SDN 기반 IoT 디바이스 인증

김남우*, 김영갑*,†
*세종대학교 정보보호학과
e-mail: nowsec@nate.com, alwaysgabi@sejong.ac.kr

SDN-based Authentication for IoT Devices

Nam-Woo Kim*, Young-Gab Kim*
*Dept. of Computer and Information Security, Sejong Univ.

요 약

사물인터넷(Internet of Things)은 모든 사물들을 인터넷에 연결해 사람과 사물, 사물과 사물간의 정보를 상호 소통하여 지능형 서비스를 제공하는 기술을 의미한다. 그러나 IoT 환경은 유선 및 무선의 네트워크에 의한 연결이 필수이기 때문에 정보전달과 통신 과정에서 디바이스에 대한 인증이 반드시 필요하다. 따라서, 본 논문에서는 사물인터넷 네트워크 환경에서 사용자 디바이스 인증을 위해 SDN 기반의 IoT 디바이스 인증 모델을 제안한다.

1. 서론

최근 정보통신분야에서 이슈가 되고 있는 사물인터넷(Internet of Things; IoT)은 현실 세계 사물들과 가상 세계를 인터넷에 연결하여, 사람의 개입 없이 상호간에 스스로 정보를 공유하고 분석하여 사용자에게 적합한 서비스를 제공하는 차세대 통신기술로 떠오르고 있다. 미국의 IT 자문기관 가트너(Gartner)는 2020년까지 절반 이상의 신규 비지니스 프로세스와 시스템에 IoT의 부분적인 요소가 적용되고 1000억대 이상의 디바이스들이 인터넷에 연결될 것으로 예측했다 [1]. 현재 활발하게 진행되고 있는 IoT 기술로는 스마트 시티(smart city), 지능형교통시스템(intelligent transportation system), 스마트 카(smart car) 등이 있으며, 앞으로 더욱 다양한 스마트 디바이스들이 인간이 생활화는 모든 분야에 빠르게 확산되어 인간에게 편의를 제공해줄 것이다. 앞서 언급한 다양한 서비스들을 제공하기 위해 안전한 통신은 필수적인데, 안전한 통신을 위해서는 IoT 디바이스들 간의 인증이 필수적이다. 그러나, IoT 환경에서 일부 디바이스들은 제한된 자원을 가지고 있어 현재 IT 환경에서 사용되고 있는 인증 및 보안 기술을 IoT 디바이스에 적용하기는 제한적이다 [2].

기존 IoT 디바이스 인증에 관한 연구로는 세션키(session key) 분배를 통한 인증, 아이디 기반 암호화(ID-Based Encryption; IBE) 인증 등이 있는데 이러한 기술들은 센서 간 비밀 키 공유를 위해 베이스 스테이션(base station)과 지속적 통신을 해야 하는 번거로움이 있다. 또한, 키를 교환하는 과정에 보안적 결함을 가지며, 경량화 된 IoT 환경에서 복잡한 통신 및 인증 방식은 매우 비효율적이다. 따라서 본 논문에서는 비효율적인 IoT 디바이스 인증 문제를 해결하기 위해, 소프트웨어 정의 네트워크(Software Defined Network; SDN) 기반의 IoT 디바이스 인증 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 IoT 보안 기술과 디바이스 인증을 위한 기존 연구들을 분석하고, 3장에서는 본 논문에서 제안하는 SDN 기반 디바이스 인증 모델을 제시한다. 마지막으로 4장에서는 결론 및 향후 연구에 대해 설명한다.

2. 관련연구

2.1 IoT 환경을 위한 경량화 보안 기술

인터넷표준화기구(IETE)는 TCP/IP 기반 인터넷 환경에 적용되는 TLS(Transport Layer Security), IPSec(Internet Protocol Security), DTLS(Datagram Transport Layer Security) 보완 프로토콜을 IoT 환경에 적용시키는 방안을 고려하고 있다. 하지만 기존 IP 기반 보안 프로토콜을 IoT에 적용하기 위해서는 계산 능력과 메모리 공간을 고려하여 기존 보안 프로토콜을 경량화 시킬 방안이 필요하다. DTLS 프로토콜을 경량화 하는 방법에는 핸드 쉐이크 메시지의 패킷 개수를 줄이거나 인증서에 대한 검증과정을 간단히 하는 방법이 있다. 하지만 제안된 시스템은 결국 장치와 서버 간 DTLS 프로토콜을 전부 올려야 하며

† 교신저자

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW특성화 대학/대학원 (SW중심대학) 지원사업의 연구결과로 수행되었음(R70151510010001002)

암호화 모듈을 탑재하지 못하는 초경량 센서에는 적용할 수 없다 [3].

2.2 디바이스간 인증 및 세션키 분배 방안

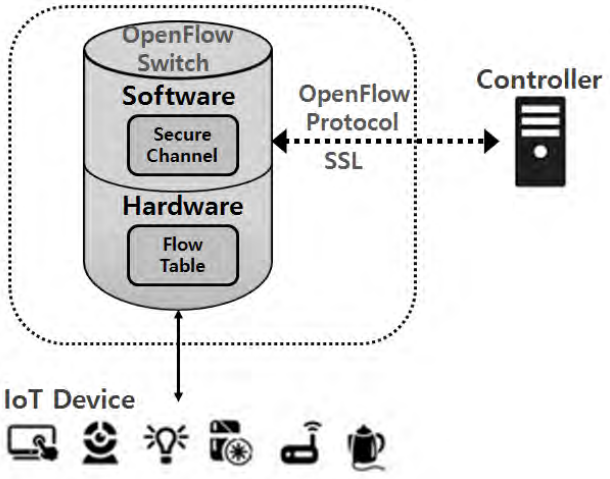
일반 IT 환경과 달리 무선 센서 네트워크와 IoT는 한정된 자원을 가지고 있다. 무선 센서 네트워크 환경에서의 통신은 인프라 노드(infra node)와 센서 노드(sensor node) 간 통신을 한다는 점에서 센서 간 통신이 주를 이루는 IoT 환경과 차별성을 가진다. 특히, IoT의 범주에 속하는 WoT(Web of Things)를 구성하는 장치는 웹 서버와 웹 클라이언트의 기능을 동시에 수행할 수 있다. 이런 차이로 기존 센서 네트워크 환경을 기반으로 제안되었던 일반적인 방안을 그대로 IoT환경에 적용하기 어려워 베이스 스테이션과 키 분배 센터를 통한 공유키 설정 및 세션키 분배 방안이 제안되었다. 하지만, 제안 기술은 비밀 키 공유를 위해 베이스 스테이션과 통신을 하고 베이스 스테이션의 키 분배센터와 통신을 다시 해야 하는 번거로움이 있다. 또한, 암호화와 해시 함수를 모두 사용하므로 자원제한적인 IoT 디바이스에 탑재할 수 없는 문제가 있다 [4].

2.3 ID-Based Encryption 인증

아이디 기반 인증기술은 ID를 기반으로 암호기술을 이용한 인증기술이다. 아이디 기반 암호기술은 사용자의 이름, 메일 주소 등 유저의 고유 정보를 이용하여 암호화 및 복호화 하는 암호기술이다. 아이디 기반 인증기술은 일련의 과정을 통해 공개키와 비밀키를 생성하고, 두 주체는 암호 통신을 위해 신뢰받은 제3자인 PKG(Public Key Generator)에게 통신을 위한 키 생성을 요청한다. 아이디 기반 인증은 사전에 키 분배가 필요하지 않으며, 키 크기가 작아 연산량이 적은 장점이 있다. 하지만, 위장 ID를 이용한 키 발급 공격에 취약하며, 공개키와 개인키가 상위 기관에 보관되는 문제점이 존재한다 [5].

2.4 SDN 핵심 기술

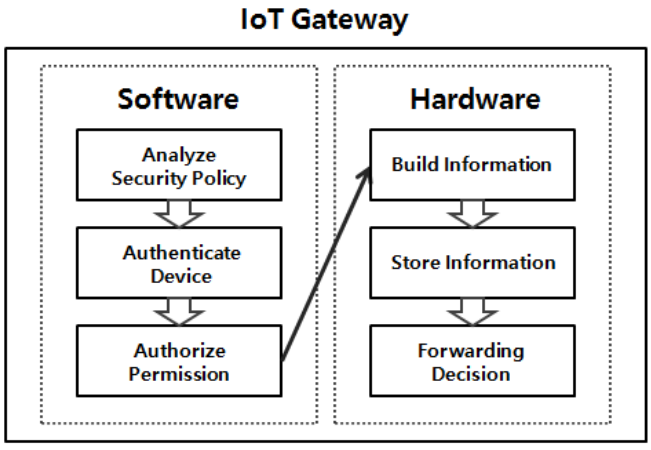
본 논문에서는 SDN의 중앙 집중적 제어와 프로그래밍을 통해 네트워크를 원하는 대로 제어 할 수 있는 특성을 IoT에 접목시켜 SDN 기반 IoT 디바이스 인증을 제안한다. 소프트웨어 정의 네트워크(SDN)란 스위치와 같은 기존 네트워크 장비에서 하드웨어 기능과 소프트웨어 기능을 분리하고, 네트워크 장비의 기능을 정의할 수 있는 오픈 API를 외부에 제공하여 직접 프로그래밍을 지원하는 새로운 네트워크 아키텍처 개념이다. SDN 기술의 시작은 스탠퍼드 대학의 오픈플로우(OpenFlow)에서 비롯되었는데 초기 오픈플로우 기술은 초기 네트워크 보안을 위해 다양한 정책을 네트워크에 손쉽게 적용 할 수 있도록, 스위치의 제어 부문을 중앙 집중적인 구조로 분리하고, 플로우 기반으로 네트워크를 관리하는 기술로부터 시작된 것이다. 최근 SDN이 각광을 받는 이유는 네트워크 관리 측면에서 효율성 향상과 새로운 비즈니스 생태계 구축을 통해 침체되어 있는 네트워크 시장을 활성화 시킬 수 있을 것이라는 기대감 때문이다. OpenFlow는 SDN을 구현하기 위해 처음으로 제정된 표준 인터페이스이며, OpenFlow Controller와 OpenFlow Switch로 구성된다. (그림 1)에서와 같이 컨트롤러와 스위치는 OpenFlow Protocol로 연결되며, 스위치 내부에는 Secure Channel과 Flow Table이 존재한다 [6].



(그림 1) OpenFlow 컴포넌트 [7]

III. SDN/OpenFlow 기반 IoT 디바이스 인증 모델

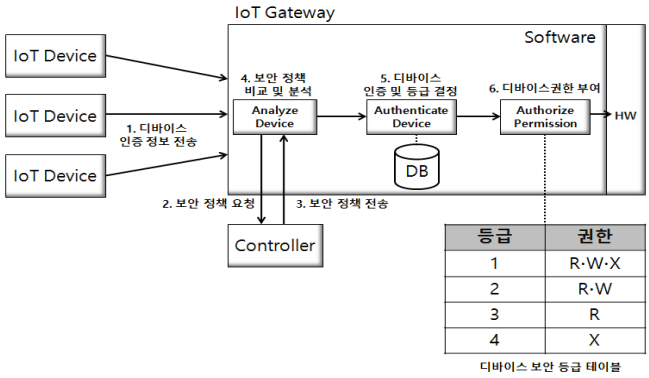
본 연구에서는 IoT 디바이스 인증 문제를 해결하기 위해 (그림 2)와 같이 디바이스 인증을 위한 SDN 기반 IoT 인증 모델을 제안한다.



(그림 2) SDN 기반 IoT 인증 아키텍처

제안한 SDN 기반 IoT 인증 아키텍처는 (그림 2)와 같이 기존 게이트웨이 네트워크 장비를 하드웨어 기능과 소프트웨어 기능으로 분리하여 직접 프로그래밍을 지원한다. IoT 게이트웨이 내부에는 하드웨어 영역과 소프트웨어 영역이 존재하는데 소프트웨어 영역에는 보안 정책 분석(Analyze Security Policy), 디바이스 인증(Authenticate Device), 권한 부여(Authorize Permission) 모듈로 구성되

며, 하드웨어 영역에는 데이터 모델링(Build Information), 데이터 저장(Store Information), 포워딩 결정(Forwarding Decision)으로 구성된다. (그림 3)은 SDN 기반 인증 절차를 보다 구체적으로 보여준다.



(그림 3) IoT 디바이스 인증 절차

IoT 디바이스가 게이트웨이에 인증 정보(디바이스 고유번호, ID, Password 등)를 전송하면, Analyze Device 모듈에서 컨트롤러에게 보안 정책을 전송 받아 디바이스로부터 받은 인증 정보와 컨트롤러에게 요청한 보안 정책을 비교분석하여 접근하는 디바이스의 출처를 정확히 확인하고, 인가된 디바이스인지 검증한다. 여기에서 보안 정책은 모든 디바이스가 기본적으로 만족해야 하는 요구사항이다. 비교분석한 결과 요청한 디바이스가 인가된 디바이스라는 것이 확인되면 Authenticate Device 모듈에게 분석한 결과를 넘겨준다. Authenticate Device 모듈에서는 분석된 디바이스 인증 정보와 컨트롤러가 업데이트한 데이터베이스 테이블의 값을 비교하여 디바이스의 권한 등급을 결정하고 Authorize Permission 모듈에게 인증 정보와 결정한 등급 정보를 전달한다. Authorize Permission 모듈에서는 전달 받은 정보에 따라 디바이스 보안 등급 테이블을 참고하여 디바이스의 접근 권한 레벨에 따라 권한을 부여한다. 예를 들어, 인증을 요청한 디바이스 등급이 1일 경우 읽기(read), 쓰기(write), 실행(execute) 권한을 준다.

기존 게이트웨이는 하드웨어 기반의 테이블을 이용하여 디바이스의 요청을 처리하고 있다. 하지만 본 논문에서 제안한 SDN 기반 IoT 게이트웨이는 소프트웨어 컨트롤러를 통해 인증 정보 및 인증 정책을 실시간으로 제어가 가능하다. 이는 네트워크 관리자가 분산되어 있는 IoT 게이트웨이 장비들을 프로그래밍 방식으로 단순화시켜 게이트웨이의 인증시스템을 제어할 수 있게 해주며, 네트워크 관리자가 일일이 수동으로 설정을 변경해야 했던 수고를 줄일 수 있다.

Ⅳ. 결론 및 향후 연구

본 논문에서는 SDN 기반 IoT 디바이스 인증을 위해 기존 IoT 환경의 보안 기술에 대하여 살펴보았다. 또한 기존 IoT 보안 및 디바이스들 간 인증을 위한 연구들을 분석하였고, SDN 기반 IoT 디바이스 인증 모델을 제안하였다.

향후 연구로, 본 논문에서 제안된 모델을 보다 구체적으로 기술하고, 실제 SDN 기반 IoT 디바이스 인증 기술을 구현하고 제안된 모델의 실효성을 판단할 수 있는 연구가 요구된다.

참고문헌

[1] The Internet of Things, Worldwide, Gartner, Inc. 2013

[2] Ministry of Science, ICT and Future Palnning, “Internet of Things Information”

[3] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, “Towards viable certificate-based authentication for the Internet of Things”, In Proc. of the Second ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec13), pp. 37-42 Apr. 2013

[4] W.S Juang, “Efficient user authentication and key agreement in wireless sensor networks,” Lecture Notes Comput. Sci., vol. 4298, pp.15-29, Aug. 2006

[5] 임종인, “사물통신에서의 정보보호를 위한 효율적 인증시스템 연구”, Sep. 2010

[6] 한국정보통신기술협회, “Software defined Networking ”, Dec. 2014

[7] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner, “OpenFlow: Enabling Innovation in Campus Networks”, Mar. 2008