프로토콜 역설계를 이용한 전자전시험장비 제어 및 신호분석 소프트웨어 개발

Development of Control and Analysis Software for Electronic Warfare Test System Using Reverse Engineering of Network Protocol

정 인 화*
Jung, In-Hwa

ABSTRACT

In this paper, we have proposed a method and procedure which can find out the unknown network protocol. Although it seems to be difficult to identify the protocol, we can find out the rule in the packet according to the method we have proposed. We have to recognize functions of the system and make the list of events first. Then we capture the network packet whenever the event are occurred. The captured packets are examined by means of the method that is finding repeated parts, changed parts according to the input value, fixed parts and changed parts according to regular rules. Finally we make the test program to verify the protocol. We applied this method and procedure to upgrade Electronic Warfare Test System which is operated by ADD. We have briefly described the redesign of control and analysis software for Electronic Warfare Test System

주요기술용어(주제어) : Network Protocol(네트워크 프로토콜), Reverse Engineering(역설계), Signal Processor(신호처리기), Tuner(튜너)

1. 머리말

현대의 군사용 무기체계 및 시험체계는 시스템 성능을 효율적으로 향상시키기 위해 각 기능 단위별로 모듈화된 개별 장비로 구성되고 각각의 장비간에 네트워크를 기반으로 정보를 교환하도록 설계되고 있다. 네트워크를 통하여 장비간의 통신을 원활하게 하기 위해서는 통신방법에 대한 규칙과 약속, 즉 프로토콜을 정의하고 연동되는 모든 장비가 이에 따라 데이터를 주고 받는다. 그러나, 현재 군 또는 관련기관에서 운용되고 있는 시스템 중에는 외국에서 도입되어 시스템 간의 통신 프로토콜이 공개되지 않거나 정보가 부정확하여 개량 및 유지보수에 어려움을 겪는 경우가 많다.

따라서 본 논문에서는 시스템을 구성하는 장비 간에 공개되지 않은 네트워크 프로토콜을 체계적으로 해독하는 방법과 절차를 제시하고 개량전 정비유지에 상당한 어려움을 겪어온 전자전시험체계에 본 논문에

† 2008년 3월 31일 접수~2008년 5월 2일 게재승인
* 국방과학연구소(ADD)
주저자 이메일 : inhwaj@add.re.kr

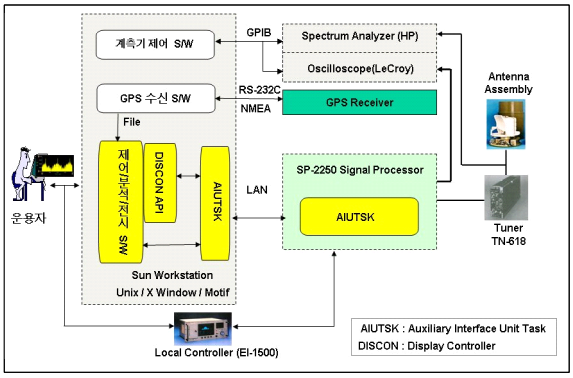
서 제시한 방법을 적용하여 구성 장비인 신호처리기와 워크스테이션 간의 네트워크 프로토콜을 해독하였다. 프로토콜 역 설계 작업은 먼저 기존 시스템의 기능 및 동작을 기능단위로 분류하고 각 이벤트에 따라 패킷을 수집한다. 다음으로 수집된 패킷을 분석하여 프로토콜을 추정하고 마지막으로 단위 기능별 테스트 프로그램을 작성하여 추정 프로토콜을 검증하는 단계로 이루어진다.

본 논문은 2장에서 전자전시험체계의 구조와 프로토콜 역설계 과정을 상세히 제시한다. 3장에서는 역설계 과정을 통해 새롭게 구현된 소프트웨어를 기존의 제어분석부 소프트웨어와 비교·분석하였으며 마지막으로 4장에서 결론을 도출하였다.

2. 통신 프로토콜 역 설계

가. 전자전시험체계 제어분석부 시스템 구성

전자전시험체계의 제어분석부는 그림 1과 같이 수신 안테나, 광대역 튜너(TN-618), 신호처리기(SP-2250), 워크스테이션, GPS 수신기 및 계측장비 등으로 구성된다[1~4].



[그림 1] 전자전시험체계 제어분석부 시스템 구성도

위 구성도에서 전자전시험체계 프로토콜 분석을 통한 시스템 역설계 대상은 워크스테이션의 제어, 신호분석 및 전시 소프트웨어와 신호처리기 간의 이더넷 통신 프로토콜 등이며, 초기 통신설정 기능, 튜너제어 기능 및 실시간 신호분석 기능 중 일부에 대한 프로토콜 분석과정을 기술하였다.

나. 기존 시스템의 기능 및 이벤트의 분류

프로토콜 역 설계 작업을 효과적으로 수행하기 위해서는 먼저 시스템의 기능과 동작 상태를 충분히 이해하고 이에 따른 이벤트를 체계적으로 분류하여야 한다. 시스템의 시작부터 종료까지 사용자의 입력에 따라 발생하는 이벤트를 구분할 수 있는 최소 단위까지 설정하고 분류표를 작성해야 한다. 표 1에 전자전성능시험체계의 주요 이벤트를 기능별로 분류하였다.

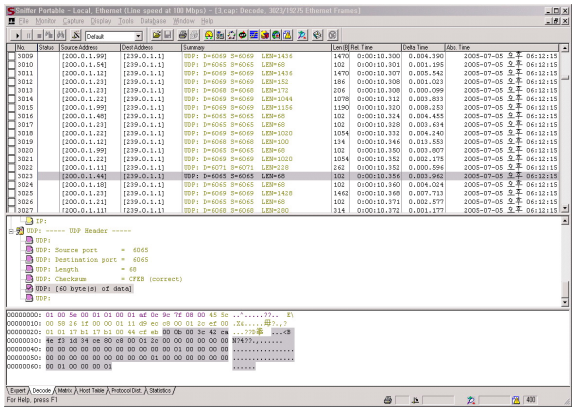
[표 1] 기능별 이벤트 분류표

기능	이벤트
통신 설정	- 통신연결 요청(IP/Port 정보교환) - 연결 요청 정보 확인 및 응답 - 주기적 상태 확인 및 응답
튜너 제어	- 튜너 활성화 요청 및 응답 - 동조 주파수 설정 - 입력 레벨 임계값 설정 - Tune/Scan 모드 변경 - 자체점검 신호 확인
실시간 신호분석 (진폭 대 주파수, 시간 대 주파수, 진폭 대 시간, 시간 대 펄스간격)	- 신호전시 요청 - 신호전시 명령(파라메터) 및 응답 - 실시간 데이터 송신 - 신호전시 중단 요청
PDW 수집	- 신호수집 요청 - 신호수집 명령(파라메터) 및 응답 - 신호 도착시간(TOA) 정보 송신 - 신호 데이터(펄스 제원) 송신 - 신호수집 중단 요청
수신 안테나 제어	- 수신 안테나 수동 제어 요청 - 수신 안테나 수동 제어 명령 및 응답 - 수신 안테나 신호전시 데이터 송신 - Point/Spin/Sector 모드 변경 요청 - 수신 안테나 신호전시 중단 요청

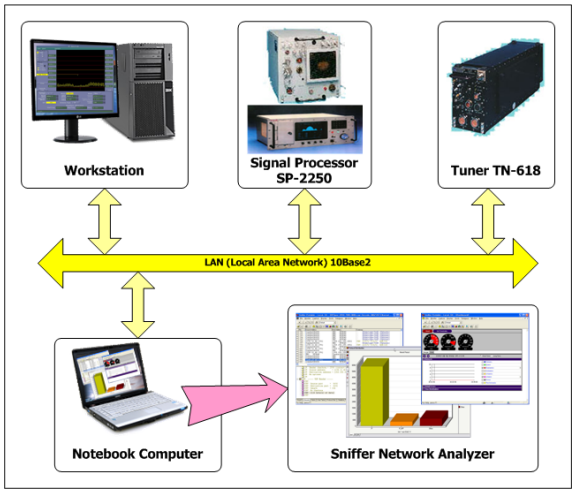
다. 네트워크 패킷 수집

역 설계 작업의 두 번째 단계는 패킷수집 단계로서 작성된 기능 및 이벤트의 분류표에 따라 스니퍼

(Sniffer)와 같은 네트워크 분석기(Network Analyzer)를 이용하여 각각의 기능단위로 패킷을 수집하였다[5,6]. 패킷수집을 위하여 워크스테이션(WS : Work Station)과 신호처리기(SP : Signal Processor) 사이에 설치된 스위칭 허브를 통해 별도의 분석 컴퓨터를 연결하였다.



[그림 2] 네트워크 패킷 수집 프로그램



[그림 3] 네트워크 패킷 수집 구성도

라. 패킷분석 및 프로토콜의 추정

역 설계 작업의 세 번째 단계는 프로토콜 역 규명 작업에 있어 가장 중요한 패킷분석 및 프로토콜 추정 단계로서 수집된 패킷을 분석하여 예상되는 프로토콜을 추정하는 과정이다.

프로토콜 추정에는 다음과 같은 몇 가지 방법을 복합적으로 이용하였다.

1) 패킷 중첩 및 반복 부분의 추적

수집된 패킷을 순차적으로 나열한 뒤 이중 공통적으로 반복되는 부분을 찾는다.

표 2의 통신설정 기능 패킷 중에서는 c6 16 28 b2, c6 16 28 94, 20 00 등의 부분이 중첩되거나 반복되고 있으며 이들 값을 변환해 보면 결국 다음과 같은 정보를 얻을 수 있다.

c6 16 28 b2 = 198.22.40.178 (신호처리기 IP 주소)
c6 16 28 94 = 198.22.40.148 (웍스테이션 IP 주소)
20 00 = 8192 (UDP 포트)

2) 변하지 않는 고정 값의 추출

패킷 중에는 어느 경우에도 변하지 않는 고정된 부분이 있을 수 있다. 이는 프로토콜로서 별다른 기능을 가지지 않는 의미가 없는 부분으로 재설계시 Padding 처리한다. 표 2의 패킷 중 86 00 b2 01 06 21 06 00 부분은 의미가 없는 Padding이다.

3) 입력 값의 변화에 대한 패킷 변화의 추적

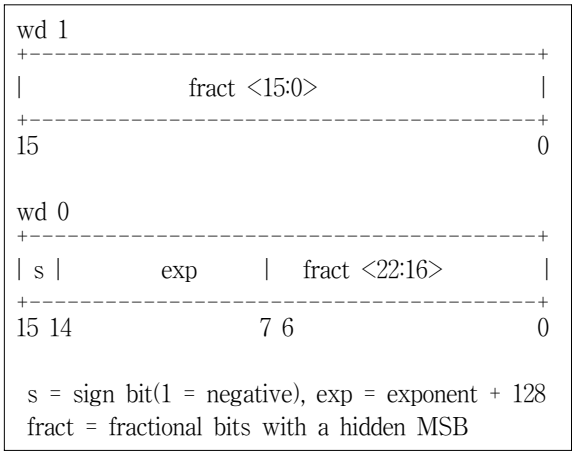
입력 값을 다양하게 변화시키면서 이에 따른 패킷 변화 부분을 찾는다. 예를 들어, 표 3에서 튜너제어 기능 중 동조 주파수 입력 값의 변화에 따른 패킷의 변화는 다음과 같다. 이는 그림 4와 같이 DEC사의 32 비트 부동소숫점으로 표기되어 있으므로 이를 해석하면 아래와 같다.

동조 주파수(MHz)
f9 46 00 f8 = 7999.0 MHz
7a 45 00 00 = 1000.0 MHz

fract = 1111|1001|1111|1000|0000|0000
fract = 0.1111|1001|1111|1 = 1111|1001|1111|1/2^13
= 7999 / 2^13
exp = 0x46 << 1 = 0x8D = 141
exponent = exp - 128 = 13
value = (7999 / 2^13) * 2^13 = 7999

[표 2] 해독된 통신설정 프로토콜

No	전송	패킷
1	SP→WS	28 28 ff ff 20 7f 01 00 c6 16 28 b2 20 00 04 00 86 00 b2 01 06 21 06 00
		* 연결 요청 대기 * c6 16 28 b2 = 198.22.40.178 * 20 00 : 8192 (UDP 포트)
2	SP←WS	28 28 03 00 20 7f 01 00 c6 16 28 94 20 00 02 00 81 ff 10 00
		* 연결 요청 * c6 16 28 94 = 198.22.40.148 * 20 00 = 8192 (UDP 포트)
3	SP→WS	28 28 ff ff 20 7f 01 00 c6 16 28 b2 20 00 05 00 86 00 b2 01 06 21 06 00 c6 16 28 94 20 00 02 00 00 ff
		* 연결 요청 정보 확인
4	SP←WS	28 28 03 00 20 7f 06 00 c6 16 28 b2 20 00 05 00 02 ff c6 16 28 94 20 00 03 00 80 ff 10 00
		* 연결 요청 정보 확인(응답)
5	SP→WS	08 18 ff ff 20 7f 02 00 b2 80 c6 16 28 b2 20 00 10 00 c6 16 28 94 20 00
		* 연결 승락
6	SP→WS	28 28 ff ff 20 7f 01 00 c6 16 28 b2 20 00 06 00 86 00 b2 01 06 21 06 00 c6 16 28 94 20 00 03 00 04 ff
		* Alive-checking 확인
7	SP←WS	28 28 03 00 20 7f 06 00 c6 16 28 b2 20 00 06 00 06 ff c6 16 28 94 20 00 04 00 80 ff 10 00
		* Alive-checking 확인 응답



[그림 4] DEC사 32비트 부동소숫점 표기법

[표 3] 해독된 튜너 제어 프로토콜

No	전송	패킷
1	SP←WS	18 08 03 00 08 81 b2 00 ff bf 00 00 80 02 c0 00
		* Tuner 제어 시작
2	SP→WS	08 18 03 00 1d 7f 08 01
		Acknowledgement
3	SP←WS	18 08 03 00 00 81 01 00 7a 45 00 00 fa 45 00 00 f9 46 00 f8 10 10 01 00 00 42 92 81 32 80 58 1f ff 00 83 3b 6f 12 00 00
		* Tuner Enable
4	SP→WS	08 18 03 00 1d 7f 00 01
		Acknowledgement

4) 일정한 규칙에 따라 변화하는 값의 추적

패킷의 내용 중에는 일정한 규칙에 따라 변화하는 부분이 있다. 이는 다음과 같은 경우들이 될 수 있으며 주로 데이터부의 앞이나 끝에 위치하는 경우가 많다.

- 데이터의 전송 순서(이 경우는 주로 일련번호가 된다)
- 지금까지 전송한 데이터의 크기(이 경우는 점차 증가한다)
- 지금까지 수신된 데이터의 크기(이 경우 역시 점차 증가한다)
- 남은 데이터의 크기(이 경우는 점차 감소한다)
- 현재 전송되고 있는 데이터의 크기(이 경우는 주로 동일한 값이 반복되다가 마지막에 값이 작아진다)

표 4의 해독된 신호전시 프로토콜에서 전송되는 패킷 번호(Sequence Number)가 차례대로 증가함을 알 수 있다. 패킷의 앞부분은 신호크기 대 주파수의 실시간 전시 데이터 전송을 의미하고, 패킷 뒤의 4워드는 실제 전시되는 데이터의 X 좌표와 Y 값인 신호크기를 나타내는데 사용된다.

[표 4] 해독된 진폭 대 주파수 신호전시 프로토콜

No	전송	패킷
1	SP→WS	0c 54 03 00 29 18 00 01 00 01 00 04 80 00 81 01 00 20 80 00
		* RTD(진폭대 주파수) 데이터 전송 * 첫 번째 데이터 전송
2	SP→WS	0c 54 03 00 29 18 00 02 00 01 00 04 80 00 81 03 00 24 80 00
		* 두 번째 데이터 전송
3	SP→WS	0c 54 03 00 29 18 00 03 00 01 00 04 80 00 81 05 00 21 80 00
		* 세 번째 데이터 전송
4	SP→WS	0c 54 03 00 29 18 00 04 00 01 00 04 80 00 81 06 00 22 80 00
		* 네 번째 데이터 전송

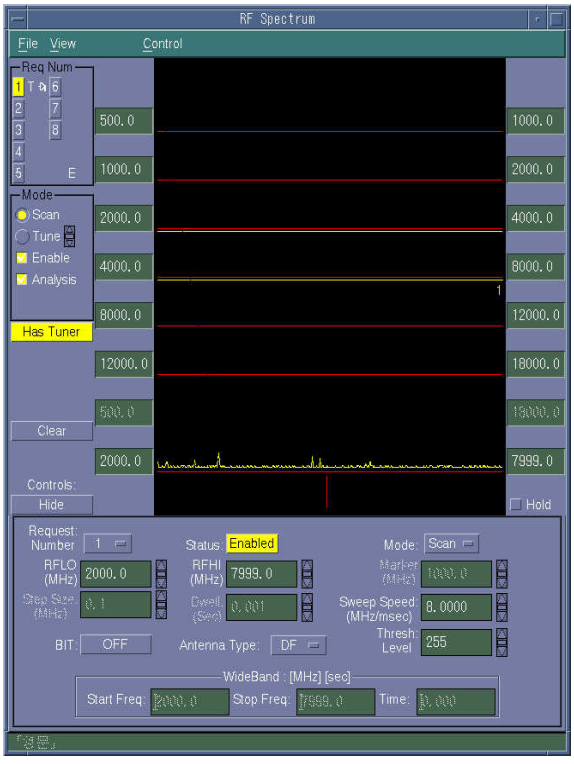
마. 기능별 테스트 프로그램 작성 및 프로토콜 검증

프로토콜 역 규명 작업의 마지막 단계로 추정된 프로토콜에 따라 기존의 유닉스 기반 제어 프로그램을 표본으로 단위 기능별 테스트 프로그램을 윈도우 기반으로 작성하고 이를 실제 시스템에 적용하여 추정된 프로토콜을 검증하였다.

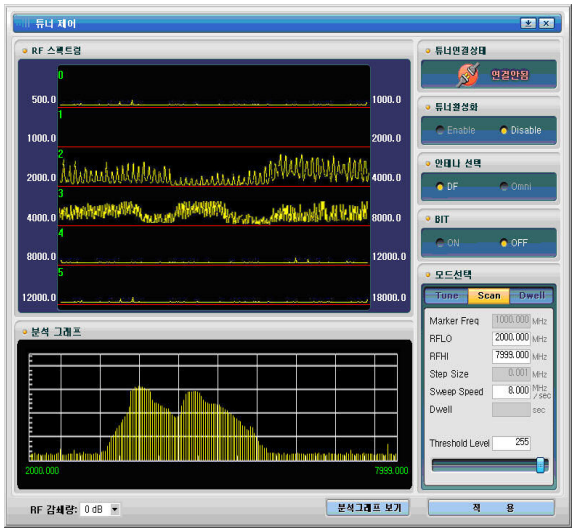
테스트 프로그램은 실제 시스템에서 운용 빈도가 많고 중요한 기능들을 선별하여 처음에는 가능한 한 단순하게 작성하고 각 단위기능 별 시험을 순차적으로 진행하여 시험이 반복됨에 따라 나머지 기능들을 추가하여 점차 시스템 전체 프로토콜 설계방안을 수립하였다.

이와 같은 프로토콜 역 규명작업에서는 시스템 기능을 세부적으로 이해하고 있어야 시간과 노력을 단축할 수 있다.

그림 5와 그림 6은 기존의 유닉스 기반의 튜너 제어화면과 역 규명 과정을 통하여 윈도우 기반에서 재설계된 튜너제어 화면을 나타낸다.



[그림 5] 유닉스 기반 튜너제어 화면

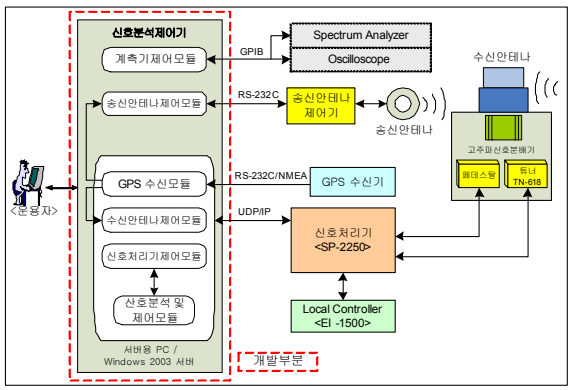


[그림 6] 윈도우 기반 튜너제어 화면

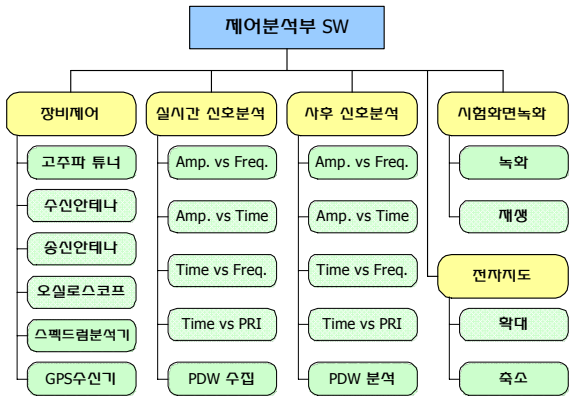
본 연구에서는 위에서 설명한 전자전시험장비 제어분석부의 통신설정 기능, 튜너제어 기능 및 실시간 신호분석 기능 외에도 수신 안테나 제어기능, PDW (Pulse Description Word) 수집 기능에 대한 프로토콜 분석을 수행 하였다[7].

3. 제어분석부 소프트웨어 설계

전자전시험체계의 제어분석부 소프트웨어의 개량 목적은 시스템 유지 보수 및 사용자 교육에 어려움이 있는 기존의 유닉스 기반의 운용환경을 윈도우 기반으로 재설계 하는 것이다. 기존 유닉스 기반의 제어분석부 S/W는 미들웨어, 저수준 응용 프로그램 및 운용자 프로그램으로 구성되어 있었으나 재설계를 위한 제작사의 자료제공이 매우 미비하였다. 따라서 본 논문에서 제시하는 방식으로 신호처리기와 워크스테이션간의 통신 프로토콜을 역설계하여 단위 기능 프로그램을 작성하였고 이를 토대로 기존의 유닉스 기반 제어분석부 S/W를 윈도우 기반으로 재설계하였다. 그림 1의 기존 유닉스 기반 제어분석부 구성도는 개량후 그림 7과 같이 윈도우 기반으로 구성된다. 재설계한 제어분석부 소프트웨어의 기능은 그림 8의 메뉴 구조를 보면 알 수 있다.



[그림 7] 전자전시험체계 제어분석부 구성도



[그림 8] 제어분석부 S/W 메뉴 구조

제어분석부 S/W는 송·수신안테나, 계측기, GPS 수신기, 고주파 튜너를 제어하는 장비제어 모듈, 레이더 펄스 분석/전시 모듈, 시험화면 녹화/재생 모듈 및 전자지도 모듈로 구성된다.

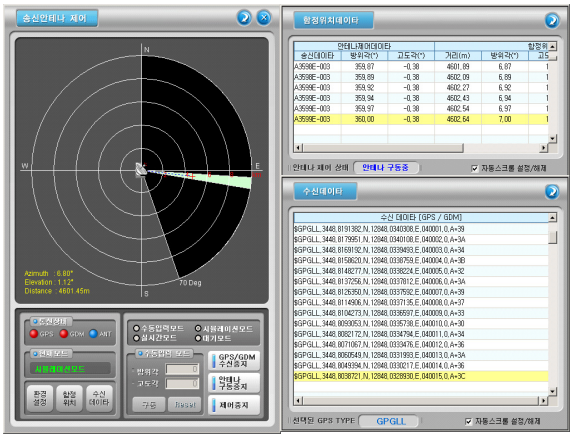
송신안테나 제어 모듈은 함정의 위치정보를 데이터링크로부터 수신한 다음 송신 안테나에서 함정까지의 방위각과 고각을 계산한 후 안테나 제어기로 전송하여 송신 안테나를 구동한다. 그림 9는 송신안테나 제어 화면이다.

수신안테나 제어 모듈은 신호처리기가 안테나 페데스탈을 제어할 수 있도록 명령어 데이터를 보낸다. 그림 10은 수신안테나 제어 화면이다.

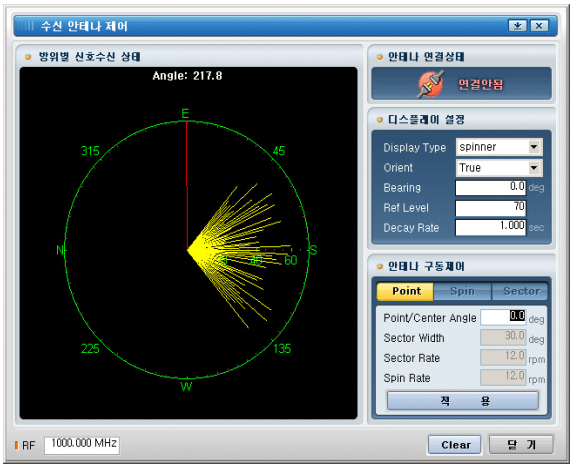
GPS 수신 모듈은 송·수신 안테나를 지심도 시험소에서 함정방향으로 구동할 수 있도록 GPS 데이터를 수신하여 해석한 후 송·수신 안테나 제어 모듈로

데이터를 넘겨준다.

신호처리기 제어모듈은 레이더 신호를 실시간으로 수집/분석하기 위해 튜너와 신호처리기를 제어한다.

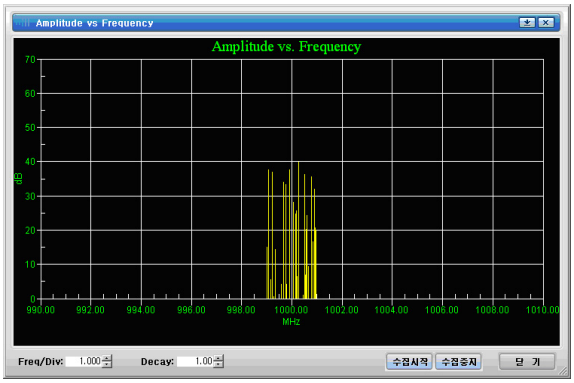


[그림 9] 송신안테나 제어 화면

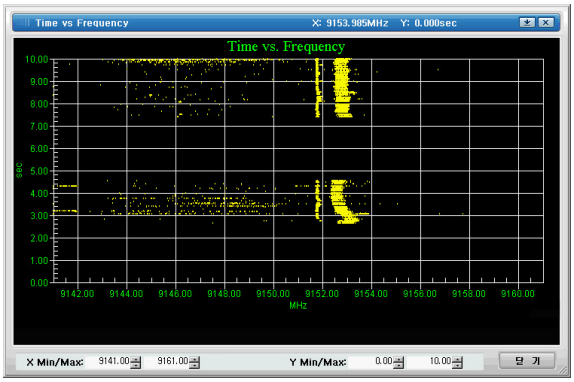


[그림 10] 수신안테나 제어 화면

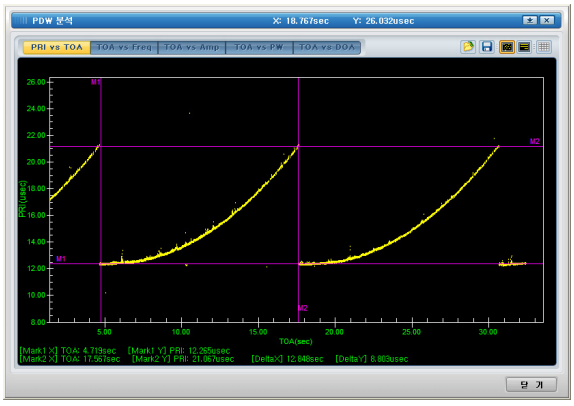
신호분석/전시 모듈은 운용자와 인터페이스를 통해서 실시간으로 분석된 결과를 다양한 형태의 그래픽 화면으로 전시한다. 레이더 및 전자전장비의 신호를 수집하여 제원을 분석하기 위하여 진폭 대 주파수, 진폭 대 시간, 시간 대 주파수 및 시간 대 펄스 반복율 화면을 제공한다. 그림 11은 진폭 대 주파수 화면이고 그림 12는 시간 대 주파수 화면으로 실제 수신되는 레이더 신호를 실시간으로 전시한다.



[그림 11] 실시간신호분석(진폭 대 주파수)



[그림 12] 실시간 신호분석(시간 대 주파수)



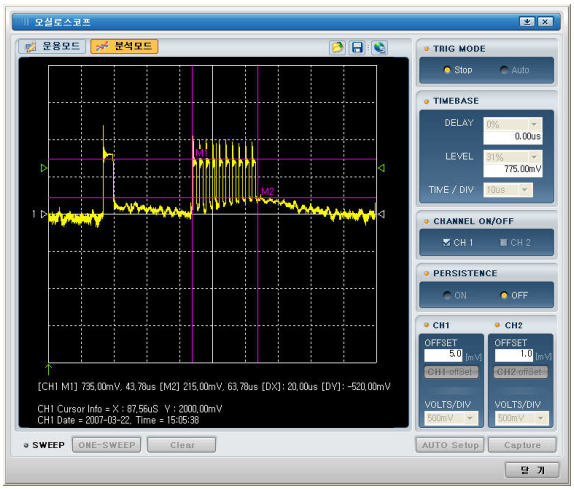
[그림 13] PDW 분석 화면(RGPO)

또한 신호분석/전시 모듈은 신호를 수집하여 정밀분석하기 위해서 PDW를 수집하고 이전에 수집된 PDW를 전시하여 진폭, 주파수, 펄스간격 및 스캔특

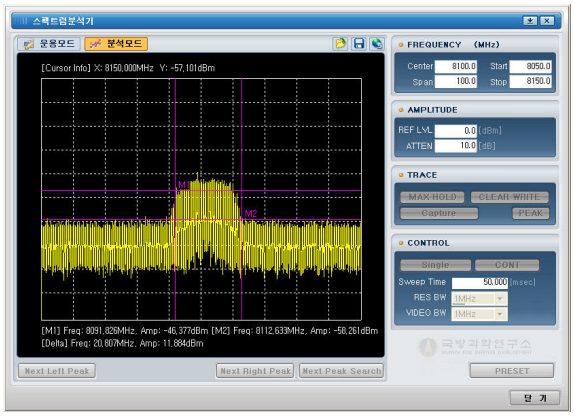
성 등의 제원을 분석하는 기능을 제공한다. 그림 13은 수집된 PDW를 분석하는 화면으로 RGPO(Range Gate Pull Out) 재밍신호의 특성을 보여주고 있다.

계측기 제어 모듈은 수신되는 RF 신호의 주파수 특성을 분석하는 스펙트럼 분석기(HP-8563)와 시간 특성을 분석하는 오실로스코프(LeCroy-9310A)를 원격으로 제어하며 신호의 분석, 전시 및 저장기능을 수행한다[8,9].

그림 14는 오실로스코프 제어/분석 화면으로 MFT (Multiple False Target) 재밍신호를 보여주고 있다. 그림 15는 스펙트럼분석기 제어/분석 화면으로 레이더 신호의 점유 주파수 대역폭을 보여주고 있다.



[그림 14] 오실로스코프 제어/분석 화면



[그림 15] 스펙트럼분석기 제어/분석 화면

4. 맺음말

본 연구에서는 현재 국방과학연구소 지심도 시험소에서 운용중인 전자전시험체계 제어분석부의 네트워크 통신 프로토콜을 해독하여 유닉스 기반의 제어분석부 프로그램을 윈도우 기반으로 재설계하였다.

프로토콜이 공개되지 않은 시스템 간에 네트워크를 통하여 전송되는 통신패킷의 구조를 파악하여 프로토콜을 역으로 해석하기란 그리 쉬운 일이 아니다. 그러나, 프로토콜이란 반드시 일정한 규칙이 존재하기 마련이며 본 논문에서 제안한 기법과 같이 시스템의 기능 및 이벤트의 분류, 패킷의 수집, 패킷 분석 및 프로토콜의 추정, 그리고 단위 기능별 테스트 프로그램의 작성 및 추정 프로토콜의 검증 등의 몇 가지 체계적인 단계를 거쳐 최종적인 프로토콜을 추출할 수 있다. 패킷 분석단계에서 수집된 패킷에 대하여 중첩 또는 반복 부분의 추적, 입력 값의 변화에 대한 패킷 변화의 추적, 변하지 않는 고정 값의 추출, 일정한 규칙에 따라 변화하는 값의 추적 등의 방법을 통하여 복합적으로 분석하였다.

본 연구에서 제안된 방법은 지심도 전자전시험체계 제어분석부의 성능 개량사업에 성공적으로 적용되었으며 더 나아가 제작사에서 공개하지 않은 LPX, KDX의 전투체계 미들웨어인 SPLICE(Signaal Modular Architecture for Logical InterConnection Engine) 및 KDCOM(Korean Destroyer Commander)의 네트워크 통신 프로토콜을 해석하는데 토대가 되었다.

참 고 문 헌

[1] 이성호, 정회인, 정인화, “전자전시험체계 제어분석부 패킷분석 결과 보고서”, 국방과학연구소, ADDR-514-080378, 2008.

[2] 이성호, 정회인, 김정호, 정인화, “전자통신시험체계 신호분석제어기 소프트웨어 설계 보고서”, 국방과학연구소, ADDR-514-070853, 2007.

[3] “TN-618-15 RF Tuner Maintenance Instructions”, Condor System Inc., 1998.

[4] “CS-5052-01 ESM Subsystem Operation and

Maintenance Manual", Condor System Inc., 1998.
[5] "Snifferbook Ultra Installation and Operations Guide, Release 4.5", Network Associates Inc., 2000.
[6] 서승호, 구수용, 신해준, 김서우, 정연기, 김영탁, "TCP/IP 프로토콜 분석 및 네트워크 프로그래밍", 정익사, 2002.
[7] "Signal Processor Packet Definition for Compact Data Format(CDF) and Pulse Description Word(PDW) Format", Condor System, Inc., 1998.
[8] "LeCroy Remote Control Manual", LeCroy Inc., 1992.
[9] "User's Guide 8560 E-Series Spectrum Analyzers", Agilent Technologies, 2000.
[10] "LAN Interface Control Document", Condor System, Inc., 1997.
[11] Filippo Neri, "Introduction to Electronic Defense Systems", Artech House, 2001.
[12] Barton, David Knox, "Radar System Analysis and Modeling", Artech House, 2004.
[13] Mahafza, Bassem R., Elsherbeni, Atef Z., "MATLAB Simulations for Radar Systems Design", CRC Press, 2004.