快递机器人有望6月上岗

物业不许快递员入内，取快递还得亲自下楼，这一“快递最后一公里”难题将被攻克。由海淀驻区企业研发的快递机器人，经过清华大学、中关村智造大街、多个封闭小区7000公里路测和调试，目前已实现小规模量产，有望今年6月在北京一些小区投入使用。快递成本将由人工每单1.5元左右降至1元以下。

6轮设计，车高一米左右，承重30公斤，爬坡高度35度，速度可达12公里每小时，续航可达8小时，定位精度1厘米到3厘米。在北京真机智能科技有限公司，记者见到了外观萌萌的快递机器人——“真机小黄马”。

“日常生活中，收快递常常受时间、空间限制。在许多园区，物业不允许快递员入内，客户需要到固定地点或快递柜取快递。”北京真机智能科技有限公司创始人、CEO刘智勇介绍，“真机小黄马”就是为解决封闭园区“最后一公里”配送问题设计的智能配送机器人。有了它，用户只需要在手机里设定好送货时间和地点，“体内”装满包裹的机器人就可以自主按时送达，手机扫码开箱取货，快捷安全。

技术人员告诉记者，要让机器取代人工完成末端配送，最核心的是打造一套软硬件一体的无人配送网络，或者说是一套“云+端”的天地一体智能系统。终端就是高性价比、高可靠性、可量产的无人配送车队，云端则是一整套的高配送效率、高响应速度的调度系统。

“真机智能利用云计算和机器学习等技术，构建了我们称之为‘玄机’的调度大脑。通过零人工干预的高速实时闭环，形成智能派单和智能规划，构建了无人配送局部网络。”刘智勇介绍。“玄机”调度大脑使调度更智能、高效，同时极具可拓展性，逐渐构建起无人配送的全局网络。“玄机”调度大脑可以在数据罗盘实时看到所有机器人的动态，并与行业合作伙伴的系统进行无缝对接。

快递机器人配备了一系列高端“装备”，包括激光雷达、摄像头和传感器等。针对核心技术之一的定位技术，真机智能选择了“多线激光雷达+GPS+惯导”等多传感器融合定位的方案，实现了精准定位和自主导航。因为搭载多线激光雷达，“真机小黄马”可以在夜间自主巡航，24小时配送。针对路况变化、行人众多等复杂环境，机器人可以通过摄像头进行行人检测、车辆检测，激光雷达进行障碍物识别，采用深度学习的环境建模技术识别行人和物体，提高避障的准确度。

这么萌的机器人上路，怎么防止被抱走？“有GPS摄像头和语音警报系统，一旦有人想抱走它，它会用语音发出警告。”工作人员介绍。

“物流行业中人力成本超过50%，巨额成本吞噬着企业利润和服务质量。在全国400多万名物流从业人员中，末端配送人员就有200多万。‘最后一公里’的配送成本是前一千公里的5倍。这组数据说明了‘最后一公里’的配送是一个巨大的问题。”刘智勇介绍，有了智能配送机器人，可以大幅度降低成本，和人工配送相比，机器人配送可以把每单的成本从1.5元左右降低到1元以下。

目前，公司已和多家物业园区达成合作。根据不同园区业主的需求，开发了两款快递机器人：一款能直接从收发室取货并送至业主楼下；一款则拥有乘坐电梯送货的功能，可以将货物送到业主家门口。此前，“真机小黄马”已在广东的两个小区投入使用，今年，产量预计可达千台左右，6月份有望走进北京一些小区。

真机智能团队目前正在研发“四足智能配送机器人”，预计今年6月产出第一批样机，届时，可以实现自主上台阶功能。未来，快递机器人还会走出园区，通过连接无人配送局部网络，像快递员一样在大街上穿梭送快递。

（据人民网）

WiFi密码分享有风险 破解或违法

最近几天，两款分别名为WiFi万能钥匙和WiFi钥匙的免费软件热度很高。可惜的是，它们出的是“恶名”。据报道，这两款软件被举报“窃取各类WiFi密码”。

举报称，软件会将所有的WiFi信息放进它编织的后台程序里，只要消费者下载并使用，软件就会借用消费者的手机，窥探这部手机周边和经过地点所有的WiFi信息，悄悄偷取各类WiFi的密码。

甚至，两款软件连国家重要机关、金融机构的WiFi网络密码也不放过，带来很大安全风险。

关于这两款应用如何“偷取用户密码”，某安全机构技术人员表示其实它们获取的密码通常是先由用户“分享”出去的，这和WiFi万能钥匙的回应基本相符。用户使用此类软件连接免费WiFi时，所在位置、连接成功的WiFi热点的名称、密码等信息会被WiFi万能钥匙收集，进入密码库，其他用户查询该区域的WiFi时，可以直接调用存在密码库中的WiFi密码。这种“共享模式”从诞生之初就伴随安全争议。但由于用户量庞大，大家共享、大家使用的局面逐渐形成。

而这中间却蕴含着安全风险：连在同一个局域网（这里就等于连在同一个WiFi）里很容易被攻击，因为很多数据的传输是不加密的，于是被截取信息、被篡改信息的情况很容易发生。

落实到具体情境中，只要国家机关或银行中有任何人共享过WiFi密码，且这个密码后来没有被修改过，它就一直在密码库中，其他人都可以调用。

对此，记者采访到的安全行业从业人员都对其运营模式表达了不满。他们表示：“很多人近年来一直在努力科普公共WiFi要慎连这个问题，主要就是公共WiFi的安全风险很高，但此类软件却力推把所有WiFi变成半公共WiFi。”

“如果此类软件分享的WiFi热点并未获得所有者允许，这种行为就是对他人上网流量的‘盗窃’行为。”中国政法大学知识产权研究中心特约研究员李俊慧表示。WiFi共享本身并无问题，关键是WiFi所有者是否同意。WiFi热点设置人使用的流量已付费，如果其共享行为是自愿、自发的，就没有太大法律问题。

为此，记者联系了WiFi万能钥匙的相关负责人，对方强调自家产品的原理是“分享而非破解”，主要以给予回报的形式鼓励商家共享密码。

不过相关应用的密码库非常可观，从初始密码的WiFi到自主设置了复杂密码的WiFi，从个人用户到商家再到国家机构，都能轻松调用。从监管层面来看，此类APP上架时，审核其可连接的WiFi热点是否已经过用户允许难度较大。因此多数情况下，违规行为只能依靠用户举报，予以事后监管。

WiFi密码是用于连接WiFi时的授权验证，目的是实现对连入热点设备数量和人员的管理。“如果所有者密码设置方式不当，比如将自己的手机号设为密码，或将其他与资金安全相关的数字设为了密码，就存在一定的风险。”李俊慧强调，这种风险已经超出WiFi万能钥匙等应用的控制。

对于WiFi钥匙等应用，李俊慧表示，用户最好“敬而远之”，“分享自己的WiFi密码会给自己带来网络安全风险，而分享其他人或机构的密码的行为也不当，对自己没有所有权或管理权的商品或服务进行分享，是对他人管控权的侵犯”。

（据新华网）