

# 移动医疗向“看病难”说再见

“互联网+医疗”是医疗转型的新路径,移动医疗也借着“互联网+医疗”的东风正在深入到传统医疗的方方面面,解决了部分“看病三分钟、排队三小时”等现实问题。

## 一台智能终端或能解决“看病难”现状

“看病难、挂号难”是一直困扰着我们的社会难题,其实你手里的那一台小小的智能终端或许就能够突破这一瓶颈。近日,以单病种为主的移动医疗医生团队平台在广州上线,患者通过这一平台可足不出户完成预约挂号、分诊咨询、远程门诊、线上付费、检查预约、住院床位预约、慢病随访等医事服务。此平台将类似于帕金森、慢阻肺等单病种的

优质医生组织起来,应用远程高清音视频、电子处方及医保系统的连接,实现了医生与患者间的在线远程诊疗。用户在家中通过手机APP、电脑用户端,利用远程诊疗,就可以享有实体医院专家的服务。

这家“赢医通医生团队平台”的技术体系负责人叶让介绍,该平台同药店合作,由各合作药店将就医用药配送到家,打通药品配送“最后一公里”,方便患者。

## 智能手机测癌症准确率达99%

提起iPhone的功能,我们想到的或许是打电话、拍照片,但你有没有想过它能诊断癌症呢?由华盛顿州立大学助理教授李雷领导的研究团队,已成功研发

一项利用iPhone协助进行光谱分析的移动型实验室,可精确检测癌症,并且准确度达到99%。

可携式实验室检测的是人类的细胞激素IL-6,IL-6被视为辨识肺癌、前列腺癌、肝癌、乳腺癌和上皮癌症的生物标记。

李雷表示,整个可携式实验室的主要组件包括智能手机、微板支架和一个电池支架、背光面板和定制设计的微棱镜阵列。他的团队还创建了一个自定义应用程序来设置光学感测参数,将每个样品与相应的通道对齐。

李雷说:“在没有实验室的偏远诊所和医院,这种可通过智能手机驱动的可携式实验室将发挥作用,成本不到150



美元。”

移动医疗正在让医疗服务变得随手可得,解决了医疗信息不对称、医疗资源不对等等问题。利用移动网络便可实现远程“求医问药”,也让患者掌握了看病的主动权。

人民网 2016.10.27 文/王迪

# 马铃薯主食产业化：雷声大雨点小

近日,有媒体报道,马铃薯全粉高出面粉两倍以上价格劣势,是马铃薯主食产业化“雷声大雨点小”的主因。对此,国家马铃薯主食化课题组负责人、中国农科院农产品加工所所长戴小枫和该所传统食品加工与装备研究室主任张泓作出明确回应。

## 用熟全粉来做是老皇历了

所谓价格劣势,是指目前市场上,马铃薯全粉每吨价格高达9000多元,而同期面粉每吨仅4000—5000元。

张泓解答说,每吨9000多元的是马铃薯熟全粉,生全粉价格只是略高于面粉。关键在于,用熟全粉来做马铃薯面条,那是一年多前的“老皇历”了。一年来,马铃薯生粉掺面粉制备挂面技术攻关早已获突破。他表示,最新技术是,直

接用薯泥掺面粉做成面条,成本更低,口感更好。

“马铃薯主食化关键技术已经基本得到解决”,这是戴小枫对马铃薯主食化技术现状的基本判断。

## 产业化路上的“拦路虎”

在戴小枫看来,马铃薯主食产业化路途上的“拦路虎”主要有三:观念、成本、品种,其中最大的问题在于观念。

他所说的观念,就是国人长期以来“不把土豆当干粮”。马铃薯在中国一直被拿来主要当菜吃,根本原因是,中国人的主食“四大件”——馒头、面条、米饭、米线,都需二次加工成型;而马铃薯全粉不像小麦粉那样可以轻易做成馒头、面条,更不像稻米那样可以直接做成米饭、米线,顶多做成粉条当副食吃。而在西方,

土豆泥、薯片甚至是未经加工的土豆块直接蒸煮熟,都是大众喜闻乐见的主食。

## 产能建设和释放需要一个过程

张泓以挂面为例算了这样一笔账:目前全国挂面生产线有500万吨产能,马铃薯挂面要在市场上形成批量和受众反应,至少要有挂面1/4到1/3的产能,“这得费些时间”。这也说明了为什么我们在北上广深这样的一线城市市场上,还很少能感知到马铃薯主食;而更大范围内企业的上产意愿,直接取决于其市场接受度,这是个观念问题。

所以,马铃薯主食从小众走向大众,在技术、成本、政策等层面,已经“万事俱备,静候佳期”了。这个“佳期”,是建立在观念转变基础上的产能释放过程。

《科技日报》2016.10.30 文/瞿剑

# “无限流量”的电话卡能否成未来主流？

随着3G时代,尤其是4G时代到来,语音通话、视频通话、4K高清视频、网络直播、大型网游、VR等新技术、新产品的出现,使得手机用户对流量需求越来越多,一天使用几百兆流量的事情常有。

近日,有运营商在一些地区推出了无限流量卡的业务,再度引起了人们对无限流量的讨论,是否可能成为未来国内三大运营商主推业务呢?

## 多地推“限速版”无限流量卡

今年9月19日,中国联通江苏分公司在其官网上公布,将推出“沃快无限流量卡”,同时,还赠送1800分钟的省内通话。

需要注意的是,这款无限流量卡会实施限速方案,它的最高网速可以达到450Mbps,但是月数据总流量(含套餐内外各种收费、免费、定向等流量,含国际及港澳台漫游流量)达到40G之后,则下行限速至384Kbps,上行限速至最高128Kbps,一直到第二个月的1日恢复原网速。

除江苏外,北京、福建、安徽三个省份也有类似业务推出。

## 完全无限流量技术上达不到

那么这种限速版的无限流量是否可能大规模推广呢?彻底的无限流量在未来是否可能呢?

独立IT和通信分析师付亮:基站资源有限,不太可能完全不限制。在目前来看,限速版的无限制流量比较常见,当使用一定的量之后,对速度进行限制,以减少基站的负荷。

通信行业观察家项立刚:完全不限制流量的推广可能性很小。和固网不同,移动网络是有限的。比如,一个基站能够承受几百兆的流量,在2G时代,处理文字和文件时,只需要几K流量,那么同时让大家无限制地使用。但是现在大家看高清视频,玩VR游戏,瞬间流量都能达到几十兆几百兆,如果大家都无限制的使用,基站受不了。《南方日报》2016.10.27

# 是什么让航海家郭川落了水？

北京时间10月19日5时24分11秒,中国职业帆船选手郭川驾驶“中国·青岛号”三体帆船于从旧金山金门大桥出发,以上海金山为目的,进行单人不间断跨太平洋创纪录航行。

然而在时间过了6天半,也就是北京时间10月25日之后,帆船在美国夏威夷海域出现航速减慢的状况。郭川岸队在观察到这一现象后,尝试联系郭川,但均无应答。此后,郭川持续失联。

郭川失联的消息不断牵扯着国人的心。人们也在不断的发问:究竟是什么让航海家郭川落了水?

## 海风中纠结的大三角帆

在郭川岸队航海技术专家看来,事故发生主要有两种可能,其中最有可能的出現问题的地方,就是三体帆船的大三角帆。当时的风速应该是13到20节,郭川用缩降一级的主帆和位于最前方的大三角帆航行,这是合理的帆面组合。正常情况下,到了傍晚,三角帆就可以落下,晚上能航行得更安全。于是在下午

他尝试迎风面落帆,这对于单人航行的水手来说是个难度相当高的操作——首先是收帆的落脚点过于狭窄,其次是风速过快,船速过高,船身不平稳。第三是因为双手操作过于繁琐。或许就在那一瞬间,由于失去了对帆索的控制,大三角帆突然落下。而郭川又试图去阻止大三角帆的落水,造成了船体突然剧烈晃动,把他甩入水中。

## 身体透支 不堪重负

由于事发前几天天气状况奇佳,郭川几乎是透支了全部的体力去尽可能的维持帆船的航行,以至于他每天晚上只能够睡2~4个小时。如此巨大的体力消耗使得郭川在航行过程中身体状况极不稳定。在船速几乎达到顶点的10月25日,郭川只要稍不留神就可能出现危险。在经历了数日近乎不眠的漂泊之后,精神上产生恍惚也是情理之中了。

## 船体碰撞 与不明物的硬接触

在郭川的航海日记中有这样一段描述:“在海面上遇到了鲸鱼,险些发生碰



撞”。在海上航行的船只在高速行驶之下撞到暗礁、鲸鱼,甚至是其他出事船只的碎片,都是极有可能发生的“正常现象”,而对于郭川的三体帆船来讲,这样的碰撞发生一次就极有可能酿成无法挽回的大祸——因为三体帆船为了提高速度减轻重量,通体为玻璃钢制成,强度着实有限。一旦发生就很容易破损,在几分钟之内就有可能沉船。不过船只破碎已经被排除了可能。但这却不排除轻微碰撞或是紧急规避之下强大的惯性作用于郭川的情况。

以上的种种都只是围绕着科学的猜测,无论这些分析有多缜密有多透彻,终究只是猜测。

光明网 2016.10.29 文/毕孝斌

日前,美国两家网络供应商遭遇网络攻击,诸多知名网站一时间无法登陆,号称半个美国互联网被弄瘫。调查显示,这是黑客利用病毒感染物联网设备,进而利用这些设备发起网络攻击。

# 空调能窃听,插座能放火 物联网成了“危”联网？

## 物联网搞定了互联网？

360攻防实验室负责人刘健皓表示,此次感染病毒的物联网设备数以十万计,包括网络摄像头等。主要原因还是这些接入互联网的设备存在大量漏洞,有些漏洞属于系统通用性漏洞,容易被控制。

为什么一次技术含量不高的攻击,却能造成这么大的伤害?

专注物联网安全投资的永洲创投创始合伙人陆一舟介绍,因为物联网设备都讲究通用性,物联网设备都是标准化的,一次出货可能就是几万台甚至几十万台。一旦一个漏洞被发现,黑客就能劫持一批产品。如果不加注意,将来物联网引起的安全事件会比想象的更多。

空调能窃听、插座能放火:智能硬件还有多少坑?

“现在的物联网设备基本都是在‘裸奔’。”陆一舟直言不讳地说。他举了一个例子,有厂商为了检测一款空调的噪音以改进产品,就在空调里安装了收集声音的装备,这些设备可以回传众多空调的分贝数。但很快被安全专家发现了漏洞,只需要略施小计,就可以将其变成“窃听器”。

安天实验室首席技术架构师肖新光介绍,现在很多人家里都买了扫地机器人,这个机器人都有麦克、摄像头等装置,也需连接网络,这就相当于一台潜在的监控设备。一旦遭到攻击,家庭隐私也就无处可藏。

专家表示,现在的智能插座的安全漏洞是比较多的,如果被黑客攻破利用,轻则可制造一批用户无故断电,重则可以让插座过载发热,成为放火的“凶器”。

至于现在风头正劲的新能源车特斯拉也被攻破过。如果黑客能远程遥控一辆智能汽车,对于车主将是件多么可怕的事情。

## 拒绝还是拥抱物联网？

一方面,物联网时代已经逐渐降临,消费者购买的智能硬件也越来越多;而另一方面,物联网的安全却仍非常脆弱。作为消费者,我们该如何应对呢?

对于物联网安全,消费者能做的不多。肖新光说:“不像电脑、手机等设备具有诸如下载杀毒软件等成熟的安全措施,智能硬件无法形成交互。”

为此,对于那些可能出现的安全问题,物联网设备厂商们“贵无旁贷”。

新华社 2016.10.25 文/叶健 阳娜