스마트 그리드상의 보안 프로토콜 시뮬레이션

이광식, 한승철
명지대학교 컴퓨터공학과
e-mail: saetian@mju.ac.kr bongbong@mju.ac.kr

TCP-friendly Application Level Security Protocol Simulations for Smart Grid

Kwang-Sik Lee, Seung Chul Han
Dept of Computer Engineering, Myongji University

요 약

스마트 그리드는 IT 기술을 전력망에 도입함으로써 전력 인프라의 신뢰성, 효율성, 안전성 등을 향상시키고 공급자와 소비자 간의 양방향 통신을 가능하게 하여 전력 선택 범위를 넓히고 전력 인프라의 효율성을 향상시키는 차세대 지능형 전력망이다. 그러나 스마트 그리드의 효과적인 운용을 보장하기 위한 보안서비스 제공을 위해서는 전력망 내의 통신환경에 대한 특성 파악과 보안 서비스가 전력 통신망에 끼치는 영향을 파악하여야 한다. 본 연구에서는 보안 서비스와 네트워크 부하가 전력 통신망에 어떠한 영향을 주는지 실험을 통해서 분석한다.

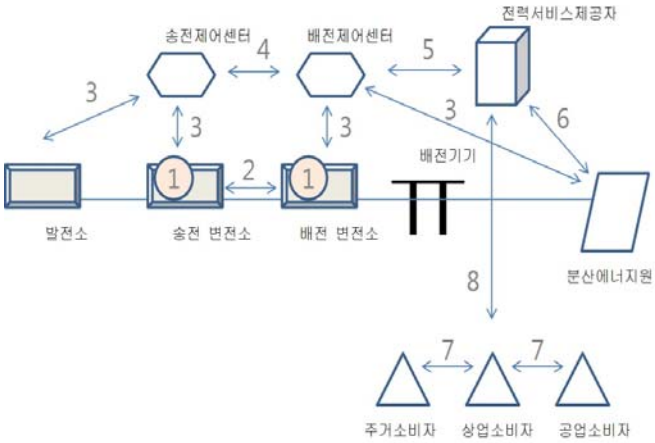
1. 서론

스마트 그리드는 IT 기반의 미래형 전력망으로 전력, 통신망, 센서 등의 IT 기술을 전력망에 도입함으로써, 전력 인프라의 효율성, 안전성, 유연성, 보안성, 신뢰성 등을 향상시키고 전력 생산, 계통 시스템과 사용자 간의 양방향 통신을 가능하게 하여 사용자의 전력 선택 범위를 넓히고, 이를 통해 에너지 부문의 인터넷으로써 전반적인 전력 인프라 시스템의 효율성을 향상시키는 친환경적인 디지털 시대를 위한 지능형 전력망이라고 정의할 수 있다[1].

스마트 그리드는 단순히 사용자단의 검침시스템에 대한 고도화나 기능의 자동화만을 의미하는 것이 아니라, 유틸리티와 사용자간의 양방향 통신을 이용하여, 전력의 발전부터 송배전에까지 참여함으로써, 다양한 전력 서비스를 창출하고, 효율적으로 에너지의 수요와 공급의 균형을 맞추는데 목적이 있다. 현재 논의되고 있는 스마트 그리드에서는 사용자단의 검침기로부터 유틸리티에게 전력 사용내역이나 선호시간 등의 상세한 소비자 데이터가 전송되며, 이를 이용하여 유틸리티가 전력을 통제하는 상향식 데이터 흐름 및 하향식 통제 흐름의 구조가 나타난다. 이러한 구조는 본질적으로 전력 공급에 대한 소비자 참여와 맞물려서 프라이버시, 측정가능성 같은 보안 문제들을 야기할 것으로 예측된다. 또한 전력 시스템의 안정적인 동작을 위해 필요한 중요 데이터들이 통신망을 통해 전송되는데, 이러한 데이터들의 분실이나 변조는 전체 전력 서비스에 치명적인 영향을 줄 수 있다. 예를 들어, 송전선이 단락되면 감시 센서가 즉시 그것을 감지해 제어 센터로 데이터를 빠르게 전달함으로써, 다른 송전선을 통해 전기를 공급할 수 있게 해야 하지만, 중간에 데이터가 분실되거나 ns]변조된다면 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 신호들이 통신망을 통해 전달되기 때문에, 안전하고 안정적인 전력망 서비스를 위해서는 높은 수준의 정보 보안이 반드시 뒷받침 되어야 한다[2].

스마트 그리드에서의 보안 서비스제공을 위해서 선결되어야 할 문제는 다음과 같이 두 가지로 정리할 수 있다. 첫 째로, 스마트 그리드에서는 발전소, 변전소, 제어 센터, 소비자 등이 다양한 통신 환경을 구성한다 (그림 1). 따라서 암호화, 접근 제어와 같은 다양한 보안 서비스를 제공하기 위해서는 각 통신망의 특성을 먼저 파악해야 한다. 두 번째, 다양한 보안 서비스를 적용할수록 보안성은 강화되지만 보안 서비스의 적용은 CPU 사용량을 증가 시키거나 추가 데이터 전송 등의 네트워크 부하를 발생시키기 때문에, 통신 속도 감소와 지연 증가의 요인이 될 수도 있다. 따라서 보안 서비스가 네트워크에 미치는 영향을 파악하여야 한다[3].

본 연구에서는 발전소, 변전소, 제어 센터, 사용자로 구성되는 다양한 가상의 스마트 그리드 통신 환경을 구축하고, 응용계층에서 동작하는 TCP-friendly 보안 프로토콜의 시뮬레이션을 통해, 보안 서비스와 네트워크 부하가 전력 통신망에 미치는 영향을 측정한다. 2장에서는 스마트 그리드 보안 요구사항을 정리하고 TCP-friendly 보안 프로토콜을 제안한다. 3장에서는 실험결과를 분석하고, 마지막으로 4장에서 결론을 내린다.



(그림 1) 스마트 그리드 통신 환경

2. 스마트 그리드 보안 요구사항과 프로토콜

스마트 그리드에서의 보안이슈가 전력 데이터와 관련된 각 기술에서의 보안취약점으로 인해 존재하는 경우, 이에 대한 대응방안으로써 기술적인 보안조치를 고려해야 한다. 각 보안 이슈에서 요구되는 보안 요구사항을 바탕으로, 이러한 보안요구사항을 만족시킬 수 있는 기술적 보안조치를 중심으로 응용 계층 스마트 그리드 보안 프로토콜을 제안한다. 먼저, 스마트 그리드에서 기본적으로 제공되어야 하는 보안 요구사항을 살펴보면,

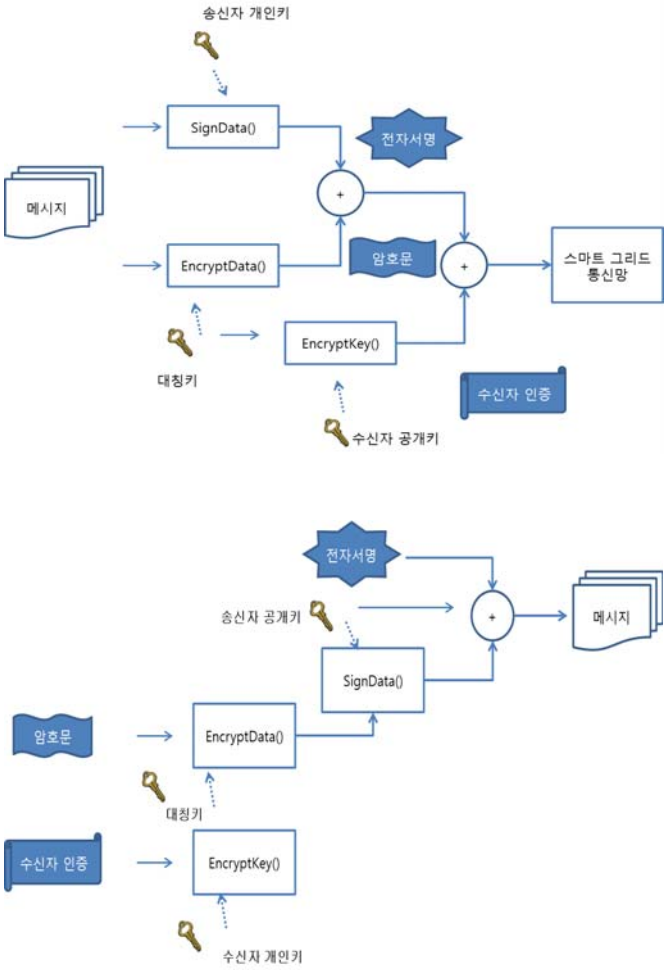
▷ 기밀성(Confidentiality)
데이터 및 메시지의 전송과정이나 처리과정에 있어서 정보가 인가되지 않은 개체에 누설되거나 공개되지 않아야함을 의미한다.

▷ 무결성(Integrity)
데이터 및 메시지의 전송과정에서 정보가 고의적 또는 우발적으로 변경 파괴되지 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.

▷ 인증(Authentication) 및 부인방지(Non-Repudiation)
인증은 송, 수신자가 서로 상대방을 식별할 수 있음을 나타낸다. 부인방지의 일반적인 의미는, 계약 또는 통신의 한 상대가 문서에 있거나 또는 보내어진 메시지에 첨부된 서명의 확실성을 부정할 수 없도록 보증하는 능력을 가리킨다.

이러한 기술적 보안 조치 및 보안 요구사항을 정리하면, 스마트 그리드에서 발생하는 보안 이슈는 일반적인 IT 보안 요구사항과 같이 기밀성, 무결성, 가용성, 부인방지가 요구되며, 인증, 암호화, 접근통제관리, 로그 관리 등과 같은 기존 보안 기술의 사용으로 이들 요구사항을 충족시킬 수 있다. 하지만 이러한 기존의 보안 기술이 그대로 스마트 그리드에 적용될 수 있는가는 다른 문제이다. 예를 들어, 인터넷 서비스 중에서 지연에 가장 민감한 서비스 중 하나인 실시간 인터넷 전화 서비스도 30 msec까지 통신 지연을 허용하는 반면, 스마트 그리드의 변전소 내의 통신은 훨씬 대량의 데이터 전송을 요구하면서도 4 msec 이하의 매우 짧은 지연을 허용한다. 이러한 특성은 보안기술 적용에 제약을 가져온다.

본 연구에서는 다음 (그림 2)와 같은 기밀성, 무결성, 인증 및 부인 방지를 제공하는 응용 계층의 보안 프로토콜이 네트워크에 미치는 영향을 실험을 통해 분석한다.

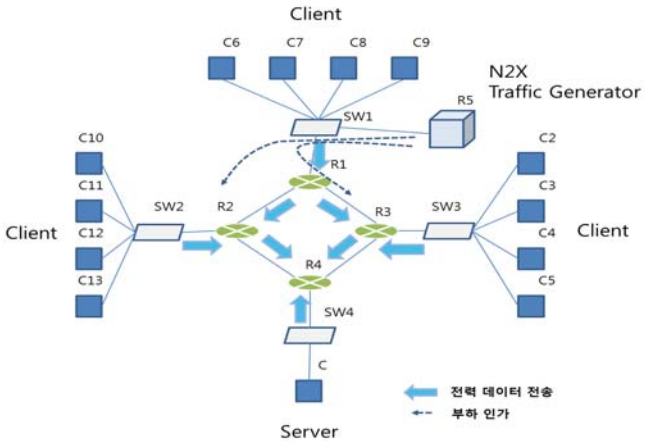


(그림 2) 보안 프로토콜

3. 실험

본 실험에서는 스마트 그리드의 각 통신환경에 따른 보안 서비스와 네트워크 부하의 영향을 측정한다.

실험을 위한 네트워크의 구성은 (그림 3)과 같다. 각 클라이언트들은 라우터와 스위치들을 통해서 서로 전력 데이터를 주고받으며, 라우팅 프로토콜은 OSPF를 사용한다. 트래픽 발생기는 스위치에 직접 연결되어 네트워크에 부하를 발생시킨다.



(그림 3) 네트워크 구성도

테스트 프로그램의 개발은 Windoews7 32bit, .NET Framework 4.5, Visual Studio 2012에서 소켓 프로그램으로 작성되었다. 테스트 프로그램의 구성요소는 서버, 클라이언트, 전력데이터이다. 서버는 클라이언트와 1:N 통신을 수행하며 연결된 클라이언트들의 통신상태 제어와 전력 데이터 수집을 수행한다. 클라이언트는 서버와 1:1 통신을 하며 전력 데이터를 전송한다. 전력 데이터는 XML 파일 포멧을 이용한다. 전력 데이터를 전달하는 패킷의 구조는 그림 4와 같다. (각 필드들에 대한 자세한 설명은 Appendix 참조)

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

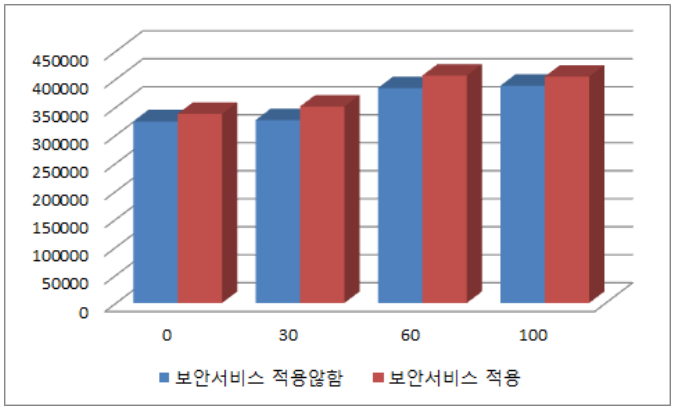
(그림 4) 패킷 구조

본 실험에서는 네트워크상의 서버와 클라이언트들이 각각 화력발전소, 수력발전소, 변전소의 역할을 하며 전력 데이터를 주고받으며, 트래픽 발생기는 네트워크에 부하를 발생한다. 각 경우에 있어서 보안 서비스를 제공하는 경우와 그렇지 않은 경우를 비교한다.

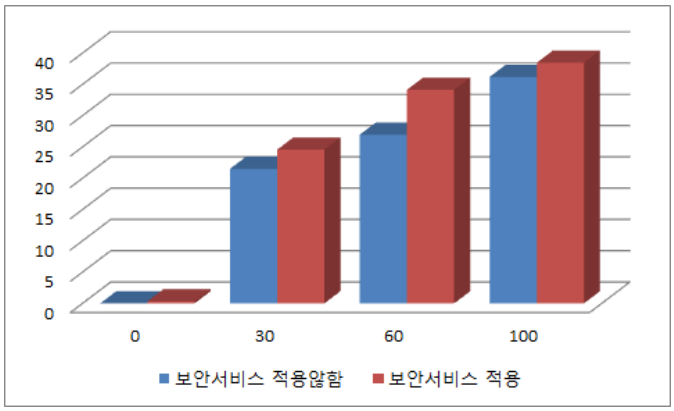
그림 5와 6은 발전소간 1:1 통신을 할 경우의 지연시간(delay time)과 패킷 분실율(loss rate)을 측정한 결과이다. 실험에서는 트래픽 발생기를 통하여 네트워크 부하를 각각 0, 30, 60, 100%로 주었다. 지연시간의 경우는 부하가 커질수록 지연시간이 증가하였다. 또한 보안 서비스를 제공할 경우가 약간 큰 지연시간을 갖는 것을 보였다. 패킷 분실율의 경우도 네트워크 부하가 커질수록, 보안 서비스를 제공하는 경우가 조금 큰 패킷 분실율을 보였다.

<표 1> 테스트 장비 사양

장비	사양
Cisco 2821,2851 라우터	• 256M DRAM, 128M Flash Memory • 10/100/1000 Ethernet • T1/E1/XDSL • PoE 전원공급장치
Cisco WS-C2960G-24 TC-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 트래픽 발생기	• 10/100/1000 Base-T, 1000 Base-X(SFP)지원
Cisco WS-C2960G-24 TC-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



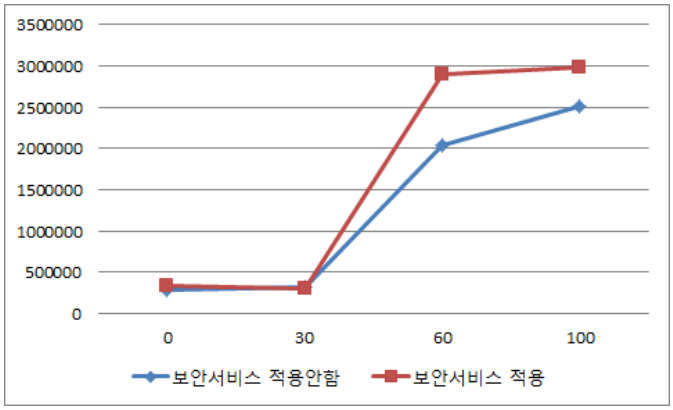
(그림 5) 발전소간 1:1 통신의 지연시간



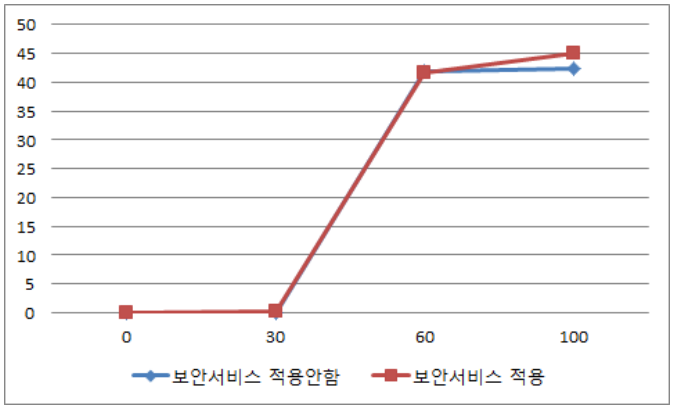
(그림 6) 발전소간 1:1 통신의 패킷 분실율

그림 7과 8은 수력발전소간 1:4 통신을 할 경우의 지연시간과 패킷 분실율을 측정한 결과이다. 보안서비스를 제

공하는 경우와 그렇지 않는 경우 모두 네트워크 부하가 30%이하일 경우에는 거의 영향을 받지 않음을 알 수 있다. 하지만 네트워크가 30~60%구간에서는 네트워크 부하에 민감하게 반응함을 알 수 있다. 이는 네트워크 부하가 어느 일정 한계를 넘으면, 1:N통신으로 인해서 각 클라이언트들의 통신들이 서로 영향을 끼친다고 분석된다. 그림 9는 수력발전소간 1:8 통신을 할 경우의 지연시간을 측정한 결과이다. 1:4경우와 마찬가지의 결과를 보였다. 또한 실험에서는 변전소간의 1:N통신에 대해서도 같은 결과를 보였다. 결론적으로 스마트 그리드에서의 보안서비스가 전체 네트워크에 끼치는 영향은 미미하며, 1:N통신의 경우 스마트 그리드 통신망에 영향을 미치는 주요 요소는 네트워크 부하임을 알 수 있다.



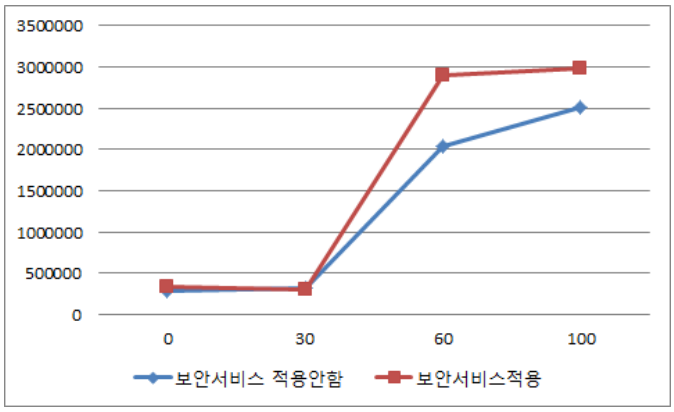
(그림 7) 수력발전소간 1:4 통신의 지연시간



(그림 8) 수력발전소간 1:4 통신의 패킷 분실율

4. 결론

스마트 그리드가 가능하기 위해서는 무엇보다도 보안이 보장되어야 함에도 불구하고, 아직까지는 스마트 그리드에 대한 관심에 비해 보안의 고려가 미흡한 상태이다. 아직 스마트 그리드가 실체적인 모습을 갖추는 초기단계이고, 스마트 그리드에서 사용될 기술들 또한 한창 논의·개발 중 임을 고려하면, 아직 스마트 그리드에서 요구되는 보안 요구사항을 논의하는 것은 시기상조일지 모르지만, 보안의 고려가 초기에부터 동반되지 않는다면, 차후 문제 상황이 발생하였을 때 피해의 복구가 어려울 수 있기 때문에 본 문서와 같은 보안의 논의가 스마트 그리드의 개발과 더불어 동반되어야 한다고 생각한다. 본 연구의 결과는 향후 다양한 스마트 그리드 보안 서비스 제공에 기여할 것으로 기대된다.



(그림 9) 수력발전소간 1:8 통신의 지연시간

참고문헌

[1] "한국형 스마트 그리드 비전", 지능형 전력망 로드맵 추진위원회

[2] 이경복, 유지연, 이숙연, 임종인, "스마트 그리드에서의 사용자 참여와 보안이슈", 정보보호학회지 19(4) 2009

[3] CISCO, "Securing the Smart Grid", 2009

APPENDIX

서버와 클라이언트 사이에 전송되는 패킷구조의 각 필드의 내용은 다음과 같다.

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