



南京大學

研究生毕业论文 (申请硕士学位)

论文题目 基于惯性传感器的人体运动感知机制研究

作者姓名 蔡庆亮

学科、专业方向 计算机科学与技术

指导教师 谢磊 副教授

研究方向 分布式计算

2017年5月

学 号 : MG1433002
论文答辩日期 : 2017 年 6 月 1 日
指 导 教 师 : (签字)

Body Movement Sensing Based on Inertial Sensor

by

Qingliang Cai

Directed by

Dr. Lei Xie

Department of Computer Science and Technology
Nanjing University

May 2017

*Submitted in partial fulfilment of the requirements
for the degree of MS in Computer Science and Technology*

南京大学研究生毕业论文中文摘要首页用纸

毕业论文题目： 基于惯性传感器的人体运动感知机制研究
计算机科学与技术 专业 2014 级硕士生姓名： 蔡庆亮
指导教师（姓名、职称）： 谢磊 副教授

摘要

近年来，由于可穿戴设备的便携性，可穿戴设备在人们的日常生活中变得越来越流行。现代的可穿戴设备基本都配备有惯性传感器，其中包括加速度计和陀螺仪。基于惯性传感器的人体运动感知机制也成为了近年来的研究热点。在本文中，我们主要关注基于惯性传感器的人体运动感知机制中的两个方面：多传感器设备的安全认证以及多传感器设备的空间同步。

首先，无线热点网络允许设备之间自发地查找对方并且进行交互，但是由于无线网络的性质，设备之间的安全认证成为了一个重要的问题。在本文中，我们提出了一个基于陀螺仪的姿态跟踪模型（GYAT），并基于此模型设计和实现了一个基于惯性传感器的安全认证系统。两个手腕上佩戴可穿戴设备的用户可以通过现实世界中的握手动作建立设备之间的安全认证。在认证过程中，我们抽取惯性传感器数据的相关性，并且在用户设备上独立地生成密钥。我们在MOTO 360智能手表上实现了基于惯性传感器的安全认证系统，实验显示我们的GYAT算法可以获得平均85%的设备间数据相关性，以及平均14b/s的密钥生成速率。

其次，我们定义了多传感器设备的空间同步概念。空间同步技术可以为很多应用服务，比如说虚拟现实的动作感知以及人机交互（HCI）。在本文中，我们提出了一个基于人体运动的空间同步框架（MOSS），它适用于任何包含加速度和陀螺仪的设备。当人体向前运动时（比如走路和跑步），系统利用人体上多个移动设备的加速度数据进行空间同步；当人体停止向前运动时，此时我们无法获得一致向前的力，系统将利用移动设备的陀螺仪数据来维持空间同步。我们在6个移动设备上，包括1个Google Glass，5个Samsung S5智能手机。实验显示我们的MOSS框架可以获得平均6.8°的角度误差以及平均93%的测量相似度。

本文的主要贡献如下：

1. 我们提出了一个基于陀螺仪的姿态跟踪模型（GYAT），它能够追踪节点的运动，并且校准了传感器数据，使得设备间的传感器数据能够获得最大的相似度。

2. 我们实现了基于惯性传感器的握手认证系统，并在真实环境下进行了实验分析，实验结果显示我们的安全认证系统取得了平均85%的设备间数据相关性，以及平均14b/s的密钥生成速率。
3. 我们提出了多传感器设备空间同步的MOSS框架。特别地，我们提出了一个用来获取空间同步的一致方向估计器与一个维持空间同步的基于陀螺仪的姿态追踪器。
4. 我们在COTS移动设备上实现了基于多传感器设备的空间同步系统，实验结果显示我们的系统可以获得平均6.8°的角度准确度，以及平均93%的测量相似度。

关键词： 惯性传感器；人体运动感知；认证系统；空间同步

南京大学研究生毕业论文英文摘要首页用纸

THESIS: Body Movement Sensing Based on Inertial Sensor

SPECIALIZATION: Computer Science and Technology

POSTGRADUATE: Qingliang Cai

MENTOR: Dr. Lei Xie

Abstract

In recent years, due to the portability of wearable device, wearable device has become increasingly popular in people's daily life. Modern wearable devices are basically equipped with inertial sensor including accelerometer and gyroscope, etc. The human body motion sensing mechanism based on inertial sensor has also become a hotspot in recent years. In this paper, we focus on two aspects of human motion sensing based on inertial sensor: authentication of multi-sensor devices and space synchronization of multi-sensor devices.

First, the wireless ad hoc network allows devices to spontaneously find and interact with each other. However, due to the nature of Wireless ad hoc network, authentication between devices has become a serious problem. In this paper, we propose a gyroscope based attitude tracking model called GYAT and implement an authentication system based on inertial sensor. By using our system, Two Users with wearable devices can build authentication through real-world handshake. During the authentication process, we explore the correlation of the Inertial Sensor data, and extract secret keys independently on the devices. We implement our system on MOTO 360 smart watch. The experiments show that our GYAT algorithm can achieve an average data similarity of 85%, and an average key generation rate of 14b/s.

Second, we define the concept of space synchronization for mobile devices. Space synchronization can be the enabling technology for many applications such as motion sensing in virtual reality and Human Computer Interaction (HCI). In this paper, we propose a scheme called Mobile Space Synchronization (MOSS) for devices with two sensors: an accelerometer and a gyroscope, which are available on most mobile devices. Accelerometer readings from multiple mobile devices on a human subject are used to achieve space synchronization when the human subject is moving forward, such

as walking and running. Gyroscope readings from multiple mobile devices on a human subject are used to maintain space synchronization when the human subject stops moving forward, which means that we can no longer obtain the consistent acceleration caused by body moving forward. We implemented our MOSS system on six mobile devices including one Google Glass and five Samsung S5 smart phones. Experiment results show that our MOSS scheme can achieve an average angle deviation of 6.8° and an average measurement similarity of 93%.

The main contribution we made in this paper are as follows:

1. We propose a gyroscope-based attitude tracking model called GYAT, which can track the attitude of the wearable device and calibrate the sensor data, so that the sensor data between the devices can achieve maximum similarity.
2. We implement an authentication system based on inertial sensor and carried out the experimental analysis in the real environment. The experimental results show the out authentication system can achieve an average data similarity of 85%, and an average key generation rate of 14b/s.
3. We define the concept of space synchronization for mobile devices and propose the MOSS scheme to achieve space synchronization among multiple mobile devices.
4. We implemented MOSS on COTS mobile devices, and the experiment results show that our MOSS scheme can achieve an average angle deviation of 6.8° and an average measurement similarity of 93%.

Keywords: Inertial Sensor; Body Movement Sensing; Authentication System; Space Synchronization

目 录

目录	v
第一章 绪论	1
1.1 研究背景介绍	1
1.2 研究的目的和意义	2
1.2.1 多传感器设备的安全认证	2
1.2.2 多传感器设备的空间同步技术	3
1.3 研究工作及主要内容	4
1.4 本文的组织结构	5
第二章 相关工作	7
2.1 多传感器设备的安全认证	7
2.2 基于惯性传感器的姿态跟踪	7
2.3 基于惯性传感器的方向估计	8
2.4 本章小结	8
第三章 基于惯性传感器的握手认证系统	9
3.1 设计目标与挑战	9
3.2 可行性研究	10
3.3 系统设计	11
3.4 数据预处理	12
3.4.1 握手监测与数据采集	12
3.4.2 时域对齐	13
3.5 数据转换	14
3.5.1 简单方案	14
3.5.2 姿态跟踪模型	15
3.5.3 初始姿态参数计算	18
3.6 在线参数学习	21

3.7	密钥生成	22
3.7.1	数据量化	22
3.7.2	不一致比特协商	23
3.7.3	随机性抽取	25
3.8	性能评估	26
3.8.1	实验设置	26
3.8.2	结果分析	27
3.9	本章小结	28
第四章	基于多传感器设备的空间同步系统	29
4.1	设计目标	29
4.2	人体运动的研究与分析	30
4.2.1	人体运动测量	30
4.2.2	室内环境下的磁力计精确度	30
4.2.3	人体运动的特征	31
4.2.4	人体运动模型	33
4.3	系统设计	34
4.4	获得空间同步	36
4.5	相关力的抽取模型	37
4.5.1	预处理	37
4.5.2	主成分抽取	37
4.5.3	方向估计	38
4.6	基于陀螺仪的姿态跟踪扩展	41
4.6.1	运动时陀螺仪的精确度	41
4.6.2	基于旋转的模型	42
4.6.3	利用MMSE估计进行校准	43
4.7	实现与评估	44
4.7.1	实现	44
4.7.2	实验设置与标准	45
4.7.3	前进方向估计	46
4.7.4	基于陀螺仪的追踪	48

4.8 案例	49
4.8.1 通过摇晃手机进行空间同步	49
4.8.2 利用人的行走/跑步/跳跃进行空间同步	50
4.9 本章小结	52
第五章 总结与展望	53
5.1 总结	53
5.2 展望	54
参考文献	55
简历与科研成果	59
致谢	60

表 格

插 图

3.1 系统场景图	9
3.2 随机性和相似性实验	11
3.3 系统框架	11
3.4 系统协议	12
3.5 握手监测	13
3.6 时域对齐算法案例	14
3.7 线性加速度在重力方向上的投影	15
3.8 参考坐标系模型	18
3.9 S_1 和 S_2 数据相关性与 S_2 初始角度 $\theta_2(0)$ 的关系	20
3.10 初始角度 θ 最优时, S_1 和 S_2 三个维度加速度数据的相关性	21
3.11 空间转换后, S_1 和 S_2 加速度的3d矢量图	21
3.12 Level Crossing 算法	22
3.13 Level Crossing 阈值选择	23
3.14 比特串协商案例	25
3.15 独立子串分割案例: 比特11代表当前状态是11, 所以它的下一个比特0属于子串 S_{11}	26
3.16 性能评估试验	28
4.1 数据采集设定	30
4.2 磁力计精确度测量	31
4.3 一致/不一致的加速度在不同设备上的方向和大小	32
4.4 不同方向加速度的均值和方差	33
4.5 系统架构	35
4.6 全局坐标系导出图	36
4.7 将加速度 $f_i(t)$ 投影到水平面上	37
4.8 PCA分析图	38
4.9 PCA估计结果vs 真实值	39

4.10 根据PCA结果识别正向加速度的时间区间	40
4.11 陀螺仪的角度偏移情况	42
4.12 估计旋转矩阵 $At, t + \delta t$	43
4.13 安卓手机上的MOSS界面	45
4.14 实验环境	46
4.15 评估一致前进方向估计的准确性	47
4.16 评估基于陀螺仪追踪的准确性	48
4.17 多个设备以不同的部署进行摇晃	49
4.18 评估角度的大小和相似度	49
4.19 人体的复合运动	50
4.20 复合运动实验结果	51
4.21 评估CFDE和GOT的准确性	52

第一章 绪论

1.1 研究背景介绍

近年来，可穿戴设备在人们的日常生活中变得越来越流行。可穿戴设备的用途十分广泛，包括健康监控、运动监控、导航、游戏操控、通信等等。现代的可穿戴设备基本都装有惯性传感器，其中包括加速度计和陀螺仪，部分可穿戴设备也包含磁力计、心率计等其它传感器设备。基于惯性传感器的人体运动感知机制也成为了近年来的研究热点。在本文中，我们主要关注基于惯性传感器的人体运动感知机制中的两个方面：多传感器设备的安全认证以及多传感器设备的空间同步。

首先，无线热点网络允许设备之间自发地查找对方并且进行交互，但是由于无线网络的性质，设备之间的认证和安全成为了一个重要的问题[37]。多传感器设备之间的安全认证研究也是近几年来的研究热点。目前常用的可穿戴设备之间的安全认证有两种，一是通过端到端的蓝牙认证[32]，二是通过第三方的证书机构进行认证[12]。端到端的蓝牙认证无须第三方设施介入，认证成本较低，但是蓝牙认证需要人为介入进行设备查找并且进行手动确认，操作较为繁琐，人机交互体验不强；通过第三方证书的机构进行认证的方式尽管操作对用户透明，但是需要在当前网络环境中设立第三方证书机构，成本较为昂贵，且由于第三方的介入导致认证方式较慢。经我们观察，当两个用户进行握手动作时，他们手臂的物理动作具有一定的相关性。基于这一观察，我们想到可穿戴设备上的惯性传感器可以采集这些动作的相关数据，通过分析这些传感器数据，我们可以提取其中的相关性，从而生成一致的密钥进行设备之间的安全认证。

其次，惯性传感器的读数是基于设备的局部坐标系的，并由其设备姿态决定（更准确地说是它的主板）。由于多个移动设备放置在人体不同部位，造成了惯性传感器的局部坐标系的不同。因此，统一所有可穿戴设备的坐标系对多传感器的协作应用是必不可少的，这种技术我们称之为空间同步技术。利用空间同步技术，这些传感器可以在统一的坐标系下对物理运动进行采样，从而更好地协作分析人体的运动。我们也称统一的坐标系为全局坐标系或参考坐标系。空间同步技术可以为很多应用服务，比如虚拟现实的动作感知以及人机交互。例如，在虚拟现实游戏中，一个移动的人可能在不同部位（比如头，手臂，腿）装备多个移动设备取追踪人体的移动。一种直接的进行移动设备空间

同步的解决方案是利用磁力计设备。磁力计允许各个设备获取相同的地球磁场方向。配合各设备相同的重力方向，所有的设备可以进行空间同步。这个解决方案，尽管简单，但是有两个缺点。首先，大多数现有的可穿戴设备（比如Apple Watch S₁, Samsung Watch Gear2和MOTO Watch 360）并没有装备磁力传感器；相比较而言，大多数可穿戴设备都有加速度和陀螺仪。第二，由于室内建筑结构的复杂以及其它电子设备引起的磁场干扰，磁力计在室内的读数会非常不准确。先前的工作显示在室内环境下磁力计的平均误差有17°，是室外误差的15倍[33]。简单地把两个设备放在一起也会干扰磁力计的读数。基于磁力计的这一性质，我们需要提供一种在不使用磁力计的情况下进行空间同步的技术。经观察，人体在向前运动时，身体上各部位的可穿戴设备均受到一个一致的力，我们想到如果可以利用这个一致的力，就可以用来替代室内准确度较低的磁力计，从而实现空间同步技术。

1.2 研究的目的和意义

本文的研究目的是对基于惯性传感器的人体运动感知机制研究。本文从两个方面进行着手，一个是多传感器设备的安全认证机制研究，一个是多传感器设备的空间同步技术研究。

1.2.1 多传感器设备的安全认证

对于多传感器设备之间的安全认证机制研究，我们的目的是设计和实现一个交互自然、无须人为干预的安全认证系统。当用户之间进行握手行为时，他们的握手动作具有一定的相关性，而惯性传感器可以采集握手动作相关的物理数据。基于这一观察，我们想到可以从握手期间产生的惯性传感器数据中提取出用户之间握手动作的相关特征，从而生成设备之间一致的密钥，而且这种过程不需要传递整段原始传感器数据。但是为了实现这个系统，我们仍需要解决如下几个挑战：

1. **时域上的不一致：**由于可穿戴设备是佩戴在不同用户的手臂上进行数据采集的，我们无法保证用户的握手动作是完全同步进行的，这就有可能造成不同设备采集到的惯性传感器数据在时域上是不对齐的，也就直接导致数据间的相关性大大减小。
2. **坐标系的不一致：**目前可穿戴设备的传感器数据都是基于设备的局部坐标系的。不同用户的可穿戴设备的佩戴的位置和姿态均会有所不同，也就是

说，各设备的局部坐标系是不一样的。即使是相同的力作用在这两个设备上，设备所测量的传感器数据是也都完全不一样的。而且，在用户握手过程中，设备的姿态一直在发生变化，如果不解决坐标系不一致的问题，会严重影响不同设备的数据相关性。

3. **第三方的监听：**在建立认证的过程中，设备间的交互均是以广播模式进行，这中间传递的信息就有可能被第三方攻击者窃听。为了防止第三方的监听，我们将不能在信道中发送整段传感器数据，不同传感器设备之间只能传递少部分协商信息，且这部分协商信息要在密钥中剔除，密钥的生成过程需要在穿戴设备本地完成[4]。
4. **惯性传感器数据内部的相关性：**人体的握手运动是连续的过程，所以，基于这种运动采集的惯性传感器数据内部必然在时域上存在一定的相关性，如果不消除这种数据内部的相关性，就有可能让攻击者利用部分数据来预测其它相关的数据，使得密钥的安全性降低。

1.2.2 多传感器设备的空间同步技术

对于多传感器设备的空间同步技术研究，它的意义在于：惯性传感器的数据的采集是基于设备的局部坐标系的，当可穿戴设备之间的姿态不同时，其惯性传感器数据也完全不同，这对多传感器设备之间的协作应用造成很大困难，而空间同步技术可以将惯性传感器的基于局部坐标系的数据转换到统一的坐标系中，使相同的物理运动在不同的穿戴设备上具有一致的读数，从而使基于多传感器设备协作的应用开发更为方便有效。我们的想法是，当人向前移动时，所有装备在人身上的设备会拥有一个相同的向前的加速度，我们称它为一致加速度。我们利用加速度计抽取一致加速度并来获得空间的同步。但是，我们仍需要面临如下几个挑战：

第一个挑战是当人体向前运动时抽取身体移动的一致加速度。因为一致的和非一致的力是混合在一起的，所以这具有很大的挑战性。因为移动设备装备在人不同的身体部位上，他们获得的加速度方向和大小都具有很大的不同。为了解决这个挑战，我们提出了一个基于主成分分析（PCA）的框架从观测到的加速度中移除不一致的加速度。一个关键的点是一致的加速度对所有装备在人体上的移动设备的观测加速度都具有贡献。也就是说，各个设备的观测加速度信号值包含了一致加速度信号（所有设备都一样）以及不一致加速度（每个设备都不一样）。此外，由于人体内部运动的幅度大小比前进移动的幅度大小小，一致的加速度信号比不一致的加速度信号更占主导权。因此，观测到的多设备

信号是强烈相关的而且我们可以用PCA取抽取主导的成分。注意到当人体走路或跑步时，移动不仅仅是水平向前的，而且有竖直上校的运动。为了消除这种竖直方向的影响，在PCA之前，我们将加速度向量投影到由重力向量决定的水平面上。

第二个挑战是处理当人体停止向前运动时为了维持空间同步造成的累计误差。众所周知，基于陀螺仪的姿态追踪是具有累积误差的[38]。而且，如果人体运动中有大的角速度和线性加速度，误差将会增加更多。当前的解决方案主要依赖卡尔曼滤波器；然而，这对计算能力有限的移动设备来说是非常耗资源的[11]。为了解决这个问题，我们提出了一个简单但是高效的补偿滤波器。它能基于重力向量的稳定性取校准陀螺仪的追踪。我们提出了一个定义正交重力向量和平行重力向量旋转的旋转模型。我们利用这个模型以及最小均方误差估计器校准了基于陀螺仪的估计。

1.3 研究工作及主要内容

在本篇论文中，我们首先分别对多传感器设备的安全认证技术以及多传感器设备的空间同步技术的相关工作进行了归纳和总结，分析了其中的优缺点。

在多传感器设备的安全认证机制方面，我们设计和实现了一个基于惯性传感器的握手认证系统，该系统能够抽取两个用户握手过程中产生的惯性传感器数据的相关性，并利用该相关性生成一致的密钥进行安全认证。首先，我们对该系统进行了可行性实验分析并设计了系统的框架；其次，我们对密钥生成过程中的主要模块进行了研究与分析。针对设备坐标系不一致的问题，我们重点分析了惯性传感器数据的空间转换模型以及基于陀螺仪的姿态跟踪模型（GYAT）；最后，我们实现了基于惯性传感器的握手认证系统，并在真实环境下对其进行了实验与性能评估。

在多传感器设备的空间同步技术方面，我们首先介绍了获得和维持空间同步的模型；其次，我们重点介绍了如何在不利用磁力计的情况下，基于惯性传感器对穿戴设备的水平运动方向进行估计；接着在维持空间同步状态方面，我们对基于陀螺仪的姿态跟踪技术进行了扩展研究，引入了重力方向加速度的校准机制；最后，基于上述两个模块，我们设计与实现了一个基于多传感器设备的空间同步系统，并对实现的系统进行了详尽的实验评估，还在真实的环境下进行了系统的案例分析。

我们在本论文中的贡献点如下：

1. 我们提出了一个基于陀螺仪的姿态跟踪模型（GYAT），它能够追踪节点的

运动，并且校准了传感器数据，使得设备间的传感器数据能够获得最大的相似度。

2. 我们实现了基于惯性传感器的握手认证系统，并在真实环境下进行了实验分析，实验结果显示我们的安全认证系统取得了平均85%的设备间数据相关性，以及平均14b/s的密钥生成速率。
3. 我们提出了多传感器设备空间同步的MOSS框架。特别地，我们提出了一个用来获取空间同步的一致方向估计器与一个维持空间同步的基于陀螺仪的姿态追踪器。
4. 我们在COTS移动设备上实现了基于多传感器设备的空间同步系统，实验结果显示我们的系统可以获得平均6.8°的角度准确度，以及平均93%的测量相似度。

1.4 本文的组织结构

本文的主要研究内容是基于惯性传感器的人体运动感知机制，全文共分为五章，内容和组织结构如下：

第一章绪论。本章首先介绍了多传感器设备的安全认证以及多传感器设备的空间同步的研究背景，其次对本课题的研究目的和意义进行了说明，阐述了现有的问题以及问题的解决思路，最后对研究内容以及研究的贡献进行了简要介绍。

第二章相关工作。首先本章介绍了多传感器设备之间建立安全认证的现有常用手段，接着介绍了目前基于物理层进行密钥生成的相关研究工作，然后介绍了基于惯性传感器（比如加速度、陀螺仪、磁力计等）的姿态跟踪以及方向估计相关工作，与我们的工作进行了对比，并分析了这些工作的某些局限性。

第三章基于惯性传感器的握手认证系统。首先提出了系统实现的目标与挑战，接着对基于惯性传感器的握手认证技术的可行性进行了分析，然后我们设计并实现了基于惯性传感器的握手认证系统，最后我们在真实环境下对系统的性能进行了详尽地评估。

第四章基于多传感器设备的空间同步系统。本章设计了一个基于多传感器设备的空间同步系统，首先对人体运动进行了研究分析，其次介绍了获得空间同步以及维持空间同步的模型，然后重点介绍了相关力的抽取模型以及基于陀螺仪的姿态跟踪扩展，最后对系统进行了详尽的实验分析。

第五章总结与展望。对文中提出的基于惯性传感器的可穿戴设备感知机制感知机制研究进行总结，并对可穿戴设备空间同步技术和感知技术未来的工作进行展望。

第二章 相关工作

2.1 多传感器设备的安全认证

目前，多传感器设备的安全认证的常用解决方案有两种，一种是基于蓝牙的端到端认证，一种是基于第三方证书系统的公钥密钥机制。但基于蓝牙的端到端认证需要人为的查找设备以及手动确认授权，人机交互体验不强，基于第三方证书系统的公钥密钥机制在某些局域网环境下是无法进行的。近年来，有很多工作开始研究基于设备间物理上的相关信息生成一致的密钥[6, 14, 21, 26, 40]。如Liu等人的论文中，为了解决动态移动环境下的缺乏第三方密钥管理机构的安全通信问题，她们通过利用OFDM提供的细粒度的通道信息来进行多传感器设备之间的密钥生成[21]。在Zhu等人的论文中，为了解决车联网中两辆车之间建立一个无线安全通信信道的问题，他们提出了一个让两辆车从RSSI（接收信号强度）值中抽取密钥的框架，且邻近的其它车辆无法生成相同的密钥[40]。在Daniel Bichler的论文中，为了在人体无线网络区域中提供高效且友好的密钥生成方式，他们提出了通过摇晃两个设备区建立安全连接的方式[6]。

这些工作都是利用物理层信息的变化生成一致的密钥，但是这些工作有些是在车辆上进行，有些是在设备之间相对坐标系固定的情况下进行，没有一个工作是在多个佩戴穿戴设备的人之间进行的。由于人体的运动更加复杂，而且当可穿戴设备在不同的人体上时，穿戴设备的坐标系往往是不一致的，这对多传感器之间的密钥生成产生了更大的挑战，直接运用上述论文中的方法在多个人体的设备之间生成密钥效果是非常差的，因此我们需要研究新的方法去解决穿戴设备佩戴在不同用户上的密钥生成问题。

2.2 基于惯性传感器的姿态跟踪

已经有很多研究工作利用加速度，陀螺仪和磁力计传感器估计移动设备（比如智能手机）的姿态[3, 18, 22, 24, 35, 36, 38]。与我们的工作像比较，大多数工作都利用了磁力计。比如说Madgwick，提出了一个结合加速度和磁力计进行姿态估计的四元数呈现[22]，以及Zhou利用加速度计和磁力计去配合陀螺仪选择最好的感知能力去进行姿态估计[38]。先前这方面的工作仅有两个系统Autowitness[13]和Nericell[27]，没有利用磁力计找到了局部坐标系以及参考

坐标系之间的旋转矩阵。他们从加速度计中获取用一个车辆向前的加速度（加速和减速）。与我们的工作相比较，他们在车辆上放置移动设备而不是在人体上放置有两个重要的限制。首先，车辆没有人体内部的运动，丙炔车辆比人体移动更加笔直，他们不需要处理我们第一个技术挑战。第二，当车辆停止时，移动设备不会移动能够，他们也不需要处理我们第二个技术挑战。

2.3 基于惯性传感器的方向估计

最近的一些工作研究估计基于航位推测导航框架的朝向估计[1, 19, 20, 29, 31, 34, 39]。相比较我们的工作，这些大部分工作利用磁力计取估计朝向，同时尝试减弱室内环境的磁场干扰。比如说，WalkCampass用磁力计估计人体的走路朝向[29]。Walkie-Markie利用智能手机中的磁力计和陀螺仪取获得走路朝向和人体的转角，并在此基础上获得室内路线地图[31]。Wang用磁力传感器，陀螺仪传感器和WiFi地标去估计人体走路的正对朝向[34]。这个类目的先前工作中，只有APT系统没有利用加速度计和陀螺仪取获得人体的走路朝向[39]。相比较我们的工作，APT只用了一个移动设备，并没有解决多个移动设备的空间同步问题。而且，这个类目中大多数先前的工作利用了应用相关的特征去提升了估计人体上智能手机朝向的准确性。相对的，我们提出了一个更加通用的解决方案在不同但是相关的加速度中去估计多个可穿戴设备的朝向。我们的解决方案既不依赖不准确的磁力计，也不会利用任何应用相关的特征。

2.4 本章小结

首先本章介绍了多传感器设备之间建立安全认证的现有常用手段，接着介绍了目前基于物理层进行密钥生成的相关研究工作，然后介绍了基于惯性传感器（比如加速度、陀螺仪、磁力计等）的姿态跟踪以及方向估计相关工作，与我们的工作进行了对比，并分析了这些工作的某些局限性。

第三章 基于惯性传感器的握手认证系统

在现实世界中，两个人之间的握手动作代表两个人互相认可的一种信息，且这种握手动作在物理运动上是具有相关性的，而惯性传感器可以记录这种物理过程的相关特征。基于这一观察，我们设计了一个新颖的基于惯性传感器的握手认证系统。

我们系统的应用场景如图3.1所示，两个用户的手腕上都戴着配备有惯性传感器的智能可穿戴设备，当两个用户进行握手时，系统可以实时感知用户握手的动作，并抽取用户之间握手动作的相关性特征，生成一致的密钥，最后两个用户之间的可穿戴设备即可利用生成的密钥建立安全认证。



图 3.1: 系统场景图

3.1 设计目标与挑战

我们的目标是利用两个用户握手过程中产生的惯性传感器数据，抽取惯性传感器数据之间的相关性特征，然后利用该相关性特征生成一致的密钥。该过程须要对用户完全透明，且为了防止被第三方监听者攻击，密钥生成过程需要在设备本地进行。

根据实验发现，我们发现有很多干扰因素会影响设备之间生成独特且一致的密钥。我们必须解决如下具有挑战性的问题：

1. **时域上的不一致：**由于可穿戴设备是佩戴在不同用户的手臂上进行数据采集的，我们无法保证用户的握手动作是完全同步进行的，这就有可能造成

不同设备采集到的惯性传感器数据在时域上是不对齐的，也就直接导致数据间的相关性大大减小。

2. **坐标系的不一致：**目前可穿戴设备的传感器数据都是基于设备的局部坐标系的。不同用户的可穿戴设备的佩戴的位置和姿态均会有所不同，也就是说，各设备的局部坐标系是不一样的。即使是相同的力作用在这两个设备上，设备所测量的惯性传感器数据也都是完全不一样的。而且，在用户握手过程中，设备的姿态一直在发生变化，如果不解决坐标系不一致的问题，会严重影响不同设备的数据相关性。
3. **第三方的监听：**在建立认证的过程中，设备间的交互均以广播模式进行，这中间传递的信息就有可能被第三方攻击者窃听。为了防止第三方的监听，我们将不能在信道中发送整段惯性传感器数据，不同传感器设备之间只能传递少部分协商信息，且这部分协商信息要在密钥中剔除，密钥的生成过程需要在穿戴设备本地完成[4]。
4. **惯性传感器数据内部的相关性：**人体的握手运动是连续的过程，所以，基于这种运动采集的惯性传感器数据内部必然在时域上存在一定的相关性，如果不消除这种数据内部的相关性，就有可能让攻击者利用部分数据来预测其它相关的数据，使得密钥的安全性降低。

3.2 可行性研究

为了测试这项工作的可行性，我们必须满足两个基本指标，内部数据的随机性以及设备间数据的相关性。内部数据的随机性是指用户每次握手产生的数据随机的程度，设备间相关性是值每次握手的两个用户产生的传感器数据的相关程度。高随机性代表了传感器的数据更难预测，生成的密钥也就越安全，另一方面高相关性代表着可以利用更少的传感器数据生成一定长度的密钥。这两个指标对安全认证系统都是必须的。

在本文中，我们令两个用户佩戴的智能可穿戴设备分别为 S_1 和 S_2 。为了估计传感器数据的相关性，我们先简单地采用合加速度特征进行相关性计算。在本文中，我们采用Person方法计算数据之间的相关性[5]，计算方法如公式3.1所示：

$$\rho_{X,Y} = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \quad (3.1)$$

我们令加速度的在三个轴上的数据分别为为 X_i 、 Y_i 、 Z_i ，则合加速度 A_i 的计算方式为： $A_i = \sqrt{(X_i)^2 + (Y_i)^2 + (Z_i)^2}$ 。

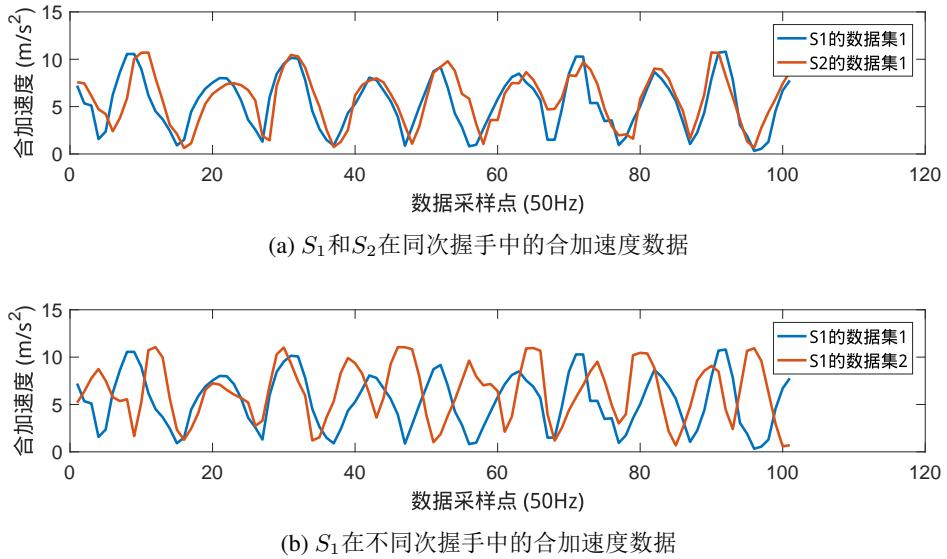


图 3.2: 随机性和相似性实验

我们的样本是在同次握手过程中，设备 S_1 和 S_2 产生的加速度数据。图3.2a显示了当两个人握手的时候，两个设备产生的合加速度数据具有较高的相关性，约为0.765，这足够用来生成一个密钥。为了估计传感器数据的随机性，我们比较 S_1 在两次握手时产生的传感器合加速度数据的相关系数，图3.2b显示了它们在这种情况下几乎没有相关性，相关性约为−0.046。通过相关性和随机性的验证性试验，可见不同用户之间进行握手的惯性传感器数据可以满足密钥生成的需求。

3.3 系统设计

为了实现系统，我们首先设计了系统的整体框架，如图3.3所示，系统包含四个模块：数据预处理模块、数据转换模块、在线参数学习模块和密钥生成模块，各模块的具体工作原理将在下面几节描述。

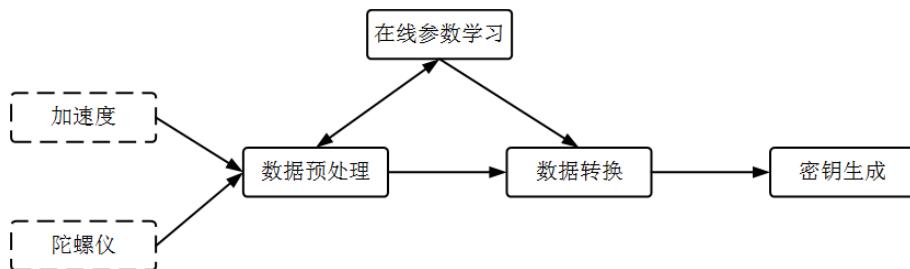


图 3.3: 系统框架

其次我们设计了一套密钥生成过程的协议，来描述不同设备间各模块的任务以及交互情况。我们的协议设计包含四个阶段，如图3.4所示：

阶段1：数据预处理：在这个阶段，我们需要监测握手事件，截取出握手过程的传感器数据，并对数据进行平滑操作以滤掉一些高频噪声。

阶段2：在线参数学习：在这个阶段，我们须要在传感器设备之间进行协作，然后学习得到时域对齐以及坐标系对齐的相关参数。发起连接的设备 S_1 需要发送它数据的一部分作为训练数据给另一方 S_2 。接收数据的 S_2 利用双方的训练数据学习得到对齐时域和坐标系的相关参数，然后再发还给 S_1 。

阶段3：数据转换：在这个阶段，设备 S_1 和 S_2 会分别利用学习得到的参数对传感器数据时域的对齐以及空间的转换，以提高 S_1 和 S_2 数据的相关性。

阶段4：密钥生成：在这个阶段，设备 S_1 和 S_2 将在本地对转换后的传感器数据进行数据量化、不一致比特协调以及随机性抽取，最终生成一致的密钥。

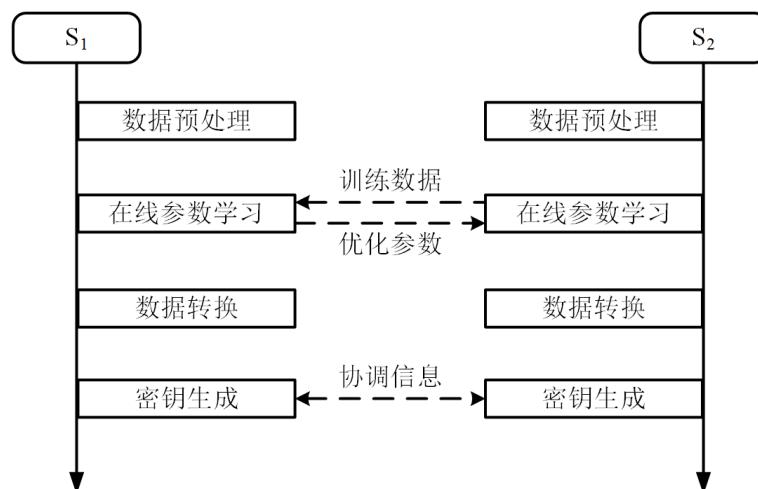


图 3.4: 系统协议

3.4 数据预处理

3.4.1 握手监测与数据采集

设备 S_1 和 S_2 的惯性传感器数据只在握手的过程中存在数据相关性，因此，我们需要监测出握手的事件，并且截取出握手过程的传感器数据。图3.5a显示了用户从静止到握手再到静止的合加速度图像，我们观察到在静止阶段加速度的波动很小，而在握手阶段加速度的波动非常大。

基于这一观察，我们利用一个长度为 k 的滑动窗口持续地采集传感器数据，

并实时计算滑动窗口内部合加速度数据的方差 V_i , V_i 的计算方式如下:

$$V_i = \frac{\sum_{j=i}^{j=i+k} (A_j - \bar{A}_{k,i})^2}{k} \quad (3.2)$$

其中 A_j 为窗口内某一时刻的加速度, $\bar{A}_{k,i}$ 为窗口内的平均加速度。图3.5b为对应的合加速度的方差图像, 我们观察到在静止阶段, $V_i \approx 0$; 在握手阶段, $V_i > T$ 。因此, 当 $V_i > T$ 时, 我们认为此时用户有可能在做握手运动, 此时我们开始截取传感器数据, 当 $V_i < T$ 时, 我们结束传感器数据的截取。

数据截取完成后, 系统向外部广播密钥认证邀请, 若没有其他穿戴设备回应时, 则判断该段数据为无效数据, 然后重新开始监测。获得握手区间的传感器数据后, 由于数据存在一定的高频噪声, 我们简单地通过滑动平均对传感器数据进行平滑处理。此时, 我们便完成了传感器数据的预处理工作。

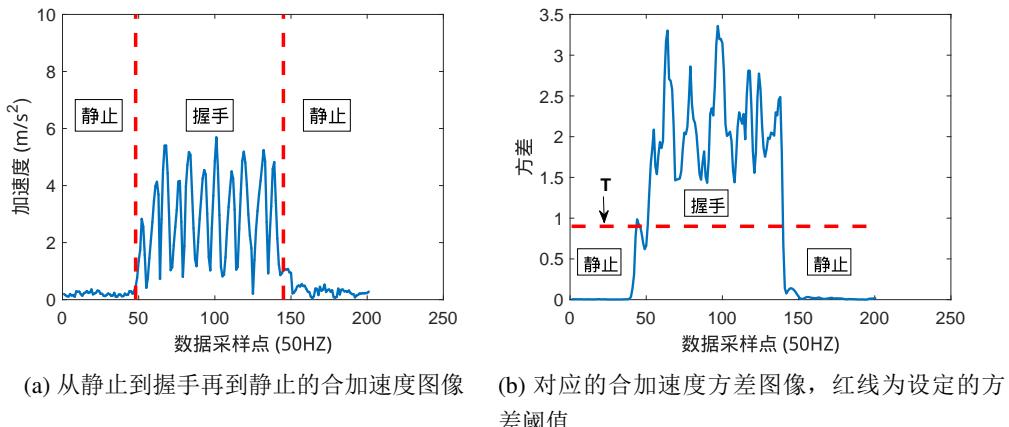


图 3.5: 握手监测

3.4.2 时域对齐

由于 S_1 和 S_2 采样的开始时间以及 S_1 和 S_2 开始握手机动作时间不一定完全一致, S_1 和 S_2 传感器的数据在时域上也就存在不对齐的问题。如图3.6中红色虚线所示, 如果不经过时域校正, S_1 和 S_2 的相关性将会非常低, 只有0.408的相关度。在本文中, 我们利用一个交叉相关的方法对 S_1 和 S_2 的数据进行对齐。

其大致思想如图3.6所示: 我们分别令 S_1 和 S_2 的合加速度数据为 A_{S_1} 和 A_{S_2} , 以其中一个设备的传感器数据为基准。不失一般性地, 首先我们以 S_1 在区间 $[T, T + L]$ 的合加速度数据为基准, 然后我们用一个长度为 L 的滑动窗口的起始点在 S_2 的 $[T - t, T + t]$ 区间移动, 在每一个移动点上, 我们计算 A_{S_1} 和 A_{S_2} 的相关性。移动完成后, 最大相关性对应的点即为 S_1 和 S_2 传感器

数据的时域对齐点。我们令 T_O 为 A_{S_1} 和 A_{S_2} 的时域对齐点, cor 为相关性函数, 则 $T_O = \underset{t_o}{\operatorname{argmax}} cor(A_{S_1}[T, L + T], A_{S_2}[t_o, t_o + L])$, 其中 $t_o \in [T - t, T + t]$ 。值得一提的是, 我们只须对齐 S_2 的长度为 $L(L << |A_{S_1}|)$ 的滑动窗口内的数据即可, 由于传感器数据的连续性, 整段传感器数据可以根据 S_2 的时域对齐点 T_O 完成时域对齐工作。时域对齐的参数 T_O 的学习将由在线参数学习模块完成。

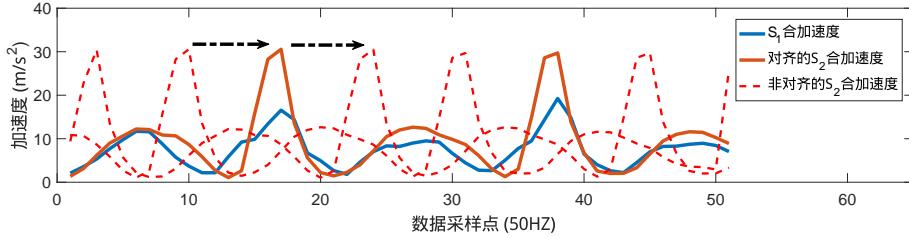


图 3.6: 时域对齐算法案例

3.5 数据转换

传感器节点由不同的用户佩戴在不同的位置, 这必然造成传感器坐标系的不一致性。由于传感器数据是基于传感器的局部坐标系测量得到的, 这就导致了不同设备之间传感器数据的相关性大大减小, 严重影响了密钥生成算法的性能。于是, 我们决定将不同设备间基于局部坐标系的传感器数据进行坐标系的对齐, 然后利用对齐的参考坐标系对原始的传感器数据进行转换。然而在握手过程中, 传感器的局部坐标系一直在变化, 这对坐标系的对齐造成了很大困难。

3.5.1 简单方案

我们首先尝试了三种不同的简单方案去解决坐标系不一致的问题:

- 1) **计算合加速度 (RACC):** 合加速度忽略了方向信息, 这能够避免坐标系不对齐的问题。然而, 它会损失加速度的方向信息, 不能充分地利用三个维度的信息。
- 2) **将线性加速度投影到重力方向上 (GACC):** 在一般情况下, 人握手的主要是在重力方向上来回运动。由于重力相对于人的握手产生的力是一个稳定的成分, 我们可以利用低通滤波器将重力加速度与线性加速度进行分离[8], 然后我们可以将线性加速度投影到重力方向上得到该特征, 投影方法如图3.7所示。
- 3) **基于主成分分析 (PACC):** 主成分分析 (PCA) 是一个统计性的方法, 它可以利用正交转化, 将一系列可能相关的变量转化成一些列线性不相关的变量也

就是主成分[16]。由于握手动作的相似性，这一正交转换相当于在统计意义上对传感器数据进行了坐标系的校正。

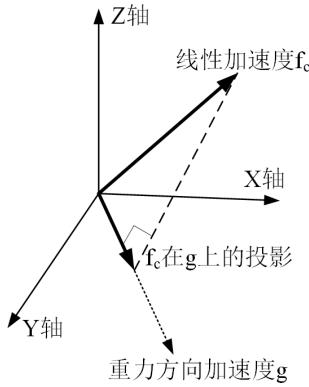


图 3.7: 线性加速度在重力方向上的投影

尽管上述三个方法可以避免系统不一致的问题，但是仍然存在一些不足之处：合加速度和重力方向投影无法充分利用三轴信息；主成分分析需要大量的统计数据且只是统计意义上的坐标系校正，使得密钥生成性能不是非常理想。因此，我们需要找到一个方法，它既能巧妙地滤除不相关信息，又能充分利用传感器数据三轴的信息，最大程度地提升设备间的数据相关性和数据内部的随机性。

3.5.2 姿态跟踪模型

我们想到，假如能够将 S_1 和 S_2 基于局部坐标系的数据转换到基于一个统一的参考坐标系的数据，这个问题就可以很好地解决。但我们会遇到两个问题：首先，尽管我们可以利用低通滤波器滤出重力分量[8]，但是为了构造从局部坐标系到全局坐标系的旋转矩阵，我们需要找到另一个参考坐标系的坐标轴向量。现有的常用方案是利用磁力计去解决这个问题。但是，磁力计在室内环境下容易受到干扰，而且短时间内准确度较低，所以无法满足我们的系统需求。其次，由于设备的坐标系一直在变化，我们需要用一个模型追踪设备的坐标系变化。在本节中，我们提出了一个基于陀螺仪姿态跟踪的模型（GYAT）。

我们首先解决如何跟踪坐标系变化的问题，我们假定设备的另一个参考坐标系的坐标轴向量已知（这个向量的位置参数我们将在3.5.3节描述）。由于坐标系的变化可以归结为坐标系的旋转运动，陀螺仪可以反映三轴的微小旋转，于是我们很自然地想到用陀螺仪去跟踪坐标系的变化。

旋转可以三种方式表示：旋转矩阵、欧拉角和四元数。

欧拉角必须以特定的旋转顺序表示，并且不能表示某些特殊的姿态；四元数可以被认为是绕着特定向量的旋转但并不适合我们的系统。旋转矩阵中，局部坐标系到全局坐标系的转换可以用一个 3×3 的旋转矩阵 C 表示，其中每一列是局部坐标系中的一个坐标轴的单位向量在全局坐标系中的表示。一个定义在局部坐标系中的向量 v_b 等于向量

$$v_g = Cv_b \quad (3.3)$$

在全局坐标系中的表示。逆转化为：

$$v_b = C^T v_g \quad (3.4)$$

这是因为旋转矩阵的逆等于它的转置。

为了追踪传感器的姿态，我们需要随时间变化跟踪 C ，我们令 t 时刻的姿态为 $C(t)$ ，那么 C 的变化为：

$$\dot{C}(t) = \lim_{\delta t \rightarrow 0} \frac{C(t + \delta t) - C(t)}{\delta t} \quad (3.5)$$

其中 $C(t + \delta t)$ 可以写成两个矩阵的乘积：

$$C(t + \delta t) = C(t)A(t) \quad (3.6)$$

其中 $A(t)$ 是 t 时刻的局部坐标系到 $t + \delta t$ 时刻局部坐标系的旋转矩阵。如果 $\delta\phi$ ， $\delta\theta$ 和 $\delta\psi$ 分别是局部坐标系 t 到 $t + \delta t$ 关于x、y和z的微小旋转，那么利用小角度的近似[24]我们可以将 $A(t)$ 写成：

$$A(t) = I + \delta\Psi \quad (3.7)$$

其中

$$\delta\Psi = \begin{pmatrix} 0 & -\delta\psi & \delta\theta \\ \delta\psi & 0 & -\delta\phi \\ -\delta\theta & \delta\phi & 0 \end{pmatrix} \quad (3.8)$$

替代之后即为：

$$\dot{C}(t) = \lim_{\delta t \rightarrow 0} \frac{C(t + \delta t) - C(t)}{\delta t} \quad (3.9)$$

$$= \lim_{\delta t \rightarrow 0} \frac{C(t)A(t) - C(t)}{\delta t} \quad (3.10)$$

$$= \lim_{\delta t \rightarrow 0} \frac{C(t)(I + \delta\Psi) - C(t)}{\delta t} = C(t) \lim_{\delta t \rightarrow 0} \frac{\delta\Psi}{\delta t} \quad (3.11)$$

在 δt 趋于0情况下，小角度的近似是合理的，然后，

$$\lim_{\delta t \rightarrow 0} \frac{\delta \Psi}{\delta t} = \Omega(t) \quad (3.12)$$

其中

$$\Omega(t) = \begin{pmatrix} 0 & -\omega_{bz}(t) & \omega_{by}(t) \\ \omega_{bz}(t) & 0 & \omega_{bx}(t) \\ -\omega_{by}(t) & \omega_{bx}(t) & 0 \end{pmatrix} \quad (3.13)$$

是角速度向量的对称形式 $\omega_b(t)$ 。所以为了追踪姿态旋转的算法必须解决微分方程

$$C(t) = C(0) \cdot \exp\left(\int_0^t \omega(t) dt\right) \quad (3.14)$$

其中 $C(0)$ 是设备的初始旋转矩阵。

一个惯性传感器实际上提供的是给定频率采样的角速度向量，而不是提供一个连续的信号 $\omega_b(t)$ 。所以我们必须将采样数据进行积分，在本文中我们用矩形规则进行积分计算。

令连续的角速度向量采样的时间间隔为 δt 。在一个时间周期 $[t, t + \delta t]$ 内，公式3.14可以写成：

$$C(t + \delta t) = C(t) \cdot \exp\left(\int_t^{t+\delta t} \Omega(t) \delta t\right) \quad (3.15)$$

用矩形规则我们可以写成：

$$\int_{t+\delta t}^t \Omega(t) dt = B \quad (3.16)$$

其中

$$\mathbf{B} = \begin{pmatrix} 0 & -\omega_{bz}\delta t & \omega_{by}\delta t \\ \omega_{bz}\delta t & 0 & \omega_{bx}\delta t \\ -\omega_{by}\delta t & \omega_{bx}\delta t & 0 \end{pmatrix} \quad (3.17)$$

其中 $\omega_b = (\omega_{bx}, \omega_{by}, \omega_{bz})^T$ 是对应于更新周期的角速度向量样本。令 $\sigma = |\omega_b \delta t|$ ，将公式3.16和公式3.17带入到公式3.15中，最终进行指数项的泰勒展开，我们得到

$$C(t + \delta t) = C(t)\left(I + B + \frac{B^2}{2!} + \frac{B^3}{3!} + \frac{B^4}{4!} + \dots\right) \quad (3.18)$$

$$= C(t)\left(I + B + \frac{B^2}{2!} - \frac{\delta^2 B}{3!} - \frac{\delta^2 B^2}{4!} + \dots\right) \quad (3.19)$$

$$= C(t)\left(I + \left(1 - \frac{\delta^2}{3!} + \frac{\delta^4}{5!} \dots\right)B + \left(\frac{1}{2!} - \frac{\delta^2}{4!} + \frac{\delta^4}{6!} \dots\right)B^2\right) \quad (3.20)$$

$$= C(t)\left(I + \frac{\sin \delta}{\delta} B + \frac{1 - \cos \delta}{\delta^2} B^2\right) \quad (3.21)$$

根据导出的公式3.18，我们就可以用实时的陀螺仪采样数据不断地更新旋转矩阵。

3.5.3 初始姿态参数计算

现在，我们已经知道如何利用实时的陀螺仪采样数据连续地更新旋转矩阵 $C(t)$ 。现在我们需要计算传感器设备的初始旋转矩阵 $C(0)$ 。目前，我们可以通过低通滤波滤出重力向量 \bar{g} ，为了构造 $C(0)$ ，我们需要得到另一个参考坐标系的坐标轴向量的在局部坐标系中初始坐标，我们令这个坐标轴向量为 \bar{x} 。在这里，我们用最大似然的方法计算这个向量 \bar{x}_g 。

首先，根据旋转矩阵的定义，参考坐标系的坐标轴向量 \bar{x}_g 与另一个坐标轴（也就是重力向量） \bar{g} 正交，所以参考坐标系的坐标轴向量 \bar{x}_g 在与 \bar{g} 正交的平面上（我们记为 H ）。我们将局部坐标轴 \bar{x}_b 投影到平面 H 上，记为 \bar{x}_p ，由于重力向量 \bar{g} 已知，则 $\bar{x}_p = \bar{x}_b - \frac{\bar{g} \cdot \bar{x}_b}{|\bar{g}|}$ 。

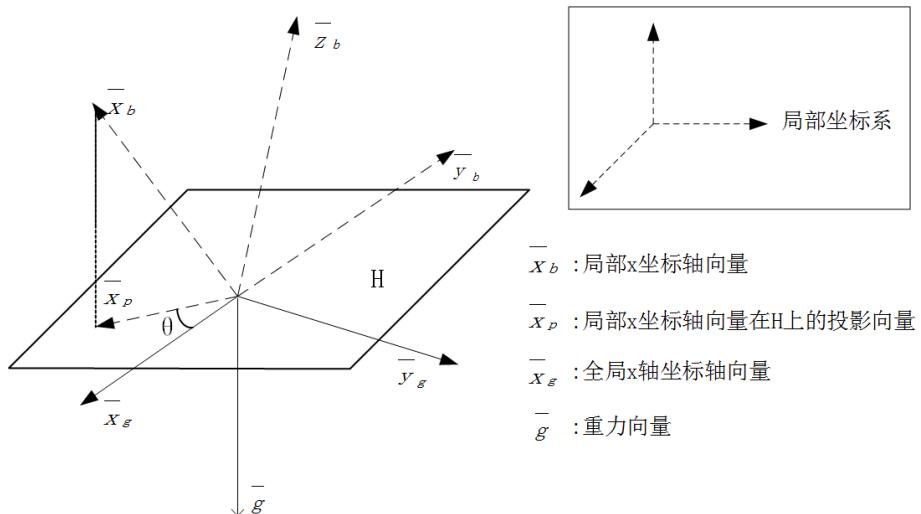


图 3.8: 参考坐标系模型

然后我们令 \bar{x}_p 与 \bar{x}_g 的夹角为 θ ，如图3.8所示。根据旋转矩阵的定义， \bar{x}_g 为单位向量，且 \bar{x}_g 与 \bar{g} 正交，那么， \bar{x}_g 可由方程组3.22解出：

$$\begin{cases} \bar{x}_g \cdot \bar{g} = 0 \\ \frac{\bar{x}_p \cdot \bar{x}_g}{|\bar{x}_p||\bar{x}_g|} = \cos\theta \\ |\bar{x}_g| = 1 \end{cases} \quad (3.22)$$

由于我们只需要对齐两个设备的坐标系，不失一般性地，我们令 t_0 时刻 S_1 的参考坐标轴向量 \bar{x}_{g_1} 与其局部坐标轴向量在平面 H 上的投影向量 \bar{x}_{p_1} 的夹

角 $\theta_1(0)$ 为0, 令 t_0 时刻 S_2 的参考坐标轴向量 \bar{x}_{g_2} 与其局部坐标轴向量在平面H上的投影向量 \bar{x}_{p_2} 的夹角为 $\theta_2(0)$ 。我们的目标是找到一个最优的 $\theta_2(0)$ 使得 S_1 和 S_2 的三轴线性加速度数据的相关性最大。由于握手过程传感器数据量不大(只有100到500个采样点), 这里我们简单地采用在 $(0, 2\pi)$ 中进行迭代的方式。

根据双方握手机动的物理运动, 设备 S_1 和 S_2 的传感器数据在基于统一的参考坐标系下有一定的相关性。基于这个假设, 如果我们找到一个初始的 $\theta_2(0)$ 角能够最大化参考坐标系下的两个传感器数据的相关性, 则我们可以由方程组3.22计算得到 \bar{x}_g 。我们得到了参考坐标系的两个坐标轴向量, 第三个坐标轴向量 \bar{y}_g 可由 \bar{x}_g 和 \bar{g} 叉乘得到, 即: $\bar{y}_g = \bar{x}_g \times \bar{g}$ 。此时, t_0 时刻的局部坐标系到参考坐标系的旋转矩阵 $C(0)$ 也可以由 \bar{g} 、 \bar{x}_g 和 \bar{y}_g 表示了。

我们的目标是最大化 S_1 和 S_2 的全局加速度数据 A_{g1} 和 A_{g2} 的相关性, 如公式3.23表示:

$$\underset{\theta_2(0)}{\operatorname{argmax}} \quad \rho(A_{g1}(t), A_{g2}(t)) \quad (3.23)$$

其中全局加速度数据 $A_g(t)$ 的计算, 是通过局部坐标系到参考坐标系的旋转矩阵 $C(t)$ 左乘局部加速度数据 $A_b(t)$ 得到的, 即 $A_{g1}(t)$ 和 $A_{g2}(t)$ 可以由公式3.24计算:

$$A_g(t) = C(t)A_b(t) \quad (3.24)$$

其中旋转矩阵 $C(t)$ 随着时间 t 的变化而不断更新, 关于 $C(t)$ 的计算与更新方式我们已经在3.5.2和3.5.3节中讨论过了, 我们可以根据上一个时刻的旋转矩阵以及实时的陀螺仪数据来更新当前的旋转矩阵。我们已经得到了 t_0 时刻 $C(0)$ 关于 θ 的表示方式, 而且局部加速度数据 $A_b(t)$ 已知, 那么在替换 $C(t)$ 之后, $A_g(t)$ 也可以由关于 θ 的函数计算得到(我们令这个函数为 f)。综上所述, $\theta_2(0)$ 可以公式3.25计算得到:

$$\theta_2(0) = \underset{\theta_2(0)}{\operatorname{argmax}} \quad \rho(f(0)A_{b1}(t), f(\theta_2(0)A_{b2}(t))) \quad (3.25)$$

在对这个坐标系轨迹进行建模之后, 我们将在 $(0, 2\pi)$ 范围内迭代 S_2 初始的角度 $\theta_2(0)$, 目标是找到一个使 S_1 和 S_2 三轴数据平均相关性最大的点。算法1描述了这个具体过程。图3.9显示, S_1 和 S_2 的数据相关性随着 S_2 的初始角度 $\theta_2(0)$ 的变化而改变, 当 $\theta_2(0) = 5.013(\text{rad})$ 时, S_1 和 S_2 在三个维度上的平均数据相关性最大, 即找到了 S_2 最优的初始夹角 $\theta_2(0)$ 。

Algorithm 1 最优初始姿态参数查找

输入: S_1 和 S_2 的加速度数据 A_{b1} 、 A_{b2} , 陀螺仪数据 G_{b1} 、 G_{b2} 和迭代次数 $INum$

in

输出: t_0 时刻 S_2 局部坐标轴投影 \bar{x}_p 与参考坐标轴 \bar{x}_g 的最优夹角 $\theta_2(0)$ out

- 1: 利用低通滤波分别分离 S_1 和 S_2 加速度数据中的重力分量 \bar{g}_1 、 \bar{g}_2 和线性加速度分量 \bar{l}_{b1} 、 \bar{l}_{b2}
- 2: 令 S_1 和 S_2 的最大数据相关性 $MaxCor = 0$, 对应 S_2 的初始夹角 $\theta_2(0) = 0$, 对应 S_2 的初始夹角 $\theta_1(0) = 0$
- 3: **for** $i = 1$ to $INum$ **do**
- 4: 令 $\theta'_2(0) = 2\pi/INum \times i$
- 5: 利用 t_0 时刻的重力分量 $\bar{g}_1(0)$ 、 $\bar{g}_2(0)$ 和夹角 $\theta_1(0)$ 、 $\theta'_2(0)$ 分别构造 S_1 和 S_2 在 t_0 时刻的旋转矩阵 $RM_1(0)$ 和 $RM_2(0)$
- 6: 用 G_{b1} 、 G_{b2} 更新 S_1 和 S_2 的所有时刻的旋转矩阵 RM_{i1} 、 RM_{i2}
- 7: 利用 RM_{i1} 、 RM_{i2} 和 \bar{l}_{b1} 、 \bar{l}_{b2} 计算 S_1 和 S_2 的全局加速度数据 \bar{l}_{g1} 和 \bar{l}_{g2}
- 8: 计算 \bar{l}_{g1} 和 \bar{l}_{g2} 的相关性 $CuCor$
- 9: 用 $CuCor$ 和 $\theta'_2(0)$ 分别更新最大相关性 $MaxCor$ 以及 S_2 对应的夹角 $\theta_2(0)$
- 10: **end for**
- 11: **return** S_2 最优的初始夹角 $\theta_2(0)$

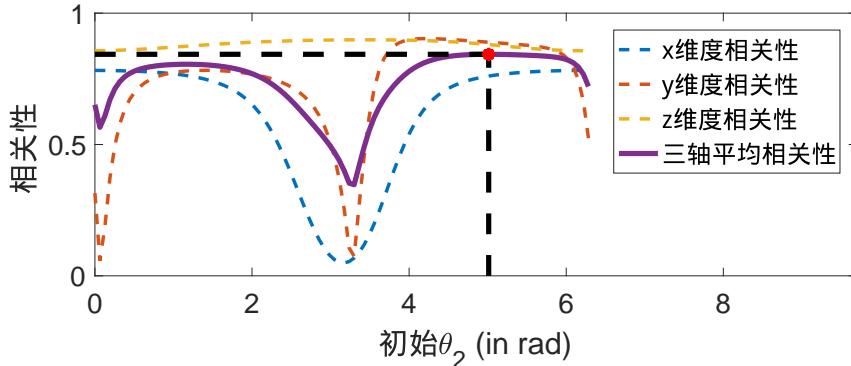


图 3.9: S_1 和 S_2 数据相关性与 S_2 初始角度 $\theta_2(0)$ 的关系

在得到最优的初始角度 θ 后, 我们利用基于陀螺仪的姿态跟踪模型 (GYAT) 对惯性传感器数据进行空间转换, 然后再比较 S_1 与 S_2 之间的数据相关性。图3.10显示了在空间转换后, 我们会分别在三个轴上获得0.859、0.732以及0.749的相关性 (原始的数据相关性分别为0.682、0.481和0.113)。图3.11a和图3.11b显示了在数据转换到参考坐标系后, S_1 和 S_2 的加速度数据在3D空间中的

位置比原始的位置更加一致了，这说明我们对数据的空间转换是非常有效的。

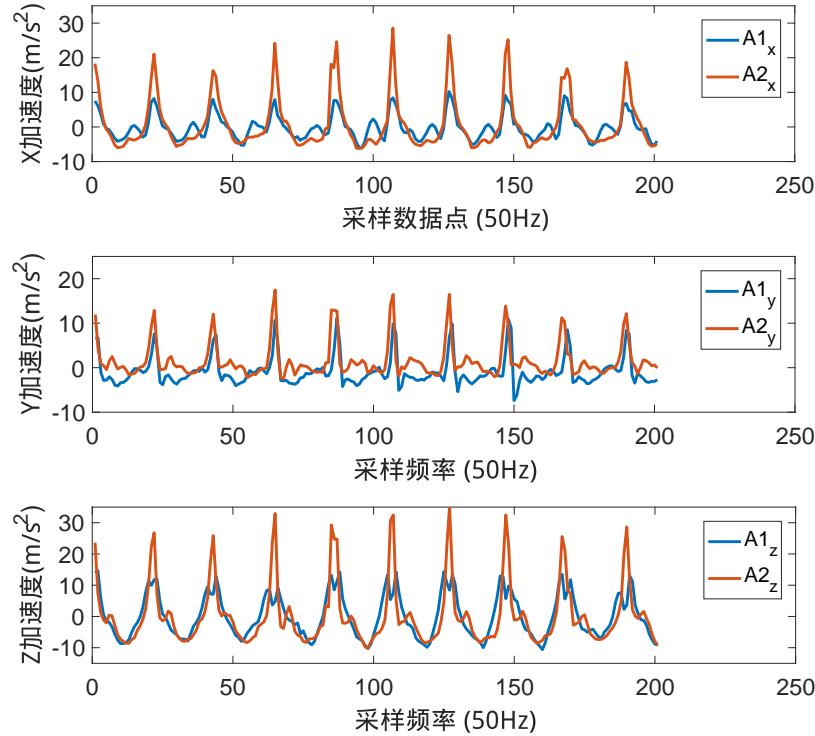


图 3.10: 初始角度 θ 最优时, S_1 和 S_2 三个维度加速度数据的相关性

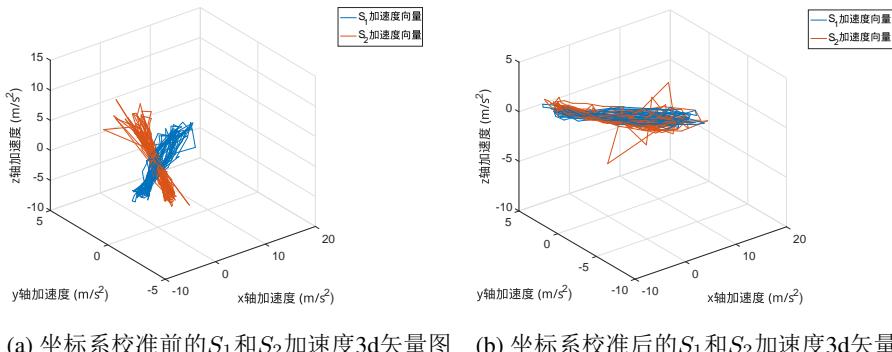


图 3.11: 空间转换后, S_1 和 S_2 加速度的3d矢量图

3.6 在线参数学习

这个阶段，我们需要学习时域对齐的参数以及坐标系对齐的相关参数。在3.4.2、3.5.2和3.5.3节中，我们已经介绍了时域对齐参数和坐标系对齐参数的计算方法。为了防止数据被第三方攻击者监听，我们不能直接将整段传感器数

据在网络中传输。由于数据的连续性，时域对齐和数据转换只要在初始的一小部分数据内进行，然后利用该段数据的对齐参数和初始姿态参数即可对剩下的传感器数据进行时域对齐和数据转换。

基于这个观察，我们将 S_1 的初始 m 个采样点的数据和 S_2 初始的 m 个点的采样数据取出来作为参数的训练数据（分别记为 D_{t_1} 和 D_{t_2} ），不失一般性地，我们将 S_1 的训练数据 D_{t_1} 发送给 S_2 ，在 S_2 的计算模块中利用 D_{t_1} 和 D_{t_2} 训练时域对齐参数 T_o 和初始姿态参数 θ 。然后我们将训练的到的时域对齐参数 T_o 和初始姿态参数 θ 发还给 S_1 。这样 S_1 和 S_2 在不传递完整传感器数据的前提下即可对传感器数据进行时域上的对齐和初始姿态的校正。

3.7 密钥生成

3.7.1 数据量化

在数据转换完成之后，传感器数据之间的相关性得到很大程度的提升，但 S_1 和 S_2 数据之间的幅度仍存在不一致性，我们无法直接使用该数据进行密钥生成，还需进一步量化处理，以消除幅度的差异性。

3.7.1.1 Level Crossing 算法原理介绍

在本文中我们利用Level Crossing方法对传感器数据进行量化处理[25]。Level Crossing方法的原理如图3.12所示，当 $A(t) > q^+$ 时， $Q(t) = 1$ ，当 $A(t) < q^-$ 时， $Q(t) = 0$ ，其中 $q^+ = \mu_A + \alpha\delta_A$ ， $q^- = \mu_A - \alpha\delta_A$ 。在Level Crossing之后，传感器数据就变成了由0和1构成的比特串，即完成了量化过程。

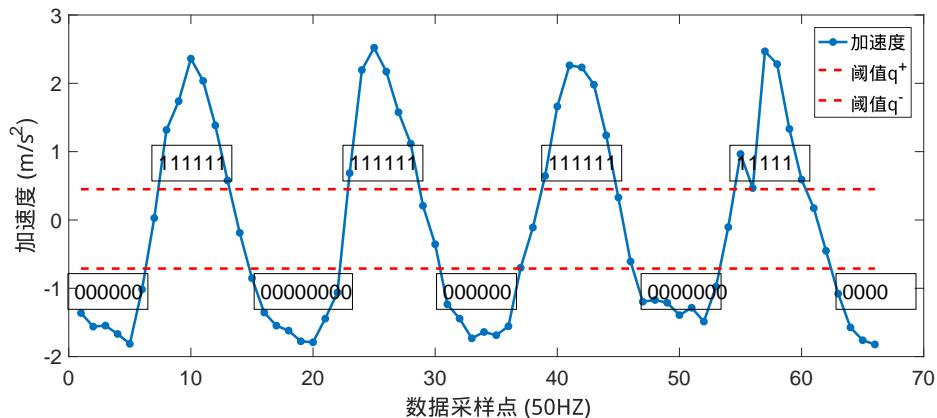


图 3.12: Level Crossing 算法

3.7.1.2 Level Crossing 阈值选择

我们数据量化的目标是：(1)使 S_1 和 S_2 量化后的比特尽可能一致；(2)使量化后的比特包含的信息量尽可能大。由此，我们定义一个指标 T_l ，计算方式如公式3.26所示：

$$T_l = E/(n - n_m) \quad (3.26)$$

其中 E 为量化后比特的信息熵 ($E = \sum_i P(A_i) \log_b P(A_i)$) [30]， n 为量化后的比特数， n_m 为量化后不一致的比特数， L 为传感器数据的长度。

我们在线下设定Level Crossing的不同阈值 α 进行量化实验，并分别计算量化后的 T_l 值。图3.13显示了当 α 在0~0.3范围内时， T_l 随着 α 的增加逐渐增加，这是因为当 α 过小时，量化的不一致比特数随着 α 的增加而增加；当 $\alpha > 0.3$ 时， T_l 随着 α 增加而减少，这是因为 α 增加时，量化后的信息量减少。根据实验结果，我们在本文中设定 $\alpha = 0.3$ 。

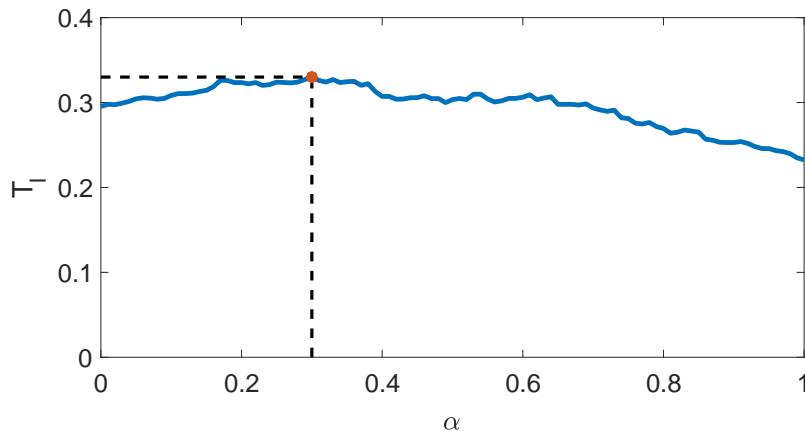


图 3.13: Level Crossing 阈值选择

3.7.2 不一致比特协商

在对传感器数据进行Level Crossing之后， S_1 和 S_2 生成的比特串中仍然存在不一致的比特。所以我们需要设计一个调解协议去纠正或者消除不匹配的比特。在本文中，我们实现了一个协议Cascade[7]，它的实现比较简单并且高效。在本节中，我们会介绍Cascade的原理与实现。

我们首先介绍一下在Cascade协议中会使用的原始操作。

BINARY: 当字符串 A 和 B 有奇数个错误时，那么 S_1 和 S_2 会进行对一个错误进行二分查找，以如下方式在公共通道中交换数量小于 $\lceil \log n \rceil$ 的比特：

1. S_2 发送字符串的前一半的奇偶性给 S_1 。

2. 通过测试前一半的奇偶性，然后与 S_2 发过来的奇偶性进行比较，判断奇数个错误发生在前一半还是后一半字符串。
3. 这个过程重复地在步骤2判断的半区。最终可以发现一个错误。

Cascade 在交换中进行。交换的次数是由 S_1 和 S_2 在发送前决定的。这个决策和参数 p 相关。令 $A = A_1, \dots, A_n, B = B_1, \dots, B_n$ (with $B_i, A_i \in \{0, 1\}$)，分别为 S_2 和 S_1 的字符串。

在交换过程1中， S_2 和 S_1 选择 k_1 ，然后将它们的字符串分割成大小为 k_1 的比特块。这个位置在 $K_v^1 = \{l | (v-1)k_1 < l \leq vk_1\}$ 的比特将在阶段1形成块。 S_2 发送她所有的比特块的奇偶性给 S_1 。利用 **BINARY** 操作， S_1 可以在每一个块奇偶性与 S_2 对应块奇偶性不一致的块中纠正一个错误。这时， S_1 的所有块和 S_2 所有块的错误都是偶数个的。

在每一个步骤号大于1的阶段， S_1 和 S_2 选择 k_i 和 a 个随机函数 $f_i : [1..n] \rightarrow [1 \dots \lceil \frac{n}{k_i} \rceil]$ 。这些位置在 $K_j^i = \{l | f_i(l) = j\}$ 中的比特将在阶段 i 中形成快。 S_2 发送 S_1 ：

$$a_j = \bigoplus_{l \in K_j^i} A_l \quad (3.27)$$

对于每个 $1 \leq j \leq \lceil \frac{n}{k_i} \rceil$ 。 S_1 用相同的方式计算它的 b_j ，然后与 a_j 比较。对于每个 $b_j \neq a_j$ ， S_1 和 S_2 在由 K_j^i 定义的块上执行 **BINARY** 操作。 S_1 会发现 $l \in K_v^u$ ，然后会有奇数个错误。令 κ 为这些快的集合。 S_2 和 S_1 现在可以选择在 κ 中最小的块，然后用 **BINARY** 操作找到另一个错误。令 l' 为这个错误在字符串 A 和 B 的位置。在纠正 $B_{l'}$ 后， S_1 可以纠正这个 β 由从每个一个第1到第 i 个阶段中包含 $B_{l'}$ 的块的一个错误。他同时也可以通过如下计算决定偶奇数个错误的块的集合 κ' ：

$$\kappa' = \beta \downarrow \kappa. \quad (3.28)$$

如果 $\kappa' \neq \emptyset$ ，那么 S_1 用同样的方式找到了另外一个错误。这个过程会重复执行，知道没有块有奇数个错误位置，这时过程 i 结束，然后每个在过程1到 i 的块有偶数个错误（可能为0个）。

图3.14 显示了一个简单的调解案例，在过程1中：所有的bits串分割成6个块。然后对于每个块， S_1 和 S_2 执行 **BINARY** 操作去纠正奇数个错误。现在每个块要么包含偶数个错误要么没有错误。在阶段2中：双方的比特串重新排序并分成6个不同的块。然后像阶段1一样执行相同的操作，如果一个块中的错误在前一个阶段没有被发现，然后前面对应的块应该包含另外一个错误。

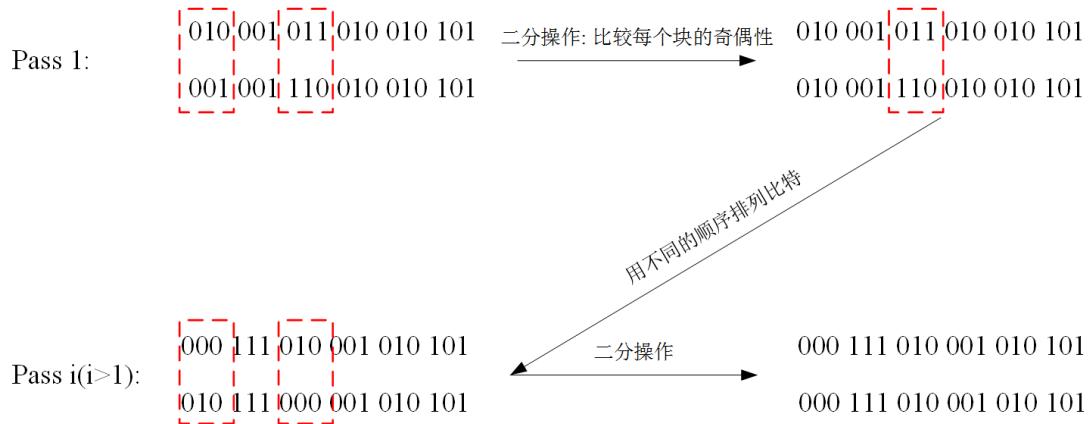


图 3.14: 比特串协商案例

3.7.3 随机性抽取

在进行信息调解纠正不匹配串之后，双方都有了相同量化的比特串。但是这些比特串内部存在依赖性，可能是不安全的。为了解决这个问题， S_2 和 S_1 从他们自己的量化比特串中抽取出随机的比特。这个过程可以利用一个基于比特串马尔科夫模型的随机性抽取算法实现[10]。

这个随机性抽取过程包含两步。首先，比特串按如下方式分割成子串。假定马尔科夫链的阶数是 k ，那么子串的数量为 2^k ，每个子串对应马尔科夫链的一个状态。子串中的比特对应这个比特之前的马尔科夫状态，且这个状态由这个比特的前 k 个比特决定。在本实验中，我们令马尔科夫链的阶数 $k = 2$ ，图3.15给出了一个分割子串的案例。

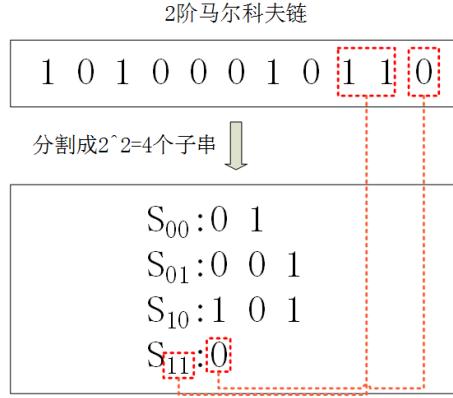


图 3.15: 独立子串分割案例: 比特11代表当前状态是11, 所以它的下一个比特0属于子串 S_{11}

其次, 我们将各个子串映射到新的编码, 我们从每个子串中抽取出非偏斜的比特。如果比特为0的概率和比特为1的概率是不一样的, 则比特是偏斜的。偏斜的比特生成模式会被攻击者利用。不失一般性地, 我们假设这些比特是偏斜的。给定固定长度为 N 的比特, 令1的个数为 k 。由于这些比特是独立的, 所有 C_N^k 种排列可能性都是等概率事件。我们利用一个编码表将每一种长度为 N 的偏斜比特映射到一个长度为 $\log C_N^k$ 的新编码上。编码表可以离线构造, 只须 S_1 和 S_2 的编码表相同即可。在本文中, 我们设定 $N = 5$ 。

完成随机性抽取后, 设备 S_1 和 S_2 分别得到了一致的密钥 K_1 和 K_2 , 且 $K_1 = K_2$, 此时我们便完成了密钥生成的工作。 S_1 和 S_2 利用一致的密钥 K_1 和 K_2 即可进行设备间的认证工作。

3.8 性能评估

3.8.1 实验设置

我们在MOTO 360智能手表的安卓平台上实现了基于惯性传感器的握手认证系统。我们请5组同学, 每组2个人, 每个人佩戴一个MOTO 360智能手表进行了系统的相关性能实验。每组同学分别进行大幅度和小幅度的握手机动, 每种幅度握手50次, 每次握手持续5秒。传感器采样频率设为50HZ, 用一个智能手机作为数据接收与处理端, 智能手机与手表之间采用蓝牙连接。我们在智能

手机上实现了数据接收和密钥匹配算法。我们将用两个指标来评价我们的算法：数据的相关性和有效密钥的比特率。数据相关性指：双方数据转换后的相关性。有效密钥的比特率是指：单位时间生成的有效密钥比特数。

3.8.2 结果分析

时间窗口的影响：然后我们分别计算了不同时间窗口下，利用陀螺仪跟踪姿态算法处理的 S_1 和 S_2 平均数据相关性。图3.16b显示了，在窗口为6s的情况下， S_1 和 S_2 数据相关性最好，为0.884。而在窗口为8s时， S_1 和 S_2 数据相关性降低到0.754，这是因为，在短时间内，陀螺仪跟踪的姿态效果较好，且数据越长，相关性越好。但是随着时间增加，陀螺仪的累计误差会不断增大，造成数据相关性降低。

算法对比：我们分别用合加速度（RACC）、投影到重力方向（GACC）、基于PCA转换（PACC）以及基于陀螺仪姿态跟踪模型（GYAT）四种不同的算法对 S_1 和 S_2 的传感器数据进行处理，然后计算 S_1 和 S_2 传感器数据的相关性。图3.16a的柱状图显示了我们的陀螺仪姿态跟踪算法（GYAT）获得了最好的效果0.884，而其它算法的数据相关性均在0.75以下。

动作幅度的影响：为了研究动作幅度对陀螺仪跟踪姿态算法的影响，我们设定时间窗口为4s，然后分别在小幅度握手和大幅度握手的情况下进行了实验，时间窗口设为4s。图3.16c显示了，小幅度的握手情况下， S_1 和 S_2 的数据相关性为0.884，要好于大幅度握手情况下的数据相关0.794。这是因为当动作幅度变大时，陀螺仪的累计误差也会相对更大。

最后，我们计算了上述四种算法的量化比特生成率，其中陀螺仪跟踪姿态算法的时间窗口设为4s，握手幅度为小幅度。图3.16d显示，合加速度（RACC）、投影到重力方向（GACC）、基于PCA转换（PACC）三种方法取得的密钥生成速度分别为5b/s、6b/s以及6b/s，我们的基于陀螺仪姿态跟踪算法（GYAT）的密钥生成速度最高，为14b/s，是其它算法性能的2倍左右，这是因为我们陀螺仪姿态跟踪算法充分利用了加速度三个维度的信息。

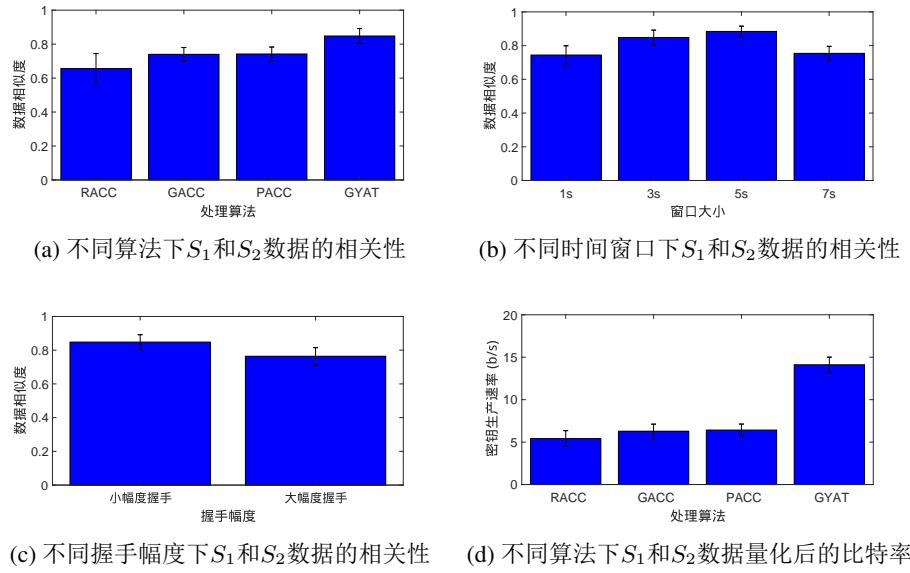


图 3.16: 性能评估试验

3.9 本章小结

本章首先提出了基于惯性传感器的握手认证系统的设计目标与挑战，并对系统的可行性并进行了探究性实验。其次，我们对系统进行了框架和协议设计。然后，我们分别介绍了系统框架中的每一个模块，并重点介绍了基于陀螺仪的姿态跟踪模型（GYAT）。最后，本章对实现的握手认证系统进行了性能评估与分析。实验结果表明我们的系统可以很好地在用户握手过程中对多传感器设备建立安全认证。

第四章 基于多传感器设备的空间同步系统

尽管多设备时间同步研究以及非常成熟，据我们所知，空间同步先前还没有被正式地定义和系统地研究过[2, 9, 15, 17]。在这个章节中，我们提出了一个基于人体运动的空间同步框架（MOSS），它能适所有用于包含加速度计和陀螺仪的设备上（大部分移动设备都包含这两个传感器）。

4.1 设计目标

当人体向前运动时（比如走路和跑步），人体上多个设备的加速度计可以用来获得空间的同步。我们的想法是，当人向前移动时，所有装备在人身上的设备会拥有一个相同的向前的加速度，我们称它为一致加速度。我们利用加速度计抽取一致加速度并用来获得空间的同步。尽管由于人体局部的运动（利用手臂和腿的移动），这些移动设备也会受到其它不同的加速度（我们称这些为不一致的加速度）。因为内部的移动比向前的移动更小，我们仍然可以把它们当做噪声处理；而且，我们可以利用信号处理技术滤掉大部分的噪声。然后，我们可以从加速度数据中抽取一致的加速度，从而计算前进的方向。另一方面，利用例如巴特沃斯滤波器的低通滤波器[8]，我们可以从局部坐标系的加速度的数据中抽取重力加速度。然后，我们以前的方向和重力的方向作为参考坐标轴，根据坐标轴的定义，第三个坐标轴与两个参考的坐标轴分别正交，那么第三个坐标轴可以由两个参考坐标轴叉乘得到。最后，根据这三个坐标轴，我们可以构建各个设备的同步坐标系。

当人停止运动时，这意味着我们无法利用人体运动抽取一致的力，此时我们利用多设备上的陀螺仪去维持空间上的同步。在人停止向前移动时，人的身体部位仍可能轻微移动或者旋转。多设备的陀螺仪数据允许我们持续地追踪设备局部坐标系三个坐标轴的轻微旋转。我们通过对所有时刻不同坐标轴的旋转角速度进行积分，推导出一个实时的旋转矩阵。利用重力向量在空间坐标系的稳定性，我们又对陀螺仪跟踪得到的旋转矩阵进行了校准。所以，我们能够在人体停止移动的时候还能维持空间的同步。

4.2 人体运动的研究与分析

4.2.1 人体运动测量

4.2.1.1 实验设置

我们在人体不同的部位上放置六个移动设备，其中包括一个智能眼镜(Google Glass 2)和五个智能手机(Samsung Galaxy S5)，在用户的日常活动中不断收集惯性传感器数据。如图4.1所示，Google Glass放在头部，五个手机放在人体五个不同的部位上。这些设备装备着加速度计、陀螺仪和一个磁力计。我们用磁力计获得的三个坐标轴作为参考全局坐标系。

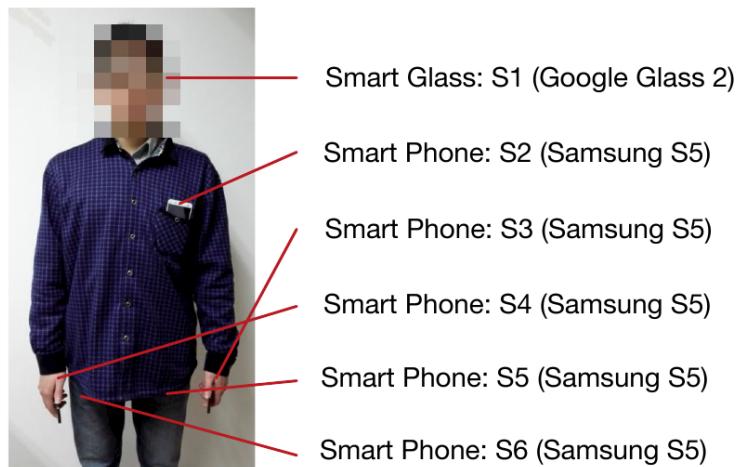


图 4.1: 数据采集设定

4.2.2 室内环境下的磁力计精确度

我们观察到磁力计在典型的室内环境中不太可靠。在磁力计测量和真实的北极的夹角最大可达 110° 。我们在一个典型的包含金属物(如电脑和电子器具)的办公室中，利用Samsung Galaxy S5智能手机测量磁力计读数和真实地球坐标系北极的夹角偏差。磁力计读数是通过投影磁力计读数到地球水平面获得的。我们在 6×10 的网格中的60个位置中分别测量了南北和东西两个方向。任意两个邻接的点的距离是120cm。我们将手机的Y轴对准地球的北极方向。因此，偏角应该等于磁力计算值和Y轴的夹角。图4.2画出了实验结果。我们观察到由于周围金属物体的干扰，偏角有整整 110° 。也就是说磁力计不适合室内环境下的空间同步。

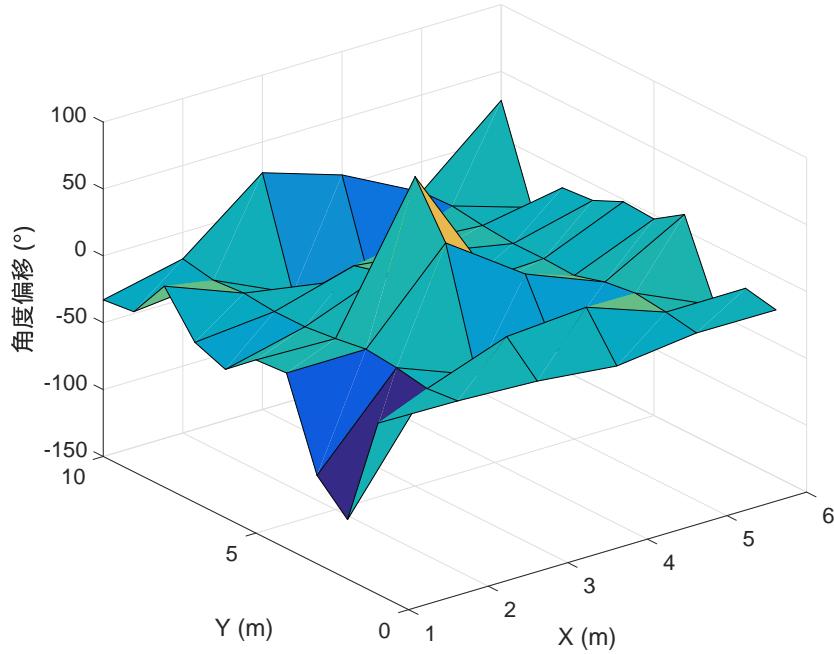


图 4.2: 磁力计精确度测量

4.2.3 人体运动的特征

我们观察到当人装备有多个移动设备向前移动时，不同设备间一致的加速度有相似的方向和大小，但是不一致的加速度有不同的方向和大小。尤其是，在一个大的时间窗口内（比如15秒）人体内部的平均加速度接近0。因为胸口的不一致力基本上可以忽略，我们用一个额外的惯性传感器放置在胸口用于估计真实的一致力。我们将六个设备的加速度读数作为混合的加速度，然后通过抵消一致的加速度从而获得不一致的加速度。为了展示一致和不一致的加速度的方向和大小，我们在地球水平面将它们用向量的形式画出。我们收集了五秒内以100ms为周期的不一致加速度。不失一般性地，图4.3展现了设备 S_1 , S_2 , S_3 , S_6 的一致加速度和不一致加速度的方向和大小。我们用虚线箭头表示一致加速度的方向，实线箭头表示不一致加速度的方向和大小。我们观察到不同设备的一致加速度方向和大小一致。我们也观察到不用设备间的不一致加速度的大小各不相同，因为这取决于人体不同部位的运动幅度大小。我们还观察到不一致加速度的方向基本都是在水平面上分散的，这是由于人体部位（如手臂）前后移动造成人体内部的加速度发生互相偏移。

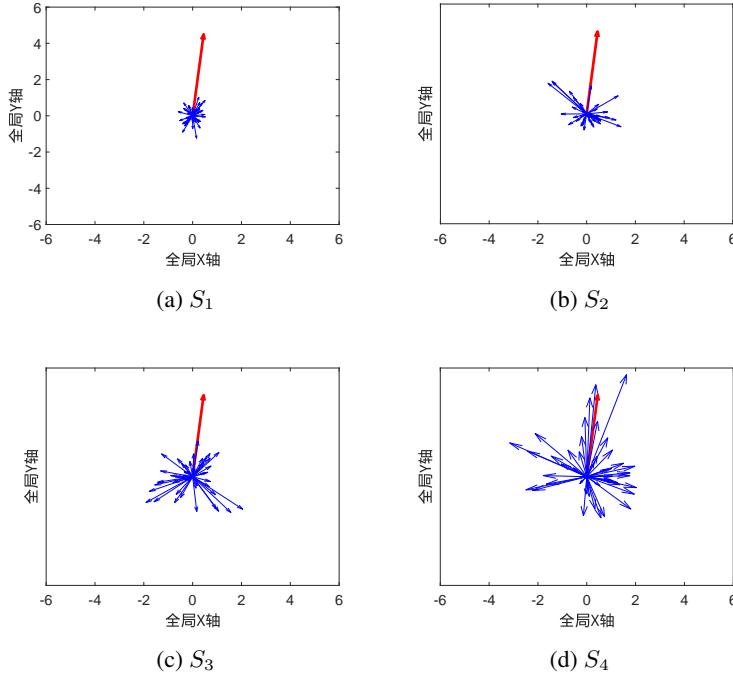


图 4.3: 一致/不一致的加速度在不同设备上的方向和大小

我们现在分析不同设备混合的、一致的以及不一致的加速度的统计特征。图4.4分别展示了混合加速度、一致加速度以及不一致加速度在前后方向以及左右方向的人体运动偏移的平均值和标准差。我们观察到，尽管所有加速度的标准差都差不多大，他们的平均值都相对非常小。左右方向的平均加速度值在三个加速度轴上几乎为 0，而混合加速度以及一致加速度的前后方向上的加速度平均值与不一致加速度的平均值相比而言是比较大的。比如说，混合加速度和一致加速度的平均加速度值的量级是 $10^{-1} m/s^2$ ，而不一致力的平均值的量级是为 $10^{-5} m/s^2$ ，这是因为人体运动一致向前的力在向前运动中占据了主导地位。这说明了不一致力的混合加速度的影响是可以忽略不计的。

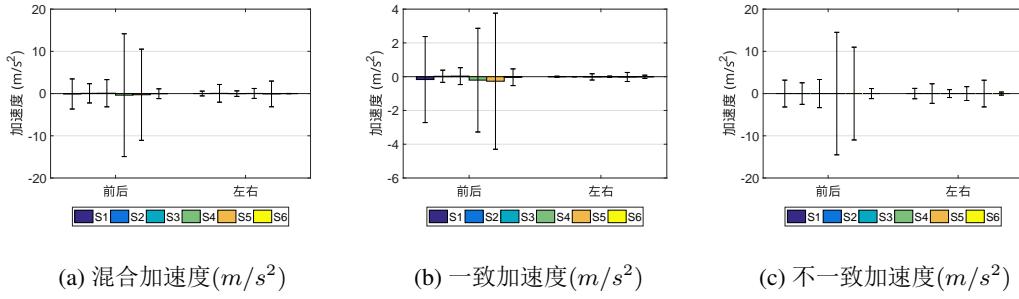


图 4.4: 不同方向加速度的均值和方差

4.2.4 人体运动模型

让 $f_i(t)$ 指代从设备 D_i 在 t 时刻获得的混合加速度。 $f_i(t)$ 包含里一致加速度 $f_c(t)$ 以及不一致加速度 $f'_i(t)$ 。i.e., $f_i(t) = f_c(t) + f'_i(t)$ 。加速度是根据设备的局部坐标系测量的。当人体运动时，局部坐标系相对于地球坐标系进行旋转；所以，测量的加速度不能稳定地描述人体的运动。假设我们可以构造一个相对地球坐标系固定的坐标系。对于固定的坐标系，我们用 $f_{i,x}(t)$ 、 $f_{i,y}(t)$ 以及 $f_{i,z}(t)$ 表示 $f_i(t)$ 分别在x、y以及z轴上的投影，并用 $f'_{i,x}(t)$ 、 $f'_{i,y}(t)$ 、 $f'_{i,z}(t)$ 分别表示 $f'_i(t)$ 在x、y、z轴的投影。 t 时刻 $f_c(t)$ 与x、y、z轴的夹角分别表示为 $\alpha_i(t)$ 、 $\beta_i(t)$ 以及 $\gamma_i(t)$ 。因为 $f_c(t)$ 相对于坐标系有一个固定的方向， $\alpha_i(t)$ 、 $\beta_i(t)$ 、 $\gamma_i(t)$ 都是不随时间变化的固定值。所以， $f_c(t)$ 的方向可以表示为一个单位向量 $\langle \cos\alpha_i, \cos\beta_i, \cos\gamma_i \rangle$ 。用 $f_c(t)$ 指代前进方向的一致加速度的大小；所以它在x、y、z轴上的投影分别是 $f_c(t)\cos\alpha_i$ 、 $f_c(t)\cos\beta_i$ 和 $f_c(t)\cos\gamma_i$ 。在三个轴上的投影如下

$$\begin{cases} f_{i,x}(t) = f_c(t)\cos\alpha_i + f'_{i,x}(t) \\ f_{i,y}(t) = f_c(t)\cos\beta_i + f'_{i,y}(t) \\ f_{i,z}(t) = f_c(t)\cos\gamma_i + f'_{i,z}(t) \end{cases} \quad (4.1)$$

所以，如果我们能够计算 $\cos\alpha_i$ 、 $\cos\beta_i$ 以及 $\cos\gamma_i$ 的值，我们就可以计算一致加速度 $f_c(t)$ 在对应坐标系的方向。而且，对于任何人体内部运动的不一致加速度，我们观察到只要时间窗口足够大，不一致加速度的平均值都趋向于0，下面的定理描述了以上特征：

定理4.2.1.

对于一个相对于地球坐标系固定的坐标系，对于任何由人体内部运动不一致的加速度 $f'_i(t)$ ，在一个足够大的时间窗口 $[t_s, t_e]$ 中，不一致加速度 $f'_i(t)$ 的期望值近

似等于0。也就是说，

$$E[f'_i(t)] = \frac{1}{t_e - t_s} \int_{t_s}^{t_e} f'_i(t) dt \quad (4.2)$$

证明：不失一般性地，我们在x轴上证明这个定理。我们的证明适用于其它坐标轴。让 $\Delta v_{i,x} = \int_{t_s}^{t_e} f'_{i,x}(t) dt$ 。当人体部位前后移动时，人体内部的振幅一般比较小并且任何方向上不会有显著的变化。所以， $\Delta v_{i,x}$ 应该比一个固定的阈值 $C = v_{f,max} + v_{b,max}$ 小的多，其中 $v_{f,max}$ 和 $v_{b,max}$ 分别指代在人体内部运动期间人体部位在前后方向上相对的最大速度。所以，在 $[t_s, t_e]$ 时间窗口内，对加速度 $f'_{i,x}(t)$ 的期望值 $E[f'_{i,x}(t)]$ ，我们有

$$E[f'_{i,x}(t)] = \frac{1}{t_e - t_s} \int_{t_s}^{t_e} f'_{i,x}(t) dt = \frac{\Delta}{t_e - t_s} < \frac{C}{t_e - t_s} \quad (4.3)$$

如果时间窗口 $\Delta t = t_e - t_s$ 足够大，i.e., $\Delta t \gg C$ ，则 $E[f'_{i,x}(t)] \approx 0$ 。定理4.2.1意味着在一个足够大的时间窗口内比如10s，不一致的加速度可以基本忽略，因为不一致的加速度在前后移动期间可以互相抵消，而一致加速度的期望值是不可忽略的，尤其是在人体加速度者减速的期间。这就解释了我们的实验中一致加速度的量级是 $10^{-1} m/s^2$ ，而不一致加速度的量级是 $10^{-5} m/s^2$ 。

4.3 系统设计

图4.5显示了MOSS的系统框架。MOSS包含了两个组件：一个获取空间同步的一致方向估计模块和一个维持空间同步的基于陀螺仪的姿态追踪模块。一致方向估计模块利用主成分分析从多个设备中抽取一致的加速度，然后估计一致加速度的方向。结合从加速度计中抽取的重力方向，它为空间同步生成了一个旋转矩阵。基于陀螺仪的姿态追踪模块利用陀螺仪持续估计局部坐标系的姿态变化。利用全局坐标系中重力加速度的稳定性，我们用最小均方差估计器校准了旋转矩阵。

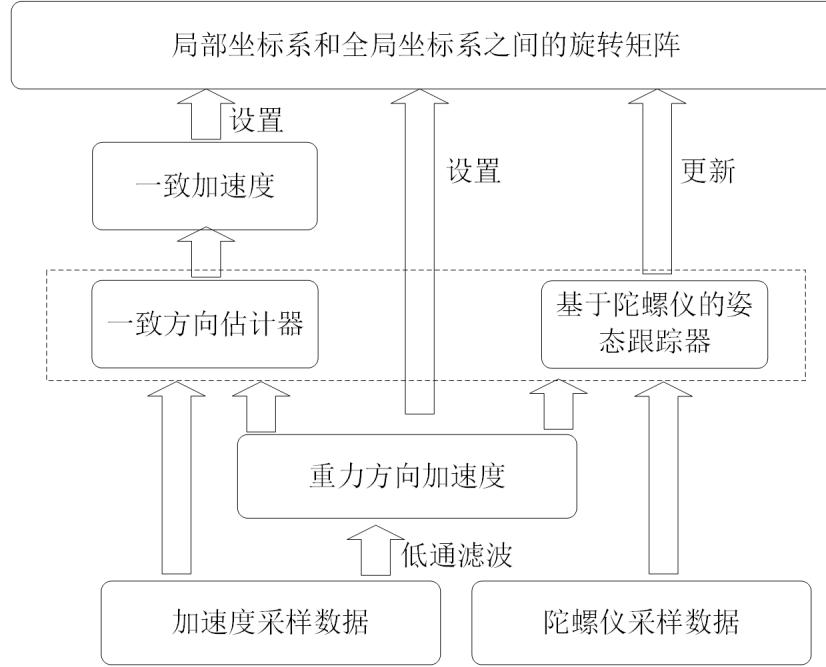


图 4.5: 系统架构

为了在多设备中进行空间同步，MOSS利用一个服务端与这些设备交互信息并且处理相应的数据。我们可以设定其中一个移动设备（比如一个智能手机）作为一个服务端，只要它能够通过wifi与其它设备通信并且有足够的计算能力进行信号处理。MOSS包含如下步骤：

1. **节点广播:** 服务端首先向所有设备广播一个同步的数据包。然后所有的设备在收到同步数据包之后开始记录加速度与陀螺仪。我们将该时刻设为 t_0 。
2. **陀螺仪跟踪的本地测量:** 在一个时间窗口W内的每个时刻t，每个设备 D_i 从局部坐标系的加速度中抽取重力加速度 $g_i(t)$ 以及线性加速度 $f_i(t)$ 。同时，每个设备 D_i 利用陀螺仪抽取每个轴的旋转速度 $\omega_i(t)$ ，然后计算从 t_0 到t时刻的旋转矩阵 $A_{t_0,t}^i$ 。在时间窗口W后，设备 D_i 发送下面的信息到服务端：所有 $t \in W$ 时刻的旋转矩阵 $A_{t_0,t}^i$ ，重力向量 $g_i(t)$ 以及线性加速度 $f_i(t)$
3. **主成分分析:** 在收到所有设备的响应后，服务端利用PCA抽取每个设备在局部坐标系下的一致加速度大小，并且估计它的方向，然后对每个设备在 t_0 时刻构造一个旋转矩阵 $C_{t_0}^i$ ，并发送 $C_{t_0}^i$ 到各个设备。

4. 本地旋转更新：每个设备 D_i 在本地用基于陀螺仪追踪的旋转矩阵 $A_{t_0,t}^i$ 更新旋转矩阵 C_t^i ，也就是 $C_t^i = C_{t_0}^i A_{t_0,t}^i$ 。然后将加速度和陀螺仪的数据从局部坐标系转换到全局坐标系。

4.4 获得空间同步

空间同步的目标是将移动设备的局部坐标系与它们的全局坐标系对齐。我们利用方向余弦表示法去量化局部坐标系和全局坐标系的姿态区别。在方向余弦表示法中，相对于全局坐标系，局部坐标系由 3×3 的旋转矩阵 C 表示，每一列是局部坐标系的一个轴在全局坐标系的单位向量表示。一个在局部坐标系定义的向量 v_l 等于在全局坐标系中定义的向量 $v_g = Cv_l$ 。逆转化是 $v_l = C^t v_g$ ，这是因为旋转矩阵的逆等于它的转置。

对于设备的局部坐标系，假设我们可以从加速度计中抽取一个一致的力 f_c ，并且利用低通滤波器抽取一个一致的重力加速度 g （比如巴特沃斯滤波器[8]），我们可以如下计算旋转矩阵并构建全局坐标系。首先，我们根据重力的方向定义一个水平面。让前进方向 f_c 在水平面的投影方向作为X轴，让重力 g 的反方向作为Z轴。因为X是水平的并且Z是竖直方向的，利用Z轴和X轴的叉乘，我们可以轻松地获得垂直于Z轴和X轴定义平面的Y轴。第二，在我们获得局部坐标系的向量 X_o , y_o 和 z_o 时（它们分别对应于全局的X、Y、Z轴），我们可以推导出旋转矩阵 C^T 。图4.6描述了上述过程。

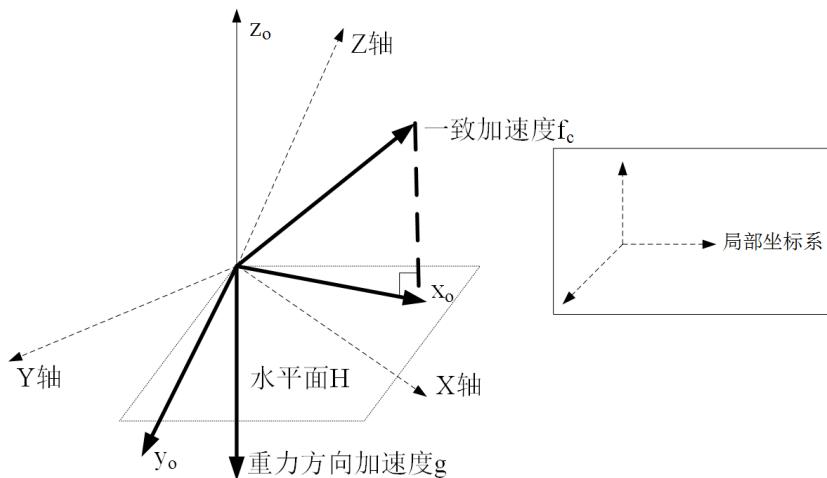


图 4.6: 全局坐标系导出图

4.5 相关力的抽取模型

当多个设备的加速度高度相关时，我们用主成分分析（PCA）抽取向前移动过程期间的一致加速度。这包含了三个步骤：预处理、主成分抽取以及方向估计。

4.5.1 预处理

假定每个设备 D_i 的局部坐标系 $L_i(t)$ 的x、y和z轴的加速度 $f_i(t)$ 可以被获取到，表示为 $\langle x_i(t), y_i(t), z_i(t) \rangle$ 。那么我们可以用旋转矩阵 $(A_{t_0,t}^i)^T$ 将加速度从当前t时刻的局部坐标系 $L_i(t)$ 转换到 t_0 时刻的参考局部坐标系 $L_i(t_0)$

$$\begin{bmatrix} x_i(t_0) \\ y_i(t_0) \\ z_i(t_0) \end{bmatrix} = (A_{t_0,t}^i)^T \begin{bmatrix} x_i(t) \\ y_i(t) \\ z_i(t) \end{bmatrix} \quad (4.4)$$

然后，我们可以获得在不随时间变化的参考局部坐标系，也就是 t_0 时刻的局部坐标系下的加速度数据。

不仅如此，因为我们是在水平面上进行前进方向加速度的抽取，为了避免人体运动期间竖直方向上造成的加速度干扰，我们将线性加速度 $f_i(t)$ 投影到参考局部坐标系的水平面上，如图4.7所示。

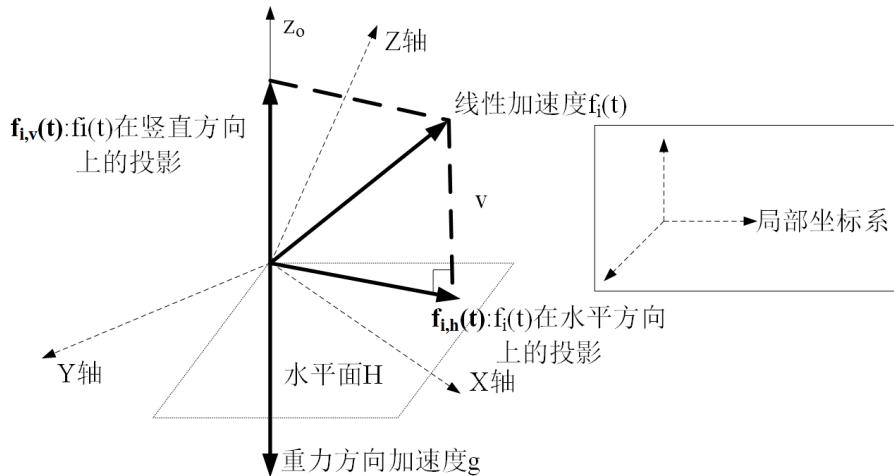


图 4.7: 将加速度 $f_i(t)$ 投影到水平面上

4.5.2 主成分抽取

如公式4.1所示，由于一致加速度 $f_c(t)$ ，多个设备的不同轴的加速度是强烈的相关的。这个现象可以从图4.8看出，我们画出了6个设备三个轴的共18个加速

度流5秒时间内的数据。所以，为了有效地抽取一致加速度 $f_c(t)$ ，我们用PCA从加速度数据流中发现相关性。利用PCA，我们可以在加速度数据中跟踪不同时刻下的相关性，并且抽取这些流的主成分。这包含了下面三个步骤。

- (1) 预处理：假设设备数量为 m ，我们将数据转换成一个 p 列的矩阵 X ，包含了 m 个设备局部坐标系3个坐标轴的加速度数据，其中 $p = 3 \times m$ 。矩阵 X 的每一列对应在一个大小为 n 的采样窗口下的加速度数据流。我们选择默认的采样窗口为10秒，因为人体运动的采样过程不应该太长，同时采样的数量必须足够大以确保准确的相关性估计。矩阵 X 的维度为 $n \times p$ 。我们先计算数据矩阵 X 每一列的均值 μ_i ，然后再从每列 ($i = 1 \dots p$) 中减掉均值向量 μ_i 。
- (2) 协方差估计：我们计算协方差矩阵为 $X^T \times X$ 。协方差的维度是 $p \times p$ ，其中 p 是加速度数据流的数量。然后，我们获取协方差矩阵的特征向量和特征值，并用公式 $x_j = X \times q_j$ 构造主成分，其中 q_j 和 x_j 分别是第 j 个特征向量以及第 j 个主成分。
- (3) 一致的前进方向加速度抽取：我们选择第一个主成分 x_1 去估计一致加速度的大小。然后，我们在图4.9中画出PCA结果与真实的一致加速度比较。根据实验结果，PCA结果和真实值的相关性高达0.961，这意味着我们可以利用PCA准确地抽取一致的加速度。

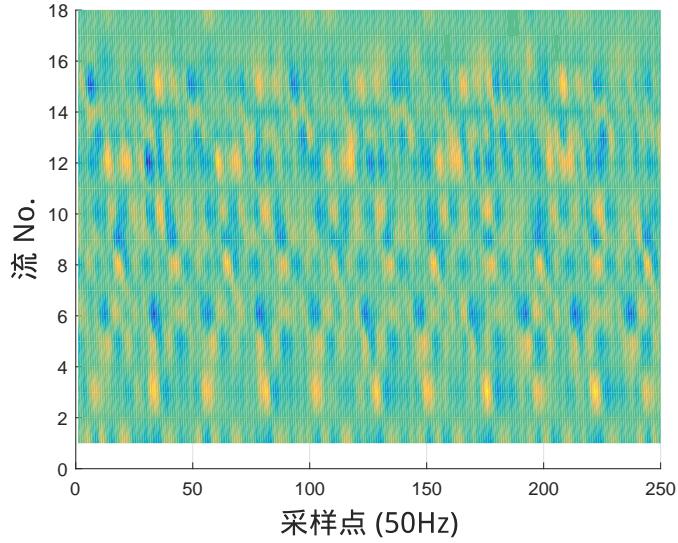


图 4.8: PCA分析图

4.5.3 方向估计

在主成分分析后，我们获得了一致加速度 $f_c(t)$ 的大小，如图4.9所示。已知 $f_c(t)$ 相对于参考坐标系有一个固定的方向。在人体移动期间， $f_c(t)$ 的大小一

直沿着这个固定的方向变化。然后，如果我们设定 $f_c(t)$ 沿着这个固定的方向为正，则沿着该固定方向反方向为负。下一步，对于每个设备 D_i ，我们需要估计 $f_c(t)$ 在局部坐标系的方向。

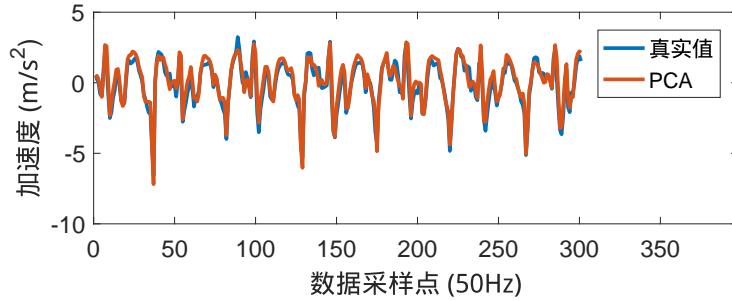


图 4.9: PCA 估计结果 vs 真实值

根据定理4.2.1，在一个足够大的时间窗口下，人体内部不一致加速度（IA）的期望近似等于0。相比与前进方向的一致加速度，它可以被当做白噪声，这是因为它的大小量级小于一致加速度的大小量级。所以，为了抽取不同轴上的一致加速度（CA）成分，同时消除来自不一致加速度（IA）的干扰，我们可以选择一个足够大的时间窗口，累加每个轴的加速度数据，然后获得各相应轴的成分估计。然而，我们需要处理下面的问题：如图4.9所示，让人体向前运动时，一致加速度 $f_c(t)$ 在向前运动的一步过程中不断的在0点上下变化。不仅如此，在宏观的视角，人体运动的速度一般保持恒定且不会变化太多。这意味着当人体以一个几乎恒定的速度移动时，这 $f_c(t)$ 的期望值应该接近于0。在这个问题下，尽管一致加速度 $f_c(t)$ 比不一致加速度 $f'_i(t)$ 的幅度要大，当我们累加一致加速度（CA）时，正负的成分互相抵消到达了一个足够小的值，这导致我们无法区别一致加速度（CA）和不一致加速度（IA）。

幸运的是，由于我们可以通过主成分分析获得 $f_c(t)$ 的幅度变化，利用类似线性差值的技术，我们可以区分 $f_c(t)$ 为正的区间，我们称这些时间为正向时间区间。类似地，当 $f_c(t)$ 值是负的时候，我们称这些时间为负时间区间。图4.10展示了一个根据PCA结果选出的正时间区间。然后，对于每个轴，不失一般性地，我们仅仅累加正时间区间的加速度数据来抽取一致加速度 $f_c(t)$ 的累积正向加速度。根据公式4.1，对已累加的加速度数据， $f_c(t)$ 正向累加幅度大小远大于不一致加速度 $f'_i(t)$ 的累加加速度大小（趋近于0）。利用这种方法，根据 $f_c(t)$ 在不同轴的正向幅度，我们能够估计局部坐标系下的 $f_c(t)$ 的方向。

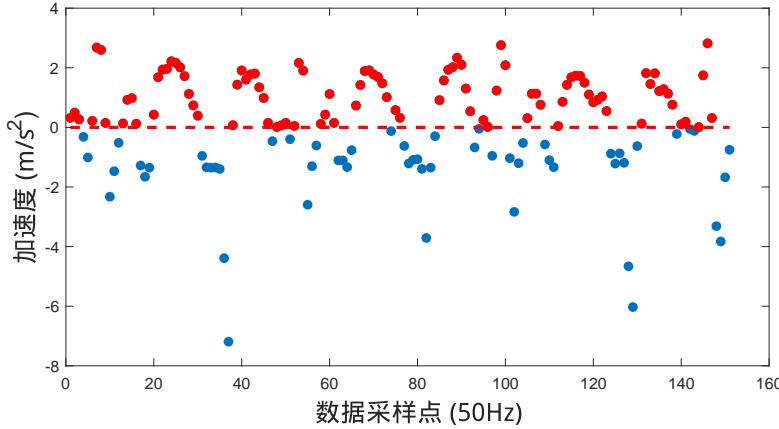


图 4.10: 根据PCA结果识别正向加速度的时间区间

因为一致加速度 $f_c(t)$ 相对于地球坐标系有一个固定的方向，这个方向相对于参考局部坐标系也是固定的。在参考局部坐标系中，令 $f_c(t)$ 与 x 、 y 与 z 轴的夹角分别为 α_i 、 β_i 、 γ_i 。它们应该都是固定值。 $f_c(t)$ 的方向可以用一个单位向量 $\langle \cos\alpha_i, \cos\beta_i, \cos\gamma_i \rangle$ 表示。根据定理4.5.1，我们可以估计 $f_c(t)$ 的方向。

定理4.5.1.

令 α_i 、 β_i 和 γ_i 分别为一致加速度 $f_c(t)$ 与参考局部坐标系 x 、 y 和 z 轴的夹角。令 $f_c(t)$ 为向量 $f_c(t)$ 的大小， $f_{i,x}(t)$ 、 $f_{i,y}(t)$ 、 $f_{i,z}(t)$ 分别为加速度数据在 x 、 y 和 z 轴的加速度数据。然后 $\cos\alpha_i$ 、 $\cos\beta_i$ 和 $\cos\gamma_i$ 可以被如下估计：

$$\begin{cases} \cos\alpha_i = \frac{E[f_{i,x}(t)]}{E[f_c(t)]} \\ \cos\beta_i = \frac{E[f_{i,y}(t)]}{E[f_c(t)]} \\ \cos\gamma_i = \frac{E[f_{i,z}(t)]}{E[f_c(t)]} \end{cases} \quad (4.5)$$

证明：不失一般性地，我们证明等式 $\cos\alpha_i = \frac{E[f_{i,x}(t)]}{E[f_c(t)]}$ 。根据公式4.1，对于 x 轴， $f_{i,x}(t) = f_c(t)\cos\alpha_i + f'_{i,x}(t)$ 。我们在一个足够大的时间窗口 W_p 下正向时间区间中获得 $f_{i,x}(t)$ 的序列，这些正时间窗口的 $f_{i,x}(t)$ 的和可以被如下描述：

$$\sum_{t \in W_p} f_{i,x}(t) = \sum_{t \in W_p} [f_c(t) \cdot \cos\alpha_i] + \sum_{t \in W_p} f'_{i,x}(t). \quad (4.6)$$

根据定理4.2.1， $\sum_{t \in W_p} f'_{i,x}(t)$ 应该近似等于0。而且，由于 $f_c(t)$ 的值是从正向时间区间抽取的， $\sum_{t \in W_p} [f_c(t) \cdot \cos\alpha_i] \gg \sum_{t \in W_p} f'_{i,x}(t)$ 。然后

$$\sum_{t \in W_p} f_{i,x}(t) \approx \sum_{t \in W_p} [f_c(t) \cdot \cos\alpha_i]. \quad (4.7)$$

而且，由于 $\cos\alpha_i$ 是一个常量，则

$$\cos\alpha_i \approx \frac{\sum_{t \in W_p} f_{i,x}(t)}{\sum_{t \in W_p} f_c(t)} \approx \frac{E[f_{i,x}(t)]}{E[f_c(t)]}. \quad (4.8)$$

所以 $\cos\alpha_i$ 的估计，也就是 $\hat{\alpha}_i$ 应该等于 $\frac{E[f_{i,x}(t)]}{E[f_c(t)]}$ 。类似地，我们可以证明 $\cos\beta_i = \frac{E[f_{i,y}(t)]}{E[f_c(t)]}$ 以及 $\cos\gamma_i = \frac{E[f_{i,z}(t)]}{E[f_c(t)]}$ 。

所以，根据定理4.5.1，我们估计 $f_c(t)$ 方向的解决方案如下所述：首先，我们选择一个足够大的时间窗口取获得相应的PCA结果，然后从PCA结果中找出加速度大于0的区间作为正向时间窗口。然后对于参考局部坐标系，我们计算在上述正向时间区域的加速度数据的期望值。在那之后，我们可以根据公式4.5计算角速度 α_i 、 β_i 和 γ_i ，然后就可以估计 $f_c(t)$ 的方向。因为 $E[f_c(t)]$ 的值在公式4.5所有的三个方程式中都相等，所以实际上没有必要去计算 $E[f_c(t)]$ 的值。实际上，根据前面的分析，我们有 $\sqrt{E[f_{i,x}(t)]^2 + E[f_{i,y}(t)]^2 + E[f_{i,z}(t)]^2} \approx E[f_c(t)]$ 。

4.6 基于陀螺仪的姿态跟踪扩展

4.6.1 运动时陀螺仪的精确度

我们观察到陀螺仪在包括水平和竖直的所有方向上追踪的误差会随着时间的增加进行累积。而且，线性加速度越大，陀螺仪追踪的累积误差越大。为了评估陀螺仪的追踪误差，我们持续收集陀螺仪的读数并且用[24]中的方法计算旋转矩阵。因为重力和磁力方向在地球坐标系中是固定的，我们分别用重力和磁力方向作为竖直和水平方向的基准。然后我们比较了从旋转矩阵获得的重力 / 磁力计的方向以及真实重力 / 磁力的方向。图4.11显示了陀螺仪随着时间增加在重力和磁力方向上的角度偏移情况。不失一般性地，我们展示了设备 S_3 和 S_6 的陀螺仪误差。我们观察到陀螺仪的追踪误差在两个方向上有累积误差。因为我们在人体不同部位上放置设备，这些设备的角速度和线性加速度是不同的。这也导致了不同的跟踪误差。比如说，在60秒后，设备 S_3 的在水平方向上平均追踪误差为 23° ，而设备 S_6 在水平面上的平均追踪误差为 50° ，这是因为腿部的角速度和线性加速度一般大于手部摇摆。而且，当角速度和线性加速度增加时，平均追踪误差也会增加。比如说，设备 S_6 在竖直方向的追踪误差为 27° ，在水平方向上的累积误差为 50° 。水平方向的追踪误差明显大于竖直方向上的追踪误差，这是因为人体运动的方向是在水平面上的。

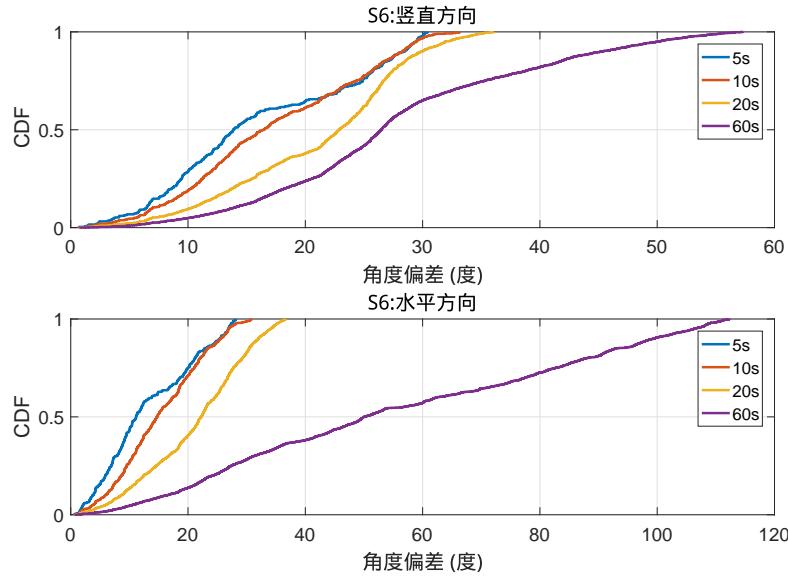


图 4.11: 陀螺仪的角度偏移情况

4.6.2 基于旋转的模型

因为利用陀螺仪获得的角速度信息积分去追踪与更新旋转矩阵，陀螺仪信号的误差会传播到计算的姿态误差中，时间增加时会导致很大的累积误差。前进方向的角速度和线性加速度越大，在各个方向上的追踪误差 $e_x(t)$ 、 $e_y(t)$ 、 $e_z(t)$ 就会越大。所以基于陀螺仪的跟踪所推导的旋转矩阵 $A_{t,t+\delta t}$ 在长时间之后会造成很大的累积误差。因此，利用其它测量方法（比如加速度计测量）来进行更好的校准是非常有必要的。

我们的解决方案是基于这样一个观察现象：抽取的重力向量在全局坐标系中是稳定的。这个观察将被用于校准基于陀螺仪跟踪得到的旋转矩阵 $\hat{A}_{t,t+\delta t}$ 。对于设备 D_i ，假设重力向量在 t 时刻的局部坐标系 $L_i(t)$ 中的向量表示为 $g = \langle g_x(t), g_y(t), g_z(t) \rangle$ 。那么在追踪一段时间后，重力向量可以表示为在 $t + \delta t$ 时刻局部坐标系 $L_i(t + \delta t)$ 下的一个不同的向量 $g' = \langle g_x(t + \delta t), g_y(t + \delta t), g_z(t + \delta t) \rangle$ 。 g 和 g' 向量之间的不同是由于时刻 t 到时刻 $t + \delta t$ 的局部坐标系旋转造成的，我们令这个旋转矩阵为 $A_{t,t+\delta t}$ 。所以，我们有 $g' = A_{t,t+\delta t}g$ 。根据以上的关系，旋转矩阵 $A_{t,t+\delta t}$ 可以被如下计算。注意到由于局部坐标的旋转，向量 g' 和向量 g 之间可能存在 0 到 θ 的角度，这个计算方式为： $\theta = \arccos\left(\frac{g \cdot g'}{\|g\| \|g'\|}\right)$ 。其中 \cdot 操作是指两个向量的内积。在旋转过程中，为了将向量 g 和向量 g' 对齐，必须绕着轴 \mathbf{u} 旋转一个 θ 的角度。其中旋转轴 u 垂直于向量 g 与 g' 所在平面。所以，旋转轴 u 可以

通过计算 g 与 g' 的叉乘得到：

$$u = \frac{g \times g'}{\|g \times g'\|}. \quad (4.9)$$

我们称上述的旋转为竖直方向的旋转。所以，根据Rodrigues' 旋转公式[28]，我们计算出对应的旋转矩阵 R 为：

$$R = I + (\sin\theta)U + (1 - \cos\theta)U^2 \quad (4.10)$$

其中 I 是一个 3×3 的矩阵， U 代表向量 u 的叉乘矩阵。

到现在为止，我们已经利用局部坐标系从前一个时刻的重力向量 g 在竖直方向上旋转到当前时刻的重力向量 g' 获得了相应的旋转矩阵。但是，在水平面上仍然存在其它的自由度，这是因为局部坐标系可以在水平面上绕着当前的重力向量 g' 旋转任意的角度 θ' 。所以，我们需要进一步计算在水平面上旋转矩阵 R' 的旋转角 θ' ，才能更好地估计旋转矩阵 $A_{t,t+\delta t}$ 。因为局部坐标系是绕着当前的重力向量 g' 旋转的，所以旋转轴可以被定义为重力向量 g' 的单位向量。根据Rodrigues旋转公式，假定水平面的旋转脚为 θ' ，我们可以如下计算对应的旋转矩阵 $R'(\theta')$ ：

$$R'(\theta') = I + (\sin\theta')U' + (1 - \cos\theta')U'^2 \quad (4.11)$$

其中 I 是一个 3×3 的矩阵， U' 指代向量 u' 的叉乘矩阵。我们称上面的旋转为水平方向上的旋转。所以，旋转矩阵 $\hat{A}_{t,t+\delta t}$ 可以被如下估计：

$$A_{t,t+\delta t}(\theta') = RR'(\theta') \quad (4.12)$$

4.6.3 利用MMSE估计进行校准

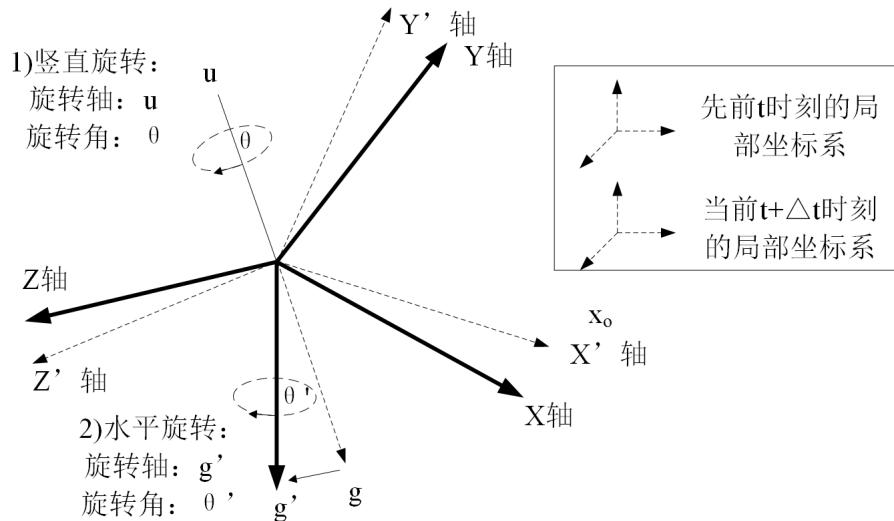


图 4.12: 估计旋转矩阵 $A_{t,t+\delta t}$

根据4.2.1节的观察以及4.4节的分析，我们知道在一个长的时间追踪之后，对于陀螺仪跟踪估计的旋转矩阵 $\hat{A}_{t,t+\delta t}$ 会有一个很大的误差。幸运的是，我们已经从基于旋转的模型中计算了一个旋转矩阵 $A_{t,t+\delta t}(\theta')$ 。由于重力向量可以通过类似巴特沃斯滤波器的低通滤波器中准确地抽取出来，我们实际上获得了一个带一个未知变量 θ' 的关于旋转矩阵 $A_{t,t+\delta t}$ 的公式。所以，为了根据陀螺仪追踪估计的 $\hat{A}_{t,t+\delta t}$ 去估计旋转角度 θ' ，我们利用了最小均方差错误估计器（MMSE）。我们将估计误差矩阵定义为 $E = \hat{A}_{t,t+\delta t} - A_{t,t+\delta t}$ ，其中最小均方误差（MSE） e 为：

$$e(\theta') = \sum_{i=1}^3 \sum_{j=1}^3 (E_{i,j}(\theta'))^2 = \sum_{i=1}^3 \sum_{j=1}^3 (\hat{A}_{i,j} - A_{i,j}(\theta'))^2 \quad (4.13)$$

然后我们计算 θ' 的最优值，使得估计的 $\hat{A}_{t,t+\delta t}$ 获得最小的均方误差：

$$\theta'^* = \operatorname{argmin}_{\theta'} e(\theta') \quad (4.14)$$

然后，在计算这个最优值 θ'^* 之后，我们将旋转矩阵 $A_{t,t+\delta t}(\theta'^*)$ 作为旋转矩阵 $A_{t,t+\delta t}$ 的校准后的估计值。

4.7 实现与评估

4.7.1 实现

硬件：我们在6个移动可穿戴设备上实现了MOSS：一个智能眼镜（Google Glass 2）和五个智能手机(SAMSUNG Galaxy S5)。图4.1显示了它们是在人体上放置的位置。这些设备通过蓝牙4.0接口连接到一个安卓智能手机(SAMSUNG Galaxy S5)。这个安卓手机持续收集这些设备的加速度和陀螺仪数据，然后处理这些数据。

软件：我们用JAVA语言在安卓智能手机上以可执行软件的形式实现了MOSS框架。我们的软件对来自多个设备的惯性传感器数据进行信号处理，然后运行章节4.5和章节4.6描述的空间同步算法。图4.13显示了运行在Samsung S5智能手机上的MOSS图形用户界面。4.13a展示了放置在人体不同部位手机的3D图。为了更清楚地展示，我们分别用蓝色和红色显示了地球坐标系和同步坐标系。然后我们显示了在地球坐标系中手机的局部坐标系，同时展示了对应的旋转矩阵。在这种方式下，我们可以检查不同设备之间两个坐标系的夹角是否相近，以检验空间同步的效果。图4.13b展示了在它们同步坐标系下不同设备的加速度数据。这样，我们可以描述不同设备在它们对齐的3D坐标系下的加速度数据。

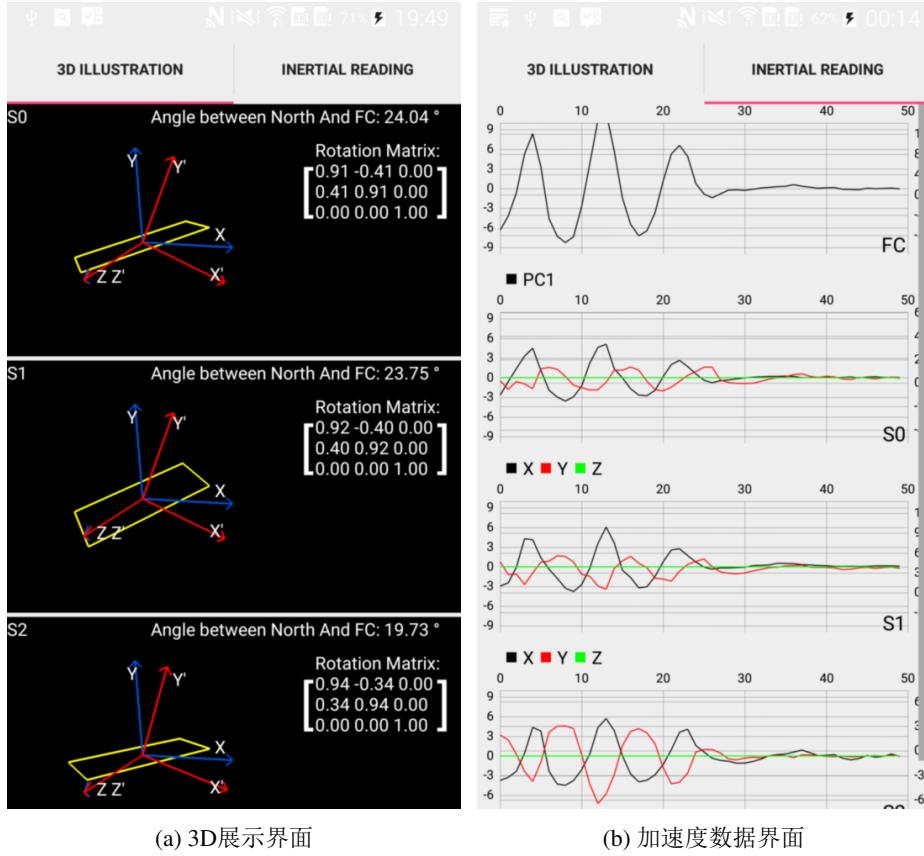


图 4.13: 安卓手机上的MOSS界面

4.7.2 实验设置与标准

在实验中，我们让5个志愿者在室外沿着3条不同的直线路径行走，如图4.14所示。它们用三种不同的模式沿着路线行走：1) 走路：人以正常速度（0.5~1m/s）小幅度地行走；2) 跑步：人以较快的速度（2~3m/s）大幅度地跑步；3) 跳跃：人体大幅度地向前跳跃。对于每个路线每个移动模式，我们分别收集了20次数据。每次数据收集，我们持续采集30秒所有设备的加速度、陀螺仪和磁力计数据。我们总共收集了120条轨迹的惯性传感器数据。为了与真实值比较验证效果，我们从惯性传感数据中抽取了磁力方向和重力方向并利用它们构建地球坐标系作为参考坐标系E。我们用两个标准去评估MOSS算法：(1) 角度的准确度：估计的前进方向与其真实值的夹角；(2) 坐标系准确度：同步坐标系的数据与其真实值的相关性。

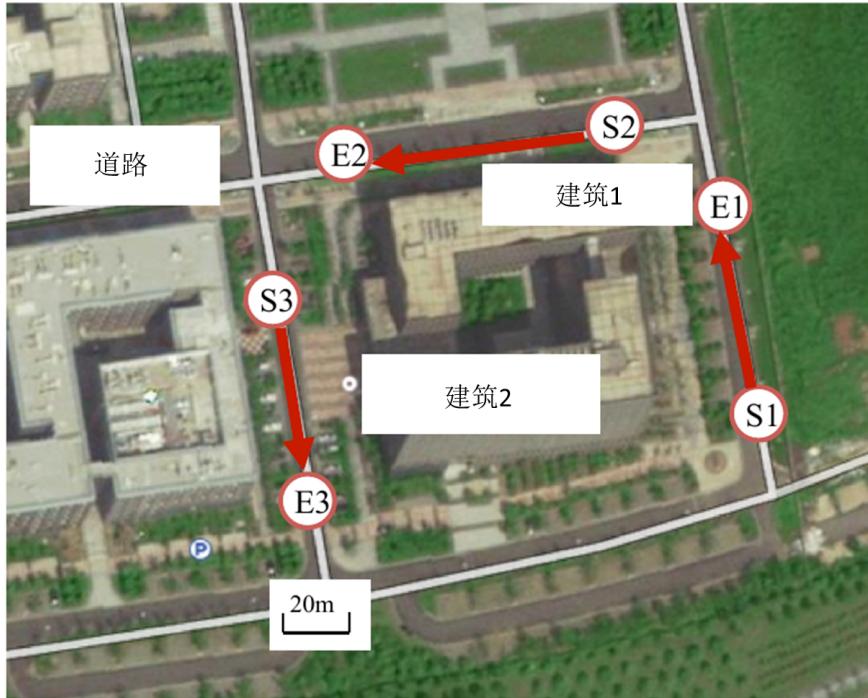


图 4.14: 实验环境

4.7.3 前进方向估计

为了评估一致前进方向的准确度，我们首先以如下方法获得前进方向的真实值。因为每一条实验轨迹都是一个直线，我们将一个智能手机放在道路上，并将其局部坐标系的y轴对准路径方向，然后每隔100米用内置的磁力计测量道路上的磁场方向。这样，通过计算局部坐标系y轴和磁场方向的平均夹角，我们可以获得前进方向的真实值，而且，根据重力向量和前进方向，我们可以构建真实的全局坐标系 G 。为了比较实验性能，我们将我们的解决方案与两个启发式的解决方案比较，1) MeanACC: 它通过在一个时间窗口内分别对局部坐标系的三个轴上的加速度数据进行平均，从而得到前进方向的估计值，这个解决方案在运动过程中设备局部坐标系变化不大时比较有效；2) RefMeanACC: 它通过在一个时间窗口内分别对参考局部坐标系的三个轴上的加速度数据进行平均，从而得到前进方向的估计值，这个解决方案利用了陀螺仪的追踪，即使设备的局部坐标系一直变化也是有效的。

实验结果显示MOSS算法在所有时间窗口，所有运动模式以及所有设备中都获得了很好的角度准确度。我们首先在人体以普通行走模式下评估MOSS。图4.15a画出了前进方向与真实方向的偏角，其中我们展示了所有6个设备偏角的平均值和标准差。对于MOSS，6个设备的平均偏角均小于15°，同

时标准值均小于 9° 。对于MeanAcc和RefMeanAcc两者，平均角度偏差都远大于MOSS。进一步，我们分别在走路、跑步和跳跃的模式下评估平均角度偏差，如图4.15b所示。我们观察到MOSS在所有三种运动模式下都获得较好的效果，这表明MOSS对实际的运动方式并不敏感。值得一提的是，MOSS在跳跃模式下获得了最好的性能，这是因为跳跃产生了更大的一致向前的加速度，这有助于空间的同步。在跑步模式下的性能有一定程度的下降，这是因为跑步时四肢的大幅度移动产生了更大的不一致力。我们分别在1到9s秒的采样时间窗口下评估了平均角度偏差，如图4.15c所示。当采样窗口增加时，MOSS在某些设备中获得了一些角度偏差的增加，这是因为一致前进方向发生了一定变化。

实验结果显示MOSS获得了很好的坐标系准确度。对于所有设备，所有运动模式以及所有时间窗口大小，MOSS都可以获得一个较高的数据相关性。我们首先评估人体走路时的效果。图4.15d画出了同步坐标系下的数据与真实数据的相关性。对于MOSS，6个设备的相关性均大于95%，平均相关性为97%。对于MeanACC，大部分相关性都小于60%，其中 S_4 的相似度甚至为49%。对于RefMeanACC，效果有一定程度地提升，然而，平均相似度仅为73%。我们进一步评估在不同运动模式下的数据相关性，如图4.15e所示，MOSS在所有三个模式下都获得了比较好的相关性。我们还分别评估了1s到9s的时间窗口下数据的相关性，如图4.15f所示。当采样窗口为3秒，且其它参数都设定为最优情况时，所有设备能够获得最好的性能。

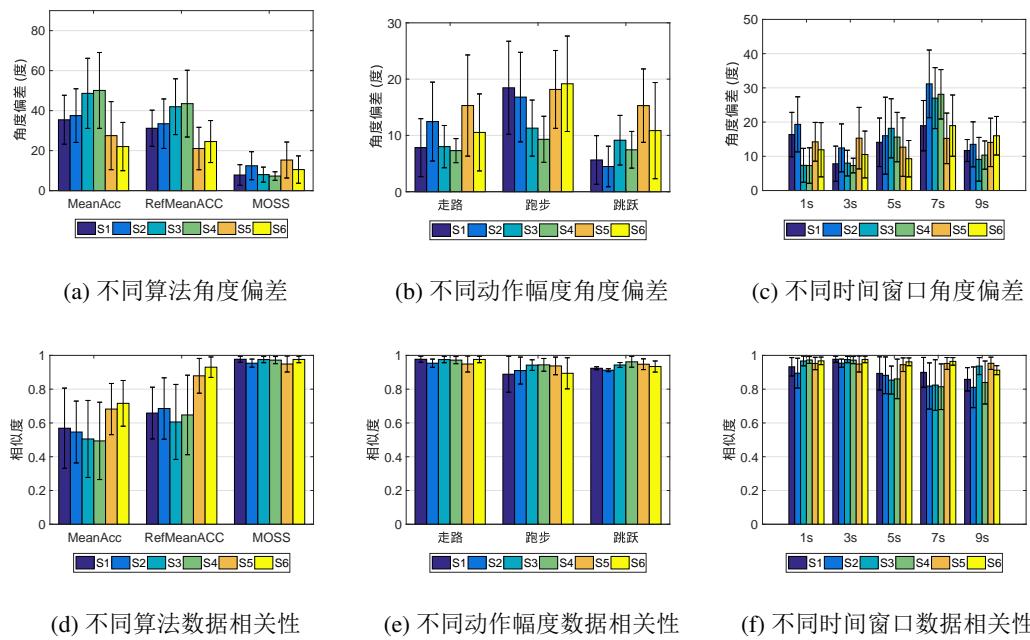


图 4.15: 评估一致前进方向估计的准确性

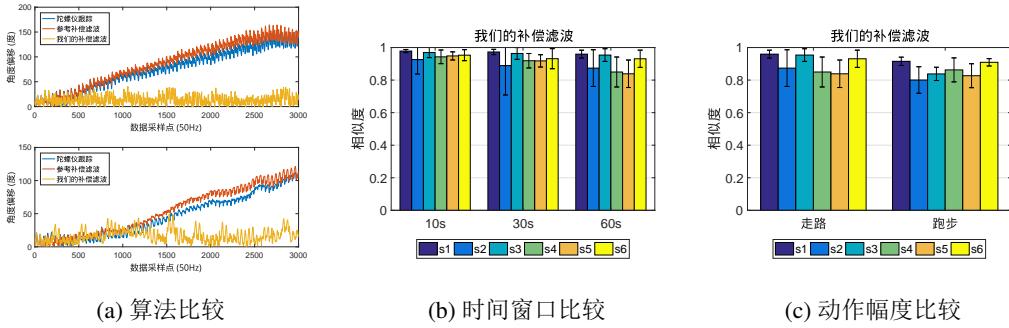


图 4.16: 评估基于陀螺仪追踪的准确性

4.7.4 基于陀螺仪的追踪

为了评估基于陀螺仪的追踪性能，我们实现了如下的解决方案用于性能比较：1) 陀螺仪追踪：完全基于陀螺仪数据进行姿态追踪的框架。2) 参考的补偿滤波：一个普通的结合加速度和陀螺仪进行追踪姿态的补偿滤波[23]。3) 补偿滤波：章节4.6描述的我们的补偿滤波解决方案。

实验结果显示MOSS获得了很好的角度准确度。特别的，MOSS在不同的移动模式以及不同的时间窗口下，对于基于陀螺仪的追踪能够有效地控制累积误差。为了评估不同的解决方案下的累积误差，我们分别评估了重力和磁力方向的偏角。为了测量竖直方向和水平方向的累积误差，实验的计算均在参考坐标系下进行。图4.16a画出了竖直方向和水平方向的累积误差。不失一般性地，我们选择设备 S_4 的数据作为例子。我们观察到在两个方向下，基于陀螺仪追踪的误差和参考补偿滤波的误差随着时间增加不断增加，而我们的补偿滤波的误差随着时间增加不会累积。在30秒之后，前面两个解决方案的误差超过了 110° ，而我们解决方案的误差不超过 20° 。

实验结果显示MOSS能够获得很好的坐标系准确度。特别地，MOSS算法在不同的移动模式和不同的时间窗口下，对基于陀螺仪追踪能够获得一个很高的数据相关性。如图4.16b所示，我们评估了不同时间窗口大小下同步坐标系中的数据与真实数据的相关性。随着时间窗口大小增加，我们观察到陀螺仪追踪和参考补偿滤波器得到的数据相关性不断地减少，而我们解决方案的数据相关性维持在一个较高的水平。如图4.16c所示，我们还在不同的运动模式下评估了数据相关性。对于跑步模式，陀螺仪和参考补偿滤波器的数据相关性相比较行走模式有大幅度地下降，这是因为大的角速度和线性加速度引起的误差累积。然而，MOSS在行走模式和跑步模式下都能维持一个较高的数据相关性。

4.8 案例

4.8.1 通过摇晃手机进行空间同步

我们首先用简单的动作对多个设备进行空间同步，也就是用一个一致的加速度对多个设备一起摇晃。在摇晃过程中，除了相对偏移造成轻微的不一致加速度，多个设备受摇晃动作的近乎一致的加速度影响。在这个案例研究中，不失一般性地，我们将手机以三种不同的形式摆放，如图4.17c所示，然后沿着一个特定的方向前后摇晃这些设备。为了更直观地评估算法性能，在这个案例研究中，我们用一个新的标准代替4.7.2章节中提到的角度准确度进行评估。具体来说，在案例“局部坐标系重叠”和“局部坐标系平行”中，由于多个设备的局部坐标系有同样的平面，我们将两个手机局部坐标系的x轴的夹角作为评估标准；在“局部坐标系相交”案例中，由于多个设备的局部坐标系有不同的平面，我们用设备局部坐标系的z轴夹角，也就是不同平面间的夹角，作为评估标准。



图 4.17: 多个设备以不同的部署进行摇晃

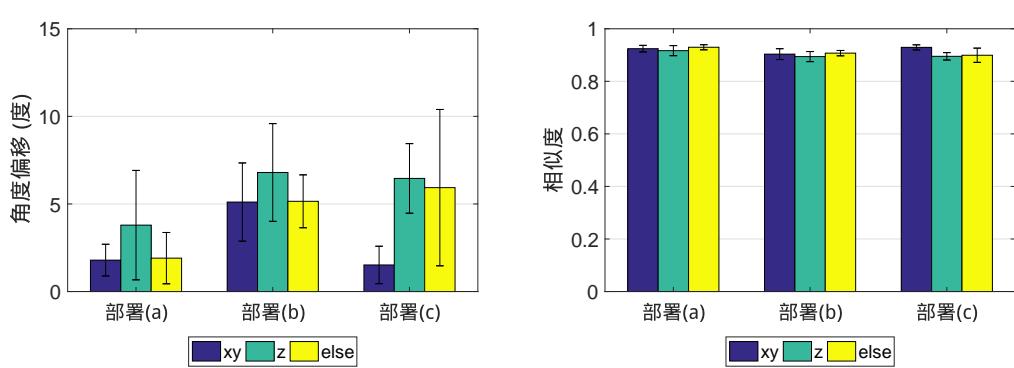


图 4.18: 评估角度的大小和相似度

4.8.2 利用人的行走/跑步/跳跃进行空间同步

我们在一个更加复杂的场景下对空间进行同步，具体地，人体在他/她身体上的不同部位戴上6个移动设备，然后随意在室外环境下进行走路、跑步、跳跃和休息的复合动作，具体运动顺路如图4.19所示。与4.7.2章节的实验设置类似，我们让志愿者在室外环境下沿着不同的直线运动。唯一的不同点是人体的运动可以是走路、跑步、跳跃的任意一种模式。我们利用人向前走时一致的加速度去获得空间的同步。而且，在移动过程中，人体可以停止前进然后进行休息，但他/她的手臂依然在动。当人体停止向前移动时，我们用陀螺仪维持空间同步。我们共收集了5个志愿者共30条轨迹的数据取评估性能。类似地，我们用角度准确度和坐标系准确度取评估实际的性能。

不失一般性地，我们选择了一个样例轨迹然后针对其中一个设备 S_2 ，然后持续监控MOSS框架的角度/坐标系准确度。采样窗口设置为3s。图4.19显示了具体运动的时间区间以及相应的实验结果。对于角度准确度，我们发现角度偏移随着时间增加持续变化。在走路、跑步、跳跃的时间窗口下，平均角度偏差为9°。在休息的时间窗口期间，角度偏差随着时间轻微增加，这是由于缺乏一致加速度造成的。不仅如此，所有的角度偏移均小于18°。对于坐标系准确度，我们发现相似度一直随着时间变化，而且均大于81%。



图 4.19: 人体的复合运动

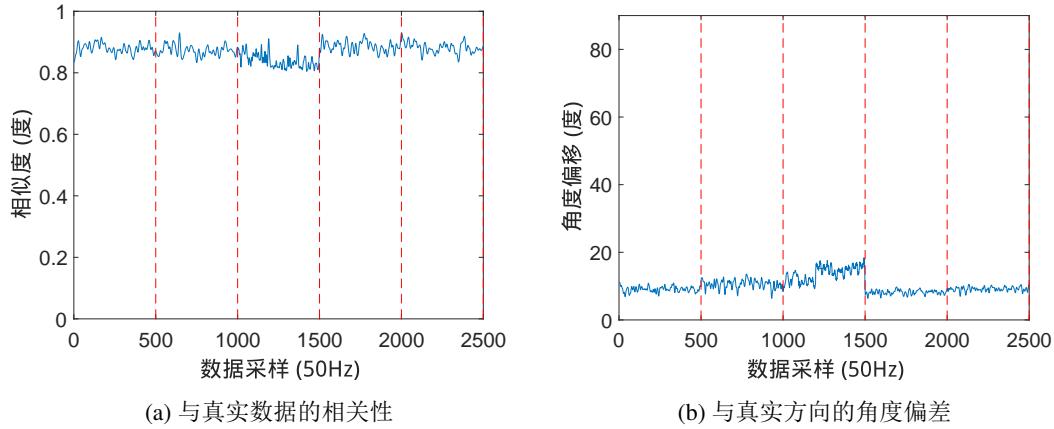


图 4.20: 复合运动实验结果

然后我们分别用一种统计性的方法评估了一致前进方向估计 (CFDE) 以及基于陀螺仪姿态追踪 (GOT) 的性能。图4.20显示了在复合移动过程的实验结果。如图4.21a所示，对于CFDE的性能，即使移动过程包含了多种运动类型，所有设备的角度准确性均小于 17° ，平均角度准确度为 12° 。在图4.21c中，所有设备的坐标系准确度均大于87%，平均坐标系准确度为91%。对于GOT的性能，这时人体停止移动，我们评估了30秒的准确度。如图4.21b所示，即使是时间区间有30s这么大，所有设备的角度准确度小于 26° ，平均角度准确度为 21° 。在图4.21d中，所有坐标系的准确度均大于80%，而坐标系准确度为84%。

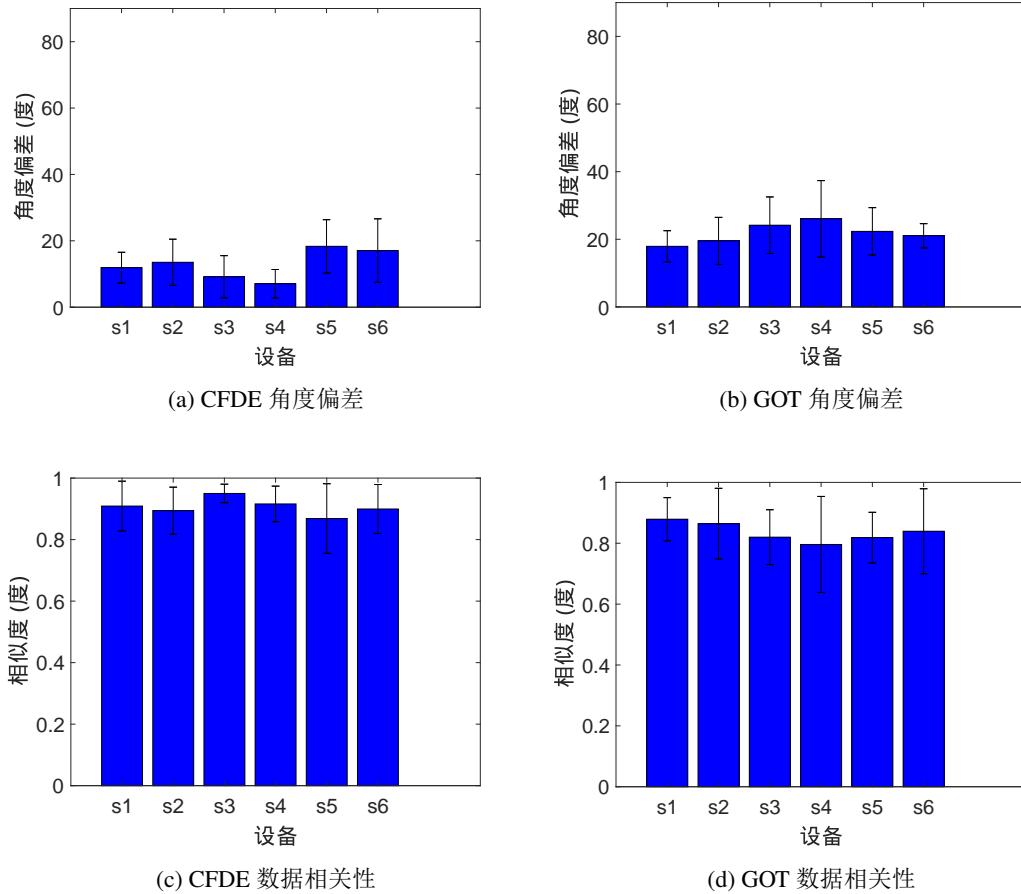


图 4.21: 评估CFDE和GOT的准确性

4.9 本章小结

本章首先定义了多移动设备空间同步的概念，接着对人体运动进行了研究和分析，建立了人体运动的模型，然后提出了用来在多移动设备之间获得空间同步的MOSS框架。特别地，我们提出了一个可以用来获得空间同步的一致方向估计器，然后扩展优化了基于陀螺仪的姿态跟踪器，并且用它来维持空间同步。本章在COTS移动设备上实现了MOSS框架，最后实验结果显示我们的MOSS框架可以获得 6.8° 的平均角度偏差以及93%的平均相似度。

第五章 总结与展望

5.1 总结

近年来，可穿戴设备在人们的日常生活中变得越来越流行。基于惯性传感器的人体运动感知机制也成为了近年来的研究热点。在本文中，我们主要关注基于惯性传感器人体运动感知机制的两个方面：多传感器设备的安全认证问题以及多传感器设备的空间同步问题。

首先，无线热点网络允许设备之间自发地查找对方并且进行交互，但是由于无线网络的性质，设备之间的认证和安全成为了一个重要的问题[37]。经我们观察，当两个用户进行握手动作时，他们手臂的物理动作具有一定的相关性。基于这一观察，我们想到可穿戴设备上的惯性传感器可以采集这些动作的相关数据，通过分析这些传感器数据，我们可以提取其中的相关性，从而生成一致的密钥进行设备之间的安全认证。

其次，惯性传感器的读数是基于设备的局部坐标系的，并由其设备姿态决定（更准确地说是它的主板）。由于多个移动设备放置在人体不同部位，造成了惯性传感器的局部坐标系的不同。因此，统一所有可穿戴设备的坐标系对多传感器的协作应用是必不可少的，这种技术我们称之为空间同步技术。利用空间同步技术，这些传感器可以在统一的坐标系下对物理运动进行采样，从而更好地协作分析人体的运动。经观察，人体在向前运动时，身体上各部位的可穿戴设备均受到一个一致的力，我们想到如果可以利用这个一致的力，就可以用来替代室内准确度较低的磁力计，从而实现空间同步技术。

本文首先对基于惯性传感器的人体运动感知机制的相关工作进行了介绍。在多传感器设备的安全认证方面，本文在第三章中设计与实现了基于惯性传感器的握手认证系统，分别介绍了握手认证系统框架中的每一个模块，重点介绍了基于陀螺仪的姿态跟踪模型（GYAT），并在第三章的最后对系统进行了详尽地实验分析。在多传感器设备的空间同步方面，本文在第四章中设计与实现了一个基于多传感器设备的空间同步系统，重点介绍了基于惯性传感器的方向估计以及基于陀螺仪的姿态跟踪扩展研究，并对系统进行了性能评估和案例分析。具体来说，本文的主要贡献如下：

1. 我们提出了一个基于陀螺仪的姿态跟踪模型（GYAT），它能够追踪节点的运动，并且校准了传感器数据，使得设备间的传感器数据能够获得最大的

相似度。

2. 我们实现了基于惯性传感器的握手认证系统，并在真实环境下进行了实验分析，实验结果显示我们的安全认证系统取得了平均85%的设备间数据相关性，以及平均14b/s的密钥生成速率。
3. 我们提出了多传感器设备空间同步的MOSS框架。特别地，我们提出了一个用来获取空间同步的一致方向估计器与一个维持空间同步的基于陀螺仪的姿态追踪器。
4. 我们在COTS移动设备上实现了基于多传感器设备的空间同步系统，实验结果显示我们的系统可以获得平均6.8°的角度准确度，以及平均93%的测量相似度。

5.2 展望

在多传感器设备的安全认证方面，本文设计了一套基于惯性传感器的握手认证系统；在多传感器设备的空间同步方面，本文设计了一套基于多传感器设备的空间同步系统。但是，我们的工作仍存在一些不足点。

在基于惯性传感器的握手认证系统中，我们还须要进行深入研究的有：（1）对噪声的处理目前还是基于简单地平滑处理，未来需要对噪声进行进一步滤除；（2）对Level Crossing方法阈值的选择仍是基于线下实验的，未来需要尝试在线上动态选择阈值；（3）在软件方面，未来需要优化认证算法的速度并提升软件的用户体验。

在基于多传感器设备的空间同步系统中，我们还须要进行深入研究的有：（1）目前对同步的时机筛选机制较为粗糙，未来须要更精确地定位适合同步的惯性传感器数据区间；（2）优化同步算法的性能。（3）目前对复合动作的算法性能不够好，未来须要对复合动作的空间同步算法进行深入分析和研究。

参考文献

- [1] Afzal, M.H., Renaudin, V., Lachapelle, G., 2011. Magnetic field based heading estimation for pedestrian navigation environments, in: Indoor Positioning and Indoor Navigation (IPIN), 2011 International Conference on, IEEE. pp. 1–10.
- [2] Association, I.S., 等, 2002. Standard for a precision clock synchronization protocol for networked measurement and control systems. IEEE 1588 .
- [3] Barshan, B., Durrant-Whyte, H.F., 1995. Inertial navigation systems for mobile robots. *IEEE Transactions on Robotics and Automation* 11, 328–342.
- [4] Batina, L., Mentens, N., Verbauwhede, I., 2005. Side-channel issues for designing secure hardware implementations, in: On-Line Testing Symposium, 2005. IOLTS 2005. 11th IEEE International, IEEE. pp. 118–121.
- [5] Benesty, J., Chen, J., Huang, Y., Cohen, I., 2009. Pearson correlation coefficient, in: Noise reduction in speech processing. Springer, pp. 1–4.
- [6] Bichler, D., Stromberg, G., Huemer, M., Löw, M., 2007. Key generation based on acceleration data of shaking processes, in: International Conference on Ubiquitous Computing, Springer. pp. 304–317.
- [7] Brassard, G., Salvail, L., 1993. Secret-key reconciliation by public discussion, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer. pp. 410–423.
- [8] Butterworth, S., 1930. On the theory of filter amplifiers. *Wireless Engineer* 7, 536–541.
- [9] Cristian, F., 1989. Probabilistic clock synchronization. *Distributed computing* 3, 146–158.
- [10] Elias, P., 1972. The efficient construction of an unbiased random sequence. *The Annals of Mathematical Statistics* , 865–870.

- [11] Fourati, H., 2015. Heterogeneous data fusion algorithm for pedestrian navigation via foot-mounted inertial measurement unit and complementary filter. *IEEE Transactions on Instrumentation and Measurement* 64, 221–229.
- [12] Gehrman, C., Mitchell, C.J., Nyberg, K., 2004. Manual authentication for wireless devices. *RSA Cryptobytes* 7, 29–37.
- [13] Guha, S., Plarre, K., Lissner, D., Mitra, S., Krishna, B., Dutta, P., Kumar, S., 2012. Autowitness: locating and tracking stolen property while tolerating gps and radio outages. *ACM Transactions on Sensor Networks (TOSN)* 8, 31.
- [14] Guo, Y., Yang, L., Ding, X., Han, J., Liu, Y., 2013. Opensesame: Unlocking smart phone through handshaking biometrics, in: *INFOCOM, 2013 Proceedings IEEE*, IEEE. pp. 365–369.
- [15] Gusella, R., Zatti, S., 1989. The accuracy of the clock synchronization achieved by tempo in berkeley unix 4.3 bsd. *IEEE transactions on Software Engineering* 15, 847–853.
- [16] Jolliffe, I., 2002. Principal component analysis. Wiley Online Library.
- [17] Lamport, L., 1978. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM* 21, 558–565.
- [18] Lee, H.J., Jung, S., 2009. Gyro sensor drift compensation by kalman filter to control a mobile inverted pendulum robot system, in: *Industrial Technology, 2009. ICIT 2009. IEEE International Conference on*, IEEE. pp. 1–6.
- [19] Lee, S.W., Jung, P., Song, S.H., 2013. Hybrid indoor location tracking for pedestrian using a smartphone, in: *Robot Intelligence Technology and Applications 2012*. Springer, pp. 431–440.
- [20] Link, J.A.B., Smith, P., Viol, N., Wehrle, K., 2011. Footpath: Accurate map-based indoor navigation using smartphones, in: *Indoor Positioning and Indoor Navigation (IPIN), 2011 International Conference on*, IEEE. pp. 1–8.
- [21] Liu, H., Wang, Y., Yang, J., Chen, Y., 2013. Fast and practical secret key extraction by exploiting channel response, in: *INFOCOM, 2013 Proceedings IEEE*, IEEE. pp. 3048–3056.

- [22] Madgwick, S.O., Harrison, A.J., Vaidyanathan, R., 2011. Estimation of imu and marg orientation using a gradient descent algorithm, in: Rehabilitation Robotics (ICORR), 2011 IEEE International Conference on, IEEE. pp. 1–7.
- [23] Van de Maele, P.J., 2014. Reading a imu without kalman: The complementary filter. Publicación electrónica: <http://www.pieter-jan.com/node/11> Consultada 12.
- [24] Marins, J.L., Yun, X., Bachmann, E.R., McGhee, R.B., Zyda, M.J., 2001. An extended kalman filter for quaternion-based orientation estimation using marg sensors, in: Intelligent Robots and Systems, 2001. Proceedings. 2001 IEEE/RSJ International Conference on, IEEE. pp. 2003–2011.
- [25] Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A., 2008. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in: Proceedings of the 14th ACM international conference on Mobile computing and networking, ACM. pp. 128–139.
- [26] Mayrhofer, R., Gellersen, H., 2009. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Transactions on Mobile Computing* 8, 792–806.
- [27] Mohan, P., Padmanabhan, V.N., Ramjee, R., 2008. Nericell: using mobile smart-phones for rich monitoring of road and traffic conditions, in: Proceedings of the 6th ACM conference on Embedded network sensor systems, ACM. pp. 357–358.
- [28] Rodriguez, O., 1840. Des lois geometriques qui regissent les desplacements d’ un systeme solide dans l’ espace et de la variation des coordonnees provenant de deplacements consideres independamment des causes qui peuvent les produire. *J Math Pure Appl* 5, 380–440.
- [29] Roy, N., Wang, H., Roy Choudhury, R., 2014. I am a smartphone and i can tell my user’s walking direction, in: Proceedings of the 12th annual international conference on Mobile systems, applications, and services, ACM. pp. 329–342.
- [30] Shannon, C.E., 1951. Prediction and entropy of printed english. *Bell Labs Technical Journal* 30, 50–64.
- [31] Shen, G., Chen, Z., Zhang, P., Moscibroda, T., Zhang, Y., 2013. Walkie-markie: indoor pathway mapping made easy, in: Proceedings of the 10th USENIX confer-

- ence on Networked Systems Design and Implementation, USENIX Association. pp. 85–98.
- [32] Stajano, F., 2003. Security for whom? the shifting security assumptions of pervasive computing, in: Software Security — Theories and Systems. Springer, pp. 16–27.
 - [33] Sun, Z., Purohit, A., Pan, S., Mokaya, F., Bose, R., Zhang, P., 2012. Polaris: getting accurate indoor orientations for mobile devices using ubiquitous visual patterns on ceilings, in: Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications, ACM. p. 14.
 - [34] Wang, H., Sen, S., Elgohary, A., Farid, M., Youssef, M., Choudhury, R.R., 2012. No need to war-drive: unsupervised indoor localization, in: Proceedings of the 10th international conference on Mobile systems, applications, and services, ACM. pp. 197–210.
 - [35] Woodman, O.J., 2007. An introduction to inertial navigation. Technical Report. University of Cambridge, Computer Laboratory.
 - [36] Zhang, L., Li, X.Y., Huang, W., Liu, K., Zong, S., Jian, X., Feng, P., Jung, T., Liu, Y., 2014. It starts with igaze: Visual attention driven networking with smart glasses, in: Proceedings of the 20th annual international conference on Mobile computing and networking, ACM. pp. 91–102.
 - [37] Zhou, D., 2003. Security issues in ad hoc networks, in: The handbook of ad hoc wireless networks, CRC Press, Inc.. pp. 569–582.
 - [38] Zhou, P., Li, M., Shen, G., 2014. Use it free: Instantly knowing your phone attitude, in: Proceedings of the 20th annual international conference on Mobile computing and networking, ACM. pp. 605–616.
 - [39] Zhu, X., Li, Q., Chen, G., 2013a. Apt: Accurate outdoor pedestrian tracking with smartphones, in: INFOCOM, 2013 Proceedings IEEE, IEEE. pp. 2508–2516.
 - [40] Zhu, X., Xu, F., Novak, E., Tan, C.C., Li, Q., Chen, G., 2013b. Extracting secret key from wireless link dynamics in vehicular environments, in: INFOCOM, 2013 Proceedings IEEE, IEEE. pp. 2283–2291.

简历与科研成果

基本情况

蔡庆亮，男，汉族，1991年12月出生，浙江宁波人。

教育背景

2014.9~2010.6	南京大学计算机科学与技术系	硕士
2010.9~2007.6	苏州大学计算机科学与技术学院	本科

已发表或录用的论文

- Lei Xie, Jianqiang Sun, Qingliang Cai, Chuyu Wang, Jie Wu, and Sanglu Lu. Tell Me What I See: Recognize RFID Tagged Objects in Augmented Reality Systems, In Proceeding of ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), 2016.
- Jianqiang Sun, Lei Xie, Qingliang Cai, Chuyu Wang, Jie Wu, Sanglu Lu. RF-ISee: Identify and Distinguish Multiple RFID Tagged Objects in Augmented Reality Systems[C], IEEE, International Conference on Distributed Computing Systems. IEEE, 2016:723-724.(Poster Paper)

已申请的专利

- 一种基于射频识别技术的手势隔空互交系统及其工作方法，谢磊，蔡庆亮，孙健强，石聪聪，陆桑璐，申请号：201610441208.6
- 一种基于惯性传感器感知握手的认证系统及其工作方法，谢磊，蔡庆亮，陆桑璐，申请号：201710320799.6

致 谢

首先我要感谢我的导师谢磊副教授，在三年的研究生期间，谢老师不论在学习还是生活上，都给了我很多有帮助的指导。这篇论文也是在谢老师的悉心指导下完成。在这篇论文的选题、实验设计、难点攻克等方面，谢老师都给了很多建设性意见和帮助。谢老师对工作以及对学生的要求都很高，这也让我们在科研道路上迅速进步着。在谢老师身上，我学习到的是对学术的严谨认真以及高效执行力的重要性。同时也要感谢陆桑璐教授，陆老师在研究生期间对我们的生活和学习提供了很多宝贵的建议，举办了很多次讨论班与讲座，同时也让我们自己有在讲台上讲述自己科研工作的机会，锻炼了我们很多软技能。

我还要感谢其他所有帮助过我的老师和同学们，是他们带给了我一个积极向上的学术氛围，让我可以向他们学习很多东西，也让我的研究生生活更加精彩！

最后，我向参加本文审稿以及答辩的老师表示诚挚的感谢！