제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

Ad Hoc 네트웍에서 효율적인 라우팅 설계에 대한 RSA 인증 알고리즘

이현주*
*충북대학교 전자계산학과
e-mail:leehyn2@hanmail.net

RSA Authentication Algorithm for Efficient Routing Scheme in Ad Hoc Network

Hyun Ju Lee*
*Dept. of Computer Science,ChungBuk National University

요 약

Ad Hoc 네트워크는 베이스 스테이션이나 이동 스위칭 센터와 같은 기존의 고정된 infrastructure가 없는 이동 호스트들을 위한 새로운 패러다임이다. 본 논문에서는 기존의 Table-driven 방식과 On-demand 라우팅의 장점을 접목시킨 2-tier 계층구조를 사용한 다이나믹 라우팅 기법과 이를 바탕으로 효율적인 routing 경로를 확보하면서도 구조적으로 취약한 보안 위협 요소들에 대한 안정성을 제공하는 클러스터 노드간에 RSA기법을 사용한 인증 알고리즘을 제안한다.

1. 서 론

Ad Hoc network는 베이스스테이션과 같은 고정된 인프라가 없는 이동 단말들 간의 다중 홉을 통해 패킷 통신이 이루어지는 무선 네트워크로서, 이동 노드들은 한정된 채널을 통해 서로 통신이 이루어지므로, 무선 backbone이나 centralized 된 개체가 없는 것이 특징이다. 이동 Ad Hoc 네트워크에는 통신을 위한 특별한 라우터나 스위치들이 없으며, 모든 이동 호스트 혹은 그 중 몇 개의 호스트들이 라우터나 스위치의 역할을 하고 있어 이동 호스트들 상호간의 다이나믹한 구성이 가능하다.

Ad Hoc네트워크는 경제적인 측면에서 유선 네트워크를 구성하기 어렵거나 또는 네트워크를 구성한 후 단기간 사용하는 경우에 적합한 네트워크 구성 방식으로 군사적인 용도에서부터 학교, 병원, 응급 구조상황, 외국 귀빈의 방문시 경호 등 매우 다양한 분야에 적용 가능하며 이동 단말의 급증과 관련된 응용 서비스의 출현에 따라 그 필요성도 점차 높아지고 있다.[1]

이에 따라 Ad Hoc 네트워크에 관한 많은 연구가 IETF MANET WG 이나 Bluetooth Consortium 과 같이 다양한 그룹들에 의해서 이루어 지고 있으며[8,9,10], 차세대 wireless LAN 환경의 유망한 후보로서 주목받고 있으나 기존의 라우팅 기법만으로는 Ad Hoc 네트워크가 직면한 다양한 문제에 총체적인 solution을 제공할 수 없고, 실제적인 네트워크상에 적용하는 데 있어 상당한 오버헤드를 가지고 있기 때문에 전통적인 라우팅 기법들을 차세대 이동 Ad Hoc 환경에 적용할 수 없다. 또한 Ad Hoc 망이 3세대 무선 통신망(battery-powered devices) 서비스와 연동을 위하여 Ad Hoc망 내에서 BS(Base-Station)와 통신할 수 있는 메커니즘과 개체가 필요하다.

이 논문에서는 효율적인 라우팅 경로의 설정과 망구성을 위하여 2-tier 계층 구조를 사용하여 서로 다른 클러스터 노드 사이에 안정적인 통신을 위한 인증 알고리즘을 제안한다.

2. A Secure Efficient Routing (ESR)

Z.J. Haas는 re-configurative wireless Network에 관한 연구에서[3] 계층구조를 유지하고 클러스터 헤더 상호간 연관을 갖는 것은 네트워크 자원을 너무 많이 사용하기 때문에 flat routed network를 사용하는 것이 더 적절하다는 주장을 하였으나, 본 논문에서는 2-tier Ad Hoc 네트워크를 구성함에 있어 상위계층(tier-2)은 proactive 방식을, 하위 계층(tier-1)은 reactive 라우팅의 장점을 응용하여, 효율적인 network 관리와 함께 경로 설정을 위한 오버헤드와 전송 지연시간을 줄이고자 한다. 또한 Threshold 기법[7,2]을 이용하여 시스템 키 관리 서비스의 책임을 각 CH에게 분할해서 관리함으로써 각 CH의 신뢰 여부를 확인하며, 클러스터 헤드가 변질된 경우 그 CH를 네트워크에서 배제하고 하위 tier에 속한 이동 노드 중 새로운 클러스터 헤드 역할을 수행할 노드를 신속하게 생성하여 네트워크를 재 구성[LCC[6]+ ③] 한다.

[그림 1]과 같이 2개의 tier 계층구조에서 tier-1에 속한 노드들 중 한 노드가 상위 계층으로 통하는 게이트웨이의 역할을 수행 하도록 CH로서 지정되며 상위 계층에 속한 노드들은 CGSR(Cluster-head Gateway Switch Routing) protocol을 이용하여[1,6] 네트워크를 구성한다.[4]

하위 계층에 속한 노드들은 AODV[5] 알고리즘을 통해 On-Demand 방식으로 라우팅 경로를 설정하며 서로 다른 하위 계층에 속한 이동 노드들의 통신에서는 게이트웨이 역할을 수행하는 CH를 통하여 통신코자 하는 노드가 속해있는 CH를 통해 전달된다. 또한, 기존의 BS와 통신이 필요할 경우에도 신뢰할 수 있는 CH와 상호 연동 가능성을 제고한다.

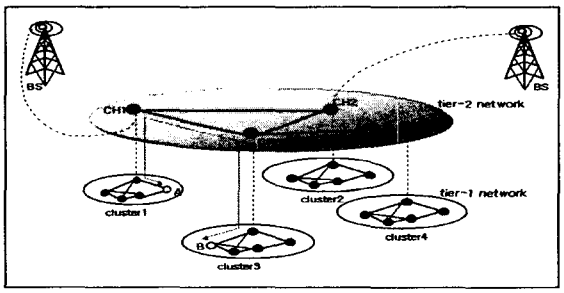

그림1. ESR(A Secure Efficient Routing Scheme)

3. CH 재 구성 알고리즘

2-tier 계층 네트워크 구조에서 각각의 CH는 하위 계층에 속해 있는 이동 노드들의 라우터 역할과 함께 세션 키를 생성하고 키 관리에 대한 책임을 다른 CH와 함께 담당한다. 그러므로 한 CH가 적에 의해 공격을 당하거나 다른 이동 노드로부터 신뢰를 상실하게 된 경우 이 CH를 네트워크에서 배제하고, 변질된 클러스터 헤더를 대체할 새로운 CH를 생성하여 네트워크를 재 구성해야 할 필요가 있다. LCC(Least Cluster Change) 알고리즘[6]의 경우엔 클러스터 헤드를 생성할 경우를 단지 2가지로 제한하였으나, 변질된 클러스터 헤더가 발견될 경우 안정적인 라우팅을 위하여 본 논문에서는 LCC에 3)의 경우를 보완하여 다음과 같은 경우 클러스터 헤드를 재 생성한다.

1) 한 개의 클러스터 헤더가 자기의 영역을 벗어나 다른 클러스터 헤더가 있는 곳으로 이동할 경우
2) 한 이동 노드가 클러스터 헤더가 없는 곳으로 이동할 경우[6]
3) Threshold 기법이 특정 CH의 변질을 증명할 경우

4. 인증 Strategy

이 논문이 제안한 구조에서 신뢰할 수 있는 인증 알고리즘을 수행하기 위하여 다음 세 가지의 경우에 대하여 고찰한다.

1) Cluster Head 와 새롭게 진입한 node 사이의 인증
2) 클러스터 내의 한 노드가 현재의 클러스터를 떠나 다른 곳으로 이동할 때
3) 다른 Cluster내에 있는 두 노드 A와 B 사이의 인증

4.1 인증 알고리즘

모든 CH는 전체 네트워크의 안정성 확보를 위해 시스템의 분할된 키를 가질 뿐만 아니라 자신의 공개/비밀 키 쌍을 가지며 , 클러스터내 소속된 노드간 통신을 위하여 교유한 클러스터 키를 가진다. 네트워크내의 모든 노드들은 시스템의 공개 키를 알고 있으며, 또한 자신의 공개/비밀 키 쌍을 가지고 있다고 가정한다. 또한 클러스터 헤더에 의해 생성된 세션 키는 오직 한 번의 TCP 세션에만 유효하다고 가정하며.메시지 전송 시 외부 적의 replay 공격을 방지하기 위해 메시지와 함께 time stamp를 암호화하여 전송한다.

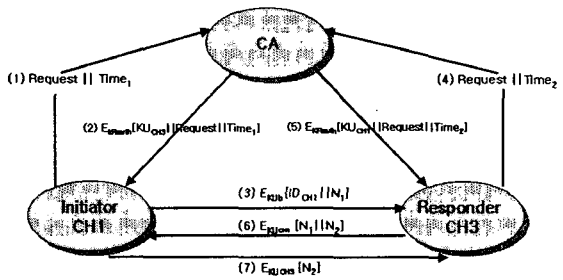

그림2. 공개키 분배 시나리오

• CH1은 CH3의 공개키 요구를 위해 클러스터 헤더 중에서 power있는 CH(CA 역할을 함)에게 time stamp와 함께 request 메시지를 보낸다.

• CA의 비밀키를 사용하여 암호화된 메시지를 보내면 CH1은 CA의 공개키를 사용하여 메시지를 복호화한다.

• CH1은 CH3의 공개키를 저장하고 CH1의 ID와 nonce N1을 CH3의 공개키로 암호화 하여 보낸다.

• CH3는 CH1의 공개키를 위와 같은 방법으로 얻는다.

이러한 과정에 의해 각 클러스터 헤더는 CH1과 CH3 내에 있는 두 노드간에 라우팅을 위한 서로 신뢰할 수 있는 공개키를 비밀리에 전송할 수 있다.

4.1.1 Cluster Head 와 Node 사이의 인증

이동 노드가 네트워크에 새롭게 진입하게 되면, 각 노드들의 주기적인 ' HELLO' 메시지 multicasting에 의해 CH에게 발견된다. 이때 시스템 키를 이용하여 시도 - 응답(challenge and response)방식으로 상호 인증을 한다. 상호 인증이 이루어지면 CH는 자신의 공개 키를 tier-1 네트워크의 통신을 위하여 이동 노드에 전달한다.

1) CH1은 난수 r을 생성하여 자신의 클러스터 키와 함께 진입 노드 A 에게 보낸다

2) 진입노드 A는 local communication을 위해 클러스

터 키를 보관하고, 난수 r를 CH1의 공개키로 암호화해서 CH1에게 보낸다.

$$E_{CH_{1_p}}(r) \rightarrow CH1$$

3) CH1은 암호화된 난수 r를 자신의 비밀키로 해독하여 자신이 생성한 난수 r 과 같은지 확인한다.

4.1.2 한 노드가 현재의 클러스터를 떠나 다른 곳으로 이동할 때

한 노드가 자신이 속해있던 클러스터를 떠나 다른 새로운 클러스터에 진입하게 될 때, 새로운 클러스터는 그 진입 노드를 자신의 클러스터내의 노드로 간주하여 시스템 키를 이용하여 시도-응답(challenge and response)방식으로 인증을 수행한다. 상호 인증이 끝나면 새로운 클러스터 헤더는 진입노드에게 새로운 클러스터의 키를 제공하며, 이 이동 노드가 속해 있던 옛 클러스터 헤드는 일정 시간 후에 hello메시지를 수신하지 못하는 모든 노드에 대 한 엔트리를 삭제한다.

4.1.3 다른 Cluster내에 있는 두 노드 A와 B가 통신을 하고자 할 때

완전한 메시지의 기밀성을 위해 전체 패킷을 세션 키를 사용하여 암호화한 후 전송한다. 이 세션 키는 통신을 원하는 두 노드만이 공유할 수 있기 때문에 인증을 위해 사용된다. 우리는 각 패킷에 대해 강력한 인증을 수행하는 신뢰성 있는 알고리즘을 제안한다. 이때, 클러스터 헤드는 모든 노드들에 대해 CA(Certification Authority)의 역할을 하고 CH 키는 세션 키를 비밀리에 교환하기 위해 사용된다. A와 B가 통신하고자 한다면, 다음 절차에 의해 데이터 인증이 이루어진다.

1) node A -> CH1 : 세션 설립 요청

2) CH1이 N1(Nonce 1)과 CH1의 ID를 CH3의 공개키로 암호화하여 CH3에게 보냄

$$\text{CH1} \rightarrow E_{CH3_p}[N_1 \| ID_{CH1}] \rightarrow CH3$$

3) CH3 : 받은 메시지를 자신의 비밀키로 해독, CH1에게서 온 메시지인 것을 확인

4) CH3 : CH1을 인식한 후 CH3는 CH1의 공개키로 암호화해서 응답 메시지를 CH1에게 보낸다. 이때, 응답 메시지 안에 받은 N1과 CH3의 신원을 확인할 수 있는 N2를 포함하여 CH1에게 보냄.

$$\text{CH3} \rightarrow E_{CH1_p}[N_1 \| N_2] \rightarrow CH1$$

5) CH1 : N2를 받으면 CH1은 N2를 CH3의 공개 키를 사용해서 암호화한 뒤 CH3에게 보냄.

$$\text{CH1} \rightarrow E_{CH3_p}[N_2] \rightarrow CH3$$

이 절차가 수행되고 나면, 두 클러스터 헤더는 상호 신뢰할 수 있으므로 안전한 통신을 위한 세션을 성립할 수 있다.

6) CH1은 세션키 K_S를 생성하고 자신의 비밀키로 암호화한 뒤 CH3의 공개키로 암호화하여 CH3에게 전달. 이때, CH1의 비밀 키는 전자서명의 역할을 한다. 오직 두 CH 상호간에만 세션 키를 공유할 수 있다.

7) CH3 가 메시지 M을 해독하여 세션 키 K_S를 얻음.

$$\text{CH3} \rightarrow D_{CH1_P}[D_{CH3_R}[M]] = K_s$$

8) CH1과 CH3는 세션키 K_S를 노드 A와 B에게 각각 전달.

9) A 노드는 메시지를 세션키로 암호화 하여 B 노드에게 전송. 암호화 된 메시지 안에는 재전송 공격을 대비하여 메시지 M과 time stamp t_1이 포함한다.

$$\text{Node A} \rightarrow E_{K_S}[M, t_1] \rightarrow B$$

10) B노드는 A로부터 받는 메시지를 복호화 하고, 응답 메시지 R과 함께 time stamp t_2를 세션 키로 암호화하여 A노드에게 전달.

$$\text{Node B} \rightarrow E_{K_S}[R, t_2] \rightarrow A$$

11) 두 노드 간의 안전한 전송이 이루어진 후, 각 노드 A, B는 각각의 CH에게 세션 종료 요청을 하며, CH는 세션 키 K_S를 제거한다.

5. 결론 및 향후 연구 과제

2-tier Ad Hoc 네트워크상에서 기존의 Table-Driven 방식과 On-Demand 라우팅 방식의 한계점을 극복하고, 기존의 3GPP 서비스들과의 연동가능성을 고려하여, 새로운 라우팅 기법(ESR)을 제안하였다. 또한 Threshold cryptography기법을 응용하여 CH가 변질될 경우 신속하게 새로운 CH를 생성하여 네트워크를 재 구성할 수 있도록 LCC[6] 알고리즘을 보완하였으며 제안된 라우팅 기법 위에서 신뢰성을 확보할 수 있는 RSA를 이용한 인증 알고리즘을 제안하였다. 기존의 베이스 스테이션을 기반으로 한 무선 네트워크 환경과 2-tier Ad Hoc 망의 CH들과의 상호 연동 연구와 테스트가 향후 과제이다.

참고 문헌

[1] E. M. Royer and C-K. Toh, " A Review of current Routing Protocols for Ad Hoc Mobile wireless Network" Proc. IEEE Personal Communications ' 99, April. 1999

[2] L. Zhou and Z. J. Haas, " Securing Ad hoc Network " , IEEE Network, Volume 13, No.6, Nov/Dec.1999

[3] Z. J. Haas, " A New Routing Protocol for the Reconfigurable wireless network" , April 1, 2000 http://www.ee.cornell.edu/~jaas/wnl.html,

[4] Charles E. Perkins, Pravin Bhagwat, " Highly Dynamic Destination-Sequenced Distance-vector Routing(DSDV) for Mobile Computers

[5] Charles E. Perkins, E. M. Royer, " Ad hoc On-Demand Distance Vector Routing"

[6] Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, Mario Gerla, " Routing In Clustered Multihop," . Mobile Wireless Networks with Fading Channel" 1997

[7] Y. Desmedt. " Threshold Cryptography" , European Transactions on Telecommunications, 5(4) : 449-457, July □ Aug. 1994

[8] Internet Engineering Task Force, MANET WG Charter, http://www.ietf.org/html.charters/manet-charter.html

[9] J.P. Macker, M.S. Corson, " Mobile Ad Hoc Networking and the IETF" , ACM Mobile Computing and Communications Review, Vol. 3, No. 2, pp. 7-9, April. 1999

[10] The Bluetooth Special Interest Group, Specification of the Bluetooth System, Vol. 1: Core, v1.0 B, Dec. 1999