EE6390

Introduction to Wireless Communications Systems

Fall 1999

Research Report

Mobile IP in General Packet Radio System

Kelvin K. W. Wong
Ramzi Hamati

Date: Dec. 6, 1999

1.0 Abstract

Tunneling is one of the key elements in General Packet Radio Service (GPRS), a service offered by Global System for Mobile (GSM) communications. GPRS Tunneling Protocol (GTP) implemented in GPRS will provide data tunnels between GSM mobile subscribers and external data networks. However, a potential problem exists in that GPRS cannot provide optimal routing, in turn causing traffic contention in GPRS networks. In this paper, we investigate this problem and provide a mechanism that will optimize the routing by distributing the Location Directory (LD) information away from Gateway GPRS Support Node (GGSN). Also, we present our LD design and implementation in a GPRS mobile IP network.

2.0 Introduction

In GPRS architecture, the tunneling mechanism is deployed to allow transferring multi-protocol packets between the mobile station (MS) and external networks. GTP is implemented between the Service GPRS Support Node (SGSN) and the GGSN. However, this implementation will cause all datagrams to be routed to the GGSN. In other words, traffic contention will occur in the GGSN, thus impacting GPRS performance. In the next section of this paper, we analyze the potential problem of GTP in GPRS. Then, we present a scheme to efficiently distribute LD information, which provides the information necessary to locate the forwarding address of a mobile host in a mobile networking system, away from GGSN. We discuss the significance of distributing LD information with respect to optimizing the routing traffic in GPRS. Finally, we present our LD design and implementation in a GPRS network.

3.0 Problems in GPRS

As figure 1 illustrates, datagrams destined for a mobile node will be routed to its home network in the same way as for any IP datagram. Then, the home agent GGSN tunnels the datagrams to the mobile node's current care-of address. The Internet host is required to route each datagram for the mobile indirectly through its home agent. Similarly, the mobile node has to route each datagram via its home agent to the Internet host. Clearly, the GGSN is serving as the gateway between of mobile and Internet hosts. Working with the assumption that mobile hosts in networking systems move randomly and frequently, it

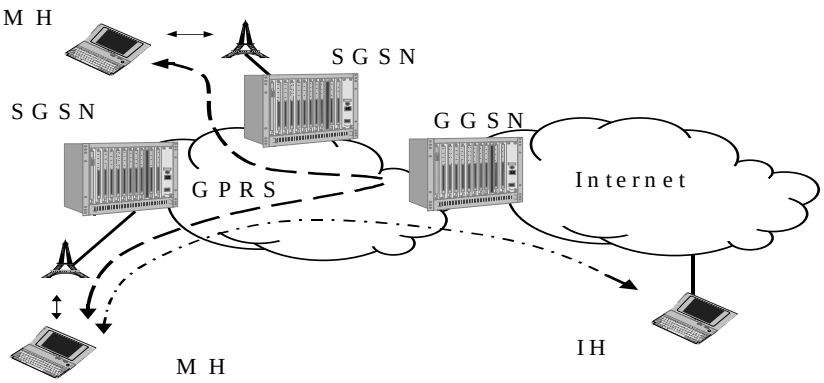

Figure 1 GPRS Network Structure

is more efficient to have a GGSN serving as a central node storing mobile location directory information and forwarding the mobile's packets to its SGSN.

However, the problem contained in the network structure has received considerable attention due to its lagging performance. Consider the following two common scenarios:

- Transferring packets between mobile and Internet host.
- Transferring packets between two mobile hosts in the same GPRS network.

All traffic in the current GPRS architecture is routed to GGSN, thereby causing contention that negatively impacts the performance of the mobile network.

4.0 Proposed Solution

One key issue in achieving high performance mobile networking is providing optimal routing. Over the past several years, many proposals have been made for supporting mobile IP networks. A vast majority of these proposals have been designed to be compatible with today's TCP/IP-based Internet. But only a few of them are really focused on improving the routing efficiencies. Furthermore, security issues also prevent these proposals from becoming widely adapted standards of mobile IP.

However, there are two proposals that can solve the performance problem in GPRS and provide adequate security protection for mobile hosts. Let us consider two common scenarios and present their role in improving the performance of GPRS

- *Triangle Routing*

Internet Engineering Task Force (IETF) has created a group to come up with a proposal for near-term Internet deployment (Figure 2). In this design, each mobile host retains its home address regardless of its location. When mobile host visits a foreign network, it registers with the foreign agent; the home agent keeps LD information associated with the mobile's current point of attachment. All datagrams addressed to a mobile host are routed via the home agent. However, the packets in the reverse direction (those originating from mobile host to Internet host) are relayed along the shortest path by the Internet routing system. This technique is known as the triangle routing. This proposal prohibits caching of LD information because of security concerns. Hence, route optimization is not possible but it releases the traffic from home agent in the reverse direction.

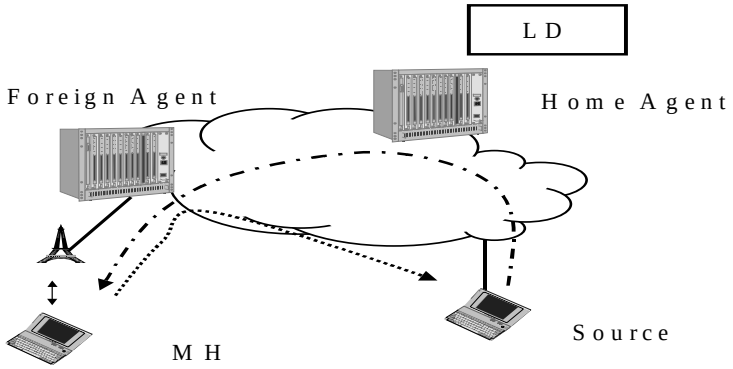

Figure 2 Triangle Routing Mobile IP Proposal

- *Loose Source Routing*

The Loose Source Routing (LSR) proposal (Figure 3), also based an existing IP, allows each mobile host to retain its home address regardless of current location. Similar to

triangle routing, the home agent stores the mobile host's LD information. The packets sent to the mobile host first arrive at the home agent. To forward the packet, the home agent inserts an LSR option, specifying the current foreign agent as the transit router. The inserted option causes this packet to be routed to the mobile host via the foreign agent. When the mobile host sends a reply to the source, it also inserts the LSR option in all outgoing packets, which designate the current foreign agent as a transit router. When the source host receives this packet, it will reverse the recorded route. All outgoing packets originating from the source host will have the reversed route inserted, and therefore will be routed along the optimal path. This proposal relies on the end host's ability to perform route reversal. Unfortunately, the vast majorities of Internet hosts either do not perform correct route reversal or drop LSR packets due to the security risk involved.

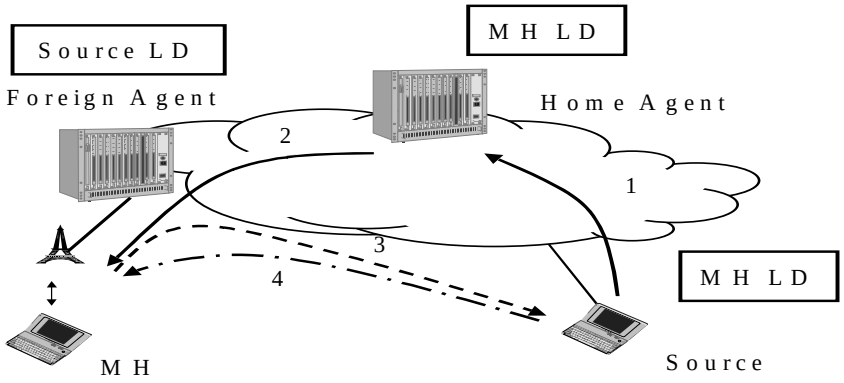

Figure 3 LSR Mobile IP Proposal

Although the two proposals appear to be different, they share many similarities: a basic network architecture similar to the current GPRS network, a home agent GGSN and a foreign agent SGSN, mobile hosts retain home address regardless of current location, home agent stores LD information. Based on the pros-and-cons discussed earlier, we argue the merit of each proposal in the following cases:

- *Transferring packets between mobile host and Internet host.*

We submit that triangle routing is the best candidate for this scenario. It can retain the original security advantages of a GPRS network. For instance, firewalls in the GGSN block unspecified packets from entering via the Internet. It also releases approximately half of the capacity burden from GGSN.

- *Transferring packets between two mobile hosts in the same GPRS network.*

We believe that security is no longer an issue if source and destination are on the same GPRS network. GTP can secure communication within GPRS networks. In addition, we can implement new routing schemes on GTP without changing the existing IP network. In addition, LSR can be deployed to optimize GRPS performance on route reversal. After forwarding the first incoming packet to the destination mobile host, the GGSN will be not involved in handling any further packets between the two mobile hosts until one of the mobiles hands off to a new foreign agent.

5.0 Implementation

In order to implement these two proposals, we first have to rearrange the original GPRS

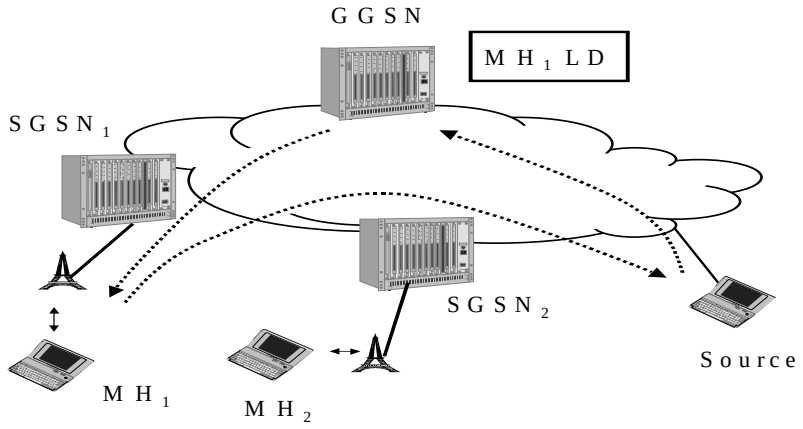

Figure 4 Triangle Routing in GPRS

network (Figure 1). We combine the GPRS and the Internet networks together. Therefore, the GGSN will no longer be a gateway node. Rather, it becomes a regular node in an IP network (Figure 4). In this case, the foreign agent SGSN can apply the triangle routing scheme to return packets to the Internet host via the shortest path.

With the same network configuration, we can also implement our modified LSR scheme on GPRS. In our modified LSR scheme, the mobile host will not keep its destination mobile host's LD information. The foreign agent SGSN, which serves the mobile host, caches the LD information. If the SGSN has LD information for the destination mobile host, it will be able to send packets directly back to the mobile node without the service of the GGSN. First, let us introduce three LSR optional messages used for distribution of LD information:

- LD warning message (from SGSN to SGSN) is used to inform the source SGSN that it has out-of-date LD information for the mobile node.
- LD request message (from SGSN to GGSN and forwarded to destination SGSN) is used by the SGSN to request the destination mobile host's current LD information from the GGSN.
- LD update message (from SGSN to SGSN) is used to send a notification regarding a mobile host's current LD on reversal direction.

These messages contain information such as the care-of address of a mobile host, the IP address of the SGSN, and additional control information specifying features made available by SGSN. Therefore, any SGSN in GPRS may maintain LD information to optimize its own communication with mobile hosts.

Figure 5 is an example that shows how LD information is cached over SGSNs when the first packet is sent from a source mobile host to a destination mobile host:

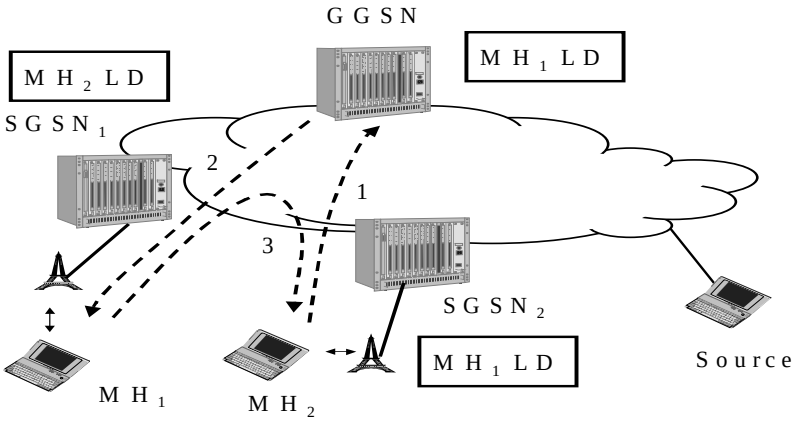

Figure 5 LSR in GPRS

1. The source SGSN extracts the destination address from the packet and searches if this destination is in the same GPRS network from its routing entries. If the outcome is true, it forwards the packet to the GGSN with an LD request message.
2. The GGSN forwards the packet to the destination SGSN with an LD request message that includes the LD information of the source mobile host. The destination SGSN caches the address of source mobile host and source SGSN.
3. On the reverse direction, the destination SGSN returns the packet with an LD update message to the source SGSN. Therefore, the source SGSN can cache the destination mobile host's LD information.

However, when a mobile host changes its SGSN, a procedure known as handoff, LD information in the GGSN will be changed first upon the mobile host's registration from the new SGSN. Then the LD information in the old SGSN will be during the registration process. Due to the fact that the GGSN has no knowledge of which SGSN has the old mobile host LD information, there is no any mechanism to update all old LD information

distributed over other SGSNs. If a mobile host sends to the old SGSN, the old SGSN will forward the packet back to the source SGSN with LD warning message. The source SGSN will remove the LD information and send the packet to the GGSN to start the whole process of caching the new LD information again.

6.0 Conclusion

Given the new modifications in the GPRS networks, the amount of traffic to the GGSN is dramatically reduced. In particular, the triangle route approach eliminates one-half of the data packets from entering the GGSN, which will improve the performance of the GPRS network. The future and ultimate success of mobile IP hinges around the effectiveness of routing algorithms capable of obtaining optimal routes without compromising security of the network.

7.0 Reference

1. ESTI, “Digital cellular telecommunication system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1,” GSM 02.60 version 5.2.0, Valbonne France.
2. Charles Perkins, Pravin Bhagwat and Stish Tripathi, Network Layer Mobility: An Architecture and Survey, IEEE Personal Communications, June 1996.
3. Peter Wong and David Britland, Mobile Data Communication Systems, Boston, Artech House, 1995