韓國 컴퓨터情報學會 論文誌
第9卷 第2號, 2004. 6.

2004-9-2-1-6

외부 이동단말의 접근제어를 위한 IP 프로토콜 설계 및 성능 개선에 관한 연구

박 대 우*

A Study on the Design and the Performance Improvement of IP Access Control Protocol for External Mobile terminal

Daewoo-Park*

요 약

유비쿼터스 시대에 접근제어 프로토콜은 외부 이동단말이 내부 정보서버로 접속 시에 접근제어를 위한 검증을 하여야 한다. 본 논문에서 제안하는 외부 이동단말을 위한 IP 접근제어 프로토콜은 이동단말기에서 서명의 암호화 연산 시 연산시간의 효율성을 고려한다. 신뢰성 있는 통신기관에서 발급해준 개인 식별정보를 공개키로 사용하도록 하고, 서명 암호화 생성과 검증에 사용되는 암호화 알고리즘은 ECDSA에서 정의한 변수를 사용하며, 타원 곡선상의 키값은 160비트 이상을 사용한다. 또한 접근제어는 IP 계층에서 실시하며 IPv6의 프레임 구조를 갖도록 설계한다. 외부 이동단말의 접근제어를 위한 암호화 인증과 검증의 과정에서 프로토콜의 보안성을 강화하였고, 기존의 프로토콜들에 연산시간에 비해 4배 이상의 성능향상이 이루어졌음을 증명하였다.

Abstract

Access control protocol have verified security of external mobile terminal that access to inner information sever at Ubiquitous ages. In this paper, I would design for IP Access Control Protocol of considering operation time when make cipher digital signature. Public key are used Individual identification number that issued from certify communication company, and cipher algorithm are used ECDSA definition factor for generation and verification of digital signature and it used Elliptic Curve with over 160 bit Key. Also, Access control operate on IP level that designed IPv6 frame architecture. I would conclude that IP Access Control Protocol have verified security and improved performance in operation time more 4 times than before protocols when through the communication of use cipher digital signature for authentication and verification.

▸ Keyword : access control protocol, information security, IPv6, mobile terminal.

* 숭실대학교 컴퓨터학과

Ⅰ. 서 론

이동통신과 부가 서비스가 활성화 되면서 유선과 무선 네트워크가 통합되고, 홈 네트워크, 인체 네트워크, 마이크로 네트워크 등의 연계를 통한 유비쿼터스(Ubiquitous) 시대가 형성되고 있다. 특히 이동통신은 시간과 공간의 제약을 극복하면서 이동(상)거래(mobile-commerce), 인터넷 전자상거래 등의 무선 인터넷과 VPN(Virtual Private Network)[1]등을 이용하고 있다. 특히 IPv6 (Internet Protocol version 6)[2]로 인하여 이동단말기 한대에 고유한 주소를 갖게 되면서, 금융, 물류, 경영 정보 등을 통해 정보교환 과 무선 업무영역이 더욱 확대하고 있다.

2004년 4월의 KrCERT에 접수된 해킹사고 신고[3]는 총 2,444건으로 이중 웜과 스팸릴레이가 101%이상의 증가를 보이고 있다. 따라서 정보보호를 위한 이동단말 사용자의 확인 및 본인 행위에 대한 부인방지[4]을 위해 접근에 대한 인증과 정보보안이 필요하며, 특히 단말기 기능과 업무 확대에 따른 외부 이동단말을 위한 내부 네트워크에서의 접근제어 프로토콜이 요구 되고 있다.

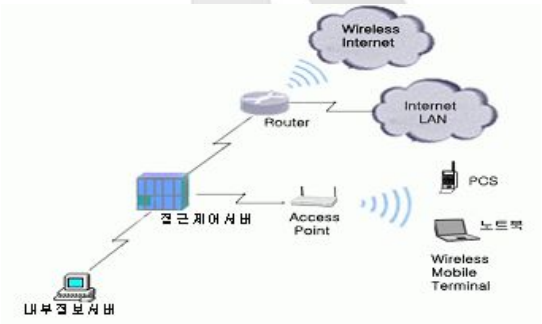


그림 1. 이동 단말기의 접근제어
Fig. 1 Access Control of Mobile Terminal

이러한 요구를 해결하기 위해 본 논문에서 제안한 프로토콜은 외부 이동단말 사용자가 <그림 1>과 같이 내부의 중요 정보서버로 접속 시에 내부 네트워크에 확인 인증을 받기 위한 접근제어 프로토콜이다. 접근제어를 위한 인증을 받을 시 이동단말기에서 전자서명의 생성과 검증 시에 연산시간의 개선을 목표로 한다. 이를 위해 신뢰성 있는 통신기관에서 본인에게 발급해준 개인 식별정보를 그대로 공개키로 사용하도록 하는 방법을 도입한다. 따라서 외부 이동단말에서 이러한 과정이 효율적으로 수행되도록 IPv6에서 적용되는 프레임을 설계하고, 보안성과 안전성을 수식을 통해 검증한다. 그리고 프로토콜에 사용되는 서명 암호화 생성과 검증을 위한 연산시간의 개선이 이루어 졌음을 증명 하고자한다.

Ⅱ. 프로토콜의 관련 연구

외부 이동단말의 접근제어에서 필요한 것은 인증이다. 인증 시에 요구되는 확인과정은 전자서명으로 할 수 있다. 전자서명을 통한 인증은 사용 단말기와 사용자의 신원을 확인하는 것으로 공개키(public Key)와 타임스탬프를 이용한 인증기법[5]들이 있다. 이때 전자서명의 암호화 알고리즘은 서명자와 검증자가 보안성을 유지하면서 서명의 진위를 확인하여 접근통제를 할 수 있게 한다.

지금까지의 제안되었던 프로토콜에서 전자서명알고리즘들은 대부분이 PKI (Public Key Infra- structure) 방식이다. 이는 키쌍을 검증하는 Diffie -Hellman 방식[6]의 지수승 연산인 $(y_a g^r)^s \mod p$로 구현 하였으며, 암호화 알고리즘도 RSA(Rivest-Shamir-Adleman)나 3DES (Data En cryption Standard)[7] 등을 이용하였다. 최근 무선이 발달 하면서 우리나라도 KCDSA(Korea Certicate-Base Digital Signature Algorithm)[8]를 표준으로 하고, 미국에서도 무선 프로토콜을 지원하는 ECDSA[9]를 표준으로 하는 암호화 알고리즘을 사용하고 있다.

프로토콜의 연산시간은 메시지를 암호화할 때의 변수의 생성과 지수승 연산 시간이 많이 걸린다. 따라서 검증자와 세션키의 생성 시에만 스칼라 곱셈을 사용하도록 하고, 서명 생성 시에 XOR연산을 사용[10]하면 연산의 시간을 절약할 수 있어 통신시간의 효율성을 개선 할 수 있다.

III. IP 접근제어 프로토콜의 설계

1. IP 접근제어 프로토콜의 설계

제안한 프로토콜은 내부 네트워크의 인증을 받지 않은 외부 이동단말이 내부 네트워크의 중요 정보서버에 접속을 요청 할 시 접근제어를 위해 사용 된다.

외부의 이동단말기와 사용자는 통신기관에 처음 가입 시 신뢰성을 증명하는 신분증을 제출하여 확인 받거나, 단말기 대여 시에 본인의 신분을 확인 후 통신기관으로부터 직접 발급받은 통신키를 공유한다. 이 통신키를 검증키로 이용하여서 내부 정보서버로의 접속을 제어한다. 검증자는 통신기관에서 받은 검증키와 접속요청을 한 이동단말기의 키와 비교를 통해 접속 신청자의 정당성을 검증한다. 이때 이동단말기 사용자와 접근제어를 위한 검증에서 통신기관은 키 전달센터의 역할을 하며, 서명의 생성과 검증에 필요한 인자를 중계한다.

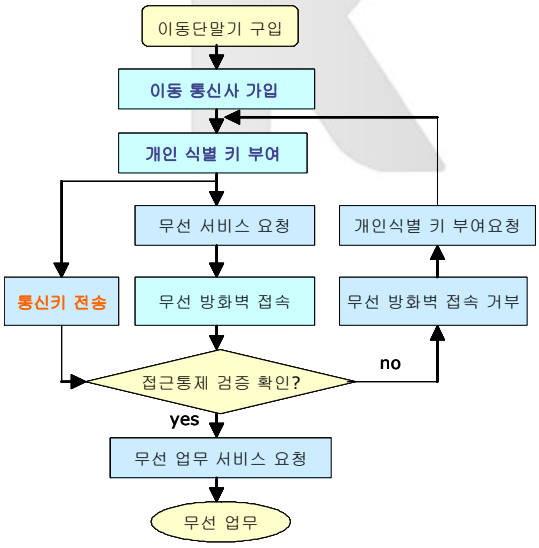


그림 2. 접근제어 프로토콜의 흐름도
Fig. 2 Flow of Access Control Protocol

접근제어 프로토콜은 이동 단말기에서 서명의 생성과 암호화 연산 시의 연산시간 효율성을 고려하여, 통신기관에서 본인에게 발급해준 개인 식별 정보를 공개키로 사용하도록 <그림 2>와 같이 설계한다.

제안한 프로토콜의 서명 암호화생성과 검증에 사용되는 암호화 알고리즘은 ECDSA에서 정의 한 변수를 사용하며, 키값은 160비트 이상을 사용한다. 접근제어 프로토콜의 제어는 IP 계층에서 실시한다.

2. IP 접근제어 프로토콜의 프로세스

제안된 IP 접근제어 프로토콜의 프로세스는 <그림 3>과 같다. 단말기에서 접속요청을 하면 접근제어 서버는 단말기가 내부 인증을 받지 않는 단말기임을 확인하고 신뢰성 있는 통신기관에 단말기에 대한 통신키를 요청하여 이 키를 전달 받아서 이동 단말기의 인증을 확인한 후 내부 업무 서버에 접속을 허용한다.

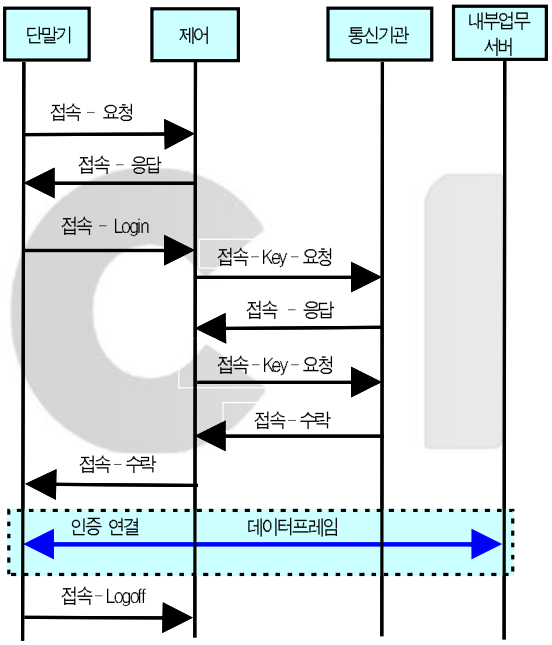


그림 3. 접근제어 프로토콜의 프로세스
Fig. 3 Process of Access Control Protocol

3. IP 접근제어 프로토콜의 전개

IP 접근제어 프로토콜의 알고리즘에 따라서 이루어질 이동 단말기의 접근제어 프로토콜 메시지 검증 방법에 관한 내용 전개는 아래와 같다.

3-1 접근제어 프로토콜 파라미터

- E : $GF(q)$ 선상의 곡선 암호화 알고리즘
- G : 곡선 위의 기본 점
- n : G의 위수 ($nG=0$)
- T : 타임스탬프
- MT_a : 이동단말기의 비밀키
  $MT_a \in \{2,..., n-1\}$
- MT_A : 이동단말기의 공개키
  $MT_A = MT_a\ G$
- MT_b : 접근제어의 비밀키
  $MT_b \in \{2,...n-1\}$
- MT_B : 접근제어의 공개키
  $MT_B = G\ MT_b$
- MB : 신뢰성 있는 통신기관
- MT_{KA} : 통신기관의 이동단말기 가입자 A의 식별키
- MT_{KB} : 통신기관과 연결된 접근제어 B의 식별키
- x : $x \in \{2,..., n-1\}$에서 랜덤 수
- $Hash()$: 일 방향 해쉬 함수
- M : 메시지

3-2 접근제어 프로토콜에서 통신키 공유

신뢰성 있는 통신기관 MB는 이동단말기의 소유자 A가 처음 개통하거나 임대를 요청 할 때, 본인의 신분확인 후 가입자에게 이동 단말기에 대한 식별키 MT_{KA}를 발행하여 안전하게 공유한다. MB는 접근제어의 검증자 B가 처음 개통할 때, 신분 확인 후 접근제어 식별키 MT_{KB}를 발행하여 키를 공유 한다. MT_{KA}, MT_{KB} 키는 A와 B의 신원정보와 함께 안전하게 보관한다.

3-3 접근제어 프로토콜 이동단말기의 서명 생성

이동단말기에서 메시지에 대한 서명 생성과정은 아래와 같다.

$$\Pi = Hash(xG) \quad \text{(식 2.1)}$$

$$c = E_{x_1}(T\ M) \quad \text{(식 2.2)}$$

$$(x_1, y_1) = x\ MT_{KB} \quad \text{(식 2.3)}$$

$$r = c\ XOR\ \Pi \quad \text{(식 2.4)}$$

$$s = \frac{rx - r - 1}{MT_{KA} + 1} \mod n \quad \text{(식 2.5)}$$

(식 2.1)에서 임의의 수 x를 이용하여 해쉬값을 생성한다. (식 2.2)에서 원문 메시지에 타임스탬프를 찍고 암호화하여 검증자 C값을 생성한다. (식 2.3)에서 접근제어 검증자 공개키 MT_B를 이용하여 값을 생성한다. 그리고 이동단말기의 서명을 검증 하는 접근제어에게 검증값 r을 전달하기 위해, 통신기관인 MB가 공유하고 있는 MT_{KB}로 r를 암호화하여 전송한다. MB는 보관중인 신원정보와 함께 이 값을 비교하여 값이 같으면, 이동단말기 A를 인증하고, 정당한 단말기임을 확인하여, A의 신원정보와 함께 안전하게 보관한다.

3-4 접근제어 프로토콜의 서명 검증

접속 신청을 한 이동단말기를 위해 전송한 정보를 받은 접근제어는 신뢰성있는 통신기관 MB에게 이동단말기가 생성한 검증 값 r의 전송을 요청한다. 통신기관은 접근제어와 안전하게 공유중인 MT_{KB}로 r을 암호화하여, 접근제어에 전송한다. 접근제어는 전송받은 정보를 복호화하여 검증값 r을 이용하여 복원하면서 메시지의 정당성을 검증한다. 이 때 이동단말기의 서명을 검증하는 과정은 아래와 같다.

$$\Pi' = hash(P) \quad \text{(식 2.6)}$$

$$P = \frac{1 + r + s}{r} G + \frac{s}{r} MT_A = xG \quad \text{(식 2.7)}$$

(식 2.6)과 같이 서명을 검증하기 위해 접근제어에서 만들어진 값으로 두 번의 스칼라 곱셈이 사용되며, (식 2.7)에서 전달받은 검증값 r을 복원한다. 이때 전송된 서명 메시지를 검증하기 위해접근제어에서 이동단말기로부터 받은 메시지를 검증하기위해 c XOR Π를 실행한다. 그 결과로 추출된 r'값이 이동단말기에서 전송받은 원래의 r값과 같으면($r = r'$) 이 메시지는 무결성이 검증된 메시지이므로 접근제어에서 접근을 허용한다. 하지만 단말기 원래의 r값과 비교하여 다르거나($r \neq r'$), 타임스탬프 시간이 다르거나, 타임스탬프의 유효기한이 지난 것이면 폐기시킴으로써 이동 단말기의 접근을 차단한다. 따라서 제안된 방법의 접근제어에서 원래의 메시지를 복원하는 전체의 과정이 필요 없이 접근제어를 할 수 있도록 서명메시지를 검증하는 프로토콜을 설계 하였다. 이 방법은 C. Gamage가 서명된 메시지로 접근제어를 할 때 수신자의 비밀키 없이 원문의 내용을 노출시키지 않는 상태에서 알고리즘만으로 서명의 정당성을 검증할 수 있는 방식을 제안[11] 한 것을 응용한 것이다.

4. 접근제어 IPv6 프로토콜의 프레임 설계

최근 시험 가동되고 있는 IPv6 환경을 위해 본 논문에서 IP 접근제어 프로토콜의 프레임을 IPv6 환경에서 <그림 4>와 같이 설계한다. 인증데이터 32비트 중에 위의 10비트를 사용하고 나머지 비트는 패딩으로 처리하여 32비트를 맞춘다. 이는 다른 보안 시스템을 작동할 시 프로토콜의 변경이나 설정에 따라서 재설계를 할 수 있도록 한 것이다.

그림 4. 접근제어 프로토콜의 IPv6 프레임 구조
Fig. 4 Frame structure for IPv6 of Access Control Protocol

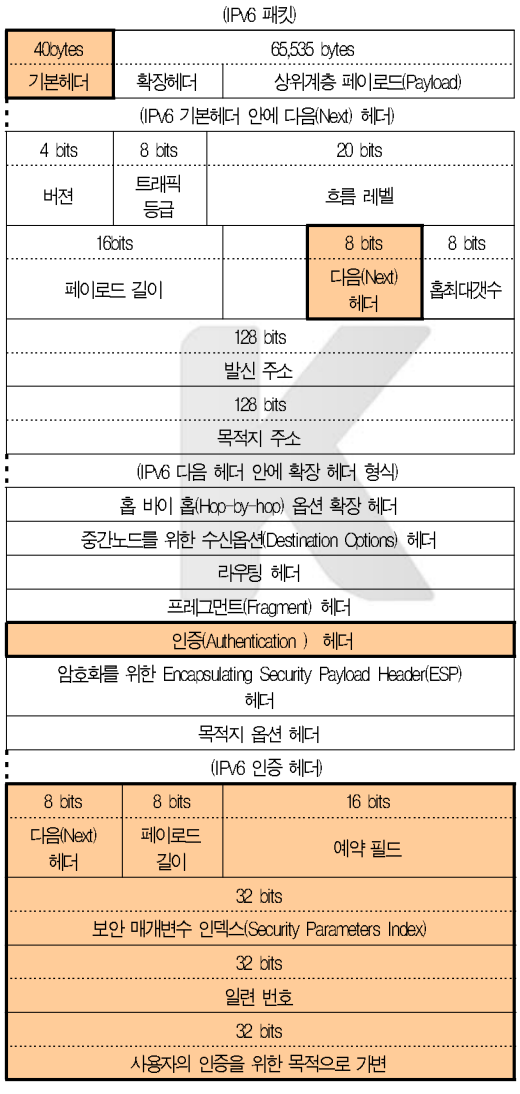


표 1. 접근제어 프로토콜의 IPv6 프레임 필드 설계
Table. 1 IPv6 Frame fielld of Access Control Protocol

구분	인증 필드형태	인증 필드값	설계 기능 내용
인증 필드	접근 제어용 4비트	000001	이동단말기의 사용 검증 요청
		000010	이동단말기의 검증 응답 확인
		000011	이동단말기의 검증 확인
		000100	이동단말기의 접근제어에 접근 거부
		000101	이동단말기의 접근제어에 접근 허용
		010001	통신기관에 통신키 요청
		010010	통신기관에 통신키 수신 확인
		010011	통신기관에 통신키 검증 확인
		010100	통신기관에 통신키 검증 실패

IPv6 환경에서 <표 1>처럼 40바이트의 기본 헤더 안에 8비트의 다음(Next) 헤더가 있는데 이 중에서 인증 헤더를 사용한다.

이 인증헤더는 IP 데이터 그램에 대한 사용자의 인증을 위한 목적으로 인증데이터는 길이가 지정되어 있지 않으므로 일단 앞에 4개 비트를 할당하여, 그 중 접근지점용은 '0001', 접근제어용은 '0010', 원거리통신 용은 '0011'으로 구분해서 사용하고 나머지 6개 비트로 보안 인증을 위한 내용을 설계한다. 페이로드 길이는 10비트로 사용을 명시해 준다.

Ⅳ. IP 접근제어 프로토콜의 보안 검증

제안된 IP 접근제어 프로토콜은 외부접속 이동단말에 대한 접근제어 서버에서 서명검증을 할 때 보안검증은 서명 생성자의 비밀키인 MT_a 로 서명을 생성하고 난수인 x 를 사용하여, 비밀키를 모르거나 재사용을 통한 위조를 할 수 없다.

통신기관에서 접근제어에 대한 공개키를 이용하여 서명을 암호화 하고 전송하기 때문에 안전한 서명 검증을 통해 접근제어를 할 수 있다. 또한 신뢰성있는 인증확인을 통해 외부이용자라 하더라도 접근제어의 공개키 MT_B 를 이용하여 키값을 검증 할 수 있어, 접근제어를 확실 하게 할 수 있다. 서명자 인증에서는 서명자의 공개키 MT_A를 이용하

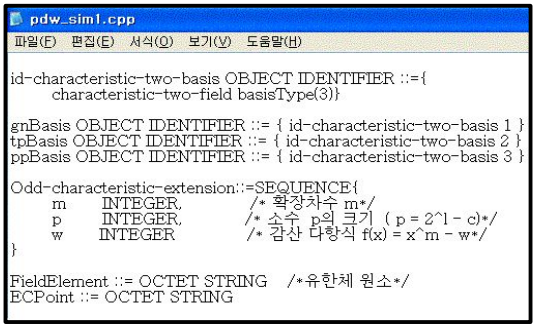
여 서명자를 검증할 수 있으며, 또한 서명 생성자의 비밀키에 타임스탬프를 이용했기 때문에 접속 및 서비스 제공시간에 대해 감사기록과 타임스탬프 T와의 비교를 통해 부인방지를 할 수 있다.

인증과 검증과정에서도 원래의 메시지를 서명 검증자와 서명 생성자만이 알 수 있는 세션키로 암호화하기 때문에 메시지의 무결성을 보장할 수 있으며, 세션키로 암호화하기 때문에 세션키를 알지 못하는 다른 사람은 메시지의 내용을 알 수 없으므로 기밀성을 보장할 수 있다.

V. IP 접근제어 프로토콜의 성능비교

1. 접근제어 프로토콜의 비교분석

본 논문에서는 제안된 프로토콜이 무선 환경에서 외부접속 이동 단말기의 제약성을 극복하고, 접근제어 서버에서의 접근제어에 사용되는 프로토콜의 서명의 생성과 검증 시에 필요한 연산시간 개선에 초점을 맞추고, 한국정보통신기술협회의 실험규격[12]에 맞추어 통신실험실에 실험 환경을 구축 하였다. 실험내용은 접근제어를 위해 서명의 생성과 검증 시 필요한 타원곡선 암호화를 이용한 변수의 생성 및 공개키를 통한 서명생성 및 검증이다. 타원곡선의 암호화 알고리즘의 적용 방법 및 변수에 대한 규격 사용은 EC-KCDSA[13]와 ECDSA의 연방표준인 FIPS 186-2[14]의 규격에 의한 변수설정 방법을 따르고, 제안한 프로토콜의 알고리즘을 적용시켜 성능 분석에 사용하였다.


pdw_sim1.cpp

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
id-characteristic-two-basis OBJECT IDENTIFIER ::={
        characteristic-two-field basisType(3)}

gnBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 1 }
tpBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 2 }
ppBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 3 }

Odd-characteristic-extension::=SEQUENCE{
        m       INTEGER,        /* 확장차수 m*/
        p       INTEGER,        /* 소수 p의 크기 ( p = 2^l - c)*/
        w       INTEGER         /* 감산 다항식 f(x) = x^m - w*/
}

FieldElement ::= OCTET STRING   /*유한체 원소*/
ECPoint ::= OCTET STRING
```

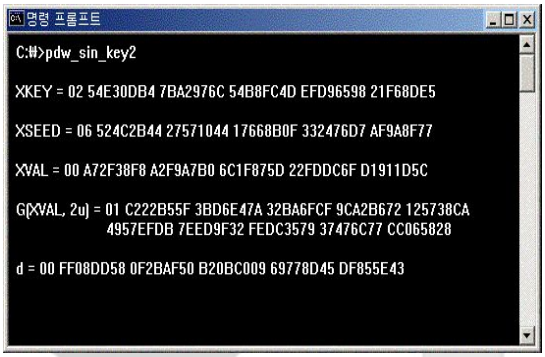
그림 5. 프로토콜 성능 측정 프로그램
Fig. 5 Performance counting program of protocol

<그림 5>의 성능 측정 프로그램을 통해 측정방법은 각각의 정해진 기준에 따라서 100회의 값을 측정을 하고 이 값을 평균하여 5회 측정값으로 하고 이를 다시 평균하여 값을 산출 하였다. 실험기기는 외부 이동단말기와 내부 이동단말기 그리고 접속지점과 접속 포인트에 연결되어 있는 접근제어 서버로 구성하였다.

실험기기의 사양은 다음과 같다.

- 접근제어 서버
  Pentium III, 1CPU(1GHz), Windows 2000,
- 외부 네트워크의 이동단말기
  SA110, 1CPU(233MHz), 16비트 Linux,
- 내부 네트워크의 이동단말기
  Power PC, 1CPU(333MHz), 16비트 Linux.

성능 측정단위는 프로토콜의 서명의 변수설정 및 생성 그리고 검증과정은 밀리(millis) 초인 $1/10^{-3}$초 단위로 측정을 하였고, 표시는 밀리 초인 "ms" 로 하였다.


명령 프롬프트

```
C:#>pdw_sin_key2

XKEY = 02 54E30DB4 7BA2976C 54B8FC4D EFD96598 21F68DE5

XSEED = 06 524C2B44 27571044 17668B0F 332476D7 AF9A8F77

XVAL = 00 A72F38F8 A2F9A7B0 6C1F875D 22FDDC6F D1911D5C

G(XVAL, 2u) = 01 C222B55F 3BD6E47A 32BA6FCF 9CA2B672 125738CA
              4957EFDB 7EED9F32 FEDC3579 37476C77 CC065828

d = 00 FF08DD58 0F2BAF50 B20BC009 69778D45 DF855E43
```

그림 6. 생성된 전자서명
Fig. 6 the generation of digital signature

<그림 6>은 실험 중에 생성된 전자서명으로 접근제어 프로토콜의 인증과 검증에 사용된다.

사용한 알고리즘은 본 논문에서 제안하는 IP 접근제어 프로토콜의 암호화 알고리즘으로 160비트 키 값을 갖는다. 비교 대상은 현재 유선에서 일반적으로 사용되고 있는 RSA 암호화 알고리즘과 함께, 무선에서 우리나라 표준에서 채택하고 있는 KCDSA 암호화 알고리즘을 채택한 실험값이다. 이 두 기준의 값은 한국정보통신기술협회에서 실험한 결과를 인용하여 비교 기준 값으로 채택 하였다.

실험값의 비교 기준은 사용자 인증 프로토콜에 전자서명의 필수과정인 변수의 생성, 키쌍 생성, 공개키 검증, 전자서명생성, 전자 서명검증에 걸리는 연산시간을 측정하였다.

비교 분석 대상에서 접근제어서버와 외부 네트워크 이동

단말기에서의 연산시간을 비교하여, 이들의 값의 차이를 비교 하였으며, 이 차이를 연산시간 수치로 나타내고, 이를 쉽게 확인하기 위해 비교 값을 분석 그래프를 통해 나타냈다. 그리고 성능개선에 나타나는 값을 제안한 IP 접근제어 프로토콜과 기존의 프로토콜에서 사용되는 값을 비교하여 그 차이를 %로 표시하여 본 논문에서 주장하는 연산시간의 성능개선을 확인한다.

표 2. 이동단말의 접근제어 시간 (단위 : ms)
Table. 2 Access Control Time of Mobile Terminal

프로토콜 / 환경	접근제어 RSA	접근제어 KCDSA	제안된 프로토콜
변수 및 키 생성	1396.2	538.7	17.1
공개키 검증 및 서명	17.2	17.3	3.2
서명 검증	0.9	9.3	4.6

제안한 IP 접근제어 프로토콜의 타원곡선 알고리즘을 기반으로 한 연산시간 성능실험 결과 값을 <표 2>에 나타내었다, 연산시간 결과에 나타난 값에서 제안한 IP 접근제어 프로토콜의 타원곡선 알고리즘의 서명을 위한 변수 및 키 생성에서 8,065% 개선되었고, KCDSA에 비해 3,050% 개선되었다. 또한 공개키 검증 및 서명 연산시간도 RSA에 비해 438% 개선되었고, KCDSA에 비해 441% 개선되었다. 그리고 서명의 검증에 소요되는 연산시간에서는 RSA에 비해 -80%로 증가하였고, KCDSA에 비해서는 102% 가 개선되었다.

따라서 비교대상에서 상대적으로 연산 시간이 많이 소요되는 부분에서 제안한 IP 접근제어 프로토콜의 연산시간이 감소하여, 기존의 프로토콜에 비해 연산시간 감소로 인한 통신 속도의 성능개선이 이루어 졌음을 확인 하였다.

이러한 연산시간 감소로 인한 성능 개선의 효과를 비교 그래프로 나타낸 것이 <그림 7>이다. 이 결과 값을 토대로 본 논문에서 제안한 IP 접근제어 프로토콜이 상대적으로 제약 사항이 있는 이동단말에서 효율적인 접근제어을 위한 인증과 검증을 수행할 수 있는 프로토콜로 증명되어 본 논문에서 주장하는 프로토콜의 연산시간에 대한 성능개선이 이루어 졌음을 확인하였다.

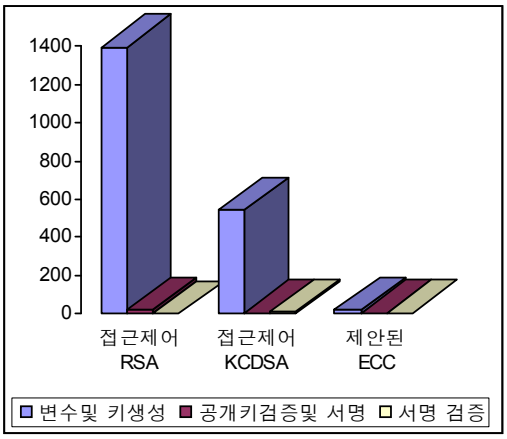


그림 7. 이동단말의 접근제어 시간 (단위 : ms)
Fig. 7 Access Control Time of Mobile Terminal

VI. 결론 및 향 후 연구과제

유비쿼터스 시대의 비대면적인 전자상거래 및 무선을 통한 이동단말에서 업무처리는 정보산업화 사회에서 도태냐 경쟁이냐 하는 갈림길을 정하는 경쟁력을 갖춘 정보화 수단이 되었다. 이동단말 서비스의 접근을 위해 신뢰성을 갖춘 통신기관이나, 사용자 인증과 검증을 하는 금융기관이나 대리인, 이를 검증 해줄 PKI 인증 센터들 사이에 서명을 생성하거나 검증해야한다. 이때 변수 및 키 생성과 서명생성, 서명검증을 빠르고 안전하게 해주는 접근제어 프로토콜이 필요하다. 본 논문에서는 이러한 개선방향과 요구들을 해결하였다. 이동단말을 위한 통신환경에서 기밀성 및 보안성을 제공하면서도 부인방지를 통해 접근제어를 효율적으로 실행 할 수 있도록 하였다. 그리고 IP 접근제어 프로토콜에 대한 설계를 하고 보안성을 검증하여 이들의 성능을 비교 분석 하였다.

접근제어 IP 프로토콜은 내부인증을 받지 못한 외부의 사용자를 위해서 IPv6프레임을 갖추도록 설계한 프로토콜이다. 그리고 통신기관의 신뢰성 있는 개인 식별 통신키를 전달 받아 공개키로 사용함으로써 보안성을 강화 시켰다. 또한 키 전달과정에서도 메시지 내용을 참조하지 않고 서명을 검증할 수 있는 방식을 도입하였고, 연산을 접근제어 서버에서 지원함으로써 프로토콜의 프로세스에 개선을 가져왔다. 또한 외부에서 내부인증을 받지 못하는 이동단말기에게도 서비스

를 제공하여 기존 프로토콜의 단점을 보완하였다,

또한 제안된 IP 접근제어 프로토콜은 타원형기반 암호화 알고리즘의 160 비트의 곱셈 연산을 사용한다. 따라서 일반적으로 사용되는 RSA 암호화 알고리즘 지수 승 연산인 방식에 비해 연산시간에서 438%이상의 성능을 개선하면서도 같은 비도를 갖는 안전성을 유지시켰다. 또한 무선 접근제어 KCDSA 방식에 비해서도 101% 이상의 연산시간 개선으로 성능향상을 가져와 효율적인 접근제어 프로토콜로 평가되었다.

향후 연구되어야 할 과제로는 첫째, IP 접근제어 프로토콜에서 단일화된 신뢰기관에서의 표준화된 개인 식별정보 기반의 인증 알고리즘에 대한 연구 및 개선이 이루어 져야한다. 둘째, 외부 이동단말이 내부로 접속 한 후에 내부에서 고의적인 공격을 시도할 때 애플리케이션 트래픽 분석과 공격 패턴매치[15]등을 차단하는 지능화된 기능을 가질 수 있도록 연구 되어져야 한다.

참고 문헌

[1] 박대우, 전문석, "K4방화벽의 CPU및 보안규칙의 증가에 따르는 성능평가연구." 한국전자거래학회 학회지, 제7권 제3호, pp203-218 2002. 12. 31.

[2] ipv6, http://www.ipv6.org/rfc/, August 1998.

[3] 해킹바이러스 통계 및 분석 월보, http://www or.kr/statistics/download.jsp?file=0404_statistics.pdf&mode=reps/hack/guest, 2004.5.4.

[4] 박대우, "Solalis K4방화벽에 대한 기능별 운영체제(32비트, 64비트)별 성능비교연구." 한국통신학회논문지, 제28권 제12B호, pp1091-1099, 2003. 12. 30.

[5] A. Buldas, H. Lipmaa and B. Schoenmakers, "Optimally Efficient Accountable Time Stamping", http://home.cyber.ee/helger/papers/bls00.html, PKC 2000.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Trans. on Information Theory. vol. IT-22, no. 6, pp. 644-654, 1976.

[7] RSA, 3DES, http://www.kisa.or.kr/

[8] 정보통신단체표준, "부가형 전자서명 방식 표준-제2부:확인서 이용- 전자서명 알고리즘," www.kisa.or.kr, 1998.

[9] ANSI X9.62, " Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA)", http://www.x9.org/, 1999.

[10] 박대우, "접근제어와 사용자 인증 프로토콜의 성능개선에 관한연구." 숭실대학교 대학원 박사논문, pp71-83, 2003. 12.

[11] C. Gamage, J. Leiwo and Y. Zheng, "An Efficient Scheme for Secure message Transmission using Proxy-Signcryption." Proceeding of the Twenty Second Australasion Computer Science Conference. pp.18-21 Jna. 1999.

[12] 한국정보통신기술협회, http://www.tta.or

[13] EC-KCDSA,http://www.tta.or.kr/StdInfo/jnal/jnal60/htmfile/6-3.htm , 2001.12.

[14] FIPS 186-2, http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf,2000.1.27.

[15] US-CERT, CCIPS, http://www.us-cert.gov/current/current_activity.html, http://www.usdoj.gov/criminal/cybercrime/cccases.html, May 2004.

저 자 소 개

박 대 우

1987년 서울시립대학교 경영학과 졸업 (경영학사)

1995년 숭실대학교 컴퓨터학부 (전산부전공)

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직캐슬정보통신 연구소 소장, 부사장

2003년 숭실대학교 겸임조교수

<관심분야> 통신S/W, 인터넷S/W, 인터넷보안, 정보보안, 이동통신 및 IMT-2000 보안, Cyber Reality