中国研究生操作系统开源创新大赛

项目功能说明书

学　　校：	电子科技大学
参 赛 队 伍：	MobiNetS
队 伍 成 员：	马浩天 李嘉诚 王振华
指 导 教 师：	赵志为
完 成 日 期：	2024年8月

目录

第 1 章 绪 论

1.1 目的与意义

本作品意在实现一套多设备键鼠共享系统，可以**不依赖任何硬件**仅通过软件实现一套键盘和鼠标在**多设备、多系统**上的无缝切换和共享，并且相较于众多现有的键鼠共享方案有着更好的跨平台性、通用性以及安全性。

1.1.1 应用场景

1）办公环境

在开放式的办公环境中，用户经常需要使用不同的计算机系统同时处理多个任务。而多设备键鼠共享系统可以让员工通过一套键鼠设备在多台计算机之间无缝切换，显著提升工作效率。

2）会议演示

在会议室或需要演示场合，可以通过共享键鼠系统来控制多台计算机进行展示，减少硬件设备的使用和反复切换，提高会议效率。

3）软件开发和测试

开发人员通常需要在多台设备上进行代码编写、调试和测试，使用键鼠共享系统开发人员可以在不同设备之间切换。测试人员可以在不同的操作系统和设备上进行测试，确保软件的跨平台兼容性和稳定性，提高测试效率和覆盖率。

4）教学互动

在远程教学过程中，教师可以通过一套键鼠控制多台计算机，进行教学内容的展示和互动，提升教学效果。

5）家庭娱乐

家庭用户可以通过共享键鼠系统来控制家中的多台计算机、电视、游戏机等设备，提升娱乐体验。

1.1.2 设计目的

在信息化时代，每个人可能会有不止一台计算机主机，而在操作计算机时鼠标、键盘等 Hid Input 主机又是比不可少的，如果为每一台主机都配备一套键鼠，会造成很大的资源浪费。为此，我们希望设计实现一套通用性强的跨主机 Hid Input 设备共享方案，仅依靠一套键鼠便可操控多台主机，节约资源的同时提高操作效率。尽管目前存在一些多设备

键鼠共享的软硬件解决方案（详见 1.2.2），但是它们存在着通用性差、跨平台性差、依赖硬件资源等问题。具体表现在以下方面：

- 跨平台和兼容性问题。项目需要实现多台主机的协同共享，当主机平台不一致时，可能会产生兼容性问题。在主流 KVM 软件中，Synergy 作为一款付费软件可以支持 Windows、Linux、macOS 等操作系统，但由于其更新较慢，在一些 Linux 发行版和 macOS 新版本中可能遇到兼容性问题，需要特定配置或补丁，ShareMouse 主要支持 Windows 和 macOS，不支持 Linux。
- 配置复杂问题。现有的 KVM 软件对集群内主机列表的管理，一般是通过用户手动添加主机并配置 IP 地址等信息实现的，不能实现局域网内主机的自动发现和配置，这可能影响用户的使用体验。现有软件中，Synergy 需要用户配置集群内主机信息，尽管提供了可视化的操作界面，但是对非技术用户而言，对主机 IP 信息等的添加和配置仍可能有困难，这有可能影响用户体验。

为此我们的设计目标如下：

1）提升工作效率：通过在多台设备之间流畅地无缝切换键鼠控制，减少用户频繁地切换设备的时间，提升整体工作效率。

2）简化操作流程：提供简单的键鼠初始化配置和控制界面，简化用户使用的操作流程，提升用户体验。

3）节省硬件成本：避免为每台设备单独配备键盘和鼠标，且不需要依赖额外的硬件设施，节省硬件成本和空间。

1.1.3 作品概述

图 1 DeviceShare 项目示意图

DeviceShare 基于软件 KVM 方案，可实现局域网内多主机共享一套 Hid Input 设备功能，并支持在 openKylin 操作系统的 Wayland 桌面环境下运行。目前为止该项目支持功能如下表 1 所示：

表 1 项目功能完成度

编号	功能说明	完成度
1	支持一套键鼠控制多台主机，同一时刻仅有一套设备响应。	已实现
2	鼠标可跨设备移动、单击、双击、滚轮滑动、拖动。	已实现
3	键盘支持基本跨设备输入，支持组合快捷键，支持 MacOS 系统键位映射。	已实现
4	支持主机间剪切板功能共享。	已实现
5	支持以图形化的方式配置主机之间相对位置的功能，鼠标移动范围及方向受相对位置限制。	已实现
6	具备良好的图形化界面及桌面通知机制。	已实现
7	具备自动设备发现机制，支持超时断连机制。	已实现
8	支持多主机间文件共享。	已实现
9	采用公私钥认证和加密机制，保证安全性。	已实现
10	支持 Linux（包括 OpenKylin），Windows，MacOS 操作系统。	已实现
11	支持接收器热插拔的方式，在无需主机安装软件的情况下实现多主机共享键鼠	已实现
12	设备共享延迟低，可满足日常办公基本需求。	已实现

项目开源地址：https://www.gitlink.org.cn/mahaotian/DeviceShare

项目演示 Demo 视频地址：http://file.dtlab.qylh.xyz/demo2.mp4

1.2 项目背景

1.2.1 需求分析

项目主要面向的场景是用户需要控制多台主机，若为每台主机均配备一套输入设备可能需要频繁切换设备，造成效率低下，且过度浪费硬件资源。因此需要一种方案，能够实现多台主机共享一套输入设备，能实现设备在主机间的自由切换。

基于赛题要求，将项目的业务流程概括如下：使用一套输入设备直接对一台主机进行控制，同时支持通过网络通信方式对集群内的其他主机进行控制，主控机负责管理被控机并配置屏幕间的相对位置，被控机接收来自主控机的控制信号并进行处理。项目需求如表 2 所示：

表 2 项目功能需求

功能名称	功能描述
鼠标共享	使用主机鼠标设备控制多台主机，实现光标在主机间的自由切换，支持左右键单机，双击，拖拽，滚轮滑动。
键盘支持	支持键盘对相应主机的输入操作，支持按键组合，支持快捷键，支持 mac 键盘映射。
单设备响应	同一时刻只有一台设备响应输入。
相对位置配置	可以在 GUI 界面上灵活配置被控机相对主控机的位置。
剪贴板共享	通过网络传输，使主机的剪贴板内容能在多台主机之间共享。
文件拖拽	利用键鼠操作和网络通信实现不同主机间的快捷文件传输。

安全性需求	提供主机准入机制，敏感信息加密进行传输。
通用性需求	在无额外硬件支撑的条件下，支持在 Windows、MacOS、Linux(wayland、x11 等桌面环境)下运行，支持不同操作系统之间进行设备共享。
性能需求	设备共享时输入到响应延迟应尽可能低，不影响正常使用。
可用性需求	提供可视化的界面配置屏幕相对位置。

1.2.2 技术路线调研

实现多台主机的输入设备共享是提高工作效率的一个重要手段，为此，目前已有部分技术可以利用硬件和软件方法不同程度地实现设备共享，主要包括远程桌面连接、硬件设备共享器、KVM 技术等。

1. 远程桌面

远程桌面是最常见的实现设备共享的方式。目前已有远程桌面协议（RDP），通过该协议，计算机可以利用网络通信实现远程桌面控制，使用户以可视化的方式浏览和控制远程计算机。(Microsoft, 2023)除此之外，还有一些可以实现远程控制的第三方软件，如 TeamViewer、AnyDesk、ToDesk 等，该类远程桌面方式往往适用于物理距离较远的多台主机，且其直接访问远程桌面的方式对通信带宽有很高的要求，并不适用于赛题需求的环境。

2. 硬件设备共享器

除了软件方式，也有一些硬件技术可以满足输入设备的共享，例如USB共享器，这一技术允许多台计算机共享一个 USB 设备（如键盘、鼠标、打印机等），通过按钮或自动检测切换控制，目前已有成熟的产品实现这一功能，如 Ugreen USB 3.0 Sharing Switch，其支持两台电脑共享一个 USB 设备，通过物理按钮快速切换 USB 设备的控制权。(Ugreen, 2023)但是该技术只允许两台计算机之间的设备共享，使得其应用受到限制，并且设备的切换只能通过硬件方式实现，无法完成主机的自由切换。

3. KVM 技术

KVM 切换器（英语：KVM switch），一般简称 KVM，又名多电脑切换器，可以使用户通过一组键盘、显示器和鼠标控制多台电脑。KVM，即键盘、显示器、鼠标的英文首字母缩写（Keyboard、Video、Mouse）。此技术按照具体技术路线可以分为三种：

1) 硬件 KVM 切换器

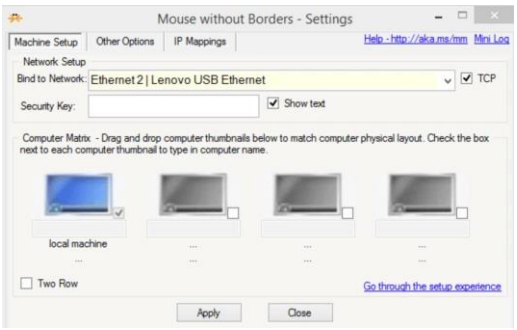
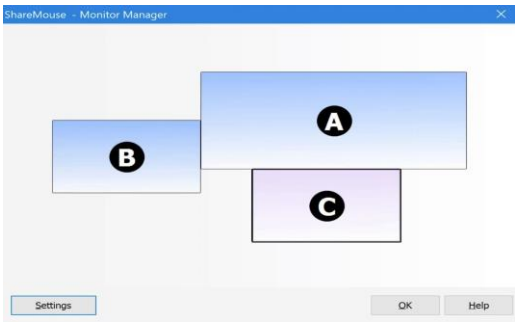
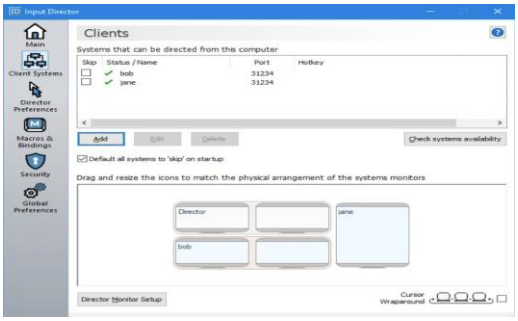
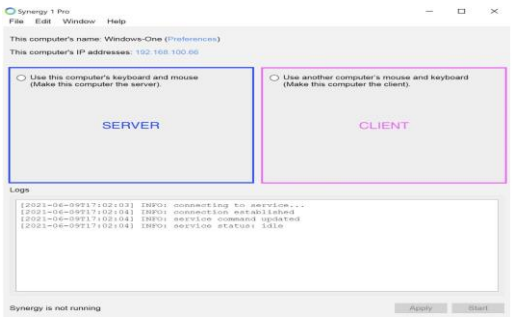
图 2 硬件 KVM

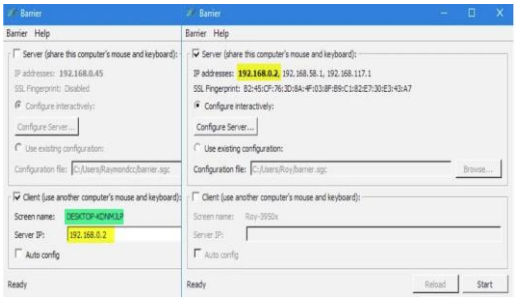
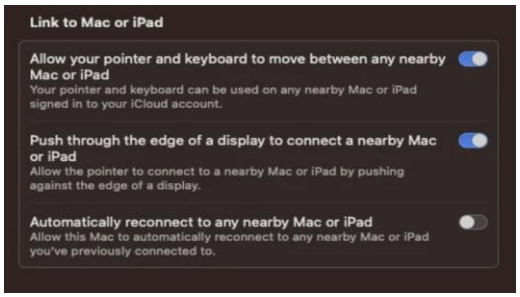
作为一种硬件设备，硬件 KVM 切换器可以通过一组键盘、显示器和鼠标来控制多台计算机。用户可以通过物理按钮、键盘快捷键或远程管理来切换控制不同的计算机，相比 USB 共享器，其切换器可以支持更多的接口，包括 HDMI、DVA 等。目前 ATEN、Belkin、StarTech 等厂家提供了这种切换器设备，产品包括 ATEN CS1922（支持 2 台电脑，支持 HDMI、USB 接口）(ATEN, 2024)、Belkin SOHO F1DS104L（支持 4 台电脑，支持 DVI、USB 接口）等(Belkin, 2024)。

2) 软件 KVM

软件 KVM 技术利用网络来共享键盘和鼠标，允许用户通过网络连接来控制多台计算机，用户一般在需要共享设备的计算机上安装软件客户端，使用网络连接而不是硬件切换器实现设备共享。相比硬件切换方法，使用网络传输的方式可以在使用上更自由而不受限于主机的物理距离。现有 Synergy(Synergy, 2017)、ShareMouse(ShareMouse, 2023)等实现：

表 3 软件 KVM 现有解决方案调研

现有方案	功能描述	缺点
Mouse WithOut Borders		只适用 Windows 操作系统；延迟高稳定性差
ShareMouse		商业软件，完整功能 80 美元价格昂贵；仅支持一台显示器
Input Director		只适用 Windows 操作系统；初始配置十分繁琐
Synergy		商业软件无免费版，定价 29 美元；至多支持 3 台设备连接；没有安全加密

Barrier		初始配置十分繁琐；至多支持 2 台设备同时连接
Universal Control		苹果内置功能，仅限于 Mac OS 或 IOS 系统
Logitech Flow		罗技专有软件，仅局限于罗技设备使用

技术路线对比如表 4 所示，经过对比发现软件 KVM 方案更贴近赛题的应用场景和具体需求。

表 4 技术路线对比

技术路线	优点	缺点
远程桌面	✧ 支持屏幕共享 ✧ 不受物理距离限制	◆ 依赖网络带宽，延迟 ◆ 对机器性能要求高

硬件设备共享器	✧ 性能优秀 ✧ 延迟低	◆ 需额外硬件支持 ◆ 受物理位置限制 ◆ 切换需手动操作 ◆ 无法共享剪切板 ◆ 无法实现文件共享
硬件 KVM	✧ 性能优秀 ✧ 延迟低 ✧ 支持显示器共享	◆ 需额外硬件支持 ◆ 受物理位置限制 ◆ 切换需手动操作
软件 KVM	✧ 无需硬件支持 ✧ 延迟较低 ✧ 不受物理位置限制 ✧ 切换便捷	◆ 较为依赖网络稳定性

1.2.3 项目贡献和突破

总结我们的方案贡献和突破点如下：

- **跨设备：**实现了使用一套 Hid Input 设备控制多台主机的功能，**支持所有键鼠操作，包括拖动、快捷键等**，支持剪切板共享。
- **强通用性：**支持在**不同硬件不同操作系统（Windows、Linux、MacOS）**的主机平台上运行，支持在**异构主机**间共享 Hid Input 设备。同时还针对 **Wayland 桌面**协议进行了适配。
- **用户友好：**采用开箱即用的配置方案，提供高效的 GUI 配置界面，支持**服务自动发现**机制，**无需额外学习成本**。
- **高安全性：**采用公私钥认证和加密机制，可**避免恶意设备加入连接，数据安全性**得以保证。
- **性能优秀：**基于**多线程并行**模型设计，运行性能优秀。

第 2 章 技 术 理 论

2.1 设计思想

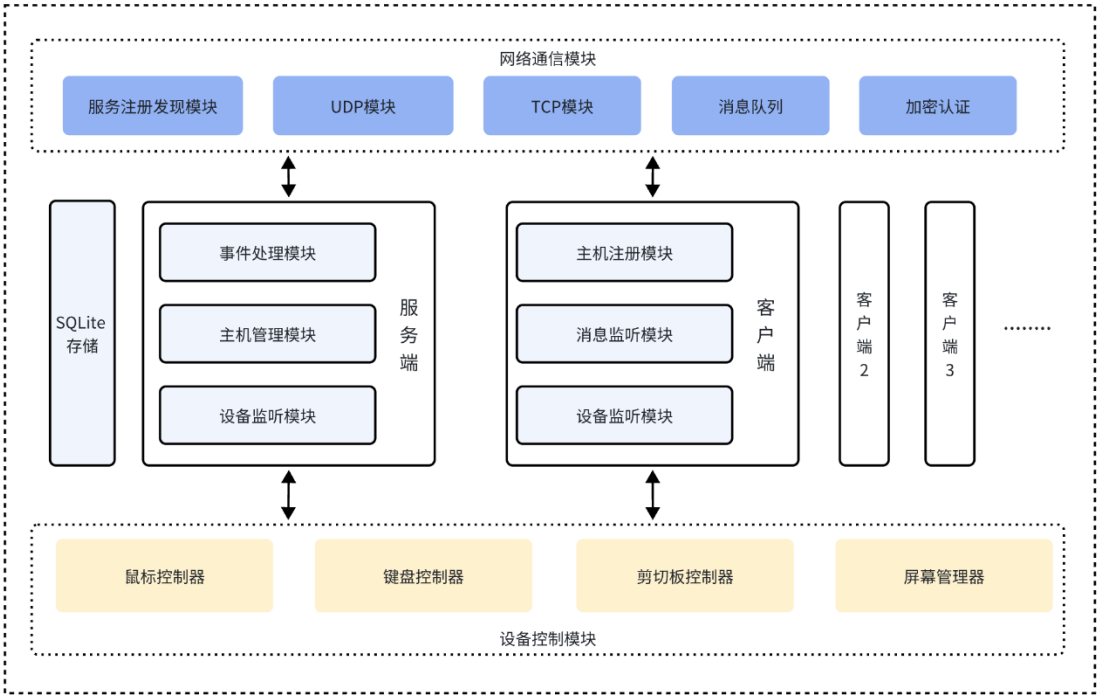


图 3 设计框架

软件整体以 C/S 架构运行，项目的整体设计框架如图 3 所示，整体由以下四个部分构成：

1. 服务端：服务端为 Hid Input 设备的拥有者，可向其他被客户端主机共享其拥有的输入设备。
2. 客户端：客户端为使用主机共享的输入设备的主机。
3. 网络通信模块：用于服务端和客户端的数据传输。
4. 设备控制模块：用于读取 Hid Input 设备信息及控制 Hid Input 设备。

软件的运行流程如图 4 所示，具备 Hid 设备的主机作为服务端启动，进行服务注册。其他主机以客户端形式启动，向服务端发起连接请求。服务端处理客户端连接请求，当服务端主机的光标移出屏幕范围后，会自动判断接下来被控的主机，并将本机输入设备产生的输入拦截，通过网络模块转发给客户端，客户端收到输入信息后响应相应的控制信号。

当客户端的光标移出范围后向服务端主机发送事件标志，服务端主机停止控制信号的转发，并恢复输入事件的响应。

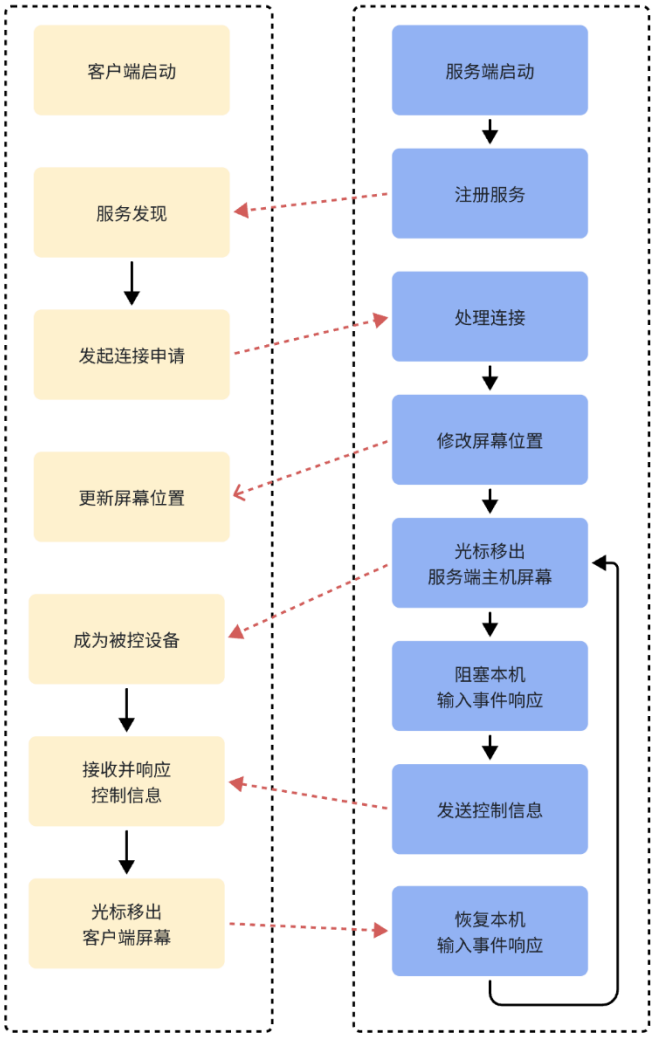


图 4 运行流程

2.1.1 服务端

服务端为具备 Hid Input 设备的主机，其运行状态机如图 5 所示，服务端由以下几个线程构成：

- 主线程：服务注册及启动其他线程
- TCP 监听线程：用于监听处理 TCP 连接，并为每一个连接创建子线程。
  - TCP 处理线程，用于处理与客户端的 TCP 连接

- 消息监听线程：监听客户端消息，主要为心跳信息和剪切板信息
- 设备监听线程：监听 Hid Input 设备的输入信息和剪切板信息。
- GUI 线程： GUI 界面的显示和处理。
- 协调线程：协调控制上述三个线程的运行。

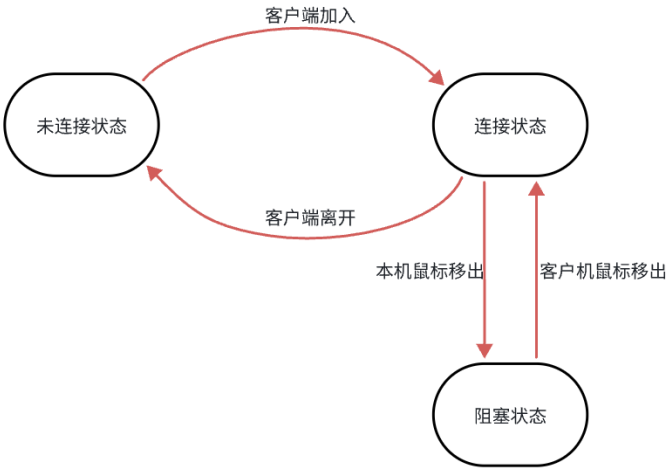


图 5 服务端状态机

2.1.2 客户端

客户端为需要使用服务主机的 Hid Input 设备的主机，其运行状态机如图 6 所示，客户端由以下几个线程构成：

- 主线程：处理服务发现，发起连接请求，启动其他线程。
- 心跳包线程：定期发送心跳包。
- 消息监听线程：用于接收并响应主机传递的控制信息。
- GUI 线程： GUI 界面的显示和处理。
- 设备监听线程：用于监听鼠标移出事件及剪切板更新事件。

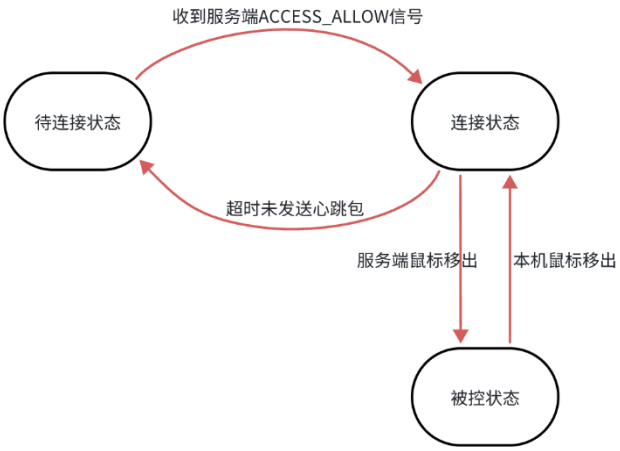


图 6 客户端状态机

2.2 技术路线

2.2.1 设备控制方案选择

不同的操作系统以及不同的桌面环境对 Hid Input 设备的控制逻辑不同，为此我们选用了基于 Python 语言的 **pynput** 来对 Hid Input 设备进行控制和监听(Palmér, 2024)，然而由于 Wayland 桌面环境去除了 X server，导致无法获取和处理输入事件，我们选用 **evdev** 获取输入事件(Gvalkov, 2024)，选用 **uinput** 以虚拟设备的方式进行事件输入。

2.2.2 网络通信协议

为了在不同设备之间实现键鼠事件的传输，我们选用高效的网络通信协议，采用了 TCP/IP 协议进行数据传输，保证数据的可靠传递。同时，针对键鼠事件的实时性要求，进行了协议优化，尽量减少数据包的大小和传输延迟。

2.2.3 设备发现与连接管理

在多设备键鼠共享系统中，自动化配置可以提高软件使用效率，降低学习成本。为此我们借助 **mDNS** 协议进行服务注册和服务发现(IETF, 2013)。这样设备可以自动发现网络中的其他主机。同时，为了提高连接的稳定性，设计超时断连机制，确保当设备离线或网络中断时，系统能够及时响应并重新建立连接。

2.2.4 GUI 界面设计

为了保证软件的跨平台性，我们使用了 Python 语言结合 QT 来开发应用界面和核心逻辑。我们基于 **PyQT5** 设计良好的图形化用户界面，使用户可以方便地配置和管理多个设备。(Pypi, 2024)用户可以通过拖放操作在界面上设置设备之间的相对位置，系统会根据这些设置限制鼠标的移动范围及方向。基于 PyQT5 还可实现桌面通知机制，当设备连接或断开时，用户会收到相应的通知，提升用户体验。

2.2.5 安全性

为保证跨设备通信的安全性，我们采用 **RSA 公私钥认证和数据加密机制**(Ron Rivest, 1983)。在设备连接时，双方需要进行公私钥的认证，确保通信双方的合法性。数据传输过程中，所有数据都经过加密处理，防止数据在传输过程中被截获或篡改。

2.2.6 剪切板与文件共享

在实现剪切板和文件共享功能时，我们需要考虑不同操作系统之间的差异。对于剪切板共享，我们采用跨平台的剪切板管理库 **pyperclip**，确保不同系统之间剪切板内容的兼容性(Sweigart, 2014)。然而由于 wayland 环境的安全性考量，pyperclip 无法正常工作，采用 **wl-clipboard** 方案进行适配。文件共享功能则通过网络文件传输协议实现，用户可以在不同设备之间方便地传输文件，提升工作效率。

2.2.7 延迟优化

为满足日常办公的基本需求，需对系统的延迟进行了优化。通过减少数据包大小、优化网络传输协议和高效的事件处理机制，我们将设备共享的延迟控制在可接受的范围内，确保用户在使用过程中不会感受到明显的延迟。

2.3 代码原创说明

本项目主要实现多设备键鼠共享功能，涉及图形用户界面、键鼠事件捕捉与发送、设备发现与连接管理等多个模块。表 5 是各个模块中第三方 Python 库的详细引用情况：

表 5 第三方 Python 库引用情况

第三方模块	功能	引用情况
qt-material	提供 QT 的开源样式	提升 QT 界面美观度
pillow	图像处理库	用于处理图片
PyQT5	GUI 界面设计	用于软件 GUI 开发
pynput	提供键盘和鼠标事件监听和控制的接口	用于监听本地设备的键鼠事件，并根据需要进行处理和传输
pyperclip	跨平台的剪切板操作库	用于实现多设备之间的剪切板内容共享
pyevdev	读取/dev/input 数据	用于 wayland 下监听输入事件
zeroconf	实现局域网内设备的自动发现和连接	服务注册和服务发现
netifaces	提供网络接口信息	用于获取本地设备的网络接口信息
rsa	实现 RSA 公私钥加密和解密	用于设备连接时的身份认证和数据传输的加密，确保数据安全
screeninfo	提供屏幕分辨率和多显示器信息	用于获取多显示器的配置信息，辅助实现跨设备的鼠标移动

第 3 章 软件介绍

3.1 软件功能介绍

软件基于 C/S 架构，整体架构如图 7 所示。借助设备控制模块进行输入事件的监听和模拟，借助网络通信模块进行主机间连接和事件通信。使用 SQLite 作为本地数据存储方案。

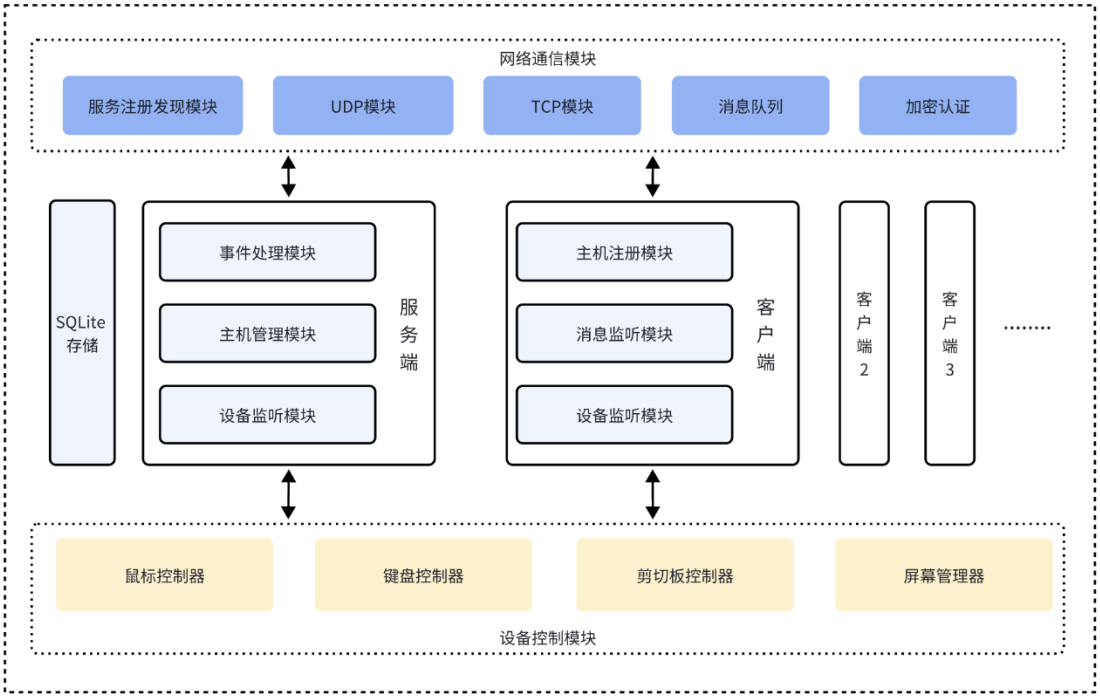


图 7 软件架构框图

3.1.1 设备控制模块功能介绍

项目通过封装设备控制模块，来提供 Hid Input 设备控制和输入监听功能，其具体实现原理为监听主控机上的输入事件，通过网络模块传递到被控设备，模拟进行事件输入。主要基于 pynput 实现，同时基于 evdev 和 uinput 对 Wayland 桌面环境进行了额外适配，具体原理是通过读取/dev/input 下的输入设备来获取每种设备的输入，通过多个线程监听潜在的输入设备，同时为了模拟输入设备的输入，通过 uinput 创建虚拟输入设备，并写入输入事件。

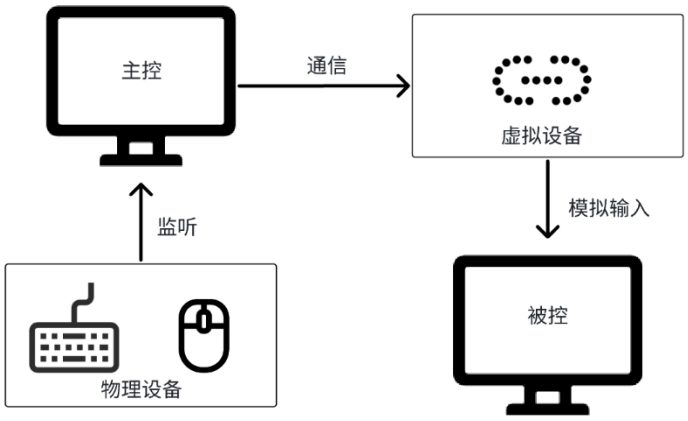


图 8 设备控制原理

该模块由鼠标控制模块、键盘控制模块、剪切板控制模块三个子模块构成，各个模块功能如表 6 所示，同时由于操作系统的不同，在子模块内部实现针对不同的操作系统进行了适配，保证了上层模块调用时的透明性。

表 6 设备控制模块功能表

模块	函数	功能
鼠标控制模块	get_position	鼠标位置获取
	update_last_position	鼠标位置记录，用于获取位移
	move_to	鼠标位置设置
	move	鼠标位移控制
	click	鼠标点击控制
	scroll	鼠标滚轮控制
	mouse_listener	鼠标事件监听器

键盘控制模块	click	键盘点击控制
	press	键盘 press 控制
	release	键盘 release 控制
	keyboard_listener	键盘监听器
	encode	键盘编码
	decode	键盘解码
剪切板控制模块	paste	设置剪切板内容
	copy	获取剪切板内容
	clipboard_listener	剪切板监听器

3.1.2 网络通信模块功能介绍

项目的网络通信模块包含 UDP 模块和 TCP 模块，UDP 主要用于广播，心跳机制以及输入设备控制信息的转发。TCP 模块主要用于主机间事件的通信以保证通信的可靠性。同时为了平衡设备间数据处理能力的差距，还增加了消息的缓冲队列。所有传输的数据由消息类型和消息体构成，目前系统的消息类型及说明如表 7 所示：

表 7 消息类型说明

消息类型	说明	协议
CLIENT_HEARTBEAT	心跳包	UDP
SUCCESS_JOIN	服务端对主机成功加入的回应	UDP
MOUSE_BACK	光标从被控机移出回到主机	TCP

MOUSE_MOVE	光标移动事件，消息体为具体坐标	UDP
MOUSE_MOVE_TO	光标移动事件，消息体为移动位移	TCP
MOUSE_CLICK	鼠标点击事件，包括 Press 和 Release	UDP
MOUSE_SCROLL	鼠标滚轮事件	UDP
KEYBOARD_CLICK	键盘点击事件，包括 Press 和 Release	UDP
CLIPBOARD_UPDATE	剪切板更新事件	UDP 广播
POSITION_CHANGE	屏幕位置更新事件	TCP
SEND_PUBKEY	发送公钥	TCP
TCP_ECHO	TCP 的回应	TCP
KEY_CHECK	公私钥校验	TCP
KEY_CHECK_RESPONSE	公私钥校验结果	TCP
ACCESS_DENY	允许被控机连接	TCP
ACCESS_ALLOW	禁止被控机连接	TCP

为了简化设备连接的操作，基于 Zeroconf 实现了被控机主机自动查找服务地址功能，在局域网环境下无需人工干预即可发现服务地址(IETF, 1999)，基本原理是服务端将服务的地址等信息创建为一个服务信息对象并借助 mDNS 广播该服务信息。被控机监听 mDNS 广播，使用 ServiceBrowser 对象进行服务发现，当有符合条件的服务出现时便能及时获得服务地址。

3.1.3 加密认证功能介绍

设计实现基于公私钥机制的准入模块设计，可以确保系统的安全性和数据的完整性，保证 Hid input 设备共享时的安全性。仅有经过授权的主机才可加入连接，其流程图 9 所示，具体流程如下：

1. 客户端生成公私钥对
    a) 客户端首次启动时，使用 RSA 算法生成一对公私钥（K_{Cpub}、K_{Cpri}）
    b) K_{Cpri}保存在客户端本地，K_{Cpub}将用于身份验证
2. 客户端发起连接请求
    a) 客户端向服务器（Server）发起连接请求，同时携带其公钥K_{Cpub}
3. 服务器处理连接请求
    a) 服务器接收到连接请求后，提取客户端的公钥K_{Cpub}。
    b) 如果服务器拒绝该连接请求，则直接断开连接。
    c) 如果服务器接受该连接请求，生成一个随机序列 R 作为验证字符
    d) 服务器使用客户端的公钥K_{Cpub}对 R 进行加密生成密文$C = E(K_{Cpub}, R)$。
    e) 服务器将加密后的密文 C 返回给客户端。
4. 客户端处理验证消息
    a) 客户端接收到加密的随机序列 C 后，使用K_{Cpri}进行解密，$R' = D(K_{Cpri}, C)$得到序列R'。
    b) 客户端将解密后的结果 R' 发送回服务器。
5. 服务器验证解密结果
    a) 服务器接收到客户端发送的解密结果R'
    b) 服务器将收到的解密结果R'与 R 进行比较。
    c) 如果两者一致，则验证成功，允许连接。如果不一致，则验证失败，拒绝连接。

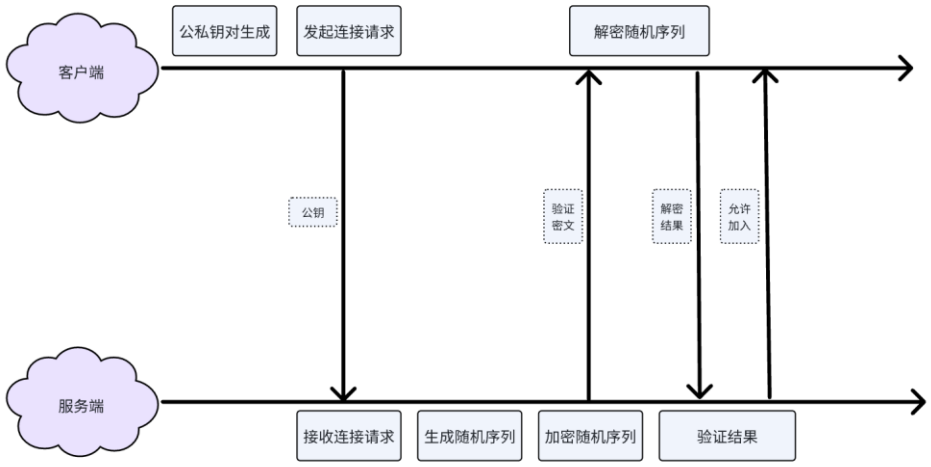


图 9 认证机制流程图 A

以上机制可以防止未经授权的客户端伪装为授权客户端加入连接，但无法处理恶意主机伪装为服务端，如需应对此安全风险，可增加安全级别，在客户端上存储服务端的公钥，在此情况下连接流程如图 10，具体流程如下：

1. 客户端提前存储服务端公钥
    a) 客户端在初始配置阶段，存储服务端的公钥K_{Spub}
2. 客户端发起连接请求
    a) 客户端生成一个随机序列R_a
    b) 客户端使用服务端的公钥K_{Spub}加密R_a，生成密文$C_a = E(K_{Spub}, R_a)$
    c) 客户端向服务器发起连接请求，携带自身的公钥K_{Cpub}和加密后的C_a，消息体为$\{K_{Cpub}, C_a\}$
3. 服务器处理连接请求
    a) 服务器接收到连接请求后，提取并验证客户端的公钥K_{Cpub}。
    b) 如果服务器拒绝该连接请求，则直接断开连接。
    c) 如果服务器接受该连接请求，使用私钥K_{Spri}解密C_a，得到序列$R_a{}'$
    d) 服务器生成一个随机序列R_b，使用客户端的公钥K_{Cpub}加密R_b，生成密文$C_b = E(K_{Spub}, R_b)$

e) 服务器返回消息体$\{R_a', C_b\}$

4. 客户端验证服务器响应

a) 客户端接收到服务器的响应后，验证解密后的R_a'是否与最初生成的一致。若不一致则放弃连接请求

d) 一致则客户端使用私钥K_{Cpri}进行解密，得到序列$R_b' = D(K_{Cpri}, C_b)$。

b) 客户端将解密后的R_b'返回给服务器。

5. 服务器验证客户端响应

a) 服务器接收到客户端发送的R_b'后，验证其是否与最初生成的R_b一致，如果一致，则允许连接。如果不一致，则拒绝连接。

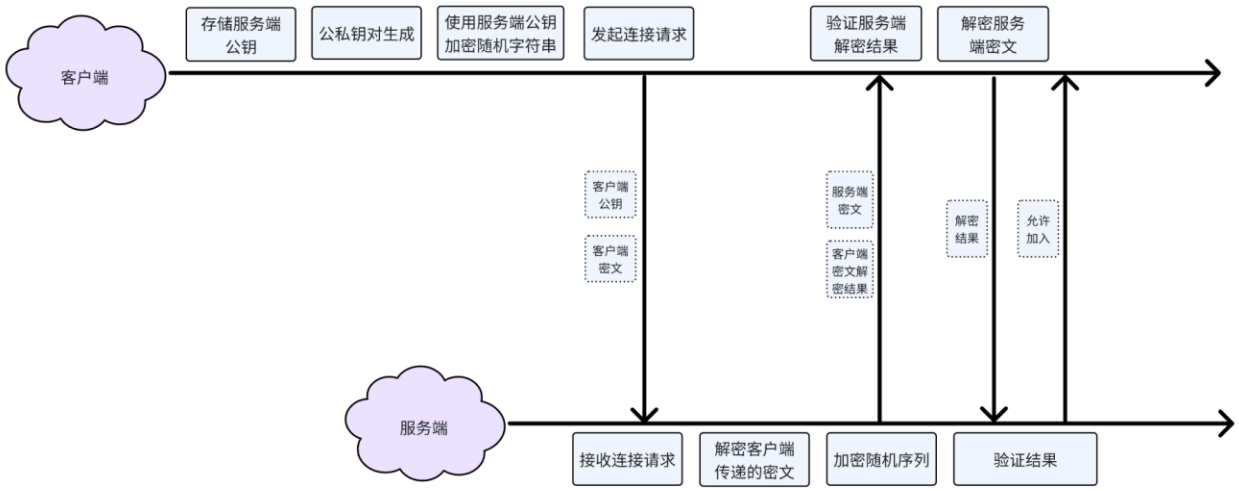


图 10 认证机制流程图 B

经过以上处理可以保证连接的安全性，此外还需保证数据的安全性，确保数据不被泄露不被伪造，方案流程如图 11，具体流程如下：

1. 服务端生成控制信息并签名

服务端使用自己的私钥K_{Spri}对控制信息$M_{control}$进行签名，生成签名S，将签名附加到控制信息上，形成消息$\{M_{control}, S\}$

$$S = \mathrm{Sign}\left(K_{Spri}, M_{control}\right)$$

服务端使用目标客户端的公钥K_{Cpub}对消息进行加密，生成密文C，将加密后的密文 C 发送给客户端

$$C = E\left(K_{Cpub}, \{M_{control}, S\}\right)$$

2. 客户端解密和验证签名

客户端接收到密文 C 后，使用自己的私钥K_{Cpri}进行解密，得到消息$\{M_{control}, S\}$，客户端使用服务端的公钥K_{Spub}验证签名S，如果验证通过，客户端接受并处理控制信息$M_{control}$。

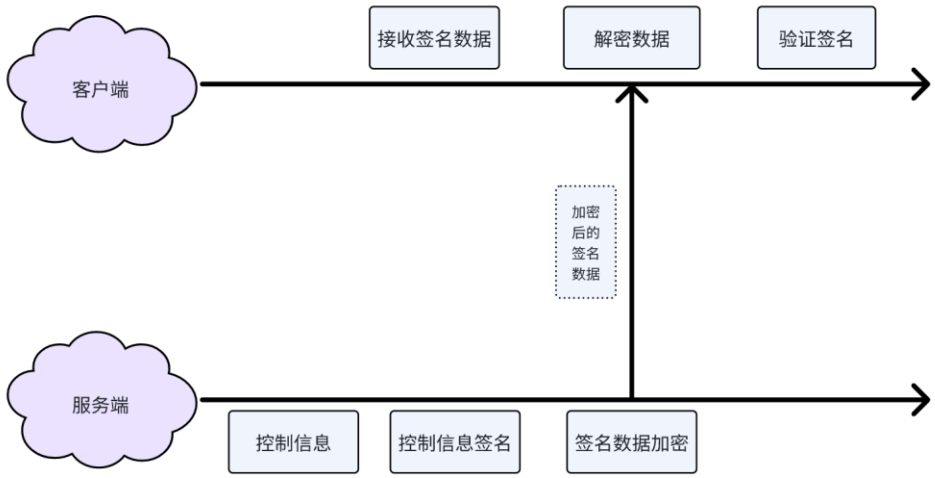


图 11 数据签名加密流程图

此外由于剪切板内容涉及到多台主机之间的共享，为保证整个过程的安全性，还需对剪切板内容进行处理，处理流程如图 12，具体流程如下：

1. 客户端加密剪切板信息

客户端使用服务端的公钥K_{Spub}对剪切板信息$M_{clipboard}$进行加密，生成密文$C = E\left(K_Spub, M_{clipboard}\right)$。将加密后的密文$C$发送给服务端。

2. 服务端解密剪切板信息

服务端接收到密文C后，使用自己的私钥K_{Spri}进行解密，得到剪切板信息$M_{clipboard}$。

3. 服务端分发剪切板信息

服务端分别使用各个目标客户端的公钥K_{Cpub_i}对剪切板信息$M_{clipboard}$ 进行加密，生成对应的密文$C_i = E\left(K_{Cpub_i}, M_{clipboard}\right)$。将加密后的剪切板信息$C_i$发送给各个客户端。

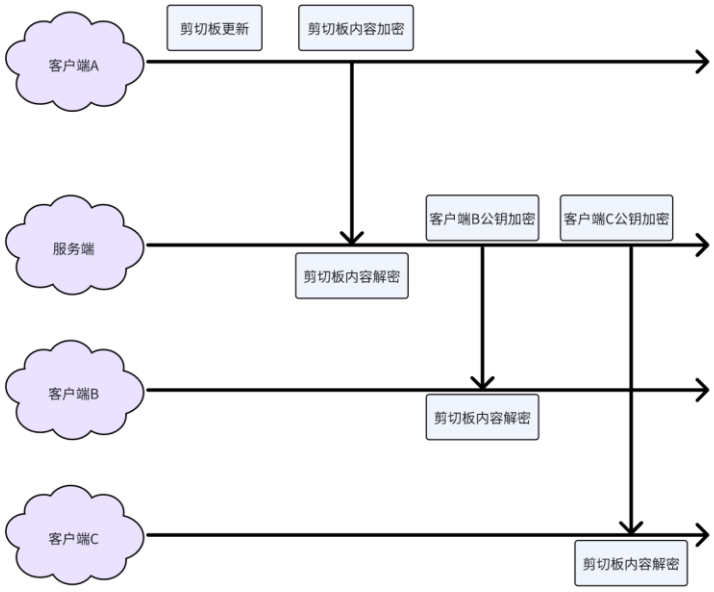


图 12 剪切板内容加密机制

3.1.4 文件拖拽共享功能介绍

为了实现文件拖拽共享功能，每个主机的桌面上存在一个文件共享区域，服务端基于队列机制在多线程环境下负责维护整个主机群的共享文件列表，当有文件拖入时记录文件路径及文件所在主机，当其他主机上进行文件拖出时，获取文件所在主机的 ip 和路径，借助网络传输模块获取文件内容。具体设计方案如下：

- 文件拖拽区域：每一台主机都显示一个文件拖放区域，区域内的文件信息在多台主机之间共享同步。利用 Tkinter 的拓展 TkinterDnD 创建了一个具有下沉边框的拖放区域(Python Software, 2024)，并注册了 DND_FILES 以接收文件拖放事件。
- 文件列表框：文件列表框用于显示拖放进来的文件信息。利用 Tkinter 的列表框组件，用于显示在共享剪切板上的文件路径和源文件所在的主机 IP 地址。
- 文件拖放处理：on_drop 方法在文件被拖放到窗口时调用，将拖放的文件路径解

析成列表。对于每个文件路径，创建一个 fileDto 对象（假设是一个数据传输对象，封装了文件信息），然后调用 display_file_list 方法显示文件信息，并将文件对象放入共享队列 shared_queue 中。

- 文件拖拽到相应目录：通过 on_listbox_press、on_listbox_move、on_listbox_release 三个方法处理列表项的拖拽操作，完成将文件从原路径复制到指定目录的任务。这里用户可以在菜单栏指定本地保存的目录，当用户执行鼠标拖动操作将文件列表从共享剪切板拖出时，被控机向指定 IP 的主机发送请求并获取到 base64 编码的 json 格式的源文件数据，并执行解码将文件保存在相应的目录中。
- 数据共享：通过共享队列 shared_queue，可以在多线程环境中共享文件传输对象，每次拖放文件时，fileDto 对象会被放入队列。这样，其他线程就可以从队列中读取文件信息，实现文件的共享和传输。

3.2 软件界面

项目基于 PyQt 框架构建了桌面软件进行人机交互，从而便于用户查看主机信息并配置屏幕相对位置，更好地实现设备共享。

首先，软件将主控机和被控机两部分功能模块集成起来，并在桌面软件上提供了选择接口，作为软件的入口界面，设计如图 13 所示：

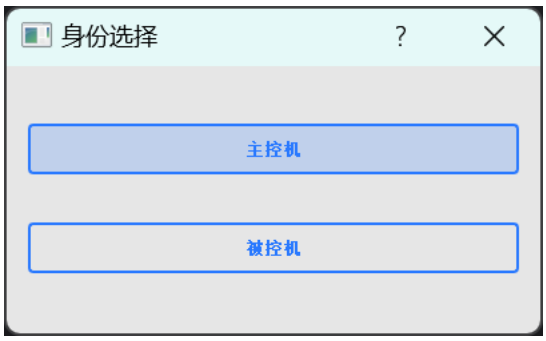


图 13 入口 GUI 界面

在入口界面中，提供了主控机和被控机两种角色供用户进行选择，当用户点击下方“进入”按钮时，根据其选择的角色转入相应模块执行。在选择受控机（被控机）角色的情况下，该主机会加入共享设备集群，并向服务器发送信息宣布其已上线或请求加入。在

选择主控机（服务器）角色的情况下，用户能够实时地查看集群内的被控机信息并配置其相对位置，主控机界面如图 14 所示：

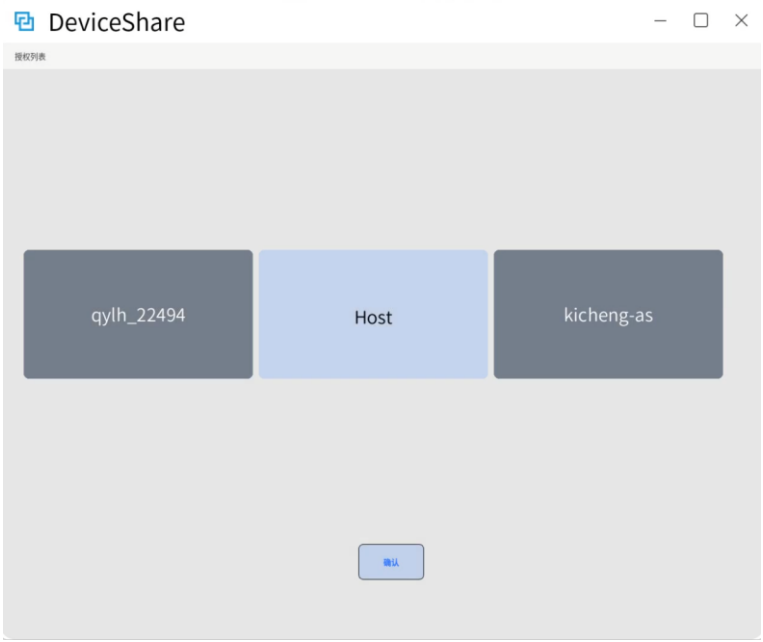


图 14 被控机相对屏幕位置配置界面

主控机角色下的 GUI 界面主要提供了两方面功能，分别是查看被控机状态以及配置相对位置。

1. 软件设计了位于软件坐上角的授权列表，展示被控机的在线、离线状态，此列表悬停在软件左上角，通过菜单栏的“授权列表”控制其显示和隐藏。
2. GUI 的主体是配置屏幕相对位置功能，在这一部分中，考虑到被控机相对服务器屏幕有上下左右四种相对位置，将界面设计成十字形，中心表示主控机屏幕，四个方向分别用 4 个矩形框表示相应的屏幕，用相应位置是否为空表示该方向是否配置了被控机，并对离线状态的被控机进行一定的虚化处理以直观地表现其状态。当用户拖动图像时，可以将其移动至不同方向的矩形框，以修改对应被控机的相对位置，为了提供用户友好的图形操作界面，软件还进行了一定的优化处理，如移动到某个矩形框附近时，对应矩形框高亮显示以提示用户，在此状态下释放鼠标，图形自动和中心图像，即服务器屏幕对齐，从而提供更好的用户体验。下方的确认按钮用于对修改的相对位置信息进行保存。

为了方便处于主控机角色下的用户实时地获取被控机状态，软件还设计了消息弹窗，在被控机上线或下线时立即通知服务器。此外，软件还提供了托盘图标，通过右键即可进行简单的登录或退出，进一步简化了操作，其效果如图 8 所示：

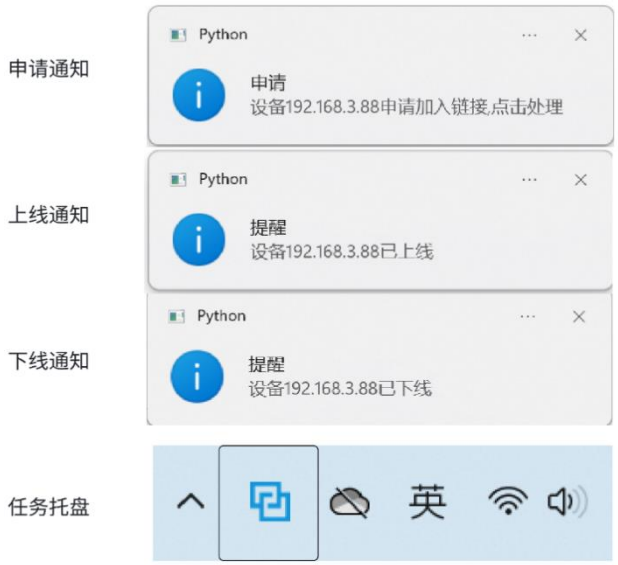


图 15 通知弹窗及系统托盘

当作为被控机的主机首次上线时，可以发出加入集群的申请，服务器对此进行处理，得到同意的被控机会被主控机加入其授权列表。此后，被控机的上线或下线消息均会发送至服务器，并在 GUI 界面上修改其状态信息。

第 4 章 软件测试

4.1 软件使用说明

针对 x86 架构的 Windows、OpenKylin 操作系统，我们打包构建了可执行程序，可在 Release 界面下载合适的版本。

若在 Linux 下运行，采用脚本 run.sh 启动程序，将 run.sh 复制到 dist 目录下，执行 sudo chmod 777 run.sh 赋予执行权限，执行 bash run.sh 启动程序,windows 下无需执行此步骤,直接运行 exe 文件即可。

若构建的版本无法支持目标机器，可选择源码运行或自行打包。该方案需具备 Python 3 环境，具体步骤如下：

1. 获取项目源代码

2. 使用 pip install -r requirements.txt 命令安装依赖

3. 执行 python deviceShare.py 启动程序

4. 安装 pyinstaller: pip install pyinstaller

5. 使用 pyinstaller 打包目标程序: pyinstaller deviceShare.spec

6. 运行 dist 目录下生成的可执行文件

7. 将 resources 目录复制到 dist 目录下

使用时，将主控机和被控机连接到同一局域网环境下，保证两台机器能够互相 ping 通，分别按照要求启动软件，选择各自的角色。

1. 被控机上线后，主控机将弹出通知，点击通知允许被控机连接。
2. 右键单击主控机右下角的桌面托盘，点击设置，可以看到被控机屏幕位置示意图，可拖动修改位置，修改完成后点击确定。
3. 在主控机上将光标移动到靠近被控机方向的边缘即可进入被控机。
4. 在被控机上将光标移动到靠近主控机方向的边缘即可回到主控机。
5. 在主控机和被控机上分别右键单机托盘图标选择退出即可关闭软件，注意在 open Kylin 环境下由于收到消息提醒，此时托盘图标可能变成小灯泡形式。

注意 Kylin 操作系统在安装 python 的 evdev 依赖时可能出现错误，请选择安装预编译版本 evdev-binary，参考 https://python-evdev.readthedocs.io/en/latest/install.html

此外该系统也支持运行在树莓派，Jetson 等小型主机上，以在不便连接外设的电脑场景下使用。

图 16 小型主机示意图

4.2 软件测试说明

项目在 Windows10、Debian12、Ubuntu20.4、MacOS、openKylin 等多个平台进行运行测试，服务端主机连接 usb 键鼠，所有主机以无线局域网的形式连接，测试环境如图 11 所示。

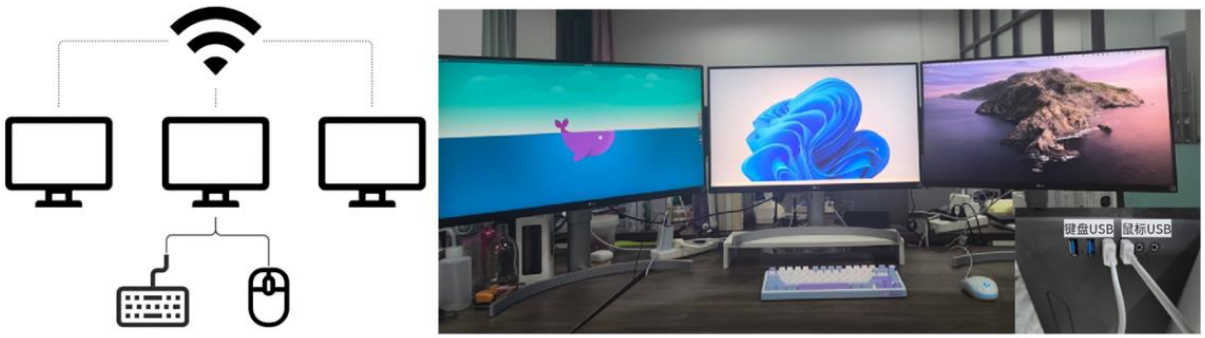


图 17 测试环境

4.3 软件测试结果

为了确保项目运行的正确性，在测试环节使用不同的测试环境对程序的运行进行了测试，检验其运行流程，从功能、性能、兼容性、稳定性等方面进行测试。

4.3.1 功能测试

功能测试主要针对多屏幕管理、设备监听、鼠标控制、键盘控制、剪切板控制等功能模块进行。

1. GUI 功能测试

此模块用于实现多台主机进行设备共享时，通过可视化方式操纵屏幕间的相对位置，实现服务器主机对被控机的不同控制方式。

表 8 GUI 功能测试

测试功能	测试步骤	结果
身份选择	启动软件，分别选择成为主控机和被控机	软件正常启动，分别进入主控机和被控机程序。
连接请求	被控机启动，发送连接申请 主控机分别选择同意和拒绝	点击同意后设备加入，显示上线通知。点击拒绝后设备无法加入。
连接记忆	同意被控机连接后，被控机重新上线	无需再次确认，直接显示设备上线通知。
设备加入监听	在主机上启动 client 程序，通知服务器	服务器监听到主机加入并在可视化界面添加对应屏幕，并显示桌面通知。
相对位置控制	拖动被控机对应图像	通过鼠标拖动操作实现了被控机屏幕相对主机的位置改变
位置保存	点击确定	被控机的信息及相对位置，鼠标进行相应移动发现位置修改成功。

2. 设备监听功能测试

被控机启动时，可以通过广播方式通知服务器其加入了设备共享，此模块用于实现该功能并实现对多被控机的管理。

表 9 设备监听测试

测试功能	测试步骤	结果
设备加入	在被控机启动 client 程序	服务器正常接收被控机的广播。消息并将其加入客户列表
设备退出	中止 client 程序	主控机检测到被控机通信中止，将其从客户列表删除

3. 鼠标控制模块

此模块用于实现多主机的鼠标共享，在主控机，当控制鼠标移动到特定位置后（具体取决于多屏幕管理中的相对位置设置），可以通过网络通信控制对应的被控机，并需要实现鼠标在不同主机间的自由切换。

表 10 鼠标控制测试

测试功能	测试步骤	结果
主控机鼠标控制	在主控机移动鼠标，并进行点击等操作	屏幕光标可随着鼠标控制移动，且点击、滚轮等操作均正常执行
切换至被控机	在主控机移动鼠标至屏幕右侧	主控机的光标移动到固定位置且不可移动，被控机端光标位置可随着鼠标移动移动
鼠标移动	在切换至被控机后进行鼠标移动操作	被控机端光标可以随着主控机的鼠标进行移动。

鼠标点击	在切换至被控机后进行左键右键点击操作	在被控机器上鼠标点击事件可以正确接收且处理，同时主控机阻塞响应。
鼠标滚轮	在切换至被控机后进行鼠标滚轮操作	在被控机器上滚轮事件可以正确接收并处理，同时主控机阻塞响应。
鼠标拖动	在切换至被控机后进行鼠标拖动操作	在被控机器上鼠标拖动可以正确接收并处理，同时主控机阻塞响应。
回到主控机	在对应模式下将光标移动至屏幕左侧	被控机端光标无反应，鼠标可以正常控制主控机

4. 键盘控制模块

此模块用于实现多主机的键盘共享。

表 11 键盘控制测试

测试功能	测试步骤	结果
主控机鼠标控制	在主控机进行键盘点击、press、release 等操作	键盘操作均生效
切换至被控机	在主控机移动鼠标至屏幕右侧	主控机的光标移动到固定位置且不可移动，被控机端光标位置可随着鼠标移动移动
被控机键盘点击	在切换至被控机后，在记事本等程序上测试键盘点击	主控机的键盘按键可被接收并能正常在被控机输入
被控机组合键	在被控机进行组合键测试 ctrl+c	事件可被正常处理

回到主控机	在对应模式下将光标移动至屏幕左侧，并进行键盘测试	键盘操作仍可在主控机生效

5. 剪切板控制模块测试

表 12 剪切板控制测试

测试功能	测试步骤	结果
剪切板内容获取	在主控机控制被控机，通过 copy 等操作获取	剪切板内容可被获取
剪切板内容设置	在主控机通过 paste 等操作设置剪切板内容	剪切板内容可以正常传输

4.3.2 性能测试

在性能测试中，我们测试了鼠标和键盘在共享时的操作传输延迟，该延迟定义为主控设备发生操作到被控设备产生响应的时间间隔，通过在事件传输时添加时间戳来测试时间，因两台设备间存在时钟偏差，在测试时借助 clockdiff 工具测试偏差值，并在计算延迟时对时钟偏差进行补偿，并测试 20 次操作的平均值，测试结果如下：

表 13 操作延迟测试

测试项	平均传输延迟
鼠标点击延迟	32ms
鼠标移动延迟	41ms
键盘输入延迟	36ms

鼠标的点击和输入延迟对使用体验的影响相对较弱，根据调研，市面上的普通有线鼠标的移动延迟大约在 30ms 左右，而专业电竞鼠标可以达到 10ms 以下，从测试结果来

看，共享操作会对鼠标的响应速度产生影响，但此影响在日常办公时基本无感，可满足日常办公需求。

4.3.3 兼容性测试

考虑到项目在多平台上的兼容性，在测试时使用了不同的操作系统，试运行并调试了项目代码。

测试环节使用 OpenKylin1.0.2、Windows11、Debian12、Ubuntu20.04、MacOS 13 四个平台均运行了程序，并尝试在不同平台上分别运行被控机和服务器，结果显示，项目可以实现在以上平台上的兼容。

第 5 章 实现难点说明

DeviceShare 在实现多设备之间的键鼠共享软件 KVM 时，涉及到跨设备、跨系统、通用性和安全性等多个方面。项目的重难点及解决方案如下

5.1 项目重难点

5.1.1 兼容性和通用性

在系统 API 和驱动差异性上，不同操作系统（如 Windows、macOS、Linux）以及 Linux 不同的桌面协议(Wayland、X11、Xorg 等)下有不同的驱动机制(Linux community, 2024)，这会影响键鼠的输入和输出，处理这些差异要编写针对不同操作系统的适配性程序；此外在输入设备对操作系统的兼容性上，键盘鼠标本身可能会具有不同的布局和功能键，例如相同的键盘键位对于 Windows 操作系统和 MacOS 操作系统中可能会有不同的意义。在权限和安全的差异性上，不同操作系统对硬件访问有不同的权限限制和安全机制，比如在 Wayland 环境下会限制应用程序对输入设备的访问。

5.1.2 快速配置

由于软件使用的网络环境可能比较负责，手动配置通信地址会给非专业用户带来困扰。产生额外的学习成本，需要实现快速的配置方案，来降低软件的使用难度。

5.1.3 安全性

在一些保密场景下，数据安全是十分重要的，因此在不同设备之间传输键盘和鼠标数据时，需要确保数据的保密性和完整性，防止敏感信息泄露。在设备的访问控制上，要考虑防范病毒软件和脚本程序伪装成主控机或被控机进行恶意攻击和破坏性操作，确保只有通过授权的用户和设备才能加入。具体来说可能存在以下三种风险：

1. 恶意机器伪装成被控机加入连接
2. 恶意机器伪装成主控机控制其他主机
3. 恶意窃取软件运行过程中的网络数据（如键盘输入信息，剪切板内容）

5.1.4 低延迟通信

在多设备间实现键鼠共享，要求系统能够实时响应用户的操作，低延迟是关键指标。不同设备的硬件性能和网络环境也会影响通信的实时性。

5.2 解决方案

DeviceShare 为解决以上难题，从兼容性、通用性和安全性上提供了针对性的解决方案。

5.2.1 兼容性解决

为了保证软件的兼容性采取了以下解决措施：

1. 使用 Python 语言开发，一套代码可在多个平台上运行和打包
2. 采用跨平台的开发包，如 PyQT5、pynput 等
3. 针对 Wayland 环境进行单独适配，依靠 evdev、uinput 等更底层的方案进行输入设备的控制和监听。
4. 设计键码转换中间层，进行不同平台的键盘编码转换。

5.2.2 快速配置方案

采用基于 mDNS 广播的 ZeroConf 协议，系统启动时自动检测当前网络环境和设备配置，进行服务注册，被控机上线时自动发现潜在的服务，用户无需进行手动配置。

5.2.3 安全性

设计实现了公私钥加密认证机制进行主控机和被控机的身份验证及加密数据的交换，防止未经授权的访问，并保护键鼠和设备交互信息的机密性和完整性。

5.2.4 低延迟通信

采用基于 TCP/IP 的 Socket 编程，建立高效的点对点通信机制。使用高性能消息队列优化数据传输速度和稳定性；并在数据传输前对键鼠事件进行压缩，减少数据包的大小，从而降低传输延迟，使用高效的序列化协议来编码和解码数据。

总的来说，DeviceShare 实现多设备键鼠共享软件涉及多个复杂的技术挑战，包括跨设备兼容性、跨系统兼容性、通用性和安全性。通过设计抽象层、设计专用跨网络通信模块、使用跨平台技术、实现自动化用户配置、加强数据传输加密和身份验证，可以有效地解决这些难点，提供一个稳定、安全且易于使用的键鼠共享系统。

第 6 章 总 结

在整个项目过程中，我们依托 Gitlink 平台按照严谨的流程进行开发。整个项目经历了需求分析、架构设计、技术选型、设计开发、测试优化等多个阶段，在 6 个分支上进行了近 300 次 commit，最终实现了一个功能全面的 Hid Input 设备共享方案。

在整个项目的开发过程中我们的创新意识、协作和解决问题的能力有了进一步的提升。我们对开源精神有了进一步的理解和认识，也将继续激励我们未来投身开源项目中，凝聚智慧，推动技术进步、知识共享和社会创新。此外特别感谢 openKylin 社区在国产操作系统上提供的支持，感谢 Gitlink 提供的代码协作平台，感谢 pynput、pyevdev 等第三方开源库的开发者们。

目前 DeviceShare 已经完成了赛题的基本要求，并在赛题的基础上增加了设备发现、认证加密等额外功能，同时具备非常好的的跨平台兼容性，能够在搭载不同操作系统的主机间共享输入设备。性能可满足日常办公需求。未来团队将在以下方面继续进行完善该项目：

- 完成文件共享模块的设计与实现
- 解耦各设备共享模块，支持用户自定义开关相关功能
- 探索非局域网主机设备共享方案
- 优化代码质量，提升代码可读性，提高软件性能
- 在更多操作系统上进行测试，支持更多类型的系统

参 考

[1]. openKylin. openKylin document. https://docs.openkylin.top/en/home

[2]. Microsoft. 了解远程桌面协议 (RDP). https://learn.microsoft.com/zh-cn/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol [2023-12-26]

[3]. Ugreen. UGREEN 4 Port USB 3.0 5Gbps High-Speed Switch Selector. https://uk.ugreen.com/products/ugreen-4-port-usb-3-0-5gbps-high-speed-switch-selector [2024]

[4]. ATEN. 2-Port USB 3.0 4K DisplayPort KVMP™ Switch (Cables included) - CS1922. https://www.aten.com/global/en/products/kvm/desktop-kvm-switches/cs1922 [2024]

[5]. Belkin. F1DS102L and F1DS104L User Guide. https://www.belkin.com/cn/support-article/?articleNum=3804 [2024]

[6]. Ubuntu. SynergyHowto. https://help.ubuntu.com/community/SynergyHowto. [2017-09-16]

[7]. ShareMouse. Share one Mouse and Keyboard with Multiple Computers. https://www.sharemouse.com [2024]

[8]. Palmér. Pynput. https://pynput.readthedocs.io/en/latest/index.html [2024-03-10]

[9]. Gvalkov. Pyevdev. https://python-evdev.readthedocs.io/en/latest/. [2024-03-08]

[10]. Cheshire. Multicast DNS. https://www.rfc-editor.org/rfc/rfc6762 [2013-2]

[11]. Pypi. PyQt5. https://pypi.org/project/PyQt5/. [2024-7-19]

[12]. Ron Rivest et. 1983. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems[J]. Communications of the ACM. 26: 96-99

[13]. Wayland. https://wayland.freedesktop.org/.

[14]. Sweigart. Pyperclip's documentation. https://pyperclip.readthedocs.io/en/latest [2014]

[15]. IETF Zeroconf. Zero Configuration Networking (Zeroconf). http://www.zeroconf.org [2024]

[16]. Python Software Foundation. tkinter.dnd — Drag and drop support. https://docs.python.org/3/library/tkinter.dnd.html [2024-07-31]

[17]. Linux community. The Linux Kernel. https://www.kernel.org/doc/html/latest/usb/usbip_protocol.html.