클러스터 기반의 이동 Ad Hoc 네트워크에서 DAA 기술을 통한 신뢰할 수 있는 인증 모델 설계

이기열°, 양석환, 최수길+, 정목동
부경대학교, 한국전자통신연구원+
zestgame@hanmail.net tigergal@chol.com sooguri@etri.re.kr mdchung@pknu.ac.kr

Design of a Secure Authentication Model using DAA Technology in the Clustered Mobile Ad Hoc Network

Kiyeal Lee°, Seokhwan Yang, SuGil Choi+ and Mokdong Chung
Pukyong National University, Electronics and telecommunications Research Institute+

이동 Ad Hoc 네트워크(Mobile Ad Hoc Network, MANET)는 1970년 초에 제안된 Mobile Packet Radio에서 발전한 무선 네트워크 연구 분야로, 기존의 네트워크 인프라(유선 기반 망 혹은 액세스 포인트)가 없어도 노드들 간에 통신을 가능하게 해주는 네트워크 기술이다. MANET은 기존의 인프라 없이 무선 네트워크 통신 기술을 이용할 수 있으나 자원에 대한 제약, 동적인 변화, 중앙 시스템의 결여와 같은 문제점으로 인해 기존의 유선 네트워크보다 보안에 대한 문제점이 더욱 큰 시스템이다. 하지만 현재까지 제안된 보안 기술들은 이러한 보안 요구사항을 만족하지 못하면서 노드가 가지는 자원한계에 대한 한 관리를 체계적으로 지원하지 못하고 있는 실정이다. 특히 인증 시스템들은 MANET 기반에서 제 3의 신뢰 기관을 요구하거나, 단순한 ID를 통한 인증 기술을 제시하는 등 안전하고 효율적이지 못하다는 단점을 지니고 있다.

본 논문에서는 이러한 문제점을 해결 할 수 있는 DAA 기반의 인증 시스템을 제안한다. DAA를 제안한 TCG는 이종 컴퓨터 플랫폼에서 컴퓨팅환경의 보안을 강화시키려는 목적으로 설립된 비영리 산업표준화 기관이다. TCG에서 제안한 TPM은 하드웨어의 보안을 강화시키기 위한 많은 기능과 구조를 제공하고 있다. 또한 TPM과의 상호작용을 위한 TSS (TCG Software Spec)라는 인터페이스를 제공하여 TPM과의 데이터 교환을 지원하고 있다.

TCG는 TPM의 인증 기술로 자신의 프라이버시를 보호하면서 자신의 타당성과 신뢰성을 인증 할 수 있는 DAA 기술을 채택하였다. DAA는 플랫폼 사용자에 대한 프라이버시를 보호하고 동시에 TPM 하드웨어의 원격 인증을 제공하는 서명 기법으로 Fiat-Shamir가 제안한 그룹서명을 기반으로 하고 있다. 하지만 사용자의 프라이버시를 제공하기 위해서 그룹서명의 open 기능을 삭제하였다.

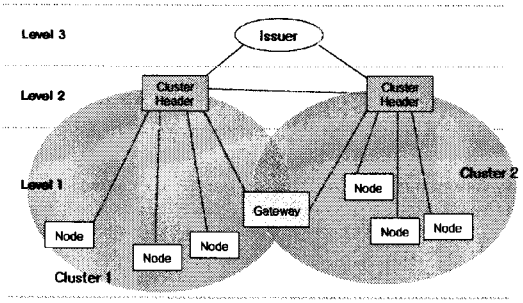

그림 1 CBRP 프로토콜을 이용한 인증 모델 구성

본 논문에서는 DAA 인증 과정을 클러스터화 된 MANET 기반에 적용하여 PKI, ID, Threshold cryptography등을 적용한 인증 기술보다 효율적인 기능을 제공하는 인증 기술을 제안하였다. 제안된 인증 기술의 구성은 그림 1과 같이 이루어 진다.

클러스터 헤더 산출 알고리즘을 통해서 노드에서 클러스터 헤더를 결정하고, 결정된 클러스터 헤더중 하나의 Issuer를 선출함으로써 위와 같은 그림의 구성을 가지게 된다. 따라서 인증 모델은 level 1의 노드와 게이트웨이, level 2의 클러스터 헤더, level 3의 Issuer로 구성되게 되는데 각 구성요소의 역할은 다음과 같다.

① 노드 : 클러스터 헤더에게 자신이 MANET 구성원임을 등록하고 Issuer에게 인증서를 받은 후 인증을 통해서 다른 노드와의 통신을 수행 한다.
② 게이트웨이 : 다른 클러스터에 존재하는 노드와 통신을 위한 통로 역할을 한다.
③ 클러스터 헤더 : 자신에 속한 각 노드들의 공개키 목록을 Issuer로부터 받아오고, Issuer가 발행한 인증서를 검증하는 역할을 한다. 또한 다른 클러스터 헤더들의 리스트도 가지고 있다. 클러스터 헤더 선출은 클러스터 내에서 접근이 가장 적은 클러스터로 선출한다.
④ Issuer : 노드가 MANET 구성원으로 등록하기 위해 필요한 인증서 발급에 대한 기능을 수행한다.

각 노드들은 DAA의 인증 과정인 Setup, Join, Sign, Verification 과정을 이용하여 클러스터화 된 내부의 구성안에서 인증을 효율적으로 처리할 수 있다. 본 논문에서 제안된 인증 모델은 Strong RSA와 Decisional Diffie Hellman 가정을 기반으로 하기에 ID 기반의 인증 기술보다 강력하다. 또한 영지식 증명을 통해서 인증서를 생성하기에 별도의 CA가 필요치 않으며 Join 프로토콜 이후 노드 자체에서 인증서 생성이 가능하고 클러스터 헤더를 통해서 검증이 가능하므로 Threshold cryptography 기법에서 인증서 생성 및 검증 시 요구되는 많은 노드들의 참여가 필요하지 않아 제한된 리소스기반에서의 효율적인 인증 방법이라 할 수 있다.

하지만 제안된 인증 모델 역시 높은 수준의 계산량을 요구하여 노드의 수명에 영향을 미칠 수 있으므로 계산량을 줄이기 위한 알고리즘 최적화가 지속적으로 연구되어져야 할 것이다

참고 문헌

[1] A. Shamir, "How to Share a Secret," Massachusetts Institute of Technology, Communication of the ACM, 22(11), pp. 612-613, 1979.
[2] A. Ephremides, J. Wieselthier and D. Baker, "A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling," Proc. IEEE 75(1), pp. 56-73, 1987.
[3] E. Brickell, J. Camenisch, and L. Chen: "Direct anonymous attestation," In Proceedings of 11th ACM Conference on Computer and Communications Security, ACM Press, 2004 Practical Solutions to Identification and Signature Problems, ACPC 86, LNCS, 1987
[4] Fiat and Shamir, "How to prove yourself : Practical solutions to identification and signature problems", CRYPTO 86, 1987
[5] He ge, "A Method to Implement Direct Anonymous Attestation," citeseer.ist.psu.edu/ge06method.html, 2006
[6] Smyth, B., Ryan, M. & Chen, L. "Direct Anonymous Attestation (DAA): Ensuring privacy with corrupt administrators," In proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks. Lecture Notes in Computer Science (LNCS), volume 4572, pp. 218-231, Springer-Verlag 2007
[7] TCG, TCG Specification Architecture Overview Specification Revision 1.3, 2007
[8] The Mobile ad-hoc network(MANET) working group, http://www.ietf.org/html.charters/manet-charter.html
[9] Y. Desmedt and Y. Frankel. "Threshold cryptosystems," In CRYPTO'89, volume 435 of LNCS, pages 307-315. Springer-Verlag, 1990.
[10] 봉진숙, 윤미연, 신용태, "Ad-hoc 네트워크에서 공개키 기반 구조를 이용한 신뢰적 인증 메커니즘," 한국 정보 과학회 가을 학술 발표 논문집, 제 31권 제 2호, pp. 437-439, 2004
[11] 박배효, 이재일, 한진백, 양대헌, "이동 Ad Hoc 네트워킹에서 Threshold Cryptography를 적용한 클러스터 기반의 인증서 생성 및 관리 모델 연구", 한국SI학회지, 3권 2호, p.119-127, 2004
[12] 이혜원, 문영성, "CGSR 기반의 이동 애드 혹 네트워크에서 신뢰성 있는 통신을 위한 노드 간 인증 기법", 정보과학회 논문지, 제 32권 제 1 호, p.659-667, 2005