논문 2008-45TC-10-5

모바일 애드혹 네트워크에서 임의의 CA 그룹을 이용한 이동노드의 인증과 홈 CA를 이용한 인증방법의 성능 비교

(Performance Comparison between Random CA Group Authentication and Home CA Authentication in Mobile Ad hoc Network)

이 용*, 이 구 연**

(Yong Lee and Goo Yeon Lee)

요 약

기존의 기반 구조에 의존하지 않고 이동 노드들에 의해 자가 구성되는 모바일 애드혹 네트워크는 네트워크 관리에 필요한 주요 정보들이 자치적으로 구성되는 노드들에 의해 관리되므로 보안이 중요한 이슈가 된다. 특히 이동 노드들의 인증 메커니즘은 네트워크 구성에 참여하는 노드들의 신뢰 구축에 필수적이다. 기존의 네트워크에서 사용되는 인증 모델은 모바일 애드혹 네트워크의 특성상 적용하기 어렵고 가장 널리 사용되는 방법의 하나인 공개키 알고리즘 기반 방법 역시 기반 구조를 갖지 않는 모바일 애드혹 네트워크에 그대로 적용되기 어렵다. 이 논문에서는 모바일 애드혹 네트워크에서 공개키 알고리즘에 기반한 이동 노드의 인증 알고리즘을 제공하기 위해 [1]에서 제안한 임의의 CA 그룹 알고리즘과 홈 CA 방법을 성능 비교한다. 그 결과 CA의 기능이 분산되고 인증 정보에 대한 접근이 효율적인 방법인 임의의 CA 그룹 방법이 모바일 애드혹 네트워크 내에서 인증 메커니즘을 제공하는 데 높은 신뢰도를 가지며 저비용을 소요하는 것을 보여준다. 이러한 결과는 이동 노드의 이동 속도나 네트워크 내의 CA의 수, 이동 노드들의 업/다운 시간 비율에 상관없이 나타나는 것을 알 수 있다

Abstract

Security of self organized mobile ad hoc networks is an important issue because administration information in the networks is managed by the constituent nodes. Especially authentication mechanism is necessary for trust setup between newly joining nodes and the network. The authentication models and protocols which are based on the wireline infrastructure could not be practical for mobile ad hoc network. Although public key algorithm-based method is widely used for authentication, it is not easy to be applied to mobile ad hoc networks because they do not have infrastructure such as centralized CA which is needed for certificate verification. In this paper, we consider the public key based random CA group method proposed in [1] to provide efficient authentication scheme to mobile ad hoc networks and analyze the performance of the method, which is then compared to the home CA method. From the analysis results, we see that the random CA method where the function of CA is distributed to some mobile nodes and the authentication information is propagated to randomly chosen CAs shows higher reliability and lower cost than home CA method.

Keywords: Authentication, Public Key, Randomized CA Group, 홈 CA, Certificate, Mobile Ad Hoc Network

I. 서 론

최근의 네트워크 동향은 단말의 소형화로 인한 이동성 확보, 고속의 통신 기술 확보 등으로 자율성을 보장하고 실시간 구축이 가능한 네트워크 구성이 그 추세이다. 이런 추세에 따라 모바일 애드혹 네트워크는 기존

* 정회원, 충주대학교 전자통신공학전공
(Dept. of Electron. and Comm., ChungJu National University)
** 정회원-교신저자, 강원대학교 컴퓨터학부
(Dept. of Computer Eng. Kangwon National University)
※ 이 논문은 강원도-앨버타주 공동연구의 결과임
접수일자: 2008년3월8일, 수정완료일: 2008년10월16일

의 유선 기반의 인프라의 도움이 없이 이동 노드들에 의해 자가 조직되고 자가 운영되는 네트워크이다. 어떤 이동 노드이든지 모바일 애드혹 네트워크의 구성멤버가 될 수 있으므로 이동 노드들 간의 신뢰는 네트워크 구축과 안정성 확보에 매우 중요하다. 모바일 애드혹 네트워크가 어떤 고정된 인프라도 필요로 하지 않기 때문에, 인프라를 기반으로 하는 전통적인 인증 메커니즘을 적용하는 것은 적합하지 않다. 이동 노드들은 이동성을 가지고 자주 움직일 수 있지만 전력의 제한이나 대역폭의 제한 문제로 인해 네트워크에 접속했다가 끊어지는 것을 빈번하게 반복하게 된다. 이런 불안정성으로 인해 모바일 애드혹 네트워크는 다양한 공격에 취약한 특성을 가지게 된다[2]. 네트워크 불안정성을 이용하여 도청자는 비밀 정보를 취득할 수도 있으며 네트워크의 통신 비밀성을 깨뜨릴 수도 있다. 악의적인 노드는 직접 네트워크를 공격하여 노드간에 주고받는 메시지를 위조하거나 정당한 노드인 척 위장하여 인증 과정을 위반하고 네트워크에 침입하여 네트워크 구성을 방해할 수도 있다. 이러한 보안상의 문제들을 해결하기 위해서는 우선적으로 모바일 애드혹 네트워크가 인증된 노드만으로 구성될 수 있도록 하는 인증 메커니즘이 필요하다.

공유 비밀 정보를 사용하는 대칭키 메커니즘은 많은 이동 노드들이 미리 비밀 정보를 공유해야 하는 어려움으로 인해 모바일 애드혹 네트워크에는 적합하지 않다. 더구나 모바일 애드혹 네트워크는 기존의 인프라를 갖지 않으므로 키 분배 센터(Key Distribution Center) 같은 중앙 집중식 시스템을 적용할 수가 없다.

공개키 기반 구조(Public Key Infrastructure : PKI)는 노드간 신뢰의 기반을 제공하여 동적인 네트워크에서 인증 메커니즘을 제공하는 가장 성공적인 방법의 하나로 인식되고 있지만[3], 공개키와 공개키의 소유자를 연결하는 인증서에 서명해 주는 인증기관 (Certificate Authority : CA)같은 고정된 인프라를 필요로 하므로 현재의 방법대로는 모바일 애드혹 네트워크에 적합한 방법이 아니다. 따라서 CA의 기능이 어떻게 수행되느냐 하는 문제는 PKI를 모바일 애드혹 네트워크에 적용할 때 중요한 이슈가 된다. CA의 기능이 유선 네트워크에서처럼 중앙 집중화되어 홈 영역에만 존재한다면 네트워크 구성이 불안정한 모바일 애드혹 네트워크에서는 이동성을 가지고 여기저기 이동하는 이동 노드가 CA 서비스를 이용하기 어렵게 된다. 이를 해결하기 위한 방법의 하나로 CA의 기능을 이동 노드들에게 분산시키는 것이 가능하나, 이 경우 분산된 CA 기능간의 연동 방법이 중요한 요소가 될 것이다. 즉 CA의 기능이 분산된 경우 CA들 간의 연동이나 신뢰 구축을 위해 CA들의 공개키 정보와 같은 인증 정보를 효율적으로 공유하는 방법이 필요하다.

이 논문에서는 분산된 CA들의 인증정보를 효율적으로 공유하는 방법으로 [1]에서 제안한 모바일 애드혹 네트워트에서 임의의 CA 그룹 방법을 고려하고, 이 방법의 성능을 분석한다. 분석된 결과는 홈 CA에만 의존하는 방법과 비교하여 임의의 CA 그룹 방법의 우수성을 증명하고자 한다.

II. 모바일 애드혹 네트워크에서의 인증 방법 및 관련 연구

1. CA의 구성방법

이 절에서 우리는 모바일 애드혹 네트워크에서 적용되어질 수 있는 CA의 구성방법에 대하여 알아본다.

(가) 하나의 글로벌한 CA

본 구성방법에서는 전체 네트워크에서 하나의 글로벌 CA 만이 존재한다. 이런 모델의 경우, 많은 이동 노드들이 전 세계에 흩어져 네트워크를 이루고, 모든 노드들은 이 글로벌 CA로부터 인증서를 발급받는다. 글로벌 CA는 노드들에게 인증서를 발급하고 CRL을 관리하여야 하므로 CRL(Certificate Revocation List) 크기는 매우 커지고 이 글로벌 CA의 역할은 매우 중요하게 된다. 어떤 노드들은 모바일 애드혹 네트워크 환경에서 이 글로벌 CA에 접속할 수 없는 사태가 발생할 수도 있다. 이 글로벌 CA로부터 무척 먼 거리에 위치한 이동 노드는 이 CA로부터 인증서를 발급받는 것이 어려울 수도 있다. 설령 이런 노드들이 인증서를 발급받더라도, 이 노드들이 상대 노드들을 인증하기 위해 먼 거리를 거쳐서 글로벌 CA로부터 CRL을 획득하여 검증하는 것도 어려울 수 있다. 만약 이 글로벌 CA가 다운된다면, 네트워크의 모든 이동 노드들은 CA 서비스를 사용할 게 없게 되며, 이동 노드의 인증에 관련된 모든 메커니즘은 정지될 것이다.

결론적으로 이런 방법은 이동 노드들이 필요할 때에 CA로부터 상대 노드에 대한 인증정보를 얻지 못하거나 상대 노드의 인증서를 검증하지 못하는 경우가 발생할 수 있고, 네트워크 전체에 대하여 글로벌 CA의 공개키를 갱신하거나 분배하는 것도 어렵다.

(나) 영역별 CA 구성

본 구성에서는 전체 네트워크를 작은 단위영역으로 나누고 각 단위 영역 별로 하나의 CA가 존재한다. 예를 들면 각 나라별로 하나씩 CA를 갖는 경우가 가능하다. 각 나라의 CA는 자기 나라에 속한 이동 노드들에 대하여 인증서를 발급한다. 만일 이동 사용자가 한 나라에만 계속 산다면, 이 사용자가 가진 이동 노드는 그 나라에서 인증서를 발급 받아서 그 나라에서만 사용하는 간단한 모델이 된다. 그러나 이동 사용자가 세계를 여기저기 돌아다닌다면, 이 사용자가 다른 나라를 여행할 때마다 비자처럼 여행하는 나라의 CA로부터 인증서를 발급받아야 하며 이런 인증서들을 저장소에 관리하여야 한다. 이동 노드가 여러 나라를 한번씩 방문한다면 한번만 사용할 인증서에 대한 발급 비용과 관리 비용이 상당한 부담이 될 것이다. CA는 자기 영역을 방문한 이동 노드들에게 발급한 인증서를 지속적으로 갱신하여야 하고 CRL을 관리하여야 하는 문제가 발생한다.

(다) 홈 CA 구성

각 나라 별로 하나의 CA가 존재하여 이동 노드들은 자신이 처음 속한 나라를 홈 영역으로 하여 홈 CA로부터 인증서를 발급받아서 이 인증서를 다른 나라의 네트워크에 걸쳐서 사용하는 구조이다. 이 경우에 이동 노드들은 하나의 인증서만 가지므로 관리가 쉽고 각 영역마다 CA가 존재하므로 CA에 대한 접근이 쉬워진다. 그러나 이 모델의 경우 이동 노드가 홈 영역에서 발급받은 인증서를 다른 영역에서 사용할 수 있도록 하는 방법이 필요하다. 즉, 이동 노드가 다른 나라로 이동할 때, 방문한 나라의 CA는 방문 노드를 인증하기 위하여 방문 노드에게 인증서를 발급한 CA의 공개키와 인증 정보를 요구한다. 이 방법에서는 이동 노드가 네트워크의 모든 나라들을 방문할 지도 모르므로 각 CA들은 네트워크의 모든 나라에 존재하는 CA에 대한 공개키를 알아야 한다. 어떤 CA가 인증서를 발급한 이동 노드들이 다른 나라로 전혀 이동하지 않는다면, 그 CA의 공개키 정보를 저장한 CA들은 그 공개키 정보를 한번도 사용하지 않을 수도 있다. 사용되지 않을 수도 있는데도 불구하고 모든 CA들의 공개키를 저장하고 관리하는 것도 또한 비효율적이고 부담이 될 것이며 이것은 공개키 뿐만 아니라 CRL 분배에서도 같은 문제가 된다. 그 이유는 CRL은 인증서가 폐지될 때마다 CA에 의해 비정기적으로 발급되고 CA는 갱신된 CRL을 모든 다른 CA들에게 알려야 하기 때문이다. 이동 노드는 인증서를 검증하기 위해 CA로부터 CRL을 받아서 검증하여야 하는데 모든 CA들로부터 발급된 CRL을 모으는 것은 어려운 일이다.

(라) 임의의 노드 그룹에의 CA 기능 분산

본 구성은 위에서의 3가지 CA 구성의 문제를 해결하기 위한 방법으로, CA의 기능을 여러 개의 노드에 분산시키는 방법이다[1]. 인증 정보는 분산된 여러 개의 CA 노드 중에서 임의로 선정된 CA 그룹에 의해 발급되고, 전달되며, 검증되어진다. 이 방법은 III장 2절에서 자세히 다룬다.

2. 관련 연구

현재까지 모바일 애드혹 네트워크의 인증 문제를 해결하기 위한 많은 방법들이 제안되었다. Haas 등은 애드 혹 네트워크에서 threshold cryptography를 이용한 분산 공개키 관리 스킴을 제안하였으며[4] 이후 많은 연구가 이 결과를 이용하고 있다[3, 5~6]. Kravets 등은 threshold cryptography를 사용하여 몇 개의 이동 노드들 사이에 CA 기능을 분산시키고 PKI를 제공하는 방법을 제안하였다[3, 5]. 이들은 이동 노드들의 다양성에 주목하여 성능이 더 뛰어난 이동 노드가 이동 CA로서의 기능을 갖고 threshold cryptography에 따라 인증 정보를 공유하도록 하였다. 그러나 이런 방법은 동적으로 구성되는 모바일 애드혹 네트워크 환경에서 이동 노드들간의 성능 비교가 어렵다는 점에서 적용이 어려운 문제를 갖는다.

Zhang 등은 확장성을 갖는 분산 인증 방법을 제안하였다[6~7]. 이 방법은 k 노드가 비밀키를 공유하도록 하여 노드가 부담을 공유하게 하였으며 이동 노드는 이 k 노드가 공유한 비밀키로 인증서을 받으면 인증된 것으로 하였다. k 노드들은 한 홉 거리의 노드들로 가까운 거리를 이용하여 주변 노드들을 감시할 수 있다. 그러나 이 연구는 주변 k 노드들로부터 발급받은 인증서를 검증할 방법에 대해서는 제시하지 못하고 있다.

Hubaux 등은 PGP와 유사한 알고리즘을 적용하여 모바일 애드혹 네트워크가 자가 구성되는 방법을 제안하였다[8~9]. 여기서는 인증서가 잘 아는 노드로부터 발급되고 노드간 신뢰 체인을 이용하여 다른 노드를 인증하게 된다. 이를 위해 노드들은 다른 노드를 만났을 때 상대노드가 가진 신뢰 체인 정보를 주고 받게 된다. 이 외에도 인증서 폐지 기능을 포함하여 애드 혹 네트워크

에서 인증서 관리에 대한 제안들이 연구되고 있다[10~11].

Ⅲ. 홈 CA 방법와 임의의 CA 그룹 방법의 동작 과정

본 논문에서 고려하고 있는 네트워크 구성환경은 다음과 같다.

- 매우 넓은 영역에 걸쳐 많은 이동 노드가 분포되어 있다.
- 이동 노드는 임의의 속도로 임의의 방향으로 한 영역에서 다른 영역으로 이동할 수 있다.
- CA를 포함하여 이동 노드들은 빈번하게 네트워크에 연결되거나 연결이 끊어지는 과정을 반복하다.
- 임의의 CA 그룹 방법의 경우, 모바일 애드 혹 네트워크가 구성될 때, 노드의 일부가 CA로 선택된다.
- 인증 정보는 CA의 공개키, CRL과 최신 갱신 시간을 나타내는 숫자로 구성된다.

1. 홈 CA를 통한 인증 방법

홈 CA를 통한 인증 방법은 전통적으로 사용되는 인증 방법과 유사하며 자세한 과정은 다음과 같다. 이동 노드가 인증서를 발급받는 CA가 그 이동 노드의 홈 CA가 된다. 이동 노드의 인증 정보는 오직 홈 CA만이 가지고 있다. 즉 이 노드를 인증하기 위해서는 이 노드의 인증서에 서명한 CA의 공개키와 같은 인증 정보를 홈 CA에게서만 얻을 수 있다. 이동 노드가 다른 CA의 영역으로 이동했을 때, 방문한 영역의 CA는 이 노드의 인증서를 검증하기 위해 이 노드의 홈 CA에게 인증정보를 요청하게 된다.

이런 모델에서는 방문한 영역이 이 노드의 홈 CA의 영역으로부터 멀리 떨어져 있다면, 방문 CA는 방문 노드의 홈 CA와 직접 통신하기 힘들고 따라서 인증 정보를 획득하기 어렵게 된다. 또한 홈 CA만이 인증 정보를 가진 유일한 CA이므로 방문 CA가 인증 정보를 요청한 때에 마침 홈 CA가 다운된다면 역시 인증 정보를 획득하기가 어렵게 된다. 또한 이동 노드가 인증서를 폐지해야 할 경우에도, 홈 CA만이 이 이동 노드의 인증서를 폐지할 수 있다. 이동 노드가 홈 CA의 영역에 있지 않을 경우 이동 노드는 원거리 통신을 통해 홈 CA에 어렵게 접속해서 인증서를 폐지하여야 하며 홈 CA와 접속이 되지 않을 경우 인증서를 폐지할 수 없게 된다. <그림 1>은 이와 같은 과정을 보여준다.

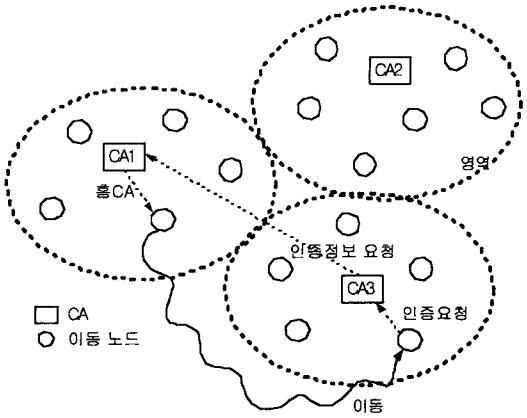


그림 1. 홈 CA를 통한 이동 노드의 인증 방법
Fig. 1. Authentication method by Home CA.

따라서 이 방법은 인증 메커니즘이 매우 단순하지만 홈 CA에 의존적이라 이동 노드가 제 때에 인증을 받기도 힘들고 인증서 폐지나 갱신 등의 CA 서비스를 이용하기 힘들게 되는 등 CA 가용성이 떨어지게 된다.

2 임의의 CA 그룹 인증 방법

가. 인증 과정

임의의 CA 그룹 방법을 이용한 인증 과정을 간단히 살펴보면 다음과 같다. CA들은 임의의 크기로 그룹을 구성하고 임의의 그룹들은 다른 그룹과 중복되어 겹쳐진 CA들을 갖는다. 즉 한 그룹에 포함되어 인증 정보를 얻은 CA들은 다른 그룹에도 중복되어 포함될 수 있고 그룹 내의 다른 CA들과 인증정보를 공유하게 된다. 이런 식으로 동작을 하게 되면, 한 CA가 얻은 인증 정보가 다른 CA들로 전파될 수 있게 된다. 인증정보(예. CA의 공개키, CRL)가 네트워크의 일부 CA들에 의해 공유될지라도 CA 그룹은 임의로 선택되고 CA 노드들도 네트워크 내의 다른 영역으로 이동할 수 있으므로 인증정보는 네트워크 전체에 걸쳐서 전파될 수 있고 모든 노드들에 의해서 사용될 수 있게 된다. 만약 임의의 그룹의 크기가 최적이라면 일부 CA가 다운되더라도 필요로 하는 인증 정보는 여전히 획득될 수 있게 된다. 임의의 CA 그룹 인증 방법의 분석을 위해 다음과 같은 모델을 가정한다.

- 모든 노드들은 가장 가까운 CA로부터 한 개의 인증서를 발급받는다.
- CA는 노드에게 인증서와 CRL을 발급하고 자신의 DB에 노드들의 인증 정보를 저장한다.

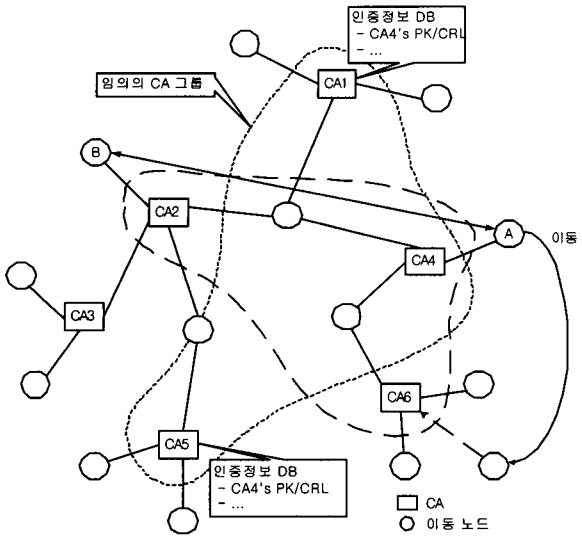


그림 2. 임의의 CA그룹을 이용한 인증 방법
Fig. 2. Authentication method by Random CA Group (RCG).

- CA는 자신이 발급한 인증서가 아닌 어떤 인증서에 대해서도 CRL을 발급할 수 있다.

<그림 2>는 이와 같은 과정을 보여준다.

이런 모델은 모바일 애드 혹 네트워크가 기존의 인프라를 사용할 수 없을 때에도 모든 이동 노드가 널리 알려진 CA의 공개키를 알고 있다고 가정할 수 있고 따라서 CA는 널리 알려진 CA가 서명한 인증서를 검증할 수 있게 된다.

CA가 아닌 일반 노드는 가장 가까운 CA로부터 인증서를 발급받는다. 인증서를 발급받은 이동 노드는 모든 네트워크에 걸쳐서 이 인증서를 사용할 수 있게 된다. 이동 노드가 다른 CA의 영역으로 이동했을 때, 자신의 인증서를 새로운 영역의 CA에게 보낸다. CA는 인증서를 검증하기 위해 인증서에 서명한 CA의 공개키가 필요하며 CRL을 통해 인증서가 폐지되었는지를 체크해야 한다. 따라서 CA는 서명한 CA의 공개키와 CRL을 임의의 CA 그룹 멤버로부터 획득하여 인증서를 검증한다.

초기 CA 선출과정 이후에 CA가 다운되거나 다른 영역으로 이동했을 때, 남아있는 노드들 중에 새로운 CA가 선출된다. 예를 들어 CA_i가 다운되면 노드들은 이 CA_i를 대신할 CA가 필요하다. 노드들은 이미 CA_i가 서명한 인증서를 가지고 있고 CA들 사이의 초기 신뢰구축 이후에 다른 CA들이 CA_i를 인증하였으므로 CA들은 CA_i의 인증서를 신뢰한다. 따라서 새로운 CA에 대한 신뢰는 새로운 CA에게 CA_i가 발급한 인증서에 의해 얻어진다.

나. 임의의 CA 그룹의 구축 방법

제안하는 방법에서 임의의 CA 그룹의 구축 과정은 다음과 같다.

- 이동 노드 중에 일부가 CA로 선택된다. CA는 자가 서명하여 자신에게 인증서를 발급한다. 초기에 CA들이 임의의 그룹을 형성할 때 CA들 간의 인증은 널리 알려진 CA가 발급한 인증서를 사용하여 이루어진다. 초기 신뢰 구축 이후에 CA들은 자가 서명한 인증서를 사용하여 다른 CA들을 인증하고 더 이상 널리 알려진 CA가 발급한 인증서는 사용하지 않는다.
- 임의의 CA 그룹을 구성하는 CA는 말 그대로 임의로 선택된다.
- CA가 정해진 시간 이상 다운된다면, 새로운 노드가 CA로 선출된다.
- n개의 CA가 주어지고 그룹의 크기가 k라면, k CA들로 임의의 CA 그룹이 구성되어 이동 노드들의 인증 정보가 저장된다.
  - 이동 노드가 홈 CA에 인증을 요청할 때, 홈 CA는 접근가능한 임의의 CA 그룹을 선택하여 이동 노드의 인증 정보를 전달한다.
  - CA가 임의의 CA 그룹으로부터 이동 노드의 인증 정보를 얻는다면 CA는 인증 정보에 있는, 이동 노드의 인증서에 서명한 CA의 공개키를 이용하여 이동 노드의 인증서를 검증할 수 있게 되고 임의의 CA 그룹으로부터 획득한 모든 CRL을 통해 최신의 CRL을 구성하여 인증서가 폐지되었는지를 확인할 수 있다. 이와 같은 과정에서 최신의 CRL은 일련번호가 사용된다.

IV. 성능 평가

1. 시뮬레이션 모델

임의의 CA 그룹 방식의 성능을 분석하고, 이를 홈 CA 방식의 경우와 비교하기 위한 시뮬레이션을 수행하기 위하여 다음과 같이 모바일 애드혹 네트워크를 구성한다.

- 이동 노드의 수 : m
- CA의 수 : n

- 임의의 CA 그룹 방법에서 임의의 CA 그룹의 크기 : k
- 이동 노드의 이동 모델은 random waypoint 모델을 사용한다[12].
- 이동 노드의 이동에 따라 한 영역에 위치하는 이동 노드의 수는 제한하지 않는다.

CA를 포함하여 이동 노드가 업인 기간은 평균 t_U 기간을 갖는 지수분포로 가정하며, 이동 노드의 다운 기간은 평균 t_D 기간을 갖는 지수분포로 가정한다. 즉, 평균 기간 t_U 동안 이동 노드는 업이고 이후 평균 기간 t_D동안은 다운된다. CA가 제한 시간 T를 넘어서까지 다운된 상태라면, T 시간 이후에 같은 영역에 속하는 이동 노드 중의 임의로 선택된 이동 노드가 새로운 CA로 선출된다. 이때, 원래 CA노드는 더 이상 CA가 아니고 일반 이동 노드가 된다. 같은 영역에 속하는 이동 노드들은 CA가 다운된 경우 CA로부터 어떤 신호도 받을 수 없으므로 CA가 다운된 것을 알 수 있게 된다. 이동 노드의 영역 체류 시간은 (random waypoint 모델의 경우, pause 기간을 의미함) 영역내에 도착하여 떠나는 순간까지의 시간으로 t_M의 평균 시간을 갖는 지수 분포로 가정한다. 즉, 이동 노드는 평균 t_M 시간 동안 영역내에 체류한다.

CA노드가 다른 CA영역으로 이동하면 방문 영역에 있는 CA를 감지하고 이동한 CA는 일반 이동 노드가 된다. 이동한 CA가 있었던 영역에서는 CA가 없어졌으므로 CA가 다운된 것과 같은 상황으로 간주하여 임계 시간 T를 기다린 후에 남은 이동 노드들이 새로운 CA를 선출한다. 크기 k를 갖는 임의의 CA 그룹은 모든 CA들 중에서 임의로 선택되고 선택된 CA들은 업이거나 다운된 상태일 수 있다.

모든 이동 노드들은 임의로 선택된 노드들에게 λ_O의 속도를 갖는 포아슨 모델로 호를 생성하여 보낸다. 각 노드의 인증서 폐지는 평균 레이트 λ_R의 지수분포를 갖는다고 가정한다. 임의로 선택된 노드가 CA에게 인증서 폐지를 요청하면, CA는 인증서를 폐지하고 CRL을 갱신한다. 인증서가 폐지된 후 지수분포를 갖는 시간 t_i 후에 이동 노드는 CA에게 새로운 인증서 발급을 요청한다. CA의 인증서가 폐지되고 t_i가 T보다 크다면 영역내의 새로운 CA가 선출된다.

본 절에서 우리는 두 가지 성능을 비교한다. 하나는 인증 과정을 수행하기 위해 인증 요청, 인증 정보 갱신, 인증 실패로 인한 비용 등을 고려한 총비용, C 이다. C는 다음과 같이 정의된다.

$$C = c_l \cdot E_{fail} + c_u \cdot E_{write} \quad (1)$$

여기서 c_l은 인증 실패로 인한 단위 비용이며 c_u는 인증 정보를 갱신하기 위해 CA의 DB를 한번 액세스하는 단위 비용이다. E_{fail}은 단위 시간당 인증 요청이 실패한 총 수이고 E_{write}는 단위 시간 당 DB에 기록한 총 수 이다. 이 시뮬레이션에서 우리는 c_l = 100 과 c_u = 1 으로 가정한다.

두 번 째 성능은 시스템의 신뢰도, R 이며 다음과 같이 정의된다.

$$R = \frac{\text{성공한 인증 횟수}}{\text{노드가 요청한 총 인증 횟수}} \quad (2)$$

2. 성능 분석 결과

이 절에서는 제안하는 임의의 CA 그룹 방법과 홈 CA를 통해 인증을 수행하는 방법을 비교하여 성능을 보여주고자 한다. 임의의 CA 그룹 방법에서 CA 그룹의 크기는 [1]에서 최적의 크기로 증명된 12를 선택하였다.

<그림 3>은 네트워크 내의 CA 수의 변화에 따른 신뢰도와 총비용을 비교하여 보여준다. <그림 3a>에서 임의의 CA 그룹 방법이 홈 CA 방법에 비해 높은 신뢰도를 갖는 것을 알 수 있다. 이러한 높은 신뢰도는 총비용에도 영향을 두어 <그림 3b>에서 역시 임의의 CA 그룹 방법의 총비용이 더 낮음을 알 수 있다. 홈 CA 방법에서 CA 수가 많은 경우 한 CA가 다운되더라도 그 CA의 영향을 받는 노드의 수가 적으므로 신뢰도가 덜 떨어진다. 반면에 CA 수가 작은 경우, 한 CA의 업/다운에 영향을 받는 이동 노드의 수가 많아지고 신뢰도에 영향을 주게 된다. 이것은 총 비용의 경우도 마찬가지이다.

임의의 CA 그룹 방법은 CA 수가 증가할 경우 그 영역 내에 있는 이동 노드의 수가 감소하고 CA 영역 내에 이동 노드가 오래 체류하면 인증 횟수가 줄어들게 되므로 오히려 CA들에게 인증 정보가 전파되는 것을 방지하는 효과를 갖게 된다.

<그림 4>는 이동노드의 영역내의 체류시간 변화에 따라 신뢰도와 총비용을 비교한 그래프이다. 역시 임의의 CA 그룹 방법이 홈 CA 방법에 비하여 높은 신뢰도와 낮은 총비용을 보여준다. 이동 노드의 체류 시간이

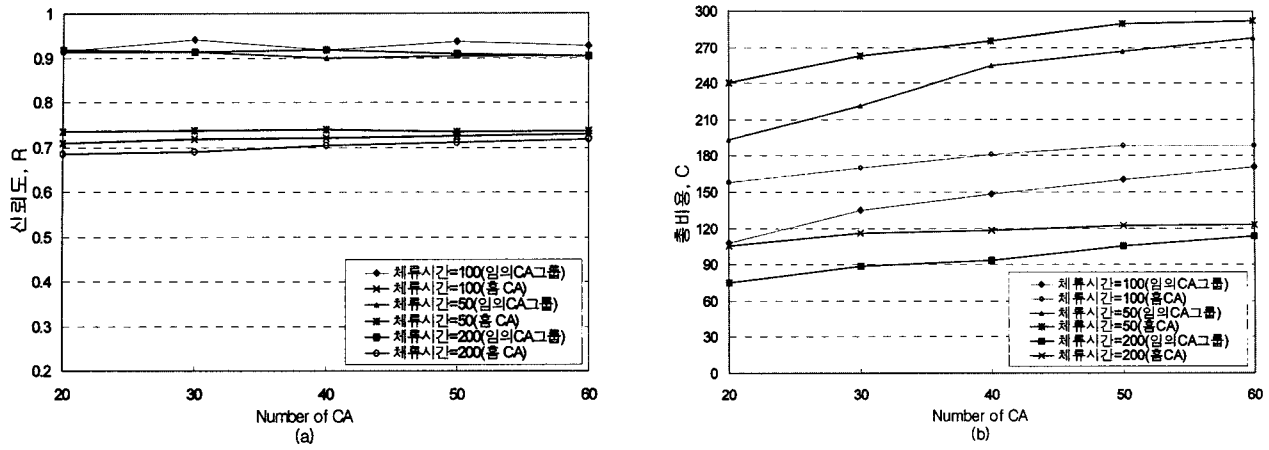


그림 3. CA의 수 증가에 따라 임의의 CA그룹 방법과 홈 CA 방법에 대한 총비용과 신뢰도 비교
Fig. 3. Comparison of reliability and total cost for RCG and home CA in when parameter is number of CA.

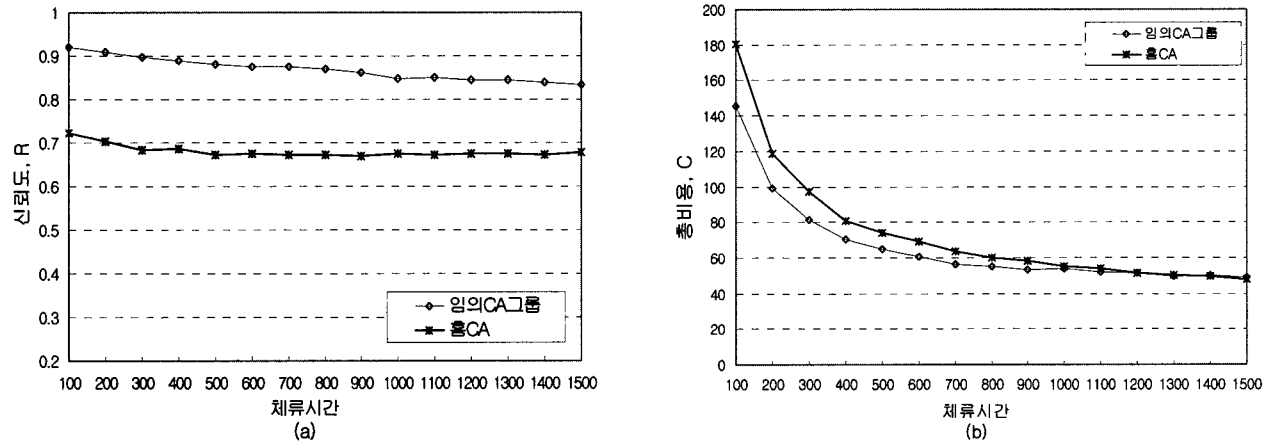


그림 4. 이동 노드의 체류시간 변화에 따라 임의의 CA그룹 방법과 홈 CA 방법에 대한 총비용과 신뢰도 비교
Fig. 4. Comparison of reliability and total cost for RCG scheme and home CA in when parameter is residence time.

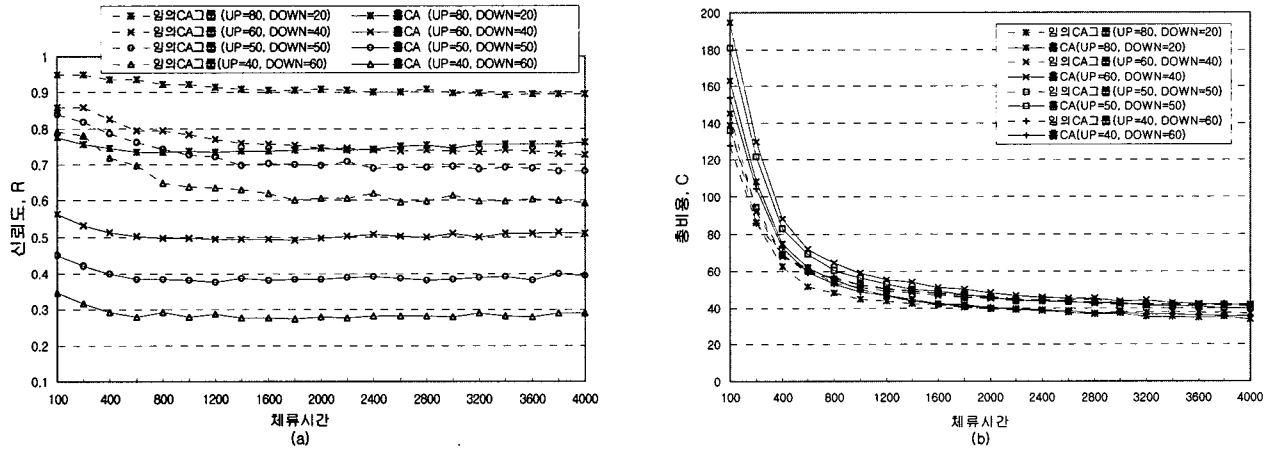


그림 5. 이동 노드의 업/다운 비율에 따라 임의의 CA그룹 방법과 홈 CA 방법에 대한 총비용과 신뢰도 비교
Fig. 5. Comparison of reliability and total cost for RCG scheme and home CA when parameter is UP/DOWN ratio.

증가하는 경우 이동 노드의 이동성이 낮고, 인증 요청의 수가 감소하는 것을 의미하며 인증요청 수가 작으므로 두 방법의 총비용이 거의 같아짐을 볼 수 있다.

<그림 5>는 임의의 CA 그룹 방법과 홈 CA 방법의 결과를 단위시간당 CA의 업/다운 비율에 따라 비교한 것이다. CA의 업/다운 비율은 CA의 안정성을 보여주

는 기준으로 볼 수 있다. 노드의 업 시간 비율이 클 때, 총비용이 낮고 신뢰도가 높은 것을 알 수 있다. <그림 5(a)>는 CA가 업인 시간이 작을 때, 홈 CA 방법의 시스템의 신뢰도가 임의의 CA 그룹 방법에 비해 훨씬 낮음을 보여준다. 이런 이유는 홈 CA가 다운된 경우 임의의 CA 그룹 방법에서와 달리 홈 CA 방법에서는 방문 CA가 이동 노드에 대한 인증 정보를 다른 CA들로부터 얻을 수가 없어서 인증은 실패하게 되기 때문이다.

이동 노드의 이동이 거의 없어서 이동 노드는 대부분의 시간을 홈 CA의 영역에서 보내고 다른 CA의 영역으로는 이동하지 않는다면 이 이동 노드는 다른 CA에게 자신을 인증 받을 필요가 없고 다른 CA에 인증 정보를 기록할 일도 없을 것이다. 그러므로 이동 노드의 영역 체류 시간이 큰 경우는 홈 CA 방법의 총 비용이 임의의 CA 그룹 방법보다 작다. 이는 홈 CA 방법의 경우 CA 노드들에 대한 인증 정보 기록 비용(E_{write})이 없기 때문이다. 이동 노드의 체류 시간이 감소하여, 즉 이동 노드가 자주 움직이게 된다면, 방문 CA는 이동 노드를 인증하기 위해 이동 노드의 인증 정보를 홈 CA로부터 얻어야 한다. 홈 CA에 대한 접근은 홈 CA의 안정성, 홈 CA로부터의 거리와 라우팅 등에 영향을 받는다. 임의의 CA 그룹 방법에서는 CA의 일부가 다운되더라도, 방문 CA는 임의의 선택한 CA 그룹 중에서 살아있는 일부로부터 인증 정보를 얻을 수 있으므로 신뢰도가 높아진다.

<그림 5(b)>는 두 가지 방법의 총 비용에 대한 비교를 보여준다. 그림에서 업/다운 비율이 60%일 때, 노드들의 체류 시간이 증가함에 따라 홈 CA 방법의 총 비용이 임의의 CA 그룹 방법의 총 비용 보다 낮은 것을 알 수 있다.

전체적으로 임의의 CA 그룹 방법의 경우 CA그룹에 대한 E_{write} 비용이 많고 인증 실패로 인한 E_{fail} 비용이 작으며 홈 CA 방법은 한 CA로만 업데이트가 발생하므로 E_{write} 비용은 작지만 E_{fail}가 높아진다.

V. 결 론

모바일 애드 혹 네트워크의 특성상 기존에 사용되는 인증 방법들을 적용하기 어려운 문제가 있다. 기존 네트워크 환경에서 가장 널리 사용되는 알고리즘의 하나인 공개키 알고리즘 기반의 PKI 역시 CA라는 기반 구조를 필요로 하는 특성상 이동 노드들에 의해 자치적으로 운영되는 모바일 애드 혹 네트워크에는 적용이 적합하지 않다.

[1]에서는 이런 문제를 해결하기 위해 CA의 기능을 이동 노드들에게 분산시키고 CA들 간에 인증 정보를 효율적으로 공유하기 위하여 임의의 CA 그룹을 이용한 인증 방법을 제안하였다. 본 논문에서는 임의의 CA 그룹 방법과 홈 CA 방법에 대하여 성능을 비교분석하였다.

홈 CA 방법은 전통적으로 사용되는 PKI 방법으로 CA의 기능은 영역별로 분산되지만 CA 간의 연동 문제를 가지고 있어서 인증 정보를 효율적으로 공유하는 방법을 제공하지 못한다.

비교 결과, 인증 방법의 신뢰도와 총비용의 측면에서 임의의 CA 그룹 방법이 홈 CA 방법에 비해 우수한 성능을 보여줌을 알 수 있다. 이러한 결과는 네트워크 내에 분포하는 CA의 수나 이동 노드의 영역 내 체류시간, 업/다운 비율에 무관하게 나타난다. 임의의 CA 그룹의 경우 CA들에게 인증 정보를 업데이트하는 비용이 인증 요청 발생에 영향을 받는 반면에 인증 실패 비용이 작고, 홈 CA 방법이 경우 CA들에 대한 인증 정보 업데이트 비용이 낮으나 인증 실패 비용이 큰 것을 알 수 있었다.

이 논문의 결과로부터, 모바일 애드혹 네트워크에서는 효율적인 인증 메커니즘 확보를 위해 CA 기능을 분산시키고 인증 정보를 CA들 간에 효율적으로 공유하는 방법이 적합함을 알 수 있다. 이는 향후 다양한 애드 혹 네트워크 환경에 활용될 수 있다.

참 고 문 헌

[1] Y. Lee and Z. Haas, "Authentication in Very Large Ad Hoc Networks using Randomized Groups," 16th Annual IEEE PIMRC 2005, Berlin, Germany, Sep. 2005.

[2] N. Milanovic, M. Malek, A. Davidson and V. Milutinovic, "Routing and Security in Mobile Ad Hoc Networks," *IEEE Computer Magazine*, pp. 69-73, Feb. 2004.

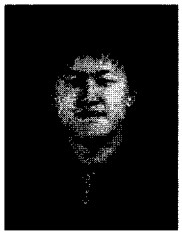
[3] S. Yi and R. Kravets, "Practical PKI for Ad Hoc Wireless Networks," Technical Report UIUCDCS-R-2002-2273/UILU-ENG-2002-1717 University of Illinois at Urbana-Champaign, May 2002.

[4] L. Zhou and Z. J. Haas, "Securing Adhoc

network," *IEEE Network Magazine*, pp.24-30, Nov/Dec 1999.
[5] S. Yi and R. Kravets, "MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks," 2nd PKI 03, Gaithersburg, Maryland, April 2003.
[6] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE 9th ICNP'01, 2001.
[7] H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "Self-securing Ad Hoc Wireless Networks" the Seventh IEEE ISCC'02, pp 567-574, 2002.
[8] S. Capkun, L. Buttyan and J. P. Hubaux, "Self-Orgainized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computings*, Vol. 2, No. 1, pp.52-64 Jan.-Mar. 2003.
[9] S. Capkun, L. Buttyan and J.-P. Hubaus, "Mobility Helps Security in Ad Hoc Networks," MobiHoc'03, Annapolis, USA. June 2003.
[10] M. C. Morogan and S. Muftic, "Certificate Management in Ad Hoc Networks," IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, USA. Jan. 2003.
[11] C. R. Davis and C. Crepeau, "A Certificate Revocation Scheme for Wireless Ad hoc Networks," 2003 ACM Workshop on SASN'03, Fairfax, VA, USA Oct 2003.
[12] T. Camp, J. Boleng and V. Davies, "A Survey of Mobility Models for Ad Hoc Networks Research," WCMC, vol.2, no.5, pp. 483-502, 2002.
[13] Z. J. Haas and Ben Liang, "Ad Hoc Location Management Using Quorum Systems," *ACM/IEEE Transactions on Networking*, Apr. 1999.
[14] Z. J. Haas and B. Liang, "Ad Hoc Mobility Management with Randomized Database Groups," IEEE ICC'99, Vancouver, Canada, June 1999.
[15] D. Balfanz, D.K Smetters, P. Stewart and H. C. Wong, "Talking to Strangers : Authentication in Ad-Hoc Wireless Networks," In Sysmposium on NDSS '02, San Diego, USA, Feb. 2002.
[16] S. Bhargava, D. P. Agarawal, "Scalable Security Schemes for Ad Hoc Networks," IEEE Milcom 2002, Anaheim, USA, Oct. 2002.

저 자 소 개

이 용(정회원)
1997년 연세대학교 컴퓨터과학과 (석사)
2001년 연세대학교 컴퓨터과학과 (박사)
1993년~1994년 디지콤정보통신 연구소
2001년~2003년 한국정보보호진흥원 선임연구원
2004년~2005년 코넬대학교 방문연구원
2005년~2007년 삼성전자 통신연구소 책임연구원
2007년~현재 충주대학교 전자통신공학전공 조교수
<주관심분야 : Mobile and Wireless Security, Ubiquitous Sensor Network, Wireless Mesh Network, Mobile Ad hoc network>



이 구 연(정회원)
1988년 KAIST 전기및전자공학과 (석사)
1993년 KAIST 전기및전자공학과 (박사)
1993년~1996년 디지콤정보통신 연구소
1996년 삼성전자
1997년~현재 강원대학교 컴퓨터학부 교수
<주관심분야 : 이동통신, 네트워크보안, 초고속통신망, ad-hoc 네트워크>