



VoWi-Fi 技术的实现原理与架构分析

曹磊¹, 王波¹, 邵震², 沈骁², 李一明²

(1. 中国电信集团公司 北京 100033; 2. 中国电信股份有限公司上海研究院 上海 200122)

摘要:随着 VoLTE 技术的商用以及苹果手机等终端对 Wi-Fi calling(Wi-Fi 呼叫)的支持, VoWi-Fi 技术又一次成为了业界关注的热点。对 VoWi-Fi 技术的实现原理、架构及关键问题进行了介绍与分析, 研究了其他几种 VoWi-Fi 的技术实现方案, 并提出了与 VoLTE 融合的 VoWi-Fi 技术在部署中应考虑的问题。

关键词: VoWi-Fi; Wi-Fi 呼叫; S2b

doi: 10.11959/j.issn.1000-0801.2015219

Principle and Architecture Analysis of VoWi-Fi Technology

Cao Lei¹, Wang Bo¹, Shao Zhen², Shen Xiao², Li Yiming²

(1.China Telecom Corporation, Beijing 100033, China;

2.Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: With the commercial application of VoWi-Fi technology and support of terminals such as apple mobile phone for Wi-Fi calling technology, VoWi-Fi technology has become a hot spot in the industry once again. The principle and architecture and key issues of the VoWi-Fi technology were introduced and analyzed, other VoWi-Fi technical implementation schemes were also studied. The problem of technology deployment of VoWi-Fi technology which merges with VoLTE which should be considered was put forward.

Key words: VoWi-Fi, Wi-Fi calling, S2b

1 引言

很长一段时间以来, 随着移动互联网业务的高速发展, 电信运营商始终专注于网络功能的增强和性能的升级, 以应对呈爆发式增长的数据业务, 而对于语音业务则甚少关注, 但随着 LTE 网络的规模发展, VoLTE 技术已经成为移动通信业的热点。

2014 年苹果推出 iOS 8.0 操作系统中的 Wi-Fi calling (Wi-Fi 呼叫) 技术, 支持基于 3GPP S2b 方案^[1]的 VoWi-Fi, T-Mobile、EE 等多家运营商同步提供了相应的 VoWi-Fi 商

用产品, 同时对 Wi-Fi calling 技术在终端产业链上的支持力度也得到了大幅提升, 更多的如三星、HTC 等 Android 终端也陆续开始支持 3GPP S2b 方案。

对于电信运营商而言, VoWi-Fi 技术可以利用近几年已在室内大量建设的 Wi-Fi 网络, 弥补蜂窝网室外基站对室内的覆盖不够而使得用户接收信号较差的不足, 在提高资源利用率的同时有效提升语音业务的用户满意度。对用户而言, 使用 VoWi-Fi 业务可以在基本不改变业务使用习惯的基础上, 在更多的区域内使用语音业务, 从而降低国际漫游费用的支出。

收稿日期: 2015-05-30; 修回日期: 2015-08-31

论文引用格式: 曹磊, 王波, 邵震等. VoWi-Fi 技术的实现原理与架构分析. 电信科学, 2015219

Cao L, Wang B, Shao Z, et al. Principle and architecture analysis of VoWi-Fi technology. Telecommunications Science, 2015219

本文将主要介绍基于 3GPP S2b 方案的 VoWi-Fi 技术的实现及关键问题的分析,并简单介绍了其他 VoWi-Fi 实现方案,最后提出了对电信级 VoWi-Fi 运营的建议。

2 基于 3GPP S2b 方案的 VoWi-Fi 组网架构

图 1 是基于 3GPP S2b 方案的 VoWi-Fi 与 VoLTE 组网架构,其中虚线部分为 VoWi-Fi 涉及的接口,实线部分为 VoLTE 涉及的接口,PGW 作为跨网络切换的锚点。

3GPP 在引入演进的分组核心网 (EPC) 之初就将非 3GPP 网络接入作为目标架构的一部分,Wi-Fi 接入 3GPP EPC 架构可以分为 S2a、S2b 和 S2c 3 种场景^[1]。

- S2a 方案是基于授信 Wi-Fi 网络与 EPC 互通,采用 GTP/PMIP 的 S2a 接口 (授信非 3GPP 网络与 PGW 之间)。这种方案中 Wi-Fi 网络通过运营商城域网与移动网络的 PGW 相连,因此需要对城域网的网关设备 BRAS 进行改造,以支持移动性的要求。
- S2b 方案是应用于非授信 Wi-Fi 网络,Wi-Fi 网络基于 ePDG 设备接入 EPC 网络。S2b 方案要求终端和 ePDG 之间建立 IPSec 隧道,因此需要终端支持 IPSec。
- S2c 方案是一种基于终端的 Wi-Fi 网络与 EPC 互通解决方案,UE 和 PGW 之间通过 DSMIP 隧道连接,这样 UE 和 EPC 网络交互的数据可以在固网与城域网之间实现透传,这种方案要求终端支持 DSMIPv6。

在 S2b 方案中,网络侧通过新增 ePDG 网元来实现业务从 Wi-Fi 网络接入 EPC,ePDG 网元部署在公网(也可以部署在内网中)。终端和 ePDG 之间使用 SWu 接口,该接口通过 IKEv2^[2]消息传递用户认证信息,在认证通过后在终端和 ePDG 间建立 IPSec 隧道^[3]来承载用户的 Wi-Fi 数据流;ePDG 与 3GPP AAA 服务器间使用 SWm 接口,此接口通过 Diameter 消息传递用户认证信息;ePDG 与 PGW 之

间则使用 S2b 接口,此接口使用 GTP/PMIP 建立 Wi-Fi UE 与 PGW 的会话(session)。3GPP S2b 方案中的语音流最终从 EPC 网络通过 PGW 进入 IMS 核心网,实现与运营商所提供的 VoLTE 业务相同的管控。

S2b 方案支持 Wi-Fi UE 从其他运营商或私有的非授信 Wi-Fi 网络接入移动运营商的 EPC 网络中,因此要求终端支持建立 IPSec 隧道。由于 IPSec 的额外开销较大,对终端功耗有很大的影响,直至 Wi-Fi calling 的出现才使得此方案有了用武之地。目前在 Wi-Fi calling 技术中 S2b 方案仅承载 Wi-Fi 语音流,对数据流(上网业务等)不进行统一控制,即 IPSec 隧道仅封装语音流,这样能降低对终端处理能力的要求,也能节省终端的功耗。

3 基于 3GPP S2b 的 VoWi-Fi 方案的关键问题

3.1 用户认证

要使用 VoWi-Fi 业务,用户需进行 3 个步骤的认证注册过程。

第 1 步,在 Wi-Fi 网络注册。用户首先需要在 Wi-Fi 网络进行接入认证,确定能成功登入 Internet,这一认证方式及流程由该 Wi-Fi 网络自行决定。该 Wi-Fi 网络可以是用户归属运营商的 Wi-Fi 网络,也可以是用户家庭、商家或其他电信运营商的 Wi-Fi 网络。Wi-Fi 的加密方式由该 Wi-Fi 网络自行定义,可以是不加密的,也可以是加密的。EPC 网络注册流程如图 2 所示。

第 2 步,在 EPC 网络注册。用户在 Wi-Fi 网络通过认证登入 Internet 后,需要继续在 EPC 网络进行接入认证。该认证过程由终端触发,例如在苹果 iOS 操作系统中,当用户打开“Wi-Fi calling”使能开关时,终端会使用 DNS 方式发现 ePDG 网元,并通过 ePDG 和 3GPP AAA 网元在 EPC 网络进

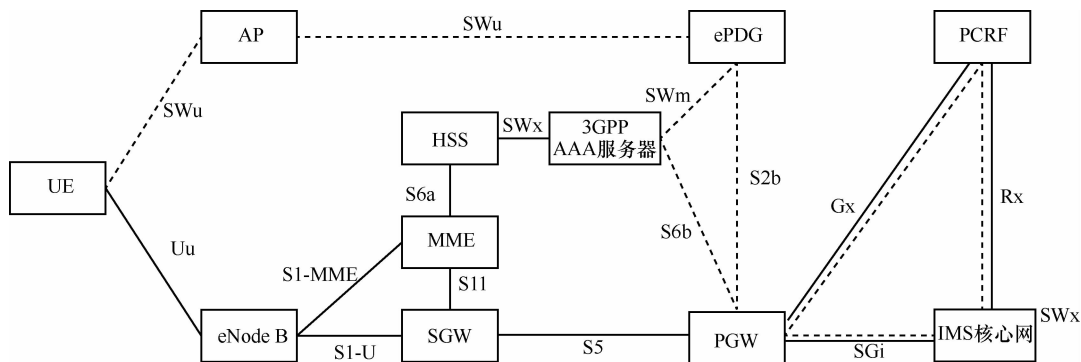


图 1 基于 3GPP S2b 方案的 VoWi-Fi 与 VoLTE 组网架构



行注册。测试结果显示,此步骤(从第一条 IKE_SA_init 消息到最后一条 IKE auth answer 消息)耗时在 1 s 左右。EPC 网络注册流程如图 2 所示。

第 3 步,在 IMS 网络注册。用户在 EPC 网络注册成功后,将继续在 IMS 核心网进行注册。这一过程在 EPC 网络注册成功后自动触发。只有在 IMS 注册成功后,用户才可以正常使用 VoWi-Fi 的主/被叫业务和发送/接收短信业务。

3 个步骤的认证过程如图 3 所示。

上述 3 个认证过程中,第 2 个步骤即用户在 EPC 网络的注册是 S2b 方案的关键,3GPP 定义在这一过程中使用基于 USIM 卡的 EAP-AKA^[4] 认证算法,在认证过程中 EAP-AKA 认证算法封装在 IKEv2 消息中。

3.2 语音流的安全传输

由于 S2b 针对的是非授权的 Wi-Fi 网络,因此必须保

障用户语音业务的安全性。S2b 方案在终端与 ePDG 间建立加密的 IPSec 隧道,ePDG 与 PGW 间建立 GTP/PMIP 隧道,这样用户数据全程都封装在隧道中,终端与 ePDG 间的 IPSec 隧道解决了 ePDG 网元以下段在非授权网络中的业务安全性问题,ePDG 与 PGW 间则采用与 EPC 网络相同的安全机制,这样可以有效实现语音流的端到端安全传输。语音流的传输示意如图 4 所示。

3.3 VoWi-Fi 与 VoLTE 的无缝切换

在 S2b 方案中,语音流通过 Wi-Fi 网络接入 PGW 后,以 PGW 作为锚点,可以实现 LTE 网络和 Wi-Fi 网络间的无缝切换,确保了跨网络切换时语音业务的连续性。用户语音数据的切换如图 5 所示。

无论是从 VoWi-Fi 切换到 VoLTE,还是从 VoLTE 切换到 VoWi-Fi,都是先在目标网络建立新的连接,之后将业务

No.	Time	Source	Destination	Protocol	Length	Info
360	14.444042000	188.6.40.3	58.60.106.133	ISAKMP	330	IKE_SA_INIT
361	14.458737000	58.60.106.133	188.6.40.3	ISAKMP	330	IKE_SA_INIT
363	14.513775000	188.6.40.3	58.60.106.133	ISAKMP	330	IKE_AUTH
365	14.541075000	121.40.1.85	192.120.1.222	DIAMETER	394	cmd=Diameter-EAP Request(268) flag
371	14.605662000	192.120.1.222	121.40.1.85	DIAMETER	226	cmd=Diameter-EAP Answer(268) flags
372	14.642633000	58.60.106.133	188.6.40.3	ISAKMP	202	IKE_AUTH
373	14.649748000	188.6.40.3	58.60.106.133	ISAKMP	186	IKE_AUTH
374	14.671076000	121.40.1.85	192.120.1.222	DIAMETER	414	cmd=Diameter-EAP Request(268) flag
385	14.771402000	192.120.1.222	121.40.1.85	DIAMETER	310	cmd=Diameter-EAP Answer(268) flags
388	14.804247000	58.60.106.133	188.6.40.3	ISAKMP	218	IKE_AUTH
392	14.903751000	188.6.40.3	58.60.106.133	ISAKMP	154	IKE_AUTH
393	14.921049000	121.40.1.85	192.120.1.222	DIAMETER	390	cmd=Diameter-EAP Request(268) flag
398	15.018778000	192.120.1.222	121.40.1.85	DIAMETER	670	cmd=Diameter-EAP Answer(268) flags
399	15.063847000	102.40.1.81	102.12.1.3	GTPv2	209	Create Session Request
404	15.346696000	102.12.1.3	102.40.1.81	GTPv2	180	Create Session Response
407	15.374124000	58.60.106.133	188.6.40.3	ISAKMP	122	IKE_AUTH
412	15.458074000	188.6.40.3	58.60.106.133	ISAKMP	138	IKE_AUTH
413	15.502938000	58.60.106.133	188.6.40.3	ISAKMP	314	IKE_AUTH

图 2 EPC 网络注册流程

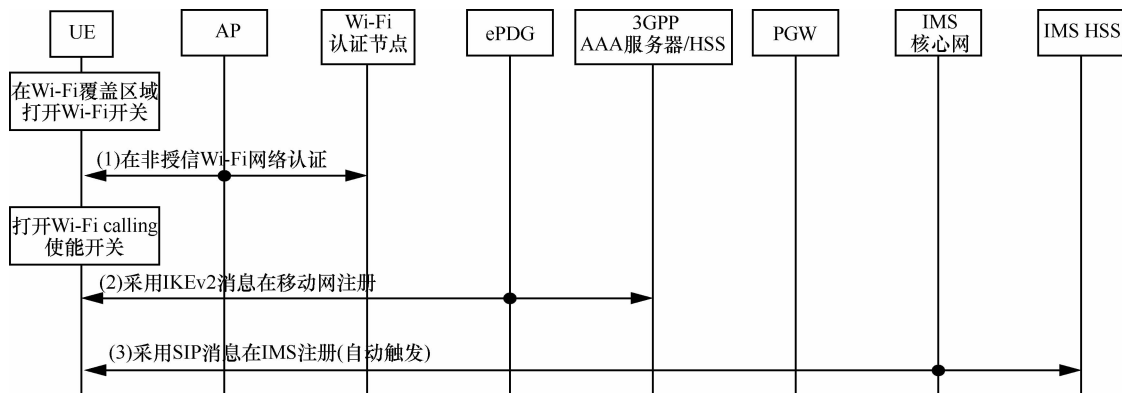


图 3 基于 S2b 的 VoWi-Fi 的认证注册过程

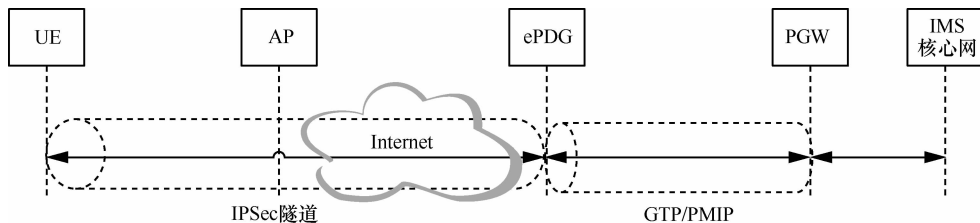


图 4 VoWi-Fi 语音流的传输示意

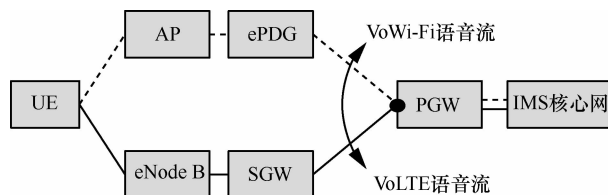


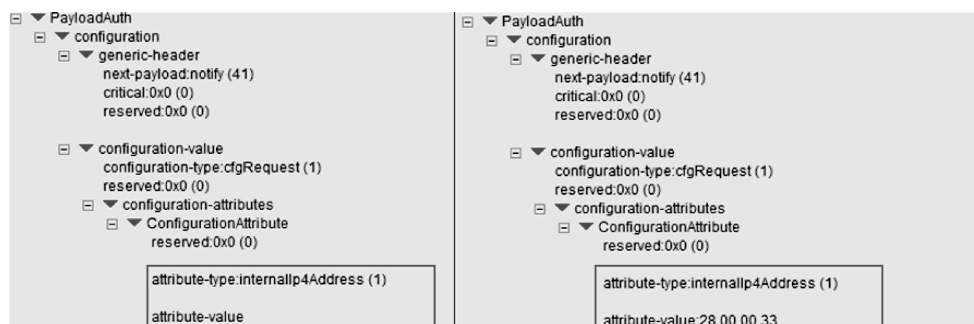
图 5 用户语音数据切换示意

承载到新的连接上,再拆除源网络上的连接。在这一过程中,由于锚点 PGW 的存在,无论用户在 Wi-Fi 网络上附着还是在 LTE 网络上附着,用户的 IP 地址均由 PGW 分配,因此在切换过程中,用户发起目标网络的连接建立请求时,只需在 GTPv2 消息(若采用 S2b GTP)中携带在源网络获取的 IP 地址,PGW 就可识别该连接建立请求是一个切换过程的连接建立而不是一个新建连接的建立,这样 PGW 只需在目标网络上将原 IP 地址分配给终端,即可保证用户的 IP 地址不变,从而实现了业务的连续性。当从 VoWi-Fi 切换到 VoLTE 时,终端在 LTE 网络下可以发送“Handover”指示,此时 EPC 网络可依照跨 eNode B 切换流程进行处理,但当 VoLTE 切换到 VoWi-Fi 时,终端在 Wi-Fi 网络下无法发送“Handover”指示(3GPP 标准不作定义要求),此时则通过终端上报在 LTE 网络获取的 IP 地址,由 ePDG 发起“Handover”指示来实现,如图 6 所示。

切换测试中分别定义了用户面和信令面两种切换时延(以 VoLTE 切换到 VoWi-Fi 为例)。

(1) 用户面

用户面切换时延是监测 PGW 的 GTP 接口,以在 LTE



普通 Wi-Fi 附着过程, 不携带 IP 地址

LTE 切换到 Wi-Fi 过程, 携带之前在 LTE 使用的 IP 地址

图 6 VoLTE 无缝切换到 VoWi-Fi 的实现

2142	17.257573000	2.31.111.40	40.0.0.52	GTP <AMR-WB>	PT=AMR-WB, SSRC=0x5976FFC, Seq=49494, Time=20507
2146	17.358940000	102.12.1.4	102.11.1.2	GTPv2	Delete Bearer Request
2147	17.359338000	102.12.1.3	102.40.1.81	GTPv2	Create Session Response
2148	17.360471000	102.11.1.2	102.12.1.4	GTPv2	Delete Bearer Response
2150	17.363438000	102.12.1.3	102.40.1.81	GTPv2	Create Bearer Recuest
2151	17.363886000	40.0.0.50	2.31.111.40	GTP <AMR-WB>	PT=AMR-WB, SSRC=0x5976FFC, Seq=49495, Time=20507
2154	17.434335000	2.31.111.40	40.0.0.52	GTP <AMR-WB>	PT=AMR-WB, SSRC=0x5976FFC, Seq=49495, Time=20507
2156	17.525218000	40.0.0.50	2.31.111.40	GTP <AMR-WB>	PT=AMR-WB, SSRC=0x5976FFC, Seq=49496, Time=20507

图 7 抓取分组示意

侧最后一个报文以及 Wi-Fi 侧第一个报文之间的时间差。统计的抓取分组示意如图 7 所示,虚线框内为 LTE 侧的最后一个报文,实线框内为 Wi-Fi 侧的第一个报文,用户面切换时延可以反映出用户对业务发生切换的真实感受。

(2) 信令面

信令面切换时延则是监测 ePDG 侧的信令,统计 ePDG 从初始切换的第一条 IKE_SA 消息到最后一条专有承载建立完成的 create bearer response 消息之间的时间差。如图 8 所示,虚线框内为 IKE_SA_init 消息,实线框内为 create bearer response 消息,信令面切换时延是便于网络侧对网内用户的切换情况进行统计,由于在信令面的切换完成前,用户的接入网并未切换,因此业务也不会中断。

从目前实验室测试结果看,在无线环境良好的情况下,VoWi-Fi 与 VoLTE 间的切换时延是百毫秒级的,用户几乎无感知。目前信令切换时延稍长,但对切换时通话质量无任何影响。在切换过程中,当专用承载未能建立起来时,语音流可临时走缺省承载,当专用承载建立后,语音流再切换至专有承载。具体测试结果见表 1。

3.4 VoWi-Fi 的语音编码

VoWi-Fi 的语音编码方案完全参照 VoLTE,编码格式和速率在 UE 与 IMS 平台协商后确认,在图 9 中的测试编码格式为 AMR-WB,编码速率为 12.65 kbit/s。

4 其他的 VoWi-Fi 实现方案

除了基于 3GPP S2b 的 VoWi-Fi 方案外,目前业界还



No.	Time	Source	Destination	Protocol	Info
2741	61.865155000	102.11.1.1	129.102.12.2.129	GTPV2	Echo Request
2790	64.292503000	188.6.40.3	58.60.106.133	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2792	64.308622000	58.60.106.133	188.6.40.3	ISAKMP	IKE_SA_INIT MID=00 Responder Response
2807	64.381093000	188.6.40.3	58.60.106.133	ISAKMP	IKE_AUTH MID=01 Initiator Request
2811	64.411444000	121.40.1.85	192.120.1.222	DIAMETER	cmd=Diameter-EAP Request(268) flags=RP-- appl=3GPP Swm(16777264) h2h=
2813	64.461997000	192.120.1.222	121.40.1.85	TCP	diameter-ndmp [ACK] Seq=257 Ack=597 win=32767 Len=0
2814	64.465086000	192.120.1.222	121.40.1.85	DIAMETER	cmd=Diameter-EAP Answer(268) flags=P-- appl=3GPP Swm(16777264) h2h=
2815	64.492590000	58.60.106.133	188.6.40.3	ISAKMP	IKE_AUTH MID=01 Responder Response
2816	64.495767000	121.40.1.85	192.120.1.222	TCP	ndmp-diameter [ACK] Seq=597 Ack=429 win=65535 Len=0
2817	64.501613000	188.6.40.3	58.60.106.133	ISAKMP	IKE_AUTH MID=02 Initiator Request
2818	64.521392000	121.40.1.85	192.120.1.222	DIAMETER	cmd=Diameter-EAP Request(268) flags=RP-- appl=3GPP Swm(16777264) h2h=
2824	64.607913000	192.120.1.222	121.40.1.85	TCP	diameter-ndmp [ACK] Seq=429 Ack=957 win=32767 Len=0
2825	64.609671000	192.120.1.222	121.40.1.85	DIAMETER	cmd=Diameter-EAP Answer(268) flags=P-- appl=3GPP Swm(16777264) h2h=
2826	64.638665000	58.60.106.133	188.6.40.3	ISAKMP	IKE_AUTH MID=02 Responder Response
2830	64.695762000	121.40.1.85	192.120.1.222	TCP	ndmp-diameter [ACK] Seq=957 Ack=685 win=65535 Len=0
2831	64.738701000	188.6.40.3	58.60.106.133	ISAKMP	IKE_AUTH MID=03 Initiator Request
2835	64.756095000	121.40.1.85	192.120.1.222	DIAMETER	cmd=Diameter-EAP Request(268) flags=RP-- appl=3GPP Swm(16777264) h2h=
2837	64.805847000	192.120.1.222	121.40.1.85	TCP	diameter-ndmp [ACK] Seq=685 Ack=1293 win=32767 Len=0
2841	64.856320000	192.120.1.222	121.40.1.85	DIAMETER	cmd=Diameter-EAP Answer(268) flags=P-- appl=3GPP Swm(16777264) h2h=
2842	64.889028000	102.40.1.81	102.12.1.3	GTPV2	Create Session Request
2843	64.895736000	121.40.1.85	192.120.1.222	TCP	ndmp-diameter [ACK] Seq=1293 Ack=1301 win=65535 Len=0
2847	65.116032000	102.12.1.3	102.40.1.81	GTPV2	Create Session Response
2849	65.119923000	102.12.1.3	102.40.1.81	GTPV2	Create Bearer Request
2850	65.149074000	58.60.106.133	188.6.40.3	ISAKMP	IKE_AUTH MID=04 Responder Response
2858	65.268427000	58.60.106.133	188.6.40.3	ISAKMP	IKE_AUTH MID=04 Initiator Request
2859	65.312967000	58.60.106.133	188.6.40.3	ISAKMP	IKE_AUTH MID=04 Responder Response
2904	65.774403000	40.0.0.51	2.31.111.40	GTP <SIP>	Request: REGISTER sip:ims.mnc008.mcc460.3gppnetwork.org (1 binding)
2918	65.945105000	2.31.111.40	40.0.0.51	GTP <SIP>	Status: 200 OK (1 binding)
2928	65.994647000	2.31.111.40	40.0.0.51	GTP <SIP/XML>	Request: NOTIFY sip:40.0.0.51:49972;transport=tcp
2940	66.165709000	40.0.0.51	2.31.111.40	GTP <SIP>	[TCP Retransmission] Status: 200 OK
3193	67.974400000	102.12.1.3	102.40.1.81	GTPV2	Create Bearer Request
3202	68.001417000	102.40.1.81	102.12.1.3	GTPV2	Create Bearer Response
3497	71.046590000	192.120.1.222	121.40.1.85	TCP	diameter-ndmp [ACK] Seq=321 Ack=361 win=8576 Len=0

图 8 抓取分组示意

表 1 VoWi-Fi 与 VoLTE 的无缝切换时延测试结果

切换场景与条件	控制面切换时延/ms	用户面切换时延/ms
LTE 切换到 Wi-Fi	3 175 (含专用承载建立请求重传等待时间:3 000 ms)	147
Wi-Fi 切换到 LTE	LTE 有 RoHC 压缩 186.6	128
	LTE 无 RoHC 压缩 184	121

Adaptive Multi-Rate
Payload decoded as RFC3267 bandwidth-efficient mode
1111...=CMR: No mode request(15)
...0...=F bit: Last frame in this payload
...001 0...=FT bit: AMR-WB 12.65 kbit/s(2)/Frame OK
...1...=Q bit: OK
Frame Data(32 byte)

图 9 VoWi-Fi 的语音编码协商

有其他几种 VoWi-Fi 实现方式。

4.1 普通 App 的 OTT 方式

有代表性的包括微信电话、Skype 等,其主要通过在终端上安装 App 客户端软件的方式实现基本的 VoIP,其存在的主要问题有各种通话软件与现有电信网络以及通话软件间均难以互通;实时被叫需要 App 客户端软件时刻开启,这样也就难以保障语音的随时可达;一般无法实现 Wi-Fi 网络与移动蜂窝网的切换等。虽然,类似易信电话的应用能通过运营商网络中部署 IP 电话网关来增强实现 App 客户端到现有电信网络号码的主叫能力,但始终无法实现 App 客户端的被叫功能。OTT 方式的 VoWi-Fi 实现组

网如图 10 所示。

4.2 App+信令网关方式

有代表性的如 Wi-Fi-phone 等,这种方式是运营商定制的 VoWi-Fi 方案,其除了在终端上安装客户端软件外,还需在运营商网络内部署 Wi-Fi-phone 平台,并利用信令网关实现与 HLR 互通,由此将 Wi-Fi 网络视为移动蜂窝网中的一个普通基站,从而完成用户在移动核心网中的位置注册、IMS 的注册及呼叫信令接续。与普通 App 的 OTT 方式相比,这种方式可以通过 App 语音平台来实现原有的运营商分配的号码与 App ID 的绑定,从而完成用户的主/被叫接续,但与 3GPP S2b 方案相比,其作为一种 App 的拓展,使用时仍然要求 App 客户端软件时刻开启,并且无法实现 Wi-Fi 网络与移动蜂窝网的切换,同时对移动核心网有新增网元的改造要求。App+信令网关方式的 VoWi-Fi 实现组网如图 11 所示。

App+信令网关方式中的 IMS 网络注册过程为:App 客户端通过 Wi-Fi 进入 Internet 并连接到 Wi-Fi-phone 平台,由 Wi-Fi-phone 平台完成客户端的鉴权后,向 IMS 发起标

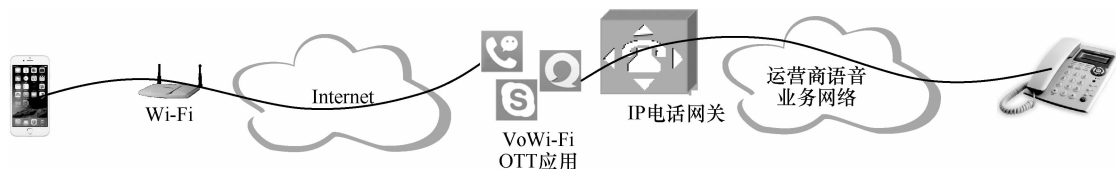


图 10 OTT 方式的 VoWi-Fi 实现方案

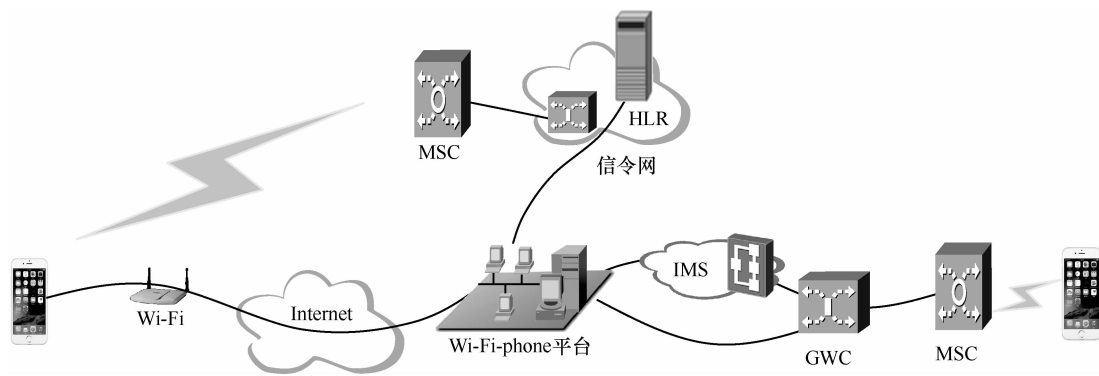


图 11 App+信令网关方式的 VoWi-Fi 实现方案

准注册过程。

主叫处理过程：由 App 客户端发起的呼叫通过 Wi-Fi 与 Internet 发送到 Wi-Fi-phone 平台中的信令网关，由信令网关解密后发送至 IMS；呼叫到达 IMS 后由 IMS 负责处理将呼叫路由到 MSC 完成后续呼叫。

被叫处理过程：App 客户端在 Wi-Fi-phone 平台完成鉴权后，平台会通知 HLR 进行用户位置的注册，当前用户的位置就是处于 Wi-Fi-phone 平台覆盖区域，平台需分配被叫路由的 TLDN (temporary local directory number, 临时本地号码) 号段。主叫 MSC 根据 TLDN 分析，选 GWC (gateway controller, 网关控制器) 方向进行路由；GWC 基于 TLDN 的分析选定 IMS 方向，GWC 与 IMS 间走信令链路途经 Wi-Fi-phone 平台，由平台完成该 TLDN 与原手机号码变换，IMS 收到的被叫号已变为该注册的手机号，最终由 IMS 完成呼叫接续。

4.2 Google 推出的 Project Fi 业务

近期 Google 推出了 Project Fi 业务，该业务除实现 VoWi-Fi 外，还可通过与 T-Mobile、Sprint 合作，实现与这两个运营商的移动蜂窝网之间的语音切换，目前仅有一款终端 (Nexus 6) 支持该业务。目前 Google 尚未公布其具体的实现方案，据新闻报道中提及 T-Mobile US CEO 透露“Project Fi 实现 LTE 与 Wi-Fi 的无缝切换不是使用 Wi-Fi calling 技术”^[5]。由于现阶段信息公开的局限，后续将进一步对 Project Fi 的实现机制进行研究分析。

5 VoWi-Fi 发展建议

现阶段 VoWi-Fi 能成为业界聚焦的热点，主要在于其能形成对 VoLTE 的有效补充，运营商可以利用数量庞大的 Wi-Fi 公共热点和家庭 Wi-Fi 覆盖的资源优势解决 VoLTE 业务覆盖不连续性的问题，VoWi-Fi 将与 VoLTE 同

步融合并一起作为基础的语音业务能力提供给用户。因此，VoWi-Fi 从提供业务的能力上来说，需要继承现有电路域语音业务的基本业务及补充业务能力；而从用户使用习惯上来说，也需要延续现有的操作体验，应与 VoLTE 的操作体验保持统一性。

目前国内通信市场仍处于 LTE 的牌照发放后的网络建设初期，LTE 网络使用高频段进行部署，短期内无法达到 900 MHz GSM 或者 800 MHz CDMA 网络的覆盖水平。加之运营商对于高层住宅楼宇中移动语音业务的覆盖与质量问题，始终没有找到好的技术手段加以应对，这也给 VoWi-Fi 带来一个较好的发展时机，部署时应重点考虑以下几方面的问题。

(1) 技术方案的选择

基于 3GPP S2b 方案的 VoWi-Fi 技术方案与前文所述几种技术方案相比，最大的区别在于将语音业务完整地接入运营商的 EPC 与 IMS 网络中，从而可以在移动分组域中实现对 Wi-Fi 语音业务的管理与控制。同时能实现与电信网络号码的互通以及与 LTE 网络间语音业务的无缝切换，Wi-Fi calling 以此作为 VoLTE 业务的强力补充，能有效解决 LTE 网络覆盖不足所带来的 VoLTE 业务不连续性的问题。除此以外，Wi-Fi calling 这项功能内置于终端中，用户无需下载安装 App，其拨打/接听电话和收发短信等操作也与现有电路域语音业务及运营商提供的 VoLTE 业务所要求的操作完全一致，这样的使用方式保证了用户的体验，更易于接受。

(2) 对现有网络的改造

由于基于 3GPP S2b 方案本身是针对非授权的 Wi-Fi 网络，因此对运营商的 Wi-Fi 网络无特殊改造要求，而对于移动网络，需要在 EPC 中新增 ePDG 网元作为 Wi-Fi 侧接入网关，新增或升级 3GPP AAA 网元支持对用户的



EAP-AKA 认证算法。

(3)对关键网元 ePDG 的功能和部署要求

ePDG 设备作为 S2b 方案的关键网元,需要具备以下主要功能。

- 支持将用户侧 IKEv2 认证消息转换为 EPC 要求的 Diameter 消息,发送到 3GPP AAA 服务器进行用户认证。
- 支持与用户建立 IPSec 隧道,将用户语音流封装于其中。
- 支持与 PGW 建立 GTP/PMIP 隧道,将用户语音流封装于其中,建议采用 S2b GTP。
- 由于 ePDG 网元暴露在公网上,需要考虑对网元实施安全性保护。
- 有别于国外运营商的集中部署方式,在国内分省部署时需要解决省际漫游的问题。
- 加快融合 VoWi-Fi 功能的 VoLTE 终端研制。

基于 3GPP S2b 方案的 VoWi-Fi 更依赖于终端的生态系统支持,目前在欧美地区获得了苹果的 iOS 终端和三星、HTC 等 Andriod 终端的支持,终端产业链已经初具规模,因此需要制定相关行业或企业的终端规范来推进国内主流终端厂商迅速开展融合 VoWi-Fi 功能的 VoLTE 终端的研制。同时,针对 IPSec 隧道的耗电性能、语音业务的 LTE 优先功能等技术细节进行探讨与功能完善,提前做好商用终端的准备。

(4)VoWi-Fi 业务质量

通常 Wi-Fi 网络是以承载数据上网业务为主,其 QoS 保障能力与 LTE 网络存在一定差距。尽管关于 Wi-Fi 网络服务质量的标准已经发布,但目前 Wi-Fi 设备对其支持率较低,因此用户未来能否获取与 VoLTE 一致的 VoWi-Fi 业务质量体验有待进一步评估。

6 结束语

本文从组网、接入认证、传输安全性与 VoLTE 的无缝切换、语音编码以及部署建议等方面分析了基于 S2b 方案的 VoWi-Fi 技术实现,同时对其他 VoWi-Fi 实现方案的优缺点进行了分析,将有助于运营商提前做好各方面的技术准备,加快 VoWi-Fi 的商用进程。

参考文献

- 1 3GPP TS23.402. Architecture Enhancements for Non-3GPP

Accesses, 2011

- 2 IETF RFC5996. Internet Key Exchange Protocol Version 2 (IKEv2), 2010
- 3 IETF RFC4301. Security Architecture for the Internet Protocol, 2005
- 4 IETF RFC4187. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), 2006
- 5 Google 不是想做运营商,是玩运营商, <http://www.aiweibang.com/yuedu/23436242.html>
Google wants to do more than be an operator, <http://www.aiweibang.com/yuedu/23436242.html>

[作者简介]



曹磊,男,中国电信集团公司技术部高级工程师、处长,主要从事移动通信、现代通信技术的研究与管理工,承担过多项国家、省、市科技项目的研究与开发,近年来在学术刊物及国内外学术会议上发表学术论文 10 余篇,被评为中国电信集团级优秀人才。

王波,男,中国电信集团公司技术部高级工程师、业务经理,CCSA TC6 WG2 副主席,多年从事宽带技术研究与技术管理工作,主要研究方向为网络智能化、PON、DSL、WLAN 等,主持制定了多项宽带接入领域的国际、国内行业标准和电信集团的企业标准,先后发表了多篇学术论文,发明专利近 10 项,先后获得国家科学技术进步奖二等奖和多次省部级奖励。

邵震,男,中国电信股份有限公司上海研究院基础网络部高级工程师,主要研究方向为无线接入与移动网络协同,先后承担过国家重点专项课题、中国电信集团项目等 20 多项,发明专利近 12 项,发表学术论文多篇。

沈晓,男,中国电信股份有限公司上海研究院基础网络部助理工程师,主要研究方向为移动网络智能协同,先后承担中国电信集团与中国电信股份有限公司上海分公司项目等 10 多项,发明专利近 10 项,在国内学术刊物发表多篇论文。

李一明,男,中国电信股份有限公司上海研究院基础网络部高级工程师,长期从事移动前沿技术及其发展、移动互联网产品及商业模式等方面的研究工作,先后承担中国电信集团项目等 30 多项,多次获得中国电信集团公司、中国电信股份有限公司上海分公司相关科技奖励,在国内外学术刊物发表学术论文 20 余篇。