

Ad-Hoc망과 Internet망과의 연결 방안

진민숙*, 박준희**, 김상하*
충남대학교 컴퓨터 과학과*
한국전자통신연구원**

(badamul, shkim)@ccclab.cnu.ac.kr*, juni@etri.re.kr**

The Mechanism of Interworking Ad-Hoc and Internet Network

Min-Sook Jin*, Jun-Hee Park**, Sang-Ha Kim*
Dept. of Computer Science, Chung-Nam National University*
Electronics and Telecommunications Research Institute(ETRI)**

요 약

Ad-hoc 망은 인터넷과는 다른 독립적인 망을 구성하는 경우 사용되게 된다. 이러한 Ad-hoc의 특정 호스트가 인터넷 망과의 연결을 시도하는 경우, 이 호스트로의 패킷의 라우팅을 위해서는 모든 경로상의 라우터에서 이 호스트에 대한 정보의 엔트리가 추가되어야만 한다. 이는 망 구현 과정에서 확장성(Scalability) 문제를 야기하게 된다. 즉, 라우팅 테이블 엔트리의 증가로 차지하는 라우터의 메모리 문제나, 해당 호스트의 정보를 찾고자 할 때의 소요시간으로 적용하기 어렵다. 이러한 확장성 문제를 제거하는 방법으로 자동으로 주소를 설정 하는 방식인 DHCP(Dynamic Host Configuration Protocol)에 대해서 알아 보았다. 그리고, DHCP의 문제점인 기존의 라우팅 정보를 손실되는 문제가 있어 적용하기 어렵다. 이에 본 논문은 확장성 문제를 제거하는 동시에 액세스 포인트(access point)에서 NAT(Network Address Translation) 기술을 적용하여 AODV(Ad-Hoc On-Demand Distance Vector) 라우팅 프로토콜과 인터넷의 연동을 위한 메커니즘을 제안한다.

1. 서 론

Ad-hoc 네트워크는 기지국(Base Station)과 같은 인프라스트럭처(Infrastructure)가 없는 환경에서 이동노드가 패킷을 목적으로 전송하기 위해 이동노드에 의해 임시적이고 임의적으로 형성되는 네트워크를 의미한다. 이러한 특성으로 인해서 Ad-hoc 네트워크에서는 모든 노드가 라우터 역할을 수행해주어야 한다. 기지국의 기지국이나 라우터가 수행하던 역할이 Ad-hoc 네트워크를 구성하는 노드들에게로 전가된다. 또, Ad-hoc 네트워크는 네트워크의 토폴로지가 상당히 동적으로 변하게 된다. 그러므로, 잦은 링크의 절단을 발생시키고 라우팅을 위해 많은 컨트롤 패킷을 발생시켜서 망의 간섭 및 에러율을 높일 뿐만 아니라, 이동 노드의 취약점인 배터리 소모 문제까지 발생하게 된다. 또한, Ad-hoc 네트워크에서 패킷은 방향성이 없다. 즉, 노드의 전송 방향 내의 모든 노드는 그 노드에서 발송하는 모든 패킷을 받아보게 된다.

Ad-hoc 네트워크는 기존의 무선 네트워크가 가지고 있는 특성을 그대로 이어받는다. 즉, 사용자의 의지에 의해 이동하는 특성, 높은 간섭 및 에러율, 전송 미디어(주파수대역)의 공유 등이 그것이다.

이에, ad-hoc네트워크의 특정 호스트 주소가 인터넷과의 연결을 시도하는 경우, 이 특정 호스트 주소로 패킷이 라우팅이 되어야 한다. 이 때 라우팅을 위해서는 모든 경로상의 라우터에 이 호스트에 대한 엔트리가 추가되어야만 한다. 이는 경로상의 모든 라우터의 라우팅 테이블 엔트리가 상당히 증가된다. 그 결과 이러한 네트워크의 구현 과정에서 확장성이 문제된다. 그러므로, 호스트 주소의 정보가 필요로 하여 검색할 때 시간적 소모가 커지는 문제가 발생된다. 이를 해결하기 위해 자동으로 주소 설정하는 방식인 DHCP를 사용할 경우를 기술해 보고, 이에 따른 문제점을 지적해 보았다.

본 논문에서는 확장성 문제를 제거하는 동시에 액세스 포인트에서 NAT 기술을 적용하여 AODV 라우팅 프로토콜과 인터넷의 연동을 위한 메커니즘을 제안한다. 외부 망의 호스트가 NAT망 내부의 호스트로 연결하지 못하는 단점이 있으나 ad-hoc 네트워크 특성상 문제가 되지 않는다. 우선 2 장에서는 ad-hoc 네트워크의 프로토콜중에서 AODV 프로토콜 메커니즘을 설명하였고, 3 장에서는 DHCP를 설명하였고, 4 장에서는 본 논문에서 제안하는 NAT 메커니즘을 기술하였다. 5 장에서는 NAT를 사용한 AODV와 인터넷과의 연동 메커니즘을 제시한다. 결론과 함께 향후 연구 방향은 6장에서 제시한다.

2 AODV(Ad-Hoc On-Demand Distance Vector)

AODV 라우팅 프로토콜은 Ad-Hoc 네트워크 환경의 이동단말노드에서 사용되어 요구가 있을 때만 경로 설정 절차를 수행하는 On-Demand 라우팅 프로토콜이다. Source routing를 사용하는 DSR과는 다르게 AODV는 Next Hop에 대한 정보만을 관리하며 중간 경로상의 노드에 의해 라우팅 정보가 관리된다. AODV 동작 방식은 사용자의 응용 프로그램에 의해 라우팅 테이블이 검색된다. 만약 라우팅 테이블에서 목적지에 대한 정보를 발견하지 못하면 Path Discovery 과정이 시작된다. Discovery 과정이 수행되는 동안 사용자 응용 프로그램은 중단(block)되어 있다.

2.1 Path Discovery 과정

목적 노드에 대한 경로가 없는 경우 경로를 찾기 위해 이웃 노드들에게 Route Request(RREQ) 메시지를 브로드캐스트

한다. RREQ 패킷은 다음과 같은 필드를 포함하고 있다.
 <src_addr, src_seq_#, broadcast_id, dest_addr, dest_seq_#, hop_count>

RREQ를 전송 받은 이웃 노드는 목적 노드에 대한 경로를 알고 있다면 소스노드에게 Route Reply(RREP) 메시지를 사용하여 경로를 알려준다. 경로에 대한 정보가 없다면 RREQ의 hop_count(hop_count)를 증가 시킨 후 주변 노드에게 다시 브로드캐스팅 한다. 이 과정에서 역 경로와 포워드 경로를 위한 정보를 저장한다. 중복 처리를 방지하기 위해 중간 노드들은 같은 RREQ 메시지를 받았을 경우, 같은 <src_addr, broadcast_id>를 가진 메시지를 받은 적이 있는지 검사한다. 중복된 RREQ 메시지라면 이는 폐기하고 다시 브로드캐스트 하지 않는다.

2.2 Reverse Path Setup

RREQ 메시지에 소스 노드가 가지고 있는 소스 노드의 시퀀스 번호와 목적 노드의 시퀀스 번호가 포함되어 있다. 모든 시퀀스 번호는 RREP 메시지에 의해 목적지에 도달하기 위한 경로가 업데이트 되고, 정보를 관리하기 위해 사용한다.

RREQ 메시지는 주변 노드에게 브로드캐스트 된다. RREQ를 전송 받은 노드는 다음과 같은 정보를 엔트리에 저장한다.

<Destination IP Address, Source IP Address, Broadcast_id, Expiration Time for Reverse Path Route Entry>

목적지에 도달 불가능한 노드도 RREQ 메시지를 전송 받고 역 경로 설정을 위한 엔트리를 저장하게 된다. 이러한 RREQ 메시지는 소스 노드에서 다양한 목적지에 전달 할 수 있다. 이 메시지가 소스 노드로 돌아오게 하기 위해 자동으로 노드는 RREQ 메시지를 처음 전달 받은 이웃 노드의 주소로 Reverse Path 라우트 엔트리에 기록한다.

2.3 Forward Path Setup

RREQ를 받은 중간 경로의 노드는 자신의 시퀀스 번호가 RREQ의 시퀀스 번호보다 크거나 같은 경우에만 응답을 해준다. 만약 RREQ 메시지의 시퀀스 번호가 중간 경로의 시퀀스 번호보다 작다면, 노드는 RREQ를 다시 브로드캐스트 한다.

<source_addr, dest_addr, dest_sequence_#, hop_count, lifetime> RREQ 메시지를 브로드캐스트하는 노드는 목적 노드와의 연결을 위해 역 경로를 설정하고, 각 노드의 역 경로를 RREP 메시지를 수신한 노드에게로 포워드 포인터를 설정한다. 그리고, 소스 노드와 목적 노드에 대한 라우트 엔트리 중 timeout에 관한 정보를 업데이트하고, 요청된 RREQ 메시지 내용 중 목적 노드에 대한 목적지 시퀀스 번호를 기록한다.

목적 노드의 RREP 메시지가 경유하지 않는 경로 상의 노드는 ACTIVE_ROUTE_TIMEOUT 시간이 지난 후 timeout되어 Reverse Pointer는 삭제될 것이다.

RREP 메시지에 포함되어 있는 목적 노드의 시퀀스 번호가 이전의 RREP 메시지의 시퀀스 번호보다 크거나, 같은 목적지의 시퀀스 번호와 작은 hop_count를 가진 경우 라우팅 엔트리를 업데이트 한다. 소스 노드는 최초의 RREP 메시지를 받은 후 곧 데이터를 전송 할 수 있게 되고, 이후 더 좋은 경로를 얻는다면 이를 업데이트하여 경로로 사용 할 수 있다.

2.4 Route Table Management

Reverse Path 라우팅 엔트리는 타이머로 연관되어 있으며 이를 Route Request Expiration Timer라고 부르고, 값은 ad-

hoc네트워크 크기에 따라 결정되고, 목적은 active path에 있지 않은 노드들의 Reverse Path를 제거하는 것이다. 이웃 노드들은 최근의 active_timeout 사이에 목적지로 최소한 하나의 패킷을 보내거나 경로 중간에서 중계를 하는 것을 동작 중이라고 간주한다. 관련된 정보는 모든 노드에서 관리 되고, 정보는 모든 동작 중인 소스 노드들에게 목적지에 도달하기 위한 경로의 링크가 끊어졌음을 알려 줄 수 있다. 이렇게 관심이 있는 목적 노드에 관한 라우트 테이블 엔트리를 관리한다. 각 라우트 테이블 엔트리는 다음과 같은 정보를 포함하고 있다.
 <Destination, Next hop, Number of hops, Sequence number for the destination, Active neighbor for this route, Expiration time of the route table entry>

2.5 Path and Local Connectivity Maintenance

소스 노드가 active session 동안 이동한다면, 목적 노드에 도달하기 위한 새로운 경로를 찾기 위해 다시 Path Discovery 과정이 시작될 수 있다. 목적 노드나 중간 경로의 노드가 이동할 때는 HELLO 메시지를 영향을 받는 소스 노드에게 주기적으로 전송하여 대칭 링크를 확인하고 링크의 결손도 발견 할 수 있다. Hello_interval 시간 동안 노드가 아무런 패킷을 전송하지 않았다면 노드의 이웃들에게 노드의 시퀀스번호가 포함되어 있는 HELLO 메시지가 브로드캐스트 된다. 이 HELLO 메시지는 다시 브로드캐스트 되는 것을 방지하기 위해 1의 TTL(Time To Live)값을 갖는다. HELLO 메시지를 사용한 connectivity 관리는 이웃 노드가 양방향 통신을 가능 하게 하며 이를 유지하기 위해 사용한다.

다음 hop 노드가 도달 불가능해지면, 무한대의 Hop 수와 기존의 시퀀스번호보다 증가된 새로운 시퀀스 번호를 갖는 RREP 메시지를 upstream 방향의 이웃 노드들에게 전송 한다.

링크의 결손 통지를 받았을 때, 그 목적 노드에 대한 경로가 계속 필요한 경우 소스 노드는 Discovery 과정을 다시 시작한다. 이때 상위 프로토콜은 연결이 설정되어 있는 상태로 남아 있게 된다.

3 DHCP(Dynamic Host Configuration Protocol)

구현과정에서의 확장성 문제를 가지고 있는 네트워크에서 자동으로 주소 설정하는 방식인 DHCP를 살펴 보았다. DHCP의 메커니즘은 새로운 장소에서 재부팅 되지 않길 원하는데 재부팅 될 때 Nomadicity가 충분하고, 이동성이 필요하지 않다는 것이다. 그리하여, 잃어버리기 전의 라우팅 정보를 사용할 수 없고, 새로운 라우팅 정보가 생성된다는 문제점이 있다. 이에 NAT를 알아 보았다.

4 NAT(Network Address Translator)

인터넷을 사용하는 컴퓨터들은 인터넷이라는 거대한 네트워크 안에서 단 하나의 유일한 IP 주소를 할당 받게 된다. IP의 고갈과 라우팅에서의 스케일이 계속 커지고 있는 현상 때문에 해결책으로서 생겨난 것이 바로 NAT이다.

NAT의 마스크레이딩(masquerading)은 동적모드(Dynamic mode)로서 일반적으로 내부 사설 IP 클래스가 공인 IP 클래스보다 상위 클래스를 사용하는 경우에 설정될 수 있는 모드이다. 즉, 내부 사설 IP 보다 공인 IP가 부족할 때 유용한 모드이다. 내부 클라이언트에 의해 초기화된 연결 세션이 NAT 라우터의 유일한 포트를 동적으로 할당하기 때문에 여러 사용자가 하나의 동일 공개 IP 주소를 사용하여 인터넷에 접속하는 것이 가능하다.

5 NAT를 사용한 AODV와 인터넷과의 연동 메커니즘

Ad hoc 네트워크는 모든 이동노드가 라우팅 기능을 가지고 있으며, 이동 노드가 패킷을 목적지로 전송하기 위해 이동 노드에 의해 라우팅이 수행되며 이동 노드에 의해 동적인 임시 네트워크를 형성한다.

Ad hoc 노드가 인터넷의 연결을 위해서는 이동성에 대한 다음과 같은 사항을 고려해야 한다.

- 기존의 ad hoc 네트워크의 속성을 유지해야 한다.
- 사용자가 통신하던 세션(session)을 잃지 않아야 한다.
- Ad hoc 노드와 연결을 위하여 액세스 라우터 또는 액세스 포인트에서 ad hoc 프로토콜을 지원해야 한다.
- 액세스 포인트를 통하여 default routing을 통하여 인터넷에 접근 할 수 있어야 한다.

목적지 노드의 IP 주소를 참고하여 이 노드가 ad hoc 네트워크 또는 인터넷에 존재하는지 알 수 없다. Host Prefix 기반의 라우팅을 수행하므로 Network Prefix를 구분할 수 없기 때문이다. 이를 구별하기 위하여 AODV 노드는 먼저 ad hoc 네트워크에 대하여 Path Discovery 과정을 수행한다.

RREQ 메시지에 의해 ad hoc 네트워크에서 목적 노드가 발견되면 Reverse Path와 Forward Path를 사용하여 통신한다. 하지만, RREQ 메시지에 의해 발견되지 않고 RREP 메시지를 받은 경우 default 라우팅 경로를 알고 있다면 이를 사용하여 패킷을 전송한다. Default 라우팅 경로를 갖고 있지 않다면 목적지 IP 주소를 '0.0.0.0' 으로 설정하여 액세스 포인트를 찾기 위한 Path Discovery 과정을 수행한다. Default 라우팅 경로 역시 라우팅 테이블에 의해 관리되며, 경로의 수정 정보를 관리하기 위해 시퀀스 번호를 사용한다. 액세스 포인트는 전력에 대하여 비의존적이므로 ad hoc 네트워크의 노드보다 짧은 주기로 Local connectivity 관리를 수행한다.

AODV 노드는 기본적으로 32bit의 Host Prefix를 가진다. 이처럼 Host Prefix를 갖는 ad hoc 노드를 직접 인터넷이 연결하려면 통신 경로 상의 라우터가 Host Prefix 정보를 알아야 한다. 이는 확장성 문제를 야기하여 현실적으로 불가능하다. 이러한 문제를 해결하기 위해 DHCP를 사용한다.

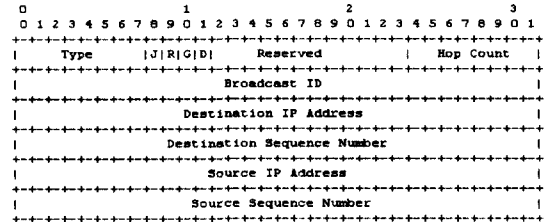
해당 도메인의 DHCP 기능을 가진 액세스 포인트에 접근하여 도메인의 네트워크 Prefix를 갖는 새로운 IP 주소를 할당 받는다. Ad hoc 노드는 이 IP 주소를 사용하여 도메인의 액세스 라우터의 라우팅 테이블을 수정 없이 인터넷에 접근 할 수 있다. 하지만 DHCP를 사용할 경우 ad hoc 노드는 새로운 IP 주소를 할당 받게 된다. IP 주소 변경으로 인하여 ad hoc 네트워크의 속성을 잃게 되며 또한 기존의 세션의 연결을 잃는다. AODV 노드의 경우 새로운 Path Discovery 과정을 수행해야 하며, 기존의 주변 노드들의 라우팅 테이블도 모두 수정되어야 한다.

DHCP의 문제점을 해결하기 위해 액세스 라우터에 NAT 기법을 사용한다. NAT를 사용하면 다음과 같은 장점을 가진다.

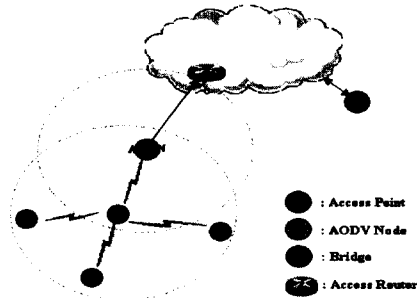
- AODV 노드의 IP 주소를 변경하지 않으므로 기존의 AODV의 속성 및 세션을 유지할 수 있다.
- 액세스 라우터의 라우팅 테이블에 영향을 주지 않으므로 확장성 문제를 야기하지 않는다.
- AODV 노드의 IP 주소에 영향 받지 않고 통신 할 수 있다.

NAT 특성상 외부에서 NAT 내부망으로 접근이 불가능 하다. 하지만 AODV 네트워크의 특성을 고려 할 때, 외부에서 AODV 노드의 서비스를 사용 할 가능성은 매우 적으며, ad hoc 망에서만 주로 사용되므로 AODV와의 연동에 영향을 받지 않는다.

RREQ 메시지에 '0' 필드를 추가하여 RREQ 메시지 브로드캐스트 과정에서 Default 경로를 발견하고 이를 RREP 메시지를 사용하여 전송 받을 수 있게 한다.



RREQ 메시지 형식



6 결론 및 향후 연구 방향

본 논문에서는 Ad-Hoc 네트워크의 특정 호스트가 인터넷 망과의 연결을 시도하는 경우에 발생하는 확장성 문제를 제거하는 동시에 액세스 포인트에서 NAT 기술을 적용하여 AODV 라우팅 프로토콜과 인터넷의 연동을 위한 메커니즘을 제안하였다.

제안된 메커니즘에서 추후 고려할 사항으로는 DSR(Dynamic Source Routing), TORA(Temporally Ordered Routing Algorithm), LAR(Location Aid Routing) 등의 라우팅 프로토콜과 인터넷 연동 방안을 구체적인 방안을 제시할 예정이다.

참고문헌

[1] C.E.Perkins and E.M.Royer, " Ad-hoc On-Demand Distance Vector Routing," Proceedings of 2nd IEE Workshop on Mobile Computing Systems and Applications, Feb. 1999.
 [2] K. Egevang and P. Francis, " The IP Network Address Translator (NAT)," RFC 1631, May 1994.
 [3] U. Jonsson et al, " MIPMANET-Mobile IP for Mobile Ad Hoc Networks," MobiHOC. 2000, 2000. pp.75-85.