The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 4, pp.33-41, Aug. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.4.33
JIIBC 2015-4-5

M2M 환경에서 안전한 데이터 공유를 위한 상호인증 및 키 교환 기법

Mutual Authentication and Key Establishment Mechanism for Secure Data Sharing in M2M Environment

박중오*, 김상근**

JungOh Park*, Sangkun Kim**

요 약 기계간의 통신을 지칭하는 M2M(Machine to Machine) 환경은 최근 융합 서비스의 등장과 동시에, 수많은 장치의 활용으로 인한 전반적인 보안 요구사항이 증가하고 있으며, 관련 각 표준화단체는 이러한 장치간의 보안요구사항을 충족하기 위해 각 영역별 보안기술에 대해 표준화를 진행 중에 있다. 본 논문에서는 다수의 M2M 장치들 간에 상호인증을 위한 키 관리 방법에 대해 제안한다. 본 논문에서 제안하는 방법은 M2M 디바이스와 서버 간에 상호인증을 기반으로 서비스 영역이 다른 디바이스 간에 안전한 데이터 공유를 수행한다. 제안하는 기법은 현재 M2M 표준의 보안 요구사항에 따른 안전성을 충족하고, 기존 연구에서 제안된 인증기술보다 성능이 향상된 타원곡선 알고리즘 기반 프로토콜을 사용하여 효율성을 강화하였다.

Abstract With rapid rise of virtualization technology from diverse types of cloud computing service, security problems such as data safety and reliability are the issues at stake. Since damage in virtualization layer of cloud service can cause damage on all host (user) tasks, Hypervisor that provides an environment for multiple virtual operating systems can be a target of attackers. This paper propose a security structure for protecting Hypervisor from hacking and malware infection.

Key Words : M2M, WoT, MTC, Key Management, Mutual Authentication

Ⅰ. 서 론

M2M 환경에서 각 통신 장치들은 서로 정보를 수집하고 정보를 상호 공유한다. 즉, 사람이 아닌 사물 간에 통신을 이용하여 정보를 공유하는 사물지능통신을 M2M 통신이라고 한다[1]. 유사한 용어로는 Smart Object, WoT(Web of Things), MTC(Machine type Communication), D2D(Device-to-Device) 등이 있다[2]. M2M 시장은 현재 CE(Consumer Electronic), Intelligent Bulilding, Utilities, Automotive, Heahthcare 분야를 기준으로 2020년 전체 시장의 91%를 차지하고, 연결 가능한 Device 중 CE 분야가 2011년 4천만 개에서 2020년 42억 개로 100배 이상 성장할 전망이다[3][4][5]. 이는 CE 분야의 활성화에 따라 현재의 문화 공간, 지역 고객, 기업 비즈니스 등 대상에서 향후 CE을 대상으로 스마트 Device 중심의 서비스를 제공할 것으로 예상할 수 있다.

*정회원, 동양미래대학교 전기전자통신공학부
**정회원, 성결대학교 컴퓨터공학부 (교신저자)
접수일자 2015년 6월 18일, 수정완료 2015년 7월 20일
게재확정일자 2015년 8월 7일

Received: 18 June, 2015 / Revised: 20 July, 2015 /
Accepted: 7 August, 2015
**Corresponding Author: sgkim@sungkyul.edu
Dept of Computer Engineering, Sungkyul University, Korea

M2M 서비스는 기존 셀룰러망의 분리된 특정 통신사 인프라를 이용하는 형태가 아닌 모든 사업자의 공통 인프라 환경을 이용하는 형태이기 때문에 전반적인 서비스 기능을 수행하는 미들웨어 플랫폼의 보안 요구사항이 증가할 것으로 예상된다.

국제 표준화 기구인 ITU-T, 3GPP, ETSI, IETF 등은 oneM2M(총 7개 기관 참여)을 중심으로 M2M 관련된 표준화를 진행하고 있다. 보안기술 관련에는 ITU-T에서 SG17[6]과 연계하여 M2M 통신 암호화 기반 프로토콜을 개발 중이며, 3GPP의 SA3 워킹그룹에서 MTC 보안을 위한 TR 33.868[7], ETSI에서 애플리케이션, 서비스 등 보안 요구사항을 위한 TS 102 689[8] 등 각 기관에서 담당하는 영역 별로 보안기술 표준화를 진행하고 있다. 공통 통신 프로토콜 관련으로는 IETF의 CORE 워킹그룹에서 메모리, 에너지, 성능 등에 제약이 있는 M2M 환경을 위한 차세대 웹 기반 프로토콜인 CoAP(Constrained Application Protocol)을 표준화를 진행하고 있다[9].

기존 M2M 환경에서 보안을 위한 연구[10][11][12]들은 프로토콜 및 알고리즘의 자체 성능분석과 안전성 분석 등으로 M2M Device 적용 범위가 한정적이고, 다수 Device 간에 프로토콜 수행에 따른 성능 오버헤드에 대한 부분을 고려하지 않았다. 또한 M2M 환경에서 사용 가능한 기존 디바이스 인증기술들[13][14][15][16]등과 연계성이 낮아 활용도가 낮다.

본 논문은 IETF 표준에서 핵심으로 진행 중인 CoAP 프로토콜[17]을 기반으로 서비스 별 프로토콜 과정을 정의한다. 또한 다중 Device간의 성능적인 효율을 위해 타원곡선 알고리즘을 사용하고, 프로토콜을 최적화 한다. CoAP 프로토콜을 사용할 수 없는 표준 및 비표준 장치는 기존 RFID 환경과 같은 암호 알고리즘의 적용할 수 없는 극히 제한적인 환경으로 본 논문의 적용 대상에서 제외한다. 본 논문의 2장 관련연구는 현재 표준 진행 중인 M2M 보안기능과 요구사항과 CoAP 프로토콜 분석 3장 제안하는 프로토콜 4장 안전성 분석 5장 결론으로 마친다.

II. 관련연구

1. M2M 보안기능 및 보안 요구사항

ETSI TS 102 689[18]는 M2M 서비스 요구사항을 정의하고 있는 표준 규격으로, M2M서비스의 일반적 요구사항과 관리, M2M 서비스를 위한 기능 요구사항, 보안, 네이밍 및 어드레싱 요구사항 등을 정의하고 있다. M2M Device의 보안관리(DESC) 기능은 M2M 단말 및 M2M 서비스 공급자 사이의 성공적인 상호 인증을 통해 M2M 서비스 구동 및 연결을 위한 인증키들을 도출하고, 보안환경 외부로부터의 무단 접근으로부터 이들 인증키들을 보호한다. M2M 단말 애플리케이션을 인증하기 위해 서비스 구동 및 연결과정에서 생성된 인증키들을 활용하여 애플리케이션 인증을 위한 인증키를 생성하고 단말의 서비스 기능 계층 내에서 이들 인증키들을 관리한다. 또한 M2M 장치 및 M2M 서비스 공급자 간의 상호 인증을 통해 서비스 기능 계층의 등록을 수행한다. M2M 환경에서 각 보안기능 별 보안 요구사항은 표 1와 같다.

표 1. 보안기능 별 요구사항
Table 1. Security functional requirements

구분	보안기능	보안 요구사항
인증키 관리 기능	M2M 서버 플랫폼의 NSCL과의 정보 데이터를 주고받기 전에 서비스 연결을 위한 인증키들을 생성하고 저장 관리	생성된 인증키의 암호학적 안전성
		암호키의 안전한 저장 관리
인증, 권한설정	M2M 단말 애플리케이션과 메시지 전송을 시작하기 전에 애플리케이션 인증키를 통해 인증을 수행	Device와 서버간의 상호인증
		통신 내용의 암호화
	서비스 기능 계층의 리소스 데이터에 접근하기 전에 접근 권한을 설정	서비스 사용자 별 올바른 접근권한 설정
데이터 무결성 체크	M2M 단말 애플리케이션과 DSCL 사이의 데이터 전송 시 데이터의 무결성을 체크	Device와 DSCL 사이의 데이터 무결성 체크
	서비스 기능들 사이에 데이터 전송 시 데이터의 무결성을 체크한다.	동일 또는 다른 서비스 사이의 데이터 무결성 체크
	M2M 단말과 M2M 서버 플랫폼 사이에 데이터 전송 시 데이터의 무결성을 체크	종단 간 데이터 무결성 체크

현재 M2M 표준에서 특정 서비스 또는 인증기술을 규정하기 보다는, 사용 환경들을 기본으로 요구사항을 충족시키는 인증기술을 선택적으로 적용하는 것이 상황이다. M2M 환경은 주변기기를 제어하는 서비스, 서로 다른 플랫폼, 서로 다른 통신 기술 등 서로 다른 환경과 다

른 기기들과의 통신을 위한 상호 인증기술이 기본적으로 요구된다. 또한 민감한 정보에 대한 암호화 기술과, 무결성을 체크할 수 있는 부인방지 기술이 요구된다. 보안 요구사항에는 공통적으로 Device 간 인증, 권한관리, 데이터 암호화, 무결성 검사 등이 보안 요구사항 필수요소로 정의된다. 현재 표준은 환경적인 면에서 공통적으로 인증기술의 호환성과 제한적인 환경을 위한 경량 화된 프로토콜이 요구하고 있으며, 향후 서비스가 확대될 것으로 예상했을 때 서비스적인 면에서는 상이한 서비스 별 상호인증에 사용되는 인증키와 권한인가를 위한 키 관리 기법 표준이 요구될 것으로 분석된다.

2. CoAP 프로토콜

인터넷 표준 단체인 IETF는 다양한 기기가 인터넷에 연결될 것을 예상하여 IPv6, 6LowPAN 등 표준 활동을 진행해 왔으며 각 워킹 그룹에서 저전력, 소형 장치에 들어가는 표준을 개발하고 있다. 현재 UDP 기반의 CoAP 표준화와 3차 시험이 완료(2013년 11월)되었으며 이외에 다른 전송계층(SMS, TCP 등)에서 CoAP 사용에 관한 표준화를 진행 중이다[19]. CoAP 프로토콜은 저전력 센서 노드를 위한 IEEE 802.15.4 표준을 기반으로 네트워크 계층인 IPv6 프로토콜과 IEEE 802.15.4 표준과의 인터페이스를 위한 계층으로 6LoWPAN 프로토콜이 위치하고 있다[20]. CoAP의 적용대상은 노드가 저성능의 CPU, 적은 용량의 램 및 롬을 가지는 조건인 Constrained 노드를 대상으로, 주요 목표는 REST 아키텍처를 기반으로 이기종의 M2M Device 간에 경량 화된 응용계층을 제공하는 것이다. 그림 1은 추상적 계층상의 CoAP의 위치를 나타낸다.

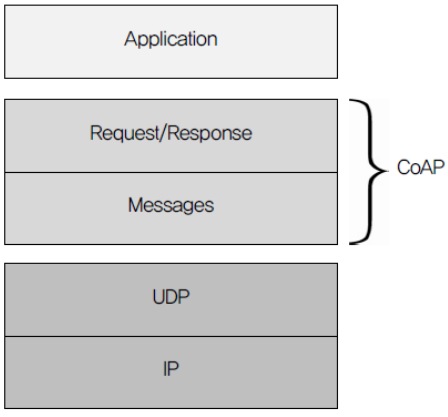

그림 1. CoAP의 추상적 계층
Fig. 1. Abstract layer of CoAP

HTTP 위에서 동작하여 호환성을 높이고, 프록시 내부의 캐시기능을 제공하여 기존의 통신망에 있는 HTTP 영역의 노드들(Non-Constrained Node)과 CoAP 영역에 있는 노드(Constrained Node)들 간에 프로토콜 변환의 역할을 할 수 있다. 그림 2은 CoAP의 메시지 포맷을 나타낸다.

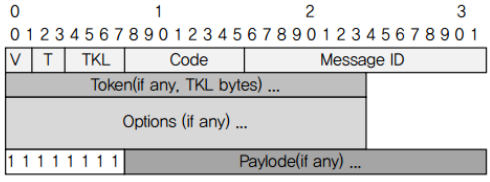

그림 2. CoAP 메시지 포맷
Fig. 2. CoAP message format

통신과정을 위해 CoAP는 확인형, 비확인형, 승인, 리셋의 4가지 메시지 타입을 정의하고 있다. 기본적으로 요청(request)과 응답(response)의 상호작용으로 전달되며 각 메시지 ID를 이용하여 신뢰성 메시지 전송과 비확인성 메시지 전송을 수행하여 동작에 필요한 프록시 동작, 서비스 및 리소스 탐색 방법, 멀티캐스트, HTTP 연계 등을 수행한다. 그림 3은 신뢰성, 비신뢰성 메시지 전송을 나타낸다.

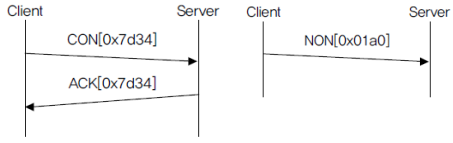

그림 3. CoAP의 메시지(신뢰성, 비신뢰성) 전송
Fig. 3. CoAP message (reliable, non-reliable) transfer

CoAP 요청에 따른 응답은 토큰 이라는 필드를 통해 서로 짝을 이루며, 유지된 토큰을 이용하여 Sleep 모드에 들어간 M2M Device에 대한 뒤늦은 지연에 대해 응답 처리할 수 있다. Http 기반 Get, Post 요청 방식을 지원하기 때문에 서버의 자원 접근이 용이하며, 링크 포맷 표준에 여러 대의 센서에 대한 링크 정보를 포함하여 센서 간에 데이터 공유 기능을 수행할 수 있다.

Ⅲ. 제안하는 기법

1. M2M 환경 구성도 및 가정사항

본 논문에서 정의하는 M2M 환경 구성은 그림 4와 같다. 표준에서 정의하는 M2M Device, M2M Gateway, M2M Server를 포함하며 서비스 구성요소에 요구되는 가정 사항은 다음과 같다.

1. 서비스 1:1 또는 1:N 구성으로 상호 응용되어 사용자에게 통합된 스마트 융합 서비스 제공이 가능하다.
2. M2M Device는 상호인증에 필요한 키 교환을 위한 고유한 파라미터 전달을 위해서 사용자 등록을 반드시 한번 이상 수행해야 한다.
3. 표준에서 통합되는 M2M 플랫폼으로 인해 단일 또는 다중 Device가 각 다른 서비스에서 연동될 수 있다.
4. M2M 게이트웨이는 프로토콜 수행에서 유지해야 할 세션 및 식별자 등을 저장하고 유지 할 수 있는 저장 공간이 존재한다.
5. 서버는 M2M 플랫폼 표준에서 정의하는 사용자 정의 프로필과 키 관리 기능을 제공하며 신뢰된 서버로 가정한다.
6. 서버는 M2M 플랫폼으로 통신하는 모든 M2M Device에 대해 최소한의 식별정보를 저장하고 있다. 이는 사용자 등록단계에서 수행된다.
7. 모든 통신과정은 사용자 등록(키의 생성) 단계이후 키 갱신 및 키 폐지 등 모든 과정을 자동으로 수행한다.

2. 키 교환 및 암호화 알고리즘 정의

서비스 등록 과정에서 사용되는 키 교환 알고리즘은 디피-헬만 공개키 교환을 수행하고, 암호화 알고리즘은 다수 Device 간 통신의 성능을 고려하여 타원곡선 암호(Elliptic curve cryptography) 기반의 ElGamal 공개키 암호 표준을 사용한다.

유한체 GF(2p)를 기반의 타원곡선은 이동통신기기 기반의 환경에서 VLSI chip 같은 특수목적 연산장치(Chip)에 구현에 적합하다. 표 2은 본 논문에서 사용되는 암호화 알고리즘에서 사용되는 파라미터를 나타낸다.

표 2. 암호화 알고리즘 파라미터
Table 2. The encryption algorithm parameters

No.	Parameters	Description
1	DevicePu_Key	Device's Public Key
2	ServerPu_Key	Server's Public Key
3	DevicePr_Key	Device's Private Key
4	ServerPr_Key	Server's Private Key
5	M	Identification Message
6	K_G	KeyGroup
6	r	Random Number(Session Key)
7	D_S_1, D_S_2	Deivce's Digital Signature
8	S_S_1, S_S_2	Server's Digital Signature
9	Ts	Time Stamp
10	D_C	Device's CiperText
11	S_C	Server's CiperText

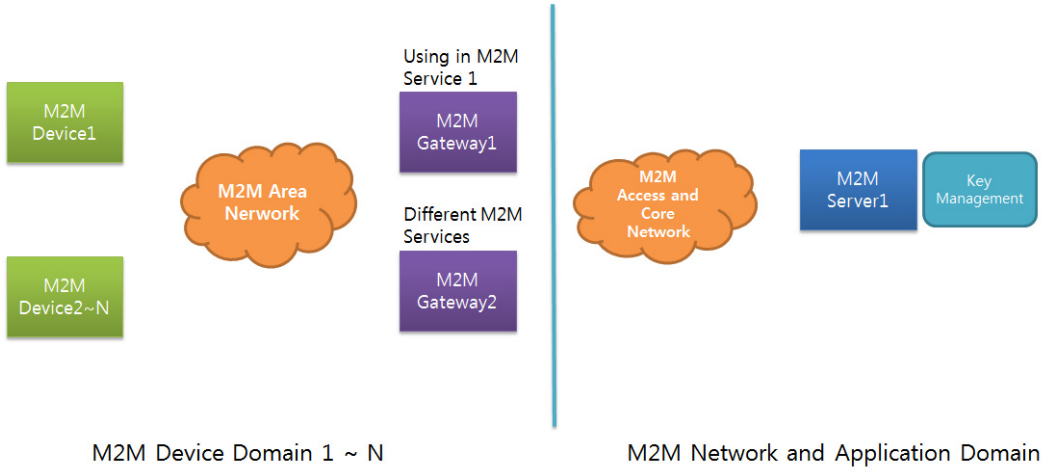

그림 4. M2M 환경 구성도
Fig. 4. M2M environment Configuration

각 개인키와 공개키의 생성은 ElGamal 기반의 타원곡선 알고리즘, 타원곡선 기반의 디지털 서명 구조(ECDSA)를 이용하고, 해쉬 함수는 SHA-1 160비트를 사용한다. 서명값은 동기화과정 이전에 제 3자가 메시지를 가로채어 저장한 후 재전송 공격을 방지를 위한 타임스탬프를 포함한다. 표 3은 각 키 생성과 디지털 서명을 생성하는 방법을 나타낸다.

표 3. 개인키, 공개키, 서명, 암호문 생성
Table 3. The private key, public key, signature, generating cipher text

No.	Parameters	Description
1	DevicePr_Key	163bit Interger Number
2	DeivcePu_Key	$E_1(a_1, b_1)$ $E_2(a_2, b_2) = E_1(a_1, b_1) \times$ DevicePr_Key
3	ServerPr_Key	163bit Integer Number
4	ServerPu_Key	$E_1(a_1, b_1)$ $E_2(a_2, b_2) = E_1(a_1, b_1) \times$ ServerPr_Key
5	D_S_1, D_S_2	$D\_S_1 = r \times (E_1(a_1, b_1)\|\|Ts)$ $D\_S_2 = (h(M\|\|Ts) + DevicePr\_Key \times D\_S_1)r^{-1} \bmod q$
6	S_S_1, S_S_2	$S\_S_1 = r \times (E_1(a_1, b_1)\|\|Ts)$ $S\_S_2 = (h(M\|\|Ts) + ServerPr\_Key \times S\_S_1)r^{-1} \bmod q$
7	r	Random Number
8	D_C	$D\_C = M + r \times E_2(a_2, b_2)$ $M = D\_C - (DevicePr\_Key \times D\_S_1)$
9	S_C	$S\_C = M + r \times E_2(a_2, b_2)$ $M = S\_C - (ServerPr\_Key \times S\_S_1)$

모듈로 p 덧셈연산으로 얻는 타원곡선을 Ep(a, b)로 정의한다. 공개키로 선언되는 파라미터는 사전에 동의한 타원곡선p, E1(a1, b1), E2(a2, b2)이다.

3. 프로토콜 단계 및 보안 메카니즘

프로토콜의 통신단계는 서비스 요청, 사용자 등록, Device 추가, 데이터 공유, 해제 총 5가지 단계를 수행한다.

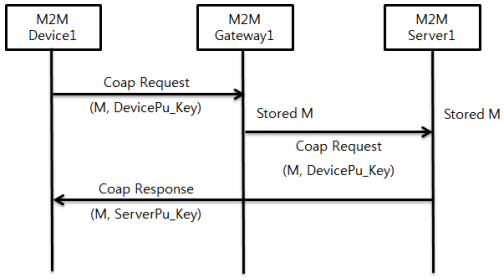

그림 5. 서비스 요청 단계
Fig. 5. Service Request step

① 서비스 요청 단계

사용자 등록이전의 요청 메시지는 CoAP의 메시지 ID(M)를 전송하여 식별을 수행한다. 사용자 등록과정에서 필요한 키를 생성하고 교환하기 때문에 등록과정 이전에 교환하는 요청 메시지는 단순히 식별 가능한 메시지를 사용한다. 그림 5는 서비스 요청 단계를 나타낸다.

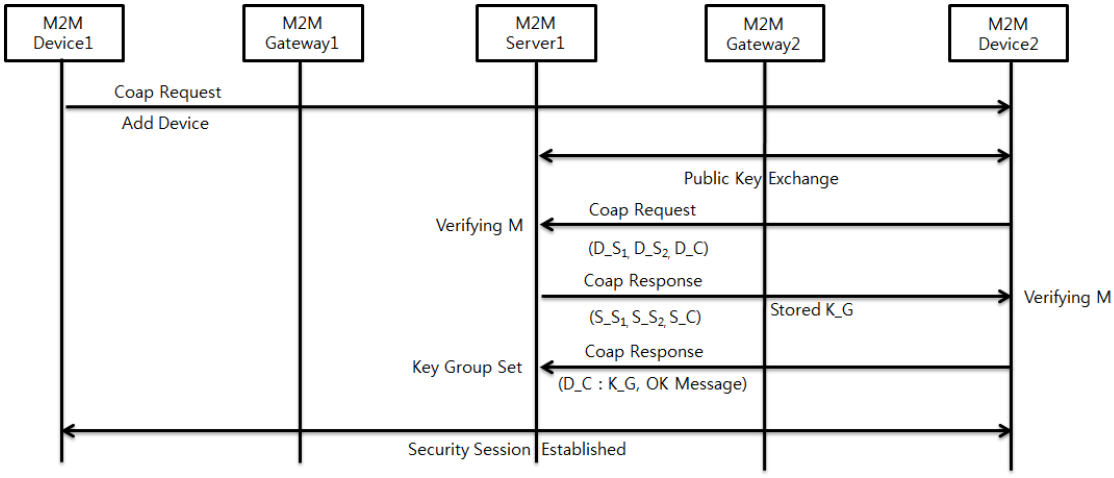

그림 7. 데이터 공유를 위한 Device 추가 단계
Fig. 7. Device additional steps for data sharing

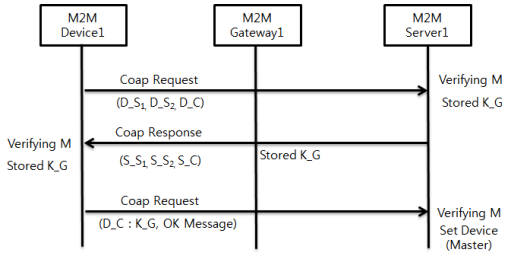

그림 6. 초기 사용자 등록 단계
Fig. 6. The initial registration phase

② 초기 사용자 등록 단계

초기 사용자 등록을 위해 올바른 M2M Device로 통신하는지 확인할 필요가 있기 때문에 상호인증을 위한 키 교환 사전단계를 수행한다. Device에서 전달받은 식별 메시지는 공개키와 맵핑하여 게이트웨이와 서버에 저장하고 이후 암호화된 메시지를 서버로 전송한다. 서버는 M2M Device 식별 값들을 저장하고 이후 통신에서 키 갱신 마다 식별 값들을 확인하여 올바른 Device와 통신하는지 확인한다. 사용자 등록 단계에서 처음 등록된 Device는 마스터 Device로 지정한다. 그림 6는 초기 사용자 등록 단계를 나타낸다.

서명 값은 r값과 타원곡선 상에 선택된 좌표의 곱에 의해 생성되는 값으로 제 3자가 메시지를 가로채어 저장한 후 재전송 공격을 방지를 위한 타임스탬프를 포함한다. 각 생성된 암호문은 평문 M, 임의의수 r, 타원곡선 상의 점 E2을 이용하여 암호화를 진행하고, 복호화의 경우 자신의 개인키와 각 전송받은 서명을 이용하여 복호화를 진행한다.

③ 데이터 공유를 위한 Device 추가 단계

사용자는 각 다른 서비스의 Device를 추가하여 M2M 서비스를 이용할 수 있다. 신뢰된 M2M 서버를 통하여 새로운 Device에 대한 요청을 수행한다. 추가 Device는 등록단계와 동일하게 안전한 상호인증을 위한 공개키 교환과 암호문을 교환한다. 초기 등록한 마스터 Device 키 그룹에 Device를 추가하고, 서버로부터 생성된 새 세션키를 갱신하여 암호문을 교환하고 통신을 진행한다. 그림 7는 데이터 공유를 Device 추가 단계를 나타낸다.

④ Device 간 데이터 공유 단계

인증된 Device에 대한 보안 세션이 설립된 이후 데이터 공유를 위해 서버는 새로운 세션키를 생성하여 각 Device와 새션키가 포함된 암호문을 교환한다. 여기서 생성된 세션키는 기존의 서명 생성시 사용한 r값을 갱신하여 연산을 수행한다. 그림 8는 Device 간 데이터 공유 단계를 나타낸다.

⑤ 서비스 및 Device 해제 단계

해제단계는 마스터 Device가 해제되어 연동된 Device가 모두 해제되거나 특정 Device가 해제되는 경우를 의

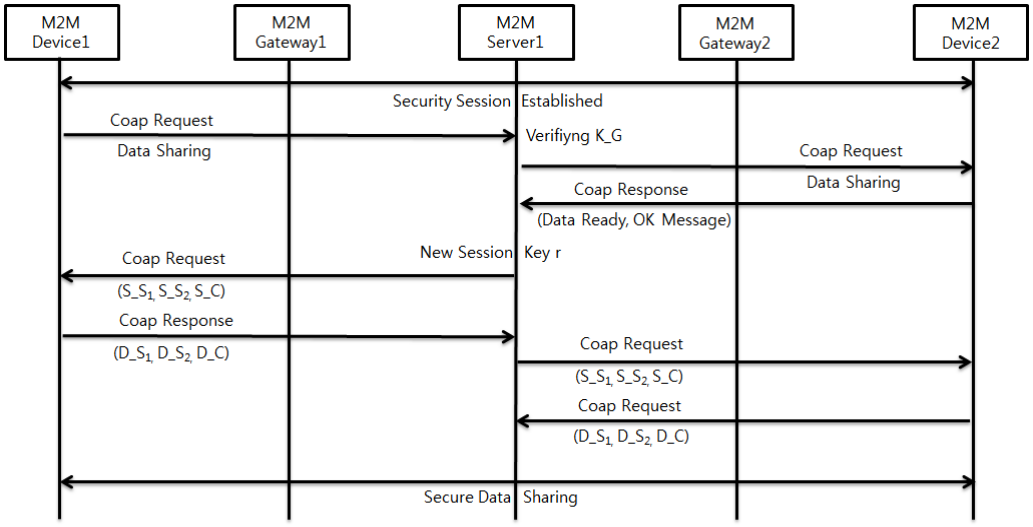

그림 8. Device 간 데이터 공유 단계
Fig. 8. Device data sharing between steps

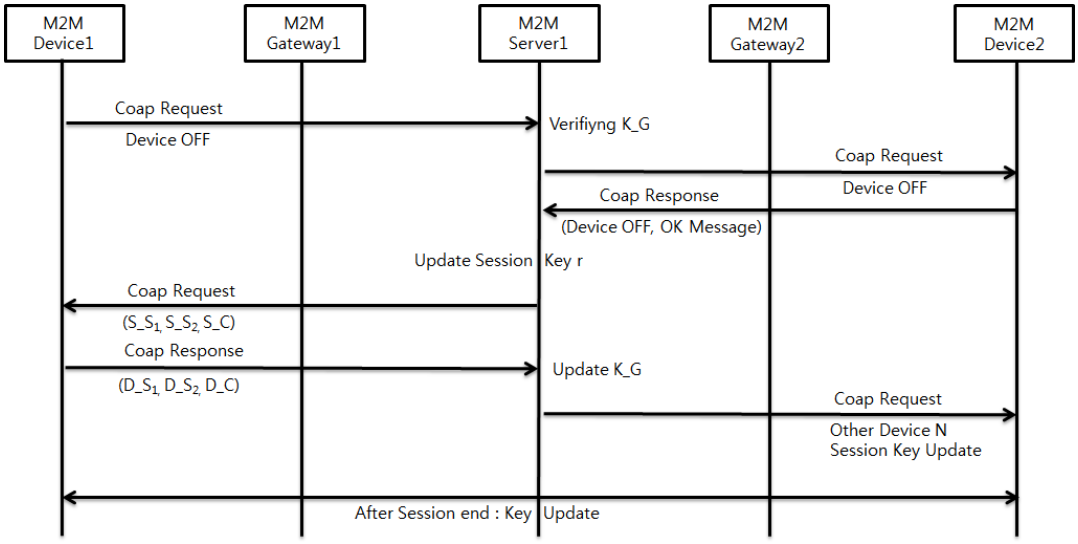

그림 9. 서비스 및 Device 해제 단계
Fig. 9. Service and Device off stage

미한다. 마스터 Device를 해제할 경우 초기 등록에서 설정된 키 그룹에 추가된 모든 Deivce에 대한 키를 폐지하고, 특정 Device의 경우 기존 보안 세션을 유지하고 해제 대상인 Device를 K_G에서 해제한다. 일반적으로 서비스 이용 시 마스터 Device는 사용자가 해제하지 않고, 세션을 유지하면서 특정 Device를 추가하거나 해제하는 형태로 사용되기 때문에 마스터 Device의 키 갱신은 Device의 종료(꺼짐), 기지국의 이동(핸드오버), 사용자의 요청(재등록)의 경우 키를 폐지하도록 한다.

해제 이후 공유 단계와 동일한 세션키 갱신을 수행하여 세션 재설립과 키그룹 갱신을 통해 안전한 데이터 공유를 진행한다. 그림 9는 서비스 및 Device 해제 단계를 나타낸다.

Ⅳ. 안전성 분석

본 장에서는 M2M 서비스 보안 요구사항 항목에 따른 제안하는 프로토콜의 안정성을 분석한다.

1. 인증키 관리 기능

M2M 서버 플랫폼의 데이터 공유를 위한 키 교환을 통해 정당한 Device 인지 상호인증을 수행할 수 있도록 RSA 1024bit의 안정성에 준하는 163bit 키 길이의 타원곡선 알고리즘을 사용하였다. 알고리즘 내에 사용된 타원곡선 기반 서명용 개인키의 보안성은 공격 시도의 제한이 없는 오프라인 수준에서 RSA와 동일한 수준인 1024bit의 키에 대하여 $(1/2)^{1024} \times 100\%$ 수준의 공격 성공률을, 2048bit의 키에 대하여 $(1/2)^{2048} \times 100\%$ 수준의 공격 성공률로 공격이 어렵다. 프로토콜 내 사용된 타원곡선 알고리즘의 개인키 163bit 키를 증가시킬 경우 알고리즘 수준의 복잡도를 배수 단위로 증가시킬 수 있다. M2M 서버는 기존 신뢰할 수 있는 기관인 CA와 같은 개념으로 전 동작과정에 사용자의 개입 없이 키의 생성과, 갱신, 폐지 등 키 관리를 수행할 수 있도록 하였다.

2. 인증, 권한설정

초기 사용자 등록 단계를 통해 Deivce의 데이터 공유 이전에 각 Deivce 간 상호인증을 수행하며, 생성된 인증키는 첫 식별자 M과 공개키 교환이외에 모든 과정이 암호화되어 교환되기 때문에 안전하다고 할 수 있다. 공격자는 설립된 보안 세션에 대하여 Device나 서버로 위장하더라도 각 생성된 암호문에서 사용된 개인키의 역원값을 알지 못하므로 올바른 메시지와 세션키를 유추할 수 없다. 또한 각 다른 Device의 통신 내용의 암호화를 위해 데이터 공유시 새로운 세션키를 생성하고, 사용자가 요청한 동일한 Device에 대한 키 그룹인지 확인하여 Device간에 접근권한을 인가할 수 있도록 하였다.

3. 데이터 무결성 체크

데이터 암호화 내 데이터 무결성을 위해 생성된 서명 내에 메시지와 타임스탬프를 포함하여 해쉬함수를 사용한다. 타임스탬프는 재사용 공격을 방지한다. Device와 서버의 식별자, 공개키 이외에 모든 메시지가 갱신된 세션키를 암호화되어 전송되기 때문에 이전 세션에서 수집한 메시지를 다음 세션에 재사용하는 재사용 공격에 안전하다. 적용된 SHA-1이외에 적용될 수 있는 대칭키 알고리즘으로는 DES, 3DES, RC4 등 환경의 특성에 따라 확장하여 적용될 수 있다. 사용자가 초기에 등록하는 Device를 마스터로 설정하여 다른 서비스에서 추가되는 Device인 경우라도 서버에서 세션키를 포함한 서명을 이용하여 암호화하고 분배하기 때문에 전 과정에 무결성 체크를 모두 충족한다. 서명에 생성되는 연산의 효율성을 위해 세션키만을 갱신하여 알고리즘을 수행한다. 서명을 다시 생성하는 경우는 Device가 해제 된 경우만 수행하도록 하여 연산의 오버헤드를 최대한 감소시켰다.

V. 결론

M2M 환경은 보안기능 제공에 앞서 Device의 통신 모듈의 성능적인 부분에 대한 표준화가 반드시 고려해야 한다. 최근 M2M 기술이 다양한 응용 분야로 확대될 것으로 예상하고 있지만, 현재 표준은 모듈 스펙과 보안기능 적용에 대한 요구사항에 대하여 아직 정의되어 있지 않다. 앞으로 M2M 통신 환경의 특징으로 인해 개인 휴대용 단말기뿐만이 아닌 홈 네트워크, 웨어러블 등 사용자의 실생활에 확대되는 보안위협들을 예방·차단을 위해서는 빠른 표준화 진행에 따른 보안기술 도입이 선행되어야 한다.

본 논문에서는 서비스 사용자 시점으로 M2M 환경구성과 Device 간 데이터 공유에 대한 보안요구사항을 분석하고, 사용자 등록부터 통신, 폐지 등 키 관리에 대한 전반적인 과정에 대한 보안 메카니즘을 제안하였다. 제안하는 프로토콜은 상호인증 및 데이터 무결성, 재사용 공격 등 M2M 보안요구사항을 충족하며 기존 연구들에 비해 가벼운 타원곡선 기반 알고리즘을 사용하여 M2M 응용 분야에 보다 안전한 보안 메커니즘으로 활용할 수 있을 것으로 예상한다.

References

[1] TTA, “Mobile networks based M2M and International Standards Report”, Electronics and Telecommunications Research Institute, Electronic and Telecommunications Trends, Vol 26 No.2, 2011

[2] ETRI, “Trends of Converging Smart Devices with IoT Technology”, Electronic Communication Trends Analysis, 2013.

[3] Machina Research, "GSMA & Machina Research", 2011

[4] Machina Research, "M2M Cummunication in sectors", 2011

[5] Machina Research, "M2M Communication in CE 2010-2020", 2011

[6] ITU-T, "http://www.itu.int/en/ITU-T/focusgroups/m2m/Pages/default.aspx", 2013

[7] 3GPP, "Study on security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements", 2014

[8] ETSI, "TS 102 689 - V2.1.1 - Machine-to-Machine communications", 2013

[9] Z. Shelby, K. Hartke, and C. Borman, “Constrained Application Protocol (CoAP),” draft-ietf-core-coap-18 (work in progress), IETF, June 2013

[10] Tien-Dung Nguyen, Eui-Nam Huh, "A Dynamic ID-based Authentication Scheme for M2M Communication of healthcare Systems", The International Arab Journal of Information Technology, Vol 9, No 6, 2012

[11] Jie-Ren Shih, “Securing M2M With Post-Quantum Public-Key Cryptography”, Emerging and Selected Topics in Circuits and Systems, IEEE Journal on Volume:3 , Issue: 1

[12] Eun Seon Gi, “Mutual Authentication and Key Establishment Protocol to Implement Secure M2M Communication Environments”, Korean Institute of Information Security, Vol 20. No.1, 2010.2, 73-83 (11 pages)

[13] Mui Van Nguyen, Al-Saffar, A. ; Eui-Nam Huh, "A dynamic ID-based authentication scheme", Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on, 2010
[14] ETSI TS 102 921 V1.1.1, "Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces", 2012
[15] Dennis Fu, "CCF M2M Certification: Demystifying the testing for M2M devices", CDMA Certification Forum, 2012
[16] VerSign, "VeriSign Cable Modem Authentication Service", http://www.verisign.com/stellent/groups/public/documents/data_sheet/005349.pdf, 2005
[17] Z. Shelby, "Constrained Application Protocol (CoAP)draft-ietf-core-coap-18", IETF", 2013
[18] ETSI TS 102 689 v1.1.1, 'Machine-to-Machine communications(M2M); M2M service requirements', 2010
[19] C. Bormann, "CoRE Roadmap and Implemen tationGuide", draft-bormann-core-roadmap - 05", IETF, 2013
[20] Z. Shelby, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18, IETF, 2013

저자 소개

박 중 오(정회원)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 현재 : 동양미래대학교 조교수

- 관심분야 : PKI, Network security, 암호학
- E-mail : jopark13@dongyang.ac.kr

김 상 근(정회원)

- 1996년 : 중앙대학교 컴퓨터공학과 (공학박사)
- 2003년 ~ 2004년 : Sydney University, 방문교수
- 1996년 ~ 현재 : 성결대학교 컴퓨터 공학부, 교수

- 관심분야 : PKI, 정보보안, 소프트웨어공학
- E-mail : sgkim@sungkyul.ac.kr