제19회 한국정보처리학회 춘계학술발표대회 논문집 제10권 제1호 (2003.5)

Ad-Hoc 네트워크에서 클러스터 기반의 라우팅을 위한 인증 프로토콜

김선형*, 이원준*, 이상근*
*고려대학교 컴퓨터학과
e-mail:shaklim@korea.ac.kr

An Authentication Protocol for CBRP in Mobile Ad-Hoc Networks

Sun-Hyoung Kim*, Won-Jun Lee*, Sang-Keun Lee*
*Dept. of Computer Science & Engineering, Korea University

요 약

Ad-Hoc 네트워크는 인프라 구조가 없는 네트워크로 정의된다. 즉 고정된 라우터나 백본망과 같은 인프라 구조가 없는 네트워크 상에서 Ad-Hoc 노드들이 이동하면서 무선 채널을 사용하여 통신하는 구조를 일컫는다. 기존의 무선 네트워크에서는 인증 기관의 역할을 하는 고정된 기지국이 존재하여 인증에 관련된 모든 작업을 기지국이 수행하였지만 네트워크 토폴로지가 수시로 변화하는 Ad-Hoc 네트워크 환경에서는 이러한 효과를 기대하기 힘들다. 본 논문에서는 클러스터를 기반으로 하는 Ad-Hoc 네트워크 환경에서 종단 노드 사이의 상호 인증과 안전한 세션키를 공유하는 방안을 제안한다.

1. 서론

Ad-Hoc 네트워크[1]는 고정된 라우터나 백본망과 같은 인프라 구조가 없는 네트워크로 정의된다. 기존의 무선 네트워크에서는 기지국이 유선 통신망에 연결되어 있는 구조로 되어 있는 반면, Ad-Hoc 네트워크는 모든 노드가 빈번하게 이동하는 환경에서 직접적인 무선 전송 범위에 위치하지 않은 노드들 간에 원활한 데이터 통신을 하기 위해 다중 홉 무선 링크로 구성된 새로운 형태의 통신망이다. Ad-Hoc 네트워크의 중간 노드들은 전송되는 데이터를 포워딩하거나 라우팅하며 전시의 군 통신망과 긴급 구조 상황, 대규모 무선 회의, 센서 통신망에서 사용하기에 적합한 특성을 갖고 있다.

기존의 무선 네트워크에서는 유선망과 연계된 고정된 기지국이 존재하고 이동 노드들은 이를 통해 상호 인증을 수행하고 세션키를 수립할 수 있다. 즉 기지국은 자신의 영역 안에 있는 이동 노드에 대하여 인증 기관(Certificate Authority)의 역할을 수행하게 된다. CA는 완전하게 신뢰된 기관으로서 인증이 필요한 노드에게 인증서를 발급한다. 그러나 이러한 메커니즘들이 인프라가 구축된 무선 네트워크에서는 잘 동작이 된다 하더라도 네트워크 토폴로지가 수시로 변화하는 Ad-Hoc 네트워크 환경에서는 적합하지 않을 수 있다[2].

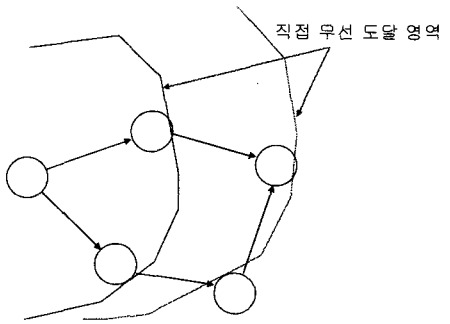

그림 1. Ad-Hoc 네트워크의 라우팅

지금까지 Ad-Hoc 네트워크를 위해 연구된 보안 기법들 중에는 Threshold Cryptography를 이용한 비밀 분산 기법[3], 공개키 암호 시스템을 Ad-Hoc 환경에 적용한 인증 기법[4], 안전한 라우팅을 위한 보안 기법[5,6]들이 있다. 그러나 기존의 보안 기법들은 Ad-Hoc 환경에서 작동하기에는 계산 복잡도가 높을 뿐만 아니라 이동 노드의 전력 소비량이나 처리 능력들을 고려하지 않은 것들이 대부분이다.

본 논문에서는 CBRP[7] 기반의 Ad-Hoc 네트워크에서 각 이동 노드들의 상호 인증 및 세션키를 수립하는 인증 프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2 장과 3 장에서는 각각 CBRP와 이를 기반으로 한 인증 기법을 소개한다. 4 장에서는 본 논문에서 제안하는 새로운 인증 프로토콜을 기술하고, 5 장에서 제안한 프로토콜을 분석한다. 6 장에서 결론을 맺음으로써 본 논문을 마친다.

2. CBRP(Cluster-based Routing Protocol) [7]

클러스터 기반의 구조는 경로를 탐색하는 패킷의 플러딩을 최소화하기 위해 고안되었다. CBRP는 클러스터링을 통하여 클러스터 헤드와 멤버를 갖는 클러스터를 구성한다. 클러스터 구조는 중첩되는 클러스터와 2 홉 반경의 클러스터로 분할되어 있다.

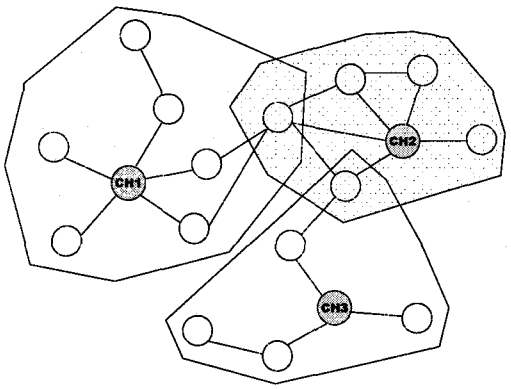

그림 2. 여러 개의 클러스터로 분할된 네트워크

클러스터 헤드는 클러스터 내에 있는 멤버들의 정보를 유지하기 위해 클러스터 선출 알고리즘에 따라 선출된다. 클러스터 내의 각 노드는 자신의 클러스터 헤드를 알고 있으며 모든 노드는 주기적으로 HELLO 메시지를 브로드캐스트한다. HELLO 메시지는 이웃 노드에 대한 정보와 인접한 클러스터에 대한 정보를 포함하고 있으며 이러한 HELLO 메시지는 2 홉의 토폴로지를 유지하는데 사용된다.

3. CBRP 기반의 인증 기법

[8]에서 제안된 클러스터 기반의 인증 기법에서는 노드가 처음으로 네트워크에 가입할 때, 노드가 다른 클러스터에 가입할 때, 그리고 노드가 클러스터에서 벗어나 다른 클러스터에 속한 노드와 통신할 때의 세 가지 시나리오를 고려하고 있다.

3.1 가정

클러스터 기반의 인증 기법에서는 다음과 같은 사항을 가정하고 있다.

- 네트워크의 모든 노드는 상호 간에 서로를 신뢰하고 있다.
- 각 노드는 암호 알고리즘과 키 생성 알고리즘을 수행할 수 있는 처리 능력이 충분하다.
- 각 노드는 키를 저장하기에 충분한 저장 공간을 내장하고 있다.

3.2 키의 분배

노드가 네트워크에 가입하면 system public/private key 쌍을 받으며 이 키 쌍은 네트워크의 모든 노드들에 의해 공유된다. 이 system key 이외에 각 노드는 다른 클러스터와 구별되는 유일한 cluster key를 클러스터 속한 모든 노드들이 공유하고 있다. 이 키는 클러스터 헤드에 의해 생성되고 system public key로 암호화되어 모든 클러스터 멤버에게 분배된다. 각 클러스터 헤드는 head key라고 불리는 유일한 public/private key 쌍을 갖게 되며 헤더로 선출된 노드는 이를 브로드캐스트한다. 따라서 각 노드들은 system public/private key의 쌍, cluster key, cluster id를 구성하는 테이블과 헤드의 public key를 알고 있어야 하다. 각 클러스터 헤드는 자신의 private key를 안전하게 저장하고 있어야 한다.

3.3 프로토콜 단계

1. 노드가 다른 노드와 세션을 성립할 때 헤더에 요청 메시지를 보낸다.
2. 헤드는 k 개의 임의의 소수 $(R_1, R_2, \ldots, R_3)$를 생성한다.
3. k 개의 소수들은 head의 private key인 $E_p v$로 암호화된 후 다시 cluster key인 $E_c k$로 암호화된다.

4. 헤드는 $E_c k(E_p v(R_1, t_v))$에서 $E_c k(E_p v(R_k, t_v))$까지 k 개의 암호화된 메시지를 브로드캐스트하며 모든 클러스터 멤버들은 수신된 데이터를 인증 태그로서 사용한다.
5. 송신 노드는 태그에 check 함수를 계산하여 전송하려는 패킷에 첨가하여 보낸다.
6. 수신 노드가 패킷을 수신하게 되면 태그의 check 함수를 계산하여 송신 노드가 보낸 값과 일치하면 수락하고, 그렇지 않으면 무효로 처리한다.

4. 제안하는 종단간 인증 메커니즘

두 이동 노드의 통신은 클러스터의 외부 공격자뿐만 아니라 내부의 공격자에 대해서도 보호될 수 있어야 한다. 즉 두 이동 노드 사이에 교환된 세션키에 대한 정보는 자신의 클러스터에게조차 노출되어서는 안 된다. 따라서 종단 노드 간의 상호 인증과 세션키의 확립을 위해서는 두 이동 노드 사이에서의 보안뿐만 아니라 이동 노드와 클러스터 사이에서의 보안이 제공되어야 한다. 다음은 프로토콜에 사용되는 기호들이다.

기 호	설 명
h_1, h_2, h_3	일방향 해쉬 함수
H_A, H_B	각 클러스터 A, B의 헤드
M_A, M_B	각 클러스터 A, B의 멤버
r_A	A가 생성한 random number
t_A	A가 생성한 time stamp
id_A	A의 신원
$Sig_A\{X\}$	메시지 X에 대한 A의 서명
$Cert_A$	A의 인증된 공개키 인증서 (g^{x_A})

4.1 가정

본 논문에서 제안한 클러스터 기반의 종단간 인증 기법에서는 다음과 같은 사항을 가정하고 있다.

- 각 이동 노드 M_A, M_B는 각 클러스터 헤드 H_A, H_B에 의해 서명된 인증서를 가지고 있다. 또한 각 노드는 자신이 속한 클러스터 헤드와 공통의 비밀 통신키를 공유하고 있다.
- 각 클러스터 헤드 H_A, H_B는 서로의 비밀 통신키를 공유하고 있으며 클러스터 내의 각 노드들과도 공통의 비밀 통신키를 공유하고 있다.

4.2 프로토콜 모델

제안하는 논문에서는 그림 3과 같이 하나의 클러스터 내에 있는 노드가 다른 클러스터 내에 있는 노드와 인증 절차를 수행하는 상황을 고려하고 있다.

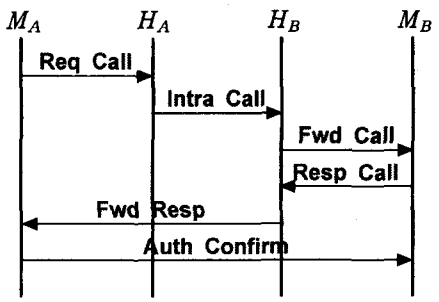

그림 3. 메시지 전달 과정

4.3 프로토콜 단계

1. Request Call

$$M_A \rightarrow H_A :$$
$$\left\{ id_{M_A} \| id_{M_B} \| g^{r_{M_A}} \right\}_{K_{M_A H_A}}$$

클러스터 A의 멤버인 M_A가 다른 클러스터 B의 멤버인 M_B와 통신하기 위해 자신의 개인키와 공개키 $g^{r_{M_A}}$를 생성하여 클러스터 헤드 H_A에게 공유하고 있는 비밀 통신키로 암호화하여 전송한다.

2. Intra-call Forwarding

$$H_A \rightarrow H_B :$$
$$\left\{ id_{M_A} \| id_{H_A} \| g^{r_{M_A}} \right\}_{K_{H_A H_B}}$$

클러스터 헤드 H_A는 M_B가 속한 클러스터 헤드 H_B와 공유하고 있는 비밀 통신키로 암호화하여 M_A의 공개키를 클러스터 헤드 H_B에게 전송한다.

3. Forward Call

$$H_B \rightarrow M_B :$$
$$\left\{ id_{M_B} \| g^{r_{M_A}} \right\}_{K_{M_B H_B}}$$

H_B는 H_A로부터 받은 M_A의 공개키 정보를 M_B와 공유하고 있는 비밀 통신키를 이용하여 암호화하여 M_B에게 전달한다.

4. Respond Call

$M_B \rightarrow H_B$:
$\{r_{M_B}, h2(K_{M_AM_B}, r_{M_B}, id_{M_B}), t_{M_B}, Cert_{M_B}\}_{K_{M_BH_B}}$

M_B는 자신의 비밀키와 M_A의 공개키를 기반으로 세션키 $K = h1(r_{M_B} \| g^{x_{M_B} r_{M_A}})$를 생성한 후 자신의 공개키 정보가 포함된 $Cert_{M_B}$를 H_B와 공유하고 있는 키로 암호화하여 통신 요청에 대한 응답 메시지를 전송한다.

5. Forward Response

$H_B \rightarrow M_A$:
$r_{M_B}, h2(K_{M_AM_B}, r_{M_B}, id_{M_B}), t_{M_B}, Cert_{M_B}$

H_B는 M_A에게 메시지를 전달하며 이 메시지를 통하여 M_B와 마찬가지의 과정을 통해 세션키 K를 계산한다. 수신된 K 값과 비교함으로써 M_B가 정당한 통신 상대자임을 인증한다.

6. Confirm Mutual Authentication

$M_A \rightarrow M_B$:
$\{Sig_A(h3(g^{r_{M_A}}, g^{r_{M_B}}, r_{M_B}, id_{M_B}, t_{M_A}), Cert_{M_A}\}_{K_{M_AM_B}}$

M_B는 K로 암호화된 M_A의 서명된 메시지를 확인함으로써 M_A와의 인증 절차를 마치게 되고, 프로토콜이 수행된 후에 양 통신 노드는 인증된 세션키를 획득하게 된다.

5. 프로토콜 분석

CBRP를 기반으로 한 기존의 인증 기법에서 각 노드는 자신이 생성하는 public/private key의 쌍 이외에 system key의 쌍과 cluster key 쌍, 그리고 head key의 쌍을 각각 저장하고 있어야 한다. 반면 제안하는 논문에서는 최소한의 키를 사용하여 개체 간의 상호 인증과 키 인증에 대한 안전성을 보장하고 있다.

또한 클러스터 헤드와 멤버 사이에서 기밀성이 요구되는 메시지는 대칭키 방식을 이용하여 처리 비용을 낮추고, 클러스터 멤버끼리의 통신에서는 공개키 방식을 도입하여 키 관리의 문제를 해결하고 있다. 해쉬 함수를 적용하여 메시지의 무결성과 전자 서명을 통해 발신자의 부인 방지 기능을 제공한다.

6. 결론 및 향후 연구 과제

본 논문에서는 Ad-Hoc 네트워크에서 CBRP를 기반으로 하여 서로 다른 클러스터 내에 속한 노드들 간의 상호 인증 및 비밀 세션키를 수립하기 위한 프로토콜을 제안하였다.

향후에는 다양하고 이질적인 Ad-Hoc 네트워크 환경에서도 보안성을 제공하는 인증 메커니즘이 연구되어야 할 것이다.

참고문헌

[1] S. Corson and J. Macker, Mobile Ad Hoc Networking (MANET), IETF RFC 2501, January 1999.

[2] Frank Stajano and Ross Anderson, "The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks," The 7th International Workshop on Security Protocols, LNCS 1796, Springer-Verlag, 1999.

[3] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, Vol.13, No.6, pp.24-30, November/December 1999.

[4] Srdjan Capkun, Levente Buttyan and Jean-Pierre Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," Swiss Federal Institute of Technology Lausanne (EPFL) Tech. Report, June 2002.

[5] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Routing for Mobile Ad Hoc Networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

[6] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Technical Report TR01-383, December 2001.

[7] Mingliang Jiang, Jinyang Li and Y. C. Tay, Cluster Based Routing Protocol(CBRP), http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-manet-cbrp-spec-01.txt, August 1999.

[8] Lakshmi Venkatraman and Dharma P. Agrawal, "A Novel Authentication Scheme for Ad Hoc Networks," Wireless Communications and Networking Conference (WCNC 2000), IEEE, Vol.3, pp.1268-1273, 2000.