韓國 컴퓨터情報學會 論文誌
第9卷 第2號, 2004. 6.

2004-9-2-1-2

이동단말을 위한 TCP 사용자 인증 타원곡선 알고리즘 프로토콜의 설계 및 성능 개선에 관한 연구

임 승 린*, 박 대 우**

A Study on the Design and the Performance Improvement of TCP User Authentication ECC Algorithm Protocol for Mobile terminal

Seung-in Lim*, Daewoo-Park**

요 약

인터넷 비대면 거래에서, 이동단말기를 이용하는 사용자는 본인의 의사결정에 따른 정상적인 사용인지에 대한 사용자 인증 및 확인에 대한 프로토콜이 요구된다. 사용자 인증은 접근제어에 비해 검증시간이 더 소요된다. 따라서 사용자 인증 프로토콜은 부인방지와 안전성이 보장되어야하고, 이동단말에서 통신시간에 대한 성능향상이 필요하다. 이 문제를 해결하기위해, 본 논문에서는 이동단말을 위한 TCP 사용자인증 타원곡선 알고리즘 프로토콜을 설계하고 성능을 시험한다. 알고리즘은 160비트의 키를 가지고, IPv4와 IPv6에서 적용된다. 제안된 프로토콜은 기존 프로토콜의 암호화된 서명메시지 보다 인증과 검증의 과정에서 부인방지와 안전성, 기밀성이 높아졌으며, 이동단말의 연산시간에서 기존의 방법에 비해 1배에서 17배의 성능향상이 이루어졌음을 증명하였다.

Abstract

It requires that user have to verify and conform with user authentication protocol on non-meet face to face internet services offered by mobile terminal which user make known user's own intention, and user be using the normal. It is more operation time authentication protocol than Access control protocol. That is what need to be user authentication protocol have verified security, non-reputation, and improved high-performance in operation time for mobile terminal. In order to solve the above demand, in this paper, we would design for mobile terminal of TCP User Authentication ECC Algorithm Protocol with a performance test. Algorithm has 160 bit key and designed IPv4 & IPv6 frame architecture. We should conclude that the proposed protocol have more verified security, non-reputation, confidentiality, and improved high-performance in operation time of mobile terminal from 1 to 17 times than before.

▸ Keyword : ECC, information security, IPv6, mobile terminal. user authentication protocol

* 수원과학대학 인터넷정보과 교수 ** 숭실대학교 컴퓨터학과

Ⅰ. 서 론

정보통신에 대한 정보보호의 필요성은 정보화 및 개방화 사회가 발전할수록 더욱 중요하게 되었고, 인터넷을 통한 비대면적 거래에서 본인의 의사 표현과 신뢰성을 확인하는 사용자 인증 및 검증이 필수적으로 요구된다. 이동통신 서비스는 유비쿼터스(Ubiquitous) 네트워크가 형성되면서 이동단말기는 IPv6(Internet Protocol version 6)[1]를 통해 자신만의 고유한 주소를 갖게 되면서, 금융, 물류, 경영정보 등을 통해 무선 업무영역을 더욱 확대 할 것이다.

특히 무선은 통신 내용이 공중으로 방송되어 사용자에 대한 인증과 검증의 중요성[2]은 유선망에 비하여 더욱 크다. 특히 전자상거래, 이동(상)거래(mobile-commerce), 안전한 전자우편(Secure E-mail), 사업 파트너간의 안전한 정보교환 등의 무선 인터넷이나, VPN(Virtual Private Net- work)[3]과 같은 무선 인트라넷으로 확장된 사용자 인증에 대한 프로토콜을 통한 정보보호가 더욱 중요하게 여겨지고 있다.

따라서 이동단말기를 통한 무선통신에서 업무를 처리 할 때 <그림 1>과 같이 사용자의 확인 및 본인 행위에 대한 부인방지[4]에 대한 인증과 보안이 필요하고, 본인이 사용한 서비스에 대한 확인 및 검증과 함께 받아야 한다는 것이다.

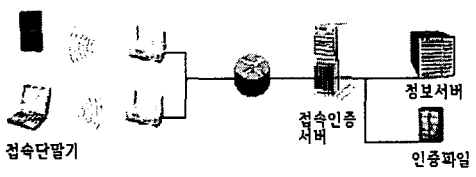

그림 1. 이동 단말기의 인증
Fig. 1 Authentication for Mobile Terminal

특히 외부 이동단말기는 고정단말기에 비해 상대적인 제약성이 있다. 적은 연산능력과 적은 메모리, 적은 배터리, 불편한 입출력 장치 등의 환경을 극복하고 무선 인터넷상의 업무를 하려면 지금 사용되고 있는 지수 승 연산보다 빠르고 적은 연산으로 빠른 통신시간을 갖는 사용자인증에 대한 프로토콜이 요구된다.

또한 현재 이동단말기에 대한 인증이나 사용자에 대한 따로따로의 인증은 이동단말기에서의 불법적인 사용을 막을 수 없는 단점이 있다. 따라서 이러한 단점을 극복하고 사용자 인증에 대한 이동단말기에서의 통신 속도를 개선하기 위해 본 논문에서 사용자를 위한 인증 타원곡선 알고리즘 프로토콜을 제안한다. 이 프로토콜은 접속 이동단말기가 접근제어에서 접근을 허용 받아서 통과한 후 전자상거래를 수반하는 사용자 서비스를 요청 할 시 사용된다. 사용자 인증 방법은 기존에 신뢰성을 확보하고 있는 금융기관이나 대리서명 대리인을 이용하는 방법이다. 이를 통해 이동단말기에서의 연산량을 줄일 수 있다. 제안된 프로토콜은 신뢰성 있는 사용자 인증을 위해 TCP (Transmission Control Protocol) 계층에서 서명에 대한 검증을 할 수 있는 프로토콜로 설계한다. 이 프로토콜은 타원 곡선상의 암호화 알고리즘에 160비트의 키를 가지고, IPv4와 IPv6에서 적용되며, 이동단말의 연산시간이 기존의 방법에 비해 성능개선이 이루어지도록 한다. 또한 프로토콜의 메시지 검증에서도 부인방지와 안전성, 기밀성을 높이는 타원곡선 기반의 암호화 알고리즘을 갖춘 새로운 프로토콜을 제안한다.

Ⅱ. 사용자인증 프로토콜의 관련 연구

전자서명은 전송하려는 전자문서에 본인의 서명을 확인해 주는 기술이다. 전자서명에서의 인증은 사용을 요청하는 주체의 신원을 확인하는 것으로 유선 네트워크에서는 공개키(public key)와 타임스탬프를 이용한 인증기법[5]들이 있다. 전자서명 알고리즘은 서명자가 전자서명을 생성 할 수 있도록 하고, 검증자는 서명의 진위를 확인 할 수 있게 하여 인증을 한다. 이때 서명자는 자신만의 비밀키와 사용자에게 공개되는 공개키를 가지는 데, 비밀키는 서명의 생성에 사용되고, 공개키는 서명 검증에 필요하다. 이 두 과정에서 서명되는 메시지는 해쉬 함수에 의해 압축되고, 비밀키를 모르는 타인이 서명을 위조하는 것은 계산상 불가능하도록 비도를 높이고 있다.

인증을 통한 사용자 프로토콜과 유사한 기존의 제안은 아래와 같다. 1985년 A. Shamir[6]에 의한 ID-based 암호시스템을 이용한 개인 식별정보 기반 방식과, 1991년 독일의 Schnorr[7]가 알고리즘에 해쉬함수를 포함시키며 짧

은 서명길이를 가지는 변형된 서명기법을 제시하였다. 1997년 Y. Zheng[8]은 서명암호화 방식을 제안하였고, 1998년 F. Bao[9]가 Y. Zheng의 수신자가 서명을 검증할 수 있는 수정된 방식을 제안 하였다. 1999년 C. Gamage[10]는 서명된 메시지로 검증을 할 때 수신자의 비밀키 없이 원문의 내용을 노출시키지 않는 상태에서 알고리즘만으로 서명의 정당성을 검증할 수 있는 방식을 제안하였다. 또한 지금까지 제안되었던 프로토콜에 사용되었던 알고리즘들은 대부분이 통신에서 PKI 방식 등으로 키쌍을 검증하는 Diffie-Hellman 방식[11]의 지수승을 연산으로 구현 하였으며, 사용되는 알고리즘도 RSA(Rivest-Shamir-Adleman)나 3DES(Data Encryption Standard) 등을 이용하는 것이 대부분이었다. 또한 무선 환경에서 무선인터넷이 발달 하면서 우리나라도 KCDSA(Korea Certicate-Based Digital Signature Algorithm) [12]를 표준으로 정하여 지원하였고, 미국에서는 ECDSA[13]를 표준으로 하는 암호화 알고리즘을 사용하고 있다.

III. 타원곡선 알고리즘의 설계

본 논문에서 제안하는 TCP 사용자인증 타원곡선 알고리즘 프로토콜에 사용되는 ECC 알고리즘은 ECDSA를 개선하여, 임의의 타원곡선 (Random Elliptic Curve)과 Koblitz 타원곡선(Koblitz Elliptic Curve)을 사용하며, 160비트 키 값을 갖고 있다. 변수에 및 규격 사용은 TTA[14]의 표준안인 EC-KCDSA[15] 방식과 미국의 ECDSA의 연방표준인 FIPS 186-2[16]의 규격을 따랐다. 사용자 인증에 사용되는 전자서명을 위한 함수들을 이용하며, 크게 타원곡선 도메인 변수의 생성 및 검증 과정, 타원곡선 키 쌍의 생성 및 공개키의 검증 과정, 그리고 타원곡선 전자 서명의 생성 및 검증과정으로 이루어져 있다.

1. 타원곡선 도메인 변수의 생성 및 검증

도메인은 사용자들이 공유하는 공개정보로, 한 사용자나 다수의 사용자들이 그룹 혹은 복수개의 사용자 그룹들로 구성된다. 도메인 변수들은 유한체를 정의하는 변수들, 타원곡선을 정의하는 변수들, 타원곡선상의 순환군과 관련된 변수들로 구성되어 있다. 타원곡선을 정의하는 기본점 G는 타원곡선 암호에 사용되는 모든 점을 생성하는 점이다.

1-1 타원곡선 도메인 변수 및 변수 생성

유한체는 특성값과 확장차수에 따라서 $GF(p)$, $GF(2^m)$, $GF(p^m)$으로 나누어지며 이들은 각각 다른 변수들을 가진다. 타원곡선 도메인 변수는 160비트 이상의 소수 p와 160비트 길이를 가지는 비트 열, 그리고 $GF(p)$의 두 원소 a와 b ($E : y^2 = x^3 + ax + b$) 및 타원곡선 E상의 기본점 $G=(x\,G,\ y\,G)$ (단, $G \neq 0$)와 점 G의 위수 n, 그리고 선택사항으로 여인자 $h = \#E(GF(p))/n$으로 구성된다.

전자 서명 안전성을 확보하기 위해서 타원곡선 상의 도메인 변수를 생성하여야 한다. $GF(p)$ 타원곡선 방정식 E : $y^2 = x^3 + ax + b$을 위한 변수 a, b $\in$ $GF(p)$로 한다. $GF(2^m)$상의 방정식의 변수 생성은 삼항 다항식 $x^m + x^k + 1$의 형태와 오항 다항식 $x^m + x^{k3} + x^{k2} + x^{k1} + 1$의 형태로 $y^2 + xy = x^3 + ax^2 + b$ 을 위한 변수 a, b $\in$ $GF(2^m)$로 한다. $GF(p^m)$는 소수 $p = 2^l - c$를 구성하고, 타원곡선 방정식 E : $y^2 = x^3 + ax + b$을 위한 변수 a, b $\in$ $GF(p^m)$로 한다.

1-2 타원곡선 도메인 변수의 검증

전자 서명의 안전성을 확인하기 위해 도메인 변수의 유효성을 검증하여야 한다. 사용자들은 이 검증을 통해 전자서명을 신뢰한다. 따라서 제3의 인증기관은 공개키에 대한 인증서를 발급하기 전에 도메인 변수의 유효성을 검증하여야 한다. $GF(p^m)$상의 타원곡선의 도메인 변수 검증 알고리즘은 〈표 1〉과 같으며 이 검증과정을 통과한 경우에만 "유효함"을 출력하고, 그렇지 않은 경우에는 "유효하지 않음"을 출력한다.

표 1. $GF(p^m)$상 도메인 변수의 검증
Table. 1 Verification of Domain variable on $F(p^m)$

입력 : $GF(p^m)$에서 정의된 타원곡선 도메인 변수들로 이루어진 집합.
출력 : 타원곡선 도메인 변수들이 "유효함" 혹은 "유효하지 않음".
Verify m = prime number, prime number p 〉 3
Verify $x^m - \varpi$ in $GF(p)$
Verify integer a, b, $x\,G$ $y\,G$ ($\in$ [0, $p^m - 1$])
Verify Bit stream Seed (〉 160 bits), ~

Verify $4a^3 + 27b^2 \neq 0$ in $GF(p^m)$
Verify $y G^2 = x G^3 + ax G + b$ in $GF(p^m)$
Verify $nG = 0$
Verify n () 160 bits && prime number), & n
$\sqrt{}$ $4(p^m)$(Option) Calculate h =
$\sqrt{}$ $((p^m)+1)^2/n$ & Verify $h = h'$
Verify $p^{mB} \neq 1$ mod n $(1 \leq B \leq 30)$
Verify $\#E(GF(p^m)) \neq p^m$, ~
if Verification = Ok through ~
then print "Valid"
else print "Invalid"
end if

2. 타원곡선상의 키 쌍의 생성

전자 서명의 안전성은 서명에 사용된 공개키가 주어진 타원곡선 도메인 변수 상에서 정상적인 생성을 가정으로 하여 공개키의 유효성을 확인한다. 따라서 검증은 공개키 인증서를 발급하는 인증과정에서도 이루어지며, 서명 검증자도 수행할 수 있다.

표 2. 키 쌍의 생성
Table. 2 Creation of Key pairs

입력 : 유효한 타원곡선 키 쌍의 생성
출력 : 타원곡선 도메인 변수로부터 생성된 키 쌍.
Select Ta ($\in$ (1, n-l), unique and unexpected)
Calculate Ta = 1 mod n, (1< Ta^{-1}<n)
Calculate $T_A = (x T_A, y T_A) = Ta^{-1} G$
Print pair of public & private key (T_A, Ta)

〈표 2〉의 키 쌍 생성은 통계적으로 유일하고 예측이 불가능한 정수 Ta를 [1, n-1]에서 선택하고, 여기에서 Ta의 역원 Ta^{-1}을 계산하여, $T_A = (x T_A, y T_A) = Ta^{-1}G$를 계산하여 공개키와 개인키의 쌍 (T_A, Ta)를 출력한다.

Ta를 선택할 때에는 임의의 랜덤 수를 사용하여야 한다. 이 경우 랜덤 수 생성 방법은 초기값의 구현에 따라 시스템 내부나 외부에서 사용자가 입력하여 선택적으로 사용할 수 있으며, 어느 경우나 초기값은 개인키와 같은 보안이 요구된다.

3. 타원곡선상의 공개키 검증

공개키 T_A의 유효성 및 해당 타원곡선 도메인 변수와의 연계성에 대한 검증은 인증과정을 통해 이루어지며, 신뢰를 확보하지 못한 경우에는 유효성에 대한 검증을 요구할 수 있다.

표 3. 공개키 T_A 의 검증
Table. 3 Verification of Public Key T_A

입력 : 유효한 타원곡선 도메인 변수, 검증하고자 하는 공개키 T_A.
출력 : 해당 공개키가 "유효함" 혹은 "유효하지 않음".
Verify $T_A \neq$ Infinite 0
Verify $x T_A$ & $y T_A \in GF(q)$
if q = p
then $x T_A$ & $y T_A \in$ integer (0, p-l)
if $q = 2^m$
then $x T_A$ & $y T_A$ = m-bit bit stream
if $q = p^m$
then $x T_A$ & $y T_A \in$ integer (0, p^m-l)
if (q = p) || ($q = p^m$)
then Verify $y T_A^{\,2} = x T_A^{\,3} + ax T_A + b$
in $GF(q)$
if $q = 2^m$
then Verify $y T_A^{\,2} + x T_A\, y T_A =$
$x T_A^{\,3} + ax T_A^{\,2} + b$ in $GF(2^m)$
Verify $n T_A = 0$
if Verification = Ok through ~
then print "Valid"
else print "Invalid"
end if

〈표 3〉은 공개키 T_A의 검증과정을 나타낸 알고리즘이다. 이 검증과정을 통과한 경우에만 "유효함"을 출력하고, 그렇지 않은 경우에는 "유효하지 않음"을 출력한다.

4. 타원곡선상의 전자 서명의 생성

4-1 메시지에 대한 해쉬 코드의 생성

전자 서명 생성 및 검증 과정에 사용되는 해쉬 함수는 160비트의 해쉬 코드를 출력하는 해쉬 함수인 표준 HAS 160을 사용한다. 그리고 해쉬 함수 Π의 입력 데이터 형과 출력 데이터 형을 모두 바이트 열로 재 정의하여 사용한다. 서명하고자 하는 메시지 M에 대한 해쉬 코드는 해쉬 함수 Π을 이용하여 $\Pi(c T_A \,||\, M)$과 같이 생성된다. 메시지 M 앞에 덧붙이는 $c T_A$는 서명자의 공개키이며, $T_A = (x T_A, y T_A)$에 의존하는 서명자 고유의 상수로 다음과 같이 계산된다. $c T_A = LMB(x T_A \,||\, y T_A, L)$.

4-2 서명 생성 과정

개인키 Ta를 가진 서명자의 메시지 M에 대한 서명은 〈표 4〉와 같은 과정을 통하여 생성된 바이트 열 r과 s의 쌍으로 구성된다. 서명 생성 과정의 랜덤 값 k를 생성하여 타원곡선의 점은 바이트 열로 변환되어 (x1, y1)= kG를 계산하고, log256 n 길이의 바이트 열 s로 변환하여 M에 대한 서명으로 바이트 열 { r, s}를 출력한다.

표 4. 서명 M의 생성
Table. 4 Creation of Message M

```
입력 : 서명할 메시지 M, 서명자의 타원곡선 도메인 변수 및 개인
       키/공개키 쌍
출력 : M에 대한 서명으로 바이트열 { r, s}.
 Create random value k ∈ {1, 2, ... , n-1}
 Calculate (x1, y1) = kG, ~
 Calculate r = Π(x1), First part of signature
 Calculate v = Π(c T_A || M),
            Message hash code
 Calculate e = r ⊕ mod n, Mid-term value
 Calculate t = Ta( k-e) mod n
   if t = 0
      then return to stage_1
      Change t to byte stream s (log256 n)
Print byte stream { r, s} by signature for M
```

4-3 서명 검증 과정

수신된 메시지 M'에 대한 서명{ r', s'}이 공개키 T_A를 가진 서명자의 유효한 서명인지를 검증하는 과정은 〈표 5〉와 같다. 이 과정을 통과한 경우에만 "유효함"을 출력하고, 그렇지 않은 경우에는 "유효하지 않음"을 출력한다.

표 5. 서명 M의 검증
Table. 5 Verification of Message M

```
입력 : 수신된 메시지 M '과 서명{ r', s'}, 서명자의 타원곡선
       도메인 변수 및 공개키 T_A,
출력 : 메시지 M '에 대한 서명자의 서명 { r', s'}이 "유효함"
       혹은 "유효하지 않음".
 Verify = (length-hash function) & 0〈 t'〈 n
          (integer t'= 2th Message r'(0,n-1))
 Calculate Message hash code
       v' = Π(c T_A || M ')
 Calculate Mid-term value e' = r' ⊕ v' mod n
 Calculate (x2, y2) = t' T_A + e' G, ~
 Verify Π(x2) = r'
  if Verification = Ok through ~
    then print "Valid"
      else print "Invalid"
  end if
```

지금까지 본 논문의 TCP 사용자인증 타원곡선 알고리즘 프로토콜에 사용되는 알고리즘을 설계하였다. 타원곡선 도메인 변수는 유한체와 타원곡선 그리고 타원곡선상의 순환군과 관련된 변수들로 구성되어 있으며, 유한체는 특성값과 확장차수에 따라서 $GF(p)$, $GF(2^m)$, $GF(p^m)$의 각각 다른 변수들을 가지므로 이들 각각의 타원곡선 상의 도메인 변수의 검증의 알고리즘을 각각 설계하였다.

또한 타원곡선 도메인 변수로부터 공개키와 개인키를 생성하고, 이 공개키 T_A의 유효성 및 해당 타원곡선 도메인 변수와의 연계성에 대한 검증에 대한 알고리즘을 나타내었으며, 이들이 인증과정을 통해 신뢰를 확보하지 못한 경우에는 유효성에 대한 검증을 요구할 수 있는데, 이때에도 서명할 메시지 M, 서명자의 타원곡선 도메인 변수 및 개인키/공개키 쌍으로 출력된 M에 대한 서명으로 된 바이트열 { r, s}을 이용한 수신된 메시지 M'과 서명{ r', s'}, 서명자의 타원곡선 도메인 변수 및 공개키 T_A이며, 이 메시지 M'에 대한 검증 알고리즘을 통해 서명자의 서명 { r', s'}을 검증하여 서명의 "유효함" 혹은 "유효하지 않음"을 출력하는 프로토콜의 알고리즘을 설계하였다.

IV. TCP 사용자 인증 프로토콜의 설계

1. TCP 사용자 인증프로토콜의 설계

〈그림 2〉는 이동단말을 통한 사용자 인증 프로토콜의 흐름을 나타내었다. 서명 암호화생성과 검증에 사용되는 암호화 알고리즘은 ECDSA에서 정의한 변수를 사용하며, 키값은 160비트 이상을 사용한다.

TCP 프로토콜의 세그먼트(Segment)는 예약비트 6비트를 이용하여 이동단말기에서 전자상거래와 관련한 무선업무를 요청 할 때 단말기에서 접속 신청 프로세스의 식별자인 포트번호의 접속사용 서비스요청을 확인한 후, 이동단말기의 사용자에 대한 사용자 인증을 검증을 하기 위하여 TCP 프로토콜에서의 프레임을 설계한다.

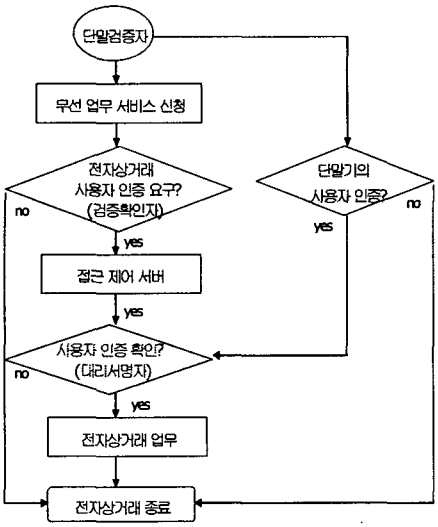

그림 2. 이동단말의 사용자인증의 흐름도
Fig. 2 Flow of mobile terminal's User Authentication

2. TCP 사용자 인증 프로토콜의 프로세스

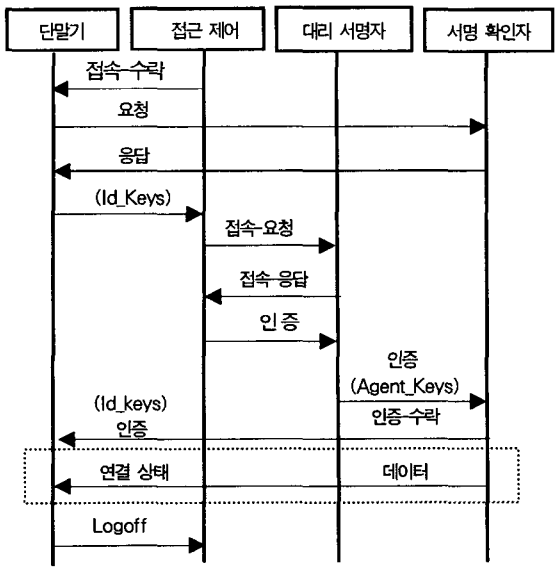

그림 3. 이동단말의 사용자인증의 프로세스
Fig. 3 Process of mobile terminal's User Authentication

제안된 사용자 인증 프로토콜의 프로세스는 TCP 계층에서 이루어지며 〈그림 3〉과 같이 접속 단말기 사용자에 대한 사용자 검증확인 요청, 사용자에 대한 요청 확인, 접속 단말기에서 접근제어로 접속 요청, 접근차단, 접근허용, 접근제어가 대리서명자에게 접속 단말기 사용자에 대한 사용자 인증에 대한 검증 요청, 검증 성공, 검증 실패, 접속 단말기가 서명 확인자에게 사용자 인증의 인증 요청, 요청 확인, 무선랜 접속 단말기가 서명 확인자에게 사용자 인증에 대한 검증 실패, 검증 성공의 기능을 내용으로 하고 있다.

3. TCP 사용자 인증 프로토콜의 전개

프로토콜의 알고리즘에 따라서 이루어질 접속 단말기의 사용자인증 프로토콜의 메시지 검증 방법에 관한 내용을 전개하면 아래와 같다.

3-1 사용자 인증 프로토콜의 위임 서명 생성

접속 단말기 사용자나 외부 이동통신 가입자는 금융기관이나, 대리서명 대리인에게 서명생성을 위한 위임 서명 정보를 생성한다. 이때 랜덤수를 이용하여 해쉬값 Π을 생성한다. 그리고 원문 메시지 M 에 타임스탬프 T를 찍고 암호화 하여 검증자 c값을 생성하고 대리서명 대리인의 공개키 MA_C를 이용하여 값을 생성한다. 접속 단말기 사용자는 (식 2.1)에서와 같이 세션키 s 생성 시 일회성을 갖는 랜덤값 x 를 이용하여 서명을 생성하여, 생성된 위임 서명 정보 s, c, r 및 서명을 수행할 메시지 M과 타임스템프 T를 사용한 후 사용자 인증을 위한 서명 검증을 하는 대리서명 대리인에게 전송한다.

$$s = \frac{rx - r - 1}{MT_a + 1} \mod n \quad \cdots\cdots \text{(식 2.1)}$$

3-2 사용자 인증 프로토콜의 위임 서명 확인

대리서명 검증인은 수신된 값을 통하여 접속 단말기 사용자에 대한 인증의 정당성을 확인한다. 서명의 검증을 하기 위해 해쉬값을 이용한다. 그리고 (식 2.2)와 같이 전달받은 r값을 이용하여 복호화 한다.

$$P = \frac{1 + r + s}{r} G + \frac{s}{r} MT_A \quad \cdots\cdots \text{(식 2.2)}$$

대리서명 검증인은 대리서명 대리인이 접속 이동단말기 사용자로부터 받은 메시지를 검증하기 위해 전송된 서명 메시지를 검증하기 위해 c XOR Π를 실행하고 r'값을 생성하여, 대리서명 대리인이 전송해준 r값과 같으면 ($r = r'$) 정보서버의 접근의 통과를 허용하고, r값과 다르거나($r \neq r'$), 타임스탬프의 값이 다르거나, 유효기한이 지난 것이면 폐기시켜 내부정보 서버로의 접근을 즉시 차단한다.

3-3 사용자 인증 프로토콜의 대리서명 수행

대리서명 대리인은 랜덤수 x'및 G을 선택하고, 메시지 M과 타임스탬프 T를 사용한 후 사용자 인증을 위한 서명을 생성하고, 대리서명 인증자의 부정행위를 방지하기 위한 개인키 MA_c로 이용하여 대리서명을 생성한다. 대리서명 대리인은 서명 수행을 생성 후 c ,r ,s 를 계산하여 서명 검증자에게 값과 정보를 전송한다.

3-4 사용자 인증 프로토콜의 대리서명 검증

대리서명 검증인은 대리서명 대리인이 송신한 값을 통해 IT'값을 생성하고, 전송해온 c ,r ,s 값을 통해 접속 단말기 사용자의 사용자 인증에 대한 정당성을 확인하여 사용자 인증을 한다. 이때 검증확인 시간에 대한 타임스탬프 및 사용되어진 접속 사용자의 사용자 정보 및 대리서명 대리인 정보는 사용자인증 감사 기록 테이블로 이동되어 저장 된다.

4. TCP 사용자 인증 프로토콜의 프레임 설계

TCP 프로토콜은 응용계층과 인터넷계층 사이에 응용 프로그램과 네트워크 동작 사이의 중계자 역할을 하는 신뢰성을 가진 연결 지향성 프로토콜로 TCP와 UDP(User Datagram Protocol)는 각각의 헤더필드 안에 16비트의 포트번호 필드를 가지고 있어 65,535개만큼의 포트별 서비스를 가질 수 있다. 따라서 수신지 IP주소가 선택된 후에는 포트번호를 통해서 호스트 내에 있는 여러 프로세스 중 하나의 프로세스를 사용한다.

TCP 프로토콜의 세그먼트 헤더는 옵션이 없이20 바이트이며 옵션을 첨가할 수 있는 비트 중 6 비트의 예약 비트가 있다. 〈표 6〉에서 사용자 인증 프로토콜의 TCP 프레임에서 예약 6비트의 필드의 값을 설계하였다. 접속 이동단말기에서 전자상거래와 관련한 무선업무를 요청 할 때 호스트에서 프로세스의 식별자인 포트번호의 접속사용 서비스 요청을 하면, 접속 이동단말기의 사용자에 대한 인증을 하기 위한 프로토콜의 프레임이다.

사용자 인증 TCP 프로토콜은 사용자의 인증을 위한 프로토콜이므로 사용자가 무선 서비스를 요청 할 시 사용자의 패킷에서 나오는 정보 중 사용자의 서비스 포트에 관한 정보를 검색 하여, 접속 단말기의 사용자가 원하는 무선업무 서비스를 파악 할 수 있어 TCP 계층에서 이루어져야 사용자의 신뢰성 있는 서비스의 제공이 이루어 질 것이다.

표 6. 사용자 인증 프로토콜의 프레임 설계
Table. 6 frame Structure of User Authentication Protocol

구분	프레임 형태	예약 필드값	설계 기능 내용
헤더 확장 사용 예약	예약 필드	000001	접속 단말기의 검증확인 요청
		000010	접속 단말기의 검증확인 요청 확인
		000101	접속 단말기의 접근제어의 요청
		000110	접속 단말기의 접근제어의 접근차단
		000111	접속 단말기의 접근제어의 접근허용
		001110	접근제어 서버의 대리서명자에게 검증 요청
		001001	접근제어 서버의 대리서명자에게 검증 성공
		001100	접근제어 서버의 대리서명자에게 검증 실패
		010000	접속 단말기의 서명 검증자에 대한 사용자 인증 요청
		010001	접속 단말기의 사용자 인증 요청 확인
		010100	접속 단말기의 사용자 인증 검증 실패
		010101	접속 단말기의 사용자 인증 검증 성공

V. TCP 사용자 인증 프로토콜의 보안 분석

1. TCP 사용자 인증 프로토콜의 보안 검증

유비쿼터스 시대에 인터넷 전자상거래에 대한 보안이 전사적 관리의 차원에서 확장되고 요구되어 진다. 제안한 프로토콜은 금융기관과 PKI 인증센터를 연계하여 수신지정 서명방식을 이용하여 사용자 인증을 검증하는 프로토콜이다. 따라서 기존에 제시되었던 전자서명 방식들과 비교하여 아래와 같은 특성들에 대해 이동단말의 정보 보안에 관한 요구사항을 만족하고 있다.

본 제안방식은 수신자 지정 서명방식을 채택함으로서 오직 검증자만이 서명자의 신원을 확인할 수 있기 때문에, 제3자에 의한 불법적인 해킹으로부터 서명자에 대한 기밀성을 확보하고 있다. 비대면 전자상거래를 수행할 경우, 거래의 투명성과 안정성을 확보하기 위해 꼭 필요한 인증을 수신자 지정 서명방식을 이용한다. 따라서 접속단말기에 대한 인증뿐만 아니라, 사용자에 대한 사용자 인증을 해 줌으로써 전

자상거래에 확실한 보안 요소를 제공한다. 또한 서명생성 시 타임스탬프를 이용하여 대리서명을 수행한다. 따라서 위임서명자가 서명생성 의뢰에 대한 부인방지를 하여 보안성을 확보 할 수 있다.

이때 위임서명자는 연산능력이 상대적으로 뛰어난 대리서명 대리인이나 접근제어에서 연산을 지원해준다. 이로써 이동단말기상의 서명생성 및 검증에서 소요되는 연산시간을 획기적으로 줄여준다.

위임정보 전송 시에도 일회용 패스워드 방식의 비밀서명을 제공하게 되고, 대리서명 대리인도 자신의 비밀정보를 생성하여 서명암호화를 통한 검증자를 생성해 서명암호화 자료를 전송하게 된다. 따라서 위임 서명자 및 대리서명 대리인이 할 수 있는 불법적인 서명생성을 못하게 함으로써 기존의 단점을 보완하는 보안에 대한 안전성을 높이게 된다.

2. 제안된 프로토콜의 보안성 비교 분석

제안한 TCP 사용자 인증 프로토콜과 기존에 제시 되었던 프로토콜과의 보안성을 비교분석하여 〈표 7〉에 나타내었다.

서명자 기밀성은 인가되지 않는 자가 서명을 획득하여도 비밀키를 모르는 상태에서 서명을 생성·위조할 수 없다는 뜻이다. (식 2.1)과 같이 접속 단말기의 비밀키인 MT_a로 서명을 생성했기 때문에 서명을 위조할 수 없다. 따라서 서명자의 개인 비밀키로 서명하면 서명자 기밀성이 있다고 판단한다.

인증성은 접속 이동단말기의 사용자의 인증에서, 최초 접속 때 직접 신분확인을 통해 신뢰성이 확인되어야하는데, 인증을 위한 키 전달 시에 (식 2.2)와 같이 서명자의 공개키 MT_A를 이용하여 서명자를 검증하였다. 이와 같이 공개키를 이용한 검증은 인증성 기준이 있다고 판단한다.

부인방지는 서명 생성 시에 표준시간의 타임스탬프 T와 함께 서명하여 사용자의 정보 및 대리서명자의 대리인에 관계되는 정보는 감사기록에 저장되고, 서명자의 비밀키 MT_a를 사용하여 서명자는 자신의 서명 내용에 대해서 부인 할 수 없다. 따라서 감사기록 및 부인방지를 위한 자료확인이 되면 부인방지 기준이 있다고 판단한다.

유효성 기준은 서명자의 비밀키를 사용하고 서명 암호화 생성 시 난수인 x를 사용하면 다른 문서의 서명으로 재사용 할 수 없으므로 유효성의 기준이 있다고 판단한다.

안전성은 서명 시 공인된 SHA-1로 해쉬하여 중간에서 서명을 가로채도 내용을 알 수 없어야 한다. 따라서 서명 시에 SHA-1 함수를 이용하여 쉬한다면 안전성의 기준이 있다고 판단한다. 표준화의 기준은 국제적인 표준화단체에서 토론과 승인을 거쳐 공식적인 프로토콜로 인정받아 세계표준으로 채택되고 사용된다면 표준화의 기준을 획득한 것으로 판단한다.

표 7. 사용자 인증 프로토콜의 정보보안 기준 비교
Table. 7 Compare of Information Security Criteria in User Authentication Protocol

보안성 / 제안자	기밀성	인증성	부인방지	유효성	안전성	세계표준
Mambo[17]	X	O	X	O	X	X
Won[18]	O	O	O	X	X	X
Gamage	O	O	X	O	X	X
제안한 프로토콜	O	O	O	O	O	X

VI. 사용자 인증 프로토콜의 성능비교분석

본 논문에서는 제안한 프로토콜이 유비쿼터스 환경에서 이동단말기의 제한성을 극복하고, 이동단말의 사용자 인증 시에 사용되는 프로토콜에서 서명의 생성과 검증 시에 필요한 연산시간 실험에 초점을 맞추고, TTA의 실험규격에 추어 통신실험실에 실험 환경을 구축 하였다.

실험내용은 제안한 타원곡선을 이용한 타원곡선상의 키 쌍과 변수의 생성, 공개 검증키의 검증 및 타원 곡선상의 전자서명의 생성 및 검증에서 외부 네트워크에서의 이동단말기와 내부 네트워크의 이동단말기에 연결되어 있는 접근제어 서버로 구성하였다.

실험기기의 사양은 다음과 같다.

- 접근제어 서버
  Pentium III, 1CPU(1GHz), Windows 2000,
- 외부 네트워크의 접속 단말기
  SA110, 1CPU(233MHz), 16비트 Linux

통신 속도 측정 프로그램을 통해 측정방법은 각각의 정해진 기준에 따라서 100회의 값을 측정을 하고 이 값을 평

균하여 5회 측정값으로 하고 이를 다시 평균하여 값을 산출하였다. 성능 측정단위는 프로토콜 서명의 변수설정 및 생성 그리고 검증과정은 밀리(millis) 초인 $1/10^{-3}$초 단위로 측정을 하였고, 표시는 밀리 초인 "ms" 로 하였다. 성능 비교대상으로는 현재 우리나라 유선통신에 쓰이는 RSA 알고리즘과 무선통신 표준에서 채택하고 있는 KCDSA 암호화 알고리즘의 실험값을 이용하여 비교기준으로 하였다. 이 두 기준의 값은 TTA에서 실험한 결과를 인용하여 비교 기준값으로 채택 하였다.

비교 분석의 방법은 프로토콜에서 전자서명 키 생성과 서명 및 검증에 사용되는 연산시간을 수치로 나타내고, 이 차이 시간을 대비한 비교 그래프와 함께 나타내고, 알고리즘별로 연산속도를 기준과 비교 분석하여 배수로 표현한다.

표 8. 이동단말의 사용자인증 시간 (단위 : ms)
Table. 8 Mobile Terminal of User Authentication Time

프로토콜 / 환경	사용자인증 RSA	사용자인증 KCDSA	제안된 프로토콜
변수 및 키 생성	5206.1	1427.3	77.1
공개키 검증 및 서명	39.1	44.6	4.4
서명 검증	2.4	24.5	9.4

제안한 프로토콜의 타원곡선 알고리즘을 기반으로 한 실험 결과 값을 〈표 8〉에 나타내었고, 실험 결과 값을 비교하는 그래프를 〈그림 4〉에 비교하였다. 이 성능 비교실험의 결과에서 나타난 바와 같이 서명을 위한 암호화 알고리즘 계산에 서 변수 및 키 생성에 연산시간은 RSA에 비해66배 줄었고, KCDSA에 비해 17배 줄었다.

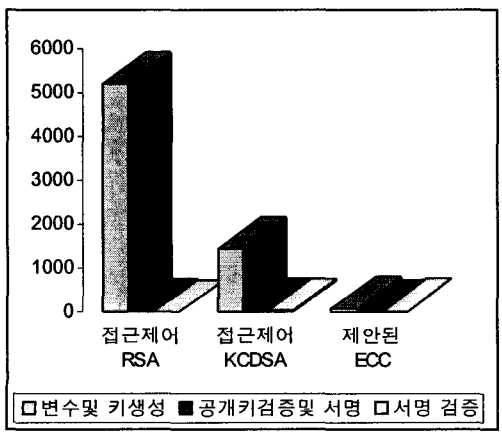

그림 4. 이동단말의 사용자인증 시간 (단위 : ms)
Fig. 4 Mobile Terminal of User Authentication Time

또한, 공개키 검증 및 서명시간도 RSA에 비해 7배 감소되었고, KCDSA에 비해 9배 감소하였다. 서명 검증시간은 RSA에 비해 3배 증가하였지만 KCDSA에 비해 1배 이상 감소하였다.

표 9. 사용자 인증 프로토콜의 정보보안 기준 비교
Table. 9 Compare of Information Security Criteria in User Authentication Protocol

항목 / 제안자	알고리즘	통신 연산 방법	단점 및 보완점
Zheng	RSA	지수승 연산 $(y_a g^r)^s \bmod p$	부인방지 못함. 수신자만 검증 가능한 단점.
Bao	RSA	지수승 연산 $(y_a g^r)^s \bmod p$	메시지 검증 값을 수신하여 검증하도록 보완
Gamage[19]	RSA	지수승 연산 $(y_a g^r)^s \bmod p$	검증 값 없이 알고리즘만으로 검증가능 하게함
제안한 프로토콜	ECC	XOR 연산 $y_a \ XOR \ p$	알고리즘만으로 검증 후에 연산시간을 개선함

결국 제안한 프로토콜이 지금 유선에서 사용되는 RSA나 무선에서 사용되는 KCDSA에 비해, 상대적으로 많은 연산시간이 걸리는 변수의 키 생성 시간에서 9배에서 17배로 줄었고 서명검증에서도 1배 이상의 연산시간을 감소 시켰다. 그 원인 중에 하나는 〈표 9〉와 같이 현재 유선에서 일반적으로 사용되고 있는 RSA 암호화 알고리즘에서 ECC 알고리즘을 사용하였으며, 알고리즘도 기존 알고리즘의 단점을 보완하며 통신연산 시간을 개선하였다.

따라서 TCP 사용자인증 타원곡선 알고리즘은 사용자의 인증 및 검증을 위한 서명에 대한 연산시간을 감소시켜 하드웨어적인 제약사항이 있는 이동단말기에서 효율적인 프로토콜로 증명되었다.

VII. 결론 및 향 후 연구과제

현재의 이동단말은 가입자 단말기에 대한 식별번호나 사용자에 대한 단순 인증만을 수행하고 있다. 따라서 불법적인 단말기 도용에 대한 안전성을 확보하지 못한다. 또한 연산능력, 메모리 등 이동단말기에 대한 제약사항으로 인해

암호화 및 검증에 걸리는 연산시간이 길다는 단점이 있다.

본 논문에서는 수신자 지정 서명방식을 채택하고 부인방지 및 안전계층에 대한 사용자 인증의 보안성을 강화 시켰다. 또한 사용자 인증에 지정인증 방식을 도입하여 검증자와 안전한 채널을 형성하게 하여, 송신자와 대리서명 대리인의 부정에 대한 단점을 보완하였다.

또한 프로토콜에 타원곡선상의 160비트의 암호화 알고리즘을 적용하여 같은 비도의 보안성을 유지하였다. 여기에 대리서명자의 공개키를 이용한 검증방식의 알고리즘으로 연산시간에 대한 성능은 KCDSA 방식에 비해 1배에서 17배의 개선효과를 가져와 이동단말기에서 성능을 향상시켰다. 이로써 TCP 계층에서 사용자 인증 및 검증의 프로토콜에 대한 보안성을 강화시켰고, 연산시간을 줄임으로써 통신 속도의 성능 향상을 가져와 이동단말을 위한 효율적인 사용자 인증 프로토콜임을 증명 하였다.

향후 연구되어야 할 과제로는 사용자 인증 프로토콜도 접속 단말기에 대한 인증과 사용자에 대한 인증을 하드웨어나 펌웨어(firmware)적인 방법을 통해 동시 일괄처리(One Time Process) 되는 방법에 대한 연구와 검증을 통해 이동단말에서 보다 신속하게 인증 및 검증 될 수 있도록 연구 되어져야 한다.

참고문헌

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

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

[3] 박대우, "무선방화벽의 설계 및 구현에 관한 연구." 한국컴퓨터정보학회논문지, 제8권 제1호, pp44-50, 2003. 3. 31.

[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] A. Shamir, "Identity-based cryptosystems and signature schemes", Advanced in Cryptology (ProceedingsofCrypto'84). Springer-Verlag, pp.47-53, 1985.

[7] C. Schnorr, "Method for identifying sub-scribers and for generating and verifying electronic signatures in a data exchange system." U.S. patent #4,995,082, 1991.2.

[8] Y. Zheng, "Signcryptionor How to Achieve Cost(Signature & Encryption) << Cost (Signature) + Cost(Encryption)". CRYPTO'97, 1997.

[9] F. Bao and R. H. Deng, "A Signcryption by Public Key, PKC'98, 1998.

[10] C. Gamage, J. Leiwo and Y. Zheng, "Encyrpted Message Authentication by Firewalls." PKC'99, 1999.

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

[12] KCDSA, http://www.istf.or.kr/pdf/2_1_issw.PDF, 2001.

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

[14] TTA, http://www.tta.or.kr/Home2003/ittl/it_service.jsp

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

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

[17] M. Mambo, K. Usuda and E. Okamoto, "Proxy Signatures for delegating signing operation." Proc. Third ACM Conference on Computer and Communications Security. pp. 48-57. 1995.

[18] D. H. Won, S. J. Kim and S. J. Park, "Nominative Signatures." Proc. ICEIC '95 pp.I68-II71. 1995.

[19] 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.

저 자 소 개

임 승 린

1979년 숭실대학교 컴퓨터학과(학사)
1987년 숭실대학교 대학원 컴퓨터학과(석사)
1999년 숭실대학교 대학원 컴퓨터학과(박사)
1989년 수원과학대학
현재 인터넷정보과 부교수
〈관심분야〉 응용S/W, 정보시스템, DataBase, 컴퓨터 네트워크 및 인터넷, 지식관리시스템,

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〉 인터넷S/W, 보안S/W, 인터넷보안, 정보보안, 이동통신 및 IMT-2000 보안, Cyber Reality