

광대역 위성 액세스 망 분석 및 규격 제안

오 흥 룡*, 김 문 기**, 류 종 호***, 김 락 현*, 염 흥 열*

요 약

본 논문에서는 국내 광대역 위성 액세스 망(BSAN: Broadband Satellite Access Network)에 적용 가능한 보안 기능을 위한 가이드 라인을 살펴보고, RCST(Return Channel Satellite Terminal)와 NCC(Network Control Centre)간에 인증 및 키 관리 기능을 위하여 요구되는 주요 핵심 보안 메커니즘에 대하여 기술한다. 더불어 국내 광대역 위성 액세스 망의 ETSI(European Telecommunications Standards Institute) 표준을 분석한다. 특히 위성 망에서 이용되는 세 가지 키교환 메커니즘 MKE(Main Key Exchange), QKE(Quick Key Exchange), EKE(Explicit Key Exchange)에 대해 분석하였으며, 국내 보안 알고리즘과 키교환을 위한 향상된 보안 알고리즘을 적용한 규격을 제안하였다.

I. 서 론

본 논문에서는 국내 광대역 위성 액세스 망(BSAN)에 적용 가능한 보안 기능을 위한 가이드 라인을 살펴보고, RCST와 NCC 간에 인증 및 키 관리 기능을 위하여 요구되는 주요 핵심 보안 메커니즘에 대하여 기술한다.

이를 위하여 기존의 위성 액세스 망의 국제 표준인 ETSI에서 표준화된 EN 301 790 표준에서 보안 영역을 분석하였고, 이를 근거로 광대역 위성 액세스망 보안을 위하여 요구되는 기본 암호 기술을 분석하였다. 그리고 이를 근거로 국내 광대역 위성 액세스망 보안을 위한 가이드라인을 기술하였다.

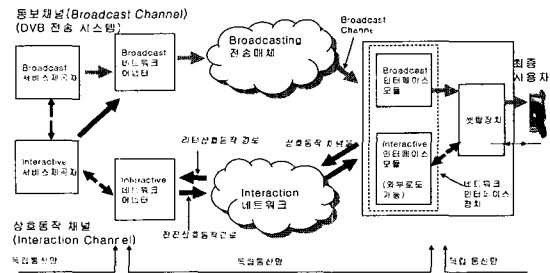
보안 기능을 위한 암호 프리미티브는 대칭성 암호 알고리즘, DH(Diffie-Hellman) 공개키 교환 알고리즘, 해쉬 알고리즘, 그리고 HMACSHA-1 알고리즘 등이 필요함을 제시하고, 또한 국내 광대역 위성 액세스망을 위한 가이드라인을 기술하였다. 여기서는 보안 기능을 위하여 이용될 수 있는 다양한 채널을 고찰하고, 국내 광대역 위성 액세스망을 위하여 요구되는 암호 프리미티브의 종류를 본 논문의 II장에서 제안하였다.

II. 본 론

1. ETSI EN 301 790 V1.2.2 개요

본 장에서는 위성망에서의 보안방식을 설명한 ETSI EN 301 790 V1.2.2의 개요에 대하여 설명한다. [그림 1]은 Interactive 시스템의 참조 모델을 나타낸 것이며, [그림 2]는 위성 Interactive 망의 참조 모델을 나타낸 것이다^[8].

보안은 정확한 위치를 포함한 사용자 인증이나, 사용자들 간의 데이터의 흐름이나, 사용자와 관리자간의 데이터의 흐름을 저해하는 악의적 공격 또는 허락되지 않은 불법적인 접근으로부터 데이터를 보호하는 것이다.

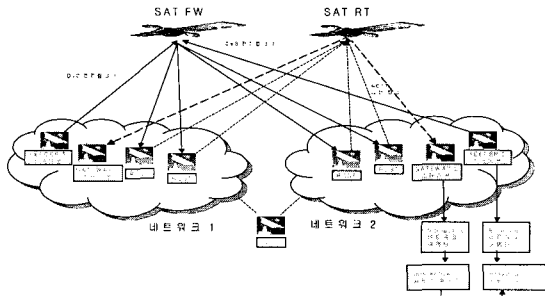


(그림 1) Interactive 시스템의 참조 모델

* 순천향대학교 정보보호학과

** APEX Wireless

*** 순천향대학교 전자공학과



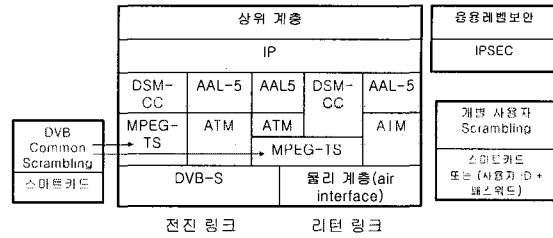
(그림 2) 위성 Interactive 망의 참조 모델

위성망에서의 보안 서비스의 종류는 크게 세 가지로 구분할 수 있으며, 이는 정확한 위치를 포함한 사용자 인증 보안, 사용자로 향하거나 사용자로부터의 신호 채널 보안, 그리고 사용자로 향하거나 사용자로부터의 데이터 트래픽 채널 보안을 의미한다.

위성망에서의 데이터링크 계층 보안은 상위 레벨 보안에 의존하지 않고 위성 구간을 보호할 수 있도록 한다. 전진링크(Forward Link)의 경우에는 DVB (Digital Video Broadcast) 공동 스크램블링이 필수적으로 요구된다. 전진링크에 있어서 각각의 스크램블링은 각 세션 레벨마다 사용되어 질 수 있으나 RCST가 메시지를 필터(filter)하기 위한 방법으로 MAC (Medium Access Control) 어드레스를 이용하기 때문에 사용자의 MAC 어드레스는 확실히 RCST에 남게된다. 전진링크는 MPEG-TS(Moving Picture Experts Group-Transport Stream) 계층에서 스크램블링 적용을 적용함으로써 제공된다. 단 MPEG-TS 헤더는 평문으로 남는다. 리턴링크(Return Link)의 경우에 클라이언트 측의 장치는 IPsec을 이용하기 때문에 게이트웨이(Gateway)측의 라우터(Router)가 이 IPsec 이용을 허용 또는 조정함으로써 보안을 제어한다. 이는 ATM(Asynchronous Transfer Mode), DSM-CC에서 스크램블링이 적용함으로써 제공되며 위 경우와 마찬가지로 ATM, DSM-CC 헤더는 평문으로 남는다.

위성 액세스 시스템에서의 보안서비스가 제공되기 위해서는 다음과 같은 가정이 필요하다.

- 보안은 개별 RCST 보다 상위 레벨에서 정의되어야 한다.
- RCST 당 하나 이상의 사용자들이 존재해야 하며, 사용자는 자신만의 보안 기법을 가지고 있어야 한다. 이와 같은 보안 기법을 통하여 사용자 신원을 확인용 인증 알고리즘으로 사용자 로그인이름(logon



(그림 3) 보안 서비스가 제공되는 계층에 따른 구분

name)과 패스워드(password)를 검사하거나, RCST에 있는 스마트카드를 검사하여 사용자 인증을 수행한다.

- 사용자로 향하는 모든 트래픽 데이터와 제어 데이터는 개별 사용자 단위로 스크램블링 된다. 또한 사용자는 NCC/Gateway 이외의 누구도 모르는 제어워드(control word)를 비밀스럽게 간직하고, 이를 이용하여 데이터를 암호화하거나 복호화 한다.

ETSI EN 301 790 V1.2.2에서는 다음과 같은 사항을 토대로 인증 서비스를 제공한다.

- 클라이언트 장치에서 사용자 이름과 패스워드를 요구함으로써 사용자를 인증한다.
- 사용자 장치가 PC인 경우 RCST는 인증 기능이 필요 없다.
- RCST가 프락시 클라이언트라면, RCST는 NCC에게 인증 받아야 한다. 이는 인증 서버가 NCC에 존재해야 함을 의미하며 이 인증서버가 각 사용자의 인증을 관리한다.
- RCST에 스마트카드가 있다면 인증은 필요 없고, RCST는 링크 계층 개별 제어 워드 암호를 위하여 사용된다.

제공되는 보안 메커니즘은 NCC와 RCST간의 인증과 키관리를 위하여 사용되는 MAC 메시지들의 집합이다. 이는 세션 설정, 또는 동작 중에 키 갱신 시에 이용된다. 그리고 동작 중에 NCC와 RCST간의 페이로드(payload) 데이터 스트림의 암호화와 복호화가 된다.

세션키 생성은 3가지 요구/응답 MAC 메시지-쌍에 의해서 생성이 되며, 세션키는 세션과 연관된 페이로드 스트림에 한정된 세션키이다. 이렇게 생성된 세션키는 NCC와 RCST간에 공유되게 된다. 세션키의 생성은 DH 공개키 공유 알고리즘과 쿠키(cookie)에 바탕을 두고 있다. 여기서 쿠키란 NCC와 RCST 간에

공유되는 장기간 비밀 정보이다. 쿠키의 길이는 160 비트이고 RCST가 NCC에게 인증 될 때 이용된다. 쿠키의 저장 위치는 RCST의 경우 비휘발성 메모리에 저장되고 NCC의 경우 쿠키를 위한 데이터베이스에서 관리된다. 쿠키의 갱신 주기는 보안 정책에 의해서 결정되며 쿠키와 세션키는 암호학적 안전성 측면에서 독립적으로 구성되어야 한다.

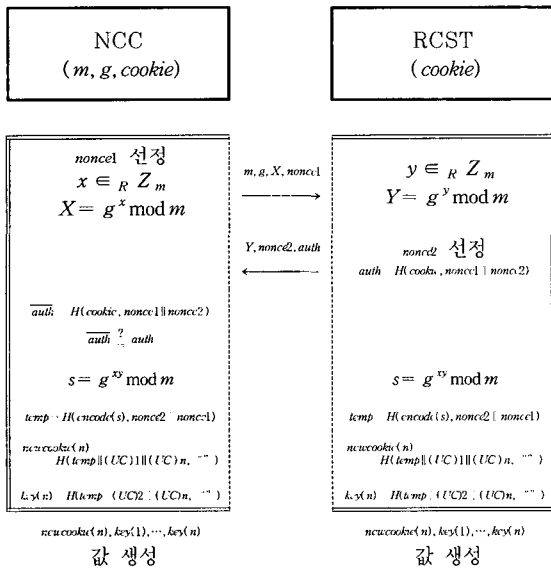
RCST 방지 대책으로는 8 비트 카운터를 이용하는 방법이 있으나, 이는 NCC와 RCST 간에 동기적으로 증가되는 단점이 있다.

2. 안전한 키 교환 메커니즘

이번 장에서는 위성 망에서 이용되는 세 가지 키 교환 메커니즘 MKE, QKE, 그리고 EKE에 대하여 설명한다. 특히 MKE 프로토콜 설명 부분에서는 상호간에 메시지를 교환할 때 정의되는 메시지 구조에 대하여 살펴본다. 이 메시지 구조는 ETSI EN 301 790 V1.2.2의 보안 영역에 정의된 사항이다.

2.1 Main Key Exchange (MKE)

MKE 방식은 NCC와 RCST 간에 비밀값을 공유하기 위해 DH 키 공유 방법을 사용한다. 또한 RCST가 NCC에게 사용자 신분을 확인하기 위하여 쿠키값이 이용된다^{[4],[5],[7]}. MKE 프로토콜의 진행 단계는 [그림 4]와 같다.



(그림 4) MKE 프로토콜

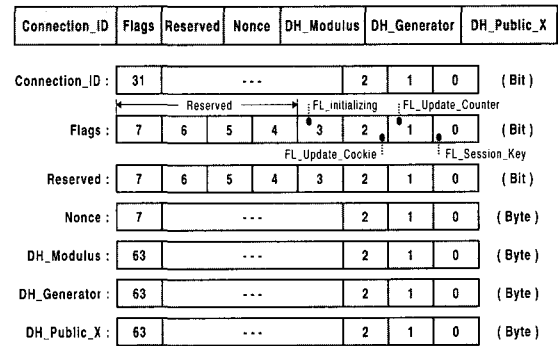
MKE 프로토콜은 다음 단계로 이루어진다.

- ① NCC가 nonce1 랜덤하게 생성하고 자신의 공개키와 함께 RCST에게 전송
- ② RCST는 nonce2 랜덤하게 생성하고 nonce1 값을 이용하여 인증값 auth를 계산하여 NCC에게 자신의 공개키와 nonce2, auth를 전송
- ③ NCC를 자신이 계산한 \overline{auth} 값과 RCST에 받은 auth값을 비교
- ④ $\overline{auth} = auth$ 같은 상호간에 인증
- ⑤ NCC와 RCST는 공유된 비밀값 s, temp, newcookie 그리고 세션키를 계산

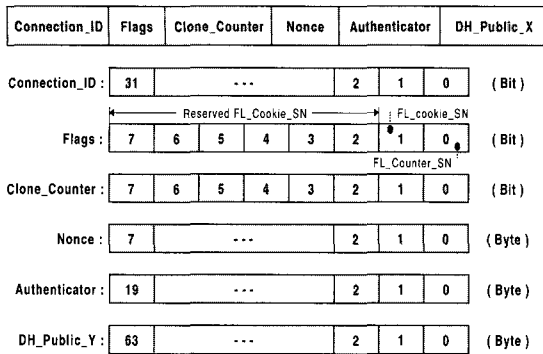
이 프로토콜을 통하여 RCST를 인증, 새 비밀값 s 상호공유, 새 쿠키값 newcookie 계산, 새 세션키들 key(1), ..., key(n) 상호공유의 결과들을 얻게 된다.

최종적으로 이 프로토콜을 통해서는 페이로드 스트림 데이터를 처리하기 위하여 사용된 보안 문맥(security context)에서의 공유 비밀 정보를 유도하기 위한 부분으로 사용된다. 프로토콜에서 사용된 기호 중에서 “||”는 concatenation을 의미하고, (UC)x는 값 x를 unsigned char형으로 바꿈을 나타내며, “”는 empty string(zero length)을 의미한다. 또한 nonce1은 NCC가 지닌 랜덤열(random string)이고 nonce2는 RCST가 지닌 랜덤열이다. 그리고 그림의 상단 박스는 참여자들의 아이디 및 그들이 사전에 지니고 있는 정보를 의미한다.

[그림 5]는 MKE 메시지 구조를 도시한 것이다. MKE는 RCST와 쿠키-독립 키교환 방식(Cookie independent key exchange)을 통하여 이루어지며 RCST에게 쿠키 값과 클론 카운터 값을 갱신할 수 있도록 구성된다. FL_Session_key은 보안 문맥에서



(그림 5) MKE 메시지 구조



(그림 6) MKE 응답

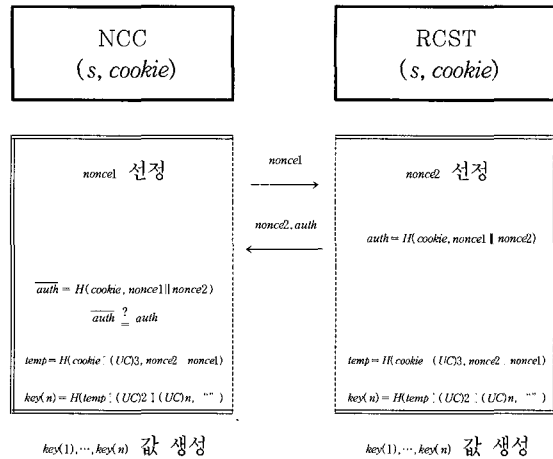
갱신할 세션키의 종류를 나타내고, FL_Update_Counter는 RCST에게 클론 검출 카운터를 증가시킬 것을 명령한다. FL_Update_Cookie는 새로운 쿠키를 생성하고 클론 검출 카운터를 리셋(reset)시키기 위한 부분이며 FL_Initializing은 RCST에게 Authenticator 필드를 무시할 것을 지시하기 위한 부분이다.

[그림 6]은 MKE 응답 메시지 구조를 도시한 것이다. MKE 응답 메시지는 RCST를 인증하고 RCST가 NCC와 쿠키-독립 키교환 방식을 이루도록 구성된다. 또한 현재의 클론 검출 카운터 값을 지닌다. FL_Cookie_SN는 인증을 위하여 사용되는 쿠키의 순서 번호를 의미하고, FL_Counter_SN는 클론 검출 카운터의 현재의 순서 번호를 나타낸다. Clone_Counter 필드는 현재 카운터의 값이 들어있다.

만약 NCC가 보낸 FL_Update_Cookie가 "set" 되어 있다면, RCST는 새 쿠키를 생성하고 쿠키 순서 번호를 갱신하고 클론 카운터를 "0"으로 설정 후 클론 순서 번호를 "0"으로 수정한다. 또한 만약 NCC가 보낸 FL_Update_Counter가 "set" 되어 있다면, RCST는 클론 카운터를 증가하고 클론 카운터 순서 번호를 갱신하게 된다.

2.2 Quick Key Exchange (QKE)

QKE방식은 기존의 쿠키와 기존의 비밀 공유 값을 이용하여 키를 교환한다. 이것은 기존의 쿠키를 이용하여 RCST가 인증됨을 의미한다^{{6}{7}}. QKE방식이 MKE방식과 다른 점은 NCC와 RCST가 통신 전에 비밀값 s와 cookie값을 공유하고 있다는 가정하에 s를 계산하는 과정이 없고, 따라서 비밀 s를 계산하기 위한 DH 파라미터들의 교환이 요구되지 않는다. 또한 새로운 쿠키 계산 과정이 없다는 것이다. 다음 [그림 7]은 QKE의 과정을 나타낸 것이다.



(그림 7) QKE 프로토콜

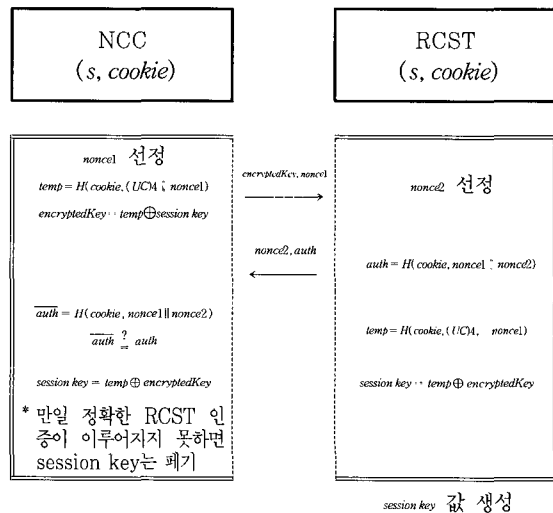
2.3 Explicit Key Exchange (EKE)

이 방식은 NCC가 자신이 미리 결정한 세션키를 RCST에게 전달하는 것이 특징이다. 이 방식에서는 현재의 쿠키값을 이용하고 인증 기능이 제공된다^{11}. 세션키를 암호화하기 위한 암호화 키는 쿠키로부터 유도된 임시키(temporary key)를 사용한다. 다음 식 (1)과 식 (2)는 임시키와 encryptedKey을 나타낸다.

$$temporary\ key = H(cookie || (UC)4 || nonce1) \quad (1)$$

$$encryptedKey = temporary\ key \oplus session\ key \quad (2)$$

[그림 8]은 EKE의 과정을 나타낸 것이다.



(그림 8) EKE 프로토콜

[표 1] 보안 기능 제공 협상을 위한 채널

	채널	신호 요소	용도
전진링크 (NCC → RCST)	전진링크의 터미널 한정 메시지인 TIM	logon initialize descriptor의 security_handshake_required 요소 (1비트)	"1"이면 보안 핸드셰이크가 사용되어야 함을 의미함
리턴링크 (RCST → NCC)	리턴링크의 CSC (Common Signalling Channel)	RCST Capability 필드의 security mechanism 파라미터	"1"이면 보안 능력이 있는 RCST임을 의미함

3. 국내 위성 시스템에 적용하기 위한 가이드라인

3.1 보호해야 할 데이터 및 보호 협상을 위한 채널
 위성 시스템에서 제공되는 보안 서비스는 크게 RCST의 인증 서비스와 RCST와 NCC 간의 기밀성 서비스로 구분할 수 있다. 단 무결성 서비스와 부인방지 서비스는 제공되지 않는다⁹⁾. 보호되어야 할 데이터 보호 메커니즘은 NCC와 RCST간의 MPEG-TS에 대하여 수행된다. 기본적으로 보안 기능은 선택사항이며 이는 NCC와 RCST는 보안 기능을 제공하기 이전에 이를 사전 협의해야 함을 의미한다. NCC와 RCST는 [표 1]과 같은 채널과 신호 요소를 이용한다.

3.2 보안을 위하여 사용되는 채널

보안 MAC 메시지는 전진링크의 <MAC>Security Sign-On, <MAC>Main Key Exchange, <MAC>Quick Key Exchange, <MAC>Explicit Key Exchange로 구성되며, 리턴링크의 <MAC>Security Sign-On Response, <MAC>Main Key Exchange Response, <MAC>Quick Key Exchange Response, <MAC>Explicit Key Exchange Response로 구성된다. 이 대한 사항이 [표 2]에 기술되어 있다.

비밀 교환, 세션키 교환, 쿠키 및 복제방지 카운터 갱신은 [표 3]과 같은 시점에 수행되어야 한다.

인증은 NCC가 RCST를 인증하는 모드와 RCST가 NCC를 인증하는 모드가 있으나, 기본적으로 NCC가 RCST를 인증하는 인증 모드만을 사용한다. 이 인증에서는 서로 비밀정보인 쿠키를 알고 있다는 것에 바탕을 둔 쿠키를 이용한 인증 방식을 사용한다.

3.3 보안 알고리즘의 규격 제안

지금까지 표준안에 표준화된 보안 알고리즘은 분야별로 다음과 같다. 여기에 국내 보안 알고리즘과 키교

[표 2] 전진, 리턴링크의 MAC 보안 메시지 전달을 위한 채널

	채널	신호 요소	용도
전진링크 (NCC → RCST)	잘 알려진 전용PID를 갖는 MEG-TS	DSM-CC private section	○보안 기능을 갖는 RCST는 이 PID를 필터링 해야 함
리턴링크 (RCST → NCC)	Data unit labelling method (DULM)	IE (information element)	○Type : · 0x0d : security sign-on response · 0x11 : main key exchange response · 0x13 : quick key exchange response · 0x15 : explicit key exchange response

[표 3] 비밀·세션키 교환, 쿠키 또는 복제방지카운터 갱신 시점

	수행 시점	과정	대표 값
비밀교환	로그온시	MKE 과정	하루 한번 단위로
세션키 교환	로그온시	MKE, QKE, EKE 과정	로그온 후에 새로운 세션 개시 때마다 또는 1시간마다
쿠키 또는 복제 방지 카운터 갱신	세션 중 필요시 갱신함	MKE, QKE, EKE 과정	1분 또는 10분 단위로

환을 위한 향상된 보안 알고리즘을 적용한 규격은 [표 4]와 같다.

현재 ETSI 표준안에는 위의 표 내용 중에서 default 값으로 표준화되어 있고, 각 비트 단위를 설정함으로써 NCC와 RCST 간의 보안 알고리즘이 협상된다. 비트 단위로 설정하는 경우 최대 8가지의 보안 알고리즘의 설정이 가능하다. 기본적으로 8가지 이상의 보안 알고리즘의 표준화가 당분간 필요할 것 같다. 따라서 현재 하나만 설정되어 있는 각 비트의 용도에 더하여 유보된 나머지 7비트를 위의 각 알고리즘에 할당하면 NCC와 RCST간에는 다양한 보안 알고리즘의 협상이 가능하다. 그러나 만약 시기가 경과되어 8가지 이상의 보안 알고리즘의 설정이 요구되어 또 다른 하나의 선택사항으로 만약 이 필드를 uimsb 형태로 부호화한다면, 전체 256가지의 알고리즘의 선택이 가능해져 보안 알고리즘의 선택에 있어 선택성을 높일 수 있다. 따라서 국내 규격 선정 시 다음과 같이 security sign-on 메시지의 구조를 [표 5]와 같이 설정할 것을 제안한다.⁽¹⁾⁽²⁾⁽⁴⁾.

[표 4] 보안 알고리즘 유형과 보안 파라미터 크기

		보안 파라미터 크기		비고
		키 크기 (비트)	출력크기 (비트)	
키교환	Diffie-Hellman	512	512	ETSI 방식
	Diffie-Hellman	764	764	-
	Diffie-Hellman	1,024	1,024	-
	RSA	512	512	-
	RSA	764	764	-
해쉬 알고리즘	HMAC SHA1		160	ETSI 방식
	HMAC MD5		128	-
	HMAC HAS160		160	한국 표준 해쉬 알고리즘
기밀성 알고리즘	DES	40	64	ETSI 방식
	DES	56	64	ETSI 방식
	SEED	128	128	한국표준알고리즘
	AES	128 이상	128	차세대 미국 표준 알고리즘
의사난수 생성기	유형 정의하지 않음		64	ETSI 방식

[표 5] 국내 security sign-on 메시지 구조

종류	비트 수	해석	예
키교환을 위한 공개키 알고리즘	8	uimbsb	- 0: PKA_DH_512 - 1: PKA_DH_764 - 2: PKA_DH_764 ...
해쉬 알고리즘	8	uimbsb	- 0: HMACSHA1 - 1: HMACMD5 - 2: HMACSHA160 ...
암호 알고리즘	8	uimbsb	- 0: HMACSHA1 - 1: HMACMD5 - 2: HMACSHA160 ...
년스 크기	8	uimbsb	- 0: 64 비트크기 - 1: 128 비트 크기 - 2: 160 비트 크기 ...

기밀성 서비스 관련 주요 사항은 [표 6]에 기술되어 있는 것과 같다.

일반적으로 세션키는 2가지 종류가 있다. 이중 현재

[표 6] 스크램블링 관련 규격

	default 알고리즘	모드	키	초기값
DVB 방식	DES	CBC	- 두 개의 세션키 중 하나 선택	all "0"
대안 1	SEED	CBC	- 두 개의 세션키 중 하나 선택	all "0"
대안 2	AES	CBC	- 두 개의 세션키 중 하나 선택	all "0"

[표 7] 암호화된 페이로드 확인을 위한 필드

방식	단위	확인자	의미
DVB Multiprotocol encapsulation section	DVB Multiprotocol Encryption	48 비트 MAC 주소	- DVB Multiprotocol Encapsulation section에서 datagram_data_bytes(MAC 주소부와 CRC 검사부 사이에 존재함) 필드를 암호화함 - 스테핑 바이트가 부가될 수 있음
ATM cell	ATM 페이로드	VPI/VCI	- ATM cell 페이로드에 대해 적용됨

[표 8] 현재 세션을 암호화하고 하고 있는 세션키의 종류

방식	필드	크기 (비트)	의미
DVB Multiprotocol encapsulation section	section header의 payload_scrambling_control 필드	2	- 00: 암호화되지 않음 - 01: 유보 - 10: 세션키 0으로 암호화됨 - 11: 세션키 1로 암호화됨
ATM cell	GFC의 MFC 상위 2 비트	2	- 00: 암호화되지 않음 - 01: 유보 - 10: 세션키 0으로 암호화됨 - 11: 세션키 1로 암호화됨

암호화된 정보가 어떤 키로 암호화되어 있는지를 확인하는 비트는 다음과 같으며 [표 8]에 기술되어 있다.

암호화의 기본 단위 신호는 페이로드 데이터 스트림이다. 보안 문맥은 일반적으로 두 개의 세션키로 구성된다. 두 개의 세션키의 각각은 전진 링크와 리턴 링크의 페이로드를 암호화하는데 사용된다. 두 개의 키를 번호 "0" 키와 번호 "1" 키라고 정의하자. 일반적으로 세션키는 번갈아 가면서 사용된다. 세션키 번호 "1"이 사용되는 동안 다음에 사용될 세션키 쌍이 새로 교환된다. 이렇게 함으로써 연속된 페이로드 암호화가 가능해진다.

일반적으로 키교환의 주도권은 NCC에 있어야 한다. 이는 NCC가 키교환을 위한 요청 메시지를 전송함을 의미한다. RCST는 현재 NCC는 전진 링크에서의 키 번호를 갖는 키를 리턴 링크에서 사용해야 한다.

보안 설정을 위한 각 단계 설정 시 실패하는 경우 조치사항은 [표 9]에 정리되어 있으며 다음과 같은 특성을 지닌다.

[표 9] 각 보안 단계 실패 시 조치사항

단계	수행되는 업무	이용 메시지	수행 시점	실패 시 조치사항
〈MAC〉 security sign-on 과정	- 보안 기능 제공 여부 협상 - 보안 알고리즘 유형과 키의 크기 협상	security sign-on	로그온 과정	암호화되지 않은 통신 모드 유지
키교환 과정	- 하나의 세션키 교환 - 쿠키 값의 갱신 가능 (MKE 이용 시) - 복제 방지 카운터 값 변경 가능 - RCST 인증	MKE, QKE, EKE	로그온 세션	로그오프
〈MAC〉 security sign-on 과정	- 새로운 보안 문맥(세션키) 갱신 - 쿠키 값과 복제 방지 카운터 값의 갱신은 불가능	QKE, EKE	로그온 후에	로그오프

보안 설정은 크게 〈MAC〉 security sign-on 핸드셰이크 과정, 키교환 과정, 로그온 후에 보안 문맥 (security context) 갱신과정으로 구성된다. 여기서 보안 문맥은 세션키를 의미한다. 첫 과정은 보안 알고리즘과 기밀성 알고리즘의 키의 크기를 협상한다. 두 번째 과정은 세션키를 공유하는 과정이다. 단 로그인된 RCST는 새로 로그인 과정 없이 과정 3을 이용하여 세션키를 교환한다. 단 이 단계에서는 쿠키 값과 복제 방지 카운터를 갱신하지 않는다. 새로운 세션키가 교환되는 동안에는 그 이전에 교환된 세션키로 패이로드를 암호화하거나 전혀 암호화되지 않아야 한다.

따라서 기본적으로 MKE 과정을 수행하면 보안 문맥(세션키)과 새로운 세션키의 갱신이 가능하지만, QKE나 EKE를 수행하면 보안문맥(세션키)의 갱신만 가능하고 쿠키의 갱신은 불가능하다.

일반적으로 세션키와 쿠키 값을 갱신하는 과정은 크게 3가지 방법이 있으나 이 중 MKE와 QKE는 지점간의 패이로드를 위하여 사용되고, EKE는 멀티캐스트 전송을 위하여 사용된다. 각 보안 과정의 이용 용도와 사용처는 다음 [표 10]과 같다.

[표 10] 각 보안 단계의 용도

단계	주요 기능	용도	비고
MKE 과정	- 하나의 세션키쌍 교환 - RCST 인증 - 새로운 쿠키 갱신	지점간 스크램블링	- DH 알고리즘 파라미터 실장
QKE 과정	- 하나의 세션키쌍 교환 - RCST 인증	지점간 스크램블링	- MKE 보다 고속 동작 가능함
EKE 과정	- 하나의 세션키 교환 - RCST 인증	멀티캐스트 암호	- 하나의 세션키를 생성함

앞장에서 제시된 세 가지 방법의 키교환 방식의 특징을 비교하면 [표 11]과 같다.

[표 11] 3 가지 키교환 방식의 비교

	MKE	QKE	EKE
RCST 인증	○ (기존의 쿠키값 이용)	○ (기존의 쿠키값 이용)	○ (기존의 쿠키값 이용)
비밀값 교환	○ (DH 키교환 알고리즘 이용)	×	×
새로운 쿠키값 갱신	○	×	×
키생성 주도권	NCC, RCST	-	NCC
키의 개수	2	2	2
복잡도	×	△	△
중간자 공격	가능	-	-

III. 결 론

본 논문에서는 ETSI의 위성 interactive 망을 위한 참고 모델을 분석하고, 키관리 및 인증을 위하여 요구되는 사항을 고찰하였으며 이를 토대로 국내 가이드라인 제시에 활용하여 기술하였다. 또한 국내 광대역 위성 액세스 망을 위한 가이드라인을 고찰하였으며 기존의 ETSI에서 제안한 방식에 더하여 국내에서 개발한 다양한 암호 알고리즘을 이용한 방식을 제안하였다. 추후에는 위성 망에서 응용할 수 있는 다양한 보안 알고리즘과 계산량을 줄일 수 있는 EC를 적용한 알고리즘 연구가 필요할 것으로 고찰된다.

참 고 문 헌

- [1] Steven M. Bellovin and Michael Merritt. "Encrypted Key Exchange : Password-Based Protocols Secure Against Dictionary Attacks". In Proc. IEEE Computer Society Symposium on Research in Security and Privacy. Oakland. pp. 72-84. 1992.
- [2] R.L. Rivest, A. Shamir and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". ACM, Vol.

21. no.2, Feb. 1978, pp. 120-126.
- [3] W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644-654, November 1976.
- [4] M. Bellare, D. Pointcheval and P. Rogaway, "Authenticated key exchange secure against dictionary attack." Eurocrypt 2000.
- [5] V. Boyko, P. Mackenzie and S. patel, "Provably secure password authenticated key exchange using Diffie-Hellman," Eurocrypt 2000.
- [6] P. Mackenzie and R. Swaminathan, "Secure network authentication with password identification," Presented to IEEE P1363a, August 1999.
- [7] A. Menezes, P. van, Oorschot, S. Vanston, Handbook of applied cryptography, CRC Press, Inc., 1997.
- [8] ETSI EN 301 790 V1.2.2: "Digital Video Broadcasting (DVB): Interaction channel for satellite distribution systems:" 2000. 12, European Standard (Telecommunications series).
- [9] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".
- [10] 염홍열, 김락현, 류종호, 현상우, 김문기, "위성 액세스 시스템의 Security 방식에 관한 연구", 한국전자통신연구원, 2001.12.

〈著者紹介〉



오 흥 룡 (Oh, Heung Ryong)
학생회원

2002년 2월 : 순천향대학교 전자공학과 졸업

2002년 3월~현재 : 순천향대학교 일반대학원 정보보호학과 석사과정

관심분야 : 공개키 기반구조, 보안 프로토콜

E-mail : master@elec.sch.ac.kr



김 문 기 (Kim, Moon Ki)
일반회원

2001년 2월 : 순천향대학교 전자공학과 졸업

2003년 2월 : 순천향대학교 일반대학원 전기·전자공학과 정보보호전

공 석사 졸업

2003년 3월~현재 : APEX Wireless S/W팀 연구원
관심분야 : 보안 프로토콜, 이동통신보안, 무선 보안

E-mail : kmoong@elec.sch.ac.kr



류 종 호 (Ryu, Jong Ho)
일반회원

1998년 2월 : 순천향대학교 전자공학과 졸업

2000년 2월 : 순천향대학교 일반대학원 전기·전자공학과 석사 졸업

2003년 3월 : 순천향대학교 일반대학원 전기·전자공학과 박사수료

관심분야 : 암호이론, 공개키 기반구조, 네트워크 보안, 보안 프로토콜

E-mail : youjh@elec.sch.ac.kr



김 락 현 (Kim, Rack Hyun)
학생회원

1997년 2월 : 순천향대학교 전자공학과 졸업

1999년 8월 : 순천향대학교 일반대학원 전기·전자공학과 석사 졸업

2000년~현재 : 순천향대학교, 청운대학교, 홍성기능대학교, 아산정보기능대학 외래강사

2001년 2월~현재 : 순천향대학교 일반대학원 정보보호학과 박사과정

관심분야 : 암호 이론, 공개키 기반구조, 네트워크 보안, 보안 프로토콜

E-mail : rhkim70@orgio.net



염 홍 열 (Yum, Heung Youl)

정회원

1981년 한양대학교 전자공학과 졸업

1983년 한양대학교 대학원 전자공학과 석사

1990년 한양대학교 대학원 전자공

학과 박사

1982년~1990년 한국전자통신연구소 선임연구원

1990년~현재 : 순천향대학교 공과대학 정보기술공학부 교수

1997년~2000년 : 순천향대학교 산업기술연구소 소장

2000년~현재 : 순천향대 산학연컨소시엄센터 소장

1997년~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사

관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안

E-mail : hyyoum@sch.ac.kr