(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012 년 11 월 22 일 (22.11.2012)

WIPO | PCT

(10) 국제공개번호
WO 2012/157880 A2

(51) 국제특허분류: 미분류

(21) 국제출원번호: PCT/KR2012/003570

(22) 국제출원일: 2012 년 5 월 7 일 (07.05.2012)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2011-0045421 2011 년 5 월 13 일 (13.05.2011) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **주식회사 케이티 (KT CORPORATION)** [KR/KR]; 경기도 성남시 분당구 정자동 206, 463-815 Gyeonggi-do (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **김의직 (KIM, Euijik)** [KR/KR]; 서울시 서초구 우면동 17 KT 연구개발센터, 137-140 Seoul (KR). **배정일 (BAE, Jeongil)** [KR/KR]; 서울시 서초구 우면동 17 KT 연구개발센터, 137-140 Seoul (KR). **장덕문 (CHANG, Deokmoon)** [KR/KR]; 서울시 서초구 우면동 17 KT 연구개발센터, 137-140 Seoul (KR). **윤성숙 (YOON, Sungsook)** [KR/KR]; 서울시 서초구 우면동 17 KT 연구개발센터, 137-140 Seoul (KR). **김유선 (KIM, Yuseon)** [KR/KR]; 서울시 서초구 우면동 17 KT 연구개발센터, 137-140 Seoul (KR).

(74) 대리인: **김은구 (KIM, Eungu)** 등; 서울특별시 강남구 역삼동 636-15 상원빌딩 2 층, 135-908 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

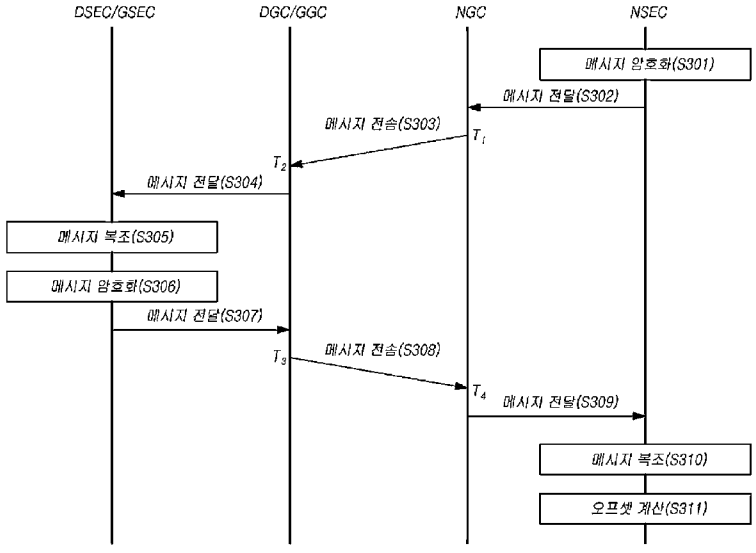
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ,

[다음 쪽 계속]

(54) Title: TIME SYNCHRONIZATION METHODMETHOD FOR TIME SYNCHRONIZATION IN A MACHINE-TO-MACHINE COMMUNICATION SYSTEM

(54) 발명의 명칭 : 사물 통신 시스템에서 시간 동기화 방법

[Fig. 3]



S301 ... Encrypt a message
S302 ... Deliver the message
S303 ... Transmit the message
S304 ... Deliver the message
S305 ... Decode the message
S306 ... Encrypt the message
S307 ... Deliver the message
S308 ... Transmit the message
S309 ... Deliver the message
S310 ... Decode the message
S311 ... Calculate an offset

(57) **Abstract**: The present invention relates to a time synchronization methodmethod for time synchronization between individual machines in M2M machine-to-machine communication.

(57) **요약서**: 본 발명은 사물 통신(M2M communication)에서 개체들 간의 시간 동기화 방법에 관한 것이다.

WO 2012/157880 A2

TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서

발명의 명칭: 사물 통신 시스템에서 시간 동기화 방법

기술분야

[1] 본 발명은 사물 통신(M2M communication)에서 개체들 간의 시간 동기화 방법에 관한 것이다.

배경기술

[2] 사물 통신은 M2M(Machine to Machine communication), MTC(Machine Type Communication), IoT(Internet of Things), 스마트 장치 통신(Smart Device Communication, SDC), 또는 사물 지향 통신(Machine Oriented Communication) 등으로 다양하게 불려질 수 있다. 사물 통신은 사람이 통신 과정에 개입하지 않고 통신이 이루어지는 다양한 통신을 지칭한다. 사물 통신은 지능형 검침(Smart Meter), 전자 보건(e-Health), 통신 가전(Connected Consumer), 도시 자동화(City Automation), 차량 응용(Automotive Application) 등을 포함하는 다양한 분야에 사용될 수 있다.

[3] 이러한 사물 통신에서 각 개체가 갖고 있는 내부 시계가 가르키고 있는 시간 정보는 정확성 및 신뢰성이 유지되어야 한다. 그리고, 이러한 시간 정보는 존재할 수 있는 다양한 악의적인 공격으로부터 보호받아야 한다.

발명의 상세한 설명

기술적 과제

[4] 본 발명은 사물 통신 시스템에서 시간 정보를 악의적인 공격으로부터 보호하면서 개체 간의 시간을 동기화할 수 있는 방법을 제공하는 것을 목적으로 한다.

과제 해결 수단

[5] 상술한 목적을 달성하기 위해 본 발명의 일 실시예는, 제 1 개체가 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 생성한 메시지를, 상기 제 2 개체가 상기 제 1 개체로부터 수신하는 단계; 상기 제 2 개체가 상기 암호화한 메시지를 복호화하여 상기 시간 정보를 추출하는 단계; 및상기 제 2 개체가 상기 시간 정보와 상기 암호화한 메시지를 수신한 시간에 기초하여 시간 오프셋을 계산하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법을 제공한다.

[6] 본 발명의 다른 실시예는, 제 1 개체가 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 메시지를 생성하는 단계; 및 상기 제 1 개체가 상기 암호화한 메시지를 상기 제 2 개체로 전송하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법을 제공한다.

[7] 본 발명의 다른 실시예는, 다른 M2M 개체와 개인 통신망 또는 근거리 통신망에 의해 연결되고, 상기 M2M 개체와 키를 공유하는 M2M 장치로서, 상기

M2M 개체가 상기 키를 이용하여 시간 정보를 암호화하여 생성한 메시지를 상기 M2M 개체로부터 수신하는 통신부; 및 상기 암호화한 메시지를 복호화하여 상기 시간 정보를 추출하며, 상기 시간 정보와 상기 암호화한 메시지를 수신한 시간에 기초하여 시간 오프셋을 계산하는 암호화 처리부를 포함하는 것을 특징으로 하는 M2M 장치를 제공한다.

[8] 본 발명의 다른 실시예는, 다른 M2M 개체와 개인 통신망 또는 근거리 통신망에 의해 연결되고, 상기 M2M 개체와 키를 공유하는 M2M 장치로서, 상기 M2M 개체와 공유하는 키를 이용하여 시간 정보를 암호화하여 메시지를 생성하는 암호화 처리부; 및 상기 암호화한 메시지를 상기 M2M 개체로 전송하는 통신부를 포함하는 것을 특징으로 하는 M2M 장치를 제공한다.

[9] 본 발명의 다른 실시예는, 제 1 개체가 제 1 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 제 2 개체로 전송할 때, 상기 제 2 개체가 상기 제 1 메시지를 제 2 시간에 수신하는 단계; 상기 제 2 개체가 상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하는 단계; 상기 제 2 개체가 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 단계; 및 상기 제 2 개체가 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 제 1 개체로 전송하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법을 제공한다.

[10] 본 발명의 다른 실시예는, 제 1 개체가 제 1 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 단계; 상기 제 1 개체가 상기 제 1 메시지를 상기 제 2 개체로 전송하는 단계; 상기 제 2 개체가 상기 제 1 시간 정보, 상기 제 2 개체가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 1 개체가 상기 제 2 메시지를 제 4 시간에 수신하는 단계; 상기 제 1 개체가 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하는 단계; 및 상기 제 1 개체가 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법을 제공한다.

[11] 본 발명의 다른 실시예는, M2M 플랫폼과 통신하는 M2M 장치로서, 상기 M2M 플랫폼이 제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 장치로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및 상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를를 포함하고, 상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 M2M 플랫폼으로

전송하는 것을 특징으로 하는M2M 장치를 제공한다.

[12] 본 발명의 다른 실시예는, M2M 플랫폼과 통신하는 M2M 게이트웨이로서, 상기 M2M 플랫폼이 제 1 시간 정보를 상기 M2M 게이트웨이와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 게이트웨이로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및 상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를 포함하고, 상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 M2M 플랫폼으로 전송하는 것을 특징으로 하는M2M 게이트웨이를 제공한다.

[13] 본 발명의 다른 실시예는, 다른 M2M 장치 또는 M2M 게이트웨이와 통신하는 M2M 장치로서, 상기 다른 M2M 장치 또는 M2M 게이트웨이가 제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 장치로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및 상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를 포함하고, 상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 다른 M2M 장치 또는 M2M 게이트웨이로 전송하는 것을 특징으로 하는 M2M 장치를 제공한다.

[14] 본 발명의 다른 실시예는, M2M 장치 또는 M2M 게이트웨이, 그리고 어플리케이션 서버와 통신하고, 상기 어플리케이션 서버의 어플리케이션에 의하여 공유되는 기능을 제공하는 M2M 플랫폼으로서, 제 1 시간 정보를 상기 M2M 장치 또는 M2M 게이트웨이와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및 상기 제 1 메시지를 상기 M2M 장치 또는 M2M 게이트웨이로 전송하고, 상기 통신상기 M2M 장치 또는 M2M 게이트웨이가 상기 제 1 시간 정보, 상기 M2M 장치 또는 M2M 게이트웨이가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고, 상기 암호화 처리부는 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 플랫폼을 제공한다.

[15] 본 발명의 다른 실시예는, M2M 장치와 통신하는 M2M 게이트웨이로서, 제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및 상기 제 1 메시지를 상기 M2M 장치로 전송하고, 상기 M2M 장치가 상기 제 1 시간 정보, 상기 M2M 장치가 상기 제 1

메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고, 상기 암호화 처리부는, 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 게이트웨이를 제공한다.

[16] 본 발명의 다른 실시예는, 다른 M2M 장치와 통신하는 M2M 장치로서, 제 1 시간 정보를 상기 다른 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및 상기 제 1 메시지를 상기 다른 M2M 장치로 전송하고, 상기 다른 M2M 장치가 상기 제 1 시간 정보, 상기 다른 M2M 장치가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고, 상기 암호화 처리부는 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 장치를 제공한다.

발명의 효과

[17] 상술한 본 발명에 따르면, 사물 통신 시스템은 시간 정보를 악의적인 공격으로부터 보호하면서 개체 간의 시간을 동기화할 수 있다.

도면의 간단한 설명

[18] 도 1은 본 발명의 실시예들이 적용될 수 있는 M2M 시스템의 구조를 도시하는 도면,

[19] 도 2는 본 발명의 실시예들에서 사용될 수 있는 키의 구성을 예시하는 도면,

[20] 도 3은 제 1 실시예에서 시간 동기화의 방법을 예시하는 흐름도,

[21] 도 4는 제 2 실시예가 적용될 수 있는 시스템의 예를 도시하는 도면,

[22] 도 5는 제 2 실시예에서 시간 동기화의 방법을 설명하기 위한 시계열도,

[23] 도 6은 제 2 실시예에 따른 M2M 장치의 구성을 도시하는 블록도,

[24] 도 7은 제 3 실시예가 적용될 수 있는 시스템의 예를 도시하는 도면,

[25] 도 8은 제 3 실시예에서 시간 동기화의 방법을 설명하기 위한 시계열도,

[26] 도 9는 제 3 실시예에 따른 M2M 게이트웨이의 구성을 도시하는 블록도,

[27] 도 10은 제 3 실시예에 따른 M2M 장치의 구성을 도시하는 블록도, 및

[28] 도 11은 본 발명의 실시예들에 적용될 수 있는 리소스의 구조를 예시하는 도면.

발명의 실시를 위한 형태

[29] 이하, 본 발명의 일부 실시예들을 예시적인 도면을 통해 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에

대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[30] 본 발명의 실시예들은 사물 통신을 중심으로 설명한다. 사물 통신은 M2M(Machine to Machine communication), MTC(Machine Type Communication), IoT(Internet of Things), 스마트 장치 통신(Smart Device Communication, SDC), 또는 사물 지향 통신(Machine Oriented Communication) 등으로 다양하게 불려질 수 있다. 사물 통신은 사람이 통신 과정에 개입하지 않고 통신이 이루어지는 다양한 통신을 지칭한다. 사물 통신은 지능형 검침(Smart Meter), 전자 보건(e-Health), 통신 가전(Connected Consumer), 도시 자동화(City Automation), 차량 응용(Automotive Application) 등을 포함하는 다양한 분야에 사용될 수 있다.

[31] 도 1은 본 발명의 실시예들이 적용될 수 있는 M2M 시스템의 구조를 도시한다.

[32] 도 1을 참조하면, 전체 M2M 시스템(100)은 네트워크 어플리케이션 서버(Network Application Server, 이하 "NA"라 함)(110), M2M 서비스 캐퍼빌러티 서버(M2M Service Capabilities Server, 이하 "NSC"라 함)(120)(또는 M2M 플랫폼으로 불림), 코어망(Core Network)(130), 접속망(Access Network)(140), M2M 장치(M2M Device)(150a, 150b, 160, 170a, 170b, 170c), M2M 게이트웨이(M2M Gateway)(180), 및 지역망(Local Network)(190)을 포함할 수 있다.

[33] NA(110)는 어플리케이션 서버이다. NA(110)는 사용자 인터페이스를 제공할 수 있다.

[34] NSC(120), 또는 M2M 플랫폼은 다양한 어플리케이션에 의해 공유되는 M2M 기능을 제공하는 서버이다. NSC(120)는 NA(110)와 다른 사업자에 의해 운영될 수 있다.

[35] NSC(120)는 다양한 어플리케이션에 의해 공유되는 기능을 제공하는 서비스 캐퍼빌러티(Service Capability, 이하 "SC"라 함)(121~124)를 포함할 수 있다.

[36] 이중 NSEC(Network SECurity Capability)(121)는 M2M 서비스 등록, 인증, 인증을 위한 키의 관리 등 보안과 관련된 기능을 수행할 수 있다.

[37] NGC(Network Generic Communication Capability)(122)는 M2M 게이트웨이(150), M2M 장치(170a, 170b) 및 NSC(120) 내의 SC(121, 123, 124) 사이에서 메시지를 전송하기 위해 사용될 수 있다.

[38] NIP(Network Interworking Proxy Capability)(123)는 소정의 M2M 표준을 따르지 않는 장치(170a)와 통신을 위해 사용될 수 있다.

[39] 그리고, NSC(120)는 복수의 다른 SC(124)를 포함할 수 있다.

[40] NSC(120)는 NGC(122)를 통해 코어망(130)에 연결될 수 있다. 코어망(130)은 최소한 IP(Internet Protocol) 연결은 포함하는 연결 수단을 제공할 수 있다.

[41] 접속망(140)은 M2M 게이트웨이(160) 및 M2M 장치(150a, 150b)가

코어망(130)과 통신하게 하는 네트워크이다. 접속망(14)은, 예를 들면, xDSL(Digital Subscriber Line), HFC(Hybrid Fiber Coaxial), PLC(Power Line Communication), 위성, GERAN(GSM EDGE Radio Access Network), UTRAN(UMTS Terrestrial Radio Access Network), eUTRAN(evolved UMTS Terrestrial Radio Access Network), W-LAN(Wireless Local Area Network), WiMAX(Worldwide Interoperability for Microwave Access) 등일 수 있다.

[42] M2M 장치는 직접 또는 M2M 게이트웨이를 통해 또는 다른 M2M 장치를 통해 접속망(140)에 연결될 수 있다. 또는, M2M 장치는 코어망(130)이나 접속망(140)을 통하지 않고 NSC(120)에 의해 제어될 수 있다.

[43] M2M 장치(150a, 150b)는 직접 접속망(140)에 연결될 수 있다. M2M 장치(150a, 150b)는 인증, 승인, 등록, 관리, 및 제공과 같은 과정을 수행할 수 있다. M2M 장치(150a, 150b)는 장치 서비스 캐퍼빌러티 모듈(Device Service Capabilities, 이하 "DSC"라 함)(151a, 151b) 및 장치 어플리케이션 모듈(Device Application, 이하 "DA"라 함)(159a, 159b)을 포함할 수 있다. DSC(151a, 151b)는 DA(159a, 159b)에서 실행되는 어플리케이션에 의해 공유되는 기능을 제공한다.

[44] DSC(151a, 151b)는 장치 어플리케이션에 의해 공유되는 기능을 제공하는 SC를 포함할 수 있다. SC는 M2M 서비스 등록, 인증, 인증을 위한 키의 관리 등 보안과 관련된 기능을 수행하는 DSEC(Device SECurity Capability)(152a, 152b)를 포함할 수 있다. SC는 NGC(122), DSC(151a, 151b) 내의 SC(152a, 154a, 155a, 152b, 155b) 사이에서 메시지를 전송하는 DGC(Device Generic Communication Capability)(153a, 153b)를 포함할 수 있다. SC는 소정의 M2M 표준을 따르지 않는 M2M 장치(170b)와 통신을 위한 DIP(Device Interworking Proxy Capability)(154a)를 포함할 수 있다. 그리고, SC는 복수의 다른 SC(155a, 155b)를 포함할 수 있다.

[45] M2M 장치(160)는 M2M 게이트웨이(180)를 통해 접속망(140)에 연결될 수 있다. M2M 장치(160)는 M2M 지역망(M2M Area Network)(190)을 이용하여 M2M 게이트웨이(180)에 연결될 수 있다.

[46] M2M 장치(160)는 장치 어플리케이션 모듈(DA)(169)을 포함할 수 있다. 그러나, M2M 장치(160)는 어플리케이션을 위한 SC는 제공하지 않는다.

[47] M2M 게이트웨이(180)는 연결된 M2M 장치(160)를 대리하여 M2M 네트워크의 프록시(proxy)로서 작동할 수 있다. 이러한 M2M 게이트웨이(180)는 연결된 M2M 장치(160)의 측면에서 인증, 승인, 등록, 관리, 및 제공과 같은 과정을 수행할 수 있다.

[48] M2M 게이트웨이(180)는 게이트웨이 서비스 캐퍼빌러티 모듈(Gateway Service Capability, 이하 "GSC"라 함)(181) 및 게이트웨이 어플리케이션 모듈(Gateway Application, 이하 "GA"라 함)(189)을 포함할 수 있다. GSC(181)는 GA(189)에서 실행되는 어플리케이션에 의해 공유되는 기능을 제공할 수 있다. 또한, GSC(181)는 DA(179)에서 실행되는 어플리케이션에 요구되는 기능을 제공할 수

있다.

[49] GSC(181)는 GA(185)에서 실행되는 게이트웨이 어플리케이션 또는 DA(165)에서 실행되는 장치 어플리케이션에 의해 공유되는 기능을 제공하는 SC를 포함할 수 있다. SC는 M2M 서비스 등록, 인증, 인증을 위한 키의 관리 등 보안과 관련된 기능을 수행하는 GSEC(Gateway SECurity Capability)(182)를 포함할 수 있다. SC는 NGC(122), GSC(181) 내의 SC(182, 184, 185) 사이에서 메시지를 전송하는 GGC(Gateway Generic Communication Capability)(183)를 포함할 수 있다. SC는 소정의 M2M 표준을 따르지 않는 M2M 장치(170c)와 통신을 위한 GIP(Gateway Interworking Proxy Capability)(184)를 포함할 수 있다. 그리고, SC는 복수의 다른 SC(185)를 포함할 수 있다.

[50] M2M 장치(160) 및 M2M 게이트웨이(180)를 연결하는 지역망(190)은, 예를 들면, IEEE(Institute of Electrical and Electronics Engineers) 802.15.x, Zigbee, IETF(Internet Engineering Task Force) ROLL(Routing Over Low power and Lossy networks), ISA(International Society of Automation) 100.11a 등과 같은 개인 통신망(Personal Area Network, PAN), 또는 PLC(Power Line Communication), M-BUS(Meter-BUS), 무선 M-BUS, KNX 등과 같은 근거리 통신망(Local Area Network, LAN)일 수 있다.

[51] 또는, M2M 장치(170a, 170b, 170c)는 소정의 M2M 표준을 따르지 않는 장치이고, M2M 장치(170a, 170b, 170c)는 NSC(120), M2M 게이트웨이(180), 또는 다른 M2M 장치(150b)와 통신할 수 있다. 상술한 바와 같이, 이러한 통신은 NIP(124), GIP(184), 또는 DIP(154b)를 통해 성립될 수 있다.

[52] 상술한 M2M 장치에서, 직접 접속망에 연결될 수 있는 M2M 장치(150a, 150b)는 D 타입, 지역망(190)으로 연결된 게이트웨이(180)를 통해 접속망에 연결될 수 있는 M2M 장치(160)는 D' 타입, 소정의 M2M 표준을 따르지 않고 NSC(120), M2M 게이트웨이(180), 다른 M2M 장치(150b)에 연결된 M2M 장치(170a, 170b, 170c)는 d 타입으로 불릴 수 있다.

[53]

[54] 상술한 NSEC(121), DSEC(152a, 152b), GSEC(182)는 키(key)를 이용하여 보안과 관련된 작업을 실행할 수 있다.

[55] 도 2는 본 발명의 실시예들에서 이용될 수 있는 키의 구성을 예시한다.

[56] 도 2를 참조하면, 키는 루트 키(root key)(K_R), 서비스 키(service key)(K_{S1}~K_{Sm}), 어플리케이션 키(application key)(K_{A1}~K_{An})를 포함할 수 있다.

[57] 루트 키(K_R)는 서비스 부트스트랩 동안 M2M 장치(150a, 150b)/게이트웨이(180) 및 MSBF(M2M Service Bootstrapping Function)에 의해 생성될 수 있다. 루트 키(K_R)는 접속망 자격(credential) 또는 사전에 제공된 부트스트랩 자격에 기초하여 생성될 수 있다. 루트 키(K_R)는 M2M 장치(150a, 150b)/게이트웨이(180) 및 M2M 인증 서버(M2M Authentication Server, MAS)에 의해 서비스 등록시 M2M 장치(150a, 150b)/게이트웨이(180)와 NSC(120) 사이의 상호 인증 및 서비스 키(K_S

) 생성을 위해 사용될 수 있다.

[58] 서비스 키(K_S)는 서비스 등록 동안 M2M 장치(150a, 150b)/게이트웨이(180) 및 MAS에 의해 생성될 수 있다. 서비스 키(K_S)는 루트 키(K_R)에 기초하여 생성될 수 있다. 서비스 키(K_S)는 DSEC(152a, 152b)/GSEC(182) 및 NSEC(121)에 의해 어플리케이션 키(K_A) 생성을 위해 사용될 수 있다.

[59] 어플리케이션 키(K_A)는 어플리케이션 등록 동안 DSEC(152a, 152b)/GSEC(182) 및 NSEC(121)에 의해 생성될 수 있다. 어플리케이션 키(K_A)는 서비스 키(KS) 및 어플리케이션 식별자에 기초하여 생성될 수 있다. 어플리케이션 키(K_A)는 DGC(153a, 153b)/GGC(183) 및 NGC(122)에 의해 어플리케이션의 인증 및 승인, 어플리케이션 데이터 전송의 보호를 위해 사용될 수 있다.

[60] 상술한 루트 키(KR), 서비스 키(KS), 어플리케이션 키(KA)는 예시를 위한 것으로서, 본 발명은 이에 제한되지 않는다. 서로 다른 개체들 사이에서 공유될 수 있는 키는 본 발명의 실시예들에서 이용될 수 있다.

[61] 또한, 키는 xSEC(NSEC, DSEC, GSEC), 또는 xGC(NGC, DGC, GGC)와 같은 SC에 의해 다루어지는 것으로 기술되었지만, 본 발명은 이에 제한되지 않는다. 예를 들면, SC를 갖지 않는 M2M 장치(160, 170a, 170b, 170c) 또한 키를 저장할 수 있는 환경을 지원하는 메모리를 가질 수 있다.

[62] 도 1의 시스템에서 각 개체(entity) 사이에서는 시간이 동기화될 필요가 있을 수 있다. 다양한 M2M 어플리케이션에서는 위치 정보와 함께 시간 정보가 중요한 역할을 할 수 있다. 예를 들면, 이동 물체의 추적을 위한 M2M 장치와 어플리케이션에서는 시간 정보가 중요한 역할을 할 수 있다.

[63] 시간 정보의 정확성을 유지하는 시간 동기화 메커니즘은 본질적으로 다양한 악의적인 공격에 취약하다. 예를 들면, 악의적인 개체가 불법적으로 다른 개체의 신분을 소유하고 그 개체로 위장하여 통신하는 공격인 신분 위장 공격(Masquerade attack), 프로토콜에서 유효 메시지를 골라서 복사한 후 나중에 재전송함으로써 정당한 사용자로 가장하는 공격인 재전송 공격(Replay attack), 메시지를 변경하면서 공격하는 메시지 조작 공격(Message manipulation attack), 시간 메시지를 지연시키면서 공격하는 지연 공격(Delay attack) 등의 공격을 받을 수 있다.

[64] 시간 동기화는 코어망(130)과 접속망(140)을 이용하여 통신하는 NSC(120)와 M2M 장치(140a, 140b) 사이에서, 또는 NSC(120)와 M2M 게이트웨이(180) 사이에서 성립될 수 있다. 또는, 시간 동기화는 지역망(190)을 이용하여 통신하는 M2M 게이트웨이(180)와 M2M 장치(160) 사이에서 성립될 수 있다. 또는, 시간 동기화는 M2M 표준을 따르지 않는 M2M 장치(170a, 170b, 170c)와 M2M 표준을 따르는 개체(120, 140b, 180) 사이에서 성립될 수 있다.

[65] **제 1 실시예**

[66] 도 3은 본 실시예에서 시간 동기화의 방법을 예시하는 흐름도이다.

[67] 도 3을 참조하면, NSC(120) 내의 NSEC(121)는 시간 동기화를 위한

메시지(패킷)를 암호화한다(S301 단계). 암호화하는 메시지는 전송 개체(NSC(120))의 주소, 수신 개체(M2M 장치(150a, 150b) 또는 M2M 게이트웨이(180))의 주소, NSC(120)에서 암호화된 정보를 전송하는 시간(T1)을 포함할 수 있다. 이러한 정보의 암호화는 전송 개체와 수신 개체가 서로 공유하는 키를 이용할 수 있다. 즉, 키는 루트 키(K_R), 서비스 키(K_S), 어플리케이션 키(K_A)일 수 있다. 다음의 수학식 1은 NSEC(121)에서 메시지를 암호화하는 수식을 예시한다.

[68] [수학식 1]

[69] $$\text{Timing} - \text{message0} = \text{MAC}_{K_S}\left[node1, node2, N_A, T_1\right]$$

[70] 상기 수학식 1에서 Timing-message0는 암호화한 정보를 나타내고, node1은 전송 개체(NSC(120))의 주소, node2는 수신 개체(M2M 장치(150a, 150b) 또는 M2M 게이트웨이(180))의 주소, N_A는 지연 공격을 방지하기 위한 난수, 그리고 T_1은 암호화한 정보가 전송되는 시간을 나타낸다. 상기 수학식 1에서 암호화 기법으로 MAC(Migration Authorization Code)가 사용되는 것으로 나타나지만, 다른 암호화 기법도 사용될 수 있다. 상기 수학식 1에서 암호화를 위해 서비스 키(K_S)가 사용되는 것으로 나타나지만, NSC(120)와 M2M 장치(150a, 150b)/게이트웨이(180)가 공유하는 다른 키도 사용될 수 있다.

[71] NSEC(121)에서 암호화된 정보는 NGC(122)로 전달되고(S302 단계), 시간(T_1)에 NGC(122)로부터 전송된다(S303 단계). NGC(122)로부터 전송된 암호화된 정보는 시간(T_2)에 DGC(153a, 153b)/GGC(183)에 의해 수신되고, DSEC(152a, 152b)/GSEC(182)로 전달된다(S304 단계). NGC(122)로부터 전송된 암호화된 정보는 DSEC(152a, 152b)/GSEC(182)에서 공유되는 키를 이용하여 복호화된다(S305 단계).

[72] DSEC(152a, 152b)/GSEC(182)는 시간 동기화를 위한 메시지(패킷)을 암호화한다(S306 단계). 암호화하는 메시지는 전송 개체(M2M 장치(150a, 150b)/M2M 게이트웨이(180))의 주소, 수신 개체(NSC(120))의 주소, S302 단계에서 전송된 정보의 전송 시간(T_1), S303 단계에서 수신된 정보의 수신 시간(T_2), 전송 개체에서 암호화된 정보를 전송하는 시간(T_3)을 포함할 수 있다. 이러한 정보의 암호화는 전송 개체와 수신 개체가 서로 공유하는 키를 이용할 수 있다. 즉, 키는 루트 키(K_R), 서비스 키(K_S), 어플리케이션 키(K_A)일 수 있다. 다음의 수학식 2는 DSEC(152a, 152b)/GSEC(182) 에서 메시지를 암호화하는 수식을 예시한다.

[73] [수학식 2]

[74] $$\text{Timing} - \text{message1} = \text{MAC}_{K_S}\left[node2, node1, N_A, T_1, T_2, T_3\right]$$

[75] 상기 수학식 2에서 Timing-message1는 암호화한 정보를 나타내고, node2은 전송 개체(M2M 장치(150a, 150b)/M2M 게이트웨이(180))의 주소, node2는 수신

개체(NSC(120))의 주소, N_A는 지연 공격을 방지하기 위한 난수(수학식 1과는 다른 난수가 사용될 수 있다), T_1은 수학식 1의 암호화한 정보가 전송되는 시간, T2는 수학식 1의 암호화한 정보가 수신된 시간, T3는 수학식 2의 암호화한 정보가 을 나타낸다. 상기 수학식 2에서 암호화 기법으로 MAC(Migration Authorization Code)가 사용되는 것으로 나타나지만, 다른 암호화 기법도 사용될 수 있다. 상기 수학식 2에서 암호화를 위해 서비스 키(K_S)가 사용되는 것으로 나타나지만, NSC(120)와 M2M 장치(150a, 150b)/게이트웨이(180)가 공유하는 다른 키도 사용될 수 있다.

[76] DSEC(152a, 152b)/GSEC(182)에서 암호화된 정보는 DGC(153a, 153b)/GGC(183)으로 전달되고(S307 단계), 시간(T_3)에 DGC(153a, 153b)/GGC(183)으로부터 전송된다(S308 단계). DSEC(152a, 152b)/GSEC(182)로부터 전송된 암호화된 정보는 시간(T_4)에 NGC(122)에 의해 수신되고, NSEC(121)로 전달된다(S309 단계). DSEC(152a, 152b)/GSEC(182)로부터 전송된 암호화된 정보는 NSEC(121)에서 공유되는 키를 이용하여 복호화된다(S310 단계).

[77] NSEC(121)는 시간 T1 내지 T4를 이용하여 시간 오프셋(θ)을 계산할 수 있다(S311 단계). 시간 오프셋(θ)은 다음의 수학식 3에 의해 결정될 수 있다.

[78] [수학식 3]

[79]

$$\theta = \frac{(T_2 - T_1) + (T_4 - T_3)}{2}$$

[80] 수학식 3에 의해 계산된 시간 오프셋(θ)은 NGC(120)와 M2M 장치(150a, 150b)/M2M 게이트웨이(180)가 시간을 동기화하는데 사용될 수 있다. 즉, 시간 오프셋(θ)은 M2M 장치(150a, 150b)/M2M 게이트웨이(180)의 내부 시계의 시간을 수정하기 위해 사용될 수 있다. NGC(120)의 NSEC(121)에서 계산된 오프셋(θ)은 M2M 장치(150a, 150b)/M2M 게이트웨이(180)로 전송될 수 있다. 또는, M2M 장치(150a, 150b)/M2M 게이트웨이(180)는 시간 T_1 및 T_2를 이용하여 독립적으로 시간 오프셋(θ)을 계산할 수 있다($\theta=T_2-T_1$).

[81]

[82] **제 2 실시예**

[83] 도 4는 본 실시예가 적용될 수 있는 시스템의 일예를 도시하는 도면이다.

[84] 도 4를 참조하면, M2M 게이트웨이는 시간 정보에 있어 기준 노드가 되어, M2M 게이트웨이를 중심으로 복수의 노드, 즉 복수의 M2M 장치(예를 들면, 도 1에서 D' 타입 M2M 장치(160))가 지역망을 통해 동시에 연결된다. 즉, 복수의 노드는 M2M 게이트웨이로부터의 시간 정보를 이용하여 시간 동기화를

진행한다.

[85] M2M 게이트웨이는 시간 정보에 있어서 기준 노드로서 시간 메시지를 인접한 M2M 장치(Node A 내지 Node C)에 단일 방향성 방송(Unidirectional Broadcast)을 사용하여 전송한다.

[86] 도 5는 본 실시예에 따른 시간 동기화 방법을 설명하기 위한 시계열도이다. 도 5에서 세로축은 시간 방향이다.

[87] 도 5를 참조하면, M2M 게이트웨이로부터의 방송 신호는 노드(Node A 및 B)로 전송된다. 노드(Node A)는 시간(T_{a1})에 M2M 게이트웨이로부터의 신호를 수신하고, 노드(Node B)는 시간(T_{b1})에 M2M 게이트웨이로부터의 신호를 수신한다.

[88] 각 노드(Node A 및 B)는 M2M 게이트웨이로부터의 신호를 수신한 시간(Ta1 및 Tb1)을 포함하는 메시지를 암호화한다. 다음의 수학식 4는 메시지를 암호화하는 수식을 예시한다.

[89] [수학식 4]

[90]

$$\text{Timing} - \text{message\_A} = \text{MAC}_{\text{K}} \quad [nodeA, nodeB, N_A, T_{a1}]$$

$$\text{Timing} - \text{message\_B} = \text{MAC}_{\text{K}} \quad [nodeB, nodeA, N_A, T_{b1}]$$

[91] 수학식 4에서 제 1 행은 노드(Node A)에서 메시지 암호화를 나타내는 식이고, 제 2 행은 노드(Node B)에서 메시지 암호화를 나타내는 식이다. 수학식 4에서 nodeA는 노드(Node A)의 주소를 나타내고, nodeB는 노드(Node B)의 주소를 나타낸다. N_A는 재전송 공격을 방지하기 위한 난수이다. 제 1 행과 제 2 행에서 난수는 서로 다를 수 있다. T_{a1} 및 T_{b1}은 노드(Node A 및 B)에서 M2M 게이트웨이로부터의 방송 신호를 수신한 시간이다. 그리고, 상술한 정보들은 노드(Node A 및 B)에서 서로 공유하는 키(K)를 이용하여 암호화된다(예를 들면, MAC 암호화 기법으로).

[92] 노드(Node A)에서 암호화된 메시지는 노드(Node B)로 전송되고, 노드(Node B)에서 암호화된 메시지는 노드(Node A)로 전송된다. 암호화된 메시지를 수신한 각 노드(Node A 및 B)는 암호화된 메시지를 복호화하여 시간(T_{a1} 또는 T_{b1})를 추출하고, 추출된 시간 정보(T_{a1} 또는 T_{b1})와 암호화된 메시지를 수신한 시간(T_{a2} 또는 T_{b2})을 이용하여 시간 동기화를 진행할 수 있다. 즉, 노드(Node A)는 노드(Node B)로부터 전송된 암호화된 메시지에서 추출한 시간(T_{b1})과 암호화된 메시지를 수신한 시간(T_{a2})을 이용하여 시간 동기화를 진행하고, 노드(Node B)는 노드(Node A)로부터 전송된 암호화된 메시지에서 추출한 시간(T_{a1})과 암호화된 메시지를 수신한 시간(T_{b2})을 이용하여 시간 동기화를 진행할 수 있다. 이러한 방식으로 노드들 사이에서 시간 동기화가 진행될 수 있다.

[93] 본 실시예에서 M2M 게이트웨이와 지역망을 통해 연결된 D' 타입 M2M 장치를

예를 들어 기술하였지만, 본 실시예는 M2M 게이트웨이 또는 M2M 장치와 연결된 복수의 d 타입 M2M 장치의 경우에도 적용될 수 있다.

[94] 도 6은 본 실시예에 따른 M2M 장치의 구성을 도시하는 블록도이다.

[95] 도 6에 도시된 M2M 장치(600)는 M2M 게이트웨이와 연결된 D' 또는 d 타입의 장치를 포함한다. M2M 장치(600)는 통신부(610) 및 암호화 처리부(620)를 포함한다.

[96] M2M 장치(600)가 암호화된 메시지를 전송하는 개체인 경우, 암호화 처리부(620)는 지역망에 의해 연결된 다른 M2M 장치와 공유하는 키를 이용하여 시간 정보를 암호화하여 메시지를 생성하고, 통신부(610)는 암호화한 메시지를 다른 M2M 장치로 전송한다.

[97] M2M 장치(600)가 암호화된 메시지를 수신하는 개체인 경우, 통신부(610)는 지역망에 의해 연결된 다른 M2M 장치가 M2M 장치(600)와 공유하는 키를 이용하여 시간 정보를 암호화하여 생성한 메시지를 수신하고, 암호화 처리부(620)는 암호화한 메시지를 복호화하여 시간 정보를 추출하고, 추출된 시간 정보와 암호화한 메시지를 수신한 시간에 기초하여 시간 오프셋을 계산한다. 그리하여, M2M 장치(600)는 시간 동기화를 진행할 수 있다.

[98] 통신부(610)는 상황에 따라 암호화된 메시지를 전송할 수 있거나 암호화된 메시지를 수신할 수 있고, 암호화 처리부(620)는 공유하는 키를 이용하여 전송될 메시지를 암호화하거나 수신된 메시지를 복호화할 수 있다.

[99] **제 3 실시예**

[100] 도 7은 본 실시예가 적용될 수 있는 시스템의 일예를 도시하는 도면이다.

[101] 도 7은 복수의 노드가 직렬로 연결된 시스템을 예시한다. 도 7을 참조하면, 노드(Node 1)는 M2M 게이트웨이에 직접 연결되고, 노드(Node 2)는 노드(Node 1)을 통해 M2M 게이트웨이에 연결된다. 이러한 방식으로 복수의 노드가 직렬로 연결될 수 있다.

[102] 이러한 경우, M2M 게이트웨이로부터 시작하여 개체간의 시간 동기화가 진행된다.

[103] 도 8은 인접한 2개의 노드 사이에서 실행되는 시간 동기화 과정을 도시한다. 도 8에서 노드(Node 1)는 M2M 게이트웨이에 가까운 노드(M2M 장치)이고, 노드(Node 2)는 M2M 게이트웨로부터 먼 노드이다.

[104] 노드(Node 1)는 시간(T_1)에 암호화된 메시지를 전송한다. 암호화된 메시지는 예를 들면 다음의 수학식 5에 의해 암호화될 수 있다.

[105] [수학식 5]

[106]
$$\text{Timing} - \text{message0} = \text{MAC}_{\text{K}} \quad [node1, node2, N_A, T_1]$$

[107] 수학식 5에서 node1은 노드(Node 1)의 주소를 나타내고, node2는 노드(Node 2)의 주소를 나타낸다. N_A는 재전송 공격을 방지하기 위한 난수이다. T_1은 노드(Node 1)에서 암호화된 메시지를 전송하는 시간이다. 상술한 정보들은

노드들(Node 1 및 2) 사이에서 공유되는 키(K)를 이용하여 암호화된다.

[108] 이러한 암호화된 메시지는 노드(Node 2)에 의해 시간(T_2)에 수신되고, 노드(Node 2)는 키(K)를 이용하여 시간(T_1)을 추출한다.

[109] 노드(Node 2)는 시간(T_3)에 암호화된 메시지를 전송한다. 암호화된 메시지는 예를 들면 다음의 수학식 6에 의해 암호화될 수 있다.

[110] [수학식 6]

[111] $$\text{Timing} - \text{message1} = \text{MAC}_{\text{K}} \quad [node2, node1, N_A, T_1, T_2, T_3]$$

[112] 수학식 6에서 NA는 수학식 5와는 다음 값일 수 있다. T_1은 노드(Node 1)에서 수학식 5의 암호화된 메시지를 전송하는 시간이고, T_2는 노드(Node 2)에서 노드(Node 1)으로부터의 암호화된 메시지를 수신한 시간이며, T_3는 노드(Node 2)에서 수학식 6의 암호화된 메시지를 전송하는 시간이다. 상술한 정보들은 노드들(Node 1 및 2) 사이에서 공유되는 키(K)를 이용하여 암호화된다.

[113] 이러한 암호화된 메시지는 노드(Node 1)에 의해 시간(T_4)에 수신되고, 노드(Node 1)는 키(K)를 이용하여 시간(T_1 내지 T_3)을 추출한다.

[114] 이러한 경우, 노드(Node 1)는 상기 수학식 3과 동일한 방식으로 시간 오프셋을 계산할 수 있다. 그리하여 두 개체(Node 1 및 2) 간의 내부 시계의 시간 오프셋을 수정할 수 있다.

[115] 이러한 시간 동기화는 우선 M2M 게이트웨이와 이로부터 가장 인접한 노드(M2M 장치) 사이에서 가장 먼저 실행되고, 차례로 인접한 노드들 사이에서 실행될 수 있다.

[116] 본 실시예에서 M2M 게이트웨이로부터 직렬로 연결된 M2M 장치를 예를 들어 기술하였지만, 본 실시예는 기준 시간을 가질 수 있는 하나의 M2M 장치로부터 직렬로 연결된 M2M 장치들의 시간 동기화의 경우에도 적용될 수 있다.

[117] 본 실시예에서 M2M 장치는 도 1의 D' 타입 M2M 장치 또는 d 타입 M2M 장치일 수 있다.

[118] 도 9는 본 실시예에 따른 M2M 게이트웨이(900)의 구성을 도시하는 블록도이다.

[119] 도 9를 참조하면, M2M 게이트웨이(900)는 통신부(910) 및 암호화 처리부(920)를 포함한다. M2M 게이트웨이(900)가 D' 타입 M2M 장치와 통신하는 경우 통신부(910)는 GAE(Gateway Applicaiton Enablement) 캐퍼빌러티에 해당할 수 있고, d 타입 M2M 장치와 통신하는 경우 통신부(910)는 GIP(Gateway Interworking Proxy) 캐퍼빌러티에 해당할 수 있다. 암호화 처리부(920)는 GSEC(Gateway SECurity) 캐퍼빌러티에 해당할 수 있다.

[120] 암호화 처리부(920)는 시간(T1)을 포함하고 M2M 장치와 공유하는 키를 이용하여 암호화된 메시지(Timing-message0)를 생성하고, 통신부(910)는 시간(T1)에 메시지(Timing-message0)를 M2M 장치로 전송한다.

[121] 메시지(Timing-message0)를 시간(T2)에 수신한 M2M 장치는 시간(T1)을

추출하고, 시간(T1 및 T2) 외에 시간(T3)를 포함하고 키를 이용하여 암호화된 메시지(Timing-message1)를 생성하며, 시간(T3)에 메시지(Timing-message1)를 M2M 게이트웨이(900)로 전송할 것이다.

[122] 통신부(910)는 시간(T4)에 메시지(Timing-message1)를 M2M 장치로부터 수신하고, 암호화 처리부(920)는 메시지(Timing-message1)를 복호화하여 시간(T1, T2 및 T3)을 추출하고, 메시지로부터 추출된 시간(T1, T2 및 T3)과 메시지를 수신한 시간(T4)을 이용하여 시간 오프셋을 결정할 수 있다.

[123] 도 10은 본 실시예에 따른 M2M 장치(1000)의 구성을 도시하는 블록도이다. M2M(1000) 장치는 통신부(1010) 및 암호화 처리부(1020)를 포함한다.

[124] M2M 장치(1000)는 M2M 게이트웨이 또는 자신보다 M2M 게이트웨이에 인접한 다른 M2M 장치와 통신하여 자신의 시간 동기화를 진행하고, 자신보다 M2M 게이트웨이로부터 이격된 다른 M2M 장치와 통신하여 다른 M2M 장치의 시간 동기화를 진행할 수 있다. 즉, M2M 게이트웨이로부터 순서대로 시간 동기화가 진행될 수 있다.

[125] M2M 장치(1000)가 자신의 시간 동기화를 진행할 때, 통신부(1010)는 M2M 게이트웨이 또는 다른 M2M 장치로부터 암호화된 메시지(Timing-message0)를 시간(T2)에 수신한다. 메시지(Timing-message0)는 시간(T1)에 대한 정보를 포함하고 공유하는 키에 의해 암호화되어 있고, 암호화 처리부(1020)는 메시지(Timing-message0)를 복호화하여 시간(T1)을 추출한다.

[126] 암호화 처리부(1020)는 메시지로부터 추출된 시간(T1), 메시지를 수신한 시간(T2) 외에 시간(T3)를 포함하고 키를 이용하여 암호화된 메시지(Timing-message1)를 생성하고, 통신부(1020)는 시간(T3)에 메시지(Timing-message1)를 자신에게 메시지(Timing-message0)를 전송한 M2M 게이트웨이 또는 M2M 장치로 전송한다.

[127] M2M 장치(1000)가 다른 M2M 장치의 시간 동기화를 진행할 때, 암호화 처리부(1020)는 시간(T1)을 포함하고 다른 M2M 장치와 공유하는 키를 이용하여 암호화된 메시지(Timing-message0)를 생성하고, 통신부(1010)는 시간(T1)에 메시지(Timing-message0)를 다른 M2M 장치로 전송한다.

[128] 메시지(Timing-message0)를 시간(T2)에 수신한 다른 M2M 장치는 시간(T1)을 추출하고, 시간(T1 및 T2) 외에 시간(T3)를 포함하고 키를 이용하여 암호화된 메시지(Timing-message1)를 생성하며, 시간(T3)에 메시지(Timing-message1)를 M2M 장치(1000)로 전송할 것이다.

[129] 통신부(1010)는 시간(T4)에 메시지(Timing-message1)를 다른 M2M 장치로부터 수신하고, 암호화 처리부(1020)는 메시지(Timing-message1)를 복호화하여 시간(T1, T2 및 T3)을 추출하고, 메시지로부터 추출된 시간(T1, T2 및 T3)과 메시지를 수신한 시간(T4)을 이용하여 시간 오프셋을 결정할 수 있다.

[130]

[131] 상술한 실시예들에서 시간 정보는 각 개체들 사이에서 공유되는 키에 의해

암호화되어 전송된다. 그리하여, 시간 정보는 보안성을 유지하고 악의적인 공격으로부터 보호받을 수 있다.

[132]

[133] 한편, 도 1의 시스템에서 NA(110), DA(159a, 159b, 169), GA(189), 그리고 NSC(120), DSC(151a, 151b), GSC(181) 내의 M2M 서비스 캐퍼빌러티 레이어(Service Capability Layer, 이하 "SCL"이라 함) 사이에서 서로 정보를 교환하기 위한 원칙으로서 RESTful 형식이 적용될 수 있다. RESTful 형식은 REST(Representational State Transfer) 원칙을 따르는 것을 의미한다.

[134] REST의 중요한 개념은 각각이 식별자로서 표시되는 리소스(resource)의 존재이다. 이러한 리소스를 처리하기 위해, 네트워크의 구성 요소들(예를 들면, 도 1의 시스템(100)에서 NA(110), DA(159a, 159b, 169), 그리고 NSC(120), DSC(151a, 151b), GSC(181) 내의 SCL)은 표준화된 인터페이스를 통해 통신하고 이러한 리소스의 표현을 교환할 수 있다. 이러한 리소스는 트리(tree) 구조를 가질 수 있다.

[135] RESTful 구조에서 리소스를 다룰 때, 다음의 4개 기본 방법이 리소스에 적용될 수 있다.

[136] - Create(C): 하위 리소스를 생성한다.

[137] - Retrieve(R): 리소스의 내용을 읽는다.

[138] - Update(U): 리소스의 내용을 쓴다.

[139] - Delete(D): 리소스를 삭제한다.

[140] 이러한 방법은 CRUD 방법으로 불릴 수 있다. 이러한 CRUD 방법에 추가하여, 리소스 교환의 신청(S), 리소스 교환에 대한 통지(N), 및 리소스에 의해 표현되는 관리 명령/태스크의 실행(E) 등이 규정될 수 있다.

[141] 상술한 시간 동기화 방법을 도 1의 시스템 구조에 적용하기 위하여, RESTful 형식에 사용되는 리소스는 도 8의 구조를 가질 수 있다.

[142] 도 11을 참조하면, <contentInstance> 리소스(1101)는 "attribute"(1111), content(1112), Time(1113)의 하위 리소스를 가질 수 있다. "attribute"(1111)는 <contentInstance>(1101)의 속성을 나타낼 수 있다. content(1112)는 인스턴스의 내용을 나타낼 수 있다. 그리고, Time(1113)은 상술한 실시예들에 적용되는 시간 정보를 나타낼 수 있다. 이러한 Time(1113)의 정보는 각 M2M 개체의 시간 정보를 나타낼 수 있다. Time(1113)의 정보는 상술한 실시예들에 의하여 결정될 수 있다.

[143] 도 8에서 Time(1113)은 <contentInstance>(1101) 리소스의 하부에 위치하는 것으로 도시되었지만, Time 리소스는 필요에 따라 다른 리소스의 하부에 위치할 수 있다.

[144]

[145] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본

발명의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 발명에 개시된 실시 예들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

[146] **CROSS-REFERENCE TO RELATED APPLICATION**

[147] 본 특허출원은 2011년 5월 13일 한국에 출원한 특허출원번호 제 10-2011-0045421 호에 대해 미국 특허법 119(a)조 (35 U.S.C § 119(a))에 따라 우선권을 주장하며, 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다. 아울러, 본 특허출원은 미국 이외에 국가에 대해서도 위와 동일한 이유로 우선권을 주장하면 그 모든 내용은 참고문헌으로 본 특허출원에 병합된다.

청구범위

[청구항 1] 제 1 개체가 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 생성한 메시지를, 상기 제 2 개체가 상기 제 1 개체로부터 수신하는 단계;
상기 제 2 개체가 상기 암호화한 메시지를 복호화하여 상기 시간 정보를 추출하는 단계; 및
상기 제 2 개체가 상기 시간 정보와 상기 암호화한 메시지를 수신한 시간에 기초하여 시간 오프셋을 계산하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 2] 제 1 항에 있어서,
상기 시간 정보는 상기 제 1 개체가 기준 시간 정보를 갖는 제 3 개체로부터 방송되는 신호를 수신하는 시간의 정보인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 3] 제 1 항에 있어서,
상기 제 1 개체 및 제 2 개체는 M2M 장치인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 4] 제 2 항에 있어서,
상기 제 3 개체는 M2M 게이트웨이인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 5] 제 1 항에 있어서,
상기 제 1 개체와 제 2 개체는 개인 통신망 또는 근거리 통신망에 의해 연결되는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 6] 제 2 항에 있어서,
상기 제 1 개체와 제 3 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 7] 제 1 개체가 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 메시지를 생성하는 단계; 및
상기 제 1 개체가 상기 암호화한 메시지를 상기 제 2 개체로 전송하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 8] 제 7 항에 있어서,
상기 시간 정보는 상기 제 1 개체가 기준 시간 정보를 갖는 제 3 개체로부터 방송되는 신호를 수신하는 시간의 정보인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 9] 제 7 항에 있어서,

상기 제 1 개체 및 제 2 개체는 M2M 장치인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 10] 제 8 항에 있어서,
상기 제 3 개체는 M2M 게이트웨이인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 11] 제 7 항에 있어서,
상기 제 1 개체와 제 2 개체는 개인 통신망 또는 근거리 통신망에 의해 연결되는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 12] 제 8 항에 있어서,
상기 제 1 개체와 제 3 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 13] 다른 M2M 개체와 개인 통신망 또는 근거리 통신망에 의해 연결되고, 상기 M2M 개체와 키를 공유하는 M2M 장치로서,
상기 M2M 개체가 상기 키를 이용하여 시간 정보를 암호화하여 생성한 메시지를 상기 M2M 개체로부터 수신하는 통신부; 및
상기 암호화한 메시지를 복호화하여 상기 시간 정보를 추출하며, 상기 시간 정보와 상기 암호화한 메시지를 수신한 시간에 기초하여 시간 오프셋을 계산하는 암호화 처리부를 포함하는 것을 특징으로 하는 M2M 장치.

[청구항 14] 제 13 항에 있어서,
상기 시간 정보는 상기 M2M 개체가 기준 시간 정보를 갖는 개체로부터 방송되는 신호를 수신하는 시간의 정보인 것을 특징으로 하는 M2M 장치.

[청구항 15] 제 14 항에 있어서,
상기 기준 시간 정보를 갖는 개체는 M2M 게이트웨이인 것을 특징으로 하는 M2M 장치.

[청구항 16] 제 14 항에 있어서,
상기 M2M 개체와 상기 기준 시간 정보를 갖는 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 M2M 장치.

[청구항 17] 다른 M2M 개체와 개인 통신망 또는 근거리 통신망에 의해 연결되고, 상기 M2M 개체와 키를 공유하는 M2M 장치로서,
상기 M2M 개체와 공유하는 키를 이용하여 시간 정보를 암호화하여 메시지를 생성하는 암호화 처리부; 및
상기 암호화한 메시지를 상기 M2M 개체로 전송하는 통신부를 포함하는 것을 특징으로 하는 M2M 장치.

[청구항 18] 제 17 항에 있어서,
상기 시간 정보는 상기 M2M 장치가 기준 시간 정보를 갖는 개체로부터 방송되는 신호를 수신하는 시간의 정보인 것을 특징으로 하는 M2M 장치.

[청구항 19] 제 18 항에 있어서,
상기 기준 시간 정보를 갖는 개체는 M2M 게이트웨이인 것을 특징으로 하는 M2M 장치.

[청구항 20] 제 18 항에 있어서,
상기 M2M 장치와 상기 기준 시간 정보를 갖는 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 M2M 장치.

[청구항 21] 제 1 개체가 제 1 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 제 2 개체로 전송할 때, 상기 제 2 개체가 상기 제 1 메시지를 제 2 시간에 수신하는 단계;
상기 제 2 개체가 상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하는 단계;
상기 제 2 개체가 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 단계; 및
상기 제 2 개체가 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 제 1 개체로 전송하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 22] 제 21 항에 있어서,
상기 제 1 개체는 M2M 장치 또는 M2M 게이트웨이, 그리고 어플리케이션 서버와 통신하고, 상기 어플리케이션 서버의 어플리케이션에 의하여 공유되는 기능을 제공하는 M2M 플랫폼이고,
상기 제 2 개체는 상기 M2M 장치 또는 M2M 게이트웨이인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 23] 제 22 항에 있어서,
상기 키는 루트 키, 서비스 키, 또는 어플리케이션 키인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 24] 제 22 항에 있어서,
상기 제 1 개체와 제 2 개체는 코어망 및 접속망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서의 시간 동기화 방법.

[청구항 25] 제 21 항에 있어서,
상기 제 1 개체는 M2M 장치 또는 M2M 게이트웨이이고,

상기 제 2 개체는 상기 제 1 개체와 통신하는 M2M 장치인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 26] 제 25 항에 있어서,
상기 제 1 개체와 제 2 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서의 시간 동기화 방법.

[청구항 27] 제 1 개체가 제 1 시간 정보를 제 2 개체와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 단계;
상기 제 1 개체가 상기 제 1 메시지를 상기 제 2 개체로 전송하는 단계;
상기 제 2 개체가 상기 제 1 시간 정보, 상기 제 2 개체가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 1 개체가 상기 제 2 메시지를 제 4 시간에 수신하는 단계;
상기 제 1 개체가 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하는 단계; 및
상기 제 1 개체가 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 단계를 포함하는 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 28] 제 27 항에 있어서,
상기 제 1 개체는 M2M 장치 또는 M2M 게이트웨이, 그리고 어플리케이션 서버와 통신하고, 상기 어플리케이션 서버의 어플리케이션에 의하여 공유되는 기능을 제공하는 M2M 플랫폼이고,
상기 제 2 개체는 상기 M2M 장치 또는 M2M 게이트웨이인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 29] 제 28 항에 있어서,
상기 키는 루트 키, 서비스 키, 또는 어플리케이션 키인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 30] 제 28 항에 있어서,
상기 제 1 개체와 제 2 개체는 코어망 및 접속망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서의 시간 동기화 방법.

[청구항 31] 제 27 항에 있어서,
상기 제 1 개체는 M2M 장치 또는 M2M 게이트웨이이고,
상기 제 2 개체는 상기 제 1 개체와 통신하는 M2M 장치인 것을 특징으로 하는 사물 통신 시스템에서 시간 동기화 방법.

[청구항 32] 제 31 항에 있어서,
상기 제 1 개체와 제 2 개체는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 사물 통신 시스템에서의 시간 동기화 방법.

[청구항 33] M2M 플랫폼과 통신하는 M2M 장치로서,
상기 M2M 플랫폼이 제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 장치로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및
상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를를 포함하고,
상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 M2M 플랫폼으로 전송하는 것을 특징으로 하는M2M 장치.

[청구항 34] 제 33 항에 있어서,
상기 키는 루트 키, 서비스 키, 또는 어플리케이션 키인 것을 특징으로 하는 M2M 장치.

[청구항 35] 제 33 항에 있어서,
상기 M2M 폴랫폼과 상기 M2M 장치는 코어망 및 접속망을 통해 통신하는 것을 특징으로 하는 M2M 장치.

[청구항 36] M2M 플랫폼과 통신하는 M2M 게이트웨이로서,
상기 M2M 플랫폼이 제 1 시간 정보를 상기 M2M 게이트웨이와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 게이트웨이로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및
상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를 포함하고,
상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 M2M 플랫폼으로 전송하는 것을 특징으로 하는M2M 게이트웨이.

[청구항 37] 제 36 항에 있어서,
상기 키는 루트 키, 서비스 키, 또는 어플리케이션 키인 것을 특징으로 하는 M2M 게이트웨이.

[청구항 38] 제 36 항에 있어서,

상기 M2M 폴랫폼과 상기 M2M 장치는 코어망 및 접속망을 통해 통신하는 것을 특징으로 하는 M2M 장치.

[청구항 39] 다른 M2M 장치 또는 M2M 게이트웨이와 통신하는 M2M 장치로서,
상기 다른 M2M 장치 또는 M2M 게이트웨이가 제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하고 상기 제 1 시간 정보의 때에 상기 제 1 메시지를 상기 M2M 장치로 전송할 때, 상기 제 1 메시지를 제 2 시간에 수신하는 통신부; 및
상기 제 1 메시지를 복호화하여 제 1 시간 정보를 추출하고, 상기 제 1 시간 정보, 상기 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하는 암호화 처리부를 포함하고,
상기 통신부는 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 상기 다른 M2M 장치 또는 M2M 게이트웨이로 전송하는 것을 특징으로 하는M2M 장치.

[청구항 40] 제 33 항에 있어서,
다른 M2M 장치 또는 M2M 게이트웨이와 상기 M2M 장치는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 M2M 장치.

[청구항 41] M2M 장치 또는 M2M 게이트웨이, 그리고 어플리케이션 서버와 통신하고, 상기 어플리케이션 서버의 어플리케이션에 의하여 공유되는 기능을 제공하는 M2M 플랫폼으로서,
제 1 시간 정보를 상기 M2M 장치 또는 M2M 게이트웨이와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및
상기 제 1 메시지를 상기 M2M 장치 또는 M2M 게이트웨이로 전송하고, 상기 통신상기 M2M 장치 또는 M2M 게이트웨이가 상기 제 1 시간 정보, 상기 M2M 장치 또는 M2M 게이트웨이가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고,
상기 암호화 처리부는 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 플랫폼.

[청구항 42] 제 41 항에 있어서,
상기 키는 루트 키, 서비스 키, 또는 어플리케이션 키인 것을 특징으로 하는 M2M 플랫폼.

[청구항 43] 제 41 항에 있어서,
상기 M2M 플랫폼과 상기 M2M 장치 또는 M2M 게이트웨이는 코어망 및 접속망을 통해 통신하는 것을 특징으로 하는 M2M 폴랫폼.

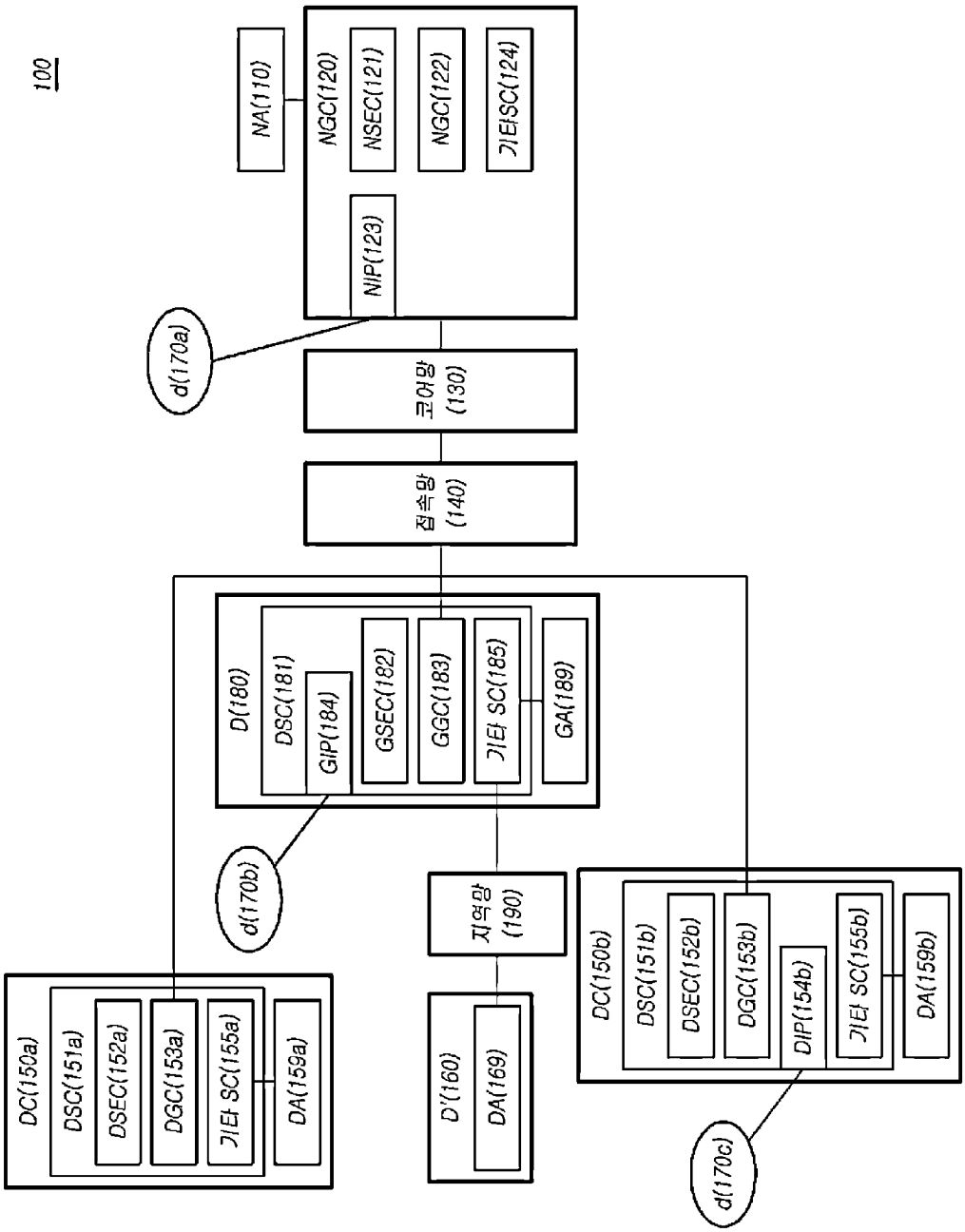
[청구항 44] M2M 장치와 통신하는 M2M 게이트웨이로서,
제 1 시간 정보를 상기 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및
상기 제 1 메시지를 상기 M2M 장치로 전송하고, 상기 M2M 장치가 상기 제 1 시간 정보, 상기 M2M 장치가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고,
상기 암호화 처리부는, 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 게이트웨이.

[청구항 45] 제 44 항에 있어서,
상기 M2M 게이트웨이와 상기 M2M 장치는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 M2M 게이트웨이.

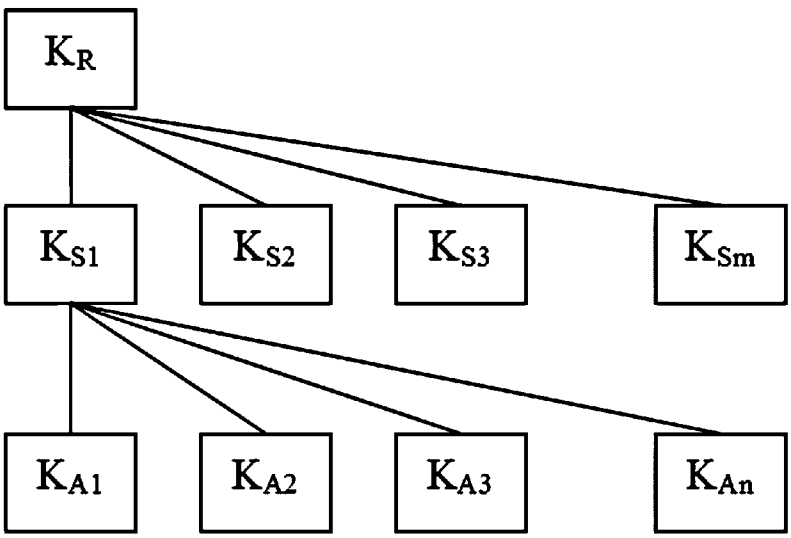
[청구항 46] 다른 M2M 장치와 통신하는 M2M 장치로서,
제 1 시간 정보를 상기 다른 M2M 장치와 공유하는 키를 이용하여 암호화하여 제 1 메시지를 생성하는 암호화 처리부; 및
상기 제 1 메시지를 상기 다른 M2M 장치로 전송하고, 상기 다른 M2M 장치가 상기 제 1 시간 정보, 상기 다른 M2M 장치가 상기 제 1 메시지를 수신한 제 2 시간 정보, 및 제 3 시간 정보를 상기 키를 이용하여 암호화하여 제 2 메시지를 생성하고 상기 제 2 메시지를 상기 제 3 시간 정보의 때에 전송할 때, 상기 제 2 메시지를 제 4 시간에 수신하는 통신부를 포함하고,
상기 암호화 처리부는 상기 제 2 메시지를 복호화하여 상기 제 1 시간 정보, 제 2 시간 정보 및 제 3 시간 정보를 추출하고, 상기 제 1 시간 정보, 제 2 시간 정보, 제 3 시간 정보, 및 제 4 시간 정보에 기초하여 시간 오프셋을 계산하는 것을 특징으로 하는 M2M 장치.

[청구항 47] 제 44 항에 있어서,
상기 M2M 장치와 상기 다른 M2M 장치는 개인 통신망 또는 근거리 통신망을 통해 통신하는 것을 특징으로 하는 M2M 게이트웨이.

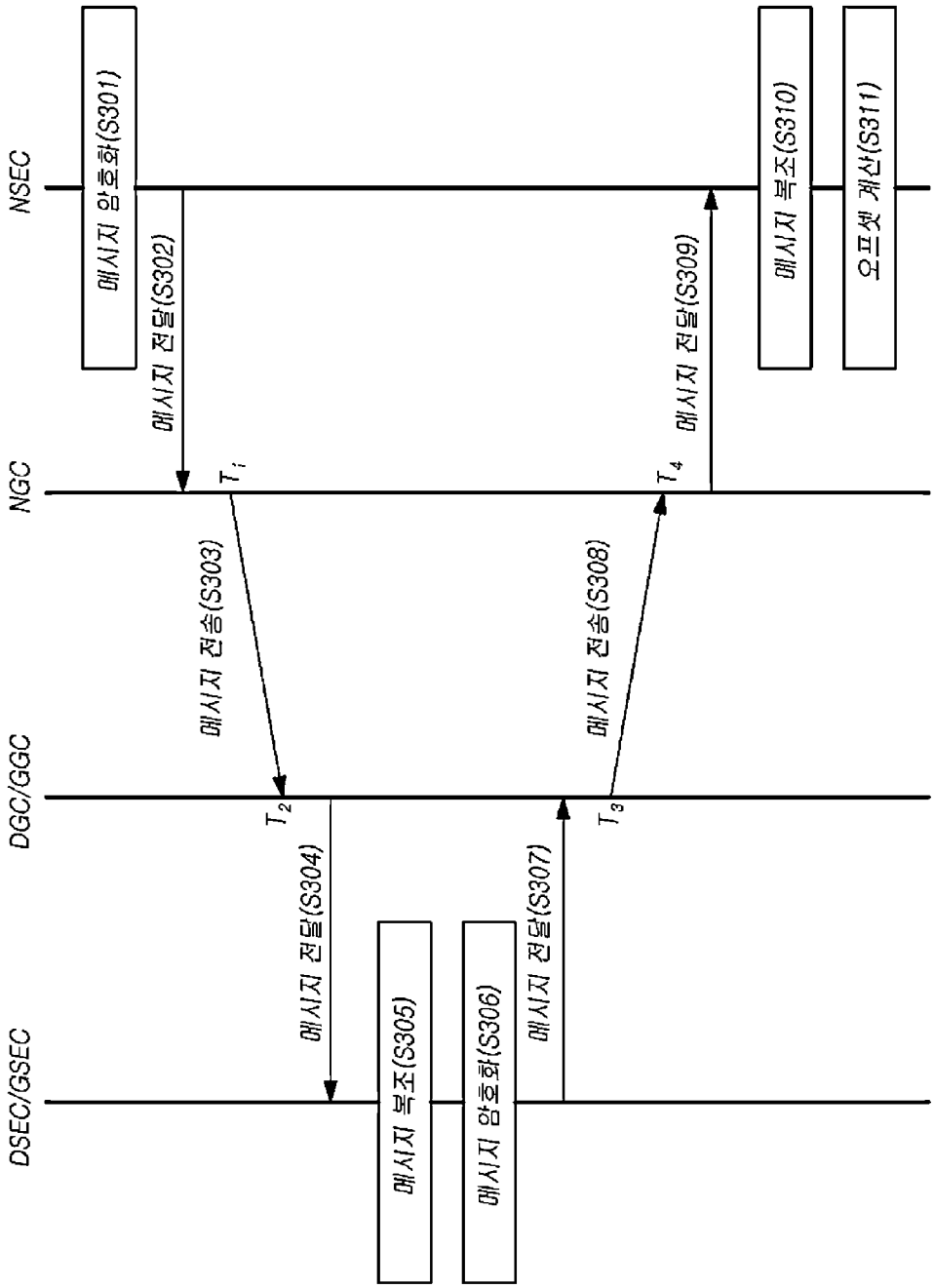
[Fig. 1]


100
NA(110)
NGC(120)
NSEC(121)
NGC(122)
기타SC(124)
NIP(123)
d(170a)
코아망 (130)
접속망 (140)
D(180)
DSC(181)
GIP(184)
GSEC(182)
GGC(183)
기타 SC(185)
GA(189)
d(170b)
지역망 (190)
DC(150a)
DSC(151a)
DSEC(152a)
DGC(153a)
기타 SC(155a)
DA(159a)
D'(160)
DA(169)
DC(150b)
DSC(151b)
DSEC(152b)
DGC(153b)
DIP(154b)
기타 SC(155b)
DA(159b)
d(170c)

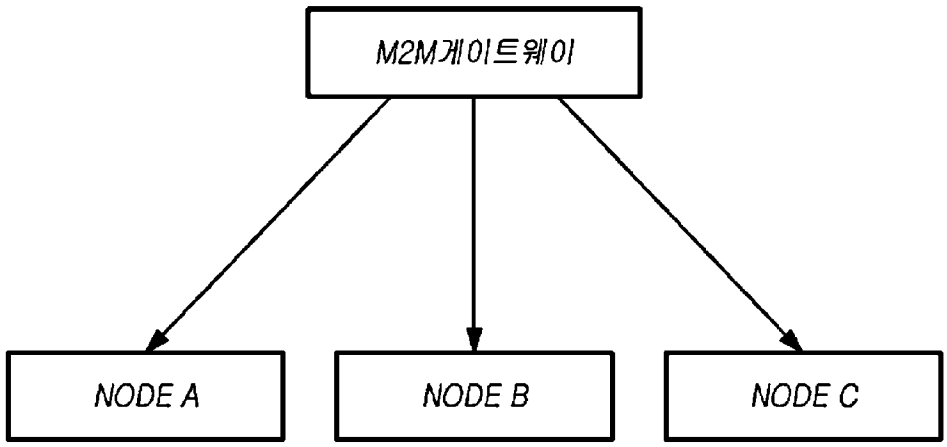
[Fig. 2]


K_R
K_{S1}
K_{S2}
K_{S3}
K_{Sm}
K_{A1}
K_{A2}
K_{A3}
K_{An}

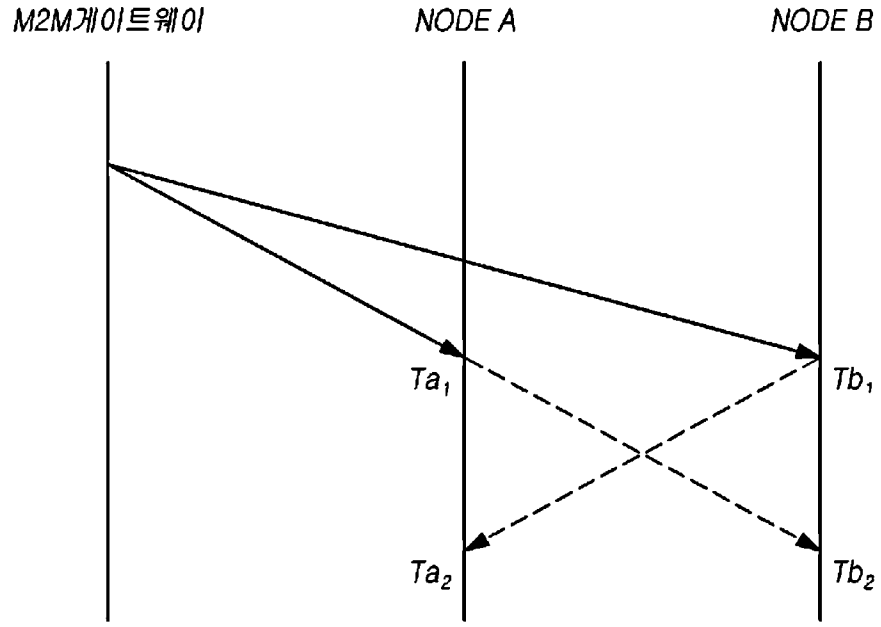
[Fig. 3]


NSEC
NGC
DGC/GGC
DSEC/GSEC
메시지 암호화(S301)
메시지 전달(S302)
메시지 전송(S303)
메시지 전달(S304)
메시지 복조(S305)
메시지 암호화(S306)
메시지 전달(S307)
메시지 전송(S308)
메시지 전달(S309)
메시지 복조(S310)
오프셋 계산(S311)
T1
T2
T3
T4

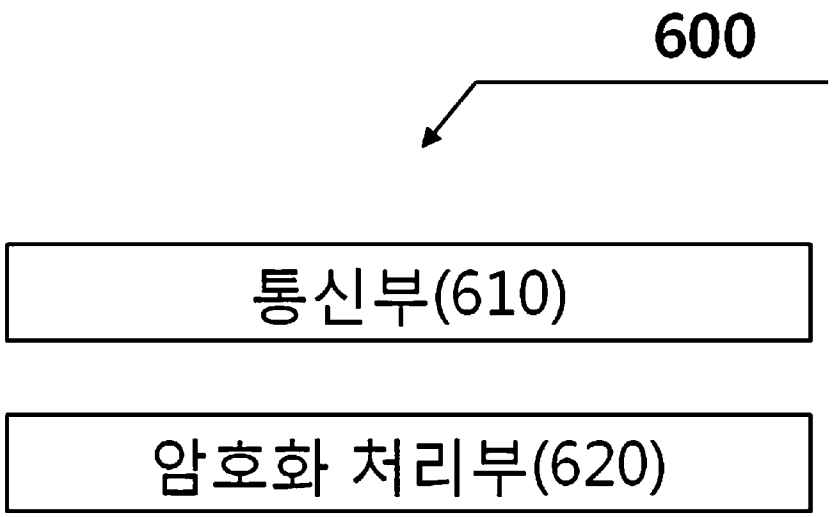
[Fig. 4]


M2M게이트웨이
NODE A
NODE B
NODE C

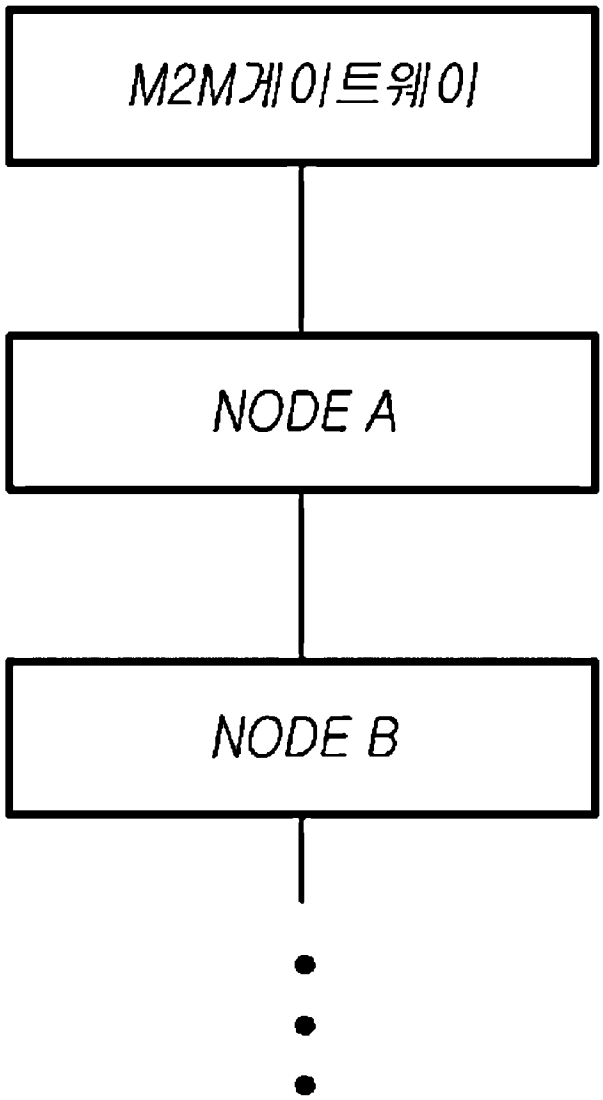
[Fig. 5]



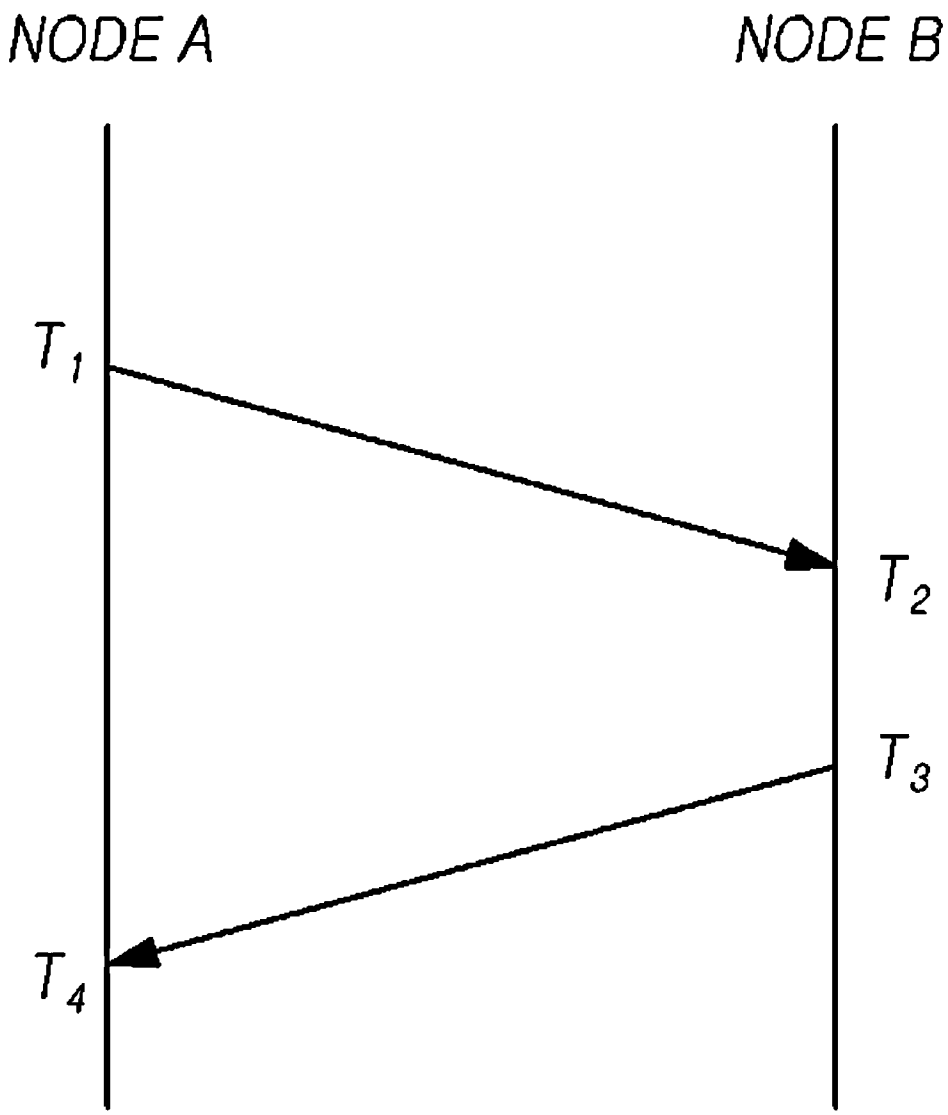
[Fig. 6]



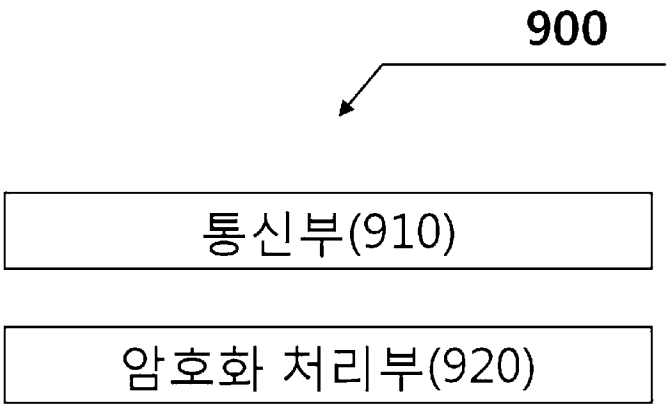
[Fig. 7]



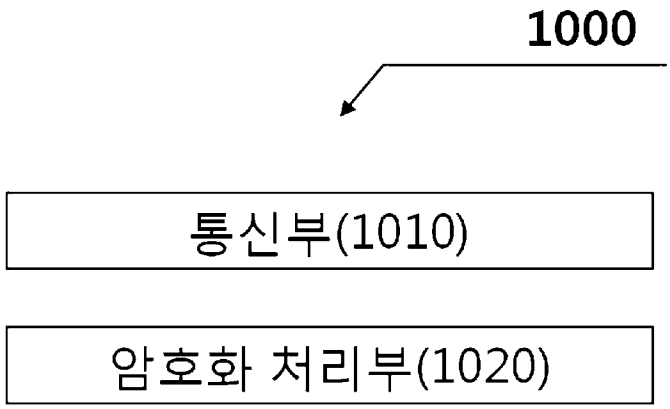
[Fig. 8]



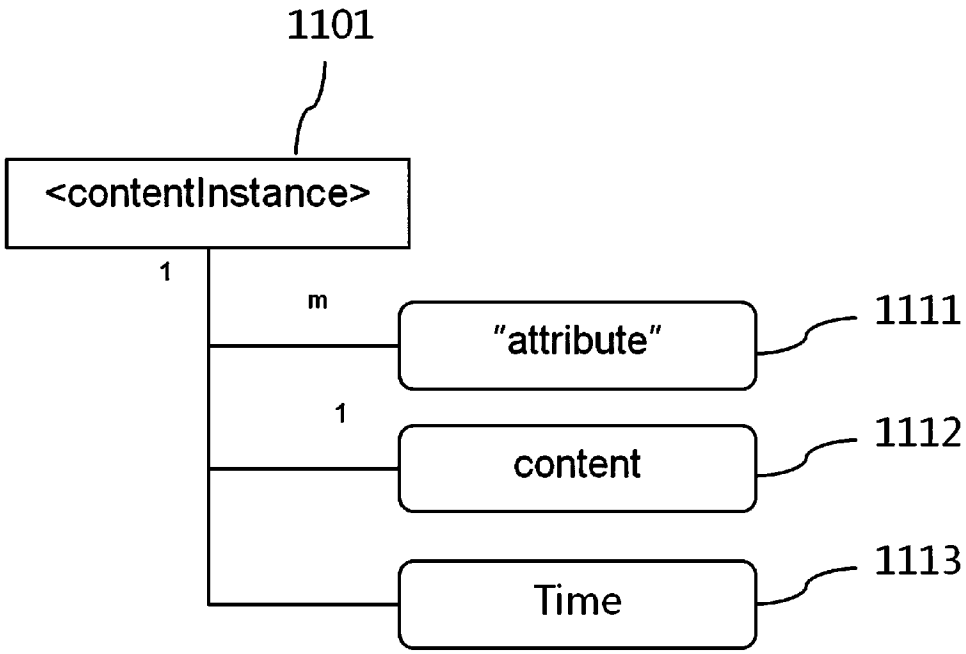
[Fig. 9]



[Fig. 10]


1000
통신부(1010)
암호화 처리부(1020)

[Fig. 11]


1101
<contentInstance>
1
m
"attribute"
1111
1
content
1112
Time
1113