2009년도 대한전기학회 하계학술대회 논문집 2009. 7. 14 - 17

무인원격발전소 원격제어시스템 유비쿼터스 기술적용 방안

안병우, **남궁붕**, 가필순, 고영환

한국수자원공사

The application of Ubiquitous Technology To The Remote Control System for Unmanned Power Plant

Byung-Woo Ahn, Bung Nam-kung, Pil-Sun Ka, Young-Hwan Go

Korea Water Resources Corporation

(Abstract)

This paper aims to analyze characteristics of Network administration and its security and study a method of applying new Ubiquitous technology which can raise up the stability and efficiency of remote control systems in unmanned power plants so that the states of systems are recognized by unrestricted and diverse access in the ubiquitous circumstance and services wanted are supplied for anyone to access to them anytime and anywhere.

1. 서 론

발전통합운영시스템은 대전에 소재한 통합운영센터에서 전국에 산재한 댐의 발·변전 및 수문설비를 첨단 IT기술을 이용하여 발전기 기동, 정지, 출력조정 및 수문개폐 등을 원격감시제어 할 수 있도록 구축된 발전통합운영시스템이다. 현재 발전통합운영 네트워크 시스템은 이중화로 신뢰성이 높지만 기존 시스템의 기능이 보강되거나 신규 기능을 추가하면 트래픽 증가로 전용선 통신비 부담이 가중될 수 있다. 이러한 단점을 보완하기 위하여 유비쿼터스 기술를 적용하여 Metro Ethernet 형태의 네트워크 구축방안과 VPN 가상사설망을 예비전송로로 구축하는 방안에 대하여 기술적으로 검토하고자 한다.

또한, 망의 효율적 감시나 네트워크 보안설비에 대한 분석을 통하여 운영자 인증시스템, IPSec 등의 프로토콜을 이용하여 제어데이터 인증 및 암호화 등의 기능적용 가능성에 대한 기술적 검토와 네트워크 보안 측면에서 각 스위치 포트에 접근할 때 인증절차를 거치도록 IEEE 802.1x 보안을 추가하는 방안에 대하여 검토한다.

2. 본 론

2.1 발전통합운영시스템 네트워크 구성

통합운영센터 LAN과 단위발전소 LAN간의 네트워크는 TDM 방식의 512kbps 전송대역폭과 384kbps 전송대역폭을 가진 두 개의 회선으로 구성되어 있으며, WAN 구성도는 그림 1과 같다. 두 개의 전용선과 각 전용선에 연결된 라우터, 디지털 전송부호화장치, 화상처리용 Video Codec 장비로 구성되어 있으며 운영형태는 주 전송로가 정상인 경우에는 Dacom 전송로(주전송로)를 통하여 SCADA 트래픽을 전송하고 ATM망(예비전송로)를 이용하여 CCTV 트래픽을 전송하고 있다가 주 전송로에 이상이 발생하게 되면 전용선 S/W가 자동절체 되어 CCTV용 트래픽은 차단되고 SCADA 트래픽이 ATM망을 통하여 처리되어 발전통합운영시스템 운영에는 전혀 영향을 미치지 않도록 구성되어 있다.

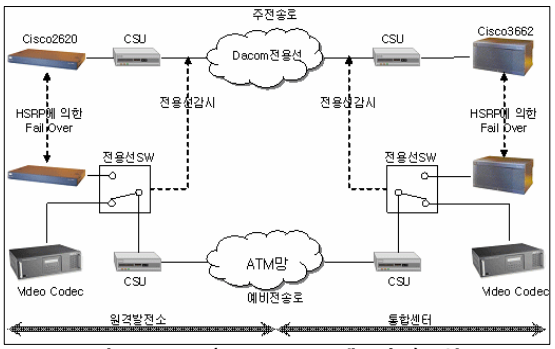

그림 1. WAN(Wide Area 네트워크)구성도

2.1.1 통합센터 및 원격발전소 Router에 HSRP 구현

CISCO에서 지원하는 HSRP은 표준 프로토콜인 VRRP의 기능을 확장하여 개발된 프로토콜로, 안정적인 통신망을 구축하기 위하여 라우터 2대로 Active 라우터가 다운 시 Stand-by 라우터가 Active 상태로 전환되면서 트래픽을 라우팅 하여 주는 백업구성 방식이다.

2.1.2 CDMA Backup 무선통신

원격발전소 PLC제어경로는 그림2와 같이 세 가지 경로로 구성되어 있다. 통합운영센터의 SCADA 서버, 원격발전소의 SCADA 서버, 그리고 기존 SCADA 네트워크 감시제어 기능과 독립적으로 무선망을 이용하여 직접 PLC를 감시·제어하는 체계로 구축되어 있다.

두 전용회선인 DACOM 망과 ATM 망의 장애, 통합운영센터내 SCADA 서버 및 LAN 장애, 그리고 단위감시제어시스템의 SCADA 서버 장애, 즉 네트워크와 SCADA 시스템의 극단적인 경우에 CDMA 망을 통해 그림 2의 ③과 같이 WAN 구간의 백업라인을 확보할 수 있다.

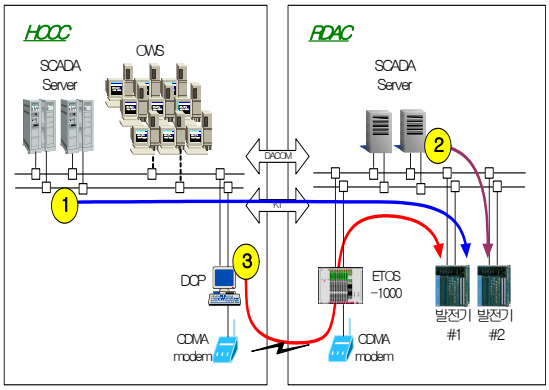

그림 2. 원격발전소 감시·제어경로 구성도

2.2 유비쿼터스 기반의 시스템 구축 방안

2.2.1 유비쿼터스 환경의 네트워크 기술

2.2.1.1 Metro Ethernet 적용

네트워크의 병목 해소 및 고품질의 서비스 제공을 위하여 LAN 영역에서 사용하던 Ethernet 기술을 Metro 영역으로 확장하여 경제적인 시스템을 구축하는 것으로 Metro Ethernet 망을 적용한다. 이 통신망의 장점은 저비용의 데이터 전송과 통계적 다중화를 통한 효율적인 대역폭 이용으로 구축 및 운영 비용절감의 효과가 있고, TDM 기반의 전송에 비해 Mbps 당 1/6 ~ 1/15로 저렴하게 구현 가능하며 서비스 요구에 따라 대역폭 확장이 유리하다.

Metro Ethernet는 Site-to-Site Connectivity 서비스로써 둘 이상의 기업 사이트 간(본사와 현장 관리단 등)에서 원격 데이터베이스 액세스, 실시간 파일전송 및 자료 공유 등과 같은 다양한 형태의 데이터 응용을 전달해주는 Transport medium을 제공하는 것으로 Private 데이터 Transport 와 Transparent LAN Service로 나뉠 수 있다.

Metro-Ethernet Private Line 서비스는 단순한 이더넷 인터페이스를 통해 전용의 대역폭을 제공할 뿐만 아니라 네트워크 availability, round trip delay 및 packet loss와 같은 성능 관련 SLA(Service Level Agreement)를 제공할 수 있다. 또한 공유의 망 자원을 통한 LAN-to-LAN Metro-Ethernet 연결을 Ethernet transparent LAN 서비스를 통해 제공할 수 있다. 이 서비스는 802.1q VLAN tagging을 사용하여 제공가능하다.

2.2.1.2 VPN을 통한 백업 네트워크

VPN을 통한 가상 사설망을 구성하여 통신비 절감에 의한 원가절감을 도모한다. 가상 사설망을 구성할 때 고려되어야 할 가장 중요한 사항은 보안과 QoS 보장사항이다. 즉, 공중망을 사용하여 사설망 사용자간 연결을 하여야 하기 때문에 전용선에 비해 보안성이 떨어지게 되는데 이를 해결하기 위해서 전송되는 패킷에 대한 인증, 암호화 및 무결성에 대한 지원이 강화되어야 한다. 또한 전송되는 패킷의 전송 품질, 트래픽의 제어 및 효율적인 패킷 전달이 지원되어야 공중망을 지나가는 다른 트래픽에 의한 손실, 지연 등을 방지할 수 있다.

KT-VPN은 보안 및 성능(대역폭 및 가용성 등) 보장을 통한 SLA 제도를 시행하여 품질 성능의 범위와 조건을 협상할 수 있으며 네트워크 환경에 따라 약간 다르겠지만 전용선 사용의 경우에 비해 약 30% 정도의 비용 절감을 가져올 수 있다. 기본적인 서비스 망 구조는 그림 3와 같다.

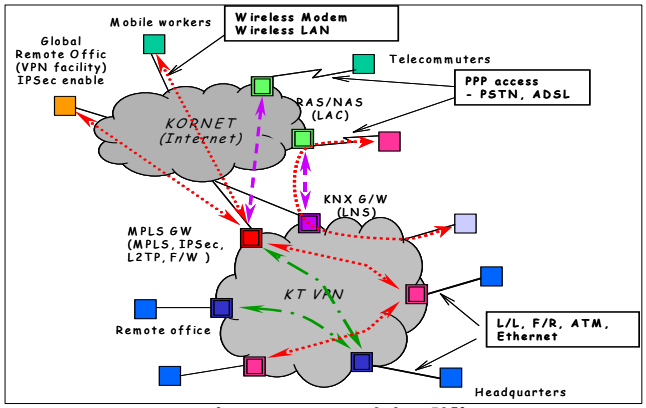

그림 3. KT VPN 서비스 현황

2.2.1.3 무선 PDA 개발 및 원격제어

발전통합운영시스템에서 사용하고 있는 유선 네트워크의 백업 기능을 가지고 있는 CDMA는 통합운영시스템 프로그램을 탑재한 무선 PDA를 개발하여 통합운영센터 ↔ 단위감시제어센터 간 통신을 수행할 수 있을 것이며, 무선 PDA에 CDMA 모뎀뿐만 아니라 blue-tooth 혹은 wireless LAN 모듈을 dual 로 설치하여 제어실 내에서 업무를 수행하게 된다.

원격지에 있는 사람에게는 휴대폰으로 주요 알람 정보에 대한 SMS 서비스가 제공되고, 제어실 반경 수십미터내에 있는 관리자들은 자유롭게 이동하면서 필요한 정보를 받아보고 필요한 경우 인증을 거쳐 통합운영센터 서버와 연결된 후 단위감시제어센터의 발전 및 수문설비 제어를 수행할 수도 있게 된다. 즉, 통합운영센터나 단위감시제어센터의 SCADA 서버에 Blue-tooth chip을 추가해 반경 10m 근처에서 PDA를 통해 통신을 하거나 Wireless AP를 Hub에 설치하고 PDA를 통해 서버와 통신하는 형태가 될 것이다. 무선 구간에서의 보안 기능을 위해서 무선 LAN의 경우 802.1x에 따른 보안 기능이 구현되어야 하며 Blue-tooth 경우도 IPsec 에서 제공하는 보안 기능이 구현되어야 한다.

2.2.2 네트워크 보안 강화

2.2.2.1 네트워크 LAN의 IEEE 802.1x 인증기능 보강

발전통합운영시스템의 네트워크는 라우터와 스위치들이 이중화되어 망을 구성하고 있다. 각 발전소에 설치되어 있는 스위치 허브의 포트 중 일부가 네트워크를 구성하고 있으며, 여러 개의 포트는 사용되지 않고 있다. 만일 외부에서 침입한 사람이 이러한 스위치허브에 남아 있는 포트를 통하여 네트워크에 불법 침입할 수 있는 여지를 가지고 있다. 따라서 스위치 포트를 통한 이런 불법적인 네트워크 사용을 방지하기 위해서는 IEEE 802.1x 에서 정의한 LAN의 인증 기능을 이용하여 스위치 포트의 불법적인 접근을 막는 기능을 추가하는 것이 바람직하다.

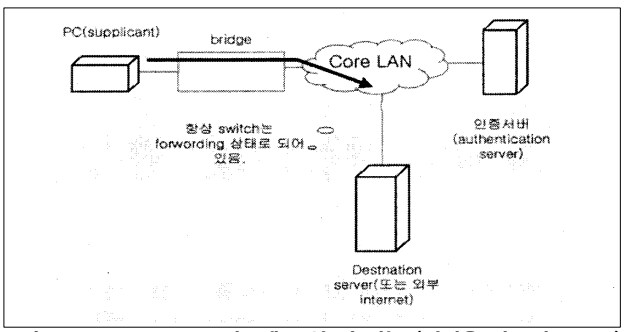

그림 4. IEEE 802.1x 시스템 구성 및 기능 (정진욱 외 1인, 2003)

브리지에 IEEE 802.1x의 포트레벨 보안기술 인증 절차를 수행하도록 한 경우에는 개별적인 과금 정책이나 사용 제한, 대역 할당 등을 사용자 개인별로 제어할 수 있는 장점이 있다. 결국 그림 4에서 보이는 바와 IEEE 802.1x 의 목표는 최종단 망 시스템인 브리지/스위치 또는 무선 액세스 포인트에서 인증을 수행한 다음에, 사용자 단말들이 망에 접근할 수 있도록 하는 것이다.

2.2.2.2 네트워크에서의 차별화 서비스 구현

발전통합운영시스템 네트워크에서 채택한 Cisco 3662 라우터나 2621 라우터에서도 IOS가 차별화 서비스를 지원하므로 configuration 작업을 통해 비교적 쉽게 구현할 수 있다. 이러한 라우터의 차별화 서비스 기능을 이용하면 발전통합운영시스템에서 전송되는 데이터의 중요도에 따라 우선순위 제어를 실시하여 중요한 데이터를 더욱 적은 지연시간과 적은 손실률을 가지도록 제어할 수 있으므로 더욱 적절한 감시제어를 할 수 있을 것이다.

2.2.2.3 방화벽을 이용한 침입방지

현재 발전통합운영시스템 방화벽에서 수행하는 기능은 단순히 ACL 설정을 통한 IP filtering 기능만 제공하고 있고 응용 계층의 방화벽 기능이나 port 번호에 따른 방화벽 기능이 부족하고 전용선 사설망에도 어떠한 인증 및 암호화 기능도 제공되고 있지 않기 때문에 보안 기능도 동작하지 않게 되어 국가 주요시설에 대한 보안성이 부족한 것으로 판단된다. 발전통합운영시스템이 발전 및 수력설비 감시제어의 중앙 집중화 및 현장 무인화와 같은 목적으로 구축되는 것이고 댐이 국가 기반시설로 차지하고 있는 중요성을 고려할 때 정보 보호를 위한 시스템 및 네트워크 보안기술인 침입탐지시스템을 반드시 구축되어야 한다. 침입탐지시스템이란 외부와 내부의 불법적인 침입을 탐지하고 대응하는 보안 메커니즘으로 분산되어 있는 노드에 침입탐지 에이전트를 설치하고 호스트나 네트워크에서 실시간으로 침입을 탐지한 후에 관리자 컴포넌트에 보고와 대응에 관한 탐지정보를 효과적으로 분배하는 통신 메커니즘이다. 침입탐지시스템과 firewall가 상호 보완하면 암호화 알고리즘이 함께 구현하여 튼튼한 보안기능을 제공할 수 있다.

또한 통합운영센터와 단위감시제어센터 간 데이터를 암호화하고 사용자 인증을 위한 보안기능으로 현재 VPN을 구성하는 라우터에 적용 가능한 가장 대표적인 인증 및 암호화 기법인 IPSec을 적용하여 라우터들과의 초기 약속한 보안키로 서로를 인증하고 전송하는 데이터마다 암호화를 수행하게 되어 임의의 가입자가 발전통합운영시스템 망에 접속하여 어떠한 명령 및 데이트 취득이 불가능하게 되어 한층 더 안전한 보완을 유지할 수 있다.

3. 결 론

본 연구를 통하여 발전통합운영시스템이 유비쿼터스 환경에 적합할 수 있도록

- Metro Ethernet 형태의 네트워크 구축과 VPN 가상 사설망의 구축
- 네트워크 보안을 위한 IEEE 802.1x 추가와 프로토콜을 이용한 인증, 암호화 기능추가
- CDMA backup 망 진화방안, 무선 네트워크와 PDA를 통한 제어
- 방화벽을 이용한 보안강화

등의 시스템 개선을 제안한다. 네트워크 개선을 통한 예산절감, 시스템 접근성의 극대화 및 철저한 보완시스템은 발전통합운영시스템 자동화에 큰 도움이 될 것이다.

[참 고 문 헌]

[1] 송형규, 박현진 『유비쿼터스 무선 네트워크 구성 기술』 2003.

[2] 정조희 『신뢰성 있는 네트워크 보호방법 및 특성』 Aug. 2004.

[3] R. Pandya et al., "IMT-2000 Standards: 네트워크 Aspects," *IEEE Personal Communications*, Vol. 8, pp. 20-29, Aug. 1997.

[4] R. Prasad et. al., "An Overview of Air Interface Multiple Access for IMT-2000/UMTS," *IEEE Communications Magazine*, Sep. 1998.

[5] TR45.5 Document, "cdma2000 Phase1 MAC Stage 3 Text", Jan. 1999.

[6] 정진욱 외 1인, "데이터통신", 2003.