제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

Ad Hoc 망에서 클러스터 기반 라우팅 인증

한효영, 심학섭, 김태윤
고려대학교 컴퓨터학과
e-mail:takeitez@netlab.korea.ac.kr

Authentication for Cluster-Based Routing in Ad Hoc Networks

Hyo-Young Han, Hak-Sub Sim, Tai-Yun Kim
Dept of Computer Science & Engineering, Korea University

요 약

Ad Hoc 망은 고정된 네트워크 기반이 없는 동적인 호스트들로 구성된 네트워크이다. 호스트가 네트워크를 연결하기 위해 이웃 노드에 의존적이다. 그래서 네트워크의 보안 사항에 있어서 전통적인 네트워크에서 사용한 보안기법을 그대로 적용하기 어렵다. 본 논문에서는 Ad Hoc 망에서의 특징에 근거하여 여러 동적인 노드들을 클러스터로 묶어서 클러스터 헤드가 멤버 노드들의 정보를 관리하는 가운데 한 클러스터 멤버가 다른 클러스터에 접속을 할 때 각 클러스터 헤드 사이에 멤버 인증서 교환을 위한 공개키 기반 인증 프로토콜을 제안한다.

1. 서론

Ad Hoc 망은 고정된 네트워크 기반이 없이 동적인 호스트들로 구성된 네트워크이다. 그리고 동적인 호스트 사이에 무선 채널을 통해 서로의 정보를 라우팅 할 수 있다. 그러나 보안 사항에 있어서 전통적인 네트워크에서 사용한 보안기법을 그대로 사용하기 어렵다. 따라서 상호 매체를 신뢰할 수 없는 상황에서 암호 키에 크게 의존하게 된다. 기존 연구 [1]에서는 패스워드 기반의 인증 및 키 합의를 다루고 있으나 패스워드의 재사용, 사용 환경의 제약, 침입자에 의한 데이터 무결성에 문제가 있다. 따라서 본 논문에서는 Ad Hoc 망에서의 특징에 근거하여 클러스터 기반 라우팅 환경에서 한 클러스터 멤버가 다른 클러스터에 접속할 때 각 클러스터 헤드 사이에 인증서 교환을 위한 공개키 기반 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 Ad Hoc 보안성의 필수조건과 기존의 연구 및 CBRP(Cluster Based Routing Protocol)에 대해 설명한다. 3장에서는 Ad hoc 환경에서의 공개키 기반 인증 프로토콜을 설명한다. 4장에서는 제안한 인증 프로토콜에 대한 안전성 분석를 하고, 마지막으로 5장에서 본 연구의 결론 및 향후과제를 제시한다.

2. 안전한 Ad Hoc 환경을 위한 요구 조건

Ad Hoc 환경에서 안전성을 지원하기 위해 요구사항을 살펴보고, 기존의 연구 및 CBRP에 대해 고찰한다.

2.1 보안 요구 사항

(1) 가용성: 서비스 거부 공격에도 서비스는 지속적으로 이뤄져야 한다.
(2) 기밀성: 클러스터 내에서 통신은 암호화를 통해 기밀성을 제공해야 한다.
(3) 무결성: 상호간 통신에서 절대 훼손되지 않은 정보에 대한 보증이 있어야 한다.
(4) 인증: 노드간의 신원을 식별할 수 있어야 한다.
(5) 부인방지: 상호간의 통신이 처리된 후에 사실을 부인하지 못해야 한다.

2.2 기존 연구

2.2.1 패스워드 기반

본 연구는 작은 그룹의 환경에서 모든 노드가 패스워드 P를 공유하여 서로를 인증한다.

① $M_i \rightarrow M_{i+1}$: $g^{S_1S_2...S_i}$, i=1,...,n-2

각 노드는 곱셈군 Z_p^*의 생성자 g와 임의의 비밀값 S를 준비한다. 각 노드는 g^S를 계산하여 다음 노드에게 순차적으로 전달한다. 그래서 M_{n-1}번째 노드는 $\pi=g^{S_1S_2...S_{n-1}}$를 얻어낼 수 있다.

② $M_{n-1} \rightarrow$ ALL : $\pi=g^{S_1S_2...S_{n-1}}$, Broadcast

M_{n-1}번째 노드는 π정보를 모든 노드와 공유를 한다.

③ $M_i \rightarrow M_n$: $P(c_i)$, i=1,...,n-1, $c_i=\pi^{\hat{s}_i/s_i}$

각 노드는 헤드 노드 M_n에게 자신의 S값을 제거하고 비밀요소 $\hat{s}$값을 추가한 값 c_i를 모든 노드가 공유하고 패스워드 P를 이용하여 암호화하여 헤드 노드에게 전달한다.

④ $M_n \rightarrow M_i$: $(ci)^{S_n}$, i=1,...,n-1

헤드 노드는 각 노드에게서 받은 값을 복호화하고 자신의 S값을 계산하여 각 노드들에게 전달한다. 이때 각 노드들은 자신의 S값을 추가하여 세션키 $K=(c_i^{S_n})^{S_n s_i/\hat{s}_i}$를 계산한다.

⑤ $M_i \rightarrow$ ALL : M_i, $K(M_i,H(M_1,M_2,...,M_n))$

해쉬 함수를 이용하여 상호간에 키 정보를 확인 및 인증을 할 수 있다.

위 연구는 적은 연산을 통해 상호간에 인증을 할 수 있으나 다음과 같은 문제점이 있다.

- 모든 노드가 프로토콜을 수행하기 위해 존재해야 한다.
- 특별한 노드를 분리시키기 어렵다.
- 복잡한 환경에서 사용하기 어렵다.

2.2.2 공개키 기반

CBRP에서 새로운 노드가 진입하게 되면 상호 인증이 이루어 진다.

① 클러스터 헤드 CH는 난수 r을 생성하고 자신의 비밀키로 암호화하여 진입노드 A에게 보낸다.

② A는 난수 r을 CH의 공개키로 암호화해서 CH에게 보낸다. $E_{CH'}(r) \rightarrow CH1$

③ CH는 암호화된 난수 r을 자신의 비밀키로 해독하여 자신이 생성한 난수 r과 같은지 확인한다.

위 연구는 다음과 같은 문제점이 있다.

- 헤드와 멤버 사이에 확실한 서명을 하지 않았기 때문에 메시지 리플레이 공격을 받기 쉽기 때문에 데이터 무결성이 취약하다.
- 상호간에 부인방지 기능이 취약하다.

2.3 CBRP(Cluster Based Routing Protocol)

CBRP[2]는 클러스터링을 통하여 클러스터 헤드와 멤버를 갖는 클러스터를 구성한다. 클러스터 헤드는 멤버 호스트와 다른 클러스터 헤드의 라우팅 정보를 가지고 있다. 모든 노드는 주기적인 HELLO 메시지를 통해 이웃 노드와 인접 클러스터에 대한 정보를 broadcast 한다. 이와 같은 구조의 라우팅 프로토콜은 여러 노드를 가진 대규모 네트워크에 적합하다. 그림 1은 클러스터 기반 헤드와 멤버를 갖는 네트워크 환경을 나타낸다.

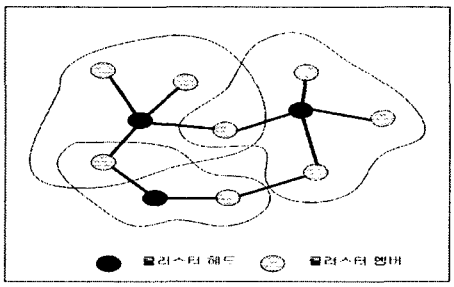

그림 1 CBRP(Cluster Based Routing Protocol)

3. 제안한 인증 프로토콜

본 장에서는 CBRP 환경에서 공개키 기반 인증 구조를 [3]에 제시된 이동통신 환경에서의 인증과정을 연계하여 새로운 인증 프로토콜을 제안한다. 다음 표 1은 프로토콜을 기술하기 위해 사용되는 기호를 나타낸다.

표 1. 제안된 프로토콜 표기법

표기법	설 명
CH_A, CH_B	클러스터 헤드 A, B
CM_A, CM_B	클러스터 멤버 A, B
g	곱셈군의 생성원
TS_A	A가 생성한 타임 스탬프
CertA	A의 공개키 인증서
ID_A, ID_B	A,B의 고유 식별자
$sig_A(msg)$	메시지에 대한 A의 서명값
$\{A\}_B$	B로 암호화된 A값

제안한 프로토콜은 다음과 같은 가정을 가진다.

- 클러스터 헤드는 정적인 상태를 유지하고 인증할 동안 다른 헤드로 바뀌지 않는다.
- 모든 클러스터 헤더들은 서로의 인증서를 가지고 있고, 각 노드들은 키를 저장할 수 있는 충분한 저장매체를 가지고 있다.

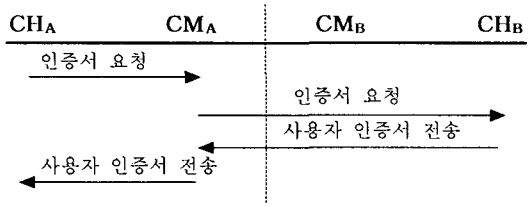

그림 2 제안한 프로토콜 모델

이동 노드 Y는 클러스터 B에서 인증기관 역할을 하는 CH_B에 의해 인증을 받았다. 그러나 Y가 새로운 클러스터 A로 이동했을 때 헤더 상호간의 인증 및 인증서 전송한다. Y가 CH_A에게 자신의 신원 정보를 보내게 되면서 인증 프로토콜을 시작한다.

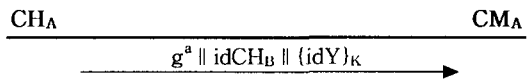

그림 3 인증 프로토콜 ①

그림 3에서는 CH_A가 난수 a를 생성하고 공개키 g^a를 계산한다. 그리고 클러스터 B의 헤더 공개키 g^b를 이용하여 세션키 $K=(g^a)^b$를 생성한다. 이와 같이 공개키 g^a, CH_B의 신원 $idCH_B$, 자신의 신원을 세션키로 암호화한 $\{idY\}_K$를 CM_A에게 보낸다.

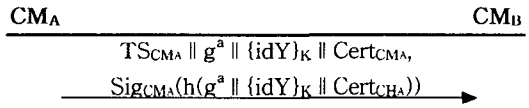

그림 4 인증 프로토콜 ②

그림 4에서는 CM_A가 전송받은 정보와 자신의 타임스탬프 TS_{CM_A}, 인증서 $Cert_{CH_A}$, 공개키 g^{CM_A}, 전자서명을 CM_B에게 보낸다.

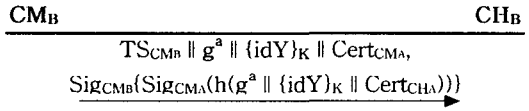

그림 5 인증 프로토콜 ③

그림 5에서 CH_B는 세션키 K를 계산하여 idY값을 얻어낸 후 Y의 인증서 CertY찾는다. CH_B는 클러스터마다 다른 신뢰기관을 가지고 있을 때 사용하는 인증서 체인을 사용하여 서로간의 전자서명을 검증할 수 있는 공개키를 인증서 체인 형식을 이용하여 전달한다.

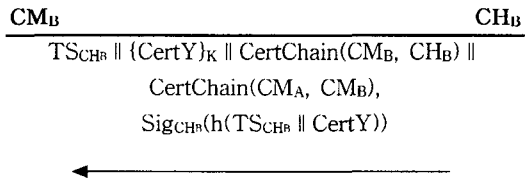

그림 6 인증 프로토콜 ④

그림 6에서는 CH_B가 전송받았던 인증서를 이용하여 $CertChain(CM_A, CM_B)$를 생성하고, CH_B는 또한 $CertChain(CM_B, CH_B)$를 만들어내서 CMB는 그것을 이용하여 전자서명을 확인할 수 있다.

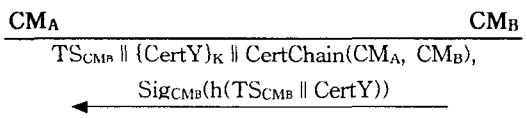

그림 7 인증 프로토콜 ⑤

그림 7에서는 $CertChain(CM_A, CM_B)$를 이용하여 $SigCH_B$를 검증할 수 있다.

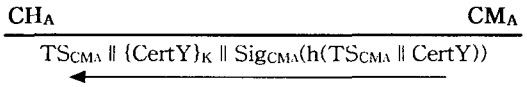

그림 8 인증 프로토콜 ⑥

그림 8에서는 전자서명을 K로 암호화 하였다. CH_A가 이전에 세션키 K를 알고 있는지 확인할 수 있다. 그리고 CH_A는 Y의 인증서 CertY를 획득한 후 Y의 인증을 할 수 있다.

4. 안전성 분석

- 기밀성: 각 헤드 사이에 교환되는 정보는 세션키 K에 의해 암호화 되어 전송되므로 기밀성이 보장된다.
- 무결성: 세션키 K는 정당한 사용자만이 알아낼 수 있는 것으로 사용자 정보에 대한 변경이 불가

능 하다.

- 부인방지: 각 노드간에 서명으로써 부인방지를 제공한다.

5. 결 론 및 향후 과제

본 논문에서 제안하는 인증 프로토콜은 Ad hoc 네트워크에서 보안 요구사항을 만족하면서 상호간에 인증 방법을 제시한다. 기존의 연구에서는 사용 환경이 좁은 지역에서 국한되었고, 침입자에 대한 데이터 무결성 및 메시지 리플레이 공격에 취약하다.

따라서 본 논문에서는 클러스터 기반 라우팅 환경에서 공개키 기반 인증을 통해 새로운 멤버노드가 별도의 인증과정을 거치지 않고 클러스터 상호간에 인증을 통해 인증과정을 제안하였다.

향후 연구 과제는 클러스터 헤드의 동적인 위치 버들에 대한 효과적인 인증방법과 그에 따른 키 합의 방법에 대한 연구가 필요할 것이다.

참고문헌

[1] N. Asokan and P. Ginzboorg, "Key Agreement in Ad-hoc Networks", *computer communications*, vol.23, pp.1627-1637, 2000

[2] Mingliang Jiang, Jinyang Li, and Y.C. Tay, "Cluster based routing protocol", Internet *Draft*, 1999

[3] G. Horn and B. Preneel, "Authentication and payment in future mobile systems", ESORICS, LNCS, vol.1488, pp. 460-482 1998

[4] L. Zhou and Z. Haas, "Securing Ad Hoc Networks", IEEE Network, vol.13, pp.24-30, 1999

[5] F. Stajano and R. Anderson, "The Resurrecting duckling: Security issues for ad-hoc wireless networks", In Proceedings of the 7th International Workshop on Security Protocols, 1999

[6] Andre Weimerskirch and Gilles Thonet, "A Distributed Light-Weight Authentication Model for Ad-hoc networks", ICISC, 2001

[7] Lakshmi Venkatraman and Dharma P. Agrawal, "A Novel Authentication scheme for Ad hoc Networks", IEEE, 2000