공용 위성 통신망의 정보 보호에 관한 연구 [1]

문 희 철, 이 필 중
포항공과대학 전자전기공학과

Technologies for Protection of Information in Public Networks using Communication Satellite

Hee Chul Moon and Pil Joong Lee
Dept. Elec. Eng., POSTECH

요약

위성 통신망은 도청의 위협이 가장 큰 통신망으로 사용자들의 민감한 정보에 대한 프라이버시의 보호가 어려운 통신망이다. 또한 위성통신의 고유한 특성상 위성체를 원격지에서 제어해야 하므로 위성 제어 신호에 대한 안전한 인증(authentication) 메카니즘이 필요하다.

본 연구에서는 공용 위성 통신망에서 사용자의 프라이버시를 위한 암호시스템과 위성 제어 신호의 안전한 인증 메카니즘을 제시하고자 한다.

1. 서론

위성통신은 전파범위(beam coverage)가 넓은 이유로 도청에 대한 위협이 가장 큰 통신 수단이다. 위성 통신 신호의 불법적인 도청을 위해서는 상당한 돈과 기술이 필요할 것으로 생각되나 정보의 누출이 있어서는 안 될 민감한 정보를 위해서는 위성과 지구국 사이의 링크가 보호되어야 한다. 이 보안 기능은 권한이 있는 수신 지구국을 제외한 어느 누구도 위성과 지구국 사이를 오가는 데이타를 해독하지 못하게 하는 것이다.

[1] 본 논문은 한국전자통신연구소 위성통신기술본부에서 수탁한 연구의 결과임.

연구 대상인 공용 위성 통신망에는 국간 중계망과 도서벽지 / 특수통신망이 있다. 국간 중계망은 주요 도시에 위치하는 소수의 국간 중계국으로 이루어지는 통신망이며 도서벽지 / 특수통신망은 도서 벽지 통신, 행정 통신, 군사 통신, 비상 재해 통신 등을 위한 통신망으로 소용량의 트래픽을 갖는 다수의 지구국으로 구성된다.

본 연구에서는 국간 중계망과 도서벽지/특수통신망에 대한 통신보안의 문제점을 각각 분석하고 그 해결을 위한 암호시스템을 제안한다. 그리고 암호시스템에 이용되는 암호키이 관리 프로토콜과 부수적으로 따르는 문제인 키이 스트림 (key stream)의 동기화에 대하여 문제점을 논하고 해결책을 제시한다.

인공위성은 고유한 특성상 위성의 동작 상태, 자세 및 위치 등을 원격지에서 명령 신호를 보내 제어해야만 한다. 만약 위성을 제어하는 명령 신호에 대한 인증 메카니즘이 불안전하면 악의를 가진 사람에 의해 위성이 사보타지 (sabotage) 될 수 있다. 따라서 위성은 수신되는 명령신호가 진정한 권한이 있는 자로부터 송신된 것인가를 확인할 수 있는 방법이 필요하다. 본 연구는 위성 제어 신호의 안전한 인증을 위한 암호 프로토콜을 제시한다.

그러나 위의 보안 기능들이 위성 통신망에 추가됨에 따라 사용자의 불편이 초래되어서는 안 될 것이다. 특히 통신상에서 이루어지는 모든 과정은 투명 (transparent) 하여 사용자들은 자신의 통신내용이 중간에 암 / 복호화를 거치는지를 알 수 없도록 해야 하며 통신 데이타에 부담이 크지 않고 통신 품질의 저하가 없어야 한다.

2. 암호시스템

암호화 방법은 크게 블록 암호 (block cipher) 와 스트림 암호 (strem cipher) 가 있다. 블록 암호는 데이타의 크기를 큰 블록 단위로 나누어 암호화하는 방법이며 스트림 암호는 비트나 문자와 같은 작은 데이타 단위를 암호화할 때 이용한다. 위성통신의 보안을 위해서는 어떤 암호 방식이 유리하며 어떤 특성을 가지고 있는지에 대한 분석이 필요하다. 본 연구에서는 관용 암호시스템만을 고려하며 공개키이 암호시스템은 이용하지 않는다.

2.1. 블록 암호 (block cipher)

블록 암호는 메시지를 일정한 길이의 블록으로 나누어 개개의 블록을 다른 블록과는 무관하게 암호화한다. 블록 암호에는 DES (Data Encryption Standard) [1] 나 FEAL

(Fast Encryption ALgorithm) [2] 과 같은 여러가지 방식이 있으며 사용 방식에는 ECB (electronic codebook), CBC (cipher block chaining), CFB (cipher feedback), OFB (output feedback) 의 4 가지 방식 [3][4] 이 있다.

그러나 블록 암호의 ECB, CBC, CFB 방식은 암호문의 전송 도중 한 비트의 에러만 발생해도 암호문을 복호했을 때 메시지 블록의 전반에 걸쳐 에러가 발생하는 에러확산 (error extension) 현상 [5] 이 나타난다. 에러확산 성질은 통신 품질의 저하를 초래하므로 높은 품질의 통신이 요구되는 위성통신에서는 위의 세 방식이 적합하지 않다. 블록 암호의 OFB (output feedback) 방식은 에러확산 성질이 없는 방식이므로 위성통신의 암호방식으로 적합하다.

OFB 방식은 그림 1 에서처럼 암호 모듈 (encryption module) 의 출력이 다시 입력으로 피드백 되어 결과적으로 일종의 의사난수 스트림 (pseudo-random stream) 을 출력한다. 이 의사난수 스트림은 그림 1 에서 보는 쉬프트 레지스터 (shift register) 의 초기값과 암호 키이의 값에 의해 계속되는 모든 값이 결정되는 특징이 있다.

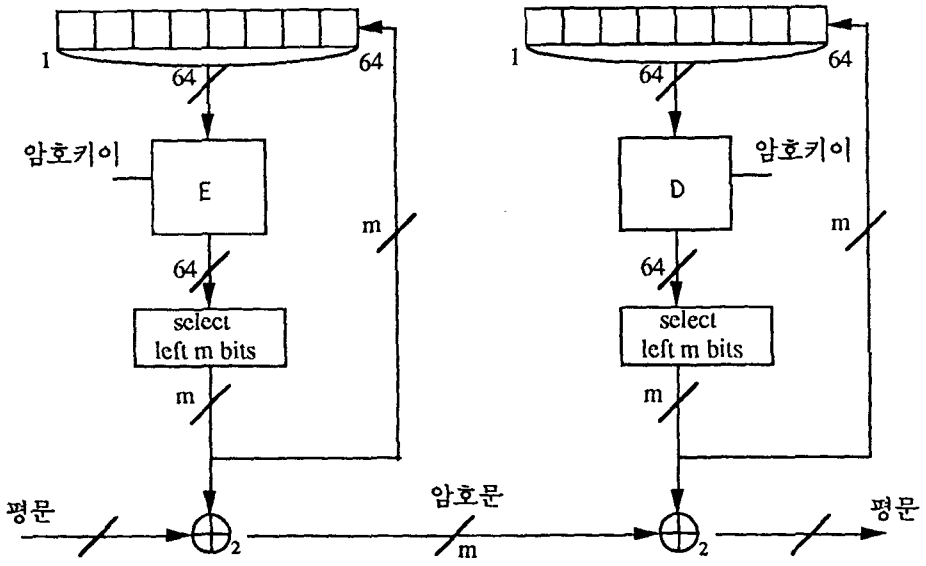

그림 1. 블록 암호의 OFB (output feedback) 식의 사용방식

의사 난수 스트림은 평문을 암호화할 때 XOR (eXclusive OR) 되고 복호할 때 다시 같은 의사난수 스트림을 XOR 하여 원래의 평문을 찾는다. 따라서 암호문의 송신측과 수신측이 의사 난수 스트림을 동기화 하는 것이 중요하며 만일 암호문의 전송 도중 한 비트라도 잃어버리거나 추가되는 동기화 에러 (synchronization error) 가

발생하면 OFB 방식은 이를 스스로 재동기하지 못한다. 이는 마치 스트림 암호 (stream cipher) 의 동기 스트림 암호 (synchronous stream cipher) 방식의 경우와 같다.

2. 스트림 암호 (stream cipher)

스트림 암호는 메시지를 시간에 따라 변하는 함수를 이용하여 암호화하는 방법으로 그 함수는 스트림 암호의 내부상태와 관련있다. 내부 상태란 기억장치 (register) 에 저장된 값으로 처음에 초기값이 주어지면 계속 상태를 변화시켜가며 암호키이와 더불어 키이 스트림 (key stream) 을 만든다. 키이 스트림은 그림 2 와 같이 평문에 XOR 되어 암호문을 만들고 복호할 때 같은 키이 스트림이 XOR 되어 원래의 평문을 복원한다.

스트림 암호에는 동기 스트림 (synchronous stream) 암호방식과 자가 동기 (self-synchronizing) 스트림 암호방식이 있다. 그 중 자가 동기 스트림 암호 방식은 에러 확산 성질이 존재하여 위성통신에 적합하지 않고 동기 스트림 암호 방식은 스트림 암호의 내부상태가 전 내부상태에만 의존하므로 에러 확산 성질이 없다. 그러나 그림 2 에서 볼 수 있듯이 블록 암호의 OFB 방식과 마찬가지로 동기화 에러의 문제가 있다.

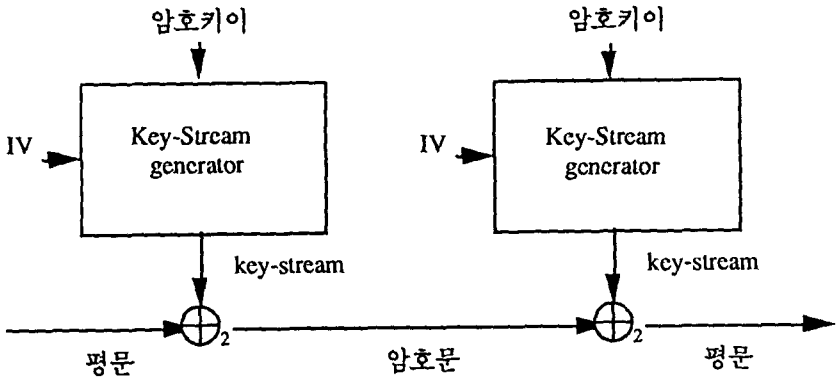

그림 2. 동기 스트림 암호 (synchronous stream cipher)

3. 국간 중계망

국간 중계국은 주요 도시의 시외 전화국에 설치되는 PCM 전화 회선 및 고속 데이타 회선용 중계국이다. 국간 중계에 할당되는 위성 중계기는 54 MHz 급 2 개

로서 2 개의 TDMA 위성망이 설치된다. 국간 중계 서비스를 위한 망은 주요 도시간의 트래픽을 전송할 수 있는 TDMA 단말 지구국 시스템들과 망을 제어하기 위한 하나의 제어국으로 구성되며 단말 지구국중의 하나가 제어국의 기능을 수행한다.

3.1. 국간 중계망의 암호시스템

국간 중계망에서 위성과 지구국간의 링크를 보호하기 위해서는 송신 지구국에서 암호시스템을 이용하여 상향 링크 (up-link) 의 신호를 암호화하고 수신국에서 하향 링크 (down-link) 의 신호를 다시 복호화한다. 위성은 본래의 중계 기능을 수행할 뿐이고 메시지의 암/복호화와는 관계가 없도록 한다.

국간 중계망의 암호방식으로는 블록 암호의 OFB 방식이나 스트림 암호의 동기 스트림 암호방식을 이용할 수 있으나 대용량의 메시지를 처리해야 하는 국간 중계망에서는 동기 스트림 암호방식이 데이타의 처리 속도면에서 적합하다.

스트림 암호로 이용될 알고리즘은 암호에 쓰이는 모든 하드웨어가 알려지고 많은 양의 암호문과 그에 해당하는 평문을 가지고 있어도 암호키이를 알아낼 수 없어야 한다. 동기 스트림 암호방식의 경우 암호를 해독하려는 자가 많은 양의 키이 스트림을 관찰하여도 앞으로 나올 키이 스트림의 예측이 불가능해야 한다. 즉 키이 스트림의 주기가 매우 길고 불규칙성이 충분해야 한다.

3.2. 암호키이의 관리와 교체

스트림 암호의 키이 스트림은 암호키이에 의하여 결정되므로 송신 지구국과 수신 지구국은 같은 키이 스트림을 생성하기 위해서 같은 암호키이를 사전에 공유해야 한다. 암호키이는 모든 국간 중계국이 같은 암호키이를 이용할 수도 있고 각 국간 중계국 사이마다 다른 키이를 이용할 수도 있다.

모든 국간 중계국이 같은 암호키이를 이용한다면 각 국간 중계국이 하나의 키이만을 보유하면 되므로 키이 관리면에서 간단하다는 장점이 있다. 그러나 일단 암호키이가 노출되면 모든 국간 중계국간의 통신내용이 해독 가능해지므로 위험이 크다는 단점을 가진다.

만약 6 개의 국간 중계국이 서로간의 통신 링크 마다 다른 암호 키이를 이용한다면 15 개 ($_6C_2$) 의 암호키이가 국간 중계망에 필요하다. 각 국간 중계국은 다른 5 개의 중계국과의 통신용으로 각 하나씩의 암호키이를 보유하므로 만일 한 국간 중계국의 모든 암호키이가 노출된다 하더라도 다른 다섯 국간 중계국 사이의 통신은 조금도 피해를 받지 않는 장점이 있다. 물론 각 국간 중계국이 보유해야 할 암호키이가 많아

지므로 키이관리가 복잡해지는 단점이 있으나 중계국의 수가 작다면 큰 문제가 되지 않는다.

그런데 암호키이는 하나의 암호키이를 너무 오래 이용하거나 그 암호 키이를 이용하여 너무 많은 암호문이 생성되면 암호해독의 위험이 커지므로 이를 막기 위해 암호키이를 주기적으로 교체해야 한다. 암호키이의 교체에는 여러 방법이 있을 수 있으나 각 중계국의 암호 시스템에 앞으로 쓰일 암호키이를 안전한 TRM (tamper resistant module) 에 저장해 두고 주기적으로 암호키이를 교체하는 방법이 가장 효율적이라고 판단된다. 지구국 A 에 필요한 암호시스템은 그림 3 과 같다.

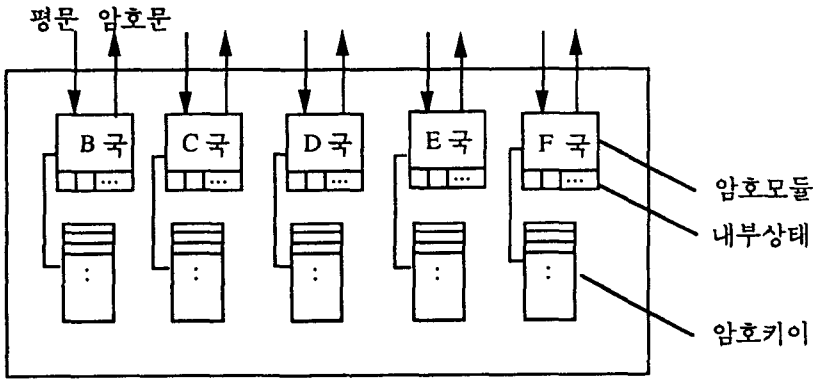

그림 3. 국간중계망 지구국의 암호시스템

암호키이를 교체할 때에는 송신과 수신의 양 측이 동시에 이루어져야 하므로 암호키이의 교체에 있어 동기화 문제가 발생한다. 이 동기화 문제를 해결하기 위한 방법은 여러가지가 있을 수 있다. 그 중 한가지는 사용자들의 이용이 뜸한 지정된 시간에 암호키이를 교체하는 것이다. 그러나 모든 국간중계국의 시계가 동기화 되어야만 키이를 동시에 정확히 교체할 수 있고 또한 교체 예정시간 전후로 얼마간의 시간에는 통신을 두절하여야 하는 단점이 있다. 만약 이 방식을 이용하여 키이 교체를 한다 해도 다른 중계국이 암호 키이의 교체를 올바르게 수행했는지를 알 수 없으므로 다른 확인 수단이 필요할 것이다.

다른 방법으로는 메모리에 저장해 놓은 암호키이 마다 식별번호를 부여하고 송신국이 통신중에 주기적으로 현재 사용중인 암호키이의 식별번호를 전송할 수 있다 [6]. 수신국측에서는 사용중인 암호키이의 식별 번호가 아닌 다른 식별번호가 두번째로 수신되었을 때 암호키이를 새로운 식별번호가 지정한 것으로 교체한다. 수신측에서는 항상 식별번호를 체크하므로 현재 이용중인 암호키이가 올바른 것인지 확신을

가질 수 있으며 교체 도중에 통신을 두절해야 하는 문제를 해결할 수 있다. 그러나 이 방법은 송신기능이 없고 수신기능만 있는 지구국이 있을 때 유용하지만 관심대상인 국간 중계망에서는 모든 지구국이 송/수신이 가능하므로 큰 장점이 없다. 특히 주기적으로 식별번호를 송신해야 하므로 통신의 부담이 증가하는 단점이 있다.

가장 좋은 방식으로 생각되는 것은 각 국간 중계국간에 암호키이의 교체가 필요하면 상호간의 통신에 의해 암호키이를 교체하는 방법이다. 하나의 암호키이를 이용한 시간이 정해진 시간보다 많아지거나 생성된 암호문의 양이 한도 이상으로 많아지면 두 국간 중계국 중 하나가 키이 교체 요구를 하여 키이 교체 프로토콜을 실행하는 것이다. 키이 교체 프로토콜은 한 국간 중계국이 키이 교체 요구를 하여 양 국간에 다음에 쓰일 암호키이의 식별 번호를 전달하고 이를 확인한 후 새로운 암호키이를 이용하는 것을 말한다. 양 국간의 암호키이 교체에 이용될 채널은 어떤 것이든지 상관없으나 키이 교체 과정은 사람의 손이 필요없이 자동으로 이루어져야 한다.

과거에 이용했던 암호키이는 파기하여 그것을 나중에 읽더라도 알아 볼 수 없도록 해야 한다. 파기하는 방법으로는 암호키이 위에 암호키이와 크기가 같은 랜덤한 숫자를 XOR (eXclusive OR) 하여 암호키이의 흔적을 없앨 수 있다.

3.3. 키이 스트림의 동기화

키이 스트림의 동기화를 위해서는 항상 이를 확인하는 절차가 있어야 하고 혹 동기화가 어긋나면 즉시 재동기가 되어야 하므로 특별한 대책이 요구된다. 이를 위해 통신중에 현재의 내부상태를 주기적으로 전송하는 방식이 하나의 해결책이 될 수 있다[6]. 이 방식은 전송 데이타 프레임중 내부상태를 정기적으로 전송할 타임 슬롯(time slot)이 필요하므로 통신에 부담을 주게 되어 좋지 않은 방법이라고 생각된다.

키이 스트림을 동기화하기 위하여 제안하는 방법은 수신측에서 메시지의 길이와 해당되는 메시지를 복호하기 위해 생성된 키이 스트림의 길이를 비교하여 동기화 에러를 수정하는 것이다. 메시지의 전송 도중 동기화 에러가 생기지 않았다면 이 두 값은 같아야 한다. 왜냐하면 메시지의 크기만큼의 키이 스트림이 생성되어 암/복호화 과정이 실행되기 때문이다. 만약 두 값이 서로 다른 경우에는 내부상태가 송신측과 수신측이 동기화되지 않았음을 알 수 있고 따라서 두 값의 차이 만큼 수신측의 내부상태를 그림 4 처럼 앞이나 뒤로 변화시켜야 한다.

수신 지구국은 TDMA 트래픽 데이타 중에서 자신에게 보내지는 데이타의 시작과 끝 그리고 크기를 알 수 있다. 그리고 그 메시지를 복호하기 위한 키이 스트림은

그림 4 와 같이 카운터 (counter) 를 이용하여 알 수 있다. 내부상태를 변화시킨다는 것은 내부상태가 클록 (clock) 이 있을 때 마다 변화한다고 생각하면 몇 클록 전이나 뒤의 내부상태로 현재의 내부 상태를 변화시킨다는 뜻이다.

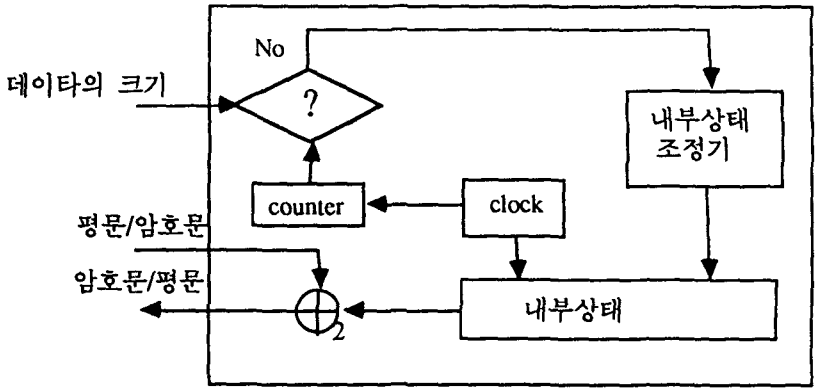

그림 4. Key stream 의 동기화

4. 도서벽지/특수통신망

도서벽지 / 특수통신망은 도서벽지 통신, 행정 통신, 군사 통신, 비상 재해 통신 등의 주로 공공통신을 위한 통신망으로서 소용량 트래픽을 갖는 다수의 지구국으로 구성된다. 도서벽지 / 특수통신 지구국 시스템의 다원 접속 방식은 소용량 트래픽의 전송에 적합한 DAMA/PAMA-SCPC 방식으로 설정한다. 시스템의 망 제어 방식은 망의 집중적인 운용, 관리 및 제어가 가능한 중앙제어 방식을 이용한다.

4.1. 암호시스템

도서벽지/특수통신망에서 위성과 지구국간의 통신정보를 보호하기 위해서 암호시스템을 이용하며 송신 지구국은 상향 링크의 신호를 암호화 하고 수신 지구국은 하향 링크의 신호를 복호화한다. 위성은 본래의 중계 기능만 을 수행하고 데이타의 암/복호화 기능과는 무관하도록 한다.

데이타의 암호화 방식은 통신품질의 저하를 막기 위해 에러확산 현상이 없는 블록 암호의 OFB 방식이나 동기 스트림 암호를 이용해야 하는데 두 방식 중 블록 암호의 OFB 방식이 더 적합하다고 판단된다. 그 이유는 도서벽지/특수통신망 의 지구국은

1 회선당 암호모듈이 하나씩 필요하고 한 회선의 전송속도는 64 Kbps 밖에 되지 않으므로 블록 암호의 속도로도 암호화 처리가 가능하기 때문이다.

4.2. 암호키이의 관리와 교체

도서벽지 / 특수통신망은 소용량의 트래픽을 갖는 다수의 지구국이 이용하므로 다원 접속 방식으로 요구할당방식 (DAMA) 을 이용하며 시스템의 망 제어 방식으로 중앙제어 방식을 이용한다. 이는 각 지구국이나 사용자가 각자에게 할당된 반송파를 장기간 가지지 않고 신호의 전송을 위해 반송파를 사용하고자 할 때마다 중앙 제어국에 요구하여 반송파를 할당받고 전송이 끝나면 사용했던 반송파를 반납하는 방식이다 [7].

도서벽지 / 특수통신망은 이와 같은 특별한 프로토콜을 이용하여 통신 하고자 하는 상대와 접속을 하고 또한 지구국의 수도 많으므로 이에 알맞는 암호키이 관리 프로토콜이 필요하다. 지구국의 수가 많으면 국간중계망처럼 지구국마다 다른 지구국과 통신에 쓰일 암호키이를 저장하기에는 메모리가 많이 필요할 뿐더러 관리상에 있어 절차가 너무 복잡해진다.

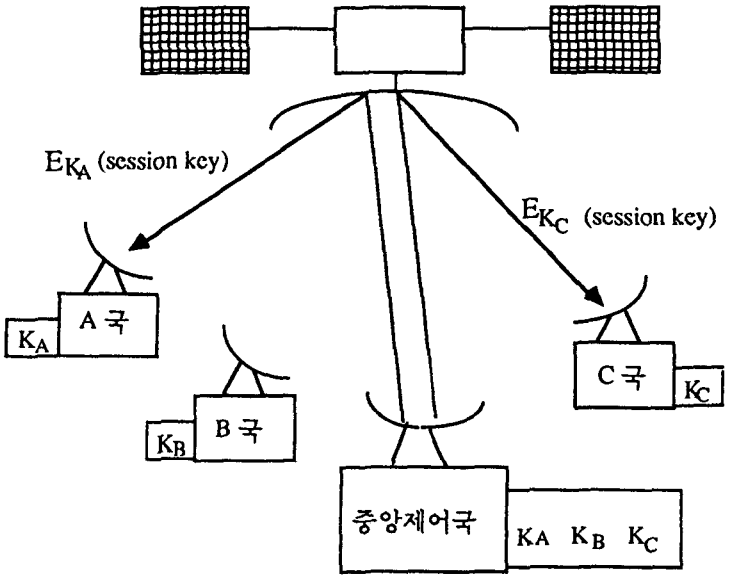

그림 5. 도서벽지/특수통신망의 세션키이 분배

따라서 도서벽지/특수통신망의 특성에 맞는 그림 5 와 같은 키이 관리 방식을 제안한다. 지구국은 국간 중계망의 지구국처럼 다른 모든 지구국과의 통신에 이용할

암호키이를 보유하지 않고 단지 자신의 암호키이 하나만 보유하고 중앙 제어국은 모든 지구국의 암호키이를 소유한다.

각 지구국은 통신회선의 접속시 중앙제어국에서 채널의 할당과 함께 그 세션에 이용할 암호키이를 분배받는다. 만약 A 국이 C 국으로 통신하고자 하여 중앙 제어국에 채널할당을 요구하면 중앙 제어국은 세션에 이용하는 세션키이를 A 국과 C 국에 각 국의 암호키이로 암호화하여 A 와 C 국에 통신회선의 접속시 전송한다 (E_{kA}(scssion key), E_{kC}(scssion key)). 중앙제어국을 제외하면 A국과 C국만이 세션키이를 복호할 수 있고 다른 지구국은 이를 해독할 수 없으므로 세션 키이에 대한 보안이 이루어진다. 이 방식은 기존의 요구할당 방식을 이용한 것으로 새로운 키이관리 프로토콜을 개발할 필요없이 기존의 프로토콜을 수정하여 이용할 수 있는 장점이 있다. 각 지구국에 필요한 암호시스템은 그림 6 과 같다.

도서벽지/특수통신망도 일정한 시간이 지나면 암호키이의 교체가 필요하다. 암호키이의 교체는 각 지구국과 중앙제어국 사이의 문제로서 각 지구국은 다른 지구국들이 암호키이를 교체하는 것을 신경쓰지 않아도 된다. 따라서 지구국의 입장에서 암호키이의 교체가 간단해지고 새로운 지구국이 참여할 때 기존의 지구국에 영향을 끼치지 않고 단지 중앙 제어국만 관계하면 되는 이점이 있다. 지구국과 중앙 제어국과의 암호키이 교체는 암호키이를 사용한 시간이나 세션의 횟수를 기준으로 실행하며 키이 교체 프로토콜을 이용할 수 있다.

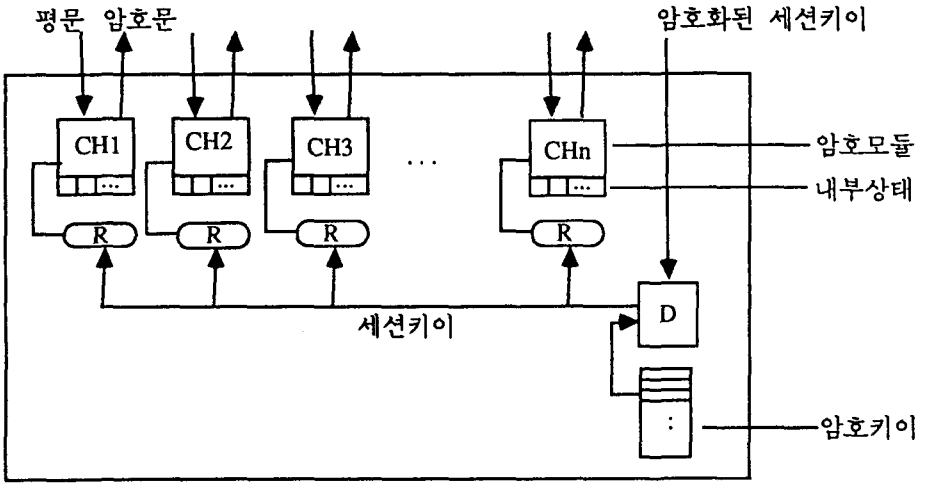

그림 6. 도서벽지/특수통신망 지구국의 암호시스템

4.3. 키이 스트림의 동기화

블록 암호의 OFB 방식도 동기화 에러를 스스로 고칠 수 없으므로 재동기를 시킬 수 있는 수단이 필요하다. 그 대책으로는 그림 4 에서 설명했듯이 데이타의 길이와 생성된 키이 스트림의 수를 비교하여 키이 스트림을 동기화할 수 있다.

5. 위성 제어 신호의 인증

위성의 동작상태의 점검, 자세 및 위치 제어와 동작 제어를 위해 위성 관제소가 필요하다. 위성 관제소는 크게 TT&C (tracking, telemetry & command station) 국과 위성 제어 센타로 분류된다. TT&C 국은 위성으로부터 텔리메트리 (telemetry) 신호를 수신하여 위성을 추적하며 위성제어 센타로부터 출력되는 명령신호를 위성으로 송신하여 위성을 제어한다.

TT&C 국에서 위성으로 전송하는 명령신호는 위성에 의하여 진정으로 TT&C 국으로부터 온 것인지를 확인할 수 있어야 하며 위성으로부터의 텔리메트리 신호 역시 위성 관제소에서 인증할 수 있도록 인증 프로토콜이 필요하다.

5.1. 제어신호의 인증방식

명령신호와 텔리메트리 신호의 인증 프로토콜은 비밀보장, 데이타의 무결성, 재전송 공격 방지의 세가지 목적을 만족해야 한다. 따라서 이를 위한 인증 신호의 형식을 다음과 같이 제시한다.

$$E_k\{M, SeqNo, H(M, SeqNo)\}$$

E는 보호할 데이타 M의 비밀보장을 위한 암호화 함수이며 k는 위성과 관제소의 공유키이다. M은 보호할 데이타인 명령신호 또는 텔리메트리이며 SeqNo는 데이타의 재전송을 막기 위해 사용하며 해쉬함수[8]인 H는 M과 SeqNo의 무결성을 보장하기 위해 이용한다.

5.2. 암호키이의 관리 및 키이 스트림의 동기화

위성과 위성 관제소 사이에 이용되는 암호키이는 두개의 TRM (tamper resistent module) 에 저장하여 하나는 위성을 쏘아 올릴 때 탑재하고 다른 하나는 위성 관제소

에서 이용한다. 암호키이의 교체는 일정시간이 지나거나 전송된 메시지의 양이 일정 한도를 넘을 때 자동으로 키이교체 프로토콜을 수행하도록 한다. 특히 *SeqNo* 는 레지스터라고 볼 수 있으므로 *SeqNo* 가 되풀이되기 전에 키이를 교체하여야 한다.

위성제어 신호의 인증에 이용되는 암호시스템도 에러확산 성질이 없는 블록 암호의 OFB 방식이나 동기 스트림 암호를 이용해야 하므로 키이 스트림의 동기화 수단이 필요하다. 이는 국간 중계망이나 도서벽지/특수통신망과 마찬가지로 메시지의 길이와 생성된 키이 스트림의 수를 비교하는 방법을 이용할 수 있다.

6. 결론

본 고에서는 공용위성 통신망인 국간 중계망과 도서벽지/특수통신망에 이용할 암호시스템을 제안하였으며 암호시스템을 이용할 때 문제가 되는 암호키이의 관리 및 교체의 문제를 분석하고 대책을 제시하였다. 그리고 제안된 암호시스템에서 나타나는 키이 스트림의 동기화 문제에 대해 논하였고 해결책을 제안하였으며 위성제어 신호의 안전한 인증을 위한 프로토콜을 제시하였다.

참고문헌

[1] "Data Encryption Standard", FIPS PUB 46, Jan., 1977.

[2] A. Shimizu and S. Miyaguchi, "Fast Data Encryption Algorithm FEAL", EUROCRYPT '87, April, 1987.

[3] DES modes of operation, FIPS PUB 81, Dec. 1980

[4] Information processing - modes of operation for a 64-bit block cipher algorithm, ISO 8372, Geneva, 1987

[5] D.W.Davis and W.L.Price, "Security for Computer Network", John Wiley & Sons, 1989

[6] Serpell, S.C., and Brookson, C.B. "Encryption and Management for the ECS Satelite Service", Proceedings of EUROCRYPT 84, Paris, France, April, 1984, pp. 437-445.

[7] 홍완표, "인공위성과 위성통신", Ohm 사, 1990