제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

ad-hoc 네트워크에서 상호 인증을 위한 메커니즘

김정범 박남섭 김태윤
고 려 대 학 교 컴 퓨 터 학 과
{qston, nspark, tykim}@netlab.korea.ac.kr

A Study of Ad-Hoc network Security for Group Management support of Multicast

Jeong-Beom kim, Yun-Jeong Lee, Tai-Yun Kim
Dept. of Computer Science and Engineering, Korea University

요 약

Ad-Hoc 네트워크는 모바일 호스트를 위한 새로운 무선 네트워크 패러다임이다. 전형적인 모바일 네트워크와는 다르게 ad-Hoc 네트워크는 어떠한 인프라스트럭처에 의존하지 않는다. 대신에 호스트들은 연결 유지를 위해 서로간에 의존한다. 이러한 특성을 지닌 ad-Hoc 네트워크의 보안은 주요 이슈라고 할 수 있다. Ad-Hoc 네트워크에서는 네트워크 Topology가 자주 변하기 때문에 이러한 특성에 맞는 확장성 있는 분산 그룹 키 분배를 제안한다.

1. 서론

대부분의 네트워크 시스템은 고정된 기지국과 같은 유선 기반 망(infrastructure)을 요구해왔다. 그러나, 유선 기반 망을 설치하기 어려운 산간 지방 또는 빙하지역 같은 오지나 지진, 홍수, 전쟁 등의 재난으로 유선기반 망이 파괴된 지역에서의 신속한 통신 복구를 위해서는 유선 기반 망이 필요 없는 네트워크의 구성을 요구하게 되었다. 또한 한 빌딩 내에서 유선 기간 망의 필요 없이 자체 통신망을 구성할 필요성이 대두되었다. 최근 이러한 연구가 MANET(Mobile Ad-Hoc Network)에서 연구 개발되고 있다[1].

이러한 Ad-Hoc망은 중앙 집중화 된 관리나 표준화된 지원 서비스의 도움 없이 임시 망을 구성하는 무선 이동 호스트들의 집합이다. 이러한 망은 백본 호스트나 다른 이동 호스트로의 연결을 제공하기 위한 고정된 제어 장치를 갖지 않으며, 각 이동 호스트가 라우터로 동작하여 이동 호스트로부터의 패킷을 다른 이동 호스트로 전달한다. 이동 ad hoc 망은 쉬운 개발 방법, 재구성, 그리고 적응성 등의 장점을 가지고 실용적인 application분야(Private networking, Home networking, 군사환경, search-and-rescue 이용등)에 사용된다

본 논문의 목적은 Ad-Hoc 네트워크에서 안전하고 효율적인 메커니즘을 제안하는 것이다. 이를 위해서는 Ad-Hoc에서 부인방지 서비스가 제공되어야 하며 부인 방지 서비스는 공개키를 기반으로 한 전자서명을 할 때 가능하다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 EKE(Encrypted Key Exchange)와 Ad hoc 네트워크에 대해 살펴보고 3장에서는 제안한 보안 메커니즘을 설명한다. 4장에서는 결론 및 향후 연구 과제에 대해 기술한다.

2. 관련연구

2.1 EKE(Encrypted Key Exchange)

ad-hoc 네트워크에서는 PKI 기반의 인증 방식을 도입하는데는 무리가 있다. 지역에 기반을 둔 인증 방식이나 패스워드 방식의 키 교환이 네트워크 성격에 맞는 방식이라 할 수 있다.

키 교환 프로토콜에서 상호 인증은 필수적이며, 사용자에게 편리하고 비용이 적게 드는 패스워드 기반의 인증 방식을 사용한다. 이러한 방식으로 널리 사용되는 방법이 EKE 키 교환 방법이다.

EKE는 Bellovin과 Merrit에 의해 제안되었으며 그 내용은 Alice 와 Bob (두 명의 사용자, 또는 사용자와 서버, 어느 쪽이든 간에) common passw-ord 인 P를 공유한다. 이 프로토콜을 사용해서, 쌍방은 서로에 대한 인증을 하고 common session key 인 K를 생성한다.

그림 1은 그 동작 과정을 보여준다.

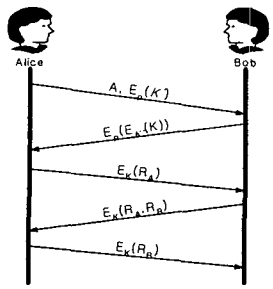

그림1 EKE 동작과정

그림 1을 살펴보면 다음과 같다.

1) Alice는 random public-key/private-key 쌍을 생성한다. *P*를 키로 하 는 대칭키 알고리즘을 통해 public-key인 *K'*를 암호화하고 Bob에게 보낸다.

2) Bob은 *P*를 알고 있다. *K'*를 얻기 위해 메시지를 복호화한다. 그러면, 그는 random session key인 *K*를 생성하고 그것을 *P*를 키로 사용하여 Alice에게 받은 공개키를 암호화한다. 다음을 Alice 에게 보낸다.

3) Alice는 *K*를 얻기 위해서 메시지를 복호화한다. Random string R_A를 생성하고 *K*를 이용해 암호화 한 후에 Bob 에게 다음을 보낸다.

4) Bob은 R_A를 얻기 위해 메시지를 복호화한다. 또 다른 random string R_B를 생성하고 *K*를 이용해서 암호화 한 후에 Alice 에게 결과를 보낸다.

5) Alice는 R_A와 R_B 를 얻기 위해 메시지를 복호화한다. Bob에게 받은 R_A가 Bob에게 단계(3)에서 보낸 것과 같다고 가정하고, R_B를 *K*를 이용해 암호화한 후에 Bob 에게 보낸다.

6) Bob은 메시지를 복호화한다. 단계(4)에서 Alice에게 보낸 것과 같은지를 확인하고 키가 올바르게 교환되었다는 것을 확인한다. 양쪽은 *K*를 session key로 이용하여 통신을 한다.

2.2 Ad-hoc Network

흔히 무선 ad hoc 네트워크라 하면 무선 인터페이스를 사용해 패킷 데이터를 전송하는 무선 노드로 구성된, 중앙 관리(central administration) 없이 형성된 네트워크를 뜻한다. 이같은 유형의 네트워크에 있는 노드는 라우터나 호스트로 이용될 수 있기 때문에 다른 노드 대신 패킷을 전송할 수도 있고, 사용자 애플리케이션들을 실행할 수도 있다. Ad hoc 네트워킹의 가장 매력적인 점은, 중앙통제로부터 완전히 독립해 사용자가 네트워크 사용에 더많은 자유와 유연성을 얻게 된다는 것이다.

Ad hoc 네트워킹을 이용하면 사용자의 통신기기간 연동이 가능하며, 비행기 출발시간, 게이트 변경 등의 업데이트 정보를 조회하는 등의 현지 정보 포인트에 연결할 수 있다. 또한 통신범위를 벗어난 통신기기 간에 트래픽을 중계해준다. 현재는 통신 커버리지를 기지국이 제공하고 있고, 중앙에서 무선 자원을 관리하며, 서비스가 시스템에 통합돼 있다. 이로써, 오늘날 무선 시스템은 양질의, 예측 가능한 서비스를 제공하는 것이다.

그림 1은 Infrastructure-less인 Ad-Hoc에 대한 그림이다.

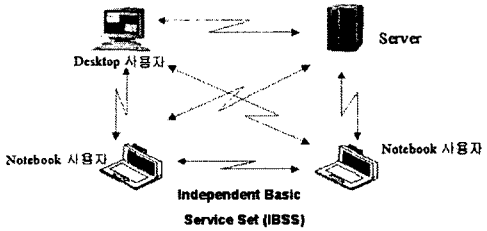

그림 2 Ad-hoc architecture

그림을 보면 Ad Hoc 네트워크는 무선 단말기간 피어 투 피어 통신을 가능하도록 한다. 단말기간 직접 통신할 수 있는 범위가 Ad hoc 네트워크 지역으로 되어 있다. 이 범위는 BSA(Basic Service Area)라고 하며, 단말기끼리 직접 통신한다. 이 방식을 사용할 경우 AP는 필요 없으며 최대 4대 까지 단말기가 동시에 접속하여 통신할 수 있다.

그림 2는Infrastructure인 WLAN의 구조를 보여준다.

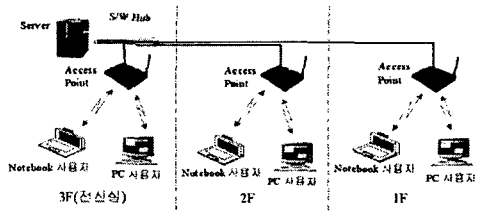

그림 3 WLAN architecture

Infrastructure 네트워크는 액세스 포인트를 중심으로 단말 시스템간 통신 네트워크가 구성되는 방식으로 모든 단말 시스템 사이의 통신은 액세스 포인트를 거쳐서 이루어지게 된다. 또한, 단말 시스템은 액세스 포인트를 통해서 유선 네트워크와 통신할 수 있다. 이러한 WLAN에서는 인증 서버인 RADIUS를 설치하여 접속하려는 노드들과의 인증을 수행할 수

있으며 이러한 연구가 현재 활발히 진행 중에 있다.

하지만 ad-hoc 네트워크인 경우 현재 라우팅 개발은 많은 발전을 가져왔지만 이 라우팅에 따른 네트워크 trust 개발은 아직 제안된 것이 없다.

trust를 위한 인증 메커니즘을 제안하기 위해서 먼저 고려해야 할 사항은 ad-hoc 네트워크는 AP와 같은 정적인 접속 포인트가 없다는 점이다. 또한 ad-hoc에서는 모든 노드들이 라우터가 될 수 있으며, CA와 같은 기관이 존재하지 않기 때문에 네트워크가 trust한 부분이 부족하다. 따라서 이러한 문제점을 해결하기 위해서 각 노드들의 상호 인증 시스템이 필요하다.

3. 제안한 메커니즘

본 논문에서는 Ad-hoc 네트워크를 trust 네트워크로 만들 수 있는 상호 인증할 수 있는 메커니즘을 제안한다.

먼저 그림 3과 같은 시나리오를 가정한다.

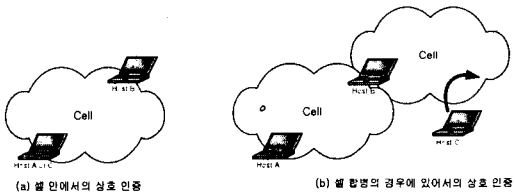

그림 4 시나리오

3a)와 같은 경우 ad hoc 호스트는 패스워드 기반의 EKE를 사용하여 상호 인증 할 수 있다. 하지만 3b)와 같은 경우 기존의 논문에서 제안된 방식들은 계층적인 구조로 설계를 하여 상하 수직적인 관계에서는 보안과 인증이 체계적으로 설계할 수 있으나 Cross 보안은 형성되지 못했다. 본 논문에서는 이러한 점을 해결하고자 ad-hoc 호스트들을 계층이 아닌 병렬 클러스트로 가정하여 Cross 보안을 해결한다. 만약 Ad-Hoc 호스트 A가 B를 거쳐서 C와 통신을 하려는 경우 공개키 기반 인증 메커니즘을 사용한다면 계산량이 많아진다. 반면에 최소 공개키 기반 인증 메커니즘을 사용할 경우 호스트 C와 A사이에 부인 방지 서비스가 제공되지 않는다. 따라서 본 논문에서는 이 둘을 적절히 응용하여 Ad-hoc에 맞는 인증 메커니즘을 제안한다.

그림 4를 보면 호스트 A, B, C에서 제안한 메커니즘의 흐름을 볼 수 있다.

그림을 살펴보면, Host C가 Host B와 EKE를 통해 키 교환 과정을 거친다. Host A에게 Host B에 대한 메시지를 전달하고 Host A가 인증한 내용을 결과를 통해 간접적으로 인증한다. 호스트 C는 호스트 A에게 전자서명을 보내고 Host A는 전자서명을 인증한다. 이로써 호스트 A는 호스트 C와 호스트 B 모두를 인증할 수 있다. 여기서 호스트 C의 전자서명은 자신이 등록한 위치 정보에 대한 중요한 부인 방지 기능을 제공하여 네트워크 관리 사용을 관리 제어할 수 있다. 호스트 A의 경우에는 호스트 B에게 전자서명을 보내어 인증 받고 호스트 C에게는 MAC를 생성시킴으로써 직접 인증 받는다. 이로써 모든 참여자에 관해 인증을 할 수 있다.

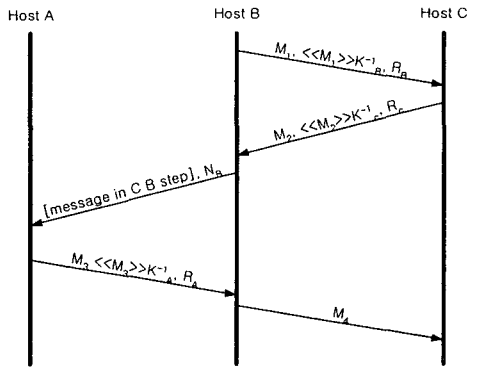

그림 5 메커니즘의 흐름

나머지 부분은 최소 공개키 기반 메커니즘과 비슷하고 다른 부분은 아래와 같다.

◎ Broadcasting
host B -> host C: M_1, $<<M_1>>K^{-1}_B$, R_B
◎ Authentication
host C -> host B: M_2, $<<M_2>>K^{-1}_C$, R_C
M_2 =*Request*, *host* C_{id}, *host* A_{id}, N_A, N_C
host A : validate using R_A
verify $<M_2>>K^{-1}_C$ *using* K_C
Validate $<<M_1>>K^{-1}_B$ *using authenticated* K_B

이렇게 함으로써 얻는 이점은 host A가 보내는 등록 대답은 비밀키를 사용한 MAC을 사용하여 성능 저하를 줄일 수 있는 점과 한번의 공개키 과정을 거쳐서 전자서명을 생성한다는 점이다. 이렇게 함으로써 총 계산량을 줄일 수 있다.

4. 결론 및 향후 연구과제

본 논문에서는 모바일 IP에서 사용하는 인증 메커니즘을 Ad-hoc 네트워크에 맞게 수정, 설계하여 전자서명을 첨가한 최소 공개키 기반 인증 메커니즘을 제안했다. 제안한 메커니즘은 적은 계산 비용으로 ad-hoc 네트워크의 호스트들에게 적합하고 전체 인증 시간이 짧다는 면에서 효율적이다. 하지만 비밀키를 사용함으로써 많은 사용자가 있는 경우 키 관리의 어려움이 있다는 단점이 있다. 또한 공개키 알고리즘에 기반을 두기 때문에 infrastructure-less인 Ad-Hoc에서는 구현이 힘들다. 향후 연구과제로는 이러한 점을 해결할 수 있는 공개키 기반 방식이 아닌 위치 기반 방식의 인증 메커니즘을 연구해야하며,

많은 사용자가 있을 경우 키 관리의 문제점의 해결 책을 연구해야 할 것이다.

5. 참고문헌

[1] Asokan, N. & Ginzboorg, Philip, Key Agr-ee ment in Ad-Hoc Networks, Elsevier Pre-prin t, 2000.

[2] Steven M. Bellovin and Micheal Merrit. En crypted Key Exchange: Password-based pro tocols secure against dictionary attacks. In Proceedings of the IEEE Symposi-um on Resear-ch in Security and Privacy, May 19 92

[3] Frank Stajano and Ross Anderson. The re-su rrecting duckling: Security issues for ad-hoc wireless networks. In Proceedings of t he 7th International Workshop on Se-curity Protocols, Lecture Notes in Comp-uter Scie nce. S-pringer-Verlag, Berlin Gemany, Apr ile 1999. Available form http://www.cl.cam.ac.kr/fms27/duckling/.

[4] Steiner, Micheal & Tsudik, Gene & Waine-r, Micheal, Diffie-Hellman Key Distribu-tion Extended to Group Communication, In 3rd, N ew Dlhi, India, 1996, ACM Press.

[5] Zhou, Lidong & Haas, Zygmunt J., Securi-ng Ad Hoc Networks, IEEE Networks, vol.13, n o.6, November/December 1999. <http://www.ee.cornell.edu/~haas/Public-at ions/network99.ps>

[6] Mobile Ad-Hoc Networks(MANET). http://www. ietf.org/html.characters/manetcharacters.h tml. Work in progress.

[7] J.P. Hubaux, L. Buttyan, and S. Capkun. Th e Quest for security in Mobile Ad Hoc Netw orks. ACM Symposium on mobile Ad Hoc Netwo rking and Computing MobiHOC 2001, 2001.

[8] Colin Boyd, ANish Mathuria, "Key Establ-is hment Protocols for Secure Mobile Com-muni cations: A Selective Survey," Infor-mation Security and Privacy(ACISP98), Vol.1438, pp.344-355, 1998.

[9] Radia Perlman, "An Overview of PKI Trust M odels," IEEE Network, pp38-43, Nov/Dec 199 9.

[10] HyperLAN2 Global Forum. http://www.hyp-er lan2.com/. Work in progress

[11] A. Josang. The Right type of trust for Di stributed systems. New Security parad-igms Workshop 1996, ACM, 1996.