Mobile Ad Hoc Networks에서 효과적인 인증서비스

An Effective Authentication in Mobile Ad Hoc Networks

김윤호(Yoon-Ho, Kim)*

초 록

MANET(Mobile Ad Hoc Network)은 노드들의 자유적인 이동을 지원하고, 고정된 인프라에 의존하지 않으며, 신속한 네트워크 구축이 가능한 점 등 다양한 장점들이 있는 반면 보안에 있어서는 많은 문제점이 존재한다. 특히 보안에 있어서 기존의 전통적인 인증서비스는 안전성, 확장성, 가용성 등의 이유로 MANET 환경에는 적용하기 어렵다.

본 논문에서는 MANET상의 인증서비스에서 Secret Sharing방식과 Threshold Digital Signature방식을 이용하여 안전하고, 효과적인 분산 인증서비스를 제안하였다. 제안된 분산 인증서비스 방안에서는 MANET을 구성하고 있는 모바일 노드들 중 일정한 수량의 안전성이 비교적 높은 노드들을 특권노드로 설정하고, 이러한 특권노드들로부터 인증서 발급이 진행된다. 인증서발급의 역할을 특권노드들에게 부여한 분산 인증시스템은 기존의 Centralized Architecture, Hierarchical Architecture에서 노드 하나의 침해로 인해 네트워크 전체의 보안에 손상을 입히는 문제점을 해결하였으며, 개인키에 대한 부분 비밀정보들을 가지고 있는 노드의 수가 줄어들면서 기존의 Fully Distributed Architecture에서의 개인키 노출 위험성을 줄여준다.

네트워크 시뮬레이션을 통해서 제안한 인증서비스 방식의 성능, 가용성을 평가하였으며, 시스템 파라메타간의 관계를 분석하였다.

ABSTRACT

The MANET has many problems in security despite of its many advantages such as supporting the mobility of nodes, independence of the fixed infrastructure, and quick network establishment. In particular, in establishing security, the traditional certification service has many difficult problems in applying to the MANET because of its safety, expandability, and availability.

In this paper, a secure and effective distributed certification service method was proposed using the Secret Sharing scheme and the Threshold Digital Signature scheme in providing certification services in the MANET.

In the proposed distributed certification service, certain nodes of relatively high safety among the mobile nodes consisting of the MANET, were set as privileged nodes, from which the process of issuing a certification started. The proposed scheme solved problem that the whole network security would be damaged by the intrusion to one node in the Centralized Architecture and the Hierarchical Architecture. And it decreased the risk of the exposure of the personal keys also in the Fully Distributed Architecture as the number of the nodes containing the partial confidential information of personal keys decreased.

By the network simulation, the features and availability of the proposed scheme was evaluated and the relation between the system parameters was analyzed.

키워드 : 인증서, 인증서 갱신, 시뮬레이션
MANET(Mobile Ad Hoc Network), CA(Certificate Authority)

이 논문은 2004년도 상명대학교 교내연구비 지원에 의하여 연구되었음.

* 상명대학교 소프트웨어학부 부교수

1. 서 론

사용자들로 하여금 언제 어디서나 네트워킹 서비스를 가능하게 해 주는 MANET (Mobile Ad Hoc Network)에 대한 연구가 IETF(Internet Engineering Task Force)의 MANET 워킹그룹[1], Bluetooth[4], Home RF(Home Radio Frequency) 워킹그룹[5] 등에서 활발하게 진행되고 있다. MANET 기술은 순수한 모바일 노드들만으로 네트워크를 구성하는 모바일 환경 하에서의 새로운 무선 네트워킹 기술이다[11,18]. 전통적인 네트워크 시스템에서는 고정된 인프라가 설치되어 있으며 유선 랜 환경은 물론 무선 랜, 이동통신 등에서도 Access Point, Base Station 등과 같은 고정된 인프라가 설치되어 있다. 그러나 유선 기반 망을 설치하기 어려운 산간 지방 또는 빙하지역과 같은 오지나 혹은 지진, 홍수, 전쟁 등 재난으로 유선기반 망이 파괴된 지역에서의 신속한 통신 복구를 위해서는 네트워크를 신속하게 구축해 줄 수 있는 기술이 필요하다. 또한 한 빌딩 내에서 유선 기간 망이 필요 없이 자체 통신망을 구성할 필요성이 대두 되었으며, MANET은 이러한 환경 하에서 신속하게 네트워크를 구성해줄 수 있다는 장점을 가지고 있다. MANET 기술은 임시적으로 혹은 자원의 부족으로 인해서 유, 무선 네트워크를 구성 할 수 없는 상황에서 신속하게 네트워크를 구성해 줄 수 있다는 장점이 있는 반면, 공중전파를 사용하는 무선통신의 고유의 특성, 그리고 고정된 인프라가 없다는 점에서 많은 보안상의 문제점이 존재한다. 또한 MANET에서는 기존의 유선망에서 사용되고 있는 보안 기법들이 그대로 적용될 수 없다. 그 이유는 MANET 환경에서의 잦은 데이터 전송 에러, 네트워크의 확장성, DoS(Denial of Service) 공격에 대한 방어의 어려움, 그리고 무선 통신에서는 어떠한 물리적인 매체에 직접 접근하지 않고도 도청을 할 수 있다는 문제점, 모바일 노드들의 베터리, 대역폭, 프로세서 등 자원에 대한 제약과 같은 많은 요인을 들 수가 있다[2,11].

네트워크 보안시스템의 구축에 있어서 가장 기본이고 핵심이 되는 부분은 안전한 인증서비스를 제공하는 것이라 볼 수 있다. 기존의 유무선 네트워크 환경 하에서는 인증서를 발급해주는 인증서 발급기관(Certificate Authority : CA)이 있다. 그러나, MANET 환경에서는 더 이상 고정된 인프라가 존재하지 않음으로 인하여 인증서 발급이 문제가 된다. 어떤 하나의 모바일 노드가 CA의 역할을 할 수 있으나, 침입자들의 공격의 목표가 될 수 있다. CA 역할을 하는 모바일 노드 하나 만에 대한 집중적인 공격만으로도 네트워크 전체의 보안 시스템을 무효화시킬 수 있으며, 만일 CA 역할을 하는 모바일 노드를 단순하게 다수로 설정해 놓는다면 보안에 있어 더 큰 위험을 초래할 수 있다.

또한 MANET 환경에서는 수동적 공격(Passive Attack)인 도청으로부터 능동적 공격(Active Attack)인 DoS공격까지 다양한 공격유형들이 존재한다.

본 논문에서는 이러한 MANET환경에서 안전하고 효과적인 인증서비스를 제공하는데 있으며 Secret Sharing, Threshold Digital Signature 방식을 이용한 분산 인증서비스 방

식을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 인증서비스에 대한 분석이 이루어지며, 3장에서는 제안된 인증서비스 방식에 기반이 되는 Secret Sharing, Threshold Digital Signature방식을 소개하고, 새로운 분산 인증서비스 방식과 이에 따른 프로토콜을 제안한다. 그리고 4장에서는 네트워크 시뮬레이션을 통해 제안된 인증서비스의 성능을 평가하고 시스템 파라메타의 설정과 관련된 내용을 자세하게 분석한다. 5장에서는 결론과 향후 연구 에 대해서 언급한다.

2. 기존의 인증서비스

보안에 있어서 가장 중요한 핵심요소중 하나는 인증서비스이다. 인증과 부인 방지는 물론 통신에 필요한 안전한 세션키의 생성을 위해서도 인증서비스가 필요하며, 또 악의적인 노드로 판단된 노드들을 MANET환경에서 배재하기 위해서도 인증서비스는 필요하다. 그리고 군사적 응용에서 뿐만 아니라 상업분야에서도 효율적인 정보의 관리를 위하여 인증서비스는 필수이다. 그러므로 MANET 환경에서 인증서비스를 어떻게 구현하는가는 네트워크 전반의 보안 시스템의 안전성에 기본적인 역할을 한다. 본 장에서는 기존의 인증 서비스에 대한 분석을 한다.

2.1 단일 CA(Single Certificate Authority)

CA의 역할을 하는 하나의 모바일 노드가 항상 존재하며 인증 서비스를 제공해준다. 관리상의 편리함이 있다고는 할 수 있겠지만 모든 공격자의 목표물이 될 수 있다. 그리고 네트워크의 확장에도 많은 제한이 따르게 된다. 통신에 있어서도 병목 현상이 일어날 위험성이 있어, 실제 환경에서는 소수의 상황을 제외하고는 거의 사용이 불가능하다.

2.2. 다수 CA(Multiple Certificate Authority)

단일 CA에서 가용성과 확장성의 문제점을 해결하기 위해서 CA의 역할을 하는 복수개의 모바일 노드들을 설치한다. 가용성, 확장성의 문제점은 해결할 수 있겠지만 CA의 개인키의 노출 위험은 증가된다.

2.3 계층구조(Hierarchical Architecture)

MANET 환경에서 지형이나 통신환경에 따라서 여러 Cluster로 나누고 각각의 Cluster에는 Cluster Header가 있어서 자신이 속해 있는 Cluster내에 속해 있는 모바일 노드들에 대해서 CA의 역할을 해 준다[14]. 지역적으로 모여서 구성된 MANET 환경에서는 네트워크 트래픽을 줄이고 확장성을 증가시키고 안전성을 증가시킨 방식이나, MANET 환경에서의 모바일 노드들은 항상 움직인다는 것을 고려할 때 Hierachical Architecture 인증 서비스는 일반적인 해결책으로 되기에는 문제점이 존재한다. Cluster 사이를 자주 이동하는

모바일 노드들에 대한 인증서비스를 해주는 과정에서 많은 트래픽과 오버헤드가 발생될 수 있다.

2.4 완전분산 인증서비스방식

완전분산 인증서비스방식[13,23,24]은 Threshold Secret Sharing기술[20], Threshold Digital Signature기술[19], Proactive Secret Share Update기술[27]을 이용해서 CA의 역할을 MANET 환경을 구성하고 있는 모든 모바일 노드들에게 분산시킨다. 모바일 노드는 단일 홉을 가지는 이웃 노드들과 통신을 해서 인증서 갱신을 한다. Fault Tolerant하게 설계된 완전분산 인증서비스에서는 기존의 인증서비스에서 CA의 개인키를 어떤 특정한 노드들이 가지고 있는 것에 반 해 어떠한 모바일 노드도 CA의 개인키를 가지고 있지 않다는 점에서 인증 서비스에서 가장 문제점이 되었던 CA 개인키의 노출 문제점을 해결했다.

Threshold Secret Sharing 기술을 이용한 인증 서비스는 기밀성, Fault Tolerance, Availability 등 면에서 많은 장점들을 가지고 있지만 CA의 개인키 노출 위험과 같은 몇 가지 문제점은 여전히 남아 있다. 그리고 또 하나의 문제점은 인증서를 갱신하려는 모바일 노드의 단일 홉 주위에는 k개의 모바일 노드가 있어야만 가능하다. 단일 홉 주위에 k개의 모바일 노드가 존재하지 않은 상황에서는 인증서 갱신이 불가능 하다.

3. 제안된 인증 서비스

3.1 기반 기술

3.1.1 인증서를 이용한 인증서비스

MANET 환경을 형성하고 있는 모든 모바일 노드들은 자신만의 ID를 가지고 있다. 예를 들면 MAC 주소와 같은 0이 아닌 숫자를 가리킨다. 모바일 i노드 의 ID를 v_i라고 하고 모바일 노드들은 자신만의 RSA 공개키 쌍 $<\overline{sk_i}\ \overline{pk_i}>$를 가지고 있다. 여기서 $\overline{sk_i}$는 모바일 노드 i의 메시지 복호화 또는 서명에 사용 될 개인키를 가리키고 $\overline{pk_i}$는 모바일 노드 i의 암호화 또는 검증에 사용 될 공개키를 가리킨다. 그 중에서 $\overline{sk_i}$는 모바일 노드 i만이 비밀로 소유하고 있고 $\overline{pk_i}$는 상호 인증 하려는 모바일 노드에게 공개된다.

모바일 노드 i의 인증서는 $CERT_i$로 표시를 한다. 인증서의 평문은 $cert_i$로 표시를 한다. 인증서 평문 $cert_i$에는 모바일 노드 i의 공개키는 $\overline{pk_i}$이며 사용가능 기간은 t이며 그 외에 신분 등 기타 사항을 명시한다. $CERT_i$는 모바일 노드 i의 인증서 평문 $cert_i$를 CA의 개인키 SK로 암호화해서 모바일 노드 i에게 넘겨준다.

$$CERT_i = (cert_i)_{sk}$$
$$cert_i = (CERT)_{ipk}$$

CA의 공개키 PK는 네트워크 전역에 걸쳐 모든 모바일 노드들에게 공개 되어 있다. 인증서 서비스에는 인증서의 발행, 갱신, 취소가 있고 그 외에 인증서 취소 리스트(Certificate Revocation Lists : CRL)를 저장하고 있다.

그리고 모든 인증서에는 해당 인증서의 사용 유효 기간 t가 적혀 있다. 모바일 노드들은 자신의 인증서를 가지고 신원 인증을 한다. 그리고 인증서 사용 유효 기간 t가 끝나기 전에 인증서 갱신 프로세스를 거쳐 새로운 인증서를 발급 받아야만 지속적인 인증서 사용이 가능하다.

3.1.2 Polynomial Secret Sharing

Secret Sharing[20]은 하나의 비밀을 n개의 조각으로 나뉘어 n개의 노드들에게 분산 시키고, 비밀을 추출해 낼 때는 k개의 비밀 조각만을 필요로 한다. 제안된 방식에서도 Polynomial Secret Sharing을 사용 한다. 어떠한 상황에서도 절대적으로 노출되지 말아야 할 CA의 개인키 SK는 네트워크 전반에 산재해 있는 n개의 특권노드들에게 공유 되어 있다. CA의 개인키 SK를 분산시킴에 있어서 네트워크 관리자 혹은 네트워크 소유자는 차수가 k-1인 다항식 하나를 선택한다.

$$f(x)=SK+f_1 \cdot x+f_2 \cdot x^2+\cdots+f_{k-1} \cdot x^{k-1}$$

다항식의 계수 $f_1 f_2, \cdots+f_{k-1}$과 다항식의 계수이자 CA의 개인키인 SK는 네트워크 소유자만이 알고 있다. 네트워크 소유자는 특권노드 v_i에게 공유 비밀 p_i를 비밀리에 넘겨준다. 어떤 악의적인 노드가 비록 k-1개의 특권노드들에 대한 침입이 성공하더라도 SK에 대한 추출이 불가능하지만 k개 또는 그 이상의 특권노드에 대한 침입이 성공하면 SK는 유출된다.

3.1.3 Threshold Digital Signature

CA의 개인키 SK를 어느 한 특정한 노드에게 노출하지 않으면서도 인증서를 발행할 수 있도록 하기 위한 Polynomial Secret Sharing과 RSA 기술을 통합한 Threshold Digital Signature 기술이 연구 되었다[19].

$$SK_{v_j}=P_{v_j} l_{v_j}(0)=$$

$$P_{v_j} \prod_{i=1, i \neq j}^{k} \frac{v_i}{v_i-v_j} \bmod N$$

라그랑지 보간법에 의하여

$$\sum_{j=1}^{k} SK_{v_j}=\sum_{j=1}^{k} P_{v_j} l_{v_j}(0)=SK \bmod N$$

즉 $\sum_{j=1}^{k} SK_{v_j}=t \cdot N+SK$

($0 \leq t<k$ 이며 정수).

특권노드 j는 자신의 추가 비밀 공유 SK_{vj}를 이용해서 인증서 에 대한 서명을 통해 부분 인증서 $cert_{vj}$를 만들어낸다.

$$CERT_{vj}=(cert)^{sk_j} \bmod N$$

k개의 부분 서명된 인증서 집합 $\{CERT_{v1}, CERT_{v2}, \cdots CERT_{vk}\}$을 부여 받은 모바일 노드는 다음과 같은 연산을 통해서 후보 인증서 $CERT'$를 만들어 낸다.

인증서를 갱신 하려는 모바일 노드는 를 부여 받은 다음 아래와 같이 $(cert)^{-N}$와 간단한 While 문을 실행해서 완전한 인증서를 만들어 낸다.

$Z := (cert)^{-N} mod N$
$j := 0, Y := CERT'$
while $j < k$ *do*
  $Y := Y \cdot Z \bmod N,\ j := j+1$
  if$(cert = Y^{PK} mod N)$ *then*
    break while
  end if
end while
output $Y = CERT$

이로써 완전한 인증서 갱신 프로세스가 끝난다.

3.2 인증 프로토콜

인증 프로토콜에 설명이 될 시스템 파라메타는 〈표 3-1〉과 같다.

제안된 인증서비스는 Polynomial Secret Sharing과 Threshold Digital Signature를 기반한 인증서비스방식이다. 네트워크를 형성하기 전에 CA의 도움을 받아서 모든 모바일 노드들이 인증서를 받는다. 그 밖에 네트워크 소유자는 특권노드를 선택한다. 특권노드는 인증서 갱신 요청이 있을 때 인증서 갱신 서비스를 해주는 노드이다. 인증서 갱신 서비스를 해 주기 위해서는 CA의 개인키 *SK*의 부분 비밀 정보들을 소유하고 있어야 한다. 특권노드에 대한 선택은 적절한 보안 정책에 의해서 안전성이 상대적으로 높고 프로세스, 메모리, 베터리 등 자원이 풍부한 노드들을 선택한다. 제안된 방식은 초기화 과정과 네트워크 생성 후 두 가지 절차로 나눈다.

초기화 과정에서는 모바일 노드들의 인증서 발급 및 특권노드들에 대한 공유 비밀(CA의 비밀키 *SK*에 대한 부분 정보) 발급 과정이 진행한다.

네트워크 생성 후의 프로세스에는 두 모바일 노드 간에 안전한 데이터 통신을 위하여 인증서를 주고 받으면서 Diffie-Hellman 키 교환 기법으로 세션 키를 생성한다. 또한 인증서에 적혀 있는 인증서 사용 유효 기간이 완료되기 전 인증서를 갱신함으로써 지속적인 네트워크 통신에 참여할 수 있다. 그리고 침입 탐지 시스템 등 보안 스킴들과 연합 하기 위해서 인증서 취소 프로세스도 진행한다. 그리고 가장 중요한 CA의 개인 키 *SK*의 안전성을 보호하기 위하여 공유 비밀 갱신 프로세스를 진행한다.

다음은 인증서비스에서 중요한 시스템 파라메타인 *k*와 *n*에 대한 설정의 차이에 따른 설명이다.

k=1,*n*=1 : 중앙집중식 방식이다. 하지만 CA의 역할을 하는 온라인 노드

〈표 3-1〉 시스템 파라메타

시스템 파라메타	나타내는 의미
k	비밀 공유에 사용되는 다항식의 차수 + 1
n	인증서 발급에 참여하는 특권노드의 수
N	MANET 환경을 구성하고 있는 전체 노드 수

하나 만에 대한 공격으로도 인증서비스에 대한 가용성을 손상시킬 수 있다.

k=1,n〉1 : 가용성을 증가시키기 위한 CA를 다수 복제하거나 Hierarchical Architecture 방식이 될 것이다. CA의 역할을 하는 노드를 다수 복제시키는 것은 CA의 개인키 유출 위험성을 초래하게 되지만 Hierarchical Architecture 방식은 지역화된 MANET 환경에서는 유용하게 사용될 수 있다.

k〉1,n=N: 기존의 완전분산 인증서비스방식이다.

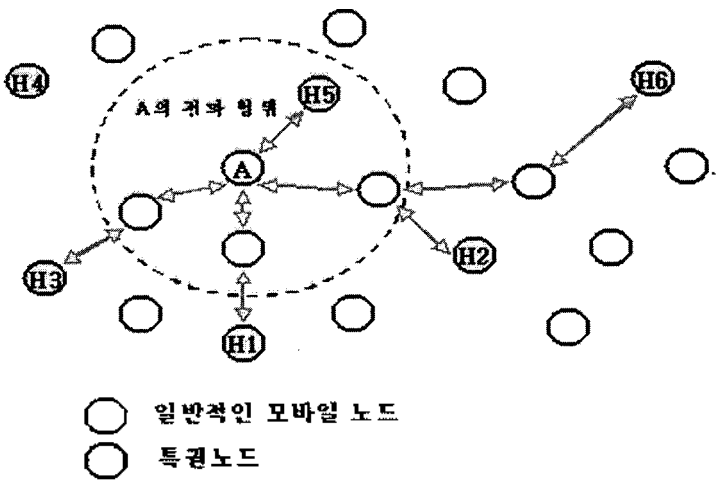
k〉1,k〈n〈N: 본 논문에서 제안한 인증서비스이다. 안전성이 높은 특정노드들에게만 인증서를 발급할 수 있는 특수 권한을 부여한다. CA의 개인키 노출 위험성을 줄이기 위한 방법으로 인증서 발급 권한을 가진 노드의 수를 줄인다.

k=n=N: 보안성은 강화되나 성능은 최저로 떨어질 것이며 fault tolerance, 가용성도 최저로 된다.

k=1,n=N: 가용성은 최대화가 되며, 모든 모바일 노드들이 인증서 발급 가능해지나 보안상 심각한 문제점이 존재하게 된다.

3.2.1 모바일 노드들의 초기화 및 인증서 갱신

초기화 과정에서는 네트워크 소유자가 네트워크를 생성하는 모든 모바일 노드들에게 인증서 $CERT_i$를 발급하며, 특권노드들에게는 공유 비밀 P_{sh}를 발급한다. 모든 모바일 노드들은 인증서 갱신시에 필요로 할 특권노드들의 ID를 가지고 있으며, 그 밖에 CA의 공개키인 PK도 가지고 있다. 모바일 노드들이 소



〈그림 3-1〉 인증서 갱신 과정

유하고 있는 인증서에는 유효기간이 있으며, 유효기간이 지나면 인증서는 더 이상 사용하지 못하도록 보안 정책상 정해진다. 그러므로 모바일 노드들이 지속적으로 MANET 환경에서의 통신에 참여하기 위해서는 인증서 유효기간이 만료되기 전에 인증서를 갱신하는 프로세스를 실행해서 인증서를 갱신시켜야 한다.

인증서를 갱신하려는 모바일 노드는 인증서 갱신 요청을 인증서 갱신 발급 권한을 가진 특권노드들 집합에게 멀티캐스팅한다. 〈그림 3-1〉에서와 같이 인증서 갱신 요청을 받은 특권노드들은 요청을 한 모바일 노드의 인증서를 검증하고 합법적인 모바일 노드로 판단되면 그 요청에 대한 응답을 한다. 인증서 갱신 요청을 했던 소스노드는 각각의 응답메시지를 보낸 특권 노드들에 대한 신원 검증을 진행한다. 인증서 갱신에 대한 응답들 중에서 가장 빨리 도착된 k개의 특권노드를 선택해서 인증서 갱신을 요청한다. 인증서 갱신요청을 받은 특권 노드들은 인증서에 부분서명을 하고 다시 소스 노드에게 보낸다.

k개의 부분 서명된 인증서들을 모두 수신한 소스 노드는 위에서 언급했던 방식으로 완전한 인증서를 만들어낸다.

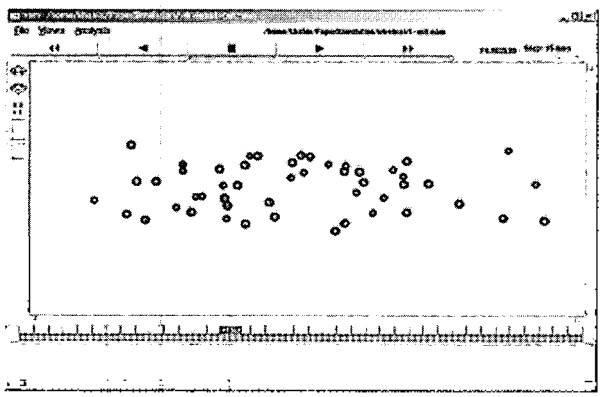
4. 시뮬레이션 및 분석

4.1.시뮬레이션 환경

시뮬레이션에서는 NS Version2 와 NAM(Network Animator)이 사용된다. 〈그림 4-1〉에서는 NAM을 통하여 모바일 노드들의 이동 및 위치를 시각적으로 보여준다. 시뮬레이션 환경은 〈표 4-1〉과 같다.

4.2 시뮬레이션 결과 및 분석

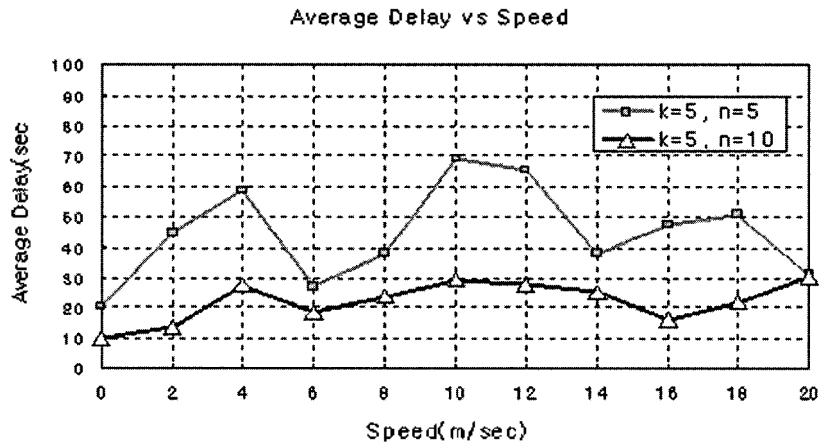
제안된 인증 서비스에서 인증서 갱신 프로세스와 관련하여 시뮬레이션을 실시하였으며, 인증서를 갱신함에 있어 시스템 파라메타



〈그림 4-1〉 NAM에서 MANET 환경

〈표 4-1〉 시뮬레이션 환경

하드웨어 환경	Processor	Pentium Ⅱ
	Memory	128M
소프트웨어 환경	OS	Linux 7.2
	Simulation Tool	NS2, NAM
	Programming Language	C++, Tcl

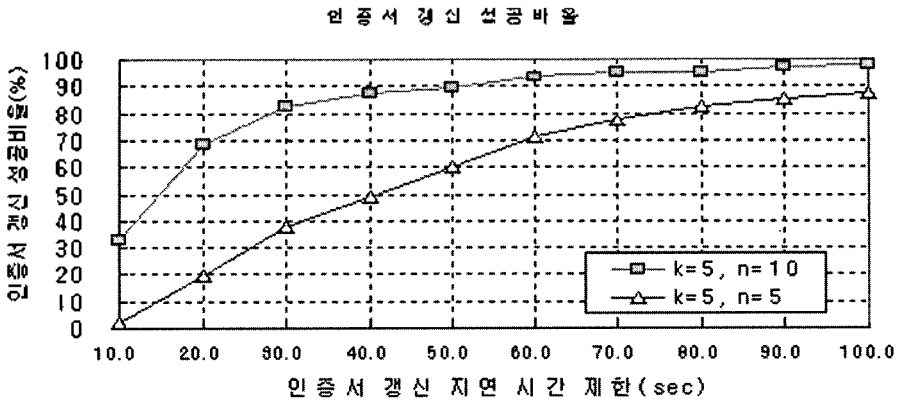


〈그림 4-2〉 Delay Time vs Speed

의 설정과 인증서 갱신시 지연시간 사이의 관계, 인증서 갱신 성공비율 등 데이터를 추출했다.

〈그림 4-2〉는 인증서 갱신 프로세스를 진행함에 있어서 모바일 노드들의 이동 속도와 인증서를 갱신 하는데 걸리는 평균 지연 시간과의 관계를 나타내고 있으며, 〈그림 4-3〉에서는 인증서 갱신 프로세스를 진행함에 있어서 인증서 갱신 프로세서 실행 시간을 각각 다른 시간구간으로 제한 할 때의 인증서 갱신 성공비율을 나타낸다.

〈그림 4-2〉에서 인증서 갱신과정에서 평균 지연시간은 시스템 파라메타 k, n을 각각 5, 5로 설정했을 때 60초 좌우로 나타났으며 시스템 파라메타 k, n을 가각 5, 10으로 설정했을 때 20초에서 30초 좌우로 나타났다. 시뮬레이션 결과에서 인증서 발급 권한을 가진 특권노드들의 수, 즉 n의 값이 커질수록 인증서 갱신 평균 지연 시간은 줄어든다. 그러므로 인증서 갱신 시의 지연 시간을 인증서 발급 권한을 가진 특권노드들의 수 n을 적당하게 증가시킴으로써 줄일 수 있다. 하지만 n의 값을 증



〈그림 4-3〉 인증서 갱신 성공비율

〈표 4-3〉 인증서비스 비교

	중앙집중	계층형	완전분산	제안된 방식
이동성	High	Low	High	High
성능	Low	Low	High	Medium
확장성	Low	Medium	High	High
취약성	Low	Low	Medium	High
가용성	Low	Low	High	High

가한다는 것은 그만큼 보안의 위험성을 증가시키게 된다. 따라서 시스템 파라메타 n의 설정에 있어서는 보안과 성능과의 tradeoff관계를 고려하여 보안정책에 따라 설정하여야 할 것이다.

〈그림 4-3〉은 인증서 갱신 프로세스와 관련된 각각 다른 제한된 시간동안 인증서 갱신에서의 성공비율에 대한 관계를 나타내주고 있다.

시스템 파라메타 k와 n을 각각 5와 5로 설정했을 때의 인증서 갱신 성공비율을 보면 시간에 대한 제한을 늘임에 따라 꾸준히 증가되는 추세를 보여주고 있다. 하지만 실제로는 시스템 파라메타 k와 n을 설정함에 있어서 $k=n$인 정책을 제안하지는 않는다. 실제적으로 응용하는 상황에서는 $k=n+\alpha$ 이 될 것이다. 다만, α에 대한 설정은 네트워크 상황에 따라, 또는 보안 정책에 따라 각기 다른 값을 취할 수가 있다.

〈그림 4-3〉에서의 또 하나의 그래프는 시스템 파라메타 k와 n을 각각 5와 10으로 설정 (α =5)했을 때의 결과그래프이다.

기존의 인증 서비스로서 중앙집중식, Hierarchical Architecture, 완전분산 인증서비스, 그리고 본 논문에서 제안한 인증 서비스에 대해서 이동성, 성능, 확장성, 취약성, 가용성 등에 대한 비교를 정리 하였다.

5. 결 론

MANET에 대한 수요가 상업적, 군사적등 다양한 응용분야에서 급증하면서 MANET 환경에서의 라우팅에 대한 연구뿐만 아니라 보안에 대한 요구도 점점 높아지고 있다. 따라서, 본 논문에서는 MANET 환경에서 안전하고도 효과적인 인증서비스방식을 제안하였다. 고정된 인프라가 더 이상 존재하지 않는 MANET 환경에서 안전하고 가용성이 높은 인증서비스를 제공하기 위하여 Secret Sharing, Threshold Digital Signature 기술을 이용한 새로운 분산 인증서비스방식을 제안하였으며, 기존 인증서비스들에 대해서 분석하고 그 문제점들을 파악하고 그에 적합한 해결방법을 찾는데 중점을 두었다.

기존 완전분산 인증서비스에서는 인증서를 발급받으려는 모바일 노드의 주위에 항상 k개의 모바일 노드가 있다고 가정을 함으로써 인증 서비스의 가용성에 대한 제한이 존재했다.

본 논문에서는 중점적으로 MANET 환경에서의 인증서비스를 다루었으나, 앞으로 인증서비스를 기반으로 한 내·외부공격에 대한 방어시스템의 구축에 관한 연구가 필요하다. 내부 공격에 대한 방어로 Secure Message Transmission 프로토콜, 그리고 침입탐지시스템과 외부 공격에 대한 방어로 Secure Routing Protocol, Secure Aware Routing Protocol 등 보안 기법들과 인증서비스를 통합해서 보다 완벽한 보안 시스템을 구축해야 할 것이다. 그 외에도 인증서 갱신과 관련해서 인증서 갱신 시의 지연시간을 줄이는 기법에 대한 연구도 필요하다. 적절한 인증서 갱신 프로세스에 대한 설계와 전송계층 프로토콜, 그리고 라우팅 프로토콜의 적절한 조합으로 인증서 갱신의 지연시간은 줄일 수 있을 것이다.

참 고 문 헌

[1] The Mobile Ad-hoc Networks (MANET) working group. *http://www.ietf.org/html.charters/manet-charter.html*

[2] A. Bayya, S. Gupte, Y. Shukla, and A. Garikapati, "Security in Ad-hoc networks". *CS 685, Computer Science Department University of Kentucky.*

[3] C-K Toh. (Chai-Keong) "Ad Hoc Mobile Wireless Networks Protocols and Systems" *pp. 57-77.*

[4] The Bluetooth special interest group, *http://www.bluetooth.org*

[5] The HomeRF working group, *http://www.homerf.org*

[6] P. Papadimitratos and Z.J. Haas. *"Secure Routing for Mobile Ad hoc Networks". SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.*

[7] Y. Hu, A. Perrig, D.B. Johnson. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks". *In Proceedings of MOBICOM, September 2002.*

[8] S. Yi, P. Naldurg, R. Kravets. "A Secure-Aware Routing Protocol for Wireless Ad Hoc Networks". *UIUCDCS-R-2001-2241 Technical Report, Aug. 2001.*

[9] C.E. Perkins, E.M. Royer, S.R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing". *draft-ietf-manet-aodv-11.txt. IETF MANET Working Group, June. 2002.*

[10] C. E. Perkins. "Mobile Ad Hoc Networking Terminology". *draft-ietf-manet-term-01.txt, internet draft. Nov. 1998.*

[11] Z.J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama. "Wireless Ad Hoc Networks". *in the Wiley Encryclopedia of Telecommunications. John G. Proakis, Editor. John Wiley & Sons, New York, 2002.*

[12] S. Marti, T.J. Giuli, K. Lai, and M. Baker. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". *In Proceedings of MOBICOM, 2000.*

[13] H. Luo, P. Zerfos, J. Kong, S. Lu and L. Zhang. "Self-securing Ad Hoc Wireless Networks". *Seventh IEEE Symposium on Computers and Communications(ISCC'02).*

[14] L. Venkatraman and D.P. Agrawal. "A Novel Authentication scheme for Ad hoc Networks". *Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE, 2000.*

[15] Y. Zhang, W. Lee. "Intrusion Detection in Wireless Ad-Hoc Networks". *In Proceedings of MOBICOM, 2000.*

[16] S.A. Gupta, "Performance Evaluation of Ad Hoc Routing Protools using ns2 simulations". *http://www.cs.utk.edu/~gupta/*

[17] L. Venkatraman, D. P. Agrawal. "An Optimized Inter-Router Authentication

Scheme for Ad hoc Networks". *http://www.ececs.uc.edu/~cdmc/lakshmi-calgary.pdf*

[18] C-K Toh, (Chai-Keong) "Ad Hoc Mobile Wireless Networks Protocols and Systems" *pp. 27-38.*

[19] V. Shoup. "Practical threshold signatures". *In Proc. Eurocrypt 2000.*

[20] A. Shamir. "How to Share a Secret". *Massachusetts Institute of Technology. Communications of the ACM. 22(11):612-613, 1979.*

[21] M. G. Zapata. "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing". *draft-guerrero-manet-saodv-00.txt. IETF MANET Working Group. August, 2001.*

[22] C-K Toh. (Chai-Keong) "Ad Hoc Mobile Wireless Networks Protocols and Systems" *pp. 215-228.*

[23] H. Luo, S. Lu. "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks". *Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.*

[24] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks". *In Proceedings of ICNP '01.*

[25] D. Nguyen, L. Zhao, P. Uisawang, and J. Platt. "Security Routing Analysis for Mobile Ad Hoc Networks".

[26] "The Network Simulator - NS-2". *http://www.isi.edu/nsnam/ns/.*

[27] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. "Proactive Secret Sharing or: How to Cope with Perpetual Leakage". *Extended abstract, IBM T.J. Watson Research Center, November 1995.*

저 자 소 개

김윤호	(E-mail : yhkim@smu.ac.kr)
	서울대학교 계산통계학과 졸업(이학사)
	서울대학교 대학원 계산통계학과(이학석사)
	서울대학교 대학원 계산통계학과(이학박사)
현재	상명대학교 소프트웨어대학 소프트웨어학부 부교수
관심 분야	분산시스템, 웹 기술, 네트워크 보완