MANET 환경에서 클러스터링을 이용한 ID 기반 공개키 관리 분산

최홍준 O, 홍성제, 김종

포항공과대학교 컴퓨터공학과

{formetel O, sjhong, jkim}@postech.ac.kr

Distributing ID-based Public Key Management based on Clustering in MANET

Hong Jun Choi O, Sung Je Hong, Jong Kim

Department of Computer Science and Engineering

Pohang University of Science and Technology (POSTECH)

요 약

MANET(Mobile Ad hoc Network)에서는 고정된 인프라가 없고, 노드가 움직이기 때문에 네트워크 위상(topology)이 동적으로 변하는 특성을 가지고 있다. 따라서 고정된 TTP(Trusted Third Party)를 가지는 기존의 공개키 관리 시스템을 그대로 사용하는 것이 불가능하다. 최근에 MANET을 위한 공개키 시스템이 많이 제안되었지만, 인증서 관리와 분산된 CA(Certificate Authority)에 접근하기 위한 네트워크 오버헤드가 존재한다. 본 논문에서는 ID 기반 암호(ID-based cryptography)시스템을 이용해서 인증서와 CA을 제거하고, 추가적으로 필요한 개인키 생성자(private key generator, PKG) TTP를 클러스터링을 이용하여 효율적으로 분산시킨다. 성능 분석결과를 통하여 제안하는 방법이 기존에 제시된 키 관리 기법에 비해 키 관리에 필요한 통신 오버헤드를 감소시키는 것을 보인다.

1. 서 론

MANET(Mobile Ad Hoc Network)은 고정된 인프라 없이 무선 신호를 이용해서 서로간 네트워크를 구성한다. MANET에서의 안전한 통신은 대부분 암호학적 메커니즘을 기반으로 동작한다. 암호학적 메커니즘에서 키는 개체들의 신뢰성을 보장하는 역할을 수행한다. 따라서 MANET에서 키 관리는 기존 네트워크에서와 마찬가지로 안전한 시스템을 위한 핵심 요소라고 할 수 있다. 하지만 기존 네트워크 시스템과는 다르게 MANET은 기존의 키 관리를 그대로 적용하기에는 다음과 같은 제한사항이 존재한다[1]. 첫째 네트워크 위상(topology)이 동적으로 변하는 특성을 가진다. 네트워크의 각 노드는 이동성을 가지고 있기 때문에 노드의 위치와 그들간의 배열 및 구성이 실시간으로 변경될 수 있다. 둘째, 무선 신호를 통해서 통신을 수행하기 때문에 제한된 대역폭을 가진다. 셋째, 각 노드는 제안된 에너지 자원을 가지고 있기 때문에 복잡한 연산을 계속적으로 수행할 경우 에너지 고갈 문제가 발생할 수 있다. 마지막으로, 각 노드는 무선 신호를 통해 통신하기 때문에 송수신 되는 정보들은 누구나 중간에서 도청이 가능하다. MANET에서의 키 관리 시 이런 제한사항들을 고려한 많은 키 관리 기술들이 제안되었다[2,3,4,6,7,8,11].

키 관리 시스템은 크게 공개키 방식과 대칭키 방식으로 나눌 수 있다. 대칭키 방식은 가장 간단한 방법으로는 모든 노드가 동일한 대칭키를 공유하는 방법이다[6.7]. 이 방법은 동일한 대칭키를 가지기 위한 중앙 센터로부터 키분배 방법이 필요하다. 또 하나의 노드만 공격 당하면 전체 네트워크의 보안이 깨질 수 있다. MANET 가 같이 모든 노드가 이동성이 있는 네트워크에서는 현실적으로 적용이 불가능하다. 이와 달리 각각의 노드가 서로 다른 대칭키를 가지는 방법이 있다[11]. 이 방식은 비교적 간단한 연산을 수행함으로써 대칭키를 공유할 수 있지만 MANET의 이동성 특성으로 키 분배에서 심각한 확장성(scalability) 문제를 야기할 수 있다. 또한 대칭키 방식은 전자서명(digital signature)과 같은 강력한 암호학적 방식을 제공하지 못하는 큰 단점이 존재한다.

공개키 시스템은 각 노드가 공개키와 개인키를 사용하고, TTP(Trusted Third Party)가 그것들을 인증해주는 수단을 제공한다. 키 분배에 대한 부담이

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 지원사업의 연구결과로 수행되었음 (IITA-2007-(C1090-0701-0035))

존재하지 않고, 전자 서명과 같은 강력한 암호학적 기능을 제공할 수 있다. 공개키 시스템은 다시 인증서 기반[3,8]과 ID 기반 공개키 시스템[2,4]으로 나눌 수 있다. 인증서 기반 공개키 기법은 중앙 집중식 CA (Certificate Authority)가 노드를 인증하는 인증서와 공개키를 제공한다. ID 기반 공개키 기법은 각 노드의 고유 ID가 공개키로 사용되고 PKG (Private Key Generator)가 노드에게 개인키를 제공하는 방식으로, PKG의 공개키로 노드의 공개키를 인증하므로 인증서가 필요하지 않는다. 위의 두 가지 방식에서 CA와 PKG는 모두 TTP인데 MANET에서는 고정된 TTP를 가정할 수 없다. 이 문제를 해결하기 위해서 Threshold 암호기법(Threshold cryptography)을 사용하여 특정 수 이상의 노드가 TTP의 역할을 분산해서 수행한다. 하지만 이 방법에서는 TTP가 임의로 분산되어 있기 때문에, 각 노드가 TTP와 통신하기 위해서는 분산된 TTP의 라우팅 경로를 탐색해야 하기 때문에 라우팅 오버헤드와 대역폭 낭비 등의 문제점을 가진다.

본 논문에서는 효율적으로 TTP을 분산하는 ID 기반 공개키 관리 기법을 제안한다. 제안된 기법은 ID 기반 공개키 방식을 이용해서 인증서의 사용을 없애고, MANET의 특성을 고려하여 PKG를 효율적으로 분산시킴으로써 임의의 분산된 노드들과 통신을 해야 하는 부담을 줄인다.

본 논문의 구성은 다음과 같다. 제2장에서 인증서가 없는 공개키 관리 기법들에 대한 관련연구를 소개하고, 제3장에서는 제안된 시스템으로써 클러스터링을 이용한 ID 기반 공개키 관리 시스템에 대해서 기술한다. 제4장에서는 제안된 시스템의 성능 분석 결과를 보이고, 제5장에서는 결론을 맺고 향후 연구방향을 제시한다.

2. 관련연구

ID 기반의 공개키 시스템은 TTP가 각 노드에게 개인키를 제공하고 그 키는 TTP의 공개키를 사용하여 인증한다. 이 방식을 이용해서 기존의 공개키 방식과는 달리, 인증서가 필요 없는 키 관리 시스템들이 최근 제안되었다[2,4]. 이 방식들은 모두 (t, n)-threshold cryptography[9]를 기반으로 TTP의 기능을 여러 노드들에게 분산한다. 네트워크 초기 설정 시에 n개의 노드가 비밀을 서로 공유함으로써 분산된 TTP를 구성하는데, 이후에 참여하는 각 노드들은 분산된 TTP중 임의의 t개 이상의 노드들과 통신 후 자신의 개인키를 발급받는다. 본 장에서는 ID 기반 공개키 관리 기법과 Threshold 암호 기법에 대하여 알아보고 이전 연구들의 문제점을 제시한다.

2.1. ID 기반 공개키 관리 기법

ID 기반 공개키 관리 기법[5]은 공개키 방식 중 하나로써, 각 노드들이 공개키 대신 자신의 ID(예. MAC 주소 등)를 사용하고, 그 ID를 인증하기 위해서는 TTP가 발행한 인증서를 사용하는 것이 아니라 TTP의 공개키를 이용한다.

이 기법에서는 개인키 발급을 수행하는 PKG라는 TTP을 이용한다. PKG는 마스터 공개키/개인키를 생성하고, 각 노드들의 ID을 기반으로 비밀키를 발급해 주는 역할을 수행한다. 각 노드는 초기에 PKG에게 자신의 ID를 제출하고 PKG는 자신의 비밀키를 이용해서 노드의 비밀키를 발급해 준다. 이후에 각 노드는 자신의 ID를 공개키로 이용하여 메시지를 암호화 하고, 자신의 개인키를 이용하여 복호화한다. 또한 다른 노드들의 공개키를 인증할 때는 PKG의 공개키를 이용한다.

2.2. Threshold 암호기법

Threshold 암호기법[9]은 암호학적인 기능을 여러 노드에게 분산시켜 특정 수 이상의 노드들이 참여해야만 그 기능을 수행할 수 있도록 하는 방법이다. t-out-of-n threshold 방식에서는 n개의 노드 중에 t개 이상의 노드가 참여해야만 원하는 기능을 수행할 수 있다. 다시 말하면, 공격자는 하나의 노드만 공격해서는 원하는 기능을 수행할 수 없고 동시에 t개 이상의 노드에게 공격이 성공해야 한다.

기존 제안된 방법들[2,4]은 여러 노드에게 TTP의 기능이 임의로 분산되기 때문에, TTP와 통신을 하기 위해서는 라우팅 프로토콜 수행으로 인한 부담이 존재한다. 새로 참여한 노드들은 초기에 분산된 TTP에 대한 정보가 없기 때문에 분산된 TTP를 찾기 위해서 라우팅 프로토콜을 이용해서 직접 분산된 TTP의 위치를 모두 찾아내야 한다. 또한 분산된 TTP들의 위치가 참여한 노드들과 가까운 곳에 있다는 것을 보장할 수 없으므로 멀티 홉 라우팅이 불가피하다.

3. 클러스터링을 이용한 ID 기반 공개키 관리 시스템

이 장에서는 TTP을 효율적으로 분산하기 위한 클러스터링을 이용한 ID 기반 공개키 관리 시스템에 대해서 설명한다. 먼저 분산된 PKG 형성방법을 설명하고, 분산 PKG 하에서 노드의 비밀키를 생성하는 방법에 대하여 설명한다.

3.1. 분산된 PKG 형성

MANET에서는 기존 시스템과 같이 고정된 TTP를 사용하는 것이 어렵기 때문에 여러 노드들에게 TTP의 기능을 분산시켜야 한다. 제안된 시스템에서는 ID 기반 공개키 방식을 사용하기 때문에 개인키 발급을 위한 PKG가 필요하다. PKG역시 TTP로서 하나의 노드가 이 기능을 수행할 수 없기 때문에 초기에 분산된 threshold

PKG를 구성해야 한다.

MANET에서는 효율적인 라우팅을 위해 전체 네트워크를 여러 개의 클러스터로 구분하는 방법을 사용한다. 본 논문에서는 이미 제안되어 있는 효율적인 클러스터링 알고리즘[10]을 사용한다.

각 클러스터는 하나의 특별한 노드(cluster head, CH)를 가진다. CH는 자신의 클러스터에 속한 일반 노드들 중에서 각 노드들과 가까운 노드가 일반적으로 선택되거나, 혹은 임의적으로 선택될 수 있다. CH는 각 노드에게 주기적으로 관리 메시지를 보내면서 클러스터 멤버의 위치 정보를 관리하고 클러스터 멤버로부터 라우팅 경로 탐색 요청에 대한 정보를 제공한다. 또한 인접한 클러스터의 대한 라우팅 정보를 유지한다. CH-CH간, CH-클러스터 멤버간의 통신은 공유하고 있는 대칭키를 이용하여 안전하게 수행한다. 그림 1과 같이 CH는 논리적으로 CH들만의 overlay network을 구성할 수 있다. 이것을 이용해서 inter/intra 클러스터 라우팅을 효과적으로 수행할 수 있다.

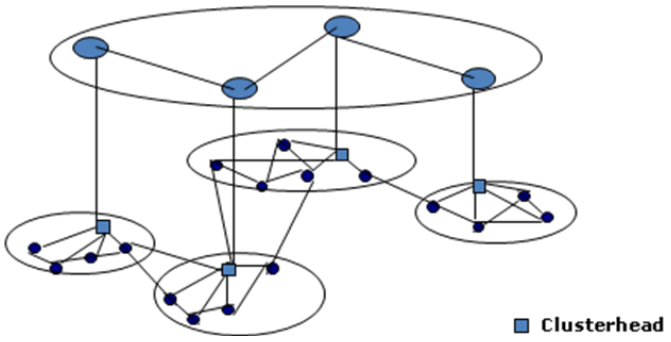

그림 1. Clustering

클러스터가 형성이 되면, CH는 저장하고 있는 이웃 CH의 라우팅 정보를 이용해서 직접적으로 인접한 n개 이상의 CH와 통신한다. 이후 Threshold 암호기법을 이용해서 각 노드의 비밀키 생성에 필요한 마스터 비밀키를 공유한다. 수행 단계는 다음과 같다.

1) 노드 N_i는 임의의 비밀값 p_i을 생성하고 Z_q상에서 $f_i(0)=p_i$가 되는 k-1차 다항식 $f_i(x)$를 선택한다.
2) 노드 N_i는 노드 N_j (j=1,2,...,n, j≠i)에 대해서 서브 비밀 $ss_{ij}=f_i(j)$를 생성한 후 모든 N_j에게 안전하게 전송한다.
3) N_j는 N-1개의 서브 비밀을 받은 후, 자신의 서브 비밀을 추가해 부분 마스터 비밀키 $s_j=\sum_{i=1}^{n} ss_{ij}=\sum_{i=1}^{n} f_i(j)$를 생성한다.
4) k개 이상의 노드는 함께 $\sum_{i=1}^{k} s_i l_i(z) \bmod q$ ($l_i(z)$는 Lagrange coefficient)를 계산해서 마스터 비밀키 $s_M=\sum_{i=1}^{n} p_i=\sum_{i=1}^{n} f(0)$ 를 복구할 수 있다.

분산된 PKG가 각각 $s_i q$(단, q는 공유값)를 계산하고 전체를 모아서 마스터 공개키 $Q_M=\sum_{i=1}^{n} s_i q$를 생성한다.

기존에 제시되었던 방식들은 모두 임의의 n개의 노드가 threshold PKG를 구성한다. 하지만 제안된 방식은 클러스터링을 이용해서 인접한 CH간에 효율적인 PKG를 구성한다. CH는 임의적으로 선택 되고 여러 노드가 비밀키를 공유하기 때문에 임의의 공격자가 자발적으로 CH로 선출되기 어렵고, 또한 하나의 노드가 아니라 동시에 t개의 노드를 공격해야 PKG의 원하는 기능을 획득할 수 있기 때문에 더욱 보안 강도가 높아졌다.

3.2 참여 노드의 비밀키 생성

PKG가 형성되면, 이후에 접속하는 모든 노드들은 자신의 개인키를 획득하기 위해서 PKG에게 PKG 서비스 요청 메시지를 전송해야 한다. 요청하는 노드는 자신의 ID(Q_{ID})를 공개키로 사용해서 k개의 PKG에게 비밀키를 요청한다. k개의 PKG는 각각 자신의 부분 마스터 비밀키를 이용해서 요청 노드의 부분 비밀키 $sk_i=S_iQ_{ID}$ (k=1,...,k)를 안전하게 전송한다. 요청 노드는 부분 비밀키를 전송 받은 후 개인키 sk를 다음과 같이 계산하여 생성할 수 있다. $sk = \sum_{i=1}^{n} s_i Q_{ID}$.

본 시스템에서는 참여 노드의 CH가 PKG와 인접한 클러스터의 CH들이 분산된 PKG을 구성하고 있으므로 참여 노드는 자신의 CH에게 바로 PKG서비스를 요청할 수 있다. 즉, 분산된 모든 PKG를 찾기 위한 라우팅 과정이 필요 없게 된다. 요청을 받은 CH는 비밀을 공유한 인접한 CH들에 대한 라우팅 정보를 직접적으로 참여 노드에게 전송할 수 있다. 그 후에 이 노드는 분산된 PKG와 통신을 통해 자신의 비밀키를 생성할 수 있다. 결국 생성된 개인 키와 자신의 ID을 공개키로 이용함으로써 안전한 통신이 가능하다.

4. 성능 분석

본 연구에서 제안된 방법을 인증서 사용 측면, 개인키 획득 측면, 클러스터링 형성 측면에서 통신 비용을 고려해 본다.

전통적인 PKI방식과 비교해 보면, 제안된 시스템은 ID 기반 공개키 관리 기법을 사용함으로써 PKG로부터 개인키를 발급 받고, 자신의 ID(예. MAC 주소)를 공개키로 사용하므로 인증서의 사용을 없앴다. 따라서 인증서 발급, 전송 등과 관련한 통신이 필요 없다.

또한 PKG로부터 개인키 획득 단계에서 이전 연구와 통신 비용을 비교해 보면, 이전 연구에서는 임의의 n개 노드들이 PKG을 구성한다. 따라서 개인키 요청을 위해서는 k개 이상의 분산된 PKG의 위치를 라우팅 프로토콜을 이용해서 찾는 과정이 필수적으로 필요하다. 또한 분산된 PKG가 참여 노드와 거리상 가깝게 배치되어 있는 것을 보장할 수 없으므로 멀티 홉 라우팅을 수행함으로써 추가적인 통신 비용을 요구한다. 하지만 제안한 방법은 PKG를 임의의 n개의 노드로 구성하는 것이 아니라, 전체 네트워크를 클러스터링을

통해 2단계 계층으로 나누고 각 클러스터 CH는 바로 인접한 CH들과 비밀을 공유해서 PKG를 형성한다. 따라서 개인키를 요청하는 노드는 분산된 PKG를 찾아야 하는 과정이 필요 없고 자기가 속한 클러스터 내의 CH로부터 분산된 PKG의 위치 정보를 직접 획득함으로써 효율적인 개인키 획득이 가능하다.

성능에서 중요한 부분을 차지하는 또 다른 요소 중 하나는 클러스터링이다. 평면적인 네트워크 구조를 계층적인 구조로 형성하기 위한 클러스터링은 초기 형성 및 재형성, 관리 및 유지에 추가적인 네트워크 통신이 분명히 존재한다. 기존의 평면적 구조에서도 이와 마찬가지로 노드의 이동으로 인한 라우팅 경로 재탐색은 필수적이다. 반면에 클러스터링을 이용한 라우팅은 노드들을 그룹으로 관리함으로써, 키 분배 이외에도 메시지를 실제로 전송할 때 효과적인 라우팅을 가능하게 한다. 즉, 라우팅 경로 탐색 시에 CH의 관리를 통해서 메시지 플러딩을 방지하고 네트워크 오버헤드를 최소화하며 속도를 향상시킬 수 있는 장점이 존재한다. 따라서 평면적인 구조에서 동작하는 기존의 PKI와 비교했을 때, 클러스터 기반 시스템이 네트워크의 크기가 증가할수록 전체 네트워크의 오버헤드 측면에서 효율적이다.

5. 결 론

본 논문은 MANET에서 효율적인 PKG 분산을 통한 ID 기반 공개키 시스템을 제안하였다. 제안한 시스템은 클러스터링 기법을 이용하여 PKG를 효율적으로 분산시켰고, ID 기반의 공개키 관리 기법을 이용하여 인증서의 사용을 제거함으로써 인증서 생성, 전송 등, 관리에 필요한 통신을 제거하였다. 기존에 제안되었던 임의의 노드가 PKG를 구성하는 방식과는 다르게 클러스터의 CH가 PKG를 구성하기 때문에 각 노드가 PKG로부터 개인키를 획득할 때의 소비되는 통신 비용이 감소한다.

향후 연구 방향으로, 실제 클러스터링 알고리즘을 적용한 네트워크 시뮬레이션을 통해서 제안된 시스템의 구체적인 성능 비교와 분석이 요구된다.

참고문헌

[1] J. Hubaux, L. Buttyan, S. Capkun, “The quest for security in mobile ad hoc networks”, Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking computing, 2001.

[2] H. Deng, A. Mukherjee, and D. Agrawal, “Threshold and Identity-Based key Management and Authentication for Wireless Ad Hoc Networks,” Proc. Int’l Conf. Information Technology: Coding and Computing (ITCC ’04), Apr. 2004.

[3] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network Mag., vol. 13, no.6, pp. 24–30, Nov./Dec. 1999

[4] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, “AC-PKI: Anonymous and Certificateless Public-key Infrastructure for Mobile Ad Hoc Networks,” Proc. IEEE Int’l Conf. Comm, pp. 3515-3519, May 2005.

[5] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil pairing,” In C. Boyd, editor, Advances in Cryptology, ASIACRYPT 2001, volum2248 of Lecture Notes in Computer Science, pages 512-532. Springer Verlag, 2001.

[6] J. Staddon et al., “Self-Healing Key Distribution with Revocation,” Proc. IEEE Symp. Security and Privacy, 2002.

[7] M. Puzar et al., “SKiMPy: A Simple Key Management Protocol for MANETs in Emergency and Rescue Operations,” Proc. ESAS’05, 2005.

[8] D. Joshi, K. Namuduri, and R. Pendse, “Secure, Redundant, and Fully Distributed Key Management Scheme for Mobile Ad Hoc Networks: An Analysis,” EURASIP J. Wireless Commun. and Net., vol. 5, no. 4, pp. 579-89, Sept. 2005.

[9] Torben Pryds Pedersen, "A Threshold Cryptosystem without a Trusted Party,” In Advances in Crytology-Eurocrypt '91, pages 522-526, 1991.

[10] M. Jiang, J. Li, and Y. C. Tay, “Cluster Based Routing Protocol,” Internet Draft, 1999.

[11] W. Diffie, and M. E. Hellman, “New Directions in Cryptography,” IEEE Trans. Info. Theory, vol. IT-22, no. 6, pp. 644-54, Nov. 1976.