doi:10.11959/j.issn.1000-436x.2015304

基于智能手表运动传感器的新型攻击及其防范

宋晨光，刘建伟，伍前红，关振宇
（北京航空航天大学 电子信息工程学院，北京 100191）

摘 要：智能手表上搭载了加速度计、陀螺仪等运动传感器，且会随着手部运动而产生位移，使通过智能手表窃取用户外部键盘输入成为了可能。研究了智能设备上基于 6 轴加速度计/陀螺仪来推断用户键盘输入的可行性，建立了用户进行键盘输入时的运动模型来对手部运动进行分类识别。当用户执行敏感输入，如在数字键盘上输入密码时，可根据传感器信息推断出密码。经实验验证，该方法可有效识别 4 位 PIN 码，证明此安全问题值得人们重视。

关键词：智能手表；运动传感器；加速度计；陀螺仪；信息泄露
中图分类号：TP309 **文献标识码**：A

New attack based on smartwatch motion sensors and the protection method research

SONG Chen-guang, LIU Jian-wei, WU Qian-hong, GUAN Zhen-yu
(School of Electronics and Information Engineering, Beihang University, Beijing 100191, China)

Abstract: Smart watch shipped with various embedded motion sensors, such as the accelerometer and gyroscope. Smart watch can follow the movement of hand to recognize the corresponding displacement, so that others can steal user's external keyboard input through smart watches. The feasibility of intelligent device based on 6 axis accelerometer/gyroscope to infer the user's keyboard input was researched, and the user's keyboard input kinematic model for motion classification recognition was established. When users perform sensitive inputting, such as passwords inputting on digital keyboard, the passwords according to sensor information can be deduced. The results show that the approach can effectively recognize the PIN code on keyboard, which absolutely prove the seriousness of this safety problem.
Key words: smart watch; motion sensor; accelerometer sensor; gyroscope sensor; information leakage

1 引言

随着 4G 移动通信和 WLAN 热点覆盖的普及，移动互联网已成为信息通信产业中发展最快、创新最活跃的领域。网络环境的改善带动了移动设备在日常生活中的深入，智能手机已经成为了人们不可缺少的一部分，但频繁的使用带来的是日益凸显的安全问题。近年来，智能手机带来的多种安全问题得到了人们的广泛关注[1,2]，其中关于智能手机的传感器安全也引起了学者们的研究兴趣[3]。

智能手机上搭载了多种运动传感器，如加速度计、陀螺仪、磁力计等，通过这些传感器可以检测到用户的使用状态，为多种应用场景提供了可能，比如利用 GPS(global positioning system)、加速度计和陀螺仪的协同工作检测用户的运动状态，从而计算出用户的跑动距离和运动强度，为医疗健康提供了有效的参考信息。但到目前为止，在 Android 和 IOS 操作系统中第三方应用程序访问嵌入式加速度

收稿日期：2015-08-30
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目(2012CB315905)；国家自然科学基金资助项目(61272501, 61370190, 61173154)；中央高校基本科研业务费专项基金资助项目(YWF-15-GJSYS-059)
Foundation Items: The National Basic Research Program of China (973 Program) (2012CB315905); The National Natural Science Foundation of China (61272501, 61370190, 61173154); The Fundamental Research Funds for the Central Universities (YWF-15-GJSYS-059)

计和陀螺仪等运动传感器均不需要安全许可[4]，这就为攻击者通过传感器发起攻击提供了可能。目前，智能手机上基于运动传感器的信息窃取攻击已经得到了大量验证，如通过智能手机来感知震动进而推断附近键盘上的用户输入[5]，通过智能手机上方向传感器的变化来推断用户输入[6]，还有基于加速度计和方向传感器协同工作进而检测触摸屏上按键输入[7]等。证明了攻击者可通过智能手机上看似安全的运动传感器来获取用户登录口令，PIN 码（personal identification number）等敏感信息，从而对人们的隐私信息和财产安全造成巨大的威胁。

在智能手机已经普及的今天，智能手表由于其可穿戴的属性引发了人们极大的兴趣，如 Apple Watch 可通过 Apple Pay 代替手机进行支付[8]，但是其安全问题还未得到足够的重视。与智能手机相似，智能手表也搭载有多种运动传感器，但与手机不同的是，当人们进行较为敏感的活动如敲击外界键盘输入密码时，智能手表会随着手腕的运动而产生位置的改变，从而记录手部的运动信息，为攻击者获取用户信息提供了可能，对外界敏感信息如普通键盘输入，ATM（automatic teller machine）密码输入等产生了新的安全威胁。

本文讨论了通过加速度计和陀螺仪 2 种运动传感器监测用户手部运动状态，从而推断外界输入的可行性，并进行了实验验证。首先，通过对加速度计和陀螺仪数据进行预处理，获得了较为准确的传感器数据；其次，针对佩戴智能手表在数字键盘上输入 PIN 码的场景提出了具体的分类模型，以处理后的加速计和陀螺仪数据作为训练样本，选用了 BP（back propagation）神经网络对手势特征进行了训练和识别，并描绘出按键轨迹从而推测出用户输入；最后，针对以智能手表为代表的可穿戴设备的信息安全问题，结合本文提出的新型安全威胁给出了防范的建议。

2 技术背景

2.1 键盘输入与智能手表

人们常常使用键盘来输入各种敏感信息，如打开计算机需要输入 PIN 码进行登录；访问网站需要输入用户名和口令；ATM 机上需要输入 6 位数字密码等。正是由于这些敏感信息的存在，攻击者经常通过计算机木马来记录用户的按键信息，从而获取用户的隐私和敏感信息。但是随着计算机安全软件的发展，普通个人计算机上对于获取用户按键信息的恶意软件的防范越来越完善，而在 ATM 机等封闭的计算机环境上安装恶意软件则相对困难。

随着智能手机的普及，各种木马软件层出不穷，因此移动操作系统上安全防范同样重要。在 Android 平台上，应用必须声明需要访问的敏感资源权限，如网络访问权限、文件读写权限、录音权限等，但系统并未将运动传感器作为敏感资源进行保护，因此第三方软件不需要安全许可即访问运动传感器[4]。而在佩戴智能手表的情况下，键盘输入必然会引起手表姿态的变化，从而被运动传感器记录下来，因此智能手表上的运动传感器可以提供给攻击者一种新的侧信道攻击方式。

2.2 数据采集及预处理

智能手表上坐标系如图 1 所示，加速度计传感器返回的数据即 3 个坐标轴方向上的加速度大小：左右方向（X 轴）、前后方向（Y 轴）、上下方向（Z 轴），单位是 $\mathrm{m/s^2}$。加速度计传感器通过测量施加在传感器上的作用力来计算设备的加速度 $A_d=-\sum\frac{F_s}{m}$。

图 1 智能手表坐标系

由于加速度传感器受到重力加速度的影响，其返回值是重力加速度和自身加速度的矢量和 $A_d=-g-\sum\frac{F_s}{m}$ [9]，使数据不能准确反映出设备的运动状态，影响识别的正确率。因此，要测出设备真实的加速度，必须去除加速度中的重力分量。

这里以 Z 轴为例，设原始加速度数据为 a_i，重力加速度为 g_i，滤波器常量为 α，其中 i 表示样本的编号，f 为采样频率，t 为滤波器的时间常数，有 $\alpha=\frac{t}{t+f}$，推出

$$g_i=\alpha g_{i-1}+(1-\alpha)a_i \tag{1}$$

滤波器常量 α 越接近 1，则 g_{i-1} 对 g_i 的影响越大，加速度 a_i 对 g_i 的影响越小，构成了一个低通滤波器分离出了重力分量，之后再用当前的加速度 a_i 减去 g_i，即能去除重力分量。图 2 显示了 Z 轴方向去除重力分量前后对比。

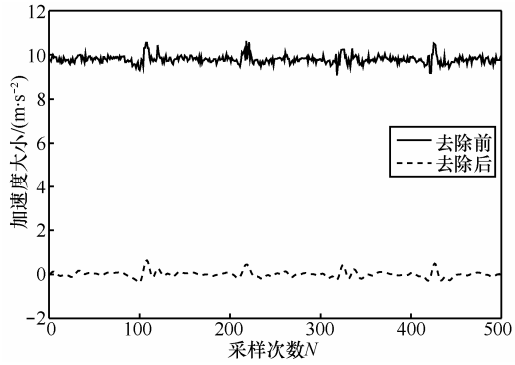


图 2　去除重力分量前后对比

由于传感器返回的数据往往存在高频的干扰噪声，在去除重力分量之后需要经过低通滤波来去除噪声，由图 3 可以看到高频分量明显降低。

陀螺仪传感器返回的数据是绕 3 个轴旋转的角速度，分别是绕 X 轴的滚转角 φ，绕 Y 轴的俯仰角 θ，绕 Z 轴的偏航角 ψ。通过对 3 个轴上的角速度进行积分便能得到角度矢量 $[\varphi,\theta,\psi]$。

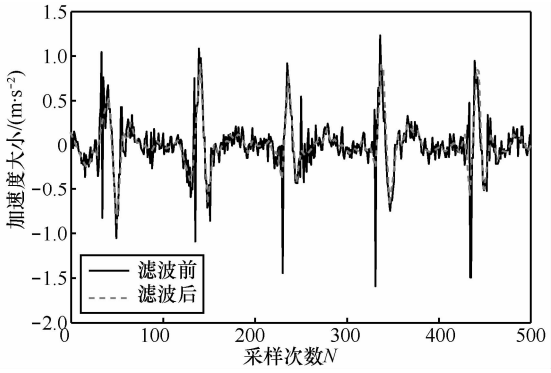


图 3　滤波前后对比

由于姿态四元数相对于欧拉角计算简单，而且避免了欧拉角的奇异性问题，可快速计算出设备姿态的连续变化，因此选用姿态四元数表示设备姿态并作为特征值进行识别。

定义设备的姿态四元数为

$$\boldsymbol{q}=\left[e_x\sin\frac{\boldsymbol{\Phi}}{2},e_y\sin\frac{\boldsymbol{\Phi}}{2},e_z\sin\frac{\boldsymbol{\Phi}}{2},\cos\frac{\boldsymbol{\Phi}}{2}\right]^{\mathrm{T}} \tag{2}$$

其中，e_x、e_y、e_z 为旋转轴在 X、Y、Z 方向的分量，$\boldsymbol{\Phi}$ 为设备绕旋转轴旋转的角度，一个四元数即表示一次旋转的方向和角度[10]，连续旋转只需将 2 个四元数相乘即可，定义 $\boldsymbol{q}$ 和 $\boldsymbol{p}$ 为连续 2 次旋转对应的四元数，则其乘积可表示为

$$\boldsymbol{q}\otimes\boldsymbol{p}=\begin{bmatrix}\boldsymbol{q}_4\boldsymbol{I}_{3\times3}-[\boldsymbol{\rho}\times] & \boldsymbol{\rho}^{\mathrm{T}}\\ -\boldsymbol{\rho}^{\mathrm{T}} & \boldsymbol{q}_4\end{bmatrix} \tag{3}$$

则 $\boldsymbol{q}\otimes\boldsymbol{p}$ 表示连续 2 次旋转后的设备状态。

2.3　设备姿态的校正

在计算设备的姿态时，由于加速度计存在温度漂移和机械噪声，而陀螺仪则会随着长时间的工作产生漂移误差，单独使用陀螺仪或者加速度计都不能准确计算出设备姿态，因此需要将陀螺仪和加速度的数据进行融合校准[11]。

由于姿态估计是一种非线性的系统，因此本文使用了一种非线性卡尔曼滤波器来计算设备的姿态[12]，图 4 分别为 Z 轴上陀螺仪的角加速度数据积分所得旋转角度和利用卡尔曼滤波校正过的旋转角度。可以看到，经过加速度计的校正，计算出的设备姿角明显更为稳定和准确。

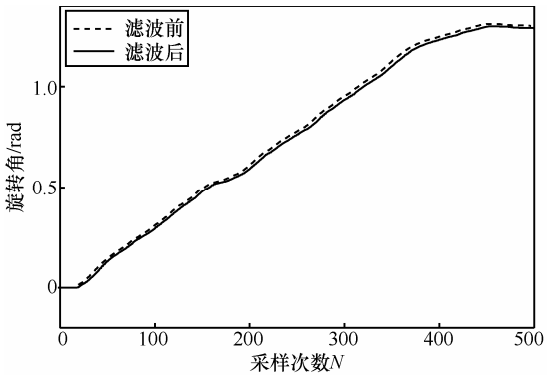


图 4　卡尔曼滤波前后对比

3　信息提取方案及系统模型

3.1　信息提取方案流程

为了获得攻击所需的运动传感器数据，攻击者可以将木马软件伪装成普通的应用程序如计步器等软件。用户安装伪装过的程序后，木马程序会在后台运行窃取用户设备上的运动传感器数据。由于数据处理和识别需要大量计算资源，因此通过网络将传感器数据发送到攻击者服务器，进而完成后续计算。

服务器获得数据后首先对数据进行预处理，得到加速度和姿态四元数矩阵。由于用户在输入时需

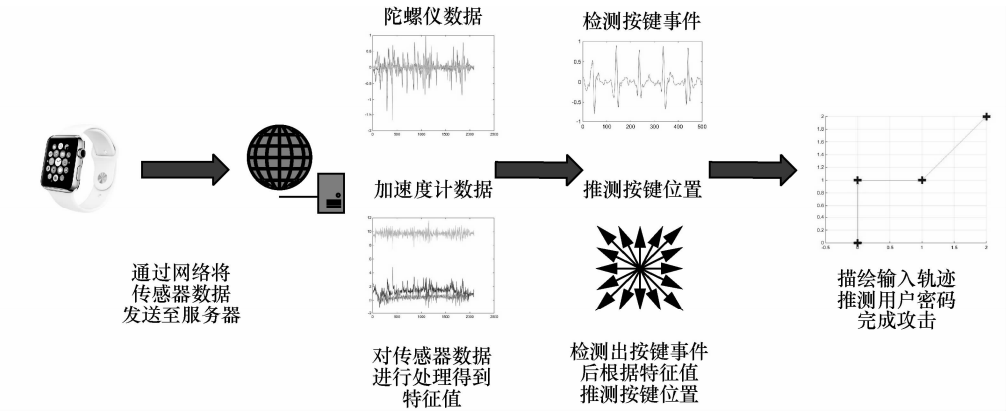


图 5 信息提取流程

要将物理按键完全按下，因此在 Z 轴方向上的加速度曲线上回形成尖峰特征，对此特征进行匹配，即可检测出每一次按键事件。

获取到按键事件发生的时间戳后可计算出 2 次按键之间三轴加速度积分所得位移大小和姿态四元数，将其作为特征值通过 BP 网络神经算法可对 2 次按键间的位移进行分类，从而检测出 2 次按键事件间的位移。

将位移矢量依次绘图可按键轨迹，进而与键盘进行匹配，最后推测出用户输入的密码。从图 5 最后结果可以看到输入依次是 1、4、5、9。

3.2 按键事件的特征提取与选择

当人们佩戴智能手表进行日常活动时，每一次移动都会带来各个方向上加速度的变化，如图 6 和图 7 所示，可看到跑步和打字的运动特征完全不同。而当人们使用数字键盘输入时，由于需要将物理按键完全按下，为了发力，手表所在部位往往会发生上下抖动，因此可以通过提取重力方向上的加速度变化来检测出每一次按键行为。

由于传感器提取出的数据往往包含大量的不相关信息，直接从这些信息中识别输入信息很难达到较高的识别率。因此，模式识别系统需要使用经过一定处理，更能反映动作特征的数据作为输入。

通过前文所述方法，首先从原始加速度数据中滤除重力分量，而后再对 Z 轴方向上的加速度进行分析。如图 8 所示，可以看到每一次的按键输入都会形成一次尖峰。对数据进行滤波处理后得到图 9 所示图像，可以看出每次按键都会形成波峰和波谷，其中包含曲率极大点，可作为特征点对加速度曲线进行匹配[13]，从而识别出按键事件，并提取每一次按键的时间戳。

首先对加速度曲线进行拟合使其成为二次可导，之后对拟合曲线离散采样提取曲率绝对值极大值点作为特征值，并通过循环移位的方法对加速度曲线进行匹配，定义阈值 ε，保留小于阈值的曲线段，然后计算出曲线段的曲率极大值点从而识别出每一次按键事件发生时的加速度曲线波峰和波谷，并分别记录波峰和波谷对应的时间 t_1 和 t_2，以 $\frac{t_1+t_2}{2}$ 作为按键事件的时间戳。

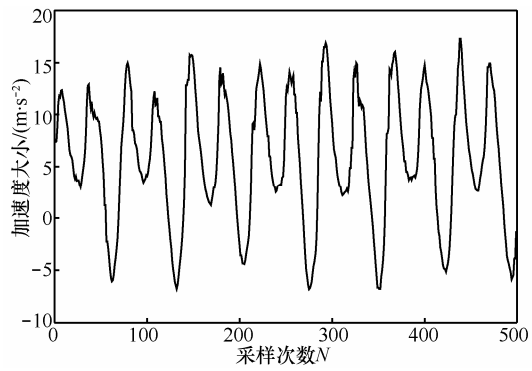


图 6 跑步时的加速度

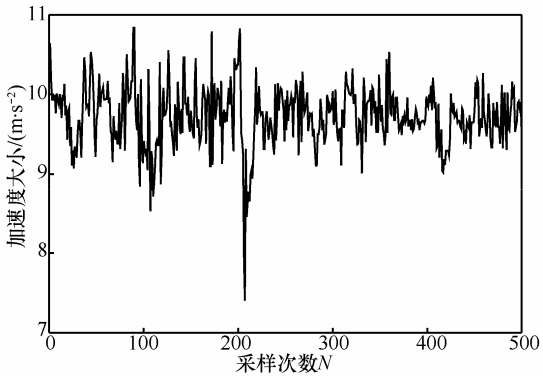


图 7 打字时的加速度

3.3　按键位置的训练模型与识别

手势识别是一个很热门的研究方向，已经取得了很多的研究成果[14,15]，如采用经典的隐马尔可夫模型可对手势进行有效的识别[16]，但按键输入识别与手势识别具有较大不同，不能简单地将之前的手势识别方法套用到按键识别中。

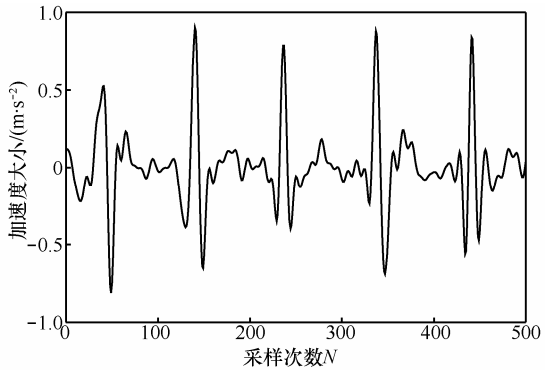


图 8　按键时的加速度

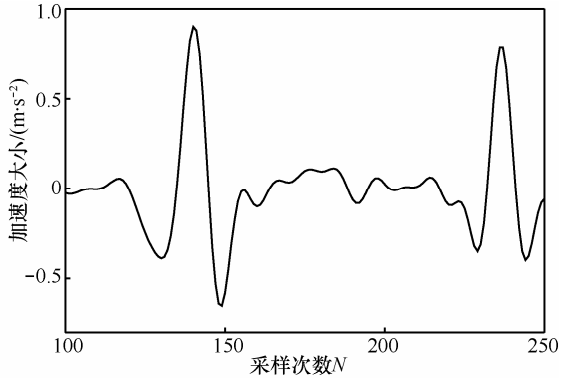


图 9　加速度特征提取

手势识别需要识别的手势个数较少，往往为确定个数，因此在训练过程中可以针对这些确定个数的手势分别进行训练，使用大量的数据对每个手势进行特征提取，在识别的过程中以现有的手势特征对待测数据进行分类，从而进行手势识别。而按键识别由于排列组合的存在，增加一位输入会带来指数型的增长，因此不能将每次的按键输入直接进行分类，需要分步识别。

在进行手势识别时 2 个手势间往往特征差别很大，2 次手势识别并未有太大联系，但在按键识别中由于已知键盘分布，可以在识别每次按键的基础上通过键盘分布辅助判断有效提高识别成功率。由于人们进行按键输入时往往是一个连续行为，比如会依次输入每一位密码，因此在已经获取每一次按键事件的前提下，可以通过分析 2 次按键之间的加速度和姿态四元数特征识别出手指从一个按键移动到另一个按键时的位移，进而描绘出运动轨迹，推测每一次按键的具体内容。

但是在进行键盘输入时手部运动较为复杂，不但有以肘部为轴的旋转运动，还有平移和上下运动，为了有效地识别出按键内容，本文对手部运动进行了分解，建立了键盘输入时的手部运动模型，并采用了 BP 神经网络算法[17,18]作为分类器对 2 次按键之间的位移进行分类。

BP 神经网络是一种按误差逆传播算法训练的多层前馈网络，是目前应用最广泛的神经网络模型之一，已广泛应用在模式识别，在人脸识别、手势识别、信号处理中均有较多应用，是一种非常经典的分类器。

BP 神经网络的学习规则是使用最速下降法，通过反向传播来不断调整网络的权值和阈值，使网络的误差平方和最小。BP 神经网络模型拓扑结构包括输入层（input）、隐层(hide layer)和输出层(output layer)，其性能主要取决于样本的特征选取方法和隐层节点的选取方法[19,20]。

(−2, 2)	(−1, 2)	(0, 2)	(1, 2)	(2, 2)
(−2, 1)	(−1, 1)	(0, 1)	(1, 1)	(2, 1)
(−2, 0)	(−1, 0)	起点	(1, 0)	(2, 0)
(−2, −1)	(−1, −1)	(0, −1)	(1, −1)	(2, −1)
(−2, −2)	(−1, −2)	(0, −2)	(1, −2)	(2, −2)

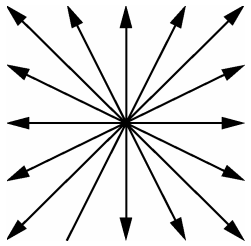


图 10　按键位移方向及分类

在样本的特种选取中，如图 10 所示，在包含 1 到 9 的数字键盘上共有 25 种不同方向和大小的位移，从起点开始移动，共有 16 种方向可供选择，并且可双击同一个按键。

为了能准确对按键间的位移进行分类，需要根据每个按键事件的时间戳计算出 2 个按键事件之间 3 个轴上的位移大小和姿态四元数，从中提取出 5 个特征值，其中姿态四元数为四维矢量。

t：2 次按键事件之间的时间间隔。

q：2 次按键事件之间的姿态四元数。

V_x：2 次按键事件之间 X 轴方向上位移大小。

V_y：2 次按键事件之间 Y 轴方向上位移大小。

V_z：2 次按键尖峰之间 Z 轴方向上位移大小。

BP 神经网络的具体步骤包括初始化连接权值及阈值；由样本输入计算隐含层、输出层输出；反馈计算新的连接权值及阈值；反复训练达到要求。但由于传统的 BP 神经网络容易陷入局部最小，因此在第三步中直接由神经网络的输入、输出来建立线性方程组，运用高斯消元法解线性方程组来求得未知权值。

最终训练模型的输入为上述 5 个特征值，其中包含姿态四元数为四维矢量，输出为二维矢量，其取值范围在(−2, −2) 到(2,2)之间。通过大量的训练样本，可训练出适用于大多数人的分类器。

在得到每 2 个按键之间的位移后，可描绘总体的移动轨迹，与键盘布局匹配后可推断出最终的几个。

4 实验结果及分析

Android 平台作为最流行的也是最开放的智能手机操作系统，在智能手表上也有相应的版本：Android Wear，其开发环境和传感器接口均与 Android 操作系统保持一致[21]。而智能手表和手机上的硬件传感器也同样相近，经过查询可知现今智能手表和智能手机绝大部分采用的均为 InvenSense 公司生成的 MPU 6 轴陀螺仪/加速度计，具体型号如表 1 所示[22]。

表 1 智能设备传感器型号

分类	设备型号	传感器型号
智能手机	MI Note	MPU-6050
	Galaxy S6	MPU-6500
智能手表	Apple Watch	MPU-6700
	Moto 360	MPU-6051

本文最终选定与智能手表 Moto 360 传感器型号基本一致的智能手机 MI Note 作为实验设备，操作系统版本为 Android 4.4，通过智能手机上的传感器来模拟智能手表，由于其参数相近，因此本次实验不失一般性。

本文对普通九宫格数字键盘进行了测试，测试平台为 Windows 8，输入内容为开机时使用的 4 位 PIN 码，且 PIN 码不包括 0，输入时要求使用食指连贯输入。本文采用了 4 个人每人 100 组数据对神经网络进行训练，其中 100 组数据平均分配到 25 种分类中，其中对按键事件的识别进行了人工校对，进一步提高了训练效果。

实验选用了 36 组数据进行测试，共包含 144 次按键事件，共测出 132 次，按键事件的识别成功率达到了 90%以上。

表 2 为按键轨迹识别结果，包含 9 组 4 次按键事件全部识别出的测试数据，描绘出的轨迹如图中所示，可以看到，其中 5 组能够准确识别出输入内容。

对于“1321”、“4239”、“6865”3 组数据，由于并未记录起始位置，在仅知道轨迹的情况下不能得出正确结果，因此识别结果可能有多种，而“5732”错误的识别为“5721”则是由于积累误差导致轨迹向左偏移，错误地将“3”识别为了“2”。

对于“7623”的识别则体现出了方案的优越性，通过键位的分布可知，“2”下方并无其他数字，因此即使位移显示出向右下方，但依然能识别出下一个数字为“3”。

从实验结果可以看出，对于大多数的数字组合，该方案能有效识别，并有一定的纠错能力，而对于不能准确识别的数字组合也能极大地缩小范围，提高效率。

5 安全防范措施

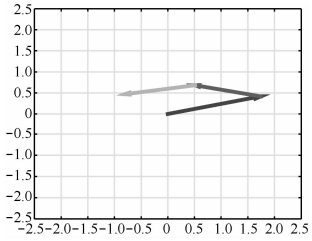
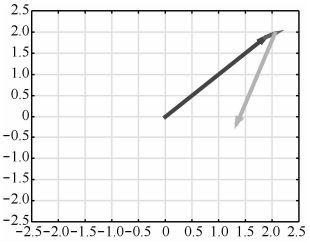
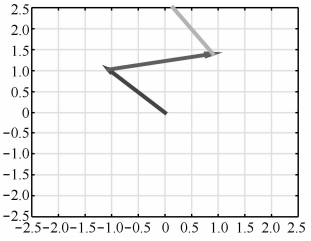
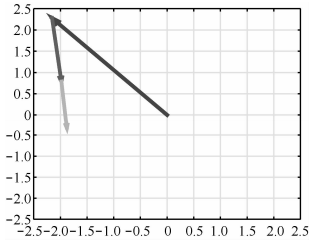
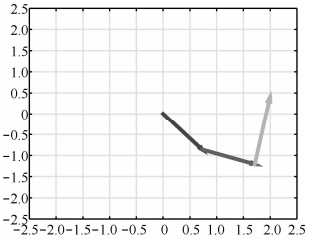
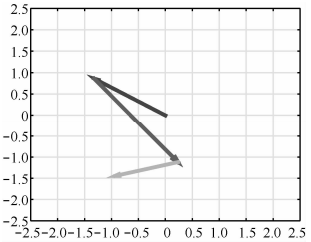
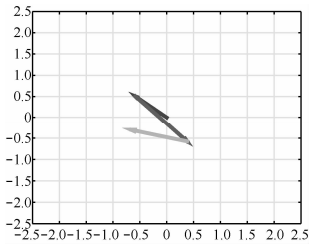
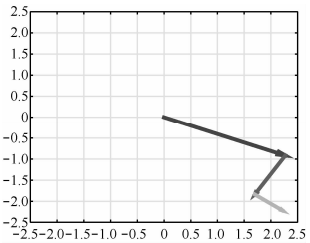
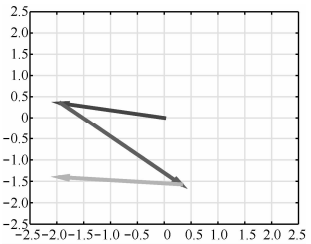
本文通过对基于智能手表运动传感器的新型攻击方法进行验证和分析，提出了以下防范措施。

1) 操作系统需要提供更完善的权限控制机制，将运动传感器同样作为敏感资源保护起来，使攻击者不能轻易获取用户的运动数据，从源头消除信息泄露隐患。

2) 针对攻击者需要预先知道键盘布局才能推测用户输入的特性，可采用智能手机上已应用的乱序键盘抵御此攻击。如图 11 显示的某银行移动客户端采用的乱序键盘，由于攻击者只能获取用户的按键轨迹而不能根据轨迹推测出具体输入，因此乱序键盘是抵御此攻击的有效方式。

3) 用户应增强信息安全意识，谨慎对待可穿戴设备。与传统智能设备不同，可穿戴设备需要贴身佩戴，会接触到用户更隐私的敏感性，一旦遭受攻

表 2　　**按键轨迹及识别结果**

轨迹图			
真实输入	1321	1992	2468
识别结果	1321 4654 7987	1992	2468
轨迹图			
真实输入	3741	4239	5732
识别结果	3741	4236 7539 7569	5721
轨迹图			
真实输入	6865	7623	9731
识别结果	6865 5754 2421 3532	7623	9731

击其后果比手机、电脑等传统设备更加严重，在敏感场合用户应避免佩戴可穿戴设备。

4) 将可信计算与运动传感器结合，通过可信计算模块实现传感器数据的安全输出，只有被可信计算模块认证过的软件才能获取到原始的传感器数据，非法软件不能轻易获取数据并上传，从而实现数据安全。

图 11　某银行客户端乱序键盘

6　结束语

本文结合实际提出了通过智能手表搭载的运动传感器识别用户敏感信息的可行方案。如图 5 所示，通过对传感器数据处理后进行分析，可识别出用户键盘上输入的 PIN 码。然后通过 Android 平台的实验进一步验证了该方案的有效性，证明在智能手表上此种安全威胁值得人们重视。最后通过对基于运动传感器识别信息方法的分析，提出了针对性的防范措施。

下一步将在此基础上进一步提高按键输入的识别成功率，并进一步分析智能手表运动传感器泄露用户信息的其他场景，如通过智能手表窃取手机上的输入信息等。

参考文献：

[1]　CHIN E, FELT A P, SEKAR V, *et al*. Measuring user confidence in

smartphone security and privacy[A]. Proceedings of the Eighth Symposium on Usable Privacy and SecurityACM[C]. 2012.

[2] JEON W, KIM J, LEE Y, *et al*. A practical analysis of smartphone security[J]. Lecture Notes in Computer Science, 2011,6771:311-320.

[3] WU L, DU X, FU X. Security threats to mobile multimedia applications: camera-based attacks on mobile phones[J]. IEEE Communications Magazine, 2014, 52(3):80 - 87.

[4] Google. Android Sensors[EB/OL]. http://developer.android.com/reference/android/hardware/SensorEvent.html.2015.

[5] MARQUARDT P, VERMA A, CARTER H, *et al*. (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers[A]. Proceedings of ACM CCS[C]. 2011.551-562.

[6] CAI L, CHEN H. Touchlogger: inferring keystrokes on touch screen from smartphone motion[A]. HotSec'11 Proceedings of the 6th USENIX Conference on Hot Topics in Security[C]. 2011.9.

[7] XU Z, BAI K, ZHU S. Taplogger: inferring user inputs on smartphone touchscreens using on-board motion sensors[A]. Proceedings of the Fifth Acm Conference on Wireless Network Security[C]. 2012. 113-124.

[8] Apple. Apple Pay[EB/OL]. http://www.apple.com/apple-pay/.2015.

[9] KELA J, KORPIPÄÄ P, MÄNTYJÄRVI J, *et al*. Accelerometer-based gesture control for a design environment[J]. Personal and Ubiquitous Computing, 2006, 10(5): 285-299.

[10] 乔相伟. 基于四元数非线性滤波的飞行器姿态确定算法研究[D]. 哈尔滨工程大学, 2011.
QIAO X W. Attitude Determination Algorithm Based on Quaternion Nonlinear Filter for Spacecraft[D]. Harbin Engineering University, 2011.

[11] KOWNACKI C. Optimization approach to adapt Kalman filters for the real-time application of accelerometer and gyroscope signals' filtering[J]. Digital Signal Processing, 2011, 21(1):131–140.

[12] TRAWNY N, ROUMELIOTIS S I. Indirect Kalman filter for 3D pose estimation[J]. University of Minnesota, Dept. of Comp. Sci. & Eng., Tech. Rep, 2005, 2.

[13] 张春莹, 潘荣江. 由整体到局部的平面曲线部分匹配算法[J]. 计算机辅助设计与图形学学报, 2008, (7):894-899.
ZHANG C Y, PAN R J. A global to local partial matching algorithm for planar curves[J]. Journal of Computer-Aided Design & Computer Graphics, 2008, (7): 894-899.

[14] CHEN F S, FU C M, HUANG C L. Hand gesture recognition using a real-time tracking method and hidden Markov models[J]. Image and vision computing, 2003, 21(8): 745-758.

[15] ZHOU S, SHAN Q, FEI F, *et al.* Gesture recognition for interactive controllers using MEMS motion sensors[A]. Nano/Micro Engineered and Molecular Systems, NEMS 2009. 4th IEEE International Conference[C]. IEEE, 2009. 935-940.

[16] FINK G A. Markov Models for Pattern Recognition: from Theory to Applications[M]. Springer Science & Business Media, 2014.

[17] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. Imagenet classification with deep convolutional neural networks[A]. Advances in Neural Information Processing Systems[C]. 2012. 1097-1105.

[18] 高鹏毅. BP 神经网络分类器优化技术研究[D]. 武汉: 华中科技大学, 2012.
GAO P Y. Study on the Optimization of Backpropagation Neural Network Classifier[D]. Wuhan: Huazhong University of Science and Technology, 2012.

[19] SHIRAKAWA K, SHIMIZ M, OKUBO N, *et al*. A large-signal characterization of an HEMT using a multilayered neural network[J]. Journal of Henan University, 2011, 45(9):1630 - 1633.

[20] 张毅. 静态手势识别的神经网络方法研究[D]. 成都: 电子科技大学, 2011.
ZHANG Y. Study on Neural Network for Static Gesture Recognition[D]. Chengdu: University of Electronic Science and Technology of China, 2011.

[21] Google. Android Motion sensors[EB/OL]. http://developer.android.com/guide/topics/sensors/sensors_motion.html ,2015.

[22] InvenSense. 6-Axis Motion Sensors[EB/OL]. http://www.invensense.com/products/motion-tracking/6-axis/. 2015.

作者简介：

宋晨光（1993-），男，河南驻马店人，北京航空航天大学硕士生，主要研究方向为可穿戴设备安全、网络与信息安全。

刘建伟（1964-），男，山东莱州人，北京航空航天大学教授、博士生导师，主要研究方向为密码学、网络与信息安全。

伍前红（1973-），男，四川安岳人，北京航空航天大学教授、博士生导师，主要研究方向为密码学、信息安全、计算安全。

关振宇（1984-），男，辽宁盘锦人，北京航空航天大学讲师，主要研究方向为空间网络安全、信息安全和密码学。