Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 11 pp. 9-15, 2021

https://doi.org/10.5762/KAIS.2021.22.11.9
ISSN 1975-4701 / eISSN 2288-4688

IoT 환경에서 무인증서 기반 디바이스 인증 기법

민소연[1*], 이재승[2]
[1]서일대학교 정보통신공학과, [2]숭실대학교 컴퓨터학과

Certificate-less based Device Authentication Scheme in Internet of Things

So-Yeon Min[1*], Jae-Seung Lee[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Dept. of Computer Science and Engineering, Soongsil University

요 약 최근 통신 기술과 디바이스들의 발전으로 인터넷으로 모든 사물들이 통신하며 사람과 사물 또는 사물과 사물 간의 상호 소통이 가능한 IoT 환경이 스마트홈, 스마트 카 등 다양한 방향으로 활용되고 있다. IoT 환경은 지능형 서비스를 제공해 주기 위해 다양하면서도 방대한 양의 데이터들을 수집 및 가공하며 사용자 편의를 중심으로 서비스가 제공되고 있다. 이러한 과정에서 다양한 종류의 IoT 기기들을 활용하게 되며, 서로 다른 디바이스들의 통신을 위해서는 올바른 표준 기반 통신이 필요하다. 하지만, IoT에서 기존 연구 및 표준 정의를 살펴보면, 센서 디바이스의 지속적인 서비스를 위해 경량화 및 안전한 통신 규약이 필요하지만, 공개키 통신이나 연산 에너지 효율이 떨어지는 보안 통신이 주를 이루고 있으며, 현재 IoT 서비스에서는 취약점이 발견된 커버로스나 다양한 수의 디바이스를 고려하지 않은 공개키 기반 보안기술이 활용되는 경우가 존재한다. 따라서, 본 논문에서는 기존 PKI 공개키 기반의 취약점인 Relay Attack 및 인증서 발급 문제 해결을 위해 Distance-Bounding에 기반한 무인증서 디바이스 인증 기법을 제안하였다. 제안하는 프로토콜은 보안 평가를 통해 기존 보안기술들이 가지는 다양한 보안 문제들을 해결하였으며, 시뮬레이션 결과를 통해 기존의 인증 기법에 비해 경량화된 통신이 가능함을 검증하였다.

Abstract Recently, with the progress in wireless communication technology and sensor devices, the IoT environment that connects people with things and things with other things based on the internet is used in various fields. The IoT (Internet of Things) environment must collect massive device information for smart services, receive services based on user information, and control devices. Communication must also be implemented based on a correct standard since various types of devices are used. However, a review of existing studies or definition of standards shows that while continued efforts to make devices lighter and a secure communication guideline are important, in most cases, there is public key communication or secure but lower efficiency in calculation energy. At present, in IoT services, PKI-based (Public Key Infrastructure Based) services that do not consider the number of sensor nodes or Kerberos that is proven to be vulnerable are used. Therefore, in this paper, we propose a secure protocol based on Distance-Bounding and Certificate-less. The proposed method was confirmed to be lighter than the existing authentication method through simulation results.

Keywords : IoT Authentication, Certificate-less Authentication, IoT Security, Key Management, IoT

본 논문은 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
email: symin@seoil.ac.kr
Received October 5, 2021 Revised October 28, 2021
Accepted November 5, 2021 Published November 30, 2021

1. 서론

사물인터넷(Internet of Things)은 네트워크를 통해 모든 사물을 연결하여 사물과 사물뿐만 아니라 사물과 사람 등이 데이터를 주고받으며, 상호 소통이 가능한 지능형 기술 및 서비스를 의미한다. 이러한 환경에서는 다양하면서도 방대한 양의 정보들을 수집하여, 사용자 정보, 환경 등 사용자 편의에 맞게 서비스를 제공받으며 디바이스를 제어한다[1,2]. 사물 인터넷의 가장 중요한 점은 언제 어디서나 시간과 장소에 구애받지 않고 서비스가 제공되어야 하며 지속성을 가져야 한다. 또한, 각기 다른 다양한 종류의 디바이스들을 가지고 환경을 구축하기 때문에, 상호 과정에서 올바른 통신 과정이 가능하도록 올바른 표준을 기반으로 해야 한다[3]. 또한, 데이터를 관리하는 디바이스들의 다양성을 고려한 보안방안을 제공하여 디바이스 통신에 제약이 없어야 한다[4].

하지만, 현재까지 다양한 규격의 IoT 표준이 존재하며, 이기종 간의 차이를 고려하지 않는 경우도 있다. 또한, 기존의 인증서 기반의 공개키 통신이나 커버로스를 사용하는 경우가 많은데, 지속적이고 경량화된 서비스가 필요한 IoT 환경에서는 적합 하지 않는 경우가 발생한다[5].

따라서 본 논문에서는 OneM2M표준에서 정의하고 있는 프레임워크를 기반으로, 각기 다른 하드웨어 제한을 가지고 있는 디바이스별 무인증서 인증 방안을 제안한다.

2. 관련 연구

2.1 무인증서 인증 기법

Barbosa와 Farshim이 처음으로 무인증서 인증 기법을 제안하였으며, Xie 등이 쌍선형 지도에 기반한 두 단계의 서명 및 복호화 과정에서 페어링 연산을 이용한 무인증서 서명 기법을 제안하였다[7,8]. 그러나, 계산 비용이 높은 문제와 페어링 연산이 가지는 한계를 가지고 있다. 이러한 문제 해결을 위해 Xie와 Zhang은 페어링을 사용하지 않으면서 높은 계산 비용을 해결한 무인증서 암호화 방법을 제안하였다[9,10].

2.2 무인증서 서명 암호화 기법

- Setup : 임의의 값 k로부터 시스템 파라미터 값과 마스터 비밀키로 활용할 마스터키를 생성한다.
- Partial-Key-Extract : Master-Key, 및 사용자 고유 값 ID로부터 부분 개인키와 부분 공개키인 Did, Pid를 생성한다.

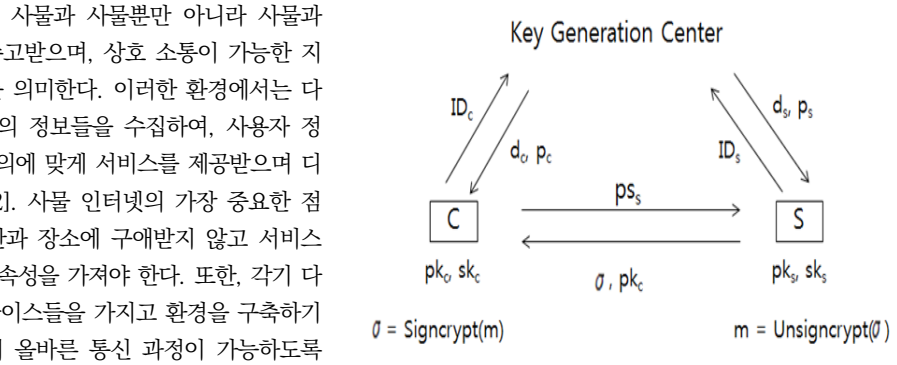

Fig. 1. Certificate-less Authentication

- Set-Secret-Value : 파라미터 값과 사용자 고유 값인 ID를 통해 Secret Value SID를 생성한다.
- Set-Public-Key : 파라미터, 사용자 고유정보 IDA와 Secret Value SID로부터 사용자의 Public-Key PKID를 생성한다.
- Set-Private-Key : 파라미터, 사용자의 부분 Private-Key DID와 Secret Value SID로부터 사용자의 Private-Key SKID를 생성한다.
- Encrypt : 파라미터, 송신자의 Private-Key sk_ID_s, Message m으로부터 암호문을 생성한다. igncrypt(params, SKID, IDR, PKID, m)이다.
- Decrypt : 파라미터, 송신자 ID, Public-Key PKID, 수신자의 Private-Key SKID 로 암호화된 Message를 복호화 하고, 암호문이 적법하다고 판단되면 메시지를 복호화하여 메시지 m을, 그렇지 않을 경우 에러가 출력된다.

Setup 및 Partial-Key-Extract 과정은 KGC(Key Generation Center)에 의해 동작하며, 부분 Private-Key DID와 부분 Public-Key PID는 사용자에게 Secure Channel을 통해 전달되며, 공개키와 개인키 쌍을 생성하는 과정과 Set-Secret-Value 알고리즘은 사용자에 의해 동작한다.

2.3 Internet of Things

사물인터넷은 주변의 사물들이 네트워크에 연결되어 서로 상호작용을 통해 데이터를 송수신하는 지능형 기술 및 서비스를 의미 한다. 기존과 다르게 사물과 사물 간에

도 사람의 제어 없이 스스로 통신하고, 분석하며 데이터를 가공하여 서비스를 제공해 줄 수 있는 디지털 혁명의 기술로 인식되고 있다.

1999년 MIT Auto-ID Center 설립자인 Kevin Ashton)이 처음으로 사물인터넷에 대한 개념과 용어를 제안하였으며, 이후 하드웨어 및 소프트웨어의 지속적 발전을 통해 다양한 기기들을 통한 서비스가 제공되어 일상생활에서 쉽게 접할 수 있게 되었다.

사물인터넷 기반 IT 제품 및 서비스는 현재 많이 상용화 되어 다양한 형태로 확인이 가능하다. 스마트 홈이나 스마트 카, e-헬스 등의 분야에서는 이미 다양한 서비스와 제품이 상용화되어있고 지속적으로 발전해 나가고 있다. 사물인터넷에서는 사물들 간 통신이 필요하며, 이를 지원하는 기반 기술이 Machine-to-Machine Communication이다. 실제로 현재 사용되어 지고 있는 대부분의 제품에서는 M2M 기술을 사용하고 있다[6].

현재 개발되고 있는 사물인터넷 서비스의 경우 동일 제조사나 협력 업체 간에 디바이스 및 동일 서비스 내에서만 작동하는 경우들이 많다. 서로 다른 제조사간의 디바이스들, 그리고 다른 사업 영역에서 통신하는 사물들, 예를 들어 스마트 홈 내에서의 각 가전제품들 등 이기종 간의 사물 통신이 이루어지기 위해서는 표준화된 통신 방식이 필요하다.

3. 제안 내용

무인증서 공개키 방식의 특징은 Device의 ID를 이용하여, 공개키를 생성하며, 각 디바이스들이 가지는 유니크한 시리얼 넘버 등을 이용한다. 이때, 사용자가 Device의 고유 정보 값을 제공한다면, 서버에서 보낸 ID 값과 비교를 통해 공개키의 연관성을 검증할 수 있다. 이에, Network를 통해 인증을 원하는 Device의 ID를 전송받고, 서버로부터 전송받은 공개키와 전송받은 ID를 KGC를 통해 검증하여, 올바른 서비스에 접속하였고 그에 따른 공개키를 전송 받았음을 검증하도록 한다. 기기에서의 무인증서 공개키 인증방식과 다르게 일반적인 스마트 홈서비스에서 무인증서 공개키 인증을 활용 시 KGC에서 공개키 검증을 추가로 담당하게 된다.

Table 1. Proposed Notation

Notation	Meaning
N_r, N_p	Nonce
MN	Middle Node
ASN	Application Service Node
ADN	Application. Dedicated Node
KGC	Key Generator Center
ID	Node ID
C_{id}	Middle Node ID
R_{I0} , R_{I1}, R_{I2}	3n Bit Divided Value
p,q,z	Prime Number
E(), D()	Encryption, Decryption

3.1 디바이스 초기인증

- 초기 단계 : 파라미터 값 k를 입력 받은 다음 소수 p,q값을 생성한다. 이때, p와 q는 q〉2k 와 q|(p-1)를 만족해야 한다. 만족한다면, g를 선택한 후, 마스터키 x를 임의로 선택하고 $y = g^x$를 계산한다. 다음으로 해시 함수 H1, H2, H3, H4, H5 를 계산하고 시스템 파라미터 params = 〈p,q,n,g,y, H1, H2, H3, H4, H5〉를 구한다.
- 부분키 생성 : 파라미터 값과 Master Key x, ID∈{0,1}*를 통해 사용자의 식별 값을 획득한 후 rID, r`ID를 선택한다. 이후, wID = grID, dID = rID + xH1(ID,wID), vID = gr`ID, σID = r`ID + xH2(ID, wID, vID)를 연산한 후 부분 비밀 키 값 DID와 PID = (wID, vID, σID)를 전달한다.
- 비밀 값 생성 : 사용자는 파라미터 값과 ID를 입력받고, z ∈R Z*q를 선택한 후, sID=z를 생성한다.
- 개인 키 생성 : 사용자의 부분 공개키 값과 pID와 앞서 생성한 sID를 통해, 사용자 개인키 skID=(dID,sID)를 만든다.
- 공개 키 생성 : 파라미터 값, 사용자의 부분 공개키 값 PID와 비밀 값 SID를 통해서 μID = gsID를 연산하고 공개키 PkID=(μID, wID,vID,σID)를 만든다.
- 서명 : 서비스 제공자(수신자의 식별 정보와 공개키 보유)에게 메시지 송신을 위해 다음 인증 절차를 거친다.

먼저, $g^{\sigma R} = v^B y^{H_2(B, Wb, vB)}$를 검증한다. 이후, 랜덤 값 r을 생성한 후

$$h = H_3(m,t,\mu^r,B,w^r,B,y^{H_1(B,wB)}r,\mu_A,w_A,\mu_B,w_B)$$

$$h' = H_4(m,t,\mu^r B,w^r,B,y^{H_1(B,wB)}r,\mu_A,w_A,\mu_B,w_B),$$

$s = r = hd_A - h\,s_A$를 계산하여 암호문 σ = (c, s, t)를 전송한다.

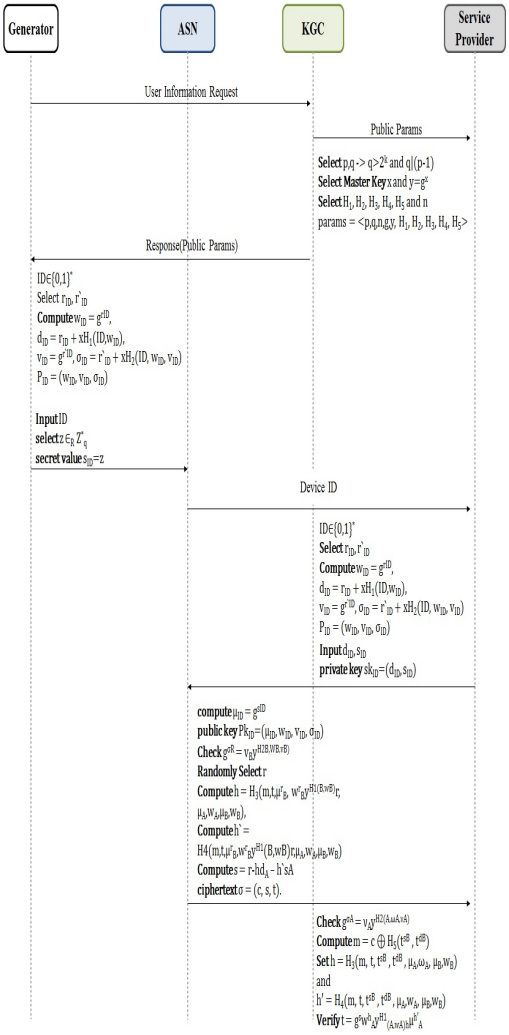

Fig. 2. ASN authentication protocol

■ 검증 : Service Provider는 $g^{\sigma A} = v^A y^{H_2(A,\,W_A,\,v_A)}$를 검증한다. 먼저, $m = c \oplus H_5(t^{sB}, t^{dB})$를 계산한다. 이후 $h = H_3(m, t, t^{sB}, t^{dB}, \mu_A, \omega_A, \mu_B, \omega_B)$, $h' = H_3(m, t, t^{sB}, t^{dB}, \mu_A, \omega_A, \mu_B, \omega_B)$값 이 만족할 경우 인증이 완료된다.

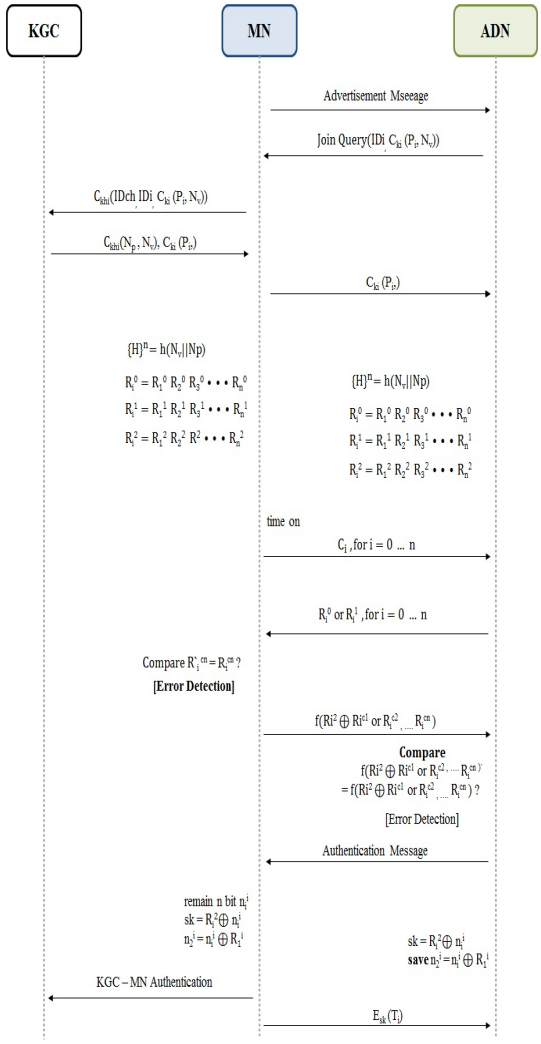

Fig. 3. ADN authentication protocol

3.2 디바이스 검증

초기 인증을 통해서 MN으로부터 데이터를 수신한 각각의 디바이스들은 가장 강한 신호로 도달한 광고메시지에 해당하는 MN에게 본인의 ID와 난수 Nv를 암호화 하여 전송한다.

난수 교환을 위해 MN도 난수를 암호화 하여 아이디와 함께 가입 요청한 노드들에게 전송한다.

난수를 교환한 MN와 센서노드는 f()를 통해 3*n bit의 임의의 값들을 생성한다.

MN는 Distance-Bounding을 응용한 인증 절차를 수행하기 위해 임의의 수 c_i 를 생성하여 한 비트씩 노드

에게 전송한다. 이때, Relay Attack을 탐지하기 위해 Time on을 통해 시간을 체크한다.

노드는 MN로부터 수신한 c_i가 0일 경우 R^0의 i번째 비트를, 1일 경우 R^1의 i번째 비트를 MN에게 전송한다. 이때, Time off를 통해 응답 값이 제시간에 도달했는지를 체크하여, 시간이 지났을 경우 Relay Attack로 간주한다.

MN는 노드 i에게 전송한 C_i의 값들을 이용하여, $R`_i^{Cn}$을 생성하며, 노드 i가 C_i에 대한 응답으로 보낸 R_i^{Cn}값과 비교하여, 같은 값인지 확인한다.

노드 i의 신뢰성을 확인한 MN는 값들을 취합하여 f() 함수를 적용 후 노드 i에게 전송한다.

MN로부터 $f(nk,R_i^{C1},R_i^{C2},\cdots\cdots.R_i^{Cn})$를 수신한 노드 i는 $f(nk,R`_i^{C1},R`_i^{C2},\cdots\cdots.R`_i^{Cn})$를 동일한 방법으로 생성하여 MN로부터 받은 값과 비교함으로서 MN를 검증한다.

MN와 노드는 R^0, R^1 남은 n비트를 통해 데이터 전송에 이용할 세션키와 비밀 값 n_2^i를 생성하고 저장하고 인증 과정을 종료 한다.

이후 MN는 KGC과 MN의 인증 과정이 끝난 후 다음 라운드 때 사용할 티켓을 노드에게 전송한다.

4. 성능 평가

4.1 Application Service Node

IoT Application Service Node에서 랜덤 오라클 모델의 보안 IND-CCA2의 검증은 다음과 같다. 우선, 불특정의 공격자가 IND-CCA2의 공격을 통해 암호화된 키 값을 찾으려고 할 경우 아래의 수식(수식 x) 에서 ϵ 이상 가져야 하는 문제를 해결해야 공격이 가능하다. 이때, (수식 1)에서 qpak, qsk 는 각각 partial key, private key 생성 쿼리, qpk는 public key를 의미하며. qpkr, qs 는 각각 public key , 암호화 쿼리를 의미하며, qu는 복호화 쿼리를 의미한다.

$$\epsilon' \geq \frac{\epsilon(1-\epsilon')^{qpkr}}{q_3+q_5+q_s+q_{pk}}(1-q_s)\frac{2q_3+q_4+q_5+3q_s}{2^k}(1-\frac{q_u}{2^k}) \quad (수식1)$$

다음은 IoT Application Service Node에서 EUF-CMA-1의 보안 성능 검증이다. 임의의 공격자가 선택한 평문에 매칭되는 암호문을 통해 공격을 시도할 경우 암호키를 획득하기 위해서는 (수식 2)의 문제를 해결해야 한다. 이때, qpk는 공개키 요청을, qpkr은 공개키 replacement 쿼리를 의미하며, 공격자가 공격하기 위해서는 암호문과 평문에 매칭되는 값에 대해 ϵ 이상 가져야 하는 문제를 해결해야 가능하다.

$$\epsilon' \geq \frac{1}{9q_{pk}}(1-\epsilon')^{qpkr} \quad (수식2)$$

4.2 Application. Dedicated Node

기존 경량화 키 관리 기법 Protocol에서 Blundo's Protocol[2]의 경우 Relay attack과 Replay attack, Leaked key의 취약점을 가지고 있으며, Mutual authentication과 Forward security and Error detection을 지원하지 않는다. PCGR[3]의 경우 Relay attack과 Replay attack에 취약점을 가지고 있으며, Dave's Protocol[4]의 경우 Replay attack와 Eavesdropping 취약점을 가지고 있다. 또한 Mutual authentication을 지원하지 않는다. 제안하는 Protocol은 변형된 Distance-Bounding 비트 전송 과정을 거쳐 각 노드의 물리적 거리를 판단하며, Relay attack등에 대응하며, 각각 KGC, MN, 센서 노드가 생성한 난수를 이용하여 R_i^0, R_i^1를 생성하고, 랜덤 임의의 수 c에 대해 약속된 응답 값 R_i^0, R_i^1를 다수 실행하여 챌린지 비트에 대한 응답 값 중 하나의 값만 위치만 잘못되어도 error detection이 가능하여 forward security와 상호인증이 가능하다. Replay attack과 메시지 위변조 공격 시에는 메시지를 탈취할 당시의 세션키가 아닌 새롭게 생성한 세션키 $sk = R_i^0 \oplus n_1$ 를 사용하며, 타임스탬프를 통해서도 Replay attack으로부터 안전성을 제공한다. 또한, 지속적으로 갱신되는 노든간의 비밀 키 값 $nk_i = k1 \oplus n_2^i$를 통해 전송되며, 디바이스 간 상호인증이 완료된 노드들의 통신으로 스니핑, 스푸핑과 같은 네트워크 공격에도 안전성을 보장한다.

Table 2. Security Analysis

	Blundo's Protocol [11]	PCGR [12]	Dave's Protocol [13]	Barbosa's Protocol [7]	Proposed scheme
Relay attack	X	X	O	O	O
Replay attack	X	X	X	O	O
Eaves dropping	O	O	X	O	O
Leaked key	X	O	O	X	O
Mutual authentication	Not-support	Support	Not-support	Support	Support
Forward security and Error detection	Not-support	Support	Support	Support	Support

4.3 효율성 검증

본 논문에서는 제안방식의 에너지 효율성을 분석하기 위해 MATLAB 프로그램을 이용한 시뮬레이션 환경을 구성하여 수행하였다.

Table 3. Simulation Initial Settings

Simulation Initial Settings	
Number of Node	30
Placement Area	20m*20
Control Center Location	X=25m, y=10
ETX, ERX	50 nanoJ
Packet Size	6000 bit

Table 3은 시뮬레이션을 위한 기본 환경 값이며 노드의 개수는 30개로 설정하였으며, 각각 ADN과 ASN환경을 구성 후 테스트 하였다. 노드의 배치는 20m×20m 지역에 랜덤하게 분포했으며, 배치에 따라 모든 센서 노드들과 게이트웨이의 거리는 25m 와 10m 사이에 존재하게 된다. 각각의 라운드는 10sec동안 되록 설정하였다.

Fig 4는 임계거리를 증가시키면서 각각 보안 프로토콜의 에너지 소비량을 비교 분석한 시뮬레이션 이다. 제안하는 ASN 인증의 경우 지수 연산을 통한 계산을 진행함으로서 PCGR 과의 에너지 효율성은 큰 차이를 보이지 않지만, 보안적인 측면에서 우수함을 확인할 수 있었다.

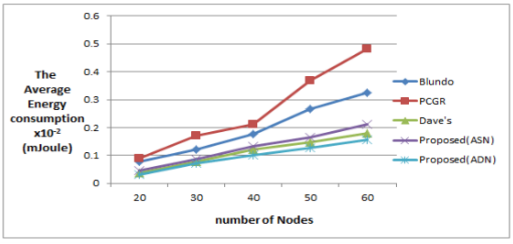

Fig. 4. Performance Analysis

5. 결론

하드웨어 및 소프트웨어의 기술 발전에 따라 IoT 보급량은 기하급수적으로 늘어나고 있으며, 다양한 디바이스 및 통신 모듈 등이 등장하고 있다. 이에 따라 이기종간의 안전한 통신 및 디바이스 성능 등을 고려한 네트워크 인증 절차가 중요시되고 있다.

제안하는 인증 프로토콜의 경우 서로 다른 연산 능력을 가진 하드웨어간 통신을 안전하고 효율적으로 지원하기 위해 무인증서 기반의 디바이스의 종류에 따라 인증 프로토콜을 제안하였다. 먼저 OneM2M 표준을 통해 Application Service Node, Application. Dedicated Node 등의 디바이스 특징을 고려하였으며, 디바이스들의 물리적인 특성과 정보 활용 능력을 고려하여 각 디바이스 군별로 디자인하였다. 또한, 보안강도 비교 분석 결과 OneM2M에서 정의하고 있는 보안 요구사항을 만족하면서, 현재 활용되고 있는 IoT 인증 기술에 비해 안전함을 확인하였다.

References

[1] ANASTASI, Giuseppe, et al. Energy conservation in wireless sensor networks: A *survey. Ad hoc networks*, pp.537-568. 2009. 7.3
DOI : https://doi.org/10.1016/j.adhoc.2008.06.003

[2] PENG, Kun. A secure network for mobile wireless service. *Journal of Information Processing Systems*, pp.247-258. 2013, 9.2
DOI : https://doi.org/10.3745/jips.2013.9.2.247

[3] GUBBI, Jayavardhana, et al. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29.7: pp.1645-1660. 2013.
DOI : https://doi.org/10.1016/j.future.2013.01.010

[4] BAYRAM, Islam Safak; PAPAPANAGIOTOU, Ioannis. A survey on communication technologies and requirements for internet of electric vehicles. *EURASIP Journal on Wireless Communications and Networking*, 2014.1: 1. 2014.
DOI : https://doi.org/10.1186/1687-1499-2014-223

[5] DAHANE, Amine; BERRACHED, Nasr-Eddine; LOUKIL, Abdelhamid. A virtual laboratory to practice mobile wireless sensor networks: a case study on energy efficient and safe weighted clustering algorithm. *Journal Article published 20 Apr 2015 in Journal of Information Processing Systems*, 11.2: pp.205-228. 2015.
DOI : https://doi.org/10.1155/2015/475030

[6] XIAO, Liang, et al. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 2018, 35.5: pp.41-49.
DOI : https://doi.org/10.1109/msp.2018.2825478

[7] BARBOSA, Manuel; FARSHIM, Pooya. Certificateless signcryption. *In: Proceedings of the 2008 ACM symposium on Information, computer and communications security. ACM,* pp.369-372. 2008.

DOI : https://doi.org/10.1145/1368310.1368364

[8] WU, Chenhuang; CHEN, Zhixiong. A new efficient certificateless signcryption scheme. *In: 2008 International Symposium on Information Science and Engineering. IEEE*, pp.661-664. 2008.
DOI : https://doi.org/10.1109/isise.2008.206

[9] XIE, Wenjian; ZHANG, Zhang. Efficient and provably secure certificateless signcryption from bilinear maps. *In: Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on. IEEE*, pp.558-562. 2010.
DOI : https://doi.org/10.1109/wcins.2010.5541841

[10] XIE, Wenjian; ZHANG, Zhang. Certificateless Signcryption without Pairing. *IACR Cryptology ePrint Archive*, 2010: 187. 2010.
DOI : https://doi.org/10.3724/sp.j.1001.2011.03891

[11] BLUNDO, Carlo, et al. Perfectly-secure key distribution for dynamic conferences. *In: Annual International Cryptology Conference. Springer Berlin Heidelberg*, pp.471-486. 1992.
DOI : https://doi.org/10.1007/3-540-48071-4_33

[12] ZHANG, Wensheng; CAO, Guohong. Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach. *In: Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, pp.503-514. 2005.
DOI : https://doi.org/10.1109/infcom.2005.1497918

[13] SINGELEE, Dave; PRENEEL, Bart. Location verification using secure distance bounding protocols. I*n: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005. IEEE*, p. 7 pp.-840. 2005.
DOI : https://doi.org/10.1109/mahss.2005.1542879

민 소 연(So-Yeon Min) [종신회원]

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신공학과 부교수

〈관심분야〉
통신 및 신호처리, 정보통신, 임베디드 시스템

이 재 승(Jae-Seung Lee) [정회원]

- 2013년 2월 : 평생교육진흥원 컴퓨터학과(공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 3월 : 숭실대학교 컴퓨터학과 박사수료
- 2019년 ~ 현재 : (주)IOSYS 연구소 연구원

〈관심분야〉
시큐어코딩, Sensor Network, IoT Security