MANET 환경에서 클러스터링을 이용한 ID 기반 공개키 관리 분산

최홍준° 홍성제 김종
포항공과대학교 컴퓨터공학과
{formetel, sjhong, jkim}@postech.ac.kr

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

Hong Jun Choi° Sung Je Hong Jong Kim
Department of Computer Science and Engineering
Pohang University of Science and Technology (POSTECH)

1. 서 론

MANET(Mobile Ad Hoc Network)은 고정된 인프라가 없고, 노드가 움직이기 때문에 네트워크 위상이 동적으로 변하는 특성을 가지고 있다. 기존의 공개키 시스템에서는 각 노드가 공개키와 개인키를 사용하고, TTP(Trusted Third Party)가 그것들을 인증해주는 수단을 제공하지만, MANET에서는 고정된 TTP를 가정할 수 없다. MANET을 위한 공개키 관리 기법들은 이 문제를 해결하기 위해서 Threshold 암호기법(Threshold cryptography)을 사용하여 특정 수 이상의 노드가 TTP의 역할을 분산해서 수행한다. 기존 제안된 방법들은 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.

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

2. 클러스터링을 이용한 ID 기반 공개키 관리 시스템

MANET에서는 효율적인 라우팅을 위해 전체 네트워크를 여러 개의 클러스터로 구분하는 방법을 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 수있다. 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. CH는 논리적으로 CH들만의 overlay network을 구성해서 inter/intra 클러스터 라우팅을 효과적으로 수행할 수 있다.

클러스터가 형성이 되면, CH는 저장하고 있는 이웃 CH의 라우팅 정보를 이용해서 직접적으로 인접한 n개이상의 CH와 통신한다. 이후 Threshold 암호기법을 이용해서 각 노드의 비밀키 생성에 필요한 마스터 비밀키를 공유한다. 1) 노드 N_i는 임의의 비밀값 p_i을 생성하고 Z_q상에서 $f_i(0)=p_i$가 되는 k-1차 다항식 $f_i(x)$를선택한다. 2) 노드 N_i는노드 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 $\sum_{i=1}^{k} s_i l_i(z)$

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

PKG가 형성되면, 이후에 접속하는 모든 노드들은 자신의 개인키를 획득하기 위해서 PKG에게 PKG 서비스 요청 메시지를 전송해야 한다. 요청하는 노드는 자신의 ID를 공개키로 사용해서 k개의 PKG에게 비밀키를 요청한다. k개의 PKG는 각각 자신의 부분 마스터 비밀키를 이용해서 요청 노드의 부분 비밀키를 안전하게 전송한다. 요청 노드는 부분 비밀키를 전송 받은 후 개인키를 계산하여 생성할 수 있다. $sk = \sum_{i=1}^{n} s_iQ_{ID}$.

제안된 시스템에서는 기존에 제시된 기법에 비해 키 관리에 필요한 통신 오버헤드가 감소한다. 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.

3. 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.