논문 2009-46TC-8-4

모바일 애드혹 네트워크에서 랜덤 CA 그룹을 이용한 인증 알고리즘에 대한 성능 분석

(Numerical Analysis of Authentication Algorithm using Randomized CA Groups in Mobile Ad Hoc Networks)

이 용*, 이 구 연**

(Yong Lee and Goo Yeon Lee)

요 약

모바일 애드혹 네트워크는 유선 환경 기반구조의 도움없이 이동 노드에 의해 자치적으로 자가조직되는 구조이다. 이동 노드가 모바일 애드혹 네트워크를 구성하기 위해서는, 라우팅 정보같이 네트워크의 관리에 필요한 정보들이 이동 노드들 간에 자치적으로 전달되는 특성으로 인해, 네트워크의 보안이 중요한 주제이다. 특히 네트워크를 구성하는 이동 노드들이 서로를 신뢰하는데 기반이 되는 인증 메커니즘은 필수적이다. 우리는 [1]에서 분산된 이동 노드들 간의 효율적인 인증을 위하여 랜덤 그룹을 이용한 인증 메커니즘을 제안하였다. 이 논문에서는 [1]에서 제안한 메커니즘의 성능을 분석하고 그 결과를 시뮬레이션 결과와 비교하였다. 성능 분석 결과는 모바일 애드혹 네트워크를 구성하는 이동노드나 CA의 수에 상관없이 랜덤 CA 그룹의 크기가 10-12일때, 최저의 비용으로 인증 메커니즘이 동작함을 보여주며, 추후 분산 인증 체계에서 공개키 방식을 적용하는 경우의 분석 모델로 활용될 수 있다.

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 [1], we addressed the problem of efficient authentication of distributed mobile users in geographically large networks and proposed 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). In this paper, we analyze numerically the performance of authentication method using randomized groups and compare with the simulation result.

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

* 정회원, 충주대학교 전자통신공학전공
(Dept. of Electron. and Comm., ChungJu National University)
** 정회원, 강원대학교 컴퓨터학부
(Dept. of Computer Eng. Kangwon National University)
※ 이 논문은 충주대학교 대학구조개혁지원사업비(교육과학기술부 지원)의 지원을 받아 수행한 연구임
접수일자: 2009년1월28일, 수정완료일: 2009년8월10일

I. 서 론

모바일 애드혹 네트워크는 기존의 유선 기반 인프라의 도움없이 많은 이동 노드들에 의해 자가조직되어 운영된다. 즉, 임의의 이동 노드가 모바일 애드혹 네트워크의 구성원이 되므로 이동 노드들간의 신뢰는 네트워

크가 안정화되는데 매우 필수적이다. 언급한 바와 같이 모바일 애드혹 네트워크는 고정된 인프라를 갖지 않으므로 인프라에 기반한 전통적인 인증 메커니즘을 적용하기가 적합하지 않다. 또한 이동 노드들이 자주 이동하며 전력의 제한이나 무선 주파수의 특성으로 인해 네트워크에 대한 접속과 단절 현상을 빈번하게 반복하므로 모바일 애드혹 네트워크는 다양한 공격에 매우 취약하다[1~5]. 이로 인하여 공격자는 비밀정보를 도청하거나 네트워크 신뢰를 깨뜨리는 것이 가능하고, 악의적인 노드가 네트워크를 직접 공격하여 메시지를 위조하거나 정당한 노드인 척 가장하여 인증과정을 위장하고 네트워크에 참가하여 공격을 하는 것도 가능하다. 이런 문제를 해결하기 위해서는, 무엇보다도 네트워크가 인증된 노드에 대해서만 접속을 허용하는 인증 스킴이 중요하다[5~7].

공유된 비밀정보를 이용하는 대칭키 메커니즘은 수많은 이동 노드들 사이에 키분배를 해야하는 문제로 인하여 모바일 애드혹 네트워크에 적합하지 않은 방법이다. 뿐만아니라 모바일 애드혹 네트워크는 어떠한 인프라도 갖지 않으므로 키분배센터(Key Distribution Center)와 같은 중앙집중식 시스템도 적용할 수가 없다. 현재까지 공개키 기반 구조(PKI : Public Key Infrastructure)는 동적인 네트워크 환경에 인증 방식을 제공하여 신뢰의 기반을 제공하는 가장 성공적인 방법의 하나로 알려져 있다[5~6]. 그러나 유선망 환경에서 널리 사용되는 공개키 알고리즘에 기반한 PKI 방식조차도 공개키와 그 소유자를 연결하는 인증서에 서명해주는 인증기관(CA : Certificate Authority)과 같은 고정된 인프라를 필요로 하므로 모바일 애드혹 네트워크 환경에 적합하지 않다[5~6]. 공개키 기반 구조의 CA의 역할이 이동 노드들에게 분산될 수 있다면, 여러 CA가 발급한 이동 노드의 인증서를 어떻게 검증할 것인가 하는 것이 어려운 문제이다[5, 9~10]. 그러므로 모바일 애드혹 네트워크에서의 인증방식을 위해 공개키 알고리즘과 인증서가 적용될 때, 인증서를 발급하는 CA들이 서로를 인증하는 방식이 중요한 주제가 된다.

Ⅱ. 제안하는 방법

[1]에서 우리는 랜덤 CA 그룹을 이용하여 모바일 애드혹 네트워크에서의 인증 방법을 제안하였다. 이 방법은 CA들이 임의의 크기의 그룹을 구성하고 하나의 CA는 여러 개의 CA그룹에 속할 수 있다. 즉, 랜덤하게 선택된 두 그룹은 서로 오버랩되는 CA가 생기게 된다. 오버랩된 CA들은 자신이 속한 하나의 그룹으로부터 인증 정보를 얻어서 역시 자신이 중복해서 속한 다른 그룹에 그 정보를 전파하게 된다. 랜덤 CA 그룹은 말그대로 랜덤하게 CA를 선택하게 되고, 이 CA 노드들이 네트워크 영역 전체를 여기저기 돌아다니게 되므로, 처음에는 네트워크의 일부 CA들이 공유한 어떤 CA의 공개키와 CRL과 같은 인증 정보들이 전체 네트워크에 걸쳐서 널리 퍼지게 되고 모든 이동 노드들이 이용할 수 있게 된다. 랜덤 그룹의 크기가 최적으로 결정된다면, 일부 CA가 다운되더라도 인증정보들은 적절하게 유지되고 이동 노드들이 필요로 하는 정보들은 구할 수 있게 된다. 따라서 다음과 같은 모델을 가정한다.

○ 모바일 애드혹 네트워크가 생성될 때, 이동 노드중에 일부는 CA로 선택된다.

○ 모든 이동 노드들은 가장 가까운 CA로부터 하나의 인증서를 발급받고 그 CA를 홈 CA로 정한다.

○ CA는 노드들에게 인증서와 CRL을 발급하고 자신의 DB에 노드의 인증 정보를 저장한다.

○ 인증서는 CA가 서명하며 CA들은 자신이 발급한 인증서가 아니더라도 임의의 인증서에 대해 CRL을 발급할 수 있다.

○ 인증 정보는 CA의 공개키, CRL 정보와 정보가 갱신된 시간을 나타내는 일련번호로 구성된다. 즉, 노드 A의 인증 정보는 노드 A의 인증서에 서명한 CA의 공개키와 여러 CA들에 의해 분배된 CRL로 구성된다.

Ⅲ. 제안하는 모델의 시나리오

1. 랜덤 CA 그룹의 구성

제안하는 방법에서 랜덤 CA 그룹은 다음과 같이 구성된다.

■ 이동 노드들 중에 일부가 CA로 선택된다. CA는 자가서명한 자신의 인증서를 발급한다. CA들이 처음

랜덤 CA 그룹을 형성하고 통신할 때는 널리 알려진 CA가 발급한 인증서를 사용하여 서로를 인증한다. 최초의 신뢰 이후에 CA들은 상대 CA의 자가서명한 인증서를 사용하여 서로를 인증하고 널리 알려진 CA가 발급한 인증서를 더 이상 사용하지 않는다.

■ 랜덤 CA 그룹을 구성하는 CA는 임의로 선택된다.

■ 만약 CA가 정해진 시간 이상 다운된다면, 그 옆에 있는 임의의 노드가 다운된 CA를 대신하여 CA로 선택된다.

■ n개의 CA가 있고 랜덤하게 선택된 k개의 CA들이 랜덤 CA 그룹(RCG : Randomized CA Group)을 구성하여 이동 노드에 대한 인증 정보를 공급받아 저장하게 된다.

- 해당 이동 노드가 홈 CA에 인증 정보 등록을 요청하는 경우 홈 CA는 다른 CA들에게 해당 이동 노드의 인증정보를 알려주기 위해 접근가능한 랜덤 CA 그룹(RCG)를 이용하게 된다.
- 이동 노드가 어떤 CA의 영역으로 이동하였을때, 이동 노드는 이동한 영역의 CA에게 인증을 요청하고 그 CA는 앞의 경우와 유사하게 랜덤하게 선택된 접근가능한 k개의 CA 그룹에 그 이동 노드의 인증 정보를 요청하는 질의를 보내게 된다.
- CA가 RCG로부터 이동 노드에 대한 인증 정보를 획득한 경우, 그 CA는 이동 노드에게 인증서를 발급한 CA의 공개키를 이용하여 인증서의 서명을 검증하고, RCG로부터 받은 CRL과 일련번호를 이용하여 최신의 CRL을 구성한 후에 이를 조사하여 인증서가 폐지되었는지를 확인한다.

2. RCG를 이용한 인증 시나리오

이 절에서는 이동 노드와 CA의 구체적인 동작을 살펴보고자 한다. 먼저 두 개의 랜덤 CA 그룹의 동작을 고려해 보자.

■ 인증서 발급(그림 1)

- $node_A$가 모바일 애드혹 네트워크에 참가하고자 할 때, 가장 가까운 CA인 CA_4로부터 인증서를 발급받는다.

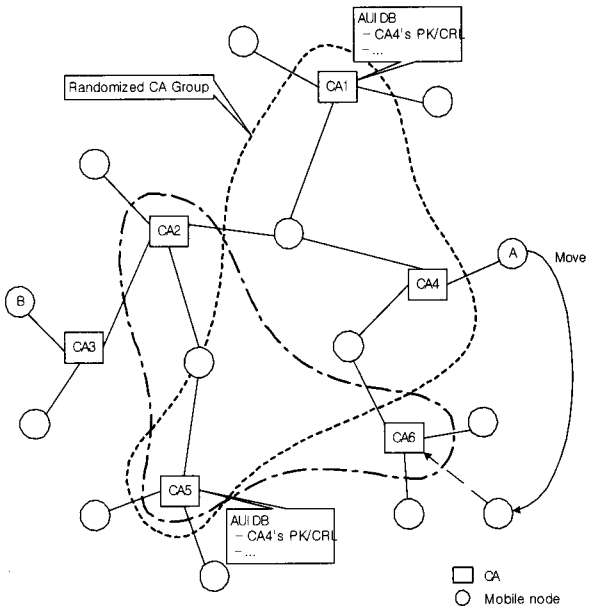

그림 1. 랜덤 CA 그룹의 구성 예
Fig. 1. Example : Randomize CA Group.

■ 인증 등록 요청(그림 1)

1. $node_A$가 다른 영역에서 자신의 인증서를 사용하기 전에(예. $node_A$가 CA_6의 영역으로 이동하거나 $node_A$가 다른 영역에 있는 임의의 노드와 통신하고자 할 때) $node_A$는 CA_4에 먼저 인증 정보 등록을 요청한다.
2. CA_4는 $node_A$의 인증 등록 요청에 따라 접근가능한, 랜덤하게 선택한 CA 그룹(예. CA_1, CA_4, CA_5)에 $node_A$의 인증 정보를 전송한다.
3. 랜덤 CA 그룹 (예. CA_1, CA_4, CA_5)은 $node_A$의 인증 정보를 얻게 되고 CA_1와 CA_5는 다른 RCG의 요청에 따라 $node_A$에 대한 인증 정보를 알려줄 수 있게 된다.

■ $node_A$가 CA_6의 영역으로 이동한 경우에(그림 1)

1. $node_A$는 CA_6에게 인증을 요청한다. 이 인증 요청은 $node_A$의 인증서를 포함한다.
2. CA_6는 $node_A$에 대한 인증 정보를 얻기 위해 접근가능한 랜덤 CA 그룹(예. CA_2, CA_5, CA_6)에 질의를 보낸다.
3. CA_2와 CA_5, CA_6는 $node_A$에 대한 인증 정보를 자신의 DB에서 검색하고 $node_A$에 대한 인증정보(CA의 공개키, CRL)를 가진 CA_5는 이를 CA_6에게 보내준다.
4. CA_6는 $node_A$의 공개키와 CRL를 이용하여 $node_A$

의 인증서를 검증하며 $node_A$를 인증한 후에 $node_A$의 접속을 승인하게 된다.

■ $node_A$가 CA_6의 영역에 머무르는 동안 자신의 인증서를 폐지하게 되는 경우(그림 2)

1. $node_A$는 CA_6에 자신의 인증서에 대한 폐지 요청을 보낸다.
2. CA_6는 자신의 CRL에 $node_A$를 추가하고 CRL에 서명한다.
3. CA_6는 접근가능한 랜덤 CA 그룹(예. CA_1, CA_2, CA_6)에 자신의 CRL을 업데이트한다.
4. CA_1와 CA_2는 최신의 CRL을 전송받게 된다.

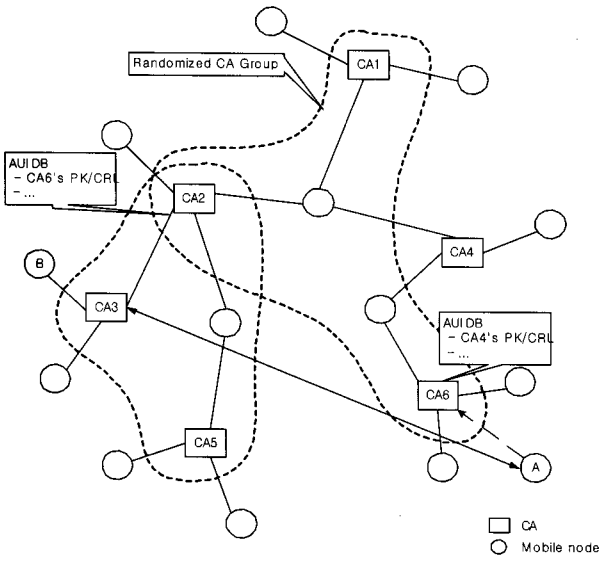

그림 2. 랜덤 CA 그룹의 동작 예
Fig. 2. Example : Randomized CA Group Operation.

■ $node_A$가 CA_3의 영역에 있는 $node_B$와 통신하고자 할 때 (그림 2)

1. $node_A$는 $node_B$에게 자신을 인증하기 위해 인증서를 보낸다.
2. $node_B$는 $node_A$의 인증서를 받는다.
3. $node_B$는 가장 가까운 CA인 CA_3에게 $node_A$의 인증 정보를 요청한다.
4. CA_3은 접근가능한 랜덤 CA 그룹(예. CA_2, CA_3, CA_5)에게 $node_A$에 대한 인증 정보를 요청한다.
5. CA_2와 CA_5가 $node_A$의 인증 정보를 가지고 있으므로 그들은 정보를 CA_3에게 보내준다.
6. CA_3은 CA_2과 CA_5의 응답을 받은 후에 CA_2의 정보와 CA_5의 정보의 일련 번호를 검사하여 최신 정보를 선택한다. 이 예에서는 CA_5가 $node_A$의 인증서가 폐지되기 전의 인증 정보를, CA_2는 폐지된 $node_A$의 인증서에 대한 정보를 가지고 있다. CA_3은 정보의 일련 번호를 통해 최근 정보를 알아내고 CA_2로부터 $node_A$를 포함하는 CRL을 얻어서 최신의 CRL을 구성하게 된다.
7. CA_3은 $node_B$에게 최신의 인증 정보를 알려주게 된다.
8. $node_B$는 $node_A$의 인증서의 서명을 검증하고 CRL을 검사한다.
9. $node_B$가 $node_A$에 대한 인증이 성공하면, $node_B$는 $node_A$에게 응답을 보내고 $node_A$에게 자신의 인증서를 보낸다. $node_A$는 동일한 과정을 반복하여 $node_B$를 인증한다.
10. $node_A$에 대한 인증이 실패한다면 $node_B$는 $node_A$의 요청을 거절한다.

CA들은 다음과 같은 경우에 랜덤하게 선택된 k개의 CA들을 이용하여 인증 정보를 교환하게 된다.

■ 이동 노드가 인증서를 갱신하는 경우
■ 인증서 폐지에 의해 CRL이 갱신된 경우
■ 이동 노드가 다른 CA의 영역으로 이동하여 인증을 요청하는 경우
■ 이동 노드가 다른 노드로부터 받은 인증서를 검증하는 경우

다음은 제안하는 방법의 장점을 살펴보고자 한다. 먼저 이동 노드들은 전체 모바일 애드혹 네트워크에서 오직 하나의 인증서만 사용할 수 있다. 인증서는 홈CA 영역이 아닌 CA들의 영역에서도 검증될 수 있고, CA는 모든 CA의 공개키 정보를 알 필요가 없으며 k개의 CA 정보만 알면 된다. CA가 검증하고자 하는 인증서에 사용된 CA의 공개키를 모를 때에도 랜덤 CA 그룹에 질의하여 인증 정보를 알아낼 수가 있게 된다. 랜덤 그룹 크기인 k를 적절하게 선택한다면, 한 CA가 두 개의 랜덤 CA 그룹에 중복되는 확률은 충분히 크게 될 것이다.

Ⅳ. 수학적 분석

1. 분석 모델

이 장에서는 분석을 위해 다음 표기를 사용한다.

- m : 모바일 애드혹 네트워크를 구성하는 이동 노드의 수
- n : CA들의 수
- k : 랜덤 CA 그룹의 크기
- r : 서로 다른 두 랜덤 그룹에 공유되는 CA의 수
- λ_a : 발신호의 평균 속도
- λ_m : 이동 노드의 평균 도메인간 이동 속도 (통과한 도메인의 수/초)
- λ_r : 이동 노드의 평균 인증서 폐지속도
- T_n : 이동 노드의 인증서 갱신 주기
- c_u : 인증 정보를 기록하기 위해 하나의 CA에 접속할 때 소요되는 기대비용
- c_r : 인증 정보를 읽기위해 하나의 CA에 접속할 때 소요되는 기대 비용
- c_l : 인증 실패로 인한 손해 비용
- T_f : 한 CA에서 발생한 두 개의 연속적인 접속 실패 사이의 평균 시간
- T_l : CA의 평균 생존 시간
- p_e : 이동 노드가 접속 불가일 확률
- t_u : 하나의 CA에서 발생한 인증 정보에 대한 갱신과 인증 정보에 대한 질의 사이의 시간 간격
- t_r : 인증서 폐지에 의한 인증 정보 갱신과 인증 정보 질의 사이의 시간 간격
- t_n : 인증서 갱신에 의한 인증 정보 갱신과 인증 정보 질의 사이의 시간 간격

하나의 CA는 자신의 영역을 가지고 영역 내에서 m/n개의 이동 노드들은 관리한다고 가정한다. 영역내의 CA가 네트워크에 오랜 시간 접속이 안되는 경우 이 CA는 실패라고 하고 이 CA가 저장한 인증정보는 모두 손실되며 CA의 역할은 다른 노드에 의해 대체된다. CA가 노드 불안정성으로 인해 짧은 시간동안 연결될 수 없고 인증정보는 유지하는 경우 이 CA는 접속불가라고 한다.

하나의 CA는 다음과 같은 상황에서 랜덤하게 선택한 k개의 CA로 구성된 그룹에 인증 정보를 기록한다 :

- ○ CA가 이동 노드에 새로운 인증서를 발급해 줄 때
- ○ CA가 이동 노드의 인증서를 폐지하고 그에 대한 CRL을 발급한 후, 새로운 인증서를 발급했을 때
- ○ CA가 이동 노드의 인증서를 갱신했을 때

하나의 CA는 다음과 같은 경우에 k개의 랜덤하게 선택한 CA 그룹에 인증 정보에 대한 질의를 보낸다.

- ○ 이동 노드가 다른 CA의 영역으로 이동하여 그 CA가 이 노드를 인증할 때
- ○ 호접속을 시도한 이동 노드가 CA에게 호 접속요구를 받은 이동 노드의 인증 정보를 요청할 때
- ○ 호접속을 시도를 받은 이동 노드가 CA에게 호 접속을 요구한 이동 노드의 인증 정보를 요청할 때

인증 정보를 요청한 첫번째 질의가 실패한 경우, 인증 정보를 얻기 위해 재시도는 하지 않는 것으로 가정하고 이 인증 결과는 실패로 정한다.

이동 노드는 매 주기, T_n마다 인증서를 갱신하고 기간이 만료된 구 인증서는 더 이상 사용하지 않는다. 이동 노드는 λ_r의 속도로 인증서를 폐지하고, 이에 CA는 이 노드에 대해 CRL을 발행하고, 새로운 인증서를 발급한다. λ_r은 지수 분포로 가정하고 확률밀도함수는 $f_r(t)=\lambda_r e^{-\lambda_r t}$이며 누적분포함수는 $F_t(t)=1-e^{-\lambda_t t}$를 가진다. 이동 노드는 CA의 도메인 간에 평균 도메인 체류 시간, $1/\lambda_m$의 분포로 이동하며 $1/\lambda_m$는 역시 지수 분포 (확률밀도함수 : $\lambda_m e^{-\lambda_m t}$, 평균이동속도 : λ_m)를 갖는다. 이동 노드는 지수 분포인 λ_a의 평균 속도로 호를 발신한다.

이동 노드는 매 주기 T_n마다 단위 비용 c_u로 k개의 CA들에게 자신의 인증 정보를 *기록*한다. 또한 이동 노드는 단위 비용 c_u로 확률밀도함수 $f_r(t)$에 따라 k개의 CA들에게 인증 정보를 *기록*한다. 하나의 이동 노드가 λ_a의 속도로 호를 발신할 때, 호를 발신하는 이동 노드와 이 호를 수신하는 이동 노드는 모두 단위 비용 c_r로 k개의 CA들로부터 상대편의 인증 정보를 *읽게* 된다. 이동 노드가 λ_m의 속도로 다른 CA의 도메인으로 이동할 때, 이동영역의 CA도 역시 단위 비용 c_r로 k개의 CA들로부터 인증 정보를 *읽게* 된다.

하나의 CA에 대한 접속 실패는 실패 사이의 평균 시간 T_f(확률밀도함수 : $\frac{1}{T_f}e^{\frac{-t}{T}}$)인 지수분포를 갖는다. 여

기서 우리는 기존 CA에 대한 접속이 실패하자마자, 새로운 CA가 선출된다고 가정한다. CA가 자신의 도메인을 벗어나면 이것은 더 이상 CA가 아니고 즉시 새로운 CA가 선출되어야 한다.

CA의 도메인 체류 시간은 평균 체류시간 $1/\lambda_m$인 지수 분포를 가진다. 그러므로 한 이동 노드가 CA로 선출되었다가 CA 접속 실패 상황이 될 때까지의 시간 간격은 평균 시간,

$$T_l = \frac{1}{\lambda_m + \frac{1}{T_f}} \quad (\text{확률밀도함수} : \frac{1}{T_l} e^{-\frac{t}{T_l}}), \tag{1}$$

의 지수 분포를 따른다. CA 동작으로 인한 처리 비용은 무시하기로 한다.

2. 수학적 분석

노드의 인증에 필요한 총비용은 다음과 같이 구할 수 있다.

$$\begin{aligned} &\text{총비용} \\ &= \text{인증실패비용} + CA\text{접속비용} \\ &= \text{호시도발생시의인증실패비용} \\ &\quad + \text{이동시의인증실패비용} + CA\text{접속비용} \\ &= c_l \cdot (E_{Cfail} + E_{Mfail}) + c_u \cdot E_{write} + c_r \cdot E_{read}. \end{aligned} \tag{2}$$

여기서 c_l은 인증 실패로 인한 손해 비용, c_u는 한번 인증 정보를 기록하기 위해 하나의 CA에 접속하는 데 소요되는 기대 비용, c_r은 한번 인증 정보를 읽기 위해 하나의 CA에 접속하는 데 소요되는 기대 비용을 말한다. E_{Cfail}은 단위 시간당 호 연결에서 발생하는 총 인증 실패의 수, E_{Mfail}은 단위 시간당 이동 노드의 이동에서 발생하는 총 인증 실패의 수, E_{write}는 단위 시간당 CA들에 대한 총 기록 횟수, 그리고 E_{read}는 단위 시간당 CA들에 대한 총 읽기 횟수를 말한다.

가. 호 연결시에 발행하는 인증 실패 비용

어떤 순간에 이동 노드가 접속이 안되는 접속불가의 확률을 p_e라고 정의하자. CA에 대한 *쓰기*나 *읽기* 동작이 발생할 때, 나머지 접속되는 CA들의 수에 대한 확률밀도함수는 다음과 같다.

$$p_{rem}(i) = C_l^n (1-p_e)^i p_e^{n-i}, \quad 0 \le i \le n. \tag{3}$$

인증 정보 갱신과 인증 정보 질의는 다른 순간에 각각 다른 이동 노드들에 의해 발생하므로 이 두 가지 과정 동안 p_{rem}이 독립적이라고 가정할 수 있다. 그러므로 갱신과정 동안 i개의 접속가능한 CA와 질의과정 동안 j개의 접속가능한 CA에 대한 joint PDF는 $p_{rem}(i)p_{rem}(j)$이다. 만약 k개 이상의 접속가능한 CA가 존재한다면, 그들 중에 오직 k개 만이 질의나 갱신에 사용된다.

그러므로 호 발신 노드에 의해 질의를 받은 CA들 중에 r_1개의 CA가 마지막 갱신과정 동안 저장된 인증 정보를 포함할 확률은,

$$\begin{aligned} g_{r_1}(r_1) = &\sum_{i=0}^{k}\sum_{j=0}^{k} p_{rem}(i)p_{rem}(j)p_{ij}(r_1) \\ &+ \sum_{i=0}^{k}\sum_{j=k+1}^{n} p_{rem}(i)p_{rem}(j)p_{ik}(r_1) \\ &+ \sum_{i=k+1}^{n}\sum_{j=0}^{k} p_{rem}(i)p_{rem}(j)p_{kj}(r_1) \\ &+ \sum_{i=k+1}^{n}\sum_{j=k+1}^{n} p_{rem}(i)p_{rem}(j)p_{kk}(r_1). \end{aligned} \tag{4}$$

이다. 여기서 $p_{ij}(r)$은 갱신정보를 받은 i개의 CA들과 질의를 받은 j개의 CA들 사이에 교집합의 크기 r의 확률밀도함수이며 다음과 같이 정의된다.

$$p_{ij}(r) = \begin{cases} \dfrac{C_r^i C_{j-r}^{n-i}}{C_j^n}, & \text{if } \max(0,\ i+j-n) \le r \le \min(i,j) \\ 0 & otherwise \end{cases} \tag{5}$$

또한 호를 수신하는 이동 노드에 의한 질의를 받은 CA들 중에 r_2개가 마지막 갱신된 인증 정보를 포함할 확률은,

$$\begin{aligned} g_{r_2}(r_2) = &\sum_{i=0}^{k}\sum_{j=0}^{k} p_{rem}(i)p_{rem}(j)p_{ij}(r_2) \\ &+ \sum_{i=0}^{k}\sum_{j=k+1}^{n} p_{rem}(i)p_{rem}(j)p_{ik}(r_2) \\ &+ \sum_{i=k+1}^{n}\sum_{j=0}^{k} p_{rem}(i)p_{rem}(j)p_{kj}(r_2) \\ &+ \sum_{i=k+1}^{n}\sum_{j=k+1}^{n} p_{rem}(i)p_{rem}(j)p_{kk}(r_2). \end{aligned} \tag{6}$$

이다. r_1개의 CA와 r_2개의 CA사이에 겹쳐지는 CA의 수가 v인 확률은 $p_{r_1 r_2}(v)$이다.

t_u를 CA에서 인증정보에 대한 마지막 갱신과 호 연결로 인한 인증정보 질의 사이의 시간 간격이라고 정의하자.

$$t_u = \min(t_r, t_n) \tag{7}$$

여기서, t_r은 인증 정보에 대한 질의(여기서는 호 연결로 인한)와 인증서 폐지로 인한 마지막 정보 갱신사이

의 시간 간격을 나타내는 랜덤 변수이고 t_n은 인증 정보에 대한 질의(여기서는 호 연결로 인한)와 주기적인 인증서 갱신으로 인한 마지막 정보 갱신 사이의 시간 간격을 나타내는 랜덤 변수이다. t_r의 확률밀도함수는 다음과 같다.

$$g_r(t)=\frac{1-F_r(t)}{\int_0^{\infty} t f_r(t)dt} \tag{8}$$

$f_r(t)$는 지수분포이고, $g_r(t)=f_r(t)=\lambda_r e^{-\lambda_r t}$라고 가정한다. t_n의 확률밀도함수는 다음과 같다.

$$g_r(t)=\frac{1}{T_n}, \qquad (t<T_n) \tag{9}$$

그러므로 t_u의 확률밀도함수는 식 (10)이 된다.

$$f_u(t)=g_r(t)(1-G_n(t))+g_n(t)(1-G_r(t)), \quad (t<T_n). \tag{10}$$

r_1, r_2, v가 주어졌을 때, 단위시간당 평균 인증 실패 횟수는 다음과 같이 구할 수 있다. 여기서 *CA의 총수* $<r_1+r_2$라고 가정하자.

$$\begin{aligned}
&E_{Cfail}|r_1,r_2,v\\
&=2\lambda_a\times\\
&[(t_u\text{내에}v\text{개의}CA\text{가실패할확률})\times\\
&((t_u\text{내에}(r_1-v)\text{개의}CA\text{가실패할확률})\\
&+(1-(t_u\text{내에}(r_1-v)\text{개의}CA\text{가실패할확률}))\\
&\times(t_u\text{내에}(r_2-v)\text{개의}CA\text{가실패할확률}))]\\
&=2\lambda_a\times\\
&\int_0^{T_n}[(1-e^{\frac{-t}{T_l}})^v\times\\
&((1-e^{\frac{-t}{T_l}})^{r_1-v}+(1-(1-e^{\frac{-t}{T_l}})^{r_1-v})(1-e^{\frac{-t}{T_l}})^{r_2-v})]f_u(t)dt.\\
&=2\lambda_a\times\\
&\int_0^{T_n}[(1-e^{\frac{-t}{T_l}})^{r_1}+(1-e^{\frac{-t}{T_l}})^{r_2})-(1-e^{\frac{-t}{T_l}})^{r_1+r_2-v}]f_u(t)dt.
\end{aligned} \tag{11}$$

여기서 λ_a는 하나의 이동 노드에서 단위시간 당 발생한 호 발신의 총 수이다. 우리는 호발신과 호수신은 대칭적으로 발생하는 것을 고려하여야 한다. 그러므로 하나의 이동 노드에서 단위 시간당 발생한 호 발신과 호수신의 평균 수는 $2\lambda_a$이다.

식(6)과 v를 고려하면 다음을 얻을 수 있다.

$$\begin{aligned}
&E_{Cfail}|r_1,r_2=2\lambda_a\sum_{v=0}^{k}p_{r_1r_2}(v)\times\\
&\int_0^{T_n}[(1-e^{-\frac{t}{T_l}})^{r_1}+(1-e^{-\frac{t}{T_l}})^{r_2}-(1-e^{-\frac{t}{T_l}})^{r_1+r_2-v}]f_u(t)dt.
\end{aligned} \tag{12}$$

r_2에 대해서는 다음을 구할 수가 있다.

$$\begin{aligned}
&E_{Cfail}|r_1=2\lambda_a\sum_{r_2=0}^{k}g_{r_2}(r_2)\sum_{v=0}^{k}p_{r_1r_2}(v)\times\\
&\int_0^{T_n}[(1-e^{-\frac{t}{T_l}})^{r_1}+(1-e^{-\frac{t}{T_l}})^{r_2}-(1-e^{-\frac{t}{T_l}})^{r_1+r_2-v}]f_u(t)dt.
\end{aligned} \tag{13}$$

마찬가지로 r_1에 대해서도 다음을 구할 수가 있다.

$$\begin{aligned}
&E_{Cfail}=2\lambda_a\sum_{r_1=0}^{k}g_{r_1}(r_1)\sum_{r_2=0}^{k}g_{r_2}(r_2)\sum_{v=0}^{k}p_{r_1r_2}(v)\times\\
&\int_0^{T_n}[(1-e^{-\frac{t}{T_l}})^{r_1}+(1-e^{-\frac{t}{T_l}})^{r_2}-(1-e^{-\frac{t}{T_l}})^{r_1+r_2-v}]f_u(t)dt\\
&=2\lambda_a\sum_{r_1=0}^{k}\sum_{r_2=0}^{k}\sum_{v=0}^{k}g_{r_1}(r_1)g_{r_2}(r_2)p_{r_1r_2}(v)\times\\
&\int_0^{T_n}[(1-e^{-\frac{t}{T_l}})^{r_1}+(1-e^{-\frac{t}{T_l}})^{r_2}-(1-e^{-\frac{t}{T_l}})^{r_1+r_2-v}]f_u(t)dt.
\end{aligned} \tag{14}$$

그러므로 호 연결에서 발생하는 단위 시간당 인증 실패로 인한 평균 피해 비용, C_{Cfail}은 다음 식(15)와 같다.

$$\begin{aligned}
&C_{Cfail}=c_l\cdot 2\lambda_a\sum_{r_1=0}^{k}\sum_{r_2=0}^{k}\sum_{v=0}^{k}g_{r_1}(r_1)\ g_{r_2}(r_2)\ p_{r_1r_2}(v)\times\\
&\int_0^{T_n}[(1-e^{-\frac{t}{T_l}})^{r_1}+(1-e^{-\frac{t}{T_l}})^{r_2}-(1-e^{-\frac{t}{T_l}})^{r_1+r_2-v}]f_u(t)dt.
\end{aligned} \tag{15}$$

여기서 c_l은 한번의 인증 실패로 인한 손해 비용이다.

나. 노드의 이동으로 인한 인증 실패 비용

노드의 이동으로 인하여 단위시간당 발생하는 인증 실패에 대한 평균 손해 비용은 C_{Mfail}라고 정의하기로 하자.

노드의 이동에 따라 인증서를 검증하기 위해 인증정보에 대한 질의를 받은 CA들중에 r개의 CA가 마지막 갱신된 최신 인증 정보를 가지고 있을 확률은 다음 식(16)과 같다.

$$\begin{aligned}
g_r(r)=&\sum_{i=0}^{k}\sum_{j=0}^{k}p_{rem}(i)p_{rem}(j)p_{ij}(r)\\
&+\sum_{i=0}^{k}\sum_{j=k+1}^{n}p_{rem}(i)p_{rem}(j)p_{ik}(r)\\
&+\sum_{i=k+1}^{n}\sum_{j=0}^{k}p_{rem}(i)p_{rem}(j)p_{kj}(r)\\
&+\sum_{i=k+1}^{n}\sum_{j=k+1}^{n}p_{rem}(i)p_{rem}(j)p_{kk}(r).
\end{aligned} \tag{16}$$

노드의 이동으로 인한 인증 정보에 대한 질의와 CA에 대한 인증 정보의 최신 갱신 사이의 시간 간격을 t_u

라고 정의하면,

$$t_u = \min(t_r, t_n) \tag{17}$$

이다. 여기서 t_r은 인증정보에 대한 질의(이 경우는 노드의 이동으로 인하여 발생한)와 인증서 폐지로 인한 인증정보의 최신 갱신 사이의 시간 간격을 나타내는 랜덤 변수이고, t_n은 인증정보에 대한 질의(이 경우는 노드의 이동으로 인하여 발생한)와 주기적인 인증서 갱신으로 인한 인증정보의 최신 갱신 사이의 시간 간격을 나타내는 랜덤 변수이다. 이 식은 앞에서 보여준 식(7)과 같다.

r이 주어진 경우, 단위 시간당 인증 실패의 평균 횟수는 다음과 같다.

$$\begin{aligned} E_{Mfail}|r &= \lambda_r \times [t_u \text{내에} r\text{개의} CA\text{가실패할확률}] \\ &= \lambda_r \times \int_0^{T_n} (1-e^{-\frac{t}{T_l}})^r f_u(t)dt. \end{aligned} \tag{18}$$

따라서 노드의 이동시에 발생하는 단위 시간당 인증 실패의 평균 손해 비용, C_{Mfail}은

$$C_{Mfail} = c_l \cdot \lambda_m \sum_{r=0}^{k} g_r(r) \int_0^{T_n} (1-e^{-\frac{t}{T_l}})^r f_u(t)dt, \tag{19}$$

이고, 여기서 c_l은 한번의 인증 실패로 인한 손해 비용을 말한다.

다. CA 접속 비용

이동 노드에서 단위 시간당 인증 정보를 읽거나 쓰기 위해 한 개의 CA에 접속하는 비용은

$$\begin{aligned} C_{access} &= c_u \cdot E_{write} + c_r \cdot E_{read} \\ &= c_u \frac{k}{T_n} + c_u \frac{k}{\int_0^{\infty} t f_r(t)dt} + c_r \cdot (\lambda_m + 2\lambda_a). \end{aligned} \tag{20}$$

이다. 여기서 $f_r(t)$는 지수분포라고 가정하면,

$$\int_0^{\infty} t f_r(t)dt = \frac{1}{\lambda_r} \tag{21}$$

이다.

최종적으로 하나의 이동 노드에서 단위 시간당 상대 노드 인증을 위해 지불하는 총 비용은

$$C_{total}(n,k,T_n) = C_{Cfail} + C_{Mfail} + C_{access}. \tag{22}$$

가 된다.

V. 결 과

이 장에서는 앞 절의 성능 분석에 따른 총비용에 대하여 그래프를 보여준다. <그림 3>은 랜덤 CA 그룹을 구성하는 크기의 변화에 따르는 총비용의 변화를 보여준다. 총 CA의 수는 *10, 20, 30, 40*으로 증가하며 그래프는 각각의 경우에 대하여 랜덤 CA 그룹의 크기를 변화해 가면서 총비용의 변화를 살펴보았다. <그림 3>에서 총 CA의 수가 증가함에 따라, 인증 과정에 대한 총 비용이 최소가 되는 최적의 랜덤 CA 그룹 크기 역시 증가함을 알 수 있다. 각 CA의 수에 따라, 최적의 랜덤 CA 그룹의 크기는 *8, 12, 14, 16* 정도로 증가함을 보여준다. 점선은 총 CA의 수가 20인 경우에 대한 시뮬레이션 결과를 보여주며 성능 분석으로 구한 그래프와 유사하게 최적의 랜덤 CA 그룹 크기를 보여줌을 알 수 있다.

<그림 4>는 CRL 갱신 주기의 변화에 따른 총 비용의 변화를 보여준다. CRL 갱신 주기, T_n이 짧은 경우, 즉 CRL을 자주 갱신하는 경우에는 CRL 갱신으로 인해 인증 정보의 갱신도 자주 이루어지므로 해당 인증 정보가 발견될 확률이 증가하게 되고 결국 인증 과정의 총 비용도 감소하게 된다. 그러나 이 경우에 랜덤 CA 그룹의 크기가 증가할수록 빈번한 인증 정보 갱신으로 인한 비용도 증가하며 이것은 총 비용의 증가를 만들게 된다. 이런 과정은 RCG의 수가 12보다 큰 경우에 T_n이 *50*인 그래프가 다른 그래프들보다 총비용이 증가하

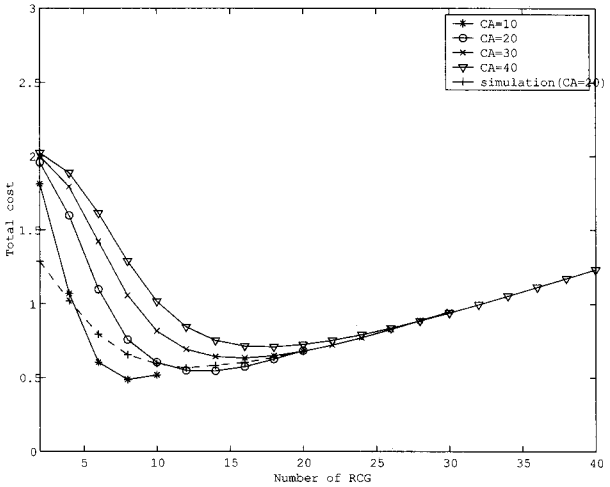

그림 3. 총 CA의 수의 변화에 따른 인증과정의 총비용 발생 변화

Fig. 3. Total Cost according to change of CA number by numerical analysis.

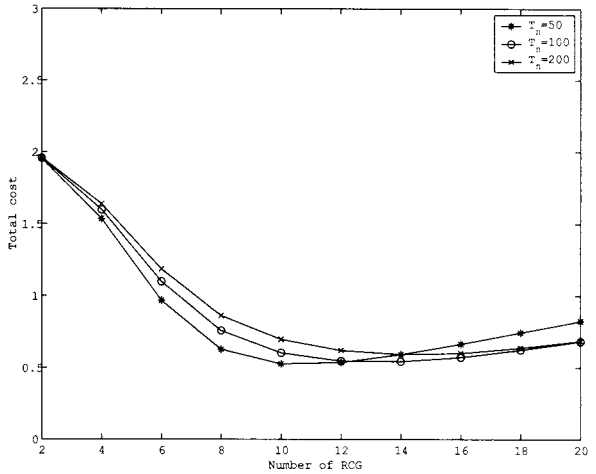

그림 4. CRL 갱신 주기 변화에 따른 총비용 발생 변화

Fig. 4. Total Cost according to change of CRL update period by numerical analysis.

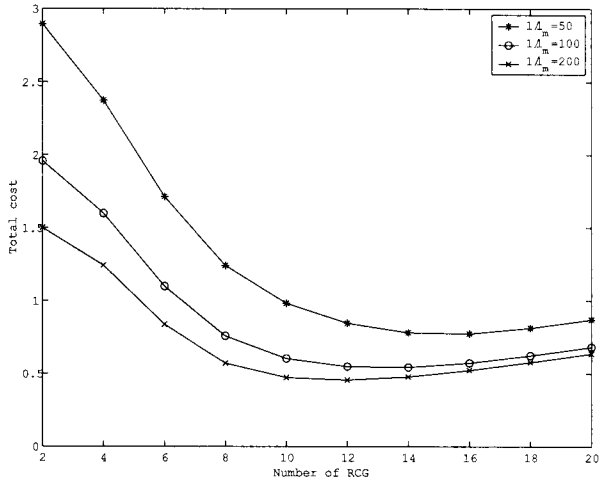

그림 5. 이동 노드의 이동 속도에 따른 총비용의 변화

Fig. 5. Total Cost according to change of node mobility rate by numerical analysis.

는 것으로 나타난다.

<그림 5>는 이동 노드의 이동 속도 변화에 따른 결과를 보여준다. 그림에서 알 수 있듯이, 이동노드의 이동 속도가 빠를 때, 인증정보에 대한 갱신이 자주 발생하므로 총비용을 증가시킨다. <그림 6>은 p_e의 변화에 따른 결과를 보여준다. 모바일 애드혹 네트워크가 불안정한 경우, 즉, p_e가 커지면, 총비용도 역시 매우 증가하게 된다. 그림에서 p_e가 *0.8*인 경우는 모바일 애드혹 네트워크가 매우 안정되어 이동 노드들에 대한 접속이 용이한 경우이다. 즉, RCG에 대한 인증 정보의 갱신 등으로 인한 CA 접속 비용이 급속히 증가하므로 다른 그래프에 비해 총비용이 상당히 높음을 알 수 있다. 그러

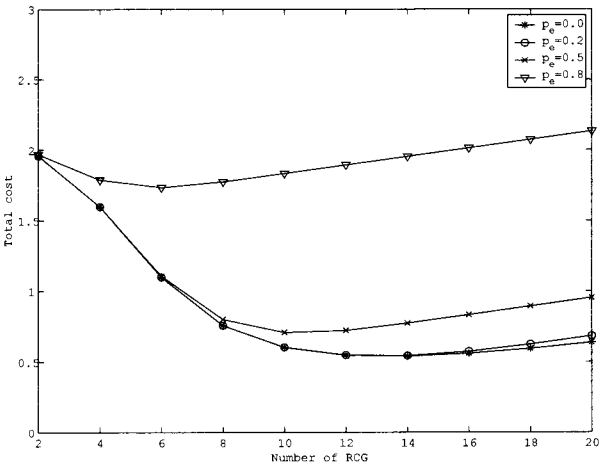

그림 6. 노드의 안정성 변화에 따른 총비용의 변화 분석

Fig. 6. Total Cost according to change of node stability by numerical analysis.

나 이 경우는 총비용이 랜덤 CA 그룹의 크기에 별로 영향을 받지 않고 비교적 안정정임을 알 수 있다. 또한 이 그래프에서는 최소 총비용을 나타내는 랜덤 CA 그룹의 크기가 *6*이다. 이것은 이동 노드들이 안정된 경우 CA에 대한 접속이 쉬우므로 인증 정보를 요청하는 랜덤 CA 그룹의 크기가 작아도 쉽게 인증 정보를 획득할 수 있음을 나타낸다. <그림 3> - <그림 6>의 모든 경우에 인증 과정으로 인한 총비용을 최소화하는 랜덤 CA 그룹의 크기는 *10* - *12*가 되며 이것은 시뮬레이션에서 보여준 결과와 유사함을 알 수 있다.

VI. 관련 연구

지금까지 모바일 애드혹 네트워크에서 이동 노드들 사이의 인증 방법에 대한 많은 연구가 진행되어 왔다.

Zhou와 Haas는 애드혹 네트워크에 대하여 threshold cryptography에 기반한 분산된 공개키 관리 방법을 제안하였으며 이후의 많은 연구들이 모바일 애드혹 네트워크에서의 인증 방법을 제공하기 위해 이 방법을 사용하였다[3~4, 6~7].

[3, 6]에서는 애드혹 네트워크에서 PKI 기술을 적용하기 위하여 여러 개의 노드들에게 CA의 기능을 분산시키는 방법으로 threshold cryptography 방법을 적용하였다. 이 논문에서는 이동 노드들의 다양성에 주목하여, 물리적으로 더 안전하고 계산 능력이 더 강력하거나, 더 신뢰할 수 있는 이동 노드들이 있다는 가정하에 네트워크 오퍼레이터가 이동 노드들의 다양성에 따라

MOCA를 선택하는 방법을 사용하였다. 선택된 MOCA 노드들은 threshold cryptography 방법을 사용하여 신뢰를 공유하고 CA 서비스에 필요한 기능인 보안과 높은 가용성을 제공하도록 하였다.

Zhang 등은 애드혹 네트워크에서 확장성있는 분산 인증 방법을 제안하였다[7~8]. 이 논문에서는 임의의 노드들이 인증 서비스에 필요한 비밀키를 공유하도록 하여 인증에 따르는 부담을 공정하게 분산하도록 하였다. 이 방안을 따르면 k개의 이동 노드가 시스템의 비밀키를 공유하도록 하고 이동 노드가 임의의 k개의 신뢰된 노드로부터 신뢰를 얻고 threshold cryptography에 의해 서명된 인증서를 받는다면, 이 노드는 신뢰할 수 있다고 하였다. 이 경우 k개의 노드들은 인증이 필요한 노드로부터 한 홉 이웃으로 구성하고 인증이 필요한 노드는 주변 이웃들로부터 신뢰를 받게 되는 것이다. 주변 이웃 노드를 구성하는 노드들은 이웃 노드가 악의적인 노드인지 잘못된 동작을 하는 지를 감시하며, 이런 지역적인 감시로 인해 악의적인 노드를 감지해 내는 경우 그 노드에 대한 인증서를 폐지한다. 이런 시스템 구조는 Sybil attack에 취약한 특성을 가지므로 공격자가 비밀 정보를 알아내는 데 필요한 충분한 식별정보를 획득할 수 있고, 이것을 이용해 시스템의 비밀키를 구성할 수 있게 된다[5].

[9~10]에서는 모바일 애드혹 네트워크의 인증 방법으로 PGP와 유사한 자가 구성에 의한 방법을 제안하였다. 이 연구에서는 노드들간의 개인적인 친숙도에 기반하여 노드간에 서로 인증서를 발급하도록 한다. 이 시스템에서는 각 노드가 자신의 개인 인증서 저장소를 관리하며 두 개의 사용자가 서로 상대의 공개키를 검증하고자 할 때, 먼저 자신의 인증서 저장소와 상대 저장소를 합쳐서 적절한 인증서 검증 체인을 구성하기 위해 시도한다.

이외에도 인증서 폐지를 포함하여 애드혹 네트워크에서의 인증서 관리에 대한 많은 연구가 진행되어 왔다[11~12].

VII. 결 론

이 논문에서는 크기가 매우 큰 모바일 애드혹 네트워크에서 이동 노드에 대한 인증 방법을 제안하고 그 성능을 분석하였다. 우리가 고려한 네트워크는 많은 수의 이동 노드들이 지리적으로 넓은 영역의 매우 큰 네트워크에 걸쳐서 분포해 모바일 애드혹 네트워크를 구성하는 경우이다. CA를 포함하여 이동 노드들은 그 특성상 빈번하게 네트워크에 대한 접속과 끊어짐을 반복하며 네트워크 내를 자주 이동하게 된다. 그러므로 이동 노드가 네트워크에 접속할 때에 이동 노드들 간에 신뢰는 중요한 이슈가 된다.

이 논문에서 제안하는 방법은 이동 노드들이 서로를 인증하기 위해 공개키 알고리즘에 기반한 인증서를 적용한다. 또한 임의로 선택된 이동 노드들이 필요에 따라 자치적으로 CA의 기능을 수행하여 이동 노드들에게 인증서를 발급하도록 하였다. 이동 노드들은 CA의 서명을 신뢰하여 인증서를 검증하고 상대 노드를 인증하고 상대노드를 확인할 수 있게 된다. CA가 서명한 이동 노드의 인증서를 검증하기 위해서, CA들은 자신의 공개키와 CRL과 같은 자신의 인증 정보를 분배하여야 한다. CA들은 CRL을 발급할 때나 질의에 대한 응답으로 랜덤하게 선택된 CA들로 구성된 RCG를 선택하고 이들에게 인증 정보를 전달한다. 또한 이동 노드의 인증서를 받은 CA는 랜덤하게 선택한 CA들에게 질의를 보낸 후 응답을 받아서 인증서를 검증하게 된다. RCG의 구성원으로 선택된 CA들 중에는 두 개의 CA 그룹에 중복해서 속하게 되고 한 그룹으로부터 어떤 CA의 인증 정보를 받아서 다른 CA 그룹에 전파할 수 있게 된다. 이 방법에서 이동 노드들은 하나의 인증서만들 사용할 수 있고 홈 CA로부터 멀리 떨어진 경우에도 임의의 CA로부터 자신의 인증서를 폐지할 수 있다.

이 방법에 대한 성능분석 결과 우리는 성공적인 인증과정이 수행되고, 인증과정에 대한 총비용이 최소화되는 최적의 랜덤 CA 그룹 크기를 구할 수 있었다. 최적의 랜덤 CA 그룹의 크기는 $10 - 12$인 경우이고 이 값은 이동 노드가 네트워크에 접속한 기간이 네트워크에 접속하지 못한 기간 보다 긴 경우에, 이동 노드의 이동 모델과 이동 노드의 총 수와 CA의 총 수에 상관없이 동일한 결과를 보여준다.

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*, February 2004. pp. 69 - 73

[3] Seung Yi andRobin 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] Lidong Zhou and Zygmunt J. Haas, "Securing Adhoc network," *IEEE Network Magazine*, Nov/Dec 1999. pp. 24 - 30

[5] Douceur, "The Sibil Attack," Proc. First International Workshop Peer-to-peer Systems(IPTPS), 2002.

[6] Seung Yi and Robin Kravets, "MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks," 2nd Annual PKI Research Workshop Program (PKI 03), Gaithersburg, Maryland, April, 2003.

[7] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang. "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.

[8] 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.

[9] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaus, "Self-Orgainized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computings*, Vol. 2, No. 1, January-March 2003. pp. 52 - 64

[10] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaus, "Mobility Helps Security in Ad Hoc Networks," MobiHoc'03, Annapolis, USA. June 2003.

[11] 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, USA. January 2003.

[12] Carlton R. Davis and Claude Crepeau, "A Certificate Revocation Scheme for Wireless Ad hoc Networks," 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), October 2003. Fairfax, VA, USA

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

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

[15] 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.

[16] D. Balfanz, D.K Smetters, P. Stewart and H. C. Wong, "Talking to Strangers : Authentication in Ad-Hoc Wireless Networks," In Sysmposium on Network and Distributed System Security(NDSS '02), San Diego, USA, Feb. 2002.

[17] Sonali 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)-교신저자
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>