情報保護學會論文誌
第11券 第4號, 2001. 8

위성 통신망 보안 위협요소 분석 및 보안망 구조에 관한 연구

손 태 식*, 최 홍 민*, 채 송 화*, 서 정 택**, 유 승 화***, 김 동 규***

A Study on Security Threat Elements Analysis and Security Architecture in Satellite Communication Network

Tae-Shik Shon*, Hong-Min Choi*, Song-Wha Chae*
Jung-Taek Seo**, Seung-Wha Yoo***, Dong-Kyu Kim***

요 약

본 논문에서는 위성통신망의 보안 위협요소를 위성통신망의 특성과 데이터를 바탕으로 Level-0(위성 전파 신호), Level-1(위성 관제 데이터), Level-2(위성 응용 데이터) 그리고 지상망 보안 단계로 분류한다. 그리고 각 보안 단계에 대한 위협 요소를 분석한다. 그 후 도출된 위성통신망 보안 위협요소에 대한 보안 요구 사항을 신호보안과 정보보안 레벨로 나누고, 이를 근거로 기존의 신호보안 수준의 대응방안에서 벗어나 위성통신 네트워크 보안, 위성통신망 시스템 보안, 위성통신망 데이터 보안등의 정보보안 레벨에서 정보보호 정책을 통한 위성통신망 보안 위협요소 대응방안을 수립한다. 이와 같은 정보보호 정책 기반의 대응방안을 통해 본 논문에서는 안전한 위성통신망 보안 구조를 제안한다.

ABSTRACT

In this paper we classify security threat elements of satellite communication into four parts; Level-0(satellite propagation signal), Level-1(satellite control data), Level-2(satellite application data) and ground network security level according to the personality and data of the satellite communication network. And we analyze each security levels. Using analyzed security threat elements, we divide security requirements into signal security level and information security level separately. And then above the existent signal security level countermeasure, we establish the countermeasure on the basis of information security policy such as satellite network security policy, satellite system security policy and satellite data security policy in information security level. In this paper we propose secure satellite communication network through the countermeasure based on information security policy.

keyword : *satellite security, satellite security threat, information policy , satellite security architecture*

Ⅰ. 서 론

급격한 통신 기술의 발전으로 사용자들은 고속, 광대역, 멀티미디어, 그리고 이동성 등이 지원되는 고품질 정보통신 서비스를 요구하고 있으며, 이러한 수요를 만족시키기 위해 지상 통신망과 위성 통신망

* 아주대학교 정보통신공학과 정보통신 및 시큐리티 연구실
** 한국전자통신연구원 부설 국가보안기술연구소
*** 아주대학교 정보통신공학과 교수

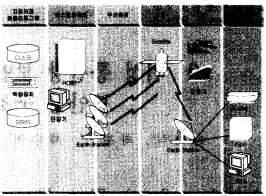
을 하나의 통합망 형태로 운영하는 방식이 사용되고 있다. 여기서 위성통신망은 장거리 대용량 통신시스템으로서 정지궤도위성을 이용하는 경우 1기의 위성으로 최대 지구 전역의 1/3을 통신 영역으로 가질 수 있고, 넓은 지역에 분포된 수신자들에게 동일한 내용의 정보를 동시에 전달 가능하며, 지형적인 영향 등으로 지상통신망을 구성하기 어려운 지역이나 긴급 상황에서 이동 지구국을 통하여 신속하게 통신망을 구성하는 것이 가능하다는 장점을 지니고 있으므로 현재 정보통신망에 있어 그 의존도는 날로 높아지고 있다. 그러나 위성통신망은 위성통신망의 장점이라 할 수 있는 광역성 및 동보성으로 인해 위성에서 송신한 신호를 누구나 수신 가능하다는 위험성을 내포하고 있으므로 통신 내용의 비밀 유지가 어렵고, 고의적인 전파방해에 대하여 취약성을 가지는 것과 같은 보안상의 문제를 지니고 있다.

따라서 본 논문에서는 위성통신망에 존재하는 보안 위협요소들을 Level-0(위성 전파 신호), Level-1(위성 관제 데이터), Level-2(위성 응용 데이터) 그리고 지상망 단계로 구분하여 위성통신망에 존재하는 보안 위협 요소를 분석하고, 그에 따른 보안 요구 사항을 도출한다. 그 후 위성통신망 취약성에 대한 대응 방안으로 기존의 위성전파 측면에 대한 신호 보안 수준의 대응방안을 살펴보고, 정보보안 측면에서의 보다 적극적인 대응 방안으로 위성통신 네트워크 보안, 위성통신 시스템 보안, 위성통신 데이터 보안의 3가지 정보보호 정책을 기반으로 안전한 위성통신 보안망 구조를 제안한다.

Ⅱ. 위성 통신망 개요

2.1 위성통신망 구성 요소

일반적으로 위성통신망은 위성 관제 센터(SCC, Satellite Control Center), 위성 망관리 센터(NCC, Network Control Center), 위성 통신 시스템, (Satellite Communication System), 위성통신 데이터를 처리하는 호스트 컴퓨터, 위성통신 데이터 저장장치, 위성통신 단말기(Terminal) 등으로 분류된다. 또한 구성요소 이외의 측면에서 보면 [그림 1]과 같이 유·무선 네트워크 환경을 추가할 수 있다. 본 논문에서는 앞서 열거한 것과 같은 위성통신망의 모든 구성요소들을 포함하여 위성통신망에 존재하는 가능한 모든 보안 위협 요소들을 분석한다.



[그림 1] 위성통신망 개체에 따른 분류

2.2 위성통신망 보안 레벨 분류

본 논문에서는 위성통신망 보안 위협요소 분석을 위한 보안 레벨을 위성통신망의 특성과 전송시 사용되는 데이터를 바탕으로 Level-0, Level-1, Level-2 그리고 지상망의 4가지 레벨로 분류한다. Level-0는 위성통신에 있어서 위성과 지상망 또는 위성과 단말 등이 상호 주고받는 전파신호에 대한 보안 레벨, Level-1은 SCC에서 위성 제어시 사용하는 위성 관제 데이터에 대한 보안 레벨, Level-2는 일반 위성 응용 통신 데이터로서 위성통신에서 사용하는 일반 데이터에 대한 보안 레벨로 분류하고, 그 외 NCC나 SCC 등 지상 네트워크 관련 구성요소들에 대한 지상망에서의 보안 레벨을 지상망 레벨로 구분한다.

이러한 4단계의 위성통신망 보안 레벨 분류를 통해 기존의 물리적 레벨 단계의 위성 전파 신호나 위성 시스템 자체에 대한 보안 위협요소의 분석을 넘어서 물리적 레벨 이상의 포괄적인 범위에서 존재 가능한 위성통신망 보안 위협요소에 대하여 분석한다.

Ⅲ. 위성통신망 보안 위협요소 분석

위성은 쏘아 올린 후, 사람에 의한 직접적인 접근 제어가 불가능하기 때문에 위성의 동작 상태, 자세 및 위치 등의 제어 명령을 원격지에서 명령 신호를 보내어 해결해야만 한다. 즉 위성의 위치, 성능 및 동작을 제어하는 명령 신호의 노출에 대한 위험과 인가되지 않은 사용자에 의한 불법적인 사용에 대한 위험이 항상 존재하고 있으므로, 위성을 제어하는

명령 신호에 대한 인증 기법의 안전성이 확보되어야 한다. 그러므로 위성은 수신되는 명령어 신호가 진정한 권한이 있는 한가닥 사용자로부터 송신된 것인가에 대한 인증 방법이 필요하며, 또한 신호 자체에 대한 보안과 신호가 담고 있는 정보에 대한 보안 역시 요구된다. 이렇듯 위성에 관한 위협요소는 위성 전파신호 그 자체 및 위성 통제신호와 일반 위성 응용데이터 그리고 지상망간의 통신 등에 광범위하게 존재하게 된다.

따라서 본 논문에서 위성에 대한 보안 위협요소를 앞서 서술된 것과 같이 위성통신망의 특성과 전송 데이터를 기반으로 하여 분류한 4가지 레벨에 따라 분석한다.

3.1 Level-0 보안 위협 요소 분석

3.1.1 핵 방사에 의한 위협

높은 고도에서의 핵폭발은 대기권과 지구자기장의 변동 및 상호작용을 유발하여 광범위한 지역에 걸쳐 모든 통신수단을 방해할 수 있는 원인을 제공한다. 또한 위성체에 대한 전자기 펄스에 의한 영향이나 X선에 의한 내부적 EMP(ElectroMagnetic Pulse) 발생이 있을 수 있다.

3.1.2 물리적 공격에 의한 위협

위성체에 대한 공격으로 레이저빔, 입자빔, 고출력 RF(Radio Frequency)빔과 같은 위성체, 비행체에 의한 직접 에너지 방사 공격과, 그리고 미사일, 로켓과 같은 지상에서의 위성 공격용 무기류 이용한 공격 등이 있다.

3.1.3 전파 경로 탑지에 의한 위협

위성체 및 단말의 위치가 노출될 경우 물리적 공격이 가능하고, 전파경로에 대한 기밀 통신 유지가 어려워지며, 공격자가 링크상의 신호 정보를 획득하여 재밍(Jamming)과 같은 공격을 할 수 있다.

3.1.4 전자적 통신 방해에 의한 위협

위성체에 대한 상향링크에 고출력 RF 신호를 방사하여 위성통신망을 교란시키거나 위성해나 위성통신경로에 대한 전자적 통신 방해가 가능하다. 또한 전파경로 링크상에서 신호를 가로채 통신을 교란시키는 스푸핑이 가능해진다.[1,2]

3.2 Level-1 보안 위협요소 분석

3.2.1 위성 제어 정보 불법 변조에 대한 위협

원격지로부터 위성 제어 정보에 대한 전송 과정 중 위성의 위치, 성능 및 동작을 제어 할 수 있는 제어 정보에 대한 불법적 위조나 변조가 가능하다.

3.2.2 위성 제어 정보 노출에 대한 위협

위성 제어 정보가 노출되어 잘못된 제어 정보가 위성에 전달되거나 제어정보의 전달을 방해하는 등의 위협요소가 존재 한다.

3.2.3 위성 제어 채널 용량 부족에 대한 위협

위성통신망 관리의 미숙이나 위성 제어 채널 용량 부족으로 인해 전송 제어정보 트래픽이 과부하를 일으킬 수 있는 위협이 존재한다.

3.2.4 비인가된 사용자의 위성제어에 대한 위협

적절한 방법을 통해 위성체에 대한 인증과정을 거치지 않고, 불법적인 방법을 통해 위성에 접속한 비인가 사용자가 위성에 잘못된 위성제어 명령을 수행하는 위협요소가 존재한다.

3.3. Level-2 보안 위협 요소 분석

3.3.1 위성 응용 데이터 불법 변조에 대한 위협

위성 통신 과정에서 전송 데이터에 대한 보호 기법의 부재로 인해 공격자로부터 전송 데이터의 수정, 삭제, 분석이 가능하다.

3.3.2 위성 응용 데이터 노출에 대한 위협

위성 응용 데이터가 악의의 목적을 가진 사람에게 노출되는 경우에 노출 정보의 악의적 이용이나 잘못된 정보를 이용한 개인이나 단체에 있어 직접적인 피해를 입히는 것과 같은 결과를 초래 할 수 있다.

3.3.3 위성 응용 데이터 채널 용량 부족에 대한 위협

부적절한 위성통신망 관리나 위성 채널 용량부족으로 인해 전송 트래픽의 과부하가 발생할 수 있으며, 병목지점에서 오류가 발생 할 수 있다.

3.4 Level-0,1,2 공통 보안 위협요소 분석

3.4.1 위성통신 시스템에 대한 위협

위성안테나, 교환기와 같은 전송장비의 파괴나 고

장으로 인한 전송 라인의 손상도 취약성이 된다.

3.4.2 위성통신 시스템의 기술적 오류

전송장비 및 운용단말에 대한 주기적인 유지보수가 안 되는 경우, 불안전한 전원 사용, 전압 변화에 대한 민감성 문제 등도 취약성이 된다.

3.4.3 위성체 시스템 성능에 의한 위협

위성체에서의 링크 용량의 제한으로 재밍 방지에 한계점이 있고, SCC나 NCC의 위성 수신안테나 이득 문제가 발생 가능하다. 위성 통신 시스템의 보안 기법의 복잡로 인해 경로상의 기밀성 유지가 어렵다.

3.5 지상망에서의 보안 위협 요소

3.5.1 사용자 신분 위장

사용자 신분확인 및 인증 기법의 부재, 보호되지 않는 패스워드 파일, 로그인 절차 무시 등의 위협이 존재한다.

3.5.2 비인가자에 의한 네트워크 접근

네트워크 접근통제 기법의 부재, IP/DNS(Internet Protocol/Domain Name Service) 스푸핑(Spoofing)이 가능, TCP/IP와 같은 네트워크 프로토콜에 대한 버그들, 가상네트워크 사용시 부적절한 네트워크 관리, 네트워크 트래픽 감시/분석 메커니즘의 부재 등의 위협 요소를 가진다.

3.5.3 비인가된 방식에 의한 네트워크 이용

네트워크 연결장치나 회선 포트 등의 방치, 네트워크 통신장비 및 시스템의 원격관리기능의 악용, 네트워크 유지 보수자에 의한 정보유출 및 악의적 행위 등이 위협 요소로 존재한다.

3.5.4 저장매체에 대한 비인가된 접근

데이터 저장 매체에 대한 데이터 무결성, 비밀성 메커니즘의 부재, 저장매체에 대한 부적절한 라벨 부착, 저장매체에 대한 완전한 내용 삭제 없이 파기 및 재사용 등이 취약성이다.

3.5.5 비인가된 방법에 의한 S/W 사용

접근통제 메커니즘의 부재, 접근권한의 잘못된 할당, 감사기록 및 추적기능의 부재, 유지보수중의 고의적인 행위 등이 취약성이다.

3.5.6 악성 S/W 사용에 의한 위협 요소

인터넷으로부터 소프트웨어 다운로드 및 사용 시 감염 및 침투, 메일폭탄 및 논리폭탄, 불법적인 소프트웨어의 반입 등이 취약성이다.

3.5.7 기술적 오류

데이터 저장매체, 하드웨어 전송장비 및 운용단말에 대한 주기적인 교환정책의 부족, 유지보수 작업의 부족 및 부적절 등이 하드웨어 고장 및 오동작을 유발할 수 있다. 소프트웨어 역시 불완전한 개발사양과 효과적인 형상관리의 부재, 물명확한 제품설치 및 사용자 매뉴얼 등이 취약성이다.

3.6 그 외의 보안 위협 요소

위에서 분석한 위성통신망 보안 위협 요소 외에 고려할 수 있는 위협 요소는 사용자 및 운영자의 실수에 의한 위협과 물리적/환경적 요인에 의한 위협 요소가 있다.

Ⅳ. 위성통신망 보안 요구 사항

위성통신망에서의 보안 요구 사항을 앞서 분류한 보안 위협요소 레벨에 따라 분석하면, 위성 전파 신호에 대한 물리적 위협요소부터 지상망 구성 요소들 간 상호 교환하는 정보에 대한 위협요소에 이르기까지 다양하게 존재한다는 것을 알 수 있다. 하지만 위성통신망 위협요소에 대한 대응방안으로 현재 고려되고 있는 것들은 대부분이 위성 전파신호 레벨(Level-0)에 대한 대응방안으로서 신호 레벨의 전파와 위성통신 시스템에 대한 위협에 해당한다. 하지만 현재 위성통신망에 대한 위협은 정보 기술의 발달과 함께 신호 레벨에 대한 위협을 넘어서 위성통신망에서 사용되는 정보에 대한 정보 보안 수준의 위협으로 올라가고 있다.

또한 위성통신망의 보안 요구 사항을 보안 위협요소의 측면이 아닌 위성통신망에서 사용되는 프로토콜의 측면에서 분석하면, 정보보호를 위한 위성과의 통신은 기존 단말기에서 사용하는 통신 프로토콜의 수정 없이 사용될 수 있어야 하고, 다른 통신망과 연결하여 사용할 수 있는 적응성을 가져야 하므로 OSI(Open Systems Interconnection) 모델에

준하여 구현되어야 한다. ISO(Internation Standard Organization) 7498-2 정보보호 관리 구조 표준에서는 패킷 교환망과 광역통신망을 기준으로 제공할 수 있는 정보보호 서비스들을 계층별로 정의하고 있다. 하지만 일반적으로 데이터 링크 계층에서 제공되는 접속 및 비 접속 비밀 보장 서비스로는 위성 통신망에서의 링크 상에서 발생할 수 있는 데이터 변경의 위협, 비 인가자의 접근에 의한 정보노출의 위협, 비 인가자가 정당한 통신상대로 가장 가능성에 대한 위협, 그리고 비 인가자에 의한 자원 이용에 대한 위협 등에 대해서 완전한 보안 대응책을 마련해줄 수 없다.[7,8]

따라서 앞서 연구된 위성통신망 위협요소 분석에 의한 결과처럼 위성통신망에서 사용되는 프로토콜의 측면에서도 역시 무결성, 비밀보장, 신분확인, 접근제어 등의 정보보호 서비스를 제공할 수 있는 상위 레벨에서의 정보보호 정책에 기반한 적극적 대응 방안이 요구되며, 이에 따라 본 논문에서는 위성 통신망의 보안 위협요소를 분류하기 위해 나누었던 4단계의 위성통신망 보안 레벨을 위성 전파 신호의 보안인 신호 보안 레벨(Level-0)과 정보보호 수준에서 보다 적극적인 대응방안을 마련할 수 있는 보안 개념을 바탕으로 위성 관련 데이터에 대한 Level-1, 2와 지상망 레벨을 함께 묶어 정보보안 단계로서 분류하여 위성 통신망 보안 요구 사항을 도출한다.

위와 같이 보안 요구 사항을 분류함으로써, 기존의 재밍 방지 기법 및 전자파 방해에 대한 생존 기법, 인터셉터로부터 회피 기법 등과 같은 소극적 대응이 대부분이었던 신호 보안 측면의 위성통신망 보안 위협 대응방안에서 벗어나 위성 관련 정보(데이터) 레벨에서 정보보호 정책을 기반으로한 사용자 인증, 접근제어, 기밀 통신 보장 등 적극적인 대응방안의 바탕을 마련한다.

4.1 신호보안 수준의 보안 요구사항

4.1.1 위성통신망의 가용성 향상

언제나 위성통신 시스템을 이용하는 정당한 사용자에게 위성통신 시스템이 폭탄 및 테러와 같은 적의 공격이나 불법적인 해킹에 대하여 안전하게 모든 서비스를 제공할 수 있어야 한다.

4.1.2 위성통신망 신호 왜곡 방지

재밍과 같은 전기적 전자기적 간섭을 이용한 공격에 대해서도 안전성을 유지하여야 한다.

4.1.3 위성통신 시스템의 기술적 안정

전송장비 및 운용단말에 대한 유지보수로 하드웨어 고장 및 오동작에 대처하여야 하며 전원장비에 대한 안정도를 높여야 한다.

4.2 정보보안 수준의 보안 요구사항

4.2.1 사용자 신분 확인 및 인증

위성통신 시스템에 접속을 시도하는 대상이 사전에 허가된 대상인지를 확인하여 불법적인 대상으로부터 위성통신 시스템과 정보를 보호하여야 한다.

4.2.2 비밀성 유지 및 보장

위성통신 시스템을 통하여 전송되는 데이터가 확인되지 않은 비인가 대상에게 노출되지 않도록 보호되어야 한다.

4.2.3 무결성 유지 및 보장

위성통신 시스템을 통하여 송수신 되는 정보의 내용이 불법적으로 생성되거나 중간에 변경되거나 삭제되지 않도록 보호하고, 정보가 변조된 경우에는 이를 탐지해 내고, 정당한 사용자에게 경고해 주어야 한다.

4.2.4 데이터 발신처 확인

원격지로부터 전송 받은 데이터가 원하는 곳으로부터 올바르게 전송된 것인지를 확인하는 방법으로서 위성통신 시스템을 통하여 송수신 되는 정보는 반드시 확인된 발신처로부터 정확하게 전송되어야 한다.

4.2.5 통신 사실의 부인 방지

위성통신 시스템에서 송신측과 수신측이 통신에 참여했던 사실을 부인하지 못하도록 하는 방법으로서 통신 경로 및 행위 추적이 가능해야 한다.

4.2.6 인가된 접근 허용

위성통신 시스템에서 허가된 사용자에게만 접근을 허용하며, 접근이 허가된 사용자일지라도 허가된 범위 내에서만 정보 자원의 이용과 상호 통신이 가능하도록 한다.

V. 기존의 신호 보안 측면 대응방안

지금까지 연구되고 있는 신호 보안 측면의 대응방안으로는 위성 전파 경로의 위협에 대한 확산 대역

방식의 사용이나 전파 경로 탐지에 대한 탐지율 저하 기법에 대한 연구 그리고 전자적 위성 통신 방해에 대한 항 재밍 기법 등이 있다.

5.1 대역 확산 통신(Spread Spectrum Communication)

대역 확산 통신 방식은 일차적인 재밍 방지 대책으로서 NATO 3, 영국의 SKYNET, 프랑스의 SYRACUSE, 미국의 DSCS III, MILSTAR등 대부분의 위성통신 시스템에서 도입하여 사용하고 있는 방식이다. 이러한 대역확산방식으로 크게 직접확산(DS, Direct Spectrum) 방식과 주파수 도약(FH, Frequency Hopping)방식으로 나뉜다.

직접확산 방식은 다중접속의 목적으로 사용될 수 있고 전송되는 신호레벨이 낮아 탐지를 회피할 수 있는 LPI(Low Probability of Interception), LPD(Low Probability of Detection) 기능면에서도 유리하나 기술적으로 구현 가능한 확산 대역폭의 제한이라는 단점을 가지고 있다.

주파수 도약 방식은 오랜 동안 군에서 주된 통신 방식의 하나로 사용되어 오고 있는 기술로 입력 데이터에 의해 변조된 반송파의 스펙트럼을 넓히기 위하여 주기적으로 반송파의 주파수를 바꾸어주는 것이다. 일반적으로 2^k개의 주파수가 입력 데이터의 대역폭 정도의 간격으로 배열되어 반송파를 대역 확산한다. 수신 단에서는 송신 단에서 사용한 것과 같은 PN(Pseudo Noise) 코드를 사용하여 역 확산을 행한다.[2]

5.2 LPI(Low Probability of Intercept)

인터셉터에 대한 위협은 크게 두 가지로 분류할 수 있다. 첫 번째는 위성단말 신호의 존재를 검출하여 위치를 확인한 후 물리적 공격에 의해 지상단말을 파괴하려는 의도이고, 두 번째는 검출된 신호를 분석함으로써 메시지 내용이나 변조기법 등 유용한 정보를 획득하여 재밍이나 시스템의 스푸핑에 이용하고자 하는 의도이다. 따라서 인터셉터에 의한 위협을 줄이는 방안으로 위성 단말에 대해서 탐지회피 기능을 이용한 은닉통신을 필수적으로 요구하고 있다. 인터셉터의 신호검출 능력은 신호검출을 위해 사용되는 수신기 종류와 수신기에서의 성능에 따라 좌우된다. 지상 단말에 더욱 가깝게 접근해야 위성 신호의 검출이 가능하다는 것을 역으로 이용하거나 신호레벨을 낮춤으로써 LPI 기능면에서 유리할 수 있고, 전송신호전력의 최소화 및 인터셉터 수신기의 적분시간을 증가시켜 신호검출 확률을 낮출 수 있다.[4,5]

5.3 안테나 널링 기법(Antenna nulling)

이 기법은 사용자 신호와 재머 신호간의 공간적 분리 특성을 이용하며 재머에 대한 영향을 줄이는 것을 목적으로 한다. 간단하게는 이미 알고있는 적진 방향에 대해서는 저 부엽 방사 패턴을 가지는 안테나의 사용으로 이득을 주지 않는 방법이 있고, 한 단계 나아가서는 부엽 제거기를 갖는 안테나 또는 어레이 소자의 적응 제어를 통해 적극적으로 재머를 억압하는 방법 등이 있다.[1]

Ⅳ. 정보보호 정책 기반의 대응방안을 통한 안전한 위성통신 보안망 구조 제시

분석된 위성통신망 보안 위협요소와 신호보안 레벨 및 정보보안 레벨의 보안 요구사항을 통해 안전한 위성통신망 보안 구조를 위하여 위성통신 네트워크 정책, 위성통신망 시스템 정책, 위성통신망 데이터 정책에 기반한 위성통신망 보안 위협요소 대응방안들을 제시한다. 본 논문에 제안된 정보보호 정책들은 NIST(National Institute of Standard Technology)의 "Framework for National Information Infrastructure Services"나 BSI(British Standards Institution)의 "BS7799 정보보호 관리 표준"과 같은 문서를 참고로 하여 만들어 졌다.[9~14]

6.1 위성통신 네트워크 보안 정책 기반의 대응방안

위성통신망 보안을 위한 위성체, 단말 그리고 지상망을 포함하는 네트워크 보안 정책은 접근 통제 정책을 기본으로 하며, 보안의 대상을 내부 네트워크와 외부 네트워크로 분리하여 각각에 대한 대응방안을 수립한다.

내부 네트워크에 대한 보안 정책으로는 단말 및 원격 장비, 호스트 서버, 통신 링크 요소, 네트워크 통제 센터 등에 대한 물리적 접근 통제 정책과 사용자 인증, 비 활동시 접속 차단, 네트워크 접근 시간 제한, 허가된 네트워크 자원의 이용 등에 관한 논리적 접근 통제 정책이 있다.

외부 네트워크 보안 정책으로는 신분 위장, 접근 가능 영역 지정, 외부 접속 서비스 관리 및 차단, 감사 추적 등 외부 사용자의 내부 네트워크 접근에 대한 보안 정책과 내부 사용자의 외부 네트워크 접속을 통한 내부 네트워크 우회 접속 시도와 공격 프로그램의 실행 방지, 내부 사용자의 외부 접근 한계 규정 그리고 내부 사용자의 외부 네트워크 사용 로그 감사 등의 내부 사용자의 외부 네트워크 접근에 대한 보안 정책이 있다.[11-13]

위와 같은 위성통신 네트워크 보안 정책에 기반한 대응방안들은 우선 내부/외부 네트워크 보안 정책에 공통적으로 필요한 인증, 기밀성, 가용성, 무결성, 부인방지 등의 정보보호 서비스를 제공할 수 있어야 한다. 이러한 정보보호 기능을 제공하기 위해선 통합 정보보호 해결[2] 과 같은 분산 환경 하에서 통합된 정보보호 기능을 수행하는 통합 정보보호 솔루션을 위성망에 적합하게 수정하여 장착하는 방안을 본 논문에서 제안한다.

그리고 외부 네트워크 정보보호 정책에 있어서는 외부 네트워크로부터의 불법적인 사용자 차단을 위한 침입차단 시스템(Firewall)을 외부 네트워크와 내부 네트워크 사이의 연결 지점에 설치하는 방안과, 지상망간 전용 기밀 통신을 제공하기 위한 가상 사설망(VPN, Virtual Private Network)을 설치하는 방안을 제안한다.

또한 내부 네트워크 정보보호 정책에 있어서 내부 사용자의 불법적인 자원 이용 시도 및 외부에서 방화벽 등의 외부 네트워크 대응방안을 무력화시키고 내부 네트워크 자원의 이용 시도 등에 대한 대응방안으로 침입탐지 시스템(IDS, Intrusion Detection System)을 제안한다.

위와 같은 네트워크 정보보호 정책에 따른 위성통신망 보안 위협요소의 대응방안을 실제로 위성통신망에 적용하기 위하여 아래의 표 [1, 2 ,3]에 위성통신망에 대응방안들을 적용시 고려해야 할 사항을 제시한다.

(표 1) 방화벽 고려 사항

항 목	세부기능	내 용
방화벽구조	패킷 필터링	TCP/IP 레벨에서 출발지/도착지 주소, 서비스 포트 기반 필터링 지원
네트워크 인터페이스	다중 interface	3개 이상의 인터페이스 구성 가능
	ATM/Ethernet	ATM, 1G/100M 이더넷 지원 가능
접근 제어	접근 제어	서비스, 사용자, 시간대별 접근제어설정
실시간 모니터링	보안위반사항 통보	보안 위반 사항의 사용자 정의 및 실시간 통보
프록시	프록시 제공	http, telnet, FTP, SMTP, POP3 등에 대한 프록시
해킹방어	해킹방어 기능	IP, DNS Spoofing, ICMP 공격 등 방어
성능	성능	1Gbps 처리속도 지원 가능 및 NAT 기능 지원
이중화구성	이중화 구성	Primary/Secondary구성 가능 실제 system takeover 신속성
VPN	VPN 지원	IPSec, DES, Triple-DES 등 지원

(표 2) VPN 고려 사항

항 목	세부기능	내 용
VPN 구조	상호 연동	보안 솔루션들과의 상호 연동이 가능
네트워크 인터페이스	다중 인터페이스	3개 이상의 인터페이스 구성 가능
	ATM,Ethernet	ATM, 1G/100M Ethernet 지원가능
접근 제어	접근 제어 기능	서비스, 사용자, 시간대별 접근제어 가능
물리적 장비 보호	물리적인 방어기능	장비 및 비상시 주요 정보의 보호 장비 불법 해체 및 장해시 자동 경보
해킹방어	해킹방어	IP, DNS Spoofing, ICMP Attack 등에 대한 방어 기능
지원 표준	VPN표준	IPSEC등 국제 표준의 VPN 지원
보안 인자	암호/인증/키	다양한 암호, 인증, 키관리 지원
성능	성능	1Gbps 처리속도 지원 가능

[표 3] IDS(Intrusion Detection System) 고려 사항

항 목	세부기능	내 용
IDS 구조	상호간 연동	Network/Host 기반 IDS 지원
네트워크 인터페이스	지원 네트워크	Fast/Giga Ethernet, ATM 등 지원
	네트워크 부하	최소한의 네트워크 성능 저하
OS 인터페이스	지원가능 OS	Unix, Linux, Netware, NT, Windows 98/2000 가능
실시간 모니터링	Active 세션 모니터링	실시간 네트워크 모니터링, 모든 TCP/IP 프로토콜 지원 가능
	침입탐지 실시간 통보	침입탐지 또는 보안문제 발생시 다양한 형태의 실시간 통보
	침입자 공격 차단 기능	세션 종료, 방화벽 재설정 등 네트워크 공격에 대한 차단 기능
	중요시스템파일 변동	네트워크 상의 주요 시스템(DNS, Web, FTP 등) 파일 변경 탐지 기능
	내/외부 공격탐지	실시간 내/외부 공격 탐지 기능
접근제어	접근제어 기능	서비스, 사용자, 시간대별 접근제어가능
리포팅	다양한 리포팅 기능	로그 검색, 로그 해쉬, 다양한 리포팅 및 도움말 기능
해킹 방어	침입유형DB보유	침입유형에 대한 자체 DB 보유 여부
	침입유형 사용자 정의	침입유형에 대한 사용자 정의(별도의 내용 포함) 가능 여부
	침입 유형 갱신	새로운 침입유형 갱신/추가 가능
	탐지 공격 종류	다양한 공격패턴 갱신/추가 가능
	악성 S/W 공격 인식	Java, ActiveX 등을 비롯한 웹이나 인터넷을 통한 악성 S/W 공격탐지기능
관리의 용이성	원경 및 중앙집중관리	침입탐지의 원격(보안성 포함) 및 중앙 집중적 관리 가능 여부
	시스템 관리 툴과 통합	Tivoli, HP Openview, CA Unicenter 등의 시스템 관리 모듈 지원

6.2 위성통신망 시스템 보안 정책 기반의 대응방안

위성통신망에서 위성체를 비롯한 위성망 구성 시스템들에 대한 시스템 보안 정책은 중요 시스템의 침입 탐지 시스템 가동, 시스템 로그 정보 관리, 트랜잭션 트레이스를 통한 침입자 추적 정책, 내부 사용자 접근 통제 정책, 시스템 데이터와 프로그램 보안 정책, 시스템 사용자 관리 정책 그리고 물리적/환경적 시스템 보안 정책 등이 있다.[11,14]

이러한 위성통신망 시스템 보안 정책을 기반으로 한 위성통신망 위협요소에 대한 대응방안으로는 중요 운영 시스템에 대해서 보안 운영체제를 사용하는 방안이 있다. 또한 시스템 사용자 계정 관리, 로긴 정보 관리, 사용자 인증 관리, 접근 제어 서버스 관리가 가능한 위성통신망 전용 시스템 보안 솔루션을 장착하는 방안이 있다.

위성통신망 시스템 보안 솔루션을 위성통신망 구성요소들에 장착하는 경우에 위성통신망 보안 위협요소 분석과 보안 요구 사항을 바탕으로 만들어진 [표 4]의 위성통신망 시스템 보안 솔루션 고려사항을 참조하여 실제적인 위성통신망 적용이 가능하다. 또한 네트워크 보안 정책에서도 적용이 제안된 통합 정보보호 엘진[10]을 위성통신망 시스템에 알맞게 수정 및 보완하여 위성통신망 시스템 보안 솔루션으로서 장착하는 방안도 정보보호 정책의 일관성 있는 적용 및 대응체계의 효율성 면에서 고려 할 수 있다.

6.3 위성통신 데이터 보안 정책 기반 대응방안

위성통신망에 사용되는 위성통신 데이터 보안 정책은 데이터에 대한 접근통제 정책, 응용 프로그램 보안 정책, DBMS(Data Base Management System) 보안 정책 등으로 구성된다.

데이터에 대한 접근 통제 정책은 데이터에 대한 접근 권한을 읽기 권한, 갱신 권한, 삭제 권한, 병합 권한 그리고 실행 권한 등으로 분류하여 통제한다. 응용 프로그램 보안 정책은 응용 프로그램이 다루는 자료의 가치와 민감성에 적합하게 자료의 비밀성 유지, 자료가 적절하게 사용될 수 있도록 자료의 무결성 확보, 허가된 사용자가 그들의 요구사항에 따라 자료를 사용할 수 있도록 자료의 가용성 확보 그리고 응용 프로그램의 효과성과 효율성을 확보하는 정책이다. 마지막으로 DBMS 보안 정책은 위성통신망에서 실제로 데이터가 저장되는 DB(Data Base)에 관한 것으로 위성통신망에서는 DBMS 사용자와 프로세스를 확인, 사용자나 프로세스의 실체가 적합

[표 4] 시스템 보안 솔루션 고려 사항

항 목	세부기능	내 용
시스템 보안 구조	지원 OS	다양한 OS에 대한 지원 여부 (Unix, NT, Windows2000 등)
	Root	서버 시스템의 슈퍼 계정인 root 권한에 대한 통제 기능 지원
사용자 계정 관리	사용자 계정 편경/만료	상요자 계정 생성, 변경, 삭제 등의 변경사항이 OS와의 연동 지원
사용자 인증	다양한 인증 방법	접근 사용자의 인최용 패스워드 발행기 또는 SSO 지원 여부
	사용자 로그 세션	인정 횟수 이상 로그인 실패시 계정 잠김 및 동시 세션 제한 가능 여부
	명령어 실행 인증	중요하고 위험한 명령어 실행에 대한 인증 부여 가능
접근 제어	IP 주소 접근 제어	시스템으로 접근 가능한 IP 주소 등록 및 등록 IP만 접근 가능
	계정/서비스 접근제어	사용자별 접근 가능 서비스/IP 주소 등록 및 허용된 서비스만 사용 가능
	시간대/그룹 접근제어	시간대별 또는 그룹별 접근 가능 서비스 제어 및 시간통제 가능 여부
	내부 파일/프로세서	로그인한 사용자에 대한 내부 파일 및 특정 프로세스 접근 제어 지원
로깅 및 감사	로깅	시스템 접근 로깅 데이터의 유용성 및 환경설정 변경 기록 여부
	감사	로깅된 데이터의 검색, 통계 및 그래프 등의 리포팅 제공 여부
모니터링	중요 이벤트 통보	관리자 설정 중요 이벤트 발생시 실시간 통보 지원(콘솔, 메일, hp 등)
시스템 점검	무결성 점검	보안 툴 자체의 무결성을 점검, 이상 발생시 경고 반영 기능 지원 여부
관리의 용이성	관리 인터페이스	GUI 및 Web 인터페이스 지원 여부
	원격/중앙집중 관리	보안 툴의 원격/중앙집중관리 지원(시스템 설정, 로그 데이터 취합 등)

확인, 위조가 없음을 입증. 인증 규칙 준수 그리고 사용자나 프로세스의 요구사항을 분석하여 인증 규칙을 강화하는 것 등이 있으며, 특히 DB에 각 사용자가 접근 할 때마다 인증 규칙에 따라 적법한 절차를 거치는 것이 중요하다.[11-13].

이와 같은 데이터 보안 정책에 따른 대응방안으로 [표 5]와 같은 위성통신망 데이터 보안 솔루션 고려 사항을 만족시키는 위성통신망 데이터 보안 솔루션을 설치하는 것을 제안한다. 또한 데이터 보안 솔루션의 요구사항에 적절한 보안 솔루션의 하나로 기밀성, 접근제어 등의 정보보호 서비스가 가능한 통합

[표 5] 데이터 보안 솔루션 고려 사항

항 목	내 용
인증사발행	암호화를 위한 인증서 발행 기능
유연성	보안정책관리 기법을 적용/업무의 변경성 신속성
버전 갱신	새로운 버전시 자동 Upgrade 기능
간편성	시스템에 대한 S/W 설치 시 간단하게 설치 가능 여부
알고리즘	대칭, 비대칭 등 다양한 알고리즘에 대한 지원 여부
키 길이	충분한 길이의 키가 지원되는지에 대한 여부
키 관리 안정성	비인가자의 물리적인 파괴로부터의 개인키 및 암호화 알고리즘의 자동 파괴 기능
법적인보호	전자서명 및 전자거래기본법에 준실한가 여부

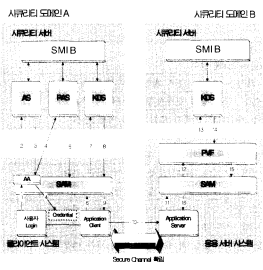
정보보호 엔진[21]을 고려 할 수 있으며, 네트워크 보안 정책이나 시스템 보안 정책과 마찬가지로 위성통신망에 적합하게 수정하는 것이 요구된다.

6.4 통합 정보보호 엔진의 위성통신망 적용

본 논문에서 연구된 위성통신 네트워크 보안 정책, 위성통신망 시스템 보안 정책, 위성통신망 데이터 보안 정책과 같은 정보보호 정책을 기반으로 한 위성통신망 보안 위협요소의 대응방안에서 공통적으로 인증, 기밀성, 접근통제 그리고 키 관리 등의 기능이 요구되었다. 이러한 정보보호 기능을 제공하기 위한 방안 중 하나로 본 논문에서는 통합 정보보호 엔진을 제안한다. 통합 정보보호 엔진의 구성은 [그림 2]와 같으며, [그림 2]에서는 통합 정보보호 엔진 구성 모듈들이 시큐리티 도메인에서 상호 동작하는 절차를 보여준다.

통합 정보보호 엔진의 작동 과정

1) 로그인 프로그램으로 사용자가 id, password, role을 입력함으로써 인증 요청이 들어오면 SAM 안의 AA가 실행된다.
2) AA는 인증 서버에게 id와 password를 넘겨주면서 인증을 요청한다.



[그림 2) 통합 정보보호 엔진 구성도

3) 인증 서버는 SMIB에게 사용자의 정보를 요청하여 받고 정당한 사용자이면 AA에게 신임장을 발부하고 사용자 이름과 신임장을 신임장 캐쉬에 추가한다.
4) AA는 인증 서버로부터 수신한 신임장을 신임장 파일에 저장하고 특정 응용 프로그램의 실행 요청이 들어오면 응용 클라이언트가 실행되고 권한과 역할에 관한 속성을 부여받기 위해 권한속성 서버와 통신한다.
5) 권한속성 서버는 SMIB에게 권한속성 정보를 요청하여 받은 후 사용자의 권한과 역할을 정의한 집합인 PAC(Privilege Attribute Certificate)를 SAM에게 보낸다.
6) 응용 클라이언트는 서버와의 안전한 세션을 확립하기 위한 세션 키를 획득하기 위해 GSS-API를 호출한다.
7) SAM은 키분배 서버에게 세션키 획득을 위한 정보를 요구한다.
8) 키분배 서버는 기본키와 세션키 패키지 등의 정보를 생성하고 SAM에게 돌려준다.
9) SAM은 키분배 서버로부터 받은 정보(PAC가 들어있는 서버스 티켓과 세션키 확립 정보)를 응용 클라이언트에게 GSS-API에 대한 반환값으로써 돌려준다.
10) 응용 클라이언트는 응용 서버에게 서비스 티켓과 세션키를 확립하기 위한 정보를 보낸다.
11) 응용 서버가 클라이언트로부터 수신한 정보에 대한 유효성을 확인 후, 세션키를 획득하기 위해 GSS-API를 호출하여 SAM을 실행시킨다.
12) SAM은 응용 클라이언트로부터 수신한 정보를 PVF에 넘겨 준다.
13) PVF는 수신한 PAC와 기타 정보들에 대한 유효성을 확인하기 위해 서비스 티켓을 로컬 키 분배 서버로 넘겨준다. 키 분배 서버는 SMIB와 통신하여 PVF들에게서 넘어온 정보들에 대한 유효성을 확인한다.
14) 이상이 없으면 키 분배 서버는 서비스 티켓의 정보들을 복호화하여 PVF로 보낸다.
15) PVF는 SAM에게 세션키 확립을 위한 정보와 응용 클라이언트에게 보낼 응답 정보를 생성하여 보내고 SAM은 이 정보를 이용하여 세션키를 확립하게 된다.
16) SAM은 GSS-API에 대한 반환값으로써 응답 정보를 응용 서버에게 전달한다. 응용 서버는 응용 클라이언트에게 응답 정보를 보내주고 안전한 세션을 확립하게 된다.

실제적으로 분산 네트워크 환경에서 통합 정보보호 엔진이 제공할 수 있는 보안 서비스로는 대칭키/비대칭키 암호 기법, 단일 인증 기능, 접근제어 기술 그리고 데이터의 기밀성과 무결성을 제공하는 데 필요한 키 분배 기능 등이 있다.

하지만 위성통신망에 통합 정보보호 엔진이 탑재된다면 제공되어야 할 기능으로는 위성통신망 구성 요소에 대한 인증 기능과 기밀 통신 기능이며, 이와 함께 인증 및 기밀 통신에서 암호화 키 생성과 분배 및 관리 기능 등이 제공 되야 한다.

결국 분산 네트워크 환경에서 사용되던 통합 정보보호 엔진을 위성통신망에 적용하는 경우에는 위성통신망의 보안을 위해 필요한 기능을 제공하도록 통합 정보보호 엔진의 관련 모듈들을 재설계하는 것이 필요하다. 그리고 유선과 무선 네트워크가 복합된 위성통신망 환경을 고려해 최적화 된 1:N, N:N 통신에서의 적은 시스템 부하 및 효율을 얻을 수 있는 인증 및 키 분배 방법의 연구가 필요하다.

통합 정보보호 엔진을 위성통신망에 적합하게 재설계하는 연구와 함께 통합 정보보호 엔진이 위성통신망에 장착될 위치를 고려해야 된다. 통합 정보보

호 엔진의 적절한 탑재 위치로는 지상망 구성 요소 중에서 메인 NCC내에 탑재되어 일반 정보보호 솔루션과 함께 종합적인 보안 관리가 이루어 질 수 있게 하는 방안을 제안한다. 통합 정보보호 엔진의 NCC 내부 장착은 NCC 내부에 장착된 다른 정보보호 솔루션들과 함께 종합적으로 관리가 가능하여 시스템들의 관리 효율성 및 추후 통합 관제 시스템과의 연동에서도 유리하다.

6.4.1 통합 정보보호 엔진을 사용한 인증 및 키 분배

Level-1 단계의 위성 관제 센터와 위성간의 통신 과정에서 사용자 인증 및 기밀 통신을 지원하기 위해 NCC 내의 통합 정보보호 엔진에서 수행되는 인증 및 키 분배 과정은 다음과 같다.

1. SCC 내의 사용자가 NCC에 장착된 통합 정보보호 엔진에 접속한다.
2. 통합 정보보호 엔진에 장착된 여러 인증 모듈(패스워드방식, 스마트카드방식, 원타임 패스워드, 생체인식 등)중 하나의 모듈을 통해 인증 과정을 수행한다.
3. 인증 성공 시 기밀 통신을 위한 키를 통합 정보보호 엔진의 키 분배 모듈을 통해 분배받아 위성과의 기밀 통신이 가능하다.

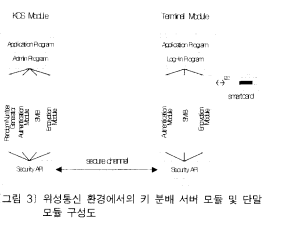
Level-2 단계에서 단말-위성-NCC 및 단말-위성-단말들간의 인증 및 기밀 통신을 위해 NCC내에 장착한 통합 정보보호 엔진을 이용하는 인증 및 키 분배 과정은 다음과 같다.

1. 단말 측면에서 단말을 사용하는 사용자에 대한 인증이 이루어진다.(본 논문에서는 스마트카드를 사용하는 단말 자체의 사용자 인증 방법만을 고려한다.)
2. 사용자를 자체 인증 한 단말이 위성을 통해 통합 정보보호 엔진에 접속하려는 경우 IS-95 등과 같은 무선망 프로토콜 자체의 단말 인증 알고리즘(IS-95의 경우 CAVE : Cellular Authentication and Voice Encryption Algorithm)을 통한 단말 식별 및 인증 과정이 이루어진다.(본 논문에서 이 과정의 인증 여부는 기본적으로 성공한 것으로 가정한다.)
3. 위의 단말 및 사용자에 대한 각 단계의 인증 과정이 성공한 후에는 사용자에 대한 간단한 식별 정보만을 이용하여 사용자를 인증 한다.
4. 인증 성공 시 위성을 통한 단말간의 상호 통신 또는 단말과 지상망간의 통신을 위한 키는 위성 통신 환경에서 요구되는 비도에 따라 다양한 키 분배 모듈 중 하나의 모듈을 통해 분배받아 기밀 통신이 가능하다.

또한 지상망 레벨에서는 기본적으로 침입탐지시스템이나 침입차단시스템 같은 일반적인 정보보호 솔루션을 통한 정보보호 기능 제공이 가능하다. 하지만 인증, 기밀 통신 등의 정보보호 기능을 위하여 통합 정보보호 엔진의 인증 및 키 분배 모듈을 사용할 수 있다.

NCC 내부에 장착되는 통합 정보보호 엔진은 위의 Level-1,2 단계에서의 인증 과정 및 지상망 레벨에서의 정보보호 기능을 제공하기 위하여 기본적으로 인증 모듈과 키 관리 모듈들을 포함한다. 그리고 이와 연관된 통합 정보보호 엔진의 클라이언트 모듈은 위성통신망에서 사용되는 각 단말들에 장착되어 스마트카드와 같은 부가적인 인증 장치들을 사용한다. 각 단말에 장착된 클라이언트 모듈은 스마트카드와 같은 부가적인 인증 장치와 함께 단말에서의 사용자 인증, 통합 정보보호 엔진에 대한 인증, 기밀 통신을 위한 키 분배 요청 등과 같은 기능들을 수행한다. [그림 3]은 위성통신 환경에서 단말과 NCC내의 통합 정보보호 엔진의 키 분배 서버간에 장착되는 모듈 구성도이다.

단말의 사용자는 맨 처음 사용자 정보가 저장된 스마트카드를 사용하여 단말에서 자체 인증 과정을 거치며 이러한 인증 과정 후 단말에 대한 위성통신망 내에서의 식별 과정이 수행된다. 앞의 과정이 모



[그림 3] 위성통신 환경에서의 키 분배 서버 모듈 및 단말 모듈 구성도

두 성공한 후에 사용자는 실제로 통합 정보보호 엔진의 키 분배 모듈에 접근하여 상대 단말과의 기밀 통신에 필요한 키를 요청하고 분배받는다.

Terminal Module

Log-In Program : 스마트카드를 사용하여 사용자 인증을 대행하는 프로그램

SMIB : 단말과 키 분배 서버에 미리 공유하는 키 및 사용자 정보 등을 보관

Authentication Module : 스마트카드의 사용자 정보와 SMIB에 미리 갖고 있는 사용자 정보를 인증

Encryption Module : 사용자 인증 및 키 분배 요청 등에 사용되는 암호화/복호화 과정 수행

Security API : KDS 및 단말과의 암호화 통신이나 사용자 인증, 키 분배 등의 과정에 사용되는 보안 인터페이스

KDS Module

Admin Program : 사용자의 정보의 갱신, 추가, 삭제 등 관리 프로그램

SMIB : 사용자 정보, 미리 가지고 있는 비밀키, 인증서 등의 정보 관리

Authentication Module : 단말이 보내온 사용자 정보에 기반하여 SMIB에 미리 갖고 있는 사용자 정보를 인증

Encryption Module : 사용자 인증 및 키 분배 요청 등에 사용되는 암호화/복호화 과정 수행

Security API : KDS 및 단말과의 암호화 통신이나 사용자 인증, 키 분배 등의 과정에 사용되는 보안 인터페이스

통합 정보보호 엔진이 제공하는 단말과 지상망간 또는 단말 사이의 통신 과정에서는 통신 프로토콜 상의 불필요한 요소를 최대한 배제하기 위해 단말 자체에서의 사용자 인증과 무선망 프로토콜 상에서의 단말 식별 과정을 통해 NCC내의 통합 정보보호 엔진에서 부가적인 인증과정을 생략하여 인증 및 키 분배 과정에 있어서의 효율성을 가져온다. [그림 4] 및 [그림 5]와 같은 위성통신 과정에서 통합 정보보호 엔진을 이용한 상호 단말간 인증 및 키 분배 과정은 우선 단말에서 사용자에 대한 자체 인증이 먼저 수행되고 무선망 프로토콜 상의 단말 식별을 통한 인증이 모두 성공적으로 수행 됐을 때, 본 논문에서는 단말간 상호 인증을 위해서 간단한 상호간 인증 프로토콜인 2-PMAP(2-Party Mutual Authentication Protocol)를 수정한 공개키 기반의 단방향 상호 인증 및 키 분배 프로토콜과 ANSI X9.17 키 분배 표준 프로토콜을 참고한 비밀키 기반 상호 인증 및 키 분배 프로토콜을 사용하는 예를 든다.

6.4.2 단말 자체의 사용자 인증 과정

단말 자체에서 이루어지는 사용자 인증 과정에 대해서 본 논문에서는 스마트카드를 사용하는 기법을 보인다. 스마트카드에 사용되는 인증 방식으로는 DES를 사용하며 NIST(National Institute of Standards Technology)에서 제안된 ASACS(Advanced Secure Access Control Systems)를 들 수 있는데 인증 방식은 다음과 같다.

[표 6] 스마트 카드 인증 과정에 사용되는 기호 설명

기호	설명
Card	스마트카드
Term	위성통신망 환경의 단말
k	스마트카드와 단말간의 비밀키
PIN	스마트카드 사용자를 식별하기 위한 개인식별번호
r1, r2	스마트카드와 단말간에 생성하는 랜덤 값

1) 스마트카드의 사용자 인증 과정

1. User -> Term : PIN
2. Card <- Term : E_k[PIN]
3. Card : if (D_k[PIN] == PIN) then Authentication

① 스마트 카드의 사용자를 확인하기 위해서 단말에 사용자만이 아는 PIN을 입력한다.

② 단말은 입력된 PIN을 자신과 스마트 카드가 공유하는 비밀키로 암호화하여 스마트 카드에 보낸다.

③ 스마트 카드는 공통의 비밀키로 암호화된 PIN을 복호화 한 후 자신이 가지고 있는 PIN과 비교하여 사용자를 인증 한다.

2) 스마트 카드와 단말간의 인증 과정

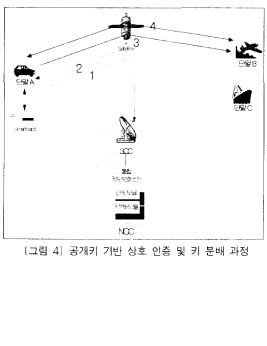
1. Card -> Term : r1
2. Card <- Term : E_k[r1 || r2

3. Card : if (D_k[r1] == r1) then ok!
4. Card -> Term : E_k[r2]
5. Term : if (D_k[r2] == r2) then
   Authentication

① 스마트 카드는 임의의 난수를 생성하여 이를 단말에 보낸다.
② 단말은 스마트 카드로부터 받은 난수를 비밀키로 암호화한 값과 새로 생성한 난수 값을 함께 스마트 카드에 보낸다.
③ 스마트 카드는 단말로부터 받은 암호화 값을 받아 복호화 한 후 자신이 가지고 있는 난수와 비교하여 같으면 새로 받은 난수를 암호화하여 단말에 보낸다.
④ 단말은 스마트 카드에서 다시 보낸 암호화 값을 복호화 한 후 자신의 난수와 비교하여 인증 과정을 마친다.

6.4.3 공개키 기반 상호 인증 및 키 분배 과정

다음의 [그림 4]는 단말 자체의 인증 과정 후에 이루어지는 단말간의 공개키 기반 상호 인증 및 키 분배 과정이다. 단말 상호간의 인증 및 키 분배는 공개키 암호화 기법을 사용하여 이루어짐으로써 키 관리의 용이성은 물론이고 향후 무선 환경을 고려하여 구축되고 있는 무선 공개키 기반 구조(WPKI : Wireless Public Key Infrastructure) 환경과의 연동도 고려 할 수 있다. 하지만 공개키 암호화 알고리즘 자체의 연산 속도 문제 및 공개키/개인키 쌍에 대한 유효성 검증 문제 등으로 공개키 기반의



[그림 4] 공개키 기반 상호 인증 및 키 분배 과정

인증 및 키 분배 프로토콜이 적용 되는 대상, 서비스 그리고 환경 등의 요소에 따라 그 사용 가능성을 결정해야 한다.

가정 : 단말 자체의 사용자 인증 과정과 외성통신망 자체의 단말 인증 과정은 성공으로 가정한다.

1. A -> EAM : ml
2. A <- EAM : E_{KU_A}[m2]||$Sign_{KEeam}$(E_{KU_B}[m2])
   E_{KU_A}[m3]||$Sign_{KEeam}$(E_{KU_B}[m3])
3. A -> B : E_{KU_B}[m3]||$Sign_{KEeam}$(E_{KU_B}[m3])
4. A <- B : E_{KS1}[N_1]
   A -> B : E_{KS1}[f(N_1)]

*m1 = (ID_A||ID_B), *m2 = (K_{S1}||ID_B||T)
*m3 = (K_{S1}||ID_A||T)

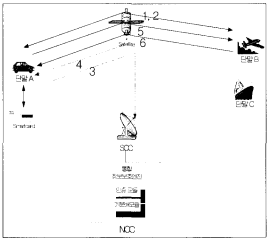
① 단말 A는 위성을 통해 EAM에 단말 B와의 통신을 요청한다. 이때 단말 A는 자신의 식별자와 통신을 원하는 상대의 식별자를 전송한다.
① EAM은 단말 A가 보낸 인증 요청 메시지의 식별자를 확인한 후에 단말 A와 단말 B 사이의 기밀 통신에 필요한 비밀키를 전송한다.
③ 단말 A는 단말 B에게 통신에 필요한 비밀키를 전송한다.
④ 단말 A, B 사이에 분배된 비밀키의 정당성을 확인하기 위해 두 단말은 특정 랜덤 값을 상호 간의 비밀키를 통해 상호 검증하여, 검증이 완료되면 기밀 통신을 확립한다.

[표 7] 공개키 기반 상호 인증 및 키 분배 용어 설명

기호	설명
IDx	단말 X의 식별 인자
EAM	통합 정보보호 엔진의 인증 모듈
KUx	단말 X의 공개키
KRx	단말 X의 개인키
KUeam	통합 정보보호 엔진의 공개키
KReam	통합 정보보호 엔진의 개인키
$Sign_{KRx}$()	X의 개인키를 사용한 서명
K_{S1}	단말 A와 단말 B가 공유하는 비밀키
T	타임스탬프
N_1	Nonce(Random Number)

6.4.4 비밀키 기반 상호 인증 및 키 분배 과정

다음은 위성통신망에서 단말 A와 단말 B 사이의 기밀 통신을 위해 비밀키를 기반으로 하는 상호 인증 및 키 분배 과정이다. 다음의 프로토콜은 ANSI X9.17 키 분배 표준의 푸쉬 모델을 적용하였다.[18]



(그림 5) 비밀키 기반 상호 인증 및 키 분배 과정

본 프로토콜은 비밀키를 기반으로 함으로써 통합 정보보호 엔진 내에 기밀 통신을 원하는 단말 수만큼의 비밀키를 관리해야되는 문제를 가지고 있다. 하지만 다양한 다이제스트 값을 생성할 수 있는 MAC 함수를 사용하여 상호 간에 전달되는 메시지의 크기를 조절할 수 있고, 단말간 비밀키 분배에 있어 단말간의 비밀키를 암호화 된 MAC 값과의 XOR 연산을 이용하여 패딩 하는 기법을 사용함으로써 분배하는 비밀키를 조합하여 전체 메시지를 암호화하는 방법에 비해 최소한의 메시지 크기에 대한 암호화를 가능하게 한다. 또한 메시지 암호화 및 다이제스트 생성에 쓰이는 알고리즘은 공개키 암호화 및 서명 알고리즘에 비하여 연산 속도가 빠른 특징을 가지고 있다. 그러므로 MAC과 관용 암호화 알고리즘을 사용하는 비밀키 기반의 상호 인증 및 키 분배 프로토콜은 위성통신망 단말의 낮은 성능과 무선 링크 환경을 고려하는 경우에 있어 최소한의 연산, 메시지 크기의 감소 그리고 메시지 크기 조절 가능이라는 장점을 가질 수 있다.

가정 : 단말 자체의 사용자 인증과정과 위성통신망 단말들에 대한 인증과정은 성공으로 가정.

1. A -> B : N_a
2. A <- B : N_b
3. A -> EKDM : N_a || N_b || ID_b
4. A <- EKDM
   : $MAC_a(m1)$ || $E_a\{MAC_b(m1)\}\oplus K_{ab}$,
   $MAC_b(m2)$ || $E_b\{MAC_b(m2)\}\oplus K_{ab}$
5. A -> B
   : $MAC_{ab}(m3)$ ||
   $MAC_b(m2)$ || $E_b\{MAC_b(m2)\}\oplus K_{ab}$
6. A <- B : $MAC_{ab}(N_a, N_b)$

*m1 = $(N_a||K_{ab}||ID_b)$, *m2 = $(N_b||K_{ab}||ID_a)$
*m3 = $(N_a||N_b||ID_a)$

① 단말 A는 B에게 임시 랜덤 값 전송.
② 단말 B는 A에게 임시 랜덤 값 전송.
③ 단말 A는 EKDM에게 단말 B와 교환한 임시 랜덤 값과 단말 B의 ID를 함께 보낸다.
④ EKDM은 단말 A에게 단말 A, B사이의 비밀키를 가지고 있는 A, B 각각에 해당하는 메시지를 전송한다. 단말 A에 해당하는 메시지는 초기에 상호간 교환했던 자신의 임시 랜덤 값(N_a), A, B사이의 공유키(K_{ab}) 그리고 상대방 식별자(ID_b)를 자신과 EKDM 사이의 비밀키로 생성된 MAC 값($MAC_a(m1)$)과 또한 생성된 MAC 값을 다시 비밀키로 암호화($E_a\{MAC_a(m1)\}$)한 후 두 단말 사이의 비밀키와 XOR 연산을 한 값($E_a\{MAC_a(m1)\}\oplus K_{ab}$)으로 구성된다.
단말 A는 EKDM으로부터 받은 메시지에서 단말간 비밀키를 얻어내기 위해 자신과 KDM과의 비밀키로 생성된 MAC값($MAC_a(m1)$)을 암호화한 후 KDM으로부터 수신한 암호화된 MAC과 단말 사이의 비밀키와의 XOR값($E_a\{MAC_a(m1)\}\oplus K_{ab}$)과 다시 XOR 연산을 수행한다.
⑤ 단말 A는 EKDM으로부터 받은 단말간 비밀키로 자신의 식별자와 임시 랜덤 값들에 대한 MAC을 생성하여 전에 EKDM으로 받은 단말 B에 대한 메시지들을 함께 보낸다.
⑥ 단말 A로부터 해당 정보를 받은 B는 A, B 간의 공유키로 처음에 교환했던 임시 랜덤 값의 MAC을 생성하여 다시 보낸다.
단말 A는 단말 B로부터의 임시 랜덤 값들의 MAC 값을 검증함으로써 상호 인증 및 키 분배 과정의 정당성을 확인한다.

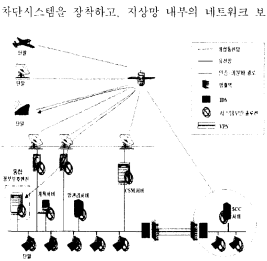
[표 8] 비밀키 기반 상호 인증 및 키 분배 과정 용어 설명

기호	설명
ID_x	단말 x의 식별 인자
EKDM	통합 정보보호 엔진 키 분배 모듈
N_x	단말 x의 임시 랜덤값
MAC_x	단말 x와 EKDM의 비밀키를 사용한 MAC값
MAC_{xy}	단말 x와 단말 y의 비밀키를 사용한 MAC값
E_x	단말 x와 EKDM의 비밀키로 암호화
E_{xy}	단말 x와 y의 비밀키로 암호화

6.5 제안하는 위성통신망 보안 구조

본 논문에서 제안하는 위성통신 보안망 구조는 앞서 연구된 위성통신 네트워크 보안 정책, 위성통신망 시스템 보안 정책, 위성통신 데이터 보안 정책에 기반하여 위성통신망 위협요소에 대한 대응방안을 위성통신망 구성요소들에 적용한 결과이다.

제안하는 위성통신 보안망은 다음과 같다. 우선 메인 NCC내에 수정된 통합 정보보호 엔진을 장착한다. 위성망에 적합하게 수정된 통합 정보보호 엔진의 장착을 통해 위성통신망에서 공통적으로 적용되는 보안 요구사항을 충족 시킬 수 있도록 인증, 암호화, 키분통신, 접근 제어, 키관리 등의 정보보호 기능들을 해공한다. 그리고 지상망 내의 중요 시스템 및 사용자 단말에는 시스템 보안 솔루션 요구사항을 충족시키는 위성통신망 시스템 보안 솔루션을 장착한다. 또한 NCC 및 SCC로 구성된 지상망의 보안을 위해 외부 네트워크와의 연결 지점에는 침입 차단시스템을 장착하고, 지상망 내부의 네트워크 보안을 위해선 침입탐지시스템을 장착하며, 지상망간의 키밀 적용 통신은 가상 사설망과 같은 보안 서버스로 위성통신망 보안 요구사항을 충족 시켜 준다.



[그림 6] 제안하는 위성통신망 보안 구조

Ⅵ. 결 론

본 논문은 위성통신망에 존재하는 보안 위협요소를 위성 전파 신호 레벨(Level-0), 위성 관제 데이터 레벨(Level-1), 위성 응용통신 데이터 레벨(Level-2) 그리고 지상망 레벨로 나누어 분석하였다. 이러한 분석에 따라 기존에 이루어진 신호 보안 대응방안(항재밍 기법, 대역확산 기법 등)의 대부분이 위성 및 시스템 전파 방해 위협에 대해 생존성 강화나, 확산코드 기법을 통한 인터셉터로부터 탐지 회피 등 소극적인 대응방안으로서 현재 정보 보안 레벨의 위협 요소를 해결하여 안전한 위성통신망을 구축하기에 어려움이 있음을 알았다.

따라서 본 논문에서는 위성통신망 보안에 위협을 가하는 악의적 사용자의 위성통신망 이용을 원천적으로 제어할 수 있도록 인증 기법, 접근 제어 기법 그리고 암호화 기법을 사용하여 정보보안 측면에서의 적극적인 대응방안을 마련하였다. 즉, 노출된 정보보안 측면의 보안 요구 사항과 함께 위성통신 네트워크 보안 정책에 기반한 침입 차단 시스템이나 침입 탐지 시스템, 가상 사설망의 장착을 제안하고 각각의 대응방안들에 대한 망 적용시 고려사항을 도출하였으며, 위성통신망 시스템 보안 정책과 위성통신 데이터 보안 정책에 대해서도 시스템 및 데이터 보안 솔루션 장착을 위한 보안 요구사항을 마련하였다. 또한 각 정책에 공통적으로 필요한 인증, 접근 제어 등의 정보보호 서비스를 제공하기 위하여 통합 정보보호 엔진을 위성통신망에 적합하게 수정하는 방안을 제안하였다.

이처럼 제안된 위성통신망 정보보호 정책에 기반한 대응방안과 위성망에 적합하게 수정된 통합 정보보호 엔진의 정보보호 서비스를 통하여 안전한 위성통신 보안망을 구축 할 수 있다. 향후에는 위성통신망 보안 위협요소 대응방안에 대한 보완과 통합 정보보호 엔진의 위성통신망 적용에 대한 구체적인 연구가 진행될 예정이다.

참 고 문 헌

[1] Pravain c. jain, "Architectural Trends

in Military Satellite Communication System", *IEEE*, 1990.
[2] A.D. Dayton and P.C. jain, "MILSATCOM architecture", *IEEE Trans, Commun*, Vol. COM-28, No. 9, Sep, 108, 1456-1459.
[3] Paymond L. Pickholtz, Security Analysis of the INTELSAT VI and VII Command Network, *IEEE*, Vol. 11, No. 5 June 1993.
[4] Robert M. Gagliardi, "LPI in Pulsed Laser Space Communications", *IEEE*, Vol. 11, No. 5, June 1993.
[5] Ralph Schoolcraft, "Low Probability of Detection Communications(LPD Waveform Design and Detection Techniques)", *IEEE*, 1991.
[6] Craig Partridge, "TCP/IP Performance over Satellite Links", *IEEE Network*, 1997.
[7] Nasir Ghani, "TCP Enhancements for Satellite Networks", *IEEE Communications Magazine*, 1999.
[8] Sead Muftic, Security Architecture for Open Distributed Systems, *John Wiley & Sons Ltd*, 1993.
[9] BS7799-1, "Information Security Management Part1 : Code of practice for information security management", *BSI*, 1999.
[10] BS7799-2, "Information Security Management Part2: Specification for information security management system", *BSI*, 1999.
[11] Organisation for Economic Co-operation and Development, "Guidelines for the Security of Information Systems", OCDE/GD(92)190, Paris, 1992.
[12] National Research Council, Computers at Risk : Safe Computing in the Information Age, (Washington, D.C.: *National Academy Press*, 1991).
[13] National Institute of Standards Technology, "Framework for National Information Infrastructure Services", *NISTR 5478* (Gaithersburg, MD: NIST, July 1994).
[14] National Institute of Standards Technology, "An Introduction to Computer Security: The NIST Handbook", *NIST Special Publication* 800-12, July 1994).
[15] R. Jueneman: S. Matyas : and C. Meyer, "Message Authentication", *IEEE Communications Magazine*, Sept.1985.
[16] Ravi S. Sandhu, "Access Control : Principles and Practice," *IEEE*, 1994.
[17] William Stallings, "Cryptography and Network Security : Principles and Practice", *Prentice hall*, 1997.
[18] ANSI, "X9.17 Financial Institution Key Management Standard", *X9-Secretarait Banker Association*, 1985.
[19] NASA, "Mission Control Center", http://www.jsc.nasa.gov/
[20] 서정태, 장준교, 김동규 외, "위성통신망 보안 프레임워크에 관한연구",춘계종합학술발표논문집, *한국정보과학회*, 2000.4.
[21] 김동규 외, "분산 통신망환경 통합 정보보호 소프트웨어 기술", *정보통신부 3차년도 보고서*, 1999.1.
[22] 홍기용 외, "메시지 인증 코드 기법을 이용한 위성명령 보안 메커니즘 설계", 종합학술발표대회논문집, *한국통신정보보호학회*, 1994.11.

〈著者紹介〉

손 태 식 (Tae-Shik Shon)
2000년 :아주대학교 정보 및 컴퓨터 공학부 졸업(학사)
2000년~현재 : 아주대학교 정보통신전문대학원 석사과정
〈관심분야〉 네트워크 보안, 인터넷 프로토콜 보안, 자바/리눅스 보안

최 홍 민 (Hong-Min Choi)
2000년 : 아주대학교 정보 및 컴퓨터 공학부 졸업(학사)
2000년~현재 : 아주대학교 정보통신전문대학원 석사과정
〈관심분야〉 네트워크 보안, 리눅스 보안

채 송 화 (Song-Hwa Chae)
1997년 : 아주대학교 컴퓨터공학과 졸업(학사)
1999년 : 아주대학교 대학원 컴퓨터공학과 졸업(석사)
1999년~1999년 9월 : 한국통신프리텔
1999년~2001년 1월 : 한국정보보호센터 인증관리팀
2001년~현재 : 아주대학교 정보통신전문대학원 박사과정
〈관심분야〉 PKI, 무선 통신보안, 전자상거래

서 정 택(Jung-Taek Seo)
1999년 : 충주대학교 컴퓨터공학과(학사)
2001년 : 아주대학교 대학원 컴퓨터공학과(석사)
2001년 11월~현재 : 국가보안기술연구소 연구원
〈관심분야〉 정보전, 시스템 및 네트워크 보안, 시스템 평가

유 승 화 (Seung-Wha Yoo)
1972년 : 서울대학교 공과대학 응용수학과 졸업(학사)
1980년 : University of Kansas(미국) Computer science(석사)
1983년 : University of Kansas(미국) Computer science(박사)
1983년~AT&T Bell Labs. 연구원, Amdahl Corporation. 수석연구원, 삼성전자 정보통신 전무, 충남대학교 공과대학 겸임교수, 한국정보과학회 부회장, 한국네트워크 연구조합 이사장 역임
1999년~현재 아주대학교 정보 및 컴퓨터 공학부 교수
〈관심분야〉 고급국지 통신망, 망관리, VoIP

김 동 규 (Dong-Kyoo Kim)
1973년 : 서울대학교 공과대학 응용수학과 졸업(학사)
1979년 : 서울대학교 자연과학대학원 전자계산학과(석사)
1984년 : 미국 Kansas State University 전자계산학과(박사)
1986년~IEEE 802.4,802.6,802.10 Working Group Member. Asiacrypt '96 조직위원회 위원장, 건설교통부 항공교통관제소 신항공 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국통신정보보호학회 부회장 역임
1979년~현재 : 아주대학교 정보 및 컴퓨터공학부 교수
〈관심분야〉 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링