한국시뮬레이션학회 논문지
Vol. 24, No. 1, pp. 17-24 (2015. 3)
http://dx.doi.org/10.9709/JKSS.2015.24.1.017
ISSN 1225-5904

시뮬레이션을 이용한 스마트 그리드 통신망 상의 응용 계층 보안 프로토콜의 부하 분석

이광식 · 한승철*

Simulation Analysis of Network Load of Application Level Security Protocol for Smart grid

Kwang-Sik Lee · Seung-Chul Han*

ABSTRACT

Smart grid is a modernized electrical grid that uses information and communication technologies to gather and act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. However, with the advent of cyber crime, there are also concerns on the security of the infrastructure, primarily that involving communications technologies. In this work, we make an in-depth investigation on the issue of security services and network loads on Smart grid. Through simulation, we analyze the relations between security services and network loads. The experimental results of this study will contribute toward designing an advanced Smart grid system that offers better quality of services. Also, the approach proposed in this study can be utilized to derive new and valuable insights in security aspects.

Key words : Smart grid, Security service, Network loads

요 약

스마트 그리드는 전력망에 정보기술을 접목하여, 전력 유틸리티와 사용자가 양방향으로 실시간 정보를 교환하여 에너지 효율을 최적화하고, 전력 전송과 분배에 있어 신뢰성과 기반시설 보호를 유지할 수 있도록 구조화 된 지능형 전력망이다. 하지만 스마트 그리드는 기존 전력망에 IT 기술을 도입하여 시스템을 개선함으로써 에너지의 효율성을 높이려는 연구에서 파생되어 시작되었기 때문에 기존 사이버범죄의 가능성이 존재하며 보안에 취약하다. 본 논문에서는 스마트 그리드의 보안 서비스 제공을 위해, 각 통신망 환경별 보안 서비스가 네트워크에 미치는 영향을 파악하고 응용계층에서 동작하는 보안 프로토콜의 시뮬레이션을 통해, 보안 서비스와 네트워크 부하가 전력 통신망에 미치는 영향을 분석한다. 본 연구의 결과는 진보된 스마트 그리드 보안 서비스 개발에 기여할 것이다.

주요어 : 스마트 그리드, 보안서비스, 네트워크 부하

1. 서 론

스마트 그리드는 전력망에 정보기술을 접목하여, 전력 유틸리티와 사용자가 양방향으로 실시간 정보를 교환하여 에너지 효율을 최적화하고, 전력 전송과 분배에 있어 신뢰성과 기반시설 보호를 유지할 수 있도록 구조화 된 지능형 전력망이다[1].

스마트 그리드는 단순히 사용자단의 검침시스템에 대한 고도화나 기능의 자동화만을 의미하는 것이 아니라,

* 본 연구는 한국연구재단의 중견연구자 지원사업(2012-0005552)과 일반연구자 지원사업(2011-0003930)의 수행 결과임.

Received: 6 August 2014, **Revised:** 7 March 2015, **Accepted:** 19 March 2015

***Corresponding Author:** Seung-Chul Han
E-mail: bongbong@mju.ac.kr
Myongji University Computer Engineering

전력 공급자와 사용자간의 양방향 통신을 이용하여 전력의 발전부터 송배전에까지 참여함으로써 다양한 전력 서비스를 창출하고, 효율적으로 에너지의 수요와 공급의 균형을 맞추는데 목적이 있다[8]. 현재 논의되고 있는 스마트 그리드에서는 각 가정의 검침기로부터 전력 유틸리티들에게 전력 사용 내역에 대한 상세한 소비자 데이터가 전송되는 상향식 데이터 흐름, 이를 바탕으로 유틸리티가 맞춤식으로 전력공급을 하는 하향식 제어 흐름의 구조가 나타난다[2]. 이러한 구조에서는 시스템의 안정적인 동작을 위해 필요한 제어 신호와 데이터들이 전력 통신망을 통해 전송되는데, 이들의 공개나 분실 혹은 변형은 전체에 치명적인 영향을 줄 수 있다[7]. 예를 들어, 송전선이 단락되면 감시 센서가 즉시 그것을 감지해 제어 센터로 데이터를 빠르게 전달함으로써 다른 송전선을 통해 전기를 공급할 수 있게 해야 하지만, 누군가 중간에 데이터를 가로채면 제어 센터가 단락 사실을 알 수 없어서 오랜 시간 정전이 지속될 수 있다. 스마트 그리드에서는 송전선 감시 신호 외에도 전력 서비스에 영향을 줄 수 있는 많은 제어 신호들이 통신망을 통해 전달되기 때문에, 안전하고 안정적인 전력망 서비스를 위해서는 높은 수준의 정보 보안서비스가 반드시 뒷받침 되어야 한다. 또한 전력 공급에 대한 소비자 참여와 분산 신재생 에너지 소스와 맞물려서 프라이버시나 측정가능성 같은 보안 요구사항도 대두된다[5, 11].

스마트 그리드는 기존 전력망에 IT 기술을 도입하여 시스템을 개선함으로써 에너지의 효율성을 높이려는 연구에서 파생되어 시작되었기 때문에, 이러한 IT 기술과의 융합 부분에 스마트 그리드의 보안 요구사항이 구체화된다. 기존 아날로그 단방향 통신이 디지털 양방향 통신으로, 유틸리티 중심의 시스템이 사용자 중심으로, 중앙 집중적 발전이 분산 발전 통합제어로, 수동 복구 감시가 자가 자동 복구로, 제한적인 가격 신호를 가지던 시장에서 수요를 지원하는 시장으로 변화되고 있으며, 이러한 특징으로 말미암아 스마트 그리드는 기존 전력망과 다른 보안 서비스들을 필요로 한다[10]. 예를 들면, 기존 전력망은 대규모 발전소로부터 생산되는 중앙전원으로부터 전력 수요자까지 폐쇄형의 단방향 전력 전달체계로 구성된 반면, 스마트 그리드에서는 사용자단에 연결되는 다수의 장비와 유틸리티들이 FTTH, HFC 등의 유선 통신과 WiFi, WiMax, 3G, TDMA, CDMA, VSAT 등의 무선 통신으로 연결된다[9]. 이러한 통신망은 기본적으로 개방형 네트워크의 형태를 취하고 있기 때문에 여러 가지 보안 취약성을 가지며, 이로 인해 웜이나 바이러스에 의한 해킹이

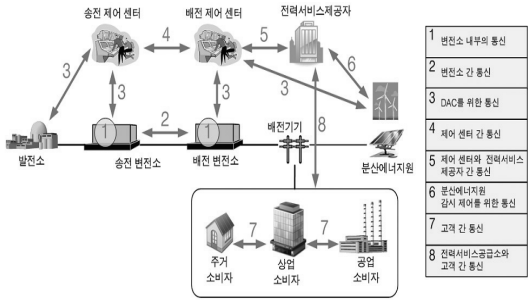

Fig. 1. Smart Grid Network

나 서비스 거부 공격, 크로스서비스 공격 등의 잠재적인 위협이 존재한다[3, 4].

스마트 그리드에서의 보안 서비스 제공을 위해서는 암호화, 인증, 접근 제어와 같은 다양한 보안 기술을 활용해야 하는데, 이를 위해서는 먼저 전력망 내 통신의 환경적 특성을 먼저 파악해야 한다. 스마트 그리드에서는 발전소, 변전소, 제어 센터, 소비자 등이 다양한 통신 환경을 구성한다(Fig. 1). 따라서 암호화, 인증과 같은 다양한 보안 서비스를 제공하기 위해서는 각 통신망의 특성을 먼저 파악해야 한다. 예를 들어, 인터넷 서비스 중에서 지연에 가장 민감한 서비스 중 하나인 실시간 인터넷 전화 서비스도 30 msec 까지 통신 지연을 허용하는 반면, 스마트 그리드의 변전소 내의 통신은 훨씬 대량의 데이터 전송을 요구하면서도 4 msec 이하의 매우 짧은 지연을 허용한다. 이러한 통신만의 특성은 보안 서비스 제공에 제약을 가져온다. 일반적으로 보안 기술의 활용은 CPU 사용량을 증가시키거나 추가 데이터 전송 등의 통신 부하를 발생시키기 때문에, 통신 속도 감소와 지연 증가의 요인이 되기 때문이다. 따라서 스마트 그리드의 보안을 위해서는 보안 기술에 대한 성능분석이 중요하다. [14]는 스마트 그리드 보안 모델을 개발하고 성능분석에 근거한 암호기술과 인증기술의 운용 방안을 제시하였다. [15]는 한국형 스마트 그리드를 위한 정보보호 체계에 대한 성능분석을 하였다. 또한 [16]에서는 스마트 그리드 AMI 환경에서 보안 성능에 대한 분석을 하였다. 그러나 기존 연구들은 스마트 그리드 내 다양한 네트워크 환경에 따라 보안 서비스가 미치는 영향을 파악하는데 미흡하였다.

본 연구에서는 발전소, 변전소, 제어 센터, 사용자 등으로 구성되는 스마트 그리드 통신 환경을 구축하고, 응용계층에서 동작하는 보안 프로토콜의 시뮬레이션을 통해, 보안 서비스와 네트워크 부하가 전력 통신망에 미치는 영향을 분석한다. 2장에서는 스마트 그리드 보안 서비스의

요구사항을 정리하고, 이를 충족시키는 응용 계층 보안 프로토콜을 3장에서 제안한다. 4장에서는 시뮬레이션 실험결과를 분석하고, 마지막으로 5장에서 결론을 내린다.

2. 스마트 그리드 보안서비스

스마트 그리드는 다양한 역할을 담당하는 시스템들이 상호작용하며 사용자에게 효율적이고 안정적인 전력공급을 담당한다. 이를 위해서는 다양한 시스템들 사이에 상호작용을 돕거나 제어기능을 수행할 수 있도록 하는 통신 프로토콜이 필요하다. 현재의 전력망은 이러한 상호 정보 교환 및 제어 명령 전달을 위해서 DNP (Distributed Network Protocol), ICCP (Inter-control Center Communications Protocol), Modbus 같은 프로토콜들을 사용하고 있다. 스마트 그리드 역시 호환성과 상호운용성 보장을 위해서 같은 프로토콜을 사용한다. 하지만 이들 통신 프로토콜은 전력망 제어 시스템이 일반 네트워크와 분리되어 있어 안전하다는 전제하에 개발되었기 때문에 보안성이 전혀 고려되어 있지 않다. 스마트 그리드 통신망에서는 사용자 정보 및 소규모 분산 전원 등과 정보 교환을 해야 하므로 통신 연계점이 생기게 마련이고, 이 경우, 보안에 취약한 현재 프로토콜들은 공격자의 침투 경로로 사용될 수 있다. 보안 서비스가 제공되지 않을 경우 공격자가 메시지를 중간에 가로채서 정보를 획득할 수 있고, 가로챈 메시지를 재사용해 잘못된 제어 명령을 내릴 수도 있다. 또한 메시지에 대한 인증 기능을 수행하지 않을 경우 제어 센터의 서버로 가장하여 모든 말단 제어 기기들을 공격자 마음대로 제어할 수 있다. 더 나아가 공격에 대한 보호 매커니즘이 존재하지 않으므로 공격자는 말단 제어기기를 가장해 악성 코드를 전송하는 방법을 통해 손쉽게 서버에 침투하여 관리자 권한을 획득할 수 있고, 이는 곧 전체 제어 네트워크를 공격자가 원하는 대로 제어 할 수 있음을 의미한다. 그러므로 스마트 그리드에서의 보안이슈가 전력 제어신호와 데이터에 관련되어 존재하는 경우, 기존의 통신 프로토콜에 덧붙여 다음과 같은 보안 서비스들을 제공해야 한다[6, 12].

① 기밀성(Confidentiality) 서비스 - 기밀성은 데이터 및 메시지의 전송과정이나 처리과정에 있어서 정보가 인가되지 않은 개체에 누설되거나 공개되지 않아야함을 의미한다. 기밀성이 낮게 되면 크게는 전기의 배전 과정이나 발전소의 동작과정 등에 침입자가 발생하여 전력계통의 안정성에 큰 영향을 줄 수도 있고 작게는 개인의 전력사용패턴 유출로 인한 프라이버시의 침해를 일으킬 수도 있다. 스마트 그리드 환경에서 원격 디바이스로부터 수집되는 데이터의 경우, 사용량이나 요금 관련 정보 등 민감한 정보들이 네트워크를 통해 전송되므로 비인가된 제3자가 데이터의 내용을 알 수 없도록 암호화 등의 매커니즘을 이용하여 중요 정보를 보호해야 한다.

② 무결성(Integrity) 서비스 - 무결성은 데이터 및 메시지의 전송과정에서 정보가 고의적 또는 우발적으로 변조되지 않고 일관성을 유지하는 속성을 의미한다. 정보를 보낸 주체는 자신이 보낸 메시지가 변경되지 않고 수신되기를 원하며, 수신자의 입장에선 이 메시지가 아무런 변화 혹은 파괴 없이 자신에게 도달되었음을 확인하는 것이다. 스마트 그리드 환경의 경우 제3자가 중간자공격(man-in-the-middle attack) 등을 이용하여 서버와 디바이스 사이에 전송되는 메시지를 위·변조하는 공격이 가능하다. 따라서 이러한 보안 위협에 대응하기 위해 개체 사이에 전송되는 데이터의 무결성을 보장할 수 있는 매커니즘이 필요하다.

③ 인증(Authentication) 서비스 - 인증은 송, 수신자가 서로 상대방을 식별할 수 있음을 나타낸다. 스마트 그리드 환경의 서버 및 사용자에 대한 인증이 제공되지 않는 경우에는 공격자가 정당한 서버 혹은 사용자로 위장하여 정당한 디바이스들이 보내는 메시지를 획득하는 공격이 가능하다. 따라서 디바이스가 메시지를 보내기 전에 정당한 서버, 사용자인지를 확인할 수 있는 인증절차가 요구된다.

④ 부인방지(Non-Repudiation) 서비스 - 일반적인 의미는, 계약 또는 통신의 한 상대가 문서에 있거나 또는 보내어진 메시지에 첨부된 서명의 확실성을 부정할 수 없도록 보증하는 능력을 가리킨다. 스마트 그리드 환경에서 메시지 송수신 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실부인을 방지하는 매커니즘이 필요하다. 이러한 매커니즘을 통해 메시지를 수신하고도 메시지가 전달된 사실이 없다고 주장하는 수신자 측의 부인을 방지하며 또는 역으로 메시지를 전달하지 않고도 송신하였다고 주장하는 송신자 측의 부인을 방지할 수 있다. 인증과 부인방지에는 전자 서명(Digital Signature)기법이 주로 사용된다. 통신망상에서 전자 서명은, 메시지나 문서가 당사자에 의해 전자적으로 서명되었다는 것을 보증하는 것은 물론, 후에

그 서명이 제시되었을 때 그가 부인할 수 없도록 보증하기 위해 사용된다.

⑤ 세션키 갱신 서비스 - 기밀성 서비스의 암호화 방법은 통신 당사자들 간에 비밀키를 공유하도록 하는데, 이를 세션키라고 부른다. 보통 세션키는 새로운 통신 연결이 맺어지는 시점에 미리 약속한 방식으로 생성 및 배포된다. 그러므로 만약 통신연결이 오래 지속되면 같은 키를 오래 사용하게 되기 때문에 유출의 위험이 있다. 이를 방지하기 위해서 연결이 오래 지속되는 통신의 경우 주기적으로 갱신해 주어야 한다. 세션키 갱신은 타임아웃시간 설정을 통해 이루어진다. 통신 연결을 맺을 때나 키가 갱신될 때마다 타임아웃 시간을 설정하여서 이 시간 후에 키 갱신이 일어나도록 한다.

3. 응용계층 보안 프로토콜

2장의 보안 서비스들을 보장하기 위해 제공되는 기술이나 방법은 그 종류가 매우 다양하다[12]. 또한 각 보안 서비스는 보장하는 보안 요구사항이 보통 서로 다르고, 같은 보안 요구사항을 보장하더라도 통신망의 특성에 따라 제공하는 보안 수준에는 차이가 있다. 본 장에서는 보안 서비스가 네트워크 부하에 미치는 영향을 측정하기 위해서, 기존의 통신 프로토콜의 상위 계층에서 유연하게 적용할 수 있는 다음과 같은 응용 계층 보안 프로토콜을 제안한다.

송신자는 자신의 개인키로 메시지 인증코드를 만들고 메시지는 세션키로 암호문을 만든다. 세션키는 수신자의 공개키로 암호화하여 암호문, 세션키, 전자서명을 전송한다. 수신자는 자신의 개인키로 세션키를 구하고 세션키로 암호문을 평문으로 복호화한다. 이 후 복호화된 평문을 약속된 메시지 인증코드 알고리즘으로 메시지 인증코드를 구하여서 수신된 메시지 인증코드와 비교한다. 두 값이 일치하면 수신자는 데이터를 정상적으로 수신하지만, 일치하지 않으면 데이터에 이상이 있는 것으로 판단한다. 메시지 인증코드 알고리즘은 비밀키를 이용하여 메시지 인증코드를 만들기 때문에 공격자가 임의로 메시지 인증코드를 생성할 수 없다.

스마트 그리드에서 발생하는 주요 보안 요구사항으로는 일반적인 IT 보안 경우와 같이 기밀성, 무결성, 인증, 부인방지, 세션키 관리가 요구되며, 제시된 보안 프로토콜의 사용으로 이들 요구사항을 대부분 충족시킬 수 있다. 하지만 이러한 보안 프로토콜이 그대로 스마트 그리드에 적용될 수 있는가는 다른 문제이다. 왜냐하면 실제 보안 모듈의 적용은 많은 CPU 자원과 시간을 소비하므로 열악한 프로세서 환경이나 매우 짧은 지연시간을 요구하는 통신환경에서는 사용이 제한되기 때문이다. 다음 장에서는 제시된 보안 프로토콜이 다양한 스마트 그리트 통신망에 미치는 영향을 시뮬레이션을 통해 분석한다.

4. 시뮬레이션

본 시뮬레이션에서는 스마트 그리드의 각 통신환경에 따른 보안 서비스와 네트워크 부하의 영향을 측정한다. 시뮬레이션을 위한 네트워크의 구성은 Fig. 3과 같으며,

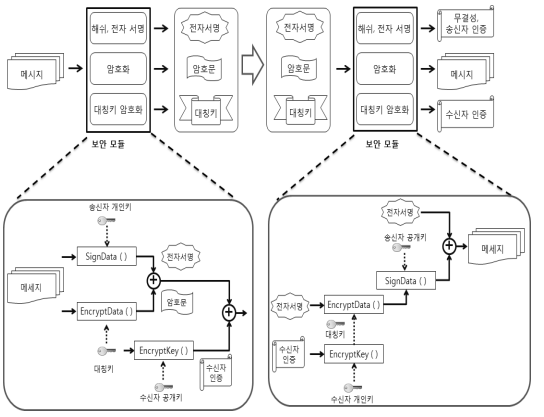

Fig. 2. Security Protocol

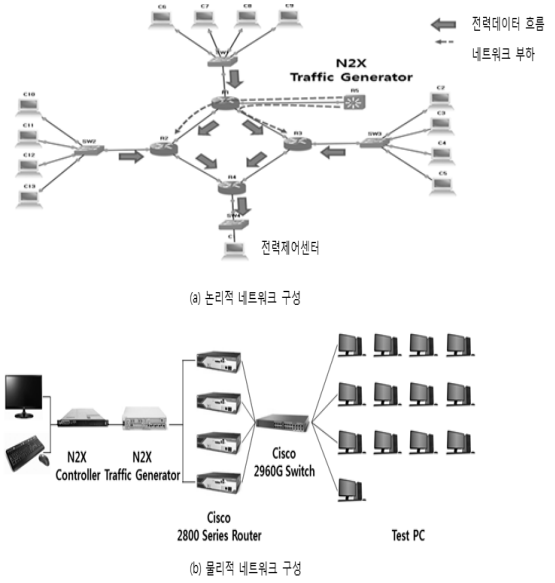

Fig. 3. Smart Grid Network Architecture

Table 1. Equipment Specification

장비	사양
Cisco 2821,2851 라우터	256M DRAM, 128M Flash Memory 10/100/1000 Ethernet T1/E1/XDSL PoE 전원공급장치
Cisco WS-C2960G-24TC-L	Catalyst 2960 24 10/100/1000 4 T/SFP LAN Base Image
HWIC 1GE SFP	GigE High speed WIC with 1 SFP slot
GLC-T	1000 Base-T SFP
Agilent N2X N5541A	10/100/1000 Base-T, 1000 Base-X(SFP) 지원
Cisco WS-C2960G-24TC-L	Dual core AMD Opteron 2200 CPU 4G RAM ECC DDR2 667MHz SDRAM Windows Server 2003 R2
Test PC	Intel 2600K i7 4G RAM Windows 7 32bit

장비들의 사양은 Table 1과 같다. 각 클라이언트들은 라우터와 스위치들을 통해서 서로 전력 데이터를 주고받으며, 라우팅 프로토콜은 OSPF를 사용한다. 트래픽 발생기는 Agilent사의 N2X N5541A[13]를 사용하였으며, 스위치에 직접 연결되어 네트워크에 부하를 발생시킨다. 발생되는 트래픽은 고정된 크기의 UDP 패킷 스트림으로 전송량은 초당 전송되는 패킷의 개수로 제어된다. 프로그램의 개발은 Windoews7 32bit, .NET Framework 4.5, Visual Studio 2012에서 C#으로 작성되었다. 프로그램의 구성요소는 서버, 클라이언트, 전력데이터이다. 서버는 클라이언트와 1:N 통신을 수행하며 연결된 클라이언트들의 통신 상태 제어와 전력 데이터 수집을 수행한다. 클라이언트는 서버와 1:1 통신을 하며 전력 데이터를 전송한다. 전력 데이터는 XML 파일을 이용한다. 전력 데이터를 전달하는 패킷의 구조는 Fig. 4와 같으며, 각 필드들에 대한 자세한 설명은 Table 2와 같다. 본 시뮬레이션에서는 네트워크상의 서버와 클라이언트들이 각각 화력발전소, 수력발전소, 변전소의 역할을 하며, 일대일(one-to-one) 혹은 다대다(many-to-many) 관계로 전력 데이터를 주고받는다.

Fig. 5는 발전소간 일대일(one-to-one) 통신망의 지연시간(delay time)을 측정한 결과이다. 실험에서는 트래픽 발생기를 통하여 네트워크 링크부하를 각각 0, 30, 60, 100%로 발생하였다. 패킷 트래픽은 일정한 간격으로 전송되는 UDP 패킷 스트림이며, 패킷간의 간격은 전송률

My ID (4bytes)	Packet ID (4bytes)	Local IP (4bytes)	Local IP (4bytes)
Host Type (4bytes)	Packet Type (4bytes)	Running Type (8bytes)	
Data Length (4bytes)	Packet Per Sec (4bytes)	Transmission Rate (4bytes)	Receiving Rate (4bytes)
Delay Type (8bytes)		Packet Ross (4bytes)	Sequence Error (4bytes)
Session Alive (1byte)	Encrypted (1byte)	Checksum (4bytes)	
Data			

Fig. 4. Packet Structure

Table 2. Field Name Description

Field Name	Description
ID	클라이언트 ID
Packet ID	각 패킷에 대한 ID
Local IP	패킷 송신자 IP
Local Port	패킷 송신자 포트넘버
Host Type	서버, 클라이언트 구분
Packet Type	(패킷의 종류구분 ACK, Alive, Data, AESKEY, RSAKEY, CONTROL, LOGIN, PROTOCOL, LOG)
Running Time	연결이후 시간표시(sec)
Data Length	데이터 길이
Packet per Sec	초당 전송 패킷수
Transmission Rate	초당 송신 패킷 bytes
Receiving Rate	초당 수신 패킷 bytes
Delay Time	전송 패킷의 지연시간(ns)
Packet Loss	패킷 손실수
Sequence Error	에러 발생수
Session Alive	클라이언트 세션여부
Encrypted	패킷의 암호화 여부
Checksum	데이터필드 checksum
Data	데이터

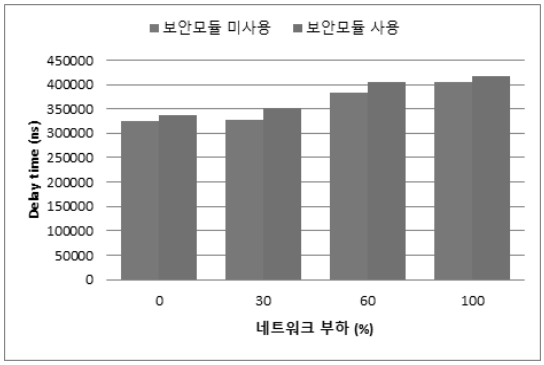

Fig. 5. One-to-one Communication

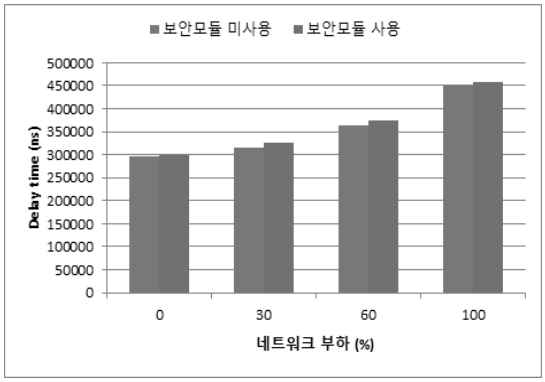

Fig. 6. Many-to-many Communication

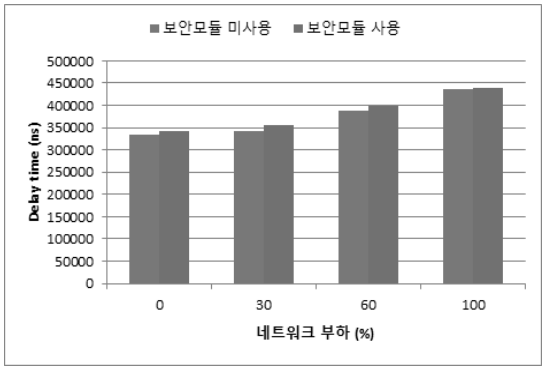

Fig. 7-a. One-to-one Communication

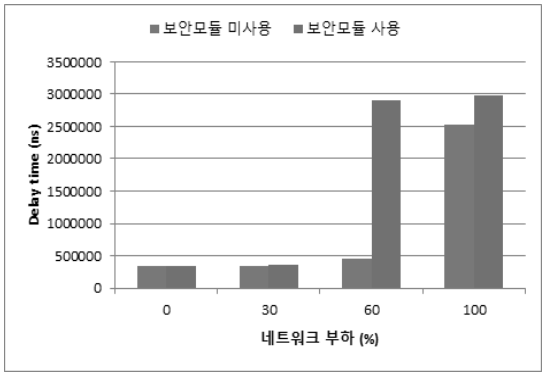

Fig. 7-b. Many-to-many Communication

(transmission rate)에 의해 결정된다. 보안모듈의 적용여부에 관계없이 네트워크 부하가 증가할수록 지연시간은 증가하였다. 보안모듈을 적용할 경우는 그렇지 않은 경우보다 지연시간이 평균 10ms정도 증가되었다. 따라서 3장에 제시된 응용 계층의 보안 서비스제공을 위해서는 10ms정도의 지연시간을 고려해야함을 알 수 있다.

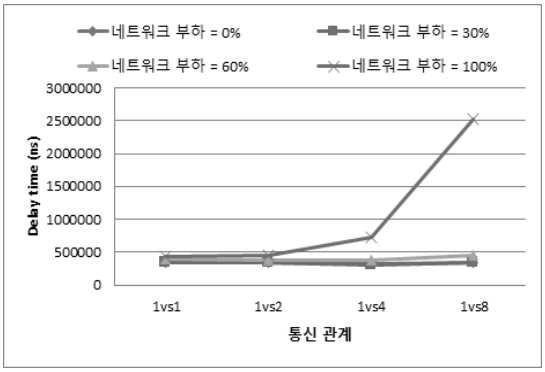

Fig. 8-a. Unapplied Secure Module

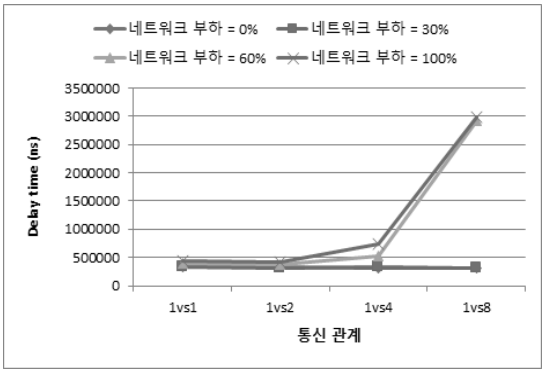

Fig. 8-b. Secure Module Applies

Fig. 6은 변전소간 다대다(many-to-many) 통신망의 지연시간을 측정한 결과이다. 그래프는 4:32관계의 결과를 보여준다. Fig. 5와 마찬가지로 지연시간은 보안모듈 적용여부에 상관없이 네트워크 부하에 따라 증가하고, 보안모듈을 적용했을 때가 그렇지 않을 때보다 지연시간이 증가함을 알 수 있다.

Fig. 7은 수력발전소간 일대일(7-a)와 일대다(7-b) 경우의 지연시간을 측정한 결과이다. 일대일의 경우에는 발전소간 통신경우와 마찬가지로 네트워크 부하가 증가할수록 지연시간이 증가하며 보안모듈을 사용할 경우 평균 10ms정도 증가하였다. 모든 경우에 동일하게 시간이 지연된 것은 3장의 응용 계층 보안 프로토콜의 처리 때문이며, 장비의 물리적 사양에 따라서 증감이 가능하다. 그러나 일대다의 경우는 네트워크 부하가 대략 60% 이상일 경우에는 보안모듈의 적용여부가 지연시간에 큰 영향을 주는 것을 알 수 있다. 이는 본 실험환경에서 네트워크 부하가 60%이상이고 다수의 노드들이 패킷을 주고받는 경우, 보안 프로토콜의 처리 때문에 전송지연(transmission

delay)가 발생했기 때문으로 분석된다. 한편 보안 프로토콜을 사용하지 않으면 네트워크 부하가 100%정도에 이르러야 지연시간이 크게 증가하였다. 결론적으로 네트워크 부하가 클 경우에는 보안모듈의 적용여부가 스마트 그리드망의 성능에 중대한 영향을 미침으로 보안 서비스 적용을 신중하게 고려해야 함을 알 수 있다.

Fig. 8은 수력발전소간의 통신관계가 1:1, 1:2, 1:4, 1:8 경우의 지연시간을 측정한 결과이다. 보안모듈을 적용하지 않는 경우(8-a)에는 네트워크 부하가 100% 경우를 제외한 모든 경우에 있어서 통신관계는 큰 영향을 미치지 않았다. 100% 경우에는 통신관계가 늘어날수록 지연시간이 크게 증가함을 알 수 있다. 보안모듈을 적용하는 경우에는 네트워크 부하가 60% 이상 경우도 통신관계가 늘어날수록 영향을 많이 받음을 알 수 있다. 따라서 보안모듈을 적용할 경우에는 네트워크 부하가 비교적 작더라도 통신관계가 증가하면 지연시간에 큰 영향을 준다는 것을 알 수 있다.

5. 결 론

고효율의 지능화된 전력망은 단순히 전력 공급망 발전의 측면만이 아니라 디지털 사회의 성장하는 수요에 적합한 새로운 전력 인프라의 구축을 위한 것이라 할 수 있으며, 또한 지속가능한 발전을 위한 환경 친화적인 인프라로써 현재의 환경문제를 해결할 것으로 예상되기 때문에 사회 전 분야에서 광범위하게 스마트 그리드에 대한 기대가 일어나고 있다. 그러나 스마트 그리드가 가능하기 위해서는 무엇보다도 보안이 보장되어야 함에도 불구하고, 아직까지는 스마트 그리드에 대한 관심에 비해 보안의 고려가 미흡한 상태이다.

본 논문에서는 발전소, 수력발전소, 변전소, 제어 센터, 사용자로 구성되는 다양한 스마트 그리드 통신 환경을 구축하고, 응용계층에서 동작하는 보안 프로토콜의 시뮬레이션을 통해, 보안 서비스와 네트워크 부하가 전력 통신망에 미치는 영향을 측정하였다. 아직 스마트 그리드가 실체적인 모습을 갖추는 초기단계이고, 스마트 그리드에서 사용될 기술들 또한 한창 논의·개발중임을 고려하면, 아직 보안 서비스가 네트워크에 미치는 영향을 파악하는 것은 시기상조일지 모르지만, 보안의 고려가 초기에부터 동반되지 않는다면, 차후 문제 상황이 발생하였을 때 피해의 복구가 어려울 수 있기 때문에 본 논문에서와 같은 논의가 스마트 그리드의 개발과 더불어 병렬적으로 수행되어야 한다고 생각한다. 본 연구의 결과는 향후 다양한 스마트 그리드 보안 서비스 제공에 기여할 것으로 기대된다.

References

1. Energy Idependence and Security AAct of 2007(EISA) Title XIII. SMART GRID. Section 1301. Statement of Policy on Modermizatin of Electricity Grid.
2. Venkat Phthamsetty, Saadat Malik, Smart Grid: Leveraging Intelligent Communications to Transform the Power Infrastructure, Cisco White Paper.
3. 지식경제부 사이버 안전센터, 연간 침해사고 탐지현황 자료, 2011년 3월.
4. Juniper Networks Inc., Architecture for secure SCADA and distributed control system networks, White Paper, Feb. 2009.
5. Arvid Kjell et al., Guide to Increased Security in Process Control Systems for Critical Societal Functions, The Swedish forum for information sharing concerning information security-SCADA and process control systems, Swedish Emergency Management Agency, 2008.
6. Alvaro Cardenas et al., Research Challenges for the Security of Control Systems, the 3rd conference on Hot Topics in Security, 2008.
7. 토니 플릭, 저스틴 모어하우스, 스마트 그리드 보안, BJpublic Inc. 2011.
8. 스마트 그리드 성능 향상을 위한 측정 지표의 활용 현황, 국토해양 기술동향, 2013.
9. Wenye Wang, Yi Xu, Mohit Khanna, A survey on the communication architectures in smart grid, Computer Networks, Elsevier, vol.55(15), 2011.
10. 김종오, 스마트 그리드 산업 및 표준화 동향, KATS 기술보고서 22호, 2010.
11. Smart grid cyber security potential threats, vulnerabilities and risks, PIER program interim project report,, California Energy Commission, 2012.
12. AMI-SEC Task Force Advanced Metering Infrastructure (AMI) System Security Requirements, December 2009.
13. N2X Traffic Generation and Analysis, Agilent Inc., http://en.wikipedia.org/wiki/Agilent_Technologies.
14. 서정택, 스마트 그리드 보안 체계 연구, 국가보안기술연구소, 2013.

15. 이철환, 홍석원, 이명호, 이태진, 한국형 스마트그리드를위한 정보보호 체계 및 대책, Internet and Information Security, 2권(1호), 2011.

16. 구본진, 전용희, 스마트그리드 AMI 통신의 보안 성능 평가, 자연과학연구논문집 10권(1호), 2012.

이 광 식 (saetian@mju.ac.kr)

2007 연세대학교 경영학과 석사
2011～2014 명지대학교 컴퓨터공학과 박사과정 수료
현재 신한금융지주회사 ICT기획팀

관심분야 : IT전략, IT거버너스, 금융보안, 스마트그리드

한 승 철 (bongbong@mju.ac.kr)

2003 Purdue University 컴퓨터학과 석사
2007 University of Florida 컴퓨터공학과 박사
현재 명지대학교 컴퓨터공학과 조교수

관심분야 : 스마트그리드, Network Security