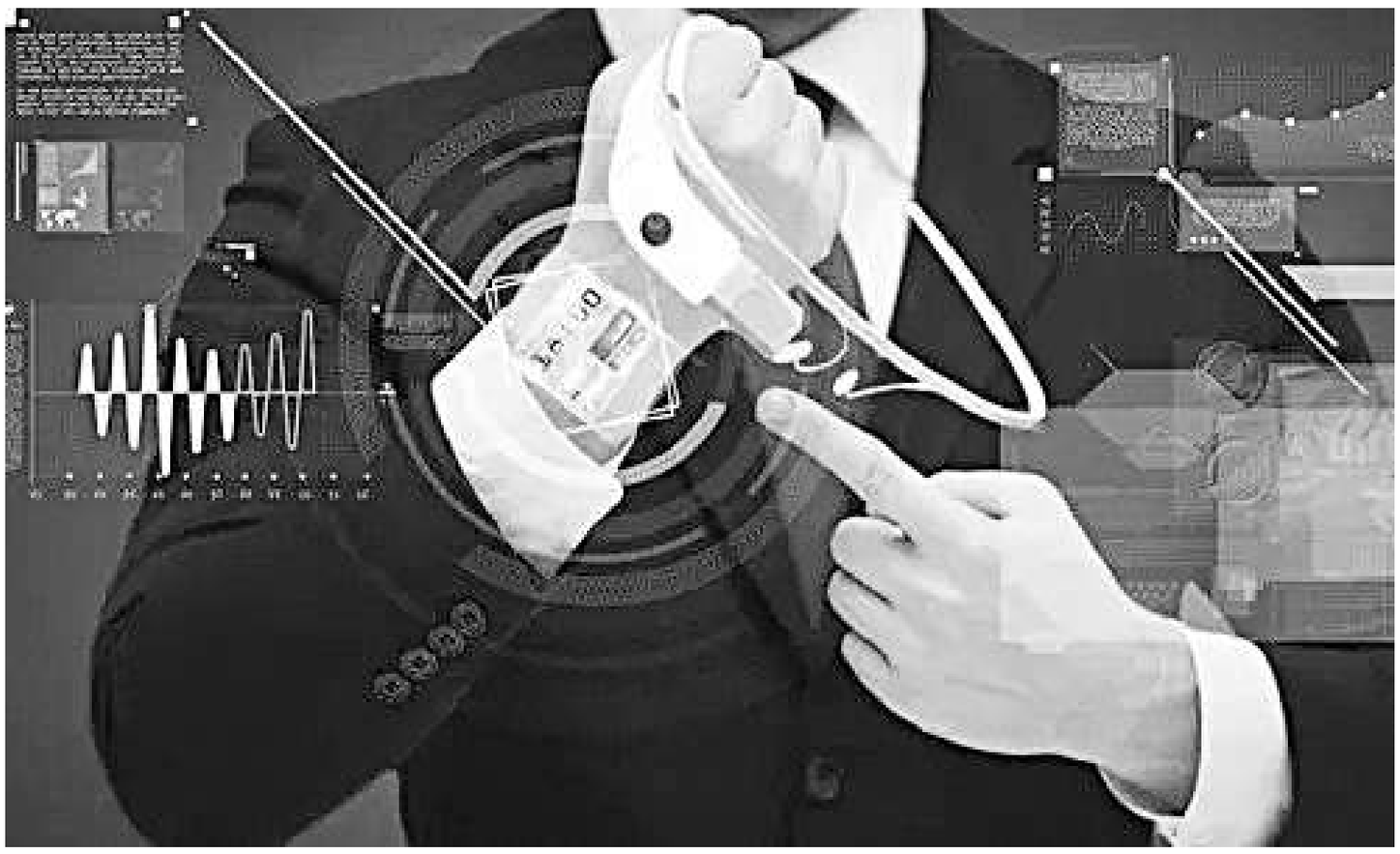
新闻热线：010—58884080
E-mail：kjrbgjb@vip.sina.com
■值班主任 王俊鸣 责编 聂翠蓉 华 凌
科技日报 2015年9月15日 星期二

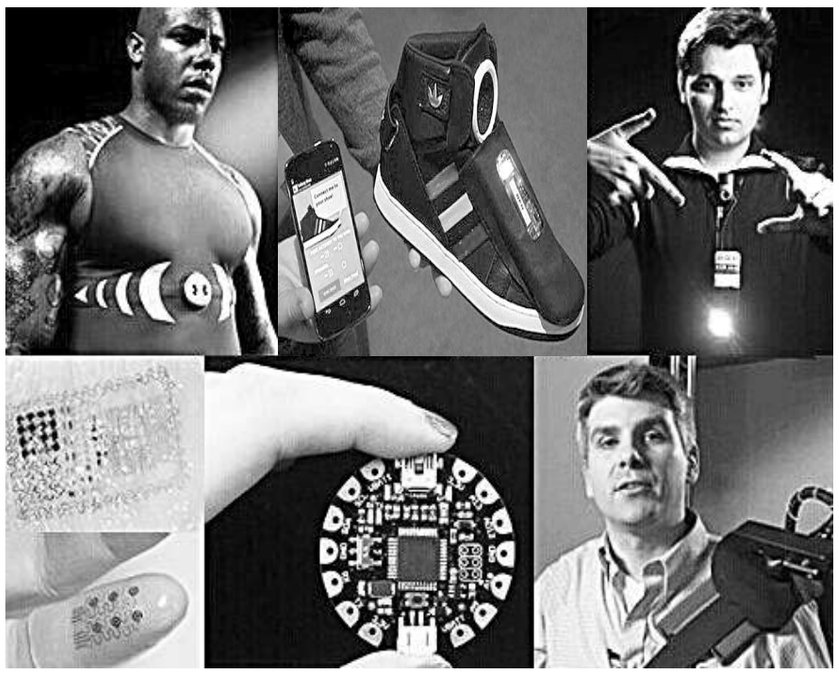
《自然》杂志网站在近日的报道中指出，佩戴在我们身体表面和嵌入人体内的电子设备与日俱增，但如何让它们安全有效地传输数据仍是一个巨大的挑战。

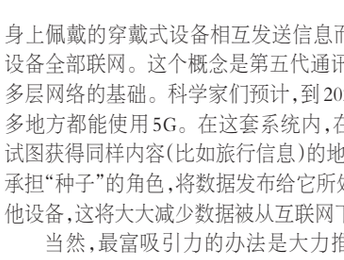
穿戴式设备：想说爱你不容易

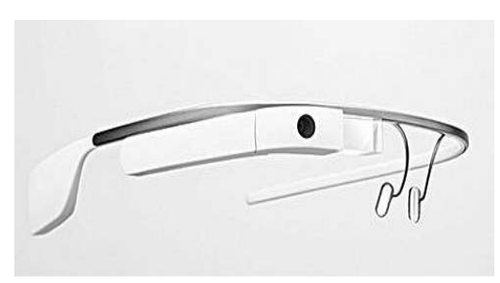
——网络拥堵和信息安全成了两只“拦路虎”

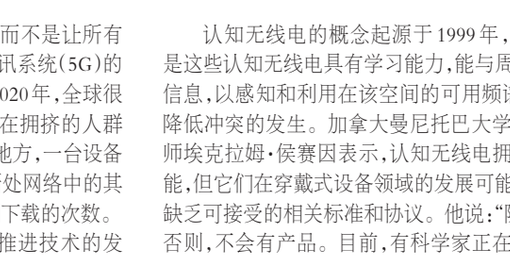
本报记者 刘 霞 综合外电

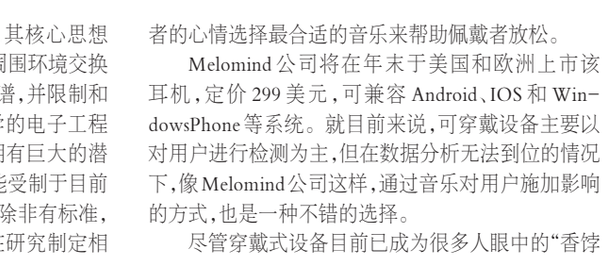












汤姆坐火车要迟到了。但是，“屋漏偏逢连夜雨”，他不知道怎么去车站，情急之下，他跑到街角一个人潮涌动的购物中心，快速拍了一些照片，然后上传到社交平台Instagram和脸谱上。随后，他让已经联网的隐形眼镜下载一副地图，告诉他如何去车站；同时，他还按下智能手表的按钮，买了一张车票并获得了站台的信息。他的隐形眼镜闪了一下，提醒他火车15分钟之后开出，但地图还没有下载完。他焦急地四处观望，对他的隐形眼镜不断高喊“刷新”。隐形眼镜向他发出了提醒：“你感到焦虑，没关系，放轻松，深呼吸。”但因为互联网上的人实在太多，汤姆下载整幅地图的希望几乎破灭了。

这是穿戴式设备纷繁无序的一幕……

严阵以待 对付“拦路虎”

穿戴式设备或能让真实世界与数字生活实现无缝对接。这些小玩意的数量与日俱增，五年之内，可能会有约5亿台设备被穿戴在人身上甚至嵌入人体内。目前，我们耳熟能详的设备大都是健康追踪设备和智能手表等，这些设备会监测我们的健康状况并为在线服务提供入口。

但有些设备号称能做更多事情，比如头盔能在佩戴者心神意乱时进行提醒；而腕带则能通过震动帮助人们戒烟。有些电子设备公司更是承诺，可以用穿戴式设备递送药物；治疗一些症状或进行医疗护理等。在癫痫病人发病初期发出警告的设备、帮助预防心脏病的设备以及帮助盲人导航的设备也蜂拥而至。

实际上，穿戴式设备的巨大潜能主要依靠它们获得并生成的海量数据。这或许会导致两个问题：首先，找到更好的方法来将数据输入和输出；其次，保证所有信息的安全。研究人员和技术开发人员正在着力解决这两个问题。

现在，包括汽车到烤面包机等在内的设备都已联网，对于带宽的需求让整个互联网系统不堪重负。仅仅去年，就有大约5亿台新设备开始通过手机无线通讯，与5年前相比，移动网络的拥堵程度增加了25倍。不仅如此，穿戴式设备的出现还导致新的安全问题——从极度私人数据的滥用到追踪人的活动来恶意攻击他们网络行动的涌现等。

马里兰大学网络安全中心主任阿努潘·乔希说：“只要有新技术出现，我们就要开始畅想其可能会为我们营造的美妙新世界和其可能带来的问题，这已经成为一种陈词滥调。但在穿戴式设备领域——更宽泛一点来说是物联网领域，我们真的正在迈入一个全新的时代，我们必须对这些问题严阵以待。”

多管齐下 纾解网络拥堵

网络技术公司思科的数据显示，到2014年年底，全球移动数据的流量为25亿GB/月。其中，全球1亿台左右的穿戴式设备每月产生1500GB的数据流量，到2019年，这一数据可能会增加5倍。德克萨斯大学奥斯汀分校电子工程系教授罗伯特·希斯表示，这些设备汹涌而来，而且，有越来越多人开始佩戴数据流量非常大的增强现实和虚拟现实头盔，未来很有可能造成网络拥堵，特别是对非常重要的网络产生威胁。

为了解决网络堵塞问题，奥巴马在2010年指示国家电信和信息管理局与联邦通讯委员会（FCC）合作，在未来10年内，从现有的联邦或非联邦频谱中腾出500MHz供无线宽带使用——500MHz大约为无线宽带目前可用频谱数量的两倍。但美国无线通讯和互联网协会（CTIA）最近公布的报告表明，即便如此也还不够。它们估计，从现在到2019年，为了满足美国无线宽带的使用需求，可能还需要增加150MHz的频谱。而且，带宽有限是一个全球性的问题，各国都在采用自己的方式试图解决这个问题。比如，印度居民的上网带宽仅为美国居民的十分之一，印度人要求频率共享并开放目前给军方的频率；而英国政府则鼓励大家使用陈旧的提供模拟信号的电视带宽；使用这些频率的首款智能设备网将于今年年底“横空出世”。

通讯公司出于利益的考虑，需要更有效地利用频率。一种方式是利用无线电波和电视频道拥挤的部分。从一个人身上的所有穿戴式设备获取的数据可能会流经一个使用完全不同波段的人体无线局域网。随后，仅仅一款设备使用这些更拥挤的波段来将所有数据传到互联网。然而，这本身也会产生问题，因为波长越短，传输需要的能量越多而且越有可能被人体遮挡。为此，包括希斯在内的研究人员正尝试解决这些问题，如通过让天线达到最优来减少干扰以及能耗等。

另一种极富前景的想法目前由科学家们提出了：使用发光二极管（LED）将无线电通讯引入可见光领域。LED会发光，而且也可以承担光接收器的功能，从而可以让穿戴式设备相互通讯或直接同互联网相连。嵌入了LED的穿戴式设备会感应人的一举一动，并让信息同房间内已经通过电线联网的灯具通讯。尽管这一技术主要依靠可见光，但信号非常细微。瑞士应用科学大学的电子工程师丹尼尔·普西尼里主要研究可见光通讯，他说：“LED闪烁得很快，人眼无法区分。”

英国爱丁堡大学电子通讯学院移动通讯系主任哈拉尔德·哈斯主要研究移动通讯，他计划明年在医院测试一种可见光系统。在这套系统中，病人将佩戴能监测体温的腕带，并使用能同医院的照明系统通讯的LED发送数据。

此外，科学家们提出的第三种解决办法：让人们身上佩戴的穿戴式设备相互发送信息而不是让所有设备全部联网。这个概念是第五代通讯系统（5G）的多层网络的基础。科学家们预计，到2020年，全球很多地方都能使用5G。在这套系统内，在拥挤的人群试图获得同样内容（比如旅行信息）的地方，一台设备承担“种子”的角色，将数据发布给它所处网络中的其他设备，这将大大减少数据被从互联网下载的次数。

当然，最富吸引力的办法是大力推进技术的发展，使设备变得更聪明，能知道何时以及如何使用通讯通道。这些“认知无线电”可以发现未被使用的宽带区域并见缝插针，提高通讯效率。为了让每个波段发挥其最大的潜能，波段需要更加开放，如此一来，设备可能会利用已获得授权的频率进行通讯，随后在其他拥有更高优先级的设备进入时跳出这个频段。尽管基于这一原则的技术已被使用了数十年，但“认知无线电”技术能将效率提高到新的层次，而且，足够聪明的设备会相互协商来分配这些可用的频道。

认知无线电的概念起源于1999年，其核心思想是这些认知无线电具有学习能力，能与周围环境交换信息，以感知和利用在该空间的可用频谱，并限制和降低冲突的发生。加拿大曼尼托巴大学的电子工程师埃克拉姆·侯赛因表示，认知无线电拥有巨大的潜能，但它们在穿戴式设备领域的发展可能受制于目前缺乏可接受的相关标准和协议。他说：“除非有标准，否则，不会有产品。目前，有科学家正在研究制定相关标准和协议。”

多措并举 保障信息安全

今年1月份，有17.6万人蜂拥至在拉斯维加斯举办的国际消费电子展（CES），其中几款新奇的穿戴式设备吸引了观众的眼球，比如，一款名为“Pacifi-i”的安抚奶嘴能监测婴儿的体温并将数据传输到父母的手机上。另外一款放松神器Melomind智能耳机能监测大脑的电波活动，并发送到手机上，然后根据佩戴者的心情选择最合适的音乐来帮助佩戴者放松。

Melomind公司将在年末于美国和欧洲上市该耳机，定价299美元，可兼容Android、IOS和WindowsPhone等系统。就目前来说，可穿戴设备主要以对用户进行检测为主，但在数据分析无法到位的情况下，像Melomind公司这样，通过音乐对用户施加影响的方式，也是一种不错的选择。

尽管穿戴式设备目前已成为很多人眼中的“香饽饽”，但很多人还是对其前景持怀疑态度。普西尼里说：“很多人仅仅将穿戴式设备看成玩具。”但有诸多迹象表明，未来它们将发挥更大作用，尤其是在医疗领域。例如，穿戴式设备在监测人体的生理机能方面的表现也日益突出，比如给大脑提供刺激，甚至可以注射药物。但对于用户来说，这些应用也伴随着潜在的危险。

穿戴式设备革命面临的另一个关键“拦路虎”是公众对于数据安全和隐私泄露的担忧。穿戴式设备会收集大量的用户私人数据，而在一个“数据为王”的数字和信息时代，这引发了公众的广泛担忧。调查表明，用户担心这些设备会侵犯他们的隐私，并将一些重要的数据泄露给商业机构。

2014年，皮尤研究中心对1600名专家进行了一个关于互联网未来的采访，很多人表达了同样的忧虑。这项报告指出：“这是个数据无所不在的世界，人们担心自己的隐私被泄露，也担心自己对生活的掌控力越来越弱。”

这些担忧并非空穴来风，有很多事件也佐证了用户的想法并加深了这种忧虑。比如当Fitbit公司活动跟踪器的用户允许人们可以公开获得他们的活动日志时，也无意中将其性生活大白于天下。2011年，Fitbit公司认识到了这一点，很快采取行动解决了这个问题。

而另外一个事件则与目前炙手可热的谷歌眼镜有关，两年前，谷歌眼镜的“呱呱坠地”触发了人们的担忧，人们担心用户会在旁人不知觉的情况下为其照相。网络安全中心的研究人员将这看成是天赐良机，他们打算开发一些能强化隐私保护的计算机代码。为此，他们开发了一个有趣的FaceBlock应用软件，这个程序会将那些要求不被谷歌眼镜拍到的人的脸部遮挡住。不过，要想这个程序起作用，谷歌眼镜用户必须安装这一应用程序。乔希说，如此看来，这样的系统可靠地提供隐私保护的唯一方式是制造商们将其整合入硬件，他说：“我认为谷歌会将这种属性内置进每副谷歌眼镜内，如此一来，它将自动遵守这些命令和要求。”

除此之外，人们也担心自己的隐私泄露。尽管密码正变得越来越普遍而且也越来越先进，但有时候，有些低端的穿戴式设备并没有使用密码。

2014年，加州信息管理公司赛门铁克称，目前在市场上广受追捧的监测器等很多健康监测设备很容易被追踪到位置。而且，其中一些监测器的密码也很容易被破译，这使它们更容易被攻击。而且，即便一台健康监测器已经被加密，但让其联网的智能手机或无线上网设备也可能成为一个弱点，因为这些智能手机或上网设备容易被恶意软件攻击。

佛罗里达国际大学的安全研究员波格丹·卡比纳尔表示：“如果你没有对数据进行加密，那么，你绝对不安全。”卡比纳尔目前正与包括IBM的前雇员在内的研究员合作，研究两个广受欢迎的低端穿戴式健康设备—Fitbit Ultra计步器和Garmin Forerunner腕表的安全漏洞。他们发现，通过冒充这两款设备授信的网络服务器，就能愚弄这两款设备，比如让其上载错误的数据，甚至包括一些毫无意义的数字，比如一天走了几百万步等。

研究人员也发现，他们可以将数据添加在这些追踪器上，这会降低数据的精确度，而且，如果健康数据同保险费关联的话，这很可能会成为一个问题。Fitbit公司对《自然》杂志表示，该公司已经意识到了这个问题，在后面推出的产品会解决这个问题。

卡比纳尔认为，对于制造商来说，提高安全性会增加金钱成本、研发时间；会让设备的体型变大从而增加能耗。不过，研究人员正努力让成本最小化。卡比纳尔在和同事研究了如何攻击设备之后，他们开始想办法为这些设备的安全“保驾护航”。为此，他们研发了SensCrypt，这款加密协议专门用于低能耗的健康追踪器，能减少通讯成本。即使设备被偷并被篡改，它也能使用“对称密钥加密”方法来对付远程攻击并提供某些安全保护。研究人员目前还无法将其用在Fitbit或Garmin设备上，因为这两款设备使用闭源代码，但他们已在开源的代理服务器上对这套系统进行了测试。

比利时鲁汶大学的密码学家布拉特·普瑞尼尔说，尽管加密程度很高，但设备仍然很容易受到攻击。普瑞尼尔专门研究旁道攻击，在这些攻击中，黑客通过探测能耗波动来渗入移动设备，并使用这些能耗波动来获得密钥以及其他安全信息。

普瑞尼尔说：“这些攻击可以在10到20米的范围内进行，20年前，银行卡就受到过这种攻击，但预防这种攻击的方式一直没有在穿戴式设备尤其是植入医疗设备上使用。”

多家公司目前正尝试通过配置生物识别设备，比如指纹识别设备和虹膜扫描设备来提高移动设备和穿戴式设备的安全标准。但即便这些生物识别设备也并不安全，研究人员和黑客已经通过实验证明，高清照相机能从远距离捕获人的虹膜并使用手机上的照相机来盗窃指纹。

但普瑞尼尔表示，如果研究人员能够研制出一些不那么容易被发现的加密方式的话，这些生物识别设备对加密大有裨益。比如，目前市面上已经出现了一些穿戴式设备，授权用户基于自己的心跳模式来做密码。普瑞尼尔估计，从长远来看，用户可以使用身体的内部信号，比如DNA或内部生物群落做穿戴式设备的密码，如此一来，设备只有在密码信息同主人非常接近时才能被解锁。

利用这些安全改进手段以及通讯网络的升级措施，未来佩戴者在迷路时，穿戴式设备也能在拥挤的商场内很好地工作。比如，汤姆会很容易获得城市的地图，而且也会放心地知道，他的私人数据已被安全地加密。

如此一来，汤姆甚至有充足的时间喝一杯咖啡，给设备充电，然后，再悠哉悠哉地到达车站。这并非某些对穿戴式设备非常狂热的人构想出的技术“乌托邦”，而是技术给我们带来的可期的未来图景。