논문 2005-42TC-11-4

Mobile Ad Hoc Network에서 이동 노드에 대한 효율적인 인증 메커니즘

(Efficient Authentication for Mobile Nodes in Mobile Ad Hoc Network)

이 용*

(Yong Lee)

요 약

Mobile Ad Hoc Networks (MANETs)은 기존의 기반구조에 의존하지 않고 자치적으로 구성·운영되는 네트워크이다. 다른 네트워크 토폴로지에서처럼, 보안은 MANET의 사용 확산에 중요한 요소이며, 특히 노드들의 구성이 자주 빠르게 변하고, 기존의 기반구조에 대한 접속이 불가능한 MANET에서 이러한 특성을 지원하는 보안 프로토콜의 개발이 중요하다. 유선의 기반구조를 적용한 네트워크에서 이미 개발되어 사용 중인 신뢰 모델과 인증 프로토콜은 MANET에서 사용될 수 없다. 이 논문에서는 아주 넓은 지역에 걸쳐 분포된 이동 사용자에게 효율적인 인증 문제를 주제로 주목하고, 위와 같은 MANET 환경에 맞는 새로운 인증 방법을 제안한다. 제안된 방법은 노드들에게 CA(Certification Authority)의 기능을 분산시키고 CA이 기능이 구현된 노드들 사이에 인증 정보를 효율적으로 공유하기 위해 randomized group을 사용한다. 또한 randomized group을 적용한 인증 메커니즘의 성능을 평가한다.

Abstract

Mobile Ad Hoc Networks (MANETs) are self-organized networks that do not rely in their operation on wired infrastructure. As in any networking technology, security is an essential element in MANET as well, for proliferation of this type of networks. But supporting secure communication in MANETs proved to be a significant challenge, mainly due to the fact that the set of nodes in the network can change frequently and rapidly and due to the lack of access to the wired infrastructure. In particular, the trust model and the authentication protocols, which were developed for wired and infrastructure-based networks, cannot be used in MANETs. In this paper, we address the problem of efficient authentication of distributed mobile users in geographically large networks. In particular, we propose a new authentication scheme for this case of MANETs. The proposed scheme exploits Randomized Groups to efficiently share authentication information among nodes that together implement the function of a distributive Certification Authority (CA). We then evaluate the performance of authentication using Randomized Groups.

Keywords: 인증, 공개키, Randomized CA Group, 인증서, Mobile Ad Hoc Network

I. 개요 및 동기

이 논문에서는 지리적으로 노드들이 넓은 지역에 걸쳐 분포된 Mobile Ad Hoc 네트워크(MANET)에서의 인증 스킴에 대하여 논의한다. MANET은 기존의 기반

* 정회원, Cornell University
(School of Electrical Eng. Cornell University)
※ 이 논문은 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(M01-2004-000-10101-0)
접수일자: 2005년4월4일, 수정완료일: 2005년11월14일

구조에 의존하지 않고 자치적으로 구성되어 운영되는 네트워크이다. MANET에서는 노드들이 자주, 예상치 못하게 네트워크를 떠나거나 새로운 노드가 언제든지 네트워크에 참가할 수 있다. 다른 네트워크 토폴로지에서처럼, MANET의 확산을 위해서는 네트워크의 디자인과 운영에 적합한 보안 방안이 중요하다. MANET의 보안 스킴, 특히 인증 스킴의 디자인은 MANET이 어떤 기반구조에 대한 접근이 보장되지 않는데서 기인하며, 이로 인하여 *Key Distribution Center (KDC)* 같은 중앙 집중 시스템은 사용될 수가 없다. KDC의 부재에서 공유정보를 사용하는 대칭키 기반의 인증 메커니즘은 많은 이동노드들 사이에 효율적인 키분배 방안의 구현이 어려운 MANET에는 적합하지 않다. *Public Key Infrastructure (PKI)*는 동적인 네트워크에서 trust 구조 제공을 위한 인증방안으로 가장 성공적인 방법으로 인식되고 있다[1]-[4]. 유선 환경에서 널리 활용되는 공개키 암호방식에 기반한 PKI는 *Certificate Authority (CA)*가 필요하다. CA는 공개키와 소유자의 identity를 연결해주는 인증서에 서명한다. 그러나 고정된 기반구조로서가 아니라, 단일 CA가 이동노드들 사이에 존재하여야 하며 MANET의 네트워크 특성상 이 CA는 항상 접근이 보장되지는 않는다. 이 경우 노드에 대한 인증이 수행될 수 없으며 결과적으로 네트워크는 운영이 중단된다. 이러한 문제를 해결하기 위해, 이동노드들 사이에 CA의 기능을 분산하는 방법이 제안되었다[5]. 분산된 CA의 구현은 특히 MANET 환경의 구성에 따라 여러 가지 형태를 가지게 된다.

우리는 이러한 네트워크 환경에서 Randomized Group을 사용하여 노드들 사이에 CA의 기능을 분산시키는 방법을 제안하고, 지리적으로 넓은 지역에 노드들이 분포한 MANET에서 이를 사용하여 인증이 어떻게 디자인되는 지를 보여준다.

Ⅱ. 네트워크 모델 과 가정

우리는 이동 노드가 매우 넓은 지역에 걸쳐 널리 분포하고, 이는 다시 작은 지역으로 나눠지는 네트워크 모델을 가정한다. MANET에서 이동 노드들은 대륙사이를 이동할 수 있으며 빈번하게 네트워크를 떠나거나 다시 접속하게 된다. 많은 노드들 사이에 CA의 기능이 분산되므로(여기서는 CA의 기능을 수행하는 노드를 CA라고 한다) 이동 노드들이 네트워크에 접속하거나 떠나는 것은 CA가 동작하거나 다운되는 것에 해당한다. 그러므로 네트워크의 운영이 계속되기 위해서는 CA의 기능을 가진 노드가 네트워크를 떠나더라도 CA 기능이 지속될 수 있도록 CA 정보가 여러 노드들에게 중복되어야 한다.

이 논문에서는 분산된 CA에 의한 인증을 고려한다. 이 방안은 노드가 이리저리 돌아다니더라도 효율적으로 자신을 인증할 수 있도록 하며 특히, 네트워크 전체에 걸쳐 모든 CA가 인증서를 저장하는 부담을 피하도록 한다. 또한 이동 노드가 네트워크를 떠나거나 키가 노출되어서 인증서를 폐지할 경우에 이동 노드의 현재 위치에 상관없이 인증서를 폐지할 수 있도록 한다. 또한 일부 CA가 다운되더라도 CA의 기능이 항상 이용 가능하여야 한다. 노드들 사이에 CA를 유지하는 비용과 노드의 인증 실패로 인한 비용은 서로 상관관계가 있으므로, 위의 모든 기능은 최소의 비용으로 제공되어야 한다.

인증 서비스를 제공하기 위해서 CA는 다음의 기능을 수행하여야 한다.

- **인증서 발급** : CA는 자신의 영역 내에 있는 이동 노드에게 인증서를 발급하여야 하며 이동 노드 인증서의 유효기간이 만료되었을 때 이를 갱신하여야 한다.
- **인증서 폐지** : 이동 노드의 키가 노출되거나, 노드가 네트워크를 떠날 경우 이동 노드의 요청에 따라, CA는 인증서 폐지목록(Certificate Revocation List:CRL)을 발급하여야 하며 이를 다른 CA들에게 공지하여야 한다.
- **이동 노드의 인증** : 이동 노드의 요청에 따라 CA는 인증을 원하는 이동 노드에게 인증서를 발급한 CA의 공개키를 이동 노드에게 제공하여야 한다. 또한 CRL도 제공하여야 한다.
- **인증 정보의 공유** : CA는 이동 노드의 인증 정보를 다른 CA들에게 분산시키고 공유하여야 한다.

또한 보통의 이동 노드들은 악의적인 노드가 될 수 있고 신뢰될 수 없지만, CA들은 네트워크에서 모든 노드들에 의해 신뢰를 얻을 수 있고 이 신뢰는 *transitive* 된다고 가정한다. 이 논문에서는 이러한 가정에 대해서는 논의하지 않도록 하며 [5]에서 제안한 *threshold*

*cryptography*에 기반한다. 여기서는 CA 노드들이 Microsoft와 같은 *Globally Known Authenticator (GKA)*로부터 받은 인증서를 소유함을 가정한다.

Ⅲ. 제안하는 인증 방법

본 논문에서는 네트워크에 M개의 이동 노드가 있고, 그 중 N개의 노드가 CA가 된다고 가정한다. CA가 되는 노드들은 한 지역 내에서 노드들에 의해 random하게 선출된다. 만일 CA 노드가 다른 지역으로 이동하거나 battery 고갈 등으로 인하여 다운된다면, 그 지역의 노드들 중에서 새로운 CA가 선출된다. CA들은 자신의 영역내의 노드들에게 CA의 개인키로 서명된 인증서를 발급한다. 네트워크에는 많은 CA들이 존재하며 CA의 구성은 끊임없이 변하기 때문에, 인증서는 인증서를 발급하는 데 사용된 공개키가 공개된 동안 혹은 신뢰할 수 있는 방법으로 이를 얻을 수 있는 동안만 유효하다.

제안하는 인증 방안은 Randomized CAs Groups (RCG)를 이용하며, 여기서 각 그룹은 임의로 선택된 k개의 CA로 구성되고 두 개의 random group에는 적어도 r개의 CA가 겹칠 수 있다[6]-[8](그림 1은 RCG의 구성을 보여주는 네트워크의 예임).

제안하는 방법에서는 CA_1이 자신의 공개키와 CRL로 구성된 인증 정보(AUthentication Information :AUI)를 임의로 선택한 RCG_1 에 보낸다. 그러면 CA_1의 인증정보가 필요한 CA_2가 역시 임의로 선택한 다른 RCG_2에 정보를 요청한다. 두 RCG 내의 일부 CA들의 중복으로 인하여, CA_2가 CA_1의 AUI를 얻을 수 있는 확률이 있으며 시스템이 적절하게 구성된다면, 이 확률은 충분히 높게 되고 이동 노드가 인증에 실패하여 지불하게 될 비용은 매우 낮게 될 것이다. CA_1은 정보 요청의 질의를 받은 RCG_2내에 위치할 필요가 없으며 CA_1의 AUI를 가진 노드만이 RCG_2내에 존재하면 될 것이다. 이는 CA_1의 AUI가 네트워크에 전파되기 때문이다. AUI 정보가 최신 정보임을 확인하기 위하여(특히 CRL의 경우), AUI는 유효기간 정보를 포함하고 AUI가 유효한 정보임을 확인하기 위하여, *GKA*에 의해 서명된 CA의 인증서가 포함되며 AUI는 CA의 개인키로 서명된다. 만일 randomized group이 적절하게 구성된다면, 일부 CA가 다운되더라도, 필요한 AUI는 RCG를 구성하는 다른 CA들로부터 얻어질 수 있다. CA의 AUI는 다음의 두 가지로 구성된다 : [(CA의 공개키, CRL)$_{\text{CA의 개인키로 서명}}$, (CA의 인증서)$_{\text{GKA나 혹은 네트워크의 다른 신뢰된 CA가 서명}}$]. CA가 아닌 이동 노드의 AUI는 다음의 두 가지로 구성된다 : [이동 노드의 인증서를 발급한 CA의 공개키와 이동 노드의 CRL]. 이동 노드의 CRL은 CA들에게 분산된다.

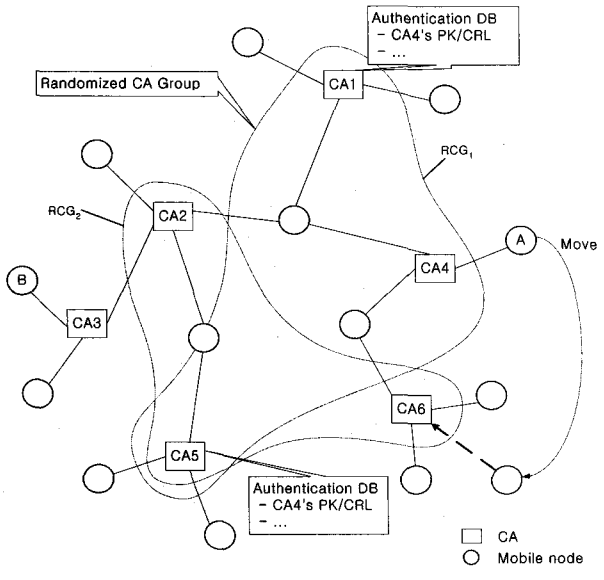


그림 1. RCG 구성을 보여주는 네트워크 예
Fig. 1. An example of a network with some selected RCGs.

이동 노드는 자신의 홈 영역을 지원하는 CA로부터 인증서를 받는다. 이동 노드가 홈 영역을 떠날 때, CA는 이동 노드의 AUI를 임의로 선택된 k CA로 구성된 RCG에 전달한다(write operation). 이동 노드가 다른 CA의 영역으로 이동한 후, 이동 노드는 새로운 CA에게 자신의 인증서를 보내서 자신을 등록한다. 인증서를 인증하기 위해 새로운 CA는 인증서를 발급한 home CA의 공개키가 필요하며 인증서가 폐지되었는지를 검증하여야 한다. 새로운 CA는 임의로 선택된 k CA의 RCG에 질의를 보내서 home CA의 공개키와 CRL를 포함한 home CA의 AUI를 얻는다.

CA가 RCG로부터 이동 노드의 AUI를 얻으면 CA는 인증서를 발급한 CA의 공개키를 사용하여 인증서의 서명을 검증하고, CRL sequence number를 이용하여 질의한 RCG의 CA들로부터 받은 CRL을 검사하고 최신의 CRL를 구성한 후에 인증서가 폐지되었는지를 검증한다.

인증서 폐지는 이동 노드가 현재 위치한 영역을 지원하는 CA에 폐지 요청을 보냄에 따라 처리된다. 폐지

요청은 이동 노드의 개인키로 서명되고 CA는 서명을 이용하여 폐지 요청의 무결성을 확인할 수 있다.

네트워크가 유지되는 동안, CA가 다운되거나 다른 지역으로 이동하면, 그 지역의 노드들이 새로운 CA를 선출한다. 새로 선출된 노드는 이전 CA가 서명한 인증서를 가지기 때문에 다른 CA들에 의해 인증을 받을 수 있으며, 이전 CA가 수행한 CA의 역할을 수행하게 된다. 새로 선출된 CA는 자신의 AUI를 RCG에 write한다. 이전 CA가 이미 RCG에 자신의 공개키를 write 하였기 때문에 이전 CA에 의해 발급된 인증서는 여전히 인증될 수 있다. 이러한 과정은 앞에서 언급한 trust transitive에 의해 가능하며 따라서 새로 선출된 CA가 되는 이동 노드의 인증서는 다른 CA들에 의해 검증이 가능하다.

Ⅳ. 성 능 평 가

이 절에서는 시뮬레이션을 통하여 RCG를 사용한, 제안하는 인증 메커니즘의 성능을 평가하도록 한다. 이 방법에서 CA는 자신의 영역의 이동 노드들에게 인증서를 발급하고 임의로 선택된 RCG에 이동 노드의 AUI를 전송한다. 인증서가 폐지될 때마다 CRL를 갱신하고 갱신된 CRL을 역시 임의로 선택된 RCG에 전송한다. 한 CA는 자신의 coverage 내의 모든 이동 노드에게 인증서를 발급하며 이동 노드는 random mobility model에 따라 CA들의 영역을 이동한다.

CA를 포함하여 모든 이동 노드는 각각 지수분포를 갖는 평균시간 t_U와 t_D초 동안 UP과 DOWN을 반복한다. CA가 T초 동안 다운되면, 다운된 CA와 같은 영역에 속하는 새로운 이동 노드가 다운된 CA를 대신하도록 임의로 선출되며, 다운된 CA는 CA가 아닌 이동 노드가 된다. 이동 노드가 CA의 영역에 머무르는 residence 시간은 평균 t_M 초의 지수분포를 가진다. CA가 자신의 영역을 떠나면 보통의 이동 노드가 되고 한 영역 내에서 CA 가 영역을 떠났는지를 결정하는 과정은 [10]을 따른다.

AUI를 write하고 read할 k개의 RCG는 임의로 선택되며 제안하는 방안의 성능을 평가하기 위해 이 논문에서는 최적의 k 값을 구할 것이다.

이동 노드들은 임의로 선택된 다른 이동 노드로 호를 요청하며 call origination은 λ_O call/sec의 평균속도를 갖는 Poisson process가 된다. 인증서 폐지 요청은 평균 속도 $\lambda_R$revocation/sec의 지수분포로 모든 노드들에서 발생한다. CA는 자신의 영역 내에 위치하는 노드의 인증서를 폐지할 수 있고 CRL을 갱신한 후에 임의의 RCG에 CRL을 전송한다. 지수분포를 갖는 시간 t_i sec 후에, 이동 노드는 현재 자신이 위치한 영역의 CA에 새로운 인증서 발급을 요청한다. 만일 CA의 인증서가 폐지되고t_i가 T보다 길다면, 그 CA는 CA로서의 기능을 중지하고 해당 영역 내에 새로운 CA가 선출된다.

노드의 인증서 유효기간이 만료될 경우 해당 노드가 위치한 영역의 CA에게 이동 노드가 유효기간 만료이전에 인증서 발급을 요청하여 갱신한다.

1. 성능 평가 파라미터

이 논문에서는 다음 두개의 성능 평가 기준을 고려한다. 첫 번째는 노드의 인증 실패로 인한 비용과 CA에서 인증정보 유지로 인한 비용으로 구성된 *Total Cost* 이다. 두 번째 기준은 시스템의 신뢰성으로 인증 요청이 성공할 확률로 계산되며 만일 질의를 받은 RCG가 최신의 AUI를 포함한다면 인증 요청은 성공한다. *Total Cost*는 다음의 식과 같이 구성된다.

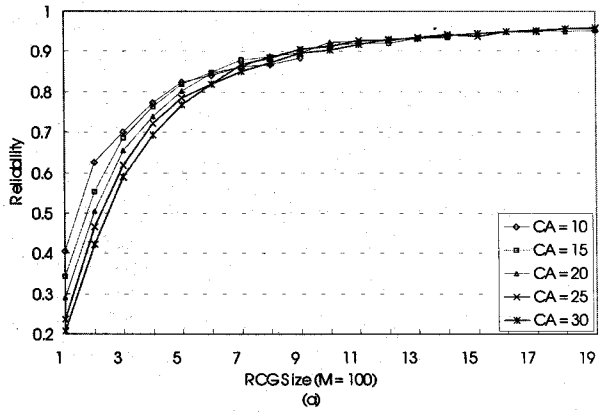
$$\text{Total Cost} = C_l \cdot E_{fail} + C_u \cdot E_{write} \quad (1)$$

여기서, C_l 은 인증 실패로 인한 기대 비용이며, C_u 는 인증 정보를 write하기 위해 한 CA를 access하는 기대 비용, E_{fail} 은 초당 실패한 인증 요청의 총 수, E_{write} 는 초당 CA에 AUI를 write한 총 수 이다. 우리는 [6][7]에 따라 $C_l = 100$ 과 $C_u = 1$ 로 가정한다. *Reliability*는 다음과 같이 계산된다.

$$Reliability = \frac{Number\ of\ successful\ authentications}{Number\ of\ authentication\ requests} \quad (2)$$

2. 성능 평가 결과

우리는 이동 노드의 이동 모델로서 *Random Waypoint* 모델을 적용하여 시뮬레이션을 수행하였다[9]. <그림 2>와 <그림 3>은 각각 *Reliability* 와 *Total Costs*에 대한 결과를 보여준다. <그림 2>에서 이동 노드 수의 증가와 RCG를 구성하는 CA 그룹 크기의 증가에 따라 *Reliability*도 증가함을 알 수 있다. 이 이유는 RCG의 크기가 증가함에 따라 RCG가 원하는 인증정보를 가질 확률도 증가하기 때문이다.



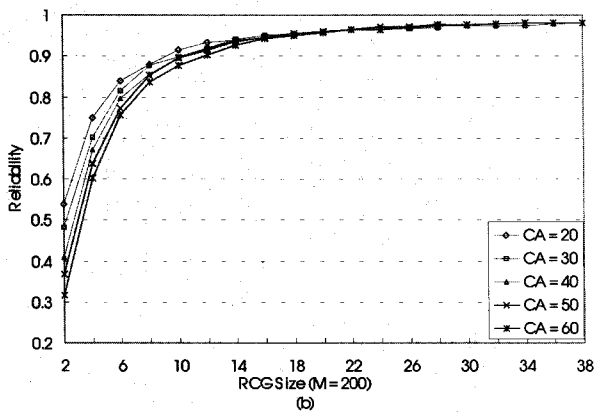
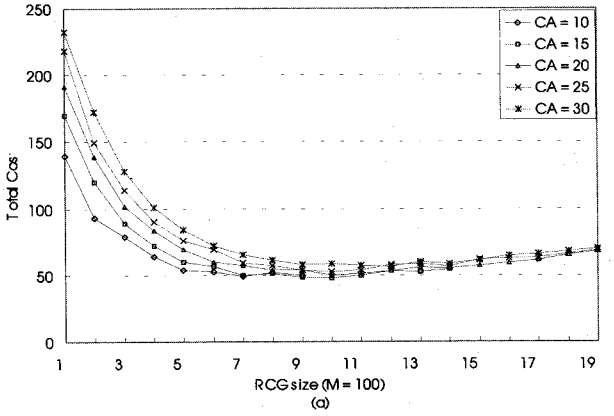


그림 2. 이동 노드의 수가 (a) 100일 때 (b) 200일 때, 제안하는 방법의 *Reliability*

Fig. 2. The *Reliability* metric, for the number of MNs (a) 100 and (b) 200.



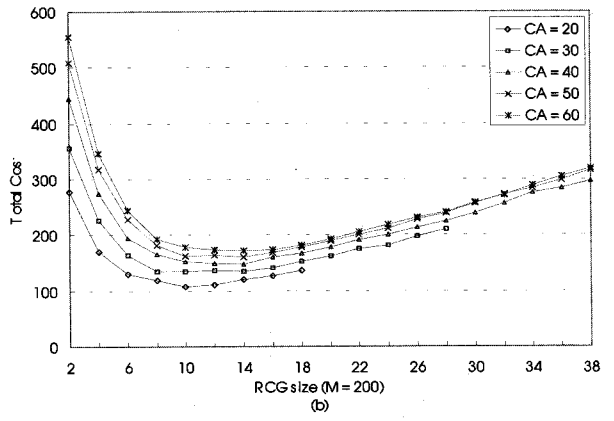


그림 3. 이동 노드의 수가 (a) 100일 때 (b) 200일 때, 제안하는 방법의 *Total cost*

Fig. 3. The Total cost metric, for the number of MNs (a) 100 and (b) 200.

<그림 3>에서는 *Total Cost*가 RCG 크기에 따라 최소값을 가짐을 보여준다. RCG 사이즈가 작을 때는 *Reliability*가 낮기 때문에, 즉, E_{fail} 가 크므로, *Total Cost*는 큰 값을 갖게 된다. 그룹 사이즈가 증가함에 따라 *Reliability*도 향상되므로 E_{fail} 가 작아지고 *Total Cost*도 증가한다. 그러나 그룹 사이즈가 너무 크게 되면, CA에 대한 업데이트의 횟수가 증가하므로 *Total Cost*는 다시 증가하게 된다. <그림 3>에서는 이동 노드의 수에 무관하게 RCG의 크기가 10 - 12 일 때, *Reliability*는 안정되고, *Total Cost*는 최소화됨을 알 수 있다.

<그림 4>에서는 총 이동 노드의 수가 200이고, CA의 수가 40(총 노드수의 20%)일 때, 이동 노드의 residence time 변화에 따른 *Reliability*와 *Total Cost*를 보여준다. 여기서도 *Reliability*는 노드의 residence time에 상관없이 그룹 사이즈가 10 - 12 범위일 때 안정화되고 *Total cost*는 최소화된다. 그러므로 우리는 CA의 영역 내에서 MN의 residence time에 상관없이 RCG 크기가 10 - 12일 때 제안하는 방안이 최적임을 알 수 있다. 이러한 결과는 RCG의 크기를 선택하는데 노드의 이동 속도가 영향을 주지 않음을 보여준다.

<그림 5>는 최적의 RCG 사이즈를 선택하는데 대한 노드의 UP과 DOWN period 변화의 효과를 보여준다. 역시 200 개의 노드와 CA의 수가 40(총 노드 수의 20%)인 경우를 고려하였다. UP period가 DOWN period보다 짧을 때 즉, 네트워크의 연결이 상대적으로 불안정할 때, *Reliability*는 낮고 *Total Cost*는 높다. UP period가 증가함에 따라, 최적의 효과를 보여주는 그룹 사이즈는 감소한다. <그림 5(b)>에서 UP period가 UP/DOWN cycle의 80%인 경우에, *Total Cost*는 그룹 사이즈, k가 10일 때 최소화된다. UP period가 60%, 50%, 40%로 감소할 때, 그룹 사이즈, k = 12, 18, 22일 때 각각 최소화된 *Total Cost*를 얻을 수 있다. 이유는 노드들의 UP period가 더 짧을 때에는, 인증정보에 대

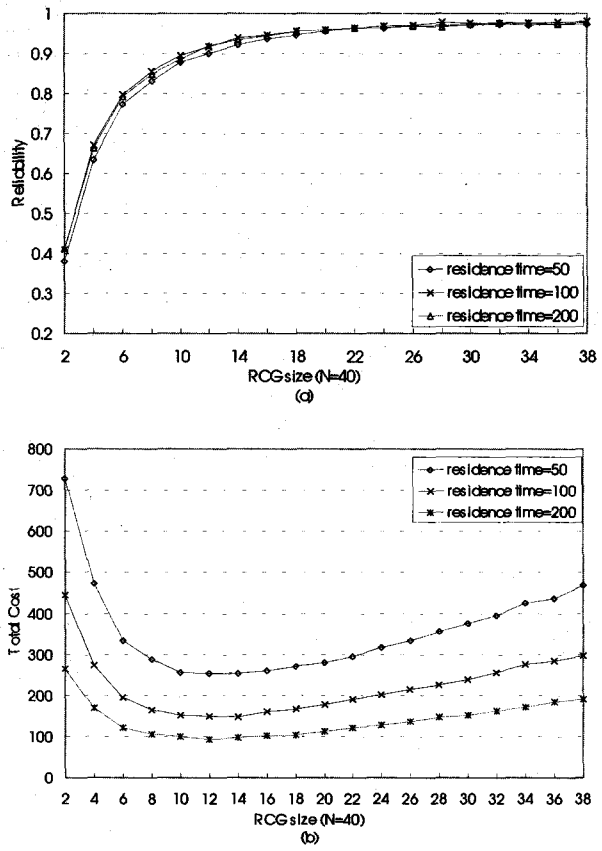


그림 4. 이동 노드의 수가 200, CA의 수가 40일 때, residence time 에 따른 *Reliability*와 *Total Cost*

Fig. 4. The *Reliability* and *Total Cost* metrics, for 200 MNs and for 40 CAs, when the residence time is a parameter.

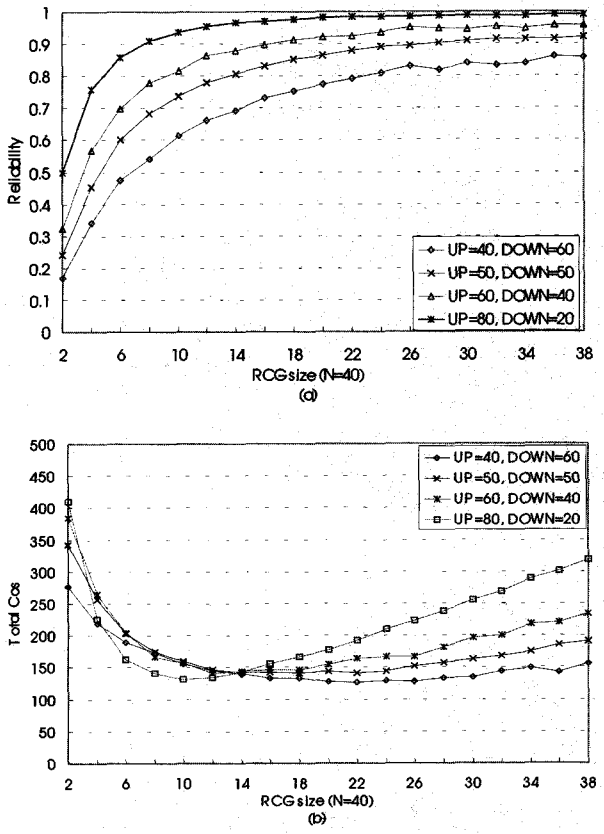


그림 5. 노드의 수가 400, CA의 수가 40일 때, UP/DOWN 비율에 따른 *Reliability*와 *Total Cost*

Fig. 5. The *Reliability* and *Total Cost* metrics, for 200 MNs and for 40 CAs, when the ratio *UP/DOWN* is a parameter.

한 질의를 받는 그룹 사이즈, 즉 CA의 수가 많아야 인증정보를 얻을 확률이 커진다는 것을 의미한다.

또한 RCG의 크기가 작을 때는 인증 실패로 인한 비용이 RCG의 크기의 영향을 덜 받는다. 그러나 RCG의 크기가 증가함에 따라, *Reliability*는 UP period가 짧을 때 비해 클 때에 빠르게 증가한다. 이로 인하여 인증 실패로 인한 비용도 업데이트의 횟수가 증가로 인한 비용보다 빠르게 감소하게 된다. 이러한 현상은 RCG를 구성하는 CA의 수가 증가함에 따라 업데이트 횟수가 증가하게 되고 *Reliability*의 안정화로 인증 실패로 인한 비용은 효과가 미미하게 되는 시점까지 계속된다. 이후에는 다시 UP period가 길어질수록 *Total Cost*도 증가함을 보여준다. 이러한 현상을 보여주는 교차점은 그룹 사이즈가 14일 때 발생한다.

Ⅳ. 결 론

이 논문에서는 Mobile Ad Hoc Network에서 이동 노드에 대한 인증 방안을 제안하였다. 제안하는 네트워크 모델은 이동 노드가 네트워크로부터 자주 연결이 끊어지고 지리적으로 넓은 지역을 이동한다고 가정하며 이동 노드들이 네트워크의 다른 노드들과 안전하게 통신하기 위하여 인증을 요청한다고 가정하였다.

제안하는 인증 방안은 인증서와 공개키 암호시스템, CA 기능이 네트워크의 여러 이동 노드들에게 분산되는 모델을 적용하였다. 각 CA들은 자신의 영역을 가지며 영역내의 노드들에게 인증서를 발급한다. 노드가 네트워크를 이리저리 이동함에 따라, 이들은 새로운 영역내에서 자신을 인증하기 위하여 인증 정보를 요구하게 된다. 즉, 먼 거리로 이동한 노드들도 자신의 인증서가 먼 거리에 위치한 홈 CA에 의해 발급되었더라도 자신을 효율적으로 인증할 수 있어야 한다.

제안하는 인증 방안은 *Randomized CAs Group (RCG)*을 기반으로 하며, 이는 CA 가 임의로 선택되어 그룹을 구성하고, 한 CA가 여러 개의 그룹에 동시에 속할 확률이 크다. RCG는 이동 노드의 인증정보가 업데이트되며 (*write* operation), 인증정보에 대한 질의 (*read* operation)를 받게 된다. 최적의 CA수로 구성된 RCG를 디자인하는 것은 제안하는 방안의 성능에 영향을 끼치게 되며, 우리는 이를 위하여 *Total Cost*와 *Reliability*의 두 가지 성능 평가 기준을 정하고 다양한 파라미터 변화에 따른 결과를 시뮬레이션을 통하여 분석하였다. 또한 위의 두 가지 기준이 RCG의 크기에 따라 어떠한 영향을 받는지를 다음의 파라미터 변화에 따라 보여주었다 : 네트워크의 총 노드의 수, CA의 수, CA의 영역 내의 이동 노드의 residence time, 이동 노드의 UP/DOWN time periods의 비율.

결론적으로 제안하는 인증 방안은 UP/DOWN ratio 가 60%보다 클 때에 네트워크 내의 이동 노드의 수와 CA의 수에 상관없이 RCG의 크기가 10 - 12 사이일 때, 우수하게 동작함을 알 수 있다.

참 고 문 헌

[1] Seun Yi and Robin 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.

[2] Haiyun Luo, Jiejun Kong, Petros Zerfos, Songwu Lu, and Lixia Zhang, "Self-securing Ad Hoc Wireless Networks," *the Seventh IEEE Symposium on Computers and Communications (ISCC'02),* pp 567-574, 2002.

[3] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactionson Mobile Computing,* Vol. 2, No. 1, pp. 52-64. Jan-Mar 2003.

[4] Matei C. Morogan and Sead Muftic, "Certificate Management in Ad Hoc Networks," *IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet,* Orlando, January 2003.

[5] Lidong Zhou and Zygmunt J. Haas, "Securing Ad hoc network," *IEEE Network Magazine,* pp. 24 -30, Nov/Dec 1999.

[6] Zygmunt J. Haas and Ben Liang, "Ad Hoc Location Management Using Quorum Systems," ACM/IEEE Transactions on Networking, April 1999.

[7] Zygmunt J. Haas and Ben Liang, "Ad Hoc Mobility Management with Randomized Database Groups,'' *IEEE ICC'99,* Vancouver, Canada, June 1999.

[8] J. Li, Z. J. Haas and B. Liang, "Performance Analysis of Random Database Group for Mobility Management in Ad hoc Network," *IEEE International Conference on Communications (ICC) 2003,* Anchorage, May 2003.

[9] Tracy Camp, Jegg Boleng and Vanessa Davies, "A Survey of Mobility Models for Ad Hoc Networks Research," *Wireless Communication and Mobile Computing (WCMC),* vol. 2, no. 5, pp. 483-502, 2002.

[10] Ben Liang and Zygmunt J. Haas, "Virtual Backbone Generation and Maintenance in Ad Hoc Mobility Management," *IEEE INFOCOM'2000,* Tel Aviv, Israel, March, 2000.

저 자 소 개

이 용(정회원)

1997년 연세대학교 컴퓨터과학과 (석사)

2001년 연세대학교 컴퓨터과학과 (박사)

1993년~1994년 디지콤 정보통신 연구소 연구원

2001년~2003년 한국정보보호진흥원 전자서명인증관리센터 선임연구원

2004년~현재 코넬대학교 방문연구원

<주관심분야 : 이동통신, Wireless PKI, Mobile Ad Hoc 네트워크, Mobile Ad hoc 네트워크 보안>