무선 PKI에서의 블러킹 확률 분석

정회원 신 승 수, 최 승 권*, 지 홍 일*, 신 동 화*, 조 용 환*

Analysis of the Blocking Probability for Wireless PKI

Shin Seung-Soo, Choi Seung Kwon*, Ji Hong-Il*,
Shin Dong-Hwa*, Cho Yong-Hwan** ***Regular Members***

요 약

본 논문에서는 기존의 무선 PKI(Public Key Infrastructure)에서 개선되어야 할 여러 가지 사항 중에서 핸드오버시 인증서 획득시간을 단축하기 위한 새로운 인증구조에서의 블러킹 확률 분석을 알아보고자 한다. 기존의 키 교환방식에서 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 인증서 시간단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 제안한 무선 PKI 구조 안에서의 핸드오버 방법과 블러킹 확률 분석에 대하여 알아보았다. 핸드오버 방법은 CRL(Certification Revocation List) 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.

Key Words : mobile PKI, FIFO, Blocking Probability, CRL, SRP

ABSTRACT

this paper, we made out blocking probability analysis for a new authentication structure for reducing the certificate acquisition time which is one of the factors that should be improved in a conventional wireless PKI. 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. Besides, we proposed advanced handover method and blocking probability analysis for wireless PKI. 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

Ⅰ. 서 론

정보 유통시 안정성과 신뢰성 확보를 위해 공개키 암호기술을 적용한 인증서 기반의 공개키 기반구조(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 신뢰기관

동명정보대학교 정보보호학과, * 충북대학교 전기전자컴퓨터공학부(yhcho@chucc.chungbuk.ac.kr), 교신저자
논문번호 : 2004-07-090, 접수일자 : 2004년 7월 8일
※본 연구는 정보통신기초기술연구지원사업의 연구비 지원에 의하여 연구되었음.

의 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 [2-4]. 무선 PKI의 보안성을 증대시키기 위해서는 강력한 인증절차와 데이터 보호를 위한 상호 인증 기능이 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 부인 봉쇄 서비스를 제공할 수 없다. 따라서 이러한 문제점을 해결하기 위하여 Sufatrio, K. Lam[5]은 공개키 기반의 인증방법을 제안하였다.

2.1 인증 알고리즘

표 2-1은 Sufatrio, K. Lam의 공개키 기반의 인증구조를 설명하기 위한 기본적인 용어를 나타낸 것이다.

기존 프로토콜은 아래와 같은 절차로 진행된다.

- 에이전트 광고 :

(AA) : Agent → MN :

$$M_1, \ll M_1 \gg K_{Agent}^{-1}, \ Cert_{Agent}$$

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

- 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 $\ll M_1 \gg K_{Agent}^{-1}$ using authenticated K_{Agent}

▪ 단계 4

: Server → Agent : M_3, $\ll M_3 \gg$

표 2-1. 기존 프로토콜의 용어

CA	인증기관
K_{Agent}, K_{Server} K_{CA}	에이전트, 서버 그리고 CA의 공개키
K_{Agent}^{-1} K_{Server}^{-1} K_{CA}^{-1}	에이전트, 서버 그리고 CA의 비밀키
$Cert_{Agent}$, $Cert_{Server}$	에이전트, 서버의 인증서
$\ll M \gg K_A^{-1}$	A의 비밀키를 사용한 메시지 M의 디지털 서명
N_{Agent}	에이전트에서 발행한 nonce
N_{Server}, N_{Agent}, N_{MN}	서버, 에이전트 그리고 모바일 노드의 nonce
MN_{HM}	모바일 노드의 홈 주소
MN_{COA}	모바일 노드의 Care-Of-Address
$Server_{ID}$, $Agent_{ID}$	서버와 에이전트의 IP 주소
$S_{MN-Server}$	모바일 노드와 서버의 비밀키
Advertisement	광고 메시지를 나타내는 비트 패턴

K_{Server}^{-1}, $Cert_{Server}$

$M_3 = M_4$, 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 $<< M_3 >> K_{Server}^{-1}$ 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

다음의 그림 2-1은 상기의 알고리즘을 단계별로 도식화한 흐름도이다.

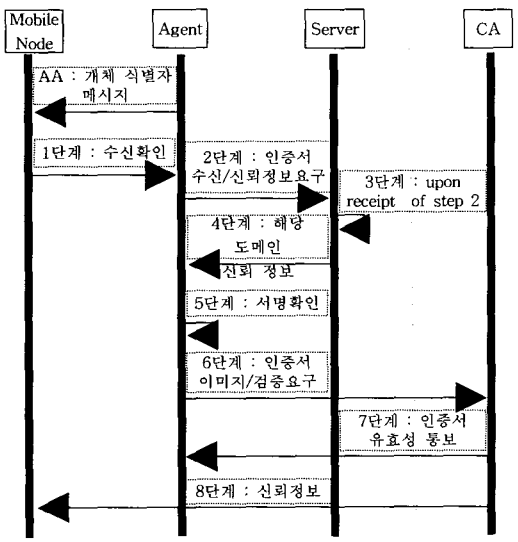


그림 2-1. 기존 알고리즘의 흐름도

Ⅲ. 인증시간 단축을 위한 무선 PKI

본 논문에서는 상호인증을 구현하기 위해 인증시간을 단축하기 위한 무선 PKI 기반의 인증구조를 제안하고자 한다. 제안한 무선 PKI 인증 구조는 타원곡선 알고리즘의 적용, OCSP의 사용, 새로운 상호인증과 핸드오버시 인증과정을 적용하여 인증시간을 단축하면서 안전성과 서비스의 안정성을 높일 수 있는 방법을 제시하였다. 제안한 무선 PKI 인증구조의 인증구조는 CA, 서버, 에이전트 그리고 모바일 노드로 이루어지고, 에이전트는 CA으로부터 필요한 정보를 획득한 후에 CA 역할을 수행할 수 있다. 특히, 인증서 시간단축을 위한 무선 PKI 인증구조에서 상호 인증과정은 SRP(Secure Remote Password) [6] 프로토콜을 바탕으로 실행된다. SRP 프로토콜은 Diffie-Hellman 키 교환 방식에 기반 한 프로토콜로 서버와 에이전트 사이에 키 교환 설정 단계에서 이산대수 문제를 이용하여 구성하고, 서버와 에이전트 사이에 상호인증은 해쉬함수를 이용하여 구성된다.

기존의 SRP는 키 교환 설정단계가 단순히 이산대수문제에 근거하여 수행되었지만 제안한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 안전성을 높이기 위하여 타원곡선을 적용하였다. 상호 인증과정은 설정단계와 실행단계로 구성된다.

3.1 인증서 신청방법

서브네트워크 안에 있는 서버와 CA사이에 항상 서로 신뢰관계가 있다고 가정한다. 모바일 노드가 인증서를 신청할 때 신청과정은 다음과 같다.

MN ⇒ Agent ⇒ Server ⇒ CA

CA가 인증서를 발급할 때 발급과정은 다음과 같다.

CA ⇒ Server ⇒ Agent ⇒ MN

CA가 응답을 하면 CA안에 저장된 모바일 노드의 정보 중에서 필요한 인증서 정보를 서버와 에이전트를 경유하여 모바일 노드에게 전달한다. 여기서, 에이전트와 서버는 상위기관으로부터 발급 받은 인증서 1부를 저장하여 보관한다. 만약 인증서 유효기간 동안에 모바일 노드가 인증서를 재 신청할 때에는 CA까지 보내지 않고 에이전트에서 인증서 사본을 발급 받는다. 발급된 인증서 유효기간 동안 서버

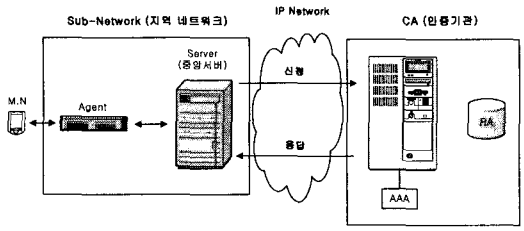


그림 3-1. 모바일 노드의 인증서 신청과정

나 에이전트가 CA의 역할을 수행할 수 있다.

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

3.2 상호 인증과정

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 이산대수 문제에 근거하여 수행되었지만 인증서 획득시간 단축을 위한 무선 PKI 인증구조의 상호인증과정에서는 키 교환 설정단계에서 타원곡선을 적용하였다. 상호 인증과정은 그림 3-2와 3-3처럼 설정단계와 실행단계로 구성된다.

3.3 OCSP를 이용한 인증서 갱신 과정

OCSP(Online Certificate Status Protocol)는 CRL (Certification Revocation List) 기반의 인증서 검증 방식의 문제점인 인증서에 대한 실시간 상태검증을 할 수 없는 것을 해결하기 위해 제안된 인증서 상태 검증방식으로 1999년 6월 IETF RFC2560 문서에 의해 공포되었다[7].

OCSP 기반의 인증서 검증방식은 OCSP 클라이언트(에이전트)가 CRL을 요청하지 않고 인증서의 현재 상태를 검증하기 때문에 실시간으로 인증서에 대한 상태검증을 할 수 있다는 장점이 있는 반면 실시간으로 인증서에 대한 유효성 검사를 수행해야 하기 때문에 많은 통신량으로 인한 네트워크 과부하 문제를 발생시킨다는 것과 네트워크 상태에 따라 인증서 유효성 검사의 수행시간이 달라진다는 단점이 있다.

OCSP 인증서 상태 검증방식은 클라이언트가 인증서 검증 작업을 수행하기 위한 인증서를 저장한 장소 URL에게 인증서 검증을 요청하고 그 결과만 클라이언트가 받아 작업을 수행하는 방식이다. 클라이언트는 받은 인증서를 OCSP 서버에게 보내서 그 인증서의 정확성 여부를 묻게 된다. 그러면 OCSP 서버가 해당하는 인증서의 검증작업을 해서 클라이언트에게 인증서의 정확성 여부를 알려 주게 된다.

그림 3-4은 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.

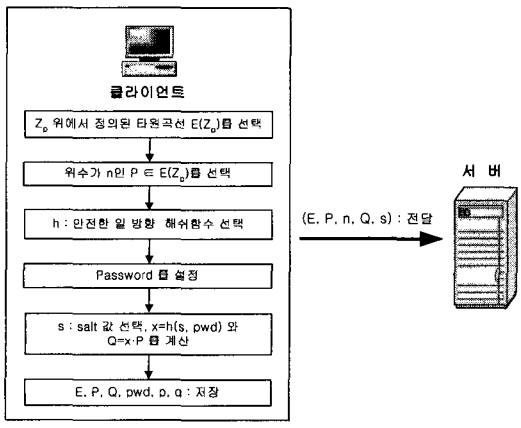


그림 3-2. 클라이언트(에이전트)와 서버간의 설정단계

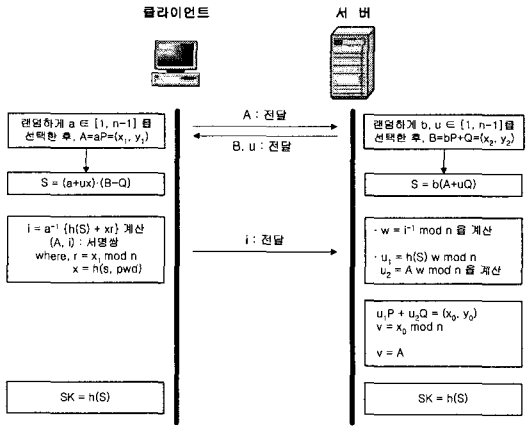


그림 3-3. 클라이언트(에이전트)와 서버간의 실행단계

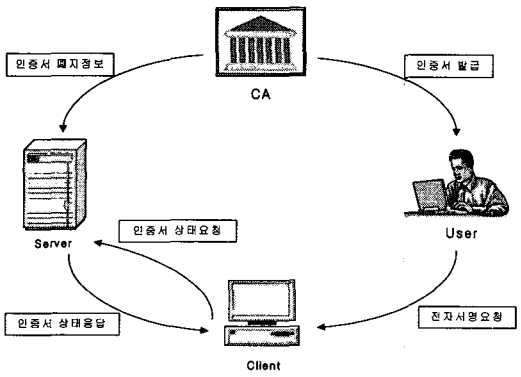


그림 3-4. OCSP 기반의 인증서 갱신과정

3.4 서명 및 검증과정

서명 및 검증방법은 ECDSA(Elliptic Curve Digital Signate Algorithm)을 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.

그림 3-5은 전자서명 과정을 나타낸 것이다.

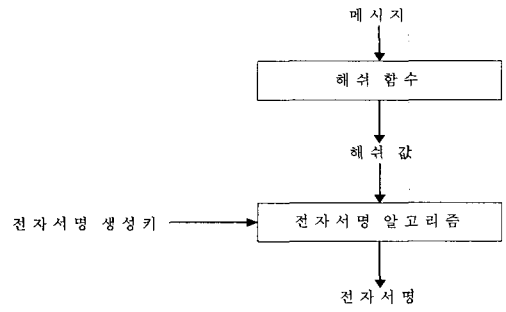


그림 3-5. 전자서명 과정

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. 이와 같은 절차를 수식으로 정리하면 다음과 같다.

다음 그림은 전자서명 검증과정을 나타낸 것이다.

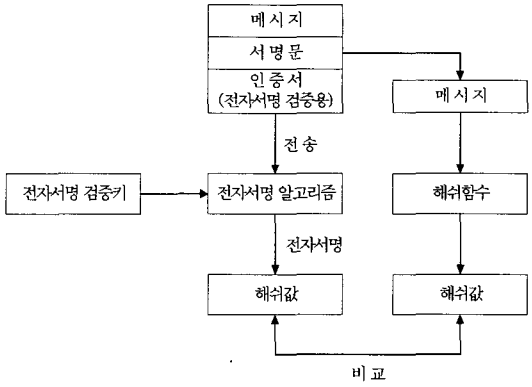


그림 3-6. 전자서명 검증과정

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 핸드

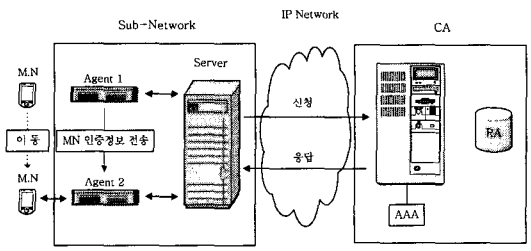


그림 3-7. 지역 내 핸드오버 과정

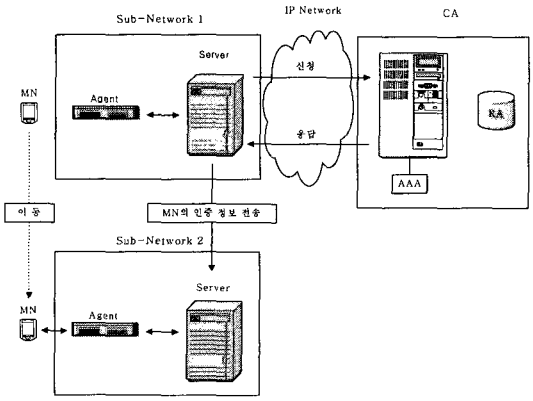


그림 3-8. 지역 간 핸드오버 과정

오버를 제공할 수 있게 된다. 이 때 사용자 인증은 에이전트와 모바일 노드간에 인증서를 통해 획득한 공개키를 사용하기 때문에 완전인증에 대응하는 안전한 인증과정을 수행하게 된다. 그림 3-7은 지역 내에서 핸드오버시 인증과정을 나타낸다.

지역 간에서 핸드오버 할 경우에 서버는 OCSP를 통해서 에이전트의 인증서 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 에이전트에게 서비스를 제공하고 있는 서버에게 사용자 인증 무효를 통보한다. 따라서 에이전트의 핸드오버시 인증과정에서 CRL 검색에 소요되는 시간만큼 에이전트에게 빠른 핸드오버를 제공할 수 있게 된다. 그림 3-8은 지역 간에서 핸드오버시 인증과정을 나타낸 것이다.

Ⅳ. 실험 및 성능분석

4.1 실 험

본 논문에서 제안한 무선 PKI 구조의 성능 평가를 위해, 기존에 제시한 Sufatrio, K. Lam 인증 알고리즘과 핸드오버시 인증 대기시간 그리고 핸드오버시 블러킹 확률 등 두 가지 측면에서 성능을 비교·분석하였다. 실험에 사용된 망의 토폴로지는 2개의 서버와 다수의 에이전트, MN이 트리의 형태로 존재하는 단일망으로 가정한다.MN의 이동 속도 등은 가정하지 않고 다만 호의 도착율을 정의하여 핸드오버를 요청하는 단말의 분포를 정의하여 실험에 사용하였다.

두 가지 측면에서 성능 분석을 위해서 버퍼 관리 기법은 [8]에서 사용한 기법 중 TAIL 기법을 이용하였으며, 이 경우 버퍼에 핸드오버 요청 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 인증 대기시간을 구하기 위한 버퍼관리 기법은 FIFO(First-In-First-Out)로 가정한다.

FIFO에 대한 큐잉 모델은 다음과 같다.

여기서, 핸드오버시 인증 대기시간의 성능 평가를 위해 사용하는 기호와 정의는 다음과 같이 가정한다.

- λ : 큐에 도착하는 핸드오버 요청 패킷의 도착율(포아송 분포)
- μ : 임의의 서비스를 받고 출력되는 핸드오버 요청 패킷의 서비스율(지수분포)
- B : 각 노드에서의 버퍼의 크기
- C : 서버의 개수
- 시스템에 제공되는 트래픽 밀도 ρ는 다음과 같다.

$$\rho = \frac{\lambda}{\mu}$$

핸드오버시 블러킹 확률을 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 핸드오버 요청 패킷이 도착하는 시간 간격과 패킷이 서비스를 받는 시간은 모든 패킷이 동일하다고 가정한다. 또한 버퍼에 있는 패킷은 그림 4-1와 같은 마코프 체인 중 birth-death 프로세스를 따른다.

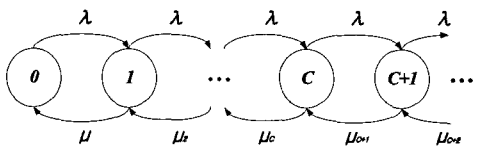


그림 4-1. 시스템의 상태 천이도

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

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

여기서,

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

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

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

핸드오프시 블러킹 확률을 구하기 위한 실험은 λ, μ, B 값을 변경하면서 결과를 분석하였다. 실험에 사용된 파라미터는 다음과 같다.

표 4-1. 실험에 사용된 파라미터

기호	정 의	값
λ	호 도착율	10
μ	서비스율	10
B	버퍼 사이즈	50,60,70
C	서버 수	2
N_{agent}	서버당 에이전트 수	5
N_{MN}	에이전트당 MN 수	5
BW_w	유선 링크의 대역폭	1Gbps
BW_{wl}	무선 링크의 대역폭	1Mbps
T_{wait}	MN이 핸드오버 중 발생되는 평균 패킷 인증시간	400ms

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 검색 과정을 얼마만큼 빠르게 처리하는지가 효율적인 서비스 제공에 중요한 영향을 미치게 된다.

그림 4-2은 트래픽 밀도 ρ값에 따른 핸드오버시 기존 알고리즘의 인증 대기시간과 제안한 인증시간 단축을 위한 무선 PKI 구조의 핸드오버시 인증 대기시간과 비교한 결과를 보여준다. 버퍼의 크기가 50일 때 트래픽 밀도 ρ값에 따른 각 노드에서의 핸드오버시 인증 대기시간을 나타낸다.

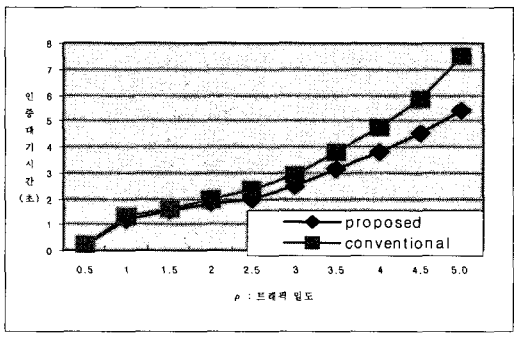


그림 4-2. 트래픽 밀도 ρ 값에 따른 각 노드에서의 핸드오버시 인증 대기시간(B=50)

그림 4-2에 나타난 바와 같이 핸드오버시 인증 대기시간은 트래픽 밀도가 증가함에 따라 인증 대기시간도 증가함을 알 수 있다. 그러나 제안한 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.

4.3 핸드오버시 블러킹 확률

제안한 인증구조에서 핸드오버시 블러킹 확률을 분석하기 위하여 다음과 같이 가정한다. 현재의 셀 내에 할당된 전체 무선 채널의 개수가 C개, 핸드오버 호의 발생률을 λ라하고, 무선 채널의 서비스율을 μ, 그리고 큐에서의 서비스 방법을 FIFO라 가정할 때 셀에서의 상태 천이도는 앞의 그림 4-1와 같다. 셀에서의 상태가 평형상태에 도달했을 때 셀의 상태가 k일 확률 P_k는 마코프 체인 중 birth-death 프로세스에 의해 구하면 식 4-4와 같다.

$$P_k = \begin{cases} \frac{\rho^k}{k!}P_0 & (1\le k\le C-1) \\ \frac{\rho^k}{C!\,C^{k-C}}P_0 & (C\le k) \end{cases}$$

$$P_0 = \left\{ \sum_{C=1}^{k=0} \frac{\rho^k}{k!} + \sum_{k=C}^{\infty} \frac{\rho^k}{C!\,C^{k-C}} \right\}^{-1} = \left\{ \sum_{k=0}^{C-1} \frac{\rho^k}{k!} + \frac{1}{C!}\rho^C \frac{C}{C-\rho^k} \right\}^{-1} \quad (4\text{-}4)$$

핸드오버 호의 블러킹 확률은 큐에서의 대기시간이 감마분포를 따르는 핸드오버 지속시간보다 클 확률이다. 확률변수 T_q를 큐에서 대기하는 시간을 나타내는 변수라고 하면,

$$W_q(t) = P_\Gamma[T_q \le t] = \sum_{k=c}^{\infty} [P_\Gamma\{k-c+ \mid completions \le t \mid arrival\ found\ k\ in\ system\}P_k] + W_q(0) \quad (4\text{-}5)$$

여기서 $W_q(0) = P_\Gamma[C-1\ or\ less\ in\ system]$을 나타내며 식 4-6과 같다.

$$W_q(0) = \sum_{k=0}^{C-1} = 1 - \sum_{k=C}^{\infty} \frac{\rho^k}{C!\,C^{k-C}} P_0 = 1 - \frac{\rho^C C}{C!(C-\rho)} P_0 \quad (4\text{-}6)$$

$k \ge C$일 때에는 시스템의 평균 서비스율을 평균이 C_μ인 포아송 분포를 따르므로 채널을 종료하는 호들의 시간간격은 평균이 $1/C_\mu$인 지수분포를 따르고 $(k-C+1)$개의 호가 종료하는데 소요되는 시간의 분포는 $(k-C+1)$ type의 Erlang 분포를 따른다. 따라서 $W_q(t)$는 식 4-7과 같이 산출된다.

$$W_q(t) = P_0 \sum_{k=C}^{\infty} \frac{\rho^k}{C!\,C^{k-C}} \int_0^t \frac{\mu C(\mu C x)^{k-c}}{(k-C)!} e^{-\mu C x} dx + W_q(0) \quad (t>0)$$
$$= P_0 \rho^C \frac{1}{(C-1)!} \int_0^t \mu e^{-\mu C x} \sum_{k=C}^{\infty} \frac{(\lambda_k x)^{k-C}}{(k-C)!} dx + W_q(0)$$
$$= 1 - P_0 \rho^C \frac{e^{-(\mu C - \lambda_k)t}}{(C-1)!(C-\rho)} \quad (4\text{-}7)$$

핸드오버 지속시간을 나타내는 확률변수가 T_h이므로 핸드오버 호의 블러킹 확률 P_{Bh}는 식 4-8과 같이 산출된다.

$$P_{Bh} = 1 - W_q(T_h) = 1 - P_\Gamma[T_q \le T_h] = 1 - \int_0^\infty W_q(t) f_{\Gamma_h}(t)\, dt \quad (4\text{-}8)$$

여기서 $f_{\Gamma_h}(t)$는 식 4-9로 주어지는 감마분포의 확률밀도함수를 나타내며, 위 적분값은 수치 해석적인 방법을 이용하여 산출한다.

$$f_{\Gamma_h}(t) = \frac{\beta^{-a} t^{a-1} e^{-t/\beta}}{\Gamma(a)} \quad (t>0) \quad (4\text{-}9)$$

여기서

$$\Gamma(x) = \int_0^\infty \tau^{x-1} e^{-\tau} d\tau, \quad a \approx \hat{a} = \frac{\{E[T_h]\}^2}{Var[T_h]}, \quad \beta \approx \hat{\beta} = \frac{VAR[T_h]}{E[T_h]}$$

이다.

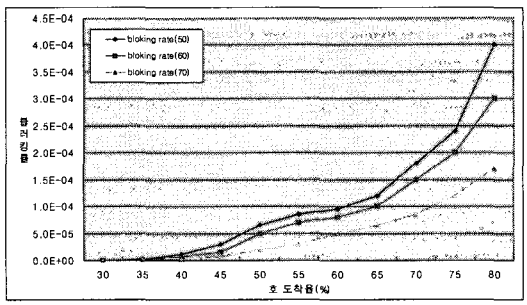


그림 4-3. 호 도착율의 변화에 따른 핸드오버 블러킹 실험결과

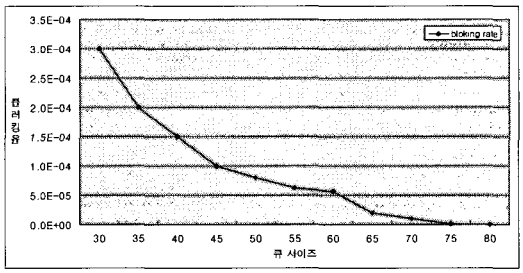


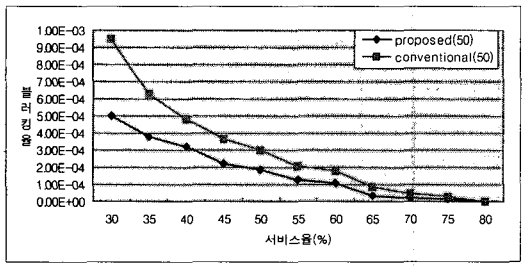
그림 4-4. 큐 사이즈의 변화에 따른 핸드오버 블러킹 실험결과

다음의 그림 4-3과 그림 4-4은 호 도착율의 변화에 따른 핸드오버 블러킹율과 큐 사이즈의 변화에 따른 핸드오버 블러킹율을 나타낸 것이다.

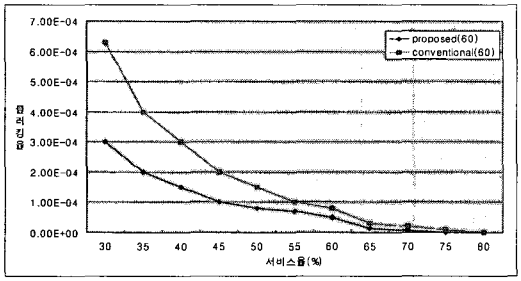
블러킹율은 처리율에 따른 버퍼에서의 대기시간과 관련이 있으며 처리율을 넘어서는 도착 호에 대

해서는 버퍼가 오버플로우 하게 되므로 블러킹이 발생하게 된다. 따라서 호 도착율이 증가함에 따라 블러킹율은 이에 비례하여 증가한다. 큐 사이즈 또한 블러킹율과 관련이 있으며 큐 사이즈가 크면 대기할 수 있는 핸드오버 호의 수가 증가하므로 블러킹 확률이 낮아지게 된다.

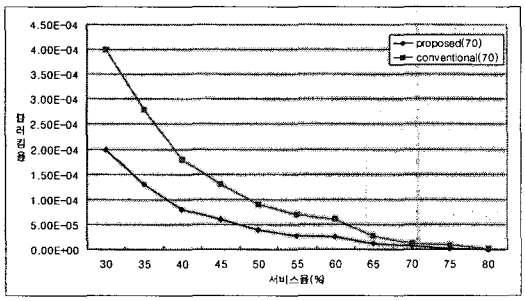
제안한 인증시간 단축을 위한 무선 PKI 구조 안에서의 핸드오버 방법은 CRL 검색시간을 단축시킬 수 있으므로 기존의 방법에 비하여 단축된 핸드오버 처리시간을 보여준다. 이에 따라 큐의 서비스율을 높일 수 있으며 이는 호의 블러킹 확률을 최소로 감소시켜줄 수 있다. 그림 4-5 (a), (b), (c)는 기존의 핸드오버시 인증방법을 이용할 경우와 제안한 핸드오버시 인증방법을 이용할 경우 블러킹율을 비교한 것이다.



(a) Queue size = 50인 경우



(b) Queue size = 60인 경우



(c) Queue size = 70인 경우

그림 4-5. 시스템 서비스율에 따른 블러킹율

V. 결 론

본 논문에서 제안한 인증구조에서 핸드오버시 인증 대기시간은 트래픽 밀도가 증가함에 따라 인증 대기시간도 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 0.5이상일 때부터 인증 대기시간의 차이가 뚜렷한 차이를 보인다는 것을 알 수 있다.

핸드오버시 블러킹율은 처리율에 따른 버퍼에서의 대기시간과 관련이 있으며 처리율을 넘어서는 도착 호에 대해서는 버퍼가 오버플로우하게 되므로 블러킹이 발생하게 된다. 따라서 호 도착율이 증가함에 따라, 또는 큐의 서비스율이 감소함에 따라 블러킹율은 이에 비례하여 증가한다. 큐 사이즈 또한 블러킹율과 관련이 있으며 실험에서는 큐 사이즈를 50, 60, 70으로 변화시키면서 블러킹율을 확인해 보았다. 실험 결과를 보면 큐 사이즈가 크면 대기할 수 있는 핸드오버 호의 수가 증가하므로 블러킹 확률이 낮아지게 됨을 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.

참 고 문 헌

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

[2] V.Boyko, P. Mackenzie, and S. Patel, "Probably Secure Password-Authenticated Key Exchange Using Diffie-hellman," advances in Cryptology-EUROCRYPT' 2000, pp. 156-171, 2000.

[3] M.Bellare, D. Pointcheval, and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks," advances in Cryptology-EUROCRYPT' 2000, pp.139-155, 2000.

[4] T. Kwon, and J. Song, "A Study on the Generalized Agreement and Password Authentication Protocol," IEICE TRANS.

COMMUN., Vol. E83-B, No.9, pp 2044-2050, SEP 2000.

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

[6] Thomas Wu, "The Secure Remote Password Protocol", Internet Society Symp., Network and Distributed Systems Security Symposium, 1998, pp. 97-111.

[7] 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.

[8] 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.

신 승 수(Shin Seung-Soo) 정회원
한국통신학회 논문지 제 26권 제 4A호 참조
현재 동명정보대학교 정보보호학과 교수

최 승 권(Choi Seung Kwon) 정회원
한국통신학회 논문지 제 25권 제 2A호 참조
현재 목원대학교 겸임교수

지 홍 일(Ji Hong-Il) 정회원
2002년 2월 충북대학교 컴퓨터공학과 대학원(공학석사)
현재 충북대학교 컴퓨터공학과 대학원(박사과정)
<관심분야> 멀티미디어통신, 네트워크

신 동 화(Shin Dong-Hwa) 정회원
2002년 2월 충북대학교 컴퓨터공학과 대학원(공학석사)
2005년 2월 충북대학교 컴퓨터공학과 대학원(공학박사)
현재 (주)아이온 커뮤니케이션즈 사원

조 용 환(Cho Yong-Hwan) 정회원

한국통신학회 논문지 제 23권 9호 참조
현재 충북대학교 전기전자 컴퓨터공학부 교수
<관심분야> .Net Framework, 멀티미디어통신, 트래픽공학, Mobile PKI, 정보통신정책