新闻热线：010—58884108
E-mail：chenm@stdaily.com
■责编 梁彦晓
科技日报
2020年3月25日 星期三

5G时代，微小基站的建设将与宏基站齐头并进。两者相互配合，才有望“织”出一张立体化、全覆盖的5G网络。

打造高质量5G 离不开这对“超强组合”

本报记者 **张 晔**

去年以来，全球5G规模化商用步伐加快，预计2020年即将发布的由全球通信行业标准化组织3GPP制定的5G R16 标准将支持和催生更多5G行业应用。

最近，我国首个5G微基站射频芯片YD9601研发流片成功，进入封装测试阶段。领衔这项开发的国家特聘专家、美国麻省理工学院博士王俊峰介绍说，5G基站分为宏基站和微小基站两种，宏基站主要用于室外覆盖，微小基站发射功率较小，主要用于室内场景。

从2G到4G，运营商只需要建设一个高高的铁塔，搭载一个宏基站，就能满足方圆数平方公里内的通信需求。到了5G时代，为何在宏基站之外还要建设微小基站？微基站的发展，将对人们的无线通信、工业互联网的数据传输和我国的通信产业带来哪些改变？科技日报记者为此走访了相关高校和企业，听听专家怎么说。

不同基站类型功率容量大不相同

“根据3GPP组织的规则，无线基站分为4类，分别是宏基站、微基站、皮基站和飞基站。”中科智达物联网系统有限公司董事长许欣说。

划分基站主要依据是功率和容量。其中，宏基站的功率在10W以上，可同时接入用户数视基站规模而定，一般在1000个以上；微基站功率为500mW—10W，同时接入用户数为128—512个；皮基站功率为100—500mW，同时接入用户数为64—128个；飞基站功率小于100mW，同时接入用户数8—16个。微基站、皮基站和飞基站，通常合称“微小基站”，也就是我们谈到与宏基站所对应时的概念。

从名字上也可以判断，“宏基站”是高大威猛，“微小基站”则是小巧玲珑。

宏基站适用于广域覆盖，微基站偏向局域覆盖，皮基站相当于企业级WiFi，而飞基站则与家庭路由器相当。

针对不同的室内场景，比如高铁站、飞机场、大商场等，必须布置多个微基站才能满足需求；而在写字楼、工厂园区等场所，人流量相对固定，皮基站就可以胜任；飞基站则是满足家庭、咖啡馆等场景的需要。

宏微交错“织”出更密5G网络

翻开人类无线通信发展史，会发现频率越来越高，这是因为人们对无线通信提出的要求也越来越高。以我国为例，2G的工作频段主要是900MHz和1.8GHz，3G和4G的工作频段主要为1.9GHz、2.1GHz和2.6GHz，而即将到来的5G则主要集中在两个频段：3.3—3.6GHz、4.8—5GHz。

“过去的无线通信是语音网，现在则是数据网，频率越高所能提供的带宽也就越大，就好比4车道的高速公路比2车道的高速公路跑的车多，而且车速还快。”东南大学信息科学与工程学院教授张川说。

然而无线信号的传输速率与穿透性往往不可兼得。“无线频率越高，穿透性就越差，同等面积必须建设更多的基站来完成覆盖，组网成本就比较高。”许欣介绍说。

目前我国正在规模建设的基站，以宏基站为主。一个5G宏基站的成本有多高呢？一般来说，宏基站的建设成本是由主设备、动力配套设备设施、土建施工共同组成。此前广东省拟建设2.4万个宏基站，计划投资60亿元，每个基站的投资额约为25万元。而据上海市的网络建设规划，2020年累积建设2万个5G基站，累计总投资超过200亿元，每个5G基站的建设成本超过了100万元。中国移动也曾经表示，建成一个5G宏基站，成本大约是4G的3倍左右。除去建设成本之外，后续的维护、使用成本等，又是一大笔开销。

在5G性能与建设成本间寻求最优解，是运营商势必要解决的问题，因此他们将目光转向了微小基站。

许欣告诉记者，微小基站不像宏基站需要专用的机房和回程网络，所以设备简单、部署灵活、成本较低。它甚至能够直接钉在墙上，或者藏身路灯杆、公交站牌等任何不起眼的角落，可以根据需求在人流密集、信号较差的地方建设。

而且有媒体做过抽样调查，几乎80%以上的用户流量来自室内，80%以上的用户投诉也来自室内，这些投诉主要集中在信号质量上。“因此可以大力在室内建设微小基站，增强室内网络覆盖的质量。”张川说。

值得一提的是，德国和日本等工业强国已经或正在为工业等行业5G应用分配频谱，打造行业专有5G网络，并且主要的设备形态就是微小基站。

当然，微小基站也不是那么尽善尽美。由于微小基站发射的信号是散射的，各微小基站之间的信号还会相互干扰，造成大量资源浪费。并且微小基站的可靠性远不如宏基站，目前还不能稳定应对室外环境，因此目前主要用于解决室内覆盖。张川认为，5G时代，微小基站的建设将与宏基站齐头并进。两者相互配合，才有望“织”出一张立体化、全覆盖的5G网络。

将微小基站核心技术牢牢抓在自己手里

无人车间、黑灯工厂、智能机器人……在高速率、低时延的5G时代，许多工业互联网的应用场景不断呈现，一个生产车间只需架设若干微小基站即可低成本接入5G网络，实现远程控制与精密制造。

微小基站的核心元器件是基带芯片和射频芯片，两者的物料成本占整个基站的50%左右，而利润可能高达90%。许欣认为，如果谁能攻克这两个核心器件，就能将发展微小基站的主动权牢牢掌握在自己手中。而当前我国在这方面的产业链比较薄弱，成为制约5G微小基站产业发展的重要因素。

王俊峰告诉记者，南京宇都通讯科技有限公司自主研发成功的YD9601射频芯片，不光覆盖700MHz广电频段，也兼容了工信部2月初刚刚颁发许可的3.3—3.4GHz的电信、联通、广电共享室内频段，可以说是为5G时代室内共享微小基站量身定做的芯片。

目前，以工业互联网为核心的智能制造浪潮，已经席卷全球。“以机械加工行业为例，目前中国有1000万台机床，但从事零部件机械加工的中小企业在设备联网和现场实时管理方面还比较落后，而工业互联网对于远程数据采集和机器控制的要求非常之高，传统网络接入方式无法满足，西门子、博世等国际巨头提出了‘5G工业内网’的解决方案。但是，工业网络对安全性要求更高，5G工业内网基站的核心器件必须自主研发，不能再受制于人。”许欣说。

据不完全统计，目前全球关于5G的专利约1.5万个，与5G工业互联网相关的仅有100多个。与5G工业互联网密切相关的5G微小基站也处于刚刚起步阶段，但是到目前为止，我国还没有出现专门的研发机构与骨干企业领衔开展微小基站的设计开发，微小基站产业发展呈现出散乱局面。

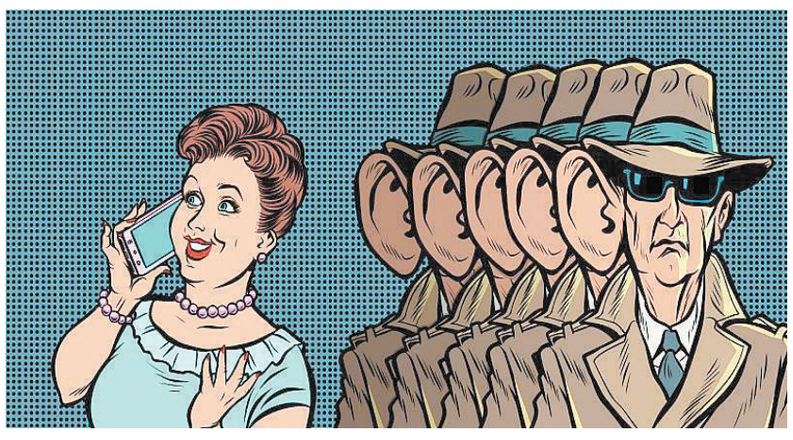
“我国拥有世界最大的5G网络和庞大的工业体系，如果中小型科技企业能抓住微小基站的机遇，我认为一定会实现我国在5G无线通信领域的又一个突破。”许欣说。

信息安全又现漏洞，传感器竟成“窃听器”

本报记者 **马爱平**

加速度计，又称加速度传感器，目前在智能手机上被广泛地应用，可以通过测量手机在各个方向上的“应力”来得出加速度，像手机中的计步器、“摇一摇”等许多功能都基于这些传感器来实现。以往业界普遍认为其和个人隐私信息无关，因此在功能设置上，手机APP可以“无门槛”调用加速度计读数或是获取相应权限。

但是近日，在国际四大信息安全会议之一的“网络与分布式系统安全会议”上，一项来自浙江大学、加拿大麦吉尔大学、多伦多大学学者团队的最新研究成果显示：部分智能手机APP可在用户不知情且无需系统授权的情况下，利用手机内置的加速度传感器来采集手机扬声器所发出声音的震动信号，实现对用户语音的窃听。



利用通话时的手机震动实现窃听

“加速度传感器是目前智能手机中最常见的一种嵌入式传感器，它主要用于探测手机本身的移动，常见的应用场景包括移动检测，步数统计和游戏控制等。”浙江大学网络空间安全学院院长、教授任奎告诉科技日报记者，它之所以能被用来监听电话，主要是由于声音信号是一种由震动产生的、可以通过介质传播的声波，手机扬声器发出的声音会引起手机的震动，而加速度传感器可以灵敏地感知这些震动，因此攻击者可以通过它来捕捉手机震动进而破解其中所包含的信息。

通过加速度传感器窃听语音的准确率有多高？“窃听语音的准确率与具体的窃听任务有关。根据我们的实验结果，在关键字检测任务中，这种窃听攻击识别用户语音中所携带的关键字的平均准确率达到了90%。”任奎说，在实际攻击中，攻击者还可以结合上下文信息和实际语言中各个词汇的使用频率，进一步提升语音窃听的准确率。

手机加速度计可以收集语音信息，这意味着攻击者可以从用户的手机中窃取多种隐私数据。“比如，攻击者也许可以从语音信息中提取出用户的家庭住址、信用卡信息、身份证号、用户名密码等一系列重要信息；通过窃听手机地图的语音导航系统，攻击者也许能提取出一些跟位置有关的关键字，推断出用户目前的位置以及目的地；通过窃听用户手机播放的音乐和视频，攻击者可以推断出用户在这些方面的偏好。”任奎总结说，这种攻击方式对用户隐私安全具有很大威胁。

此外，任奎进一步强调，这种攻击对场景并没有特别的要求，无论手机用户将手机放在桌子上还是拿在手中，“甚至边使用手机边走路，攻击者都可以准确地识别出手机扬声器所播放的语音信息。”

“传感器数据”亟待重新审视

据了解，现行的法律法规对个人敏感信息的保护，主要是针对证件号码、金融账户等具体的个人敏感信息。由于加速计数据本身并不属于个人敏感信息，攻击者可以利用计步软件等必须用到加速计的APP“合理”地对加速计数据进行收集，因此采集加速计数据这种行为本身并不违法。这就意味着，这种攻击方式目前仍处于法律法规的灰色地带。“但使用或贩卖分析出的个人敏感信息应该是违法的。”任奎说。

为有效防御此类攻击，任奎建议，首先应该从技术层面加大对移动设备物理层安全的研究投入，了解各类传感器的实际数据采集能力以及它们可能造成的隐私问题，对可能存在的各类攻击做到心中有数。然后依此重新设计智能手机操作系统中各类传感器的权限使用机制，从技术的角度尽可能地降低数据被滥用的可能性。

此外，任奎还补充道：“我们应当从法律法规上细化对敏感信息的定义和使用规范。除了对证件号码、银行账户、通信记录和内容等具体的个人敏感信息进行保护外，还应对可能包含这些信息的原始传感器数据进行保护，规范和限制这类数据的采集和使用方式。”

那么作为普通消费者，我们目前有机会防止自己的手机被窃听吗？在任奎看来，各大手机厂商提出进一步解决方案之前，消费者能够采取的最有效也最便捷的防御方式，就是通过耳机来接听电话或语音信息。手机中的加速计与耳机间存在着物理隔离，使其无法监测到耳机发出的震动，所以通过耳机播放的声音是不会被这种攻击窃听的。

行业观察

北京市互联网科技企业助力海外公民抗疫

新华社讯（记者**王晓洁**）记者近日从北京市新冠肺炎疫情防控工作新闻发布会上获悉，北京市互联网企业心系海外华人，相继推出远程医疗和咨询服务，帮助解决部分海外中国公民获得当地医疗咨询服务难、出门问诊易被感染的问题，我驻外使领馆也陆续在其官方网站进行了推荐。

北京市疾控中心副主任庞星火介绍，为应对境外疫情暴发性增长的挑战，百度健康推出了“海外抗疫公益计划”，发挥平台权威专家、服务等资源优势，免费提供线上医疗咨询、心理咨询、专家直播等实用服务。

其中，百度健康“问医生”平台有超10万名医生提供全天候的免费在线医疗咨询服务，远程咨询医师团队由接受过新冠肺炎专业诊疗方案培训的公立医院执业医生组成。所有海外侨胞和留学生都可以得到全科室专业医生咨询服务。

另一互联网平台“京东健康”上线了“全球免费健康咨询平台”，召集了在国内抗击疫情过程中积累了丰富经验的专家和医生，搭建“一线抗疫名医团”，其中包括由30多名中医专家组成的“中医抗疫专区”，提供专业的在线咨询和问诊服务。

考虑到外籍人士医疗咨询和援助的需要，京东健康同步上线了双语服务专区，目前已有20多名有英语接诊能力的医生可提供在线图文沟通形式的英语问诊咨询服务，方便外籍人士远程就医就诊。

庞星火表示，海外用户通过百度搜索“全球抗疫”、在百度APP中搜索“百度健康”或者京东APP搜索“京东健康”进入小程序即可体验全部公益服务。

“抓包”案拷问银行客户端安全流程设计

本报记者 **刘 艳**

钻“手机银行”人脸识别系统的空子，伪造76个虚假身份骗取银行账户并售卖的田某，被判刑两年。

对于中国裁判文书网公布的这起黑客入侵厦门银行手机银行的案子，网络安全工程师们表示，犯罪分子的作案手段没什么技术含量，就是利用了他们常用来做网络安全测试的“抓包”工具（软件）。在这起案件中，系统被入侵这个锅不能甩给人脸识别技术，需要复盘的是银行业务安全流程。

“抓包”骗过银行人脸识别验证

抓包（packet capture）工具是拦截查看网络数据包内容的软件，它能够将网络传输发送与接收的数据进行截获、编辑、转存、重发等操作，常被技术人员用来检查网络安全。黑客也不都是江洋大盗，利用技术来维护网络安全的黑客叫做“白帽子黑客”，他们也会用抓包工具来分析报文，针对漏洞做渗透测试，这种行为属于阳光下的操作，而“黑帽子黑客”是一群通过窃取网络资源或破解软件来获取利益的人，他们抓包就是为了破坏网络来赚钱。

早在2017年，上海警方曾破获一起特大网络盗窃案，犯罪分子仅用半天时间就非法提现人民币近千万元，警方通过调查发现，是黑客利用抓包工具拦截下银行系统内传输的数据，将实际充值的1元改为1000元或更高金额，然后把伪造的数据传回并成功欺骗了金融机构。

但所有利用抓包工具的案件都有一个共同的前提，就是有漏洞可钻。

从福建省厦门市思明区人民法院刑事判决书来看，田某偶然发现厦门银行APP漏洞后，使用虚假身份信息，在厦门银行手机银行APP注册该银行Ⅱ、Ⅲ类账户。注册中，田某先输入本人身份信息，待进入人脸识别步骤，利用抓包软件将银行系统下发的人脸识别身份认证数据包拦截并保存。尔后，在输入开卡密码步骤，田某将APP返回到第一步（上传身份证照片），重新输入伪造的身份信息，当再次进入到人脸识别的身份验证步骤时，他把之前拦截下来的包含其本人真实身份信息的数据包进行上传，使系统误以为此刻要对比的是其真实的身份信息，田某遂用本人人脸通过了银行系统人脸识别比对，成功利用虚假身份信息注册到银行账户。

简单地说，田某的作案手法是，用他本人的人脸识别身份认证数据包换掉伪造身份的人脸识别身份认证数据包，骗过银行系统的审核。

安全问题需要向内找原因

现如今，人脸识别在金融领域的应用越来越广泛。以银行为例，区别于Ⅰ类全功能账户，银行的Ⅱ、Ⅲ类账户为虚拟电子账户，在Ⅰ类账户的基础上功能递减，现在很多银行都可以通过手机终端远程开通Ⅱ、Ⅲ类账户，人脸识别已经成为核实用户身份的常用手段。铸造一道固若金汤的安全防护墙，是每一个金融消费者的诉求。

中粤联合投资创始人罗浩元说：“银行Ⅱ、Ⅲ类户开户存在的明显风险被田某用简单粗暴的手法测出来了，我们相信手机银行在功能设计、安全验证及防护等方面的完善能力，却通过此案看到了他们的‘漫不经心’。显然，这些银行对‘抓包’替换行为缺乏该有的防范措施。关键是，此前用‘抓包’非法获利的案件已有很多，金融机构需要检讨。”

北京奇安信科技有限公司董事长齐向东给金融机构开出一副“药方”，其中包括几个假设，或许对银行等金融机构检视业务安全有帮助。这几个假设是：“假设系统一定有没被发现的漏洞，一定有已发现漏洞没打补丁；假设系统已经被黑；假设一定有内鬼。”

尽管在这起案件中，人脸识别系统可以说是无辜“躺枪”，但是公众对人脸识别安全性的顾虑也被这起案件重新牵了出来。

对此，百度安全事业部总经理马杰有这样的观点，越来越多的智能设备采用了生物特征识别技术，所谓“破解生物识别”，就是“欺骗传感器”的过程。但大家不用过分担心，被发现的漏洞基本都找到了相应的解决方案。很多安全问题，可以看做安全人员与黑客之间的竞速赛，未来人脸识别技术要跟随机器学习等相关领域一同发展，才能构筑一个更加安全、更加可靠的环境。