이동 Ad Hoc 네트워크에서의 효율적인 인증기법에 대한 연구

마용재*, 이승찬*, 박건우*, 송주석*
*연세대학교 컴퓨터과학과

Effective Authentication in Mobile Ad Hoc Networks

Yong-Jae Ma*, Seung-Chan Lee*, Gun-Woo Park*, Joo-Seok Song*
*Dept. of Computer Science, Yonsei University.

요 약

PKI(Public Key Infrastructure)는 인증, 무결성, 기밀성, 부인봉쇄, 접근통제 등의 보안 기능을 일관성 있게 제공해 주는 기술로서, 이동통신과 무선 인터넷의 급속한 성장에 따른 무선 환경에서도 무선 PKI가 보안기능을 제공할 궁극적인 대안으로 여겨지고 있다. 본 연구는 이동 Ad-hoc 네트워크에서 Threshold cryptography를 이용하여 PKI의 기능을 제공할 수 있도록 하였으며, 기존의 연구들과 유사한 수준의 보안성을 가지면서도 CR(Certification Responsible) 노드의 가용성을 높여 네트워크의 성능을 향상 시킬 수 있는 인증 기법을 제시한다.

I. 서론

Ad-hoc 네트워크는 기지국과 같은 고정된 인프라의 도움 없이, 이동 단말 간에 통신이 이루어지는 무선 네트워크이다. 망 구성이 용이한 반면, 토폴로지가 동적이고 대역폭이 제한된다. 뿐만 아니라, 각 단말의 에너지 소비가 큰 관건이 되고, 보안에 취약하다는 단점을 갖는다[1].

국제 표준화 기구인 IETF(Internet Engineering Task Force)의 MANET(Mobile Ad hoc Network) 워킹그룹에서는 Ad-hoc 네트워크의 라우팅 프로토콜에 대한 연구가 중점적으로 이루어지고 있다. 그러나 Ad-hoc 네트워크는 노드의 이동, 토폴로지 변화, 중앙 집중화된 인프라의 부재 등으로 인하여 침입이나 오동작에 의한 보안상의 위험성이 훨씬 높다[2]. 따라서 본 연구에서는 Ad-hoc 네트워크에서의 보안문제에 대하여 다루고자 한다.

공개키 암호화 방식은 20년이 넘게 인증, 전자 서명, 암호화 등을 포함한 기본적인 보안을 제공하는 가장 효율적인 방법 중 하나로 인식되어 왔다. PKI(Public Key Infrastructure)는 디지털 인증서의 효율적인 관리를 위해 개발되었으며, 이는 공개키 암호화 방식에 있어 가장 중요한 요소이다. PKI를 구성하는 가장 중요한 요소는 디지털 인증서의 유효성을 증명할 수 있는 기관인 CA(Certificate Authority)이다. PKI는 연결성이 보장되는 유선 네트워크를 기반으로 개발되어, CA의 보안성과 확장성에만 초점이 맞추어져 연구되어왔다[3, 4].

그러나 이동 Ad-hoc 네트워크에는 인프라가 없기 때문에 좋은 연결성을 보장할 수 없고, 이동 노드도 물리적으로 취약하다. 따라서 Ad-hoc 네트워크에서 PKI를 제공하기 위한 많은 기법들은 노드의 취약성을 해결하기 위하여 Threshold cryptography를 이용하여 CA의 기

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

능을 여러 개의 노드들로 분산시키는 방법을 제안하고 있다[5].

본 논문은 이동 Ad-hoc 환경에서 PKI를 구현하기 위하여 Threshold Cryptography를 도입하고, 인증노드들의 가용성을 높여 좀 더 빠르고 효율적인 인증을 수행할 수 있는 방법을 제시한다.

II. 관련연구

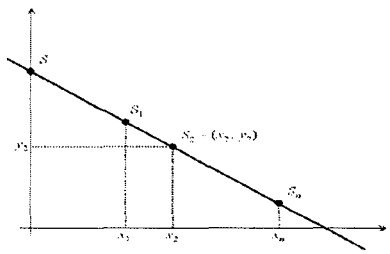
2.1. Threshold cryptography

Threshold cryptography란 데이터 D를 n개의 조각으로 나누었을 때 임의의 k(k≤n)개 이상의 조각들로부터 원래의 데이터 D를 쉽게 재생산해 낼 수 있다는 원리를 이용하여 보안을 제공하는 기법이다.

데이터 D를 D1, D2, D3, …, Dn으로 나누었을 때, (k, n) threshold 의 정리는 다음과 같다.

(1) k개 이상의 Di 조각을 알면 쉽게 계산에 의하여 D를 만들어낼 수 있다.
(2) k-1개 이하의 Di조각에 대한 정보는 D에 대한 어떠한 정보도 제공하지 않는다.

다항식을 이용하는 (k, n) Threshold 기법을 살펴보면 다음과 같다.



(그림 1) (k, n) threshold scheme

(그림 1)과 같이 2차원의 평면에서 k개의 점 (x_1, y_1), …, (x_k, y_k)은 모든 i에 대하여 $f(x_i)=y_i$를 만족하는 단 하나의 k-1차 다항식 f(x)를 결정할 수 있다. 데이터 D를 하나의 숫자라고 한다면, 우리는 D를 k개로 나누기 위해 다음의 조건을 만족하는 임의의 k-1차 다항식을 정한다.

(1) $f(x)=a[0]+a[1]*x^1+\cdots+a[k-1]*x^{k-1}$
(2) $a[0]=D$

역으로 D 를 만들어내기 위해서는 k개 이상의 좌표를 필요로 한다. k개의 점의 좌표가 모두 모이면 k-1차 방정식을 만들어낼 수 있으므로 y절편인 D값을 알 수 있다.

2.2. MoCA(Mobile Certification Authority)

이동 Ad-hoc 네트워크에서 PKI 기능을 수행하기 위한 기법으로서, 특정 노드들은 분산된 CA 기능을 수행하기 위해 MoCA 노드로 선택된다. 기능을 분산하기 위하여 Threshold Cryptography 기법을 사용하며 클라이언트 노드들은 MoCA 인증 프로토콜을 사용한다. n개의 MOCA 노들들은 CA의 공개키를 공유하며, k개 이상의 MoCA 노드들이 모이면 CA의 기능을 제공할 수 있다.

III. 제안기법

3.1. 기존의 기법이 가지는 문제점

MoCA 기법에서 CA의 기능을 수행하기 위해서는 지정된 MoCA 노드들에 접촉 하여야만 한다. MoCA 노드는 에너지 레벨을 고려하여 선택되고 이후로는 정적으로 고정되어 있기 때문에 네트워크의 상태에 따라 가용성이 떨어질 가능성이 있다.

3.2. 제안하는 아이디어

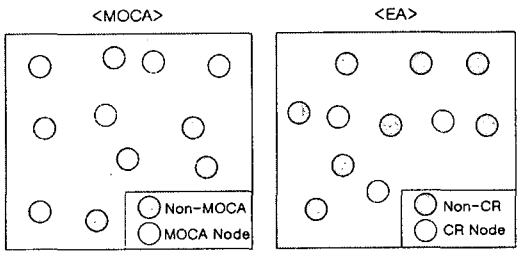
본 연구에서는 이동 Ad-hoc 네트워크에서 PKI 기능을 제공하기 위하여 Threshold Cryptography 기법을 이용하여 CA 기능을 분산시키고, 인증의 시간을 단축하고 인증의 가능성을 높일 수 있는 기법인 EA(Effective Authentication in Mobile Ad-hoc Network)를 제안한다.

EA에서는 CA의 기능을 n개의 CR (Certification Authority) 노드에 분산한다. CR 노드는 다음과 같은 과정에 의해 선택된다.

각 노드들은 자신의 주변에 있는 non-CR 노드의 개수를 감지하여 N3(Number of my Neibor Nodes except CR node)라는 필드에 저장한다. 네트워크 관리자는 처음에 NREQ (Neighbor Request)라는 패킷을 broadcast 하

고, NREQ 패킷을 받은 모든 노드들은 NREP (Neighbor Response)라는 패킷에 N3 값을 넣어 응답한다. 그러면 네트워크 관리자는 각 노드들의 N3 값을 분석하여, N3 필드의 값이 가장 큰 n개의 노드들을 CR 노드로 선정한다. 기존의 CR 노드들로부터 생성된 CA 정보는 새롭게 선택된 CR 노드에게 보내지고, 새로운 CR노드는 자신이 새로운 CR 노드가 되었음을 브로드캐스트 한다.

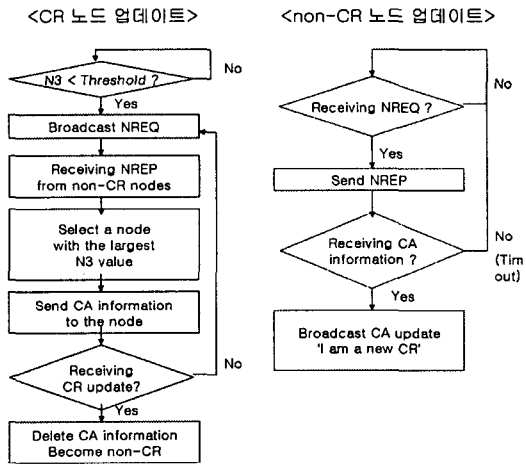
이렇게 선정된 CR 노드들은 정적이지 않고 동적으로 업데이트가 수행된다. 각 노드들은 주기적으로 자신의 N3 필드 값을 업데이트하여 주위에 non-CR 노드가 임계값보다 적어지게 되면, CR노드로서의 역할을 중단하게 된다.



(그림 2) MoCA 에서의 밀집된 노드와 EA에서의 분산된 노드

CR 노드들은 분산된 CA로서의 역할을 수행하게 되며 동적으로 업데이트 된다. 클라이언트 노드는 CREQ 패킷을 통해 서비스를 요청하여 k개 이상의 CR노드들로부터 CREP 패킷을 받아 CA의 정보를 생성한다. EH한 CA 정보를 생성한 클라이언트 노드는 다수 노드들로부터 인증을 받았으므로 새로운 CR 노드로서의 역할을 수행할 수 있도록 한다. 만약 CREQ를 받고 나서도 정해진 시간동안 CREP를 전송하지 못하면 CR노드로서의 자격을 잃게 된다. 이렇게 지정된 CR 노드들은 접근 가능한 노드들만으로 구성되므로 MoCA 기법에 비하여 CR노드에 대한 가용성이 높다. 또한 Mobile 노드들의 움직임은 미리 예측할 수 없는 경우가 많기 때문에 토폴로지의 변화에 따른 주기적 업데이트가 필요하게 된다. MoCA의 경우에는 (그림2)와 같이 MoCA 노드들이 편중되는 상황이 발생할 수 있으며, MoCA 노드로부터 멀리 떨어져 있는 노드가 인증을 받기 위해서는 많은 시간이 소비된다.

반면에 EA에서는 CR 노드가 동적으로 업데이트됨으로써 CR 노드가 어느 정도 분산되어 있음을 보장하며, 이는 CR 노드에 대한 접근 줄이고 네트워크 자원을 절약할 수 있도록 해준다.



(그림 3) 노드의 동적 업데이트 과정

IV. 성능평가

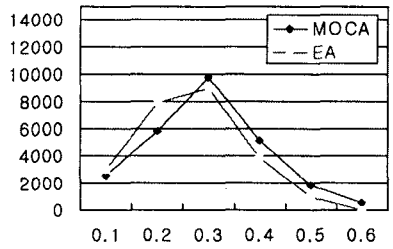
본 연구에서 제안하는 기법의 성능 평가를 위하여 기존의 MOCA와 EA에서의 인증 소요시간 및 성공률에 대한 분석을 하였다. NS-2를 이용하여 시뮬레이션을 수행하였으며 다음과 같이 파라미터를 설정하였다.

<표 1> 성능 평가를 위한 파라미터

	인증시간	인증 성공률
전체 이동 노드의 개수	150	300
CR(MOCA) node의 개수	30	50
Certification request 횟수	10 by 100	10 by 200
노드가 멈추는 시간	0, 10sec	
노드의 속도	0~20m/s random	
네트워크 면적	1000m X 1000m	
전체 시뮬레이션 시간	600sec	

성능 평가를 위하여 여러 차례 반복된 인증 요청에서 완료에 걸리는 시간을 비교하였을 때 (그림 4)와 같은 그래프를 나타내었다. 그래프에서 x축은 인증에 소요된 시간을 나타내며 y

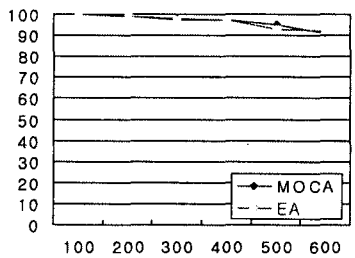
축은 해당 시간대에 완료된 인증의 횟수를 나타낸다. 그래프에서 보는 바와 같이 인증에 소요된 시간이 EA에서 더 적게 나타나는 것을 볼 수 있다. 이것은 시간이 지남에 따라 이동 노드들의 위치가 변하게 되어, MoCA의 경우 MoCA노드의 편중현상이 발생하는 경우가 생기게 됨에 따라 이러한 차이가 벌어지는 것으로 예상된다.



(그림 4) 인증에 소요된 시간 비교

(그림 5)는 MOCA와 EA에서의 인증 성공률에 대하여 나타낸 그래프이다. x축은 시뮬레이션 시간을 나타내며 y축은 인증요청에 대한 성공 백분율을 나타낸다. 그래프에서 보는 바와 같이 시간의 흐름에 따라 MOCA와 EA모두 인증 성공률이 소폭 떨어지는 것을 볼 수 있었다. 이것은 시간이 지나면서 에너지 레벨이 떨어짐에 따라 더 이상 기능을 수행할 수 없는 MoCA 노드와 CR노드가 생기기 때문인 것으로 볼수 있다. 그러나 MoCA와 EA사이의 차이는 거의 없는 것으로 보여진다.

따라서 MoCA와 EA는 같은 정도의 인증 성공률을 나타내지만 인증에 소요되는 시간에 대하여는 EA가 더 우수한 성능을 나타내고 있음을 알 수 있다.



(그림 5) 시간에 따른 인증 성공률

V. 결론

본 연구에서 제안하는 방식은 이동 Ad-hoc 환경에서 PKI 기능을 제공하기 위하여, Threshold Cryptograpy 기법을 이용하여 CR 노드가 분산된 CA의 기능을 수행하도록 하였다. 또한 CR의 동적인 업데이트를 통하여 기존의 MoCA 기법에 비하여 CR노드에 대한 접근성을 향상시켜 인증에 소요되는 평균적인 시간을 단축시킬 수 있었다.

그러나 에너지 레벨에 따른 CR 노드의 취약성에 대한 고려가 부족하고, 동적인 업데이트에 대한 추가적인 오버헤드에 대한 비용이 계산되지 않았으므로 이러한 부분에 대한 추가적인 고려를 향후 과제로 남겨놓는다.

[참고문헌]

[1] C. E. Perkins, Ad hoc Networking, New York: Addison-Wesley, 2001.

[2] L. Buttyan and J. P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks." Mobile Computing and Communications Review, vol. 6, no. 4, 2002

[3] VeriSign, Inc. Company homepage available at http://www.verisign.com/.

[4] Janne Gustafsson, Janne Lassila, and et al. Pki-security in mobile business - case: Sonera smarttrust. Available at citeseer.nj.nec.com/466933.html.

[5] J. Macker and M. Corson. Mobile ad hoc networking and the IETF. Mobile Computing and Communications Review, 1998.

[6] Seung Yi, Robin Kravets, MOCA : Mobile Ceritificate Authority for Wireless Ad Hoc Networks, Internet2 Middleware Initiative