위성통신망 보안 구조에 관한 연구

(A Study on the Security Architecture in the Satellite Communication Network)

손태식°, 최홍민, 서정택*, 채송화, 유승화, 김동규

아주대학교 정보통신공학과, *국가보안기술연구소

{tsshon, partout, portula, swyoo, dkkim}@madang.ajou.ac.kr, *seojt@etri.re.kr

요 약

위성통신은 넓은 지역의 신뢰성 있는 광역 통신을 제공하기 위한 통신 기반이 되고 있다. 특히 기존의 통신망이 가지는 취약성이 존재할 수 있는 넓은 대지/산악지역에서는 위성통신이 거의 유일한 통신 수단으로서 중요한 정보전파의 해결 방안이 되고 있다. 향후 위성에 대한 의존도는 더욱 증대될 것이라는 사실은 자명한 사실이며, 위성통신망의 광역성 및 동보성으로 인한 보안 취약성을 해결하는 것이 시급한 문제이다. 본 논문에서는 위성통신망의 취약점을 파악하여, 보안 위협요소를 체계적으로 분석하며 보안 요구사항을 도출한 후에 도출된 보안 요구 사항을 ISO 정보 보안 관리 구조 표준에 기반하여 안전한 위성통신 보안망을 구축할 수 있는 구조를 제시한다.

I. 서 론

현재의 통신은 음성, 화상, 동영상 그리고 데이터 등의 모든 정보 요소를 다루며, 환경 역시 유/무선의 구분 없이 하나의 단일 망으로 묶여지는 추세이다. 그러므로 통신 환경의 변화 속에서 지상망과 위성망을 통합망 형태로 운영하여 현재의 통신수요 및 서비스를 충족시켜 나가고 있다. 특히 위성통신망은 정보전달, 감시자료의 배포, 조기경보, 전술/전략 통신지원을 목적으로 사용되는 장거리 대용량 위성통신을 지향하므로 통신 체계에 있어 위성통신에 대한 의존도는 날로 높아지고 있다. 하지만 위성통신망의 장점이라 할 수 있는 광역성 및 동보성으로 인해 생기는 취약성은, 통신 내용의 비밀 유지 및 고의적인 전파방해 등의 여러 보안상 문제점을 가지고 있어 시급히 해결해야 될 필요성이 있다.

본 논문에서는 위성통신망에 존재하는 보안 위협요소들을 위성과의 통신 데이터를 기반으로 Level-0, Level-1, Level-2 그리고 지상망 등으로 구분하여 체계적으로 분석한 후, 보안 요구사항들을 정보보안 측면과 신호보안 측면에서 도출한다. 또한 도출된 보안 요구 사항을 ISO의 정보 보호 관리 구조 표준에 기반하여 안전한 위성통신 보안 구조를 제시한다.

II. 위성통신망

1. 위성통신망 모델링

위성통신망은 정보저장 시스템, 위성통신 시스템, 호스트 컴퓨터, 위성관리 시스템, 단말 등으로 분류된다. 그러나 이러한 요소 외에 위협을 받는 대상을 그림1에 나타난 것처럼 유·무선 통신 환경 또한 고려해야 한다.

2. 위성통신망 Level 분류

위성통신망을 통신의 특성과 전송데이터를 기준으로 분류하였다. Level-0는 위성통신 전파신호 레벨이고, Level-1은 위성관제 데이터로 위성 제어에 필요한 데이터의 송수신 레벨이다. Level-2는 일반 응용 통신 데이터로 위성통신 기반에서 응용 통신수준의 데이터 송수신 레벨이다. 마지막으로 NCC(Network Control Center)와 SCC(Satellite Control Center)등의 지상망에 대한 보안 레벨로 구분을 하였다.

III. 위성통신망 위협요소 분석

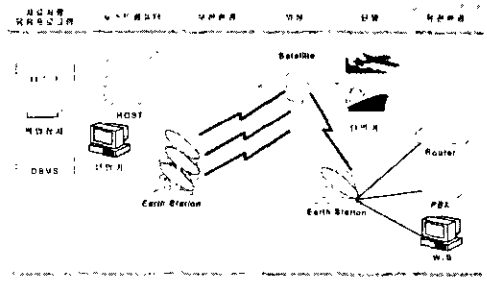

그림 1. 위성통신망 개체에 따른 분류

1. Level-0 위협요소 분석

높은 고도에서의 핵폭발은 대기권과 지구자기장의 변동 및 상호작용을 유발하여 광범위한 지역에 걸쳐 모든 통신수단을 방해할 수 있는 핵 방사 위협, 위성체나 SCC/NCC에 대한 전자기 펄스에 의한 영향이나 X선에 의한 내부적 전자파의 위협, 위성체에 대한 가능한 공격으로 레이저빔, 고출력 RF(Radio Frequency)빔 등과 같은 위성체나 비행체에 의한 직접 에너지 방사 공격과 같은 물리적 공격에 의한 위협, 전파 경로 탐지에 의한 위협, 위성체에 대한 링크에 고출력 RF신호를 방사하여 통신을 교란시키는 전자적 통신 방해에 대한 위협, 위성체의 하향 링크 용량의 제한으로 재밍 방지에 한계와 그리고 위성간의 통신 연결 이루어주는 NCC, SCC가 물리/논리적 공격에 의해 위성체간 연결확립 유지가 어려워질 수 등의 위협이 있다.

2. Level 1 & Level 2에서의 보안 위협 요소

통신상에서 전송 데이터 보호 기술의 부재로 인해 공격자로부터 전송 데이터의 재전송, 수정, 삭제, 분석등의 통신상의 위협, 전송장비 및 운용단말에 대한 주기적인 유지보수가 안 되는 경우, 불안전한 전원 사용, 전압 변화에 대한 민감성 문제 등의 위협 등이 존재한다.

3. 지상망에서의 보안 위협 요소

사용자 신분확인 및 인증 메커니즘의 부재, 보호되지 않는 패스워드 파일 등의 위협, 모뎀을 이용 전화선을 통한 인터넷 사용, 네트워크 접근통제 메커니즘의 부재 등의 위협, 네트워크

연결장치나 회선 포트 등의 방치, 네트워크 케이블의 외부노출 등의 위협, 데이터 저장 매체에 대한 데이터 무결성, 비밀성 메커니즘(암호화)의 부재 등의 위협, 사용자 부재 시 로그아웃을 안 하는 문제, 한 대의 컴퓨터를 다수 사용자가 공유하는 문제 등의 위협, 접근통제, 접근권한의 잘못된 할당, 감사기록 및 추적기능의 부재 등의 위협, 소프트웨어의 반입/반출 감시 기술 부재 등의 위협, 인터넷으로부터 소프트웨어 다운로드 및 사용 시 감염 및 침투 등의 위협, 호스트 컴퓨터에 대한 전자기 방사에 대한 민감성이나 전자기파 차단 메커니즘의 부재 등의 위협, 데이터 저장매체, 운용단말에 대한 주기적인 교환정책의 부족, 유지보수 작업의 부족 및 부적절, 통신 선로에 대한 전기적인 간섭 등의 위협 그리고 호스트 컴퓨터에 대한 부주의한 사용, 사용자의 보안인식 부족 및 불충분한 보안교육 등에서 유발하는 사용자의 실수와 컴퓨터의 부주의한 관리 및 운영, 효과적인 형상관리의 부재 등에서 발생하는 운영자의 실수 및 컴퓨터나 전송장비에 대한 물리적 보안장치의 부재, 보호되지 않은 저장소 등에 발생하는 물리/환경적 위협 요소가 있다.

Ⅳ. 위성통신망 보안 요구사항 및 관리 구조

위에서 분석된 위협요소를 기반으로 위성통신망의 정보보호 대상을 신호보안과 정보보안 단계로 구분한 후에 ISO 정보보호 관리구조를 적용하여 보안망 구축방안을 제시한다. 신호보안단계는 Level-0로서 위성전파신호의 보안이며, 정보보안단계는 Level-1, Level-2 그리고 지상망에 대한 단계로서 각각 위성 관제 데이터, 위성 통신 망 응용 데이터, 지상망 구성 요소 보안으로 구분한다.

ISO 정보보호 관리구조는 정상적인 통신의 정보 보호를 지원하고 제어하기 위해 필요하고, 분산 개방 시스템의 관리에 의해 요구되어지는 많은 정보보호 정책을 지원하는 표준이다. 정보보호 관리에는 정보보호 시스템 관리, 정보보호 서비스 관리 그리고 정보보호 메카니즘 관리가 있다.

정보보호 시스템 관리에는 전반적인 정보보호 정책 관리, 이벤트 핸들링, 보안 감사 데이터 관리, 복구 관리가 있으며, 정보보호 서비스 관리에는 정보보호 서비스 제공을 위한 정보보호 스킴의 결정과 할당, 적절한 메카니즘 선택을 위한 RULE 할당 및 유지가 있다. 정보보호 메카니즘 관리에는 키 관리, 암/복호화 관리, 전자서명 관리, 접근통제 관리, 무결성 관리, 당사자간의 프로토콜 관리, 인증 관리가 있다.

1. 신호보안 측면의 요구 사항

위성통신 시스템이 폭탄 및 테러와 같은 적의 공격이나 불법적인 해킹에 대하여 안전하여 언제나 위성통신 시스템을 이용하는 사용자에게 서비스를 제공할 수 있어야 하며, 재밍과 같은 전기적 전자기적 간섭을 이용한 공격에 대해서도 안전성을 유지하여야 한다. 또한 전송장비 및 운용단말에 대한 유지보수로 하드웨어 고장 및 오동작에 대처하며 전원장비에 대한 안정도를 높여야 한다.

2. 정보보안 측면의 요구사항

위성통신 시스템에 접속을 시도하는 대상이 사전에 허가된 대상인지를 확인하여 불법적인 대상으로부터 위성통신 시스템과 정보를 보호하여야 하고, 위성통신 시스템을 통하여 전송되는 데이터가 확인되지 않은 비인가된 대상에게 노출되지 않도록 보호되어야 하고, 위성통신 시스템을 통하여 송수신 되는 정보의 내용이 불법적으로 생성되거나 중간에 변경되거나 삭제되지 않도록 보호하고, 정보가 변조된 경우에는 이를 탐지 및 경고해야 하고, 원격지로부터의 데이터가 올바르게 전송된 것인지를 확인하는 방법으로서 위성통신 시스템을 통하여 송수신되는 정보는 반드시 확인된 발신처로부터 정확하게 전송되어야 하고, 위성통신 시스템에서 송/수신측이 통신에 참여했던 사실을 부인하지 못하도록 하는 방법으로서 통신 경로 및 행위 추적이 가능해야 하며, 위성통신 시스템에서 허가된 사용자에게만 접근을 허용하며, 접근이 허가된 사용자일지라도 허가된 범위 내에서만 정보 자원의 이용과 상호 통신이 가능하도록 한다.

V. 신호보안 관리구조

신호보안 시스템 관리에는 신호보안 시스템 요소 관리(위성 및 위성과의 통신대상의 물리적 관리)가 있으며, 신호보안 서비스 관리에는 전파의 가용성 보장 관리, 전파의 왜곡 방지 관리가 있고, 신호보안 메커니즘 관리에는 대역확산 메커니즘, 항재밍 메커니즘(안테나 널링기법, 부엽 제거기등)이 있다.

신호보안 대상의 취약점으로는 위성통신망 시스템 보안 취약성, 위성 통신 시스템에 대한 물리적 공격에 대한 위협, 핵 방사 위협, 전자적 방해 위협 등이 있다. 보안대책으로는 물리적 공격에 대비한 탐지율 저하 기법 연구(LPI, LPD등), 시스템 자체의 Fault-Tolerance 능력 향상, 대역확산기법을 이용한 전파의 기밀성 유지 등이 있다.

VI. 정보보안 관리구조

정보보안 시스템 관리에는 다단계 정보보안 정책 설정 및 관리, 정보보안 시스템 요소 관리, NCC&SCC 탑재 통합정보보호 엔진, 정보보호솔루션 그리고 위성 및 단말 탑재 정보보호 모듈이 있으며, 정보보안 서비스 관리에는 사용자 신분확인, 인증 및 접근 제어, 기밀성 및 무결성 유지 및 보장, 부인 방지등이 있고, 정보보안 메커니즘 관리에는 암호화, 전자서명, 접근통제 메커니즘 그리고 데이터 무결성 메커니즘 등이 있다.

위에서 분류한 관리 대상을 다시 지상망 보안, 외/내부 네트웍 보안, 위성통신 시스템 보안 그리고 위성통신 데이터 보안으로 나누어 취약점 및 보안 대책을 강구한다.

외부 네트웍에 연결되어있는 지상망 보안의 경우 비 인가된 인원의 접근 가능, 네트워크 침입으로 인한 시스템 자원에 대한 정보의 유출, 도용 및 파괴 등이 있으며, 보안대책으로는 F/W(FireWall), VPN(Vitual Private Network)설치 그리고 네트웍 접근제어 정책 구현이 있다.

[illegible]		
◆ [illegible]	• 패킷필터링	• TCP/IP Level 에서 송발지, 도착지 주소, 서비스 port 기반 filtering 지원
◆ 네트워크 인터페이스	• 다중 인터페이스	• 3개 이상의 인터페이스 구성 가능.
	• [illegible]	• [illegible]
◆ 접근 제어	• 접근 제어 기능	• 서비스별, 사용자별, 시간대별 접근제어 설정 가능.
◆ 실시간 모니터링	• 보안위반사항 통보	• 보안 위반사항의 사용자 경고 및 실시간 통보(PCS, Beeper, E-mail 등)
◆ [illegible]	• [illegible]	• [illegible]
◆ 해킹방어	• 해킹방어 기능	• IP, DNS Spoofing, ICMP Attack 등에 대한 방어 기능.
◆ Performance	• Performance	• 1 Gbps 처리속도 지원 가능 및 NAT 기능 지원(Hardware type 경우)
◆ 이중화 구성	• 이중화 구성	• Primary/Secondary 구성 가능성, 실제 system takeover 신속성.
◆ VPN	• VPN 기능 지원	• IPSec, DES, triple-DES 등 다양한 암호화 알고리즘 지원 가능.
◆ [illegible]	• [illegible]	• [illegible]

표1. Firewall 요구사항

[illegible]		
◆ [illegible]	• 패킷필터링	• TCP/IP Level 에서 송발지, 도착지 주소, 서비스 port 기반 filtering 지원
◆ 네트워크 인터페이스	• 다중 인터페이스	• 3개 이상의 인터페이스 구성 가능.
	• ATM, Ethernet 지원	• ATM, Giga 및 100 base Ethernet 지원 가능.
◆ 접근 제어	• 접근 제어 기능	• 서비스별, 사용자별, 시간대별 접근제어 설정 가능.
◆ [illegible]	• [illegible]	• [illegible]
◆ 프록시	• 다양한 프록시 제공	• 중요한 서비스(http, telnet, FTP, SMTP, POP3 등)에 대한 프록시.
◆ 해킹방어	• 해킹방어 기능	• IP, DNS Spoofing, ICMP Attack 등에 대한 방어 기능.
◆ Performance	• Performance	• 1 Gbps 처리속도 지원 가능 및 NAT 기능 지원(Hardware type 경우)
◆ 이중화 구성	• 이중화 구성	• Primary/Secondary 구성 가능성, 실제 system takeover 신속성.
◆ [illegible]	• [illegible]	• [illegible]
◆ reference site	• reference site	• reference site 의 종류, 수 및 납품 실적

표2. VPN 요구사항

내/외부 네트웍에 연결되어 있는 경우 F/W을 통과한 해커에 의한 내부 네트워크 시스템 자원에 대한 손상, 내부자에 의한 시스템 자원 피해 등을 들 수 있으며 보안대책으로는 내부 네트워크 및 호스트에 대한 실시간 침입 탐지, 보고 및 대응 시스템 장착이 있다.

아키텍처	• 상호간 연동	• 네트워크기반과 호스트기반 침입탐지장치의 상호 연동 기능.
인터페이스	• 지원 네트워크	• 다양한 형태의 네트워크 지원(Fase/Giga Ethernet, ATM 등).
	• 네트워크 부하	• 네트워크 성능 저하를 시키지 않고 작동.
OS 인터페이스	• 지원가능 OS	• OS 별(Unix, Linux, Netware, NT, Windows98/2000) 가능.
실시간 모니터링	• Active 세션 모니터링	• 실시간 네트워크 모니터링 및 오픈 TCP/IP 프로토콜 지원 기능.
	• 침입탐지 실시간 경보	• 침입탐지 또는 보안문제 발생시 다양한 형태(HP, 경고음, 메일) 실시간 경보
	• 침입자 공격 차단 기능	• 세션종료, 방화벽 재설정 등 네트워크 공격에 대한 차단 기능.
	• 중요시스템 파일 변동	• 네트워크 상의 주요 시스템(DNS, Web, FTP 등) 파일 변경 탐지 기능.
	• 내·외부 공격 탐지	• 실시간 내·외부 공격에 대한 탐지 기능
접근제어	• 접근제어 기능	• 서비스별, 사건대별 접근 제한 여부.
관리	• 다양한 리포팅 기능	• 로그 분석, 로그 재생, 다양한 리포팅 및 도움말 기능.

표3. IDS(Intrusion Detection System) 요구사항

위성통신망 시스템 구성 요소에 대해서 DMZ(DeMilitarized Zone) 내의 개방형 전산 자원에 대한 외부의 사용자 또는 내부 사용자가 인가하지 않은 자원에 대한 접근 등의 취약점이 있다. 보안대책으로는 관리자가 인가하지 않은 DMZ내의 자원에 대해서는 접근할 수 없도록 통제하는 보안 솔루션 적용이 있으며 이때 강력한 인증 및 접근제어가 가능한 통합정보보호엔진이 필요하다.

침입탐지 아키텍처	• 상호간 연동	• 네트워크기반과 호스트기반 침입탐지장치의 상호 연동 기능.
네트워크 인터페이스	• 지원 네트워크	• 다양한 형태의 네트워크 지원(Fase/Giga Ethernet, ATM 등).
	• 네트워크 부하	• 네트워크 성능 저하를 시키지 않고 작동.
OS 인터페이스	• 지원가능OS	• OS 별(Unix, Linux, Netware, NT, Windows98/2000) 가능.
실시간 모니터링	• Active 세션 모니터링	• 실시간 네트워크 모니터링 및 오픈 TCP/IP 프로토콜 지원 기능.
	• 침입탐지 실시간 경보	• 침입탐지 또는 보안문제 발생시 다양한 형태(HP, 경고음, 메일) 실시간 경보
	• 침입자 공격 차단 기능	• 세션종료, 방화벽 재설정 등 네트워크 공격에 대한 차단 기능.
	• 중요시스템 파일 변동	• 네트워크 상의 주요 시스템(DNS, Web, FTP 등) 파일 변경 탐지 기능.
	• 내·외부 공격 탐지	• 실시간 내·외부 공격에 대한 탐지 기능
접근제어	• 접근제어 기능	• 서비스별, 사건대별 접근 제한 여부.
관리	• 다양한 리포팅 기능	• 로그 분석, 로그 재생, 다양한 리포팅 및 도움말 기능.

표4. 시스템 보안 요구사항

위성통신망 데이터 보안에 있어서는 정보의 누설, 정보의 불법 변조, 정보의 발신/수신 부인, 데이터 해킹 후 위/변조 발생 그리고 내부 사용자들의 데이터 변조 등이 있다. 보안대책으로는 인증 및 암호화 솔루션의 장착 및 통합정보보호엔진을 통해 자원을 보호하는 방안을 적용할 수 있다.

침입탐지 아키텍처	• 상호간 연동	• 네트워크기반과 호스트기반 침입탐지장치의 상호 연동 기능.
네트워크 인터페이스	• 지원 네트워크	• 다양한 형태의 네트워크 지원(Fase/Giga Ethernet, ATM 등).
	• 네트워크 부하	• 네트워크 성능 저하를 시키지 않고 작동.
OS 인터페이스	• 지원가능OS	• OS 별(Unix, Linux, Netware, NT, Windows98/2000) 가능.
실시간 모니터링	• Active 세션 모니터링	• 실시간 네트워크 모니터링 및 오픈 TCP/IP 프로토콜 지원 기능.
	• 침입탐지 실시간 경보	• 침입탐지 또는 보안문제 발생시 다양한 형태(HP, 경고음, 메일) 실시간 경보
	• 침입자 공격 차단 기능	• 세션종료, 방화벽 재설정 등 네트워크 공격에 대한 차단 기능.
	• 중요시스템 파일 변동	• 네트워크 상의 주요 시스템(DNS, Web, FTP 등) 파일 변경 탐지 기능.
	• 내·외부 공격 탐지	• 실시간 내·외부 공격에 대한 탐지 기능
접근제어	• 접근제어 기능	• 서비스별, 사건대별 접근 제한 여부.
관리	• 다양한 리포팅 기능	• 로그 분석, 로그 재생, 다양한 리포팅 및 도움말 기능.

표5. 데이터 보안 요구사항

위에서 위성통신망 시스템 보안과 데이터 보안을 위한 보안 대책으로 통합정보보호엔진의 필요성이 대두되었는데, 통합정보보호 엔진은 대칭키/비대칭키 암호 기법, 단일 사인-온, 접근제어 기술, 인증 메커니즘 그리고 데이터의 기밀성과 무결성을 제공하는 데 필요한 키 분배 기능 등을 제공한다.

위성통신망에서의 통합정보보호엔진이 탑재된다면 정보보호 서비스 중에서도 위성통신망 구성 요소에 대한 인증기능 제공, 인증 및 데이터 전송에 필요한 키 생성 및 분배 기능 제공 그리고 1:N, N:N 통신을 위한 키분배 방법 등을 고려하여 부하가 적고 효과적인 인증, 키 분배 방법을 선택해야 된다. 또한 그 외 접근제어나 부인방지기능 등의 고려가 필요하다. 탑재 위치로는 NCC내에 탑재되어 일반 정보보호 솔루션과 함께 종합적인 보안 관리가 이루지게 해야 한다.

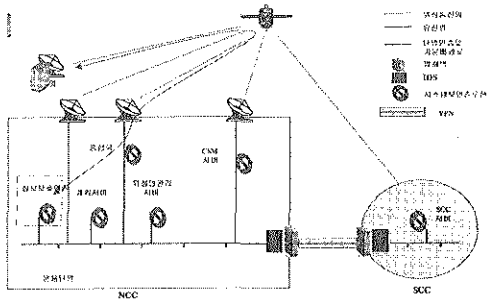

그림 2. 제안하는 위성통신망 보안 구조

VII. 결론

본 논문에서는 위성통신망에서의 보안 위협요소를 위성통신의 특성과 전송 데이터에 따라 3가지 레벨로 나누어 분석하였다. 그 다음 분석된 위협 요소들로부터 보안 요구사항을 ISO 정보보호 관리구조에 기반 하여 정보보안 측면과 신호보안 측면으로 분류한 후, 각각에 대한 보안 대책을 세워 종합적인 위성통신 보안망 구조를 제시하였다. 기존에 활용되고있는 대응 방안들은 신호보안 측면의 보안요소들이 대부분이었다. 하지만 신호보안 관리만으로 안전한 위성통신을 보장할 수 없으므로 정보보안 측면에서의 보안을 통해서 신호보안의 취약성 보완 및 총체적인 위성통신망 보안이 가능하게 된다. 따라서 신호보안 및 정보보안 관리구조에 따라 지상망에서의 통신에서는 IDS, F/W, VPN 등의 정보보호 솔루션의 장착을 제안하며, 위성과의 통신 보안에는 인증 및 키관리와 더 나아가 접근제어 등의 정보보호 서비스를 제공할 수 있는 통합정보보호엔진의 장착을 제안하였다. 향후에는 위성통신망의 특성에 따른 정책 기반의 보안망 구축 방안 제시 및 위성 통신에 최적화된 통합 정보보호엔진 장착시 고려 사항에 대한 연구가 필요하다.

참고문헌

[1]김동규외, "군 위성통신망 보안 위협요소 분석 및 보안망 구축방안연구", 제4차 통신/전자학술대회, ADD, 2000.10

[2]김동규외, " 위성통신망을 위한 보안 프레임워크에 관한 연구 ", 춘계종합학술발표논문집, 한국정보과학회, 2000.4.

[3]홍기융외, " 메세지 인증코드 기법을 이용한 위성명령 보안 메커니즘 설계 ", 종합학술발표회논문지, 한국통신정보보호학회, 1994.11.

[4]김동규외, 분산통신망 환경 통합 정보보호 소프트웨어기술, 3 차년도 보고서, 정보통신부, 1999.01

[5]Sead Muftio, " Security Architecture for Open Distributed Systems", British Libarary