비보호 저속망 환경에서의 고용량 음향데이터의 안정적 전송 및 관리 시스템 구현

선두영* · 김용득**

*아주대학교 전자공학과 석사과정

**아주대학교 전자공학과 교수

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

Doo-Young Sun* · Yong-Deak Kim**

*,**Ajou University

E-mail : *volcan@ajou.ac.kr, **yongdkim@ajou.ac.kr

요 약

음향데이터 수집체계가 다양화되고 고성능화 됨에 따라 수집되는 음향데이터의 양은 기하급수적으로 증가되었다. 이러한 수집 음향데이터는 정밀한 분석을 위하여 분석환경으로의 전송이 필요하다. 이러한 수집/분석 체계에서는 빠르고 안정적인 전송은 물론 고도의 완벽한 보안이 요구된다. 이에 본 논문에서는 일반적으로 사용되는 비보호 저속망 환경에서 고용량의 수집 음향데이터를 전송하고 관리하는 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. 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

acoustic data, security, networking, data transfer

Ⅰ. 서 론

수중의 다양한 정보를 추출하여 활용하기 위해서는 여러 종류의 음향데이터를 필요로 한다. 다양한 대역의 음향데이터를 수집하기 위해서는 여러 형태의 센서를 사용하여야 하며 이것은 음향데이터의 양을 기하급수적으로 증가시키고 있다. 또한 수집된 음향데이터는 각 대역에 적합한 신호처리 기법을 적용하여 정보를 추출하여야 하는데 이러한 이유로 수집 현장에서의 분석 보다는 육상(혹은 원격지)에 위치한 분석센터에서 전문분석 장비를 이용한 분석 전문가의 분석이 필요하다. 이러한 방식을 통해 정밀한 정보의 추출과 유가치 자료의 데이터베이스화가 가능하다. 이러

한 운용 환경에서 수집된 음향데이터를 분석센터로 전송하기 위하여 가장 유용한 방법은 WAN을 이용한 데이터 전송이다. 하지만 고용량의 음향데이터를 WAN을 이용하여 전송할 때 경우에 따라 두 가지의 취약점이 존재하는데 하나는 WAN의 전송속도가 저속 구간에 의존적이라는 것과 보안이 적용되지 않는 구간이 존재한다는 것이다. 따라서 본 논문에서는 일반적으로 사용되는 비보호 저속망 환경에서 고용량의 수집 음향데이터를 전송하고 관리하는 시스템을 제시한다. 구현되어 운용되어지고 있는 시스템은 비보호 저속망 환경에서도 안전하게 음향데이터를 전송하고 다양한 위협 요소로부터 안전하게 음향데이터를 보호한다.

II. 시스템 구성이론

구현된 시스템은 원격지에 설치되어 다양한 수집체계로부터 음향데이터를 수집하여 1차 분석 및 재처리를 수행하여 분석센터로 전송하는 운용장치와 분석센터에 설치되어 수집된 음향데이터를 취합하여 전문분석장비에게 할당해주는 관리장치로 구성되었다. 개략적인 시스템의 개요도는 다음의 그림과 같다.

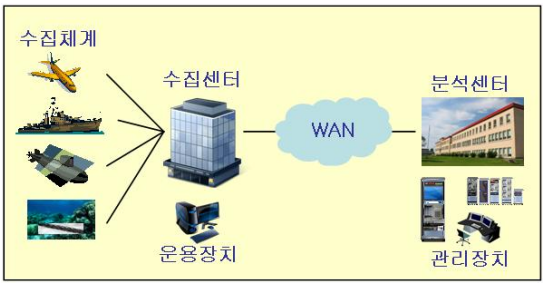

그림 1. 시스템 개요도

본 시스템은 WAN을 사용하기 때문에 전송되는 음향데이터는 저속 구간의 영향을 받아 고속 전송이 이루어지지 못하고 이론적으로 최대 10Mbps의 전송율을 제공하나, 실측치에서는 약 1~2Mbps의 전송율을 제공한다. 이러한 저속의 전송율은 고용량의 데이터를 전송하는데 많은 전송시간을 요구하며 이는 정보의 활용가치 측면과 운용성 측면에서 불이익을 강요받는 원인으로 작용한다. 또한 전용망을 사용하기는 하지만 특수목적의 폐쇠망이 아닌 관계로 해당 전용망을 사용하는 집단 내에서는 일종의 공개망의 성격을 띠게 되며 이는 자료에 대한 절취, 복제, 변형, 삭제 등의 위협이 존재함을 부인할 수 없다. 따라서 대용량의 음향자료를 저속의 환경에서도 가능한 빠르고 안전하고 완벽하게 전송하고 전송된 자료를 안전하게 보호하는 기능이 시스템에 적용되었다.

III. 전송측면의 설계 및 구현

본 시스템의 전송측면에 다음과 같은 기능을 구현하였다. 먼저 전송될 음향데이터의 양을 줄여 전송시간을 단축하기 위하여 다음의 기법을 적용하였다.

- Re-sampling 기법
- 유효구간 발췌 기법
- 전송자료 압축 기법

또한 안정적 전송을 위하여 다음의 기법을 적용하였다.

- 분할 전송 기법
- 무결성 보장 기법
- 전자서명 기법

마지막으로 운용의 편의성과 전송시간 단축을 위하여 다음의 기법을 적용하였다.

- 예약전송 기법

① Re-sampling 기법의 적용

본 시스템은 Re-sampling 기법을 적용하여 전송될 음향데이터의 양을 획기적으로 줄였다. 전송될 음향데이터는 xxKHz ~ xxxKHz의 샘플링 으로 녹음된 데이터이지만 이를 분석하는 데는 xKHz ~ xxKHz로 샘플링된 데이터면 충분하다. 따라서 수집센터에서 분석 대역에 알맞은 Re-sampling을 수행하여 음향데이터의 양을 줄이므로써 전송시간을 줄일 수 있고 또한 분석센터의 업무를 분담할 수 있다. 다음의 그림은 xxKHz로 녹음된 음향데이터를 xKHz로 Re-samplig하여 2Mpbs의 전송환경에서 전송하였을 때를 측정한 것이다.

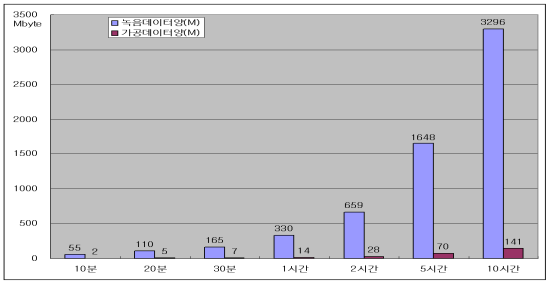

그림 2 가공 전·후 음향데이터의 크기 변화

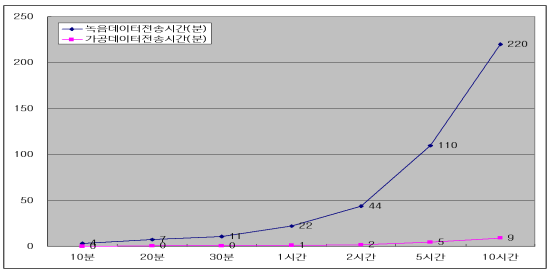

그림 3 가공 전·후 음향데이터 전송 소요 시간

② 유효구간 발췌 기법의 적용

본 시스템은 유효구간 발췌 기법을 적용하여 불필요한 부분의 제거한 유가치한 부분의 음향데이터만을 전송하여 전송의 효율을 높였다. 음향데이터의 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.

③ 전송자료 압축 기법의 적용

본 시스템은 전송을 위해 전송될 음향데이터와 로그파일 등을 압축한 후 전송함으로써 전송의 효율을 높였다. 음향데이터는 압축률이 90%정도이지만 음향데이터의 전송 시 참고가 되는 여러 가지 파일을 동시에 압축하여 전송함으로써 80% 대의 압축율을 유지할 수 있으며 아울러 음향데이터와 연계되는 로그파일 등 참고 자료가 패키지화 됨으로써 운용의 편의성을 동시에 얻을 수 있다.

④ 분할 전송 기법의 적용

본 시스템은 Application Level에서 분할 전송을 적용함으로써 송신시스템과 수신시스템의 최대 허용 속도로 음향데이터를 전송한다. 이러한 분할 전송 기법은 수신시스템의 상태를 파악하여 부하를 분산시킴으로써 수신시스템의 Application Level에서의 데이터 손상을 막을 수 있다. 또한 운용자에게 전송상태의 가시성을 제공하여 다중 작업처리의 편의를 제공한다.

⑤ 무결성 보장 기법의 적용

본 시스템은 무결성 보장 기법을 적용하여 전송된 음향데이터의 오류를 제거하였다. 먼저 분할 전송되어 수신되는 각 음향데이터 블록은 헤더 정보와 테일 정보를 분석하여 유효함을 판단하여 임시로 저장한 후, 마지막 음향데이터 블럭의 전송이 완료되면 수신 시스템은 수신된 모든 음향데이터 블록을 취합하여 음향데이터를 생성하고 생성 음향데이터에 대하여 Hash 함수를 적용함으로써 최종적으로 전송된 음향데이터의 입수 여부를 판단한다.

⑥ 전자서명 기법의 적용

본 시스템은 음향자료 송·수신 시 부인방지를 위하여 전자서명 기법을 적용하였다. 송·수신이 완료되면 먼저 수신시스템에서 수신 영수증을 발부하여 송신시스템에 전달하고, 이를 수신한 송신시스템은 확인 영수증을 발부하여 수신시스템에 전달한다. 이러한 전자서명 기법을 적용하여 송·수신에 대한 부인방지는 물론 송신시스템의 운용자와 수신시스템의 운용자 모두 상대시스템의 운용자가 action을 취하였는지를 즉석에서 확인할 수 있다.

⑦ 예약전송 기법의 적용

본 시스템은 운용자의 편의성과 전송의 효율을 높이기 위하여 예약전송 기법을 적용하였다. 제공된 망은 시간에 따라 전송속도가 매우 가변적이다. 실측결과 전송속도가 급격히 저하되는 시간대가 존재하고 반대로 전송속도가 상당히 양호한 시간대가 존재함을 파악하였다. 구현된 시스템은 이에 대응하기 위하여 고용량의 음향데이터의 경우 전송속도가 양호한 시간대에 맞추어 자동으로 전송된다. 운용자의 예약전송 결심을 받은 시스템은 (S/W적)암호화된 형태로 전송할 음향데이터를 보관하다가 해당 시간이 되면 자동적으로 예약된 음향데이터를 분석센터로 전송한다. 이러한 기능은 고용량 데이터 전송에 따른 운용자의 과다한 업무를 해결할 수 있다.

Ⅳ. 보안측면의 설계 및 구현

본 시스템의 보안측면에 다음과 같은 기능을 구현하였다. 먼저 물리적 보안 차원에서 음향자료의 보호를 위하여 다음의 기법을 적용하였다.

- 내·외부 망 분리 기법
- 방어시스템 구축 기법

또한 기능적 보안 차원에서 음향자료의 보호를 위하여 다음의 기법을 적용하였다.

- 암호화(H/W & S/W) 기법
- 완전삭제 기법

마지막으로 관리적 보안 차원에서 음향자료의 보호를 위하여 다음의 기법을 적용하였다.

- 이력 관리 기법
- 시스템접근차단 기법
- 계층별 인증 및 접근 차별화 기법

① 내·외부 망 분리 기법의 적용

본 시스템은 물리적 보안 차원으로 비보호 저속망인 외부 망과 고속의 내부 망의 교점에 위치한다. 내부망은 제안된 시설과 인원으로 보호 되지만 외부망은 보호되지 않기 때문에 구현된 시스템을 통하여 외부 망의 침입세력이 내부 망으로의 침입을 차단하여야 한다. 많은 방법이 있지만 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 다음의 그림과 같다.

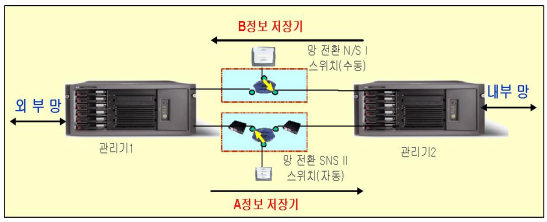

그림 4. 내·외부망 분리 구성도

② 방어시스템 구축

본 시스템은 내·외부 망이 동시에 연결되는 시스템으로 외부 망을 통한 다양한 위협으로부터 본 시스템과 내부 망에 연결된 시스템을 보호하여야 한다. 따라서 물리적 보안 차원으로 다음과 같은 방어 시스템을 구축하였다.

- 침입차단기
- 침입탐지기
- 보안용 OS
- 비밀소통용암호기
- 보안전용USB메모리

③ 암호화(H/W & S/W) 기법의 적용

본 시스템은 기능적 보안 차원으로 보음향데이터에 대하여 H/W적 암호화와 S/W적 암호화 등 2종류의 암호화를 제공한다. 전송되는 음향데이터에 대해서는 비밀소통용암호기를 통한 H/W적 암호화를 수행하고, 시스템에 보관 중인 음향데이터에 대해서는 S/W적 암호화를 수행한다. 특히 S/W적 암호화는 암호화에 사용되는 키를 음향데이터별로 시스템에서 생산하고 관리하여 본 시스템에서만 복호화가 가능함으로써 운용자의 불법적 복호화(다른 곳, 다른 장비에서의 복호화)를 방지한다.

④ 완전삭제 기법의 적용

본 시스템은 기능적 보안 차원으로 전송이 완료된 음향데이터에 대하여 자동으로 완전삭제를 수행한다. 완전삭제 방식은 마그네틱 디스크의 하드웨어적인 복구방식으로도 완벽한 안전을 위하여 35회 덮어쓰기 방식을 수행한다. 완전삭제 기법은 전송이 완료되거나 운용자가 삭제를 요청한 파일에 대하여 1차적인 덮어쓰기를 수행한 후, 시스템의 부하에 맞추어 나머지 34회의 덮어쓰기를 수행한다. 이때 덮어쓰는 블록의 크기와 블록의 내용은 모두 가변적으로 처리된다.

⑤ 이력 관리 기법의 적용

본 시스템은 관리적 보안 차원으로 음향데이터의 송·수신 및 자료 입·출력에 대한 이력을 관리한다. 이력은 자동으로 생성되며 시스템 관리자와 보안담당자에게만 접근이 허락되며, 위·변조방지를 위하여 각 이력에 대하여 Hash 함수를 적용하였다.

⑥ 시스템접근차단 기법 적용

본 시스템은 관리적 보안 차원으로 운용자의 시스템접근을 차단한다. 시스템의 운용프로그램 이외의 시스템 접근은 허락되지 않으며, 필요한 응용프로그램은 시스템의 운용소프트웨어가 자동으로 실행한다. 운용자의 시스템접근을 막기 위하여 전시되는 S/W는 응용프로그램이 유일하며, 각종 메뉴바의 접근을 차단하였고, 단축키에 의한 접근을 차단하였다. 시스템에 접근하는 유일한 방법은 정비자 계정으로 로그인한 후 은닉된 신원확인창을 통해 5단계의 암호화 인증방법을 거친 경우 허락된다. 5단계의 암호 키는 고정키와 가변키로 구분되어 있다.

⑦ 계층별 인증 및 접근 차별화 기법 적용

본 시스템은 관리적 보안 차원으로 시스템의 운용자는 일반운용자, 인증운용자, 시스템관리자, 정비자 등의 4개의 계층으로 구성되어 운용되며 각 계층별 권한은 다음의 표와 같다.

표 1. 계층별 접근 권한

계층	운용	전송	관리	시스템
일반운용자	O	X	X	X
인증운용자	O	O	X	X
시스템관리자	O	O	O	X
정비자	O	X	O	O

Ⅴ. 결 론

비보호 전송망에서 고용량의 음향데이터를 전송하는 본 시스템은 앞에서 제시한 전송측면의 설계 기법과 보안측면의 설계기법을 적용하여 구현하였다. 구현된 시스템은 국내에서 처음으로 (비보호 저속망에서의)보안측정 통과하여 현재 운용 중에 있다. 현재까지 운용에서 구현된 시스템은 비보호 저속망 환경에서도 안전하게 음향데이터를 전송하고 다양한 위협 요소로부터 안전하게 음향데이터를 보호함이 입증되었다.

참고문헌

[1] 한국정보보호센터, 정보보호개론, 교우사, 2000
[2] 국방부, 보안업무시행규칙, 국방부, 2001
[3] 정보보호실천협의회, 기업 정보보호 실천 가이드, 정보보호실천협의회, 2007
[4] 문은점,도경철,조창봉, 다중매체 DB 보안시스템 구축 개념 연구, 국방과학연구소, 2005
[5] 도경철,이상국,조창봉,조내현,선두영, 음향정보전송장비 설계서, 국방과학연구소, 2008