안전한 연산을 지원하는 Ad-hoc 네트워크 구현에 관한 연구

유세정 김효곤
고려대학교 컴퓨터정보통신대학원 정보통신공학과
e-mail : sjkeera@hotmail.com

Implementation of Ad-hoc Network Supporting Secure Computation

Se-Jung Yoo Hyogon Kim
Dept. of Information & Communication Engineering
Graduate School of Computer & Information Technology, Korea University

요 약

Ad-hoc 네트워크는 자율적으로 네트워크를 구성함으로써 유연하고 확장 가능한 특성을 가진다. 하지만 익명으로 구성되는 네트워크의 특성은 사용자의 안전을 보장하지 못함으로 Ad-hoc 네트워크 활성화에 걸림돌이 되고 있다. 여기서는 소수의 악의적인 공격자가 있는 경우에 높은 확률로 연산 결과를 신뢰할 수 있는 안전한 연산 기법들을 활용하여 Ad-hoc 네트워크에서 이루어지는 연산을 보다 안전하게 수행할 수 있는 방안을 제안한다.

1. 서론

Ad-hoc 네트워크는 이동 노드들 간에 자율적으로 구성되고 고정된 기반 네트워크가 필요 없다는 장점 때문에 많은 관심을 받고 있다. 그러나 활성화가 잘 이루어지지 않는 것은 한정된 배터리로 데이터 전달 기능을 가진 중간 노드의 구현이 어렵기 때문이다. 이와 함께 개인의 데이터가 익명의 장비를 통해 전달된다는 보안상의 문제가 사용자들을 망설이게 하고 있다. 특히 차량으로 구성된 VANET(Vehicular Ad Hoc Networks)의 경우, 주행 중 정보전달 과정의 위·변조 위협인 In-transit Traffic Tampering 등이 차량 통신을 제약하는 보안 취약성으로 분석되고 있다[1]. 여기서는 최근 센서 네트워크에서 사용되고 있는 안전한 집계(Aggregation)연산 기법을 소개하고, 이를 Ad-hoc 네트워크에 적용하는 방안을 제시한다.

2. 본론

데이터 전달 기능은 Ad-hoc 네트워크에서 많이 다루어진 분야이며 주된 연구 대상이다 [2], [3]. 이와 관련하여 현재 IETF MANET(Mobile Ad hoc NETwork)에서 표준화 작업이 진행 중이며, AODV(Ad Hoc On demand Distance Vector)[4], DSR(Dynamic Source Routing)[5]등의 프로토콜이 제안되어 있다. 하지만, 익명의 구성원들로 네트워크가 형성되는 경우, 데이터의 의도적인 변조나 고장에 의한 데이터 왜곡이 일어났는지를 검증할 방안은 연구되지 않았다. 따라서, 이 논문에서 우리는 센서 네트워크에서 사용되고 있는 안전한 집계 연산 기법을 차용하여, 이를 Ad-hoc 네트워크에 적용하는 방안에 초점을 맞추도록 하겠다.

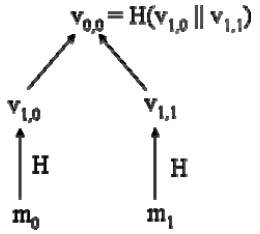
2.1 안전한 집계(aggregation) 연산 기법

안전한 집계연산 기법은 센서 네트워크에서 데이터 수집 시 악의적인 노드에 의해 결과 값이 조작되는 것을 막기 위해 제안되었다. Hu 와 Evans 는 한 노드가 조작되었을 경우에 대해서 연구하였으며[6], Wagner 는 악의적인 공격에 좀 더 견딜 수 있는 방안을 제시하였다[7]. Przydatek, Song, Perrig 은 aggregate-commit-prove 라는 아래의 3 단계 절차를 통해 노드의 조작을 방지하는 기법을 제안하였다[8].

1. aggregate 단계
   하나의 대표 노드에서 각 노드의 데이터를 수

집하여 결과값(총합, 최소값, 최대값등)을 계산한다.

2. commit 단계
대표 노드는 수집한 데이터의 결과값을 신뢰할 수 있는 노드에 제출한다. Merkle hash-tree 를 이용하여 수집된 데이터를 트리 의 leaf 에 위치시키고 바이너리 해쉬 트리를 구성하여 루트의 해쉬 값도 제출한다. Merkle hash-tree 는 두 자식 노드의 데이터를 concatenation 한 후 해쉬 함으로써 그림 1 과 같이 얻을 수 있으며 루트의 해쉬 값을 commitment 라고 부른다.



(그림 1) Merkle hash tree

3. prove 단계
신뢰할 수 있는 노드는 제출받은 데이터와 commitment 를 통해 제출된 결과의 신뢰성 여부를 검증한다.

aggregate-commit-prove 기법은 Merkle hash-tree 를 이용하여 대표 노드가 제출한 결과값에 서명한 효과를 얻을 수 있으며 잘못된 결과값 제출시 prove 단계에서 이를 검증 할 수 있다. 여기서는 신뢰할 수 있는 노드가 대표 노드를 거치지 않고 각 노드와 연결할 수 있는 경로가 있다고 가정하는데, Ad-hoc 네트워크는 여러 경로가 다양하게 생길 수 있는 환경이므로 이러한 가정은 타당하다고 생각된다. 이러한 경로를 통해 대표 노드는 각 노드를 샘플링 하고 노드의 데이터 값을 전송 받는다. 전송받은 데이터 값과 그 노드의 Merkle hash tree 경로를 찾아 해쉬 값을 제출받은 commitment 와 비교함으로써 대표노드의 조작 여부를 판별할 수 있다. 모든 노드들을 다 검증하면 조작 여부를 완벽하게 판별할 수 있겠지만, 대표 노드와 각 노드들을 연결하는 경로가 모두 있다고 보기 어렵고 또한 제한된 환경을 갖는 Ad-hoc 네트워크에서 트래픽 부하를 고려한다면 검증은 샘플링 기법을 통해 이루어지는 것이 바람직하다고 생각된다.

2.2 안전한 연산의 Ad-hoc 네트워크 적용 방안

AODV, DSR 프로토콜의 경우 On-Demand 방식으로 트래픽이 발생하는 시점에 경로를 탐색하게 되는데 악의적인 노드를 게이트웨이로 거치게 되는 경우 전체 트래픽이 노출되는 보안상의 문제점을 가지게 된다. 따라서 공격자는 자신의 노드를 게이트웨이 노드로 믿게 하기 위해 게이트웨이 선택 방식을 자신에게 유리하게 하는 방향으로 데이터 조작을 시도할 수 있다. 그러므로 Ad-hoc 네트워크에서 게이트웨이가 되는 노드는 신뢰성 있게 선택되어야 한다[9].

AODV, DSR 프로토콜을 확장하여 라우팅을 형성할 때 Merkle hash tree 를 같이 구성해 두면, 자신이 속한 서브 네트워크의 라우터를 신뢰할 필요가 있을 경우 (결재 정보를 전송하는 경우) 이를 이용할 수 있다. 먼저, 각 노드는 신뢰성 테스트를 위한 임의의 데이터를 생성하여 전송하고 게이트웨이 노드는 이러한 데이터를 수집하고 Merkle hash tree 를 이용하여 신뢰할 수 있는 제 3 의 노드(공인인증서 관리 서버 등)로 전송한다. 신뢰할 수 있는 제 3 의 노드는 임의의 시간에 연결 가능한 노드를 샘플링하여 선택한 후 게이트웨이 노드로 전송했던 데이터를 받는다. 이것을 게이트웨이 노드가 전송했던 commitment 와 비교하여 게이트웨이 노드의 신뢰성을 판별하며 조작된 정보를 보낸 것으로 확인될 경우 블랙 리스트에 올려 브로드캐스팅한다.

AODV 나 DSR 에 이러한 방식을 선택적으로 사용할 수 있게 구현한다면 큰 성능 저하 없이 악의적인 게이트웨이를 탐지할 수 있을 것이다. 여기서는 보안상 가장 문제가 될 수 있는 게이트웨이 선택 과정상의 데이터 위 · 변조 탐지만 언급하였다. 하지만 이 방식은 일반적인 데이터의 전송 왜곡 여부 판별에 동일하게 사용될 수 있다. 예를 들어, 앞에서 언급한 VANET 에서도 데이터를 수집하여 전송하는 과정에서의 위 · 변조를 탐지하는데 유용하게 적용될 수 있다.

3. 결론

Ad-hoc 네트워크는 자율성과 유연성을 특징으로 가지는 네트워크로 고정된 인프라를 사용하지 않는다는 측면에서 강점을 가진다. 하지만 신뢰성이 확보되지 않은 노드들로 구성된다는 점에서 보안상의 문제점도 많은 것이 사실이다. 다른 많은 보안상의 취약점이 있지만 여기서는 그 중에서도 가장 큰 문제가 될 수 있는 게이트웨이 노드의 신뢰성을 확보하기 위한 방안을 제시하였다. 임의의 순간에 게이트웨이 노드에 대한 신뢰성을 검증함으로써 다른 노드가 게이트웨이 노드로 선택되지 못하게 하는 것을 방지할 수 있으며, 샘플링 기법을 이용하여 네트워크 부하를 줄이고자 하였다. 앞으로는 다른 악의적인 노드가 게이트웨이 노드로 되기 위해 데이터를 조작하는 경우에 대한 연구가 필요할 것으로 판단되며 이를 통해 보다 안전한 Ad-hoc 네트워크를 구성할 수 있을 것으로 생각된다.

참고문헌

[1] 최병철, 한승완, 정병호, 김정녀, “지능형 차량 보안 기술 동향”, 전자통신동향분석 제 22 권 제 1 호, 2007, pp.114 - 118

[2] Charles E. Perkins, “Ad Hoc Networking, Addison-Wesley”, 2001.

[3] C.K. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems, Prentice Hall PTR”, 2002.

[4] C. Perkins, E. Belding-Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, RFC 3562,

July 2003.
[5] D. Johnson, Y. Hu, D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4”, Feb 2007.
[6] Lingxuan Hu and David Evans, “Secure aggregation for wireless networks”, Workshop on Security and Assurance in Ad hoc Networs, 2003.
[7] David Wagner, “Resilient aggregation in sensor networks”, Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004.
[8] B. Przydatek, D. Song, A. Perrig, “SIA: Secure Information Aggregation in Sensor Networks”, Proceedings of ACM SenSys 2003.
[9] Seunghun Jin et al, “Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network”, ETRI Journal, Volume 27, Number 4, Aug, 2005.