DTLS 기반의 CoAP 보안 메커니즘 분석 및 성능평가★

한 상 우*, 박 창 섭**, 조 정 모*

요 약

자원 제약적 IoT 환경에 최적화 된 표준 프로토콜 CoAP(Constrained Application Protocol)은 IoT 환경 내의 센서노드(CoAP Server) 와 인터넷 상의 클라이언트(CoAP Client) 간의 웹 기반 통신을 지원한다. CoAP은 클라이언트의 CoAP Request 메시지에 대하여 서버의 CoAP Response 메시지로 응답하며 동작하는 Request/Response 모델이다. CoAP에서는 메시지의 보호를 위해 CoAP-DTLS(Datagram TLS)의 사용을 권고하고 있다. CoAP-DTLS에서 권고되는 보안모드(Security Mode)는 PSK(Pre-Shared Key), RPK(Raw Public Key) 및 Certificate가 있다. 하지만 IoT환경에서의 DTLS 사용에 대한 실효성 검증은 진행 중에 있다. 본 논문에서는 보안 모드가 적용될 수 있는 환경인 IETF에서 제시하는 7가지의 활용사례(Use Cases)에 대하여 분석하고 적절한 보안모드 그룹으로 구분한다. 또한 CoAP과 DTLS 보안 모드별 분석을 수행하고, Cooja 시뮬레이터를 통하여 보안채널 생성시간, 보안채널 생성 단계별 시간, 모트의 RAM/ROM 소모량에 대한 성능평가를 수행한 후 실 환경 적용 가능성에 대하여 평가한다.

DTLS-based CoAP Security Mechanism Analysis and Performance Evaluation

Sang woo Han*, Chang seop Park**, Jung mo Cho*

ABSTRACT

Standard Protocol Optimized for Resource-Constrained IoT Environment Constrained Application Protocol (CoAP) supports web-based communication between a sensor node in the IoT environment and a client on the Internet. The CoAP is a Request / Response model that responds to the client's CoAP Request message by responding with a CoAP Response message from the server. CoAP recommends the use of CoAP-DTLS for message protection. However, validation of the use of DTLS in the IoT environment is underway. We analyze CoAP and DTLS security mode, evaluate performance of secure channel creation time, security channel creation step time, and RAM / ROM consumption through Cooja simulator and evaluate the possibility of real environment application.

Key words : IoT(Internet of Things), CoAP(Constrained Application Protocol), DTLS(Datagram TLS), Cooja

접수일(2017년 11월 01일), 수정일(1차: 2017년 12월 25일), 게재확정일(2017년 12월 29일)

★ 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용 계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음. (과제번호 H2101-17-1001)

* 단국대학교/컴퓨터학과 소프트웨어보안

** 단국대학교/소프트웨어학과

★ 본 논문은 2017년도 정부(교육부)의 재원으로 한국 연구 재단의 지원을 받아 수행된 기본 연구지원사업 성과임. (NRF-2017R1D1A1B03027862)

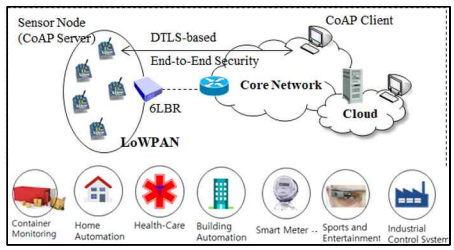
1. 서 론

LoWPAN(Low Power Personal Area Network)이 연동되는 IoT(Internet of Things) 네트워크 아키텍처 관점에서는 제어영역(Control Plane)과 데이터 영역(Data Plane)에서 보안잇슈가 발생한다. 첫째, 제어영역에서는 IoT 관련 프로토콜 자체의 보안잇슈로서 LoWPAN(IEEE 802.15.4 [1] / 6LoWPAN [2]) 보안과 같이 프로토콜에 내재된 Signaling 메시지 보호, 즉 네트워크 인프라를 다양한 보안위협으로부터 보호하는 것이다. 둘째, 데이터 영역에서는 응용계층에서의 보안잇슈로서 Subscriber-Publisher 모델에서의 MQTT(Message Queuing Telemetry Transport [3]) 또는 Client-Server 모델에서의 CoAP(Constrained Application Protocol [4, 5])에 의해 전달되는 응용 데이터에 대한 보호이다. 다양한 센싱 정보를 Sink 노드에서 수합하고 게이트웨이를 거쳐 외부로 전달하는 기존 무선센서 네트워크 보안과의 차별성은, 센서노드(CoAP Server) 자체와 인터넷상의 클라이언트(CoAP Client) 간의 종단간 보안(End-to-End Security)이 요구되는 데에 있다. 이를 위해 IETF에서는 LoWPAN 연동 IoT 환경에서 보안 메커니즘이 적용되는 7개의 활용 사례(Use Case) [6]를 기술하고 있으며 CoAP에 의해 전달되는 응용 데이터 보호를 위한 DTLS(Datagram TLS) [7]의 사용과 이에 대한 실효성 검증연구들이 진행되고 있다 [8, 9, 10]. 본 논문에서는 실효성 검증 연구의 일환으로 안전한 CoAP 응용을 위한 표준 프로토콜인 DTLS의 보안모드에 대한 분석 그리고 각 보안모드가 적용될 수 있는 응용환경 (7 Use Cases)에 대한 분석을 각 보안모드의 성능평가를 기반으로 진행한다. 또한 보안모드의 분석과 성능평가를 기반으로 응용 환경에 대한 적합한 보안 모드를 그룹 화하여 제안한다. 2장에서는 LoWPAN 연동 IoT 아키텍처 및 CoAP 보안을 소개하고 3장에서는 DTLS 기반 CoAP 보안 메커니즘을 보안모드 별로 분석한다. 또한, Use Case 별로 적절한 보안모드를 제시한다. 4장에서는 보안모드 별 성능평가를 Contiki Cooja 시뮬레이터 [10]를 이용하여 진행하며 마지막으로 5장에서 결론을 맺는다.

2. LoWPAN 연동 IoT 아키텍처에서의 CoAP 보안

2.1 LoWPAN 연동 IoT 아키텍처 환경

IETF는 IoT를 지원하는 다양한 프로토콜 표준(Resource Constrained 네트워크와 디바이스 중심으로)을 제정하고 있지만, IoT 환경의 복잡성 그리고 IoT 기반 서비스의 다양한 요구사항에 기인하는 기술적 도전 과제들이 남아있다. IETF에서 제시하는 IoT 무선센서 네트워크는 (그림 1)에서와 같이 자원제약적인 LoWPAN으로 규정하고 있으며 IEEE 802.15.4는 MAC/PHY 계층의 사실 상의 표준이다. 듀얼 스택을 탑재한 6LBR (6LoWPAN Border Router)은 6LoWPAN 기반 LoWPAN의 인터넷 연결을 가능하게 하며, 응용계층에서의 CoAP은 DTLS에 의해 보호된다.



(그림 1) LoWPAN 연동 IoT 및 IETF's 7 Use Cases

IETF ACE 워킹그룹에서는 (그림 1)에서와 같이 LoWPAN 연동 IoT 환경에서 보안 메커니즘이 적용되는 7개의 Use Case들을 규정하고 있다.

2.2 IETF's 7 Use Cases

본 절에서는 IETF ACE 워킹그룹에서 규정하는 7개의 Use Cases에 대한 요구사항 분석이 실시된다. ACE 워킹그룹은 IoT 환경을 사용 환경에 따라 7가지의 Use cases들로 구분하였으며, (그림 1)과 같이 Container Monitoring, Home Automation, Health-Care, Building Automation, Smart Metering,

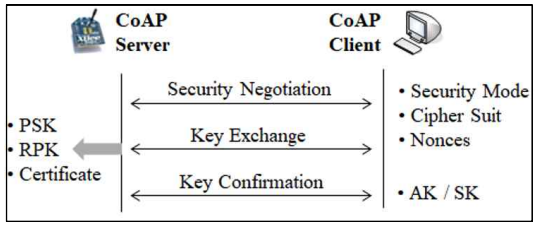
Sports 및 Entertainment, Industrial Control System로 이루어져 있다.

Container Monitoring은 운송 중에 컨테이너 내부의 상태를 실시간으로 확인할 수 있는 환경이다. 각 컨테이너의 소유자는 상이 할 수 있으며, 운송 관리자는 각 컨테이너의 소유자와 상호 인증 및 키를 공유해야 한다. Home Automation은 가정용 장치를 원격으로 액세스 및 관리가 가능한 환경이다. 일반적으로 구성이 간단하며, 쉽게 다른 장치들을 추가 시킬 수 있어야 한다. Health-Care는 사용자가 의료 기관이나 전문가에게 자신의 의료 및 건강 데이터를 제공하여 관리 받는 환경이다. 의료 데이터는 매우 민감하므로 특별한 보호 조치가 필요하며, 비상 상황에 대한 빠른 조치가 필요할 수 있다. Building Automation은 관리자가 빌딩 내의 센서들에 대하여 중앙 집중식 관리가 가능한 환경이다. 빌딩 내의 다양한 그룹이 존재 가능하기 때문에, 그룹 내 관리 및 그룹과 총 관리자 사이의 상호 인증이 필요할 수 있다. Smart Metering은 사용자의 전기, 수도 등의 요금 청구를 위해 일정 시간마다 에너지 소비를 측정하여 관리처에 전달하는 환경이다. 일반적으로 사용자와 관리처 사이의 1 : 1 종단 간 보안이 요구된다. Sports/Entertainment는 사용자가 자신의 활동 데이터를 측정하고 싶을 때 사용 가능한 환경이다. 별다른 노력 없이 간단하게 구성 가능해야 하며, 종종 다른 장치와의 상호 연결이 필요할 수 있다. Industrial Control System은 다수의 센서를 사용하여 산업 공정 제어에 관련된 계측 데이터를 수집하거나 공정을 제어할 수 있는 환경이다. 일반적으로 구성이 어렵고 한번 구성이 되면 추가적인 변경이 발생하지 않는다.

2.3 CoAP과 DTLS

IoT 환경에서의 표준 웹 전송 프로토콜인 CoAP은 자원 제약적인 디바이스(Constrained Device)와의 정보교환을 위한 경량화 된 프로토콜이다. CoAP 종단간에 CoAP Request 및 CoAP Response 메시지의 교환을 통해서 CoAP 클라이언트는 특정 명령어를 센서 디바이스에게 전송하거나 또는 센싱 정보를 CoAP 서버로부터 전달받게 된다. 특히, LoWPAN 환경의 특성을 고려하여 CoAP에서는 CoAP 메시지의 신뢰성 있는 전송을 위해 Exponential-Backoff 방식에 기반을 둔 Stop-and-Wait 전송 프로토콜이 사용된다. CoAP은 일반적인 유니캐스트 환경에서뿐만 아니라, 다수의 CoAP 서버를 대상으로 하는 멀티캐스트 환경에서도 동작된다.

DTLS는 IoT 클라이언트-서버 모델에서의 안전한 CoAP 기반 응용 보안 메커니즘의 사실 상의 표준이다. CoAP-DTLS에서 권고되는 보안모드(Security Mode)는 PSK(Pre-Shared Key), RPK(Raw Public Key) 및 ECDSA 기반 Certificate가 있다. 하지만, PSK 및 RPK의 경우 센서노드와 클라이언트 간의 일대일 사전 보안설정의 어려움으로 확장성이 떨어지고, 반면에 ECDSA 기반 Certifcate의 경우는 확장성 측면에서는 우수하지만 DTLS Full Handshake의 경우 ECC 계산 및 인증서 검증에 너무 많은 시간이 소요되는 단점을 가지고 있다.



(그림 2) DTLS Handshake 프로토콜

DTLS 보안모드는 CoAP 종단간의 상호인증 및 세션키 도출을 위해서 (그림 2)에서와 같이 3단계로 구성되는 DTLS Handshake 프로토콜의 세부동작을 규정한다. 보안협상(Security Negotiation) 단계를 통해서 보안모드 그리고 사용할 Cipher Suit 및 Nonce들이 결정된다. 키 교환(Key Exchange) 단계에서는 보안모드에 따른 인증키(Authentication Key, AK) 및 이를 기반으로 세션키(Session Key, SK)가 도출되며, 마지막으로 키 확인(Key Confirmation) 단계에서 상호인증이 수행된다. 이 모든 과정이 성공적으로 종료되면 도출된 세션키를 이용하여 CoAP 메시지에 대한 보호 작업이 DTLS Record 프로토콜을 통해 실행된다.

3. DTLS 기반의 CoAP 보안 메커니즘 분석 및 Use Cases 보안모드 선정

본 장에서는 DTLS 보안모드의 특성과 IETF ACE 워킹그룹이 규정하는 LoWPAN 연동 IoT 환경에서 보안 메커니즘이 적용되는 7개의 Use Case 별로 적합한 보안모드를 제시해본다.

3.1 DTLS 보안모드 분석

PSK 모드는 CoAP 클라이언트와 CoAP 서버간에 사전에 대칭키가 공유되어 DTLS Handshake 프로토콜이 진행된다. 4장의 성능평가를 통해서 보면 3개의 보안모드 중에서 처리시간 측면에서 가장 효율적인 보안모드이다. 하지만, CoAP 클라이언트와 CoAP 서버간에 대칭키의 사전 공유를 위해서는 별도의 키 공유 아키텍처 및 프로토콜이 요구된다. [9]에서는 별도의 키 서버를 통해서 생성된 대칭키를 양자에게 각각 전달해 주는 프로토콜을 제안하고 있으나, 이 경우에는 CoAP 클라이언트와 CoAP 서버 사이에 종단간 보안이 깨지게 되는 단점이 존재한다. 또한, CoAP 클라이언트와 키 서버 그리고 CoAP 서버와 키 서버간의 사전 보안설정이 전제되어야 하는데, 이에 대한 명확한 솔루션은 제시하지 못하고 있다.

Certificate 모드와 RPK 모드에서는 상호인증을 위해 ECDSA 기반의 공개키와 개인키가 요구된다. 4장의 성능평가에서 이들에 대한 처리시간이 가장 오래 소요되는 이유는 EC (Elliptic Curve) 덧셈연산이 수반되기 때문이다. Certificate 모드에서는 CoAP 클라이언트 및 서버의 공개키를 X.509 v3 형식의 인증서 형태로 발급하여야 함을 전제로 하고 있다. 따라서, 인증서를 발급해 주는 인증기관의 역할을 담당하는 제3의 서버가 존재해야 하며 인증서를 안전하게 발급받기 위한 별도의 보안 메커니즘이 존재해야 한다. 특히, DTLS Handshake가 진행되는 과정에서 상대방의 인증서를 전달받게 되는 쪽은 인증서의 유효성을 확인해야 하기 때문에 OCSP(On-line Certificate Status Protocol) [12]를 별도로 기동시켜야 하는 추가의 부담이 생기게 된다. 또한, 인증서의 크기가 수백 바이트에 달하기 때문에 IEEE 802.15.4 기반의 LoWPAN 환경에서는 프레임의 길이가 127바이트이어야 하는 제약에 걸려 단편화(Fragmentation) 또는 압축(Compression)의 과정을 거치기 때문에 성능 면에 있어서는 다른 2가지 모드들에 비해 현저히 떨어지게 된다. 하지만, Certificate 모드에서는 일단 인증서가 개별적으로 발급이 된 이후에는 임의의 CoAP 클라이언트와 CoAP 서버간에는 별도의 추가 절차 없이 DTLS Handshake가 진행될 수 있다.

RPK 모드는 Certificate 모드가 가지는 2가지의 단점, 첫째 인증서의 길이가 길다는 단점, 둘째 별도의 OCSP가 기동되어야 한다는 단점을 보완하기 위한 보안모드이다. 즉, CoAP 클라이언트와 CoAP 서버는 각각 상대방의 공개키를 사전에 공유하고 있다는 가정을 하고 있다. 만약, 특정 CoAP 서버가 다수의 클라이언트와 DTLS Handshake를 기동하는 응용환경에서는 결국 다수의 상대방 공개키가 사전에 공유되어 있어야 한다. 이는 결국 PSK 모드에 내재된 동일한 문제점을 가지게 된다. 하지만, Certificate 모드와 함께 RPK 모드는 PSK 모드가 제공하지 못하는 Source 인증이 요구되는 응용환경에서는 필수적인 보안모드이다. 따라서, Source 인증이 요구되지만 인증서 사용이 성능 상의 제약으로 가해지는 경우에만 활용이 가능하게 된다.

3.2 Use Case 별 보안모드 선정

본 절에서는 3.1절에서 분석된 3가지 보안모드의 특성과 4장의 성능평가에 따라서 IETF 7가지 Use Case 별로 적절한 보안모드에 대한 선정이 논의된다. Use Case들은 자원 제약적 특성, 연결 설정의 빈도. 연결 상태 지속 시간, 사용 환경을 고려하여 보안 모드를 적용할 PSK 사용 그룹, RPK 사용 그룹, Certificate 사용 그룹으로 구분할 수 있다. 첫 째, PSK 사용 그룹은 자원이 제약적이거나 연결 설정이 자주 발생하는 Use Case들이 속하는 그룹이다. 둘째, RPK 사용 그룹은 연결 설정의 빈도가 낮고 연결 상태의 지속 시간이 지속적으로 이루어지며 단일 그

룹 내에서의 인증이 필요한 환경의 Use Case들이 속하는 그룹이다. 셋 째, Certificate 사용 그룹은 RPK 사용 그룹과 같은 특성을 갖지만 다 그룹간의 인증이 필요한 환경의 Use Case들이 속하는 그룹이다.

3.2.1 PSK 사용 그룹

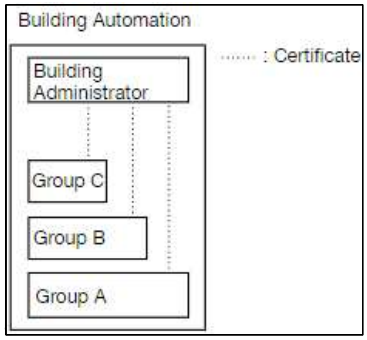
PSK 사용 그룹은 자원 제약적 특성과 사용 환경 그리고 연결 설정의 빈도를 기준으로 결정되는 그룹이다. 3.1절의 DTLS 보안모드 분석에 따르면 PSK의 경우, 처리 시간 측면에서 가장 효율적이지만 사전에 대칭키가 분배되어야 하는 문제점이 발생한다. 그렇기 때문에, 사전에 대칭키를 분배할 수 있는 환경이 만족되면서 처리시간이 적게 들어야 하는 환경에 적합하다. 4.2 절의 Handshake 완료 시간에 의하면 RPK와 Certificate에 비하여 PSK의 연결 설정에 필요한 시간이 상대적으로 빠른 것을 볼 수 있다. 연결 설정의 빈도가 잦은 환경의 경우, RPK와 Certificate는 연결 설정에 필요한 시간이 높은 비율로 증가되기 때문에 PSK 사용이 권고된다. 또한 4.3 절과 4.4 절에 의하면 PSK 모드는 서버에게 부담되는 연산 량과 RAM / ROM 소모량이 가장 적다. 이에 따라 PSK 사용 그룹에는 연결 설정이 빈번하게 이루어지는 환경이나 센서의 자원이 제약적인 환경에 적합하다. 사용자의 조작에 따라 연결 설정의 빈도가 결정되는 Home Automation, Sport/Entertainment 과 일반적으로 센서의 RAM이 10킬로바이트 미만으로 다른 환경보다 더 자원 제약적이며 처리 시간이 빠르게 요구되는 Health-Care가 PSK 사용 그룹에 속하게 된다.

3.2.2 RPK 사용 그룹

RPK 사용 그룹은 연결 상태의 지속 시간과 사용 환경에 의해 결정되는 그룹이다. 3.1 절에 의하면 RPK는 별도의 OCSP가 없이 Source 인증이 필요한 환경에서 적합하다. 별도의 OCSP가 필요하지 않다는 것은 통신이 필요한 개체 간 공개키를 사전에 공유하고 있기 때문에 Source 인증이 가능하다는 것을 말한다. 또한 4.2 절에 의해 연결 설정에 필요한 시간이 크기 때문에 연결 상태가 계속 유지되는 환경에 적합하다. 2.2절의 Use Cases 요구사항에 따라 단일 그룹 내의 보안 통신 환경으로 사전에 공개키를 분배할 수 있으면서 상호 인증이 필요한 Smart Metering, Building Automation, Industrial Control System이 해당 그룹에 속하게 된다.

3.2.3 Certificate 사용 그룹

Certificate 사용 그룹은 RPK과 같은 특징을 갖지만 다 그룹간의 보안통신이 필요한 경우에 사용되는 환경이다. 다 그룹간의(1:n) Source 인증의 경우, 3.1절의 DTLS 보안모드 분석에 따르면 사전에 공개키가 공유되어야 하는 RPK는 부적합하기 때문에 개인키·공개키를 담당하는 인증기관이 필요하게 된다. 다 그룹 간 보안통신이 필요하면서 사전에 공개키를 분배하기 힘든 환경인 Container Monitoring과 (그림 3)과 같이 빌딩 내의 여러 그룹이 존재하고 Building Administrator가 Building의 여러 그룹 내의 센서 관리의 역할을 수행하는 Building Automation 의 경우 Certificate 사용그룹에 속하게 된다.



(그림 3) Certifacate가 사용되는 Building Automation

4. 보안모드 별 성능 분석

본 장에서는 CoAP에서 지원하는 DTLS의 세 가지 모드인 PSK, RPK, Certificate 모드들을 Contiki OS상의 Cooja Simulator를 통하여 성능 분석을 실시한다. 성능 측정은 (그림 1)과 같이 자원에 제약이 있는 센서 노드(CoAP Server)를 기준으로 수행되며, 성능 측정 요소는 각 모드별 DTLS Handshake 소요

시간, Phase 당 시간, 센서 노드의 RAM / ROM 소모량으로 구성된다.

4.1 실험 환경

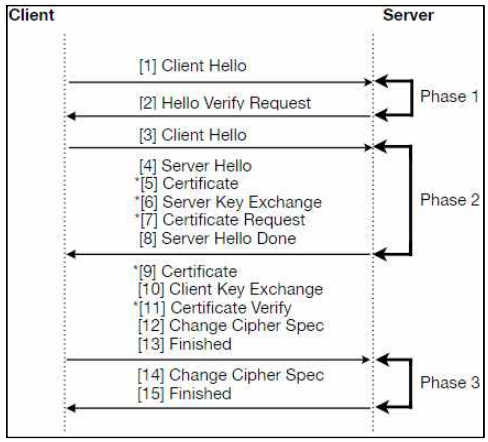
본 논문은 IoT 환경 상의 센서 노드(CoAP Server)와 인터넷 상의 클라이언트(CoAP Client)간의 안전한 통신을 위한 DTLS의 각 모드 별 성능 측정을 목표로 하여 실험 환경을 구성하였다. 성능 측정을 실행한 시뮬레이션 환경은 <표 1>과 같다. Cooja 시뮬레이터를 통해 Border Router와 CoAP 서버를 구성하였으며 tunslip6 명령어를 통하여 외부의 CoAP 클라이언트와 통신이 가능한 IPv6 주소로 매핑하였다. Cooja 상의 각 노드들(CoAP Server, Border Router)은 WSN Applications을 위한 저전력 모듈인 MSP430 시리즈의 Wismote에 컴파일하여 테스트를 진행하였다.

<표 1> 시뮬레이션 환경

환경	설명
OS	Contiki 3.0
Simulator	Cooja
Sensor Node	Wismote(TI MSP 430)
DTLS	TinyDTLS 0.8.2 psk 및 uECC / Certificate

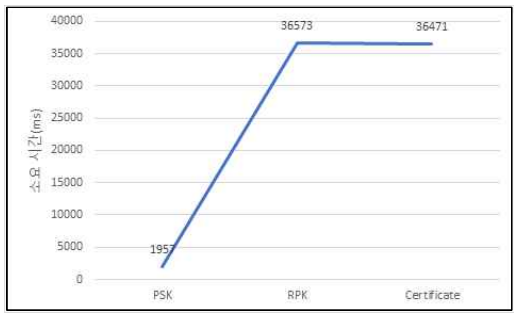
4.2 DTLS Handshake 소요시간

DTLS Handshake 완료 시간은 전체적인 성능의 척도로써 CoAP 클라이언트가 DTLS 연결 시작의 첫 번째 메시지인 CLIENT HELLO 메시지 전송 시간부터 CoAP 서버의 FINISH 메시지의 수신까지의 시간을 측정하였다. (그림 4)는 DTLS Handshake 메시지의 전 과정으로 Phase 1은 (그림 1)의 보안 협상 단계의 초반부로 클라이언트가 서버에게 DTLS Handshake를 시작함을 알리고 서버는 그에 대한 응답을 하게된다. Phase 2는 보안 협상 단계의 후반부와 키 교환의 초반부로 이루어져 있으며 클라이언트와 서버 간 보안 협상을 완료하고, 서버는 클라이언트에게 세션키를 도출하는데 사용되는 파라미터를 전송한다. 마지막으로 Phase 3는 키 교환단계의 후반부와 키 확인 단계로 이루어져 있으며 클라이언트는 서



(그림 4) DTLS Handshake Message

버에게 받은 파라미터를 기반으로 세션키를 생성하고 서버가 사용해야할 파라미터를 전송하여 서버도 동일한 세션키를 생성하게 된다. 생성된 세션키를 사용하여 키 확인 단계를 거치고 클라이언트와 서버간 DTLS 통신이 이루어지게 된다. *은 RPK와 Certificate 모드에서만 발생하는 메시지이다.

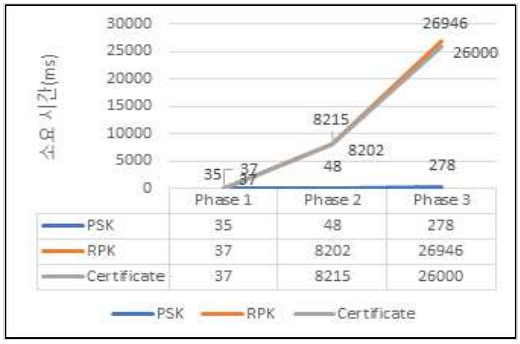


(그림 5) DTLS Handshake 소요 시간

(그림 5)를 보면 PSK의 경우, 사전에 대칭키가 공유되어 있어 별도의 계산 시간이 필요하지 않기 때문에 다른 두 방식에 비하여 상당히 빠른 소요 시간을 보인다. RPK와 Certificate 방식의 경우, 클라이언트와 서버의 상호 인증을 위한 EC(Elliptic Curve) 덧셈 연산이 수행되기 때문에 PSK에 비하여 상당한 시간이 소요된다. 하지만 Certificate 방식의 경우, 인증서의 유효성을 확인하는 OCSP에 대한 처리가 추가적으로 필요하게 되므로 실제적인 DTLS Handshake 소요 시간이 RPK보다 더 많이 소요된다.

4.3 Phase 별 시간

Phase 별 시간은 클라이언트와 서버 간 DTLS Handshake 소요 시간이 자원 제약적인 CoAP 서버에게 많은 영향을 받는다는 것을 가정하여 측정하였다.



(그림 6) Phase 당 소요 시간

(그림 6)의 Phase 별 소요 시간을 보면 Phase 1의 경우, 세 가지 모드 모두 별도의 연산과정이 필요하지 않기 때문에 시간이 비슷하게 소요된다. Phase 2의 경우 PSK는 별도의 연산과정이 필요하지 않아 Phase 1과 시간차이가 크게 나타나지 않지만 RPK와 Certificate는 자원이 제약된 서버가 키 교환에 필요한 키 재료 생성에 대한 연산과정이 필요하여 PSK에 비해 시간이 많이 소요된다. Phase 3는 클라이언트에게 받은 키 재료와 자신의 키 재료를 사용하여 세션 키 생성 알고리즘을 수행하게 된다. PSK는 사전에 대칭키를 공유하고 있기 때문에, 키 생성에 대해 별도의 시간이 추가되지 않지만 RPK 와 Certificate의 경우, 세션 키 생성에 대한 키 생성 알고리즘을 수행하여야하기 때문에 상당한 시간이 소요되게 된다.

4.4 RAM / ROM 소모량

본 절은 실제 사용되는 센서 노드의 하드웨어 자원과 DTLS 모드 별 RAM / ROM 소모량을 비교하여 사용 적합성을 논의한다. 본 성능 평가에 사용된 센서 노드는 16비트 TI MSP 430 시리즈의 Wismote를 사용하였다. Wismote는 램 16 킬로바이트, 롬 256 킬로바이트의 크기 제한이 있다. DTLS 모드 별 RAM / ROM 소모량을 알기 위해 Cooja에서 컴파일의 산출물인 .wismote 오브젝트 파일과 size 명령어를 사용하였다. 오브젝트 파일의 세션 정보를 출력하는 size 명령어는 해당 파일의 text, data, bss 세션 크기를 반환한다. text는 CPU가 실행할 Code부를 나타내고, data는 프로그램에 선언된 초기화된 변수를 나타낸다. 마지막으로 bss는 값을 설정하지 않은 배열이나 Null 포인터와 같이 초기화 되지 않은 데이터로 구성된다.

<표 2> ROM / RAM 계산 표(단위 : byte)

인증 모드	text	data	bss	ROM	RAM
PSK	71513	342	8324	71855	8666
RPK	81963	350	11084	82313	11434
Certificate	83441	374	11084	83815	11458

<표 2>의 출력된 text, data, bss 크기 값을 기준으로 ROM = text + data , RAM = bss + data로 계산하였다. 세 가지 모드 모두 Wismote의 사양에 적합하다고 평가되었다. 하지만 Wismote보다 더 자원이 제약된 sky mote 와 z1 mote와 같은 모트의 경우, 10 킬로바이트 미만의 RAM 제한을 가지고 있어 RPK와 Certificate의 경우 mote의 성능에 따라 사용이 제한될 수 있다.

5. 결 론

본 논문에서는 LoWPAN이 연동되는 IoT 네트워크 아키텍처 관점에서 CoAP 프로토콜에 적용되는 DTLS 보안모드에 대한 분석을 수행하였다. 나아가 IETF에서 제시하는 IoT 7 Use Cases 별로 적절한 보안모드를 제안하기 위해 PSK, RPK 및 Certificate 보안 모드 분석을 통한 성능 평가를 수행하였다. 성능 평가의 결과로 보안 모드 분석과 Use Cases 별 보안모드 제안에 대한 적합성을 판단하였다. DTLS에 대한 실효성 검증에 대한 연구의 일환으로써 DTLS 성능 평가와 Use Case 별 보안모드에 대한 선정은 향후 응용환경에서의 보안 메커니즘 설계에 중요한 지침으로 활용될 수 있을 것으로 판단하고 있

다. 향후, CoAP 환경뿐만 아니라 MQTT 환경에 적용될 수 있는 보안 메커니즘에 대한 분석을 통해서 Client-Server 모델 및 Subscriber-Publisher 모델에서의 보안 아키텍처 설계상의 차이점을 확인해 보고자 한다.

참 고 문 헌

[1] IEEE std. 802.15.4-2011, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), Standard for Information Technology Std., June 2011.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks,” IETF RFC 4944, Sep. 2007.

[3] ISO/IEC 20922:2016 Information technology : Message Queuing Telemetry Transport (MQTT) v3.1.1, June 2016

[4] Z. Shelby, K. Hartke, and C. Bormann, “The Constrained Application Protocol,” IETF RFC 7252, June 2014.

[5] M. Kovastsch, "A Low-Power CoAP for Contiki", IEEE Mobile Adhoc and Sensor System(MASS), 2011.

[6] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, “Use Cases for Authentication and Authorization in Constraint Environments,” IETF RFC 7744, Jan. 2016.

[7] E. Rescorla and N. Modadugu, “Datagram Transport Layer Security,” IETF RFC 6347, Jan. 2012.

[8] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," IEEE Sensors Journal, 13(10), 3711-3720, October 2013.

[9] S. Raza, L. Seitz, D. Sitenkov, and G. Selander, "S3K: Scalable Security with Symmetric Keys - DTLS Key Establishment for the Internet of Things," IEEE Transactions on Automation Science and Engineering, 2016.

[10] R. Hummen, J. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, “Towards Viable Certificate-based Authentication for the Internet of Things,” in Proc. of the 2nd ACM Workshop on Hot Topics on Wireless Security and Privacy, pp. 37-42, 2013.

[11] Contiki Community, Cooja Simulator, http://www.contiki-os.org/start.html.

[12] S. Santesson, M. Myers, R. Ankney, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IETF RFC 6960, 2015.

〔저 자 소 개〕

한 상 우 (Sang woo Han)
2017년 2월 단국대학교
컴퓨터과학과 학사
2017년 3월 ~ 현재 단국대학교
소프트웨어 보안 석사과정

email : dox13@naver.com

조 정 모 (Jung mo Cho)
2017년 2월 단국대학교
컴퓨터과학과 학사
2017년 3월 ~ 현재 단국대학교
소프트웨어 보안 석사과정

email : sixthcurio@naver.com

박 창 섭 (Chang seop Park)
1983년 2월 연세대학교
경제학과 학사
1987년 2월 Leigh University
컴퓨터과학과 석사
1990년 2월 Leigh University
컴퓨터과학과 박사
1990년 3월 ~ 현재 단국대학교
소프트웨어학과 교수

email : csp0@dankook.ac.kr