DNP3 Call Simulator

송병권*, 이상훈**, 정태의***, 김건웅****
*서경대학교 정보통신공학과, **서경대학교 전자컴퓨터공학과,
***서경대학교 컴퓨터과학과, ****목포해양대학교 해양전자통신공학부
*e-mail:maruflor@naver.com,

DNP3 Call Simulator

Byung-Kwon Song*, Sang-Hun Lee**
, Tae-Eui Jeong***, Kun-Woong Kim****
*Information Communication Engineering, SeoKyeong University
**Electronic Computer Engineering, SeoKyeong University
***Computer Science, SeoKyeong University
****Division of Marine Electronic and Communication Engineering,
Mokpo National Maritime University

요 약

Distributed Network Protocol은 Master와 Slave 개념을 적용한 이벤트 감시와 하나의 Master가 다중 Slave의 제어가 필요한 환경에서 유용하게 사용되고 있는 통신 Protocol이다. DNP는 현재 개방형 Protocol로 에너지와 관련된 산업계 분야에서 사실상의 표준으로 적용되어 사용되고 있다. 현재 상용화 되고 있는 ASE2000과 DNP3의 분석을 토대로 Master와 Slave Station을 Simulation 하고 DNP3 Message를 Generate하여 Serial Port를 사용해 종단 간에 통신하는 DNP3 Call Simulator를 설계 및 구현하였다.

1. 서론

DNP(Distributed Network Protocol)는 자동화 처리 시스템의 컴포넌트들 사이에서 Master와 Slave의 개념을 적용한 통신 프로토콜로 사용된다. 1990년 IEC875-5에 기초하여 DNP1과 2가 개발되었다. 3년 뒤 1993년 DNP3 Basic 4 Document를 발표하고, DNP Users Group을 결성하였다. 현재 전기, 석유, 가스, 수력 등의 산업계 분야에서 사실상의 표준으로써 개방형 프로토콜로 적용하여 사용되고 있다[1].

DNP3은 SCADA(Supervisory Control And Data Acquisition) 시스템에 관여 하는 장치인 Master System(or Control Center)과, RTUs(Remote Terminal Units) 또는 IEDs(Intelligent Electronic Devices) 에서 통신을 담당한다. 최근 국내에서는 한전 SCADA system의 표준 프로토콜로 선정되어 원방 감시 제어용으로 사용되고 있다. 이는 DNP3이 이벤트 감시와 다중 제어가 필요한 환경에서 유용하게 이용되고 있기 때문이다.

DNP3의 적용은 미국과 유럽에서 시작하여 근래에 국내에도 적용된 시점에서 앞으로 한전의 SCADA system 이외의 국내의 DNP3 미적용 산업에서는 이미 해외에 DNP3이 적용되어 성공한 사례들을 본보기 삼아 국내에서도 적용 될 것이다. DNP3의 산업계에서 적용이 늘어나게 되면 시스템을 구축할 때 DNP3 메시지를 Master system이 Request하고 RTU가 Response하는 과정 또는 RTU가 Unsolicited 메시지를 Master system으로 보내는 일련의 과정들을 도와주는 Simulator에 대해서 연구가 필요하다.

본 연구에서는 DNP3 메시지를 발생시켜 Master와 Slave간의 통신을 DNP3 Call Simulator로 Master system과 Slave system을 Simulation한다. Simulation을 위해서 기존 출시 되어있는 상용 소프트웨어 ASE2000 도구를 분석하여 DNP3 Call Simulator의 관련 분야를 연구하였다.

3장에서는 DNP3에 대한 이해가 없으면 Simulation자체가 불가능하기 때문에 DNP3의 Layer별 분석을 하였다. 4장에서는 DNP3 Call Simulator의 네트워크의 구조와 논리적인 설계부문 그리고 실체 Simulation 과정을 담았다.

DNP3 Call Simulator는 Master system과 Slave system이 개발환경에 지원이 되지 않더라도 해당 장비에 구애 받지 않고 DNP3 Message를 Generate해 전체 환경 구축을 진행 할 수 있으며, DNP3을 사용하는 장비와의 DNP3 통신을 확인 할 수 있는 용도로 사용할 수 있다.

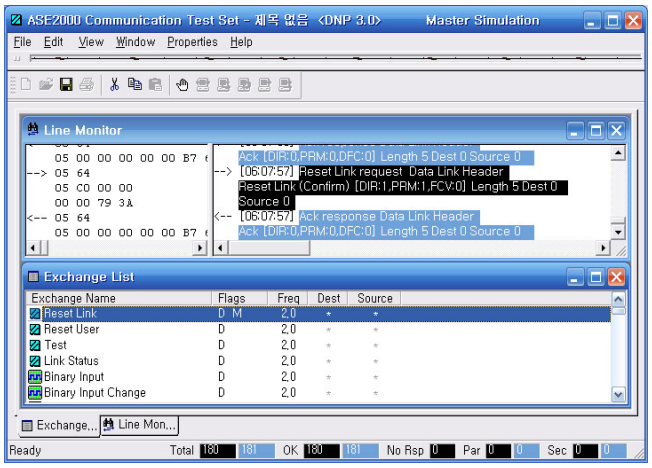
2. 관련연구

SUBNET Solutions사의 ASE2000(Applied Systems Engineering)은 Master Station과 하나 또는 그 이상의 Slave Station을 Simulation하고 그 사이에서 DNP3을 사용한 통신을 모니터링 하는 상용 소프트웨어이다.

ASE2000은 DNP3에서 Data Link Layer가 제공하는

※ 본 논문은 서울시 산학연지원 사업 신기술 개발과제 연구비로 수행되었음.

Function, Application Layer에서의 Function과 Object Code등 3개의 Layer에서 지원하는 모든 것을 손쉽게 다룰 수 있는 장점이 있다. 하지만 ASE2000의 Cabling은 ASE2000에서 외부와 통신하기 위해서는 PCMCIA to Serial Card가 반드시 있어야 한다[2]. PCMCIA카드 슬롯은 노트북 컴퓨터에서는 기본으로 장착이 되어 PCMCIA 카드를 꼽고 Null Modem을 사용해서 통신을 하므로 상관이 없다. 하지만 일반 Desktop PC에서는 메인보드의 PCI Slot에 PCI-PCMCIA Card를 꽂아서 고정을 해야만 사용할 수는 있다. 현재 메인보드에서 PCI슬롯을 줄여서 제작하고 또한 현재 사용하고 있는 PC에 빈 슬롯이 없을 경우 이를 사용하지 못하는 경우를 종종 찾아볼 수 있었다. 그래서 ASE2000은 Software가 Device에 의해서 제약을 많이 받게 된다.



(그림 3)ASE2000 실행화면

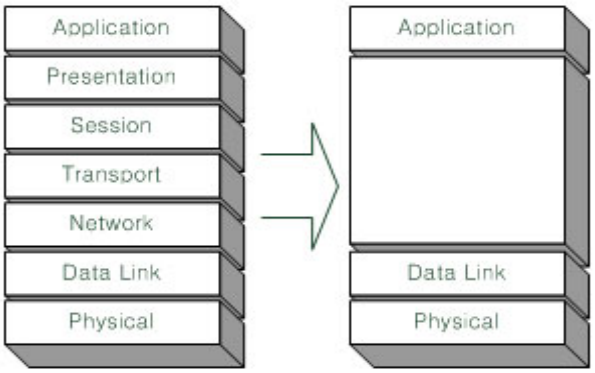
따라서 DNP Call Simulator에서는 위의 단점을 보안하기 위해 일반 PCMCIA Card가 없더라도 외부장치와 손쉽게 DNP3을 사용하여 통신하여 손쉽게 Simulation하는 것을 제안한다.

3. DNP3.0(Distributed Network Protocol V3.00)

DNP3.0은 Master/Slave 구조로 되어있다[1]. Master System(or Control Center)과 RTU(Remote Terminal Unit)사이에서는 Master System는 Master Station이 되고, RTU(Remote Terminal Unit)은 Slave가 된다. 그리고 RTU(Remote Terminal Unit)와 IED(Intelligent Electronic Devices) 사이에서는 Remote Terminal Unit이 Master Station이 되고, Intelligent Electronic Devices가 Slave가 된다.

3.1 DNP3.0 계층구조

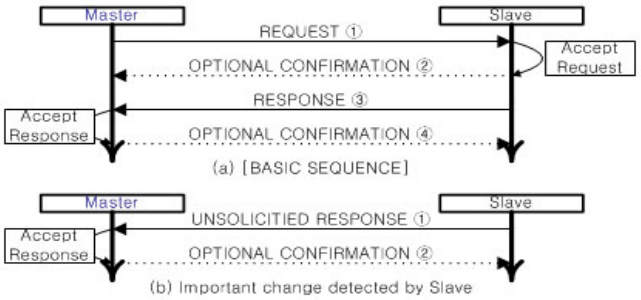
DNP3.0의 Protocol Model의 계층 구조는 ISO OSI 7 Layer에서 변형된 EPA(Enhanced Performance Architecture)를 적용하였다[1]. 아래의 (그림 4)와 같은 Physical Layer, Data Link Layer, Application Layer인, 3계층으로 되어 있다. 이는 Data가 Serial Port를 통해 연결되므로 OSI 7 Layers의 3, 4, 5, 6계층이 하는 역할이 필요하지 않기 때문에 처리시간 단축으로 인한 Performance를 향상 시킬 수 있는 구조이다.



(그림 4) ISO 7 Layer에서 EPA를 적용한 DNP3.0 3 Layer

3.2 DNP3 메시지 전달 과정

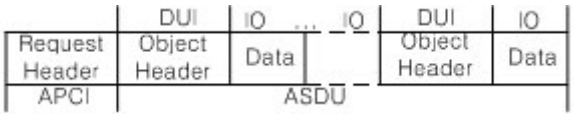
DNP3의 메시지 전달 과정은 일반적으로 (그림 5)의 (a)처럼 Master Station에서 Request를 Slave Station으로 보내어 Response를 되돌려 받는 방식으로 동장한다. 반면 Slave Station에서 기계 오작동 또는 Buffer Overflow와 같은 상태의 변환으로 이벤트가 발생하게 되면 (그림 5)의 (b)와 같은 과정을 가진다.



(그림 5) DNP3의 메시지 전달 과정

3.3 DNP3 Format

Application Layer는 DNP3의 최상위 Layer로써 (그림 6)으 구조로 되어있다. 사용자로부터 User Data를 받아서 ASDU(Application Service Data Unit)를 생성하고 Application Header인 APCI를 ASDU앞에 붙여 ASDU의 분할된 Message의 구조정보와 Message의 목적을 나타낸다.



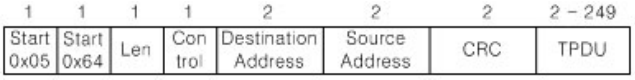
(그림 6) Application Layer Frame Format

Transport Layer는 Data Link Layer에서 LPDU(Link Protocol Data Unit)을 사용해 User Data 1 Block의 크기가 16Bytes인 단점을 보안하기 위해 EPA 3 Layer에는

없지만 Pseudo Transport Layer로 최대 크기 249Bytes인 Transport Protocol Data Unit을 사용해 대형자료를 효과적으로 보내게 되며 (그림 7)와 같은 Frame Format을 가진다. Transport Header는 TSDU(Transport Service Data Unit)에 대한 Segment 정보를 담고 있다.

(그림 7) TPDU(Transport Protocol Data Unit)

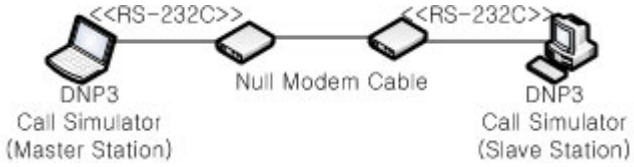
Data Link Layer는 시스템 간의 실질적인 통신을 나타내는 부분으로 (그림 8)와 같이 LPDU(Link Protocol Data Unit)를 구성하게 된다.



(그림 8) LPDU(Link Protocol Data Unit)

4, DNP3 Call Simulator 설계 및 구현

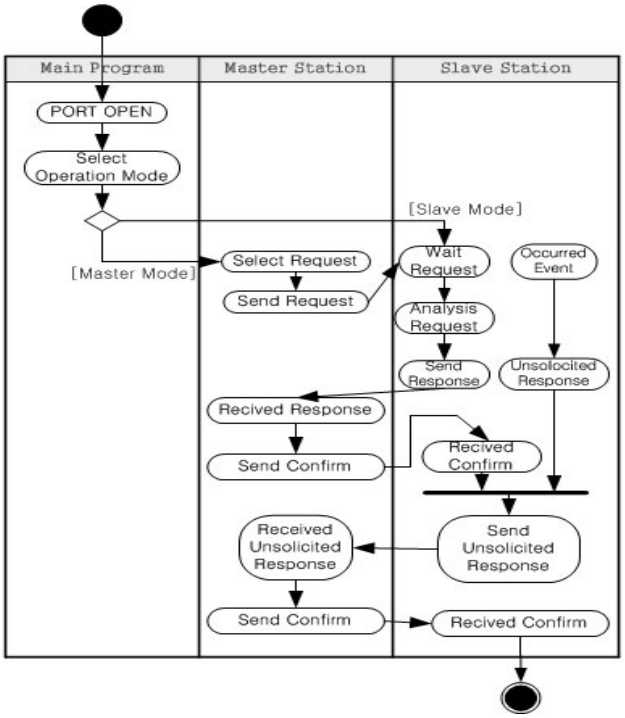
2장에서 살펴본 ASE2000에 지원하지 않은 PCMCIA 카드 없이 RS-232C를 직접 연결하며 외부와 통신할 수 있게 하며, Master와 Slave Station을 Simulation 하고 DNP3 Message를 Generate한다. 그리고 Rx와 Tx가 꼬인 RS-232C Null Modem Cable을 사용해 (그림 9)처럼 DNP3 Call Simulator를 구성하였다.



(그림 9) DNP3 Call Simulator Network Architecture

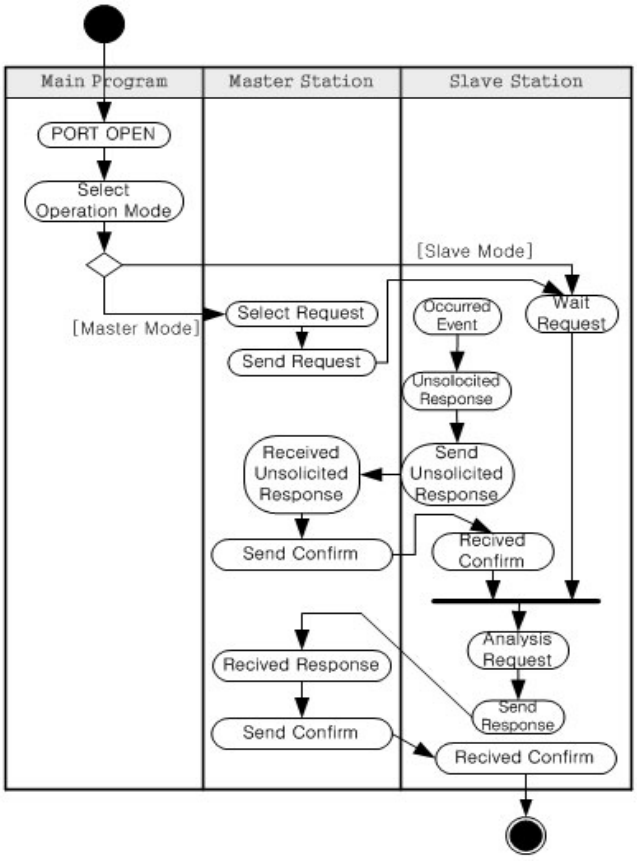
DNP3 Call Simulator는 Serial Port와 연결 후 Master Station또는 Slave Station Mode를 선택해 Simulation Mode를 결정한다. 그리고 Master Station에서 DNP3 Request를 Message를 선택하여 보내기 버튼을 누르게 되면 Slave Station으로 Request를 전송한다. Slave Station은 Request를 받아 분석 후 그에 대한 Response를 되돌려주게 된다. 또한 Slave Station에서 Unsolicited Response는 Slave에서 이벤트의 발생으로 인해 독립적으로 Master Station에게 보내는 Response이다.

그러나 Master Station에서 Request와 Slave Station의 Unsolicited Response가 동시에 발생했을 경우 충돌회피를 위해 Immediate Process Mode와 Process After Confirm Mode 둘 중 하나를 사용한다. Immediate Process Mode는 Unsolicited Response의 Confirm 보다 Master Station으로부터 수신한 Request를 우선적으로 처리해주는 것이고 (그림 11)와 같다. 예로는 시스템 데이터에 대한 READ Request를 제외한 Request에 대해서 처리하는 방식이 있다.



(그림 11) Immediate Process Mode

Process After Confirm Mode는 Request를 우선적으로 처리하는 게 아닌 Unsolicited Response Confirm을 (그림 12)처럼 계속 기다린다. 이는 시스템 Data에 대한 READ Request일 때 처리하는 방식이다.

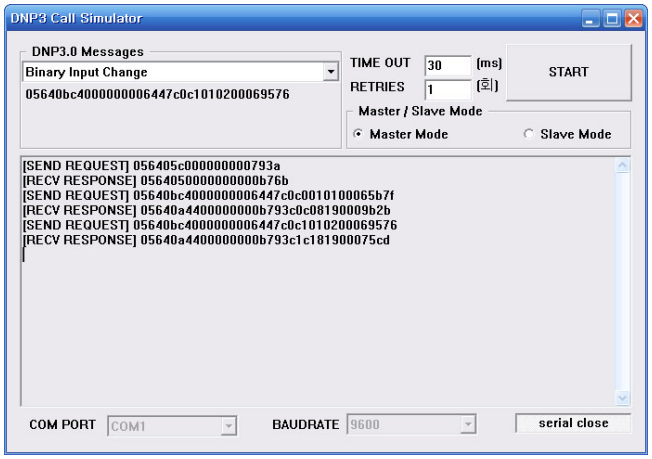


(그림 12) Process After Confirm Mode

DNP3 Call Simulator는 이와 같이 Master Station이 요구하는 종류에 따라 (그림 11), (그림 12) 두 가지 방식으로 충돌을 방지한다.

5, DNP3 Call Simulator 실행화면

아래의 그림은 DNP3 Call Simulator의 실행화면이다. Comport를 정하여 Connect Button을 눌러 Serial Port에 연결한다. 그리고 DROP LIST로 된 DNP3 Messages에서 보낼 메시지를 선택하고 Start를 누르면 (그림 13)처럼 실제 DNP3 메시지를 Serial Port를 통해 Master Station이 Request를 보내고 그에 대한 응답을 나타낸 화면이다.



(그림 13) DNP3 Call Simulator 실행 화면

6. 결론 및 향후 과제

DNP(Distributed Network Protocol)3과 ASE2000 그리고 DNP3 Call Simulator 대해서 살펴보았다. DNP3 Call Simulator와 유사한 제품은 현재 ASE2000이 상용화되어 나와 있다. 하지만 상용화 제품이라는 것과 PCMCIA카드가 반드시 필요한 것을 극복하기 위해서 윈도우즈 운영체제상에서 DNP3 Message를 Generate하고 Master와 Slave Station을 Simulation해서 DNP3을 사용한 통신 할 수 있는 환경을 제공한다. 또한 DNP3의 동작을 시각적으로 보기 쉽도록 MFC Library를 이용했다.

DNP3의 산업에서의 Open Protocol로의 적용이 더 많아 지면 Call Simulator는 앞으로 DNP3을 유용하게 분석하고, DNP3을 사용하는 장비들을 상대로 메시지의 검증을 쉽게 GUI환경에서 할 수 있을 것이다.

향후 연구로는 DNP3 Call Simulator와 Master Station 또는 RTU에 와 직접 연결해 현 프로그램을 검증하는 것과 Simulation과 동시에 메시지 분석하여 프로그램 사용자가 좀 더 편하고 이해하기 쉽게 보이는 것이 향후 연구 주제로 남아있다.

참고문헌

[1] dnp use group, “Distributed Network Protocol V3.00 Documentation”

[2] ASE2000 Communication Test Set Getting Started & User Guide. SUBNET SOLUTIONS INC.