计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200253
57(9): 1800-1809, 2020

智能家居中的边缘计算

黄倩怡[1,2] 李志洋[3] 谢文涛[3] 张 黔[3]
[1](南方科技大学未来网络研究院 广东深圳 518055)
[2](鹏城实验室 广东深圳 518055)
[3](香港科技大学计算机科学及工程系 香港特别行政区 999077)
(qianzh@cse.ust.hk)

Edge Computing in Smart Homes

Huang Qianyi[1,2], Li Zhiyang[3], Xie Wentao[3], and Zhang Qian[3]
[1](*Institute of Future Networks, Southern University of Science and Technology, Shenzhen, Guangdong* 518055)
[2](*Peng Cheng Laboratory, Shenzhen, Guangdong* 518055)
[3](*Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong* 999077)

Abstract In recent years, smart speakers and robotic vacuum cleaners have played important roles in many people's daily life. With the development in technology, more and more intelligent devices will become parts of home infrastructure, making life more convenient and comfortable for residents. When different types of specialized intelligent devices are connected and operated over the Internet, how to minimize network latency and guarantee data privacy are open issues. In order to solve these problems, edge computing in smart homes becomes the future trend. In this article, we present our research work along this direction, covering the topics on edge sensing, communication and computation. As for sensing, we focus on the pervasive sensing capability of the edge node and present our work on contactless breath monitoring; as for communication, we work on the joint design of sensing and communication, so that sensing and communication systems can work harmoniously on limited spectrum resources; as for computation, we devote our efforts to personalized machine learning at the edge, building personalized model for each individual while guaranteeing their data privacy.

Key words edge computing; smart home; Internet-of-Things; ubiquitous sensing; federated learning

摘 要 近年来,智能音箱、扫地机器人已经成为很多用户生活中不可或缺的一部分.随着物联网技术的发展,越来越多的智能设备走进家庭场景,让用户的生活变得更加便捷和舒适.当种类繁多、功能细分的智能设备通过网络进行连接和控制时,为了解决网络延时、数据安全等诸多问题,基于边缘计算的智能家居成为未来趋势.探讨智能家居场景中的边缘计算,介绍围绕感知、通信和计算3个方向所展开的研究.

收稿日期:2020-04-01;**修回日期**:2020-06-04
基金项目:香港优配研究金资助项目(CERG 16204418,16203719,FP909,R8015);国家自然科学基金项目(61872420);广东省自然科学基金项目(2017A030312008);广东省重点领域研发计划资助项目(2019B121204009);鹏城实验室大湾区未来网络试验与应用环境项目(LZC0019)
This work was supported by RGC General Research Fund (CERG 16204418, 16203719, FP909, R8015), the National Natural Science Foundation of China (61872420), the Natural Science Foundation of Guangdong Province (2017A030312008), the Key-Area Research and Development Program of Guangdong Province (2019B121204009), and the Project of "FANet: PCL Future Greater-Bay Area Network Facilities for Large-scale Experiments and Applications" (LZC0019).

在感知方面,关注边缘节点的泛在感知能力,介绍在非接触式呼吸监测上取得的进展;在通信方面,研究无线感知和无线通信的融合设计,在有限的频谱资源上兼顾感知和通信;在计算方面,关注基于边缘节点的个性化机器学习,在不泄露用户数据的前提下建立个性化机器学习模型.

关键词 边缘计算;智能家居;物联网;泛在感知;联邦学习

中图法分类号 TP393

在中国,智慧家居市场规模正以每年20%~30%的速度增长.据前瞻产业研究院预计,中国智能家居市场规模2021年将达到4 369亿元[1].2个方面的需求促成了市场的高速增长,一方面,随着社会人口老龄化,老年人口的比例逐年增加,空巢老人依赖智能家居系统给予生活辅助和健康管理;另一方面,新生代消费群体追求高效、舒适的生活,智能化已成为年轻消费者对家居环境的基本要求.面对快速增长的市场需求,国家也加大了对智能家居以及物联网技术的投入和支持.在利好政策和社会需求的大力推动下,越来越多的智能设备走入千家万户.从智能音箱到扫地机器人,从智能门锁到远程医疗,无一不体现技术在智能家居场景下的魅力和潜力.

智能家居技术主要涵盖感知、通信和计算3个层次,如图1所示.感知技术利用丰富的传感器感知周围环境和用户活动;通信技术实现智能设备的互通互联,完成数据传输和指令交互.此外,云计算、边缘计算分别利用不同节点的计算能力共同完成数据处理任务,实现智能服务.

本文关注智能家居中的健康管理.随着我国的城市化进程和社会老龄化趋势加剧,持续增加的老年人口面临照护资源的极大短缺,需要借助科技的力量来解决人口老龄化问题.随着技术的发展,利用丰富的感知技术来实现健康监测已日益完善,结合大数据的处理能力,基于观测到的数据实现智能诊断也日趋成熟.不同于现有工作,我们着重讨论如何充分发挥边缘节点在健康管理中的作用,克服现有技术面临的瓶颈与局限.

在《Edge Computing: A Primer》[2]一书中,作者将"边缘计算"定义为数据源头和云数据中心之间的计算和网络资源(we define "Edge" as any computing and network resources along the path between data sources and cloud data centers).智能手机可以视为连接可穿戴设备与云服务器的边缘节点,智能网关是智慧家居中的边缘节点.除了计算和连接的能力,智能手机和智能网关本身作为一个强大的节点,具备丰富的感知能力.例如,手机上丰富的传感器可以感知用户的活动和情境[3-4],无线路由器可以感知家中

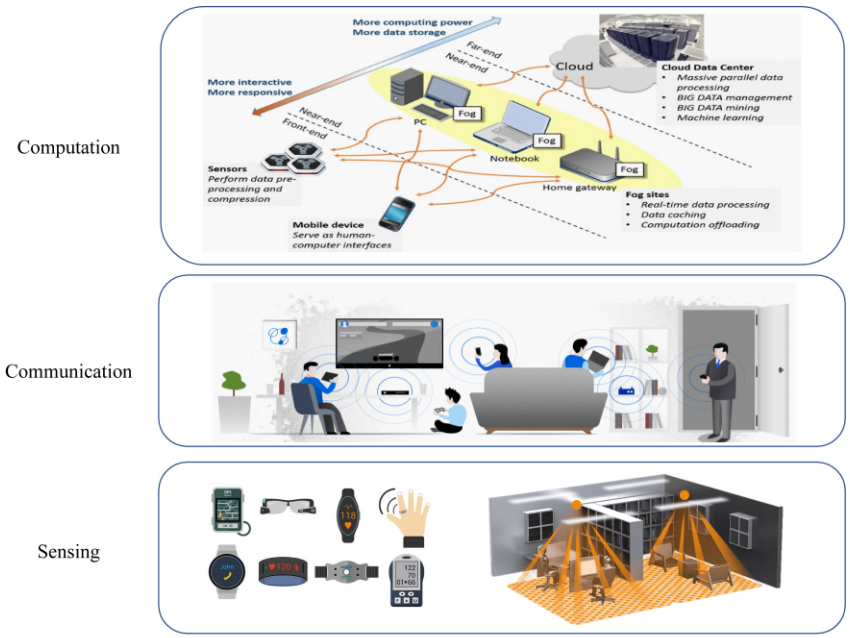


Fig. 1 Smart home technologies involve sensing, communication and computation

图1 智能家居技术主要涵盖感知、通信和计算3个层次

用户的实时位置[5-7].因此,边缘节点兼具感知、通信和计算的能力于一体.本文围绕智能家居中用户健康管理的场景,介绍我们在边缘节点的感知、通信和计算上开展的研究工作.

在感知方面,边缘节点和终端节点最大的不同在于其泛在感知能力.泛在感知根据无线信号的传播、反射和散射特性,分析信号的传播路径,从而对用户行为或周边环境进行监测.作为边缘节点的手机和无线路由器都能发送和接收信号,具备泛在感知能力.相比于接触式感知,泛在感知无需用户佩戴特定设备,因而更舒适,易为用户接受.在本文中我们以非接触式呼吸监测为例,介绍我们所做的研究和取得的进展.

引入泛在感知后,无线信号既需要承载数据信号又要完成感知任务,而通信和感知之间存在着矛盾关系.感知是通过发送已知信号来探测周围的环境变化,通信则是由发送端向接收端发送变化的、未知的信号.为了实现高效的频率利用效率,需要将感知和通信进行融合设计.在通信方面,我们研究如何在环境感知的同时向周围的设备传递信息,兼顾无线通信与无线感知.

在健康管理中,将用户的健康数据上传到云端面临隐私泄露和数据安全问题.相比之下,由边缘节点来进行数据处理可以更好地保护用户隐私,用户对数据管理具有更高的主动权.在计算方面,我们探索如何将联邦学习应用于智能家居中的感知数据,由可信任的边缘节点联合云服务器、其他边缘节点,在不泄露用户数据的前提下建立个性化机器学习模型,并通过优化降低联邦学习中数据交互和计算的开销.

1 从可穿戴设备到泛在感知:呼吸监测

2013 年前后,主导个人健康管理的可穿戴设备市场进入了快速发展的阶段,智能手环、智能手表、智能眼镜等可穿戴设备层出不穷.然而,随着时间的推移,续航能力差、长时间佩戴不舒适等因素造成用户对可穿戴设备的黏度不如预期.研究人员为了克服可穿戴设备存在的种种问题,提出了泛在感知的方式,利用周围环境中存在的无线信号来监测用户行为,从而摆脱对可穿戴设备的依赖.当无线信号在空中传播时,信号的物理特征(如幅值、相位、多普勒频移)与信号的传播途径息息相关.因此,人的位置、动作都会对信号的传播产生影响,甚至细微的手势动作、呼吸时胸腔的起伏都会在信号的物理特征中反映.因此,泛在感知利用空气中存在的无线信号,对用户进行非接触式感知.相比于可穿戴设备,泛在感知不要求用户佩戴设备,克服了续航时间短、舒适性差等问题.现有的研究工作利用 WiFi 信号、毫米波、超声信号实现了不同方面的健康监测,如睡眠监测[8-9]、跌倒检测[10-11]、步态分析[12]等.本文重点介绍我们在呼吸监测方面所取得的进展.

传统的呼吸监测方案大多依赖专有的设备,如口鼻气流传感器和胸腹部呼吸带,通过监测口鼻气流变化或腹部的压力变化得到呼吸率.这类方式虽然能获得准确的测量结果,但是舒适性差,不适合长时间监测或在日常工作、生活中使用.为了提供更舒适的监测方式,研究人员利用电磁信号(如 WiFi[13]、毫米波雷达[14])和声音信号监测呼吸率[15].这一类方法的工作原理是:在呼吸的过程中,胸腔会有周期性的起伏变化,通过分析胸腔表面反射的无线信号,实现非接触感知,摆脱了穿戴设备的束缚.

虽然有不少非接触式呼吸监测的研究工作,然而存在一些共性的不足.下面,我们将分别从声音信号和电磁信号 2 个方面分别阐述现有工作的不足以及我们所做的研究工作.

1.1 利用声音信号监测呼吸

在利用呼吸信号进行感知时,为了避免发出噪声,现有的工作通常利用 18～22 kHz 的超声频段.虽然成年人只能听到 18 kHz 以下的声音,但是婴儿和儿童可以听到 18 kHz 以上的声音[16].这些声音信号对婴儿和儿童而言就是难以忍受的噪音.然而,大部分智能手机中的麦克风和扬声器仅能支持 22 kHz 频率以下声音的发送和接收.为了解决这个问题,我们考虑利用音乐和广播节目的声音信号来实现呼吸监测.当智能音箱或手机在播放音乐或广播节目的同时监测用户的呼吸,对婴儿和儿童而言,这些声音不再是噪声.

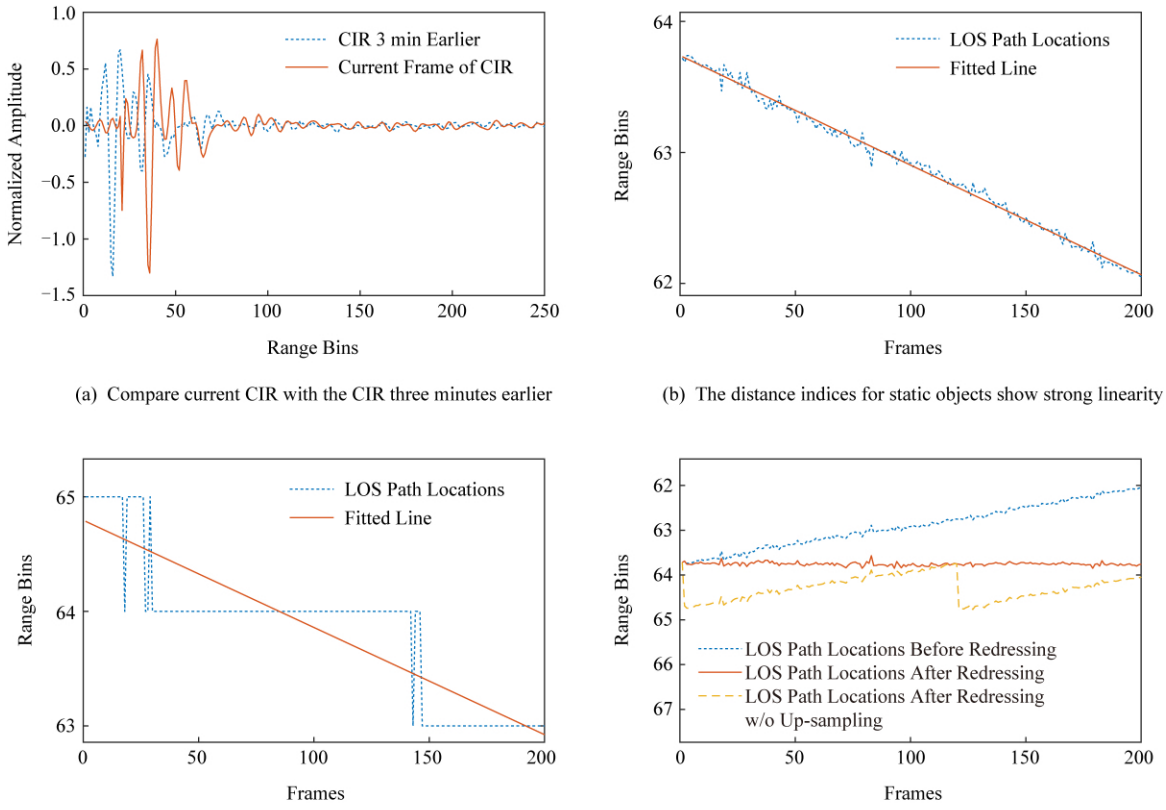
利用音乐或广播进行呼吸监测面临 2 个挑战.第 1 个挑战是,音乐和广播节目所发出的声音信号是持续且随机的,不具备帧结构以及特定的前导码,无法用现有的信道估计方法进行信道估计.第 2 个挑战是,现在手机通常采用 MEMS 封装的麦克风和扬声器,两者之间采用独立的采样时钟,2 个时钟之间存在频率差异.随着时间的推移,频率差异会不断累积导致发送和接收端存在较大的时间差,从而导致得到的信道估计失真.

为了解决第 1 个挑战,我们先将音频信号按固定时长 T_{frame} 进行切割,每一段为一帧,根据每一帧

发送出的信号和收到的信号计算信道冲击响应(channel impulse response, CIR),如图 2(a)所示.因为音乐或广播信号为连续的音频信号,由于传播延迟,收到的信号中不仅包含当前帧的内容,还包含上一帧末尾的片段,在计算 CIR 时,帧与帧之间会相互干扰.我们通过选择合适的帧长度来减小帧与帧之间的干扰.假设监测的最大距离为 4 m,已知声速为 340 m/s,最大的时延 $\tau_{\max}=2\times4/340\approx0.02$ s.在选择帧长 T_{frame} 时,如果 $T_{\text{frame}}\gg\tau_{\max}$,则上一帧末尾片段的比重趋于 0,帧与帧之间的干扰可以忽略不计;然而,如果 T_{frame} 过大,信道估计的周期太长,不能很好地反映信道变化.经过综合考量和实验结果,我们将设 $T_{\text{frame}}=0.4$ s.

为了解决第 2 个挑战,我们通过静止的传播路径估算麦克风和扬声器之间的时钟偏移,并以此校准 CIR.CIR 的横轴为时间,纵轴为幅值,而时间与距离可以由声音在空气中的传播速度相互换算,因此,CIR 表示的物理意义为来自不同距离的信号能量.时钟偏移带来的采样偏差随时间线性增加,反映在 CIR 上,即随着时间推移,CIR 会沿着时间轴平移,如图 2(a)所示.我们将同样的信道条件下 3 cm 前后测得的 CIR 进行对比,发现 3 cm 后 CIR 向后偏移了 20 多个距离区间,即 CIR 中的路径延时是真实的传播延时和时钟延时的综合反映.为了得到真实的路径延时,须消除时钟延时的影响.为此,针对每一个信号帧我们计算 CIR,找到峰值及对应的距离区间,记录每个峰值对应的距离区间;连续的 2 个帧之间,如果峰值对应的距离区间很接近,即认为是来自同一个物体的反射.例如,在第 N 帧中,找到峰值对应的索引为[7,25,43,…];在第 $N+1$ 帧中,峰值对应的索引为[8,26,44,…].我们认为,第 N 帧中索引 25 和第 $N+1$ 帧中索引 26 对应的峰值为同一个物体的反射,发生偏移的原因是收发两端的时钟差异.在静止的情况下,CIR 的变化仅由时钟偏差造成,索引会随时间线性变化.在所有记录的索引序列中,找到线性度最好的路径,视为静止路径,对其进行线性拟合,如图 2(b)所示.虚线代表原始的索引序列,实线为拟合的直线,直线的斜率反映了时钟偏移的速率,以此来修正每一帧的 CIR.

在短时间内时钟偏移带来的影响较小,通常需要一定时间的积累才能导致一个采样点的偏移,如图 2(c)所示.为了准确估计时钟偏移速率,我们将信号



(a) Compare current CIR with the CIR three minutes earlier

(b) The distance indices for static objects show strong linearity

(c) Unable to find the line that fits the distance bin without up sampling

(d) Up sampling can remove the clock drift

Fig. 2 Utilize static paths to calibrate the clock drift between the speaker and microphone

图 2 根据静止路径校准麦克风和扬声器之间的时钟偏移

进行 100 倍上采样,使得可以更精准地进行修正.例如,假设每 10 帧会产生一个采样点的偏移,在修正时,只能每 10 帧进行一次修正;然而,在进行 100 倍上采样后,每一帧都会产生 10 个采样点的偏移,可以逐帧修正时钟误差.在图 2(d)中,我们可以看到,在进行修正之前,在静止情况下估算的距离随时间线性变化(细虚线),如果不进行上采样,不能完全消除时钟偏移带来的影响(粗虚线).进行上采样处理后,可以基本消除时钟偏移的影响,测得的距离保持不变(实线).

在实验中,我们测试了不同的声音类型,包括摇滚、流行、民谣音乐和新闻,在 11 个志愿者身上的平均误差小于 0.5 BPM(beats per minute).误差随着手机与用户的距离增大而增大,当手机与用户的距离在 1 m 以内,平均误差约为 0.5 BPM.

1.2 利用电磁信号监测呼吸

现有的呼吸监测工作要求用户处于静止的状态.当用户处于运动的状态时,无法将身体其他部分的运动与胸腔的起伏分解开来,呼吸带来的信号变化湮没在更大幅度的信号变化中.我们通过测试发现,即使对于站立的用户,现有的方案也无法准确监测其呼吸率,因为用户站立时身体存在不自主的晃动,该晃动会掩盖呼吸造成的影响.

我们观察到,当在用户的身体前后各放置一个雷达时(如图 3 所示),人的呼吸导致的胸腔扩张和收缩只会影响到前方雷达的相位,而不会影响到后方雷达.当雷达在进行测距时,d_1 会发生变化而 d_2 不变;然而,当人朝着一个方向移动时,运动对 2 个雷达都会造成影响,并且该影响是相反的.因此,通过将 2 个雷达的相位相加,可以消除运动带来的变化而保留呼吸带来的变化.

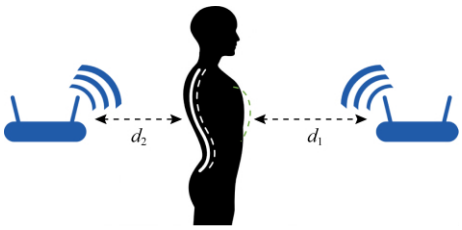


Fig. 3 Dual-radar system for breath monitoring

图 3 双雷达呼吸监测系统

假设用户运动的位移为 $x(t)$,胸腔由于呼吸造成的位移为 $d(t)$,前后 2 个雷达的相位变化分别为 $\Delta\phi_1(t)$和 $\Delta\phi_2(t)$,则 2 个雷达的相位变化可计算为:

$$\Delta\phi_1(t)=\frac{2\pi}{\lambda}\times 2[x(t)+d(t)],$$

$$\Delta\phi_2(t)=\frac{2\pi}{\lambda}\times 2[-x(t)].$$

将 $\Delta\phi_1(t)$和 $\Delta\phi_2(t)$相加,$x(t)$被消除而 $d(t)$被保留下来,即消除运动导致的位移而保留呼吸带来的胸腔起伏变化.我们通过双雷达的呼吸监测系统,可以成功地恢复出站立用户的呼吸率.在后续工作中,我们希望通过增加雷达数目来实现走路、跑步过程中的呼吸监测.

2 边缘感知与通信的融合设计

无线感知通过发出一段已知的信号序列,对比发出和收到的序列来计算信道状态信息,推测信号的传播路径,从而感知周围环境;而无线通信则利用无线信道来承载通信信号,对于接收端而言,发出的信号是变化的、未知的.无线感知和无线通信之间的差异使得两者通常被视为独立的系统来进行设计和优化.然而,在物联网时代,愈来愈多的物联网设备将通过无线频谱接入网络.有限的频谱资源既要感知周围环境,同时要满足通信需求.当感知与通信共同占用无线频谱时,需考虑如何高效、合理地利用有限的频谱资源.

虽然已有不少工作通过 WiFi 信号来感知周边环境,通过前导码序列来估算信道,由于通信和感知本质上的差异,这一类的工作存在矛盾的设计思路.从优化通信出发,希望降低前导码的比重以提升通信效率,而感知应用则希望有大量短而频繁的包来获得详尽的信道信息,从而提高感知细粒度.基于当前从前导码获取信道状态信息的设计思路,感知和通信之间存在难以调和的矛盾.为了解决这一矛盾,我们将感知和通信进行融合设计,设计可以携带信息的感知信号,不仅前导码部分可以用于感知,数据部分也可以用于感知,同时完成无线感知和无线通信.

感知和通信的融合设计难点在于,感知信号通常为宽带信号,而通信信号通常为窄带信号.一方面,感知的精度与信号带宽成反比,带宽 500 MHz 的信号可以区分相距 30 cm 的 2 个物体,带宽 1 GHz 的信号可以区分相距 15 cm 的 2 个物体,感知信号通常为大带宽信号以取得精准的感知结果;另一方面,受限于设备成本和功耗限制,常用的通信标准采用窄带信号,如 WiFi 信号的带宽为 20 MHz,蓝牙信号宽带为 1 MHz.为了解决这一矛盾,我们借助电路中存在的非线性现象来匹配两者带宽上的不同.电路的非线性特性表现为输出信号中包含输入

信号的非线性谐波,例如,当输入信号中包含频率 f_{in},非线性谐波中包含输入频率的高次谐波,如二次谐波 $2f_{in}$、三次谐波 $3f_{in}$ 等;当输入信号中包含频率 f_1 和 f_2,其二次谐波可以展开为

$$S_{in}^2=[\sin(2\pi f_1 t)+\sin(2\pi f_2 t)]^2=$$
$$\sin^2(2\pi f_1 t)+\sin^2(2\pi f_2 t)+$$
$$2\sin(2\pi f_1 t)\ \sin(2\pi f_2 t)=$$
$$\frac{1}{2}[2-\cos(2\pi 2f_1 t)-\cos(2\pi 2f_2 t)+$$
$$2\cos(2\pi f_1 t-2\pi f_2 t)-2\cos(2\pi f_1 t+2\pi f_2 t)].$$

可以看到,谐波中包含频率 $2f_1$,$2f_2$,f_1-f_2 和 f_1+f_2.这意味着,当 2 个信号输入非线性电路中会有一个谐波,其频率是 2 个输入信号的频率差.

感知雷达中常用的信号是线性调频连续波(frequency modulated continuous wave, FMCW),即雷达信号随时间线性增加(见图 4).当 2 个 FMCW 信号之间的频率差为固定值时(如图 5 所示),它们经过非线性电路时,谐波 f_1-f_2 为一个固定值,即为一个窄带信号.在现在的雷达中,为了获得更好的感知结果,通常会具备多根发送和接收天线,S_1 和 S_2 可以是不同天线发出来的信号.

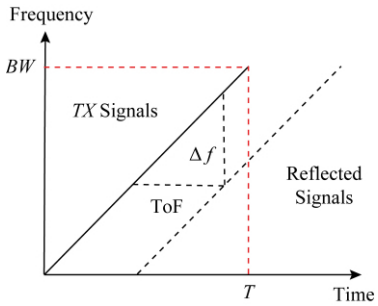


Fig. 4 Working Principle of FMCW radar

图 4 FMCW 测距原理

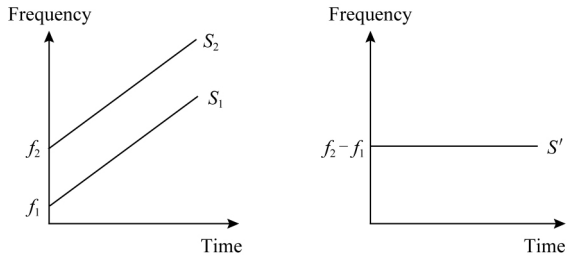


Fig. 5 Frequency modulated continuous wave (FMCW)

图 5 线性调频连续波

我们可以将数据 $s(t)$ 调制到一个信号上,如一个天线上的信号为 $TX_1=s(t)\ \sin f_1(t)t$,而另一个天线上的信号不做改变,即 $TX_2=\sin f_2(t)t$.定义 f_C 为 2 个信号的频率差,即 $f_2(t)-f_1(t)=f_C$.收到的信号可以写作:

$$RX=TX_1+TX_2+(TX_1+TX_2)^2+\cdots=\cdots+$$
$$s^2(t)[\sin f_1(t)t]^2+2s(t)\ \sin f_1(t)t\ \sin f_2(t)t+$$
$$[\sin f_2(t)t]^2+\cdots=\cdots-s(t)\cos[f_1(t)+$$
$$f_2(t)]t+s(t)\ \cos[f_1(t)-f_2(t)]t+\cdots. \quad (1)$$

根据式(1),数据被调制到了频点 $f_C=f_2(t)-f_1(t)$ 上.通过这样的设计,宽带的雷达信号中携带了窄带的数据信息,可以被通信设备解调.

更近一步地,我们让 2 个扫频信号错开半个周期,如图 6 所示.在 0 到 $T/2$ 之间,$f_C=f_1(t)-f_2(t)=BW/2$;在 $T/2$ 到 T 之间,$f_C=f_2(t)-f_1(t)=BW/2$.这种设计的优势在于,当我们在感知信号中携带通信数据时,不影响感知的精度.根据雷达理论,感知的精度和信号带宽成反比,即 $r=c/2B$,c 为光速,B 为信号带宽.因为感知信号的带宽不变,感知的精度不受影响.通过这样的设计,我们使得同样的频谱资源既可以用于感知,又能用于通信,提高了频谱利用效率,化解了现有无线感知和无线通信系统之间的矛盾关系.

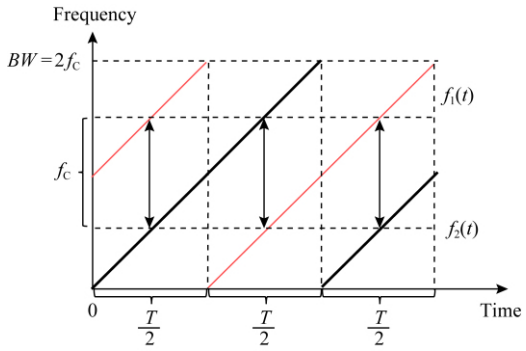


Fig. 6 Two signals are offset by the half chirp duration

图 6 2 个信号相差半个周期

以上我们讨论的是如何在感知的同时完成信号的发送,接下来我们讨论如何在感知的同时完成信号的接收,难点在于雷达需要同时接收感知信号和数据信号.如图 4 所示,雷达发送出一个线性调频连续波,信号经过传输和反射返回到雷达时产生了一定的延时,该延时即信号的传播时间.雷达接收端将收到信号与发出信号进行混频操作,得到两者之间的频率差 Δf.从图 4 可以看出,该频率差与传播时间成正比.又因为传播时间与传播距离的关系,可以从 Δf 计算物体和雷达之间的距离.假设 FMCW 信号

的带宽为 1 GHz,扫频用时 1 ms,最大可以探测的范围为 10 m.计算可得,Δf 的最大值为

$$\Delta f_{\max}=\frac{1\ \text{GHz}}{1\ \text{ms}}\times\frac{2\times 10\ \text{m}}{3\times 10^{8}\ \text{m/s}}\approx 66\ \text{kHz}.$$

由此可见,雷达接收到的感知信号经过混频操作后为一个低频信号,其最大频率取决于雷达的频率变化速率和最大可以探测的范围.

为了避免感知信号和数据信号相互干扰,我们可以在频率上将两者区分开来.根据上述分析,感知信号在基带上的频率在 0 到 $\Delta f_{\max}$ 之间.我们将数据信号下变频至频点 $\Delta f_{\max}+B$,保证在基带信号上,数据信号和感知信号至少有带宽 B 的间隔.通过这样的设计,雷达可以将感知信号和数据信号分解开来.

在实验中,我们将 LoRa 信号调制到了 FMCW 信号上.在接收端,雷达信号经过非线性电路,产生了可以被商用模块解调的 LoRa 信号,在室内的传输距离为 16 m.同时,雷达也能接收 LoRa 节点上传的数据信号.我们也通过实验测试了雷达的感知精度,与不进行数据通信时相比,雷达精度不受到影响.

3 边缘计算与机器学习

围绕着一个用户,多样的感知方式带来了丰富的数据.结合机器学习强大的能力,这些数据可以用于分析用户的行为偏好、健康状况甚至心理状态[17].现有的机器学习模型通常是为全局优化,通过收集大量人群的数据,建立一个普适的模型.然而,个体与个体之间的差异性却被忽视,普适的模型对个体而言往往不是最优的.为了解决这个问题,学者们提出了个性化机器学习(personized machine learning, PML)[18-19]的概念来对个体进行针对性优化.然而,研究面临着 2 个方面的挑战.一方面,从每个个体上采集到的数据往往数量有限且是无标签数据,无法要求每个用户花费时间精力为自己的数据添加标签.因此,仅仅依靠个体的数据无法得到一个准确的模型.因此,学者们提出了利用他人的标签数据来训练模型,针对每个个体,根据个体的数据来调整模型以最好地适配目标个体,即迁移学习中的无监督领域自适应[20-21].在无监督领域自适应中,他人的标签数据称为源域,目标个体的数据称为目标域.另一方面,个体的数据包含隐私信息,例如其健康状况、经济状况,用户不愿意将这些敏感信息交予他人.为此,学者们提出了联邦学习[22]范式,每个个体在自己的本地进行训练,在训练的过程中多方共享最新的模型参数以在本地进行下一轮的迭代优化.

有学者将 2 个角度结合起来,提出了联邦迁移学习.在这样的学习框架中,边缘计算凸显优势.相比于计算能力、功耗受限的终端,边缘节点具有更强的运算能力;相比于云服务器,将数据储存在边缘节点可以避免敏感信息泄露,用户对数据具有更强的管理权限.因此,将设备上传的健康数据储存在边缘节点,由边缘节点参与联邦学习,可以充分利用边缘节点的计算能力,并保护用户的数据隐私,如图 7 所示:

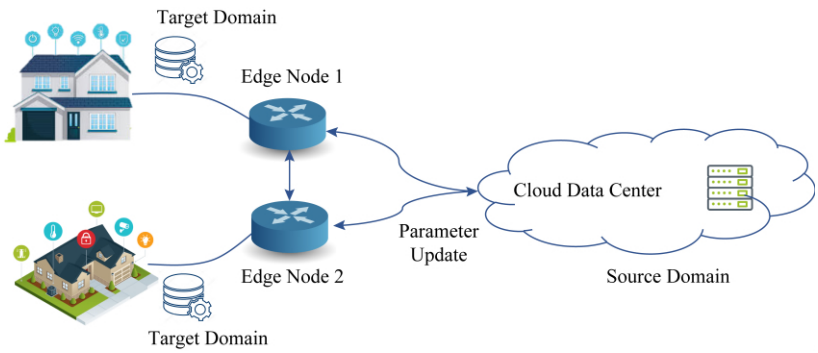


Fig. 7 Edge computing and federated transfer learning

图 7 边缘计算与联邦迁移学习

然而,现有的联邦迁移学习[23-24]不适用于我们的场景.首先,它要求个体的部分数据为标签数据,为半监督迁移学习,而并非无监督学习.在现实生活中,用户采集到的数据是不包含标签的,例如,用户无法为自己的睡眠数据添加睡眠分期标签.其次,它采用的对齐损失函数(alignment loss)不适用于我们的场景.对齐损失函数是领域自适应中用于衡量源域和目标域差异的指标,在训练过程中通过优化该指标来尽量缩小源域和目标域的差异.现有的联邦迁移学习框架的对齐损失函数是基于已知的源域-目标域

样本对[25],例如当源域是文本数据而目标域是图像数据时,某张图片和某些文本之间存在一定的语义联系,因此构成了文本-图像样本对.而在我们的场景中,不同用户的感知样本之间不一定存在这样的联系.

为此,我们针对感知的场景设计了一个联邦迁移学习的模型训练框架.无监督领域自适应的一个常用方法是将模型分为特征提取器和分类器2部分,特征提取器用于将数据映射到特征空间,分类器基于特征进行分类.为了使训练得到的分类器在目标域上达到较好的效果,需要缩小源域和目标域在特征空间的分布差异.在我们的框架中,为了衡量该分布差异,采用的对齐损失函数是最大均值差异(maximum mean discrepancy, MMD)[26-27],这也是无监督领域自适应中常用的一个对齐损失函数.无监督领域自适应的训练过程通常分为预训练和微调2部分.我们的框架采取相同的模型划分方法和训练过程.首先在源域中对特征提取器和分类器进行预训练;然后源域将特征提取器的权重发送给目标域,准备进行二者协作的微调阶段.在微调阶段,对于每一批数据的处理可以分为4步:前馈、分类损失函数及梯度计算、MMD损失函数及梯度计算、模型参数更新.其中第1,2,4步较为简单,源域及目标域独立操作即可,无需进行数据交换.第3步最为复杂,需要进行大量交互.

MMD损失函数的定义为

$$L_{\mathrm{MMD}}=\frac{1}{n_1(n_1-1)}\sum_{i=1}^{n_1}\sum_{i'\neq i}k(v_i,v_{i'})+\frac{1}{n_2(n_2-1)}\sum_{j=1}^{n_2}\sum_{j'\neq j}k(v'_j,v'_{j'})-\frac{2}{n_1n_2}\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}k(v_i,v'_j),$$

其中,函数$k(v,v')=\exp(-\alpha\|v-v'\|^2)$是核函数.该损失函数可以视为3部分的和.假设$v_i$和$v'_j$分别是源域和目标域的特征向量,那么损失函数中的第1部分源域可以独立计算,第2部分目标域可以独立计算.而第3部分需要用到2个域的数据.因此需要一方将数据加密发送给另一方.为了能够在密文上进行运算,我们的框架采用了Paillier同态加密算法[28].此外,Paillier加密算法并不支持指数函数运算,因此我们对核函数中的指数函数进行泰勒展开,将其近似转换为多项式函数.近似转换后的单个核函数可以表示为

$$k(v,v')=\sum_m c_m f_m(v)g_m(v'),$$

其中,c_m是常数,$f_m(v)$为常数1或者向量元素组成的多项式,$g_m(v')$与$f_m(v)$含义相同.因此,为了计算第3部分,需要一方把每一个特征向量的所有$f_m(v)$都发给另一方.

对于2个域的MMD梯度的计算,我们以目标域为例,对于该域而言MMD损失函数第1部分的梯度为0,第2部分的梯度可以独立计算.对于第3部分的梯度,实际上是各个核函数的梯度之和,单个核函数的梯度可以表示为

$$\frac{\partial k(v,v')}{\partial\theta}=\sum_m c_m f_m(v)\frac{\partial g_m(v')}{\partial\theta}.$$

因此,与计算第3部分损失函数类似,计算第3部分的梯度同样需要对方(此处指源域)将每一个特征向量的所有$f_m(v)$都发给另一方.这个方案具有较高的计算和通信开销.为了解决这个问题,我们进一步做了2方面的改进.

1) 基于MMD损失函数第3部分求和的特点,不对每个核函数单独考虑,而是将第3部分作为一个整体.对于第3部分的求和部分的值以及梯度可以做如下变换:

$$\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}k(v_i,v'_j)=\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}\sum_m c_m f_m(v_i)g_m(v'_j)=\sum_m c_m\times\Big(\sum_{i=1}^{n_1}f_m(v_i)\Big)\times\Big(\sum_{j=1}^{n_2}g_m(v'_j)\Big),$$

$$\frac{1}{\partial\theta}\partial\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}k(v_i,v'_j)=\sum_m c_m\times\Big(\sum_{i=1}^{n_1}f_m(v_i)\Big)\times\Big(\sum_{j=1}^{n_2}\frac{\partial g_m(v'_j)}{\partial\theta}\Big).$$

由此可见,一方只需要发送$\sum_{i=1}^{n_1}f_m(v_i)$,即所有特征向量的$f_m(v)$的和,而不是把每个特征向量的$f_m(v)$都发送一遍.当训练的批量大小为N时,该优化方法将发送$f_m(v)$的通信开销降低为原来的$1/N$.

2) 基于链式法则对梯度计算进行改进.我们不再直接计算梯度,而是先计算MMD损失函数对于特征向量的偏导,再计算特征向量对于参数的偏导:

$$\frac{\partial Part3}{\partial\theta}=\sum_{j=1}^{n_2}\sum_{l=1}^{L}\frac{\partial Part3}{\partial v'_{jl}}\times\frac{\partial v'_{jl}}{\partial\theta}.$$

这里的链式法则不用考虑对方的特征向量.由于特征向量对于参数的偏导双方可以独立计算,所以双方只需要交换数据来计算MMD损失函数对于特征向量的偏导,并发送该偏导给对方解密.假设模型

的参数数量为 M,训练的批量大小为 N,特征向量长度为 L,则优化后和优化前发送偏导及梯度的通信开销的比值是 $N\times L/M$.模型的参数数量 M 通常非常大,而 N 和 L 则小的多.在我们的一次实验中,M 约为 40 000,而 N 和 L 分别为 64 和 32.因此该方法可以降低大量通信开销.

此外,这 2 项优化还大大减少了加密、解密以及密文上运算的次数,因此也减少了大量的计算开销.在对于一个无线手势感知数据集的实验中,微调阶段的每一个批次优化前耗时至少 45 min,而优化后耗时仅 2 min.最终,微调阶段结束之后,源域将训练好的分类器权重发送给目标域.目标域将自己的特征提取器和接收到的分类器组合起来即得到最终的模型.

4 结 语

边缘计算填补了云计算在响应延时、数据安全等方面的不足,成为智能家居场景下的未来趋势.本文从感知、通信和计算 3 个方面探索智能家居场景下的边缘计算.在感知方面,以呼吸监测为例,探索边缘节点的泛在感知能力.我们研究如何利用环境中已有的声音(音乐、广播节目)进行呼吸监测,以及用双设备消除用户运动对呼吸监测的干扰.在通信方面,我们对感知和通信信号进行联合设计,使得无线信号在进行感知的同时也能向外传递信息,在有限的频谱资源上兼顾感知和通信;在计算方面,我们研究在保护用户隐私的前提下建立用户的个性化模型,并通过优化计算过程降低联邦学习中的计算和通信开销.在未来的研究工作中,我们希望继续探索边缘节点在智能家居中的潜力,加速智能家居场景落地,让技术改变人类未来的生活方式.

参 考 文 献

[1] Prospective Industrial Research Institute. Chinese Smart Home Market Outlook and Investment Strategy Planning Report for 2020—2025 [R]. 2019 (in Chinese)
(前瞻产业研究院. 2020—2025 年中国智能家居设备行业市场前瞻与投资策略规划报告[R]. 2019)

[2] Cao Jie, Zhang Quan, Shi Weisong. Edge Computing: A Primer [M]. Berlin: Springer International Publishing, 2018

[3] Lu Hong, Pan Wei, Lane N D, et al. SoundSense: Scalable sound sensing for people-centric applications on mobile phones [C] //Proc of the 7th Int Conf on Mobile Systems, Applications, and Services. New York: ACM, 2009: 165-178

[4] Lu Hong, Yang Jun, Liu Zhigang, et al. The Jigsaw continuous sensing engine for mobile phone applications [C] //Proc of the 8th ACM Conf on Embedded Networked Sensor Systems. New York: ACM, 2010: 71-84

[5] Wang Yan, Liu Jian, Chen Yingying, et al. E-eyes: Device-free location-oriented activity identification using fine-grained wifi signatures [C] //Proc of the 20th Annual Int Conf on Mobile Computing and Networking. New York: ACM, 2014: 617-628

[6] Wu Dan, Zhang Daqing, Xu Chenren, et al. WiDir: Walking direction estimation using wireless signals [C] //Proc of the 2016 ACM Int Joint Conf on Pervasive and Ubiquitous Computing. New York: ACM, 2016: 351-362

[7] Qian Kun, Wu Chenshu, Yang Zheng, et al. Widar: Decimeter-level passive tracking via velocity monitoring with commodity WiFi [C] //Proc of the 18th ACM Int Symp on Mobile Ad Hoc Networking and Computing. New York: ACM, 2017: 1-10

[8] Zhao Mingmin, Yue Shichao, Katabi D, et al. Learning sleep stages from radio signals: A conditional adversarial architecture [C] //Proc of the 34th Int Conf on Machine Learning-Volume 70. Sydney, Australia: PMLR: 4100-4109

[9] Hsu Chen-Yu, Ahuja A, Yue Shichao, et al. Zero-effort in-home sleep and insomnia monitoring using radio signals [J]. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017, 1(3): 1-18

[10] Wang Hao, Zhang Daqing, Wang Yasha, et al. RT-Fall: A real-time and contactless fall detection system with commodity WiFi devices [J]. IEEE Transactions on Mobile Computing, 2016, 16(2): 511-526

[11] Palipana S, Rojas D, Agrawal P, et al. FallDeFi: Ubiquitous fall detection using commodity WiFi devices [J]. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2018, 1(4): 1-25

[12] Hsu Chenyu, Liu Yuchen, Kabelac Z, et al. Extracting gait velocity and stride length from surrounding radio signals [C] //Proc of the 2017 CHI Conf on Human Factors in Computing Systems. New York: ACM, 2017: 2116-2126

[13] Liu Jian, Wang Yan, Chen Yingying, et al. Tracking vital signs during sleep leveraging off-the-shelf wifi [C] //Proc of the 16th ACM Int Symp on Mobile Ad Hoc Networking and Computing. New York: ACM, 2015: 267-276

[14] Yang Zhicheng, Pathak P H, Zeng Yunze, et al. Monitoring vital signs using millimeter wave [C] //Proc of the 17th ACM Int Symp on Mobile Ad Hoc Networking and Computing. New York: ACM, 2016: 211-220

[15] Nandakumar R, Gollakota S, Watson N. Contactless sleep apnea detection on smartphones [C] //Proc of the 13th Annual Int Conf on Mobile Systems, Applications, and Services. New York: ACM, 2015: 45-57

[16] Ueda M, Takahashi H. How high-frequency do children hear? [C] //INTER-NOISE and NOISE-CON Congress and Conference Proceedings. Hamburg, Germany: Institute of Noise Control Engineering, 2016: 2429-2434

[17] Zhao Mingmin, Adib F, Katabi D. Emotion recognition using wireless signals [C] //Proc of the 22nd Annual Int Conf on Mobile Computing and Networking. New York: ACM, 2016: 95-108

[18] Won Park H, Busche J, Schuller B, et al. Personalized estimation of engagement from videos using active learning with deep reinforcement learning [C] //Proc of the IEEE Conf on Computer Vision and Pattern Recognition Workshops. Piscataway, NJ: IEEE, 2019: 1-10

[19] Rudovic O, Utsumi Y, Guerrero R, et al. Meta-weighted Gaussian process experts for personalized forecasting of AD cognitive changes [J]. arXiv preprint, arXiv: 1904.09370, 2019

[20] Pan Jialin, Yang Qiang. A survey on transfer learning [J]. IEEE Transactions on Knowledge and Data Engineering, 2009, 22(10): 1345-1359

[21] Wang Mei, Deng Weihong. Deep visual domain adaptation: A survey [J]. Neurocomputing, 2018, 312: 135-153

[22] Yang Qiang, Liu Yang, Chen Tianjian, et al. Federated machine learning: Concept and applications [J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19

[23] Liu Yang, Chen Tianjian, Yang Qiang. Secure federated transfer learning [J]. arXiv preprint, arXiv: 1812.03337, 2018

[24] Sharma S, Chaoping Xing, Liu Yang, et al. Secure and efficient federated transfer learning [J]. arXiv preprint arXiv: 1910.13271, 2019

[25] Shu Xiangbo, Qi GuoJun, Tang Jinhui, et al. Weakly-shared deep transfer networks for heterogeneous-domain knowledge propagation [C] //Proc of the 23rd ACM Int Conf on Multimedia. New York: ACM, 2015: 35-44

[26] Tzeng E, Hoffman J, Zhang Ning, et al. Deep domain confusion: Maximizing for domain invariance [R]. arXiv preprint, arXiv:1412.3474, 2014

[27] Rozantsev A, Salzmann M, Fua P. Beyond sharing weights for deep domain adaptation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 41(4): 801-814

[28] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999: 223-238

Huang Qianyi, born in 1992. Research assistant professor from Southern University of Science and Technology, Shenzhen, China. Received her bachelor degree in computer science from Shanghai Jiao Tong University and her PhD degree in the Department of Computer Science and Engineering from Hong Kong University of Science and Technology. Her main research interests include mobile computing, Internet of things and security.

Li Zhiyang, born in 1995. Received his BEn degree in information security from Wuhan University in 2017, and is currently an MPhil student in the Department of Computer Science and Engineering, Hong Kong University of Science and Technology. His main research interests include wireless sensing and transfer learning.

Xie Wentao, born in 1996. Received his bachelor degree in computer science and technology from Southern University of Science and Technology. PhD candidate with both the Hong Kong University of Science and Technology and Southern University of Science and Technology, Shenzhen, China. His main research interests include smart wearables, mobile computing and sensing, and smart healthcare.

Zhang Qian, born in 1972. Full professor in the Department of Computer Science and Engineering, Hong Kong University of Science and Technology. Received her BSc, MSc, and PhD degrees from Wuhan University, China, in 1994, 1996, and 1999, respectively, all in computer science. Fellow of IEEE. Her main research interests include Internet of things, smart healthcare, mobile computing and sensing, blockchain infrastructure construction, etc.