Ad Hoc 망에서 새로운 다이나믹 하이브리드 라우팅 연구

이현주*, 최문석, 이충세
충북대학교 전자계산학과
e-mail: leehyn2@hanmail.net, bidulgia@hotmail.com,
csrhee@cbucc.chungbuk.ac.kr

A new Dynamic Hybrid Routing Scheme for Ad Hoc Network

Hyun Ju Lee*, Mun Suk Choi, Chung Sei Rhee
Dept. of Computer Science ChungBuk National Univ

요 약

이 논문에서는 기존의 Ad Hoc 네트워크 라우팅 방법중 proactive routing 과 reactive routing 의 장점을 접목시켜 2-tier 계층구조위에서 효율적인 routing 기법을 제안한다. 또한 제한된 tier-2 네트워크에서 기존의 3GPP 서비스와 상호 연동 가능성을 고려하여 네트워크의 형태 변화에 따른 클러스터 헤더의 효율적인 생성 및 안정적인 경로 확보와 함께 클러스터 헤더의 신뢰성을 제공하기 위한 키 분배 메커니즘을 고찰한다.

1. 서론

Ad Hoc 네트워크는 고정된 인프라에 의존하지 않고 이동 호스트들로만 네트워크 구성이 이루어지는 고유한 특성으로 인해 여러 방면에 걸쳐 사용될 수 있는 장점을 가지고 있으며, 이에 대한 많은 연구가 IETF MANET WG 나 Bluetooth Consortium 과 같이 다양한 그룹들에 의해서 이루어 지고 있다[8]. 그러나 모든 네트워크내의 통신이 한정된 자원(resource)의 범위 내에서 수행되어야 하므로 효율적인 이동 Ad Hoc 네트워크 관리를 위해서는 무선 스펙트럼 보존(conservation of wireless spectrum), 전송 전력 최소화(reduction in transmission power)등과 같이 해결해야 할 많은 제약이 있다.

더욱이, Ad Hoc 네트워크의 특성상 구성 형태가 신속하게 변화되기 때문에 최적의 라우팅 경로를 발견하고 관리하는 것이 중요하고 어려운 문제가 된다. 그러므로 Ad Hoc 라우팅 알고리즘은 빈번한 네트워크 형태의 변화에 신속하게 적응할 수 있어야 한다.

Ad Hoc 네트워크를 위한 모든 라우팅 프로토콜의 주요 목표는 두 노드 사이의 정확하고 효율적인 라우팅 경로를 설정하는 것이다. 특히, 라우팅 경로 설정 시에는, 제한된 컴퓨팅 자원(resource)에 대한 에너지 보존과 전송대역 소모량(bandwidth consumption)과 같은 사항들도 고려되어야 할 이슈중의 하나이다.

Ad Hoc 네트워크는 낮은 대역폭과 높은 전송 오류, 그리고 전송 회선의 불안정성 등의 이유로 전통적인 인터넷 라우팅 프로토콜을 직접 사용할 수 없다. 기존의 라우팅 프로토콜을 사용할 경우 주기적인 메시지 교환으로 인한 망의 대역폭 낭비와 망의 동적인 변화를 빠르게 대응하기 어렵다.

Ad Hoc 네트워크는 크게 flat routed 구조와 계층적(hierarchical) 구조로 나눌 수 있다[3].

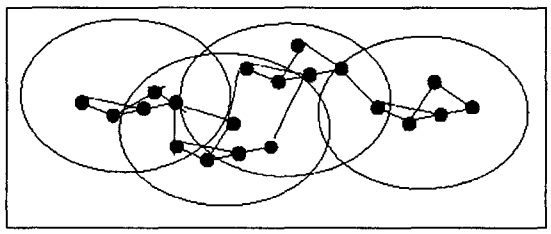

그림1. Flat-routed Ad Hoc 네트워크

네트워크의 각 이동 노드들은 클러스터라 불리는 여러 작은 그룹들로 분할된다. Flat 네트워크에서 모

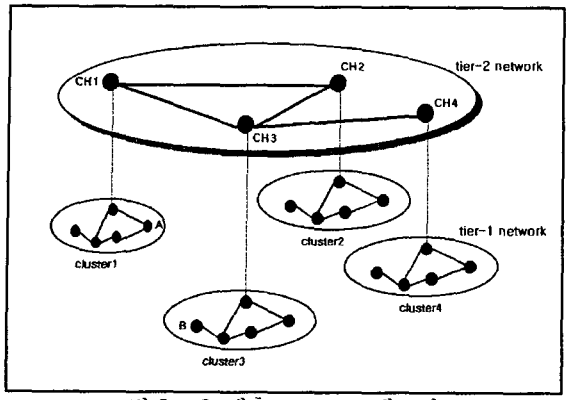

그림 2. 2-계층 Ad Hoc 네트워크

든 이동 노드는 동일한 위치를 가지며 0-tier 계층 구조와 동일한 구조를 가진다. 계층적 구조의 네트워크에서는 각각의 클러스터에 클러스터 헤더(CH)가 있어 클러스터에 소속된 모든 이동 노드들의 중심 노드로서 서버 역할을 수행한다. 계층적 구조의 특성상 이동 노드의 관리(mobility management process)가 쉽다는 장점이 있으나, 두 개의 다른 이동 노드 간의 직접적인 경로가 없으므로 종종 라우팅 경로를 확보하는데 최적 환경이 아닐 수 있다.

반면에, flat 네트워크의 장점은 시작노드(source node) 와 목적지노드(destination node)사이에 다중 경로가 존재한다는 것이며, 이것은 네트워크 혼잡 감소를 돕고, 사용자가 어떤 속성을 갖는 특정의 요구를 만족하는 최적의 경로(route)를 찾을 수 있지만 scalability 특성이 약하다. 또한, 빈번한 노드들의 위치 변화는 라우팅 테이블을 유지하기위한 시간과 에너지와 컴퓨팅 파워의 심각한 낭비를 초래할 수 있다.

2. 관련 연구

2.1 라우팅에 관한 연구(Routing Protocols)

Ad Hoc 네트워크는 크게 Table-Driven 방식(Proactive Routing Protocols)과 Demand-Driven (Reactive Routing Protocols)방식으로 나뉘며 이 두 가지 개념의 장점을 절충한 방식으로 Hybrid 방식이 있다[1].

Table-Driven 방식은 각 이동 노드가 네트워크상의 모든 노드에 대한 경로 설정 정보를 유지하며, 네트워크 형태 변화에 따라 경로 설정 정보를 네트워크 전체로 빈번하게 전파(flooding)하는 방법으로서, 거리-벡터(Distance-vector) 프로토콜 계열이 Table-Driven 방식의 예가 된다. 이 기법들의 장점은 라우팅 경로가 결정될 때 까지 지연시간이 적다는 것이다. 그러나 각 이동 노드의 라우팅 테이블을 모든 노드에게 전파하기 위하여 라우팅 정보를 계속 유지해야 하며, 이에 따른 오버헤드(excessive network capacity)로 인하여 Ad Hoc 네트워크 환경에 적당하지 못하다. 이동 컴퓨팅에서 대역폭과 battery power가 한정된 자원이기 때문에 라우팅 정보를 지속적으로 유지하는 것은 심각한 제한 사항이 된다.

Demand-Driven 방식은 라우팅 경로 설정 절차에 의해 시작노드와 목적지노드사이의 유효 경로만을 전파 탐색(flooding search) 방식에 의해 발견하는 방법으로 필요한 경로 정보만을 유지함으로써 오버헤드를 극복하려는 시도이다. 그러나 단말들이 어떠한 라우팅 정보를 공유하지 않기 때문에 경로 설정 및 재 경로 설정에 따른 많은 지연이 소요되어 실제 real-time 통신에 적용할 수 없다.

위에서 언급한 것과 같이 순수한 Table-Driven 방식과 Demand-Driven 방식은 real-time 통신에 효과적이지 못함을 알 수 있다.

이를 극복하기 위하여 위 두 가지의 개념을 절충한 HRP(Hybrid Routing Protocol)이 있다. 최근 들어 이와 같은 Hybrid 방식이 이동 Ad Hoc 네트워크에 적합한 접근 방법으로 고려되고 있으며 대표적인 HRP로는 ZRP(Zone Routing Protocol)[5]이 있다.

이 프로토콜은 Table-Driven procedure 의 영역을 zone 이라 불리는 한 노드의 이웃노드 들에게만 제한하여, Table-Driven 방식과 On-Demand 방식의 단점들을 보충하기 위하여 제안 되었다.

그러나 현존하는 라우팅 기법만으로는 Ad Hoc 네트워크가 직면한 다양한 문제에 총체적인 해결 방안을 제공하지 못하고 있으며. 제안된 많은 프로토콜들은 실제적인 네트워크상에 적용하는 데 있어 상당한 오버헤드를 가지고 있다. 또한, 현존하는 3 세대 무선 통신망(battery-powered devices) 서비스와 상호 연동이 가능하게 하기위해서 다양한 home 네트워크나 office 네트워크를 위한 차세대 이동 Ad Hoc LAN 환경에 전통적인 라우팅 기법들을 적용하는 것이 부적절하다.

2.2 보안 요소(Security issues)

Ad Hoc 네트워크의 빈번한 형태 변화 특성과 함께 무선 채널을 사용하는 구조적으로 취약한 보안 위협 요소가 존재하므로 Ad Hoc 네트워크 보안 위협요소에 대한 안정적이고 효율적인 극복 방안이 요구된다. 따라서, 보안은 Ad Hoc 네트워크를 구성함에 있어 가장 중요한 이슈 중의 하나이며, 유용성(Availability), 기밀성(Confidentiality), 무결성(Integrity), 인증(Authentication), 부인봉쇄(Non-repudiation)와 같은 요구들을 충분히 만족할 수 있는 프로토콜이 요구된다[2].

2.3 안정적인 Ad Hoc 네트워크를 위한 고려 사항

무선 링크를 사용하는 것과, 제한되어 있는 자원, 물리적인 자원의 제한, 적성 지역에서의 작전수행, 그리고 빈번하게 형태가 바뀌는 네트워크의 특성을 감안할 때 다음과 같은 상황에 대한 충분한 대응책이 요구된다.

- 무선 링크의 사용으로 인한 도청(eavesdropping):
  인가 되지 않은 비밀 정보(secret information)에 접근, 기밀성(confidentiality) 훼손
- 네트워크 외부 적의 공격(active attacks) : 메시지

삭제, 변조.

- 변질된 이동 노드(compromised node)로부터 오는 부적절한 정보 및 공격
- 빈번한 네트워크 형태의 변화를 극복할 수 있는 라우팅 프로토콜

위에서 언급한 바와 같이 각 이동 노드와 각 클러스터내의 이동 노드에 대한 책임을 지고 있는 CH 와의 신뢰할 수 있는 인증 메커니즘을 통해 네트워크 밖의 외부 적의 공격이나 인가되지 않은(unauthorized node) 사용으로 네트워크를 보호할 뿐 아니라, 변질된 노드나 심지어 클러스터 헤더까지 변질되었을 경우에도 이를 발견하고, 변질된 노드를 배제하고서도 효율적인 라우팅과 안전성을 제공할 수 있는 알고리즘이 요구된다.

3. 제안 라우팅(A New Secure Dynamic Routing)

Z.J. Haas 는 re-configurative wireless Network 을 구성시 계층구조를 사용하는데 있어 계층구조를 유지하고 클러스터 헤더 상호 연관을 갖는 것은 네트워크 자원을 너무 많이 사용하기 때문에 flat routed 네트워크를 사용하는 것이 더 적절하다는 것을 주장했지만[3] 본 논문에서는, 효율적인 2-tier 계층적 Ad Hoc 네트워크를 구성함에 있어 상위계층(tier-2)은 proactive 방식을, 하위계층(tier-1)은 reactive 라우팅의 장점을 응용하여, 효율적인 Ad Hoc 네트워크 관리와 함께 경로 설정을 위한 오버헤드와 전송 지연시간을 줄일 수 있는 새로운 라우팅 방법을 제안한다. 이와 함께 제안된 네트워크 상에서 변질된 클러스터 헤더의 발견 시 그 CH(Cluster Header)를 망에서 배제하고 하위(tier-1) 노드중 CH 의 역할을 대체 수행 할 수 있는 CH Re-configuration 알고리즘을 제안한다.

3.1 기존 라우팅 기법의 오버헤드

AODV(Ad Hoc On Demand Distance Vector)는 DSDV(Destination-Sequence Distance-Vector Routing)를 개선한 알고리즘으로서 라우팅 경로가 필요 시에만 새로운 경로를 설정하기 때문에 불필요한 라우팅 경로 요청에 대한 오버헤드를 최소화 할 수 있다. 선택된 경로에 속하지 않은 노드들은 라우팅 정보를 유지하거나 라우팅 테이블 교환에 참여하지 않아도 된다. 한 이동 노드가 다른 노드에게 메시지를 전송하려 할 때, RREQ(a Route Request)패킷을 인접 노드들에게 멀티 캐스트 하고, RREQ 를 받은 노드들은 그들의 인접 노드들에게 메시지를 전송(forwarding) 함으로써 목적한 이동노드를 발견하거나 목적 노드를 알고 있는 중간노드에 도착될 때까지 경로 탐색(a path discovery)를 시도한다.

주위의 인접 노드들에게 각 이동 노드의 정보를 전송하기 위하여 주기적으로' HELLO' 메시지를 local broadcasting 한다.

CGSR(Cluster-head Gateway Switch Routing) 알고리즘은 여러 heuristic routing schemes 을 이용한 클러스터 기반의 다중 홉 이동 무선 네트워킹을 제공한다[7]. 그러나 빈번한 클러스터 헤더의 변화는, 각 이동 노드들이 실제적인 패킷 전송보다 클러스터헤드를 구성하는데 소요되는 오보헤드가 커서 전체적인 라우팅 프로토콜의 성능에 심각한 영향을 줄 수 있다는 단점이 있다.

3.2 새로운 다이나믹 하이브리드 라우팅

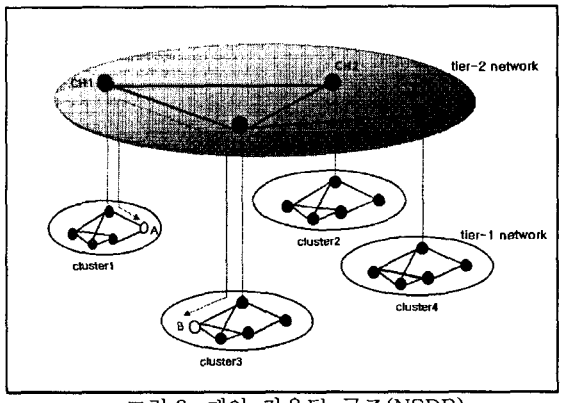

그림 3. 제안 라우팅 구조(NSDR)

본 논문에서 제안하는 Ad Hoc 네트워크에서는 그림 3 과 같이 2 개의 tier 계층이 존재한다. Tier-1 계층에 속한 노드들 중 최소한 한 노드는 상위 계층으로 통하는 게이트웨이의 역할을 수행 하도록 지정된다. 이러한 게이트웨이 노드들은 상위 네트워크를 설립하는데, 이 상위 네트워크는 계산 능력과 자원이 뛰어난 transmitters/receivers 가 요구된다. 동일한 하위계층에 속한 노드들은 AODV[6] 알고리즘을 통해 On-Demand 방식으로 라우팅 경로를 설정하며, 서로 다른 하위 계층에 속한 이동 노드들의 통신에서는 게이트웨이 역할을 수행하는 CH 를 통하여 통신하고자 하는 노드가 속해있는 CH 를 통해 전달되는데, 이때 상위 계층에 속한 노드들은 CGSR 프로토콜을 이용하여[1,7] 네트워크를 구성한다.

이 논문이 제안하는 상위계층의 네트워크는 엄밀히 말해 순수한 CGSR 이라고 볼 수는 없으며, 효율적인 네트워크 관리와 채널 제어(channel access), 대역폭 할당(bandwidth allocation)등을 고려하고, proactive 전략으로 변질된 클러스터헤더를 배제하여, 안전한 라우팅 루트를 설립할 뿐만 아니라, 기존의 3GPP 서비스를 강력한(powerful) CH 와 상호 연동시킬 가능성을 고려하여 제안하였다.

4. CH 재구성(Re-configuration) 알고리즘

2-tier 계층 네트워크 구조에서 각각의 CH 는 하위 계층에 속해 있는 이동 노드들의 라우터 역할과 함께 세션 키를 생성하고 키 관리에 대한 책임을 다른 CH 와 함께 담당한다. 그러므로 한 CH 가 적에 의해 공

격을 당하거나 다른 이동 노드로부터 신뢰를 상실하게 된 경우 이 CH 를 네트워크에서 배제하고, 변질된 클러스터 헤더를 대체할 새로운 CH 를 생성하여 네트워크를 재 구성해야 할 필요가 있다. LCC(Least Cluster Change) 알고리즘[7]의 경우엔 클러스터 헤드를 생성할 경우를 단지 2 가지로 제한하였으나, 변질된 클러스터 헤더가 발견될 경우 안정적인 라우팅을 위하여 우리의 scheme 에서는 LCC 에 3)의 경우를 보완하여 클러스터 헤드를 재생성한다. 다음은 클러스터 헤더를 재생성해야 할 경우이다.

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
3) 시스템이 클러스터 헤더가 변질된 것을 증명할 경우

5. 키 관리(Key Management Service)

우리는 공개키 암호기법의 우수성을 이용하여 라우팅 정보와 데이터 트래픽에 대한 정보를 보호한다. 클러스터 키는 모든 클러스터에 대해 유일하게 존재하고 클러스터에 속하는 모든 이동 노드에게 분배된다. 이 키는 CH 에 의해 생성되어 시스템 공개키로 암호화 되고 클러스터 멤버에게 분배된다. 각 이동 노드는 공개/개인키 쌍을 가지고 있으며, 키 관리를 위한 CA(Certification Authority)를 두어 키의 바인딩과 주기적인 갱신을 담당한다. CA 는 공개/비밀 키 쌍을 가지고 있으며, 공개키는 다른 모든 노드에게 분배되고, 비밀 키를 가지고 인증서를 서명 분배한다. 어떤 한 이동 노드가 더 이상 신뢰할 수 없거나 네트워크 영역을 벗어나게 되면 그 노드의 공개키는 폐지된다.

5.1 Threshold 암호화 기법

CA 는 전체 네트워크에 대한 보안을 책임지는 개체로서 외부 적의 집중적인 공격의 대상이 되므로, 만일 하나의 CA 를 사용하고자 한다면 집중된 외부 공격으로 인하여 CA 가 정상적인 역할을 수행하지 못하거나 혹은 적에게 변질되어 악용될 경우 상당히 심각한 문제를 야기시킬 수 있다. CA 를 이용한 서비스가 사용 가능하지 못하다면, 이동 노드들은 다른 이동 노드들의 현재 공개 키를 획득할 수 없고, 다른 이동 노드들과의 안전한 교신이 불가능하게 된다. 만일 CA 가 적에 의해 변질되어 비밀 키를 적에게 누설 한다면 적은 그 비밀 키를 이용하여 비밀키로 거짓된 인증서를 발행할 수 있게 된다. 이러한 문제점을 해결하기 위하여 우리는 Threshold 기법[4]을 이용하여 시스템 키 관리 서비스의 책임을 각 CH 에게 분할해서 분배하고, (n, t+1) Threshold Cryptography 를 이용하여[2] 2-tier 계층 구조의 중요한 요소인 각 CH 의 신뢰 여부를 확인하며, 클러스터 헤드가 변질된 경우 하위 계층에 속한 이동 노드 중 새로운 클러스터 헤드 역할을 수행할 노드를 신속하게 재생성하여 네트워크를 재구성한다[LCC[7]+3].

6.결론 및 향후 연구 과제

본 논문에서는 기존의 Ad Hoc 네트워크 라우팅 방법중 proactive routing과 reactive routing 의 장점을 접목시켜 2-tier 계층구조위에서 효율적인 routing 기법을 제안하였다. 또한, 제안된 tier-2 네트워크에서 기존의 3GPP 서비스와 상호 연동 가능성을 고려하여 네트워크의 형태 변화에 따른 클러스터 헤더의 효율적인 생성 및 안정적인 경로 확보와 함께 클러스터 헤더의 신뢰성을 제공하기위한 키분배 메커니즘을 고찰해 보았다.

제안된 시스템위에서 최적의 안정적인 라우팅 경로를 확보하면서 기존 무선 네트워크 환경과의 효율적인 상호 연동과 향상된 QoS 제공을 위한 연구가 향후 과제이다.

참고문헌

[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 networks" , IEEE Network, Volume 13, No.6, Nov./Dec. 1999

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

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

[5] Zygmunt J. Haas, Marc R. Pear Lman, Prince Samar, " The Zone Routing Protocol(ZRP) for Ad Hoc Networks-IETF draft" 1997

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

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

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