

이동 임시무선망에서의 키관리 기법에 관한 연구[†]

(On the Study of Key Management in Mobile Ad Hoc Networks)

김 시 관*, 신 윤 식*, 임 은 기*

(Si-Gwan Kim, Yoon-Shik Shin, Eun-Ki Lim)

요 약 이동성을 가진 다수의 노드들에 의해 자율적으로 구성되는 이동 임시무선망(Mobile Ad Hoc Network)은 홈 네트워크, 센서 네트워크, 개인망 등 다양한 응용 분야로의 적용이 활발히 이루어지고 있다. 이동 임시무선망은 네트워크 토폴로지, 전송 대역폭 및 전송 거리상의 제약성, 에너지 사용에 있어서의 제약성, 무선망 고유의 보안성 취약등의 여러 문제점을 극복하기 위하여 다양한 연구가 진행되고 있는데 특히 무선망이라는 속성 때문에 보안에 취약한 문제점을 안고 있다. 본 논문에서는 이동 임시 무선망에서 이동 노드들간에 보안성을 강화하기 위해 키들을 관리하는 기법을 제안한다. 임시 무선망에서 키를 분배하는 기법 중 완전 분배형 인증 기법이 널리 적용되고 있다. 기존의 연구는 임의의 노드를 중심으로 한 개의 홈 거리에 있는 노드들에 대해서만 키분배를 하는 기법을 채택하였지만 임의의 노드를 기준으로 주변에 특정 개수 이하의 노드가 활동 중인 경우에도 키 관리를 원활히 할 수 있는 기법을 제안하고 기존의 기법보다 우수함을 시뮬레이션을 통해 증명한다.

핵심주제어 : 이동 임시무선망, 키관리

Abstract This paper covers the issue of securing ad hoc networks. Such networks exhibit a number of characteristics that make such a task challenging. One of the major challenges is that ad hoc networks typically lack a fixed infrastructure both in form of physical infrastructure such as routers, servers, and stable communication links and in the form of an organizational or administrative infrastructure. Another difficulty lies in the highly dynamic nature of ad hoc networks since new nodes can join and leave the network at any time. The major problem in providing security services in such infrastructure less networks is how to manage the cryptographic keys that are needed. In order to design practical and efficient key management systems it is necessary to understand the characteristics of ad hoc networks and why traditional key management systems cannot be used. These issues are covered and we also present a new efficient key management solutions. Finally we show that the proposed method is more efficient than the previous works through simulations.

Key Words : ad hoc networks, key management

1. 서 론

이동 임시무선망(Mobile Ad Hoc Network)은 이

동성을 가진 다수의 노드들에 의해 자율적으로 구성되는 임시적인 네트워크로서, 기반망(infrastructure)이 존재하지 않거나 기반망에 기초한 네트워크의 구성이 용이하지 않은 지역에서 임시적으로 네트워크를 구성하기 위한 목적으로 연구되어 왔다. 이

[†] 본 연구는 금오공과대학교 학술연구비 지원에 의하여 연구된 논문임.

* 금오공과대학교 컴퓨터공학부

동 임시무선망의 응용은 군사용으로 시도되었는데 전투 중에 전투원들이 이동 무선 단말기를 사용하여 언제든지 작전 지시를 주고받을 수 있도록 설계가 되었다. PDA, 핸드폰, 노트북 컴퓨터, 프린터 등의 단말기들로 구성된 개인망에서는 서로의 위치가 인접하게 되면 각 장치를 접근할 수 있도록 연구가 진행되고 있으며 공항이나 회의실에서와 같은 환경에서 기반망이 없이 임시로 망을 구성하여 정보를 이용할 수도 있다. 이와 같이 최근 이동 임시무선망 기술은 홈 네트워크(Home Network), 센서 네트워크(Sensor Network), 개인망(Personal Area Network) 등 다양한 응용 분야로의 적용이 활발히 이루어지고 있으며 고유한 특성에 때문에 차세대 네트워킹 방식의 하나로서 다음과 같은 여러 문제점을 극복하기 위하여 다양한 연구가 진행되고 있다.

첫째, 노드의 이동에 따라 네트워크 토폴로지가 동적으로 변화한다. 네트워크 토폴로지의 변화는 빈번한 경로 정보의 갱신이 필요하며 경로 정보의 관리를 복잡하게 하며, 이를 위한 라우팅 제어 메시지는 네트워크의 오버헤드로서 작용한다. 둘째, 이동 노드들은 무선 인터페이스를 사용하여 서로 통신하기 때문에 기본적으로 전송 대역폭 및 전송 거리상의 제약이 있다. 따라서, 원거리 노드들 간의 통신을 위해서는 멀티-홉(multi-hop) 통신이 필수적이다. 멀티-홉 통신을 위해 각 노드는 호스트 기능 외에 메시지를 전달(forward)해 줄 수 있는 라우팅 기능도 포함되어야 한다. 셋째, 이동 노드들은 제한된 용량의 배터리를 사용하기 때문에 에너지 사용에 있어서의 제약점을 가지고 있어 불필요한 제어 메시지 생성등을 배제하는 등 여러 가지 배터리 상태를 고려한 통신이 필요하다. 넷째, 이동 노드들은 무선 인터페이스를 사용하여 서로 통신하고 있으며, 모든 노드들이 라우팅 기능을 가지고 있기 때문에 보안상으로 매우 취약하며 특히 브로드캐스팅(broadcasting)되는 라우팅 제어 메시지는 해킹의 위험이 크다[5, 6, 7].

이동 임시무선망에서 보안성을 강화하기 위하여 기밀성, 무결성, 인증성, 부인방지와 같은 성질을 고려하여야 한다. 공개키 암호 알고리즘은 비밀키 암호 알고리즘과 달리 암호화키와 복호화키가 서로 다른 알고리즘이다. 공개키 암호 알고리즘의 특징은 암호화키가 공개되더라도 복호화키가 공개되

지 않으며 이러한 성질을 얻기 위하여 공개키 암호 알고리즘은 수학적으로 풀기 어려운 문제에 기반을 두고 고안이 되었다. 공개키 암호 알고리즘은 전송된 문서의 생성자 확인을 위한 전자서명이나 사용자의 신원 확인을 위한 신분 인증에 사용될 수 있는 장점을 가지고 있지만 비밀키 암호 알고리즘에 비해 처리 속도가 늦은 단점을 가지고 있다.

이와 같이 공개키 암호 시스템에서는 각 사용자의 공개키가 다른 사용자에게 공개가 되며 이를 이용해 인증을 할 수 있다. 이동 임시무선망의 경우 공개키 암호시스템의 구축은 중앙집권식의 서비스 혹은 망의 분리(partition) 때문에 더욱 어려운 실정이다. 공개키를 관리하기 위한 가장 좋은 방법은 공개키 기반의 인증서이다. 공개키 기반의 인증서는 사용자의 공개키와 사용자의 ID를 결합한 것으로 특정 개체를 확인하고 특정 활동, 특정 권한, 특정 능력을 허가하는데 이용되며 특정 권한과 신분을 확인하기 위한 구조로 구성되어 있으며 공인인증기관(Certificate Authority, CA)의 서명문이다. 따라서, 사용자의 공개키와 사용자의 신분 확인은 CA에 의하여 수행된다.

Shamir[8]의 비밀키 공유 기법은 공개키와 비밀키 쌍을 이용하는데, 공개키는 한 개만 존재하여 공개되는 반면에 비밀키는 n 개의 노드로 이루어진 그룹에 의해 비밀 정보가 일부분씩 공유된다. 비밀키는 임계값 t 이하의 노드는 원문을 복구해 내지 못하고 $t+1$ 개 이상의 노드가 모여야만 비밀키를 얻을 수 있는 암호시스템이다. 이 시스템에서는 송신자가 메시지를 수신자에게 전송하고자 하는 경우 공개키를 가지고 원문을 암호화하여 전송한다. 수신자는 각자가 가지고 있는 비밀 정보를 믿을 수 있는 노드(trusted party)에게 안전한 채널을 통해 전송한다. 이 노드는 $t+1$ 개 이상의 비밀 정보를 모아서 비밀키를 만들어 낸 다음에 원문을 구하여 각각의 수신자에게 데이터를 전송한다.

본 논문에서는 이동 임시 무선망에서 이동 노드들간에 보안성을 강화하기 위해 키들을 관리하는 기법을 제안한다. [3]에서는 노드를 중심으로 한 홉 거리에 있는 노드와 통신을 함으로써 키 관리를 하는 기법에 대해서 제안되었다. 그러나, 노드들은 동적인 성질로 인하여 이웃 한 홉 노드들이 특정 갯수 이상의 노드로 연결되지 않을 수도 있다는 특성을 가지고 있기 때문에 키관리가 원활히

되지 않는 문제점을 가지고 있다.

본 논문에서는 주변 노드의 개수에 관계없이 키를 관리할 수 있는 새로운 기법에 대하여 제안한다. 2장에서는 키관리와 관련된 연구를 알아보고 3장에서는 본 논문에서 제안되는 기법을 제시한 뒤 4장에서는 실험, 5장에서는 결론 및 향후 연구과제에 대해서 제시한다.

2. 관련 연구

일반적으로 이동 임시무선망에서의 키 분배 기법 [1, 2, 3, 4, 5]은 분배를 해 주는 개체의 역할에 따라 부분 분배형 인증(Partially Distributed Certificate), 완전 분배형 인증(Fully Distributed Certificate) 및 자기 분배형 인증(Self-Issued Distributed Certificate)의 방법으로 분류할 수 있다.

Zhou [1] 는 특별히 지정된 서버 노드들에게 인증 서비스를 분산시키기 위한 (k, n) 임계값(threshold) 기법을 채용하고 있다. 각각의 노드들은 각 노드가 가지는 비밀키인 sk_{CA} 의 인증 배분을 사용하여 부분 인증(partial certificate)을 생성할 수가 있다. 그러나, 반드시 k 개의 이러한 부분 인증을 획득해야만 가능하다. 이 기법은 미리 계획되어 있고 장기간 사용하는 이동 임시무선망에 적당하다. 공용키 기반의 암호화를 채용하고 있기 때문에 모든 노드들은 이러한 계산 능력을 가지고 있어야 하며 모든 노드들이 서버 역할을 하고 있다.

완전 분배형 인증 기법은 Luo [2, 4] 에 의해서 제안되었는데 RSA 키를 망내의 모든 노드들에게 분배하기 위하여 (k, n) 임계값 기법을 사용한다 [20]. 부분 분배형과는 달리 특별한 노드를 지정하지 않고 모든 노드에게 공평하게 키를 분배한다는 것이 다른 점이다.

자기 분배형 기법은 Hubaux [5] 가 제안을 하였는데 PGP와 유사한 공용키 관리 기법으로서 인증센터의 도움없이 사용자 자신들이 인증을 행하게 된다. 전술한 두 가지 기법과는 달리 기준에 어떠한 관련성도 가질 필요가 없는 이동 임시무선망에 자연스럽게 적용할 수 있는 특징을 가지고 있으며 단기간동안 이용하는 무선망에 적합한 기법이다. 공용키 기반이기 때문에 각 노드는 충분한 계산능력을 보유하고 있어야 한다.

본 논문에서 제안하는 기법은 CA(Certificate Authority, 인증기관)의 기능이 망내의 모든 노드에게 고루 분배되어 있는 완전 분배형 인증을 가정한다. CA의 비밀키 sk_{CA} 가 필요한 모든 조작은 k 개 이상의 노드들이 연합하여 수행이 된다. CA가 제공하는 서비스는 인증서와 관련된 서비스와 시스템 보수 서비스로 분류된다. 인증서와 관련된 서비스는 인증서 갱신과 취소 기능이 있다. 시스템 보수 서비스에는 새롭게 망에 합류되는 노드에게 CA의 비밀키인 sk_{CA} 를 제공하는 기능과 노드들이 공격자들로부터의 타협을 피하기 위해 CA 비밀키의 일부분을 전향적으로 갱신하는 작업(Proactive Secret Sharing)인 공유 갱신 서비스도 포함한다.

3. 키관리 기법

본 논문에서 제안하는 키관리는 시스템의 기동(bootstrap)될 때, 할당의 초기화(Share Initialization), 할당의 갱신(Share Update) 및 인증서의 갱신(Certificate Renewal), 및 인증서의 취소(Revocation)로 구성되어 있으며 각각의 기능은 다음과 같다.

3.1 시스템 기동

시스템 기동 시간 동안에는 이동 임시무선망을 관리하는 딜러(dealer)가 최초로 k 개의 노드를 초기화한다. 기동 시에는 노드 id의 인증서 $cert_{id}$, 딜러의 인증서 $cert_{CA}$, CA의 비밀키 일부분 sk_{CA} 를 k 개의 각 노드에 제공한다. 딜러만이 sk_{CA} 를 알 수 있으며 초기 인증서를 발행할 수 있다. 초기 k 개의 노드를 초기화하기 위한 과정은 다음과 같다(그림 1 참조).

(1) 딜러는 링(ring) Zn상[19]에서 공유 Lagrange 다항식 $f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ 을 생성한다. 이때 $a_0 = sk_{CA}$ 이다.

(2) 한 홉 거리에 있는 노드들의 집합 P 를 결정한다. 그 개수가 k 개 이상인 경우는 단계 3으로 진행한다. k 개 미만인 경우는 집합 P 에 속한 임

의의 노드에게 그 노드에서 한 홉 거리에 있는 노드들의 정보를 요청하여 딜러에서 두 홉 거리에 있는 노드들의 집합 Q를 결정한다. 이 때, P 집합과 Q 집합의 개수가 총 k 개가 되도록 Q 집합의 노드들을 결정한다.

(3) P와 Q의 초기 각 k 개의 노드들을 차례대로 노드 $id_i = 1, 2, \dots, k$ 로 이름을 짓는다. 다항식의 부분합(partial sum)에 해당되는 $S_i = f(id_i) \bmod N$ 값을 P에 속한 노드들에게 전달한다. Q에 속한 노드 id_i 에게 중간 노드를 통해 S_i 를 직접 보내게 되면 그 중간 노드는 공격자로부터 더 쉽게 타협될 가능성이 커지게 된다. 그러므로, Q에 속한 노드들에게는 다음과 같은 암호화 과정을 거쳐 중간 노드를 통해 목적지 노드로 전달을 해야 한다. 먼저, 딜러 노드와 Q에 속한 임의의 노드 id_i 사이에 Diffie-Hellman이 제안한 양자간 키 교환 기법을 적용하여 비밀키를 생성한다. Q에 속한 임의의 노드 id_i 에게 S_i 가 암호화한 상태로 중간 노드(한 홉 거리에 위치)를 거쳐 목적지 노드에게 전송한다.

(4) 딜러는 다항식의 계수를 공유하기 위해 k 개의 $g^{a_0}, g^{a_1}, \dots, g^{a_{k-1}}$ 를 브로드캐스트한다.

(5) 각 노드는 다음 식을 사용하여 3단계에서 수신한 부분이 정당한지 검사한다.

$$g^{S_i} = g^{a_0}, (g^{a_1})^{id_i}, \dots, (g^{a_{k-1}})^{id_i^{k-1}}$$

기동이 끝나면 딜러의 역할은 종료된다.

3.2 할당의 초기화

망에 합류하는 새 노드는 CA 인증서의 비밀키인 sk_{CA} 에 대한 자신의 할당을 배당받게 된다. 시스템 기동 후에는 딜러가 더 이상 망에서의 역할이 없기 때문에 할당의 배분은 이미 초기화된 다른 노드에 의해서 처리가 된다. 이미 초기화된 노드 i 는 새 노드 p 가 부분 할당(partial share)을 요구하면 $S_{p,i} = S_i \cdot l_{id_i}(id_p)$ 을 계산하여 전달한다. $l_{id_i}(x)$ 는 Lagrange 식에서 정의되는 항이다. 합류되는 새 노드의 이웃노드의 개수가 k

개 이하인 경우는 3.1절 시스템 기동 때 사용되었던 (2)번과 (3)번 단계와 같은 방법을 사용한다. 수신된 k개의 부분 할당을 아래의 식과 같이 계산하면 새 노드에 대한 완전한 할당(complete share), 즉, S_p 를 구할 수 있다.

$$S_p = \sum_{i=1}^k S_{p,i} = \sum_{i=1}^k S_i \cdot l_{id_i}(id_p) = f(id_p) \bmod N$$

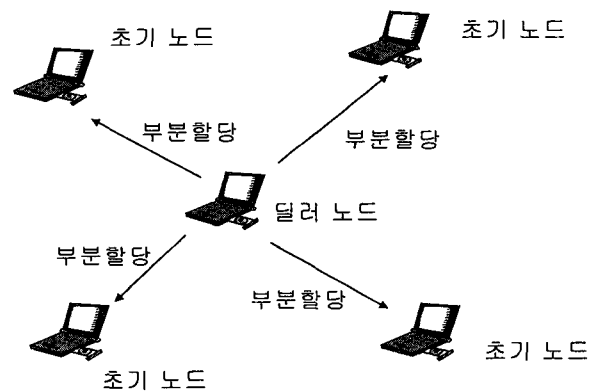


그림 1. 시스템 기동 과정

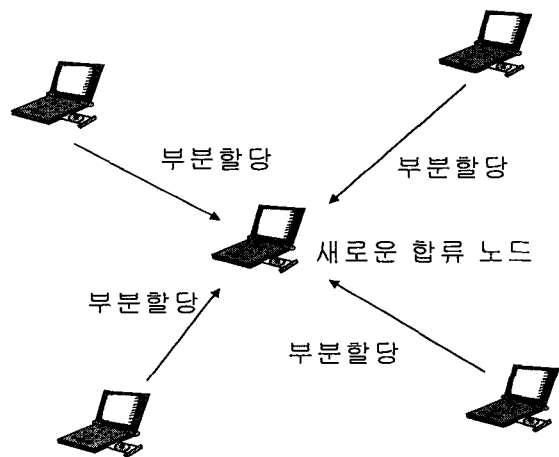


그림 2. 새로운 합류 노드로 인한 할당 초기화 과정

3.3 할당 갱신

k 개 이상의 노드를 타협할 수 있는 공격자에 대항하기 위하여 전향적 비밀 공유법(Proactive Secret Sharing)을 적용한다. 이 기법은 인증서의 비밀키 sk_{CA} 인 공유된 비밀을 재작성하는 과정

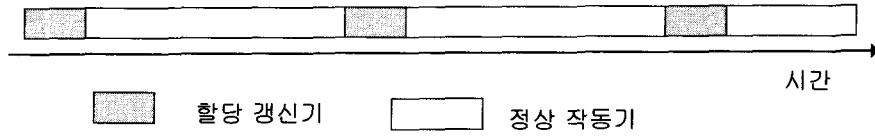


그림 3. 임시 무선망의 생명 주기

을 거치게 된다. 망의 일생은 그림 3과 같이 정상 작동기(Operational Phase)와 할당 갱신기(Share Update Phase)로 이루어져 있다고 볼 수 있다. 정상 작동기 동안은 각 노드들은 인증서를 갱신하고 할당 초기화 작업이 이루어진다. 할당 갱신기 동안은 각각의 노드들이 분산적인 방법으로 할당을 갱신하게 된다. 할당 갱신기는 다음과 같은 순서로 작업이 행해진다.

(1) 각 노드들은 서로 협동하여 갱신 다항식 $f_{update}(x) = b_1x + b_2x^2 + \dots + b_{k-1}x^{k-1} \pmod N$ 를 생성한다.

(2) 망내의 모든 노드들에게 갱신된 다항식을 분배한다.

(3) 모든 노드 p 가 각각 할당 갱신 $\overline{S}_p = f_{update}(id_p)$ 를 계산한다. 할당 갱신 초기에는 각각의 노드가 $1/n$ 의 확률로 갱신 작업을 개시한다. 할당 갱신을 개시하기로 결정한 노드는 갱신 다항식 $f_{update}(x) = b_1x + b_2x^2 + \dots + b_{k-1}x^{k-1} \pmod N$ 을 생성하는 k 개의 노드로 구성된 그룹을 결정한다. 다항식의 각 계수는 암호화한 뒤 망에 브로드캐스트한다. 이 때, 망내의 각 노드들은 $E_{pk_{CA}}(b_1), E_{pk_{CA}}(b_2), \dots, E_{pk_{CA}}(b_{k-1})$ 를 수신하게 되고 시그니처를 검증함으로써 인증을 하게 된다. 여기서, $E_{pk_{CA}}(m)$ 은 부분합 m 을 CA의 공용키로서 암호화하는 것을 나타낸다.

3.4 인증서 갱신(Renewal)

인증서의 유효 기간은 정해져 있기 때문에 유효 기간이 만료하기 전에 갱신을 하여야 한다. 노드 p 가 인증서 $cert$ 를 갱신하고자 할 때 한 홉 거리의 k 개의 이웃 노드들에게 인증서 갱신을 요청한다. 그룹 내의 각 노드 i 는 구 인증서가 만료 혹은 취소가 되지 않았는지 검사를 행한다. 갱신 요청을 수락하면 각 노드들은 부분 인증서 $cert_i$ 를 생성

하고 요청한 노드 p 에게 전달해 준다. 노드 p 는 k 개의 부분 인증서를 결합하여 갱신된 $cert_{updated}$ 를 구한다. 이 과정은 다음과 같다.

(1) 인증서 갱신을 하고자 하는 노드 p 는 한 홉 거리의 이웃 노드들에게 인증서 갱신 요청을 한다. 만약 한 홉 거리에 k 개의 노드가 없으면 3.1절에서와 같은 방법을 취한다.

(2) 요청을 수신하는 각 노드는 요구 노드의 현재 인증서 $cert$ 가 만료되었거나 취소되지 않았는지를 확인한다. 인증서가 유효하다면 노드 i 는 CA 인증서의 비밀키 sk_{CA} 의 할당을 사용하여 부분 인증서 $cert_i = cert^{S_i} \pmod N$ 를 생성한다. S_i 는 sk_{CA} 의 노드 i 의 할당이다.

(3) 요청을 받아들이는 각 노드 i 는 랜덤하게 u 를 생성하고 $A_1 = g^u$ 와 $A_2 = cert^u$ 를 계산한다. 그리고, $c = Hash(g^{S_i}, cert_i, A_1, A_2)$ 와 $r = u - c \cdot S_i$ 를 계산한다. A_1, A_2, r 은 생성된 부분 인증서 \overline{cert}_p 를 검증할 때 사용된다.

(4) 각 노드 i 는 $cert_i, A_1, A_2, r$ 을 요청 노드 p 에게 전달한다.

(5) 노드 p 는 수신된 부분 인증서 중 k 개를 선택하고 $g^r \cdot (g^{S_i})^c = A_1, cert^r \cdot (cert_i)^c = A_2$ 이 됨을 검증한다. 노드 p 는 단계 (3)에서 사용된 해쉬함수를 사용하여 c 를 생성한다. 단계 (4)에서 구한 A_1, A_2, r 값을 사용하여 $g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \dots \cdot (g^{a_{k-1}})^{id_i^{k-1}}$ 를 계산한다.(공유 다항식의 계수를 사용하여)

(6) 부분 인증서 중 하나라도 검증에 실패하면 부당한 인증서를 생성한 노드의 인증서는 폐기된다. 이 경우 다른 노드의 부분 인증서를 선택한 뒤 단계 (4)부터 다시 시작한다. 만약 k 개보다 적은 인증서를 수신했다면 인증서 갱신은 실패로 끝이 나며 임의의 시간 후 다시 시도한다.

(7) 노드 p 는 k 개의 부분 인증서를 결합하여

후보 인증서 *cert.updated*를 구하고 [3]과 같은 방법으로 갱신된 인증서를 구한다.

3.5 인증서 취소(Revocation)

인증서 취소는 모든 노드들이 이웃 노드들의 상태와 인증서 취소 리스트(CRL, certificate revocation list)를 관리하고 있다는 가정을 하고 있다. 이웃 노드의 상태가 정상이 아닐 경우는 CRL에 즉시 등록하고 이웃 노드들에게 알린다. 이런 상황을 수신하는 이웃 노드들은 이 상황이 기록된 CRL내의 취소된 노드에서 발생되지 않았음을 확인한다. 어떤 노드에 대한 취소 요구가 정당한 노드에서 발생된 것이라면 이 노드는 의심 노드(suspected node)로 기록한다. 이러한 취소 요구가 임의의 임계값 k 개를 넘어설 때는 그 노드의 인증서는 취소를 시키고 이 사실을 이웃 노드에게 브로드캐스트한다.

그림 4에서는 노드 B의 주변 노드들이 노드 B의 동작에 이상을 감지하여 인증서가 취소되는 과정을 한 예로서 보여 주고 있다. 노드 A와 노드 C는 노드 B의 작동이 비정상임을 감지하고(1a와 1b) 노드 D에게 각각 통보 한다(2a와 2b). 노드 D는 소스 노드 A와 B가 정상인 것을 노드 D가 관리하는 CRL에서 확인한 후 노드 D에서의 노드 B에 대한 취소 요구 메시지 수가 2이라는 값을 가지게 되므로(본 예에서는 임계값 $k=2$) 이웃 노드(A, C와 E)에게 노드 B의 인증서 취소를 통보(3a, 3b와 3c)한다.

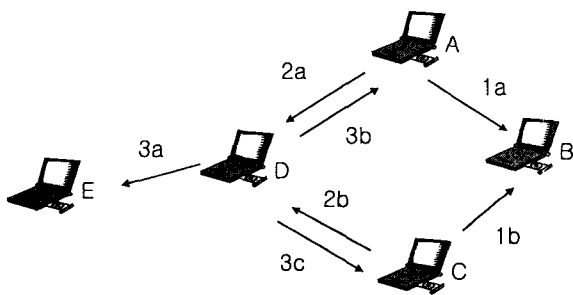


그림 4. 인증서 취소 과정의 예

4. 실험

본 장에서는 본 논문에서 제안된 기법의 성능을

측정하기 위하여 유닉스 운영체제에서 UC Berkeley 대학의 네트워크 시뮬레이터인 ns2[21]를 사용하여 실험하였다. 본 실험에서의 성능 측정치는 주어진 임의의 노드를 기준으로 얼마나 많이 인증서를 작성할 수 있는지의 비율(Certificate Success Ratio, CSR)이다. 일반적으로 주변 노드들이 부분합을 많이 보유하고 있다면 이 비율은 1의 값에 가까워지고 키의 관리가 원활히 진행되어 패킷의 전달율(Packet Delivery Ratio)이 높아지게 되어 궁극적으로 이동망의 성능이 높아지게 된다.

시뮬레이션 환경은 random waypoint model을 사용하였고 이동 공간의 크기는 1500m X 1500m, 노드의 수는 50개, 각 노드들은 휴지시간(pause time) 만큼 쉬었다가 임의의 목적지 노드들을 선택한 후 움직이며 최대 시뮬레이션 시간은 900초이다. 시뮬레이션에서 사용한 라우팅 알고리즘은 AODV [22]이다.

그림 5, 6, 7은 모두 패킷의 크기가 64바이트이며 각각 CBR(Constant Bit Rate) traffic source의 수가 10, 20, 30 일때의 임의의 노드에서 주변 노드의 부분합(partial sum)을 얻어 인증서를 완성시킬 수 있는 비율인 CSR 값의 변화를 보여 주고 있다. 그림에서 보듯이 traffic source의 수에 관계없이 전반적으로 유사한 그래프 특성을 띄고 있고 제안된 기법(Suggested로 표시)이 기존의 AODV를 사용한 기법[3]보다 성능이 개선되었음을 알 수 있다. 노드가 끊임없이 움직이고 있는 pause time=0

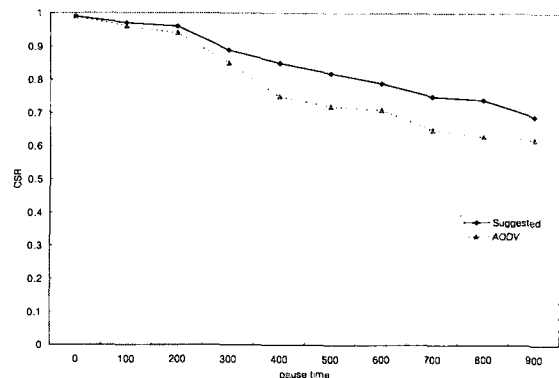


그림 5. source=10 일때의 CSR 변화 그래프

근처인 경우는 임의의 노드를 기준으로 볼 때 주변의 노드들과 많이 접촉(통신)하고 있는 관계로 기존의 방법이나 제안된 방법 모두 0.99 정도의 CSR 값을 가지고 있음을 알 수 있다. 그러나, 노드가 점점 움직임이 줄어들어 따라 기존의 방법은 부분합을 1개의 홉 거리의 노드에서만 구할 수 있기 때문에 CSR의 값이 감소하지만 제안된 기법은 부분합을 구하기 위해서 2홉 이상에서 구하려고 시도하기 때문에 기존 방법보다 CSR의 값이 비교적 완만하게 감소됨을 알 수 있다.

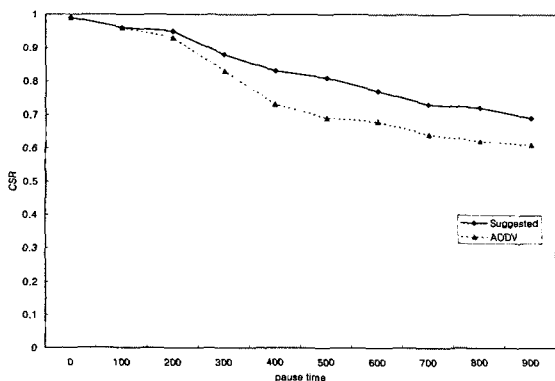


그림 6. source=20 일때의 CSR 변화 그래프

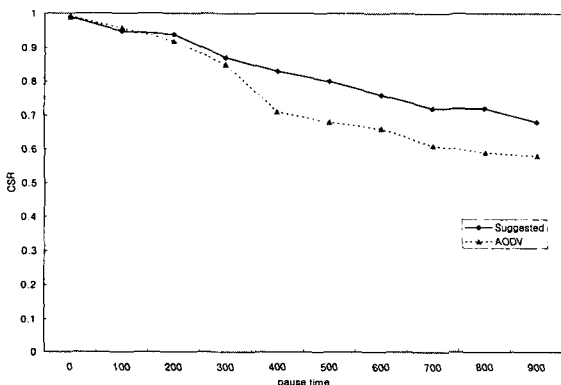


그림 7. source=30 일때의 CSR 변화 그래프

5. 결론 및 향후 과제

본 논문에서는 이동성을 가진 다수의 노드들에 의해 자율적으로 구성되는 이동 임시무선망(Mobile Ad Hoc Network)에서 무선망이라는 속성

때문에 보안에 취약한 문제점을 해결하는 방안으로 이동 임시 무선망에서 이동 노드들간에 보안성을 강화하기 위해 키들을 관리하는 기법을 제안하였다. 임시 무선망에서 키를 분배하는 기법 중 완전 분배형 인증 기법이 널리 적용되고 있으며 임의의 노드를 기준으로 주변에 특정 개수 이하의 노드가 활동 중인 경우에도 키 관리를 원활히 할 수 있는 기법을 제안하였다. 제안된 기법은 시스템의 기동(bootstrap), 할당의 초기화(Share Initialization), 할당의 갱신(Share Update) 및 인증서의 갱신(Certificate Renewal) 및 인증서의 취소(Revocation)로 구성되어 있으며 시뮬레이션을 통해 기존의 방법보다 우수함을 보인다는 것을 증명하였다. 제안된 방법은 AODV 라우팅 알고리즘을 사용하였지만 향후 다른 종류의 라우팅 알고리즘에 적용하여 성능 측정 비교를 행할 예정이다.

참고 문헌

- [1] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Networks*, Volume 13, Issue 6, 1999.
- [2] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks," Technical Report 200030, UCLA Computer Science Department, 2000.
- [3] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," *Proceedings of the 9th Conference on Network Protocols (ICNP)*, pp. 251-260, 2001.
- [4] 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)*, 2002.
- [5] J-P. Hubaux, L. Buttyán and S. Capkun, "The Quest for Security in Mobile Ad Hoc Networks," In *Proc. ACM MOBICOM*, Oct. 2001.
- [6] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi Wong, "Talking To Strangers :

- Authentication in Ad-Hoc Wireless Networks, Internet Society," *Symposium on Network and Distributed Systems Security* (NDSS '02), San Diego, California, February, 2002.
- [7] N. Asokan, P. Ginzborg, "Key Agreement in Ad Hoc Networks," *Computer Communications*, Volume 23, pp. 1627-1637, 2000.
- [8] A. Shamir, "How to Share a Secret", *Communications of ACM*. 1979.
- [9] M. Hietalahti, "Key Establishment in Ad-Hoc Networks", Laboratory for Theoretical Computer Science, Helsinki University of Technology 2001.
- [10] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *ACM SIGMOBILE* 2001.
- [11] C. Perkins, *Ad Hoc Networking*, Addison-Wesley 2001, ISBN 0201309769.
- [12] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press 1997, ISBN 0849385237.
- [13] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed., Prentice-Hall 1999, ISBN 0138690170.
- [14] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi Wong, "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks", Internet Society, Conference Proceeding of NDSS Conference 2002.
- [15] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks", *Computer Communications*, Volume 23, Pages 1627-1637.
- [16] J. Mackar and S. Corson, RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF 1999.
- [17] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks", *Security Protocols*, 7th International Workshop Proceedings, Lecture Notes in Computer Science, Springer-Verlag 1999.
- [18] H. Luo and S. Lu, "Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks", Technical Report 200030, UCLA Computer Science Department 2000.
- [19] Y. Frankel, P. Gemmell, P. D. MacKenzie and Moti Yung, "Optimal-resilience proactive public-key cryptosystems", *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS '97)*, 1997.
- [20] S. Capkun, J. Hubaux and L. Buttyan, "Mobility helps security in ad hoc networks", *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2003.
- [21] The Network Simulator NS2, <http://www.isi.edu/nsnam/ns>.
- [22] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing." *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, pp. 90-100.



김 시 관 (Si-Gwan Kim)

1982년 2월 경북대학교 공과대학
학사

1984년 2월 한국과학기술원 전산
학과 석사

1984년 ~ 1995년 삼성전자, LG
정보통신

2000년 한국과학기술원 전산학과 박사

2002년 ~ 현재 금오공대 컴퓨터공학부 교수

(관심분야 : 컴퓨터구조, 병렬처리, 이동컴퓨팅등)



신 윤 식 (Yoon-Shik Shin)

1982년 2월 경북대학교 공과대
학 학사

1985년 2월 한국과학기술원 전
산학과 석사

1988년 ~ 현재 금오공대 컴퓨
터공학부 교수

(관심분야 : 이동무선망, 소프트웨어공학, 프로그래
밍언어등)



임 은 기 (Eun-Ki Lim)

1977년 2월 서울대학교 자연대학
수학과 학사

1988년 2월 한국과학기술원 전산
학과 석사

1989년 ~ 현재 금오공대 컴퓨터공학부 교수

(관심분야 : 컴파일러, 프로그래밍언어, 데이터베이스
설계)