무선 환경에서 금융거래를 위한 프로토콜과 운영에 관한 연구

김대엽*, 신동규*, 임종인**

*시큐아이닷컴, 정보보호 연구소

** 고려대학교 정보보호 연구소

A Study on Protocol and Operation for Financial Transaction in Radio Environment

Dae-Youb Kim*, Dong-Gyu Shin*, Jong-In Lim**

*SECUI.COM, R&D Center

** Center for Information Security Technologies(CIST), Korea University

요 약

전자상거래의 활성화는 인터넷을 통한 금융거래를 보편화시켰고, 안전한 금융거래를 제공하기 위한 보안 프로토콜과 서비스가 지속적으로 개발되고 있다. 이러한 기술적 발전을 바탕으로 무선단말기를 통한 금융거래 서비스에 대한 관심이 높아지고 있다. 본 논문에서는 전용패킷교환방식의 무선데이터통신 환경 아래에서 전용 단말기를 이용한 금융거래에 필요한 인증 및 데이터 보호 등을 제공하는 프로토콜과 운영방안을 제안한다. 제안하는 프로토콜에서는 단말기와 인증서버 사이의 키 공유를 위하여 password-based protocol과 ANSI X9.17을 사용하는 키 운영방안을 제시하고, 가입자 id와 비밀번호에 근거한 인증절차와 전송 데이터 암호화를 통한 안전한 금융거래를 제공한다. 또한, 무선 Gateway에 의한 보안 제어가 아닌, End-to-End의 보안 서비스를 제공함으로, 그 신뢰성을 높이도록 설계되었다.

I. 서론

인터넷을 통한 전자상거래가 널리 보급되면서 인터넷 뱅킹, 인터넷 주식거래와 같은 금융서비스를 쉽게 접할 수 있게 되었다. 뿐만 아니라, 이러한 금융서비스들은 고객의 다양한 요구를 충족시키고, 더욱 쉽게 서비스를 이용할 수 있도록 유/무선 통합 환경에서 제공되고 있다. 이와 같은 금융서비스가 안전하게 제공되기 위해서는 변조, 도청, 신분위장, 재전송과 같은 불법적인 위협요소에 대한 대처 방안이 제공되어야 한다. 일반적으로, 위협요소로부터 정보를 보호하기 위하여 기밀성, 무결성, 인증 서비스가 제공되며, 무선 데이터 통신 환경에서도 이러한 보안 서비스를 효과적으로 운영하기 위한 연구가 계속 되어 왔다 [1][2].

본 논문에서는 전용패킷교환 방식의 무선 데이터 통신 환경에서 전용 단말기를 사용한 금융거래에 필요한 프로토콜과 운영방안을 제안한다. 제안된 프로토콜은 단말기의 성능을 고려해 공개키 암호시스템을 사용하지 않으며, 가입자 인증을 위하여 id와 비밀번호(Password , PW)를 사용한다. 기밀성을 제공하기 위해 전송되는 데이터는 블록 암호 시스템을 사용해 암/복호 되며, 데이터 무결성을 제공하기 위하여 HMAC[3]을 사용한다. 또한, 단말기와 인증서버의 키 공유를 위하여, password-based protocol과 ANSI X9.17에 기초한 키 운영 메카니즘을 사용한다[4][5][6][7].

본 논문은 다음과 같이 구성되었다. 2장 1절에서는 전용패킷교환 방식의 무선 데이터 통신을 소개한다. 2장 2절에서는 제안하는 프로토콜의 구성요소와 키 계층구조를 설명하고, 2장 3절에서는 프로토콜과 메시지의 구조에 대하여 제시한다. 2장 4절은 안전성에 대해 평가한다.

II. 무선 데이터 서비스 프로토콜

1. 무선 데이터 서비스

무선 데이터 통신(Wireless Data Communication) 서비스는 전송로의 일부를 무선화 하여 이동 중 혹은 정지 중에 사용 가능한 양방향 공중통신 서비스로 장소의 제약 없이 각종 데이터 전송이나 데이터베이스와 접속이 가능한 통신서비스이다[8][9]. 현재 서비스 중이거나 개발된 무선 데이터 통신을 분류한다면 그림 1과 같이 구분할 수 있으나, 포괄적으로는 셀룰러시스템, 전용무선패킷망, TRS망, 위성통신망 등으로 볼 수 있다.

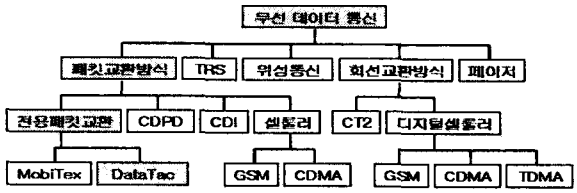

그림 1 : 무선 데이터 통신.

셀룰러시스템 방식에는 회선교환방식, CDPD, CDI 등이 있고, 전용무선패킷망으로는 Motorola의 DataTAC과 Ericsson의 Mobitex 등이 있으며, 현재 국내 무선증권거래에는 AirMedia 사가 DataTAC을 사용하여 서비스 중에 있다. DataTAC의 구조는 그림 2와 같이 구성되며 표준 X.25 망이 사용되는 곳에서는 어디서나 이동 단말 사용자가 접속할 수 있다. 비동기, 쌍동기 프로토콜을 지원하며, 제2자의 게이트웨이를 통해서 TCP/IP와 IBM의 SNA 프로토콜을 지원한다.

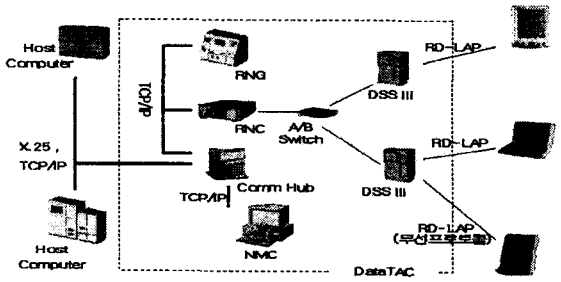

그림 2 : DataTAC 시스템 구성도.

2. 프로토콜 구성요소

1) 구성요소

전용무선패킷교환 방식의 무선 데이터 통신 환경에서 제안하는 프로토콜을 운영하기 위해 필요한 구성요소는 다음과 같다:

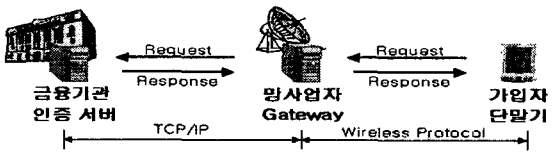

그림 3: 무선 금융거래

● 금융기관 인증서버: 가입자의 id, PW, 그리고 암/복호키를 관리하고, 가입자 인증 및 데이터 암/복호를 수행한다.

● 망사업자의 Gateway: 인증서버와 단말기 사이의 유/무선 프로토콜 변환 및 교환을 수행한다. DataTAC의 경우 무선 프로토콜은 RD-LAP를 사용하고, 유선 프로토콜은 X.25 또는 TCP/IP를 사용한다.

● 가입자의 전용 단말기: 무선거래를 위한 전용단말기로, 가입자 키와 필요한 정보를 저장/관리한다. 가입자 요청 메시지를 생성/전송하며, 인증서버로부터 전송된 응답 메시지를 처리한다.

2) 키의 종류

가입자 인증 및 전송 데이터의 암/복호에 사용되는 키의 종류와 관리방안은 다음과 같다.

● Initial Key(IK) : 단말기 기초 데이터의 암/복호에 사용된다. IK는 가입자 id와 PW, 그리고 단말기 LLI(Logical Link Identification)등의 정보와 Dictionary Attack을 막기 위한 Random Salt, Iteration Count(IC)등의 정보를 사용해서 단말기와 인증서버에서 독립적으로 생성/공유한다.

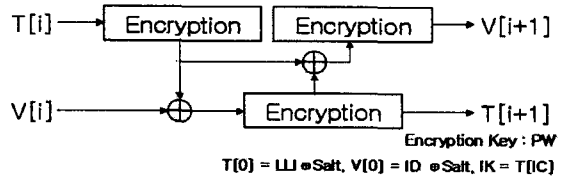

그림 4: IK 생성

● Master Private Key(MPK) : 인증서버에서 단말기에 제공하는 기초 데이터. 가입자 개인키(PK)의 갱신을 위해 사용된다.

● Private Key(PK) : 인증서버에서 단말기에 제공하는 기초 데이터. 가입자 인증 및 세션키(SK) 생성을 위해서 사용되며, Update Cycle(UC)

에 따라 주기적으로 갱신된다. UC는 PK를 갱신할 시점을 알려준다. UC의 값이 n 일 때, 단말기는 세션을 연결한 후, 해당 SN을 확인하여 식(1)을 만족하면, PK 갱신작업을 수행한다.

$$SN \equiv 0 \bmod 2^n \quad (1)$$

● Session Key(SK) : 설정된 세션 안에서 전송되는 데이터의 암/복호에 사용되는 키. 해당 세션에서만 유효하며, 세션이 종료되면 더 이상 유효하지 않다. 세션은 단말기의 전원이 공급되면 설정되고, 전원 공급이 중단되면 종료된다. 또한 거래시간이 마감되어 인증서버가 초기화되면 연결된 세션은 자동적으로 종료된다.

단말기에서 IK와 SK는 휘발성 메모리 영역인 RAM에 저장/사용된다. MPK와 PK는 EEPROM과 같은 비휘발성 메모리 영역에 IK로 암호화된 상태로 저장되고, 사용시 RAM 상에서 복호화 하여 사용한다.

3) 메시지 구조

단말기와 인증서버 사이에 교환되는 메시지의 구조는 그림 5와 같다. 단, 본 논문에서 정의되는 구조는 무선/유선에서 사용되는 프로토콜의 데이터 부분만을 의미한다.

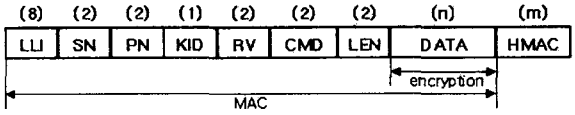

그림 5: 전송 메시지 구조.

● 단말기 번호(LLI) : 단말기에 할당된 8 바이트 고유 번호.

● 세션 번호(SN) : 단말기와 인증서버 사이에 설정된 세션에 할당된 2바이트 값으로 재사용 공격(Replay Attack)을 막기 위해 사용된다. SN은 단말기에서 설정/관리한다. 세션이 새롭게 설정될 때마다 1씩 증가하며, 0h와 FFFFh 사이의 값을 갖는다. 인증서버는 단말기 단위로 세션번호를 관리하며, 전송된 패킷의 SN이 저장되어 있는 SN 보다 작으면, 해당 패킷을 오류처리 한다. 단, 단말기와 인증서버에서 SN의 증가/비교는 mod FFFFh 아래에서 수행된다.

● 패킷 번호(PN) : 설정된 세션에서 교환되는 패킷에 할당된 번호로, 재사용 공격을 막기 위해 사용된다. 단말기에 전원이 공급되면 패킷 번호는 0h로 초기화되며, 단말기에서 생성되는 패킷마다 1씩 증가된 PN이 할당된다. 단, PN의 값이 FFFFh인 경우, 그 다음 패킷의 PN 값은 1h을 갖는다. 즉, PN은 1h에서부터 FFFFh 사이의 값으로 운영된다. 인증서버는 새로운 SN이 설정되면, PN을 0h으로 초기화하고, 단말기로부터 전송된 패킷의 PN이 저장된 PN 보다 작거나 같으면 오류처리 한다. 그렇지 않으면 전송된 패킷의 PN을 저장한다. 또한 인증서버에서 단말기로 전송되는 응답 메시지의 PN은 해당 요청 메시지의 PN과 동일한 값을 갖는다.

● 키 ID(KID) : 데이터 암호에 사용된 키를 구분하기 위해 사용된다. NULL인 경우, 전송되는 데이터는 평문임을 의미하며, HMAC은 생략된다 (표 1 참고).

표 1 : Key ID. * x:미정

Key Id bits								Key
b8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	0	no Encryption
0	1	0	0	0	0	0	0	IK
0	1	0	0	0	0	0	1	MPK
1	0	x	x	x	x	x	x	PKs
1	1	x	x	x	x	x	x	SKs

● 처리결과(RV) : 인증서버는 단말기의 요청 메시지에 대한 처리결과를 응답 메시지의 RV에 명시한다. 요청 메시지에서는 항상 NULL 값을 갖는다(표 3 참고).

● 명령(CMD) : 전송데이터의 종류(표 2 참고).

● 길이(LEN) : 전송 데이터의 길이.

● 데이터(DATA) : 메시지를 통해서 전송되는 실제 데이터.

● HMAC : LLI부터 DATA까지의 HMAC의 결과로, 데이터 암호화에 사용된 키와 동일한 키를 사용하며, 메시지의 KID가 NULL인 경우에는 메시지에서 포함되지 않는다.

3. 프로토콜

이 절에서는 제안하는 프로토콜을 설명한다. 프로토콜은 기본적으로 단말기의 요청 메시지에 대한 인증서버의 응답 메시지로 구성된다. 각 단계에서 사용되는 요청 및 응답 메시지의 구성은 표 2를 참고한다.

단말기와 인증서버는 공통적으로 수신된 메시지에 대한 오류 여부를 우선 확인한다. 즉, LLI, SN, PK, KID, CMD, LEN등의 유효성을 검사하고, DATA가 암호화되어 있으면, 해당 LLI의 KID가

표 2 : 전송 메시지 종류 및 구성 * h:16진수, b: 2진수, x:미정

메시지	KID	RV	CMD	LEN	DATA	HMAC
ReqSalt	00h	0000h	A001h	0		No
ResSalt		xxxxh	A002h	0 / n	Salt, IC	No
ReqInitBlock	40h	0000h	A003h		id, PW	No/Yes
ResInitBlock		xxxxh	A004h		MPK,(Key id,PK),UC	No/Yes
ReqAuthen	10xxxxxxb	0000h	A005h		id, PW	No/Yes
ResAuthen		xxxxh	A006h		(KeyId, SK), 계좌정보	No/Yes
ReqUpdatePK	41h	0000h	A007h		id, PW	No/Yes
ResUpdatePK		xxxxh	A008h		(KeyId, PK)	No/Yes
ReqChangePW	10xxxxxxh	0000h	A009h		id, PW, new PW	No/Yes
ResChangePW		xxxxh	A00Ah		new PW	No/Yes
ReqOrder	11xxxxxxb	0000H	B00xh		id, PW, order	No/Yes
ResOrder		xxxxh	B00xh		orderResult	No/Yes

표 3 : 오류 처리 * S:성공, W:경고, E:오류

RV		내용 : 처리	RV		내용 : 처리
0000h	S	정상.	1007h	E	부적합한 Key id 오류, 사용된 키와 명령이 부적합한 경우 발생: 단말기 기초 데이터 재설정 또는 단말기 프로그램 교체.
0001h	W	PK 갱신 필요: PK 갱신 수행.			
1001h	E	id 오류: id 재 입력 요청.			
1002h	E	PW오류: PW 재 입력 요청.	1008h	E	HMAC 오류: 사용된 키에 따라 다음과 같이 처리한다. SK-세션 재설정, PK-PK 갱신, MPK-단말기 기초 데이터 재설정 IK - IK 재 생성.
1003h	E	LC오류: 단말기 기초 데이터 재 설정.			
1004h	E	SN/PN 오류: 세션 재설정.			
1005h	E	CMD 오류: 단말기 프로그램 교체.			
1006h	E	Key id 오류, PK/SK의 동기에 이상: 사용한 키가 PK 경우는 PK 갱신을 시도하고, SK인 경우는 세션을 재 설정한다.	1009h	E	LEN 오류: 단말기 프로그램 교체.
			2xxxh	W	금융기관이 독자적으로 정의한 경고/오류.
			4xxxh	E	

나타내는 키로 복호화와 HMAC 검사를 수행한다. 인증서버의 경우, 수신 메시지에 오류가 있으면 응답 메시지의 RV에 이를 명시하고 단말기로 전송한다. 또한, 단말기는 해당 응답 메시지의 RV에 따른 오류처리를 표 3과 같이 수행한다. 이 후, 특별한 언급이 없어도 메시지 수신 후 이와 같은 오류 확인 및 처리는 항상 수행되는 것으로 간주한다.

1) 등록(Off-Line)

● 가입자는 증권사로 직접 방문해서 자신의 id와 PW를 등록하고 단말기를 제공받는다.

● 인증서버는 난수 발생기를 사용하여 Salt와 IC를 생성한다. 생성한 난수와 가입자 id/PW, 그리고 LLI를 사용해서 IK를 생성한다. IK는 그림 4와 같이 ANSI X.917 알고리즘을 기반으로 생성한다. Salt, IC, IK, LLI, 그리고 id를 데이터베이스에 저장하고 PW의 해쉬값을 저장한다.

2) 단말기 초기화 및 인증

● 전원이 공급되면, 단말기는 이전 세션에 할당했던 SN에 1을 더해서 새로운 SN 값으로 설정하고, PN을 0h으로 초기화한다. 또한 가입자 id와 PW를 가입자로부터 입력받는다.

● 단말기는 ReqSalt 메시지를 전송한다.

● 인증서버는 데이터베이스에서 해당 LLI와 함께 저장되어 있는 Salt와 IC를 읽어와 ResSalt 메시지를 생성/전송한다.

● 단말기는 IK를 생성/저장한다.

● 단말기는 Life Cycle(LC)을 확인한다. LC가 초기상태 값(FFh)을 갖고 있으면, 단말기 기초 데이터 설정 작업을 다음과 같이 수행한다:

[1] 단말기는 ReqInitBlock 메시지를 생성한다. ReqInitBlock의 DATA는 IK로 암호화되어 인증서버로 전송된다.

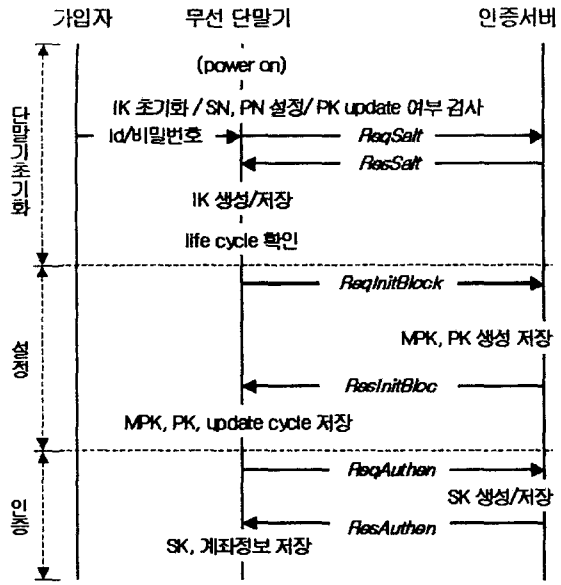

그림 6: 단말기 초기화 및 인증

[2] 인증서버는 MPK와 PK를 생성/저장하고, ResInitBlock 메시지를 생성/전송한다. DATA는 IK로 암호화된다.

[3] 단말기는 MPK, (Key id, PK), UC를 저장하고 LC를 1h로 설정한다. 이 때, MPK와 PK는 IK로 암호화되어 저장된다.

● LC가 1h이면, 단말기는 세션을 설정하고 Log-In 및 SK 생성작업을 다음과 같이 수행한다:

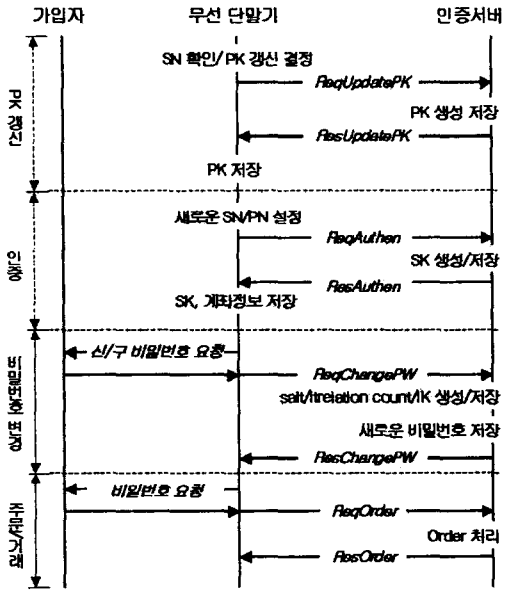

그림 7: PK/PW 변경, 주문

[1] 단말기는 ReqAuthen 메시지를 생성해서 인증서버로 전송한다. DATA는 PK로 암호화된다.

[2] 인증서버는 난수발생기를 사용하여 SK를 생성/저장하고, ResAuthen을 생성/전송한다. DATA는 PK로 암호화된다.

[3] 단말기는 (Key id, SK)와 계좌정보를 저장한다. 이제, 공유된 SK로 금융거래 요청 및 응답 메시지를 암/복호할 수 있다.

3) PK 갱신

단말기는 SN을 확인하여, PK 갱신 여부를 판단한다. PK 갱신이 필요하면 다음을 수행한다:

[1] 단말기는 ReqUpdatePK를 인증서버로 전송한다. DATA는 MPK로 암호화된다.

[2] 인증서버는 새로운 PK를 생성/저장하고, ResUpdatePK를 생성/전송한다. DATA는 MPK로 암호화된다.

[3] 단말기는 새로운 PK를 IK로 암호화 해서 저장한 후, 새로운 세션을 설정한다. 만약 HMAC 값에 오류가 발생하면, 단말기 LC를 FFh로 초기화하고, 새로운 세션을 설정한다.

4) 비밀번호 변경

● 단말기는 ReqChangePW를 생성/전송한다. DATA는 PK로 암호화 한다.

● 인증서버는 새로운 Slat와 IC를 생성한 후, 가입자 id와 변경된 PW로 새로운 IK를 생성해서 데이터베이스에 이 값들을 저장하고, 변경된 PW의 해쉬값을 저장한다.

● 인증서버는 ResChangePW를 전송한다. DATA는 PK로 암호화 한다.

● 단말기는 Salt/IC를 요청/획득하고, 새로운 IK를 생성/저장한다. PK와 MPK를 새로 생성한 IK로 다시 암호화해서 저장한다.

5) 데이터 교환

단말기와 인증서버 사이에 세션이 설정되고, SK가 공유되면, 전송되는 ReqOrder와 ResOrder의 DATA를 SK를 사용하여 암/복호 한다. Order와 그 처리결과는 금융서비스의 종류에 따라 다양하게 정의할 수 있다.

6) 인증 시스템 초기화

금융기관의 거래가 마감되면, 인증서버는 다음

거래 개시 시점까지 초기화된다. 이 때, 각 가입자의 세션번호와 패킷번호가 각각 0h로 초기화된다.

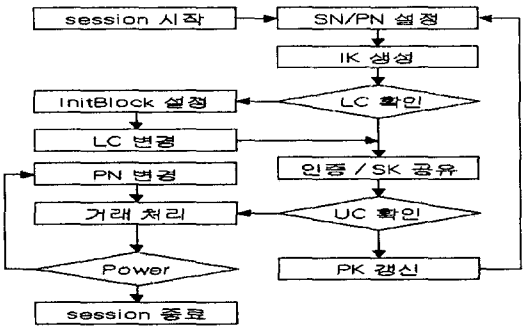

그림 8: 단말기 운영도.

4. 안전성

제안된 프로토콜은 id와 PW를 기반으로 가입자 인증을 수행한다. 전송되는 id와 PW는 암호화된 상태로 전송되기 때문에, 도청이나 위/변조가 불가능하다. 인증서버에는 해쉬된 PW가 저장되어 있기 때문에 전송된 PW를 해쉬해서 결과를 비교하며, 인증서버 데이터 베이스에 접근 가능한 운영자라 하더라도 가입자의 PW를 알 수 없다.

또한, 전송되는 패킷은 각각의 SN과 PN을 갖고 있으며, 인증서버는 가입자별로 SN과 PN을 관리하기 때문에 재전송 공격 시도는 항상 차단된다.

Salt 요청/응답 메시지를 제외한 모든 메시지는 암호화 되기 때문에, 도청에 대한 위험이 없으며, 각 메시지의 HMAC는 데이터의 위/변조 여부를 알려준다.

그리고, 단말기의 IK와 SK는 휘발성 메모리에 저장됨으로 전원 공급이 중단되면, 초기화되어 그 값을 알 수 없다. 또한 비휘발성 메모리에 저장되는 MPK와 PK는 IK로 암호화되어 저장되고, 필요시 복호화해서 사용하기 때문에 스마트카드와 같은 다른 저장 도구를 사용하지 않고도 가입자의 키를 안전하게 저장/관리할 수 있다.

단말기의 성능을 고려해서 공개키 기반의 암호 시스템을 사용하지 않기 때문에, 부인봉쇄와 같은 서비스에 취약하다. 그러나 모든 메시지에 가입자의 PW가 포함되고, 해당 PW를 아는 사람은 가입자뿐이므로 부분적인 부인봉쇄 기능은 제공된다고 할 수 있다.

III. 결론

본 논문에서는 유/무선 통합 환경에서 사용 가능한 id와 PW 기반의 프로토콜을 제안했다. 제안된 프로토콜은 무선 게이트웨이에 의한 보안 제어 형식이 아닌 단말기와 금융기관 인증서버 사이의 end-to-end 보안 형태를 취하고 있다. 무선 환경에서 단말기와 통신 성능을 고려해서 메시지를 간단하게 설계했으며, 일반적인 위험요소들에 대한 대처 방안으로 데이터의 암/복호, HMAC, 세션/패킷 번호 등을 사용했다. 또한 단말기와 인증서버 사이의 키 공유 및 관리를 위해 password -based protocol과 ANSI X9.17을 사용한 IK 공유 방안을 제시했으며, 인증에 사용되는 MPK/PK와 데이터 암/복호를 위한 SK 등을 안전하고 효과적으로 운영하도록 설계하였다.

참고문헌

[1] 정현철, 신기수, 이선우, 김봉한, 김점구, 이재광, "안전한 종합정보통신망을 위한 키 분배 프로토콜과 호 제어", 한국정보처리학회 논문지 제4권 제1호, pp 195-208, 1월 1997년.

[2] 박정현, 임선배, 이경준, "이동통신 보호를 위한 인증 방식 분석", 전자통신동향분석, 제13권 제4호 1998년 8월.

[3] H. Krawczyk, M. Bellare, and R. Canetti, "RFC2104: HMAC: Keyed hashing for Message Authentication", IETF, February 1997.

[4] S.M.Bellovin, M.Merritt,"Encrypted key exchange: Password-based protocols secure against dictionary attacks", In Proceeding of the 1992 IEEE computer Society Conference on Research in Security and Privacy, pp 72-84, IEEE Computer Society, 1992.

[5] D.P.Jablon, "Strong Password-only Authenticated Key Exchange", ACM Computer Communications Review, 1996.

[6] R.Perlman, C.Kaufman, "Secure Password -Based Protocol for Downloading a Private Key", Proc. of the 1999 Network and Distributed System Security(NDSS), 1999.

[7] RSA Laboratories, "PKCS #5 v2.0: Password-Based Cryptography Standard", March, 1999.

[8] "무선데이타 서비스", 전파진흥, 7권 5호, 1997년 9, 10월.

[9] 이재호, "정보통신망과 프로토콜", 북두출판사, 2월 2000년.