안전한 CoAP 환경을 위한 경량 인증기법

우시재*, 김대현*, 곽진**
*아주대학교 컴퓨터공학과 정보보호응용및보증연구실
**아주대학교 사이버보안학과
e-mail:sjwoo.isaa@gmail.com*, kdhop1234@gmail.com*, security@ajou.ac.kr**

A Study on Lightweight Authentication Scheme for Secure CoAP Environment

Si-Jae Woo*, Dae-Hyun Kim*, Jin Kwak**
*ISAA Lab., Department of Computer Engineering, Ajou University
**Department of Cyber Security, Ajou University

요 약

IoT 환경에서 사용되는 프로토콜 중 IETF의 CoRE 워킹 그룹에서 채택한 IoT 프로토콜 CoAP가 표준으로 사용되고 있으며 IoT 인증 프로토콜에 대한 연구도 활발하게 이루어지고 있다. CoAP 프로토콜은 저전력, 저용량 메모리 등의 제한된 환경에서 IoT 센서 디바이스들 간의 통신을 지원한다. CoAP 프로토콜은 안전성을 제공하기 위해 DTLS와 함께 사용되는데, 점점 경량화 되어가는 IoT 환경에서 오버헤드가 존재하는 DTLS에 대해 개선되어야 할 사항들이 존재한다. 이를 개선하기 위해 DTLS의 문제점을 해결하기 위한 여러 연구들이 진행되고 있으며, 본 논문에서는 LESS 인증기법을 분석하고 이를 기반으로 보다 향상된 효율성을 제공하는 기법을 제안한다.

1. 서론

IoT는 사용자의 편리함을 높임과 더불어 사회의 생활 패턴을 변화시키고 있으며, Gartner가 선정하는 10대 전략 기술에 매년 선정되어 ICT 시장의 산업을 이끌어가는 핵심 가치로 주목받고 있다[1]. 이에 따라 IoT 환경에서 사용할 다양한 프로토콜에 대한 연구들이 이루어지기 시작하였고, IETF(Internet Engineering Task Force)의 CoRE (Constrained RESTful Environments) 워킹 그룹에서는 CoAP(Constrained Application Protocol) 프로토콜을 표준으로 채택하였다[2].

CoAP 프로토콜은 IoT 센서 디바이스들을 대상으로 효율적인 환경을 제공해주지만 안전성을 제공하기 위해서 DTLS(Datagram Transport Layer)와 함께 사용된다. 하지만 DTLS는 점점 경량화 되어가는 IoT 환경에 적합하지 않은 오버헤드가 발생한다는 문제점이 발견되었고, 이를 해결하기 위한 여러 연구들이 진행되고 있다[3].

따라서 본 논문에서는 IoT 환경에서 DTLS의 문제점을 해결하기 위해 연구된 LESS 인증기법을 분석하고, 보다 향상된 효율성을 제공할 수 있는 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 CoAP과 DTLS, LESS 인증기법에 대한 관련연구를 분석한다. 3장에서는 분석한 연구를 기반으로 효율적인 인증기법을 제안하며, 4장에서 제안기법에 대한 안전성 및 효율성을 분석한다. 이후, 5장에서 결론을 맺는다.

1) 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음
(IITP-2017-2015-0-00403)

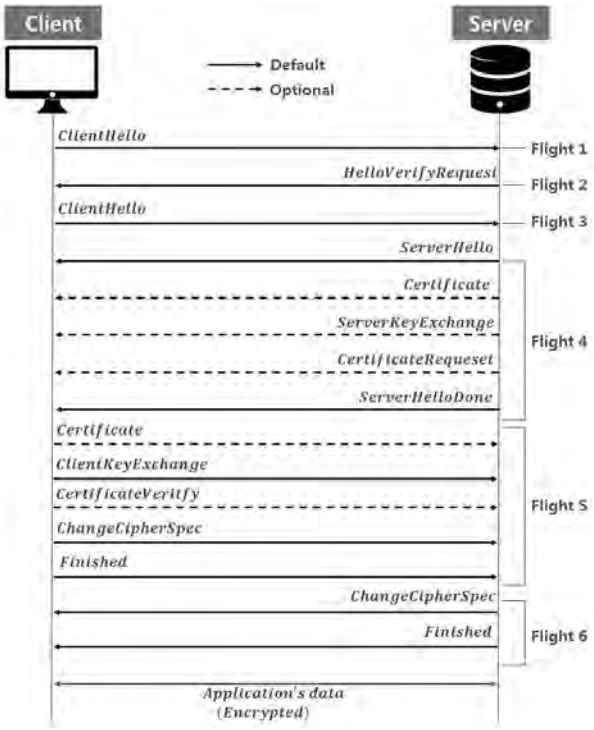
2. 관련연구

2.1 CoAP

CoAP은 M2M(Machine to Machine) 요구사항을 만족시키는 REST(Representational State Transfer) 기반 저성능 노드용 응용계층 프로토콜이다[4]. IoT 환경에서 사용되는 센서 디바이스들은 일반적으로 사용되는 PC, 스마트폰 디바이스 등과는 다르게 대부분 저전력 프로세스, 경량의 배터리 등을 사용하여 성능에 대한 제약사항을 갖는다. 이러한 성능 제약사항을 갖는 센서 디바이스들을 대상으로 제공하는 프로토콜이 CoAP이며, DTLS를 같이 사용함으로써 안전한 통신 환경을 제공한다.

2.2 DTLS

DTLS는 Transport Layer인 TCP 프로토콜에 보안성을 제공하는 TLS(Transport Layer Security) 프로토콜을 UDP 프로토콜에서도 적용하게 해주는 보안 프로토콜이다. UDP 프로토콜 기반 애플리케이션들은 DTLS를 사용함으로써 재전송 공격, 트래픽 분석을 통한 공격, 서비스 거부 공격 등 네트워크 상에서 발생할 수 있는 공격들에 대한 안전성을 제공하며 (그림 1)은 DTLS에서의 Handshake 과정을 나타낸다[5]. 하지만 DTLS는 IoT 환경에서 점점 경량화 되어 성능이 제한적인 IoT 센서 디바이스에서 사용하기에는 적합하지 않다. 그러므로 IoT 센서 디바이스를 위해 효율성 측면으로 경량화 된 인증기법에 대한 연구가 필요하다.



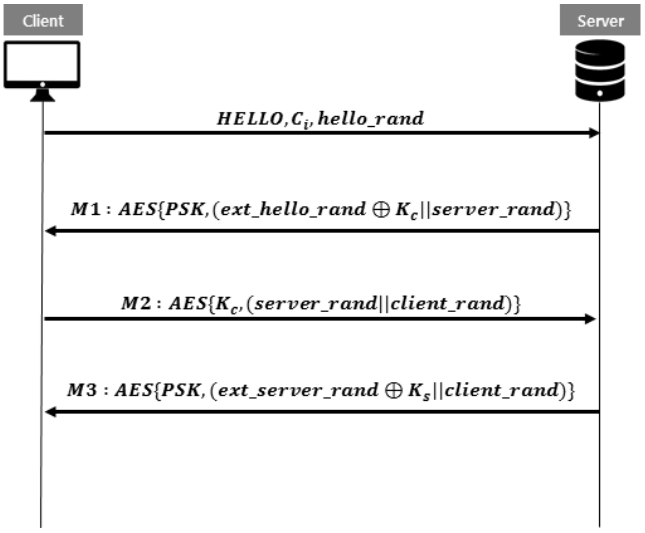
(그림 1) DTLS Handshake 프로토콜

2.3 LESS

LESS(Lightweight Establishment of Secure Session) 인증기법은 CoAP 환경에서 DTLS의 문제점을 해결하기 위해 연구된 경량 인증기법이며, DTLS에서 제공하는 안전성을 보장하면서 DTLS보다 효율적인 인증기법을 제안하였다[6]. <표 1>은 LESS 인증기법에서 사용되는 표기법을 나타내며, (그림 2)는 LESS 인증기법에 대한 전체적인 프로세스를 나타낸다. 자세한 설명은 다음과 같다.

<표 1> LESS에서 사용되는 표기법

표기법	설 명
$HELLO$	- 통신 시작을 위한 메시지
C_i	- 클라이언트의 고유 ID이며 서버에 등록되어 있는 정보
PSK	- 사전에 공유된 비밀정보
K_c	- 통신을 위해 클라이언트 측에서 암호화에 사용할 세션키
K_s	- 통신을 위해 서버 측에서 암호화에 사용할 세션키
$hello\_rand$	- 통신 시작을 위해 클라이언트로부터 $\{0, 1\}^{96}$형태로 생성된 난수
$server\_rand$	- 클라이언트 검증을 위해 서버로부터 $\{0, 1\}^{96}$형태로 생성된 난수
$client\_rand$	- 서버 검증을 위해 클라이언트로부터 $\{0, 1\}^{96}$형태로 생성된 난수
ext_*	- * 값들에 대한 128비트 확장



(그림 2) LESS 인증기법

Step 1. 클라이언트는 통신을 시작하기 위해 $HELLO$, C_i, $hello_rand$를 서버에게 전송한다.

Step 2. 서버는 C_i 검증 후 K_c, $server_rand$를 생성하고, $hello_rand$를 확장하여 ext_hello_rand를 생성한다. ext_hello_rand와 K_c를 XOR 연산한 후 $server_rand$를 연접하여 평문 M1을 구성한다. 그 후 사전에 공유된 비밀정보 PSK를 이용하여 M1을 AES 암호화하고 이를 클라이언트에게 전송한다.

Step 3. 클라이언트는 ext_hello_rand가 검증된 값이라고 가정한 후 $client_rand$를 생성한다. 검증에 대한 가정은 추후 Step에서 $server_rand$에 대한 검증을 통해 이루어진다. $server_rand$와 $client_rand$를 연접하여 M2를 구성한다. 그 후 서버로부터 생성된 K_c를 기반으로 M2를 AES 암호화하여 서버에게 전송한다.

Step 4. 서버는 $server_rand$를 검증하게 된다. 유효한 $server\_rand$ 일 경우, K_s를 생성하고 $server_rand$를 확장하여 ext_server_rand를 생성한다. ext_server_rand와 K_s를 XOR 연산한 후 $client_rand$를 연접하여 M3를 구성한다. 그 후 PSK를 이용해 M3를 AES 암호화 후 클라이언트에게 전송하게 된다. 클라이언트는 PSK를 이용해 전송받은 암호문을 복호화하며 $client_rand$에 대한 검증 후 K_s를 추출하게 된다.

위와 같은 과정으로 클라이언트와 서버는 안전한 세션을 구축하여 통신할 수 있다. 하지만 LESS 인증기법에서도 불필요한 변수들이 존재하며 초경량·저전력을 목표로 하는 IoT 환경의 센서 디바이스에 적용하기 위한 최적화가 필요하다.

3. 제안기법

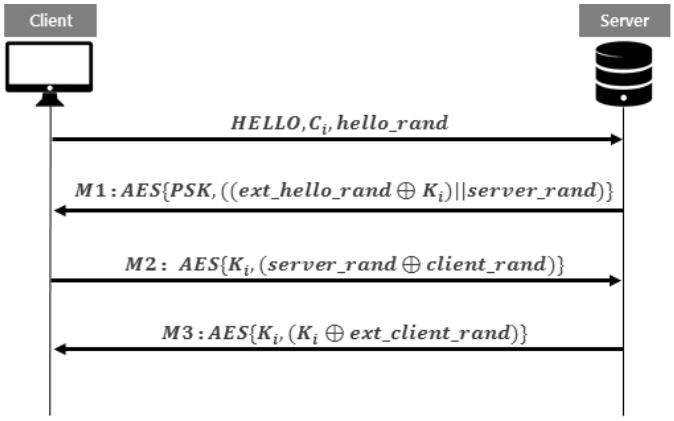
본 절에서는 2.3절에서 분석한 LESS 인증기법을 개선하여 기존 LESS 인증기법보다 경량화 된 인증기법을 제안한다. 제안기법에서는 IoT 센서 디바이스 환경을 고려하여 클라이언트 측에서 발생하는 연산량을 줄이고, 두 개의 세션키 K_c와 K_s를 하나의 K_i로 통합함으로써 기존 LESS 인증기법보다 효율적인 성능을 제공할 수 있는 인증기법을 제안한다.

<표 2>는 제안기법에서 사용할 변수들을 정의하는 표기법을 나타낸다.

<표 2> 제안기법에서 사용되는 표기법

표기법	설 명
$HELLO$	- 통신 시작을 위한 메시지
C_i	- 클라이언트의 고유 ID이며 서버에 등록되어 있는 정보
PSK	- 사전에 공유된 비밀정보
K_i	- 통신을 위한 세션키
$hello\_rand$	- 통신 시작을 위해 클라이언트로부터 $\{0, 1\}^{96}$형태로 생성된 난수
$server\_rand$	- 클라이언트 검증을 위해 서버로부터 $\{0, 1\}^{96}$형태로 생성된 난수
$client\_rand$	- 서버 검증을 위해 클라이언트로부터 $\{0, 1\}^{96}$형태로 생성된 난수
ext_*	- * 값들에 대한 128비트 확장

본 논문에서는 클라이언트와 서버 간의 통신을 기준으로 설계하였다. (그림 3)은 제안기법에 대한 Flowchart를 나타내며, (그림 4)는 제안기법에 대한 전체적인 프로세스를 나타내며 제안기법에 대한 설명은 다음과 같다.



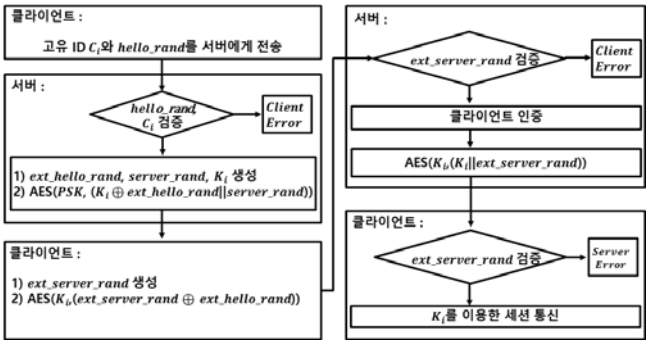
(그림 3) 제안하는 인증기법

Step 1. 통신을 시작하기 위해 클라이언트가 서버에게 $HELLO$, C_i, $hello_rand$를 전송한다.

Step 2. 서버는 $HELLO$, C_i을 검증 후 K_i, ext_hello_rand 그리고 $server_rand$를 생성한다. 그 후 K_i와 ext_hello_rand를 XOR 후 $server_rand$를 연접하여 M1을 구성한다. 사전에 공유된 PSK를 이용하여 M1을 AES 암호화 후 클라이언트에게 전송한다.

Step 3. 클라이언트는 수신받은 메시지를 PSK를 이용하여 복호화한다. 그 후 클라이언트가 생성했던 $hello_rand$를 이용하여 ext_hello_rand를 검증하고, $client_rand$를 생성한다. 생성된 $client_rand$와 $server_rand$를 XOR 연산하여 M2를 구성하고, 이를 K_i를 이용하여 암호화 후 서버에게 전송한다. 기존 LESS 인증기법에서는 연접을 사용하여 메시지 길이가 증가하였지만 본 제안기법에서는 연접을 XOR 연산으로 교체함으로써 효율적인 연산을 가능하게 한다.

Step 4. 서버는 K_i를 이용하여 수신받은 M2 메시지를 복호화한다. 메시지 평문을 $server_rand$와의 XOR 연산을 통해 $client_rand$를 추출하고 이를 확장하여 ext_client_rand를 생성한다. K_i와 ext_client_rand를 XOR 연산하여 M3를 구성한다. 이를 K_i를 이용하여 암호화 후 클라이언트에게 전송하게 되며, 클라이언트는 ext_client_rand에 대한 검증을 통해 안전한 세션을 생성한다.



(그림 4) 제안기법에 대한 Flowchart

4. 안전성 및 효율성 분석

4.1 안전성 분석

• S1 : 재전송 공격 방지

본 논문에서 제안하는 기법은 난수 $rand$를 기반으로 인증과 키 교환이 이루어진다. $rand$는 통신하는 각 클라이언트와 서버에서 하나씩 생성되며, 인증 handshake 과정에서 $rand$가 전송될 때마다 변화를 줌으로써 재전송 공격에 대해 안전성을 제공한다.

• S2 : 트래픽 분석을 통한 공격 방지

본 논문에서 제안하는 기법은 서버가 클라이언트와 공유하는 $rand$를 사용하여 K_i를 난독화한다. 따라서 공격자가 트래픽 분석을 통해 PSK를 예측할 경우, 세션키 K_i를 알아내기 위해 각 세션에 대해 AES-128에 대한 공격 복잡도인 2^{128}만큼의 계산을 시도해야한다. 그러므로 트래픽 분석을 통한 공격에 대해 안전성을 제공한다.

• S3 : 서비스 거부 공격에 대한 효과 최소화

본 논문에서 제안하는 기법은 클라이언트의 $HELLO$ 메시지 전송 후 서버로부터 생성된 $server_rand$를 올바르게 추출하여 해당 값이 올바를 경우에만 다음 Step을 진행할 수 있다. 그러므로 공격자가 유효하지 않은 메시지를 이용하여 서비스 거부 공격 시도할 경우, $server_rand$에 대한 검증을 할 수 없기 때문에 공격에 대한 효과를 최소화 할 수 있다.

4.2 효율성 분석

• IoT 센서 디바이스 연산량 감소

3절에서 설명한바와 같이 연산의 재구성을 통해 Step 3에서 사용되는 M2 메시지의 길이를 감소시켰다. M2 메시지 길이의 감소를 통해 IoT 센서 디바이스에서의 연산량을 줄임으로써 IoT 센서 디바이스에 적합한 환경을 제공할 수 있다. 이를 통해 기존 LESS 인증기법보다 향상된 효율성을 제공한다.

• 네트워크 오버헤드 감소

본 논문에서 제안하는 기법은 DTLS를 경량화한 LESS 인증기법의 연산보다 적은 수준의 연산을 이용하여 클라이언트 측에서 계산하는 연산량을 줄였다. 제안기법에서 사용한 M1~M3 메시지 길이의 총 합은 기존 LESS 인증기법보다 더 작은 길이를 갖는다. 줄어든 메시지의 길이로 인해 각 Step에서 AES 암호화 시 LESS 인증기법보다 빠른 연산을 제공할 수 있으며 이를 통해 전체적인 네트워크의 오버헤드를 감소시킬 수 있다.

다음 <표 3>은 기존 연구되었던 LESS 인증기법과 본 논문에서 제안한 기법에 대해 안전성 및 효율성을 비교하여 나타낸다.

<표 3> LESS 인증기법과 제안기법의 안전성 및 효율성 비교

기법	안전성			효율성					
	S1	S2	S3	연산		메시지 길이			
				⊕	||	M1	M2	M3	총
LESS	O	O	O	2	3	224	192	224	640
제안기법	O	O	O	3	1	224	96	128	448

5. 결론

본 논문에서는 CoAP에서 안전성을 제공하는 DTLS에 대한 문제점을 해결하기 위해 연구된 LESS 인증기법을 대상으로 분석하고 문제점을 도출하였다. 분석된 문제점을 기반으로 IoT 환경의 센서 디바이스들을 대상으로 보다 최적화된 인증기법을 제안하였다.

본 논문에서 제안한 인증기법은 DTLS를 대체할 수 있는 경량 인증기법인 LESS 인증기법을 기반으로 재설계되었다. DTLS가 제공하는 안전성과 LESS 인증기법이 제공하는 안전성을 모두 제공하도록 설계하였으며, 이에 해당하는 항목에는 재전송 공격 방지, 트래픽 분석을 통한 공격 방지, 서비스 거부 공격 방지가 있다. 또한 제안기법에서는 기존 DTLS보다 경량화 된 LESS 인증기법에서 불필요하게 사용되는 변수와 연산을 분석하였고, 보다 향상된 효율성을 제공할 수 있게 설계하였다.

본 논문에서 제안한 기법을 통해 IoT 환경에서 사용되는 센서 디바이스들을 대상으로 향상된 효율성을 제공할 수 있는 기법을 적용함으로써 초경량·저전력에 근접한 IoT 환경을 제공할 수 있다.

향후에는 DTLS를 대체하기 위해 연구된 경량 인증기법들을 분석하여 제안기법과의 비교분석을 통해 보다 다양한 안전성 및 효율성 분석이 필요하다. 또한 IoT 환경에 맞게 통신하는 개체를 클라이언트와 라우터, 서버 개체의 개수를 확장하면서 요구되는 추가 인증기법에 대한 연구가 필요하다.

참고문헌

[1] Gartner, http://www.gartner.com

[2] ZHENGGUO SHENG, SHUSEN YANG, YIFAN YU, “A Survey on the IETF Protocol Suite for the Internet of Things : Standards, Challenges, and Opportunities”, IEEE Wireless Communications, Vol. 20 Issue. 6, 2013.01.

[3] Arijit Ukil, Soma Bandyopadhyay, Abhijan Bhattacharyya, Arpan Pal and Tulika Bose, “Lightweight security scheme for IoT applications using CoAP”, International Journal of Pervasive Computing and Communications, Vol. 10 No. 4, 2014.10.

[4] Constrained Application Protocol (CoAP), RFC 7252, 2014.06.

[5] Datagram Transport Layer Security Version 1.2, RFC 6347, 2012.01.

[6] Abhijan Bhattacharyya, Tulika Bose, Soma Bandyopadhyay, Arijit Ukil, Arpan Pal, “LESS: Lightweight Establishment of Secure Session: A Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption”, 2015 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.03.