생체정보를 이용한 키 분배 프로토콜에 관한 연구

이진우*, 원동규*, 한종수*, 곽진*, 원동호*

*성균관대학교, 컴퓨터공학과

Key Distribution Protocol using Bio-information

Jinwoo Lee*, DongKyu Won*, Jongsu Han*, Jin Kwak*, Dongho Won*

*Dept of Computer Engineering, Sungkyunkwan Univ.

요 약

최근, 디지털 기술과 네트워크의 발달로 다양한 무선통신 단말기, 반도체, 디지털 방송, 전자상거래 등 다양한 분야가 융합되어 사람과 디바이스간에 실시간으로 정보를 주고받는 환경 즉, 유비쿼터스 컴퓨팅 환경에 많은 관심이 주목되고 있다. 이러한 유비쿼터스 컴퓨팅 환경에서의 통신은 통신개체간에 실시간 개체인증은 물론 전송되는 정보의 무결성, 기밀성 등 보안 서비스가 요구된다. 현재의 개체 인증은 사용자가 기억하는 패스워드 또는, 스마트 카드와 같은 보안 모듈을 사용하여 사용자와 개체간에 인증이 이루어지고 있는 실정이다. 이러한 방식은 사용자가 기억해야 할 패스워드가 증가한다거나, 보안 모듈의 손상 및 분실로 인해 자신의 프라이버시(privacy)가 노출될 수 있는 단점이 있다. 이에 본 논문에서는 사용자 고유의 생체 정보와 기억할 수 있는 패스워드를 비밀정보로 사용하여 양방향 개체 인증 키 분배 프로토콜을 제안한다.

Ⅰ. 서론

유비쿼터스 컴퓨팅 환경은 Anytime, Anywhere, Anynetwork, Anydevice, Anyservice를 지향하는 환경이다. 이러한 유비쿼터스 컴퓨팅 환경에서는 개체간의 인증은 물론 전송되는 정보, 전자결제, 전자상거래 등 다양한 서비스에서 유선 통신 환경에서와 같은 정보 보안 서비스가 이루어져야 한다. 이로인해 차세대 암호화 기술 및 IC 카드 고도 인증기술, 바이오메트릭스 인증기술 또는 DNA 개인 인증기술 등 활발한 연구가 진행되고 있다. 최근, 반도체와 One-chip 개발이 활발해지면서 단말기, 디바이스들은 연산처리 능력이 향상되고, 대용량의 메모리를 탑재하게 되었다. 그러나, 이러한 기술 발달과 함께 제 삼자의 공격방법도 향상되어 사용자 패스워드 혹은 PIN(Personal Identification Number)만을 이용한 개체 인증 방법들은 제 삼자에게 쉽게 노출될 수 있을뿐 아니라, 사용자가 각각 서로 다른 패스워드를 기억해야 되는 어려움이 있다. 이에 본 논문에서는 사용자 고유의 생체인식 정보와 기억하기 쉬운 패스워드를 같이 비밀정보로 사용하여 유비쿼터스 환경에 적합한 양방향 개체 인증 키 분배 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 사용자 생체인식 기술에 대해 알아보고, 3장에서는 본 논문에서 제안하는 키 분배 프로토콜에 대해 기술한다. 4장에서는 제안하는 프로토콜의 안전성을 분석하며, 마지막으로 5장에서는 결론과 향후 연구 계획에 대해 기술한다.

Ⅱ. 생체인식 기술

생체인식 기술은 바이오기술(BT)과 정보기술(IT)의 접목된 기술로 정보보호 시스템의 새로운

기술로 발전하고 있다. 이러한 생체인식 기술에는 얼굴, 지문, 정맥패턴, 홍채, DNA, 서명(필기체) 등 여러 가지가 있으며, 현재 국·내외에서 생체인식 기술 및 인식 시스템에 관한 표준들이 제정되고 있다. 본 장에서는 국·내외 표준협회들을 살펴보고, 생체인식 기술에 대해 알아본다.

1. 생체인식 표준

1.1 국외 표준

미국 표준화 기구 ANSI/X9F4 WG에서는 금융보안 표준 소위원회 중에 Biometrics 기관이 있으며, 1998년 ANSI X9.84 Biometric Information Management and Security표준 개발을 시작하였다. NIST(National Institute of Standard and Technology)에서는 지문데이터의 교환을 위한 표준을 개발하였으며, BioAPIConsortium 민간단체는 생체 인증기술 전분야에 적용 가능한 응용프로그램 인터페이스를 제공하기 위해 1998년 4월 구성하여 BioAPI Specification v1.1 개발하였다. 이외에 다른 표준기구로는 개방형 컴퓨터 표준화 협회 OASIS (Organization for the Advancement of Structured Information Standards) XMLCommon Biometric Format Technical Committee (XCBF) WG이 있다. 유럽 표준화 기구로는 2003년 7월에 European Biometric Forum Biometric Forum이 공식 발족하였으며, 여러 나라의 Btexact, NPL, CESG, Saflink, TUViT, TeleTrustT, KISA 등이 참여하여 유럽의 생체인식기술 중심역할을 담당하며, 생체인식 제품을 개발 보급하는 역할을 한다. 일본에는 전자상거래 응용분야에서의 생체 인증기술에 대한 표준을 제정하는 INSTAC/JSA가 있다. 국제 표준 기구인 ISO/IEC JTC1 Subcommittee 37은 응용 프로그램과 생체인식 시스템과의 상호운용성, 데이터 상호교환등을 위한 일반 화일구조, 생체인식기술 응용프로그램 인터페이스, 생체인식 데이터 상호교환 포맷, 연관된 생체인식 프로파일 기술들에 대한 응용프로그램 평가기준 표준을 개발한다.

1.2 국내 표준

생체인식기술 관련 국내 표준 기구에는 KBA (Korea Biometrics Association), TTA(Telecomm. Technology Association)가 있으며, 국내외 생체인식 기술 및 산업동향 분석 정보, Biometric 데이터의 효율적인 관리를 위해 최소한의 보안 요구사항을 명시한 K-X9.84, 그리고 생체인식 인터페이스 표준규격 K-BioAPI가 있다.

2. 생체인식 기술

생체 정보는 개인이 가지고 있는 고유의 특징을 추출한 것으로, 생체 특징 정보를 이용하여 개인식별, 정보보안 서비스에서의 비밀 값 등에 활용될 수 있다. 생체 정보를 추출하는 기술은 다음과 같다.

2.1 얼굴(Face)정보 기술

사용자의 얼굴을 이용한 인식 기술로 주시각도, 조명 등의 주변 환경이나 얼굴 모양의 다양한 변화에 민감하다는 약점을 가지고 있다. 또한, 사람의 얼굴 모양은 나이에 따라 변화하는 특징을 가지고 있어 상용화에 많은 어려움이 있는 실정이다. 얼굴을 인식하는 방법으로는 얼굴 혈관에서 발생하는 얼굴의 열상을 적외선 카메라로 촬영하는 방식의 특징점 기반 방식과 3차원 얼굴 영상을 이용하는 영상 기반 방식이 있다.

2.2 지문(Fingerprint)정보 기술

지문정보는 인간의 신체 부분 중 가장 오래 전부터 이용되어온 특성으로 신원확인 분야와 범죄수사분야에 사용된다. 지문인식 기술은 금고 및 출입통제시스템의 물리적 접근제어, 범죄자 색출을 위한 분야 등에 적용되어 왔으나, 1990년대에 들어서면서 전자상거래상의 보안 및 인증을 위한 보안시스템으로 활용되고 있다. 지문은 인체의 땀샘이 융기되어 일정한 흐름이 만들어진 것으로, 그 모양이 개개인마다 다르고, 모양이 평생동안 변하지 않고, 손상이 되어도 다시 회복된다는 것이 증명되어 실생활에서 신원확인을 위해 사용되고 있다. 또한, 사용자가 사용하기 쉬운 사용자 인터페이스를 갖는 장점을 가지고 있어 전 세계적으로 인정되는 신뢰성 있는 신원확인 방법이다.

2.3 망막, 홍채정보 기술

생체인식 기술에서 사람의 눈을 이용하여 측정하는 것은 망막, 홍채 두 가지로 나눌 수 있다. 망막과 홍채는 지문과 마찬가지로 평생동안 변하지 않고, 사람마다 다르기 때문에 신원확인을 위해 사용되고 있다. 망막 패턴은 약한 강도의 연필 지름만한 적색 광선이 안구를 투시하여 망막에 있는 모세혈관에 반사된 역광을 측정하여 얻을 수 있다. 따라서 망막 패턴의 성공적인 검색을 위해서는 사용자가 안경을 벗고 검색기에 접안하여야 하며, 접안기의 둥근 원통 내 어두운 부분 중 적색 광선이 방사되는 점에 눈의 초점을 맞추어야 한다. 망막 패턴 검색 기술은 고도의 보안성을 만족

시키지만 사용상의 불편과 두려움을 가지고 있다. 이에 반해 홍채 인식 방법은 홍채가 눈의 표면에 있기 때문에 인식 시스템과 어느 정도 거리를 둔 상태로의 자연스러운 상태에서 영상을 획득하여 이용하므로 망막인식에서의 단점이 해결되어 많은 분야로의 적용이 기대되어지고 있다.

2.4 서명정보 기술

서명(필기체)은 계약 체결 등의 서류에 대한 증빙의 목적으로 이용되기 시작했으며, 법적인 효력을 얻음과 동시에 은행을 중심으로 널리 확산되어 왔다. 서명 시스템은 서명의 물리적 특성을 인식하는 방법과 서명하는 과정, 즉 펜의 움직임, 속도, 압력 등을 동적으로 파악하는 방법으로 나누어진다. 보안 측면에서는 동적인 인식방법이 우수한 것으로 알려져 있다.

Ⅲ. 제안하는 키 분배 프로토콜

제안하는 키 분배 프로토콜은 단말기의 연산 능력과 효율성을 고려하여 타원곡선을 기반으로 한다. 타원곡선 연산과정은 많은 부담을 주는 모듈라 멱승 연산 대신 스칼라 멀티플리케이션을 사용하게 되므로 이산 대수를 사용하는 것보다 빠른 연산이 가능하다. 본 장에서는, 2장에서 살펴본 사용자 개인 생체인식 정보를 추출하여 서버간의 등록과정 및 세션키를 분배하는 타원곡선 기반 키 분배 프로토콜을 기술한다.

1. 파라미터

U : 사용자
S : 서버
A : 공격자
E_1, E_2, Q, T : 중간 값
BIO_X : 개체 X의 생체인식 정보
$Pass_X$: 개체 X의 패스워드 정보
E : $GF(q)$상의 곡선
G : 곡선 위의 기본점
n : G 의 위수
d_X : 개체 X의 임시 랜덤 비밀키
$d_X \in \{2, \ldots, n-1\}$
Q_X : 개체 X의 임시 공개키
$d_X G = Q_X$
SK : 세션키
PE_{P_X} : 개체 X의 공개키로 암호화
PD_{S_X} : 개체 X의 비밀키로 복호화
E_K : 대칭키 K로 암호화
h : 일방향 해쉬 함수
$\|$: 연접
$kdf()$: 키 유도 함수

2. 사용자 등록과정

등록 과정은 사용자를 서버에 등록하는 과정으로 초기에 단 한번만 이루어지며, 서버의 인증서는 OCSP(Online Certificate Status Protocol)을 이용하여 실시간으로 공개키 인증서의 상태 정보를 검증한다.

1) 사용자 U는 자신의 생체정보 BIO_U와 패스워드 $Pass_U$를 선택하여 $TBIO_U$를 생성한 후, 자

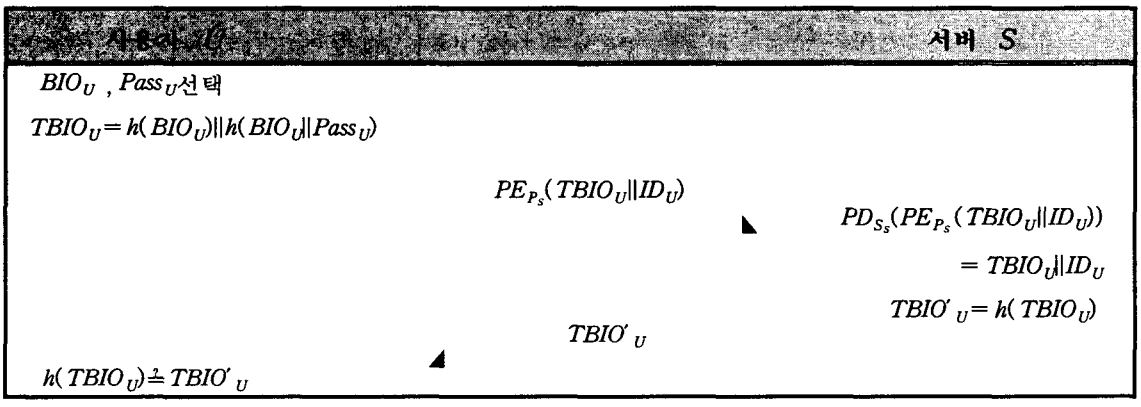

그림 1 : 사용자 등록과정

신의 아이디와 $TBIO_U$를 서버의 공개키로 암호화하여 전송한다.

$$TBIO_U = h(BIO_U) \| h(BIO_U \| Pass_U)$$

$$PE_{P_S}(TBIO_U \| ID_U)$$

2) 서버 S는 전송된 값을 복호화하여 복호된 값을 저장하고 $TBIO'_U$를 생성하여 사용자 U에게 전송한다.

$$PD_{S_S}(PE_{P_S}(TBIO_U \| ID_U))$$

$$TBIO'_U = h(TBIO_U)$$

3) 사용자 U는 자신이 가지고 있는 $TBIO_U$를 해쉬하여 $TBIO'_U$와 동일한지 비교·확인한다.

$$h(TBIO_U) \stackrel{?}{=} TBIO'_U$$

3. 키 분배 과정

제안한 프로토콜은 타원곡선의 이산대수 문제와 EC-DH(Diffie-Hellman)문제에 안전성을 둔 프로토콜이다.

1) 사용자 U는 랜덤 비밀키 d_U를 선택하고, 공개키 Q_U를 생성한다. Q를 생성하기 위하여 E_1을 계산하고, Q, Q_U, ID_U를 $h(BIO_U)$로 암호화하여 전송서버에게 전송해준다.

$$Q_U = d_U \cdot G = (x_U, y_U)$$

$$E_1 = h(x_U \| y_U)$$

$$Q = h(h(BIO_U) \| E_1)$$

$$E_{h(BIO_U)}(Q, Q_U, ID_U), \quad ID_U$$

2) 서버 S는 전송된 Q_U값을 이용하여 E'_1를 계산하고, $h(h(BIO_U) \| E'_1)$값을 생성하여 Q와 비교·확인한다. 동일하다면, 사용자 ID_U임을 확신한다.

$$Q \stackrel{?}{=} h(h(BIO_U) \| E'_1)$$

다시 서버 S는 비밀키 d_S를 선택하고, 공개키 Q_S를 생성한다. T를 생성하기 위하여 E_2을 계산하고, 세션키 SK를 생성한 후, T, Q_S, $h(SK)$를 $h(BIO_U \| Pass_U)$로 암호화하여

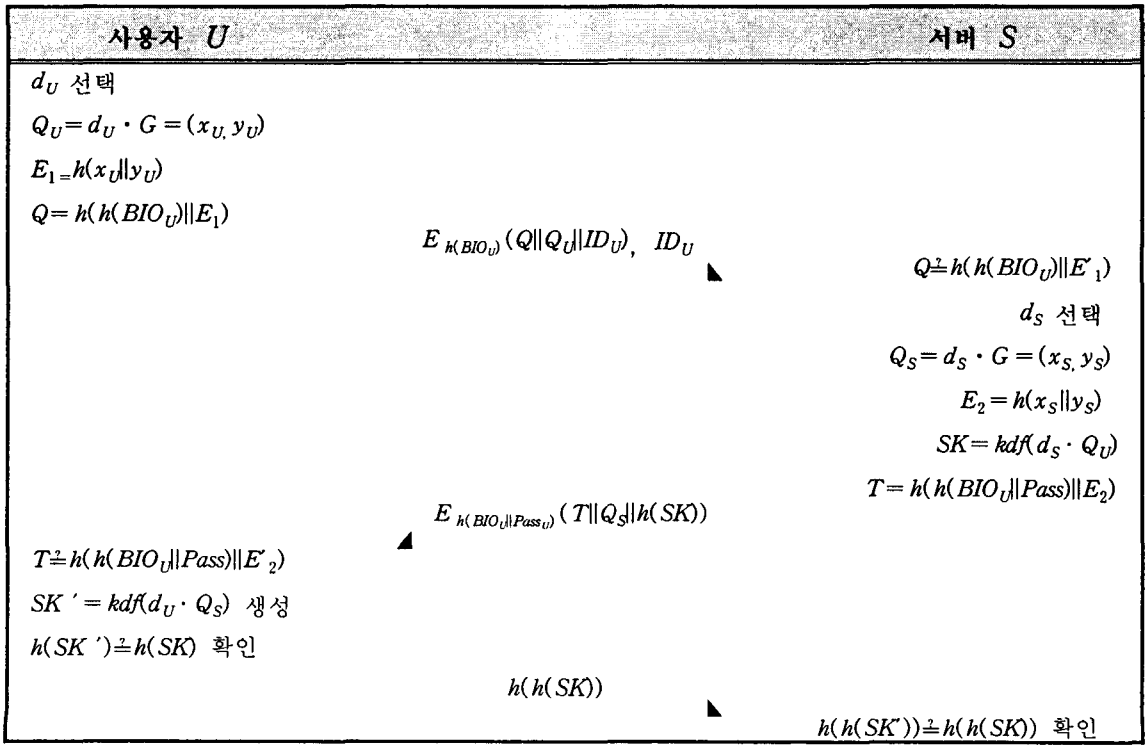

그림 2 : 타원곡선기반 키 분배 프로토콜

전송한다.

$$E_{h(BIO_U \| Pass_U)}(T \| Q_S \| h(SK))$$

3) 사용자 U는 복호된 T값과 자신이 생성한 $h(h(BIO_U \| Pass) \| E'_2)$와 비교·확인한다.

$$T \stackrel{?}{=} h(h(BIO_U \| Pass) \| E'_2)$$

다시 사용자 U는 세션키 SK'를 생성한 후, 전송된 $h(SK)$값과 비교·확인한다. 정당하다면 다시 $h(h(SK))$를 서버 S에게 전송한다.

$$h(h(SK))$$

4) 서버 S는 전송된 값 $h(h(SK))$를 비교·확인한다.

$$h(h(SK')) \stackrel{?}{=} h(h(SK))$$

4. 제안하는 프로토콜의 특징

본 절에서는 통신 횟수, 개체 인증, 키 인증, 키 확인, 키 구축, key freshness에 대해 분석한다.

표 1: 키 분배 프로토콜의 특징

	키 분배 프로토콜	
통신 횟수	3회	
개체 인증	양방향	
키 인증	U	명시적 키 인증
	S	명시적 키 인증
키 확인	양방향	
키 구축	키 동의	
Key freshness	양방향	

본 프로토콜의 키 분배 시 통신 횟수는 총 3회이며, 사용자 U와 서버 S는 모두에게 양방향 개체 인증을 제공한다. 사용자 U는 서버 S가 비밀정보 $h(BIO_U)$를 이용하여 암호화 한 암호문을 복호함으로써 서버 S를 인증할 수 있으며, 마찬가지로 서버 S는 사용자가 공유하고 있는 비밀정보로 암호화 한 암호문을 복호함으로써 사용자 U를 인증할 수 있다. 사용자 U와 서버 S는 비밀정보를 알고 있는 객체만이 세션키를 계산할 수 있기 때문에 양방향 키 확인도 제공한다. 세션키를 생성하는 과정에서 사용자 U와 서버 S가 선택한 각각 다른 임시 랜덤 비밀키 d_U, d_S를 사용하여 계산하므로 키 구축 형태는 키 동의 방식이며, key freshness을 보장한다. 또한, 프로토콜 수행 중 사용자 U와 서버 S가 각각 생성한 세션키의 해쉬 값을 비교·확인하는 과정에서 명시적 키 인증을 한다. 표 1은 제안한 프로토콜의 특징을 정리한 것이다.

Ⅳ. 제안한 프로토콜의 안전성 분석

1. 수동적 공격자에 대한 안전성

본 논문에서 제안하고 있는 키 분배 프로토콜의 안정성은 타원곡선을 기반으로 하므로 수동적 공격자가 공개 정보와 전송 정보를 이용하여 세션키를 구하는 어려움은 타원곡선의 이산 대수 문제의 어려움과 EC-DH문제를 푸는 어려움과 동일하다.

2. 능동적 공격자에 대한 안전성

2.1 Forward Secrecy에 대한 안전성

사용자 U의 비밀정보인 BIO_U와 $Pass_U$가 노출되었다 하더라도, 공격자 A는 과거의 세션키 생성에 사용된 전송 정보로부터 세션키에 사용한 랜덤 비밀 키 d_U, d_S를 계산하는 것은 EC-DH 문제를 푸는 어려움과 동일하게 때문에 과거의 세션키를 생성해 낼 수 없다. 또한, 서버 S의 비밀정보가 노출된 경우에도 사용자 U의 비밀정보가 노출된 경우와 마찬가지로 과거에 사용된 비밀 랜덤수 d_U, d_S를 계산해 낼 수 없기 때문에 과거의 세션키를 계산해 낼 수 없다.(Half Forward Secrecy)

공격자 A는 사용자 U와 서버 S의 비밀정보가 모두 노출되었다 하더라도 과거의 랜덤수 d_U, d_S를 계산할 수 없다.(Full Forward Secrecy)

2.2 Man-in-the-middle attack에 대한 안전성

공격자 A가 사용자 U와 서버 S의 통신 과정에 개입하여 서버에게는 정당한 사용자로, 사용자 U에게는 정당한 사용자로 위장하는 공격이다. 사용자 A가 자신의 비밀정보인 $h(BIO_U)$로 암호화하여 전송하기 때문에 $h(BIO_U)$를 알고있는 서버 S만이 복호화를 할 수 있으며, 서버 S가 사용자 U에게 비밀전송을 할 경우에도 상호 비밀정보인 $h(BIO_U \| Pass_U)$로 암호화하여 전송하기 때문에 비밀정보 모르는 공격자는 중간에 개입하여 메시지를 변조할 수 없기 때문에 안전하다.

2.3 Active Impersonation에 대한 안전성

공격자 A가 세션을 시작한 경우, 공격자 A가 사용자 U로 위장하여 서버 S와 세션키를 설정하는 것은 수동적 공격자의 어려움과 동일하다. 공격자 A가 서버 S와 세션을 시작하는 경우, 정당한 사용자 U의 비밀정보인 BIO_U의 해쉬 값을 알지 못하기 때문에 정당한 $E_{h(BIO_U)}(Q, Q_U, ID_U)$를 생성할 수 없으므로 위장이 불가능하다. 공격자 A가 서버 S로 위장하였을 경우, 사용자 U로 위장한 경우와 마찬가지로 비밀정보인 BIO_U, $Pass_U$의 해쉬 값인 $h(BIO_U||Pass_U)$를 모르기 때문에 정당한 암호문 $E_{h(BIO_U||Pass_U)}(T||Q_S||h(SK))$을 생성할 수 없으므로 위장이 불가능하다.

2.4 Known Key Security에 대한 안전성

세션키를 설정하기 위해서 매 세션마다 서버 S가 선택한 임시 랜덤 비밀키 값 d_S와 사용자 U가 선택한 임시 랜덤 비밀키 값 d_U를 사용하므로 이전 세션의 전송 정보와 세션키가 노출되었다 하더라도 현재의 세션키를 구하는데 아무런 도움을 주지 못한다.

V. 결론

본 논문에서는 사용자의 생체 정보와 기억할 수 있는 패스워드를 비밀 정보로 사용한 양방향 개체 인증 키 분배 프로토콜을 제안하였다. 제안하는 키 분배 프로토콜은 3회의 통신 횟수, 양방향 개체 인증과 양방향 키확인, 묵시적 키 인증을 제공하며, 키 동의 방식의 key freshness를 보장한다. 본 프로토콜에서는 단말기의 연산 능력과 효율성을 고려하여 타원곡선방식과 해쉬 함수를 사용하였으며, 프로토콜의 안전성은 기본적으로 타원곡선 방식의 이산대수문제와 EC-DH문제에 안전성을 둔 프로토콜이다.

제안한 키 분배 프로토콜에서는 생체 정보 추출 과정과 생체 정보를 해쉬 함수 사용, 그리고 다른 키 분배 프로토콜과의 안전성을 비교·분석에 관한 추후 연구가 필요하다. 또한, 유비쿼터스 컴퓨팅 환경에서는 개체와 단말기간 또는 단말기와 단말기간에 실시간으로 개체 인증 및 통신이 이루어질 것이다. 본 논문에서 제안하는 프로토콜에서의 등록과정 시 사용한 PKI 기술은 많은 단말기의 인증서 발급과정과 인증서 검증과정에서 과부하가 생길 수 있다. 이에 차세대 네트워크(유비쿼터스 환경)에 적용하기 위해 안전하고 연산 속도를 고려한 차세대 인증기술, 생체 정보를 이용한 고도의 인증 기술에 관한 연구가 필요하다.

참고문헌

[1] ANSI X9.42, "Agreement of sysmmetric Key on Using Diffie-Hellman Cryptography",2001

[2] ANSI X9.63 "Public Key Cryptography for the finanacial services industry : Keyagreement and key transport using elliptic curve cryptography", 2001

[3] W. Diffie, P.C. Oorschot, M.J. Wiener,"Authentication and Authenticated Key Exchange ", Designs, Codes and Cryptography, 2, pp 107-125, 1992.

[4] S.J. Kim, M. Mambo et al, "On the security of the Okamoto-Tanaka ID-Based KeyExchange scheme against Active attacks", IEICE Trans, pp 231-238, Jan. 2001.

[5] M. Mambo and H. Shizuya, "A note on the complexity of breaking Okamoto-Tanaka ID based key exchange scheme", IEICE Trans. Fundamentals, vol.E82-A, no.1, pp 77-80, Jan, 1999.

[6] 김병만, 이경, 박인용, 김시관, "유비쿼터스 컴퓨팅과 사용자 모델링", 정보처리학회지, pp 132-146, 7, 2003

[7] Ken Sakamura, Noboru Koshizuka, "Technologies for Computing Everywhere Enviroments", 정보처리학회지, pp 11-22, 7, 2003

[8] 김재성, "생체인식 기술 소개" 한국정보보호진흥원, 2001.