정 보 보 호 학 회 지
제25권 제5호, 2015. 10

SDN을 통한 스마트그리드 복원력(Resilience) 향상 이슈

신 인 철*

요 약

SDN (Software Defined Networking)은 동적 재설정(Dynamic Reconfiguration)기능을 통해 지금껏 존재하지 않았던 유연성(Flexibility)을 IP(Internet Protocol)에 제공한다. 또한, 네트워크 관리, QoS (Quality of Service) 최적화, 시스템 복원력(Resilience) 강화를 위한 다양한 응용프로그램을 지원한다. 스마트그리드(Smart Grid)시스템에 SDN을 적용하기 위한 다양한 연구가 진행 중이며, 본 문서에서는 다양한 사고(Failures) 혹은 불법적인 공격으로부터 해당 시스템 복원력향상을 위한 이슈에 대해 언급한다. 이와 같은 문제점들에 대한 논의 없이 전력회사는 SDN의 장점을 충분히 활용하지 못할 가능성이 높다. 본 문서를 통해, SDN을 통한 스마트그리드 복원력향상, SDN으로 인한 추가적인 보안위협 등에 대해 논의할 것이다.

Ⅰ. 서 론

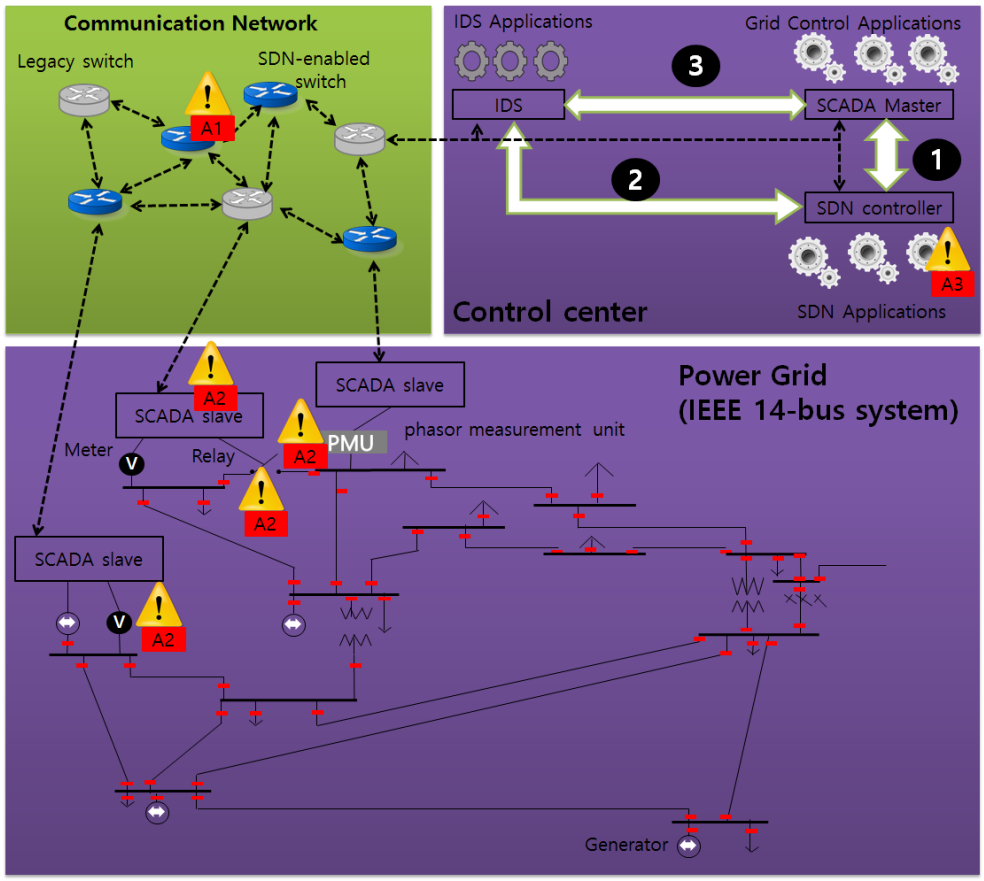
스마트그리드 통신네트워크(Communication Networks)는 광범위한 지역에 걸쳐 설치된 다양한 전력관련 기기들이 상호 연동하여 SCADA(Supervisory Control and Data Acquisition)기능을 지원하도록 구축되는 가장 기본적인 구성요소이다. 현재 전력시스템을 위한 통신네트워크는 IP 네트워킹을 기반으로 동작하고 있으며, 해당 네트워크(라우팅기능)는 시스템 설계단계에서부터 설계되어 고정되는 형태이다. 또한 전력시스템운영단계에서의 IP네트워크 재설정은 많은 자원이 요구되는 작업일 뿐 아니라 전력사고나 불법적인 공격에 단시간 내 대응이 불가능한 구성요소로 분류된다. 또한, 다양한 외부 이벤트(Events)에 대해 비순응적인(Non-Adaptive) 패러다임(Paradigm)을 내재하고 있는 IP네트워크는 스마트그리드의 성능 혹은 복원력향상에 방해가 되는 것이 사실이다.

스마트그리드는 현재까지 사용되던 전력시스템의 진보된 버전으로서 보다 유연한 통신 대역폭을 요구하면서도 다양한 형태의 네트워크와 상호연동하게 되지만, 그만큼 다양한 형태의 사이버공격에 노출될 것이다. 특히나, PMU (Phasor Measurement Units)과 전력소비자 고객의 댁내에 설치된 스마트미터(Smart Meters)의 경우 다양한 통신대역폭 만큼이나 많은 보안취약점을 가지고 있다고 알려져 있다[1,2].

다양한 사이버공격으로부터 스마트그리드 시스템을 복원하기 위한 방법으로 SDN사용이 고려되고 있다. SDN은 기존의 네트워크에서 제어와 데이터를 분리한 새로운 패러다임으로 알려져 있다[3]. SDN에서는 네트워크 스위치(Switches)란 중앙제어시스템에서 동적으로 설정이 가능하도록 만들어진 포워딩(Forwarding)기기이다. 해당 스위치와 중앙제어시스템은 OpenFlow 프로토콜 등을 사용하여 관리자에게 해당 네트워크의 동작을 실시간으로 재정의 한다[4]. 일반적인 네트워크 환경에서 SDN은 QoS를 위한 실시간 최적화 기능과 성능저하 혹은 시스템장애로부터 빠른 대응을 통한 복구기능을 지원한다[5-7].

많은 연구들이 스마트그리드에 SDN을 적용할 경우, 실시간 재설정기능을 통해 QoS성능을 향상시키며 다양한 서비스들을 효율적으로 지원이 가능할 것이라고 예측하고 있다[8-12]. 물론 QoS가 네트워크의 중요한 서비스 중 하나지만, 시스템 장애로부터 복구 및 주요기능에 대한 가용성보장은 전력시스템을 구축할 때 가장 우선적으로 고려되어야 할 부분이다. 특히나, 최근 국가기

* 국립목포대학교 정보보호학과 (ishin@mokpo.ac.kr)



〔그림 1〕 SDN이 적용된 스마트그리드 개요

반시설 제어시스템을 대상으로 하는 악성코드의 일종인 스턱스넷(Stuxnet) 및 잠자리(Gragonfly)의 등장으로 인해 시스템복원력의 중요성이 날로 높아지고 있다 [13,14].

그럼에도 불구하고, 본 문서에서는 이 같은 SDN을 스마트그리드에 적용하기 전에 인식해야할 2가지 이슈에 대해 언급하도록 한다.

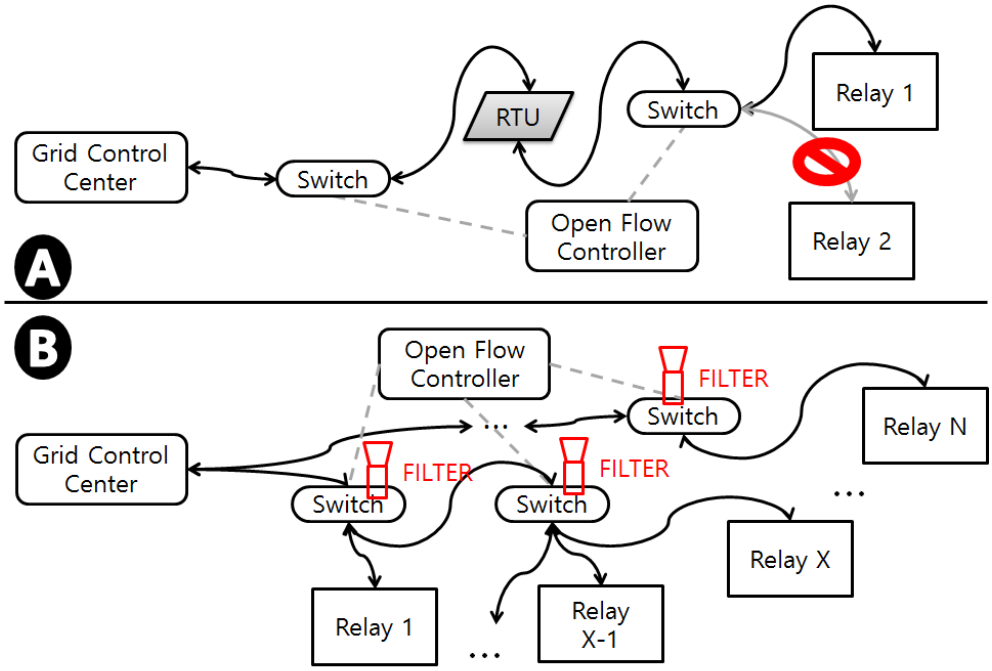
(1) SDN을 통한 스마트그리드 네트워크 복원력향상: SDN의 가장 주요한 장점은 네트워크의 재설정(라우팅경로 생성 및 삭제)에 있다.

(2) 스마트그리드에 SDN 적용 시 발생가능한 문제점

Ⅱ. SDN기반 스마트그리드 개요

SDN의 실행시간(Run-Time) 재설정기능은 스마트그리드 시스템에게 다양한 사이버공격으로부터 신속한 대응이 가능하도록 만들어준다. 본 장에서는 SDN이 적용된 스마트그리드 시스템의 개요를 설명하고 사이버공격 발생 시 이를 완화(Mitigation)하기 위한 절차를 살펴보도록 한다. (그림 1)은 SDN이 적용된 스마트그리드 시스템을 제어센터(Control Center), 통신네트워크(Communication Network), IEEE 14-Bus로 구성된 전력망(Power Grid)등 3가지 요소를 통해 보여주고 있다.

스마트그리드는 컴퓨터, 네트워크, 제어기기, S/W와 등등으로 구성된 SCADA를 통해 제어되며, SCADA 내 Control Center는 서버를 포함한 다양한 시스템으로 구성된 SCADA Master를 통해 제어 프로그램(시스템 상태 감시, 전력 및 전압제어 등등)명령을 전달한다. SCADA Master는 다양한 전력시스템 측정데이터를 수집하고 이를 기반으로 네트워크를 통해 제어명령을 전달한다. SCADA Slave들은 다양한 제어 기기들과의 상호연동을 통해 명령을 수행한다. IED (Intelligent



〔그림 2〕 SDN을 통한 스마트그리드 공격 대응

Electronic Device)나 RTU (Remote Terminal Unit)들은 다양한 센서(Sensor)를 통해 데이터를 수집하고 Actuator를 통해 명령을 실행한다.

SDN을 통해 구현된 스마트그리드는 SCADA Master, SCADA Slave, 제어기기, 센서 그리고 Actuator를 통해 공유되는 네트워크를 통해 제어명령이 전달되며, 이는 SDN 제어기(Controller)를 통해 이루어질 뿐 아니라 기존에 설치되어 운용되었던 전력시스템 또한 함께 연동되는 형태로 구축될 것이다. SDN 제어기는 QoS 최적화 및 네트워크 복원력을 극대화 하기위해 다양한 SDN 응용프로그램을 통해 네트워크를 재설정한다.

추가적으로, 제어센터는 침입탐지시스템(Intrusion Detection System)을 통해 네트워크로 유입되는 다양한 네트워크 패킷에 대한 분석을 수행할 수 있다. 세부적으로, SCADA Master, SDN 제어기 그리고 IDS는 상호연동을 통해 스마트그리드 보안성을 확보한다. ① SCADA Master와 SDN제어기는 정해진 시간에 센서로부터 데이터를 수집하고 제어메시지를 전달하기 위해 협력한다. ② IDS는 악성행위 탐지 시 해당 경로에 대한 프로파일을 작성하여 이를 SDN 제어기로 전달하고 이에 따라 네트워크 재설정 절차를 수행한다. ③ IDS는 SCADA Master에게 이 같은 외부침입을 전달함으로써, 피해의 최소화를 위한 제어변수를 조정하게 된다. 이 같은 ①, ②, ③의 절차들이 동작하는 방법은 스마트그리드 구축 방식에 따라 상이하지만, 언급된 구성요소들은 SDN 제어 네트워크로부터 분리된 LAN을 통해 연동된다. 본 문서에서는 ①과 ②과정에 대해 주로 언급하며 ③의 경우 [15]를 통해 확인가능하다.

스마트그리드는 다양한 관련 기기 및 네트워크의 상호연동, 부주의한 S/W제작, 내부적인 위협 등으로 인해 많은 취약점에 노출되어 있다. 하지만, 본 문서에서 언급하는 사이버 공격은 다음과 같은 세 가지로 분류하여 설명하도록 한다.

(공격1) 네트워크 스위치의 악성코드 감염
(공격2) 스마트그리드 기기(RTU, 릴레이, SCADA Slaves)의 악성코드 감염
(공격3) SDN 제어기 혹은 응용프로그램의 악성코드 감염

공격1과 공격2의 경우 일반적인 스마트그리드를 대

상으로 하는 공격이며, 공격3의 경우 SDN을 통해 구축된 스마트그리드를 대상으로 하는 공격이다. 다음 장에서는 SDN을 통해 이 같은 공격들에 대해 대응하기 위한 방법들에 대해 설명한다.

Ⅲ. SDN을 통한 스마트그리드 공격 대응

본 장에서는 SDN을 통해 앞서 설명한 3가지 공격에 대한 대응방법을 설명한다.

3.1. 스마트그리드 제어프로그램 보호를 위한 가상네트워크 (공격1)

악성코드에 의해 네트워크 스위치가 감염되었을 경우, 이는 탐지가 매우 어렵다. 해당 공격을 통해 감염된 네트워크 스위치는 악의적인 의도로 패킷 지연전송을 발생시키며, 이를 통해 다양한 동기화 문제, 성능저하를 일으킬 뿐 아니라 전체 시스템을 불안정한 상태로 만든다[16-18]. 이 같은 지연전송 공격의 경우 기존의 네트워크 보안 장비를 통해서는 탐지가 매우 어렵다고 알려져 있다. 특히나 공격자가 통계적인 전략을 통해 센서가 측정한 값이나 제어명령 전송을 지연할 경우 전체적인 스마트그리드 성능을 저하시킬 수 있다. 이는 암호나 out-of-band 검증을 통해 탐지가능한 무결성(Integrity) 공격과 대조적인 형태로서, 선택적으로 패킷을 전달하거나 혹은 재전송하는 공격또한 포함한다. 그럼에도 불구하고, 이와 같은 공격을 탐지 및 차단하는 것은 인적 자원을 통한 검증과정을 필요로 한다.

SDN은 물리적 통신 구간(Physical Communication Links)위에 가상 네트워크 계층(Virtural Network Layer) 구축이 가능하다[10]. 해당 계층은 이 같이 탐지하기 어려운 공격 발생 시 그 피해를 최소화 할 수 있다. 이 가상 네트워크는 필요에 따라 기기들을 연결하고 패킷을 전달하기 위해 특정 스마트그리드 제어 응용프로그램을 통해 구축된다. 이 같은 SDN을 활용한 네트워크 제어기능을 통해 보다 자세한 네트워크 상태 감시 기능을 구현할 수 있다. 예를 들어, SDN 가상 네트워크는 순응적인(Adaptive) QoS 변수계산(패킷전달 시간, 패킷손실률등)을 통해 물리적 통신구간을 변화시켜 최적화 시킨다. 이 같은 네트워크 감시를 통해 수집된 값들을 기초로 SDN 제어기는 악성코드 감염이 의심되는 스위치를 네트워크에서 분리한 뒤 최적화된 가상 네트워크 구간을 재설정한다. SDN의 재설정 기능 없이 이 같은 대응기술을 구현하기 위해서는 모든 네트워크를 인위적으로 조작하는 비효율적인 방법밖에 없다.

SDN 네트워크 상태 인지기능과 제어기능을 통해 효과적인 라우팅 구간설정이 효과적으로 이루어질 수 있으며, 제어기는 재설정(Reset)을 수행해야 하는 스위치를 효과적으로 선택하여 복구시킬 수 있다.

3.2. 주요 제어기기에 대한 공격 탐지 (공격1, 공격2)

IED나 RTU등과 같은 스마트 제어 기기들은 스마트그리드 운영에 있어 중요한 역할을 담당한다. 그와 동시에, 이 같은 스마트그리드기기 및 네트워크 장비들은 인터넷, USB 혹은 다양한 소프트웨어 취약점을 통해 공격자들의 불법적인 접근 혹은 침투대상이 된다. IT기반 방화벽과 같이 현재 주로 사용되고 있는 네트워크 보호기법들은 주로 네트워크 간 접점 혹은 경계에 위치하며, 일단 해당 위치를 통과한 네트워크 패킷들을 다시 검사할 수 있는 방법이 없는 취약점으로 인해 최근 전력제어시스템을 대상으로 하고 있는 공격들에 무기력한 것으로 알려져 있다[13,14]. 하지만,

SDN은 기존에 보안기술들이 보유하지 않았던 네트워크 동적 재설정기능을 통해 앞서 설명한 공격1과 공격2로 인해 발생된 악의적인 네트워크 트래픽 필터링가능하다. 예를 들어, (그림1)과 같이, SCADA Master와 SDN 제어기는 필요에 따라 협업을 통해 네트워크 제어명령을 보내기 위한 경로 설정이 가능하다. 공격자가 악성코드에 감염된 제어프로그램이나 네트워크 스위치를 통해 불법적인 제어명령을 확산시킬 경우, 앞서 설명한 경로를 통해 더욱 신속한 대응이 가능하다. 또한, (그림2A)에서 볼수 있듯, 공격자가 제어명령을 릴레이로 전달하는 핵심 RTU를 감염시켰을 경우에도 다른 릴레이로의 불법적인 경로설정을 통해 제어명령을 임의적으로 전달할 수 없다.

센서나 릴레이에게 특정 RTU나 데이터 수집장치에게 측정값을 보내도록 요청하는 스푸핑(Spoofing) 패킷을 보내는 공격을 살펴보자. 이는 많은 센서나 릴레이를 활용하여 공격 대상 RTU나 데이터 수집장치에게 대용량 트래픽을 전송하는 DDoS (Distributed Denial-of-Service) 공격으로 정의할 수 있다. (그림2B)

와 같이 SDN은 제어센터를 통해 동적 스위치 설정을 수행하여 네트워크 트래픽 감시를 통해 의심스러운 특정목적지로 향하는 대용량 트래픽을 식별 및 차단할 수 있다. 이와 같은 신속한 대응과정을 통해 공격대상이 되는 스마트그리드 기기들의 부하를 경감시킬 수 있으며, 스마트그리드 통신 네트워크의 가용성을 향상시킨다.

이와 같이, SDN은 조금 더 높은 수준의 네트워크 유연성, 정확성 및 주요 스마트그리드 기기를 대상으로 하는 공격에 대한 대응 효율성을 제공한다.

3.3. 전용망과 공용망의 유기적인 활용

스마트그리드는 공격1과 공격2와 같은 대규모 사이버 공격이나 자연재해로 인한 시스템 주요장애 발생 시에도, 운영을 중단해서는 안 된다. 이는 많은 네트워크 스위치, 릴레이 혹은 RTU를 악성코드에 감염시켜 네트워크의 기능을 마비시킬 만큼의 통신 트래픽을 유발시키는 DDoS 공격의 일종이다.

지금까지, 전력회사들은 주로 전용선을 통한 네트워크를 구축하거나 통신회사와의 계약을 통해 전용 네트워크를 임대해 왔다[20, 21]. 일반적으로 이 같은 네트워크는 인터넷으로부터 보다 효과적으로 격리되지만, 제한적인 대역폭과 네트워크 경로로 인해 앞서 언급한 DDoS 공격과 같은 집중적인 공격에 대해서는 취약하다. 최근 스마트그리드를 구축하고 운영하는 기관에서는 인터넷이나 무선네트워크등과 같이 기존의 전력시스템 구축방법과 다른 통신 도구들을 사용하기 시작했다. 다른 사용자들과 네트워크를 공유하는 위험성이 존재함에도 불구하고, 좀 더 효과적인 통신을 위해서 최신암호기술을 기반으로 여러 가지 통신 방식을 채용하고 있다[22]. 그러나, 많은 전력회사들이 중요한 데이터 혹은 제어명령을 인터넷을 통해 전송하는데 주저하고 있는 것 또한 사실이다.

SDN은 이 같은 전용망과 인터넷등과 같은 공용망을 동시에 사용하면서도, 사이버공격에 대한 위험을 최소화함으로써 스마트그리드 운영자에게 보다 향상된 시스템 생존성을 제공한다. 예를 들어, 스마트그리드 운영자는 일반적인 경우 전용망을 통해 통신을 수행한다. 하지만, 사이버공격 혹은 자연적인 재해로 인해 스마트그리드 통신의 일부가 마비되었을 경우, SDN을 활용해 마비된 지역을 우회하는 비상용 통신 구간 설정이 가능하다. 물론 이와 같은 과정 중에는 보안요구사항에 맞춰 전용망과 공용망 구간별 통신을 수행할 수도 있다. 좀 더 나은 보안성을 위해, 비상용 통신 구간에 위치한 네트워크 장비들과 공용망과의 연계구간에서 암호화를 수행할 수도 있다. 이와 같은 접근 방식은 전력시스템 네트워크의 피해발생 시, 보다 빠르고 안전한 대응을 가능하게 한다.

Ⅳ. SDN의 스마트그리드 적용 시 문제점

제어와 데이터를 분리한 SDN기법은 앞서 언급한 예제를 통해 알 수 있듯, 다양한 장점을 제공한다. 하지만, SDN 제어부를 대상으로 하는 다양한 공격들에 대해서는 취약점이 다수 존재하는 것이 사실이다. 이 장에서는 SDN을 스마트그리드에 적용할 경우 발생가능한 문제점에 대해 간략히 설명한다.

4.1. 공격자에 의한 통신경로 설정 (공격3)

SDN의 경우 중앙에서 네트워크를 제어하기 때문에, SDN 제어기나 해당 시스템에서 동작하는 응용프로그램이 악성코드에 감염되었 경우 전제 시스템이 위험해질 수 있다. 감염된 SDN 제어기나 응용프로그램은 악의적으로 통신 네트워크를 재설정하여, 성능저하를 위한 다양한 제어 메시지를 전송한다. 이 같은 공격에 대해 연구가 진행되었으나 해당 취약점에 대한 대응기법에 대한 연구는 현재까지 부족하다[23,24].

4.2. 중앙제어기로 인한 DDoS 공격

앞서 언급한바와 같이, 부적절한 대역폭 설정 및 SDN 네트워크 장비의 감염은 악의적인 요청 메시지를 발생시켜 대용량 트래픽을 특정 목표로 집중시킬 수 있다[25].

4.3. SDN 루트킷 감염을 통한 Darknet

공격자는 전략적으로 여러개의 스위치의 라우팅테이블을 조작함으로써, SDN 제어부를 대상으로 하는 공격을 발생시켜 Darknet을 생성할 수 있다. 이 같은 방식으로 생성된 Darknet을 통해 스마트그리드의 주요 기기들

을 공격자 임의대로 조종가능하다.

Ⅴ. 결 론

본 문서는 스마트그리드에 SDN을 적용함으로써, 시스템 복원력 향상가능성을 언급함과 동시에 추가적인 보안위협에 대해 논의 하였다.

참 고 문 헌

[1] M. Davis. Recoverable advanced metering infrastructure. In Blackhat, 2009.

[2] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. International Journal of Critical Infrastructure Protection, 5 (3):146{153, 2012.

[3] A. Greenberg, G. Hjalmtysson, D. A. Maltz, A. Myers, J. Rexford, G. Xie, H. Yan, J. Zhan, and H. Zhang. A clean slate 4D approach to network control and management. SIGCOMM Comput. Commun. Rev., 35(5), 2005.

[4] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. OpenFlow: enabling innovation in campus networks. SIGCOMM Computer Communication Review, 38(2):69 {74, 2008.

[5] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, J. Zolla, U. Holzle, S. Stuart, and A. Vahdat. B4: Experience with a globally-deployed software defined wan. In Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication (SIGCOMM), 2013.

[6] M. Reitblatt, M. Canini, A. Guha, and N. Foster. FatTire: declarative fault tolerance for software-defined networks. In Proceedings of ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN), 2013.

[7] S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson. FRESCO: Modular composable security services for software-defined networks. In Proceedings of the 2013 Network and Distributed System

[8] A. Cahn, J. Hoyos, M. Hulse, and E. Keller. Software-defined energy communication networks: From substation automation to future smart grids. In Proceedings of 4th IEEE International Conference on Smart Grid Communications (SmartGridComm), 2013.

[9] A. Goodney, S. Kumar, A. Ravi, and Y. H. Cho. Efficient PMU networking with software defined networks. In Proceedings of 4th IEEE International Conference on Smart Grid Communications (SmartGridComm), 2013.

[10] Y.-J. Kim, K. He, M. Thottan, and J. G. Deshpande. Virtualized and self-configurable utility communications enabled by software-defined networks. In Proceedings of 5th IEEE International Conference on Smart Grid Communications (SmartGridComm), 2014.

[11] E. Molina, E. Jacob, J. Matias, N. Moreira, and A. Astarloa. Using software defined networking to manage and control IEC 61850-based systems. Computers & Electrical Engineering, 2014.

[12] J. Zhang, B.-C. Seet, T.-T. Lie, and C. H. Foh. Opportunities for software-defined networking in smart grid. In Proceedings of the International Conference on Information, Communications and Signal Processing (ICICS), 2013.

[13] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, 9(3):49{51, 2011.

[14] A. Hesseldahl. Hackers infiltrated powergrids. http://on.recode.net/1FpKP7Y.

[15] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. K. Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids. In Proceedings of the Smart Energy Grid Security (SEGS) Workshop, 2013.

[16] S. Bhowmik, K. Tomsovic, and A. Bose. Communication models for third party load frequency control. IEEE Transactions on Power Systems, 19(1):543{548, 2004.

[17] R. Tan, V. Badrinath Krishna, D. K. Yau, and Z.

Kalbarczyk. Impact of integrity attacks on real-time pricing in smart grids. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2013.

[18] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose. Designing the next generation of real-time control, communication, and computations for large power systems. Proceedings of the IEEE, 93(5):965{979, 2005. Security (NDSS) Symposium, 2013.

[19] E. Hossain, Z. Han, and H. V. Poor, editors. Smart Grid Communications and Networking. Cambridge Univ. Press, 2012.

[20] H. L. Smith. A brief history of electric utility automation systems. Electric Energy T&D Magazine,14:39{44, April 2010.

[21] F. Wu, K. Moslehi, and A. Bose. Power system control centers: Past, present, and future. Proceedings of the IEEE, 93(11):1890{1908, Nov 2005.

[22] E. Al-Shaer and S. Al-Haj. FlowChecker: Configuration analysis and verication of federated openflow infrastructures. In Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration (SafeConfig), 2010.

[23] M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford. A NICE way to test openflow applications. In Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2012.

[24] M. Dhawan, R. Poddar, K. Mahajan, and V. Mann. SPHINX: Detecting security attacks in software-defined networks. In Proceedings of the 2015 Network and Distributed System Security (NDSS) Symposium, 2015.

[25] L. Zhang, S. Shetty, P. Liu, and J. Jing. Rootkitdet: Practical end-to-end defense against kernel rootkits in a cloud environment. In Proceedings of the European Symposium on Research in Computer Security (ESORICS), pages 475{493, 2014.

[26] C. Pham, Z. Estrada, P. Cao, Z. Kalbarczyk, and R. K. Iyer. Reliability and security monitoring of virtual machines using hardware architectural invariants. In Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2014.

〈저자소개〉

신 인 철 (Incheol Shin)

2002년 2월 : 한성대학교 컴퓨터공학과 졸업

2006년 8월 : University of Florida 컴퓨터공학과 석사

2010년 8월 : University of Florida 컴퓨터공학과 박사

2010년 6월~2014년 2월 : 한국전자통신연구원 부설 국가보안기술연구소

2014년 3월~현재 : 국립목포대학교 정보보호학과

관심분야 : 네트워크, 컴퓨터이론, 정보보호