이동 애드혹 네트워크 환경에서 AODV를 위한 IPv6 주소 자동 설정

(IPv6 Address Autoconfiguration for AODV in Mobile Ad Hoc Networks)

안 상 현 † 김 영 민 †† 이 영 주 ††
(Sanghyun Ahn) (Youngmin Kim) (Youngju Lee)

요 약 이동 애드 혹 네트워크(Mobile Ad Hoc Networks; MANET)의 장점은 네트워크 인프라의 도움 없이 모바일 노드들이 네트워크 토폴로지를 스스로 구성할 수 있다는 점이다. 그러나 MANET의 이러한 특징을 보다 완벽하게 하기 위해 각 노드들은 자신의 주소도 스스로 설정할 수 있어야 한다. 분리되어 있던 MANET들이 쉽게 병합할 수 있는 MANET 환경에서는 부팅 시에 충돌이 없는 주소를 할당했더라도 병합 후에 주소 충돌이 발생할 수도 있다. 본 연구에서 구현한 주소 자동 설정 프로토콜은 강한 중복 주소 감지(Strong Duplicate Address Detection; Strong DAD)와 약한 중복 주소 감지(Weak DAD)로 구성된다. 이동 노드는 "Strong DAD"를 이용하여 부팅 시에 유일한 주소를 할당하며, 애드 혹 라우팅 과정에서 "Weak DAD"를 이용하여 주소 중복을 감지하고 해결한다. 본 연구에서는 애드 혹 라우팅 프로토콜로서 AODV(Ad Hoc On Demand Distance Vector)를 사용하는 IPv6 기반 MANET 환경에서 동작하는 주소 자동 설정 기법을 구현하고, 테스트베드에서 몇 가지 시나리오들을 통해 본 연구의 구현물이 어떻게 동작하는지를 보여준다.

키워드 : IPv6 주소 자동 설정, 중복 주소 감지, 이동 애드 혹 네트워크, AODV

Abstract An advantage of the mobile ad hoc network (MANET) is that mobile nodes can self-organize the network topology without the help of network infrastructure. However, for the perfect self-organization of the MANET, each mobile node needs to self-configure its address. Even though a mobile node configures a unique address during the booting time, its address may conflict with nodes in other MANETs since MANETs containing the same address can be merged. The address autoconfiguration protocol implemented in this work consists of the strong DAD (Duplicate Address Detection) and the weak DAD. A unique address of a node is assigned by the strong DAD during the booting time and the weak DAD is used to detect address conflict and resolve address conflict during the ad hoc routing. In this work, we have implemented address autoconfiguration in the IPv6-based MANET using AODV as the routing protocol. We describe how the IPv6 address autoconfiguration is implemented and verify our implementation by showing the test scenarios on our testbed.

Key words : IPv6 Address Autoconfiguration, Duplicate Address Detection, Mobile Ad Hoc Networks, AODV

· 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 정보통신부의 유비쿼터스컴퓨팅 및 네트워크원천기반기술개발사업의 지원에 의한 것임

† 종신회원 : 서울시립대학교 컴퓨터과학부 교수
ahn@venus.uos.ac.kr
(Corresponding author임)
†† 학생회원 : 서울시립대학교 컴퓨터과학부
blhole@venus.uos.ac.kr
yjlee97@venus.uos.ac.kr

논문접수 : 2006년 5월 2일
심사완료 : 2007년 1월 31일

1. 서 론

MANET 내의 각 노드들은 네트워크 인프라의 도움 없이 멀티 홉 무선 경로를 스스로 구성할 수 있다. 그러므로 유선 네트워크를 구성하기 어려운 전장이나 긴급 상황뿐만 아니라 가정이나 직장에서도 애드 혹 네트워킹에 대한 관심이 증가하고 있다.

현재 MANET에 대한 대부분의 연구들은 라우팅 관련 연구들이며, IETF 워킹 그룹에서는 AODV[1],

OLSR(Optimized Link State Routing), TBRPF (Topology Dissemination Based on Reverse-Path Forwarding)등이 RFC로 등록되어 있으며 그 외에도 많은 draft들이 라우팅과 관련하여 제출되고 있다. 하지만 MANET 스스로 네트워크를 구성하는 특징을 완성하기 위해서는 경로를 스스로 구성하는 것과 더불어 주소도 자동 설정할 수 있어야 한다. 이동 노드에서 부팅 시에 주소를 자동 설정하더라도 둘 이상의 MANET이 병합할 경우 주소 충돌이 발생할 수 있다. 그러므로 주소 자동 설정 기법은 이러한 주소 충돌도 감지하고 해결할 수 있어야 하고, 또한 충돌이 발생한 주소를 이용해서 이전에 설정된 연결들도 유지할 수 있는 기법이 필요하다.

네트워크 기술의 발달과 편리함을 추구하는 인간의 욕구로 인해 많은 전자 장비들을 네트워크를 통해 제어할 수 있다. 128 비트의 주소공간을 가지고 있는 IPv6 주소를 이용하면 더 많은 전자 장비들에게 유일한 주소를 부여할 수 있으므로 본 연구의 구현에서는 IPv6 주소체계를 사용할 것이다.

본 연구는 "AODV를 위한 애드 혹 IP 주소 자동 설정"[2]을 기반으로 하여 AODV를 위한 IPv6 주소 자동 설정 프로토콜을 설계하고 구현하며, 테스트베드에서 어떻게 동작하는지를 보여준다. [2]에서는 주소 자동 설정을 위한 메시지 형식을 정의하고, 주소 자동 설정 기법을 AODV와 어떻게 통합하는지를 설명한다. 추가적으로 [2]에서는 다루어지지 않은 헬로우 메시지를 이용한 주소 충돌 방지 기법을 제안하며 이를 통해 이웃한 노드의 주소 충돌 여부를 주기적으로 확인 가능하다.

2절에서는 애드 혹 주소 자동 설정과 관련된 연구들을 살펴보고, "AODV를 위한 애드 혹 IPv6 주소 자동 설정"의 설계와 구현, MANET 테스트베드에서의 실험 시나리오를 3절에서 설명한다. 4절에서는 결론을 맺고 향후 연구 과제를 제시한다.

2. 관련 연구

주소 자동 설정 기법은 크게 "주소 정보를 유지하는"(stateful) 기법과 "주소 정보를 유지하지 않는" (stateless) 기법으로 나눌 수 있다. 유선 네트워크에서 흔히 사용하는 DHCP(Dynamic Host Configuration Protocol)[3]는 할당된 주소 정보를 유지하는 기법의 대표적인 방식으로 DHCP 서버가 어떤 주소를 어떤 노드의 인터페이스에 할당했는지를 관리하고 있으므로 주소 충돌이 발생하지 않는다.

노드의 이동이 빈번한 MANET에서는 특정 DHCP 서버에 지속적으로 연결하기도 어렵고 동적으로 변화하는 네트워크에 대한 정보를 유지하고 있는 DHCP 서버를 관리하는 문제도 쉽지 않으므로, 각 노드들이 스스로 자신의 주소를 결정하고 주변의 노드들에게 사용해도 되는지를 문의하는 방식인 "주소 정보를 유지하지 않는" 기법을 사용하는 것이 더 효율적이다. "IPv6 stateless address autoconfiguration"[4,5]은 유선망에서 사용하기 위해 고안된 방식으로 서로 직접 연결된 노드들끼리만 정보를 교환하여 유일한 주소를 설정하는 방법이다.

그러나, "IPv6 stateless address autoconfiguration"은 멀티 홉 네트워크인 MANET에는 적합하지 않으므로 [6]에서는 MANET을 위한 새로운 주소 자동 설정 기법을 제안한다. 이동 노드는 AREQ(Address Request) 메시지에 임의로 선택한 주소를 설정하여 자신이 속한 MANET 내의 모든 노드들에게 브로드캐스트한다. AREQ를 받은 노드의 주소와 AREQ 메시지 안의 주소가 같다면, 그 노드는 AREQ 메시지에 의해 설정된 역경로를 통해 AREP(Address Reply) 메시지를 AREQ 메시지의 발신자에게 전송한다. 또한, AREQ 메시지를 보낸 노드에서 일정 시간이 지나도록 AREP 메시지를 받지 않는다면 해당 주소를 자신의 주소로 설정하여 사용할 수 있다. 하지만, 위의 방법은 노드들이 이동하여 망의 분할과 병합이 발생하는 상황에서는 효력을 발휘할 수 없다.

노드의 네트워크가 활성화되어 최초로 MANET에 조인할 경우에 최초로 주소를 설정하기 위해 사용하는 "Strong DAD"는 정해진 시간 내에 MANET 안에 주소 중복이 있는지를 발견하기 위해 홉 수와 DAD 제어 메시지의 타이머를 이용하는 DAD 기법이다[7]. 그러나 "Strong DAD"는 DAD 제어 메시지 홉 수(또는 TTL)의 범위 밖에 있는 노드들에서 주소 중복이 발생하는지는 알 수 없으며, 일단 주소가 할당된 후 망과 망의 병합에 의한 충돌을 감지할 수 없다. 그러므로 "Strong DAD"에 의해 주소를 설정한 후에 발생할 수 있는 주소 충돌을 해결하기 위해 "Weak DAD"가 제안되었다[7].

"Weak DAD"[7]와 "Passive DAD"[8]는 둘 이상의 MANET들이 병합할 때에 발생할 수 있는 주소 중복도 감지하고 해결할 수 있다. "Weak DAD" 기법에서 이동 노드들은 임의로 선택하거나, 유일한 아이디에 기초하여 생성된 키를 라우팅 제어 메시지에 추가한다. 각 노드들은 주소 자동 설정을 위해 주소와 키의 쌍을 함께 저장하며, 라우팅 제어 메시지를 수신했을 때 자신의 주소와 라우팅 제어 메시지의 발신자 주소는 같지만 키들은 서로 다를 경우에 중복 주소임을 알 수 있다. "Passive DAD"는 인터페이스 키와 같은 추가적인 정보를 필요로 하지 않고 라우팅 제어 메시지에 기본적으로 포함되어 있는 일련번호를 이용하여 주소 중복을 감지할 수 있다.

"Strong DAD"는 아직 주소를 할당받지 못한 노드에

새로운 주소를 부여하고 그 주소와 다른 노드의 주소가 충돌하는지를 검사하는 방법이며, "Weak DAD"는 일단 주소를 가지고 있는 노드에서 망들의 병합시에 발생할 수 있는 주소 충돌을 감지하는 기법이다. "Weak DAD"를 이용할 경우 충돌된 주소를 사용하는 중에 생성된 세션들이 아직도 연결 상태라면 충돌 주소가 새로운 주소로 변경되더라도 해당 상위 계층 세션들을 계속 유지할 수 있어야 한다. 그러므로 MANET 노드가 최초로 자신의 주소를 부여 받고 이후에 지속적인 통신이 가능하기 위해서는 "Strong DAD", "Weak DAD", 상위 계층 세션 유지 기능을 반드시 필요로 한다. 본 연구에서는 "Strong DAD", "Weak DAD", 상위 계층 세션 유지를 포함하는 [2,9,10]에 기반하여 "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 구현하였다. [10]에서는 애드 혹 네트워크 환경에서 주소 자동 설정을 위한 요구사항들을 명시하며, [9]에서는 IPv4, IPv6 주소들을 자동 설정하는 과정을 명시하고, 필요한 메시지 형식들을 정의하며, TCP 세션과 같은 상위 계층 세션들을 어떻게 유지할 것인지에 대해 설명한다.

3. 주소 자동 설정

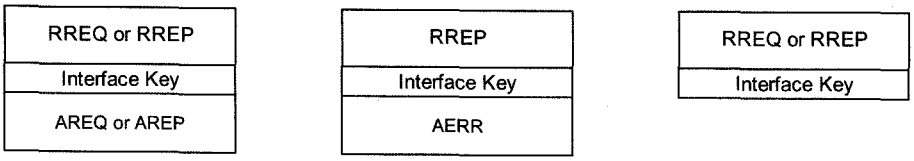
"AODV를 위한 애드 혹 IPv6 주소 자동 설정"은 "Strong DAD"와 "Weak DAD"로 이루어진다. 부팅 시에 노드의 주소는 "Strong DAD"에 의해 할당되며, "Strong DAD"로는 둘 이상의 MANET들이 병합했을 경우에 발생할 수 있는 주소 중복을 감지하지 못하므로 부팅 후에는 "Weak DAD"에 의해 라우팅 제어 메시지를 이용하여 주소 충돌을 감지할 수 있다. "Strong DAD" 과정에서는 임시 주소(Temporary address), 시도 주소(Tentative address), 영구 주소(Permanent address)가 사용된다. 임시 주소는 "Strong DAD"를 수행하는 과정에서 임시로 노드의 주소로 사용되는 주소이며, 시도 주소는 AREQ 메시지에 포함되어 다른 노드들과 충돌이 발생하는지 검사하기 위한 노드의 후보 주소이다. 주소 중복을 검사하기 위한 타이머가 종료될 때까지 어떠한 AREP도 수신하지 않는다면, 시도 주소를 영구 주소로 결정하고 노드의 무선 네트워크 인터페이스에 영구 주소를 설정한다.

이동 노드들이 움직일 경우 그 노드의 주소와 "Strong DAD" 제어 메시지의 홉 수 범위 밖에 있거나, 다른 MANET에 존재하는 어떤 노드의 주소가 서로 충돌할 수 있다. "Weak DAD"는 인터페이스 키를 포함한 라우팅 제어 메시지를 이용하여 이러한 주소 충돌을 감지하고 해결할 수 있다.

이동 노드들은 "Weak DAD"를 수행하기 위해 주소와 인터페이스 키를 이용한다. 이동 노드가 "Weak DAD"에 의해 주소 충돌을 감지하였고, 그 충돌된 주소를 사용하는 중에 생성된 세션들이 아직도 연결 상태라면 충돌 주소가 새로운 주소로 변경되더라도 해당 상위 계층 세션들을 계속 유지할 수 있어야 한다. 본 연구의 주소 변경 기법은 중복된 주소를 내부 IP 헤더의 발신자 주소로 사용하고 충돌이 없는 새로운 주소를 외부 IP 헤더에 설정하는 "IP-over-IP" 터널링에 기반한다 [2,9]. 3.1절에서는 "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 어떻게 설계하고 구현했는지 자세히 설명한다.

3.1 주소 자동 설정의 구현

본 연구에서는 MANET 라우팅 프로토콜로써 NIST의 AODV[11]에 기초하여 IPv6를 위한 AODV를 구현하였으며, "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 리눅스 커널 2.4.21에 구현하였다. 그림 1은 "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 위한 메시지 형식들을 보여주며, 상세한 메시지 형식은 [2,9]에 명시되어 있다. "Strong DAD"는 시도 주소를 포함하는 RREQ-AREQ와 RREP-AREP 메시지들에 의해 수행된다. 경로 설정 과정에서는 "Weak DAD"에 의해 주소 충돌을 감지하며 인터페이스 키를 포함한 RREQ 또는 RREP 메시지를 이용한다. 또한, RREP-AERR 메시지를 이용하여 주소 충돌을 해결할 수 있다. [2]에서는 라우팅 경로를 설정하기 위한 RREQ와 RREP 메시지만을 이용하여 "Weak DAD"를 수행하지만 본 연구에서는 헬로우 메시지를 전달하는 과정에서도 이웃 노드의 주소 충돌 여부를 확인할 수 있다. 이러한 과정을 통해 인접한 노드에 대해서는 주소 충돌을 미리 감지하고 이를 해결할 수 있기 때문에 경로 설정 과정에서 발생할 수 있는 주소 충돌 해결 과정을 줄일 수 있다.



(a) A message for strong DAD (b) A message for weak DAD (c) Control message for AODV

그림 1 AODV를 위한 이동 애드 혹 IPv6 주소 자동 설정을 위한 메시지 형식

IPv6 기반 MANET 내의 통신을 위해서는 특정 64 비트 MANET_PREFIX를 사용할 수 있다. MANET_PREFIX의 일부 공간을 "Strong DAD" 과정에서 사용되는 임시 주소를 위한 MANET_INIT_PREFIX로 사용한다. MANET_INIT_PREFIX를 제외한 MANET_PREFIX의 나머지 주소 영역은 시도 주소로 사용할 수 있다. 노드의 48 비트 MAC 주소는 128 비트 인터페이스 키의 상위 비트들을 채우며, 나머지 하위 80 비트들은 임의의 값으로 설정한다.

"AODV를 위한 애드 혹 IPv6 주소 자동 설정"의 구현은 6개의 모듈들로 구성된다. "Strong DAD" 과정은 RREQ-AREQ와 RREP-AREP 메시지를 처리하기 위한 두 개의 모듈들로 구성되며, 그림 2와 3에서 설명된다. 경로 설정 과정에서 주소 충돌을 감지하고 해결하기 위한 모듈들은 "Weak DAD"를 위해 필요한 모듈들이며, 그림 4와 5에서 설명된다. 또한 상위 계층 세션들을 유지하기 위한 송수신 모듈들이 요구되며, 그림 6과 7에서 설명된다.

그림 2는 "Strong DAD" 과정의 일부로서 RREQ-AREQ 메시지를 어떻게 전송하는지를 보여준다. RREQ-AREQ 메시지를 생성하기 위해 임시 주소와 시도 주소는 그들의 주소 영역 내에서 임의로 결정되며, MANET 전체로 브로드캐스트 한다. 주소 충돌로 인하여 다른 노드로부터 RREP-AREP 메시지를 받은 노드는 새로운 시도 주소를 생성하고 그 주소를 이용한 새로운 RREQ-AREQ 메시지를 전송한다. 모든 시도 주소들이 다른 노드의 주소와 충돌하여 fail_cnt 값이 0이 될 때까지 계속해서 새로운 RREQ-AREQ 메시지를 전송한다면, 그 노드는 영구 주소를 설정하지 못한다. 같은 시도 주소를 갖는 RREQ-AREQ 메시지를 AREQ-RETRIES 만큼 전송하는 동안 어떠한 RREP-AREP도 받지 않는다면, 그 시도 주소를 노드의 영구 주소로 결정한다. 이렇게 같은 시도 주소를 가지고 여러 번 RREQ-AREQ를 전송하는 이유는 동적이고 에러 발생률이 높은 MANET 환경에서 확실하게 주소 충돌을 감지할 수 있도록 하기 위함이다.

"AODV를 위한 애드 혹 IPv6 주소 자동 설정"의 구현에서 메시지들을 다루기 위하여 리눅스 커널의 넷필터(Netfilter)[12]를 이용한다. 노드가 RREQ-AREQ 메시지를 수신하였을 경우, 이 패킷의 중복 수신을 방지하기 위한 정보를 저장한다. 그 후 노드의 주소와 RREQ-AREQ 메시지 안의 시도 주소가 다른지를 검사하여, 다르다면 RREQ-AREQ를 다시 브로드캐스트 하기 위하여 그 패킷을 "event_queue"로 보낸다. 만일 두 주소들이 같다면, 노드는 주소 충돌을 알리기 위하여 RREP-AREP 메시지를 생성하여 RREQ-AREQ 메시지의 발신자에게 전송한다. 이러한 과정들을 그림 3에서 설명한다.

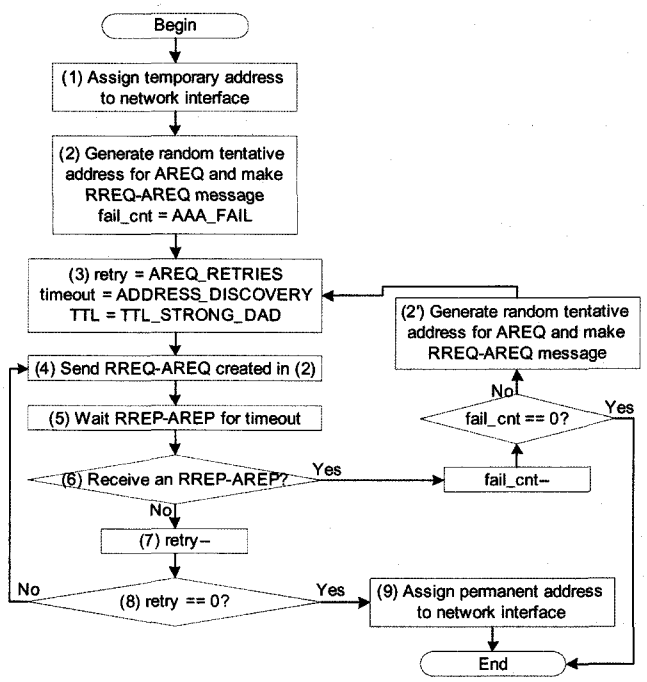


그림 2 처음으로 MANET에 진입한 노드에서의 Strong DAD 과정

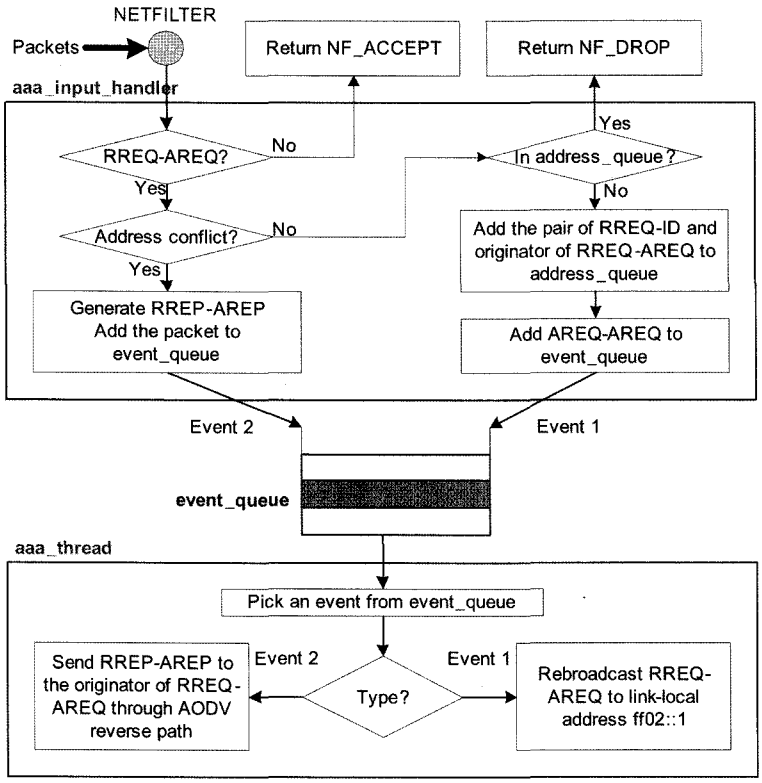


그림 3 RREQ-AREQ 메시지를 수신한 노드에서의 처리과정

AODV 경로 설정 과정에서 주소 충돌을 감지하기 위해 RREQ 메시지를 수신한 노드는 제어 메시지의 발신자 주소와 인터페이스 키 쌍을 자신의 정보나 라우팅 테이블의 정보들 중에서 찾는다. 만일 주소 충돌이 없다면 그 패킷은 정상적인 라우팅 제어 메시지로 처리 되지만, 그렇지 않다면 주소 충돌이 발생했음을 알리기 위해 코드 0을 갖는 RREP-AERR 메시지를 생성하여 "event_queue"로 보낸다. 이러한 과정들은 그림 4에 도식화 되어 있다.

RREP-AERR을 수신한 노드는 그림 5의 과정을 거쳐 주소 충돌을 해결할 수 있다. 노드가 RREP-AERR 메시지의 목적지가 아니면, 다음 홉으로 그 메시지를 전달한다. 그렇지 않다면, RREP-AERR 메시지의 코드에 따라 적절한 처리를 한다. 코드가 0이라면 같은 주소를 가진 노드가 MANET 내에 존재한다는 의미이므로 노드는 "Strong DAD"에 의해 자신의 주소를 변경한다. 추가적으로 이전 주소를 이용해 통신 중인 세션들을 유지하기 위해 코드 1을 포함한 RREP-AERR 메시지를 전송하여 자신과 통신하고 있던 노드들에게 새로운 주소를 알린다. 코드가 1인 RREP-AERR 메시지를 수신한 노드는 그 메시지의 발신자 주소가 변경된 것을 알 수 있고, "IPv6-over-IPv6" 터널링을 통해 이전 세션들을 보존하기 위해 주소 맵핑 캐쉬(address mapping cache)인 "address_map_cache"에 이전 주소와 새로운 주소 쌍에 대한 정보를 추가한다. 또한, 코드 1을 포함한 RREP-AERR 메시지를 수신한 노드들은 주소 변경에 대한 정보를 수신했으며, 새로운 발신자의 주소를 이용하여 통신할 준비가 되었음을 알리기 위해 그 패킷의 발신자에게 코드 2를 가진 RREP-AERR 메시지를 전송해야만 한다. 그림 6과 7에서는 송수신 노드에서 상위 계층 세션을 유지하기 위한 터널링이 어떻게 이루어지는지를 보여준다.

3.2 테스트베드 구축 및 실험

구현된 "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 실험하기 위해 레드햇 9.0에 리눅스 커널 2.4.21을 설치한 노트북 4대를 이용한다. 시도 주소는 임의의 값으로 설정되어야 하지만, 의도적으로 주소 충돌을 발생시키기 위해 정해진 시도 주소를 설정할 수 있도록 하였다.

그림 8에서 노드 B와 C는 이미 주소를 설정하고 있지만, 노드 A는 아직 주소를 설정하지 않은 상태이므로 노드 A는 "Strong DAD"를 통해 주소를 설정한다. 노

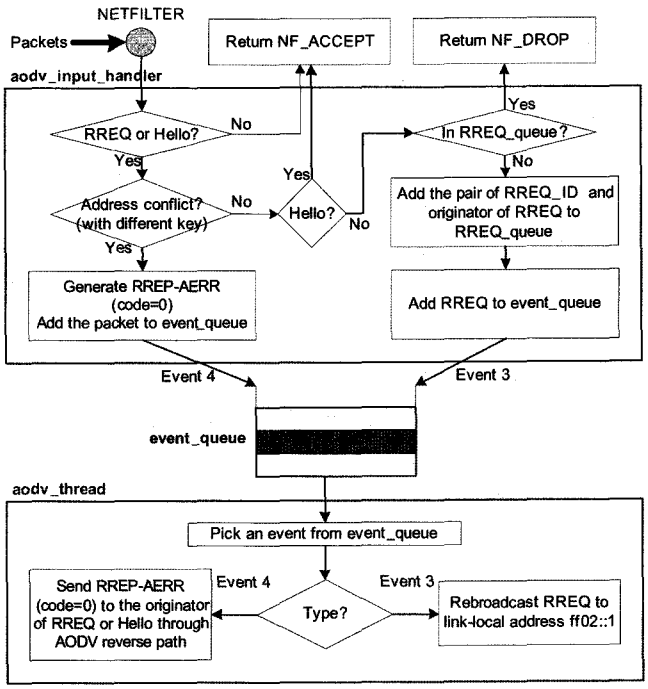


그림 4 경로 설정 중의 weak DAD 처리과정

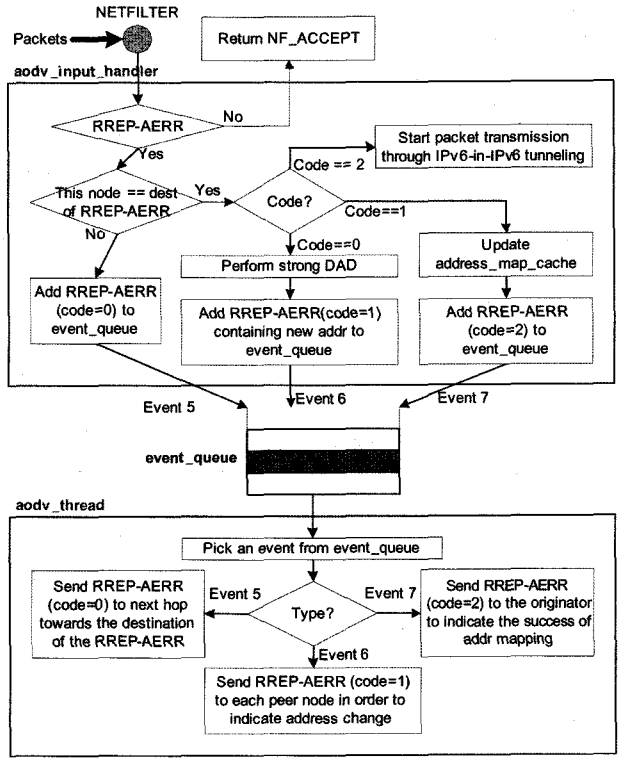


그림 5 RREP-AERR 메시지를 수신한 노드에서의 처리과정

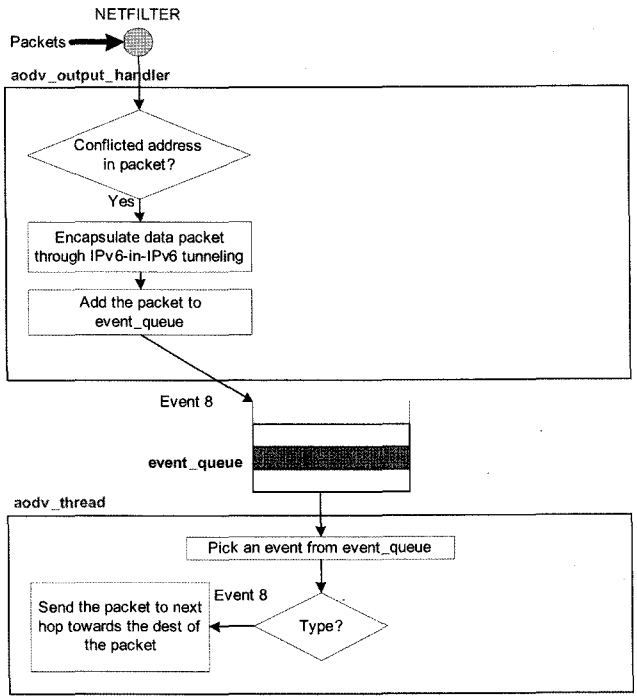


그림 6 송신 노드에서의 인캡슐레이션

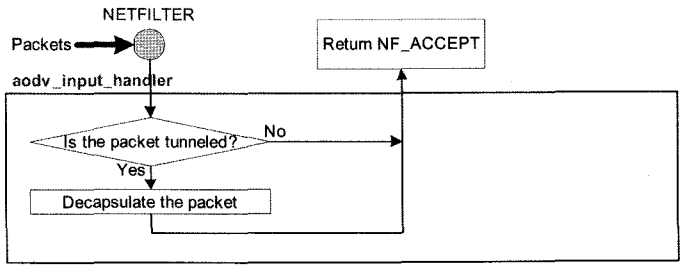


그림 7 수신 노드에서의 디캡슐레이션

드 B와 C는 헬로우 메시지를 서로 교환하여 이미 상대방에 대한 라우팅 경로가 설정되어 있다. 노드 A는 노드 C의 주소와 같은 ADDR3을 시도 주소로 선택하여 RREQ-AREQ 메시지를 브로드캐스트 한다. 노드 B는 노드 C에 대한 정보를 가지고 있으므로 RREQ-AREQ 메시지를 수신하였을 때 주소 충돌을 감지할 수 있다.

수신한 RREQ-AREQ 메시지의 시도 주소와 같은 주소를 갖지만, 인터페이스 키가 다른 경로 엔트리(ADDR3, ADDR3, KEY3)가 노드 B의 라우팅 테이블에 존재하므로, 노드 B는 노드 A에게 RREP-AREP 메시지를 전송한다. 이 메시지는 노드 A와 C에게 전달되지만, 노드 C에서는 인터페이스 키가 다르므로 그 패킷을 무시한다. 이 패킷을 수신한 노드 A는 새로운 시도 주소를 포함한 RREQ-AREQ를 전송하며, 타이머가 종료할 때까지 RREP-AREP 메시지를 수신하지 않는다면 같은 시도 주소를 가진 RREQ-AREQ 메시지를 전송한다. 같은 시도 주소를 가진 RREQ-AREQ 메시지를 3번 전송할 동안 한 번도 RREP-AREP를 수신하지 않는다면, 시도 주소를 영구 주소로 설정한다.

그림 9에서는 MANET 1의 노드 A와 MANET 2의 노드 C가 같은 주소를 가지고 있는 상황에서 MANET 1과 MANET 2가 병합될 경우, "Weak DAD"를 통해 주소 충돌을 감지할 수 있는 시나리오를 보여준다. 노드 C가 노드 B의 전파 범위에 진입한 후, 두 노드들은 헬로우 메시지를 교환하고 노드 B는 노드 A와 C의 주소 충돌을 감지할 수 있다. 그러므로 노드 B는 노드 C에게 코드 0을 포함한 RREP-AERR 메시지를 전송하고, 노드 C는 새로운 주소를 선택하기 위해 "Strong DAD"를

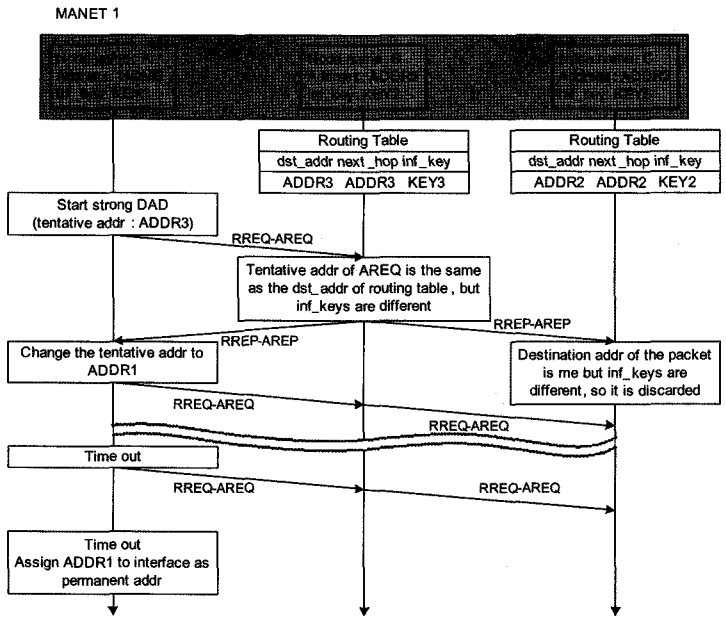


그림 8 Strong DAD의 동작을 확인하기 위한 실험

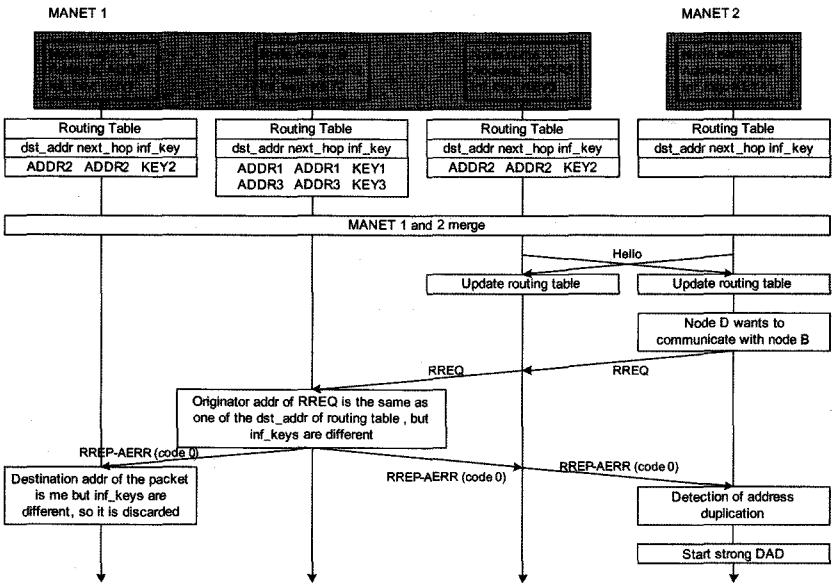


그림 9 두 MANET들이 병합할 경우 weak DAD의 동작을 확인하기 위한 실험 (RREQ 메시지 이용)

수행할 수 있다.

그림 10의 실험 시나리오에서는 노드 A, B, C로 구성된 MANET 1과 노드 D로 구성된 MANET 2가 있으며, 노드 A와 D의 주소가 같다. 노드 C와 D는 두 MANET이 병합한 후에 헬로우 메시지를 교환하여 그들의 라우팅 테이블을 갱신한다. 노드 B와 통신하기 위해 노드 D가 인터페이스 키를 가진 RREQ 메시지를 브로드캐스트 한다면 노드 A에 대한 정보를 알고 있는 노드 B는 주소 충돌을 감지할 수 있고 코드 0를 포함한 RREP-AERR을 노드 D에게 전송한다. 이를 수신한 노드 D는 "Strong DAD"를 이용하여 새로운 주소를 설정한다.

본 절에서는 구현한 "AODV를 위한 애드 혹 IPv6 주소 자동 설정" 기법이 정상적으로 동작함을 보였다.

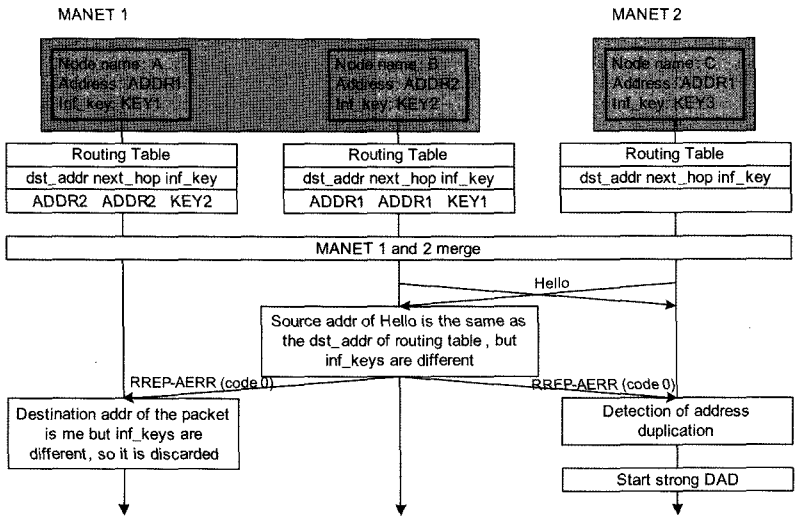


그림 10 두 MANET들이 병합할 경우 weak DAD의 동작을 확인하기 위한 실험 (헬로우 메시지 이용)

그러나 리눅스 커널 2.4.21에서는 IPv6 주소를 위한 터널링 기법을 지원하지 않으므로 상위 계층 세션들을 유지하는 모듈들은 구현하지 못했다. 이로 인하여 본 구현에서는 주소 충돌에 의해 주소를 변경하게 될 경우 기존에 연결되어 있던 세션에 대해서는 해당 세션을 끊고 새로 부여받은 주소로 다시 연결을 해야 한다.

4. 결론 및 향후 연구 과제

본 연구에서는 AODV를 라우팅 프로토콜로 사용하는 MANET 안의 노드들이 스스로 주소를 설정할 수 있도록 하는 "AODV를 위한 애드 혹 IPv6 주소 자동 설정"을 설계하고 구현하였다. 이동 노드는 "Strong DAD"를 이용하여 부팅 시에 자신의 주소를 자동으로 설정하고 애드 혹 라우팅 과정에서 "Weak DAD"와 "IPv6-over-IPv6" 터널링에 기반한 주소 전환 기법을 이용하여 주소 충돌을 해결할 수 있다. 또한 실험을 통해 "Strong DAD"와 "Weak DAD"가 잘 동작하는 것을 보였다.

향후 연구 과제로 인터페이스 키와 같은 추가 정보 없이도 경로 설정 과정에서 주소 충돌을 감지하고 해결할 수 있는 "Passive DAD"를 추가로 구현해야 하며, RREQ나 RREP와 같은 라우팅 제어 메시지와 AREQ나 AREP와 같은 주소 자동 설정을 위한 메시지들 사이의 중복된 정보를 제거하여 전체 메시지의 크기를 줄이는 방법을 연구할 것이다.

참 고 문 헌

[1] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003.

[2] J. Jeong et al., "Ad Hoc IP Address Autoconfiguration for AODV," Internet draft, draft-jeong-manet-aodv-addr-autoconf-01.txt, July 2004.

[3] R. Droms, "Dynamic host configuration protocol," RFC 2131, Mar. 1997.

[4] T. Narten, E. Nordmark and W. Simpson, "Neighbor Discovery for IP version 6," RFC 2461, Dec. 1998.

[5] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462, Dec. 1998.

[6] C. Perkins et al., "IP Address Autoconfiguration for Ad Hoc Networks," Internet draft, draft-ietf-manet-autoconf-01.txt, Nov. 2001.

[7] N. Vaidya, "Weak Duplicate Address Detection in Mobile Ad Hoc Networks," In Proc. MobiHoc 2002, June 2002.

[8] K. Weniger, "Passive Duplicate Address Detection in Mobile Ad Hoc Networks," In Proc. IEEE WCNC 2003, March 2003.

[9] J. Jeong et al., "Ad Hoc IP Address Autoconfiguration," Internet draft, draft-jeong-adhoc-ip-addr-autoconf-04.txt, Feb. 2005.

[10] J. Jeong et al., "Requirements for Ad Hoc IP Address Autoconfiguration," Internet draft, draft-jeong-manet-addr-autoconf-reqts-04.txt, Feb. 2005.

[11] Kernel AODV, http://w3.antd.nist.gov/wctg/aodv_kernel/

[12] Netfilter, http://www.netfilter.org/

안 상 현

1986년 서울대학교 컴퓨터공학과 졸업(학사). 1988년 서울대학교 대학원 컴퓨터공학과 졸업(석사). 1989년 9월~1993년 12월 University of Minnesota 컴퓨터학과(박사). 1988년 1월~1989년 8월 (주) 데이콤 연구원. 1994년 3월~1998년

2월 세종대학교 컴퓨터학과 교수. 1998년 3월~현재 서울시립대학교 컴퓨터과학부 교수. 관심분야는 애드혹 네트워크, 센서 네트워크, 홈 네트워크, 이동 통신, 라우팅 프로토콜 등

김 영 민

1999년 2월 서울시립대학교 컴퓨터·통계학과 졸업(이학사). 2001년 2월 서울시립대학교 컴퓨터·통계학과 졸업(이학석사). 2007년 2월 서울시립대학교 컴퓨터·통계학과 졸업예정(이학박사). 관심분야는 멀티홉 애드혹 네트워크에서의 라우팅, 유무선 통합망

이 영 주

2004년 2월 서울시립대학교 컴퓨터·통계학과 졸업. 2004년~현재 서울시립대학교 컴퓨터·통계학과 석사과정. 관심분야는 애드혹 라우팅, 주소자동설정