The Android Intelligent Terminal-Based Implementation for Vertical Handover between Carrier-Grade WLAN and CDMA Networks

Zhou Tao, Shao Zhen, Shen Xiao, Liu Chen, and Xu Zhengfeng

Shanghai Research Institute of China Telecom, South Pudong Road,
Shanghai 200122, P.R. China
{zhoutao,shaozhen,shenxiao,liuchen,xuzf}@sttri.com.cn

Abstract. The popularizing of intelligent terminals and the advent of mobile internet give rise to significant data demand increase upon the mobile networks, even causing data alarm of particular areas. At the same time, the WLAN feature is becoming the standard configuration of these intelligent terminals, which gives opportunity to offload the data flow from cellular networks to WLAN. Therefore, it attracts great research interests from industries to design efficient handover between cellular networks and WLAN. In this paper, we propose a carrier-grade vertical handover scheme based on the Android operation system of intelligent terminals, which will help to inter-system handover without the awareness of users.

Keywords: WLAN, CDMA, WAG, Android, handover.

1 Introduction

There are mainly two types of vertical handover implementation for heterogeneous networks, software-based method and hardware-based method, Media Independent Handover and mobile IP for example. The former is implemented by software, and the continuity of service cannot be guaranteed in this implementation, making the user experience worse. However, if the mobile IP method is applied, the carrier cannot make use of its invested assets. It costs too much for the deployment, especially when the mobiles are large in quantity. In this paper, we propose an vertical handover method applied to WLAN and CDMA networks based on the android intelligent terminals. It makes the terminals handover smoothly without the awareness of users. Particularly, this method does not require any modification for the existing networks. It is some software-based method, but must base on the network deployment of operator.

2 The Converged Architecture for Carrier-Grade WLAN and CDMA Networking

In order to implement the handover operation between WLAN and CDMA networks, it is required that users can pass the authentication of different access networks, such as

H. Qian and K. Kang (Eds.): WICON 2013, LNICST 121, pp. 25–33, 2013.

CDMA 1x PS, CDMA CDMA and WLAN, and access to core networks. Therefore, China Telecom has developed a new network element to complete the carrier-grade converged networking for WLAN and CDMA, realizing the unified authentication procedure of CDMA/WLAN interworking.

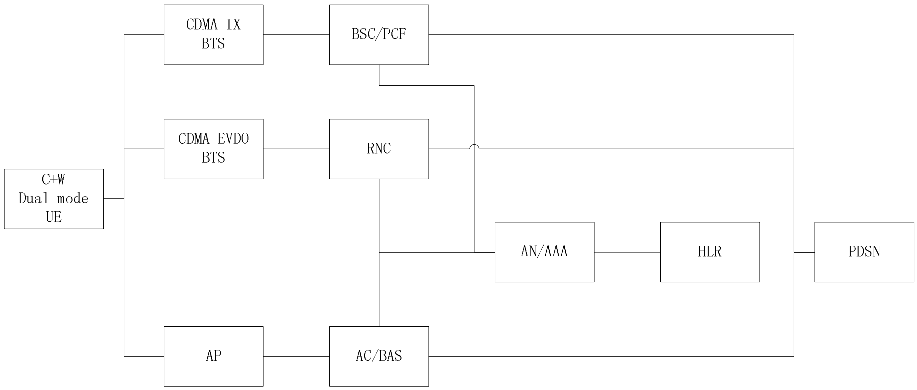

Fig. 1. The interworking architecture for carrier-grade WLAN and CDMA

The interworking architecture of carrier-grade WLAN and CDMA network is presented in Fig. 1. It is noted that the elements PDSN, AAA, AN/AAA, HLR/AuC, RNC, BSC/PCF and BTS are all standard elements in existing CDMA network, and AP, AC/BAS, WAG are the elements typically seen in carrier-grade WLAN networks. Particularly, WAG is the newly introduced converged network element, which fulfills the user authentication procedure to access to WLAN network, making use of the CDMA core network.

The signaling procedure between the terminal and WAG follows the SIP protocol. It completes the authentication procedure of user access to CDMA core networks when it is under WLAN mode. The traffic data is packaged using simple UDP tunnel. The data will pass through the Metropolitan Area Network to access the mobile packet core network and the internet.

3 The Implementation of Vertical Handover for Carrier-Grade WLAN and CDMA Networks

3.1 Signaling Procedure

The signaling procedure of handover between carrier-grade WLAN and CDMA system follows that of inter-PCF handover under the same PDSN. In the architecture of carrier-grade WLAN and CDMA interworking, the network element WAG is treated as a PCF in a manner of position and function. It signals to PDSN in the same manner of PCF.

The handover between WLAN and CDMA is hard handover, which crosses different systems. Due to the independence of CDMA and WLAN communication modules in the terminals, it can establish new communication link while at the same time sustaining the former link. After the target link is established, the terminal will relocate the PPP link route and the former communication link will be released in PDSN.

3.2 The Implementation for Android Intelligent Terminal

3.2.1 Software/Hardware Architecture

The terminal needs more modifications if it intends to handover seamlessly across the WLAN and CDMA network under the simple IP architecture for mobile core networks. The modifications assure that the PPP protocol stack is unique before and after the session handover between terminal and PDSN. The terminal will not restart the PPP negotiation when it handovers to WLAN or CDMA network. The handover control unit is installed in the application layer of terminal to sustain the PPP session connecting to PDSN. When the communication link to target system is established, the handover control unit will intercept the PPP message and handover it to the target network, and make the terminal not to restart PPP negotiation. The handover control unit communicates with the communication modules' driver by the handover control program added in adaption layer, achieves PPP datagram interception and transmission.

The CDMA and WLAN device driver are both network equipments in Android Operation System Linux core, which is controlled by standard Socket interface. The PPP data message is also monitored and intercepted using Socket interface.

3.2.2 Implementation

The mobile terminal equipment contains two processors. The operation system, user interface and applications are executed in AP (Application Processor), which is usually ARM CPU. Android, one of the open source operating system based on Linux, and WLAN communication modules are on AP. The radio communication control software of mobile terminal is operating in another separated CPU which is called Baseband Processor (BP).

This paper presents the implementation for inter-system handover based on AP. The implementation is based on networking architecture for carrier grade WLAN and CDMA interworking and the handover procedure is totally controlled by mobile terminal. No modifications are needed for existing network elements. The implementation involves the newly added handover control unit, SIP session unit, PPP protocol unit, tunneling protocol unit, WLAN communication unit, RIL interface and CDMA communication unit in BP.

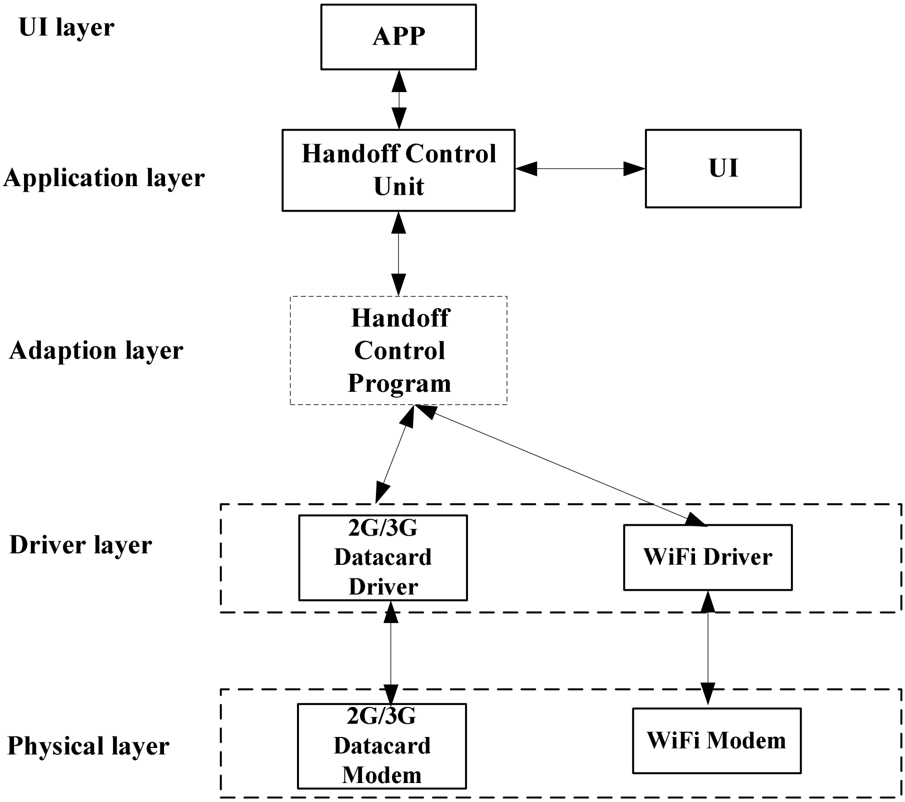

Fig. 2. The architecture for seamless handover across WLAN and CDMA network

- The handover control unit decides whether the handover condition is satisfied or not. If the handover condition is satisfied when the mobile terminal is connecting to internet using CDMA network, SIP session unit is invoked to install SIP session and trigger the handover to WLAN. After the installment of SIP session, the PPP protocol unit is invoked to start PPP dial-up process and deal with the PPP message, in order to establish the WLAN data channel. The PPP data message is intercepted and transferred to tunneling protocol unit. If the handover condition is satisfied when mobile terminal is connecting internet using WLAN, it sends Radio Link Setup Request to RIL interface to trigger the handover to CDMA network. The PPP data transferred by WLAN is intercepted and forwarded to CDMA communication unit.
- SIP session unit is called to setup SIP session by handover control unit.
- PPP protocol unit is implemented by the configuration of Linux protocol stack.（Open the Linux protocol stack management software, start the PPP protocol stack of Linux Operation System, set CONFIG_PPPOE=m and compile the PPPoE module, the PPP protocol stack is open now.）PPP protocol unit is called by the handover control unit to start the PPP dial-up and deal with the PPP message , and is

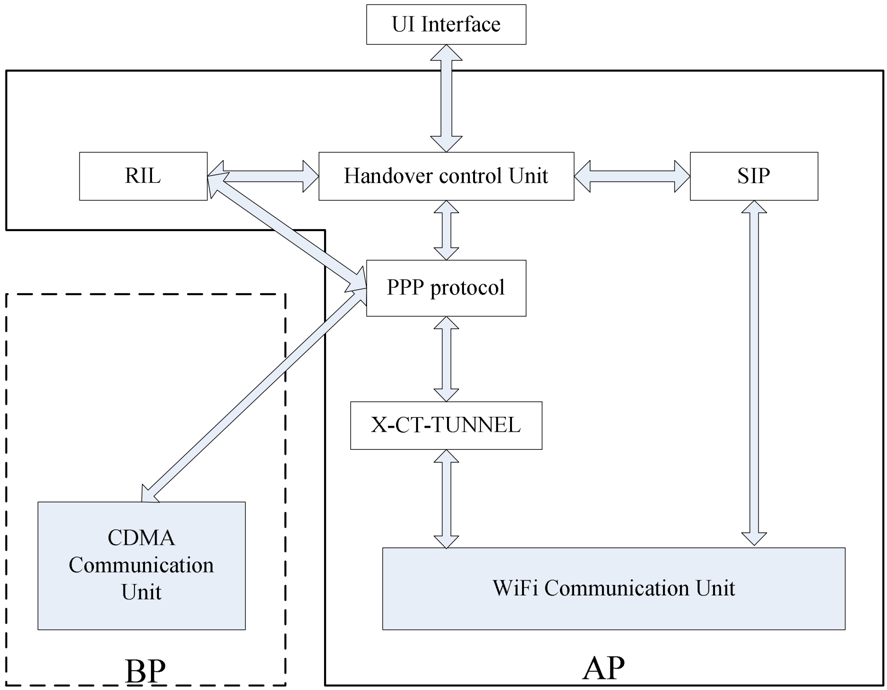

Fig. 3. The implementation based on Android terminal for seamless handover across WLAN and CDMA networks

called by the redirection request from RIL interface to use CDMA communication unit for PPP dial-up and dealing with PPP message. It means that the PPP protocol unit is used no matter the terminal is in CDMA mode or WLAN mode.

- X-CT-TUNNEL tunneling protocol unit is used for encapsulation and decapsulation of data message. The data message intercepted by handover control unit is encapsulated using specific tunneling protocol and is transferred to WLAN communication unit after encapsulation. SIP session unit, PPP protocol unit and tunneling protocol unit fulfill the communication link setup of WLAN.
- WLAN communication unit forwards the data message encapsulated by tunneling protocol unit to WLAN. It turns off the WLAN communication link when CDMA communication unit is transferring the data to CDMA network.
- RIL interface (Radio Interface Layer) redirects the communication link request from handover control unit to PPP protocol unit in AP (Application Processor). It makes use of the unique PPP protocol stack in AP both for the handover from CDMA network to WLAN and the handover from WLAN to CDMA network. RIL interface and PPP protocol unit setup the CDMA communication link.

- User Interface interacts with the handover process controller, and the dial-up or handover state is presented in UI, asking for the parameters of dial-up or handover.

- **WLAN Communication link setup**

The handover from CDMA network to WLAN, is demonstrated in Fig. 3. It includes following steps.

1) When the terminal is connecting to internet by CDMA network, the SIP session unit will be called to initiate SIP session to handover to WLAN if the handover control unit decides that the handover condition is satisfied.
2) After the setup of SIP session, the handover control unit will call for the PPP protocol unit to dial-up and deal with PPP message, in order to setup WLAN data channel.
3) The handover control unit intercepts the PPP data messages previously transferred by CDMA network, encapsulate them using X-CT-TUNNE and then forward them to WLAN communication unit.
4) WLAN communication unit transfer the encapsulated message to WLAN network.
5) CDMA communication unit terminates the CDMA communication link

- **CDMA communication link setup**

The handover from WLAN to CDMA network is also demonstrated in Fig. 3. It includes following steps.

1) When the terminal is connecting to internet by WLAN, it will send link setup request to RIL interface to handover to CDMA if the handover control unit decides that the handover condition is satisfied.
2) RIL will redirect the link setup request to PPP protocol unit in AP, and the PPP protocol unit will call for the CDMA communication unit interface to start PPP dial-up and to deal with PPP messages.
3) The handover control unit intercepts the PPP data previously transferred by WLAN and forward them to CDMA communication unit.
4) CDMA communication unit transfer the data to CDMA network
5) WLAN communication unit terminates the WLAN communication link

4 Performance Testing

The performance testing focuses on the time delay of handover between CDMA networks and WLAN of mobile phone, verification of handover result and the effect of real time service. The statistical server records the delay of handover and the variation of data rate.

1）time delay of handover from CDMA network to WLAN

We check the time delay from CDMA to WLAN in the debug information using the debug tool DebugView. The time delay is defined as the time difference between two events that the terminal receives the 200 OK message--“sent invite message” and the message --“ Switched to WiFi”. It is 90ms in following example as defined：

```
09-27 11:58:56.659 I/pppd    ( 2452): sent invite message
09-27 11:58:56.679 I/pppd    ( 2452): [100] [Call is being processed!]
09-27 11:58:56.749 I/pppd    ( 2452): [200] [Remote phone has answered!]
09-27 11:58:56.749 I/pppd    ( 2452): sip invite succ!!!
09-27 11:58:56.749 I/pppd    ( 2452): sip ok!!
09-27 11:58:56.749 I/pppd    ( 2452): config default route at dev ppp0
09-27 11:58:56.749 I/pppd    ( 2452): Switched to wifi, time use: 3826 us. TimeStamp: Thu Sep 27 11:58:56 2012
09-27 11:58:56.749 I/pppd    ( 2452): evdo === >> wifi
```

Fig. 4. One statistical example of time delay from CDMA to WLAN

2）time delay of handover from WLAN to CDMA network

We check the time delay from WLAN to CDMA network in the debug information using the debug tool DebugView. The time delay is defined as the time difference between two events that the terminal receives the message --“config default route at dev ppp0” and the message --“Switched to EVDO”. It is less than 1ms in following example as defined：

```
09-27 12:01:30.169 I/pppd    ( 2452): config default route at dev ppp0
09-27 12:01:30.169 I/pppd    ( 2452): Switched to EVDO, time use: 1940 us. TimeStamp: Thu Sep 27 12:01:30 2012
09-27 12:01:30.259 I/pppd    ( 2452): rssi -87
09-27 12:01:30.759 I/pppd    ( 2452): rssi -86
09-27 12:01:30.999 I/pppd    ( 2452): [0] [New request received!] method [BYE]
09-27 12:01:30.999 I/pppd    ( 2452): [0] [Bye Received!]
09-27 12:01:30.999 E/pppd    ( 2452): bye received
```

Fig. 5. One statistical example of time delay from WLAN to CDMA

Conclusion of testing ：

1. The handover does not affect the user experience of surfing service

1）high success rate of handover

The download service does not break off before and after the handover and during the handover. The user is not aware of the handover process, and the user experience is not disturbed. The handover success rate is 100% when the wireless signal is well. It is observed from all the test examples that the ping-pang handover will not occur. The testing shows that the performance of vertical handover between WLAN and CDMA network is overall well.

2）low time delay of handover

The time delays of handover of all the test sites are less than 90ms, which means that the service experience using wireless network card is not disturbed.

Table 1. Time delay test results of handover

Test sites	The average time delay of handover under mobility state（ms）	
	CDMA→WLAN	WLAN→CDMA
Test site 1	90ms	1ms
Test site 2	92ms	1ms
Test site 3	88ms	1ms
Test site 4	95ms	1ms
Test site 5	83ms	1ms

During the handover from CDMA network to WLAN, it will set up the tunnel with WAG via the SIP Invite message and then receives the 200 OK message. The time difference is defined as handover duration.

During the handover from WLAN to CDMA network, the radio interface of CDMA network will switch from idle to active state. Handover delay is defined between the mobile phone sends radio link establish request and receives the response of link establish. The log at mobile phone prints the time difference, which is less then 1ms.

2 It is effective to offload the data of CDMA network

The threshold of handover from CDMA network to WLAN is set to -70dBm, and the threshold of handover from WLAN to CDMA network is set to -75dBm. It makes the mobiles to reside in the WLAN for a long time, and will offload the data of CDMA network effectively.

There are three terminals in every test site, two of which are playing audio/video media file and the third is downloading file from FTP. The testing will last for more then 1 hour.

Table 2. Test results of long time keeping

Test site	Handover times		Residence duration(minute: second)			Date flow(Mbits)		
	W->C	C->W	C	W	C:W	C	W	C:W
Test site 1	79	76	27:12	74:03	36.7%	774.9	4518.45	17.15%
Test site 2	48	46	27:04	71:09	38%	790.5	3901.8	20.26%
Test site 3	36	34	48:17	97:23	49.6%	1144.04	5030.7	22.74%

Table 2. *(Continued)*

Test site 4	38	39	76:51	79:21	96.8%	1438.5	4531.95	31.74%
Test site 5	29	31	36:51	66:27	55.4%	905.48	3617.1	20.03%

5 Conclusion

Recently, China Telecom has finished the R&D work based on the scheme proposed in this paper, and the field test is also finished. It is needed to appraise the handover triggering algorithms and improve them at this moment, in order to meet the updated demand from commerce in the future. This type of implementation which does not involve protocol modification and is with minimum modifications for network and terminals, is definitely the way to future technology deployment for operators.

References

[1] 3GPP2 A.S0008-C v2.0 Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network (2009)
[2] Technical Specification for wPDIF equipment of China Telecom (2010)
[3] Smart Wi-Fi Offload Technical Report, Draft, China Telecom (2012)