Seamless PPP Migration between Disparate Wireless Networks

Takayuki TAMURA, Hosei MATSUOKA, Minoru TAKAHATA
Research Laboratories, NTT docomo
3-5 Hikari-no-oka, Yokosuka, Kanagawa, 239-8536 Japan
E-mail: { tamuratakay, matsuoka, takahatam } @nttdocomo.co.jp

Abstract: This paper proposes a method of migrating PPP connections among heterogeneous networks without interrupting active sessions. We design and implement extended PPP modules for the FreeBSD kernel and pppd-2.3. We use the extended PPP modules to demonstrate seamless migration between 3G networks and Wireless LAN (WLAN) networks; the migration is transparent to Layer-3 and above. The new PPP connection uses the same IP address assigned to the old PPP connection. The method is effective in allowing network operators to migrate network traffic from their own network to other networks, and also useful in allowing users to access higher quality wireless access links after making a connection.

1. Introduction

In recent years, a variety of wireless access networks such as 3G, WiMAX and wireless LAN (WLAN) have become available, and mobile devices that support multiple wireless access interfaces are popular in the mass-market. These different networks have their own advantage and disadvantages. The 3G networks offer wide service area but low data rates. WLANs offer higher data rates but only support small spot areas. Mobile devices with multiple wireless access interfaces offer the possibility of using these different networks in a complimentary manner. However, it was not originally possible to switch a communication session from one network to another. Several solutions have been proposed. All are designed for Layer-3 or upper layer use, so the IP address of the mobile device changes at the time of migration which disrupts real-time services. For this reason, we employ a Layer-2 approach and propose a seamless migration scheme that supports different access links and is transparent to Layer-3 and above. Currently, PPP[1] connections are used for packet communication in 3G networks. Therefore, we designed extended PPP modules that migrate active PPP connections from the 3G networks to other types of networks. In our proposal, the latter use Layer-2 Tunneling Protocol (L2TP) to support migration[2]. Since the mobile device uses L2TP to establish PPP connections over any IP network, it can set and utilize connections to the other IP networks once it obtains the IP address of the new network.

The PPP migration proposed in this paper gives MNOs and MVNOs the possibility of seamlessly migrating active connections from the 3G network to the public WLAN networks and then the reverse. It yields more efficient usage of the 3G network. Users can receive better service quality without being aware of changes in the wireless access.

The rest of the paper is organized as follows. In the next section, we review existing works in this area. Section 3 proposes PPP Extension and introduces the resulting migration scheme. Its implementation is described in Section 4. In Section 5, we discuss the findings of the scheme in actual use. Section 6 concludes the paper.

2. Related Works

Modern mobile devices contain several wireless access interfaces. Mobile devices with 3G and the WLAN interfaces can switch and use either of the networks for communication according to the situation if both networks are available. However, when a mobile device attempts to change from a 3G link to a WLAN link, the communication is interrupted due to the change in IP address.

To seamlessly replace a 3G link with another link, we need an extended protocol. Some solutions at different layers of the protocol to support migration between heterogeneous networks have been proposed[3,4,5]. They, and their drawbacks, are described below.

Mobile IP

Mobile IP[6] is a popular protocol for realizing mobility on Layer-3. In a Mobile IP system, the server called Home Agent(HA), which has a fixed IP address, transfers the IP packets from the correspondent node

(CN) to the mobile device. The mobile device can send the IP packets to the CN directly. When the mobile device moves to another network and it's IP address changes, the mobile device obtains the new IP address and notifies the IP address to HA. HA registers the new IP address to relay subsequent packets correctly. Therefore, HA can relay requests from the CN to the mobile device, wherever it is. A drawback is that the mobile device must use its home address for all communication even if only the 3G network is used. This raises the protocol overhead for normal communications through 3G networks, and may also decrease device usability in normal communication.

SCTP

SCTP[7] is a transport layer protocol standardized in IETF, which supports multi-stream communication. SCTP can establish two or more communication paths between two end-points and combines them through an association with a shared port number. The mobile device as an endpoint can select one of the communication paths in the association and change the path during communication. Unfortunately, SCTP can't add a new communication path after establishing a connection, and so cannot utilize any new network. One extension of SCTP, called mSCTP, offers dynamic address reconfiguration which allows a communication path to be added or dropped during communication[8]. Li et al. used mSCTP to migrate between UTMS and WLAN [9]. A limitation is that both end-points need to support mSCTP.

Session Handover with SIP

SIP[10] is an application layer protocol standardized in IETF for setting up and breaking down multimedia application sessions such as VoIP. SIP controls session initiation, modification, and termination. The entities of the SIP system are the user agent and the SIP servers (proxy server and redirect sever). The user agent is identified by a specific identifier such as the SIP URI. The proxy server relays the negotiation messages between the mobile device and the correspondent node. The redirect server notifies the present location of the mobile node to the correspondent node. These servers also can manage the location of the mobile device. When an SIP negotiation starts, the mobile device, as the user agent, sends communication request messages, called INVITE messages that carry the IP address of the mobile node to the correspondent node through the proxy server. The correspondent node sends back acceptance to the mobile device. After the mobile device sends back the acknowledgment message to the correspondent node directly, the SIP connection is established. Once the communication path is established, the mobile device and the correspondent node can communicate directly. If the mobile device obtains a new IP address from a new network, the mobile node sends a new INVITE message with new IP address to the correspondent node. The correspondent node can detect the new location of the mobile device and start the communication using new IP address. It enables the mobile device to provide migration. A limitation is that only SIP-based applications can use the mobility function, others cannot.

These solutions are implemented on Layer-3 or upper above, so that the IP address set for the session is changed when moving to the new network. This interrupts the provision of real-time services.

To realize seamless migration we focus on PPP, which is the basic protocol for data communication in the 3G network.

Anand et al. proposed a technique that enables a PPP connection to migrate between Packet Data Serving Node (PDSN)s for low-latency handoff [11] . Unfortunately, it targets horizontal migration in 3G networks. Our PPP Migration enables vertical handover such as from the 3G network to other networks.

Our proposal enhances the existing PPP server and PPP client with PPP Extension; that is, new network components aren't required. PPP is a Layer-2 protocol, and layer-2 migration does not demand a change in IP address for migration.

3. Proposed Extension

PPP Extension provides Layer-2 migration in which a PPP connection can be switched between networks without re-establishing the PPP connection; the original IP address does not have to be changed. Our proposal changes PPP so that it can support migration to a new network that provides better communication such as a WLAN. To enable the mobile device to establish a PPP connection over the public Internet, the proposal employs L2-tunneling.

Our proposal is suitable for 3G devices, because PPP Extension offers backward compatibility with the native PPP. In our method, the first PPP connection is established in the same way as native PPP. When handover is required, the mobile device simply establishes one more PPP communication path using the new network.

Fig.1 shows an example of the network structure for PPP migration. The mobile device accesses the PPP access server and establishes a PPP connection. In the negotiation phase, the PPP access server assigns an IP address to the mobile device. The device communicates with the corresponding node via the PPP connection

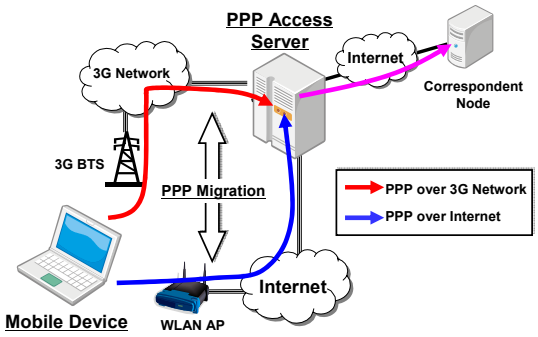

Fig.1 : Concept of PPP Migration

through the PPP access server. Our proposal establishes multiple Layer-2 connections over the different networks between the mobile device and the PPP access server. These multiple Layer-2 connections are logically aggregated to form a single PPP connection. In our PPP migration proposal, the mobile device switches between the Layer-2 connections established as PPP connections. The IP address doesn't change during migration, which realizes seamless migration.

3.1 System Components

Fig.2 overviews the system components of the proposed scheme. The mobile device has a 3G cellular interface and a WLAN interface (WLAN is described hereafter only for convenience). The PPP access server has two network interfaces; one is associated with the 3G PS (Packet Switched) network and the other is associated with the public Internet. The corresponding interfaces on the device and PPP access server are connected to each other. It is assumed that the PPP access server is connected to the gateway of 3G PS network, and the PPP connection through the 3G PS network is extended to the PPP access server. The PPP connection through the public Internet is established by L2 tunneling between the mobile device and the PPP access server. PPP Extension enables the PPP adaptor to handle multiple connections. The PPP adaptor can select and change the connection anytime, and the change is transparent to the upper layers.

3.2 PPP Extension

PPP Extension modifies the sub-protocols that configure and establish PPP connections. A PPP connection is established in 3 Phases: Link Control Phase, Authenticate Phase, and Network Control Phase. Link Control Phase uses Link Control Protocol (LCP) to configure the link-specific options and establish the PPP communication link. After that, the Authentication Phase confirms the access right of the mobile device to the PPP access server. In the Network Control Phase, the IP layer is negotiated by Network Control Protocol

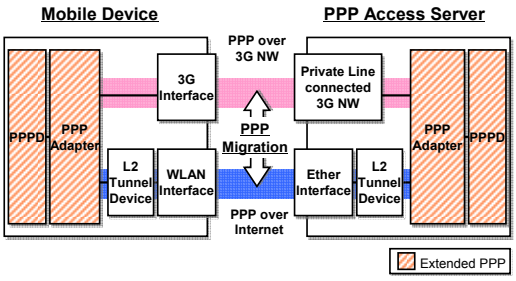

Fig.2 : System Components

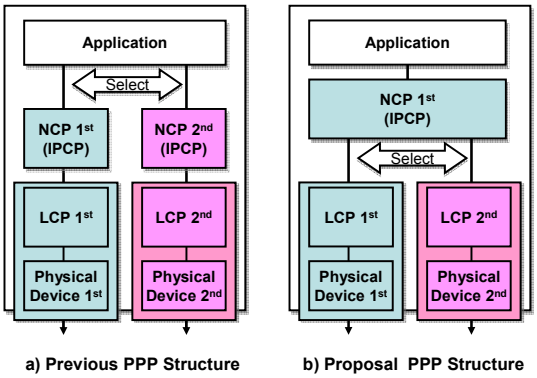

Fig.3 : Relations between Sub-protocols

(NCP). On the 3G network, Internet Protocol Control Protocol (IPCP) is generally used as NCP to configure the IP layer. IPCP enables the PPP access server to assign an IP address to the mobile device. This address allows the mobile device to use the PPP connection.

NCP can transfer IP packets through the PPP communication link established by LCP. Fig.3 shows the relations among the physical device, LCP, and NCP, when two PPP connections are established on the mobile device. Fig.3 a) shows the relations when native PPP is used, one NCP is established for each LCP. In this case, the two NCPs assign two IP addresses to the mobile device. This ensures that real-time services are interrupted at the time of migration. Our proposal, shown in Fig.3 b), associates one NCP with multiple LCPs. That is, the IP address assigned by NCP is shared by the two LCPs. When PPP migration is performed, the mobile device simply changes the IP packet flow through one LCP to the other. Sharing one IP address between the two PPP connections enables seamless PPP migration. PPP Extension performs these steps at each end-point, the same as native PPP.

When the PPP access server associates the NCP with the two LCPs, the PPP access server needs to confirm that the 1st LCP and 2nd LCP were actually requested by the same mobile device because the PPP access server will receive many request messages from many PPP clients. In principle, our proposal allows one NCP to be associated with any number of LCPs, so the PPP

access server needs to know the correct associations. To recognize each LCP, we use the one time password scheme.

In the LCP negotiation for the 1st PPP connection, the mobile device asks the PPP access sever to assign a one time ID and one time password. The server creates the unique ID and the password and associates them with the 1st PPP connection. The PPP access server sends the ID and Password to the mobile device. The ID and password are flushed from both the server and the mobile device when all PPP connections between the mobile device and the PPP access server are disconnected.

In the LCP negotiation for the 2nd PPP connection, the mobile device sends the ID and the password to the PPP access server. The PPP access server compares the ID and the password received to the ID and the password stored. After the ID and the password are confirmed, the 2nd LCP negotiation becomes complete and an association is formed with the NCP of the 1st PPP connection. If the IDs and the Passwords don't match, the negotiation is interrupted and closed at both sides.

PPP Extension is implemented in both the mobile device and the PPP access server. PPP Extension also offers backward compatibility with native PPP. This enables the clients with either native PPP or extended PPP to connect to the extended PPP access server.

3.3 PPP Extension Sequence

As mentioned above, PPP Extension sets some additional procedures when establishing and migrating PPP connections. This section describes the sequences of the additional procedures. The extended sequences shown in Fig.4 are exchanging the ID and password, LCP authentication, and migration.

The device's request for an ID and a password for LCP authentication is made during LCP negotiation for the 1st PPP connection. The mobile device sends the ID and the password request message to the PPP access server in LCP negotiation. The PPP access server accepts the request and sends back the ID and the password to the mobile device. The PPP access server saves the ID and the password in its own database. The mobile device also saves the ID and the password in its own database.

In LCP negotiation for the 2nd PPP connection, the mobile device sends the stored ID and password to the PPP access server. The PPP access server receives and compares them with its stored data. The PPP access server notifies the result of this authentication to the mobile device. If the 2nd LCP is confirmed, PPP Extension associates the 1st NCP with the 2nd LCP immediately at both the mobile device and the PPP access server. The mobile device's authentication has

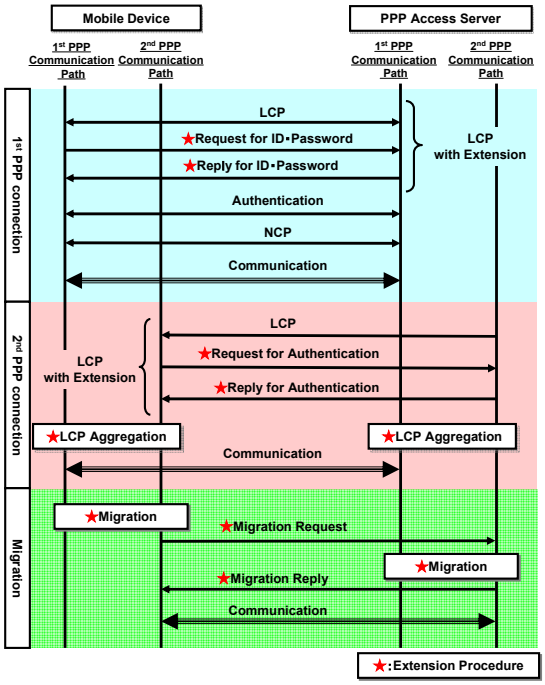

Fig.4 : PPP Extension Sequence

already been completed in the 1st PPP negotiation and the NCP is shared with the 1st PPP connection and the 2nd PPP connection, so that the authenticate Phase and the Network Control Phase of the 2nd PPP negotiation are abbreviated. After the 2nd PPP connection is established, the mobile device can perform PPP migration at any time. The two PPP communication paths between the mobile device and the PPP access server are configured and established independently. When PPP migration is triggered, PPP migration has to be achieved at both sides. The mobile device first replaces its 1st LCP with its 2nd LCP and then requests PPP migration to the PPP access server. The PPP access server receives the request and migrates the LCPs in the order specified in the request, i.e. 1st LCP to 2nd LCP. PPP migration is completed when the mobile device receives the migration reply message from the PPP access server.

PPP migration can be also triggered by LCP Aggregation. In this case, PPP migration is automatically achieved after the establishment of the 2nd PPP connection without recourse to a migration request message.

3.4 L2TP

Our proposal enables PPP migration from the 3G network to another network directly. Hence, the other network must use PPP. The use of L2-tunneling enables the mobile device to establish a new PPP communication path over many other networks and so raise the possibility of PPP migration.

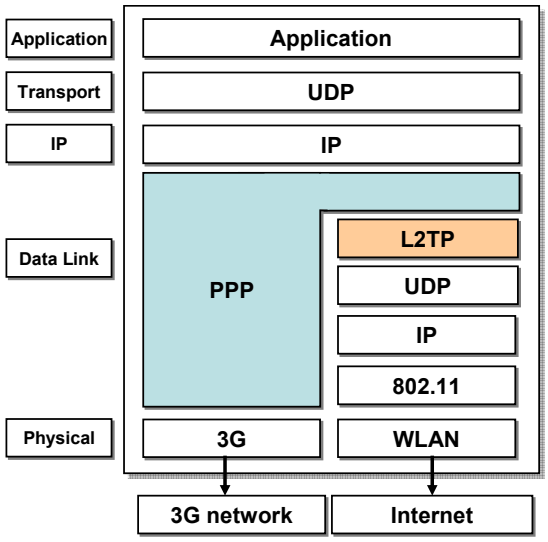

Fig.5 : Protocol Stack of PPP Extension

We employ L2TP since it can make L2-tunnels on the IP Layer. The connection of two endpoints by L2TP appears, to PPP, to be one hop. Thus PPP can establish PPP connections over L2TP tunnels. To make L2-tunnels, it is possible to use the other Layer-2 Tunneling Protocols such as PPTP[12].

Fig.5 shows the protocol stack of PPP Extension with L2TP. As an example, the establishment of a PPP connection over a WLAN network with L2TP is described below. The WLAN network uses the 802.11 standard protocol as the Layer-2 protocol. When the mobile device finds an available WLAN AP, the mobile device obtains its IP address using the DHCP mechanism. L2TP sets an L2-tunnel between the mobile device and the PPP access server using the WLAN's IP address. Once the L2-tunnel is set, the mobile device can start negotiating for PPP connection establishment with the PPP access server.

After the mobile device finishes the on-going sessions, it may destroy the established PPP connection and L2-Tunnel, then use WLAN without extra routings through the PPP access server and protocol overheads.

As mentioned, L2TP can set a L2-tunnel once it has the IP address of the new network (a WLAN in the example). The key point is that the IP address of the new network must be provided to the mobile device.

4. Implementation

In this section, we show an implementation of the proposed PPP migration scheme. We implemented PPP Extension in the PPP device deriver in the FreeBSD-4.11 kernel and pppd-2.3, ensuring backward compatibility with the existing PPP.

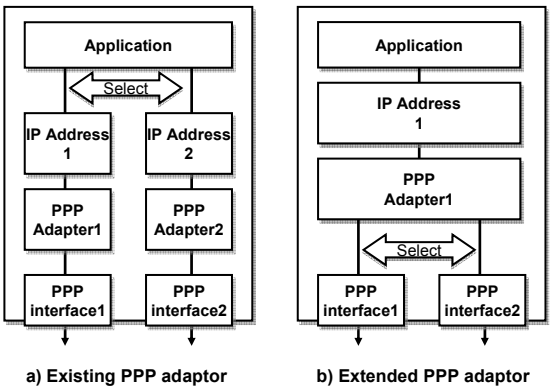

Fig.6 : PPP Extension Adaptor

4.1 PPP Device Driver

Many operating systems create a pseudo-device for a PPP connection and associate it with the physical device, when establishing a new PPP connection. Fig.6 compares the existing PPP adapter to our extended PPP adapter. The existing system creates a PPP pseudo-device for a physical device. Therefore, two PPP adapters are necessary when using two physical links. A single PPP adapter can handle a pair of IP addresses; one for the mobile device and one for the PPP access server. In this case, selecting the physical path to be used for sending packets demands choosing the PPP adapter used in the IP layer. If changing the PPP adapter means changing the IP address, real-time services will be interrupted.

Our proposal associates a single PPP adapter with multiple physical paths. Therefore, the multiple PPP connections share the IP addresses of the mobile device and the access server. In this case, changing the communication path does not require the use of new IP addresses. All active applications can maintain their sessions when the physical path used for communication is changed.

4.2 PPP Extension

pppd is an user daemon that manages the status of PPP negotiation such as LCP, Authentication, NCP. We extended pppd to include the migration function. pppd uses negotiation messages that configure and establish the PPP connection. Fig.7 shows the frame construction of a negotiation message. A negotiation message can reconfigure specific parameters of the PPP connection even during communication. This is very

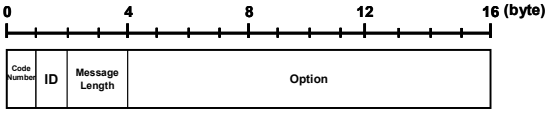

Fig.7 : Negotiation Message Format

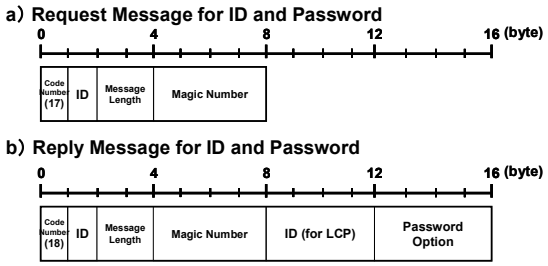

Fig.8 : ID / Password Request and Reply Message

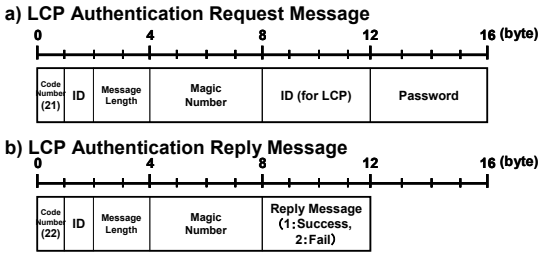

Fig.9 : LCP Authenticate Message

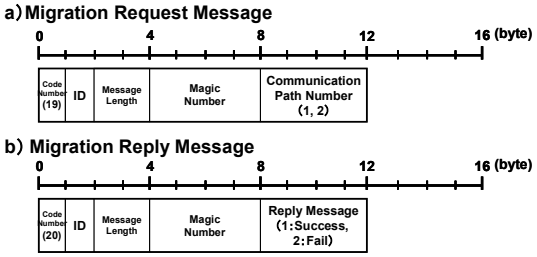

Fig.10 : Migration Message

useful since migration will occur arbitrarily. Each type of negotiation message is identified by a unique number called the code number. We created three new pairs of messages with new code numbers for PPP Extension.

The additional messages are; ID/Password request, LCP authentication, and migration request.

In LCP negotiation for the 2nd PPP connection, the PPP access server needs to confirm that the 1st PPP connection and the 2nd PPP connection are from the same mobile device to associate the LCP of the 2nd PPP connection with the NCP of the 1st PPP connection, see Fig.3. Therefore, we created a message to request the ID and password needed for confirmation. Fig.8 shows the structure of the ID/Password request and reply message. The mobile device sends the request message to the PPP access server. The PPP access server sends back the reply message carrying the ID and password.

In LCP negotiation for the 2nd PPP connection, the ID and password are sent by the LCP authenticate request message as shown Fig.9 a). It contains the ID and password given for LCP negotiation for the 1st PPP connection. The PPP access server sends back the result of authentication by using the LCP authentication reply message as shown in Fig.9 b).

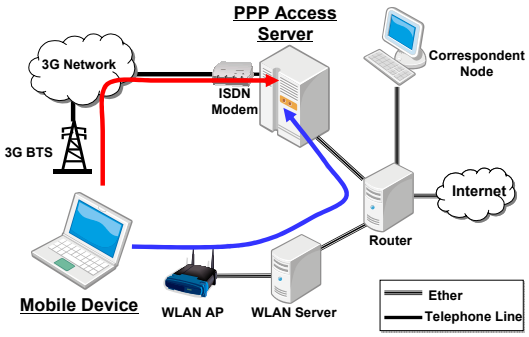

Fig.11 : PPP Migration Prototype System

When PPP migration is required, the mobile device triggers migration at the PPP access server by using the migration request message, see Fig.10 a). The migration request message indicates which path the mobile device will switch to. The PPP access server checks the path number in the message and selects the next communication path. After that, the PPP access server notifies the result of migration to the mobile device by using the migration reply message, see Fig.10 b).

4.3 Prototype System

In order to confirm PPP Extension, we constructed a prototype system consisting of a mobile device and a PPP access server with PPP Extension. The prototype system is shown in Fig.11. The mobile device had 3G and 802.11b WLAN interfaces. The PPP access server offered an ISDN modem connected to the PDSN network and an ether interface for Internet access. The WLAN server is assumed to be a public WLAN service provider and so provides the mobile device with its IP address. The router plays the role of the Internet; it was configured to place PPP access server, the WLAN server, and the corresponding node into different subnets.

The mobile device established two PPP connections to the PPP access server; one through the 3G network (1st PPP connection) and the other through an L2TP tunnel (2nd PPP connection) constructed over the Internet.

In this prototype, the 3G network provided communication speeds of up to 64Kbps (uplink and downlink). On the other hand, the 802.11b WLAN (2nd PPP connection) provided up to 11Mbps (uplink and downlink).

5. Discussion

The prototype system used a fairly basic implementation of PPP Extension. It is easy to posit an additional function that notifies the applications of any migration, allowing them to change the type of packets or own buffer size to match the communication path

being used to raise service quality.

6. Conclusion

We conclude that PPP Extension, proposed herein, provides seamless migration between 3G networks and IP networks such as WLANs.

PPP Extension is very practical since no additional network entity is needed, protocol modifications are small, and backward compatibility is provided with 3G networks. Our proposal sets L2TP in the other IP networks, such as WLANs, and so realizes PPP migration that is transparent to currently active services.

In future work, we plan to confirm the impact of the proposed PPP migration scheme on applications.

References

[1]William Simpson: “The Point to Point Protocol (PPP)”, Internet Engineering Task Force, Request for Comments 1661, 1994.

[2]W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter, “Layer Two Tunneling Protocol "L2TP" ”, IETF, RFC 2661, 1999.

[3]M. Buddhikot, G. Chandranmenon, S. Han, Y.W. Lee, S. Miller, L. Salgarelli, “Design and Implementation of a WLAN/CDMA2000 Interworking Architecture”, Communications Magazine, IEEE, Vol.41, Issue:11, pp.90-100, 2003.

[4]Li Ma, Fei Yu, Victor. C. M. Leung, Tejinder S. Randhawa: “A New Method to Support UMTS/WLAN Vertical Handover Using SCTP”, IEEE Wireless Communications, Vol.11, No.4, pp.44-51, 2004.

[5]Elin Wedlund, Henning Schulzrinne, “Mobility Support using SIP”, Second ACM/IEEE International Conference on Wireless and Mobile Multimedia(WoWMoM’99), 1999.

[6]C. Perkins, “IP Mobility Support for IPv4”, IETF RFC 3220, 2002.

[7]Randall Stewart et al.: “Stream Control Transmission Protocol”, IETF, RFC 2960, 2000.

[8]M. Riegel, M. Tuexen, “Mobile SCTP”, IETF, Internet draft, draft-riegel-tuexen-mobile-sctp-03.txt, 2004.

[9]Seok Joo Koh, Sang Wook Kim, “mSCTP for Vertical Handover Between Heterogeneous Networks”, Web and Communication Technologies and Internet –Related Social Issues-, SI2005, vol.3597, pp.28-36, 2005.

[10]M. Handley, H. Schulzrine, E. Schooler, J. Rosenberg, “SIP: Session Initiation Protocol”, IETF, RFC 2543, 1999.

[11]Anand Kagalkar, Sarit Mukherjee, Sampath Rangarajan, Katherine Guo, “PPP Migration: A Technique for Low-Latency Handoff in CDMA2000 Networks”, Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp.133 – 144, 2005.

[12]K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, “Point-to-Point Tunneling Protocol (PPTP)”, IETF, RFC 2637, 1999.