Journal of Korea Multimedia Society Vol. 12, No. 8, August 2009(pp. 1099-1108)

MANET 환경에서 중복 주소 탐지에 대한 DoS 공격을 방지하는 보안 기법과 성능 평가

임정미[†], 박창섭[††]

요 약

MANET(Mobile Ad Hoc Network) 상에서 IP 주소 할당에 관한 연구는, 특정 노드가 다른 노드들의 IP 주소를 모니터링 하여 할당하는 Stateful 방식과, 노드 스스로 IP 주소를 생성하는 Stateless 방식이 있다. MANET 상의 노드들은 이동성과 제한된 자원의 특성으로 노드 스스로 IP 주소를 생성하는 Stateless 방식이 더 적합하다. 그러나, Stateless 방식에서는 중복되지 않는 주소를 할당하기 위한 DAD(Duplicate Address Detection)과정이 필요하고, 이 과정에서 DoS(Denial of Service) 공격이 발생할 수 있다. 본 논문에서는, MANET의 특성에 맞춰 계산량이 적게 드는 일방향 해쉬 함수를 이용하여, DAD과정에서 발생할 수 있는 DoS 공격을 방지하는 보안 기법을 제안한다. 그리고, NS2를 이용하여 기존의 서명을 이용한 CGA(Cryptographically Generated Addresses) 방식과 비교, 성능평가 한다.

A Security method and Performance evaluation of preventing DoS attack against DAD in MANET

Jeong Mi Lim[†], Chang Seop Park[††]

ABSTRACT

The study of IP address allocation in MANET can be categories into Stateful and Stateless. The one, special node monitors other nodes' IP address and allocates IP address. And the other, node generates IP address by itself. Nodes in MANET have mobility and restricted resource, so Stateless is more suitable than Stateful. But, in Stateless, node requires DAD process because of unique IP address allocation. And Dos attack can be happened in DAD precess. In this paper, we propose a security method on preventing DoS attack against DAD in MANET using one-way hash function. Since, Computation of one-way hash function is suitable for nodes' restricted resource character in MANET. And we evaluate performance using NS2 and compare with other security method which is CGA using signature.

Key words: MANET(모바일 애드 혹 네트워크), IP auto-configuration(IP 자동 할당), DAD(주소중복탐지), DoS attack(도스공격), CGA(암호화 주소 생성)

1. 서 론

MANET은 무선 노드들로만 구성된 하부 구조가 없는 네트워크 형태를 말한다. 이러한 네트워크의 형태는 무선 노드들로만 구성되어 있기 때문에 네트워크의 설정이 쉽고, 노드들이 쉽게 이동할 수 있는 장점을 갖고 있다. 그러나 그림 1과 같이 데이터를 송신하는 소스 노드의 전송 범위 안에 데이터를 수신하는 목적지 노드가 존재할 경우에는 상관없으나, 그림 2와 같이 목적지 노드가 소스 노드의 전송 범위를 벗

※ 교신저자(Corresponding Author) : 임정미, 주소 : 충남 천안시 안서동(330-714), 전화 : 041)550-3460, FAX : 041) 550-3460, E-mail : redpig3@dankook.ac.kr
접수일 : 2009년 2월 13일, 완료일 : 2009년 5월 18일

[†] 정회원, 단국대학교 교양학부 강의전임 강사
[††] 정회원, 단국대학교 컴퓨터과학과 교수
(E-mail : csp0@dankook.ac.kr)

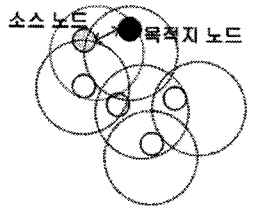


그림 1. 같은 영역

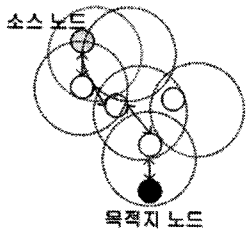


그림 2. 다른 영역

어나 있을 경우, 중간 노드들이 데이터를 전달해주어야 하므로, 각각의 노드가 호스트 역할과 라우터의 역할을 동시에 한다. 이러한 MANET 환경의 특성에서, 무선 노드들은 배터리, 메모리, 저장 공간 등의 자원이 제한적이며, 동적인 이동성으로 인하여 MANET 환경에 무선 노드가 갑자기 참여하거나, 위치를 벗어날 경우 데이터 전송이 어렵다는 단점이 있다.

네트워크 상의 모든 노드들은 통신을 위하여 각각의 노드를 식별하기 위한 중복되지 않는 유일한 IP주소를 갖고 있어야 한다. 기존의 일반 유선 네트워크에서는 DHCP(Dynamic Host Configuration Protocol)[1] 서버가 참여하고 있는 노드들에게 IP 주소를 할당한다. 그러나 MANET 환경에서는 이동성과 제한적인 자원의 특성으로 인하여, 특정 노드에게 역할을 부여하는 중앙 집중적인 방식은 적합하지 않다.

MANET에서의 IP 주소 할당에 관한 연구는 크게 두 가지가 있다. 첫째, 일반 유·무선 네트워크 환경에서와 같이 DHCP[2]와 같은 중앙 집중적인 서버에서 노드의 IP 주소를 할당해주는 방식이 있다. 둘째, 노드 스스로가 IP 주소를 할당하는 방식으로, 이 방식은 전자의 방식보다, 이동성과 제한된 자원의 특성을 갖고 있는 MANET 상의 노드들에게 더 적합한 방식이다. 그러나, 노드 스스로가 IP 주소를 생성할 경우 이미 다른 노드들이 같은 IP 주소를 사용하고 있는지 확인하는 DAD (Duplicate Address Detection) 과정이 필요하다. 이러한 DAD 과정에서 악의적인 노드에 의해서 거짓된 중복 주소 사용 메시지를 반복적으로 전송하여 DoS 공격이 발생 할 수 있다.

본 논문에서는 IP 주소 할당 방식 중, MANET의 특성에 적합한 후자의 방식을 이용하여 노드 스스로 일 방향 해쉬 함수를 이용하여 IP 주소를 생성하는 방식을 제안한다. 그리고, 중복되지 않은 주소를 할당하기 위한 DAD 과정에서 발생할 수 있는 DoS 공격을 방지하는 방식을 제안하고, NS2로 기존의 CGA방식[3] 을 이용하여 주소를 생성한 방식과 본 논문에서 제안하는 방식을 시뮬레이션하여 DAD 과정의 처리 시간과, 발생하는 메시지 전송 개수의 오버헤드를 비교 성능평가 한다.

본 논문의 구성은 2장에서 기존의 IP 주소 할당 방식을 소개하고, 3장에서는 2장에서 소개한 방식들의 단점을 고려하여 IP 주소의 충돌과 DoS 공격[4]을 탐지하는 방식을 제안하고, 4장에서는 기존의 방식과 제안하고 있는 방식을 비교 분석하였다. 또한, NS2를 이용하여 기존의 방식 중 CGA를 이용한 방식과 제안하고 있는 방식을 실험하여 비교 성능평가를 하고 5장에서 결론을 맺는다.

2. MANET의 IP 주소 할당 방식과 보안 이슈

2.1 MANET의 IP 주소 할당 방식

MANET에서의 IP 주소 할당 방식은 크게, 특정 노드가 다른 노드들의 IP 주소를 모니터링 하여 할당하는 Stateful 방식[5-9]과, 노드 스스로 IP 주소를 생성하는 Stateless 방식[10-13]으로 나뉜다.

2.1.1 Stateful 방식

MANTConf 방식[8]은 중앙 집중적인 DHCP 서버의 역할을 분산한 방식으로 그림 3과 같다. Request 노드는 MANET에 참여하려는 노드이고, Initiator 노드는 Request 노드를 대신하여 DAD 과정을 처리하는 노드이다. Requester 노드는 이웃 노드들에게 Initiator 노드를 선정하기 위한 Neighbor_Query 메시지를 브로드캐스트하여 그 중에 응답이 오는 노드 중에 하나를 Initiator 노드로 선택을 하는 방식이다. Initiator 노드는 사용하지 않는 IP 주소 리스트를 소유하고 있으며, 주소 리스트에 있는 하나의 주소를 선택하여 MANET상의 다른 노드들에게 IP

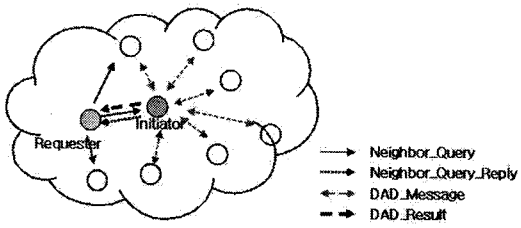


그림 3. MANETConf

주소 중복을 탐지하기 위한 DAD_Message를 주고 받는다. 만약 중복된 IP 주소를 사용하는 노드가 있다면, 자신의 IP 주소 리스트를 갱신하고, 다른 IP 주소를 선택하여 같은 과정을 반복한다. Initiator 노드는 이러한 DAD 과정의 결과로 중복되지 않는 IP 주소를 할당하여, Requester 노드에게 전달한다. 그러나 이 방식은 모든 노드들이 Initiator 노드가 될 수 있으므로, 모든 노드들이 네트워크상의 사용 중이지 않은 IP 주소를 수집, 리스트를 갖고 있어야만 한다. 그러므로 사용 중이지 않은 IP 주소를 찾기 위한 추가적인 작업으로 인한 오버헤드와 사용하지 않는 IP 주소 리스트를 유지하기 위한 추가적인 저장 공간이 요구된다.

에이전트 기반의 방식[7]은 IPv6 주소의 서브넷 ID 부분인 상위 64비트 중 16비트 부분을 주소 에이전트의 MAC 주소로 생성하고, 하위 64비트는 주소를 요청하는 노드의 MAC 주소로 생성한다. 이때, 주소 에이전트는 MANET 상의 모든 노드들의 주소 리스트를 유지해야 하며, 주소 리스트는 IPv6의 주소와 연결되는 MAC 주소를 포함하여야 한다. 또한, 48비트의 MAC 주소를 64비트의 형태로 변경하는 과정에서 중복될 수 있으므로 DAD과정이 필요하며, 주소 에이전트를 선택하는데 추가 과정이 필요하다.

그 외에도 주소 기관(AA: Address Authority)을 이용하는 방식[9]은 네트워크 상태 정보를 유지하는 주소 기관을 MANET의 이동성과 제한된 자원의 특성 때문에 PAA(Primary Address Authority)와 BAA(Backup Address Authority)로 구분한다. PAA는 네트워크 상태 정보유지 때문에 주기적으로 모든 노드들에게 Network Identifier Advertisement 메시지를 전송해야하는 단점이 있다.

2.1.2 Stateless 방식

랜덤 주소를 선택하는 방식[14]으로 IPv4에서 특정 영역인 169.254/16에서 랜덤하게 하나의 IP 주소를 선택하고, 이 IP 주소가 네트워크에 참여중인 다른 노드와 충돌이 되는지 확인하기 위하여 참여 노드는 AREQ(Address Request) 메시지를 브로드캐스트 하고, 같은 IP 주소를 사용하고 있는 노드는 참여 노드에게 중복된 IP 주소를 사용하고 있음을 알리는 AREP(Address Reply) 메시지를 유니캐스트 한다. 참여 노드는 2~3회 같은 AREQ 메시지를 브로드캐스트하고, 일정 시간이 지난 후에도 AREP 메시지가 없을 경우 중복되는 IP 주소가 없는 것으로 간주하고 사용한다. 만약, AREP 메시지가 있을 경우 다른 IP 주소를 선택하여 같은 과정을 반복한다.

MAC 주소를 이용하여 IP 주소를 생성하는 방식[6]은 각각의 노드들이 다른 유일한 IP 주소를 갖고 있어야 한다는 가정에서 제안되었지만, 사실상 네트워크 인터페이스 카드를 만드는 제조 과정에서 중복의 가능성이 있고, 명령어를 이용하여 MAC 주소의 변경이 가능하므로 적합하지 않다.

리더 노드를 이용하는 방식[11]은, 참여하는 노드가 리더 노드가 되고, 리더 노드는 가장 높은 IP주소를 갖는다. 리더 노드는 이웃 노드들에게 주기적으로 자신의 IP 주소를 포함한 hello message를 전송한다. 이를 받은 각 노드들은 리더 노드의 주소인 가장 높은 IP 주소를 저장한다. 이 방식은 악의 적인 노드가 가장 큰 IP 주소를 선택하여 반복적으로 hello message를 전송할 경우, DoS 공격이 발생하여 참여하고자 하는 노드는 정상적으로 IP 주소를 할당받을 수 없다. 또한, 중간 값의 IP 주소를 가진 노드가 네트워크에서 사라질 경우 그 노드가 사용하던 IP 주소를 재사용할 수 없다.

안전한 호스트 방식[15]은, 참여 노드의 인증 과정과, IP 주소의 할당 과정으로 나뉜다. 참여 노드와 네트워크상의 노드들은 자신의 개인키, 공개키 쌍을 갖고 있고, 난수를 생성하여 시도-응답 과정을 거쳐 상호 인증한다. 참여 노드를 인증한 이웃노드는 자신이 갖고 있는 주소 리스트의 반을 참여 노드에게 나눠주어 IP 주소를 할당한다. 이때, 악의적인 노드가 여러 개의 식별자를 가지고 요청 메시지를 반복적으로 보낼 경우 DoS 공격이 발생한다. 또한, 이 방식은 PKI 방식을 사용하므로 인증기관이 필요하고, 서명으로 인하여 계산양이 많이 발생하는 단점이 있다.

키 값과 결합하는 방식[16]은, IP 주소와 키 값을

결합하여 생성하여 IP 주소의 충돌을 줄인다. 그러나, IP 주소와 함께 키 값만큼 첨부되는 메시지의 길이가 길어지고, 데이터를 전송하기 위해서는 IP 주소뿐만 아니라 키 값까지 알고 있어야한다. 또한, 노드가 네트워크상에서 사라질 때, 사용 중이던 IP 주소는 다시 사용이 가능하나, 새로운 참여 노드는 키 값을 다시 생성 하므로, 기존의 네트워크 상의 노드들은 키 값을 갱신하여 라우팅 테이블을 갱신 하여야 하는 단점이 있다.

2.2 보안 이슈

2.1에서의 기존의 연구들을 통하여, MANET 환경에서는 Stateful 방식보다는 Stateless 방식이 적합하나, 노드와 IP 주소의 소유가 명확하지 않아 DAD 과정의 요청, 응답 메시지에서 DoS 공격이 발생함을 알 수 있다.

MANET에서 DAD 과정에서 요청·응답 메시지는, AREQ(Address Request), AREP(Address Reply) 메시지를 사용한다. 네트워크에 참여하려고 하는 노드를 참여 노드라 하고, 중복된 IP 주소를 사용하고 있는 노드를 충돌 노드라 할 때, 참여 노드는 AREQ 메시지를 브로드캐스트하고, 충돌 노드는 AREP 메시지를 참여 노드에게 유니캐스트 한다. 참여 노드는 같은 AREQ 메시지를 2~3회 반복 전송하고, 일정 시간이 지난 후에도 AREP 메시지가 없으면 충돌 노드가 없는 것으로 간주하여 할당한 IP 주소를 사용한다. 그렇지 않고, AREP 메시지를 수신하게 되면 다시 새로운 IP 주소를 할당하여 위의 과정을 반복한다.

이때, 악의적인 사용자가 같은 IP 주소를 사용하고 있다고, 거짓된 AREP 메시지를 반복적으로 보낼 경우 DoS 공격이 발생하여, 참여 노드는 IP 주소를 할당받지 못할 수 있다. 즉, 노드와 노드의 IP 주소와의 소유 관계가 명확하지 않아 DoS 공격이 발생하므로, 노드와 노드의 IP 주소의 소유권 문제를 해결하여 정당한 사용자만이 AREP 메시지를 전송할 수 있도록 해야 한다.

IP 주소 소유권 문제를 해결하기 위한 방법 중 하나는 CGA 방식[3]으로 그림 4와 같다. 참여 노드의 공개키와 개인키를 각각 PK, SK라 하고 일 방향 해쉬 함수를 Hash(), 개인키로 서명하는 것을 Sign_SK로 나타낼 때, 128비트로 구성된 IPv6의 하위 64비트

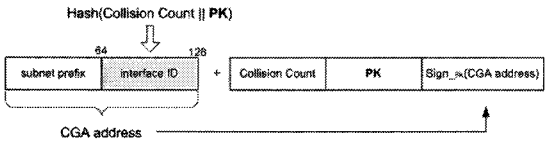


그림 4. CGA 주소의 생성과 소유권 문제 해결을 위한 구조

인 Interface ID부분을, 참여 노드의 공개키 값의 해쉬 값인 Hash(PK)의 상위 64를 사용한다. 이때 Collision Count는 IPv6 주소 중복을 방지하기 위한 값으로 같은 값이 있을 경우 0부터 2까지 1씩 증가시킨다. Collision Count 값이 2까지 증가한 후에도 값이 중복된 주소가 발견되면, 에러 처리하고, 새로운 키 쌍을 생성하여 CGA 주소를 새로 생성한다. 그림 4의 값을 수신한 노드는 첨부된 Collision Count와 PK 값의 해쉬 값을 계산하여, IPv6의 하위 64비트를 확인하고, PK값을 이용하여 첨부된 서명 값을 확인한다.

위의 CGA 주소의 생성을 응용하여 MANET 환경에서는, AREQ 메시지를 브로드캐스트하고, 동일한 IP 주소를 사용하고 있는 노드는 AREP 메시지에 개인키 값으로 서명한 값을 추가하여 유니캐스트 한다. 이때, 정당한 공개키의 사용자만이 공개키 값의 해쉬 값을 계산하여 IP 주소를 생성할 수 있고, 이에 대응하는 정당한 개인키 값을 아는 사용자만이 서명 값을 작성할 수 있음을 이용하여 IP 주소의 소유권 문제를 해결하여 DoS 공격을 방지 할 수 있다. 그러나, 서명을 이용한 방식은 계산량이 많으므로 MANET의 환경에는 적합하지 않다.

3. IP 주소의 충돌과 DoS 공격을 방지 하는 IP 주소 할당 방식 제안

앞의 2.1에서 MAENT에 참여하는 노드가 충돌하지 않는 IP 주소를 할당받을 수 있는 방식을 소개하였다. 그러나 추가적인 저장 공간을 요구하거나, 한번 사용한 IP 주소를 재사용 할 수 없거나, 노드와 노드의 IP 주소간의 소유권문제가 해결되지 않아 거짓된 메시지를 반복적으로 보낼 경우 DoS 공격이 발생 가능함을 알 수 있다. 또한, 2.2에서는 이러한 보안 문제를 해결하기 위하여 IPv6의 CGA를 이용하여 IP 주소의 소유권 문제를 해결 하여 DoS 공격을 방지하는 방식을 설명하였다. 그러나, 이동성이 있

고, 제한된 자원을 갖고 있는 MANET 상의 노드에게는 서명과 같은 계산양이 많은 방식은 적합하지 않다.

본 논문에서는 위의 점을 고려하여 일 방향 해쉬 함수의 특성을 이용하여 노드 스스로가 난수를 생성한다. 생성된 난수의 해쉬 값을 이용하여 IPv6 주소를 생성하여, CGA를 이용한 방식보다 적은 계산량과 오버헤드를 사용하여, 기존의 IP 주소와 충돌이 일어나지 않으면서, IP 주소의 소유권 문제를 해결하여 DoS 공격을 방지할 수 있는 IPv6 주소 할당 방식을 제안한다.

본 논문에서 제안하는 방식의 전체적인 과정은 그림 5와 4.2의 그림9와 같다.

1단계 : 네트워크에 참여하기를 원하는 노드는 IPv6 주소를 생성하기 위하여 난수 r을 생성한다.

2단계 : 난수 r에 해쉬 함수를 적용한 값을 $Hash(r)$로 나타낼 때, 그림 6과 같이 IPv6 주소의 하위 64비트 부분을, $Hash(r)$의 상위 64비트로 선정하여 IPv6 주소를 생성한다.

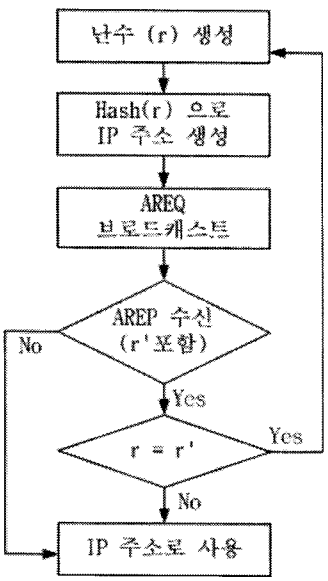


그림 5. IP 주소 할당 과정

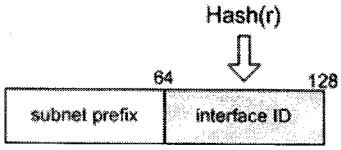


그림 6. 난수를 이용한 IPv6 주소의 형태

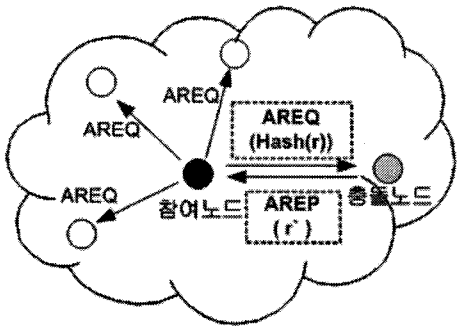


그림 7. AREQ/AREP 메시지 전송

3단계 : 2단계에서 생성한 IPv6 주소를, 네트워크에 참여하고 있는 다른 노드가 사용하고 있는지 확인하기 위하여 AREQ(Address Request) 메시지를 브로드 캐스트 한다. 이때, 노드의 이동성, 제한된 자원으로 인하여 메시지가 손실 될 수 있으므로, 같은 AREQ 메시지를 3회 정도 반복하여 브로드 캐스트 한다. 그림 7과 같이 AREQ 메시지를 수신한 노드들은 자신이 사용하는 IP 주소와 AREQ 메시지에 포함된 IPv6 주소가 같으면, 자신이 정당한 IPv6 주소의 사용자임을 밝히기 위하여, IPv6 주소를 생성할 때 사용한 난수 r'을 AREP 메시지에 포함하여 AREQ를 보낸 노드로 유니캐스트 한다.

4단계 : AREP 메시지의 수신을 확인하는 단계로, AREQ 메시지 전송 후 일정 시간 이후에도 AREP 메시지를 수신하지 못하면, 사용하고자 하는 IPv6 주소가 충돌되지 않는 것으로 간주하여 자신의 IPv6 주소로 할당하여 사용한다. 그렇지 않고, AREP 메시지가 수신될 경우, 5단계로 넘어간다.

5단계 : IPv6 주소의 충돌을 알리는 AREP 메시지가 정당한 사용자가 보낸 메시지인지 확인하기 위한 과정으로 AREP 메시지에 포함된 난수 r'과 자신이 사용하고자 하는 IPv6 주소 생성 시 사용한 난수 r을 비교한다. 두 개의 값이 같을 경우 AREP 메시지를 보낸 노드는 충돌되는 IPv6 주소의 정당한 사용자이므로, 충돌하지 않는 IPv6 주소를 할당할 수 있을 때까지, 1단계로 돌아가 반복한다.

4. 비교 분석과 성능 평가

4.1 안전성 분석

2장에서 설명한, 이웃 노드들 중에 하나가 Initiator

표 1. IP 할당 기법 비교

	MANET conf	안전한 호스트	리더 노드	난수의 해쉬 값 (제안 방식)
범주	Stateful	Stateless	Stateless	Stateless
주소 리스트 저장	필요	필요	필요	불필요
IP 주소 재사용	불가능	가능	불가능	가능
주기적 메시지 전송	필요	불필요	필요	불필요
DoS 공격 방지	불가능	불가능	불가능	가능

노드가 되고, Initiator 노드가 참여 노드 대신에 DAD 과정을 처리하고, 참여 노드에게 중복되지 않는 IP 주소를 할당해주는 MANETconf 방식, 랜덤 주소 선택 방식, 리더 노드를 이용하는 방식과, 본 논문에서 제안하고 있는 난수의 해쉬 값을 이용한 IP v6주소 할당방식을 비교하면 표 1과 같다.

MANET conf 방식은, Initiator 노드가 대신하는 DAD 과정에서 MANET상에 있는 기존 노드들이 충돌되는 IP 주소를 사용하고 있다는 거짓된 메시지를 Initiator 노드에게 보낼 경우 DoS 공격이 발생한다. 랜덤 주소를 선택하는 방식과 리더 노드를 이용한 방식 또한 충돌되는 IP 주소를 사용하고 있다는 거짓된 메시지를 참여 노드에게 보낼 경우 DoS 공격이 발생한다.

즉, 본 논문에서 제안한 방식은 사용하지 않는 IP 주소를 수집·모니터링하여 사용하지 않는 IP 주소를 선택, 할당받는 방식이 아닌, 노드 스스로가 IP 주소를 생성하는 방식으로 추가적인 저장 공간을 필요 없고, 일 방향 해쉬 함수의 특성을 이용하여 IP 주소를 생성, DAD 과정을 처리하므로, DoS 공격을 방지 할 수 있다.

본 논문에서 제안한 방식은 일 방향 해쉬 함수의 특성을 이용한 방식으로, AREQ 메시지를 받은 즉시 짧은 시간 안에 해쉬 함수의 결과 값 $Hash(r)$를 역함수를 이용하여 난수 r을 찾아 AREP 메시지를 보내는 것은 불가능하다. 즉 정확하게 난수 r을 알고 있는 IP 주소의 노드만이 AREP 메시지를 보낼 수 있으므로, 거짓된 AREP 메시지의 반복으로 인한 DoS 공격을 방지할 수 있다.

난수 r의 해쉬 값 중 상위 64비트만 IPv6 주소의 하위 값으로 사용하므로, 난수 r과 같지 않은 난수 r'이 같은 IP 주소를 생성해 낼 확률은 생일문제(birthday problem)에 의하여 출력 길이가 n인 해쉬 함수에 대해 $1.2 \times 2^{\frac{n}{2}}$ 정도의 연산이면 충돌 확률이 50%가 되므로, 본 논문에서는 64비트를 사용하므로 $1.2 \times 2^{\frac{64}{2}}$이므로, 약 5.1×10^9번 입력을 시도해야만 $r \neq r'$일 경우 $Hash(r) = Hash(r')$일 확률이 50%가 되기 때문에 정당한 IP 사용자가 거짓 사용자로 오인될 확률은 매우 작다.

4.2 패킷 구조의 비교

참여 노드는 자신이 IP 주소를 생성하고, AREQ 메시지와 AREP 메시지를 이용하여 DAD 과정을 처리한다.

그림 8은 CGA를 이용한 방식이고, 그림 9는 본 논문에서 제안하는 방식이다. CGA를 이용한 방식은 키 쌍을 생성하여, 공개키의 일방향 해쉬 함수 값을 계산하여 IPv6 주소를 생성하고, 서명의 확인 과정을 통하여 DAD과정을 처리한다. 그러나, 본 논문에서 제안한 방식은 난수를 생성하여 난수의 일 방향 해쉬 값을 계산하여 IPv6 주소생성하고, 해쉬 값의 확인 과정으로 DAD 과정을 처리한다.

각각에 적용되는 AREQ, AREP 메시지의 구조는 그림 10, 그림11과 같다. 본 논문에서는 각각 1024비

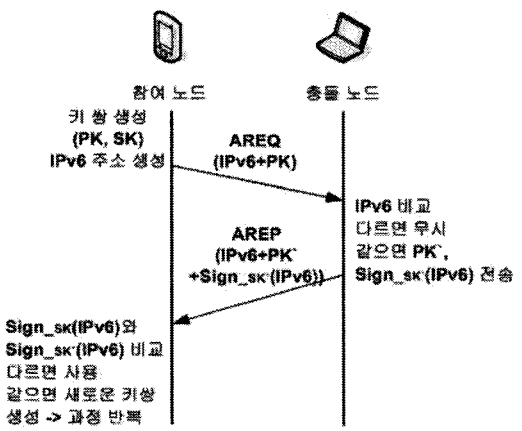


그림 8. CGA를 이용한 방식

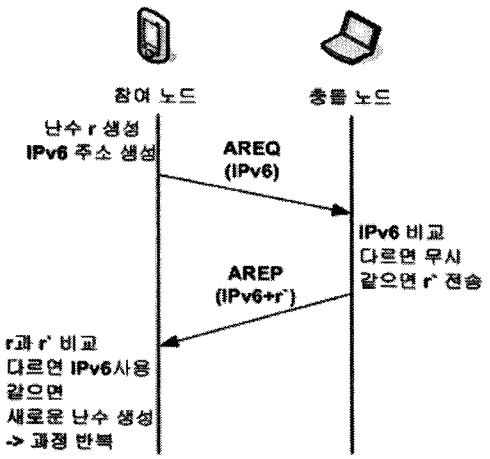


그림 9. 제안 방식

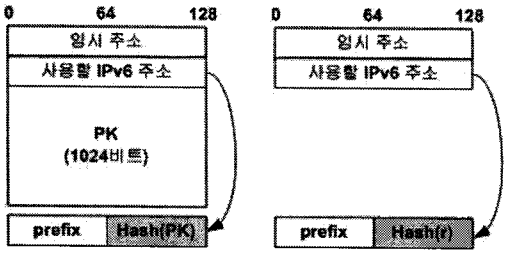


그림 10. CGA AREQ / 제안된 방식 AREQ

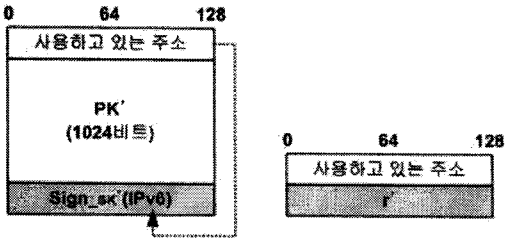


그림 11. CGA AREP / 제안된 방식 AREP

트의 공개키 값과, 128비트 난수 값을 적용한다. AREQ 메시지 길이는 그림 10에서와 같이 본 논문에서 제안하는 방식은 CGA를 이용한 방식보다 공개키 값의 길이만큼 적다. 또한, AREP 메시지 길이도 그림 11과 같이 본 논문에서 제안하는 방식은 난수 값만을 추가하여 보내므로, 공개키 값과 서명 값을 추가하여 보내는 CGA를 이용한 방식의 AREP 메시지 길이보다 공개키 값의 길이만큼 적음을 알 수 있다.

4.3 성능 평가

본 절에서는 2.2에서 설명한 CGA를 이용한 IPv6 주소 할당 방식과, 본 논문에서 제안하고 있는 난수의 해쉬 값을 이용한 IPv6 주소 할당 방식을 NS2[17]를 이용하여 실험하였다. 각각의 방식에서, DAD 과정의 처리 시간, 전송되는 메시지 개수를 측정하여 비교하였다.

4.3.1 실험 환경

본 논문에서는 그림 12와 같이, IPv6 주소를 생성하여 네트워크에 참여하는 참여 노드와 이미 중복된 IPv6 주소를 사용하고 있는 충돌 노드가 DAD 과정에서 걸리는 처리시간과, 전송되는 메시지의 개수를 측정하였다.

실험 환경은 표 2와 같이 500m × 500m의 영역에 전체 노드의 개수를 10, 20, 30, 40, 50개로 증가시켜 노드의 밀도에 대하여 처리시간과 전송되는 메시지 개수를 비교하였다. 각각의 노드들의 움직임은 최대 20m/sec으로 이용하는 random way point 모델을 적용하였다. 서명 알고리즘은 RSA 서명을 이용하였고, 일 방향 해쉬 함수는 SHA-1을 사용하였다.

그림 12와 같이 random way point로 노드를 배치, 이동하게 구성하였다. 참여하고자 하는 노드가 할당할 노드의 IPv6 주소는, 이미 참여하고 있는 노드 중에 하나의 IPv6 주소와 중복이 되도록 하여, 참여노

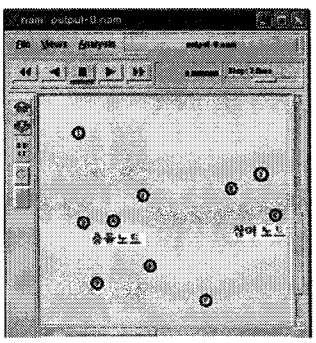


그림 12. 노드의 구성

표 2. 실험 환경

속성	값
Simulation time	100sec
Simulation area	500m × 500m
node 개수	10, 20, 30, 40, 50개
Movement model	random way point
Maximum speed	20m/sec

드가 IPv6 주소의 충돌을 탐지하는 DAD 과정에서 IPv6 주소의 충돌을 탐지하는데 걸리는 시간과 전송되는 메시지 개수를 측정하였다.

4.3.2 시간 측정

정해진 영역에 전체 노드의 개수를 10, 20, 30, 40, 50개로 증가시켜, 노드의 밀집도에 따른 DAD 처리 시간을 측정하였다. 그림 13에서 윗부분의 꺾은선이 CGA 방식이고, 아랫부분의 꺾은선이 Random number 방식이다. 전체적으로 노드의 개수가 증가할수록 밀도가 증가하므로 처리시간이 증가함을 할 수 있다. 그러나 본 논문의 실험에서는 노드의 배치와 움직임을 random way point를 사용하였으므로, 특정부분(예:20개의 노드)에서는 값이 증가, 감소함을 알 수 있다. 그러나 두 개의 방식에 같은 위치, 움직임을 환경으로 주었으므로, 특정 부분에서도 두 개의 방식을 비교하면 서명을 사용하는 CGA 방식보다 본 논문에서 제안하는 방식이 더 적은 시간이 걸림을 알 수 있다.

4.3.3 오버헤드 측정

노드의 개수에 대하여 DAD 과정 중 전송되는 메시지의 개수를 측정하였다. 즉, 라우팅 레벨과 MAC 레벨에서 발생하는 컨트롤 메시지의 개수를 측정한 값으로 그림 14와 같다. 왼쪽 막대가 본 논문에서 제안하고 있는 Random number 방식이고, 오른쪽 막대

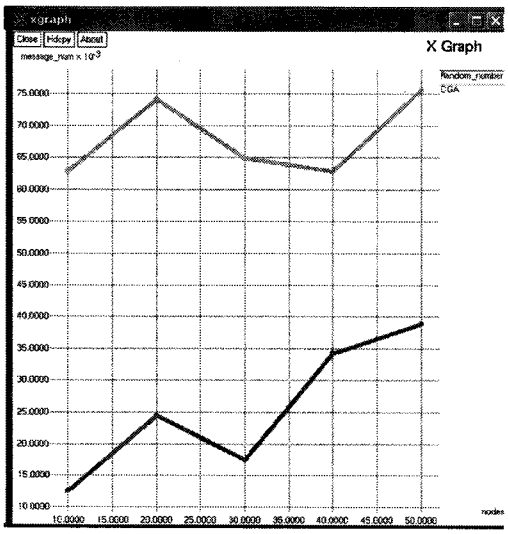


그림 13. 노드의 개수에 따른 DAD 처리 시간

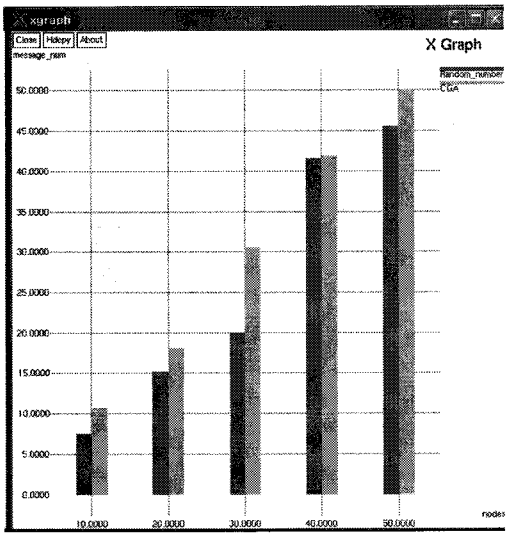


그림 14. 노드의 개수에 따른 오버헤드

가 CGA 방식이다. 측정 결과, CGA를 이용한 방식과, 제안하고 있는 방식은 노드의 개수가 증가하여 밀집도가 커짐에 따라 전송되는 메시지의 개수는 증가함을 알 수 있다. 즉, 본 논문에서 제안하고 있는 방식은 전송되는 메시지의 개수는 큰 차이는 없지만, CGA 방식과 같이 DoS 공격을 방지할 수 있을 뿐만 아니라, 5.2의 결과와 같이 CGA 방식보다 처리 시간은 더 적게 걸림을 알 수 있다.

5. 결 론

MANET 환경에서 충돌하지 않는 IP 주소를 할당하는 많은 연구들이 진행되고 있으나, IP 주소의 재사용, 추가적인 저장 공간의 요구, IP 주소의 충돌을 탐지하는 DAD 과정에서 거짓된 메시지의 반복적인 전송으로 인하여 DoS 공격이 발생하였다. 본 논문에서는 노드 스스로 IP 주소를 할당할 때 난수와 일방향 해쉬 함수의 특성을 이용하여 IP 주소의 소유권 문제를 해결하여 DoS 공격을 탐지하는 방식을 제안하였다. 또한 NS2를 통하여 MANET 환경에서 IP 주소 할당 방식 중, IP 주소의 소유권 문제를 해결하여 DAD 과정에서 DoS 공격을 방지하는 방식 중에 하나인 CGA를 이용한 방식과 본 논문에서 제안한 방식을 시뮬레이션하여 DAD 과정의 처리시간과, 라우팅 레벨과 MAC 레벨에서 발생하는 컨트롤 메시지의 전송 개수를 측정 비교하였다. 그 결과 본 논문

에서 제안한 방식이 CGA를 이용한 방식과 발생하는 메시지의 개수 큰 차이는 없지만, CGA 방식과 같이 DoS 공격을 방지 할 수 있으면서, DAD 처리 시간은 짧음을 알 수 있다.

참 고 논 문

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

[2] Bernardos C. J,. Calderon M, "A DHCP-based IP address autoconfiguration for MANETs," *In Proceedings of the I International Conference on Ubiquitous Computing: Applications, Technology and Social Issues*, 2006.

[3] T.Aura "Cryptographically Generated Addresses(CGA) draft-ietf-end-cga-06," *IETF Internet-Draft*, Apr. 16, 2004.

[4] P. Nikander, "Denial-of-Service, Address Ownership, and Early Authentication in the IPv6 World," *presented at Cambridge Security Protocols Workshop* 2001, Apr. 25~27, 2001, Cambridge University.

[5] H.Zhou, L. M. Ni, M. W. Mutka, "Prophet Address Allocation for Large Scale Manets," *Proc, IEEE INFOCOM* 2003, San Francisco, CA, Mar. 2003.

[6] IEEE. Guidelines for 64bit global identifer (eu64) registration authority. http://standards.ieee.org/*regauth/oui/tutorials/EUI64.html*, May 2001.

[7] M. Günes, J. Reibel, "An ip address configuration algorithm for zeroconf. mobile multihop ad-hoc networks," *in Proceedings of the International Workshop on Broadband Wireless. Ad-Hoc Networks and Services*, Sophia Antipolis, France, Sep. 2002.

[8] Sanket Nesargi, Ravi Prakash, "MENTconf: Configuration of Hosts in a Mobile Ad hoc Network," *In Proceedings of INFOCOM*, 2002.

[9] Y.Sun, E.M.Belding-Royer, "Dynamic Address Configuration in Mobile Ad Hoc Networks," *UCSB Technical Report* 2003-11, June 2003.

[10] J. Boleng, "Efficient Network Layer Addressing for Mobile Ad hoc Networks," *Proc, In, Conf, Wireless Networks, Las Vegas, NV*, June 2002, pp. 271~77.

[11] P. Patchipulusu. "Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks," *Master's thesis, Computer Science, Texas A&M University*, Aug. 1997.

[12] S. Thomson, T. Narten. "IPv6 Stateless Address Autoconfiguration," *RFC 2462*, IETF, Dec. 1998.

[13] Stuart Cheshire, Bernard Aboba. "Dynamic configuration of ipv4 link-local addresses." *http://www.ietf.org/internet-drafts/draft-ietf-zeroconf-ipv4-linklocal-04.txt*, July 2001.

[14] C. E. Perkins, J. T. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun. Ad hoc Address Autoconfiguration. *IETF Internet Draft, draft-ietf-manet-autoconf-01.txt*, Nov. 2001.

[15] Ana R. Cavalli, Jean-Marie Orset "Secure hosts auto-configuration in mobile ad hoc networks," *Ad Hoc Networks 3(5)*, 2005.

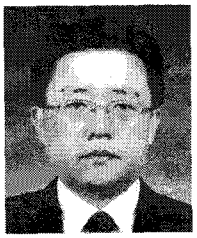
[16] Jaehoon Paul Jeong, Jungsoo Park, Hyoungjun Kim, Hongjong Jeong and Dongkyun Kim, "Ad Hoc IP Address Autoconfiguration," *draft-jeong-adhoc-ip-addr-autoconf-06.txt*, January 2006.

[17] K. Fall, K. Varadhan., "ns notes and documentation. Technical report," The VINT Project 2006.

임 정 미

2000년 단국대학교 전자계산학과 졸업 학사
2002년 단국대학교 전자계산학과 석사
2006년 단국대학교 전자계산학과 박사
2004년~현재 단국대학교 교양학부 강의전임

관심분야 : 정보보호, 네트워크 보안



박 창 섭

1983년 연세대학교 경제학과 졸업
1983년 한국 IBM 근무
1990년 미국 Lehigh Univ. 전자계산학 박사
1990년~현재 단국대학교 전자컴퓨터학부 교수

관심분야 : 네트워크 보안, 암호 프로토콜