논문 13-38B-05-09

한국통신학회논문지 '13-05 Vol.38B No.05
http://dx.doi.org/10.7840/kics.2013.38B.5.394

안전한 WEB of Things 응용을 위한 개체 인증 기술

박 지 예◆, 강 남 희°

Entity Authentication Scheme for Secure WEB of Things Applications

Jiye Park◆, Namhi Kang°

요 약

WoT(Web of Things)는 웹 표준화 기술을 이용하여 사물간 지능화 통신을 실체화하기 위해 제안된 기술이다. WoT 환경은 LLN(Low-power, Lossy Network)과 자원이 제한적인 센서 장치 등을 포함하고 있으므로 기존 인터넷 환경에 적용했던 보안 기술들을 그대로 적용하기는 어렵다. 최근 IETF 표준화 그룹에서는 WoT 환경에서 보안 서비스를 제공하기 위해 DTLS 프로토콜을 이용한 방안이 제시되었다. 하지만 DTLS 프로토콜은 사전 설정(핸드쉐이킹) 과정의 복잡성과 전송되는 메시지양이 많아 WoT 환경에서 종단간 보안 서비스를 제공하기에는 무리가 있다. 본 논문에서는 이를 개선하기 위해 WoT 환경을 DTLS 적용 가능 구간과 경량화 보안 기술이 적용될 구간으로 나누고, 경량화 구간을 위한 상호 인증 및 세션키 분배 시스템을 제안한다. 제안하는 시스템은 사용자의 관리가 용이한 스마트기기를 모바일 게이트웨이 및 WoT 프락시로 사용한다. 제안기술은 ISO 9798 표준화 기술을 수정하여 메시지 전송량을 줄이고 암호 프리미티브 계산량을 감소시키도록 했다. 또한 제안 기술은 재전송 공격, 스푸핑 공격, 선택 평문/암호문 공격, 및 DoS 공격 등에 대응 할 수 있다.

Key words : WoT(Web of Things), IoT(Internet of Things), Authentication, LLN, DTLS

ABSTRACT

WoT (Web of Things) was proposed to realize intelligent thing to thing communications using WEB standard technology. It is difficult to adapt security protocols suited for existing Internet communications into WoT directly because WoT includes LLN(Low-power, Lossy Network) and resource constrained sensor devices. Recently, IETF standard group propose to use DTLS protocol for supporting security services in WoT environments. However, DTLS protocol is not an efficient solution for supporting end to end security in WoT since it introduces complex handshaking procedures and high communication overheads. We, therefore, divide WoT environment into two areas- one is DTLS enabled area and the other is an area using lightweight security scheme in order to improve them. Then we propose a mutual authentication scheme and a session key distribution scheme for the second area. The proposed system utilizes a smart device as a mobile gateway and WoT proxy. In the proposed authentication scheme, we modify the ISO 9798 standard to reduce both communication overhead and computing time of cryptographic primitives. In addition, our scheme is able to defend against replay attacks, spoofing attacks, select plaintext/ciphertext attacks, and DoS attacks, etc.

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA- 2013-H0301-13-1003)
◆ 주저자 : 덕성여자대학교 컴퓨터공학부, jiyepark@duksung.ac.kr, 학생회원
° 교신저자 : 덕성여자대학교 컴퓨터공학부, kang@duksung.ac.kr, 정회원
논문번호 : KICS2013-04-184, 접수일자 : 2013년 4월 25일, 최종논문접수일자 : 2013년 5월 15일

Ⅰ. 서 론

오늘날 사람들은 평균적으로 스마트폰, 스마트패드, 노트북등 인터넷과 연결되는 최소 2개 이상의 스마트 기기를 가지고 있다. 2015년까지 개인당 소유 스마트 기기는 최소 7개로 증가하고, 약 250억 개의 디바이스들이 무선 인터넷을 기반으로 서로 연결될 것이라고 예상된다[1].

유럽 표준화 기구인 ETSI는 M2M(Machine to Machine)에 관한 표준화 작업을 진행하고 있으며 ITU-T의 경우 IoT(Inthernet of Things)혹은 MOC라는 용어를 사용하고 있으나 대부분 유사한 개념을 적용하고 있다[2].

IoT란 무선 통신이 가능한 각각의 사물들이 연결되어 지능화 통신을 하는 것이다. IoT는 각종 센서와 모바일 디바이스 등 이종(heterogeneous) 간 상호 접속 네트워크라는 특징을 가진다. 이러한 특징으로 인해 제조사별 기기마다 다양한 사설표준이 만들어지고 구현되어 이기종의 디바이스 간 원활한 상호운영에 어려움이 있다. 따라서 진정한 IoT 개념을 구현하기 위해서는 제조사나 기기 특성에 구애받지 않는 단일화된 표준 플랫폼이 필요하다. ETH zurich에서는 이러한 문제를 해결하고자 모든 사물을 Web으로 통합하는 WoT(Web of Things)라는 개념을 제시하였다[3]. IETF CoRE 작업 그룹에서는 WoT 환경에서 메시지 전송의 표준화 방안으로 CoAP(Constrained Application Protocol)이라고 불리는 경량화된 웹 프로토콜의 표준화를 진행하고 있다[4]. CoAP은 센서와 같은 제약이 많은 환경에서 웹 서비스를 제공하기 위한 프로토콜로 HTTP와 같이 REST(Representational State Transfer)형식을 기반으로 한다.

그림 1은 WoT 환경 구성 요소를 도식화 한 것이다. WoT 환경은 CoAP을 지원하는 센서, CoAP을 지원하지 않는 레거시 디바이스, 모바일 게이트웨이(경우에 따라 프록시기능 사용), 인터넷 환경의 서버, 클라이언트 등으로 구성된다. WoT 환경에서 센서들은 기존 센서 네트워크에서 단순히 정보를 요청받고 제공하는 역할과 다르게 정보의 제공은 물론 경우에 따라 정보를 요청 할 수 있다. 그림 1의 LLN 영역을 스마트기기를 사용하는 사용자 중심의 네트워크(e.g. BAN(Body Area Network, CAN(Car Area Network))에 적용하여 스마트 헬스케어나 스마트 카와 같은 서비스를 제공할 수 있다.

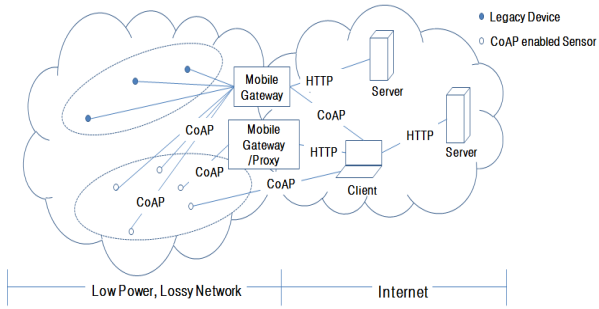


그림 1 . WoT 네트워크 구조
Fig. 1. WoT Network Architecture

WoT환경에서 스마트 헬스케어와 같은 서비스를 제공하기위해서는 정보의 기밀성이 보장되어야 하고 스마트 헬스케어에 이용되는 센서들과 실시간 센서와 통신할 수 있는 모바일 게이트웨이 간 안전한 인증이 사전에 이루어 져야한다.

CoAP 표준에서는 종단 간 보안을 제공하기위한 한 방안으로 PSK(Pre-Shared Key)를 이용한 DTLS(Datagram Transport Layer Security) 프로토콜을 적용하려 한다[4,5]. DTLS는 UDP와 같은 데이터그램 프로토콜을 사용하는 응용서비스에 데이터 기밀성, 무결성, 사용자 인증 등을 제공하는 보안 프로토콜이다. 하지만 DTLS 프로토콜을 이용한 인증, 세션키 분배과정은 많은 핸드쉐이킹 메시지로 LLN(Low-power, Lossy Network)에 적합하지 않다. 따라서 LLN환경과 Internet 환경을 구분하여 LLN환경적 특성에 맞는 인증, 세션키 분배 방안이 필요하다. DTLS나 TLS의 적용은 모바일 게이트웨이를 통해 수행된다. 다음 그림 2는 DTLS 프로토콜 적용 구간과 본 논문에서 제안하는 시스템 적용구간을 나타낸다.

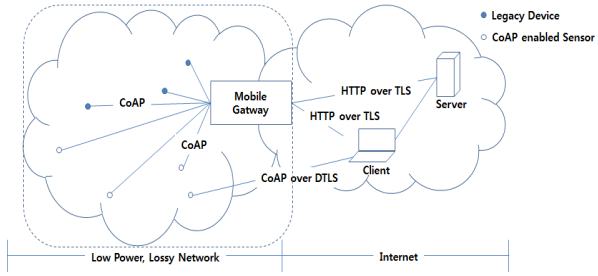


그림 2 . 두개로 구분된 보안 영역
Fig. 2. Two Different Security Domain

본 논문에서는 점선으로 표기된 LLN구간에서 센서와 모바일 게이트웨이 간 상호 인증 방안을 제안한

다. 센서와 모바일 게이트웨이는 단일 홉으로 연결된 환경으로 가정한다. 제안 시스템은 LLN환경에서 3단계로 구성된 통신절차를 통해 장치 간 상호인증과 세션키 공유 방안을 제공한다. 또한 전송량을 감소시켜 무선 자원의 효율성을 증가 시킨다. 인터넷 구간에서는 모바일 게이트웨이를 통해 HTTP/TLS 혹은 CoAP/DTLS로 동작된다.

본 논문의 구성은 다음과 같다. 2장에서는 시스템 제안 배경과 제안 시스템의 기본 개념에 대해 기술한다. 3장에서는 본 논문에서 제안한 상호인증 시스템에 대해서 기술하고, 4장에서는 제안한 시스템에 대한 보안 분석과 성능 분석을 기술한다. 최종적으로 5장에서 결론을 맺는다.

Ⅱ. 시스템 제안 배경

본 장에서는 IoT/WoT 환경에서 안전한 통신을 제공하기 위해 선행되어야 하는 장치 간 상호 인증 시스템의 제안 배경을 기술한다. 특히, IoT/WoT 환경을 고려하여 자원 제한적인 장치와 이를 도와주는 역할을 담당하는 모바일 게이트웨이(혹은 역할에 따라 모바일 프락시)의 특성을 고려한다[4].

제안하는 시스템은 ISO 9798에 기술된 인증 방안을 기반으로 설계된다. ISO 9798은 RFID 리더와 태그로 구성된 센서 환경에서 객체 간 상호 인증을 제공하기위해 표준화된 방안이다[6]. 표 1은 본 논문의 제안 시스템에서 사용되어지는 시스템 파라미터들을 보여준다.

표 1. 시스템 파라미터
Table 1. System Parameter

Parameter	Interpretation
$r1, r2$	Random nonce
I	Initiator
R	Responder
$Token$	Encrypted message

2.1. ISO 9798 3단계 상호인증

다음 그림 3은 3단계 상호인증을 도식화 한 것으로 두 주체는 비밀 키 값이 K_{AB}를 사전에 공유하고 있다고 가정한다. 동작 절차는 다음과 같다.

2.1 ISO 9798 상호인증 동작 절차

(1) 인증 절차 개시자 I는 난수 R_B를 보내 인증을 개시

(2) R은 난수 R_A를 생성 후, I로부터 받은 난수 값 R_B, 벡터 값 IV와 함께 공유된 키 K_{AB}로 암호화 한 $Token_{AB}$값을 I에게 전송

(3) I는 $Token_{AB}$을 복호화 하여 난수 R_B 값을 통해 태그를 인증하고 R_A, R_B 값을 다시 암호화 하여 R에 전송

그림 3. RFID 리더와 태그간의 3단계 상호인증 절차
Fig. 3. 3-pass Mutual Authentication Procedure between RFID reader and tags

상기 기술한 표준 방안을 IoT/WoT 환경에 변경 없이 적용할 경우 몇 가지 제한사항이 따른다. 첫째, 인증 메시지를 주고받는 양측 모두 난수 생성, 암호화, 복호화를 반드시 한번 씩 하게 된다. 이는 컴퓨팅 자원이 제한적인 센서에 부담이 될 수 있다. 둘째, 표준화 방안에서는 리더가 인증 절차를 개시한다. 그러나 IoT/WoT 응용에서는 센서가 필요 시 모바일 게이트웨이나 프록시에게 데이터를 전송할 필요가 있다. 이 경우 인증 절차의 개시는 센서가 담당해야 한다. 셋째, 표준화 방안에는 DoS 공격에 대응하거나 DoS 공격을 경감시킬 방안이 마련되어 있지 않다.

2.2. 제안 시스템의 기본 개념

본 절에서는 2.1절에 기술한 제한사항을 개선할 수 있는 방안의 기본 개념을 기술한다. 특히, RFID와 달리 모든 기기는 인증 개시자 I와 응답자 R 역할을 수행할 수 있다. 그러나 반사공격(Reflection Attakc)에 대응하기 위해 사전 설정 과정에서 I, R 역할을 결정 한 후 동작된다고 가정한다.

그림 4는 제안 시스템의 기본 개념을 나타낸 것으로 3장에서 설명할 제안 시스템의 기본 개념을 나타낸다.

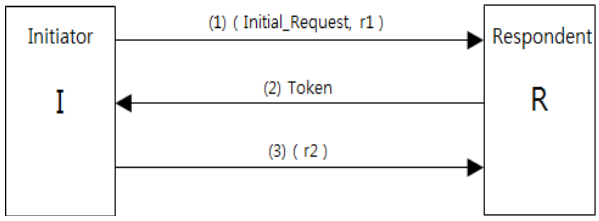


그림 4 . 제안하는 인증 절차
Fig. 4. Proposed Authentication Procedures

2.2 제안 시스템의 기본 인증 절차

(1) $I \rightarrow R$: {Initial_Request, r1}
인증 절차 개시자 I는 난수 r1을 생성한 후, R에게 Initial_Request 메시지와 함께 전송

(2) $R \rightarrow I$: {Token}, where Token =E_k(r1||r2) R은 공유된 키(k)를 이용해 전송받은 r1과 자신이 생성한 난수 r2를 암호화하여 Token을 I로 전송

(3) $I \rightarrow R$: {r2}
I는 Token에서 복호화 한 r1 값을 확인하여 R을 인증할 수 있고, R이 I를 인증할 수 있도록 r2를 전송

상기 방식은 전송되는 난수(i.e. r1, r2)가 평문으로 전송되므로 선택 평문 공격이나 선택 암호문 공격에 취약하다. 공격자는 자신이 선택한 평문 메시지(즉, 거짓 난수 r1, r2)를 인증 응답자 R에게 전송하고 이 메시지의 암호문을 도청을 통해 취득할 수 있다. 공격자는 이 과정을 반복하여 (평문, 암호문)에 대한 쌍들을 통해 암호문(Token)에 대한 난수 값들을 유추하거나 키 값을 유추해 낼 수 있다. 이와 마찬가지로 선택 암호문 공격자는 전송되는 모든 메시지를 통해 공격자가 선택한 암호문과 이에 해당되는 평문을 얻을 수 있다. 이 과정을 다수 반복한 후 수집한 (암호문, 평문) 데이터들을 토대로 공격자는 키를 유추해 낼 수도 있다. 또한 (2)번 과정에서 전송되는 Token의 크기는 r1과 r2의 연접된 데이터의 암호값이므로 전송량이 크다. 이러한 문제점을 해결하면서 계산 성능을 개선시키고 전송량을 감소시킬 수 있는 방안을 다음 장에 제안한다.

Ⅲ. 제안 시스템

3.1. 상호 인증 시스템

제안 시스템은 두 번 암호 연산을 수행하는 표준화 방안의 암호 연산을 한 번으로 줄여 성능을 향상시킨다. 또한 2.2절에 제시한 보안 취약성에 대응할 수 있도록 암호학적 해쉬 함수를 적용한다. 즉, 그림 4의 (1) 과정은 동일하나 (2)의 단계에서는 전송되는 메시지의 길이가 50% 감소되고, (3)으로 표기된 단계에서 전송되는 평문을 해쉬한 값으로 대체한다. (2)번 과정의 r1(f_h)와 r1(l_h)는 I 가 생성한 r1을 반으로 나누어 그 중 앞부분을 r1(f_h)로, 나머지 r1의 1/2을 r1(l_h)로 정한다(4.4절 참조). 인증 절차는 다음과 같다.

3.1 상호 인증 절차

(1) $I \rightarrow R$: {Initial_Request, r1}

(2) $R \rightarrow I$: {Token}, where Token = Ek(r1(f_h)||r1(l_h)⊕r2)
인증 응답자 R은 공유된 키(k)를 이용해 전송받은 r1중 r1(f_h) 부분과 r2⊕r1(l_h)부분을 연접한 후 암호문인 Token을 계산하여 I로 전송

(3) $I \rightarrow R$: {h(r2)}
I는 전송받은 Token을 복호화 하여 얻은 r2를 일방향성이 제공되는 암호학적 해쉬를 이용하여 R에게 전송

(4) R
전송받은 h(r2)를 자신이 보낸 r2를 해쉬한 후 비교 검증하여 I를 인증

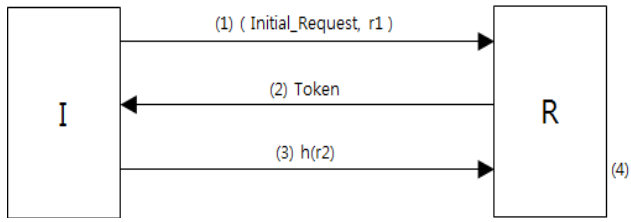


그림 5. 해쉬 함수를 적용한 상호 인증
Fig. 5. Mutual Authentication using Hash functions

3.2. 상호 인증 및 세션 키 분배 시스템

본 절에서는 2.1절에 표준화 된 방안을 적용하여 상호 인증과 세션키를 분배할 수 있는 방안을 기술한다. IoT/WoT 환경에서 센서들은 자원 제약적인 특성으로 인해 기존 인터넷 응용과 다르게 짧은 시간 활성모드로 정보를 제공하거나 취득 한 후 비활성모드(i.e. sleep mode)로 변경되어 배터리 자원을 절약한다. 이렇게 짧은 시간동안 사용될 세션키는 인터넷 응용에서 고려하는 보안 안정성을 고려한 긴 길이의 값을 사용할 필요가 없다. 따라서 두 개체가 공유하고 있는 키를 마스터

키로 사용하여 인증 절차에서 사용하고 상호 인증을 위해 사용하는 값과 같이 세션키를 전송해 줄 수 있는 방안을 제안한다. 또한 2.2절에 언급한 선택 평문 공격, 선택 암호문 공격을 막기 위한 방안도 된다.
인증 절차는 3.1에 제안된 방안과 유사하지만 (2) 절차에서 프록시가 전송해 주는 값에 세션키를 추가하게 된다. 인증 절차는 다음과 같다.

3.2 상호 인증 및 세션 키 분배 절차

(1) $I \rightarrow R$: {Initial_Request, r1}
(2) $R \rightarrow I$: {Token}, where Token=E_K(r1(f_h)||r1(l_h)⊕r2||SK)
전송 받은 r1과 자신이 생성한 난수 r2값을 연접하고 세션키 값인 S_K를 연접하여 함께 암호화 하여 전송
(3) $I \rightarrow R$: {r2}
I는 전송받은 Token을 복호화 하여 얻은 r2를 R에게 전송
(4) R
전송받은 r2를 비교 검증하여 I를 인증

위의 절차로 수행할 경우, S_K를 Blinding Factor로 사용하여 공격자가 평문(r1, r2)을 가지고 있어도 S_K를 모른다면 암호문(Token)을 유추할 수 없으므로 선택 평문 공격을 막을 수 있다. S_K는 새로운 인증 절차 때마다 R이 재계산하여 전송하므로 예측할 수 없고, 자원 제약적인 센서가 새로운 키를 생성할 필요가 없으므로 성능이 개선된다. 그리고 공격자가 암호문(Token)을 가지고 있어도 S_K를 모른다면 평문(r1, r2)을 유추해 낼 수 없으므로 선택 암호문 공격에도 대응할 수 있다.

3.3. DoS 공격대응 방안

본 논문에서 제안한 상호 인증 방안은 센서와 모바일 프록시 어느 쪽이든 먼저 인증 요청을 할 수 있다. 요청메시지는 암호화 되지 않고 전송되며 인증 요청 메시지와 난수만을 포함하기 때문에 누구나 생성 할 수 있다. 만약 여러 명의 공격자가 센서에 인증 요청을 할 경우 센서는 요청 받은 횟수에 해당하는 수만큼 난수 생성과 암호화를 수행해야 한다. 센서가 감당할 수 있는 정도를 넘어선 수준의 인증 요청은 DoS를 발생시킨다. 다음과 같은 방법으로 DoS 공격에 대응 할 수 있다. 다음 그림 6은 아래 제안하는 알고리즘을 의사코드로 나타낸 것이다. 임계값의 경우 센서의 구현/성능 특성과 적용하는 응용 서비스에 따라 다른 값을 적용할 수 있다. 본 논문에서는 최소와 최대 임계값을 60%와 80%로 설정한 예를 기술한다.

제안 의사코드

```
set sensor_capacity to 0%;
set max_threshold_value to 80%;
set min_threshold_value to 60%;
set busy_flag to true;

if(sensor_capacity==max_threshold_value) {
busy message broadcasting;
set busy_flag to false;
.. 요청받은 인증 과정 수행 .. ;
}

if(busy_flag==false && sensor_capacity ==
min_threshold_value) {
not busy message broadcasting;
set busy_flag to true;
}
```

그림 6. DoS 에 대응하기 위한 제안 의사코드
Fig. 6. DoS Defense Method expressed by Pseudo Code

(1) 센서가 수행 할 수 있는 연산 능력의 최대 임계값과 최소 임계값을 설정한다.
(2) 인증요청으로 인한 센서의 부하가 최대 임계값인 80%에 도달할 경우 센서는 통신 반경 안에 있는 모든 디바이스에 Busy 메시지를 Broadcasting 한다.
(3) Busy 메시지를 전달받은 디바이스들은 Busy 전송 기기에게 인증을 요청하지 않는다.
(4) 인증 요청 순서에 따라 암호화 된 메시지를 만들어 전송 한 후 Timer를 동작시켜 일정 시간 이후 다음 메시지가 도착하지 않으면 인증 요청한 디바이스의ID를 삭제한다.
(5) 센서의 부하가 최소 임계값 까지 감소했다면 통신 반경 안에 있는 모든 디바이스에 Not Busy 메시지를 Broadcasting 한다.
(6) Not Busy 메시지를 수신한 장치는 송신장치에게 필요 시 인증 절차를 개시할 수 있다.

Ⅳ. 보안 및 성능 분석

4.1. 재전송 공격 (Replay Attack)

공격자는 센서와 모바일 프록시간 통신 정보를 가지

고 있다가 일정 시간 이후 공격하고자 하는 대상에 재전송 공격을 수행할 수 있다. 본 논문에서 제안한 3.1절과 3.2절의 인증 방안에서는 매 세션마다 새로운 난수를 생성하여 인증에 사용한다. 만약 공격자가 일정 시간 이후 다시 재전송 공격을 한다면 공격자와 모바일 프록시간 혹은 공격자와 센서 간에 새로운 세션이 생기므로 기존의 난수를 이용하였더라도 인증될 수 없다. 따라서 상기 제시한 두 인증 방안 모두 재전송 공격을 막을 수 있다.

4.2. 스푸핑 공격 (Spoofing Attack)

본 논문에서 제안한 3.1절, 3.2절 두 가지 인증방안 모두 같은 방법으로 스푸핑 공격을 막을 수 있다. 공격자가 스푸핑 공격을 하는 경우는 다음과 같다.

(1) 공격자가 모바일 프록시를 속이는 경우 : 공격자는 난수를 생성해 모바일 프록시에 인증 요청을 수행할 수 있다. 하지만 모바일 프록시가 전송하는 암호화 된 값을 받는다 하여도 복호화 할 수 없기 때문에 다음 과정을 진행할 수 없다.

(2) 공격자가 센서를 속이는 경우 : 센서로부터 인증 요청을 받을 수 있지만 공격자는 전송받은 난수를 암호화 할 수 없다. 따라서 센서와 모바일 프록시간 안전하게 공유된 키를 모르는 경우 공격자는 스푸핑 공격을 수행 할 수 없다.

4.3. 선택 평문/암호문 공격 (Chosen Plaintext/ Ciphertext Attack)

상기 제안한 상호 인증 방안 중 해쉬 함수를 이용한 인증 방안에서는 공격자가 r1을 가지고 있다 하더라도 또 다른 난수 r2를 알 수 없기 때문에 (평문, 암호문) 쌍을 통해 공유된 키를 유추해 낼 수 없다. 역으로 암호문을 수집한다 하더라도 새로운 난수 r2를 유추해 낼 수 없으므로 선택 평문 공격, 선택 암호문 공격에 안전하다.

해쉬 함수를 이용하지 않는 상호 인증 및 공격 및 세션키 분배 방안에서는 Blinding Factor(S_K)를 추가하여 공격자가 평문(r1, r2)을 가지고 있어도 S_K를 모른다면 암호문(Token)을 유추할 수 없으므로 선택 평문 공격을 막을 수 있다. 공격자가 암호문(Token)을 가지고 있어도 Blinding Factor(S_K)를 모른다면 평문(r1, r2)을 유추해 낼 수 없으므로 선택 암호문 공격에도 대응할 수 있다.

4.4. 성능 분석

다음 표 2는 표준화된 방안과 제안 시스템의 연산 회수를 비교한다. 제안하는 시스템은 인증만을 고려할 경우 ISO 표준 기술보다 암/복호화 연산을 50% 줄일 수 있다. 세션키 분배 방식을 적용할 경우 암/복호화 보다 연산속도가 빠른 해쉬 함수를 이용하여 계산 시간을 줄였다.

표 2. Performance analysis results
Table 2. 성능 분석 결과

Property	ISO 9798		Mutual Authentication		Mutual Authentication & Key Distribution	
	IO	RO	IO	RO	IO	RO
Random Number Generation	1	1	1	1	1	1
Encryption	1	1	0	1	0	1
Decryption	1	1	1	0	1	0
Hash	0	0	1	1	0	0

(IO: Initiator operation, RO: Responder operation)

데이터 전송 오버헤드를 줄이기 위해 제안 기술은 2.2절의 인증절차에 표기된 연접 대신 XOR을 사용한다. 단순히 r1과 r2를 XOR하여 암호화할 경우 인증 개시자는 복호화 후 자신이 전송한 r1을 검증할 수 없다. 이를 해결하기 위해 제안 시스템은 r1을 반으로 구분하여 앞 부분은 r1의 검증 값으로 사용하고 뒷부분은 r2와 XOR을 적용하여 전송량을 감소시켰다.

암호 알고리즘에 사용되는 난수는 예측 불가능 한 값으로 블록 암호나 해쉬 함수를 주로 이용하여 생성한다[7]. 안전하지 않은 통신 채널에 전송되는 난수는 선택/기지 공격에 대응하고 향후 사용되어질 난수의 예측이 어렵도록 난수 생성기 출력의 두 배 이상의 길이가 권고된다. 따라서 빠르게 연산을 수행하기 위해 해쉬 함수 기반의 난수 생성기를 적용하고 AES 128bit와 동일한 안전도(즉, SHA256이상)를 갖기 위한 난수의 길이는 512bit 이상이 되어야 한다. 다음 표 3은 안드로이드 기반 모바일 환경에서 Bouncy Castle이 제공하는 SHA 256 해쉬 함수를 이용하여 입력 길이별로 연산을 20번 수행한 후 그 평균시간을 나타낸 것이다[8]. 해쉬함수와 블록 기반

암호화 프리미티브는 블록 단위로 연산되므로 입력이 길수록 더 많은 시간이 소요된다. I와 R이 AES 128bit 단위의 블록 연산을 수행하게 되므로 R1||R2와 R1⊕R2는 각각 4번과 2번의 블록 암호 연산을 수행하게 되므로 전송되는 메시지의 양을 줄일 수 있음과 동시에 연산 속도도 50% 줄일 수 있다.

표 3. SHA 256 성능 측정 결과표
Table 3. Performance result for SHA256

Hash Function	Input length (bytes)	Bouncy Castle (micro seconds)
SHA256	256	7080
	512	7187
	768	7280
	1024	8290

V. 결 론

본 논문에서는 ISO 9798에 기술된 인증방안을 기반으로 IoT/WoT 환경적 특성을 고려한 장치 간 상호 인증 시스템을 제안하였다. 제안한 상호 인증 시스템에서는 XOR를 이용하여 메시지 길이를 50% 감소시켰다. 이를 통해 자원 제한적인 LLN환경에서 전송되는 메시지의 양을 50%감소시키고 암호화, 복호화에 필요한 계산량을 감소시킴으로서 성능을 개선하였다. 제안한 상호 인증 시스템은 재전송 공격과 스푸핑 공격, 선택 평문/암호문 공격을 방어할 수 있다. 또한 각 장치의 서비스 자원의 임계값을 적용하여 DoS에 대응 할 수 있다.

참 고 문 헌

[1] EU, European Commission - Press release, Retreived Apr., 12, 2012, from http://europa.eu.

[2] S. K. Yoo, Y. G. Hong, and H. J. Kim, "Smart mobile services - M2M technology and its standardization trends," J. ETRI, vol. 26, no. 2, Apr. 2011.

[3] D. Guinard, A web of things application architecture-integrating the real-world into the web, Retrieved Dec, 1, 2012, from http://www.webofthings.org.

[4] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," IETF CoRE WG draft, Apr., 2013.

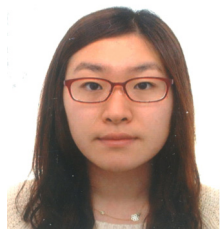
[5] O. G.-Morchon, S. L. Keoh, S. S. Kumar, R. Hummen, and R. Struik, "Security considerations for the IoT," IETF CoRE WG draft, Mar., 2013

[6] Z. Lan and Z. Huaibei, "An improved approach to security and privacy of RFID application system," in Proc. Int. Conf. Wireless, Commun., Networking and Mobile Comput., vol. 2, pp. 1195-1198, Wuhan, China, Sep. 2005.

[7] KISA, "Research for Random number generator using a domestic cipher algorithm," *KISA-WP-2011-0039*, 2011

[8] M. Son and N. Kang, "Design and implementation of Java crypto provider for Android platform," *J. KICS*, vol. 37C, no. 9, pp. 851-858, Sep. 2012.

박 지 예 (Jiye Park)



2013년 2월 덕성여자대학교 컴퓨터공학부 졸업

2013년 3월~현재 덕성여자대학원 전산정보통신학과 석사과정

<관심분야> 네트워크 보안, Web of Things>

강 남 희 (Namhi Kang)

2001년 2월 숭실대학교 정보통신대학원 공학석사

2004년 12월 University of Siegen 컴퓨터공학과 공학박사

2009년 3월~ 덕성여자대학교 디지털미디어학과 조교수

<관심분야> 유무선 인터넷통 신, 통신보안, 시스템 보안>