Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 4 pp. 1926-1934, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.4.1926

M2M 환경에서 신원기반 암호기법을 활용한 인증기법에 관한 연구

진병욱[1*], 박재표[2], 이근왕[3], 전문석[1]
[1]숭실대학교 컴퓨터학과, [2]숭실대학교 정보과학대학원, [3]청운대학교 멀티미디어학과

A Study of Authentication Method for Id-Based Encryption Using In M2M Environment

Byung-Wook Jin[1*], Jae-Pyo Park[2], Keun-Wang Lee[3] and Mun-Seok Jun[1]
[1]**Department of Computer Science, SoongSil University**
[2]**Graduate School of Information Science, SoongSil University**
[3]**Department of Multimedia Science, ChungWoon University**

요 약 M2M(Machine-to-Machine Communication)은 한 기기가 비슷한 다른 기기와 유선 혹은 무선으로 통신하는 기술로서 환경의 특성 상 저전력, 소규모, 저렴한 가격, WAN, WLAN 등 네트워크를 통하여 사물간의 통신으로 정의하고 있다. 또한 사람의 개입이 없이도 운영이 가능할 수 있는 특징이 요구된다. 그러나 사물통신 기기들의 요구사항으로 인하여 무선 통신 등에 취약점은 가지게 되고, 각 기기를 관리 혹은 제어하는 것에 대한 어려움으로 인한 취약점이 있다. 본 논문은 M2M 환경에서 Device 및 Gateway와 Network Domain간의 안전한 인증 프로토콜 기법을 제안하였다. 제안 프로토콜은 ID-Based Encryption 기반으로 인증 하며, Network Domain안에 Access Server 및 Core Server 간의 세션키를 생성한다. 그리고 생성한 세션키를 활용하여 상호간에 데이터를 송·수신하고, 키 갱신 프로토콜을 추가하여 자동으로 식별값을 갱신한다.

Abstract M2M (Machine-to-Machine Communication) refers to technologies that allow wired and wireless systems to communicate with other devices with similar capabilities. M2M has special features which consist of low electricity consumption, cheap expenses, WAN, WLAN and others. Therefore, it can communicate via a network. Also, it can handle itself without a person's management. However, it has a wireless-communicate weakness because of the machine-communicate request, and also it is difficult to administrate and control each other. So In this Paper, It suggests the safety protocol between Device, Gateway and Network Domain in M2M environment. Proposed protocol is based on ID-Based encryption's certificate and creates session key between the Access Server and the Core Server in the Network Domain. It uses that session key for sending and receiving data in mutual, and adds key renewal protocol so it will automatically update discern result. a comparative analysis of the existing M2M communication technologies and PKI-based certificate technology is compared with the proposed protocol efficiency and safety.

Key Words : Machine-to-Machine(M2M), ID-Based Encryption, Authentication

1. 서론

M2M은 사람이 개입하지 않는(혹은 최소 개입)상태에서 Machine/Machine간에 일어나는 통신이다. 특징이 비슷한 통신기기들이 유·무선으로 통신하는 기술을 지칭하며, 사물지능통신이라고 한다. M2M통신의 특성 상, M2M통신기기는 저전력, 소규모, 저렴한 가격, WAN, WLAN 등 네트워크를 통한 통신, 그리고 사람의 개입이

*Corresponding Author : Byung-Wook Jin(SoongSil Univ.)
Tel: +82-10-2690-2780 email: quddnr4511@naver.com
Received March 19, 2013 Revised April 8, 2013 Accepted April 11, 2013

없이도 운영이 가능할 수 있는 등의 특징을 요구한다[1,2].

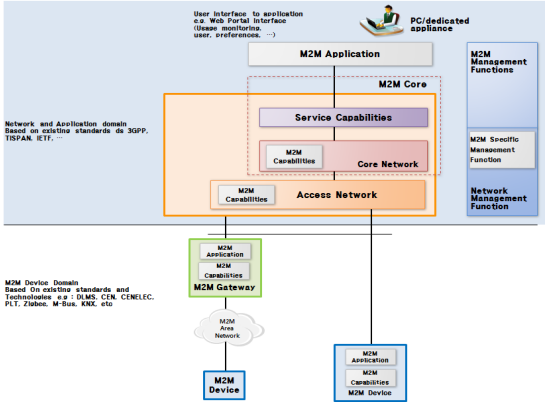
M2M 기기는 원격지 또는 보안이 취약한 장소에 설치되어 오랜 기간 동안 사용이 되며, 기능 수행을 위하여 관리가 필요하다. 또한 많은 예상사용 환경(Use Case)에서 사물통신의 구축에 있어 매우 많은 M2M 기기들이 필요하며, 이동형(Mobile)기기들도 많고, 각 개별 기기를 관리 혹은 제어하는 것은 비현실적이거나 불가능에 가깝다[3]. 이와 같은 사물통신 기기들의 요구사항들로 인하여 사물통신기기들은 무선 통신 등에 있어서 취약점을 갖게 된다. 또한 M2M환경은 사물통신 기술의 특성 상, 사람이 개입하지 않은 채 기기들 간의 상호 통신에 의하여 이루어지므로 각 기기 간 상호 인증을 하기 위한 인증기술을 요구한다. 따라서 본 논문은 사물통신기기의 안전한 인증과 M2M Network Domain의 기기 등록 및 인증기능을 설계하여 안전한 인증 기법 설계를 제안한다.

2. 관련연구

2.1 M2M(Machine to Machine)

2.1.1 M2M 통신 구조

M2M을 연구하고 있는 ETSI는 M2M 구조를 연구하고 있다. M2M의 통신 구조를 M2M Device, M2M Device Domain, M2M Gateway Domain, 그리고 M2M Network Domain으로 분류한다[8].



[Fig. 1] Functional Structure of M2M communication

(1) M2M Device Domain

M2M Device Domain은 M2M Device와 M2M Area Network로 구성된다. M2M Area Network는 M2M Device와 M2M Gateway 사이에서 연결을 제공하는 네트워크이다. IEEE 802.15, Zigbee, 블루투스 등의 PAN(Personal Area Network) 또는 PLC, M-BUS, Wireless M-BUS, KNX 등의 LAN(Local Area Network) 등의 통신 기술이 사용된다[1,8].

(2) M2M Gateway

M2M Gateway는 M2M Application과 M2M Capabilities로 구성되어 있다. M2M Gateway는 M2M Application과 M2M Capabilities를 이용하여, M2M Device들의 상호 작용을 보호한다. 또한 M2M Device가 Network Domain의 Access Network에 접근하도록 Gateway 역할을 제공한다[1,7].

(3) M2M Network Domain

M2M Network Domain은 접속 네트워크(Access Network), M2M 코어(Core), 전송 네트워크(Transport Network), M2M 응용분야(Application) M2M 관리 기능(Management Function), 네트워크 관리 기능(Network Management Function)등으로 구성된다. 접속 네트워크는 M2M Device Domain과 M2M Core Network간 통신을 할 수 있는 기능을 제공한다. M2M 코어는 코어 네트워크(Core Network)와 서비스 제공기능(Service Capabilities)으로 구성되고, M2M 통신에 있어 핵심적인 역할을 담당한다. M2M 응용분야는 M2M통신을 이용하여 수집된 정보를 가공하여 제공하는 인터페이스 등을 의미한다. M2M 관리 기능과 네트워크 관리 기능은 M2M 통신 구조 전반과, 네트워크 통신 기술 등을 관리한다[3,6].

2.1.2 M2M 통신 사용 환경별 인증 기술의 요구조건

M2M통신 환경에서는 각 사용 환경 별 요구사항을 규정하고 요구사항을 충족시키는 인증기술을 선택하는 것이 현실적이긴 하다. 사물통신 환경에서 인증기술의 일반적인 요구사항은 다음과 같이 도출할 수 있다[2,7].

- 디바이스 인증

M2M통신 환경에서 통신 서버는 전송 및 수신하고자 하는 데이터가 정당한 M2M 디바이스로부터 송·수신되었는지 여부를 식별 및 인증할 수 있어야 한다.

- 서버 인증

M2M통신 환경에서 M2M통신 디바이스 혹은 게이트웨이는 통신하고자 하는 M2M통신의 서버가 정당한 서버인지 등의 여부를 식별 및 인증할 수 있어야 한다.

• 통신 내용의 암호화

M2M통신 환경에서 따라 이루어지는 통신 내용은 개인정보 및 유출 시 사회적 및 금융적으로 피해가 예상되는 데이터일 경우 반드시 데이터의 암호화를 통하여 기밀성 및 무결성을 제공해야 한다.

• 부인 방지

M2M 통신의 인증 기술은 M2M 디바이스 및 게이트웨이를 사용하는 사용자 등이 데이터의 정당성을 부인할 수 없는 수단을 제공할 수 있어야 한다.

• 기타 환경과의 호환성

M2M통신 환경에서 사용되는 인증 기술은 기타 도메인 디바이스 등과 호환되어야 한다.

• 인증기술의 효율성

M2M 통신 환경에서 사용되어 지는 인증 기술은 기존 디바이스의 성능의 제약 및 기기의 성능을 고려야한다. 그러므로 모든 디바이스에서 사용될 수 있는 경량 화된 인증기술을 고려하여야 한다.

이와 같은 일반적인 인증기술의 요구사항 외에도, 각 사용 환경의 보안의 중요성에 따라 서로 다른 보안의 요구 사항이 예상된다. 따라서 각 환경에 M2M통신 기술의 도입 시, 예상 가능한 보안 위협 및 이를 방지하기 위한 인증기술의 요구사항의 도출이 필요하다[16].

2.2 신원 기반의 암호시스템 (Identity Based Encryption)

2.2.1 신원 기반의 암호 시스템의 개요

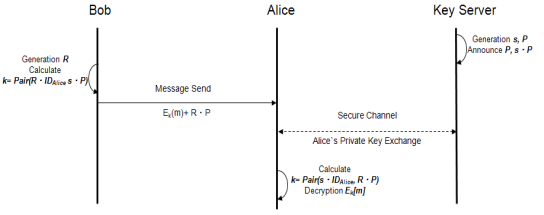
1984년 Adi Shamir가 새로운 공개키 증명을 제안한 방식이다. 암호 시스템은 사용자의 신원정보를 사용자의 공개키로 활용하는 것으로 기존의 공개키 방식의 복잡한 키 값을 대체하는 것이다. 사용자의 신원 정보를 이용하여 TTP(Trust Third Party)는 신원 정보에 대응한 개인키를 생성하고 이를 사용자에게 안전하게 전송한다. 단 TTP는 절대적으로 신뢰되어야 한다. 사용자의 신원정보로부터 개인키를 유도하는 과정은 전적으로 TTP에 의해 수행되어야 한다. 신뢰기관은 사용자 사이의 분쟁이 있을 경우에는 각 사용자의 개인키를 생성한 기관으로서 분쟁의 중재자 역할을 수행한다. Adi Shamir의 제안에서 전자서명에 대한 방식이 제안되었으나, 신원 정보 기반의 암호 전달 알고리즘은 제안 되지 못하고 단지 개념만이 제시되었다.

2.2.2 Pairing 기반의 신원 기반 암호 시스템

2001년에 Dan boneh와 Matt Franklin은 타원 곡선에서 기초한 Weil Pairing 기반의 신원 기반 암호 시스템을 제안함으로써 실질적인 구현방안을 제시하였다. Bilinear map이라고 불리는 수학적 구조를 적용하여 신원기반의 암호를 구현하였다[10].

$$Pair(a \bullet X, b \bullet Y) = Pair(b \bullet X, a \bullet Y)$$

위의 식에서 사용된 연산자 • 는 타원 곡선상의 점들의 곱을 나타낸다. 곱셈 그 자체는 용이하지만 X와 $a \bullet X$를 알고 a를 찾는 역산은 불가능하다. 키 서버는 난수로부터 s와 P를 생성하고 P와 $s \bullet P$ 값은 모든 사용자에게 공지한다. 다음 사용자 x의 개인키인 $s \bullet ID_x$를 계산하여 사용자에게 전달한다. 이 값들을 이용한 암호문 절차는 다음 Fig. 2과 같다.



[Fig. 2] Pairing based Identity Encryption

송신자 Bob은 임의의 난수 r을 정하고 다음과 같은 대칭키를 계산한다.

$$k = Pair(r \bullet ID_{Alice}, s \bullet P)$$

여기서 사용되는 $s \bullet P$ 는 키 서버가 공지한 값이고, $r \bullet ID_{Alice}$는 계산 값으로 전부 공개된 값을 이용한 것이다. 다음 메시지 m에 대하여 생성된 키 k로 암호화 한다. 수신자 Alice에게 암호문 $E_k[m]$과 $r \bullet P$를 전송한다. 수신자 Alice는 보호를 위해 복호키를 다음과 같이 계산한다.

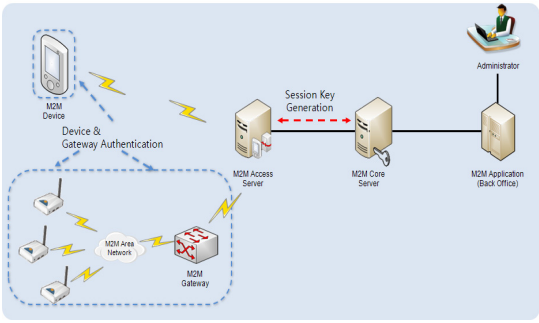
$$k = Pair(s \bullet ID_{Alice}, r \bullet P)$$

생성되는 복호용 키는 $s \bullet ID_{Alice}$라는 Alice에게 배포된 Alice의 개인키이며, $r \bullet P$는 Bob이 Alice에게 전송한 값이다. 개인키 값은 Alice만이 알고 있는 값으로 암호문의 복호화는 Alice만이 가능하다[12-17].

3. ID-Based Encryption을 활용한 M2M Device 및 Gateway 인증 기술

3.1 제안시스템

본 논문에서 제안하는 시스템은 ID-Based Encryption을 활용하여 안전한 인증 프로토콜을 설계한다. 우선 Network Domain에서 M2M Access Server와 M2M Core Server간에 세션키를 생성 후 생성된 세션키를 사용하여 M2M Device 및 Gateway와 Access Server 간의 기기 등록 및 인증을 하는 방식이다. 또한 키 갱신 프로토콜을 추가하여 Device 및 Gateway 와 Server 자동으로 키를 갱신한다. 전체 구성도는 다음 Fig. 3과 같다.



[Fig. 3] Configuration of the entire system is also proposed

제안 하는 방식은 다음과 같은 조건을 만족한다.

① M2M Network Domain에서 Access Server는 Core Server의 Parameter를 알고 있어야 한다.
② M2M Device 및 M2M Gateway는 설치되어 지기 전에 M2M Core Server에 Serial Number가 등록되어야 한다.

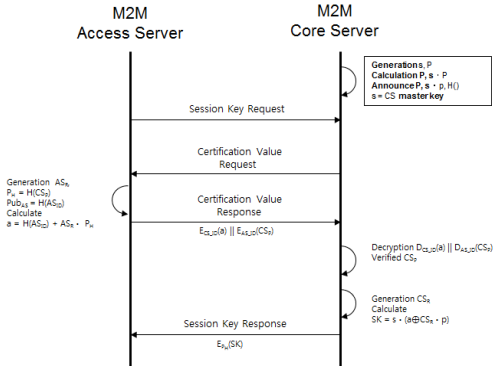
3.2 세션키 생성 프로토콜

M2M Network Domain에서 Access Server와 Core Server간에 상호간의 인증을 할 수 있는 세션키를 생성해야 한다. 세션키는 ID-Based Encryption 기반의 세션 키 생성 프로토콜을 제안한다. 다음 Table 1은 세션키 생성 프로토콜, 기기 등록 및 인증 프로토콜, 제안 시스템에서 쓰이는 약어를 정리한 것이다.

[Table 2] Summary Abbreviations

Spec.	Respondents
GW	M2M Gateway
AS	M2M Access Server
CS	M2M Core Server
$H()$	Collision Hash Function
AS_R	Access server-generated random number
CS_R	Core Server-generated random number
CS_p	Core Server의 Parameter
GW_{ID}	Generate a Key in ID of GW $Key = (R \cdot GW_{ID}, s \cdot P)$
CS_{ID}	Generate a Key in ID of CS $Key = (R \cdot CS_{ID}, s \cdot P)$
AS_{ID}	Generate a Key in ID of AS $Key = (R \cdot AS_{ID}, s \cdot P)$
SK	Session key of Core Server and Access Server
VG_i	Gateway of valid value
VD_i	Valid Device of identity value
GW_{SN}	Gateway of Serial Number
GW_R	Gateway of Random Number

Access Server와 Core Server 간의 Cert Value 값을 송·수신한다. Core Server는 Cert Value를 검증을 한 후 Access Server로 세션키를 전송한다. 세션키 생성 상세 프로토콜을 보면 다음 Fig. 4과 같다.



[Fig. 4] Session Generation Protocol

① Access Server와 Core Server간의 ID-Based Encryption 기반으로 세션키를 생성한다. 우선 Core Server에서 s, P를 생성 후 $P, s \cdot P$를 계산한다. $P, s \cdot P, H()$를 공개한다. s는 Core Server의 Master Key이다.

② Access Server는 Core Server에게 Session Key를 요청한다.

③ Core Server는 Session Key 요청 메시지를 수신 후 Access Server에게 Cert Value를 요청한다.

④ Access Server는 AS_R을 생성한다. CS_P와 AS_{ID}을 해쉬 함수를 통해 $P_H = H(AS_{ID})$, $Pub_{AS} = H(AS_{ID})$ 을 생성한다. 생성한 값을 아래 식과 같이 계산한다.

$a = Pub_{AS} + AS_R \bullet P_H$

Access Server는 a값을 Core Server의 ID값을 활용하여 $Key = (R \bullet CS_{ID}, s \bullet P)$ 을 생성한 후 암호화 하고 자신의 ID값으로 $Key = (R \bullet AS_{ID}, s \bullet P)$로 CS_P을 암호화한 후 연접하여 Core Server에게 Cert Value 메시지를 송신한다.

$Cert\ Value = E_{CS-ID}(a) \| E_{AS-ID}(CS_P)$

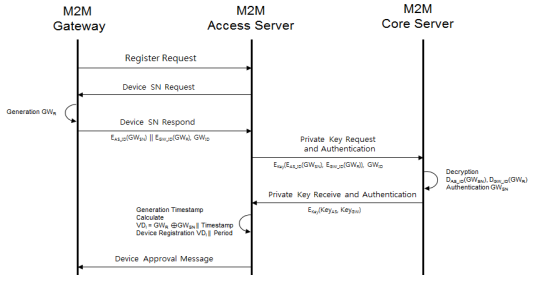
⑤ 수신 받은 Cert Value 메시지를 복호화 하고 CS_P를 검증한다. Core Server에서 CS_R을 생성 후 아래 식 값을 계산 후 세션키 값을 생성한다.

$SK = s \bullet (a \oplus CS_R \bullet P)$

⑥ Core Server는 생성한 세션키 SK를 P_H로 $Key = (R \bullet P_H, s \bullet P)$ 암호화 하여 Access Server에게 발송한다.

3.3 기기등록 및 인증 프로토콜

기기 등록 및 인증 절차를 M2M Gateway 기준으로 설명하면, 우선 Access Server와 Gateway간의 기기 식별 값을 송·수신 후 Core Server에 전송한다. Core Server는 식별 값을 인증 후 Access Server에게 키 값을 전송한다. 이후 Access Server는 키 값으로 식별 값을 복호화하여 Gateway에게 승인 메시지를 전송한다. 기기 등록 및 인증 상세 프로토콜은 다음 Fig. 5과 같다.



[Fig. 5] Device Registration and Authentication protocols

① Gateway가 설치되어지기 전에 Core Server에 Device 및 Gateway의 SN을 등록한다는 가정이 있다. Gateway는 Access Server에게 등록을 요청 메시지를 전송한다.

② Access Server는 Gateway에게 Serial Number 요청 메시지를 전송한다.

③ Gateway는 GW_R을 생성 후 Access Server의 ID로 $Key = (R \bullet AS_{ID}, s \bullet P)$ 생성 후 GW_{SN}을 암호화하고 생성한 GW_R을 자신의 ID로 $Key = (R \bullet GW_{ID}, s \bullet P)$ 값을 생성하여 암호화한 다음 연접하여 GW_{ID}과 같이 전송한다.

$E_{AS-ID}(GW_{SN}) \| E_{GW-ID}(GW_R), GW_{ID}$

④ Serial Number를 수신 받은 Access Server는 세션키 $SK = E_{Key}$ 값으로 암호화하여 Core Server에게 개인키 요청 및 인증 요청 메시지를 전송한다.

$E_{Key}(E_{AS-ID}(GW_{SN}), E_{GW-ID}(GW_R)), GW_{ID}$

⑤ Core Server는 Access Server에게 받은 메시지를 복호화하고 GW_{SN}을 인증한 후 Access Server의 키 값, Gateway의 키 값을 생성하여 세션키로 암호화하여 Access Server에게 전송한다.

$E_{Key}(Key_{AS}, Key_{GW})$

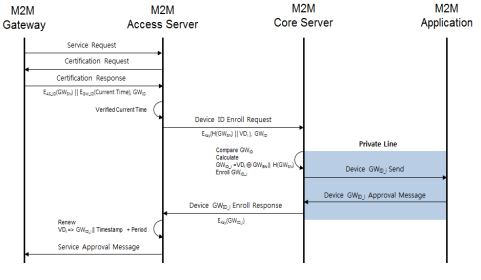
⑥ Access Server 및 Gateway의 키 값을 수신 받은 Access Server는 Serial Number를 복호화한다. 이후 TimeStamp를 생성한 후 VD_i를 생성한다.

$VD_i = GW_R \oplus GW_{SN} \| Time\ Stamp$

⑦ Access Server는 $VD_i \| Period$를 등록 후 Gateway에게 Device 승인 메시지를 전송한다.

3.4 제안시스템 동작

제안 시스템의 상세 프로토콜은 Fig. 6과 같으며 동작은 Gateway는 Access Server에게 서비스를 요청하고 상호간의 기기 식별값을 송·수신한다. Access Server는 식별값을 검증하고 기기 ID값을 Core Server에 전송한다.



[Fig. 6] Detailed protocol of the proposed system

Core Server는 Access 서버에게 ID값을 전송 후, 기존 기기 ID값을 갱신 및 등록 후 서비스 승인 메시지를 Gateway에게 전송한다.

① Gateway는 Access Server에게 서비스를 요청한다.
② Access Server는 Gateway에게 기기 식별값을 요청한다. Gateway는 Access Server의 ID로 생성한 키 값으로 GW_{SN}을 암호화하고, 현재의 시간을 자신의 ID로 암호화하여 Access Server에게 식별값을 전송한다.
$E_{AS-ID}(GW_{SN}) \| E_{GW-ID}(Current\ Time), GW_{ID}$
③ Access Server는 현재의 시간을 검증하고 VD_i, GW_{SN}을 해쉬함수를 통하여 나온 값과, GW_{SN}을 연접하고 세션키로 암호화 후 Core Server에게 등록 메시지를 전송한다.
$E_{Key}(H(GW_{SN}) \| VD_i), GW)_{ID}$
④ Core Server는 GW_{ID}를 비교 후 GW_{ID_i}를 계산한 다음 GW_{ID_i}를 등록 후 Application에게 GW_{ID_i}를 전송한다.
$GW_{ID-i} = VD_i \oplus GW \| H(GW_{SN})$
⑤ Application은 등록 후 승인메시지를 Core Server에게 전송한다.
⑥ Core Server는 GW_{ID-i}를 세션키로 암호화하여 Access Server에게 전송한다.
⑦ Access Server는 VD_i을 갱신하고 Gateway에게 서비스 승인 메시지를 전송한다.
$VD_i = GW_{ID-i} \| Time\ Stamp + Period$

4. 구현 및 비교분석

본 논문에서 구현 된 시스템 환경은 Intel(R) Core(TM) Duo CPU E7400 @ 2.80GHz 4.00GB RAM의 Microsoft Windows 7 Enterprise 32bit에서 Eclipse IDE for JAVA Developers, MY-SQL 5.1.39을 사용하여 구현하였다.

4.1 효율성 비교분석

사물통신 환경에서 PKI 기반을 활용한 인증 기술과 제안 프로토콜의 효율성을 비교하기 위해 처리시간을 비교 분석 하였다. 다음 Table 2는 PKI 기반 인증 기술과 제안한 인증 프로토콜의 기기 등록 효율성을 동작한 회수에 대한 결과값을 비교 분석하여 나타낸 것이다.

[Table 3] Comparative analysis of the efficiency of the device registration

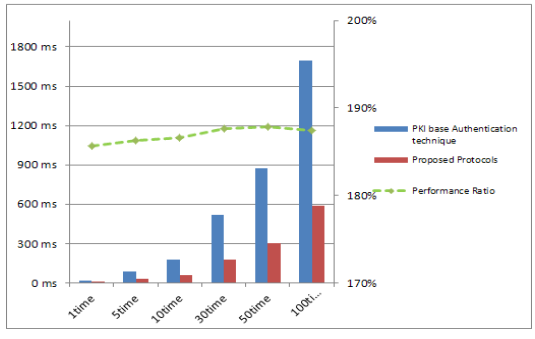
Division	PKI based Authenticaion technique	Proposed authentication Protocol
1 time	18 ms	6.3 ms
5 time	87.9 ms	30.7 ms
10 time	175.4 ms	61.2 ms
30 time	519.4 ms	180.6 ms
50 time	872.7 ms	303.2 ms
100 ime	1698.2 ms	590.9 ms

M2M Network Domain에서 Access Server와 Core Server간의 키 생성 프로토콜을 통해 나온 세션키를 활용하여 기기등록을 하였으므로, 기존의 PKI 기반의 공개키와 세션키를 설립하기 위한 추가적인 Round(인증서 전달, 2번의 인증서 확인 과정)가 없으므로 성능이 대략 2.8배가 차이가 나는 것을 알 수 있다. 그리고 다음 Table 3는 전체 시스템의 동작과정의 효율성을 비교분석하여 나타낸 것이다. 전체 동작 프로토콜은 키 갱신 프로토콜이 추가되고, 검증 및 연산하는 부분에 시간이 증가한다.

[Table 3]의 기기 등록 및 전체 동작 시스템 표를 보면 제안한 인증 프로토콜이 빠른 속도를 보이고 있다. 다음 Fig. 7, Fig. 8은 위의 표의 테스트 결과를 보기 쉽게 그래프로 표현한 것이다.

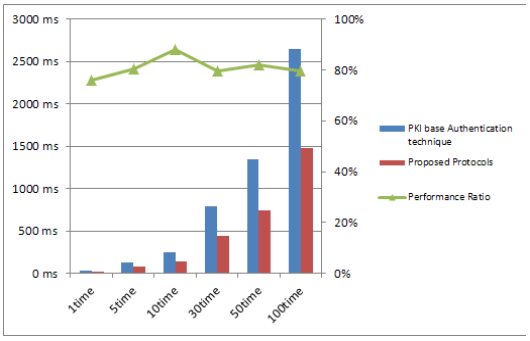
[Table 4] Comparative analysis of the efficiency of the operation of the entire system

Division	PKI based Authentication technique	Proposed authentication Protocol
1 time	27.1 ms	15.4 ms
5 time	131.8 ms	73.1 ms
10 time	251.3 ms	133.7 ms
30 time	793.3 ms	441.7 ms
50 time	1341.8 ms	737.2 ms
100 time	2649.8 ms	1476.2 ms



[Fig. 7] Comparative analysis of the efficiency graph of the proposed protocol and device registration PKI-based authentication technologies

제안 프로토콜에서는 PKI 기반 인증 기술에 비해 기기 등록 프로토콜은 약 185.7% 향상되었으며, 전체 동작 시스템은 약 83%향상 되었다. 전체 동작 시스템에서는 Device 및 Gateway에게 VD_i을 부여 및 갱신 프로토콜을 추가하여 기존 시스템보다 안정성을 높이므로 기기 등록 프로토콜보다는 향상 폭이 적은 수치를 확인할 수 있다.



[Fig. 8] Comparative analysis of the efficiency of the system graph for the complete operation of the proposed protocol and PKI-based authentication technologies

4.2 안정성 비교분석

기존 사물통신의 기술, PKI 기반 인증 기술과 제안 프로토콜의 안전성은 아래 Table 4과 같다.

[Table 5] Comparative analysis of safety

	M2M Communication	PKI Based Authentication Technique	Proposed Authentication Protocol
Physical attacks	enable	disable	disable
Compromise qualified person	enable	disable	disable
Threat of data integrity	enable	enable	disable
Middle and replay Attacks	enable	disable	disable
Attack to the core network	enable	enable	disable
Threat of confidentiality of data	enable	enable	disable

• 물리적 공격

- 조작된 장치에 인가된 인증 토큰을 삽입하거나, 조작된 소프트웨어를 설치하는 공격이다. 그러나 제안한 인증 프로토콜에서는 Device와 Gateway의 Serial Number를 등록 후 Core Server에서 인증을 하기 때문에 물리적 공격이 어렵다.

• 자격증명의 타협

-사물 통신 식별 모듈(Machine Communication Identity Module, MCIM)에 존재하는 인증 토큰에 대한 악의적인 복제 등으로 위협이 노출된다. 또한 BruteForce 공격 및 부채널 공격에 의한 피해가 예상된다. 그러나 제안한 인증 프로토콜에서는 Core Server에서 Device 및 Gateway의 Serial Number 값을 검증하고 VD_i를 생성 후 키 갱신 프로토콜을 $VD_i = GW_{ID} \| TimeStamp + Period$ 를 추가함으로써 위협에서 벗어날 수 있다.

• 데이터의 무결성 위협

- 악의적인 소프트웨어의 업데이트 혹은 설정 변경, 사물통신의 소유주, 사용자의 잘못된 설정 변경을 통한 공격이 가능하다. 또한 접근 제어리스트의 잘못된 구성으로 취약성이 발생할 수 있다. 그러나 제안한 인증 프로토콜에서는 Network Domain의 Access Network가 Device 및 Gateway에게 VD_i을 부여하고, Access server가 VD_i을 관리함으로써, 변경을 통한 공격이 어렵다.

• 중간자 및 재전송 공격

- 최초 접속에 대한 중간자 공격(Man-in-the-Middle Attack), 재전송 공격(Replay Attack), 서비스거부공격(Denial of Service, DoS)공격 및 활성화된 네트워크의 취약성을 이용하는 공격에 대한 보안 위협이 있다. 제안한 인증 프로토콜에서는 기존의 ID-Based Encryption의 인증 방식에서 세션키 생성 알고리즘으로 생성되어진 생성키 $s \cdot (a \oplus CR_R \cdot p)$을 활용하여 Network Domain의 Access Server와 Core Server간의 안전한 데이터를 송수신할 수 있어 프로토콜의 공격인 중간자 공격, 재전송 공격을 통한 인증이 불가능하다. 또한 네트워크의 취약성을 이용하는 공격을 완화시킬 수 있다.

• 코어 네트워크에 대한 공격

- Network Domain의 Core Network에 취약점에 대한 공격으로 종류는 코어 네트워크에 대한 서비스 거부 공격, 장치 위장을 통한 공격 및 인가되지 않은 위치로 장비 이동 등에 대한 취약점이 있다. 제안한 인증 프로토콜 Core Server에서 Device와 Gateway의 Serial Number을 검증하고 Network Domain하고 Device 및 Gateway Domain간의 제안한 인증 프로토콜을 사용함으로써 코어

네트워크에 대한 공격이 불가능하다.

• 기기의 데이터 기밀성 위협

- Device 혹은 Gateway가 Network Domain에 전송하는 메시지 도청, 다른 사용자 혹은 장비로 가장하여 메시지 도청에 대한 위협이 일어날 수 있다. 제안한 인증 프로토콜에서는 생성된 세션키를 활용하여 데이터를 안전하게 송·수신함으로써 사용자의 데이터와 프라이버시 공격이 불가능하다.

5. 결론

본 논문은 M2M 환경에서 취약점을 보완하고 효율성 및 안정성을 높이기 위하여 인증 프로토콜을 제안하였다. M2M Network Domain에서 Access Network와 Core Server간에 ID-Based Encryption기반으로 세션키를 생성하였고, 생성된 세션키를 활용하여 Device 및 Gateway을 검증 후 새로운 식별값을 부여하였다. 또한 식별값 안에 갱신 프로토콜을 추가하여 자동으로 식별값을 갱신한다.

기존의 사물통신 환경에서 취약점 물리적 공격, 자격증명의 타협, 변경을 통한 공격, 프로토콜 공격, 코어 네트워크에 대한 공격, 사용자 데이터 및 프라이버시에 대한 공격 등이 있다. 또한 빠르게 발전하고 있는 사물 지능 통신 장비들이 소형화 되고 있다. 그래서 제안 프로토콜에서는 기존 PKI 기반 인증 기술보다 경량화 되고 안전성도 높은 ID-Based Encryption 방식의 인증 프로토콜을 설계하였다. 제안한 인증 프로토콜을 구현하여 기존 M2M 통신 기술과 PKI 기반 인증 기술과 효율성 및 안정성을 비교분석하였다. 효율성에서는 기존 PKI기반 인증 기술보다 기기 등록 185.7%, 전체 동작 시스템은 83% 처리 속도가 향상되었다.

향후 제안한 인증 프로토콜은 다양한 사물통신에서 적용하기 위해서 활용 폭이 넓은 인증 프로토콜 연구가 필요하고, 본 논문에서 제안한 M2M 기능이 활성화된 Device가 아닌 지역 네트워크를 통하여 M2M Gateway로 수집되어진 Device에 대한 인증에 관한 인증 프로토콜이 설계가 요구된다. 그리고 아직까지 알려지지 않은 공격 유형과 또는 빠르게 발전되어지고 있는 사물지능 통신의 위험성을 분석하여 공격 유형에 대한 연구가 필요하다.

References

[1] TTA. “M2M Service Capability Structure", Telecommunication Technology Association”, 2012.06.12.

[2] TTA. “M2M Security threats and requirements of service“, Telecommunication Technology Association”, May., 23. 2012.

[3] Inhyok Cha et al. "Trust in M2M communication, IEEE Vehicular Technology Magazine, 2009. DOI: http://dx.doi.org/10.1109/MVT.2009.933478

[4] Korea Communications Commission, “Construction of communication infrastructure things basic plan (draft)”, 2009.

[5] NIA, “Law on the activation of the construction of communication infrastructure and information use things things“, 2009.11

[6] Ki Hyung Ki,. “The difference between the concept of intelligence communication things”. RFID/USN Online Forum Conference.

[7] Jae Young Ahn, “M2M technology and service network”. The 20th High-Speed Network Workshop. 2010

[8] Dong Hee Shim, “M2M (Machine to Machine Communication) In the center Europe - Standardization Trends“. TTA.

[9] Adi Shamir. “Identity-Based Cryptosystems and signature System“. SpringerLink. 1985.

[10] Dan Boneh, Matthew Franklin. “Identity-Based Encryption from the Weil Pairing”. Crypto. 2001.

[11] "How Machine-to-Machine Communication Works". HowStuffWorks.

[12] Marc Joye, Sung-Ming Yen. “Id-Based Secket-key Cryptography”. sigops. 1998.

[13] Y.-D. Joo, "Security Improvements on Smart-Card Based Mutual Authentication Scheme", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 6, pp. 91~98, 2012.

[14] J.-G. Song, T.-Y. Kim, H.-J. Lee, W.-T. Jang, "A new password authentication scheme using two-way password in Smartphone Banking", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 3, pp. 195~200, 2012.

[15] Y.-D. Joo Y.-H. An, "Improvements of a Dynamic ID-Based Remote User Authentication Scheme", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 11, No 6, pp. 303~310, 2011.

[16] Y.-H. An, Y.-D. Joo, "Security Enhancement of Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 1, pp. 231~237, 2012.

[17] M.-S. Kang, "Design of Security-Enhanced RFID Authentication Protocol Based on AES Cipher Algorithm", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 6, pp. 83~89, 2012.

진 병 욱(Byung-Wook Jin) **[정회원]**

- 2010년 2월 : 청운대학교 멀티미디어학과 (문학사)
- 2013년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

<관심분야>
네트워크 보안, 인증 시스템, 사물지능통신

박 재 표(Jae-Pyo Park) **[정회원]**

- 1996년 2월 : 숭실대학교 컴퓨터학부 (공학사)
- 1998년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2008년 9월 ~ 2009년 8월 : 숭실대학교 정보미디어 기술 연구소 전임연구원
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

<관심분야>
컴퓨터 통신, 네트워크 보안, 암호학, 멀티미디어 통신

이 근 왕(Keun-Wang Lee) **[종신회원]**

- 1993년 2월 : 한밭대학교 전자계산학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2000년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년 3월 ~ 현재 : 청운대학교 멀티미디어학과 부교수

<관심분야>
컴퓨터통신, 멀티미디어 통신, 멀티미디어 응용

전 문 석(Moon-Seog Jun) **[정회원]**

- 1989년 2월 : University of Maryland Computer Science 박사
- 1989년 9월 ~ 1991년 2월 : New Mexico State University Physical Science Lab. 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<관심분야>
정보보호, 네트워크 보안, 인증 시스템, 암호학