Ad Hoc 네트워크에서의 CBRP 기반 인증 프로토콜 설계

이근호° 서혜숙 한상범 황종선
고려대학교 컴퓨터학과
root1004@korea.ac.kr°, suh@kida.re.kr, hansb@kt.co.kr, hwang@disys.korea.ac.kr

The Design for Authentication Protocol Based on CBRP in Ad Hoc Network

Keun-Ho Lee° Heyi-Sook Suh Sang-bum Han Chong-Sun Hwang

Dept. of Computer Science & Engineering, Korea University
1, 5-ga, Anam-dong, Sungbuk-gu, Seoul, 136-701, Korea

요 약

최근 급속하게 성장하고 있는 무선 이동 통신 분야중의 한 분야가 Ad hoc 네트워크 분야일 것이다. Ad hoc 네트워크는 기존의 고정된 네트워크의 한계를 뛰어 넘는 네트워크이다.

본 연구에서는 Ad hoc 네트워크의 클러스터 기반의 라우팅 프로토콜에서의 인증에 대한 프로토콜을 멀티 계층으로 설계하였다. CBRP(Cluster Based Routing Protocol)의 라우팅 프로토콜에서는 클러스터간의 인증을 위하여 CH(Cluster Head)간의 인증을 통하여 인증을 하게 된다. CH간의 신뢰성을 위하여 MCH(Main Cluster Head)를 두어 CH간의 신뢰성을 보장함으로써 상호 클러스터간의 인증을 위한 프로토콜을 설계하였다.

1. 서 론

최근 인터넷의 확장과 단말기의 하드웨어, 무선통신 기술개발이 이루어짐에 따라 시·공간상의 제한 없이 인터넷을 사용하고자 하는 욕구 증가하고 있다. 유일한 해결방법은 무선매체를 이용하는 것이다. 이러한 추세를 가장 잘 반영하는 기술 중의 하나인 Ad Hoc 통신망은 기존의 기지국이 유선 통신망에 연결된 형태의 통신 인프라 기반과는 달리 모든 단말기가 이동하는 환경에서 서로 직접적인 무선 전송 범위에 위치하지 않은 노드간의 원활한 데이터 전송을 위해 다중 홉 무선 링크로 구성되어 여러 개의 중간 단말기들의 데이터 포워딩/경로설정(Forwarding/Routing)에 의존하게 되는 새로운 형태의 통신망이다. 이러한 Ad Hoc 통신망에 관한 연구는 활발한 편이지만 아직 Ad Hoc 보안 연구는 아직 미흡하다. 무선링크를 사용하는 무선 네트워크는 고정 네트워크에 비해서 취약한 보안 문제에 직면해 있다. Ad Hoc 통신망은 이동단말기의 이동성 문제로 인하여 보안에서 심각한 문제를 가지고 있는데 아직까지 제안된 Ad Hoc 통신망 프로토콜에는 충분한 보안에 관한 해결방안을 제시되지 못하고 있는 실정이다. 따라서 본 논문에서는 현재 제안된 Ad Hoc 네트워크의 라우팅 프로토콜 중 클러스터 기반의 CBRP라우팅 방법에 보안을 접목하여 인증 프로토콜을 설계하였다. 본 논문에서는 2 장에서는 클러스터 기반의 라우팅 프로토콜에 대하여 설명하고, 3장에서는 클러스터간의 인증 프로토콜에 대하여 설계한다. 4장에서는 성능 평가를 통하여 제안한 인증 프로토콜의 기존의 프로토콜을 비교하고, 5장에서는 결론 및 향후 연구과제에 대해서 서술하였다.

2. 관련연구

CBRP(Cluster Based Routing Protocol)[1]는 클러스터링을 통하여 CH(Cluster Head)와 노드 멤버를 갖는 클러스터를 구성한다. 클러스터 구성 방법은 지역적으로 인접한 호스트들이 자신의 ID와 이웃 호스트를 CH로 선출하게 되고 CH가 아닌 호스트들은 클러스터의 멤버가 된다. 클러스터가 형성되면 CH는 멤버 호스트와 이웃 CH로의 라우팅 정보를 유지하게 되는데 이 정보는 후에 멤버들의 라우팅 정도 획득을 위하여 사용된다. 목적지에 대하여 라우팅 정보가 필요한 호스트는 자신의 CH에게 목적지에 대한 라우팅 정보 획득을 요청한다. 요청을 받은 CH는 자신의 멤버 호스트중에 목적지 호스트가 있는지 조사하고, 없는 경우 자신의 이웃 CH에게 경로 요청 패킷을 전송하게 된다. 요청을 받은 이웃 CH는 앞의 CH와 같이 자신의 멤버 호스트중에 목적지 호스타가 있는지 조사하고 만약 목적지 호스트가 존재하면, 소스 라우트 정보를 생성하여 경로 설정을 요구했던 송신 호스트로 소스 라우트 정보를 제공한다.

3. CBRP 기반의 인증 프로토콜 설계

3.1 설계 목적

CBRP의 라우팅 프로토콜을 통하여 대규모 네트워크를 클러스터 기반으로 작성하였다. 클러스터간의 보안 위협 요소를 분석하여 ARAN(Authenticated Routing for Ad Hoc Networks)[2] 프로토콜을 이용한 APBC(Authentication Protocol Based on CBRP) 프로토콜을 설계하였다.

3.2 작성 시나리오

CBRP라우팅 프로토콜에서 MCH(Main Cluster Head)의 개념을 도입하여 MCH는 신뢰할 수 있는 인증서버이다. MCH는 CH에 대한 인증만을 담당한다. 클러스터 형성과정에서 Multi hop을 지원한다고 가정하였다. 본 제안은 일정한 공간의 컨퍼런스의 모델들이 합쳐진 형태의 시나리오를 가지고 있다. MCH는 이러한 각 컨퍼런스를 최종적으로 인증해 줄 수 있는 Trust Server의 역할을 하게 된다. MCH는 클러스터간의 이동에 필요한 인증만을 담당한다. 클러스터 내에서는 노드들 간에 선출된 CH가 각 노드를 인증 한다.

3.3 APBC 프로토콜 설계

3.3.1 CBRP 라우팅 구조 개선

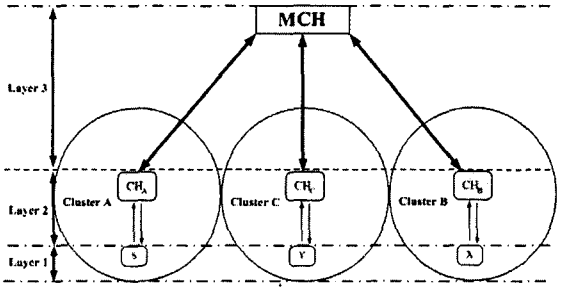

그림 1 MCH와 CH간의 구조

클러스터내에서는 ARAN 프로토콜[2]을 이용하여 각각의 노드들이 현재 가능한 근원지-목적지에 해당하는 라우팅 테이블 목록을 하나씩 유지해야 한다. 이것은 안전하지 않은 ad hoc 라우팅 프로토콜에서 사용하는 목적지당 라우팅 목록을 유지하는 방식보다 많은 비용이 요구된다. ARAN에서 라우팅 방법을 CBRP기반으로 하여 클러스터 헤드의 개념을 도입함으로써 각 노드에 라우팅 테이블 목록을 유지하는 단점을 극복하도록 라우팅 프로토콜을 개선하였다. 기존의 CBRP의 경우는 각 클러스터 단위로 클러스터 헤드를 선출[5]하여 클러스터 헤드에 의한 인증의 역할을 하였다. APBC프로토콜을 제안하기 위해서 CBRP 프로토콜를 멀티캐스트 기반의 구조로 변경하여 적용하였다. 다음은 제안 프로토콜의 설계를 위한 과정을 분류하였다. MCH로부터 CH 인증, CH와 노드 사이의 인증, 노드가 클러스터를 떠날 때, 다른 클러스터내 있는 두 노드 통신간의 인증 과정에 대한 프로토콜을 설계하였다.

3.3.2 APBC 프로토콜의 동작 과정

가) MCH(Main Cluster Head)로부터 CH 인증

MCH에서 각 CH에 대한 인증을 수행한다. 클러스터 내에서 선출된 CH에 대한 등록 과정과 인증 과정을 통하여 CH에 대한 정보만을 포함하고 있다. 만약에 CH가 인증을 요하는 경우에는 time값을 가지고 MCH의 비밀키로 응답을 해줌으로써 서로 서명하게 된다.

$$MCH \rightarrow CH : cert_{CH} = [ID_{CH\,A} \| K+_{MCH} \| e \| time1]$$

표 1 APBC에서 사용되어지는 프로토콜의 데이터

Notations	Description
MCH	Turst Server of main Cluster Head
CH_A	Cluster Head A
ID_X	Identity of X
N	Nonce
$K+_{CH}$	Public key of CH
$K-_{CH}$	Private key of CH
$Cert_X$	Certificate of X
t	Current time

나) CH와 노드 사이의 인증,

CH의 인증은 CH의 ID와 CH의 비밀키를 이용하여 노드들을 서명해 준다. CH에는 노드들의 정보를 가지고 있다. 인증을 요구할적에는 Time과 Nonce를 이용하여 인증해 준다.

$$CH \rightarrow A : cert_{CH} = [ID_{CH} \| K-_{CH} \| e \| time1], N_{CH}$$

CH를 암호화 하기 위하여 Nonce를 이용한다. r는 Nonce의 나른 표시이다.

$$E_{CH_A K+}(r) \rightarrow CH_A$$

CH는 암호화된 r를 자신의 비밀키로 복호하여 자신이 생성한 r과 같은지 확인한다.

다) 노드가 클러스터를 떠날 때

클러스터내의 노드가 다른 클러스터로 떠날 때 시스템키를 이용하여 인증을 수행한다. 서로간의 인증이 끝나면 새로운 클러스터 헤더는 진입 노드에게 새로운 클러스터 키를 제공한다. 이전 CH는 일정 시간 후에 hello메시지를 받지 못하는 노드는 CH 테이블에서 삭제한다.

라) 다른 클러스터내 있는 두 노드 통신

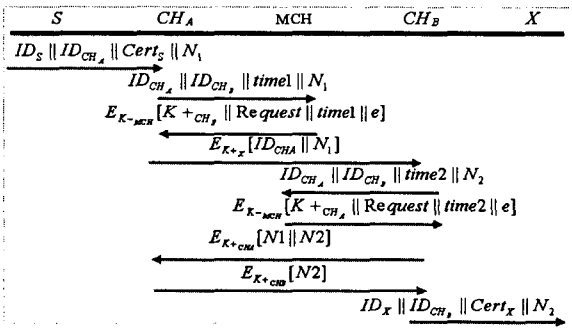

그림 2 종단간 키 교환 프로토콜

메시지 기밀성을 위해 세션 키를 사용하여 암호화하여 전송한다. 세션 키는 노드만이 공유할 수 있어 인증을 수행한다. 그림 2에서 클러스터 A와 클러스터 B 사이의

노드 끼리 통신을 하고자 할 때 다음의 프로토콜을 적용하 였다. 노드 s가 CH_A에 세션을 요청한다. 나)에서의 프로토콜이 작동하여 CH와 노드간의 세션을 형성하고 노드를 인증해 준다. Nonce를 이용하여 CH_A의 ID를 CH_B의 공개키로 암호화 하여 CH_B에게 보낸다. 이 과정에서는 CH_A와 CH_B가 신뢰 할 수 있는지를 MCH가 인증을 해준다.

$$CH_A \rightarrow E_{K+CH_B}[N_1 \| ID_{CH_A}] \rightarrow CH_B$$

CH_B 는 CH_A 의 공개키로 암호화 해서 응답 메시지를 CH_A에게 보낸다. MCH는 CH_B, CH_A 의 키 정보를 가지고 있으므로써 상호 신뢰 할 수 있도록 인증을 해준다.

$$CH_B \rightarrow E_{K+CH_A}[N_1 \| N2] \rightarrow CH_A$$

N2를 받아서 CH_A 는 N2를 CH_B 의 공개키를 사용해서 암호화 한 뒤 CH_B 에게 전송한다.

$$CH_A \rightarrow E_{K+CH_B}[N2] \rightarrow CH_B$$

위와 같은 절차를 가지게 되면 CH간의 상호 인증이 이루어진다. CH_B 와 노드간의 방법은 CH_A 에서 수행했던 방법으로 하면 된다.

$$CH_B \rightarrow D_{K+CH_A}[D_{K-CH_A} \| [M]] = K_S$$

메시지 M을 복호화 하여 세션키 K_S를 생성한다.

$$S \rightarrow E_{K_S}[M, t_1] \rightarrow X$$

재전송 공격을 대비하여 메시지 M과 time stamp t1을 포함 시킨다.

$$X \rightarrow E_{K_S}[R, t_2] \rightarrow S$$

두 노드간의 안전한 전송이 이루어진 후, 각 노드 S, X는 각각의 CH에게 세션 종료 요청을 하며 CH는 세션키 K_S를 제거한다.

MCH에 대한 방법을 통하여 CH간의 인증과 CH를 통한 노드에 대한 인증등에 관한 유형을 제안해 보았다. 이동간에 발생할 수 있는 문제점에 대한 내용을 가정으로 넣었으며 MCH에 대한 신뢰성을 증명 할 수 있는 방법과 CH 선출시에 신뢰성 부여에 관한 연구가 좀더 필요하다. 이는 향후 꾸준한 논문 발표를 통하여 지속적인 연구를 하도록 하겠다.

4. 성능 평가 및 비교

CBRP는 인증 과정시 CH에 의한 인증 과정을 거친다.

표 1 프로토콜 성능 비교

item \ protocol	CBRP	APBC
인증과정	△	0
효 율 성	△ / 0	0
확 장 성	△	0
안 정 성	△	△ / 0

× : 나쁨 △ : 보통 ○ : 좋음

CH는 멤버들중 신뢰할 만한 멤버를 CH로 설정함으로써 인증 과정에 있어서 허위 인증이 이루어 질 수 있는 반면에 APBC의 경우는 MCH가 CH에 대한 인증을 통해야 함으로써 인증 과정이 좀더 안정적이다. CBRP의 경우는 근거리 지역의 노드들을 클러스터 단위로 구별하는 반면에 APBC의 경우는 대규모의 네트워크 망에 사용할 수 있도록 구성이 되어 있으므로 확장성 면에서도 우수하다고 볼 수 있다.

5. 결론 및 향후 연구 과제

본 논문에서는 CBRP에 대한 인증 과정에 대한 내용을 살펴보았고, APBC에 대한 인증 프로토콜을 설계하였다. APBC의 기본 개념은 최상위에 신뢰성이 높은 MCH를 두는데 의의가 있다. MCH의 선출이나 MCH의 대규모 네트워크 망에서의 신뢰성을 높일수 있는 방법에 대한 연구가 추가 적으로 이뤄져야 할 것이다.

참고문헌

[1] M. Jiang, J. Li, and Y.C. Tay, "Cluster based routing protocol(CBRP)", Internet Draft, MANET working group, draft-ietf-manet-cbrp-spec-01.txt, Aug. 1999.

[2] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", In *Proc.* IEEE Network Protocols, pages 78-87, 2002.

[3] Venkatraman, L.; Agrawal, D.P, "A novel authentication scheme for ad hoc networks", In Proc. IEEE Wireless Communications and Networking Conference, pages 1268-1273, 2000.

[4] Lin, J.C, Paul. S, "RMTP: a reliable multicast transport protocol", In Proc. INFOCOM '96. Fifteenth Annual Joint Conference of the IEEE Computer Societies, pages 1414-1424, 1996

[5] Winston Liu C.-C. Chiang, Hsiao-Kuang Wu and Mario Gerla, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel", In Proc, IEEE SICON'97, 1997.

[6] Jiejun Kong, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla and Songwu Lu, "Adaptive Security for Multi-layer Ad Hoc Networks," to appear in Wireless Communications and Mobile Computing, Special Issue on Mobile Ad Hoc Networking, 2002.

[7] G. Pei et al, "A Wireless Hierarchical Routing Protocol with Group Mobility", In Proc, IEEE WCNC 99, New Orleans, LA, Sept. 1999

[8] Lidong Zhou; Haas, Z.J.; Securing ad hoc networks , IEEE Network, Volume: 13 Issue: 6 , Nov.-Dec. pages 24-30, 1999.

[9] B.Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., New York, 1996

[10] L.Zhou and Z. J. Haas. Securing ad hoc networks , IEEE Network, 13(6), pages 24-30, 1999