Enabling Route Optimization for Large Networks with Location Privacy Consideration

Vu Truong Thanh*, Hidetoshi Yokota** and Yoshiyori Urano*

* Global Information and Telecommunication Studies, Waseda University

E-mail: thanhvtr@yahoo.com, urano@waseda.jp

** KDDI R&D Laboratories, Inc., Japan, E-mail: yokota@kddilabs.jp

Abstract

Mobile IP [9] was introduced to help the mobile user to be contacted with a single IP address even though the point-of-access changes. However, mobile IP creates the so-called "triangle routing" which makes the delays for data packets longer, as well as creating unnecessary traffic at the home network of the mobile user. To overcome this, Route Optimization (RO) for mobile IP [1] was proposed, which eliminated the triangle routing phenomenon. But [1] requires that the network protocol stack of all existing hosts to change. Privacy is also another matter to be considered.

This paper introduces a scheme called Peer Agent scheme to implement RO for mobile IP without requiring existing hosts to change. Method to preserve location privacy while still enabling RO is also considered.

Keywords: Mobile IP, Route Optimization, location privacy

1. INTRODUCTION

With the popularity of notebook computers and handheld processing devices, together with the widely available of wireless technologies and access points, it is anticipated that mobile and wireless access to the Internet may outstrip all other forms of access in the future.

Mobile IP (MIP) protocol [9] has been proposed to allow the users to keep their IP connections while changing their point of attachments. However, it faces the so-called "triangle routing" phenomenon, which means the traffic from the Correspondent Node (CN) to the Mobile Node (MN) must traverse through the Home Agent (HA) first. This creates some inefficiencies, for example the HA may be overloaded, it takes longer time for the packets to reach the MN, and it creates unnecessary load on network path between the CN and the MN.

To solve the "triangle routing" problem, we need to find a way to route the traffic from CNs directly to the Care-of Address (CoA) of the MN. Several approaches have been proposed, some of which require changes to the working of the base Mobile IP protocol. In paper [4], a virtual home agent (VHA) is added to the foreign network. An MN will use the address of VHA as its home address when connecting to correspondent nodes. The HA of the MN will not in anyway involve in the communications. However, this approach only works for connections that are initiated by the MN after it has moved into the foreign network and discovered the address of the VHA, and valid only during the period the MN is still wandering inside that foreign network.

Paper [5] proposes a similar architecture, in which the VHA is now called the Temporary Home Agent (TA), which is located at the gateway router. However, the approach in [5] requires that each MN be assigned a co-located care-of address, which may become a problem with the address-depleted IPv4.

The above approaches are not compatible with the base MIP protocol; therefore it is difficult to apply to the base MIP protocol. A MIP-compatible approach to route optimization has been proposed [1] (from now on this proposal will be called Route Optimization or RO). In this proposal, a CN will maintain a binding cache containing CoAs of MNs. Upon being informed by the HA (or the MN in Mobile IPv6) about the binding of an MN, which is the (home address, care-of address) pair of the MN, the CN will update the binding into the binding cache. Using this binding information, the CN can contact the MN directly, using encapsulation, without disturbing the HA. [7], [8] show that RO does improve performance of mobile IP.

However, there are several issues arise with RO. One consideration with RO is the location privacy violation. Because the CoA (which is the address of the subnet where the MN is roaming) is sent to the CN, the owner of the CN (or those in the same subnet with CN) can map out the movement of MN, or accordingly the movement of the user. Therefore, a new flag, the private "P" flag, in the Registration Request message has been introduced in [1], which forbids the use of RO.

We can introduce a "limited privacy" context, in which the information about the care-of-address of the MN is dispersed only to the network elements of the correspondent network, but not the CN itself. This is relevant because in general, we can assume that the owner to of the correspondent network (the ISP) has no bad intentions toward the mobile user. In addition, there are networks entities in the home network and the foreign network, namely HA and FA, know about the

mobility of the user. To allow "limited privacy", a new flag, the "L" flag, is introduced into both the Registration Request and the Binding Update Request.

Another issue with RO is that it requires changes to the protocol stacks of CNs, which is almost impossible because of the large numbers of existing computers with diversifying OSs. To overcome this requirement, several approaches have been proposed. The main idea of these proposals is that the correspondent network will assume all the tasks that the CN must accomplish under the RO scheme.

Paper [2] uses the agent-based approach, introducing the correspondent agent into the network of the correspondent network, just like the HA and FA in the home network and foreign network, respectively. This approach has some intrinsic problems. The centralized correspondent agent has the probability of becoming a bottleneck. It also introduces inefficient routing inside the correspondent network, because traffic always routes through the agent, even if a more direct route exists.

This approach can hide the exact location of the MN from the CN; however the CN may guess that the MN is not at its home from the modified routing information in certain circumstances.

The agent-based approach is also used in [6]. An agent called also called the correspondent agent is introduced into the correspondent network to help transfer the packets from the CN to the MN. However, in [6] that correspondent agent also supports reverse tunneling from the FA to the correspondent nodes.

In general, the Mobility Border Router scheme [3] is similar to the Agent-based scheme, if we suppose that the correspondent agent is now placed at the gateway router.

The Mobility Border Router (MBR) maintains the binding entries (care-of-address vs. home address) for mobile hosts, and encapsulates and tunnels packets from CN to MN using the binding information.

However the solutions proposed in [2], [3], and [6] cannot be applied for large networks with more than one border router to the Internet, because they assumes that data packets should be relayed via a single border router.

This paper proposes an implementation scheme for RO called the *Peer Agent (PA) scheme* which does not requires changes to the end hosts while still being able to support large networks. It also supports "limited location privacy" described above.

The paper is organized as follows. Section 2 presents the Peer Agent scheme for RO. Section 3 explains the designs of the entities introduced with the PA schemes. Initial results of implementing the designs are also included. Section 4 compares the PA scheme with existing schemes. Section 5 concludes the paper and identifies some future works for the PA scheme.

2. PEER AGENT ROUTE OPTIMIZATION SCHEME

In this section we describe the Peer Agent (PA) route optimization approach to solve the triangle routing in MIP. The scheme should satisfy the follow requirements:

- *No changes at the end hosts are required.*
- *Reuse and compliance with RO proposal in [1]* Because the RO proposal in [1] compatibles with the base MIP, it minimizes the changes to the working of the base MIP protocol in order to enable RO. This and the above requirement facilitate the easier and faster deployment of RO in mobile IP.
- *Preserving the dynamic routing and flexible configuration of the network.* The PA scheme should not create any fixed routing scheme or constrain the network administrators from freely engineering or expanding the correspondent network.
- *Robustness.* When changes are made to the RO protocol, or when the network changes in size or configuration, the changes to the scheme's entities and working procedures should be minimized.
- *Being able to hide the movement of the MN from the CN.* The proposed scheme in this research should be able to prevent the CN from knowing the mobility of the MN, while still enable RO. In other words, this scheme should provide the "limited privacy" feature described in section 1.

2.1 The Peer Agent scheme architecture

The PA scheme includes the addition of a Peer Agent into the correspondent network and the inclusion of the binding caches at the routers of the correspondent network. Here, the jobs that a CN must perform according to route optimization protocol [1] are divided between the PA and the router.

The Peer Agent

The Peer Agent is added to the correspondent network to hide route optimization operations from CNs. A PA processes the binding messages (introduced in [1]) from HAs, and performs accordingly to install or update the binding caches at routers of the correspondent domain or the routers of the subnet where the CN is located.

The binding cache at the routers

In [1], any CN participating in the RO protocol will maintain a binding cache. In the PA scheme, the binding cache is moved to the routers. When the PA receives Binding Update messages from the HA of a MN, it will instruct the routers to create the binding entry for the MN in the binding cache. The routers then intercept the IP packets from the hosts inside the correspondent network destined to the MN, encapsulate these packets using the address in the binding cache entry for the MN, and tunnel them to the Care-of Address of the MN.

2.2 Working of the PA scheme

Because the PA is designed to compatible with that from [1], the working procedure for it follows that from [1]. The route optimization process used in this scheme can be seen as the cooperation of three separate procedures:

- Forwarding of Binding Update messages from HA to PA
- Update of binding caches in routers by PA
- Tunneling packets from CN to MN directly to the CoA by the routers

The working of the PA scheme is depicted in figure 1.

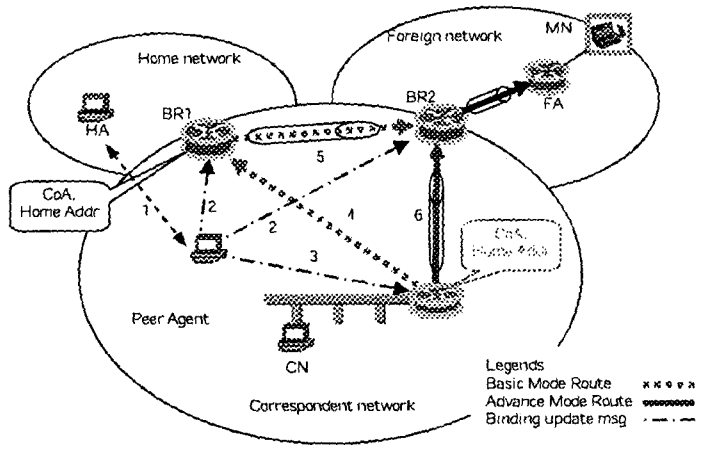

Figure 1. Operations of the PA scheme

Forwarding of Binding Update messages from HA to PA

Similar to [1], the route optimization process in the PA scheme starts when the HA receives the first packets destined for the MN from a CN, and subsequently returns a Binding Update (BU) message towards the correspondent network. However, instead of reaching the concerned CN, that BU message will be forwarded to the PA (dotted line #1 in figure 1).

There are four ways we can use to forward the BU message to the PA instead of the CN. The first method is using Domain Name Server (DNS). Before forwarding the binding message, the HA issues a DNS request for the *Peer Agent* of the CN. After getting the address of the PA, HA can send it with the Binding Update message. If the DNS request fails, then the HA sends the Binding Update message to the CN as in the original RO proposal.

The second choice is using the AAA servers. The HA sends the Binding Update message to its AAA server, using the Diameter protocol (new AVP code may have to be defined), this server will find the correspondent domain from the target node's IP address, and forward the message to the AAA server of the domain. The AAA server of the correspondent domain is configured to know the address of the peer-agent. After authenticating the binding update message, the AAA server at the correspondent network will forward the message to the PA. If the "L" flag is set for the message, then the AAA should discard the message if it cannot find the PA.

The third choice is to configure the firewall at the border router to intercept and forward the BU message to the PA. If they recognize a Binding Update message, they will forward it to the PA of that correspondent network.

If the MN does not wish to conceal its location, then the HA can send the binding warning message to the CN. The CN runs a (user) daemon listening to port number 434 (the designed port for mobile IP). Upon receiving the binding message, the daemon forwards the binding warning message to the PA. The daemon can find the PA through configuration file, which is updated manually if needed.

Updating binding cache at router

After the PA successfully authenticates the binding update message, it instructs the routers to setup the appropriate binding entry for the MN. The PA can do this by sending out a binding cache update message to the appropriate routers, or by any internal mechanism like issuing a SNMP *write* command to the routers. There are two operation modes of the PA scheme, namely the Basic mode and the Advance mode. If the operation mode is Basic, then the PA will update only the binding cache at border routers (BRs) (dotted lines #2 in figure 1), while in the Advance operation mode, the PA will update the binding cache at both the BRs and the subnet router (SR) (dotted lines #3 in figure 2).

Tunneling packets from CN to MN directly to the CoA by the routers

When packets from a CN to an MN reach a router, which has a binding entry for the MN's CoA, the router will encapsulate these packets using the binding cache entry for the MN, and tunneled these packets to the CoA of the MN. In the Basic mode, only the BRs have the bindings, so the BRs just tunnel the packets to the CoA and do nothing else (thick lines #4 and #5). We can see that if the Home and foreign networks are served by different BRs, this may cause some overhead in the correspondent network.

In the Advance mode, if the subnet router for the CN has the bindings for the MN, it will encapsulate the packets to the CoA, and does nothing else (thick line #6). The BRs will not involve in this process. If the SR does not have the binding, then the packets will ultimately reach the BRs, which will tunnel the packets to the CoA as in the case of the Basic mode.

However, in the Advance mode operation, after tunneling the packets to the CoA, the BRs will informs the PA about this new CN. The PA will update the binding cache at the SR of the new CN according to the binding cache updating procedure described above. After that, the packets from the new CN can be tunneled directly by the SR. We can see in figure 1 that tunneling by the SR (line #6) is much more efficient then tunneling by the BRs (lines #4 and #5).

3. ENTITIES DESIGNS AND IMPLEMENTATION

This section explains the modules of the Peer Agent Daemon (PAD) and the Route Binding Cache Daemon (RBCD). Then an experiment of the initial implementation of the daemons is provided.

3.1 The Peer Agent Daemon

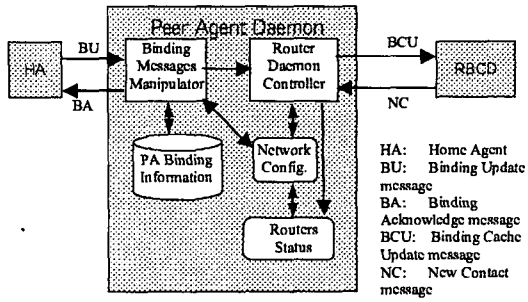

Figure 2. The Peer Agent daemon

The Peer Agent consists of the following modules:

Binding Messages Manipulator (BMM) module. This module listens to the designated UDP port for Mobile IP and exchange binding messages with HA. After authenticating the BU message from HA, it instructs the Router Daemon Controller module to update the binding cache at the routers.

Router Daemon Controller (RDC) module. The main task of this module is to receive the information from the BMM module, and update the binding caches at the appropriate routers.

PA Binding Information module. This module holds all the information necessary for the PA to perform replay protection for BU messages from HA and maybe used to preventing duplicate BU messages.

Network Configuration module. The main task of this module is to return to the RDC the list of destination routers that should receive the router cache update message, depending on the operation mode. If the RDC module asks for the list of the border routers, then that list is returned. Or if given an IP address of the CN by the RDC module, this module returns the IP address of the subnet router(s) that is (are) serving the CN.

Router Status module. This module stores the list of routers (both the Border Routers and the subnet routers) that are not currently able to accept binding cache update messages about new binding entries.

3.2 The Route Binding Cache Daemon

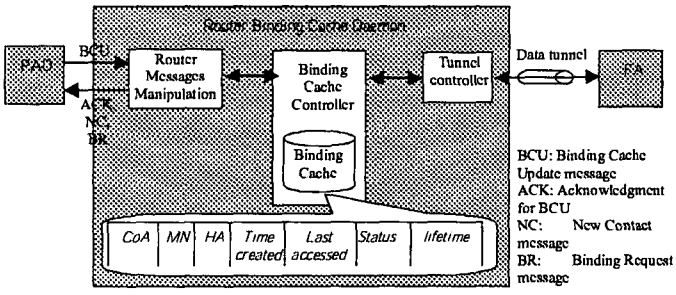

Figure 3. The RBCD daemons

The Route Binding Cache Daemon consists of the following modules:

Router Messages Manipulation module (RMM). This module receives the instructions from the PAD about a binding of an MN. It then signals the BCC module (see below) to update the binding cache and/or the tunnel/route to the CoA/MN.

Binding Cache Controller module (BCC). Upon receiving the information from the RMM, this module processes the binding cache database as well as creates the tunnel and/or the route to the CoA/MN. When a binding entry at the BCD (see below) expires, the BCC will instruct the TC (see below) to delete the correspondent tunnel/route.

Binding Cache Database (BCC) module. The Binding Cache Database module holds the binding entries, and this module is part of the BCC module. The number of entries of the binding cache should be decided according to the size of the network as well as the capability of the router.

Tunnel Controller module (TC). This module has two main jobs, the first is manipulating the tunnels and the second is monitoring the tunnels. It will create or delete a tunnel (or a route over the tunnel) based on the instruction from the BCC module.

3.3 Initial Implementation and experiment

We have implemented the Peer Agent daemons using C language in Linux environment. The daemons can cooperate to perform the basic function of the RO protocol, which is to install a route to the MN over the tunnel (from the router to the CoA) at the RBCD as a result of a Binding Update message received by the Peer Agent Daemon. However, for the time being, the daemons only work in the Basic mode.

When the PAD receives a BU message from the HA Emulator, which reads information from a configuration files to construct the Binding Update message, it sends to the RBCD a router cache update message. The RBCD will setup the binding entry for the MN (the home address is 192.169.1.20), and setup the tunnel between interface 133.9.108.34 of BR1 to interface 192.168.1.76 of BR2. The RBCD will also add a route to 192.169.1.20 to the tunnel.

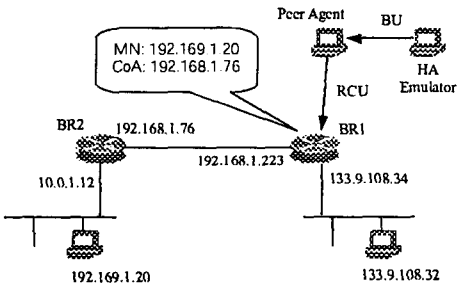

Figure 4. The experiment setting

4. ANALYSIS AND FUTURE WORKS

Compared to the RO protocol in [1], the Peer Agent scheme fulfils two most important requirements:

- Enabling RO at the correspondent network without any changes to the CNs

- Supporting "limited privacy", because only network entities such as the PA and the routers know about the mobility binding of the MN.

In addition, the working of the PA scheme is compatible with that of [1]

Compared to other similar approaches ([2], [3]), the Peer agent is the only scheme that supports efficiently for larger network with more than one border router.

However, there are some issues that need further consideration. The first is how to divide a large network into smaller ones, with each served by a PA to allow faster reaction from PA. How the network is divided may depend on many conditions, for example the routing scheme is used, or the administrative scheme for the network.

The other issue is how and when we should refresh the binding entry at the router. In [1], a binding entry can be refreshed if, for example, the CN knows that it still has an open TCP connection with the MN. It is difficult to detect that information in the PA scheme; however it is possible that we can derive such information from monitoring the traffic over the tunnel.

The last issue is that when the MN moves to another CoA, how the binding update message is sent to the PA. Because some CNs that are contacting the MN at the time of the handoff may belong to the same correspondent network served by a PA, the HA should send only a binding update message to that PA. But how the HA knows which CNs are served by which PA?

5. CONCLUSIONS

This paper proposes a scheme for Route Optimization for large network, called the Peer Agent scheme. A new agent called the Peer Agent is introduced into the correspondent network, and binding caches are added to the routers. The PA processes the Binding Update message from Home Agents, and updates the binding cache at the routers. The routers will use the entries in the binding caches to tunnel packets from hosts inside the correspondent network to the current CoA of Mobile Nodes.

This scheme helps realizing RO in large correspondent networks and the RO operation is transparent to CNs. Therefore, it does not require CNs to update their OSs, as well as it supports "limited privacy". Advance operation mode also optimizes the route of traffic inside a correspondent network.

References:

[1] C. Perkins, and D. Johnson, "Route Optimization in Mobile IP", IETF Internet Draft, September 2001.

[2] Vandali R. et. al, "Agent-based Route Optimization for Mobile IP", *Proc. Of Vehicular Technology Conference*, pp. 2731 - 2735 vol.4, 7-11 Oct. 2001.

[3] Takeshi Ihara, Hiroyuki Ohnishi and Yasushi Takagi, "Mobile IP route optimization method for a carrier-scale IP network", *Proc. Of Sixth IEEE International Conference on Engineering of Complex Computer Systems*, pp.120 – 121, 2000.

[4] Qiang Gao and A. Acampora, "A Virtual Home Agent based Route Optimization for Mobile IP", *Wireless Communications and Networking Conference*, pp. 592 - 596 vol.2, 23-28 Sept. 2000

[5] Rong Zheng, Ye Ge and J. C. Hou, "A case for Mobility Support with Temporary Home Agents", *Proc. Of Tenth International Conference on Computer Communications and Networks*, pp. 226 – 233, 15-17 Oct. 2001

[6] Chun-Hsin Wu, et. al, "Bi-directional Rout Optimization in Mobile IP over Wireless LAN", *Proc. Of Vehicular Technology Conference, IEEE 56th*, pp. 1168 - 1172, 24-28 Sept. 2002

[7] Serap Altay, Orhan Gazi, "Performance Analysis Of Mobile IPv4 With And Without Route Optimization", *IJCI Proceedings of International Conference on Signal Processing*, ISSN 1304-2386, September 2003

[8] Hao Chen and Ljiljana Trajkovic, "Simulation of Route Optimization in Mobile IP", *Proc. of the 27th Annual IEEE Conference on Local Computer Networks*, 2002

[9] C. Perkins (Ed.), "IP mobility support", IETF RFC 2002, Oct. 1996 and revised in September 2000.