The Autoconfiguration of Recursive DNS Server and the Optimization of DNS Name Resolution in Hierarchical Mobile IPv6

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

Abstract— **This paper provides the mechanism for the autoconfiguration of recursive DNS server in mobile node and the optimization of DNS name resolution in the hierarchical mobile IPv6 network. Whenever the mobile node moves into a new MAP domain, the region managed by another MAP, in the hierarchical mobile IPv6 network, it detects the addresses of recursive DNS servers which are placed in the region and replaces the old ones with the new ones for DNS name resolution. This allows the time for DNS name resolution much reduced by using the nearest recursive DNS server which exists in the region. Therefore, through DNS autoconfiguration, the mechanism of this paper can optimize DNS name resolution.**

I. INTRODUCTION

IPv6 stateless address autoconfiguration [1] provides a way to autoconfigure either fixed or mobile nodes with one or more IPv6 addresses and default routes. For the support of the various services in the Internet, not only the configuration of IP address in network interface, but also that of the recursive DNS server for DNS name resolution are necessary. Up to now, many mechanisms to autoconfigure recursive DNS server in nodes have been proposed [2]–[4].

This paper suggests not only the autoconfiguration of recursive DNS server in mobile node that moves within the hierarchical mobile IPv6 (HMIPv6) network [5], but also the optimization of the DNS name resolution in such a network. Whenever the mobile node moves into a new mobility anchor point (MAP) domain, the region managed by another MAP, in the hierarchical mobile IPv6 network, it detects the addresses of new recursive DNS servers which are placed in the region and replaces the old ones with the new ones for DNS name resolution. This allows the time for DNS name resolution much reduced by using the nearest recursive server which exists in the region. Like this, because the mobile nodes use the recursive DNS server in the same domain instead of the fixed recursive DNS server, the DNS name resolution of the mobile nodes can be optimized.

This paper is organized as follows; Sect. 2 presents related work. In Sect. 3, as a motivation for writing this paper, the benefit of using local recursive DNS server is shown. In Sect. 4, the DNS autoconfiguration and optimization in HMIPv6 are explained in detail. In Sect. 5, we analyze the delay needed for DNS name resolution in foreign network and home network, respectively. Sect. 6 suggests the security considerations. Finally, in Sect. 7, we conclude this paper and present future work.

II. RELATED WORK

A. DNS Autoconfiguration in DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) can provide IPv6 host with network configuration parameters, such as recursive DNS server, as well as automatic allocation of reusable network addresses [6]. Whenever a mobile node moved into another MAP domain in HMIPv6 network, it can find out the addresses of recursive DNS servers through DHCPv6 [2]. But, it needs some delay for the discovery of DHCPv6 server and the additional message exchange between the mobile node and DHCPv6 server, in order to get DNS information, such as the addresses of recursive DNS servers.

B. Well Known Site Local Unicast Addresses for Recursive DNS Servers

The well known site local unicast addresses can be used for recursive DNS servers [3]. Three well known addresses are defined to configure stub resolvers on IPv6 nodes to enable them to communicate with recursive DNS server with minimum configuration in the network and without running a discovery protocol on the end nodes. This method may be used when no other information about the addresses of recursive DNS servers is available. It lets the local routing system forward the packets containing DNS query message to the right place. However, in order that a mobile node get DNS service in HMIPv6 network, it has a limitation that there should be at least one recursive DNS server that is configured with well known site local addresses within every MAP domain.

III. BENEFIT OF USING LOCAL RECURSIVE DNS SERVER

So as to observe the benefit of using local recursive DNS server (RDNSS), we measured the resolution delay of a

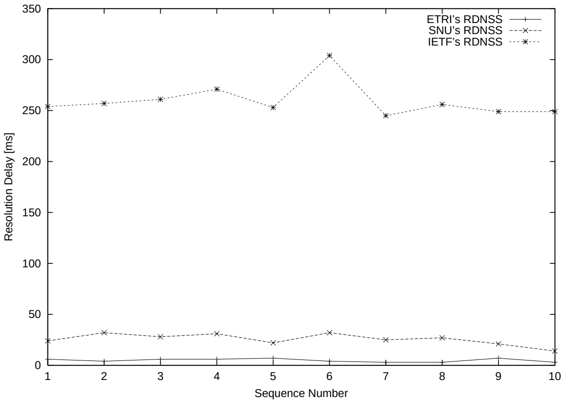

Fig. 1. Resolution Delay of a Host DNS Name at three Recursive DNS Servers

TABLE I
COMPARISON OF MEASURED RESOLUTION DELAYS

RDNSS	Hop#	MIN	MAX	Average	50th Percentile
$RDNSS_{ETRI}$	3	3[ms]	7[ms]	4.9[ms]	4[ms]
$RDNSS_{SNU}$	18	14[ms]	32[ms]	25.6[ms]	25[ms]
$RDNSS_{IETF}$	24	245[ms]	304[ms]	259.9[ms]	254[ms]

host DNS name, "www.kame.net", through three different RDNSSes; (a) $RDNSS_{ETRI}$, (b) $RDNSS_{SNU}$, and (c) $RDNSS_{IETF}$. An IPv4 host for sending the DNS query was placed at a subnet in ETRI's network. So, $RDNSS_{ETRI}$ is one of local RDNSSes. The others, $RDNSS_{SNU}$, and $RDNSS_{IETF}$, are remote RDNSSes. The second column of Table. I shows the distance between the host and RDNSS by hop count (HOP#). We used BIND9's dig in order to measure DNS name resolution delay [7]. Fig. 1 shows the measurement result of 10 samples of DNS query and Table. I describes the comparison of measured delays. The type A resource record of "www.kame.net" had already been stored in the cache of each RDNSS. When we used the local RDNSS ($RDNSS_{ETRI}$) instead of the remote RDNSS ($RDNSS_{IETF}$), we could reduce the resolution delay of 53 times on the average. Therefore, we can see that the use of local RDNSS may be beneficial for DNS name resolution.

IV. DNS AUTOCONFIGURATION AND OPTIMIZATION IN HMIPv6

Whenever a mobile node enters another MAP domain of the visited network, it receives a Router Advertisement (RA) message including MAP option from Access Router (AR) and performs the local binding update with the new MAP. If the list of the addresses of recursive DNS server (RDNSS) is included in the RA message with the MAP option, the mobile node can detect the new RDNSSes and select one of them for the DNS name resolution. Like Fig. 2, this scheme can reduce considerably the time of the name resolution between the mobile node and RDNSS. Because the mobile node uses the nearest RDNSS in the same MAP domain, RDNSS2 or RDNSS3, instead of the RDNSS in its home network, RDNSS1. When the mobile node moves into another

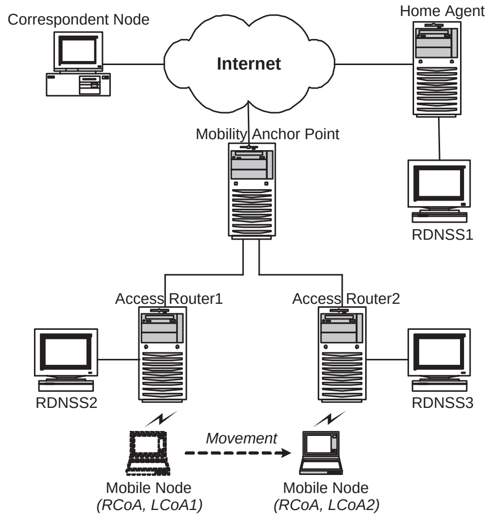

Fig. 2. Optimization of DNS Name Resolution in HMIPv6 Domain

MAP domain, it replaces the old RDNSS(es) with the new RDNSS(es) for the succeeding name resolutions.

A. HMIPv6 Extension - Advertisement of Recursive DNS Server

Because this paper considers only router advertisement for MAP discovery, all ARs belonging to the MAP domain must advertise the MAP's IP address and list of the RDNSS addresses [8].

The information of the RDNSS(es) in the MAP domain is stored in the MAP by the network administrator and advertised as a new option with MAP option through the RA message. There may be more than one RDNSS in a MAP domain. In this case, the MAP advertises RA message including the list of RDNSSes in the same domain with MAP option periodically. The RA message with MAP and RDNSS options is propagated from the MAP to the mobile node through certain configured router interfaces within the hierarchy of routers. This requires the manual configuration of the MAP and RDNSS options in the MAP and also the routers, receiving the MAP and RDNSS options, must allow themselves to propagate the options on certain interfaces.

Finally, whenever the mobile node listening to RA messages receives the new RA message, it checks if the MAP is new or not. If the MAP is a new one, the mobile node perceives it has moved into another MAP domain. It performs not only the local binding update with the new MAP, in order to establish a binding between the Regional Care-of Address (RCoA) and On-link CoA (LCoA) [5], but also the update of the list of RDNSSes in the configuration for DNS name resolution with the new ones. From the next name resolution, the mobile node uses the new RDNSSes.

B. Neighbor Discovery Extension - RDNSS Option Message Format

The mechanism of this paper needs a new option in Neighbor Discovery [9]. Fig. 3 shows the format of RDNSS option

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length( = 3) |  Pref |       Reserved        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Reserved                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                     IPv6 Address of RDNSS                     +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig. 3. RDNSS Option Message Format

TABLE II
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. The default value is 3.
Pref	Preference of an RDNSS. A decimal value of 15 indicates the highest preference. A decimal value of 0 indicates that that the RDNSS cannot be used.
IPv6 Address of RDNSS	RDNSS's IPv6 Address. The scope of the address should be global. The prefix length of the address is /64.

message and Table. II decribes the fields of the option [8].

When advertising more than one RDNSS, as many RDNSS options as the RDNSSes are included in an RA message.

C. RDNSS Selection by the Mobile Node

When a mobile node perceives multiple RDNSSes through RA message, it arranges and stores the addresses of the RDNSSes in order into the configuration which the resolver on the node uses for DNS name resolution on the basis of the value of "Pref" field and the prefix of "IPv6 Address of RDNSS" field in the RDNSS option. The following algorithm is simply based on the rule of selecting the nearest possible RDNSS from the mobile node, providing that its preference value did not reach the maximum value of 15. When the distances are the same, this algorithm uses the preference value to select the RDNSSes. The mobile node operation is shown below:

1) Receive and parse all RDNSS options.

2) Arrange RDNSSes in an ascending order of distance, starting with the nearest RDNSS and store them in the configuration for DNS name resolution used by resolver. For example, the longest prefix matching between the "IPv6 Address of RDNSS" field and mobile node's LCoA can be used to decide the distance between mobile node and RDNSS, how far away the mobile node is from the RDNSS.

3) For each RDNSS entry, check the following; If the value of "Pref" field is set to zero, exclude the RDNSS entry from the list of RDNSSes of the configuration for DNS name resolution. The value of zero indicates the failure of the RDNSS or the path to the RDNSS.

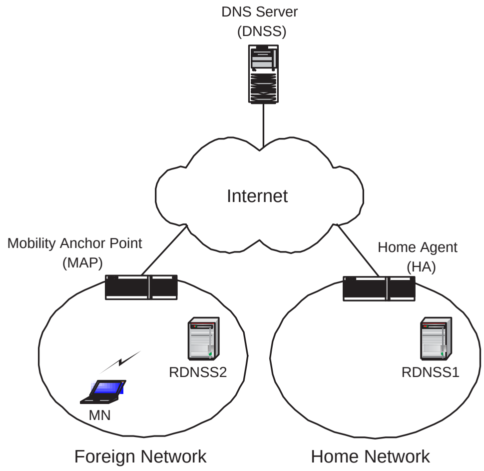

Fig. 4. Network Topology

Whenever the resolver on the mobile node performs the name resolution, it refers to the address(es) of RDNSS in the configuration for name resolution according to the current rule of selecting an RDNSS, namely from the 1st RDNSS among the RDNSSes ordered in the configuration. For example, in Fig. 2, when a mobile node moves from the subnet managed by Access Router 1 to the subnet managed by Access Router 2, it uses RDNSS3 in the same subnet instead of RDNSS2 for DNS name resolution.

As a last resort for name resolution, each mobile node should maintain the address(es) of the RDNSS(es) at its home network in the tail of the list of RDNSS addresses. Also, in the case that there are no available RDNSSes for name resolution at a new MAP domain that a mobile node visits, the node can the RDNSSes of the previous MAP domain or of its home network for name resolution.

D. Detection of RDNSS Failure

A MAP should take action to keep the list of RDNSSes up to date. As a candidate of managing the list, the MAP placed in a MAP domain may check periodically if the RDNSSes registered in the MAP are alive or not. Whenever the MAP detects the failure of any RDNSSes, it can advertise the failure down to the hierarchy with a new RA message including an RDNSS option of which "Pref" field has zero for the failing RDNSS. When a mobile node receives the RA message, it perceives that the RDNSS is out of work or the path to the RDNSS is broken and excludes the RDNSS from the configuration for name resolution.

V. ANALYSIS OF THE DELAY NEEDED FOR DNS NAME RESOLUTION

Fig. 4 shows the network topology for the analysis of the delay needed for DNS name resolution and Table. III explains the parameters for the analysis of the delay necessary for DNS name resolution. With these parameters, we can calculate and compare the delays needed for name resolution through both the current DNS mechanism and the proposed one. The

TABLE III

PARAMETERS FOR DELAY ANALYSIS

Parameter	Description
RD_{old}	Resolution Delay through the current DNS mechanism
RD_{new}	Resolution Delay through the proposed mechanism
h_1	Hop count between MN and MAP
h_2	Hop count between MN and RDNSS2
h_3	Hop count between RDNSS2 and MAP or between RDNSS1 and HA
d	Hop count between MAP and HA (i.e., the distance from Foreign Network to Home Network)
m_1	Hop count between HA and DNSS
m_2	Hop count between MAP and DNSS
α	One-way delay in a link of one hop
$Diff$	$RD_{old} - RD_{new}$

former delay is presented as RD_{old} and the latter one as RD_{new} like Table. III. The following shows the procedure of the calculation. First of all, we assume that one-way delay in every link of one hop is constant, α.

$$RD_{old} = (h_1 + d + 2 \cdot h_3 + m_1) \cdot 2 \cdot \alpha \quad (1)$$

$$RD_{new} = (h_2 + h_3 + m_2) \cdot 2 \cdot \alpha \quad (2)$$

With (1) and (2), we can get the delay difference, $Diff$, between these two mechanisms.

$$\begin{aligned} Diff &= RD_{old} - RD_{new} \\ &= ((h_1 - h_2) + d + h_3 + (m_1 - m_2)) \cdot 2 \cdot \alpha \quad (3) \end{aligned}$$

If we assume m_1 and m_2 are equal, (3) becomes reduced as follows:

$$Diff = ((h_1 - h_2 + h_3) + d) \cdot 2 \cdot \alpha \quad (4)$$

From (4), the value of $h_1 - h_2 + h_3$ is always nonnegative integer because the distance between MN and MAP plus that between HA and RDNSS1, $h_1 + h_3$, is larger than or equal to that between MN and RDNSS2, h_2, if and only if MN exists in a foreign network. Therefore, when MN moves within the foreign network, the value of $Diff$ is always positive. What is inferred from (4) is that the important factor of the delay for name resolution is the distance between foreign network and home network, d. The greater the distance is, the larger the delay is. Thus, with the proposed mechansim, we can reduce the delay for DNS name resolution and optimize the name resolution in the hierarchical mobile IPv6 network.

VI. SECURITY CONSIDERATIONS

Usually, recursive DNS servers at a site allow other visiting nodes to use them for DNS name resolution. If MAP announces its DNS information as well as prefix information, the same policy is adopted implicitly in hierarchical mobile IPv6 network. Consequently, any mobile nodes can use recursive DNS servers in the visited MAP domain.

In order to guarantee the secure delivery of router advertisement message including RDNSS option, among IPv6 nodes within a MAP domain, namely a hierarchy of routers, the router advertisement should be authenticated by AH or ESP. This security is essentially related to the security in HMIPv6 and Neighbor Discovery protocol [5], [9].

VII. CONCLUSION

This paper suggested a method of DNS autoconfiguration for reducing DNS name resolution in hierarchical mobile IPv6 environment. The method uses the router advertisement message to announce the list of recursive DNS servers' addresses within a MAP domain. Because of using the router advertisement message that provides the RCoA prefix, there is no additional time to discover recursive DNS servers.

This scheme, for the DNS autoconfiguration and optimization, can be applied to other wireless networks, such as IPv6 mobile network and mobile ad hoc network connected to the Internet [10]. For this application, we will enhance and expand our scheme of DNS service.

REFERENCES

[1] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462, December 1998.

[2] R. Droms et al., "DNS Configuration options for DHCPv6", draft-ietf-dhc-dhcpv6-opt-dnsconfig-03.txt, February 2003.

[3] A. Durand, J. itojun and D. Thaler, "Well known site local unicast addresses to communicate with recursive DNS servers", draft-ietf-ipv6-dns-discovery-07.txt, October 2002.

[4] Luc Beloeil, "IPv6 Router Advertisement DNS resolver Option", draft-beloeil-ipv6-dns-resolver-option-01.txt, January 2003.

[5] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", draft-ietf-mobileip-hmipv6-08.txt, June 2003.

[6] R. Droms et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-dhcpv6-28.txt, November 2002.

[7] BIND9 of Internet Software Consortium, http://www.isc.org/products/BIND/bind9.html

[8] 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-01.txt, June 2003.

[9] T. Narten, E. Nordmark and W. Simpson, "Neighbour Discovery for IP version 6", RFC 2461, December 1998.

[10] Jaehoon Jeong, Jungsoo Park and Hyoungjun Kim, "Name Service in IPv6 Mobile Ad-hoc Network connected to the Internet", PIMRC2003, September 2003.