情報保護學會論文誌
第14券 第3號, 2004. 6

광대역 위성 액세스 망을 위한 키 교환 프로토콜 제안

오 흥 룡,[a)†‡] 염 흥 열[b)]
한국정보통신기술협회,[a)] 순천향대학교[b)]

Key Exchange Protocols for Domestic Broadband Satellite Access Network

Heung-Ryong Oh,[a)†‡] Heung-Youl Youm[b)]
Telecommunications Technology Association,[a)] SoonChunHyang University[b)]

요 약

키 교환 방식은 안전한 암호 통신을 위하여 매우 중요하다. 키 교환 프로토콜은 안전성, 키확신, 키신선도 등의 요구사항을 만족해야 한다. 본 논문에서는 국내 광대역 위성 액세스망(BSAN : Broadband Satellite Access Network)의 보안 프로토콜과 규격을 설정하기 위하여 ETSI(European Telecommunications Standards Institute) 표준안의 내용을 분석하고 RCST(Return Channel Satellite Terminal)와 NCC(Network Control Centre)간에 인증 및 키 관리 기능을 위하여 요구되는 주요 핵심 보안 메커니즘에 대하여 분석한다. 이를 바탕으로 국내 광대역 위성 액세스 망에 적용 가능한 보안 기능을 위한 가이드라인을 제시하며, 이를 위한 여러 가지 보안 알고리즘들의 규격을 제시한다. 또한 기존의 ETSI 표준안의 키 교환 방식이 중간자 공격에 취약하고, 키의 신선도와 확신성을 제공하지 않음을 알았다. 따라서 본 논문에서는 이러한 문제를 해결하고 키의 신선도와 확신성을 갖으면서 계산적 복잡도와 교환되는 데이터 량을 감소시키기 위한 네 가지 키 교환 프로토콜을 제안하고, 제안된 프로토콜의 안전성을 분석하며, 각 제안방식들의 특성을 비교 분석한다. 특히 이러한 특성을 갖는 DH 알고리즘, MTI(Matsumoto, Takashima, Imai), ECDH(Elliptic Curve Diffie-Hellman) 기반의 여러 가지 키 교환 프로토콜들을 제안한다.

ABSTRACT

The key exchange protocols are very crucial tools to provide the secure communication in the broadband satellite access network. They should be required to satisfy various requirements such as security, key confirmation, and key freshness. In this paper, we present the guideline of security functions in BSAN(Broadband Satellite Access Network), and analyze the specification of the security primitives and the key exchange protocols for the authenticated key agreement between RCST(Return Channel Satellite Terminal) and NCC(Network Control Centre). In addition, we propose the security specification for a domestic broad satellite network based on the analysis on the security profile of ETSI(European Telecommunications Standards Institute) standards. The key exchange protocols proposed in ETSI standard are vulnerable to man-in-the-middle attack and they don't provide key confirmation. To overcome this shortcoming, we propose the 4 types of the key exchange protocols which have the resistant to man-in-the-middle-attack, key freshness, and key conformation, These proposed protocols can be used as a key exchange protocol between RCST and NCC in domestic BSAN. These proposed protocols are based on DH key exchange protocol, MTI(Matsumoto, Takashima, Imai) key exchange protocol, and ECDH(Elliptic Curve Diffie-Hellman).

Keywords : *BSAN, RCST, NCC, ETSI, ECDH*

Ⅰ. 서 론

본 논문에서는 국내 광대역 위성 액세스 망(BSAN)에 적용 가능한 보안 기능을 위한 가이드라

* 본 연구는 인터넷 침해대응기술 연구센터 지원으로 수행되었습니다.
접수일 : 2003년 10월 7일 ; 채택일 : 2004년 4월 29일
† 주저자, ‡ 교신저자 hroh@tta.or.kr

인을 제시하기 위하여 기존의 ETSI 표준안의 보안 기능과 프로토콜을 살펴보고, RCST와 NCC 간에 인증 및 기밀성 서비스를 제공하기 위한 키 교환 기능을 위하여 요구되는 주요 핵심 보안 메커니즘에 대하여 제시한다.

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 요구사항을 제시한다. 그리고 이 분석을 근거로 국내 광대역 위성 액세스망 보안을 위한 가이드라인을 제시한다.

보안 기능을 위한 암호 프리미티브는 대칭성 암호 알고리즘, DH(Diffie-Hellman) 공개키 교환 알고리즘, 해쉬 알고리즘, 난수 생성기, 그리고 HMACSHA-1 알고리즘 등이 필요하고, 또한 국내 광대역 위성 액세스망을 위한 가이드라인의 제시가 요구된다. 기존의 ETSI 표준 키 교환 방식은 임시 DH(temporal Diffie-Hellman) 비밀 교환 방식에 바탕을 두고 있다. 이 방식은 기본적으로 중간자 공격(Man-in-the-middle attack)에 취약한 방식이고, 비밀의 신선도(freshness)와 교환된 비밀의 확신(key confirmation) 기능을 제공하지 않는다. 따라서, 광대역 위성망을 위한 키 교환 프로토콜이 가져야할 요구사항과 이를 만족하는 다양한 키 교환 프로토콜의 제시가 요구되고 있다. 여기서 키 신선도는 세션마다 서로 다른 키가 교환되게 하는 것이고, 키 확신은 하나의 통신상대가 다른상대와 키 교환 프로토콜을 수행하고 나서 다른 통신 상대가 자기와 동일한 키를 가지고 있음을 확신하는 특성을 의미한다.

본 논문의 II장에서는 기존의 ETSI 표준에서 제안한 표준안을 분석하고, 각 키 교환 프로토콜의 특징을 비교분석한다. III장에서는 보안 기능을 실현하기 위하여 이용될 수 있는 다양한 채널을 고찰하고, 국내 광대역 위성 액세스망을 위하여 요구되는 암호 프리미티브의 종류를 분석하고, 국내 망을 위한 보안 구조와 보안을 위한 채널 구조를 제시한다. 제 IV장에서 기존의 NCC와 RCST간의 메시지 구조의 변경을 최소화하면서 중간자 공격에 면역성이 있고 키 신선도와 비밀의 확신 기능을 갖는 키 교환 프로토콜들을 제안하고, 이에 대한 안전성을 분석하며, 제안된 방식을 기존의 방식과 여러 특성 측면에서 비교분석한다.

II. 연구 배경

본 장에서는 위성망에서의 보안방식을 설명한 ETSI EN 301 790 V1.2.2의 내용을 분석한다. 위성 망을 위한 서비스는 그림 1과 같이 방송 서비스와 상호응답 서비스가 존재한다. 그림 2는 위성 광대역 망을 위한 참조 모델을 나타낸 것이다[8]. NCC는 망 관리 센터를 의미하며, RCST는 사용자의 위성 단말을 의미한다. 키 교환은 그림 2에서 NCC와 RCST 간에 수행된다.

광대역 위성망에서 제공되어야 할 보안 서비스는 두가지이며, 하나는 사용자(개체) 인증 서비스이고, 다른 하나는 사용자들 간의 데이터의 흐름이나 사용자와 관리자간의 데이터의 흐름을 악의적으로 공격하여 허락되지 않도록 불법적인 접근으로부터 데이터를 보호하는 기밀성 서비스이다.

위성망에서의 보안은 그림 3과 같이 세가지 레벨에서 수행되는데, DVB 공통 스크램블링 방식을 이용한 데이터링크 계층 보안, 개별 사용자의 신호 채널 보안을 위한 개별 스크램블링 보안, 그리고 데이터 링크 상위 계층에서 제공되는 응용 한정 보안 등이다. 일반적으로 리턴 링크가 필요 없는 전진 링크의 경우 DVB(Digital Video Broadcast) 공동 스크

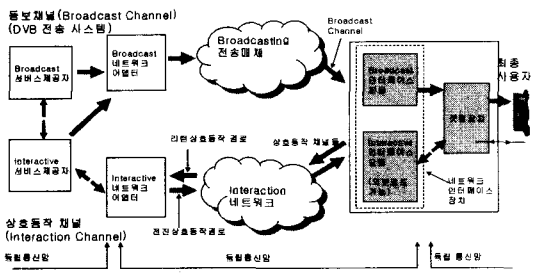


그림 1. Interactive 시스템의 참조 모델

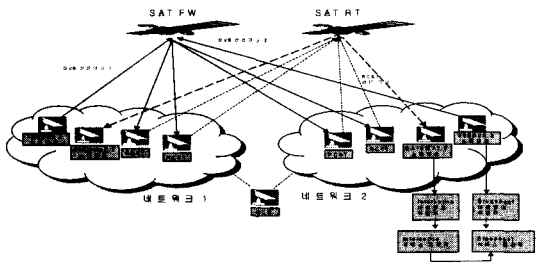


그림 2. 위성 Interactive 망의 참조 모델

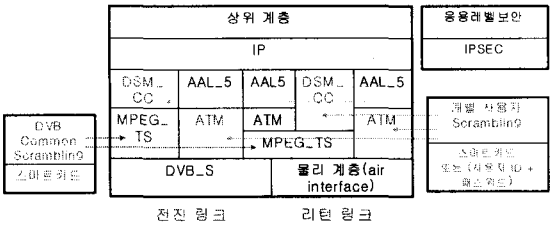


그림 3. 보안 서비스가 제공되는 계층에 따른 구분

랜블링의 사용이 필수적이다. 다음부터는 기존에 ETSI에서 제공되고 있는 세가지 방식의 키 교환 프로토콜에 대하여 분석한다.

2.1 Main Key Exchange (MKE)

MKE는 새로운 세션을 설정할 때 마다 수행되는 프로토콜이다. MKE 프로토콜은 그림 4와 같이 수행된다. MKE 프로토콜의 안전성은 전체 보안 시스템의 안전성에 큰 영향을 미친다. MKE 방식은 NCC와 RCST 간에 비밀값을 공유하기 위해 DH 키 공유 방법을 사용한다. 또한 RCST가 NCC에게 사용자 인증을 위하여 쿠키값이 이용된다[4][5][7]. 이 프로토콜을 통해 생성된 *newcookie(n)*값은 다음 세션의 사용자 인증을 위하여 이용된다.

프로토콜에서 사용된 기호 중에서 "‖"는 concatenation을 의미하고, (UC)x는 값 x를 unsigned char형으로 변경함을 의미하며, ""는 empty string(zero length)을 의미한다. 또한 *nonce1*은

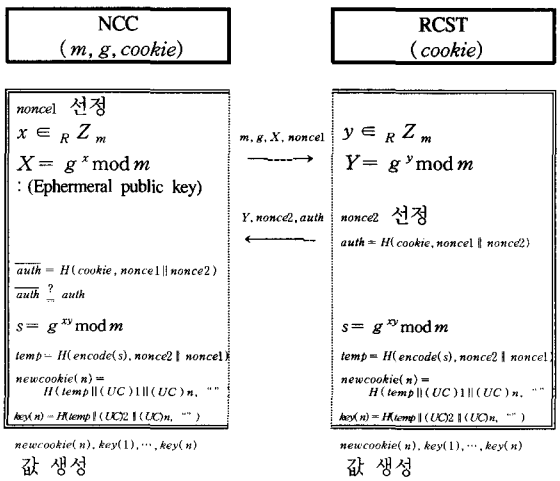


그림 4. MKE 프로토콜

NCC가 지닌 랜덤열(random string)이고 *nonce2*는 RCST가 지닌 랜덤열이다. 그리고 그림의 상단 박스는 참여자들의 아이디와 사전에 가져야 할 정보를 의미한다.

중간자 공격이란, 익명 DH 방식에서 두 통신 주체의 중간에 위치하는 공격자가 두 통신 주체들과 각각 통신하여 비밀을 공유하는 공격 방법이다. MKE 방식은 cookie를 이용하여 사용자를 인증하고, 임시의 DH 공개키를 교환하여 비밀을 공유하므로, 중간 공격자가 상대에서 오는 cookie를 그대로 넘기고, 자신의 임시 공개키를 상대에게 넘겨서, 상대와 비밀정보 s를 공유하게 하는 공격이다. 이는 기본적으로 사용자 인증을 위한 cookie와 임시 공격키가 긴밀하게 연결되어 있지 않음에 기인하는 공격이다. 결론적으로, 그림 4의 MKE 프로토콜은 공격자가 RCST와 NCC 중간에 위치하고 있다가 두 통신 주체들과 통신하여 비밀 정보 s를 계산할 수 있는 중간자 공격에 취약하다. 한번 중간자 공격에 의하여 새로운 비밀값 s를 알아내면, 계속적으로 다음 세션을 위한 새로운 cookie 값을 알아낼 수 있다. 따라서, 이후부터는 사용자 인증까지도 가능하게 된다. 이는 사용자의 임시 공개키와 사용자의 ID와 암호학적으로 결합되지 않아서 발생하는 문제이다. 또한 현재 나누어 갖고 있는 세션키 s를 확신할 수 있는 키확신 기능이 없다. 따라서, 이러한 측면에서 중간자 공격이 가능하다. 중간자 공격을 막을 수 있는 방법은 임시의 공개키를 사용하지 않고 장기간 공개키를 사용하게 하고, 장기간 공개키를 사용함으로써 발생되는 키의 신선도의 상실을 방지하기 위하여 별도의 난수를 도입하는 방식과 중간자 공격을 막기 위하여 장기간 공개키에 대한 인증서를 사용함으로써 이러한 취약점은 막아질 수 있다. 본 논문에서는 이러한 취약점을 막을 수 있는 다양한 방식을 제안한다.

2.2 Quick Key Exchange (QKE)

QKE방식은 기존의 쿠키와 기존의 비밀 공유 값을 이용하여 사용자 인증 기능만을 수행한다. 그림 5는 QKE의 과정을 나타내고 있다. 이는 기존의 쿠키를 이용하여 RCST가 NCC에 인증됨을 의미한다[6][7]. QKE방식이 MKE방식과 다른 점은 NCC와 RCST가 통신전에 비밀값 s와 cookie 값이 공유되어 있다는 가정이다. QKE 방식은 비밀값 s를 계산하는 과정이 없으므로 비밀 s를 계산하기 위한

DH 프로토콜의 수행을 요구하지 않는다. 또한 새로운 쿠키 계산 과정 역시 요구되지 않는다.

2.3 Explicit Key Exchange (EKE)

이 방식은 NCC가 자신이 미리 결정한 세션키를 RCST에게 전달하는 것이 특징이다. 이는 브로드캐스트 서비스를 위하여 사용될 수 있는 프로토콜이다. 이 방식에서는 현재의 쿠키값을 이용하고 인증 기능이 제공된다[1]. 세션키를 암호화하기 위한 암호화 키는 쿠키로부터 유도된 임시키(temporary key)를 사용한다. 다음 식 (1)과 식 (2)는 임시키와 encryptedKey을 나타낸다. 그림 6은 EKE의 과정을 나타낸 것이다. 여기서, UC는 유형 unsigned char이다.

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

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

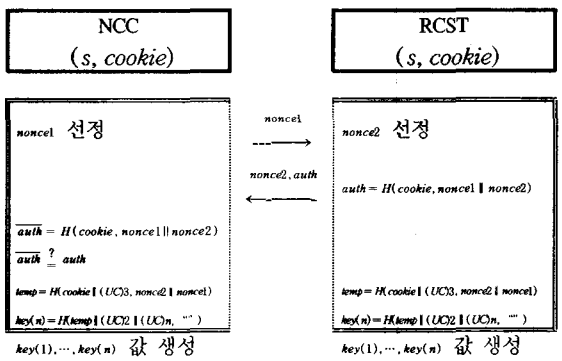


그림 5. QKE 프로토콜

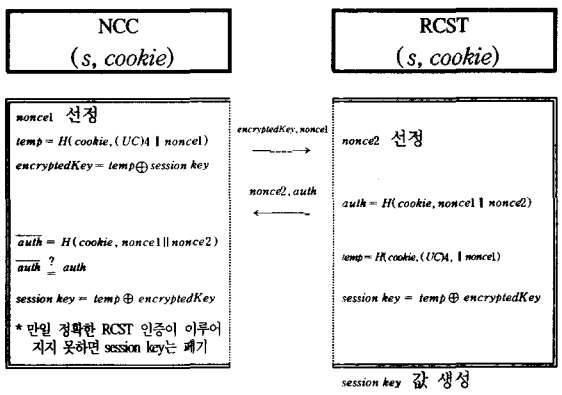


그림 6. EKE 프로토콜

Ⅲ. 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 않는다[9]. 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 1과 같은 채널과 신호요소를 이용한다.

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 _required요소 (1비트)	"1"이면 보안 핸드세이크가 반드시 요구됨을 의미함
리턴링크 (RCST → NCC)	리턴링크의 CSC (Common Signalling Channel)	RCST Capability 필드의 security mechanism 파라메터	"1"이면 RCST가 보안능력을 갖고 있음을 나타냄

3.2 보안을 위하여 사용되는 채널

보안을 위하여 사용되는 보안 MAC 채널은 전진링크의 경우 〈MAC〉Security Sign-On, 〈MAC〉Main Key Exchange, 〈MAC〉Quick Key Exchange, 〈MAC〉Explicit Key Exchange로 구성되며, 리턴링크의 경우 〈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 2에 기술되어 있다.

또한 보안 통신을 위하여 비밀 교환, 세션키 교환, 쿠키 및 복제방지 카운터 갱신은 표 3과 같은 시점에 수행되어야 한다.

인증은 NCC가 RCST를 인증하는 모드와

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

표 4. 보안 알고리즘 유형과 보안 파라메터 크기

		보안 파라메터 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	-
	RSA	1,024	1,024	-
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

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

광대역 위성망을 위한 암호 프리미티브는 키 교환 알고리즘, 해쉬 알고리즘, 기밀성 알고리즘, 그리고 난수 생성기 등이 요구된다. 기존의 ETSI 표준에는 표 4와 같은 암호 프리미티브를 사용하지만, 본 논문에서는 다양한 안전성을 고려하고, 국내의 암호 알고리즘을 포함한 표 4와 같은 암호 프리미티브에 대한 규격을 제안한다.

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 알고리즘에 대한 표준화도 조만간 요구된다. 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 5와 같이 설정할 것을 제안한다[1][2][4].

표 5. 국내 security sign-on 메시지 구조

종류	비트 수	해석	예
키교환을 위한 공개키 알고리즘	8	uimsb	- 0 : PKA_DH_512 - 1 : PKA_DH_764 - 2 : PKA_DH_1024 . . .
해쉬 알고리즘	8	uimsb	- 0 : HMACSHA1 - 1 : HMACMD5 - 2 : HMACSHA160 . . .
암호 알고리즘	8	uimsb	- 0 : DES - 1 : SEED - 2 : AES . . .
넌스 크기	8	uimsb	- 0 : 64 비트크기 - 1 : 128 비트 크기 - 2 : 160 비트 크기 . . .

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 패이로드 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 - 스터핑 바이트가 부가될 수 있음
ATM cell	ATM 패이로드	VPI/ VCI	- ATM cell 패이로드에 대해 적용됨

기밀성 서비스 관련된 주요 규격은 표 6과 같다. 일반적으로 세션키는 2가지 종류가 있다. 이중 현재 암호화된 정보가 어떤 키로 암호화되어 있는지를 확인하는 비트는 다음과 같으며 표 8에 기술되어 있다.

암호화의 기본 단위 신호는 패이로드 데이터 스트림이다. 보안 문맥은 일반적으로 두 개의 세션키로 구성된다. 두 개의 세션키의 각각은 전진 링크와 리턴 링크의 패이로드를 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 패이로드 암호화가 가능해진다.

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

일반적으로 키 교환의 주도권은 NCC에 있어야 한다. 이는 NCC가 키 교환을 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 9에 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

일반적으로 키 교환의 주도권은 NCC에 있어야 한다. 이는 NCC가 키 교환을 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 9에 정리되어 있으며 다음과 같은 특성을 지닌다.

보안 설정은 크게 〈MAC〉 security sign-on 핸드세이크 과정, 키 교환 과정, 로그온 후에 보안 문맥(security context) 갱신 과정으로 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 페이로드를 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.

표 10. 각 보안 단계의 용도

단계	주요 기능	용도	비고
MKE 과정	- 비밀 공유 - RCST 인증 - 새로운 쿠키 갱신 - 세션키쌍 교환	지점간 스크램블링	- DH 알고리즘 파라메터 설정
QKE 과정	- RCST 인증 - 세션키쌍 교환	지점간 스크램블링	- MKE보다 고속 동작 가능함
EKE 과정	- 비밀 공유 - 세션키 교환 - RCST 인증	멀티캐스트 암호	- 하나의 세션키를 생성함

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	-	-

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

앞장에서 제시된 세 가지 키 교환 방식의 특징을 비교하면 표 11과 같다. 표 11에서 쿠키값은 통신 상대를 인증하기 위하여 사용되며, 키 생성 주도권은 누가 키 교환 프로토콜을 시작하는지를 결정한다.

Ⅳ. 국내 위성 시스템을 위한 키 교환 알고리즘 제안 및 안전성 분석

4.1 키 교환 프로토콜에 대한 요구사항과 기존 키 교환 프로토콜의 단점

국내 위성망을 위한 키 교환 방식이 가져야할 주요 요구사항은 다음과 같다. 첫째, 교환된 비밀은 안전해야 한다. 둘째, 키 교환방식은 중간자 공격(Man-in-the-middle attack)에 면역성이 있어야 한다. 셋째, 교환된 비밀은 신선도(freshness)를 유지하는 특성을 가져야 한다. 키 신선도는 교환되는 비밀이 교환되는 난수와 연관되어 생성됨으로써 달성된다. 넷째, 교환된 비밀은 통신상대가 교환된 키를 공유하고 있다는 것을 또 다른 통신상대에게 보여줄 수 있어야 한다. 이 특성을 키 확신(key confirmation) 기능이라고 한다. 따라서 키 교환 방식은 기본적으로 이러한 네가지 요구조건을 만족하는 비밀을 교환하는 것이 바람직하다. 그러나 기존의 광대역 위성 액세스 망을 위한 MKE 방식은 임시 DH 키 교환 파라메터를 이용하여 비밀 정보를 교환하므로 교환되는 비밀은 세션마다 변경되나, 중간자 공격에 취약한 단점이 있고, 키 확신 기능도 제공되지 못하는 단점이 있다. 중간자 공격에 면역성이 있어야 할 이유는 NCC와 RCST 사이에는 수 많은 전송 장치와 네트워크 요소들이 존재하게 되고, 전송 장치나 네트워크 요소에 존재하는 공격자에 의한 중간자 공격이 기존의 MKE 방식에서는 언제든지 가능하기 때문이다.

4.2 키 교환 프로토콜 제안과 제안 방식의 안전성 분석

본 논문에서는 키 확신 기능을 갖고, 중간자 공격

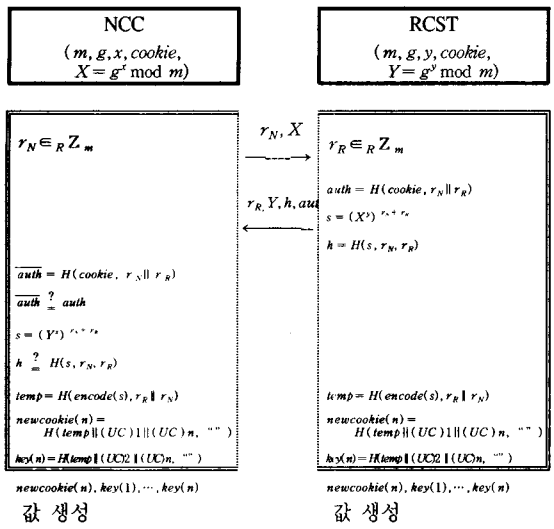


그림 7. 제안 방식1 프로토콜

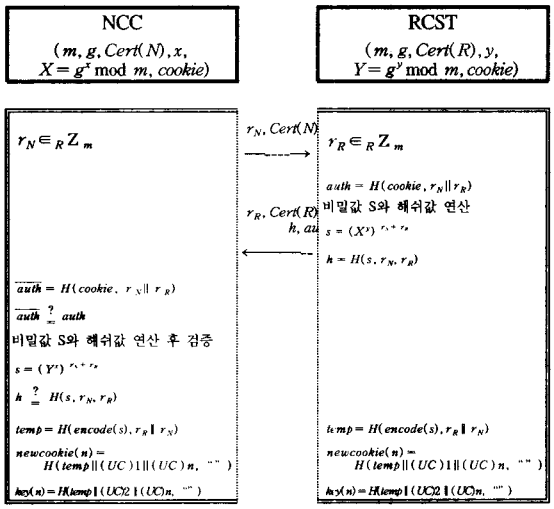


그림 8. 제안 방식2 프로토콜

에 면역성이 있으며, 키 신선도가 유지되는 MKE를 위한 키 교환 방법을 제안한다. 이 방식은 기존의 MKE를 위한 보안 관리 메시지의 변경을 최소화하면서, 비밀의 신선도를 보장하고 키 확신 기능을 제공한다. 제안 방식은 각각 그림 7, 8, 9, 10과 같다.

그림 7과 같은 제안방식 1은 기본적으로 MKE 방식과 동일하나, 장기간 공개키를 도입하고, 장기간 공개키의 도입으로 인하여 비밀의 신선도가 제공되지 않은 단점을 극복하기 위하여 교환되는 비밀 s가 난수와 DH 변수에 의하여 결정되도록 하였다. 교환되는 비밀이 난수 값에 의하여 결정되므로 비밀값이 변하게 된다. 그러나 제안 방식 1역시 중간자 공격에 취약함을 쉽게 알 수 있다.

이러한 문제의 근본 원인은 사용자의 ID 와 공개키가 긴밀하게 암호학적으로 결합되지 않음에 기인하므로, 이를 막기 위하여 그림 8과 같은 제안 방식 2에서는 장기간 공개키에 대한 인증서를 도입하게 되었다. 여기서 $Cert(N)$은 NCC의 공개키 $X = g^x \bmod m$를 포함하고 있고, $Cert(R)$은 RCST의 공개키 $Y = g^y \bmod m$를 포함하고 있다. 따라서, 이 방식은 중간자 공격이 불가능하게 되고, 키 확신 기능이 있고 비밀의 신선도를 보장하는 특징이 있다. 한편, 인증서에는 RCST 나 NCC의 장기 공개키를 포함하고 있다.

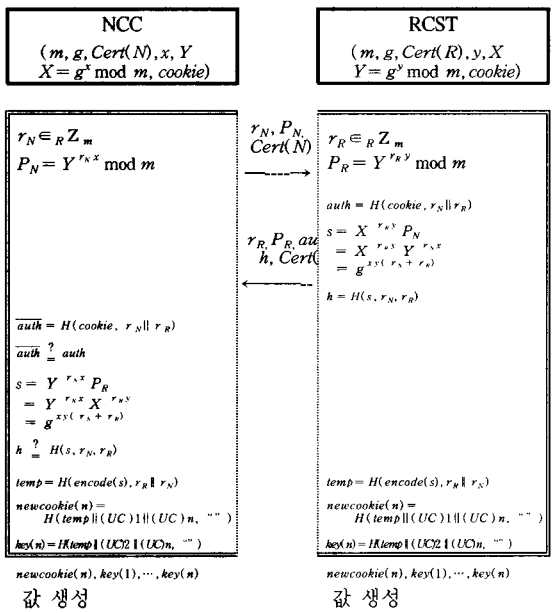


그림 9. 제안 방식3 프로토콜

그림 9의 제안 방식 3은 제안 방식 2와 키 분배 방식으로 DH 방식을 이용하지 않고 MTI 키 교환 방식을 이용하고 있다. 따라서, 제안 방식 2와 제안 방식 3은 기반 키 교환 방식이 다르고, 키 확신과 키 신선도를 갖는 방식이다. 이 방식 역시 장기간 공개키에 대한 인증서를 교환하여, 중간자 공격에 면역이 있는 특성이 있다.

그림 10의 제안 방식 4는 제안 방식 2를 타원 곡선 방식으로 변경한 방식이다. 이 방식 역시 인증서

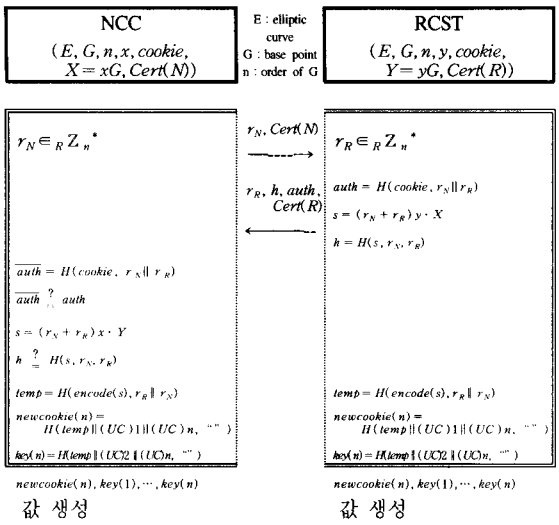


그림 10. 제안 방식4 프로토콜

방식을 도입함으로써, 역시 중간자 공격에 면역을 갖는 방식이다. *Cert(N)*에는 장기간 공개키 $X = xG$를 포함하고 있고, *Cert(R)*에는 장기간 공개키 $Y = yG$를 포함하고 있다. 이 방식 역시 키 신선도를 갖고, 키에 대한 확신기능이 있는 방식이다.

기존의 MKE 방식은 키 신선도를 제공하기 위하여 임시의 DH 공개키/개인키를 생성하고, 이를 교환함으로써 비밀을 공유한다. 그러나, 이 방식은 중간자 공격에 취약하다. 이는 통신상대의 중간에 존재하는 공격자가 두 통신상대와 별도의 비밀을 교환함으로써, 궁극적으로 키를 알게 되고, 결국 두 통신상대간의 비밀통신을 도청가능하게 한다. 만약 중간공격이 불가능한 환경이라고 가정하면, MKE도 안전하다고 할 수 있다. 그러나, 중간공격이 없다고 가정하기는 위성 링크에는 수많은 망요소의 취약점으로 인하여 이를 가정하기가 매우 어렵다. 만약 하나의 망요소가 공격자에 의하여 점유되게 되면, 중간자 공격이 가능하다는 것은 너무나 자명하다. 따라서 광대역 위성망에서 사용될 수 있는 MKE의 중간자 공격에 취약함을 방지할 수 있는 새로운 방식의 제안이 무엇보다도 필요하다.

제안방식 1과 기존의 MKE 와의 차이점은 기존의 MKE는 x, y라는 세션마다 선택되는 임시키(temporary key)를 이용하므로 공유되는 비밀의 신선도를 유지한다. 그러나, 제안방식 1은 x, y가 임시키가 아니고, NCC와 RCST의 장기간 개인키이다. 따라서 제안방식 1의 경우, x, y가 세션마다 선택되지 않으므로 교환되는 비밀의 신선도가 제공되지 않는다. 따라서 비밀의 신선도를 주기 위하여 난수 r_N, r_R의 도입이 필요하게 되었다. 키 분배에서 키 확신 기능은 매우 중요한 특성 중의 하나이며 세션마다 변경되는 비밀의 키확신성을 보장하기 위하여 하나의 해쉬값 ($H(s, r_N, r_R)$)을 전송하게 된다. 제안방식 1과 MKE와의 차이점은 장기간 키쌍을 사용 여부와 키확신성을 제공 여부이다.

키 신선도를 제공하기 위하여 제안 방식 1, 2에서는 *nonce1*, *nonce2*의 값을 대신하여 임의의 난수 r_N, r_R의 값과 상대방 공개키를 이용하여 기존의 DH 프로토콜을 수행함으로써, 세션마다 변화된 비밀값 s를 계산한다. 따라서 r_N, r_R이 바뀌면 교환되는 비밀값 s의 값도 바뀌게되므로 비밀의 신선도를 제공하며, 프로토콜에서 인증자를 제공함으로써 서로간의 키 확신성을 제공하는 방식이다. 또한 제안된 프로토콜이 수행되는 동안 *key*(n)값에 대한 어떠한 지식도 수동적 도청자에게 노출되지 않는다. 수동적 도청(passive eavesdropping)에 대한 보안이 DLP(Discrete Logarithm Problem)를 바탕으로 안정성을 향상시키고 있다. 프로토콜에서 공격자가 공개 채널에서 r_N, r_R값을 알고 있다하더라도, 공격자가 비밀값 $s = (X^y)^{r_N + r_R} = g^{xy(r_N + r_R)}$을 구하는 것은 DLP를 풀어내는 것만큼 어렵다.

제안방식 1은 중간자공격에 여전히 취약한 단점이 있지만, 제안 방식 1에서 x, y는 세션마다 임시적으로 할당되는 값이 아니다. 이 값은 NCC와 RCST의 장기간 개인키이므로, 세션마다 동일한 개인키를 사용하게 되므로 비밀이 일정하게 되며, 물론 이러한 경우라도 *temp* 값의 신선도는 유지되나 비밀(s)의 신선도는 유지되지 않는다. 따라서, 안전성 측면에서 모든 키의 근본이 비밀의 신선도를 보장하는 것이 *temp*에 대한 신선도를 주는 것보다 암호학적으로 안전하다.

제안 방식 2는 제안방식 1의 문제점인 중간자 공격을 방지하기 위하여 제안 방식1에서의 공개키를 인증서(certificate)로 대체하여 전달하는 방식이다. 이 방식은 인증서가 갖는 특성을 이용함으로써, 중간자 공격에 면역이 있다. 또한 비밀의 신선도와 확신성을 제공한다.

제안 방식3은 MTI 키 분배 방식[13]에 기반을 둔 방식으로 사전에 상대방의 고정 공개키(X, Y)를 가

지고 있으며 이를 이용하여 임시 공개키를 만든다. 이는 기존의 방식과 다르게 난수 r_N, r_R을 이용하여 비밀의 신선도를 제공하고, 상대방의 고정 공개키를 이용하여 만든 P_N, P_R은 MTI 키 일치 프로토콜을 이용하여 DHP(Diffie-Hellman Problem), DLP (Discrete Logarithm Problem)를 바탕으로 안정성을 향상시켰다. 여기서, X, Y : 고정 공개키, x, y : 고정 개인키, r_N, r_R : 임시 개인키, P_N, P_R : 임시 공개키 역할을 한다.

제안 방식4는 타원곡선 암호기법을 이용한 키 교환 방식을 제안한다. 타원곡선 암호기법은 160비트의 키 길이로 DH 1024비트의 키 길이와 비슷한 강도를 가지기 때문에 제안 방식 4는 계산적 복잡도와 교환되는 통신량의 측면에서 기존의 방식보다 효율적이고, 키의 신선도와 확신성을 제공하는 방식이다.

제안된 프로토콜들은 능동적 중간자 공격(active man in the middle attack)에 강인하다. 능동적 중간자 공격은 공격자가 양쪽 개체를 합법적으로 가장하거나 혹은 NCC와 RCST 사이에서 메시지를 가로챈 다음, 공격자와 NCC, 공격자와 RCST 사이에 각각의 가장공격(impersonation attack)과 동일하다. 공격자는 프로토콜 내의 모든 대화내용을 이용하더라도 정확한 *cookie*값을 모르면 $\overline{auth} \neq auth$를 통과하지 못하지만, 키 교환 프로토콜과 사용자 인증 프로토콜이 독립적으로 수행되므로, 중간의 공격자가 이를 바로 넘김으로써 중간자 공격은 가능케 하는 단점이 있다.

제안된 프로토콜들은 재생공격(replay attack)에 강인하다. 재생공격은 공격자가 NCC의 이전 사용된 값을 재전송 하여 이미 정상적으로 생성된 이전의 $key(n)$을 다시 생성하기 위함이다. 그러나 모든 통신에서 매 세션마다 균일한 확률 분포에서 랜덤한 난수 값을 이용하기 때문에 이 공격에 대한 공격자의 성공 확률은 무시할 수 있다. 또한 공격자가 전단계 통신에서 사용된 $newcookie(n)$값을 모른다면 $\overline{auth} \neq auth$를 통과하지 못한다.

기존의 ETSI MKE 방식과 네 가지 제안 방식과의 키 교환, 키 신선도, 키확신, 중간자 공격, 계산 복잡도, 통신 복잡도, 동일 강도의 키길이 비교는 다음의 표 12와 같다. 키 신선도는 임의의 난수를 통해 비밀 s값이 바뀌는지에 대한 유무이고, 키확신은 NCC와 RCST간에 통신 후에 동일한 키를 나누어 가졌는지의 유무이다. 계산 복잡도와 통신 복잡도는

표 12. ETSI 방식 MKE와 제안 방식의 비교(○:있음, △:보통, ×:없음)

	MKE	제안방식 1	제안방식 2	제안방식 3	제안방식 4
키 교환	○ (DH방식)	○ (DH방식)	○ (DH 방식)	○ (MTI 방식)	○ (타원곡선 방식)
키 신선도	○	○	○	○	○
키확신	×	○	○	○	○
중간자 공격에 대한 안전성	×	×	○	○	○
계산 복잡도	○ (하나의 멱승 연산)	△ (2 개의 멱승 연산과 하나의 가산 연산)	× (2개의 멱승연산, 하나의 가산 연산, 하나의 인증서 검증 연산)	△ (2 개의 멱승 연산과)	○○ (하나의 승산 연산과 가산연산, 하나의 EC상의 상수배 연산)
통신 복잡도	○ (난수, 공개키) 2048+160비트	△ (해쉬값, 난수, 공개키, 인증자) 2048+320비트	△ (해쉬값, 난수, 인증자, 인증서) 2048+320비트	△ (해쉬값, 난수, 공개키, 인증자) 2048+320비트	○○ (하나의 해쉬값, 난수, 공개키좌표, 인증자) 800비트
동일 강도의 키길이	1,024비트	1,024비트	1,024비트	1,024비트	160비트
키의 수명	임시 키쌍	장기적인 키쌍	인증서내의 키쌍	장기적인 키쌍	장기적인 키쌍

표 13. 제안된 방식을 위한 MKE Response 메시지 구조 변경(○:있음, △:보통, ×:없음)

메시지	비트	바이트	기능 설명
Main_Key_Exchange_Response() {	32	4	
Connection_ID			
Falgs Reserved_FL_Cookie_SN FL_Cookie_SN FL_Counter_SN Clone_Counter	 6 1 1 8	 1	 유보됨 인증을 위하여 쿠키가 사용됨 복제방지순서번호 표시 복제방지 순서번호
Nonce		P_{ns}	동일
Authenticator		P_{ha}	동일
DH_Public_Y		P_{pka}	동일
Hashed_Value }		P_{ha}	키확신을 위하여 부가됨

통신 과정에서 사용되는 연산 방법 및 연산 횟수, 계산되는 비트수이다. 표 12에서 적용된 해쉬 알고리즘은 HAS160을 사용하였고, DH 방식의 소스 p의 길이는 1024비트로 가정하였다. 또한 타원곡선은 소수 p의 길이가 160 비트인 유한체를 이용함을 가정하였다.

표 12에서 중간자 공격은 불법적인 공격자가 두 통신 상대의 중간에 존재하여 두 통신 상대와 각각 별도의 비밀을 교환함으로써, 두 통신 상대간의 비밀 정보를 도청하는 공격이다. 이를 해결하는 방법으로 제안방식 2, 3 ,4의 경우처럼 인증서를 이용하면 해결된다. 그러나, MKE 방식은 키 확신 기능이 없고, 중간자 공격에 취약한 단점이 있는 반면, 제안 방식 2, 3, 4는 키 확신 기능이 제공되고, 중간자 공격이 불가능하며, 제안방식 4는 타원곡선상의 방식이므로, 키의 길이와 교환되는 교환량이 작아지는 장점이 있다. 하지만, 이런 인증서를 이용하는 방식은 인증서 생성 및 인증서 취소 목록 유지 등의 또 다른 인증서 관리 작업을 해야 한다.

기존의 MKE 응답 메시지는 RCST를 인증하고 RCST가 NCC와 쿠키-독립 키 교환 방식을 이루도록 구성된다. 또한 현재의 클론 검출 카운터 값을 지닌다. 메시지 중의 플래그 필드는 Reserved_ FL_Cookie_SN, FL_cookie_SN, 그리고 FL_ Counter_SN을 지닌다. FL_Cookie_SN는 인증을 위하여 사용되는 쿠키의 순서번호를 의미하고, FL_Counter_SN는 클론 검출 카운터의 현재의 순서 번호를 나타낸다. Clone_Counter 필드는 현재 카운터의 값이 들어있다.

만약 NCC가 보낸 FL_Updata_Cookie가 "set" 되어 있다면, RCST는 새쿠키를 생성하고 쿠키 순서 번호를 갱신하고 클론 카운터를 "0"으로 설정 후 클론 순서 번호를 "0"으로 수정한다. 또한 만약 NCC가 보낸 FL_Updata_Counter가 "set" 되어 있다면, RCST는 클론 카운터를 증가하고 클론 카운터 순서 번호를 갱신하게 된다.

만약 중간자 공격이 위성 환경에서 가능하지 않다고 가정하면 제안 방식 1이 타당하다. 제안 방식 1,2,4를 이용하는 경우, 교환되는 정보를 전달하기 위하여 키확신을 위하여 해쉬값(P_{ha})을 추가하해야 하므로, 표 13과 같이 MKE 보안 메시지 중 Main Key Exchange Response를 변경해야 한다.

V. 결 론

본 논문의 목적은 기존의 프로토콜이 중간공격에 취약함을 보이고, 이를 해결하는 방법을 제시하기 위한 4가지 방식을 제시하는 것이다. 중간자 공격을 막기 위하여 세션마다 임시키를 이용하여 비밀을 공유하는 것이 아니라, 장기간 키 쌍을 도입하였고, 또한 이를 위한 인증서 방식을 제안하게 되었다. 또한 제안방식 3에서는 기존의 DH 키 분배 방식이 아닌 MTI 기본의 프로토콜로 제안했으며, 실용적인 측면에서 의미가 있는 타원곡선에 기반을 둔 제안방식 4를 제시한 것입니다. 이를 위하여 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 제시하였으며 기존의 ETSI 에서 제안한 방식에 더하여 국내에서 개발한 다양한 암호 알고리즘을 이용한 방식을 제안하였다. Ⅳ장에서 제안한 제안방식 1과 2, 3 키 교환 프로토콜은 기존 표준안에서 제시되고 있는 방법에 비해 키의 신선도와 확신성을 갖는 반면에 계산 복잡도를 약간 증가시킨다. 그러나 제안방식 2는 키 신선도, 중간자 공격 면역성 등 여러 특성이 있어서 활용이 기대된다. 그리고 타원곡선을 이용한 제안방식 4의 키 교환 방식이 계산의 복잡도와 교환되는 통신량 측면에서 기존의 방법과 비슷한 복잡도를 가지고 있고, 키의 신선도와 확신성을 제공하는 가장 우수한 방법이라고 할 수 있다. 따라서 제안방식 4의 알고리즘이 광대역 위성망을 위한 키 공유 방식으로 가장 적합하다고 여겨진다. 추후에는 제안방식 들에 대한 하드웨어 또는 소프트웨어를 실현하기 위한 연구를 수행할 예정이다.

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, "Autheticated key exchange secure against dictionary attack," Eurocrypt 2000.

[5] V. Boyko, P. Mackenzie and S. patel, "Provabley 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, Auguest 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] ETSI homepage, http://www.etsi.org/home.htm.

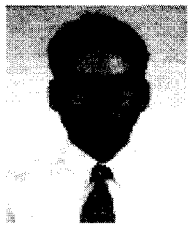
[11] ETSI EN 301 192 : "Digital Video Broadcasting(DVB) : DVB specification for data broadcating".

[12] Dr.Reinhard Scholl, "The ETSI Bake-off Service as a Way to Enhance the Quality of Standards", KT본부 Mailzine 표준화 동향 제3호, 2000, 10.

[13] T. Matsmoto, Y. Takashima and H. Imai, "On Seeking Smart Public-key Distribution Systems," The Transaction of the IECE of Japan, E69, pp.99-106, 1986.

〈著者紹介〉

오 흥 룡 (Heung-Ryong Oh) 정회원
2002년 2월 : 순천향대학교 전자공학과 학사
2004년 2월 : 순천향대학교 정보보호학과 석사
2004년 2월~현재 : 한국정보통신기술협회(TTA)
〈관심분야〉 보안 프로토콜, 정보보호표준



염 흥 열 (Heung-Youl Youm) 정회원
1981년 2월 : 한양대학교 전자공학과 학사
1983년 2월 : 한양대학교 대학원 전자공학과 석사
1990년 2월 : 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
2003년 9월~현재 : ITU-T SG17/Q10 Associate Rapporteur
〈관심분야〉 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안