위성통신망을 위한 보안 프레임워크에 관한 연구

서정택°, 이규호, 박종운, 장준교, 김동규

아주대학교 컴퓨터공학과

Study on the Security Framework for Satellite Communication

Jung-Taek Seo°, Kyu-Ho Lee, Jong-Woon Park, Jun-Kyo Jang, Dong-Kyoo Kim

Department of Computer Engineering, Ajou University

요 약

현재 위성통신망의 활용도가 증가하고 있으며 그 의존도가 높아지고 있다. 그러나 위성통신망은 동보성, 광역성의 특성상 보안상의 취약점을 내포하고 있다. 본 논문에서는 위성통신망의 보안 위협요소를 분석하여 이에 필요한 보안기능 요구사항을 도출하며, 안전한 위성통신망 체계를 위해 통합 정보보호 엔진을 활용한 보안 프레임워크를 제시한다.

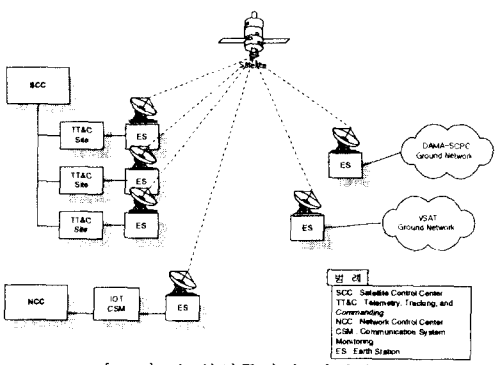
1. 서 론

21 세기의 지식정보화 사회는 정보통신의 초고속화, 광대역화, 멀티미디어화, 그리고 이동성 등을 특히 요구하게 되며, 이러한 요구를 만족시키기 위해 지상망과 위성망을 하나의 통합망 형태로 운영하는 방식이 이용되고 있다. 위성에 의한 망 구축은 동보성, 광역성, 이동성, 광대역성, 회선 설정의 유연성, 안정성 등 위성 고유의 특성과 지진 및 긴급상황 등에 대처하기 쉬워 광케이블보다 비용 면에서 효율적이며, 고품질, 대용량의 통신체계를 지원한다. 그 이용도 통신, 기상, 방송, 자원탐사, 군사위성 등 다양하게 이용되고 있다. 또한 네트워크 속도에 지친 인터넷 사용자들에게 고속의 데이터 통신을 가능하게 함으로써 수요를 높이고 있다.[4]

반면 위성통신망이 가지는 동보성, 광역성 등의 특성상 위성통신망은 많은 보안상의 취약점을 내포하고 있다.

본 논문에서는 위성통신망에 존재하는 여러 보안 위협요소를 체계적으로 분석하고 보안 요구사항을 정보보안 측면과 신호보안 측면에서 도출하였다. 두 가지 측면 중 정보보안 측면에서 그에 상응하는 대처 기법으로 통합 정보보호 서비스 엔진을 이용한 안전한 위성통신망을 제시한다.

2. 위성통신망 시스템 구조



[그림 1] 위성통신망 전체구조

3. 현 위성 통신망의 문제점

위성통신망의 특성상 Level 0, Level 1, Level 2 의 3 단계로 구분하여 각 통신상의 보안 위협요소를 도출하여 분석한다.

3.1 Level - 0 (위성 전파 신호)

: 위성 통신 전파 신호의 공격노출 위험성

• Spread Spectrum : PN(Pseudo Noise) sequence 에 의한 주파수 대역 확산 기술로 PN sequence 가 일치하지 않는 다른 모든 신호들을 잡음으로 간주하여 특정 개인에 대한 정보를 보호할 수 있다. 즉, PN sequence 를 알고 있는 개체만이 정보를 해독할 수 있다.

• Frequency Hopping : 시간에 따른 주파수 대역 변화로 특정 주파수 대역의 도청을 방지할 수 있다. 각 개인마다 고유한 주파수 대역의 sequence 를 설정할 수 있으므로 보안의 목적을 달성할 수 있다.

• Scrambling : 송신 프로그램인 영상, 음성과 데이터

서비스를 정당하지 않은 사용자는 이용하지 못하도록 신호의 특성을 변화시킨다.

위와 같은 기술들이 사용될 경우, Random Sequence, bit permutation 등이 포함되어 있어, 보안적 특성을 지니고 있으나, Security 를 완전히 보장할 수 있는 것은 아니다.

3.2 Level - 1 (위성 관제 데이터)

: 위성 제어에 필요한 데이터 송수신 레벨

• 수신 가능한 모든 지점에서 위성의 수신안테나로 신호 송신 가능

• 정당하지 않은 사용자의 위성 제어 엑세스 가능

• 제 3 자의 고의적인 저 출력 방해전파에 의한 위성 무력화 가능 (위성 제어 데이터 전송 방해로 가용성 손실)

3.3 Level - 2 (일반 응용 통신 데이터)

: 위성통신 기반 위의 응용 통신수준의 데이터 송수신 레벨

• 정당하지 않은 사용자의 위성 접근 가능

• 위성으로부터 지상으로 송신되는 다운링크의 노출로 도청 및 통신 기만이 용이

• 위성통신의 특성상 유선망의 회선 tapping 같은 방법보다 훨씬 쉽게, 많은 다운링크 정보를 얻을 수 있다. (암호화된 데이터의 경우도 많은 샘플을 얻을 수 있어 암호화 해독이 유선망 보다 용이)

4. 위성통신망 보안 요구사항

기존의 위성통신 시스템 및 보안 위협요소를 정보보안 측면과 신호보안 측면으로 구분하여 요구사항을 도출하고 요구사항에 대한 대처 기법을 제시하고자 한다.

4.1 정보보안 측면[1]

• 사용자 신분 확인 및 인증 : 위성통신 시스템에 접속을 시도하는 대상이 사전에 허가된 대상인지를 확인하여 불법적인 대상으로부터 위성통신 시스템과 정보를 보호하는 것

• 비밀성 유지 및 보장 : 위성통신 시스템을 통하여 전송되는 데이터가 확인되지 않고 인가되지 않은 상대방에게 노출되지 않도록 보호하는 것

• 무결성 유지 및 보장 : 위성통신 시스템으로 통하여 송수신 되는 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호하고, 정보가 변조된 경우에는 이를 탐지해 내고, 정당한 사용자에게 경고해 주는 것

• 데이터 발신처 확인 : 원격지로부터 전송 받은 데이터가 원하는 곳으로부터 올바르게 전송된 것인지를 확인하는 방법으로서 위성통신 시스템을 통하여 송수신 되는 정보는 반드시 확인된 발신처로부터 정확하게 전송되도록 하는 것

• 통신 사실의 부인 방지 : 위성통신 시스템에서 송신측과 수신측이 통신에 참여했던 사실을 부인하지 못하도록 하는 방법으로서 통신 경로 및행위 추적을 위한 기능

• 인가된 접근 허용 : 위성통신 시스템에서 허가된 사용자에게만 접근을 허용하며, 접근이 허가된 사용자일지라도 허가된 범위 내에서만 정보 자원의 이용과 상호 통신이 가능하도록 하는 것

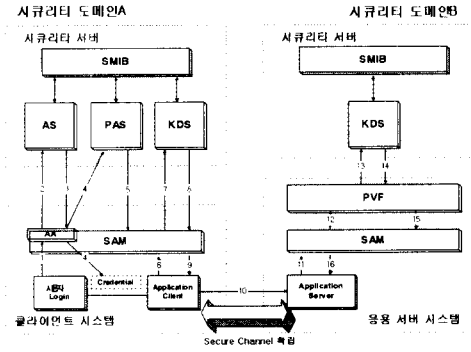
4.2 신호보안 측면

• 가용성의 향상 : 위성제어 데이터의 송수신을 위한 전파의 가용성을 향상시킴으로써, 서비스 거부(Denial Of Service) 공격을 사전에 차단하기 위한 연구

• 신호 왜곡 방지 : 전파의 특성을 이용한 공격 및 에러검출 및 정정 기술에 관한 연구

5. 위성통신 체계에 적용하고자 하는 통합 정보보호 서비스 엔진

통합 정보보호 서비스 소프트웨어 엔진은 인증 서비스를 기반으로 기밀성 서비스, 무결성 서비스, 접근통제 서비스, 부인방지 서비스를 복합적으로 제공하기 위해 인증서버, 권한 속성 서버, 키 분배 서버, 암호화 함수 모듈, 정보보호 관리 정보 베이스로 하부 메커니즘이 구성되어 있다.[2][3]



[그림 2] 통합 정보보호 서비스 엔진 시스템 구조

5.1 인증 서버(AS : Authentication Server) : 사용자가 통신망 상에 존재하는 자원을 사용하기 위해, 먼저 스마트카드를 이용해 인증 서버로부터 인증을 받아야 한다. Challenge-Response 스킴이 이용되며, 인증 결과로서 신임장을 발급 받게 된다. 신임장은 SSO(Single-Sign-On)방식을 이용하여 단 한번의 인증으로 통신망을 계속해서 사용 가능하다.

5.2 권한속성 서버(PAS : Privilege Attribute Server) : 인증 서버로부터 받은 티켓을 검증하고, 검증 후에 통신 서비스를 받으려고 하는 객체의 정보를 SMIB 로부터 넘겨받아 이를 바탕으로 객체의 권한 속성 및 접근권한을 규정하고 이를 서버 측에 기밀성과 무결성을 지켜가며 안전하게 전달한다.

5.3 키 분배 서버(KDS : Key Distribution Server) : 통신 채널을 확립하기 위해 필요로 되어지는 세션키를 키 분배 서버의 공개키 암호화 시스템을 이용하여 안전하게 분배하는 일을 수행한다. 또한 사용자의 레벨에서 공개키 암호화 시스템을 적용하지 않고 이를 한 레벨 올려 세션키 분배를 성취함으로써 공개키 기반 구조의 효율을 높였으며 사용자가 관리해야 하는 키의 수를 줄임으로서 사용자의 편리성을 증진시킬 수 있게 설계되었다.

5.4 안전한 문맥 연결 관리기(SAM : Secure Association Management) : 통신상의 응용 프로그램이 통합 정보보호 서비스 소프트웨어 엔진을 이용할 수 있는 중개자의 역할을 수행한다. GSS-API 를 이용한다.

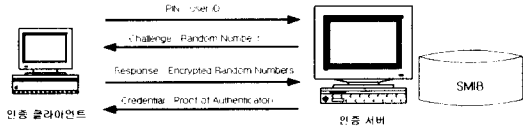
5.5 SMIB(Security Management Information Base) : 인증 관련 정보, 키 관련 정보, 부인방지 관련 정보, 로그 정보, 시스템 관련 정보 등을 각 시큐리티 서버 및 관리 시스템과 기밀성 및 무결성을 유지하며 통신하도록 구현되

었다.

5.6 정보보호 서비스 관리기능(SMF : Security Management Function) : 각 서버들의 작동 및 관리 기능, 시큐리티 도메인 내의 사용자 등록, 수정, 삭제의 관리기능, 그리고 시큐리티 도메인 내에서 제공되는 서비스의 목록을 관리하는 기능 및 로그 파일을 관리하는 기능을 수행한다.

6. 통합 정보보호 서비스 엔진 기반 위성통신망 보안 프레임워크

6.1 사용자 신분확인 및 인증 서비스 : 토큰을 이용한 사용자 신분확인 시스템은 인증 클라이언트의 요청을 받아 인증 서버가 SMIB 에 접근하게 되며, SMIB 에 있는 해당 사용자의 정보를 이용하여 정당한 권한을 가진 사용자로 증명이 되면, 인증 서버는 사용자에게 해당 응용에 접근할 수 있는 신임장(Credential)을 발부하게 됨으로 모든 사용자 인증 작업이 마무리 되게 된다. 이러한 일련의 수행과정을 다음과 같다.



[그림 3] 지능형 토큰 이용 사용자 신분확인 시스템 구조

① 인증 클라이언트는 사용자 식별자(Identifier)를 인증 서버에게 전달한다.

② 인증 서버는 인증 클라이언트로부터 받은 사용자 식별자를 가지고, SMIB 에 있는 패스워드를 찾아 인증 클라이언트와 Challenge-Response 를 수행한다.

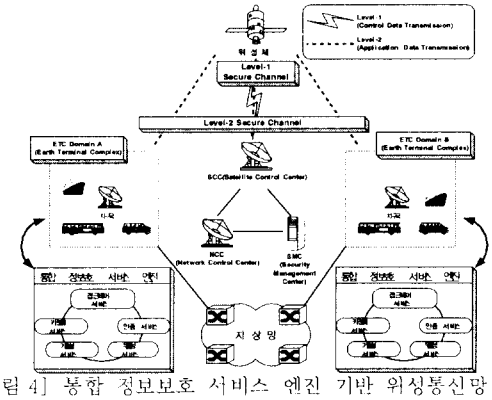
③ Challenge-Response 수행 결과, 사용자가 정당한 권한을 가진 것으로 확인되면, 인증 서버는 인증 클라이언트에게 응용 서비스를 이용할 수 있는 신임장(Credential)을 발부하게 된다.[1]

6.2 기밀성 및 무결성 서비스 : 기존의 암호화 알고리즘을 미리 프로그램으로 구현하고 간단한 함수 형태의 Interface 를 지원하는 라이브러리로 만들어 놓은 CSF(Cryptographic Support Facility)를 이용한다. 이 모듈은 키 분배 서비스, 각 서버간 메시지 전송, 전자서명 등에 사용되어 기밀성 및 무결성 서비스를 제공 한다. CSF 의 사용 알고리즘의 예는 다음과 같을 수 있다. 하지만, 이 부분은 구현 방법에 따라 다른 알고리즘들로 대치될 수 있다.[2]

- 대칭 암호화 및 복호화 → DES-CBC
- 비대칭 암호화 및 복호화 → RSA
- 단방향 해쉬 → MD5(Message Digest 5)

6.3 접근제어 서비스 : 사용자는 자신의 권한에 대해 증명을 할 수 있어야 하는데, 사용자 권한에 대한 인증서를 발급해 주는 기능을 하는 곳이 PAS 이다. 시큐리티 도메인 내에서 사용자가 자원에 접근하여 오퍼레이션을 하려면 AS 에서 정당한 사용자임을 인증 받아야 하고, 인증된 사용자는 AS 가 발행한 PAS 티켓을 가지고 PAS 에 의해 권한 속성을 검증 받아야 한다. 이 과정을 거친 사용자는 PAS 가 발행한 PAC 을 가지고 자원에 접근하고, 자원이 있는 응용서비스 서버는 자신의 접근제어 정책에 따라 PAC 안의 사용자 정보와 직무를 응용서비스 서버의 접근제어리스트 (ACL - Access Control List) 와 비교하여 접근제어를 결정하게 된다. 접근제어 절차는 다음과 같다. 먼저 접근요청을 위해 제출된 PAC 의 정보에 의해 사용자 ID 에 의한 사용자의 식별과 사용자와 그 사용자가 속한 그룹과 연계하여 적절한 권한이 부여된다. 이 절차를 지원하기 위해서 접근제어에 대한 ACL 의 적절한 관리가 필수적이다. ACL 관리자는 그룹의 권한 부여를 정의하고 그룹과 권한에 대한 매핑을 하면 된다.[2]

6.4 부인방지 서비스 : 비대칭키 암호화 시스템을 사용하면서도 부인방지 증명서의 생성을 통신 당사자가 생성하지 않고 상위의 신뢰할 수 있는 시큐리티 서버가 생성하게 함으로써 통신 당사자 사이에 공정성을 유지할 수 있다. 설계된 프로토콜에서는 증명서 생성이 시큐리티 서버에서 이루어지므로 자체적으로 신뢰할 수 있는 타임 스탬프를 사용하여 증명서의 유효 시간과 만료 시간을 신뢰할 수 있게 하였다. SMIB 에 부인방지 증명서가 저장됨으로 추후에 분쟁 발생시 저장된 증명서에 의해 분쟁을 해결하게 했으며 사용자는 SMIB 에 접근 할 수 없기 때문에 임의로 증명서를 변조할 수 없기 때문에 증명서의 신뢰성을 높였다.[3]



[그림 4] 통합 정보보호 서비스 엔진 기반 위성통신망 보안 프레임워크

7. 결론 및 향후연구방향

본 논문에서는 위성통신망에서 보안 위협요소를 분석하고 보안 요구사항 도출하였으며 정보보안측면에서의 대응방안으로 통합 정보보호 서비스 엔진 모델을 보완 및 재설계하여 위성통신망에 적합한 통합 정보보호 프레임워크를 제시하였다. 향후 통합 정보보호 서비스 엔진에서 제공하는 인증, 기밀성, 무결성, 접근제어, 부인방지 서비스를 위성환경에 알맞게 보완하고 재설계하여 위성통신망에서의 보안상의 취약점을 극복할 수 있다.

참고 문헌

[1] 김동규외, 분산통신망 환경 통합 정보보호 소프트웨어기술, 1 차년도 보고서, 정보통신부, 1997.01

[2] 김동규외, 분산통신망 환경 통합 정보보호 소프트웨어기술, 2 차년도 보고서, 정보통신부, 1998.01

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

[4] 홍기융외, "메세지 인증코드 기법을 이용한 위성명령 보안 메카니즘 설계", 종합학술발표회논문지(CISC'94), 한국통신정보보호학회, 1994.11