Name Service in IPv6 Mobile Ad-hoc Network connected to the Internet

Jaehoon Jeong, Jungsoo Park, Hyoungjun Kim
Protocol Engineering Center, ETRI,
161 Gajong-Dong, Yusong-Gu, Daejon 305–350, Korea
Email: {paul,pjs,khj}@etri.re.kr
Telephone: +82–42–860–1664, Fax: +82–42–861–5404
WWW home page: http://www.adhoc.6ants.net/

***Abstract*— This paper suggests an architecture of DNS service system for IPv6 mobile ad-hoc network connected to the Internet. The DNS resolution of DNS names of mobile nodes within mobile ad-hoc network is performed by multicast DNS and that of DNS names of nodes in the Internet is performed through DNS autoconfiguration of recursive DNS server. In the former, each mobile node plays a role of DNS name server for the DNS resource records associated with DNS name of which authority it has. The latter allows mobile node to receive the global Internet service, such as web service, in IPv6 mobile ad-hoc network that is connected to the Internet. These two kinds of DNS name resolution are processed automatically without the intervention of users in mobile ad-hoc network.**

I. Introduction

Mobile Ad-hoc Network (MANET) is the network where mobile nodes can communicate with one another without communication infrastructure such as base station or access point [1]. When mobile nodes want to communicate with one another in the environments such as battle field and public vehicles (e.g., airplane, bus and boat), they need to construct a temporary and infrastructureless network. Recently, according as the necessity of MANET increases, ad-hoc routing protocols for multi-hop MANET have been being developed by IETF Manet working group [2]. Ad-hoc multicast routing protocols as well as ad-hoc unicast routing protocols have been being developed and implemented to provide mobile users in MANET with multicast service such as video conference and computer-supported collaborative work (CSCW). Also, the global connectivity for IPv6 MANETs has been being researched, of which object is to support the communication between the mobile ad-hoc node and Internet node [3].

With this trend, IPv6 that has many convenient functions including stateless address autoconfiguration [4], [5] and multicast address allocation [6] has become mature and been being deployed in the whole world. The users in MANET will be able to communicate more easily through the IPv6 zero-configuration that provides easy and convenient configuration [7], [8]. Accordingly, if we adopt IPv6 as the network protocol of MANET, we will create a number of useful services for MANET and benefit from them.

DNS is one of the most popular applications in the Internet. It provides the name-to-address resolution among nodes in the Internet. DNS must be a necessity of MANET but the current DNS is inappropriate to MANET that has dynamic topology because the current DNS works on the basis of dedicated and fixed DNS name servers. Therefore, a new DNS architecture appropriate to this MANET became necessary.

In this paper, we propose an architecture of name service system which can provide mobile nodes in IPv6 mobile ad-hoc network with the name-to-address resolution and autoconfiguration technology for easy configuration related to name service including the generation of unique domain name of mobile node and generation of zone file for name service. We also suggest service discovery performed through the name service system of this paper and DNS service resource record (SRV) [9]. This service discovery mechanism provides ad-hoc user with the information of a service with the specified transport protocol (TCP or UDP) that is needed for the connection to the service in MANET, such as IP address and port number. The suggested system allows mobile node within IPv6 MANET connected to the Internet via Internet gateway to resolve DNS name of Internet node into global IPv6 address and the mobile node to communicate with the Internet node via Internet gateway.

This paper is organized as follows; Sect. 2 presents related work. In Sect. 3, we suggest the name service within IPv6 MANET. In Sect. 4, the name service for the Internet is explained. Sect. 5, descibes the implementation of the name service system. Finally, in Sect. 6, we conclude this paper and present future work.

II. Related Work

A. Automatic Configuration of IP Hosts

IETF Zeroconf working group has defined the technology by which the configuration necessary for networking is performed automatically without manual administration or configuration in the environment such as ad-hoc network, small office home office (SOHO) networks, airplane networks and home networks, which is called zero-configuration or autoconfiguration [7], [8]. The main mechanisms related to the autoconfiguration technology are as follows;
(a) IP interface configuration, (b) IP multicast address allocation, (c) Name service (e.g., Translation between host name and IP address), and (d) Service discovery.

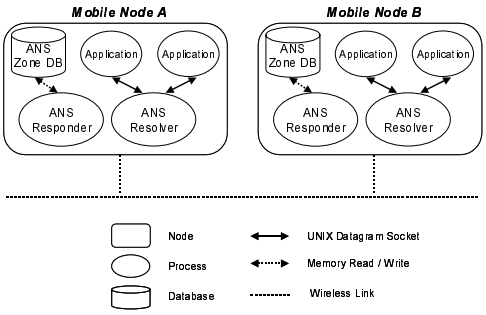

Fig. 1. ANS System for Name Service in IPv6 MANET

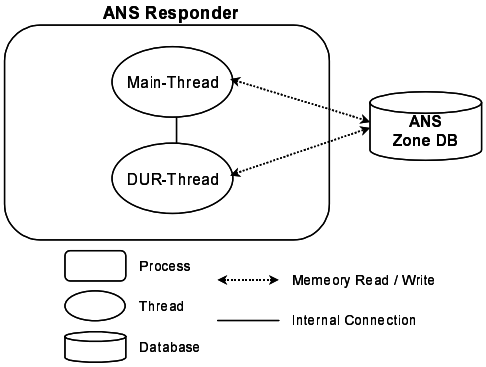

Fig. 2. Architecture of ANS Responder

B. Autoconfiguration Technology in IPv6 MANET

ETRI has developed the autoconfiguration technology for the automatic configuration of ad-hoc nodes as well as implemented IPv6 ad-hoc routing protocols, IPv6 AODV and MAODV [10]. The four main mechanisms related to the autoconfiguration technology are as follows;
(a) IPv6 ad-hoc unicast address autoconfiguration regarding IP interface configuration [11], (b) IPv6 ad-hoc multicast address allocation [11], (c) Name service through multicast DNS [12], and (d) Service discovery through multicast DNS and SRV resource record [13].

III. Name Service within IPv6 MANET

A. Ad-hoc Name Service System for IPv6 MANET (ANS)

ANS is the name service system that provides the name resolution and service discovery in IPv6 MANET which is site-local scoped network. We assume that every network device of mobile node should be configured by ad-hoc stateless address autoconfiguration [11] or by manual configuration. ANS System consists of ANS Responder that works as name server in MANET and ANS Resolver that performs the role of DNS resolver for name-to-address translation. Fig. 1 shows the architecture of ANS System for name service in MANET. Each mobile node runs ANS Responder and Resolver. An application over mobile node that needs the name resolution can receive the name service through ANS Resolver because ANS provides the applications with the functions for name resolution through which they can communicate with ANS Resolver. ANS Resolver sends the DNS query for a name in the multicast address with which ANS Responder in each mobile node has joined for the name [12]. When ANS Responder receives DNS query from ANS Resolver in other mobile nodes, after checking if it is responsible for the query, it decides to respond to the query. When it is responsible for the query, it sends the appropriate response to ANS Resolver in unicast.

B. Architecture and Operation of ANS System

1) Architecture and Operation of ANS Responder: Fig. 2 shows the architecture of ANS Responder, which is composed of Main-Thread and DUR-Thread.

Main-Thread manages ANS Zone database (DB) for name service and processes DNS queries to send the corresponding response to the querier. It initializes ANS Zone file that contains DNS resource records into ANS Zone DB. When it receives a DNS query, it checks if it is responsible for the query. If it is responsible, it sends the response corresponding to the query to ANS Resolver that sent the query.

DUR-Thread performs the dynamic update request (DUR) during the verification of the uniqueness of DNS resource record. The verification is initiated by ANS Resolver on another node that has receivied multiple responses with the same domain name and resource record type for the DNS query that it sent in multicast [12]. The destination address of the multicast packet for the verification is the solicited name multicast addresss corresponding to domain name [12]. The ANS Resolver sends the first response to every ANS Responder that sent a response except the Responder that sent a response first. Every ANS Responder that receives a response managed by itself performs the verification of the uniqueness of the resource record included in the response through DUR-Thread. If DUR-Thread detects the duplication of the resource record, it invalidates the record in its ANS Zone DB.

2) Architecture and Operation of ANS Resolver: Fig. 3 shows the architecture of ANS Resolver, which consists of Main-Thread, Resolv-Thread and Timer-Thread.

When Main-Thread receives DNS query from application on the same node through UNIX datagram socket, it first checks if there is the valid response corresponding to the query in ANS Cache. If there is the response, Main-Thread sends the response to the application directly. Otherwise, it executes Resolv-Thread that will perform the actual name resolution and asks Resolv-Thread to respond to the application through the name resolution.

When Resolv-Thread receives the request of name resolution from Main-Thread, it makes DNS query message and destination multicast address corresponding to the domain name of the query and then sends the message in the multicast address. If Resolv-Thread receives a response message from an ANS Responder, it returns the the result of the response to the application that asked for the name resolution through UNIX datagram socket. Whenever a new resource record is

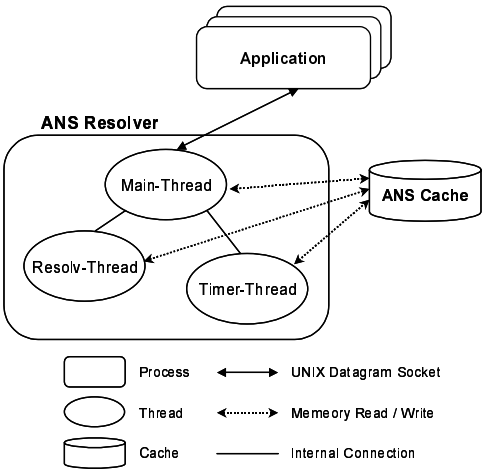

Fig. 3. Architecture of ANS Resolver

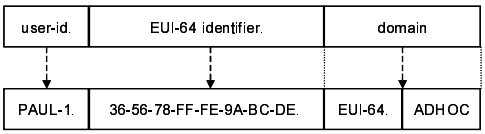

Fig. 4. Format of Unique Domain Name based on EUI-64 Identifier

received by Resolv-Thread, it caches the response in ANS Cache. When a record is registered in ANS Cache, ANS Cache timer is adjusted for ANS Cache management. If Resolv-Thread receives the multiple responses for the query, it initiates the dynamic update request in the responders that sent the same response except the 1st responder [12].

Whenever ANS Cache timer expires, Timer-Thread checks if there are entries that expired in ANS Cache. Timer-Thread invalidates the entries and makes the resource records of the entries unused for name resolution. After the work, Timer-Thread restarts ANS Cache timer.

C. Name Service in ANS

We define the domain for ad-hoc network as “ADHOC.”.

1) Generation of Unique DNS Name: The mechanism of name generation makes a unique DNS name with user-id, device-id (network device’s address extended into EUI-64 identifier) and domain like Fig. 4 [14]. user-id is the user identifier selected by user and device-id is EUI-64 identifier derived from the network device’s built-in 48-bit IEEE 802 address. domain indicates the kind of network where a node is placed, which should include “EUI-64” sub-domain which indicates that the DNS name is based on EUI-64. We define the domain of ad-hoc network for the generation of unique DNS name as “EUI-64.ADHOC”. For example, when user-id is “PAUL-1”, device-id is “36-56-78-FF-FE-9A-BC-DE”, and domain is “EUI-64.ADHOC”, a unique DNS name would be “PAUL-1.36-56-78-FF-FE-9A-BC-DE.EUI-64.ADHOC”. The advantage of the above mechanism guarantees that no name conflict happens without the verification procedure of the uniqueness of the resource record related to the domain name

```
/* Configuration File of ANS Responder (ans.conf) */
    options {
      user-id "PAUL-1";
      domain "ADHOC.";
    };
```

Fig. 5. Configuration File of ANS Responder (ans.conf)

```
$TTL   20
$ORIGIN   ADHOC.

PAUL-1.36-56-78-FF-FE-9A-BC-DE.EUI-64  IN   AAAA    FEC0:0:0:0:3656:78FF:FE9A:BCDE
PAUL-1                  IN    CNAME   PAUL-1.36-56-78-FF-FE-9A-BC-DE.EUI-64.ADHOC.

;; DNS SRV Resource Records
; Unicast Service : SERVICE-1
_SERVICE-1._TCP                         IN  SRV  0  1  3000  PAUL-1.ADHOC.
_SERVICE-1._UDP                         IN  SRV  0  1  3000  PAUL-1.ADHOC.

; Multicast Service : SERVICE-2
_SERVICE-2._UDP                         IN  SRV  0  1  4000  @.3.5.
```

Fig. 6. Zone File of ANS Responder

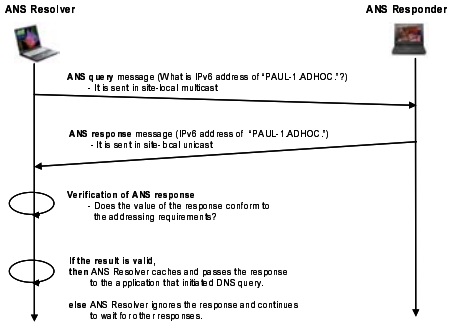

Fig. 7. Procedure of DNS Name Resolution through ANS

although users in other nodes use the same user-id. But it is valid only when all the nodes in MANET should use the above name generation mechanism. Nevertheless, even though a node configures its domain name by manual configuration or other methods, mobile nodes can detect the name conflict through the dynamic update request [12]. user-id and domain are registered in options statement of the configuration file of ANS Responder (ans.conf) like Fig. 5.

2) Generation of Zone File: ANS Responder generates a zone file that contains the DNS name generated above and site-local scoped IPv6 address of the network device corresponding to the name like Fig. 6. The IPv6 address of the name, “PAUL-1.36-56-78-FF-FE-9A-BC-DE.EUI-64.ADHOC”, is “FEC0::3656:78FF:FE9A:BCDE”.

3) DNS Name Resolution and Service Discovery: Ad-hoc node can not only resolve DNS name into IP address, but also perform service discovery through ANS. Fig. 7 shows the procedure in which a DNS name “PAUL-1.ADHOC.” is resolved into IPv6 site-local address. The service discovery is performed in the same way as the name resolution [13]. For service discovery, DNS SRV resource record is used like Fig. 6 [9], [13]. In the zone file of Fig. 6, two unicast services and one multicast service are registered. The unicast services are “_SERVICE-1._TCP.ADHOC.” and “_SERVICE-1._UDP.ADHOC.”. The multicast service is “_SERVICE-

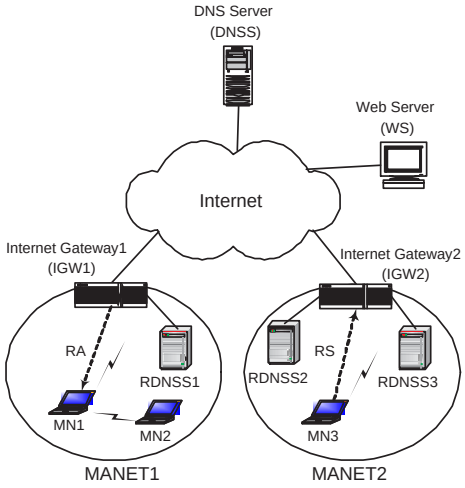

Fig. 8. IPv6 Mobile Ad-hoc Networks connected to the Internet

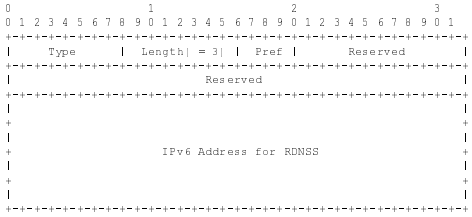

Fig. 9. RDNSS Option Message Format

TABLE I
RDNSS OPTION MESSAGE FIELDS

Field	Description
Type	Message type. Its value is to be assigned by IANA.
Length	Length of the option (including the type and length fields) in units of 8 octets.
Pref	Preference of an RDNSS. A decimal value of 15 indicates the highest preference.
IPv6 Address for RDNSS	RDNSS's IPv6 Address. The scope of the address is site-local.

2._UDP.ADHOC.". For the query of these services, the response of the corresponding service information , the DNS name and port number of the server providing the service, is delivered by the corresponding server [13].

4) Security Consideration: We assume the truested nodes generate their own domain name with the name generation mechanism of this paper. Therefore, there can not be the name conflict within the group of the trusted nodes.

In order to provide securer name service including service discovery in ANS, we can use IPsec ESP with a null-transform to authenticate ANS response, which can be easily accomplished through the configuration of a group pre-shared secret key for the trusted nodes and the use of the keyed hash method such as HMAC [13].

IV. NAME SERVICE FOR THE INTERNET

When a mobile node in MANET connects to a web server in the Internet, it needs an Internet gateway that connects the MANET and Internet. Also, it needs a recursive DNS server that tranlates the DNS name of the web server into the global IP address. Recently, the mechanism supporting the global connectivity for IPv6 MANET has been being developed by IETF MANET working group [2]. The name service for the Internet in IPv6 MANET is performed over the global connectivity for IPv6 MANET.

A. Global Connectivity for IPv6 MANET

Internet gateway informs mobile node of the address of its MANET address and IPv6 global scoped prefix for stateless address autoconfiguration through RA (router advertisement) message [3]. In Fig. 8, mobile node, MN1, receives an RA message from Internet gateway in MANET1, IGW1. MN1 autoconfigures its IPv6 global address with the prefix included in the RA message and sets up default route toward IGW1.

B. DNS Autoconfiguration for the Internet Connectivity

IPv6 address of recursive DNS server (RDNSS) managed by Internet gateway is advertised through RA message including prefix option for IPv6 stateless address autoconfiguration, which is delivered by RA message as a new RA option for recursive DNS server.

When mobile nodes use proactive routing protocols, such as OLSR and TBRPF, Internet gateway advertises RA message periodically. Whenever a mobile node enters into a new MANET, it receives another RA message from another Internet gateway and performs IPv6 stateless address autoconfiguration with the new prefix included in the RA message. In MANET1 of Fig. 8, we can see a mobile node, MN1, receives an RA message indicating the recursive DNS server in the MANET where MN1 is placed is RDNSS1 from Internet gateway in MANET1, IGW1. When MN1 receives IGW1's RA message, it can autoconfigure its IPv6 global address, set up default route, and configure recursive DNS server for the resolution of global DNS name.

When mobile nodes use reactive routing protocols, such as AODV and DSR, mobile nodes solicit Internet gateway for RA message through RS (router solicitation) message. Whenever a mobile node resolves a global DNS name into IPv6 global address, , it sends RS messages via IPv6 site-local all node multicast address. When an Internet gateway in the MANET receives the RS message, it responds to the RS message with RA message. In MANET2 of Fig. 8, we can see a mobile node, MN3, sends RS message for RA message. IGW2 in the same MANET responds to MN3's RS message with RA message indicating the recursive DNS servers in the MANET where MN3 is placed are RDNSS2 and RDNSS3. When MN3 receives IGW2's RA message, it can autoconfigure its IPv6 global address, set up default route, and configure recursive DNS server for the resolution of global DNS name.

When mobile node moves into another MANET, it receives another RA message. It replaces the old RDNSS information with the new one for the succeeding name resolution.

1) Neighbor Discovery Extension - RDNSS Option Message: The mechanism of this paper needs a new option in

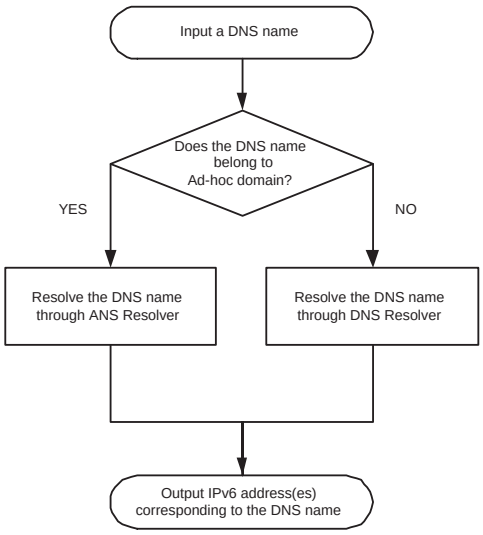

Fig. 10. Procedure of the Resolution of DNS Name into IPv6 address

Neighbor Discovery [5]. Fig. 9 shows the format of RDNSS option message. Table. I decribes the fields of the option [19].

When advertising more than one RDNSS, as many RDNSS options as the number of RDNSSes are included in an RA message. When a mobile node perceives multiple RDNSSes through RA message, it stores the addresses of the RDNSSes in the descending order of the value of the preference field "Pref" in the RDNSS option into the configuration file (e.g., /etc/resolv.conf in Linux) which the resolver on the node uses for DNS name resolution. The greater the value of the preference is, the higher the priority of the preference is.

2) Extension of Global Connectivity for IPv6 MANET: RA message used in the global connectivity for IPv6 MANET delivers RDNSS option with prefix option. Also, network manager of Internet gateway configures the address(es) of the recursive DNS server manually in the part of RA configuration of the router. The recursive DNS server can runs on the Internet gateway or another node connected to the Internet gateway.

V. Implementation of Name Service System

The function of the library related to DNS resolver for the DNS resolution, "getaddrinfo()", should be modified for the support of DNS name service in MANET. The DNS name for the domain belonging to MANET, of which suffix is "ADHOC.", is resolved through ANS Resolver of ANS System. The other DNS names are resolved through the current DNS resolver which uses DNS resolver's configuration file including the recursive DNS server(s) advertised by Internet gateway. Fig. 10 shows the procedure of resolving a DNS name into IPv6 address(es).

A part of IPv6 stateless address autoconfiguration should be modified to process the RDNSS option. When IPv6 stack of mobile mode receives RA message including RDNSS option from Internet gateway, it replaces the address(es) stored in DNS resolver's configuration file with the new address(es) included in RDNSS option.

VI. Conclusion

This paper suggested a DNS name system can provide mobile nodes in the environment, such as ad-hoc network, where the current DNS system can not be used for supporting DNS service to the modile nodes. The system can provide mobile nodes in IPv6 mobile ad-hoc network with the DNS name service, such as the name-to-address resolution, service discovery and autoconfiguration of DNS name and zone file.

Also, this paper suggested a mechanism to allow mobile node within IPv6 MANET connected to the Internet via Internet gateway to resolve DNS name of Internet node into global IPv6 address and the mobile node to communicate with the Internet node via Internet gateway.

In future work, we will enhance the security function of the name system including ANS system to provide securer name service against the various security attacks.

References

[1] Elizabeth M. Royer and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April 1999.
[2] IETF Manet working group, http://www.ietf.org/html.charters/manet-charter.html
[3] Ryuji Wakikawa, Jari T. Malinen, Charles E. Perkins, Anders Nilsson, Antti J. Tuominen, "Global connectivity for IPv6 Mobile Ad Hoc Networks", draft-wakikawa-manet-globalv6-01.txt, July 2002.
[4] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462.
[5] T. Narten, E. Nordmark and W. Simpson, "Neighbour Discovery for IP version 6", RFC2461.
[6] Jungsoo Park and Myungki Shin, "Link Scoped IPv6 Multicast Addresses", draft-ietf-ipv6-link-scoped-mcast-02.txt, October 2002.
[7] A. Williams, "Requirements for Automatic Configuration of IP Hosts", (work in progress) draft-ietf-zeroconf-reqts-12.txt, September 2002.
[8] IETF Zeroconf working group, http://www.ietf.org/html.charters/zeroconf-charter.html
[9] A. Gulbrandsen, P. Vixie and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC2782, February 2000.
[10] Implementation of IPv6 AODV and MAODV, http://www.adhoc.6ants.net
[11] Jaehoon Jeong and Jungsoo Park, "Autoconfiguration Technologies for IPv6 Multicast Service in Mobile Ad-hoc Networks", ICON2002, August 2002.
[12] Jaehoon Jeong, Jungsoo Park, Hyoungjun Kim and Kishik Park, "Name Service in IPv6 Mobile Ad-hoc Network", ICOIN2003, February 2003.
[13] Jaehoon Jeong, Jungsoo Park, and Hyoungjun Kim, "Service Discovery based on Multicast DNS in IPv6 Mobile Ad-hoc Networks", VTC2003 Spring, April 2003.
[14] Jaehoon Jeong, Jungsoo Park and Hyoungjun Kim, "Unique DNS Name Generation", draft-jeong-name-generation-01.txt, February 2003.
[15] Cedric Adjih et al., "Optimized Link State Routing Protocol", draft-ietf-manet-olsr-08.txt, March 2003.
[16] R. Ogier, M. Lewis and F. Templin, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", draft-ietf-manet-tbrpf-07.txt, March 2003.
[17] Charles E. Perkins, Elizabeth M. Belding-Royer and Samir R. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", draft-ietf-manet-aodv-13.txt, February 2003.
[18] David B. Johnson, David A. Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", draft-ietf-manet-dsr-08.txt, February 2003.
[19] Jaehoon Jeong, Jungsoo Park, Kyeongjin Lee and Hyoungjun Kim, "The Autoconfiguration of Recursive DNS Server and the Optimization of DNS Name Resolution in Hierarchical Mobile IPv6", draft-jeong-hmipv6-dns-optimization-00.txt, February 2003.