韓國 컴퓨터情報學會 論文誌
第9卷 第3號, 2004. 9.

2004-9-3-3-3

핸드오버시 인증 대기시간 단축을 위한 성능 분석

신 승 수*, 서 정 만**

Performance Analysis for Reducing Authentication Time in Hand-over

Seung-Soo Shin *, Jeong-Man Seo **

요 약

본 논문에서는 기존의 무선 PKI에서 키 교환방식의 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 제안한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에 타원곡선을 적용하였다. 제안한 무선 PKI 구조 안에서의 핸드오버 방법은 CRL 검색시간을 단축시킬 수 있으므로 기존의 방법에 비하여 단축된 핸드오버 처리시간을 보여준다. 기존 알고리즘과 제안한 인증구조를 비교하여 실험해 보았을 때 호 도착율, 큐의 서비스율, 큐 사이즈 변화에 관계없이 제안한 인증 기법이 모든 환경에서 기존 알고리즘보다 우수한 성능을 보였다.

Abstract

In this paper, a conventional key exchange method simply performs the key exchange setup step based on discrete algebraic subjects. But the mutual-authentication procedure of wireless PKI for reducing authentication time uses an elliptical curve for a key exchange setup step. Proposed handover method shows reduced handover processing time than conventional method since it can reduce CRL retrieval time. Also, we compared proposed authentication structure and conventional algorithm, and simulation results show that proposed authentication method outperforms conventional algorithm in all environment regardless of call arrival rate, queue service rate, queue size.

▸ Keyword : Handover, PKI(Public Key Infrastructure)

• 제1저자 : 신승수
• 접수일 : 2004.08.09, 심사완료일 : 2004.08.21
* 목원대학교 정보통신전파학부 겸임교수, ** 한국재활복지대학 컴퓨터게임과 교수

Ⅰ. 서 론

정보 유통시 안정성과 신뢰성 확보를 위해 공개키 암호 기술을 적용한 인증서 기반의 공개키 기반 구조(PKI: Public Key Infrastructure)가 현재 각종 분야에 가장 보편화되어 있는 방법이다. PKI에서는 사용자의 신상정보와 공개키를 확인할 수 있도록 제 3자인 인증기관(CA: Certificate Authority)으로부터 인증서를 발급 받는다. 그러나 기존의 잦은 인증서 발급으로 통화량의 증가와 비용 및 시간의 소모, 키 관리 등 복잡한 문제가 발생하고 있다. 따라서 사용자간에 실질적인 통신시 제 3자의 신뢰기관의 접촉 없이 독립적으로 안전한 사용자 인증 및 키 분배가 가능한 시스템에 대한 연구가 필요하다[1].

현재의 무선 PKI 프로토콜에서는 라우터 최적화, Ingress 필터링, 이동노드의 이동 관리와 데이터 전송 기법 등과 같은 기술적인 문제와 구현상의 문제들이 여전히 남아 있다. 그러나 무선 PKI의 가장 큰 당면 과제는 상호인증 문제이다. 모든 통신에서 상호인증 문제는 필수적으로 해결해야 할 부분이다. 무선 PKI에서도 전자상거래, 데이터통신, 전자메일 등 다양한 서비스가 원활하게 제공되기 위해서는 상호인증 문제가 해결되어야 한다. 특히 인터넷에서 사용 중인 다양한 인증구조들과 무선 PKI가 공존할 수 있도록 하기 위한 연구가 계속 진행되고 있다. 무선 PKI의 보안성을 증대시키기 위해서는 강력한 인증절차와 데이터 보호를 위한 상호 인증기능이 필요하다. 무선 PKI에서는 호스트들의 이동성 지원을 위해 무선 환경을 사용하게 되므로 무선 환경에 적합한 인증 프로토콜이 구축되어야 한다.

Ⅱ. 기존 무선 PKI 인증 알고리즘

비밀키를 기반으로 하는 현재의 무선 PKI 인증은 확장이 힘들다는 단점이 있다. 또한 전자상거래에서 중요한 부인봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Sufatrio, K. Lam[2]은 공개키 기반의 인증방법을 제안하였다.

2.1 인증 알고리즘

기존 프로토콜은 아래와 같은 절차로 진행된다.

(1) 에이전트 광고

(AA) : Agent → MN :

M_1 , $<< M_1 >> K^{-1}_{Agent}$, $Cert_{Agent}$

M_1 = [Advertisement , $Agent_{ID}$, MN_{COA}]

(2) 인증 과정

[단계 1]

MN → Agent : M_2 , $< M_2 > S_{MN-Agent}$

M_2=[Request, $Agent_{ID}$, $Server_{ID}$, MN_{HM}, MN_{COA} , N_{Server}, N_{MN},

[message in AA]]

[단계 2]

Agent → Server : [message in step 1] , N_{Agent}

[단계 3]

Server : (upon receipt of step 2)

- validate $< M_2 > S_{MN-Server}$ using $S_{MN-Server}$
- check whether $Agent_{ID}$ in AA1 = $Agent_{ID}$ in M_2
- validate $Cert_{Agent}$ based on existing PKI at $Server$
- validate $<< M_1 >> K^{-1}_{Agent}$ using authenticated K_{Agent}

[단계 4]

Server → Agent : M_3 , $<< M_3 >> K^{-1}_{Server}$, $Cert_{Server}$

M_3 = M_4 , N_{Agent}

M_4 = [Reply, Result, $Agent_{ID}$, $Server_{ID}$, MN_{HM}, N'_{Server}, N_{MN}, $<M_4>$ $S_{MN-Server}$]

[단계 5] : Agent

- validate N_{Agent}
- validate $Cert_{Server}$ based on existing PKI at $Agent$
- validate $<<M_3>> K^{-1}_{Server}$ using authenticated K_{Server}
- log this message as a proof of serving MN(perhaps used in conjunction with the billing protocol)

[단계 6]

Agent → Server → CA : 인증서 검증요구

[단계 7]

CA → Server → Agent : (upon receipt of step 6)

- Agent에게 인증서 유효성을 통보

[단계 8]

CA → Server → Agent → MN : 신뢰 정보

III. 무선 PKI 인증구조

상호인증을 구현하기 위해 새로운 무선 PKI 기반의 인증구조를 제안하고자 한다. 제안한 무선 PKI 인증구조의 인증구조는 CA, 서버, 에이전트 그리고 모바일 노드로 이루어지고, 에이전트는 CA으로부터 필요한 정보를 획득한 후에 CA 역할을 수행할 수 있다. 특히, 새로운 무선 PKI 인증구조에서 상호 인증과정은 SRP[3] 프로토콜을 바탕으로 실행된다. SRP 프로토콜은 Diffie-Hellman 키 교환 방식에 기반 한 프로토콜로 서버와 에이전트 사이에 키 교환 설정단계에서 이산대수 문제를 이용하여 구성하고, 서버와 에이전트 사이에 상호인증은 해쉬함수를 이용하여 구성된다. 기존의 SRP는 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 새로운 무선 PKI 인증구조의 상호인증 과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다.

3.1 인증서 신청방법

(그림 3-1)은 모바일 노드의 초기 인증서 신청과정에서 모바일 노드가 에이전트와 서버를 경유하여 초기 인증서를 신청하는 과정을 나타낸 것이다.

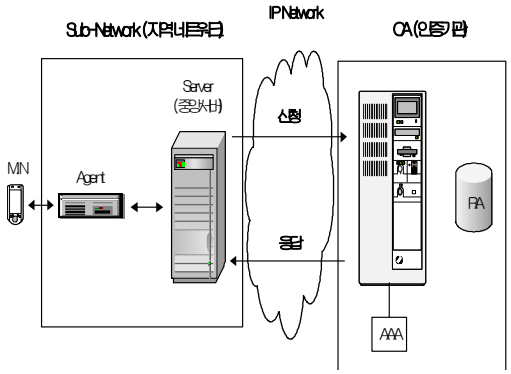

그림 3-1. 모바일 노드의 인증서 신청과정
Figure 3-1. Certificate request procedure of mobile node

3.2 상호 인증과정

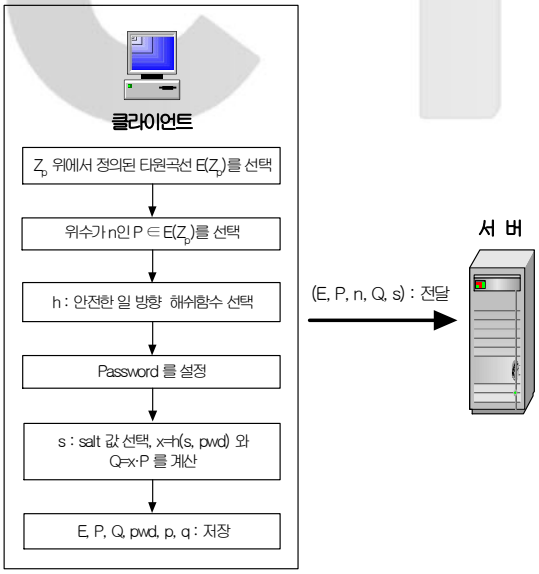

그림 3-2. 클라이언트와 서버간의 설정단계
Figure 3-2. Setup step between client and server

기존의 SRP는 키 교환 설정단계가 단순히 이산대수 문제에 근거하여 수행되었지만 새로운 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 상호 인증과정은 (그림 3-2)와 (그림 3-3)처럼 설정단계와 실행단계로 구성된다.

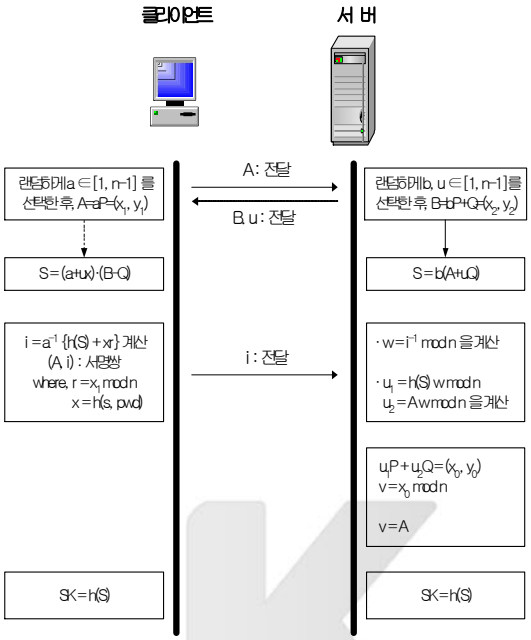

그림 3-3 클라이언트와 서버간의 실행단계
Figure 3-3 Execution step between client and server

3.3 OCSP를 이용한 인증서 갱신 과정

(그림 3-4)은 인증서 갱신과정을 나타낸 것이다. 인증서 갱신과정은 모바일 노드가 CA로부터 인증서를 발급 받은 후 모바일 노드가 정해진 포맷으로 OCSP 클라이언트에게 전자서명을 요청하면 OCSP 클라이언트는 정해진 포맷으로 OCSP 서버에게 인증서 상태정보를 검색하여 전자서명을 수행한 후 수행 결과에 대한 응답을 OCSP 클라이언트로 넘겨줌으로써 실시간으로 인증서에 대한 유효성 검사를 수행한다.

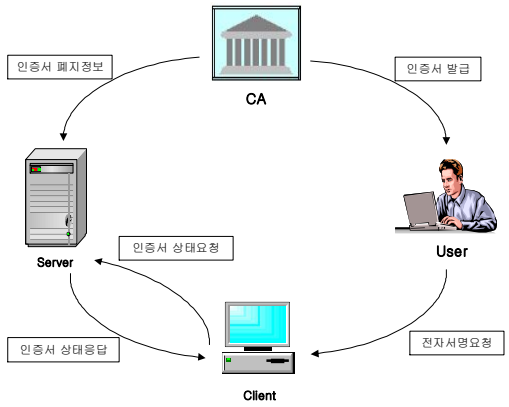

그림 3-4. OCSP 기반의 인증서 갱신과정
Figure 3-4. OCSP-based certificate renewal procedure

3.4 서명 및 검증과정

서명 및 검증방법은 ECDSA을 이용해서 하나는 공개키를 구성하고 또 하나는 비밀키를 구성하는데 사용되는 두 세트의 수 체계를 유도하는 작업이 수반된다.

비밀키는 공개키에 의해 암호화된 메시지를 복호화 할 때 사용된다. 발신자는 중앙의 관리자로부터 수신자의 공개키를 찾은 다음, 그 공개키를 사용하여 보내는 메시지를 암호화할 수 있다. 수신자는 그것을 받아서, 자신의 비밀키로 복호화하면 된다. 프라이버시를 확실하게 하기 위해 메시지를 암호화하는 것 외에도, 자신의 비밀키를 사용하여 디지털 서명을 암호화해서 함께 보냄으로써, 그 메시지가 틀림없이 바로 발신자에게서 온 것임을 수신자에게 확신시켜줄 수 있다.

전자서명 검증과정은 우선 수신자는 송신자의 메시지와 함께 전송된 인증서에 포함된 전자서명 검증키를 사용하여 수신된 전자서명으로부터 메시지 해쉬값을 복원 후 수신자가 생성한 메시지의 해쉬값을 서명자가 서명하여 전송한 해쉬값과 비교하여 서명자의 신원 및 메시지의 변조 여부를 확인한다.

3.5 핸드오버시 인증과정

공개키 기반 구조(PKI)를 사용하는 무선 환경의 사용자가 증가함에 따라 인증서 폐지 목록(CRL) 크기도 커질 것이며, 이는 곧 인증시간의 증가를 의미한다. 따라서 모바일 노드(MN)의 핸드오버시 인증과정에서 CRL를 매번 검색하는 것은 많은 시간이 소비되어 효율적인 무선 서비스를 제공할 수 없다. 따라서 모바일 노드의 인증과정에서 CRL 검색과정을 얼마만큼 빠르게 처리하는지가 효율적인 서비스 제공에 중요한 영향을 미치게 된다.

모바일 노드가 이동할 때 에이전트의 SNR(Signal to Noise Ratio)값이 기준치 이하로 떨어지면 새로운 에이전트를 찾기 위하여 스캐닝을 시작하며 가장 큰 SNR을 갖는 에이전트를 선택한다. 이동할 에이전트를 결정한 후에는 모바일 노드와 이동할 에이전트간에 인증과정이 수행된다. 이전 에이전트와 이동할 에이전트는 이미 상호인증을 수행한

신뢰할 수 있는 객체들이기 때문에 이전 에이전트가 수행한 모바일 노드에 대한 인증과정이 끝나기 전까지는 이전 에이전트와 세션을 계속 유지한다. 지역 내에서 핸드오버 할 경우에 에이전트는 OCSP를 통해서 모바일 노드 인증서의 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 모바일 노드에게 서비스를 제공하고 있는 에이전트에게 사용자 인증 무효를 통보한다. 따라서 모바일 노드의 핸드오버시 인증과정에서 CRL 검색에 소요되는 시간만큼 모바일 노드에게 빠른 핸드오버를 제공할 수 있게 된다. 이때 사용자 인증은 에이전트와 모바일 노드간에 인증서를 통해 획득한 공개키를 사용하기 때문에 완전인증에 대응하는 안전한 인증과정을 수행하게 된다. (그림 3-5)은 지역 내에서 핸드오버시 인증과정을 나타낸다.

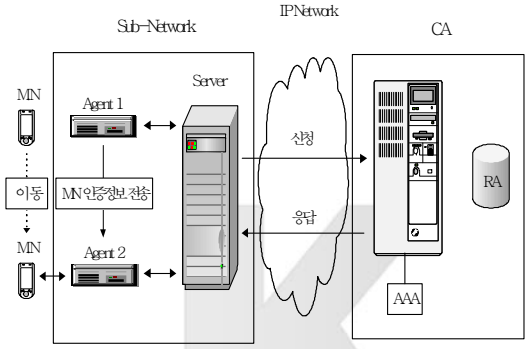

그림 3-5. 지역 내 핸드오버 과정
Figure 3-5. The intra-domain hand-over

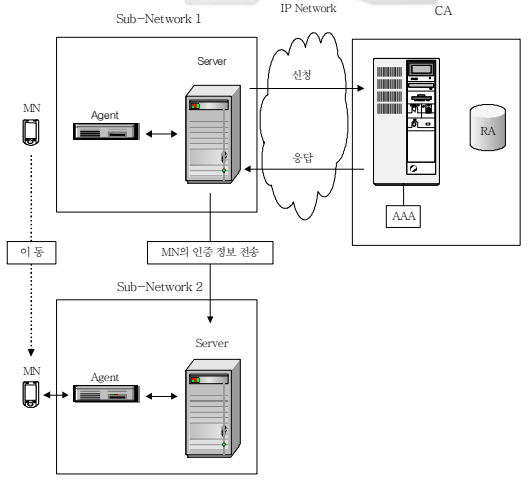

그림 3-6. 지역 간 핸드오버 과정
Figure 3-6. The extended inter-domain hand-over

지역 간에서 핸드오버 할 경우에 서버는 OCSP를 통해서 에이전트의 인증서 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 에이전트에게 서비스를 제공하고 있는 서버에게 사용자 인증무효를 통보한다. 따라서 에이전트의 핸드오버시 인증과정에서 CRL 검색에 소요되는 시간만큼 에이전트에게 빠른 핸드오버를 제공할 수 있게 된다. (그림 3-6)은 지역 간에서 핸드오버시 인증과정을 나타낸 것이다.

Ⅳ. 실험 및 성능분석

4.1 실험

본 논문에서 제안한 무선 PKI 구조의 성능 평가를 위해, 기존에 제시한 Sufatrio, K. Lam 인증 알고리즘과 핸드오버시 인증 대기시간에 관한 성능을 비교·분석하였다.

성능 분석을 위해서 버퍼 관리 기법은 [5]에서 사용한 기법 중 TAIL 기법을 이용하였으며, 이 경우 버퍼에 패킷을 수용할 확률을 정의하는 함수 $\alpha(k)$는 1이며, k는 $0 \le k \le B-1$이다. 여기서 k는 큐에서 대기중인 핸드오버 호의 개수를 의미하고, B는 각 노드에서의 버퍼의 크기이다.

핸드오버시 인증대기시간을 분석하기 위하여 현재의 셀 내에 할당된 전체 무선 채널의 개수가 C개, 핸드오버 호의 발생율을 λ라하고, 무선 채널의 서비스율을 μ, 그리고 큐에서의 서비스 방법을 FIFO라 가정한다. 또한 버퍼에 패킷이 도착하는 시간 간격과 패킷이 서비스를 받는 시간은 모든 패킷이 동일하다고 가정한다. 또한 버퍼에 있는 패킷은 (그림 4-1)와 같은 마코프 체인 중 birth-death 프로세스를 따른다.

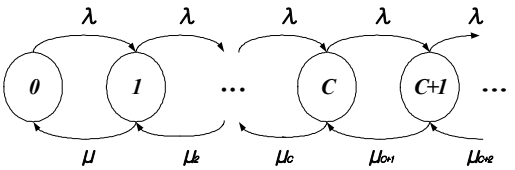

그림 4-1 시스템의 상태 천이도
Figure 4-1 Movement of system

즉, 패킷은 상태 k에서 $\lambda\alpha(k)$의 속도로 발생되고, μ ($k \neq 0$이라면)의 속도로 소멸된다. 여기서 상태 k는 큐에서 대기중인 핸드오버 호의 개수를 의미한다. 따라서 버퍼 내용의 정상 분포는 다음과 같이 계산한다.

$$\pi(k) = \pi(0)\,\rho^{k} \prod_{i=0}^{k-1} \alpha(i) \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (4\text{-}1)$$

여기서,

$$\pi(0) = \left[\sum_{k=0}^{B} \rho^{k} \prod_{i=0}^{k-1} \alpha(i) \right]^{-1} \quad \cdots\cdots\cdots\cdots \quad (4\text{-}2)$$

따라서, 각 노드의 큐에 n개의 패킷이 있다면, 각 노드의 큐에서 기대되는 핸드오버시 인증 대기시간은 다음과 같이 계산한다.

$$D = \frac{1}{\mu} \sum_{k=0}^{B-1} (1+k)\,\pi(k)\,\alpha(k) \quad \cdots\cdots \quad (4\text{-}3)$$

4.2. 핸드오버시 인증 대기시간

공개키 기반 구조(PKI)를 사용하는 무선 환경의 사용자가 증가함에 따라 인증서 폐지 목록(CRL)의 크기도 커질 것이며, 이는 곧 인증시간의 증가를 의미한다. 따라서 모바일 노드(MN)의 핸드오버시 인증과정에서 CRL를 매번 검색하는 것은 많은 시간이 소비되어 효율적인 무선 서비스를 제공할 수 없다. 따라서 모바일 노드의 인증과정에서 CRL 검색과정을 얼마만큼 빠르게 처리하는지가 효율적인 서비스 제공에 중요한 영향을 미치게 된다.

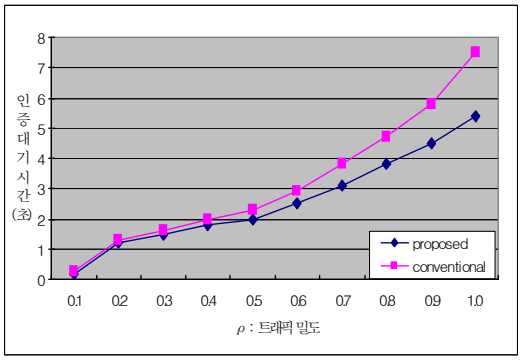

그림 4-2. 핸드오버시 인증 대기시간(B=10)
Figure 4-2. Certificate waiting time in hand-over

(그림 4-2) 트래픽 밀도 ρ값에 따른 핸드오버시 기존 알고리즘의 인증 대기시간과 제안한 인증시간 단축을 위한 무선 PKI 구조의 핸드오버시 인증 대기시간과 비교한 결과를 보여준다. 버퍼의 크기가 10일 때 트래픽 밀도 ρ값에 따른 각 노드에서의 핸드오버시 인증 대기시간을 나타낸다.

V. 결 론

본 논문에서 제안한 인증구조에서 핸드오버시 인증 대기시간은 트래픽 밀도가 증가함에 따라 인증대기시간도 증가함을 알 수 있다. 그러나 제안한 방법에서 핸드오버시 방식을 사용하였을 경우 트래픽 밀도가 0.5일 때까지는 인증 대기시간이 기존의 알고리즘과 별 차이가 없다가 트래픽 밀도가 0.5이상 일 때부터 인증 대기시간의 차이가 뚜렷한 차이를 보인다는 것을 알 수 있다.

기존 알고리즘과 제안한 인증구조를 비교하여 실험해 보았을 때 호 도착율, 큐의 서비스율, 큐 사이즈 변화에 관계없이 제안한 인증 기법이 모든 환경에서 기존 알고리즘보다 우수한 성능을 보였다. 무선 PKI에서 핸드오버시 여러 가지 인증문제점이 있다. 이러한 원인을 해결해야할 문제점들이 향후 연구되어야 할 것이다.

참고문헌

[1] R. Anderson and T. Lomas, "Fortifying Key negotiation schemes with poorly chosen passwords," Electronics Letters, 1994, Vol. 30, No. 13.

[2] Sufatrio, K. Lam, "Mobile IP Registration Protocol : A Security Attack and New Secure Minimal Public-Key Based Authentication," I-SPAN'99, June 1999..

[3] Thomas Wu, "The Secure Remote Password Protocol", Internet Society Symp., Network and Distributed Systems Security Symposium, 1998, pp. 97-111.
[4] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, Internet X.509 Public Key Infrastructure On-line Certificate Status Protocol-OCSP," RFC2560, 1999.
[5] S. Bellovin and M. Merritt, Augmented Encrypted Key Exchange", in Proceedings of the First ACM Conference on Computer and Communication Security, pp. 244-250, 193.
[6] 이재영, 이지영, "디지털서명과 은닉에관한연구", OA 학회, 제5권 3호, 2000, 9.
[7] 고병수, 장재혁, 최용락, "디지털 콘텐츠 유통 및 보호를 위한 인증 시스템 설계 및 구현". OA학회, 제8권 3호, 2003.

저 자 소 개

신 승 수

2001년 2월 충북대학교 수학과 이학박사
2003년 9월 ~ 현재 목원대학교 겸임교수

서 정 만

2003년 2월 충북대학교 컴퓨터공학과 공학박사
2002년 ~ 현재 한국재활복지 대학 컴퓨터게임개발과 교수