비보호 저속망 환경에서의 고용량 음향데이터의 최적화 전송 및 보호 시스템 구현

선두영* · 김덕영** · 김용득***

An implementation of stable transmission and security management system of
massive acoustic data in unsecurity and low speed network area

Doo-young Sun* · Duk-young Kim** · Yong-deuk Kim***

요 약

음향데이터 수집체계가 다양화되고 고성능화 됨에 따라 수집되는 음향데이터의 양은 기하급수적으로 증가되었다. 이렇게 수집된 음향데이터는 정밀한 분석을 위하여 분석환경으로의 전송이 필요하다. 이러한 수집/분석 체계에서는 빠르고 안정적인 전송은 물론 고도의 완벽한 보안이 요구된다. 하지만 기존시스템은 전송방식을 사용하기 때문에 자료전달에 많은 시간이 필요하다. 아울러 네트워크를 사용하는 경우에 비보호 저속망은 전송 안정성과 자료 보호성이 취약하여 구현이 불가능하다. 이에 본 논문에서는 일반적으로 사용되는 비보호 저속망 환경에서 고용량의 수집 음향데이터를 전송하고 보호하는 시스템을 제시한다. 구현된 시스템은 비보호 저속망 환경에서도 안전하게 음향데이터를 전송하고 다양한 위협 요소로부터 안전하게 음향데이터를 보호한다.

ABSTRACT

The amount of acoustic data gathered from the acoustic data gathering system is increased dramatically as the acoustic data gathering system become various and highly effective. It is needed to transmit this acoustic data to analysis environment for precise analysis. In this gathering/analysis system, it is also needed the stable transmitting as well as highly perfect security. But the existing system using the conveying method needs a lot of time. In case of using networks, the low speed networking vulnerable in the stable transmitting and the information security is impossible to materialize. In this paper, I would like to propose a transmitting and management system sending a massive gathering acoustic data in the unsecurity and low speed networking environment. The implemented system is to transmit the acoustic data safely in low speed networking environment and secure the acoustic data from various threats.

키워드

음향데이터, 보호, 보안, 네트워크, 데이터 전송

Key word

acoustic data, security, networking, data transfer

* 아주대학교 전자공학과 석사과정(volcan99@naver.com)

접수일자 : 2010. 01. 05

** 아주대학교 전자공학과 박사과정

심사완료일자 : 2010. 05. 17

*** 아주대학교 전자공학과 교수

I. 서 론

수중과 수상의 해양환경에서 표적을 탐지하고 식별하는 가장 효과적인 방법은 음향데이터를 획득하여 분석하고, 축적된 표적식별정보와 비교하는 것이다. 이를 토대로 표적의 탐지 여부와 탐지된 표적의 식별을 수행함으로써 최종적으로 피·아를 확정하고 이에 따른 공격/방어/감시 등의 전술을 결심한다.

이러한 전술적 방법을 지원하기 위해서는 다양한 표적의 특징정보를 축적해야 한다. 여러 종류의 음원에서 발생하는 음향데이터를 수집하기 위하여 선배열센서, 예인센서, 소노부이, 능·수동센서 등을 사용하여 다양한 대역의 음향데이터를 수집한다. 수집된 음향데이터는 마그네틱 테이프, 하드디스크, 광학디스크 등의 물리적 매체에 저장한 후, 전송(인편으로 직접 전달하는 행위)의 방법을 통해 분석센터로 전달되며, 분석센터는 전달받은 매체를 재생하여 표적의 특징정보를 추출하고 유가치 영역을 발췌하여 데이터베이스화하며, 필요시 구축된 데이터베이스의 정보를 물리적 매체에 저장한 후, 전송하는 방식을 통해 수집체계와 타격체계에 전달한다[1].

하지만 기존의 방법은 음향데이터의 전달에 전송 방식을 사용하기 때문에 획득된 음향데이터의 즉각적인 공유와 분석이 불가능하며, 또한 분석된 결과도 타격체계와 수집체계에 필요한 시점에 제공하지 못하는 문제점을 가지고 있다. 다음의 그림 1은 기존 시스템의 운영 개념이다.

그림 1. 기존 시스템 운영 개념

Fig 1. Operating Concept of existing system

그림 1과 같이 기존 시스템은 수집된 음향데이터의 정밀분석과 데이터베이스 구축을 위하여 수집현장에서

원격지에 위치한 분석센터로 음향데이터를 전달하는데 이때 사용되는 방식이 인편을 통한 전송방식이다. 또한 분석센터에서 수집된 음향데이터를 정밀 분석하여 구축되어진 표적식별용 데이터베이스를 타격체계와 수집체계에 전달하는 방식도 역시 인편을 통한 전송방식을 사용한다. 전송방식은 자료의 절취, 복제, 변형, 삭제 등의 위협요소에 대해서는 안전하게 자료를 전달할 수 있지만 인편을 통한 전달방식이기 때문에 자료 전달에 많은 비용과 시간을 필요하다. 기존 시스템의 수집현장과 분석센터의 거리가 가장 먼 경우 전송 시간은 최소 10시간 이상이 소요된다[1]. 또한 지속적인 경비의 지출과 운용인력의 공백이 존재하게 된다. 비용과 인력의 문제로 인하여 수집된 음향데이터를 일정기간 축적한 후 전달하는 방법이 적용되는 경우엔 자료를 필요한 시점에 제공하지 못한다는 문제점을 가지고 있다.

이러한 기존 체계의 문제점을 해결하기 위한 가장 효과적인 방법은 WAN을 통한 음향데이터의 전송이지만 WAN을 통해 음향데이터를 전송하는 경우 두 가지의 문제점이 있다. 먼저 WAN의 전송속도가 저속 구간에 의존적이라는 것이며, 또한 보안이 적용되지 않는 구간이 존재한다는 것이다. 즉 음향데이터는 높은 분해능과 장시간의 녹음으로 고용량이며 보안을 유지해야 할 비밀자료이기 때문에 보안을 보장받지 못한 WAN을 통한 전송은 허가되지 못하는 상황이다[2].

이러한 문제점을 해결한 것이 본 논문에서 제시하는 시스템이다. 구현된 시스템은 고용량으로 수집된 데이터를 수집현장에서 분리, 재표본화, 발췌 등의 1차 처리하여 전송할 데이터의 양을 최적화한 후, 완벽한 보안전송 방식으로 자료를 전송하고 안전하게 관리한다. 본 논문에서는 비보호 저속망을 통해 비밀자료인 고용량 데이터를 전송할 때 구현된 시스템을 통해 최적화 전송을 수행하는 방식과 다양한 위협 요소로부터 음향데이터의 안전하게 보호하는 방식을 제시한다.

II. 시스템 구성

기존 시스템의 문제점을 해결하기 위하여 본 시스템은 다음의 그림 2와 같은 운용방식을 적용하였다.

그림 2. 구현된 시스템 운영 개념
Fig 2. Operating concept of implemented system

본 시스템은 기존에 각 수집체계/타격체계가 수집한 음향데이터를 각 분석센터에서 보내던 방식을 주요 지역별로 수집센터를 두어 음향데이터의 전송을 전담하게 하는 방식으로 전환하였다. 음향데이터의 전송은 기존의 체송방식에서 WAN을 이용한 네트워크방식으로 적용하였다. 이를 위하여 수집센터에는 운용장치를 설치하였고 분석센터는 관리장치를 설치하였다. 운용장치는 수집센터에 설치되어 각 수집체계에서 수집된 음향데이터를 안전하게 보관하고 최적화된 전송을 실시하며, 해당 데이터를 완벽하게 폐기한다. 관리장치는 분석센터에 설치되어 수집센터에 설치된 운용장치와 네트워크로 연결되어 음향데이터 전송의 서버역할을 수행한다. 관리장치 역시 전달된 음향데이터를 안전하게 보관하고 사용이 완료된 음향데이터는 완벽하게 폐기한다. 또한 비보호 네트워크에서 비밀자료를 전송하기 위하여 운용장치와 관리장치 모두 보안정책과 장치를 구성하여 비밀자료의 소통이 가능하였다.

본 시스템은 비보호 저속망에서 비밀자료인 고용량 음향데이터를 전송하기 위하여 전송측면과 보안측면에서 다양한 설계 방법을 적용하여 구현되었으며 적용된 대표적인 기법으로는 데이터 최적화 기법, 전송 최적화 기법, 물리적·논리적 위협요소 대응 기법 등이다.

2.1 전송측면의 설계 및 구현

본 시스템은 전송측면에서 저속망을 통해 고용량의 음향데이터를 전송해야 하므로 전송할 데이터의 양을 줄일 필요가 있었다. 이를 위하여 음향데이터를 최적화할 수 있는 설계가 반영되었다. 또한 전송된 자료의 신뢰도를 높이기 위하여 응용 수준(Application Level)에서 전송 대기시간을 줄이고 오류에 따른 재전송을 최소화하는 전송 최적화 방식의 설계가 반영되었다.

2.1.1 음향데이터 최적화 기법

본 시스템은 WAN을 사용하기 때문에 전송되는 음향데이터는 저속 구간의 영향을 받아 고속 전송이 이루어지지 못한다. 본 시스템이 사용하는 망은 10Mbps의 전송율을 제공하지만 실측치에서는 약 1~2Mbps의 전송율을 제공함이 확인되었다[1]. 다음의 그림 3은 구현된 시스템이 사용되는 실제 망 환경에서 3일 동안 측정된 결과이다.

그림 3. 비보호 저속망 전송속도 측정 결과
Fig 3. Checking result of transmit speed in unsecurity and low speed network

측정된 결과에서 심야시간 등 비운용 시간대를 제외한 운용 시간대의 평균 속도는 약 250Kcps(=2Mbps, cps는 character per second의 약어로 초당 전송 문자열을 의미하며, 1cps는 8bps와 같다.)라 할 수 있다. 이러한 저속망은 고용량 음향데이터를 전송에 많은 시간이 소요되며 망 자체에 부하를 주게 된다. 따라서 고용량 음향데이터의 최적화가 필요하였다. 본 시스템은 고용량 음향데이터를 최적화하기 위하여 Re-sampling 기법, 원음분리 기법, 유효구간 발췌 기법을 구현하여 고용량 음향데이터를 최적화하였다.

① Re-sampling 기법의 적용

본 시스템은 Re-sampling 기법을 적용하여 전송될 음향데이터의 양을 획기적으로 줄였다. 전송될 음향데이터는 xxKHz~xxxKHz(이하 기재된 모든 주파수는 보안 사항으로 필요 시 국방과학연구소의 협조 후, 제공될 수 있다.)의 샘플링으로 녹음된 데이터이지만 이를 분석하는 데는 xKHz~xxKHz로 샘플링된 데이터면 충분하다. 따라서 수집센터에서 분석 대역에 알맞은 Re-sampling을 수행하여 음향데이터를 재가공하는 방법을 통해 음향데이터의 양을 줄일 수 있었다. 다음의 그림 4와 그림 5는 xxKHz로 녹음된 음향데이터를 xKHz로 Re-sampling

하여 2Mbps의 전송환경에서 전송하였을 때를 측정한 것으로 고용량 음향데이터일수록 효과적임을 알 수 있다.

그림 4. 가공 전·후 음향데이터의 크기 변화
Fig 4. Transition of acoustic data size by data processing

그림 5. 가공 전·후 음향데이터 전송 소요 시간
Fig 5. Required acoustic data transmit time by data processing

② 원음분리 기법의 적용

본 시스템은 원음분리 기법을 적용하여 전송될 음향데이터의 크기를 절반으로 줄였다. 전송될 음향데이터는 원음과 음성의 두 채널이 녹음되어 저장된 wave file 형태이다. 원음은 분석센터에서 반드시 사용하지만 음성은 더미파일인 경우가 대부분이다[1]. 따라서 본 시스템에서는 전송될 음향데이터에서 음성데이터부분을 제거하는 방식을 적용하였다. 다음의 그림 6은 음성데이터부분을 제거하는 일련의 절차이다.

그림 6. 원음분리 처리 절차
Fig 6. Procedure of raw data separation

③ 유효구간 발췌 기법의 적용

본 시스템은 유효구간 발췌 기법을 적용하여 불필요한 부분의 제거한 유가치한 부분의 음향데이터만을 전송하는 방식을 통해 전송의 효율을 높였다. 수집된 음향데이터를 수집센터에서 수집 유형에 맞는 적응신호처리를 수행하여 그림 7과 같이 무가치구간과 유가치구간을 구분한 후, 유가치구간을 발췌하여 불필요한 음향데이터의 전송을 제거함으로써 전송 효율을 높였다.

그림 7. 유가치영역의 발췌
Fig 7. Extracting of value existence area

유효구간 발췌 기법은 전시된 신호처리 결과에 따라 운용자가 유효구간을 선택하면 운용프로그램은 자동으로 해당하는 음향데이터 원본에서 선택구간에 알맞게 음향데이터를 재 추출하고 헤더를 변경하여 새로운 발췌된 음향데이터를 생산한다.

이상의 기법을 통해 음향데이터를 최적화하는 방법이 적용되어 본 시스템은 최대 약 96:1의 비율까지 음향데이터를 최적화 할 수 있었다. 예를 들어 xxKHz의 샘플링으로 1시간가량 녹음된 음향데이터가 96Mbyte인 경우 Re-sampling을 통해 24:1의 최적화가 가능하기 4Mbyte로 변환되며, 여기에 원음분리 기법이 적용되면 불필요한 음성데이터가 제거되어 2Mbyte로 변환된다. 마지막으로 유효구간 발췌 기법을 적용하여 30분의 유효구간을 발췌하게 되면 1Mbyte로 변환되어 최종 전송대상이 되는 음향데이터는 1Mbyte가 된다.

그림 8은 96Mbyte의 음향데이터를 기준으로 각 기법이 적용된 경우를 나타낸 것이다. 음향데이터의 양을 축소할 때 Re-sampling 기법이 가장 효과적이며, 3가지 기법이 모두 적용될 때 최적의 음향데이터를 만들 수 있다.

그림 8. 기법적용조합에 따른 데이터 축소량
Fig 8. Reduction size by method combination

2.1.2 전송 최적화 기법

본 시스템은 전송 대기시간을 줄이고 재전송을 최소화하기 위하여 분할전송 기법과 분할된 차등오류검사 기법을 적용하였다.

① 분할전송 기법의 적용

본 시스템은 Application Level에서 분할전송 기법을 적용함으로써 송신시스템과 수신시스템의 최대 허용 속도로 음향데이터를 전송한다. 이러한 분할전송 기법은 수신시스템의 상태를 파악하여 부하를 분산시킴으로써 수신시스템의 Application Level에서의 데이터 손상(버퍼나 메모리 큐의 덮어쓰기와 시간초과로 인한 데이터 버림 등을 의미함.)을 막을 수 있다. 또한 운용자에게 전송상태의 가시성을 제공하여 다중작업처리의 편의를 제공한다.

그림 9. Data Slicing별 따른 전송속도
Fig 9. Transmit speed according data slicing

그림 9는 10Mbps 환경에서의 100Mbyte의 데이터를 64Kbyte에서 50Mbyte까지 총 10가지의 유형으로 데이터를 분할하며 전송하며 전송속도를 측정한 결과이다. 실험은 Intel Core 2 Duo 2.67GHz CPU가 장착된 2대의 컴퓨터를 직접 연결한 후, 운용 부하를 위해 5개 이상의 응용프로그램을 실행시킨 상태에서 측정하였다. 구현된

시스템은 본 결과에 근거하여 최대의 전송속도를 발휘하는 1Mbyte로 음향데이터를 분할하여 전송을 실시하고, 분석센터는 수신 후 이를 다시 조합하여 고용량의 음향데이터를 생산한다.

② 차등오류검사 기법의 적용

본 시스템은 분할된 오류검사 기법을 적용하여 재전송을 최소화하였다. 본 시스템은 고용량의 음향데이터를 전송하기 때문에 전송 상에 오류가 발생하여 고용량의 음향데이터를 다시 전송한다면 적지 않은 시간적 손실이 발생한다. 따라서 본 시스템은 1Mbyte 단위의 음향데이터 조각에 대해서는 헤더영역 및 테일영역의 정밀검사와 데이터영역의 CRC(Cyclic Redundancy Check, 순환중복검사)를 수행하여 수신된 음향데이터 조각의 신뢰성을 빠르게 확보하고, 모든 음향데이터의 조각이 수신되어 음향데이터가 조합된 상태에서는 Hash함수를 이용하여 음향데이터에 대한 무결성을 입증한다. 이러한 2종류의 데이터 유형에 따른 오류검사 기법을 적용함으로써 네트워크 상에서 발생한 오류에 대해 음향데이터 전체의 재전송이 아닌 1Mbyte의 음향데이터 조각에 대한 재전송을 수행하기 때문에 전송의 효율화를 이룰 수 있으며, 최종적으로는 Hash함수를 이용하여 무결성을 검사하여 수신된 음향데이터의 신뢰성을 제공한다. 음향데이터 조각에 대해서 CRC를 적용한 이유는 높은 신뢰성보다는 빠른 검수를 통한 전송 부담을 줄이기 위함이고, 전체 음향데이터에 Hash함수를 적용한 이유는 수신이 완료된 상태에서는 빠른 검수보다는 높은 신뢰성이 필요하기 때문이다.

2.2 보안측면의 설계 및 구현

본 시스템은 보안측면에서 보호되지 못하는 일반망을 통해 비밀자료인 음향데이터를 전송해야 했다. 따라서 본 시스템에서 자료의 절취, 복제, 변형, 삭제 등의 위협요소에 직접적으로 대응할 수 있어야 했다[3][4]. 이러한 이유로 본 시스템은 보안측면의 설계가 반영되어 구현되었다. 본 시스템에 적용된 보안측면의 설계는 외부 위협요소로부터 비밀자료를 보호하기 위한 설계와 내부 위협요소로부터 비밀자료를 보호하기 위한 설계가 반영되었다.

2.2.1 외부 위협요소 대응 기법

본 시스템에 제공되는 망은 군에서 사용하는 특수목

적의 폐쇄망이지만 모든 군이 접근하여 사용할 수 있기 때문에 군 내부에서는 일종의 공개망 성격을 갖는다. 따라서 비밀인 음향데이터의 취급이 허가된 자 이외에 망에 접근할 수 있는 자는 경우에 따라 비밀인 음향데이터에 절취, 복제, 변형, 삭제 등의 위해를 가할 수 있다. 따라서 이러한 외부 위협요소에 대한 대응이 필요하였다. 본 시스템은 이를 위하여 망분리 기법과 방어 시스템 구축 기법을 적용하여 비밀자료인 음향데이터에 대한 외부 위협요소에 대응하였다.

① 내·외부 망 분리 기법의 적용

본 시스템은 물리적 보안 차원으로 비보호 저속망인 외부 망과 고속의 내부 망의 교점에 위치한다. 내부망은 제한된 시설과 인원으로 보호 되지만 외부망은 보호되지 않기 때문에 구현된 시스템을 통하여 외부 망의 침입 세력이 내부 망으로의 침입을 차단하여야 한다[3][5]. 따라서 본 시스템이 외부망에서 시도되는 외부 위협요소의 공격을 방어하지 못하면 내부망의 모든 시스템이 공격을 받게 된다. 그림 10은 내·외부망이 분리되지 않고 구성되는 일반적인 망 교점 시스템의 구성이다.

그림 10. 일반적인 망 교점 시스템 구성
Fig 10. General network system composition

이러한 이유로 본 시스템은 내·외부 망의 물리적 차단 기법을 적용하였다. 본 시스템을 2개의 부분으로 분리하여 하나는 수집센터와의 음향데이터 전송을 수행하는 관리기1과 다른 하나는 내부의 정밀분석 시스템으로 음향데이터를 전달해 주는 관리기2로 구성하였다. 관리기1과 관리기2는 물리적으로 차단되어있으며 유일한 자료 전달은 저장장치를 통해서 이루어지며 저장장치는 동시에 관리기1과 관리기2에 연결되지 않는다. 따라서 외부의 침입세력이 관리기1까지 침입하였다고 가정해도 관리기2 이후 부분인 분석센터 내부의 모든 장비에 대한 접근은 불가능하다. 내·외부 망 분리 구성은 그림 11과 같다.

그림 11. 내·외부망 분리 구성
Fig 11. Inner and outer network separated composition

② 방어시스템 구축

본 시스템은 비보호망에 연결되기 때문에 적합한 방어시스템이 구축되어야 하였다. 일반적으로 적용되는 소규모 망 구축 시의 방어시스템 구성은 다음의 그림 12와 같다[6].

그림 12. 일반적인 방어시스템 구성
Fig 12. General prevent system composition

점선안의 암호장비는 송신자료를 암호화하고 수신자료를 복호화하는 기계적인 장치로 본 시스템의 보안 측면에서 반드시 필요한 장비이다. 이러한 구성의 문제점은 침입탐지기가 외부의 공격에 대해서는 효과적으로 대처할 수 있지만 내부 사용자에 의한 불법적 행위는 암호장비 때문에 본래의 기능을 수행할 수 없다는 문제점이 존재한다.

그림 13. 적용된 방어시스템 구성
Fig 13. Implemented prevent system composition

따라서 본 시스템은 그림 13과 같이 구성하였다. 암호장비 이후에 침입탐지기를 설치하여 내부 사용자에 의한 불법적 행위에 대한 대처가 가능하게 하였다. 외

부 사용자의 공격은 방화벽인 침입차단기가 1차 방어 역할을 수행하며 암호장비가 추가적인 방어 역할을 수행하는 2중의 방어체계가므로 침입탐지기가 방어를 수행하지 않아도 보안성이 확보된다. (본 내용은 정보통신 보안측정(K4등급) 평가 시 주관 기관으로부터 제안된 권고안 임.)

2.2.2 내부 위협요소 대응 기법

모든 시스템은 운용자에 의한 내부 위협요소가 존재한다. 이는 의도적인 경우도 있으며 의도하지는 않지만 발생하는 경우도 있다[3]. 따라서 본 시스템은 내부 위협요소에 대응하기 위한 기법을 적용하였다. 먼저 2.2.1절에서 기술한 방어시스템도 내부 위협요소에 대응하기 위한 기법이며 또한 본 시스템은 내부 운용자에서 기인한 위협요소에 대응하기 위하여 자동완전삭제 기법을 통해 자료를 보호하고, 이력관리검증 기법을 통해 불법적인 운용에 대응한다.

① 자동완전삭제 기법

본 시스템은 자료의 절취와 불법적인 사용을 방지하기 위하여 자동완전삭제 기법을 적용하였다. 일반적으로 삭제는 복구용 S/W로 복구가 가능하기 때문에 삭제된 자료를 복구하여 사용될 수 있으며, 경우에 따라서는 데이터 섹터를 스캔하는 방식의 물리적 복구가 가능하다. 아울러 운용자가 사용이 완료된 비밀자료를 삭제하지 않는 경우도 존재한다[7].

이러한 문제점을 해결하기 위하여 본 시스템은 전송이 완료된 음향데이터에 대하여 자동으로 완전삭제를 수행한다. 완전삭제 방식은 마그네틱 디스크의 물리적인 복구에 대해서도 안전성이 보장된 Gutmann, US DoD 5220-22.M, Pseudorandom (ISSAAC 알고리즘) 기법에서 권장하는 35회 덮어쓰기 후 삭제하는 방식을 적용하였다. 완전삭제 기법은 전송이 완료되거나 운용자가 삭제를 요청한 파일에 대하여 운용자의 개입 없이 시스템이 자동으로 1차적인 덮어쓰기를 수행한 후, 시스템의 부하에 맞추어 나머지 34회의 덮어쓰기를 수행한다. 이때 덮어쓰는 블록의 크기와 블록의 내용은 모두 가변적으로 처리된다. 이러한 완전삭제는 비밀자료에 대하여 운용자의 개입을 차단하고 시스템이 판단하여 사용이 완료된 비밀자료에 대하여 즉시 완전삭제를 수행한다.

② 이력관리검증 기법

일반적인 이력은 불법적인 접근에 의해 이력이 위·변조의 위험 때문에 이력내용을 암호화하여 관리한다. 이러한 방식은 많은 저장공간을 사용하게 되고 검색 수행에 많은 시간이 소모되는 단점이 존재한다[1].

따라서 본 시스템은 위·변조방지를 위하여 각 이력항목의 각각에 대하여 Hash 함수를 적용하였다. 이력이 기재될 때 기재내용은 Hash함수가 적용되어 검증값으로 적용되며, 이력의 위·변조 여부를 검증할 때 다시 Hash함수를 적용하여 검증값을 추출하는 방식으로 기재된 값과 검증값의 일치를 확인하여 이력의 위·변조를 방지한다. 본 시스템에 적용된 이력관리검증 기법은 암호화 이력관리 기법보다 적은 저장공간을 사용하며, 빠른 검색 속도를 제공한다.

III. 시스템 성능 분석

기존의 시스템과 요구되어진 시스템, 그리고 본 시스템의 성능을 비교 분석한 것이 다음의 표 1이다.

표 1. 시스템 간 성능 비교
Table 1. Performance compare of each system

항목	구현 시스템	요구 시스템	기존 시스템
전달 시간 (100Mbyte기준)	1분 미만	7~8분	10시간 이상
보안성	우수	취약	보통
현장 분석기능	있음	없음	없음
운용에 따른 추가비용	없음	없음	있음
운용 공백	없음	없음	있음
구축 비용	저비용	고비용	-
자료 보호 기능	있음	없음	없음

표 1에 기재된 바와 같이 구현 시스템은 모든 측면에서 기존 시스템보다 우수한 성능을 발휘하고 있으며 특히 보안측면에서 사람에 의존하던 것을 시스템이 담당함으로써 내부자에 대한 보안성을 구축할 수 있다.

IV. 결 론

비보호 전송망에서 고용량의 음향데이터를 전송하는 본 시스템은 앞에서 제시한 전송측면의 설계 기법과 보안측면의 설계기법을 적용하여 구현하였다. 본 시스템의 성과는 다음의 3가지로 요약 할 수 있다.

- 국내 최초 XXX망에서 비밀자료 전송 승인
- 현재 000부대 외 X개 부대에서 운용 중
- 미설치부대를 위한 양산 계획 심의 중

본 시스템은 국내에서 처음으로 XXX망(비보호 저속 망)에서의 비밀자료 전송을 승인 받았다. 승인은 국군 기무부대 주관으로 실시된 정보통신 보안측정(K4등급)을 수행하고 이를 통과함으로써 획득하였다. 본 시스템이 XXX망에서의 비밀자료 전송에 대한 승인을 획득함으로써 비밀자료의 전송이 필요한 다른 체계들이 본 시스템의 보안측면의 설계를 적용할 때 XXX망을 통해 비밀자료의 전송에 대한 승인을 동일하게 받을 수 있다는 근거를 제시해 주었다. 이는 비밀자료 전송을 위해 필연적으로 고비용의 전용 폐쇄망을 구축해야만 하는 방식에서 기존에 구축된 XXX망을 활용함으로써 체계 개발 및 구축에 소요되는 비용의 절감과 일정의 단축이 가능하다는 장점을 제공해 주었다.

또한 안정화되고 최적화된 전송측면의 설계와 운용의 편리성을 통해 구현된 시스템은 현재 4,000시간 이상 운용되어지고 있다. 이러한 성능과 운용성이 기반이 되어 본 시스템은 X개소의 미설치 부대에 설치를 위한 양산 계획을 심의 중에 있으며, 근래에 배치/운용될 예정이다.

참고문헌

- [1] 도경철외 4명, 음향정보전송장비 설계서, 국방과학연구소, 2008
- [2] 문은점, 도경철, 조창봉, 다중매체 DB 보안시스템 구축 개념 연구, 국방과학연구소, 2005
- [3] 국방부, 보안업무시행규칙, 국방부, 2001
- [4] 김종일, 박동섭, 이성중, 정보보호핵심지식, 정일, 2002

- [5] Kevin Gennuso, Disconnect from the Internet-Whale's e-Gap In-Depth, SANS Institute InfoSec Reading Room, Sep. 13, 2001
- [6] Tom Thomas, Network Security First-Step, Macmillan Technical Pub, 2004
- [7] 나기현외 8명, 컴퓨터 하드디스크 복구에 대한 연구, 국립과학수사연구소 연보 제36권, 2004

저자소개

선두영(Doo-Young Sun)

한국항공대 전자계산학 학사
아주대학교 전자공학과 석사과정
LIG넥스원 책임연구원(현)

※ 관심분야 : Network Security, M&S, Test & Evaluation, Software Engineering

김덕영(Duk-Young Kim)

광운대학교 대학원 석사
아주대학교 전자공학과 박사과정
LIG넥스원 수석연구원(현)

※ 관심분야 : 수중감시, 수중통신, 해양환경모델링, 해양음향토모그래피

김용득(Yong-Deuk Kim)

연세대학교 대학원 석사
연세대학교 대학원 박사
아주대학교 전자공학과 교수(현)

※ 관심분야 : 무선 네트워크 알고리즘, 영상인식 알고리즘, 지능형 교통 시스템