http://dx.doi.org/10.14400/JDC.2014.12.4.285

OpenFlow를 이용한 유무선 통합 네트워크 환경에서의 인증 시스템

문정경*, 조한진**, 김진묵*
선문대학교 IT교육학부*, 극동대학교 스마트모바일학과**

A secure authentication system on wired wireless integrated network using OpenFlow

Jeong-Kyung Moon*, Han Jin Cho, Jin-Mook Kim***
Division of IT Education, Sunmoon University*
Dept. of Smart Mobile, Far East University**

요 약 최근 무선 통신장치들이 매우 빠르게 발전되고 사용자에게 보급되고 있다. 이로 인해서 기존의 유선 네트워크 장치들과 새로운 무선 네트워크 장치들을 통합한 새로운 메쉬 네트워크에 대한 요구가 급속히 발전하고 있다. 이런 유.무선 통합 네트워크 환경에서 자동으로 네트워크를 구성하고, 이런 환경에서 사용자 또는 유.무선 통신장치에 대해 인증서비스를 반드시 제공해야만 한다. 하지만 현실적으로 이런 서비스를 제공하고 있지 못하다. 그러므로 본 논문에서 유.무선 통합 네트워크 환경에서 오픈플로우를 사용해 네트워크를 자동으로 구성하고, 커베로스를 응용한 사용자 인증시스템을 제안하였다. 우리가 제안한 인증시스템은 장치 또는 사용자에 대한 인증서비스를 제공할 수 있을 뿐만 아니라, 비밀성, 무결성 서비스를 제공할 수 있다. 추가로 중간자공격에 대해서도 막을 수 있다.

주제어 : 오픈플로우, 인증시스템, 비밀성, 무결성, 중간자공격

Abstract Recent, development of wireless communication devices are rapidly and these device being deployed to the user very fast. By this results, a wired network device and the new device such as wireless devices incorporate. Then a demand of new mesh network is rapidly growing. In this wired/wireless integrated network environment, the network is configured automatically, and a user or wireless communication devices must be provided for authentication services. But, these services do not in the real world. Therefore, in this paper, we propose that wired/wireless integrated network environment to automatically configure the network using OpenFlow and the authentication system using Kerberos method. Our proposed system to be able to provide authentication services, confidentiality, integrity services for user or wired/wireless communication devices. And it can be prvented as well to man-in-the-middle attacks.

Key Words : OpenFlow, Wired/Wireless communication network, Authentication system, Confidentiality, Integrity, Man-in-the-Middle attack.

Received 3 February 2014, Revised 26 February 2014
Accepted 20 April 2014
Corresponding Author: Jin-Mook Kim(Sunmoon Univ.)
Email: calf0425@sunmoon.ac.kr

ISSN: 1738-1916

1. 서론

최근에 스마트폰, 기타 무선 네트워크 장치들이 폭발적으로 공급되고 있다. 이처럼 복잡한 유·무선 통합 네트워크 환경에서 독립적이고 자동 네트워크 구성이 가능한 시스템이 반드시 필요하다. 더구나 기존의 유·무선 네트워크 장치들을 그대로 사용하면서 통합 네트워크를 구성하고자 할 때 다음과 같이 5가지 문제점을 가지고 있다.

첫 번째, 기존의 서버-클라이언트 네트워크 환경은 새로운 네트워크 환경의 변화에 능동적으로 대응할 수 없다[6].

두 번째, 기존의 네트워크 구조는 네트워크 장비들이 계층적인 구조를 갖기 때문에 추상화하기 어렵다. 그러므로 기존의 네트워크 장치들은 새로운 네트워크를 빠르게 자동으로 구성하여야만 하는 사용자정의 네트워크(Software-Defined Network) 요구에 적합하지 않고, 네트워크 추상화를 지원하는 것이 매우 어렵다.

세 번째, 최근의 네트워크는 트래픽 패턴이 자주 변화하기 때문에 정확한 네트워크 규모를 측정하기가 어렵다. 이런 환경에서 네트워크 규모를 파악하고 적합한 서비스를 즉각 제공하는 것은 매우 어렵다.

네 번째, 기존의 네트워크 구성은 버추얼머신(VM)의 위치 이동과 주소체계의 변화에 빠르게 적응하지 못한다. 하지만 VM의 위치 이동과 무선 장치들의 주소체계 변화에 대한 빠른 변화는 새로운 유·무선 네트워크 통합 환경을 구성하기 위해서 반드시 필요하다[8].

마지막으로 기존의 네트워크 장비들은 표준 API나 개방형 인터페이스(Open Interface)가 없다. 그러므로 새로운 네트워크를 구성하기 위해서는 기존에 사용하던 네트워크 장치들을 포기하고 모두 교체해야 하는 문제가 발생한다. 이로 인해 높은 장치 교체 비용과 네트워크 복구 시간이 소모된다.

시대적 요구에 따라 새로운 유·무선 통신장치들끼리 자동으로 네트워크를 구성하고, 통신할 수 있도록 하는 새로운 네트워크 서비스에 대한 연구가 반드시 필요하다[6, 12, 13, 18].

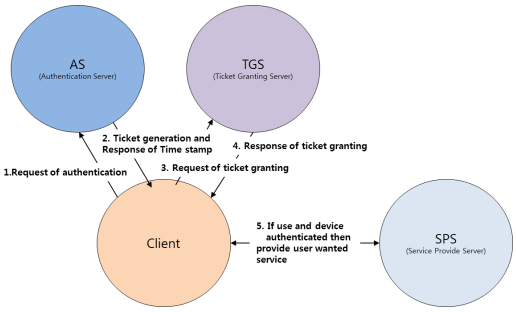
하지만 사용자정의 네트워크를 사용해 유·무선 장치들을 조합해 새로운 네트워크를 구성한다고 해도 사용자에게 안전한 네트워크 환경을 제공하기 위해서는 반드시 보안 문제를 선행해서 해결해야만 한다. 그러므로 본 논문에서는 오픈플로우를 사용해 네트워크를 쉽게 구성하고, 오픈플로우의 확장 필드들을 활용해서 기밀성, 무결성 서비스를 제공할 수 있도록 새로운 시스템을 제안하고자 한다. 우리가 제안한 새로운 인증 시스템은 기밀성, 무결성을 제공할 수 있을 뿐만 아니라, 네트워크를 구성하는 터미널 자체에 대한 인증 서비스를 제공할 수 있다. 이를 통해서 우리는 보다 안전한 소프트웨어 정의 네트워크 시스템을 구성할 수 있음을 보인다[15].

2. 관련연구

본 논문에서는 자동으로 무선 장치들로 구성된 새로운 네트워크를 구성한다. 변화가 많은 새로운 네트워크 환경에서 사용자 또는 장치에 대한 인증을 수행하고, 비밀성과 무결성 서비스를 제공할 수 있는 안전한 인증 시스템을 설계 및 구현하고자 한다. 이를 위한 관련 연구를 2가지 기술하였다.

2.1 커베로스(Kerberos)를 기반으로 한 인증 시스템

커베로스 프로토콜은 분산 컴퓨팅 환경에서, MIT의 Athena 프로젝트의 결과물로 개발되었다.



[Fig. 1] Kerberos architecture and process

커베로스는 대칭키 암호 알고리즘을 이용해서 사용자에게 인증을 제공할 수 있도록 개발된 중앙 집중형 인증 방식이다. 이것은 Needham-Schroederm의 신뢰할 수 있는 제 3 자 프로토콜을 기반으로 만들어진 모델이다.

[Fig. 1]에서 보여주고 있는 것처럼, 커베로스는 사용

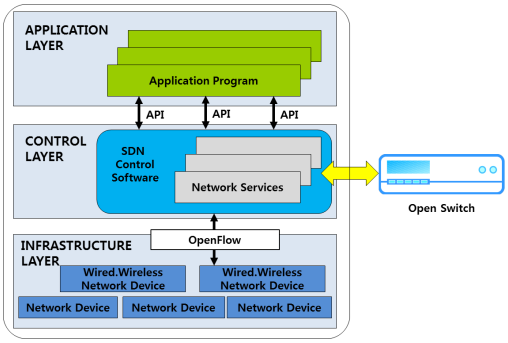
자가 요청한 서비스를 올바르게 제공하기 위해서 사용자를 인증하기 위한 티켓을 발행하는 과정을 통해서 사용자와 사용자의 서비스 요구에 대해서 인증 서비스를 제공한다. 이처럼 커베로스 프로토콜을 응용하면 유·무선 장치들을 통합한 네트워크 환경에서도 빠르고 쉬운 인증 서비스를 제공할 수 있다[7].

2.2 SDN/OpenFlow

본 절에서 우리는 새로운 제안시스템을 설계 및 구현하기 위해서, 기존에 많은 유·무선 통신장치들이 자동으로 네트워크를 구성할 수 있는 사용자정의 네트워크에 대해서 살펴본다. 그리고 사용자정의 네트워크를 구성하기 위해서 가장 널리 사용되는 오픈플로우에 대해 설명한다[3, 4].

2.2.1 사용자정의 네트워크: SDN(Sofrtware-Defined Network)

사용자정의 네트워크는 기존의 하드웨어 종속적인 네트워크 구조 및 구성 방식을 벗어나서, 자유롭게 네트워크를 재-구성할 수 있도록 소프트웨어 방식을 사용한 네트워크 구성 메커니즘이다.

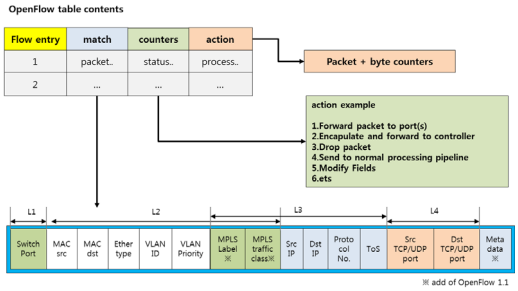


[Fig. 2] conceptual SDN structure

[Fig. 2]에서 보이는 것처럼, SDN은 3계층 구조를 가지고 있으며, 그 중에서도 제어 계층에서 소프트웨어 방식으로 서로 다른 기종의 스위치나 라우터 등에서 사용자가 원하는 방식으로 제어를 위한 네트워크 패킷과 데이터 전송을 위한 패킷을 구분해서 처리할 수 있다[1, 2, 9, 16].

2.2.2 오픈플로우(OpenFlow)

스탠포드 대학이 제안한 오픈플로우는 여러 가지 유·무선 장치들에 관계없이 독립적으로 네트워크 트래픽을 제어하기 위해서 사용하는 프로토콜이다. 오픈플로우를 사용하는 스위치에서는 다음과 같은 오픈플로우 데이터 필드 구조를 갖는다. 이를 [Fig. 3]에 나타냈다.



[Fig. 3] OpenFlow Tables and Head(ver.1.1)

[Fig. 3]에 나타낸 것처럼, 오픈플로우 스위치는 오픈플로우 테이블을 사용해서 서로 다른 유·무선 네트워크 장치들에게 독립적으로 패킷 제어를 수행할 수 있도록 3개의 구성요소를 갖는다[17].

본 논문에서 우리는 조건 필드의 헤더 정보들 중에 메타 정보 뒤에 확장 필드를 추가해서 사용자 또는 단말장치에 대한 인증을 위한 정보들을 추가한다. 그리고 해당 인증 정보에 대한 처리 방법을 처리 필드에 추가한다[5].

3. 제안시스템

본 절에서는 오픈플로우를 사용해 유·무선 통합 네트워크 환경에서 안전한 인증시스템에 대해서 제안한다. 제안시스템은 유·무선 단말장치들이 종단 지점에 위치해 있고, 사용자 또는 단말장치에 대한 사용자 인증을 수행한다. 이를 위해서 커베로스를 응용해 인증시스템을 설계하였다.

3.1 제약사항

본 논문에서 제안한 인증 시스템은 다음과 같이 6가지 제약사항을 갖는다.

(1) 제안시스템에서 통신의 주체가 되는 오픈 컨트롤러와 오픈 스위치 사이의 통신은 TLS ver.3과 같은 보안 프로토콜을 사용한다.

(2) 오픈 스위치들끼리는 비밀성 서비스를 보장하기 위해서 IDEA와 같은 대칭키 암호 알고리즘을 사전에 탑재하고 암호화된 통신을 실시한다. 이를 아래와 같이 수식으로 나타내었다.

$$Switch_A \rightarrow Switch_B : Enc_{KeyA \leftrightarrow B}(\text{OpenFlow Table Contents} \mid \text{Extension Field})$$

(3) 오픈 컨트롤러들 사이에서의 통신에서도 비밀성 서비스를 제공하기 위해서 오픈 스위치들과 마찬가지로 IDEA 암호 알고리즘을 사용하였다. 아래의 수식은 대표적인 오픈 컨트롤러인 NOX 모듈을 사용해서 비밀성 통신을 수행하는 과정을 나타내고 있다.

$$NOX_A \rightarrow NOX_B : Enc_{KeyA \leftrightarrow B}(\text{TLS}\{\ \text{NOX\_Auth\_Info} \mid \text{Time\_Stamp} \mid \text{Key\_Info}\ \})$$

(4) 제안시스템을 통해서 유·무선 통신장치들이 인증절차를 수행할 때, 오픈플로우 테이블의 확장필드 데이터를 메타 데이터 필드 뒤에 첨부해서 처리하여야만 한다. 이것은 기존의 오픈플로우 테이블 ver.1.1을 그대로 유지하면서 최소한의 변화를 통해서 쉽고 빠른 인증절차를 수행하기 위해서이다.

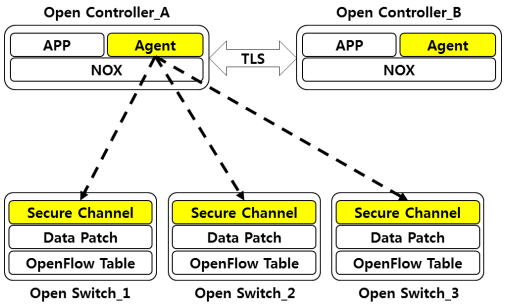
(5) 제안시스템은 사용자 또는 유·무선 단말장치에 대해서 인증을 먼저 수행한 후, 사용자가 요구하는 서비스를 나중에 처리한다. 만약 위와 같이 사전에 인증과정을 수행하지 않고 서비스를 요청할 경우에 발생할 수 있는 보안상의 문제점들을 미리 해결하기 위해서이다.

(6) 오픈 컨트롤러는 오픈 스위치들과 주기적으로 통신을 하면서 네트워크 트래픽에 대한 제어를 수행하고, 자신이 관리하는 서브 네트워크에 포함된 오픈 스위치들에 대한 정보를 수집하고 관리한다.

우리가 제안한 인증시스템은 커베로스의 인증 메커니즘을 응용하여 사용자 또는 유·무선 통신장치에 대한 인증을 수행한다. 이때 단말장치들간의 비밀성 서비스를 제공하기 위해서 IDEA 대칭키 알고리즘을 사용해 범용성을 높였다.

3.2 제안시스템 구조

제안시스템은 아래 [Fig. 4]와 같이 오픈 컨트롤러와 오픈플로우 스위치들로 구성된다. 하나의 컨트롤러들은 여러 개의 오픈 스위치들을 관리한다.



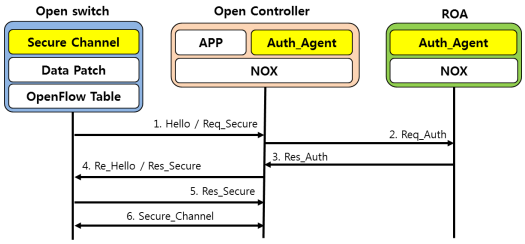
[Fig. 4] Proposed system architecture and relation

오픈 컨트롤러들의 상위 계층에 RoA(Router of Authority)가 있다. 이것은 오픈 컨트롤러들 간의 상호인증을 위한 것이다. 그리고 오픈 컨트롤러들 간의 상호 인증을 수행하거나 상위 계층의 RoA와의 안전한 통신을 위해서는 TLS ver.3를 사용하여 설계했다.

그리고 제안시스템은 오픈 스위치와 오픈 컨트롤러 간의 안전한 통신을 위해서 표준 대칭키 암호 알고리즘인 IDEA를 사용한다. 이를 통해서 유·무선 단말장치들 사이에 암호화된 데이터를 송·수신함으로써 중간자 공격이나 데이터 위·변조 공격을 막을 수 있다.

3.3 제안시스템 인증절차

[Fig. 5]는 제안시스템의 오픈플로우 스위치와 오픈 컨트롤러사이에서 사용자 또는 단말장치에 대한 인증절차에 대해서 설명하였다.



[Fig. 5] Authentication Procedures

오픈 컨트롤러에 대한 장치 인증을 위해서 상위 계층의 RoA를 통한 인증절차가 추가적으로 필요하다. 제안

시스템의 세부적인 인증 처리절차는 총 6단계로 구성되었다. 세부적인 인증절차는 다음과 같다.

(1) 오픈 스위치가 오픈 컨트롤러에게 통신을 요청하고, 안전한 통신을 위해서 비밀키 할당을 요청한다. 이를 아래와 같이 수식으로 나타내었다.

$$Req\_Secure_{sw \rightarrow cont.} = \{ sw_{ID} \mid TS_{SW} \mid Req_{Token} \}$$

(2) 오픈 컨트롤러는 자신에 대한 장치 인증과 오픈 스위치에 대한 서비스 요청에 대한 인증을 검토받기 위해서 RoA에게 인증을 요청한다. 이를 아래 수식과 같이 나타낸다. 수식 4에 나타낸 것처럼, 오픈 컨트롤러와 RoA 사이에는 안전한 TLS 프로토콜을 사용한다.

$$Req\_Auth_{cont. \rightarrow RoA} = \text{TLS}(\text{M})$$
$$\text{M} = \{ SW_{ID} | TS_{SW} | Req_{Token} \}, \{ Cont._{ID} | TS_{cont.} \}) \}$$

(3) RoA는 미리 약속된 해쉬 알고리즘을 사용해 오픈 컨트롤러에 대한 인증을 허락하는 토큰(Token)을 생성해서 오픈 컨트롤러에게 전달한다. 이때 사용하는 암호화 세션 키는 TLS 프로토콜을 통해서 별도로 안전하게 전달한다. 이를 아래 수식에 나타내었다.

$$Res\_Auth_{RoA \rightarrow cont.} = \text{TLS}(\text{Token})$$
$$\text{Token} = \{ \text{M} \mid HASH_{S\_key} (\{ SW_{ID} | TS_{SW} | Req_{Token} \}, \{ Cont._{ID} | TS_{cont.} \}) \}$$

(4) 오픈 컨트롤러는 자신의 장치 인증을 확인하고, IDEA 암호 알고리즘을 사용해서 전달받은 토큰 과 타임 스템프(Time stamp) 값을 암호화한 후, 오픈 스위치에게 암호화한 토큰 정보를 전달한다. 이를 아래 수식에 나타내었다.

$$Res\_Secure_{cont. \rightarrow sw} = Enc_{S\_key} (\text{Token} \mid TS_{cont.}+1)$$

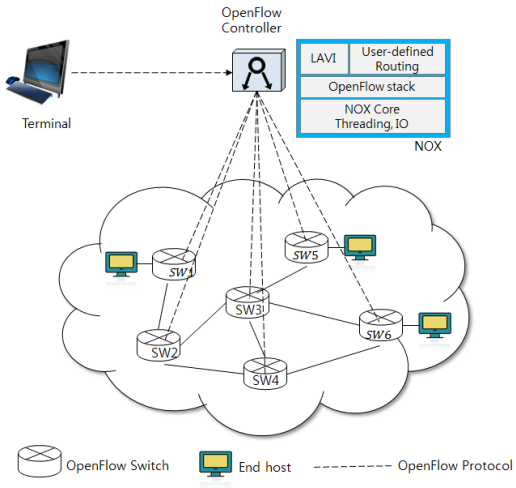
(5) 오픈 스위치는 전달 받은 토큰이 올바른지 확인하기 위해서 타임스템프 값을 미리 약속된 처리를 수행한 후, 오픈 컨트롤러에게 전달한다. 이를 아래 수식에 나타내었다.

$$Res\_Secure_{sw \rightarrow cont.} = Enc_{S\_key} (\text{Token} \mid TS_{sw}+2)$$

(6) 마지막으로 오픈 스위치와 오픈 컨트롤러 가 서로 정당한 사용자 또는 장치임이 인증되면, SDN 방식을 사용해서 두 장치 사이에 안전한 서비스를 제공할 수 있는 통신 채널을 설정한다.

4. 평가 테스트 및 결과

본 논문의 제안시스템을 테스트하기 위해서 [Fig. 6]과 같이 평가 환경을 구성하였다.



[Fig. 6] Experiment environment

[Fig. 6]과 같이, 오픈 스위치들을 6개 연결하고, 오픈 스위치_1과 오픈 스위치_5, 그리고 오픈 스위치_6에 데스크 탑 PC를 연결하였다. 그리고 오픈 컨트롤러에 노트북을 연결하고 제안한 인증 시스템을 탑재하였다.

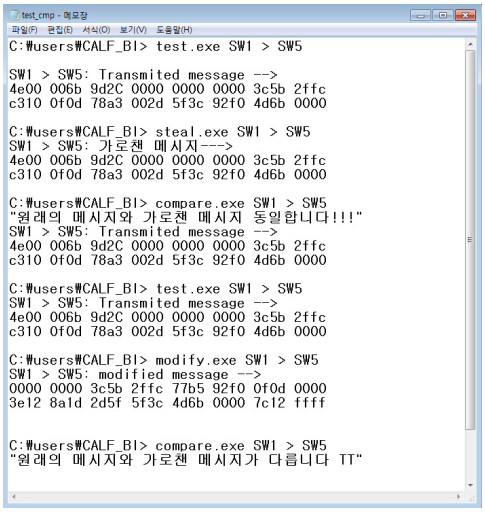
실험 시나리오 1)

오픈 스위치_1과 오픈 스위치_5 사이에서 송·수신하는 데이터 패킷을 터미널에서 가로채어 확인해서 가로챈 내용이 올바르게 암호화되어 있는지 확인한다.

실험 시나리오 2)

오픈 스위치_1과 오픈 스위치_6 사이에서 터미널에서 가로챈 정보를 재-전송하였을 경우, 오픈 스위치_6이 원래의 통신 패킷이 아닌 변조된 것임을 확인할 수 있는지 실험한다.

실험은 윈도우 7이 설치된 데스크톱과 노트북을 사용하였다. 그리고 제안한 인증시스템은 MS-Visual Studio 2010 환경에서 C++를 사용해서 구현하였다. 아래 [Fig. 7]은 시나리오에 따른 실험결과를 나타내고 있다.



[Fig. 7] Result of Experiment

[Fig. 7]과 같이, 제안한 인증시스템은 해커가 중간에서 데이터를 가로채는 공격에도 비밀성 서비스를 보장할 수 있다. 그리고 중간자 공격 등을 통해서 수집한 정보를 변조하여 전달할 경우, 이를 감지할 수 있다. 제안시스템은 타임스템프와 해쉬함수를 사용하기 때문에 중간자 공격을 감지할 수 있다.

5. 결론

클라우드 컴퓨팅 환경에 대한 수요가 급증할 수록 OpenFlow를 기반으로 한 사용자정의 네트워크에 대한 수요가 급증하고 있다. 더욱이 유무선 통합 네트워크 환경에서 사용자 요청은 더욱 높아지고 있다.

그러므로 우리는 향후 네트워크 시장의 가장 큰 변화로 다가올 사용자정의 네트워크에서 적용하기 위한 보안 프로토콜이 가져야 할 제약사항들에 대해서 정의하였다. 그리고 제약 조건을 갖는 유·무선 네트워크 환경에서도 동작 가능한 사용자 또는 단말장치에 대한 인증시스템을 제안하였다.

제안시스템은 많은 유·무선 통신장치들로 통합 네트워크 환경을 구성하고 오픈플로우 프로토콜과 커베로스 인증 방식을 응용해 설계하였다. 이는 사용자정의 네트워크 기술을 활용해 자동으로 네트워크를 구성할 수 있다. 그리고 기존의 오픈플로우 테이블에 확장 필드를 적용함으로써 인증 서비스를 쉽고 빠르게 구현할 수 있다.

제안시스템이 비밀성, 무결성 서비스를 제공할 수 있는지 확인해 보기 위해서, 실험 환경을 구성하고 구현한 시스템을 실험해 보았다. 실험 결과, 제안시스템은 비밀성, 무결성 서비스를 제공할 수 있을 뿐만 아니라, 중간자 공격을 통한 데이터 재-사용에 대해서도 안전하였다. 향후 제안 시스템에 대한 성능 평가와 다양한 유·무선 장치들을 이용한 확장된 실험들을 추가로 수행할 계획이다.

REFERENCES

[1] Min-Sik Kim, Sun-Ock Lim, “SDN appear and future: next generation network control and management technology(I)”, KISDI report vol.24, no.12, pp.1-18, 2012.7.

[2] Min-Sik Kim, Sun-Ock Lim, “SDN appear and future: next generation network control and management technology(II)”, KISDI report vol.24, no.14, pp.1-22, 2012.8.

[3] Jae-Hyung Yu, Woo-Sung Kim, Chan-Hyun Youn, “SDN/OpenFlow Technique Trand and Future”, KNOM Review Vol. 15,

[4] N. Blefari-Melazzi, A. Detti, G. Morabito, S. Salsano, L. Veltri : Information Centric Networking over SDN and OpenFlow. In : arXiv:1301.5933, 2013

[5] Meral Shirazipour, Wolfgang Johny, James Kempf, Howard Green and Mallik Tatipamula: Realizing Packet-Optical Integration with SDN and OpenFlow 1.1 Extensions. In: Communications (ICC), 2012 IEEE International Conference on, pp. 6633-6637, 2012

[6] YUKIO ITO : A New Paradigm in optical communications and networks. In : IEEE Communications Magazine, 2013

[7] Jeong-Kyung Moon, Jin-Mook Kim and Hwang-Rae Kim : A Secure Authentication Protocol for Cloud Services in: JAITC, MANUSCRIPT, Vol. 1, No. 2, 2011

[8] Z. Cheng, J. Wang, T. Huang, P. Li, N. Yen, J. Tsai, Y. Zhou and L. Jing, A Situation-Oriented IoT Middleware for Resolution of Conflict Contexts Based on Combination of Priorities, Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Springer Netherlands, pp. 441-454, 2014

[9] Lee Jae-Joon, Jinsuk Kang, and Jaesung Lim, Adaptive Networking for Continuous and Reliable Data Delivery in Wireless Sensor Networks, Advanced in Computer Science and its Applications, Springer Berlin Heidelberg, pp.77-82, 2014

[10] Open Networking Foundation, Software-Defined Networking: The New Norm for Networks, ONF White Paper, April 13, 2012

[11] Christian E. Rothenberg et. al., Revisting Routing Control Platforms with the Eyes and Muscles of Software-Defined Networking, HostSDN'12, August 13, 2012

[12] Min Yoon, Yong-Ki Kim, Jae-Woo Chang, An Energy-efficient Routing Protocol using Message Success Rate in Wireless Sensor Networks, Journal of Convergence, Vol.4, No.1, pp.15-22, March 30, 2013

[13] Trusted M-banking Verification Scheme based on a combination of OTP and Biometrics, Journal of Convergence, Vol.3, No.3, pp.23-30, September 30, 2012

[14] Facebook: Design Principles in the Open Compute Project. In: OFC'2012, 2012

[15] ONF White Paper: Software-Defined Networking: The New Norm for Networks

[16] Open Networking Foundation (ONF) https://www.opennetworking.org/

[17] OpenFlow switch specification version 1.0, https://www.opennetworking.org/

[18] http://www.dt.co.kr/etc/article_print.html?article_no=2013051502019931795002

문 정 경(Moon, Jeong-Kyung)

- 1993년 2월 : 배재대학교 원예학과 (학사)
- 2006년 2월 : 단국대학교 인터넷정보학과(공학석사).
- 2013년 2월 : 공주대학교 컴퓨터공학과(공학박사)
- 2012년 3월 ~ 현재 : 선문대학교 IT교육학부 계약교수
- 관심분야 : 클라우드 컴퓨팅, 정보보안, 사용자 인증
- E-Mail : moonjk@sunmoon.ac.kr

조 한 진(Cho, Han-Jin)

- 1999년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2002년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 3월 ~ 현재 : 극동대학교 스마트모바일학과 교수
- 관심분야 : 모바일, 애플리케이션 보안, 네트워크 보안
- E-Mail : hanjincho@hotmail.com

김 진 묵(Kim, Jin-Mook)

- 1998년 2월 : 배재대학교 전자계산학과(공학사)
- 2000년 2월 : 배재대학교 컴퓨터공학과(공학석사).
- 2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
- 2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
- 2008년 3월 ~ 현재 : 선문대학교 IT 교육학부 부교수
- 관심분야 : 유·무선 네트워크, 센서네트워크 보안, 인증
- E-Mail : calf0425@sunmoon.ac.kr