스마트그리드를 위한 통신서비스 품질과 보안 요구사항

이은동 | 권기풍 | 김성우 | 서승우
서울대학교

요 약

미국 국립표준원(NIST), 전기전자공학회(IEEE) 등의 주도로 진행중인 스마트그리드 프로젝트에서는 미래 전력시스템을 위한 통신망으로 인터넷 기반의 단일화된 통신망을 유력한 후보로 검토하고 있다. 인터넷기반의 전력통신망은 최선노력서비스(best-effort-service)를 기본으로 하기 때문에 종단간 지연을 보장할 수 없으며 패킷 손실이 발생할 수 있다. 따라서 기존 전력통신망이 보장해주던 높은 통신 품질과 보안성을 보장해주지 못한다. 본 논문에서는 현재 그리고 미래의 전력관련 통신 서비스가 인터넷 기반의 통합망에서 사용가능한지 검증하여 본다. 이를 위해 현재의 전력시스템에서 사용되는 통신 서비스들로부터 품질, 보안성 등의 요구조건을 도출하고 이를 바탕으로 스마트그리드 환경에서 추가 될 통신 서비스들이 미래 인터넷 기반 통합망에서 사용가능한지를 검증하여 본다. 마지막으로 현재 인터넷 기술로 만족하지 못한 요구조건을 수용하기 위한 해결방안을 제시한다.

I. 서 론

스마트그리드(Smart Grid)란 전력시스템에 진보된 통신 기술과 새로운 전력 기술을 적용하여 효율성, 안정성, 신뢰성을 극대화 하는 차세대 전력 인프라를 의미한다. 현재의 전력시스템은 대상과 목적에 따라 다양한 통신 기술을 사용하고 있다. 변전소간의 통신에는 IEC 61850[1]을 사용하고 있으며, 전력시스템의 제어를 위해 SCADA[2]시스템을, 그리고 업무지원용으로 전화망과 VoIP등을 사용하고 있다. 하지만 스마트그리드를 실현 하기 위한 요구조건들을 만족시키기 위해선 좀 더 지능화 되고 표준화된 통신망이 필요하다.

이를 위해 미국 NIST, IEEE 등 많은 스마트그리드 프로젝트 그룹들은 인텔리그리드[3]를 필두로 인터넷 구조 기반의 통합된 통신망을 고려하고 있다. 통합망을 가지게 되면, 실시간 정보 제공이 가능해, 빠른 의사 결정이 가능해져 신속히 대처할 수 있게 된다. 또한 모든 데이터를 단일방식으로 관리하므로 유지보수 비용을 줄일 수 있고, 확장 및 수정이 용의하여 좀더 효율적으로 운용할 수 있게 된다.

전력망에 사용되는 통신서비스는 전력시스템의 안정성에 직접적인 영향을 주기 때문에 엄격한 통신 품질이나 보안성을 필요로 한다. 하지만 TCP/IP나 UDP/IP를 사용하는 인터넷 기반 통합망은 전력시스템이 요구하는 높은 수준의 데이터 전송 신뢰성 및 종단간 지연을 보장하지 못하므로 특정 서비스는 사용이 불가능하다.

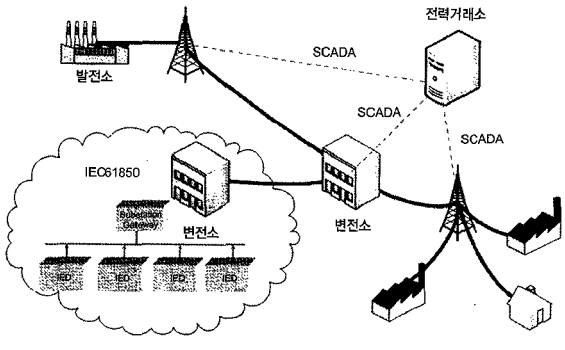
본 논문에서는 현재 그리고 미래의 전력관련 통신 서비스가 TCP/IP기반 인터넷 통합망에서 사용가능한지 검증하여 본다. 먼저 현재 전력망에서 사용되는 통신 서비스의 특성을 파악하고, 품질, 보안 요구사항을 도출한다. 이 요구사항을 바탕으로 스마트그리드 환경에서 전력관련 통신 서비스가 인터넷 기반의 통합망에서 사용가능한지 검증하여 보고, 만족하지 못한 요구조건들에 대해서 해법을 제시한다.

본 논문은 총 6개의 장으로 이루어져 있다. 제 2장에선 기존 전력시스템에서 사용되는 통신서비스에 대해서 알아본

다. 제 3장에서는 기존 시스템에서 전송되는 서비스들을 통신품질, 보안성의 기준에 따라 분류 한다. 제 4장에서는 스마트그리드 환경에서 새롭게 만들어질 통신 서비스들을 예측해보고, 제3장에서 사용하였던 기준에 따라 분류 한다. 제 5장에서는 제 4장에서 나눈 기준에 따라 현재 인터넷 기반 시스템에서 수용하지 못한 요구조건들에 대한 해결책을 제시한다. 마지막으로 제 6장에서 본 논문의 결론을 맺는다.

II. 기존 전력용 통신 시스템

현재의 변전소 내 설비는 SCADA(Supervisory Control and Data Acquisition) 시스템을 필두로 많은 부분 자동화, 무인화 되어 있다. 하지만 대부분의 전력용 통신 시스템은 기존 기능을 디지털화하면서 비 표준 통신 기술을 통해 자동화 작업을 해왔었다. 그리하여 변전소마다 사용하는 통신 규격이 모두 달라서 상호 호환시 어려움이 많았는데 이를 해결하기 위해, 국제표준규격 IEC61850을 제정하였다. 본 장에선 현재 전력용 통신 시스템을 대표하는 SCADA와 IEC61850에 대해서 간략히 살펴본다.



(그림 1) 현재의 전력통신망

SCADA는 필드 장비들로부터 각종 필요한 정보를 수집하기 위한 시스템이며, 주로 시간 지연에 민감한 데이터를 취급한다. SCADA는 매 2-4초마다 정기적으로 필드 장비들로부터 전력, 전압, 전류, 온도 등의 필요한 데이터를 수집하는데, 이러한 데이터는 상태 추정, 자동발전제어 등 빠른 시간 안에 연산을 처리하여 결과를 출력해야 하는 여러 응용들에 이용되므로 보통 약 500 ms 이내에 전달되어야 한다.

〈표 1〉 현재의 주요 통신서비스

네트워크	서비스	반응시간
SCADA	Emergency event notification	6ms이하
	Routine transactions	540ms이하
	Routine HMI status polling from substation field device	매2초
IEC 61850	Fast speed message	10ms이하
	Medium speed message	10ms~500ms
	Low speed message	500ms이상

SCADA 시스템은 약 6 ms 이내에 전달되어야 하는 긴급 메시지를 취급하기도 한다. SCADA 데이터는 전력 네트워크 토폴로지나 전력 네트워크 상황을 나타내는데, 이러한 정보는 보통 전력회사들이 경쟁 전력회사 등에 공개하기를 꺼려하는 데이터이므로 높은 수준의 기밀성이 보장되어야 한다. 또한 상태추정과 자동발전제어와 같은 응용들은 항상 정확한 데이터를 필요로 하므로 높은 수준의 무결성과 가용성 또한 보장되어야 한다.

변전소간 통신을 위한IEC 61850은 고지능화 및 스마트화 요구에 따라 모든 데이터 및 정보에 대한 통일된 접근 방식을 만드는 국제 표준이다. IEC 61850에서 주고받는 메시지는 시간제한에 따라 크게 3가지로 나누고 있다. 샘플링 데이터나 GOOSE[1]처럼 변전소 내에서 중요도가 높고 실시간 처리가 요구되는 고속 메시지는 10 ms 안에 전송이 되어야 한다. 중간 속도 메시지는 100 ms 이내에 전달이 되어야 하는 메시지들로서 상태표시 메시지, 단일 측정값을 포함한다. 마지막으로 저속 메시지는 500 ms 이상의 지연을 허용하는 메시지로서 일반적으로 파일 등을 전달 하는데 사용되거나 이벤트 기록을 전달하는데 사용이 된다.

III. 전력용 통신시스템 요구조건

제2장에서는 현재의 전력용 통신시스템들에 대해 간단히 알아 보았다. 이 통신시스템들은 목적에 따라 여러 가지 제

한요소들을 가지고 있다. 제3장에서는 이들 제한요소를 나누는 기준을 알아보고 이 기준에 따라 제한요소들을 나누어 본다. 제한요소는 크게 통신 품질과 보안성으로 분류 할 수 있으며, 통신품질은 대역폭보장, 실시간성으로, 보안성은 기밀성, 무결성, 가용성으로 분류할 수 있다. 전력관련 메시지는 제어메시지, 측정 메시지 등 크기가 적은 메시지가 대부분을 차지하므로, 대역폭관련 요구조건은 다루지 않는다.

3.1. 통신 품질 – 실시간성

전력 시스템에서 사용되는 통신 시스템의 상당수는 지연에 매우 민감하다. 전체 전력계통의 안정성에 큰 영향을 미치는 정보나 사고에 의한 긴급상황 대처에 필요한 서비스의 경우 통신메시지가 최대한 빠른 시간에 도착을 해야만 오동작에 의한 피해를 줄일 수 있다. 반면 단순 파일 전송이나 원거리 전력검침 등과 같은 경우엔 1초 정도의 전송 지연이 발생하여도 아무런 문제가 되지 않는다.

본 논문에서는 IEC 61850에서 사용하고 있는 시간제한에 따른 메시지 분류 기준에 따라 아래의3가지로 실시간성에 관련된 요구조건을 나누었다.

빠른 메시지 : 10ms이하
보통 메시지 : 10ms ~ 500ms
느린 메시지 : 500ms이상

〈표 2〉 기존의 전력용 통신시스템 분석

네트워크	메 시 지	요 구 조 건			
		통신품질	보 안 성		
		실시간성	무결성	기밀성	가용성
IEC 61850	시간동기	H	L	L	L
	파일전송메시지	L	M	H	M
	이벤트기록 전송 메시지	M	H	M	H
	보호기능 관련메시지	H	H	H	H
SCADA	측정된 데이터	H	M	L	M
	긴급메시지	H	H	H	H

TCP/IP 전송 프로토콜의 경우엔 처음 세션을 맺을 때 3-way handshake를 필요로 한다. 그로 인해 다른 프로토콜보다 전송과정에서 좀 더 많은 시간이 걸리며, 빠른 메시지와 보통 메시지의 경우에는 현재 인터넷 시스템에서의 TCP/IP로는 전송이 불가능할 수도 있다. 그러므로 실시간성은 전송 프로토콜을 설정하는데 중요한 변수라고 할 수 있다.

3.2. 보안성 – 무결성

무결성은 네트워크에서 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 도달했음을 확인하는 것이다.

무결성은 데이터를 주고받을 때 뿐만 아니라 저장된 데이터에 대한 무결성도 포함 한다. 인터넷 망과 같은 공개망을 사용하여 메시지를 전송하는 경우는 사설망을 사용하는 경우보다 외부 공격자의 침입이 용이하여 무결성이 낮다고 볼 수 있다.

본 논문에서는 높음, 보통, 낮음의 3가지 등급으로 무결성의 등급을 나누었으며, 높은 등급의 무결성을 요구하는 데이터는 무결성의 손실로 인한 변화가 전체 계통에 큰 영향을 야기 할 수 있는 경우, 낮은 등급의 무결성을 요구하는 경우는 시간동기와 같이 수신자가 이전의 데이터가 있을 경우 어느 정도는 자체적으로 데이터의 변화 유무를 감지할 수 있는 메시지, 보통 등급의 경우엔 그 중간 정도의 수준을 가지는 경우를 의미한다. 인터넷에서는 PKI기반 전자서명, SHA-1, MD5, HMAC등 무결성 보장을 위한 다양한 표준이 있으며, 기본 기술들이 충분히 가능한 상황이다.

3.3. 보안성 – 기밀성

기밀성은 네트워크에서 데이터 및 메시지의 전송과정이나 처리과정에 있어서 정보가 인가 되지 않은 개인에 누설되거나 공개되지 않아야 함을 의미하는 속성이다. 기밀성이 낮게 되면 크게는 전기의 배전 과정이나 발전소의 동작과정 등에 침입자가 발생하여 전력계통의 안정성에 큰 영향을 줄 수도 있고 작게는 개인의 전력사용패턴 유출로 인해 프라이버시의 침해를 일으킬 수도 있다.

본 논문에서는 높음, 보통, 낮음의 3가지 기준으로 기밀성의 등급을 나누었으며 기밀성을 결정짓는 기준은 정보의 변화나 유출이 계통이나 주체에게 얼마나 큰 피해를 줄 수 있는 가에 따라 판단 하였다.

높은 기밀성 : 외부인에게 절대 공개되어서는 안 되는 메시지 중 계통의 동작에 큰 영향을 줄 수 있는 메시지
보통 기밀성 : 외부인에게 공개되어서는 안되나 계통의 동작엔 영향을 주지 않는 메시지
낮은 기밀성 : 일반인에게 공개되어도 아무런 문제가 없는 메시지

시간동기나 전기 가격과 같은 메시지의 경우엔 외부인에게 공개 되어도 문제가 없으므로 낮은 기밀성 등급을 가지지만, 전체 전력을 총괄하는 기관에서 나오는 동작 명령 메시지나 개인회사들의 발전 용량 분배 관련 입찰메시지 등은 노출이 될 경우 특정 개인이나 단체에 큰 피해를 줄 수 있다. 그러므로 이러한 메시지들은 높은 기밀성 등급을 가지며, 시간이 좀 걸리는 단점이 존재하더라도 외부의 침입에 영향을 받지 않는 안전한 방법을 사용해서 전송이 되어야만 한다. 현재 인터넷 망에서는 AES-128bit, DSA와 같은 기밀성을 높이기 위한 암호화 알고리즘들이 사용되고 있다.

〈표 3〉 스마트그리드에서 추가될 통신서비스의 예

메 시 지	요 구 조 건			
	통신품질	보 안 성		
	실시간성	무 결 성	기 밀 성	가 용 성
부하제어메시지	M	H	H	H
분산 전원 및 전기 저장장치 제어 메시지	M	H	H	H
고객 측 전력품질 감시 메시지	H	H	H	H
고객과의 계약 정보 메시지	L-M	M	M	M
에너지 관리 관련 메시지	M	M-H	M	M
제어센터 간 업무용 메시지	L-M	H	M-H	L-M

3.4. 보안성 – 가용성

가용성이란 권한을 가진 사용자가 시스템으로부터 특정 정보를 필요로 할 때, 항상 접근하여 사용할 수 있음을 나타내는 속성이다. 가용성이 높아야 하는 데이터는 각 시스템의 상태 체크 메시지, 배전소간의 상태 변화메시지 등이 있다. 본 논문에서는 높음, 보통, 낮음의 3가지 기준으로 가용성을 나누었으며 그 기준은 다음과 같다.

높은 가용성 : 99.99%이상의 가용성
보통 가용성 : 99%이상의 가용성
낮은 가용성 : 90%이상의 가용성

가용성을 결정짓는 기준은 정보에 대한 접근 주기와 정보를 얻을 수 있는 확률에 따라 판단 할 수 있다. 최선노력서비스를 기본으로 하는 인터넷 구조 기반의 통신 네트워크는 종단간 지연을 보장할 수 없으며, UDP/IP의 경우엔 패킷 손실도 발생 할 수 있으므로 가용성을 완벽하게 만족시킬 수 없다.

IV. 새로운 통신서비스

제 2장, 제 3장에서는 현재의 전력시스템에서 사용되고 있는 통신서비스들의 요구사항을 통신품질과 보안성에 따라 분류를 하였다. 본 장에서는 스마트그리드 환경에서 새롭게 등장할 통신 서비스들을 예측해보고, 서비스 구현에 고려해야 할 요구사항에 따라 나누어 본다.

〈표 3〉은 스마트그리드 구축과 함께 새롭게 나타날 것으로 예상되는 응용 및 통신 서비스와 품질 및 보안 요구사항을 나타낸다. 〈표 3〉에 나타나는 통신서비스들은 인텔리그리드 Use Cases[3]를 바탕으로 도출된 것으로서, 주로 고객 측과의 통신을 위한 것이다. '부하제어 메시지'는 피크 수요의 감소를 위해 고객의 부하를 직접 제어하기 위한 메시지로서 보통은 수 초 내에 전달되면 되지만 긴급하게 큰 부하를 절제하여야 할 경우에는 1초 이내에 전달되어야 한다. '분산전원 및 전기저장장치 제어를 위한 메시지'는 안정적이고 고품질의 전력을 공급하기 위해 분산전원과 전기저장장치의 on-off 및 출력을 제어하기 위한 메시지로서 1초 이내에 전달되어야 한다. '고객 측 전력 품질 감시 메시지'는 고객 측에서 발생하는 주파수 및 전압변화나 사고 발생을 감시하기 위한 메시지로서 품질 변화와 사고에 대한 빠른 대응을 위해 수백 ms 이내에 전달되어야 한다. 이 세 가지 메시지는 제어 및 감시 정보를 담고 있기 때문에 높은 수준의 기밀성, 무결성 및 가용성이 보장되어야 한다.

'고객과의 계약 정보 메시지'는 고객이 소유한 부하제어,

분산발전원 제어 등의 응용을 원활히 운영하기 위해 주고받아야 하는 메시지로서, 고객의 실시간 전력 사용 패턴 전송, 고객과의 분산발전원 입찰 및 낙찰 정보 교환, 부하제어를 위한 사전 계약 정보 등을 포함한다. 정보의 종류에 따라 전달 시간이 중요하지 않은 메시지도 있겠지만 보통 수초 내에 메시지가 전송되어야 할 것이다. '고객과의 계약 정보 메시지'는 보통 프라이버시 및 금전적 이해와 관련이 되기 때문에 기밀성과 무결성이 요구되나 제어 및 감시신호에 비해 낮은 가용성이 요구된다. '에너지 관리 관련 메시지'는 고객의 에너지 사용을 최적화하기 위해 에너지 서비스 공급자가 고객의 전기 기기의 상태 정보를 취득하거나 전기 기기의 출력 패턴을 조정하기 위한 메시지로서 고객과 에너지 서비스 공급자 간에 수 초 내에 전달되어야 하며, 서비스 제공을 위한 메시지와 같은 이유로 중간 수준의 기밀성과 무결성, 그리고 낮은 가용성이 요구된다.

'제어센터 간 업무용 메시지'는 전력 제어 센터 간에 업무에 필요한 정보를 주고받기 위한 메시지이다. 업무지시, 보고서 등의 문서 뿐 아니라 설계도면과 같은 그림 파일을 전송할 수 있으므로 다른 메시지에 비해 큰 데이터 용량을 가진다. 높은 수준의 기밀성과 무결성이 보장되어야 하나 시간조건이나 가용성에 크게 구애 받지 않는다.

V. 요구사항 수용을 위한 방안

제 2장부터 제 4장까지 스마트그리드의 통신 네트워크를 통해 전송될 메시지와 각 메시지들의 통신 및 보안 요구사항을 도출하였다. 상당수의 메시지들은 요구사항을 만족하지 않을 경우 전송 도중 누락되거나 느리게 전송됨으로 인해 전력 시스템에 치명적인 악영향을 미칠 수 있다. 그러나 최선노력서비스를 기본으로 하는 인터넷 구조 기반의 통신 네트워크로는 통신 및 보안 요구사항을 완벽하게 만족시킬 수 없다. 최선노력서비스는 근본적으로 데이터 전송의 신뢰성 및 종단간 지연을 완벽하게 보장하지 못하기 때문에 실시간성에서 낮은 품질을 제공하게 된다. 그러므로 높은 수준의 실시간성을 필요로 하는 〈표 2〉의 '보호기능 관련 메시지', '긴급 메시지', 〈표 3〉의 '부하제어 메시지', '고객측 전력품질 감시 메시지'의 경우엔 현재 인터넷 기반의 통신망을 사용할 수 없다. 따라서 이러한 메시지들의 통신서비스품질을 보장하기 위해서는 종단간 지연을 보장하기 위한 별도의 기술이 뒷받침 되어야 한다.

90년대 말에 제안된 MPLS (Multi-protocol Label Switching)는 네트워크 레벨에서 대역폭 예약을 사용하는 접근 방식을 취한다. MPLS는 라우터가 특정 트래픽에 대해 별도의 대역폭을 할당할 수 있도록 함으로써 종단간 지연을 보장한다. 비교적 최근에 광대역 감시제어 시스템을 타깃으로 개발된 Astrolabe [4], GridStat [5]는 미들웨어 기반의 트래픽 엔지니어링 방식으로서 네트워크 내의 미들웨어를 탑재한 노드들이 자신의 트래픽을 조정함으로써 네트워크의 혼잡을 제어하는 접근 방식을 취한다. 미들웨어 방식은 MPLS와는 다르게 전통적인 라우터를 변경 없이 사용할 수 있고, 이상적으로는 총 네트워크 트래픽이 총 네트워크 용량보다 항상 작도록 보장 한다는 장점이 있지만, 네트워크 내의 모든 노드들이 미들웨어를 탑재하여야만 항상 100 퍼센트의 종단간 지연을 보장할 수 있다.

보안성을 강화하기 위한 연구도 진행되고 있다. PMI (Privilege Management Infrastructure)[6]는 단순히 인증서 소유자의 신원 확인에만 중점을 두고 있는 PKI(Public Key Infrastructure)의 단점을 보안하기 위해 제안된 새로운 정보보호 인프라 체계로서, 인증서 발급개체가 권한 소유자에게 권한의 일부나 전부에 대한 인증서를 발급하여 특정 시스템에 접근할 수 있는 권한을 차등 부여함으로써 보안을 책임지는 기반구조다. 그로 인해 중앙 집중적 권한 관리, 복잡한 권한 체계를 시스템화 하는 장점이 존재한다. PMI는 전력회사들이 사용자 별 다른 서비스를 제공하는 미래 인터넷 구조의 통합된 망에서 적합한 정보보호 인프라이다.

앞서 소개한 기술들은 인터넷 구조 기반 네트워크에서 지연에 민감한 메시지들의 종단간 통신품질을 보장하거나 보안성을 강화 하여 준다. 그러나 이러한 기술로도 10ms 이내의 고속 메시지 전송과 높은 보안성을 요구하는 메시지를 전송하기는 어려울 것으로 보인다. 따라서 이러한 메시지는 분리된 전용망을 사용하여 전송하는 것이 좋을 것으로 보인다.

VI. 결 론

지금까지 전력시스템에서 사용되고 있는 통신시스템들의 종류를 살펴보고 각각에 대한 제한요소들에 대해서 알아 보았다. 이것을 이용하여 스마트그리드로 발전하는 과정에서 새롭게 생겨날 부하제어나, 분산전원 관련 통신 서비스들을 분류를 하였으며, 현재 인터넷 구조 기반의 환경에서 사용 가능한 서비스와 현재 시스템에서 사용이 불가능한 서비스들을 구분하였다.

전력통신망이 가지는 높은 제한조건에 의해서 기존 데이터통신용 인터넷 기반 구조에 바로 적용이 불가능한 서비스들은 분리된 전용망을 사용하여 해결할 수도 있다. 하지만, 대역폭 예약을 통해 종단간 지연을 보장해주는 MPLS방식, 미들웨어 기반의 품질을 향상시키는 Astrolabe와 GridStat, 보안성을 높이는 PMI와 같은 많은 보완 연구들을 통하여 인터넷 기반의 통합망에서도 적용이 가능해질 것으로 보인다.

참 고 문 헌

[1] International standard IEC 61850-5, Communica-tion Networks and Systems in Substations - Part5 : Communication Requirements for Functions and Device Models 2003.

[2] "Supervisory control and data acquisition (SCADA) systems," National Communications System, Technical Information Bulletin 04-1, Oct. 2004. [Online]. Available : http://www.ncs.gov/librar-y/tech bulletins/2004/tib 04-1.pdf.

[3] EPRI, "The Integrated Energy and Communication Systems Architecture - Volume 2. Power System Functional Requirements - Appendix D. Use Cases", IntelliGrid Architecture Published Results- www.intelligrid.info,

[4] K. P. Birman, J. Chen, K. M. Hopkinson, R. J. Thomas, J. S. Thorp, R. Van Renesse, and W. Vogels, "Overcoming communications challenges in software for monitoring and controlling power systems," Proc. IEEE, vol. 93, no.5, pp. 1028-1041, May 2005.

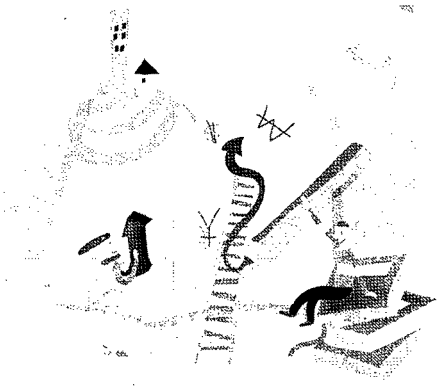
[5] I. Dionysiou, K. H. Gjermundrod, and D. Bakken, "Fault tolerant issue in publish-subscribe status dissemination middleware for the electric power grid," presented at the IEEE Supplement of the 2002 International Conference on Dependable Systems and Networks (DSN), Washington, DC, 2002.

[6] Nian Liu, Bin Duan, Jian Wang and Shenglong Huand, "Study on PMI based access control of substation automation system", IEEE Power Engineering Society General 2006

[7] Kenneth Hopkinson, Gregory Roberts Xiaoru Wang, and James Thorp, "Quality-of-Service considerations in utility communication networks" IEEE Transactions on power delivery, vol. 24, no.3, July 2009

[8] Gregory M. Coates, Kenneth M. Hopkinson, Scott R. Graham, and Stuart H kurkowski, "Collaborative, Trust-based security mechanisms for a regional utility intranet" IEEE Transactions on power systems, vol. 23, no.3, August 2008

[9] Davies R. W. "The Data Encryption standard in perspective," Computer Security and the Data Encryption Standard, pp. 129-132. (http://www.nist.gov/aes).



약 력

2007년 한국과학기술원 학사
2009년 서울대학교 석사
2009년 ~ 현재 서울대학교 박사과정
관심분야 : 정보 보안, 데이터 통신, 스마트그리드

이 은 동

2009년 성균관대학교 학사
2009년 ~ 현재 서울대학교 석사과정
관심분야 : 정보 보안, 데이터 통신, 스마트그리드

권 기 풍

2005년 고려대학교 학사
2007년 고려대학교 석사
2007년 ~ 현재 서울대학교 박사과정
관심분야 : 정보 보안, 제어 통신망, 지능형 자동차

김 성 우

1987년 서울대학교 학사
1989년 서울대학교 석사
1993년 펜실베니아 주립대학 박사
1996년 ~ 현재 서울대학교 교수
관심분야 : 정보 보안, 유/무선 네트워크, 전기자동차, 스마트그리드

서 승 우