Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.467

사물인터넷 환경에서 센서 네트워크에 대한 개선된 인증 프로토콜 설계*

김 득 훈,[1†] 곽 진[2‡]
[1]순천향대학교 정보보호학과, [2]아주대학교 정보컴퓨터공학과

Design of Improved Authentication Protocol for Sensor Networks in IoT Environment*

Deuk-hun Kim,[1†] Jin Kwak[2‡]
[1]Department of Information Security Engineering, Soonchunhyang University,
[2]Department of Information and Computer Engineering, Ajou University

요 약

사물인터넷에 대한 관심이 증가하면서 사물인터넷에 적합한 여러 보안 기술들이 연구되고 있다. 특히 디바이스 센서 네트워크 영역에서는 사물인터넷의 특성상 저사양 디바이스의 사용이 증가하고 다양화되었다. 그러나 현재의 인증 기술 등의 보안 기술을 저전력·저사양 디바이스에 그대로 적용하기에 어려움이 있고, 이로 인해 보안 위협도 증가하였다. 따라서 사물인터넷의 센서 네트워크 통신상의 엔티티간 인증 프로토콜이 연구되고 있다. 2014년 Porambage 등은 타원곡선 암호 알고리즘에 기반한 센서 네트워크 인증 프로토콜을 제안하여 사물인터넷 환경의 안전성을 향상하고자 하였지만, 취약성이 존재하였다. 이에 따라 본 논문에서는 Porambage 등이 제안한 타원곡선 암호 알고리즘 기반 인증 프로토콜의 취약성을 분석하고, 사물인터넷 환경에서 센서 네트워크에 대한 개선된 인증 프로토콜을 제안한다.

ABSTRACT

Recently interest in Internet of Things(IoT) is increasing, and a variety of the security technologies that are suitable for Internet of Things has being studied. Especially sensor network area of the device is an increased using and diversified for a low specification devices because of characteristic of the Internet of Things. However, there is difficulty in directly applying the security technologies such as the current authentication technologies to a low specification device, so also increased security threats. Therefore, authentication protocol between entities on the sensor network communication in Internet of Things has being studied. In 2014, Porambage et al. suggested elliptic curve cryptography algorithm based on a sensor network authentication protocol for advance security of Internet of Things environment, but it is vulnerability exists. Accordingly, in this paper, we analyze the vulnerability in elliptic curve cryptography algorithm based on authentication protocol proposed by Porambage et al. and propose an improved authentication protocol for sensor networks in Internet of Things environment.

Keywords: Internet of Things, Authentication Protocol, Sensor Networks, Security, Impersonation Attack

접수일(2015년 2월 12일), 수정일(2015년 4월 6일), 게재확정일(2015년 4월 6일)
* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.NRF-2014R1A2A1A11050818).
† 주저자, dhkim.isaa@gmail.com
‡ 교신저자, security@ajou.ac.kr(Corresponding author)

I. 서 론

최근 통신의 주체가 모든 사물로 확대되면서 시·공간 제약 없이 정보와 지식을 통하여 새로운 가치 창출을 실현하기 위한 기술인 사물인터넷(Internet of Things)이 사회적 이슈이다[1]. 사물인터넷은 모든 사물이 센서를 내장하며, 사용자는 센서를 통해 디바이스와 정보를 상호 통신한다. 하지만 저사양 디바이스의 사용이 증가하고 다양화되는 반면에 현재 인증 기술 등의 보안 기술을 디바이스에 그대로 적용하기 어렵기 때문에 사물인터넷 보안 위협이 증가하고 있다[2]. 이에 따라 사물인터넷의 센서 네트워크 통신이 이루어지는 센서 노드 대 노드, 센서 노드 대 사용자 간에 접근하는 정당성 여부를 검증하는 인증 프로토콜이 연구되고 있다[3-9].

2014년 Porambage 등은 사물인터넷 환경에서 센서 네트워크의 인증 프로토콜을 제안하였다[9]. 이 방식은 저사양 디바이스의 성능을 고려하여 암·복호화 연산 속도가 높은 타원 곡선 암호 알고리즘에 기반하여 인증 절차를 진행한다. 또한, 상호 인증을 지원하여 위장 공격(Impersonation attack)에 대하여 안전하다고 주장하였다. 그러나 Porambage 등의 인증 프로토콜은 위장 공격에 안전하지 않으며, 다른 공격에도 취약함을 보였다.

따라서 본 논문에서는 Porambage 등의 보안 취약성을 분석하고, 사물인터넷 환경의 안전성이 향상된 센서 네트워크 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 사물인터넷의 개념과 센서 네트워크에서 발생할 수 있는 보안 취약성을 분석한다. 3장에서는 Porambage 등이 제안한 프로토콜의 진행 절차를 살펴보고 취약성을 분석하고, 4장에서는 Porambage 등의 프로토콜을 개선하여 취약성을 보완한다. 5장에서는 개선된 프로토콜의 안전성 및 효율성을 분석하고, 마지막으로 6장에서 결론을 맺는다.

II. 관련 연구

2.1 사물인터넷(Internet of Things)

사물인터넷은 ICT(Internet Communication Technology)를 기반으로 모든 사물을 유·무선 네트워크로 연결하여 사용자 대 사물, 사물 대 사물 간의 정보를 상호 통신하는 지능형 환경이다. 미국의 시장조사 전문기관인 가트너(Gartner)는 현재 관심이 고조된 기술의 최상위 분야로 사물인터넷을 선정하였다[10].

사물인터넷은 세 가지 큰 범주로써 디바이스(단말·센서) 영역, 네트워크(유·무선) 영역, 서비스 인터페이스(플랫폼·어플리케이션) 영역으로 구분한다. 디바이스 영역은 사물에 내장된 통신 기능을 이용하여 특정 사물에서 수집 및 추출한 데이터를 다른 사물로 전송한다. 네트워크 영역은 사용자 대 사물, 사물 대 사물 간 전송되는 데이터를 송수신하는 유·무선 통로이다. 서비스 인터페이스 영역은 데이터를 처리하여 정보를 생성하며, 다양한 디바이스를 제어 및 관리한다.

2.2 보안 취약성

본 절에서는 센서 네트워크상의 엔티티 인증 프로토콜에서 발생할 수 있는 취약성을 나타낸다.

2.2.1 위장 공격(impersonation attack)

위장 공격은 공격자가 센서 네트워크에서 정당한 서버인 것처럼 위장하여 클라이언트가 인증 요청을 할 때, 프로토콜을 진행하고 센서 또는 사용자와의 인증 키를 불법으로 획득하는 공격이다.

2.2.2 재전송 공격(replay attack)

재전송 공격은 센서 네트워크에서 엔티티 간의 인증 절차에서 사용되었던 요소를 저장한 후, 이후의 인증 절차에서 재사용하여 인증 받게 되는 공격이다.

2.2.3 인증 키 추측 공격 (authentication key guessing attack)

인증 키 추측 공격은 공격자가 센서 네트워크에서 사용자 대 센서, 센서 대 센서 간의 인증 절차를 도청 또는 위장하여 송수신된 요소를 저장하고, 이를 통해 최종 합의된 인증 키와 동일한 키를 찾아내는 공격이다.

2.2.4 서비스 거부 공격(denial of service attack)

서비스 거부 공격은 공격자가 인증 절차에 관여하여 센서 또는 사용자가 인증을 요청하여도 응답을 가

로막아서 인증 서비스가 거부되는 공격이다.

2.2.5 프라이버시 침해(invasion of privacy)

프라이버시 침해는 센서 네트워크상의 인증 절차에서 송수신되는 요소로부터 통신에 참여하는 주체가 노출되어 프라이버시가 침해되는 것이다.

III. Porambage 등의 인증 프로토콜 분석

3.1 Porambage 등의 프로토콜

Porambage 등의 인증 프로토콜[9]은 IoT 환경에서 센서 노드, 사용자 및 인증기관을 엔티티로 설정하고 등록 단계와 인증 단계로 구성되어 있다. 등록 단계에서는 센서 노드 또는 사용자가 인증 등록 요청자로서 인증기관과 인증 요소를 분배하는 절차를 나타낸다. 인증 단계에서는 센서 노드 또는 사용자를 클라이언트로 설정하고 다른 센서 노드를 서버로 설정하여 등록 단계에서 얻은 인증 요소를 통해 인증을 진행하는 절차를 나타낸다. Table 1.은 Porambage 등의 인증 프로토콜에 사용된 용어를 나타내며, 특히 타원곡선 암호 연산에 기반하여 인증 프로토콜이 진행되므로 소수 q와 유한체 F_q상에서 $4a^3+27b^2 \neq 0$을 만족하는 타원 곡선 $y^2 = x^3 + ax + b$상에 위치하는 점 G가 해당 프로토콜의 인증 연산 요소로 사용된다. 등록 및 인증 단계의 진행은 다음과 같다.

3.1.1 등록 단계

- ***Step 1.*** 인증 등록 요청자는 인증기관에게 Hello 메시지와 설정할 암호 그룹 및 자신의 식별자 $\{U\}$를 전송한다. 이때, 암호 그룹은 상호간에 설정하여 등록 과정에서 사용할 타원 곡선 암호의 요소, 메시지 인증 코드에 사용되는 키(K), 해쉬 함수(H) 및 암호 알고리즘의 키 크기를 정의한다.
- ***Step 2.*** 인증기관은 인증 등록 요청자의 식별자 $\{U\}$를 검증한다. 식별자가 정당할 경우 Hello 메시지와 등록 과정에서 사용할 암호 그룹 및 자신의 공개 키 $\{Q_{CA}\}$를 인증 등록 요청자에게 전송한다.
- ***Step 3.*** 인증기관의 Hello 메시지를 받은 인증 등록 요청자는 다음 수식을 계산한다.

$$r_U \in_R [1, ..., n-1]$$
$$R_U = r_U G \quad (1)$$

또한, 랜덤한 비표값 $\{N_U\}$를 생성하여 메시지 인증 코드값 $\{MAC_K[R_U, U, N_U]\}$를 계산하고 생성된 요소 $\{R_U, N_U, MAC_K[R_U, U, N_U]\}$를 인증기관에 전송하여 인증 등록을 요청한다.

- ***Step 4.*** 인증기관은 전송받은 인증 등록 요청 요소에서 메시지 인증 코드 값 $\{MAC\}$을 검증한다. 메시지 인증 코드가 정당할 경우 다음 수식을 통해 인증 응답 요소를 계산한다.

$$r_{CA} \in_R [1, ..., n-1]$$
$$Cert_U = R_U + r_{CA} G \quad (2)$$

$$e = H(Cert_U) \quad (3)$$

$$s = er_{CA} + d_{CA} (\mathrm{mod} n) \quad (4)$$

또한, 랜덤한 비표값 $\{N_{CA}\}$를 생성하여 메시지

Table 1. Notation

Notation	Description
K	Symmetric key for initial message authentication
U	Identity of node U
r_U	Secret random integer value generated by U
R_U	Elliptic Curve point for certificate request sent by node U
G	Base point generator with order of prime n
$Cert_U$	Implicit certificate of i^{th} node
e	Integer used to keep hash value of $Cert_U$
s	Integer used to compute private key of the requestor node
d_U	Node $U's$ private key
Q_U	Node $U's$ public key
N_U	Random cryptographic nonce generated by node U
K_{UV}	Link key between nodes U and V
$H(\bullet)$	One-way hash function

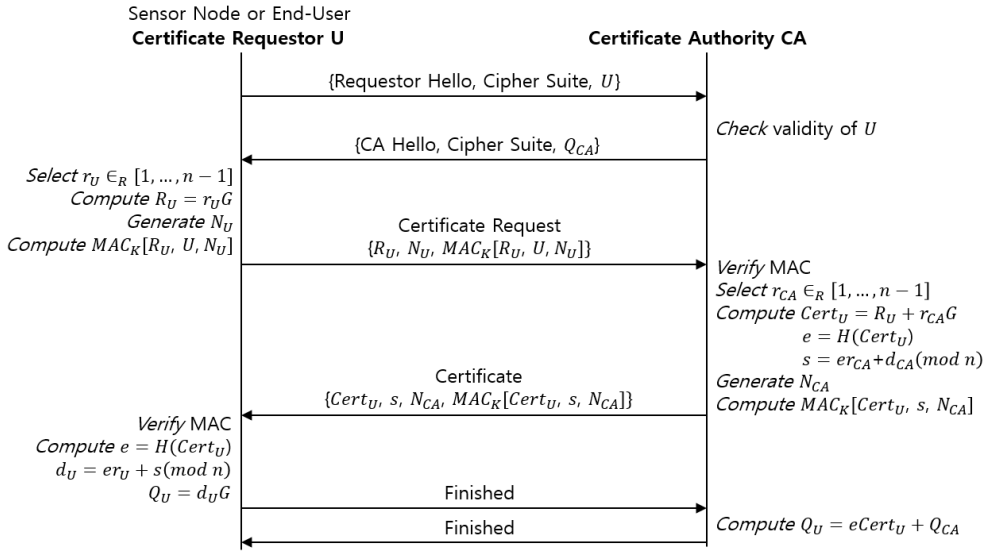

Fig. 1. Registration phase

인증 코드값 $\{MAC_K[Cert_U, s, N_{CA}]\}$를 계산하고 생성된 요소 $\{Cert_U, s, N_{CA}, MAC_K[Cert_U, s, N_{CA}]\}$를 인증 등록 요청자에게 전송하여 요청에 대한 응답을 한다.

- ***Step 5.*** 인증 등록 요청자는 전송받은 인증 등록 응답 요소에서 메시지 인증 코드 값 $\{MAC\}$을 검증한다. 메시지 인증 코드가 정당할 경우 다음과 같은 수식을 통해 인증 등록을 완료하고 인증기관에게 Finished 메시지를 전송한다.

$$e = H(Cert_U) \tag{5}$$

$$d_U = er_U + s \pmod n \tag{6}$$

$$Q_U = d_U G \tag{7}$$

- ***Step 6.*** 인증기관은 인증 등록 요청자에게 Finished 메시지를 받으면 다음과 같은 수식을 계산하고 인증 등록 요청자에게 Finished 메시지를 전송한다.

$$Q_U = e\,Cert_U + Q_{CA} \tag{8}$$

3.1.2 인증 단계

- ***Step 1.*** 클라이언트는 서버에게 Hello 메시지와 인증 과정에서 설정할 암호 그룹 및 자신의 식별자 $\{U\}$를 전송한다.
- ***Step 2.*** 서버는 클라이언트로부터 Hello 메시지와 암호 그룹을 받으면, 자신의 암호 그룹 리스트와 비교를 한다. 전송받은 암호 그룹이 리스트에 존재할 경우 서버는 Hello 메시지와 암호 그룹 및 자신의 식별자 $\{V\}$를 전송한다. 만약 암호 그룹이 리스트에 존재하지 않을 경우 클라이언트와 인증 과정을 종료한다.
- ***Step 3.*** 클라이언트는 서버로부터 Hello 메시지를 응답받으면, 랜덤한 비표값 $\{N_U\}$를 생성하여 메시지 인증 코드값 $\{MAC_K[Cert_U, U, N_U]\}$를 계산하고 생성된 요소 $\{Cert_U, N_U, MAC_K[Cert_U, U, N_U]\}$를 서버에게 전송한다.
- ***Step 4.*** 서버는 클라이언트로부터 전송받은 메시지 인증 코드 값 $\{MAC\}$을 검증한다. 메시지 인증 코드가 정당할 경우 다음과 같은 수식을 계산한다.

$$e = H(Cert_U) \tag{9}$$

$$Q_U = e\,Cert_U + Q_{CA} \tag{10}$$

또한, 랜덤한 비표값 $\{N_V\}$를 생성하여 메시지 인증 코드값 $\{MAC_K[Cert_U, V, N_V]\}$를 계산하고

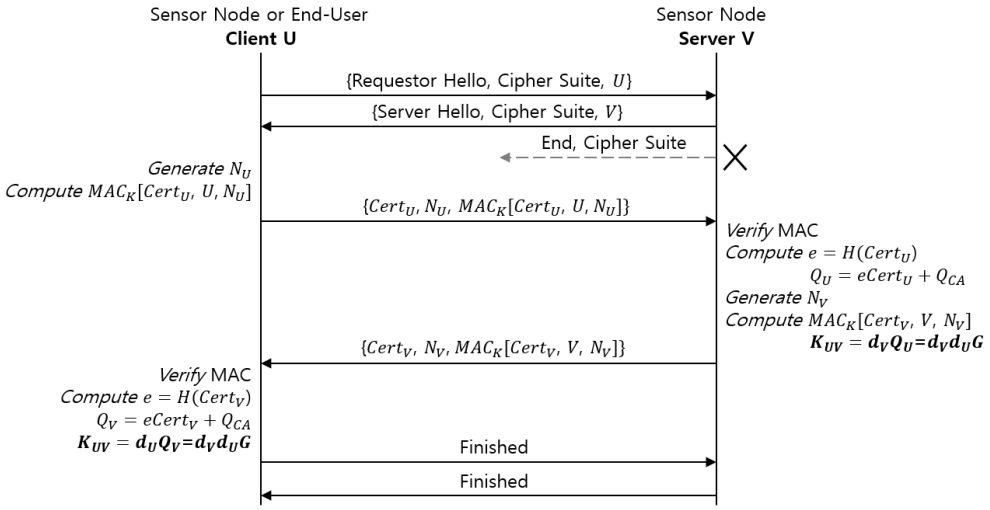

Fig. 2. Authentication phase

생성된 요소 $\{Cert_V, N_V, MAC_K[Cert_V, V, N_V]\}$를 클라이언트에게 전송하며 클라이언트와 통신 키를 다음과 같이 계산한다.

$$K_{UV} = d_V Q_U = d_V d_U G \quad (11)$$

- ***Step 5.*** 클라이언트는 전송받은 메시지 인증 코드 값 $\{MAC\}$을 검증한다. 메시지 인증 코드가 정당할 경우 다음과 같은 수식을 통해 서버와의 통신 키를 획득하고 서버에게 Finished 메시지를 전송한다.

$$e = H(Cert_V) \quad (12)$$
$$Q_V = e\,Cert_V + Q_{CA} \quad (13)$$
$$K_{UV} = d_U Q_V = d_V d_U G \quad (14)$$

- ***Step 6.*** 서버는 클라이언트로부터 Finished 메시지를 받으면 클라이언트에게 Finished 메시지를 재전송하고 인증 절차를 완료한다.

3.2 Porambage 등의 프로토콜에 대한 취약성 분석

3.2.1 위장 공격

공격자는 클라이언트가 통신을 하려는 상대방의 식별자를 검증하는 단계가 없기 때문에 정당한 서버인 것처럼 위장하여 인증 절차를 진행할 수 있다. 이때, 공격자는 인증기관과 등록과정을 진행하여 인증기관에게 $Cert_{V'}$를 부여받고 $Cipher\,Suite$의 취약점을 통해 공격을 시도한다[11]. 클라이언트가 인증을 요청하면 공격자는 Hello 메시지, 클라이언트와 자신의 암호 그룹을 설정하는 메시지 및 식별자 $\{Server\,Hello, Cipher\,Suite, V'\}$를 클라이언트에게 전송한다. 이후 클라이언트는 비표값$\{N_U\}$를 생성하고 메시지 인증 코드$\{MAC_K[Cert_U, U, N_U]\}$를 계산하여 위장한 공격자에게 전송한다. 공격자는 클라이언트와 암호 그룹 설정을 통해 분배된 메시지 인증 코드 키 값(K)를 $Cipher\,Suite$의 취약점을 통해 알아낸 후 해당 값을 이용하여 메시지 인증 코드 검증을 한다. 또한 공격자의 비표값$\{N_{V'}\}$를 생성하고 메시지 인증 코드$\{MAC_K[Cert_{V'}, V, N_{V'}]\}$를 계산하여 클라이언트에게 전송한다. 클라이언트는 메시지 인증 코드 검증을 통해 공격자를 정당한 서버로 인식하고 최종적으로 인증 키$(K_{UV'} = d_U Q_{V'} = d_{V'} Q_U)$를 합의한다. 이를 통해 Porambage 등의 인증 프로토콜이 위장 공격에 취약하다는 것을 확인할 수 있다.

3.2.2 인증 키 추측 공격

공격자가 위장 공격에 성공할 경우 합의된 인증 키의 계산상 성질$(d_U Q_{V'} = d_{V'} Q_U)$를 이용하여, 최종적으로 $d_U = \dfrac{d_{V'} Q_U}{Q_{V'}} = \dfrac{d_{V'}(e\,Cert_U + Q_{CA})}{e\,Cert_{V'} + Q_{CA}}$가 되

므로 인증 과정에서 사용된 요소 대입을 통해 클라이언트 측면의 센서 또는 사용자의 비밀 키 값$\{d_U\}$에 대한 추측이 가능하다.

3.2.3 서비스 거부 공격

Porambage 등은 공격자가 서비스 거부 공격을 시도할 때 인증 요청 메시지{Requestor Hello, Cipher Suite, U}에 포함된 암호 그룹을 서버 측에서 비교하여 리스트에 존재하지 않을 경우 프로토콜을 종료함으로써 서비스 거부 공격에 안전하다고 하였다. 그러나 공격자가 서버에서 정당한 암호 그룹 비교 후 서버에서 클라이언트로 보내는 인증 응답 메시지의 전송을 차단할 경우, 클라이언트와 서버는 각각 상대방의 응답을 계속 기다리게 되므로 서비스 거부 공격이 발생할 수 있다.

3.2.4 프라이버시 침해

인증 단계를 수행할 때, 클라이언트는 자신의 식별자 값 U를 인증 요청 메시지{Requestor Hello, Cipher Suite, U}에 그대로 포함하고 서버도 식별자 값 V를 인증 응답 메시지{Server Hello, Cipher Suite, V}에 그대로 포함한다. 이에 따라 해당 정보를 볼 경우 클라이언트가 U라는 것을 알 수 있으며, V라는 센서와 통신하는 것이 노출됨으로써 프라이버시를 침해당할 수 있다.

IV. 제안하는 인증 프로토콜

본 장에서는 Porambage 등의 인증 프로토콜 취약성을 보완하고 센서 네트워크에 대한 보안 요구사항을 고려하여 개선된 인증 프로토콜을 제안한다. Table 2.는 Porambage 등의 인증 프로토콜에 사용된 용어 이외에 제안하는 인증 프로토콜에서 추가적으로 사용하는 용어를 나타낸다.

Table 2. Proposed notation

Notation	Description
w_{CA}	Random integer value generated by CA
x_{CA}	
AID_U	Alternative identity of node U
T_U	Timestamp of node U
$\triangle T$	Valid time interval for transmission delay
SK_U	Value for distribution x_{CA}
$\oplus$	Bitwise XOR operation
$\|$	Concatenation

4.1 등록 단계

- ***Step 1.*** 인증 등록 요청자는 인증기관에게 Hello 메시지와 설정할 암호 그룹 및 자신의 식별자 $\{U\}$를 전송한다. 이때, 암호 그룹은 메시지 인증 코드에 사용되는 키$\{K\}$를 제외한

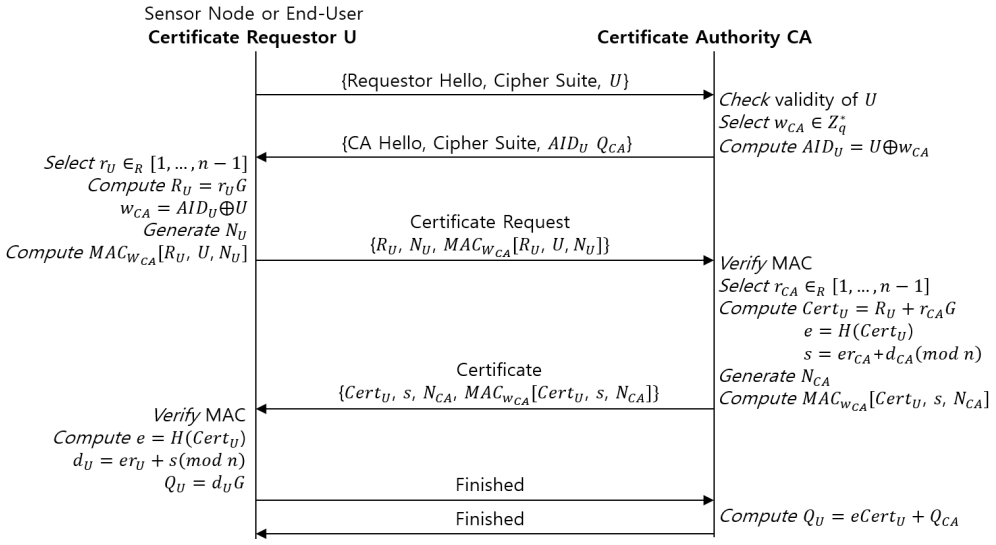

Fig. 3. Proposed registration phase

$CERT\_ECC\_WITH\_AES128\_CBC\_SHA256$ 의 암호 그룹을 이용한다.

- ***Step 2.*** 인증기관은 인증 등록 요청자의 식별자 $\{U\}$를 검증하여 식별자가 정당할 경우 대체 식별자 생성을 위해 다음과 같은 수식을 계산한다.

$$w_{CA} \in Z_q^*$$
$$AID_U = U \oplus w_{CA} \quad (15)$$

이후 Hello 메시지, 등록 과정에서 사용할 암호 그룹, 자신의 공개 키 $\{Q_{CA}\}$ 및 대체 식별자 $\{AID_U\}$를 인증 등록 요청자에게 전송한다.

- ***Step 3.*** 인증기관의 Hello 메시지를 받은 인증 등록 요청자는 기존의 Porambage 등의 프로토콜에서 진행되는 계산과 추가적인 계산을 다음과 같이 수행한다.

$$r_U \in_R [1, ..., n-1]$$
$$R_U = r_U G \quad (16)$$

$$w_{CA} = AID_U \oplus U \quad (17)$$

- ***Step 4.*** 이후에 진행되는 등록 과정은 메시지 인증 코드의 키 값을 $\{K\}$에서 $\{w_{CA}\}$를 이용하는 것 이외에 기존 Porambage 등의 등록단계 4~6번과 동일하게 수행한다.

$$MAC_{w_{CA}}[..., ..., ...] \quad (18)$$

4.2 인증 단계

- ***Step 1.*** 클라이언트는 서버에게 Hello 메시지와 인증 과정에서 설정할 암호 그룹 및 자신의 대체 식별자 $\{AID_U\}$, 타임스탬프 값 $\{T_U\}$와 해

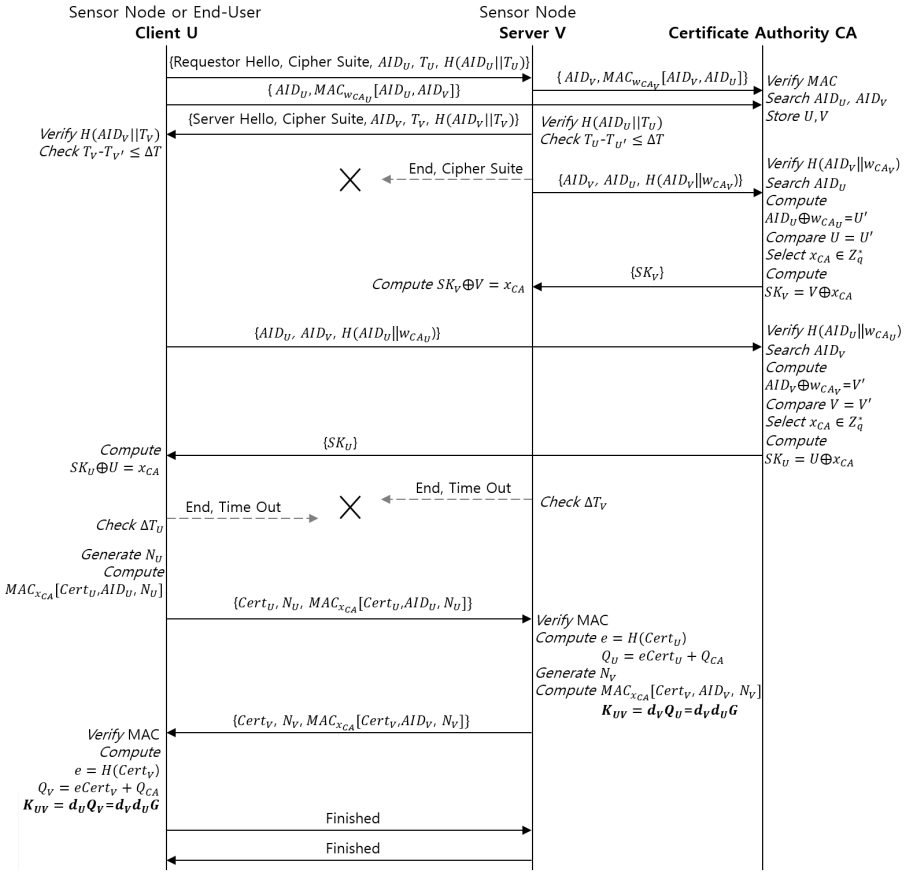

Fig. 4. Proposed authentication phase

쉬 값 $\{H(AID_U \| T_U)\}$를 전송한다. 또한, 자신의 대체 식별자와 통신하고자 하는 상대방의 대체 식별자를 등록과정에서 분배된 랜덤 값 $\{w_{CA_U}\}$를 이용하여 메시지 인증 코드 $\{MAC_{w_{CA_U}}[AID_U, AID_V]\}$를 대체 식별자 $\{AID_U\}$와 같이 인증기관에게 전송한다. 서버는 클라이언트로부터 Hello 메시지를 받으면, 클라이언트와 마찬가지로 자신의 대체 식별자와 클라이언트의 대체 식별자를 등록과정에서 분배된 랜덤 값 $\{w_{CA_V}\}$를 이용하여 메시지 인증 코드 $\{MAC_{w_{CA_V}}[AID_V, AID_U]\}$를 대체 식별자 $\{AID_V\}$와 같이 인증기관에게 전송한다.

- ***Step 2.*** 인증기관은 클라이언트 및 서버에게 전송받은 대체 식별자를 검색하여 얻은 랜덤 값 $\{w_{CA_U}, w_{CA_V}\}$를 통해 메시지 인증 코드를 검증하고, 정당할 경우 클라이언트와 서버의 식별자를 저장한다.
- ***Step 3.*** 서버는 클라이언트로부터 Hello 메시지와 암호 그룹을 받으면, 자신의 암호 그룹 리스트와 비교를 한다. 전송받은 암호 그룹이 리스트에 존재할 경우 서버는 클라이언트에게 받은 대체 식별자와 타임스탬프를 연접하여 해쉬한 값을 검증한다. 또한 클라이언트가 보낸 타임스탬프의 유효시간을 계산한다.

$$T_U - T_{U'} \leq \Delta T \tag{19}$$

모든 요소가 정당할 경우 서버는 Hello 메시지와 암호 그룹 및 자신의 대체 식별자 $\{AID_V\}$, 타임스탬프 값 $\{T_V\}$와 해쉬 값 $\{H(AID_V \| T_V)\}$를 전송한다. 만약 암호 그룹이 리스트에 존재하지 않을 경우 클라이언트와 인증 과정을 종료한다.

- ***Step 4.*** 클라이언트는 서버로부터 Hello 메시지를 응답받으면, 서버의 대체 식별자와 타임스탬프를 연접하여 해쉬한 값을 검증한다. 또한 클라이언트가 보낸 타임스탬프의 유효시간을 계산한다.

$$T_V - T_{V'} \leq \Delta T \tag{20}$$

- ***Step 5.*** 클라이언트와 서버는 통신 상대방의 대체 식별자를 검증받고 메시지 인증 코드의 키를 분배하기 위해 각각 인증기관과 인증 절차를 수행한다. 서버는 자신의 대체 식별자 $\{AID_V\}$와 클라이언트의 대체 식별자 $\{AID_U\}$ 및 등록 단계에서 분배받은 랜덤 값 $\{w_{CA_V}\}$를 자신의 대체 식별자와 해쉬한 값 $\{H(AID_V \| w_{CA_V})\}$를 인증기관에게 전송한다. 클라이언트도 자신의 대체 식별자와 서버의 대체 식별자 및 랜덤 값 $\{w_{CA_U}\}$를 자신의 대체 식별자와 해쉬한 값 $\{H(AID_U \| w_{CA_U})\}$를 인증기관에게 전송한다.
- ***Step 6.*** 인증기관은 클라이언트 및 서버로부터 메시지를 전송받으면 검증과 조사를 실시한다. 서버에게 메시지를 받은 인증기관은 서버의 대체 식별자를 통해 등록 과정에서 분배된 랜덤 값 $\{w_{CA_V}\}$를 획득하여 서버가 보낸 해쉬 값을 검증한다. 수행한 결과가 정당할 경우 인증기관에 저장된 클라이언트의 대체 식별자 $\{AID_U\}$를 조사하여 랜덤 값 $\{w_{CA_U}\}$와 식별자 $\{U'\}$를 획득하고, 기존에 저장된 식별자 $\{U\}$를 이용하여 다음과 같은 계산을 실시한다.

$$AID_U \oplus w_{CA_U} = U \tag{21}$$

$$U = ? U' \tag{22}$$

$$x_{CA} \in Z_q^* \tag{23}$$

$$SK_V = V \oplus x_{CA} \tag{24}$$

또한 클라이언트에게 메시지를 받은 인증기관은 클라이언트의 대체 식별자와 랜덤 값 $\{w_{CA_U}\}$를 획득하여 해쉬 값을 검증한다. 수행한 결과가 정당할 경우 인증기관과 서버가 수행한 절차와 동일하게 클라이언트 측면에서 다음과 같은 계산을 실시한다.

$$AID_V \oplus w_{CA_V} = V \tag{25}$$

$$V = ? V' \tag{26}$$

$$x_{CA} \in Z_q^* \text{(22번과동일)} \tag{27}$$

$$SK_U = U \oplus x_{CA} \quad (28)$$

인증기관은 메시지 인증 코드 키 값 $\{x_{CA}\}$를 분배하기 위해 계산된 $\{SK_V\}$와 $\{SK_U\}$를 각각 서버와 클라이언트에게 전송한다.

- ***Step 7.*** 인증기관으로부터 값을 전송받은 서버와 클라이언트는 각각 자신만 알고 있는 식별자를 이용하여 다음과 같은 계산으로 동일한 메시지 인증 코드 키 값 $\{x_{CA}\}$를 얻는다.

$$SK_V \oplus V = x_{CA}(\text{서버}) \quad (29)$$

$$SK_U \oplus U = x_{CA}(\text{클라이언트}) \quad (30)$$

- ***Step 8.*** 서버와 클라이언트는 자신의 타임스탬프를 포함한 메시지를 보낸 후 상대방으로부터 일정 시간내에 응답이 오지 않을 경우 프로토콜을 종료한다. 시간내에 응답이 올 경우 이후에 진행되는 인증 과정은 식별자를 대체 식별자 $\{AID_U, AID_V\}$로 사용하는 것과 메시지 인증 코드의 키 값을 $\{K\}$에서 $\{x_{CA}\}$를 이용하는 것 이외에 기존 Porambage 등의 프로토콜 인증단계 3~6번과 동일하게 수행한다.

$$MAC_{x_{CA}}[\ldots, AID_{U \text{or } V}, \ldots] \quad (31)$$

V. 안전성 및 효율성 분석

본 장에서는 제안한 인증 프로토콜을 취약성 분석에 기반하여 안전성 분석 및 연산량에 따른 프로토콜 효율성 분석을 실시한다. Table 3.은 제안한 인증 프로토콜과 Porambage 등의 프로토콜 외에 연구된 센서 네트워크에 대한 인증 프로토콜[3, 5]을 비교 분석한 것이며, 이를 통해 제안한 기법이 다른 연구보다 안전하다는 것을 알 수 있다.

5.1 안전성 분석

5.1.1 위장 공격

기존의 인증 프로토콜은 공격자가 정당한 서버로 위장하여 *Cipher Suite*를 설정한 후 얻은 메시지 인증 코드 키 값 $\{K\}$를 이용하여 공격하였다. 그러나 제안한 프로토콜은 대체 식별자를 통해 클라이언트와 서버간 상호 인증을 수행한다. 또한, *Cipher Suite*에서 메시지 인증 코드 키 값을 배제시켰으며, 인증기관에서 선택한 랜덤 값 $\{w_{CA}, x_{CA}\}$를 메시지 인증 코드의 키 값으로 인증 절차를 진행한다. 이에 따라 공격자는 클라이언트가 확인하는 메시지 인증 코드 $\{MAC_{x_{CA}}[Cert_V, AID_V, N_V]\}$를 생성할 수 없으므로 위장 공격에 실패한다.

5.1.2 재전송 공격

기존의 인증 프로토콜은 공격자가 재전송 공격만으로는 자신에게 유용한 정보를 획득할 수 없었다. 하지만 클라이언트와 서버간에 전송되는 *Cipher Suite*가 포함된 정보를 도청한 후에 취약한 *Cipher Suite*로 변경하여 인증을 유도할 수 있으며, 이를 통해 메시지 인증 코드 값에 대한 유추가 가능하다. 이에 따라 제안한 프로토콜은 인증 절차 초기 2단계에서 대체 식별자를 포함한 메시지를 송·수신할 때 타임스탬프 $\{T\}$를 적용하여 메시지 재전송이 다른 공격에 영향을 주는 것을 방지한다.

Table 3. Comparative analysis of security

Classification	Impersonation attack	Replay attack	Authentication key guessing attack	Denial of service attack	Invasion of privacy
Zhao et al. Protocol	○	○	△	×	×
Mahalle et al. Protocol	○	○	△	○	×
Porambage et al. Protocol	×	△	×	△	×
Proposal Protocol	○	○	○	○	○

5.1.3 인증 키 추측 공격

제안한 프로토콜은 위장 공격이 방지된다. 이에 따라 공격자는 인증 키의 계산상 성질을 이용하기 위한 요소 $\{d_{V'}, Q_{V'}\}$를 연산한 수식을 얻을 수 없기에 타원 곡선 암호에 기반한 인증 키를 추측하기 어렵다.

5.1.4 서비스 거부 공격

공격자가 센서 노드 서버를 타겟으로 지속적인 메시지를 전송할 경우, 서버와 설정한 암호 그룹 리스트 검증을 통해 서비스 거부 공격을 방지한다. 또한 서버가 클라이언트에게 메시지를 보내거나, 클라이언트가 서버에게 메시지를 보내고 일정 시간을 계산한 뒤에 통신 상대방으로부터 응답 메시지가 오지 않을 경우 타임 아웃을 설정하여 서비스를 이용할 수 없는 상황에 대한 신속한 탐지가 이루어질 수 있도록 지원한다.

5.1.5 프라이버시 침해

제안한 프로토콜은 사용자의 식별자를 인증 과정에 직접 사용하는 것이 아니라 대체 식별자 $\{AID\}$를 이용하여 프로토콜을 진행한다. 또한 최종적으로 인증 키를 분배하기 전까지 대체 식별자를 이용하므로 공격자가 메시지를 도청하여도 통신을 진행하는 클라이언트와 서버를 알아낼 수 없다. 이를 통해 사물인터넷의 센서 네트워크에서 프라이버시 침해를 방지한다.

5.2 효율성 분석

사물인터넷 환경은 저사양의 디바이스 및 센서가 사용되므로 센서의 배터리 측면을 고려해야 한다. 이에 따라 인증 프로토콜의 연산량을 낮춰서 오버헤드를 감소시켜야한다. 제안하는 프로토콜은 기존의 Porambage 등의 프로토콜 취약성을 보완하기 위해 인증 단계에서 인증기관이 통신에 개입된다. 또한 센서의 측면으로 볼 때, 기존 프로토콜 대비 XOR 연산 3번, $H(\cdot)$ 연산 2번, MAC 연산 1번이 추가적으로 수행되며, 사용된 연산 기법은 저연산량으로 수행되며, 오버헤드가 많이 발생하지 않는다. 이에 따라 기존 프로토콜의 취약성을 보완하며, 연산량이 적게 수행되므로 효율성이 보장된다.

VI. 결 론

사물인터넷 환경은 저사양 디바이스의 사용량이 증가하고 다양화되었지만, 기존의 사물 또는 사용자 인증 기술을 그대로 적용하는데 어려움이 존재한다. 이에 따라 사물인터넷 환경을 고려한 인증 기술이 현재 활발히 연구되고 있다.

Porambage 등이 제안한 사물인터넷 환경에서 센서 네트워크에 대한 인증 프로토콜은 암호 연산 속도가 빠르고 안전성의 강도가 높은 타원 곡선 암호 알고리즘에 기반하여 사용자 대 센서, 센서 대 센서의 인증 프로토콜을 제안하였다. 그러나 주장하는 보안적 측면과 달리 위장 공격, 서비스 거부 공격 이외의 많은 취약성이 존재하였다. 이에 따라 본 논문에서는 Porambage 등의 인증 프로토콜에 대한 취약성을 분석하고, 센서 네트워크에 대한 보안 요구사항을 고려하여 사물인터넷 환경에서 센서 네트워크에 대한 개선된 인증 프로토콜을 제안하였다. 또한 제안 프로토콜의 안전성 분석을 실시하여 위장 공격, 재전송 공격, 인증 키 추측 공격, 서비스 거부 공격 및 프라이버시 침해에 대하여 안전하다는 것을 입증하였으며, 효율성 분석을 통해 성능을 입증하였다. 이를 통해 향후 사물인터넷 환경에서 디바이스, 네트워크, 서비스 인터페이스 영역의 사용자 및 사물 인증 프로토콜 연구에 도움이 될 것으로 기대한다.

References

[1] National Intelligence Service, Ministry of Science, ICT and Future Planning, Korea Communications Commission, Ministry of Security and Public Administration, "2014 State of Information Security White Paper," Apr. 2014.

[2] Ministry of Science, ICT and Future Planning, "Internet of Things Information Security Roadmap," Oct. 2014.

[3] Guanglei Zhao, Xianping Si, Jingcheng Wang, Xiao Long and Ting Hu, "A novel mutual authentication scheme for

Internet of Things," 2011 International Conference on Modeling Identification and Control, pp. 563-566, Jun. 2011.

〔4〕 Muhamed Turkanovic, Bostjan Brumen and Marko Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," AD Hoc Networks, vol. 20, pp. 96-112, Sep. 2014.

〔5〕 N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, "Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things," *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309-348, Mar. 2013.

〔6〕 Kaiping Xue, Changsha Ma, Peilin Hong and Rong Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, issue. 1, pp. 316-323, Jan. 2013.

〔7〕 Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig and Georg Carle, "DTLS based security and two-way authentication for the Internet of Things," AD Hoc Networks, vol. 11, issue. 8, pp. 2710-2723, Nov. 2013.

〔8〕 Canming jiang, Bao Li and Haixia Xu, "An efficient Scheme for User Authentication in Wireless Sensor Networks," 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 438-442, May. 2007.

〔9〕 Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov and Mika Ylianttila, "Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications," 2014 IEEE Wireless Communications and Networking Conference(WCNC), pp. 2728-2733, Apr. 2014.

〔10〕 Gartner, "Gartner Hype Cycle 2014," http://www.gartner.com/

〔11〕 Yunyoung Lee, Soonhaeng Hur, Sangjoo Park, Donghwi Shin, Dongho Won, and Seungjoo Kim, "CipherSuite Setting Problem of SSL Protocol and It's Solutions," *The KIPS transactions*, Part C Part C, vol.15C, no.5, pp. 359-366, 2008.

〈저 자 소 개〉

김 득 훈 (Deuk-hun Kim) 학생회원
2013년 8월: 순천향대학교 정보보호학과 학사
2013년 9월~현재: 순천향대학교 정보보호학과 석사과정
〈관심분야〉 클라우드 컴퓨팅 보안, 암호프로토콜, 사물인터넷 보안, 응용서비스 보안

곽 진 (Jin Kwak) 종신회원
2000년 8월: 성균관대학교 학사
2003년 2월: 성균관대학교 석사
2006년 2월: 성균관대학교 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 1월~2009년 12월: 정보통신연구진흥원 주간기술동향 집필위원
2007년 1월~현재: 한국정보기술융합학회 이사
2007년 3월~2015년 2월: 순천향대학교 정보보호학과 교수
2008년 1월~현재: 한국정보보호학회 논문지편집위원
2008년 1월~현재: 한국정보보호학회 이사
2008년 4월~현재: 한국인터넷정보학회 논문지편집위원
2008년 12월~현재: 정보통신산업진흥원 기술평가위원
2009년 1월~2009년 12월: 순천향대학교 공과대학 교학부장
2009년 1월~2010년 12월: 순천향대학교 정보보호학과 학과장
2009년 5월~현재: TTA 표준화로드맵 기술표준기획전담반 위원
2010년 1월~2012년 12월: 순천향대학교 SCH BIT 창업보육센터장
2010년 3월~현재: 조달청 기술평가위원
2010년 5월~2010년 7월: 교육과학기술부 국가기술수준평가 위원
2011년 1월~현재: 한국정보처리학회 이사
2011년 1월~현재: JIPS 논문지 편집위원
2011년 2월~2012년 12월: 순천향대학교 중소기업산학협력센터 센터장
2011년 7월~현재: 지식경제부 지식경제기술혁신평가단 위원
2012년 ~현재: 한국암호포럼 운영위원
2012년 ~현재: 한국방송통신전파진흥원 평가위원
2013년 ~현재: 교육부 정책자문위원
2013년 ~현재: 금융보안연구원 보안기술 자문위원
2013년 ~현재: 금융감독원 인증방법평가위원
2015년 3월~현재: 아주대학교 정보컴퓨터공학과 교수
〈관심분야〉 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가