Distributed balancing with Application-Layer Anycast for Home Agent Discovery on the Mobile IPv6

Yun-Sheng Yen, Chia-Chang Hsu, and Han-Chieh Chao
Department of Electrical Engineering, National Dong Hwa University
Hualien, Taiwan, R.O.C
E-mail: d9223008@em92.ndhu.edu.tw
m9123030@mail.ndhu.edu.tw
hcc@mail.ndhu.edu.tw

Abstract

The anycast protocol is essential for supporting distributed service and recovery. This work presents an Application-Layer Distributed Home Agent Discovery on Mobile IPv6 forming anycast Mobile IPv6 framework to offer distributed home agents discovery protocols, enabling the mobile node (MN) to find the best suitable Home Agent (HA) and correspondent node (CN) to forward datagram. The simulation results prove that Mobile IPv6 owns the advantages including service reliability, less latency and shorter route path with the help of anycast.

Keywords: Anycast, mobile IPv6, Internet

1. Introduction

Mobile IPv6 [1] is a new-generation Internet technology that supports ambulation deliveries. Through this technology, the mobile node (MN) does not cause on-line interruption in a multifarious movement. In the Mobile IPv6 structure, to let the correspondent node (CN) send datagrams to the mobile node in the ambulation, must have more than one home agent (HA) on Internet. The datagrams sent by the correspondent node would, based on the packet information, spread to the home domain. The home agent then receives the datagrams and builds a tunnel to forward them to the current care-of-address (CoA) where the MN is up. Initially, each mobile node is recognized by its home address, regardless of its current point of attachment. When an MN moves from the home link to the foreign link, it obtains a CoA from either a stateless address by auto-configuration or a stateful address from DHCPv6. That is, CoA at present uses a unicast IP address. If the mobile node moves, it sends a binding update (BU) to informing its HA by its CoA.

Nevertheless, Mobile IPv6 still has many weaknesses which need to be overcome. If a mobile node moves toward another scalable domain such as a different Internet Service Provider (ISP) or mobile network company, then the serious problems, like registration delay, transmission latency, and packet loss would occur due to the BU registered by the MN back to its original HA. Some proposals, such as smooth hand-off techniques [2] and hierarchical Mobile IPv6 [3], remain unresolved.

Anycast is a new IPv6 protocol used in point-to-point datagram communication between a single source and the nearest destination node. The data are transferred the end to the nearest node in the group allocated by an anycast address. Selecting the nearest group with the anycasting scheme based on the network topology is called network anycast, whose metrics are determined by cost, router hops and calculated distance. By contrast, the metrics of application anycast include available capacity, measured response times and number of active connections. Most studies involving application layer anycast use the domain name server (DNS) service or enhanced switch server to choose the nearest group member. Application layer anycast is effective in loading balance, and also has an advantage of changing less network architecture than the network anycast.

In an analysis of IPv6 anycast [4], Jun-ichiro iotjun Hagino and K. Ettikan, discuss most anycast problems on current networks and attempt to adapt anycast on IPv6 networks. Their study discussed the limitations
and characteristics of anycast with respect to discovering destination, nondeterministic packet delivery, assigning anycast address to hosts and anycast address in source address. Hui Deng, Xiaolong Huang et al. [5] have proposed a hybrid load balance mechanism. Their mechanism extends the Dynamic Home Agent Address Discovery (DHAAD) protocol on Mobile IPv6 to release and prevent traffic burning. HAs in hybrid load balance mechanism use a special traffic load table and new HA reassignment algorithm to achieve hybrid load balance. W. Zegura [6] et al proposed a server selection architecture in a relocated web service using application layer anycast. Zegura et al’s approach, called anycast name resolution, uses DNS to choose the server. The most important role in anycast name resolution is the anycast resolver, which handles anycast domain name request. The anycast resolver selects the nearest server return to client according the authoritative resolver’s list information. Yu Chen and Terrance Boult [7] proposed dynamic home agent reassignment in Mobile IP, a technique which allows foreign agent to perform the HA partial function. This work substitutes the HA for the mobility agent. A foreign agent which supports dynamic home agent reassignment can then receive HHR (HA hand off request) to take over the HA’s role.

Dina Katabi and John Wroclawski [8, 10] introduce a novel technique called global IP anycast, in which anycasting is deployed on a large scale deployment, and the anycast address space is aggregated on the Internet. Hence, anycast routing can work in different domains across autonomous system boundaries and anycast becomes globally scalable. Datagrams address foreign anycast sites through a border gateway protocol (BGP) protocol to determine and install anycast routes. The border router searches the nearest node and replies indicating the source in the foreign domain. The border router detects the shortest path either to the nearest anycast node, or back to the home domain. The greatest advantage of this approach is only the change of border router making the network architecture easy to achieve.

This paper proposes an Application-Layer Distributed Home Agents Discovery (AL-DHAD) method on global network to identify an MN’s nearest HA to improve mobile IPv6 anycasting performance. AL-DHAD is also a home agent discovery protocol for selecting the most appropriate HA for communication. As explained later, AL-DHAD must be implemented using HAs to make DHAD usable.

The remainder of this work is organized as follows. Section 2 describes the background and related work. Section 3 presents the proposed approach in detail. Section 4 presents and discusses the simulation results. Conclusions and areas of future research are finally pointed out in Section 5.

2. Background and Related Works

2.1. Background

Figure 1 illustrates the anycast mobile IPv6 framework. All border routers support the anycast function, enabling datagrams to transmit to the nearest server node, which is an HA. The CN can connect to MN’s nearest HA, even connecting directly to the MN in a complete anycast mobile IPv6 framework, because the MN and HA are both anycast route destinations. Then, datagrams are sent to the MN or the HA via an anycast route. An HA is not essential in an anycast mobile IPv6 framework because datagrams can be transmitted directly to the MN. However, anycast routing is defined as a less-variant routing, indicating that routing table exchange does not occur frequently in routers. In mobile IPv6, the MN always moves, but the router near the CN’s routing table does not have the current record of the MN’s anycast IP address. The HA must still ensure that packets are forwarded to the MN correctly. Additionally, the MN requires the HA during MN handoff. The MN sends a BU to the HA when the MN moves to another range of base station, then the HA tunnels the stream to a new mobile node location. Although mobile IPv6 has a routing optimization procedure which can send a BU to directly to a CN, the return routability must be obtained first via the HA.

![Figure 1. Anycast Mobile IPv6 Network](image)

Another important problem about the limited range of anycast IP addresses in the anycast mobile IPv6 network framework is that anycast has two surprising regulations in RFC 2373 [9]. These regulations are that an anycast address must not be used as the source address of an IPv6 packet, or be assigned to an IPv6 host. That is, an anycast IP may be only assigned to an IPv6 router. However, many studies extensively enable anycast IPs to be assigned to
hosts. Therefore, the main problem seems to be that an anycast IP address cannot be used as an IPv6 packet’s source address. This study shows that mobile IPv6 can tolerate this restriction. Mobile IPv6 includes a procedure called triangle routing that let an MN sending packet to its HA and receive the reply packet as its CoA. The procedure may also be used to overcome the limitation that anycast cannot be used in the source address.

If mobile IPv6 could alleviate the limits of anycast, then no problem would occur in data continuity. Anycast’s limits are intended to prevent data or messages from transferring to different servers. For example, in Figure 2, host B and host C have same the anycast IP. If host A transfers data or messages to an anycast IP, the data or message are forwarded to B or C according to the route-changing condition. However, this condition does not arise in mobile IPv6. For example, the anycast IP in Figure 3 is assigned to the MN as its home address, meaning that two home agents possess an anycast home domain. When the CN sends a packet to the MN’s anycast IP, the packet may be transferred to a different HA. However, the mobile IPv6 procedure means that the packet must be tunneled to the MN, avoiding data non-continuity. Furthermore, the packet moves to a fixed HA in most cases in the proposed scheme, because HAs are distributed in different domains with route vectors which are not close to each other. The proposed scheme is robust and recoverable, and leads to fewer abnormal packet sequences.

![Figure 2. Disconnect packets transmit in anycast framework.](image)

![Figure 3. Anycast used in mobile IPv6.](image)

2.2 Related Works

Dynamic Home Agent Address Discovery (DHAAD) [1] adopts anycast technology to achieve loading balance of home agents. Multiple HAs must be aggregated in the same link in DHAAD protocol architecture. When an MN is up and sends a BU to the HA, it transmits an ICMP Home Agent Address Discovery Request Message with anycast IP in its IP header’s destination IP section. An HA in the local link will receives and replies with an ICMP Home Agent Address Discovery Reply message including HAs’ unicast IP list. When the MN receives the ICMP reply, it specifies an appropriate HA and send a BU to it at the its unicast IP. Then, the HA can use Proxy Neighbor Discovery to intercept any IPv6 packets addressed to the MN’s home address on the home link.

The mobile network enables users to communicate with one another conveniently and efficiently. However, some problems remain unresolved. For example, route optimization enables an MN delivering a datagram to connect directly to a CN in mobile IPv6, but also increases handoff delay and causes the IPSec problem. Route optimization must run the activity return routability (RR) procedure in advance, and accomplish the notification between the MN and the CN through the HA using a correspondent registration. Security problem is usually a major issue in route optimization. However, if route optimization is abandoned, then the HA’s location becomes a very important issue. If the mobile and correspondent nodes are in the same domain and interconnect via the same HA, then the performance of registration time and transmission delay would be the worst case. This study proposes an Application Layer Dynamic Home Agent Discovery (AL-DHAD) scheme using global network anycast to locate the nearest HA to the MN and thus improve the network’s performance by enabling the mobile and correspondent nodes to interconnect closely at the lowest cost.

3. Application Layer - Distributed Home Agents Discovery (AL-DHAD)

This study presents the Application-layer Distributed Home Agents Discovery as a mobile IPv6 anycasting application. AL-DHAD is also a home agent discovery protocol to select a suitable HA for communication. In addition to the mobile and correspondent nodes, AL-DHAD must implement HAs to be able to use DHAD.

Many home agents are located in different domains. The master HA manages multi-HAs and processes initialing message, and owns the mobile node’s home domain. Other HAs, called slave HAs, have the same function as master HAs in all software and hardware architecture. However, a slave HA’s IP address is not memorized by MNs, and does not have its own home domain. Figure 4 illustrates the HA framework in