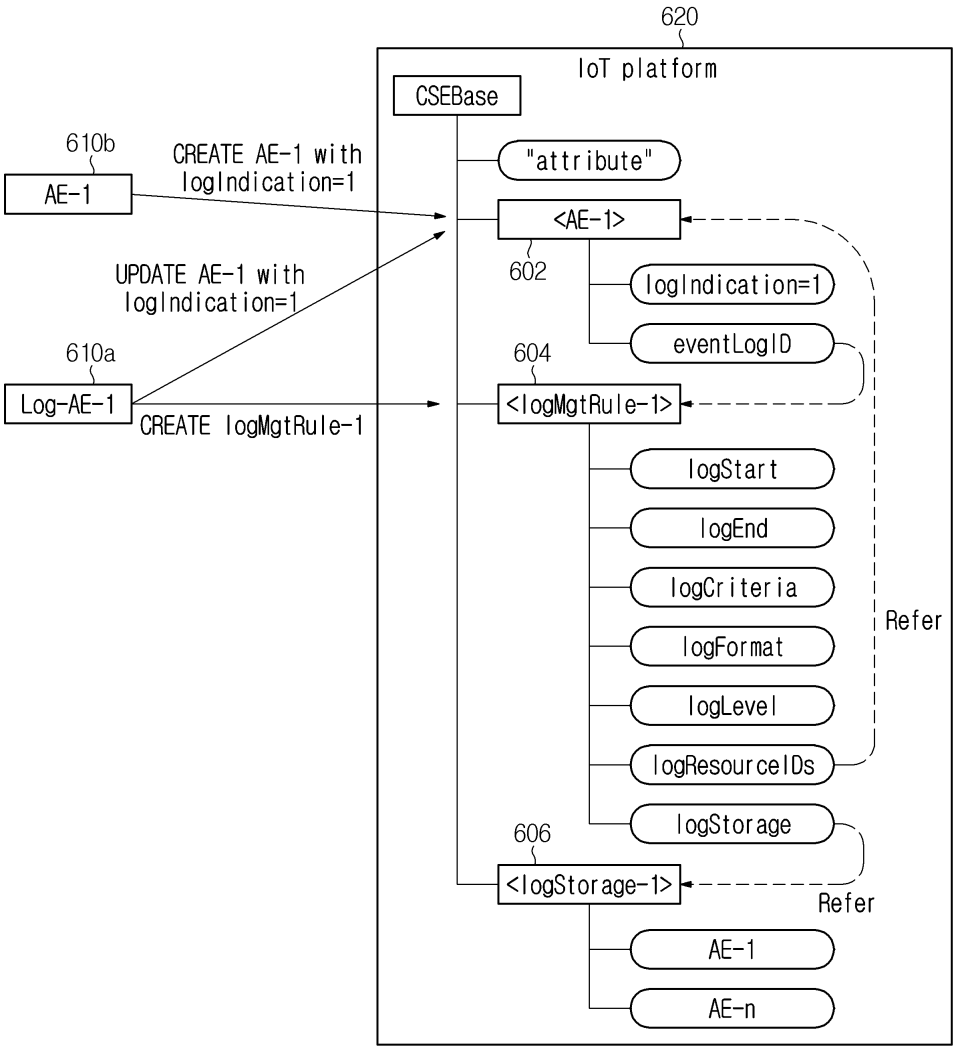
도면4


Application Entity (AE)
Mca Refreence Point
Mcc Refreence Point
Mcn Refreence Point
Underlying Network Service Entity (NSE)
Common Services Entity (CSE)
402
Application and Service Layer Management
404
Communication Management/ Delivery Handling
406
Data Management & Repository
408
Device Management
410
Discovery
412
Group Management
414
Location
416
Network Service Exposure/Service Ex+Triggering
418
Registration
420
Security
422
Service charging & Accounting
424
Subscription and Notification

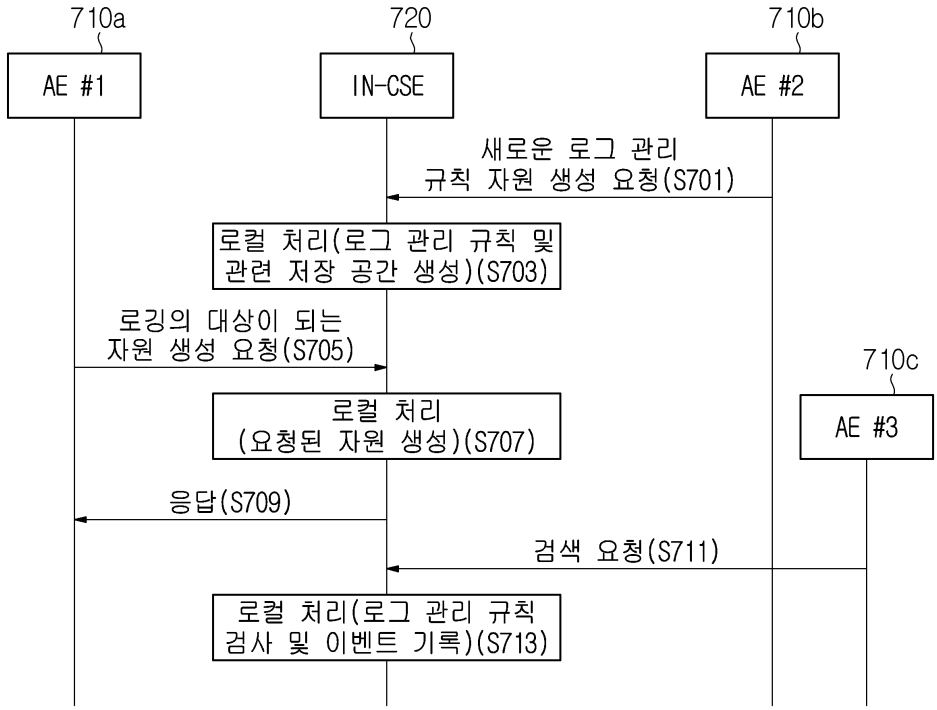
도면5


510
520
Originator
(CSE or AE)
Receiver
(CSE or AE)
Request
Processing
Response

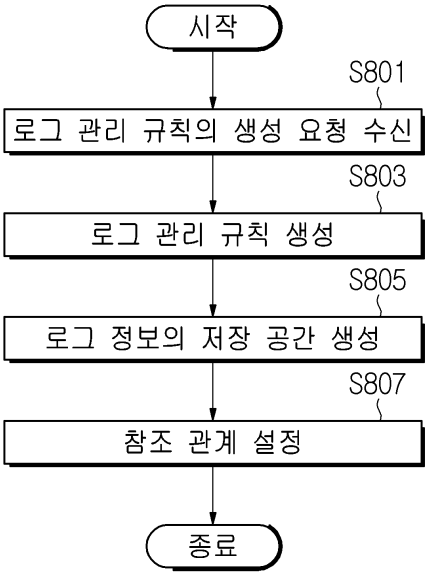
도면6


620
IoT platform
CSEBase
610b
AE-1
CREATE AE-1 with
logIndication=1
"attribute"
<AE-1>
602
logIndication=1
eventLogID
UPDATE AE-1 with
logIndication=1
610a
Log-AE-1
604
<logMgtRule-1>
CREATE logMgtRule-1
logStart
logEnd
logCriteria
logFormat
logLevel
logResourceIDs
Refer
logStorage
606
<logStorage-1>
Refer
AE-1
AE-n

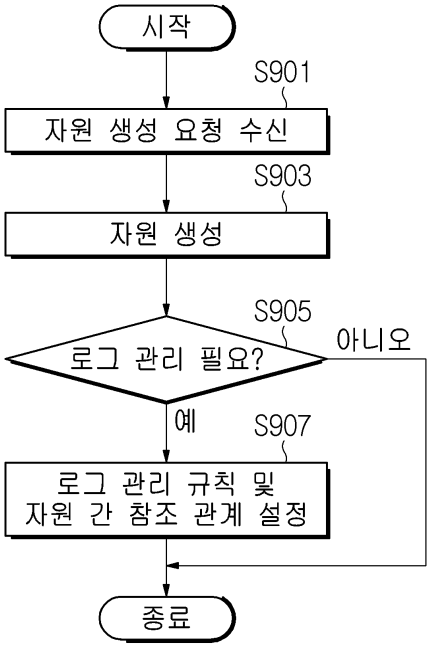
도면7


710a
AE #1
720
IN-CSE
710b
AE #2
새로운 로그 관리
규칙 자원 생성 요청(S701)
로컬 처리(로그 관리 규칙 및
관련 저장 공간 생성)(S703)
로깅의 대상이 되는
자원 생성 요청(S705)
710c
AE #3
로컬 처리
(요청된 자원 생성)(S707)
응답(S709)
검색 요청(S711)
로컬 처리(로그 관리 규칙
검사 및 이벤트 기록)(S713)

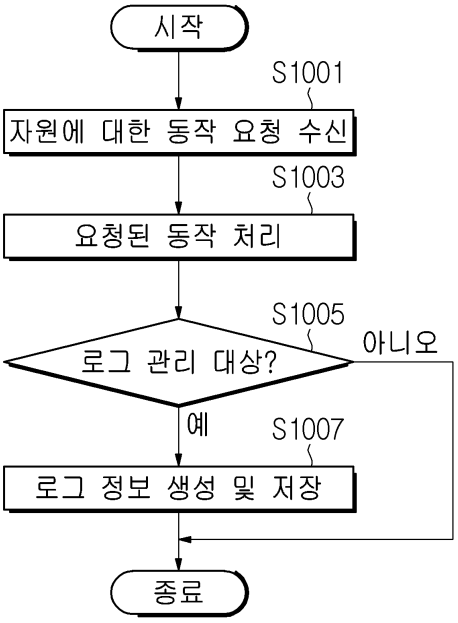
도면8


시작
S801
로그 관리 규칙의 생성 요청 수신
S803
로그 관리 규칙 생성
S805
로그 정보의 저장 공간 생성
S807
참조 관계 설정
종료

도면9



도면10



도면11

