



多等价路径场景下 VoWi-Fi 注册成功率提升的研究

程德恽, 乔健

(上海市信息网络有限公司, 上海 200081)

摘要: 3GPP 的 VoWi-Fi S2b 规范要求客户端用 IPSec 隧道通过城域网注册到局端的 ePDG, 其在大网多等价路径环境中面临某条路径转发故障时, 无法主动规避, 进而导致业务无法注册使用。对故障原因进行分析并提出了解决方案: 通过在 IKE_AUTH 阶段改变客户端源端口实现路径更换, 能显著改善 VoWi-Fi 注册成功率, 并通过实验进行了验证。其次通过在城域网边缘和 ePDG 端之间的双向网络路径全遍历检测, 能快速定位并消除故障。

关键词: VoWi-Fi; 互联网密钥交换协议; IPSec; 3GPP R10; 等价路径

中图分类号: TP393.1

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019011

Research on improving the registration success rate of VoWi-Fi under multiple equivalent path scenarios

CHENG Deyi, QIAO Jian

Shanghai Information Network Co., Ltd., Shanghai 200081, China

Abstract: The 3GPP's VoWi-Fi S2b specification requires the client to use the IPSec tunnel to register with the ePDG through the metropolitan area network. When IPSec faces a path forwarding fault in a multi-equivalent path environment of a metropolitan area network, it can't actively evade, and the service can't be registered. The cause of the malfunction was analyzed and an optimized solution was proposed. By changing the client source port in the IKE_AUTH phase to achieve path replacement, the VoWi-Fi registration success rate can be significantly improved and verified by experiments. Secondly, through the full traversal detection of the bidirectional network path between the edge of the metropolitan area network and the ePDG end, the fault can be quickly located and eliminated.

Key words: VoWi-Fi, IKE, IPSec, 3GPP R10, ECMP

1 引言

VoWi-Fi(voice over Wi-Fi)也叫 Wi-Fi calling, 客户可以用有此功能的终端, 以普通的拨号方式

通过 Wi-Fi 进行语音和视频呼叫及通话。目前的 VoWi-Fi 解决方案采用 3GPP 的 VoWi-Fi S2b 标准架构, 将 ePDG、3GPP AAA 和 IMS 作为核心控制架构, 使普通用户在通过 Wi-Fi 热点接入网络



获得高清语音/视频的同时,实现与 VoLTE 之间的无缝切换。VoWi-Fi 的优点是可以提供低成本的语音通信和漫游,能增加运营商的整体竞争力并使其获取更多的收益。VoWi-Fi 用户无需特别设置就可以在不同地点实现通话,在网络覆盖较弱或受干扰的地方只要能连上 Wi-Fi,就可实现通话,有效地解决了 VoLTE 覆盖不足的问题。为了深入研究 VoWi-Fi 业务部署的语音质量和 VoLTE 切换速度,某电信运营商在多个城市对 VoWi-Fi 业务试点进行了场外测试,从测试结果来看,在实际网络条件下有可能出现 VoWi-Fi 注册困难问题。本文对测试结果进行了分析研究并给出了优化方案。

2 VoWi-Fi S2b 在多等价格路径场景下面临的问题

VoWi-Fi 有多种方案:(1) UMA (unlicensed mobile access) 方案;(2) 直接连接 IMS 的软终端方案;(3) 非可信任域接入 EPC/IMS 方案;(4) 可信任域接入 EPC/IMS 方案;(5) OTT 方案。从发展情况来看,方案(3)、(4)具备商业部署能力。其中方案(4) 3GPP R12 标准支持,由于存在不支持第三方 Wi-Fi、尚无芯片支持的问题,因此目前主流方案是 3GPP R10 标准支持的非可信任域接入 EPC/IMS 方案。非可信接入 ePDG(EPC)/IMS 方案是利用公共 WLAN、运营商 Wi-Fi、企

业或个人 Wi-Fi 非可信地接入 3GPP 网络(S2b 接口),将 PGW 作为 Wi-Fi 和 LTE 切换的锚点。方案要求终端和 ePDG 之间的通信采用 IPSec VPN 隧道,需要终端支持 IPSec 以及 IKEV2 鉴权。此方案的特点是支持 VoWi-Fi 与 VoLTE 之间的无缝切换,终端成熟。

2.1 注册测试

2017 年某运营商在多个城市针对多种场景:交通枢纽、商业中心、写字楼、家庭宽带、校园、商业街、咖啡店、餐厅等,对 VoWi-Fi 进行了测试,包括定点拨打测试、随机移动测试、承载性能测试、微信、WiPhone 对比测试等。手机客户端在场外测试中大多数能一次注册 VoWi-Fi 成功,但是在某些场景下发生了持续不能注册的现象。以某城市 VoWi-Fi 现场测试结果为例,在全市测试中有 5 处注册困难,见表 1。

由于现场测试中室内外 Wi-Fi 网络环境复杂,为了准确判断故障原因,选择 3 处故障场地进行 IPSec 穿越测试。测试拓扑图如图 2 所示,其中发流端发起不同源端口(源端口为 33000 到 56000)的 IPSec 流给 ePDG 防火墙下的接收服务器(目的端口为 UDP500 和 UDP4500)。发送分组速率为 300 个报文/min,即每分钟使用 300 个源端口。发送端每次源端口+1,向 UDP500 和 UDP4500 端口发送 IPSec 注册流量。

表 1 VoWi-Fi 注册困难问题汇总

序号	测试地点	测试时间	网络	问题描述
1	某设计院 8F	3 月 17 日	OA 热点	TTL 存活时间超时
2	某郊区工业园区	4 月 13 日	会议室热点	IPSec 建立困难,偶尔成功
3	某机场 T2 航站楼	4 月 19 日	airport-free	使用机场热点无法注册,抓取分组后显示 ePDG 无回复,切换 Wi-Fi 到 4G 手机热点后一切正常
4	郊区某用户宽带	4 月 26 日	家庭 Wi-Fi	使用运营商宽带,IPSec 无法建立,切换 Wi-Fi 到手机 4G 热点后一切正常
5	市中心某商厦	5 月 18 日	星巴克	一部三星 S7 手机能注册,另外一部始终无法注册,切换 Wi-Fi 到手机 4G 热点后一切正常。确认手机本身无问题后,重启手机恢复

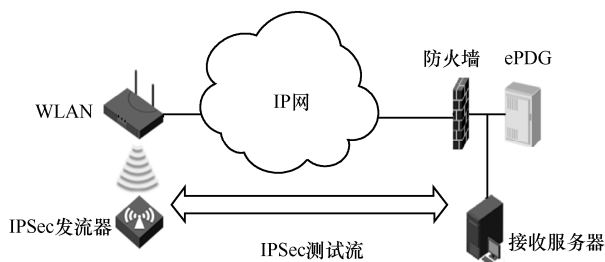


图2 IPSec 穿越测试示意图

测试过程中为了排除偶发性分组丢失引起的误判,对同一段源端口范围执行 3 次,测试开始时间分别是 T_0 、 $T_0+15\text{ min}$ 、 $T_0+30\text{ min}$ 。若同一个源端口在连续 3 次测试中都丢失,则判定受阻。IPSec 穿越测试结果见表 2。

表2 IPSec 穿越测试情况汇总

测试地点	目标端口 UDP500 受阻率	目标端口 UDP4500 受阻率
某机场 T2 航站楼	7.67‰	13.16‰
某设计院	365‰	456‰
市中心某商厦	205.2‰	318.66‰

2.2 技术分析

VoWi-Fi 的 S2b 方案采取 IPSec 协议作为终端设备和 ePDG 设置之间的加密承载协议。注册过程(如图 3 所示)中需要手机和 ePDG 之间使用 IPSec 建立起加密通信,在 RFC 3947-Negotiation of NAT-Traversal in the IKE 中规定 IPSec 在 IKE_SA Init 阶段会使用 UDP 源端口 500 和目标端口 500 通信来进行 NAT 侦测^[2]。为了判断两台主机之间是否存在 NAT,需要检测是否存在 IP 地址或端口沿路径的变化。方法是将两端的 IKE 对等体的 IP 地址和端口的散列值发送到另一端来校验,如果两端协商双方计算出来的散列值与它收到的散列值一样,判断没有 NAT,反之则认为存在 NAT 环境。主机后续的 IKE 分组和 ESP 分组(IMS 信令)则需要用 UDP 封装从随机源端口发送到目的端口 4500^[3]。因此 NAT 环境下 IPSec 的建立需要使用两对 UDP 端口 $\langle 500, 500 \rangle$ 和 $\text{UDP} \langle 500, 4500 \rangle$ 。

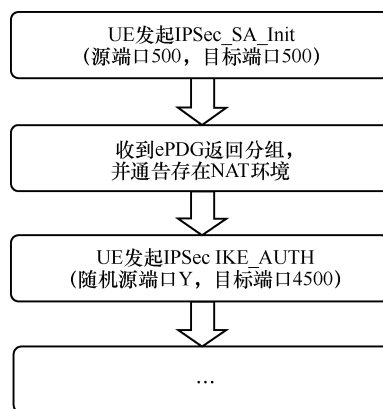


图3 VoWi-Fi 注册过程

从两部测试手机的抓取分组结果看,如果在 IPSec 的 IKE_SA_Init 阶段没有收到响应,源端口 500 保持不变,终端将持续用 500 端口发送分组。而在 IKE_AUTH 阶段,如果源的随机 X 端口转发受阻,终端同样不改变其发送分组源端口。

当源 IP 地址和目的 IP 地址之间存在多条等价路径环境下,网络设备对流量做路径选择时会遵循采用 RFC2992 的散列类算法^[5]。路由器首先对分组头中决定流向的各个域(五元组:源 IP 地址、源端口、目的 IP 地址、目的端口、传输层协议)混合后进行散列运算(例如 CRC16),得到一个决策码(key)。将决策码的可能取值空间划分成 N 个区域,给每个不同的下一跳分配其中的一个区域。这样,路由器就可以用根据决策码处在哪个区域中来决定下一跳的路由。假定目的地址有 4 个不同的下一跳地址可供选择,对每个下一跳都在 16 bit 空间中分配一块区域。为使机会均等,路由器会使每块区域的大小都相同,即 $65\ 536/4$,哪个区域包含了这个决策码就选择相应的下一跳地址。因此在 VoWi-Fi 业务中当终端侧发起 IPSec 协商请求,而该请求恰好被映射到有故障的等价路径时,终端侧并不会主动改变源端口,而是继续使用该端口重发。因此通过散列运算得到的路径选择决策码保持不变,导致重发的后续报文仍然会被映射到原有的故障等价路径上,造成业务持续无法注册。如图 3 所示,VoWi-Fi 在 NAT 环境下,这两对端口组 UDP



<500, 500>和 UDP<500,4500>中任何一对被故障路径承载,均会导致业务受阻。VoWi-Fi 注册受阻示意图如图 4 所示。

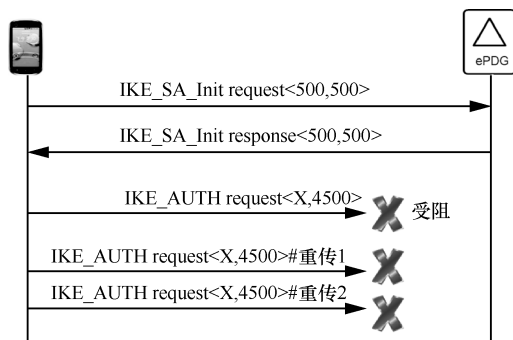


图 4 VoWi-Fi 注册受阻示意图

VoWi-Fi 业务中,非授信 Wi-Fi 接入点到局端 ePDG 往往会穿越多个不同的运营商网络,运营商网内节点普遍采用多条光纤上联核心节点,因此会存在多条等价路径(ECMP)。如路由器配置、转发硬件故障、路由策略、报文过滤策略等因素,使得某条等价路径转发面有问题,而 VoWi-Fi 业务恰好被有故障的路径承载,那么业务注册就会受阻。从故障概率上分析,假设等价路径上某路径出现故障的概率为 N ,CE 端发生故障的概率为 M ,则流量通过多等价路径发生注册受阻的概率为 $M+N_1 \times N_2 \times N_3 \times \dots \times N_i$,如果转发过程中只使部分端口无法通信,则注册受阻的概率更低。因此从概率方面考虑,注册受阻是小概率事件。

3 VoWi-Fi 优化方案

虽然 VoWi-Fi 发生注册受阻的概率较低,但是一旦发生会使部分用户无法使用 VoWi-Fi 业务,直至终端重启或者进程重置,才有可能切换到其他正常路径后注册成功。而后期维护人员到现场进行故障复测时,复测业务请求难以恰好映射到故障路径,往往不能及时重现并发现故障。因此为了改善客户的使用感知度,有必要提高 VoWi-Fi 业务在多等价路径情况下的报文注册成功率。本文提出两种优化改进方案:对 VoWi-Fi 中终端侧

的 IPSec 模块进行修改,通过改变五元组参数,使得路径选择的散列决策码发生改变,在多等价路径场景中改变数据流的承载路径,绕过出问题的路径;采用端到端路径全遍历的主动式双向检测,在等价路径中发现有问题的路径并进行解决。

3.1 修改终端 IPSec 模块改变散列运算决策码

网络设备在选择等价路径时根据五元组进行散列计算,根据所得决策码对数据流进行路径选择。改变五元组会直接影响路径选择结果。通过修改终端侧 IPSec 模块行为,使其行为从源端口不变改成源端口可变,可以迫使转发路径发生变化,从而避开故障路径,提升其适应性和业务注册成功率。

IKE_SA_Init 阶段由于 RFC3947 标准限定使用 UDP<500,500>端口进行 NAT 探测,而 RFC2408 标准限定使用 UDP<500,500>进行密钥交换。因此即使修改了源端口,也会在 IKE 对等体收到数据分组后,在进行数据完整性校验时发生失败而被丢弃。因此本优化方案只适用于 IKE_AUTH 阶段,通过利用 NAT 环境下允许随机源端口发起到目的地址 UDP4500 端口的特点,主动修改源端口来实现路径更改。优化后的终端侧 VoWi-Fi IPSec 模块流程如图 5 所示,终端侧通过源端口 X 向 ePDG 发起 IKE_AUTH 请求,若该 IKE_AUTH 报文丢失,终端会重新挑选新源端口 Y 重新尝试。通过改变源端口而影响等价路径的选择,避开有故障的等价转发路径。

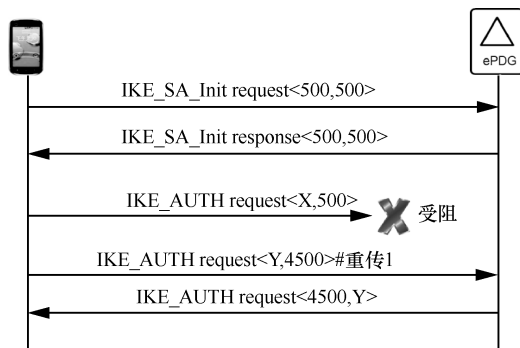


图 5 优化后的终端侧 VoWi-Fi IPSec 模块流程

3.2 端到端路径全遍历的仿真主动式双向检测

单向检测的问题只能从全局上发现某一方向

的网络异常情况,给出网络变化情况但无法精确定位故障点。因此需要采用主动式网络质量监控,在城域网边缘节点和 ePDG 处部署探针实现双向监控。探针可以采用 TWAMP 双向主动测量协议业务用于仿真流量注入。TWAMP 是在 OWAMP 单向主动测量协议的基础上演进而来的,可以进行两个网络设备间双向的网络性能测量。TWAMP-Test 协议在 UDP 层,采用基于 UDP 的 Trace route 沿着传输路径发送测量分组和返回测试分组,通过 UDP 的 TTL (time to live, 存活时间) 过期来感知转发节点。为了完成对等价路径的全遍历并能准确获得业务仿真,探针需要支持传输层 UDP 多端口同时发送分组,最大限度兑现多路径探测。通过城域网边缘和 ePDG 处探针之间全网状监控结果得到全部等价路径实现覆盖监控,从而可以准确定位路径中的故障节点。

基于硬件探针的检测分析系统虽然能提升故障定位的精确度和识别效率。但是也存在成本高、需要单独建设 DPI 探针和分析平台等不足。因此从成本效率方面考虑,目前修改终端侧 IPSec 模块行为可能是一个更佳的选择。未来随着 SDN、NFV 向城域网、IP RAN 和 MPBN 逐渐渗透,利用 SDN 控制器集中控制转发层设备的转发行为实现精确业务流量控制,可以用 SDN 控制器将需要监测的移动互联网应用以流表形式下发到边缘 SDN 交换机,边缘 SDN 交换机根据流表将应用流量牵引至感知分析平台进行感知指标分析,从而无需在 4G/5G 网、核心网部署第三方 DPI 探针,可以极大降低建设成本。

4 仿真实验

实验环境主要配置如下:思博伦 C50 网络流量测试仪、安立自动化智能手机测试仪 MD8475A、两台思科 3945 路由器、华为 USG6300 防火墙和 LinksysEA9500 无线路由器各一台、两部三星 S7 测试手机,其中一部手机厂商通过更新

Alpha 测试版软件实现 IPSec 模块修改。本文的实验数据来源于安立和思博伦测试仪表,并根据本实验需求对原始的结果样本重新进行了标注。

实验使用了思科 3945 路由器来模拟多等价路径转发环境,两台路由器使用 4 个吉比特端口互联,并配置 4 条等价路由。3945-B 上对 4 个端口分别设置访问控制列表,对部分源地址的 UDP500 端口进行限制,同时对目的端口为 4500 的数据流的部分 UDP 源端口进行限制,以模拟 IKE_SA_Init 和 IKE_AUTH 受阻状况。安立测试仪控制终端发出 IKE_SA_Init 以模拟注册 VoWi-Fi 过程,为了模拟不同的用户通过手机注册 VoWi-Fi,每一个 IKE 协商测试完成后 IP 源地址+1,开始新一次测试。安立测试仪记录每一次 IKE 协商,思博伦 C50 对 IKE 的数据分组进行数量统计,并验证安立测试仪记录。实验拓扑图如图 6 所示。

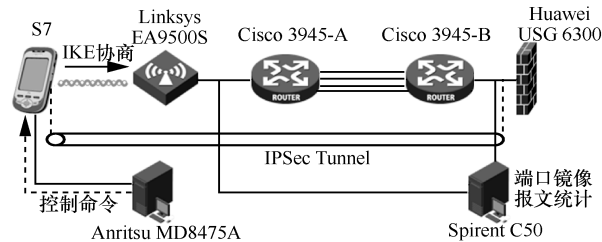


图 6 IPSec 更改源端口测试拓扑图

在高速线路环境下进行测试,为了缩短测试时间,减少了 IKE 协商等待时间,终端和防火墙都通过配置将等待时间设置为 10 s,重传次数为 2 次。测试终端每发出一次 IKE 请求后如果 20 s 内没有收到 IKE 回应,则认为注册受阻。当在 IKE_AUTH 阶段协商失败时,修改过 IPSec 模块的手机终端会使用混合同余随机数算法重新挑选源端口进行尝试,如果改变源端口后依旧受阻,则继续改变源端口,最大尝试 8 次。使用两部手机终端在相同测试环境下,以相同 IP 地址段进行了 300 次 IKE 协商对比测试。在实验环境下,在 IKE_AUTH 阶段更改源端口能提升 35% 的成功率。仿真对比测试结果见表 3。



表3 仿真对比测试结果

型号	IKE_SA_Init 受阻率	IKE_AUTH 受阻率	更改源端口后受阻率	IKE 协商总受阻率
S7	22.67%	35%	—	57.67%
Alpha S7	22.67%	38.67%	0	22.67%

表4 Alpha S7 更改端口测试

重复尝试过程	第一次更改	第二次更改	第三次更改	第四次更改
更改端口注册成功数	43	37	29	7

对于 Alpha S7 在 IKE_AUTH 阶段发生的 116 次受阻, 更改源端口后重新尝试注册的实验数据见表 4, 经过最多 4 次更改 IKE_AUTH 源端口后, IKE 协商成功。

上述仿真测试证明, 通过修改手机客户端 IPSec 模块行为, 使其在 IKE_AUTH 协商失败时更改源端口, 能完全解决 IKE_AUTH 受阻问题, 可以大幅提升 VoWi-Fi 在多等价路径下的注册成功率。

5 结束语

本文提出了两种优化方案, 其中基于 IPSec 协议以及负载均衡的选路机制, 通过利用负载均衡的五元组规则和修改 IPSec 协商阶段的源端口, 迫使存在多条等价路径 ECMP 的网络设备改变客户端到 ePDG 的原有转发路径。不仅如此, 由于修改 IPSec 端口只需要在手机端实施, 这意味着局端无需做任何更改就可使终端具备更强的网络适应能力。本文的研究成果可以解决目前 VoWi-Fi 业务在某条等价路径出现故障的情况下业务受阻的难题, 提升 VoWi-Fi 业务对复杂网络环境的适应性。本文提出的优化改进方案同时也值得其他使用 IPSec 技术进行类似保密承载的业务领域借鉴, 如微基站回传等。

参考文献:

- [1] 3GPP. Technical specification group services and system aspects; architecture enhancements for non-3GPP accesses: TS 23.402 V15.3.0[S]. 2018.
- [2] KIVINEN T. Negotiation of NAT-traversal in the IKE: RFC 3947[S]. 2005.
- [3] HUTTUNEN A. UDP encapsulation of IPsec ESP packets: RFC 3748[S]. 2005.
- [4] MAUGHAN D. Internet security association and key management protocol (ISAKMP): RFC2408[S]. 1998.
- [5] HOPPS C. Analysis of an equal-cost multi-path algorithm: RFC 2992[S]. 2000.
- [6] 谢海华. 有线 IP 城域网可视化质量监控系统的建设与运用研究[J]. 无线互联科技, 2017(23): 42-45.
XIE H H. Study on construction and application of visual quality monitoring system for CATV IP metropolitan area network[J]. Wuxian Hulan Keji, 2017(23): 42-45.
- [7] 夏刚. 互联网环境的网络质量监测体系研究与实践[J]. 中国金融电脑, 2016(7): 48-51.
XIA G. Research and practice of network quality monitoring system in internet environment[J]. China Financial Computer, 2016(7): 48-51.
- [8] 田少禧. 基于 ECMP 的 IP 网络业务量工程技术研究[D]. 成都: 电子科技大学, 2010.
TIAN S X. Research on IP network traffic engineering technology based on ECMP[D]. Chengdu: University of Electronic Science and Technology of China, 2010.
- [9] 肖子玉. SDN 技术优化的最新研究综述[J]. 电信科学, 2015, 31(Z1): 132-139.
XIAO Z Y. A review of the latest research on SDN technology optimization [J]. Telecommunications Science, 2015, 31(Z1): 132-139.
- [10] 刘明, 张治中, 程方, 等. 5G 与 Wi-Fi 融合组网需求分析及关键技术研究[J]. 电信科学, 2014, 30(8): 99-105.
LIU M, ZHANG Z Z, CHENG F, et al. Analysis of network demand and research on the key technology for integration of 5G and Wi-Fi [J]. Telecommunications Science, 2014, 30(8): 99-105.
- [11] 雷秋燕, 张治中, 程方, 等. 基于 C-RAN 的 5G 无线接入网架构[J]. 电信科学, 2015, 31(1): 112-121.
LEI Q Y, ZHANG Z Z, CHENG F, et al. 5G radio access network architecture based on C-RAN [J]. Telecommunications

Science, 2015, 31(1): 112-121.

- [12] 董振江, 董昊, 韦薇, 等. 5G 环境下的新业务应用及发展趋势[J]. 电信科学, 2016, 32(6): 58-64.

DONG Z J, DONG H, WEI W, et al. New services and development trend in 5G environment[J]. Telecommunications Science, 2016, 32(6): 58-64.

- [13] 曲桦, 栾智荣, 赵季红, 等. 基于软件定义的以用户为中心的 5G 无线网络架构[J]. 电信科学, 2015, 31(5): 42-46.

QU H, LUAN Z R, ZHAO J H, et al. Software defined user centric 5G wireless network framework [J]. Telecommunications Science, 2015, 31(5): 42-46.

- [14] 管红光, 杨宜镇, 任万里, 等. 基于 OpenFlow 的网络虚拟化技术研究应用[J]. 电信科学, 2014, 30(1): 96-102.

GUAN H G, YANG Y Z, REN W L, et al. Research and application of network virtualization technology based on OpenFlow[J]. Telecommunications Science, 2014, 30(1): 96-102.

[作者简介]



程德恽(1977-), 男, 上海市信息网络有限公司副总经理、高级工程师, 主要研究方向为计算机网络、通信网络。



乔健(1973-), 男, 上海市信息网络有限公司系统运营部高级技术经理、工程师, 主要研究方向为计算机网络、通信网络、网络安全。