中国研究生网络安全创新大赛

作品报告

作品名称：基于物理层安全的无线体域网安全系统设计与实现

提交日期：2023年11月8日

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。一经发现，取消作品参赛资格。

目　　录

摘要

当前，无线体域网广泛应用于解决老龄化加剧下医疗资源分布不均、医疗健康监测问题。本作品以其面临的身份伪造、数据窃取、隐私泄露等风险可能危及病人生命的安全形势为背景，针对现有身份认证和密钥协商方案存在Inter-WBAN层缺乏安全保障、无法抵御仿冒攻击、密钥分发复杂等问题，提出了基于物理层安全的无线体域网安全系统。系统具有两大技术特色：利用物理特性作为设备指纹实现身份认证和利用信道互易性实现密钥共享，其创新性在于：

1. 将物理指纹首次用于无线体域网内Inter-WBAN层的身份认证，无需对终端改造、无需复杂计算，突破了Inter-WBAN层缺乏安全保障的瓶颈；
2. 利用设备物理指纹的唯一性和不可克隆性抵御身份认证中的仿冒攻击；
3. 解决了设备认证基于信道的稳定性与快速密钥生成基于信道衰落过程中的不稳定性的矛盾；
4. 利用信道互易性实现轻量安全的密钥共享，无需预先配置、无需第三方参与、无需硬件修改、具有天然安全性，解决了密钥分发复杂的难题。

在静态、动态、非视距等多种场景验证了此系统用于身份认证的准确率、生成密钥的一致性、随机性、安全性。此系统还可推广应用于局域网的多种场景，如电力局域网、银行机关内网等，也可以叠加到现有安全机制之上，实现安全加固。

第一章 作品概述

1.1 背景分析

国际上，通常将60岁以上老人达到总人口的10%，或65岁以上老人占总人口的7%，作为国家和地区进入老龄化的标准。随着出生率的下降和期望寿命的增加，世界人口老龄化进程正在加速发展，据世界卫生组织预测2050年加拿大、波兰、瑞典、中国等各国60岁及以上老年人人口占比将超过30%，成为老龄化最严重的国家，如图1-1所示。

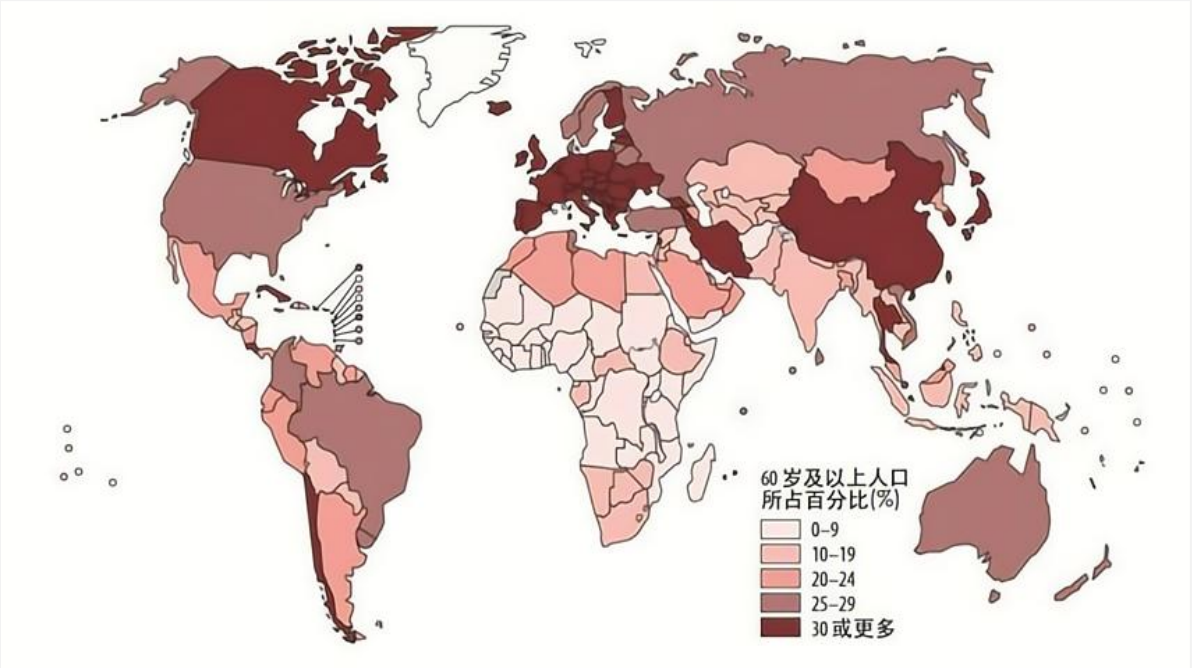


图1-1 2050年世界60岁及以上人口占总人口比估计图

根据世界卫生组织数据显示，到2030年，世界上每6个人中就有1个人的年龄在60岁及以上，而随着人口老龄化程度加剧，与年龄密切相关的疾病，诸如脑卒中、关节炎等慢性（非传染性）疾病所累及人口的绝对数字将持续增加。据世界卫生组织的数据统计，死于患慢性非传染性疾病(如心血管疾病等)的人数比例是全球的总死亡人数的71%，年龄在30-69岁中，每年死于该类型疾病的人有1500万，其中发生在中低等收入国家的这类死亡现象高达85%。近两年受新冠疫情的影响，医疗资源愈加紧张，大多数国家都面临着很多医疗和健康问题，如偏远地方医疗资源匮乏且看病难和看病贵、疾病的预防和监测不足等。在2019年全球死于心血管疾病的人中有一半以上是发

生在亚洲国家。此外，其他疾病的死亡率也居高不下，如糖尿病等。而贫穷偏远的农村地区死亡率又高于城镇，这往往是发现预防疾病过晚，导致错过了治疗的最佳时机。因此，对身体健康的实时监测和远程医疗服务就变得尤为重要。

研究发现很多慢性疾病可以通过体检和长期生理观察的方式做到疾病的早发现与早期治疗，以减少疾病的致死率[1]。传统的体检方式需要患者频繁去医院，这不仅加大了患者的时间开销和经济开销，也加大了医院的医疗负担。近年来，无线通信技术和传感器技术迅速发展，无线体域网（Wireless body area network，WBAN）是上述问题较好的解决方案。

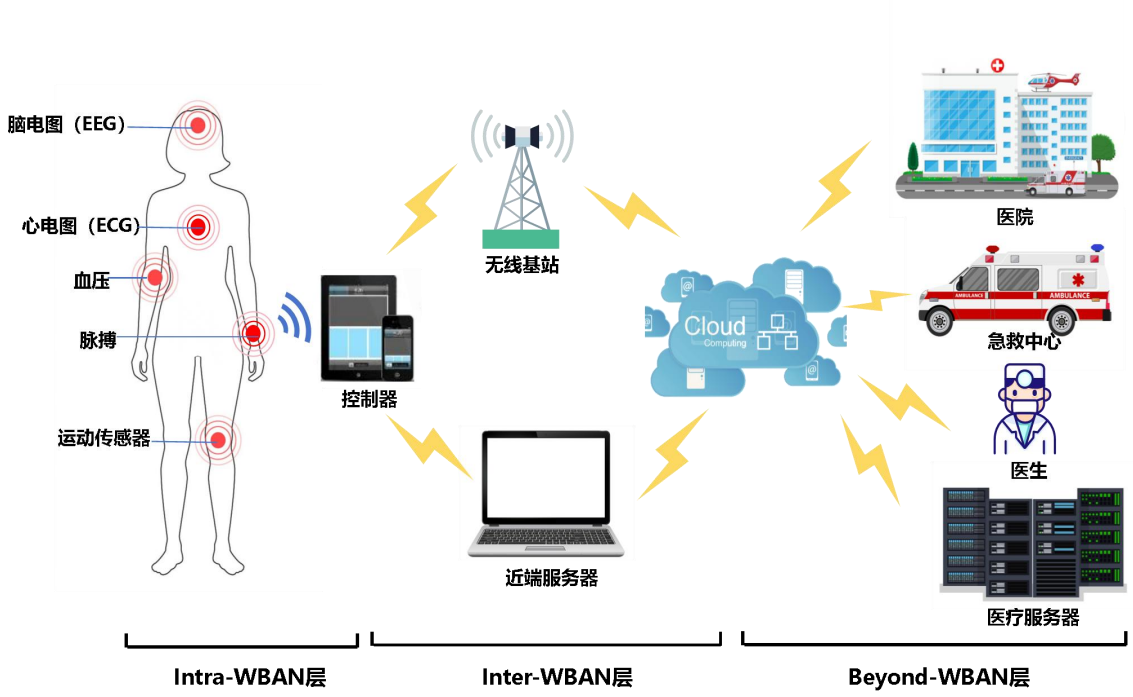


图1-2 WBAN 体系结构

无线体域网是一种短距离无线通信网络，如图1-2所示，实现病人健康检测功能的WBAN由穿戴在患者身上或植入患者体内的传感器节点、控制器节点（Controller Node，CN）、移动节点（Mobile Node，MN）、医疗服务器等组成的三层结构：第一层是由传感器节点和控制器节点组成的Intra-WBAN层，第二层是由控制器节点和移动节点组成的Inter-WBAN层，第三层由移动节点和医疗服务器组成Beyond-WBAN层用于连接枢纽节点和应用服务提供商，为用户提供医疗服务[2]。

重量轻、体积小、功耗低、可交互且智能的可穿戴传感器用于持续测量特定的生理参数如温度、血压、心率、心电图（Electrocardiogram，ECG）、呼吸频率等[3]。由于体域网中传感器节点的存储空间小、计算及通信能力有限，一般不会用来存储大

量数据和进行复杂计算等操作。因此，传感器收集到的生理信号数据，通常会利用短距离无线通信技术(例如Bluetooth）传输到控制器节点进行存储和处理，以实现进一步的转发。

控制器节点通常会放置在用户身体上或放置在身体附近且距离身体很近的位置，可能是例如智能手机、智能平板这类的手持设备，具有良好的存储和计算能力。作为Intra-WBAN层和Inter-WBAN层的接口设备，控制器节点负责将Intra-WBAN层传感器收集到的数据进行汇总和处理，并利用Bluetooth技术或Wi-Fi技术等传送到移动节点。

移动节点通常为近端服务器或远端无线基站，移动节点将来自控制器节点的数据整合发送给医学专家、急救中心、医疗服务器等，医务人员可以实时获取到患者的病理数据并对其做出医疗诊断反馈给用户，使用户能够及时用药或就医，在发生紧急情况时，还能协助通知其家人和医疗机构等。

WBAN提供了不受限制的移动自由，患者不必一直卧床，可以在房间里自由走动，甚至可以离院由医护人员远程监控身在家中的残疾人、老年人、手术后康复的患者或高发病人群的重要体征，以实现对患者身体状况的评估[4]。WBAN技术为患者用户提供的疾病诊断和治疗服务，能极大程度上解决优质医疗资源紧张及分布不均的问题。但无线体域网中传输的数据都是患者身体健康情况的重要信息，具有极强的隐私性和敏感性，由于无线信道的开放性攻击者可能通过链路层窃听或篡改敏感和机密数据信息，或由于缺乏身份认证被攻击者伪造身份查看并获取数据，一旦攻击者入侵系统，数据的机密性和完整性被破坏，不仅会泄露用户的隐私敏感信息，甚至会对用户的生命健康造成威胁[5]。因此在WBAN中交换信息的安全性和隐私性的问题亟需解决。为了解决这些问题，需要在数据交换前需要建立会话，进行相互的身份认证以确保对方是无线体域网中的合法节点。在确认对方身份的合法性后，会话的双方需要共同获得一个会话密钥，用于加密传输的数据。

目前国内外针对WBAN的身份认证和密钥协商的研究工作可以分为三大类:基于密码学的方法、基于生物特征的方法以及基于信道特征的方法。基于密码学和基于生物特征的方法能较容易同时实现无线体域网中的设备认证和密钥协商。其中传统基于密码学的方案往往依赖预置密钥，如果系统中的设备受到物理破坏则会泄露设备中的预置密钥，让攻击者有机可乘，而且这种方法通常都需要较高的计算开销或复杂的密钥管理机制。基于生物特征的方法能有效克服上述缺陷，但是基于生物特征的方案利用

用户的行为或生理特征来确保设备通信安全性，这就使得体域网中设备必须具有相同类型的传感器硬件。此外，即使拥有相同类型的传感器，不同设备之间也会因硬件差异导致测量精度不同，这将给信号处理带来较大的挑战。而基于信道特征的解决方案基于更简单的密钥协商协议，并且使用更简便的计算就能实现设备认证和密钥协商，但其认证原理基于体内外信道的区分因此设备认证局限于Intra-WBAN层，无法保障Inter-WBAN层安全[6]；其次基于信道特征的解决方案在密钥协商时多使用MAC层信息接收信号强度（Received Signal Strength，RSS）作为密钥随机源，但基于RSS的密钥生成最为突出的弱点即是粗粒度数据导致的低密钥生成速率和小密钥容量[7]，以及需要额外的随机性补充。少数基于物理层信道状态信息（Channel State Information, CSI）的密钥协商方案其提取工具需要电脑外设或需要硬件改造，无法适于无线体域网轻量级的需求。同时，有研究曾经提出基于无线信道特征同时实现设备认证和密钥协商的难题:设备认证基于通信信道的稳定性与快速的密钥生成基于信道衰落过程中的不稳定性是矛盾的。因此，鲜有研究能同时实现无线体域网中设备认证和密钥协商。另外，近年来人们对WBAN的研究取得了显著的成果，但大多数关键协议都基于AES、RSA、ElGamal、ECC、Paillier等，其计算成本昂贵，大量计算导致效率低下。考虑到WBAN内设备在计算能力和通信能力上存在资源约束，因此迫切需要解决WBAN中的身份认证与密钥协商协议轻量化和安全性的要求。

1.2 相关工作

1.2.1 身份认证机制

早期关于WBAN身份验证的研究工作基于传统的密码学，这类方法依赖于预分发的密钥、加密和解密算法[8][9]。2014年，Liu等人[10]提出了两种在无线体域网中使用无证书签名（CLS）的远程身份认证方案。但该种方案随后被证实无法提供匿名性，传输用户身份信息与常量值相关，容易遭受到窃取攻击[11]。为了突破这一局限，He等人[12]提出了一种可证明安全的身份验证方法，其中验证数据存储在网络管理器上。2019年，Arfaoui等人[13]提出了一种针对WBAN中正常情况和紧急情况的上下文感知身份验证方法，但该方案容易受到中间节点仿冒攻击。Umar等人[14]提出两种基于RSS信息和ZKP的混合身份验证方案能防御仿冒攻击。尽管这些方案在计算上很难被破解，但WBAN中的

设备缺乏足够的资源来处理其复杂的计算。

为了克服上述缺陷，有学者提出利用人体生理信号例如心电图（ECG）生成共享密钥，两个设备分别测量同一个人的相同生物特征，并将它们进行比较以进行相互认证。Choi等人[15]从ECG信号生成八个心跳功能特征并用于设备验证。然而，感知相同的人体生理信号会造成硬件成本的大幅提升同时传感器的安放位置也会受到限制。例如，ECG信号的感知需要靠近心血管。Peris-Lopez等人[16]提出了一种基于ECG的连续用户识别系统。Gyu Ho等人[17]使用初级回归分析来消除由用户呼吸引起的提取ECG信号的基线变化噪声，以实现准确的用户身份验证。基于生理特征的方案尽管无需复杂的计算但其显著的缺点是它们需要额外的ECG传感器。

近年来，也有学者提出基于用户的运动模式进行身份认证。Revadigar等人[18]利用车载加速度计传感器和用户独特的步行方式（即步态）来实现身份认证。Sun等人[19]使用惯性传感器提取的步态信号设计了一种基于步态的身份验证方案。基于用户的运动模式的方法要求指定的传感器同时需要指定的用户运动模式，存在一定的局限性。

随后，有学者发现WBAN中体内体外信道的信号强度有显著的区别[20]，因此信道特征开始被考虑用于WBAN中设备的身份认证。其应用的基本原理是对于发射器和接收器设备在同一主体上承载的体内信道，信号传播以爬行波为主，而对于体外信道因为发射器和接收器设备不在同一身体上，信号传播会受到多径和其他干扰的影响[21]。但此类方法的问题是无法保护Inter-WBAN层的通信。Inter-WBAN层中的两个合法设备控制器节点CN位于主体或主体附近而移动节点MN位于主体之外。因此，控制器节点和移动节点之间以及控制器节点和攻击者之间的信道均属于是体外信道，而体外信道的信号传播会受到多径和其他干扰的影响，这使得现有基于信道特征的身份认证方案无法区分体外设备移动节点和攻击者的信号。

综上，现有的加密认证方案计算复杂度高，非加密认证方案只能在Intra-WBAN层提供设备身份验证，Inter-WBAN层的安全缺乏有效保障，而Inter-WBAN层中的任何数据泄漏和设备仿冒攻击都可能危及患者的隐私和安全。其次，现有方案需要额外的传感器或特定的用户运动模式，在使用上有局限。

1.2.2 密钥协商技术

无线体域网中早期多使用传统密钥协商方案。此外，由于WBAN传感器节点的供电和计算处理能力受限，使用对称加密算法多于使用公钥和认证中心的非对称加密算法。随之而来需要解决的问题是如何在传感器节点和终端设备间共享密钥。传统的解决方案是出厂预配置或使用密钥管理体系。通过预先部署密钥参数来实现密钥协商，相较于动态生成密钥，该方案只需要消耗较少的系统资源。然而，受不同厂商硬件配置的差异和节点动态配对需求的影响，预配置在实际操作中非常不便，且无法随网络的变化而变化，不具备灵活性。使用密钥管理体系来实现密钥共享需要一个可信任的第三方存储密钥，这也会带来潜在的危险和连带责任。若采用Diffie-Hellman协议共享密钥[22]，对资源有限的传感器节点而言代价过于昂贵[23]。

为了克服上述缺陷，有学者提出利用人体生理信号生成共享密钥[24]。受此启发，心脏间脉搏间隔IPI(inter-pulseinterval)信号[25]、ECG(electrocardiogram)信号[26][27]相继成为生成密钥的随机信号源。但基于生理信息的密钥协商方案其原理为不同的传感器节点在同一时间采集人体的同一种生理信息，并对该信息进行处理以获得会话密钥，该方案局限于只能在Intra-WBAN层应用，无法用于保障Inter-WBAN层的数据机密性。此外，人体生理信号还可用于密钥协商[28][29]。然而，感知相同的人体生理信号会造成硬件成本的大幅提升，同时传感器的安放位置也会受到限制。

张朝阳等人[30]利用接收信号强度（Received Signal Strength，RSS）特征值仅能在通信双方共享的原理，提出了一种用于无线体域网内利用RSS提取密钥并通过IJS算法协商出共享密钥的方法，但该研究主要从密钥协议角度探讨了数据互易性，但并未深入涉及密钥生成的过程。基于RSS的密钥生成由于其数据的粗粒度将导致低密钥生成速率和小密钥容量，以及需要额外的随机性补充[7]。为了提高密钥的生成速率，Revadigar等[31]和Javali等[32]使用多个天线同时从无线体域网的多个无线信道收集RSS值，但他们需要额外的或特殊的硬件来实现。为了避免引入额外的高级硬件，Lai等[33]利用多个传感器设备协作，从多个信道中获得 RSS值，合成后生成共享密钥。

综上，传统的密钥协商方案缺少灵活性，在使用对称加密算法时面临密钥分发复杂困难或依赖于可信第三方；利用生理信号共享生成密钥局限于Intra-WBAN层，需要额外的传感器和指定的安放位置；已有的基于信道特性的密钥协商方案则多以RSS作为密钥源，密钥生成速率和随机性较低。

1.3 特色描述

基于物理层安全的无线体域网安全系统有着两大技术特色：一是创新性地将物理特性射频指纹应用于无线体域网的身份认证，二是首次将具有互易性的信道状态信息应用于无线体域网的密钥协商共享。该系统有着以下三大特点：一是指纹提取、密钥生成操作无需复杂计算具有轻量级的优势；二是身份认证得益于设备硬件的固有属性难以克隆伪造，密钥共享依赖于信道的时变性、空间去相关性具有物理层的天然安全优势；三是系统无需额外硬件修改可直接部署于无线体域网，也可推广至其余局域网场景，具有部署灵活可移植推广的特性。总的来说，本作品从物理层安全角度解决了现有无线体域网内Inter-WBAN层双向身份认证和会话密钥获得方案存在的复杂度高、易遭受仿冒攻击、计算量大、密钥协商困难等问题。

本作品的两大技术特色具体说明如下。

1. 利用物理特性实现身份认证

从设备硬件独特的物理特征会反映于Wi-Fi信号角度出发并利用信道状态信息中包含了收发设备硬件特性的特点，提取出设备的射频指纹用于身份认证，提取指纹时借助信道的互易性去除信道本身带来的干扰，减少了为抵御信道不稳定变化数据处理带来的特征损失，提高了认证准确率；还避免了传统基于加密的认证计算复杂、基于生理特征认证需要特定传感器、基于用户模式认证需要特定运动方式的弊端。另外，通过唯一、稳定、难以伪造的射频指纹匹配判断对方身份是否属实，可有效阻止不法设备通过伪装身份对无线体域网发起恶意入侵的威胁，杜绝了已有认证方式无法抵御仿冒攻击的问题，从而保障无线体域网的安全。

2. 利用信道互易性实现密钥共享

利用无线信道的互易性使得Inter-WBAN层通信双方仅需一次交互可获得密钥源，生成密钥的量化步骤可在己端进行，密钥协商也仅需一次交互，密钥生成全程相较于传统密钥管理体系无需可信第三方参与，相较于双方利用人体生理特征生成密钥，此方案硬件成本低同时不受设备安放位置的限制；相较于已有基于信道特性生成密钥的方案，所用密钥源细粒度更高、随机性更佳、维度由单值扩展到52个，密钥生成速率更高。

本作品有以下三大特点具体说明如下。

1. 轻量级

已有的应用于无线体域网的身份认证技术中，基于传统密码理论的加密认证方法计算量大，非加密的认证方法需要专用传感器、硬件。本作品中通信双方仅需通过一次交互获取无线设备的固有属性——射频指纹。射频指纹由设备内部包含的如电容、电感以及其他数字逻辑电路等电子元器件产生并依附于设备通信的Wi-Fi信号中，指纹提取仅需传输信道特性信号在频域计算比值，操作简单无需复杂计算，无需额外的传感器和特定的用户运动模式。

相较于现有的依靠预分配、可信第三方的密钥管理体系或生理特征共享的密钥协商技术，本作品提出的基于信道互易性共享生成的密钥能在不改变原有协议的情况下省去可信第三方密钥分发步骤，利用互易的信道状态信息仅需简单的协商信息交换和哈希值对比通信双方可获得一致的密钥。此方法优于需要大量交互和可信第三方的利用公钥和认证中心的非对称加密算法，避免了Diffie-Hellman协议共享密钥所需的计算资源。

2. 安全性

本作品利用设备的物理特性——射频指纹实现身份认证，射频指纹产生于设备芯片内部元件的容差、PCB板的走线、锁相环晶振引起的相噪、变压器线圈的绕制、滤波器的滤波特性、功率放大器和混频器引起的射频信号非线性等因素，即便是同一厂家同一批次生产的同类型设备其硬件特征也具有差异性，因此射频指纹无法被克隆且难以伪造和篡改，依靠射频指纹实现设备的身份识别能有效抵御仿冒攻击。其次，射频指纹的安全性不依附于计算复杂度，因此不受限于密钥泄露、算法泄露等产生的风险。

本作品利用物理层无线信道密钥生成技术来在合法双方间共享相同密钥。无线信道特征具有空间去相关性，即攻击者只有在距离接收方二分之一的波长之内的无线环境内窃听时，窃听信道才可能与接收方所在的合法信道具有很大的相关性，而半波长（在2.4GHz的信道中半波长约为12厘米）的环境增加了窃听者的暴露风险，因此在大多数超过半波长的使用场景中无线信道的信道特征具有唯一性、防窃听性，进而具有安全性。其次，无线信道特征具有时变性，即特征值会随通信环境、接收位置改变等而改变，能实现“一次一密”的效果，满足较高的安全需求。

3. 灵活性

基于物理特性的身份认证和基于信道互易性的密钥共享依赖于从通信双方接收

的Wi-Fi信号中提取信道状态信息，无需对设备做出硬件修改，不要求额外传感器、不限制对设备所处的位置和状态，可以部署移植到其余使用Wi-Fi的局域网场景中，也可以叠加到已有的安全机制中，能够满足无线体域网的安全需求，也能推广应用到其余的局域网场景，具有较强的灵活性。

1.4 应用前景分析

据预测2030年我国60岁以上老人数量将达到3.71亿，而随着越来越多的国家老龄化问题程度加深，老年人自身免疫低下以及医疗监护人员的短缺，如今的医疗保健系统将面对空前压力。传统的人工医疗监测模式已经无法满足当今社会人们对健康的需求，使用无线体域网测量并记录生命体征，例如心率、呼吸频率等层层传输到医院的数据中心，无需患者在医院停留也能实现长期的健康检测和风险预警，因此无线体域网应用于老年健康监测和疾病防治具有极大的市场潜力，无线体域网在老年人健康管理和各种慢性疾病的防治中的普遍应用势不可挡。

无线体域网目前也已被广泛应用于和各类医疗器械配合使用例如普通外科设备、诊断医学设备和植入式刺激生物传感器等，如图1-3所示，这些类型的医疗设备在全球医疗器械行业市场份额占比已经超过了四分之一。此外，无线体域网还是远程医疗的重要组成部分。近年来，国家在远程医疗方面不断出台相关政策，推动中国远程医疗建设。其中，2018年4月，国务院办公厅明确提出鼓励医疗联合体向基层提供远程会诊、远程心电诊断、远程影像诊断等服务。而得益于国家出台相关政策扶持以及需求上升，中国远程医疗市场快速增长。数据显示，2019年，中国远程医疗行业市场规模约为130亿元，到2025年，有望超过700亿元。综上，无线体域网在老龄化社会医疗问题应对、慢性病防治、现有医疗设备辅助、远程医疗方面具有极大的应用价值，而无线体域网在为人们提供便利的同时其安全问题不容忽视，因此本作品的应用前景极为广阔、市场潜力极大。

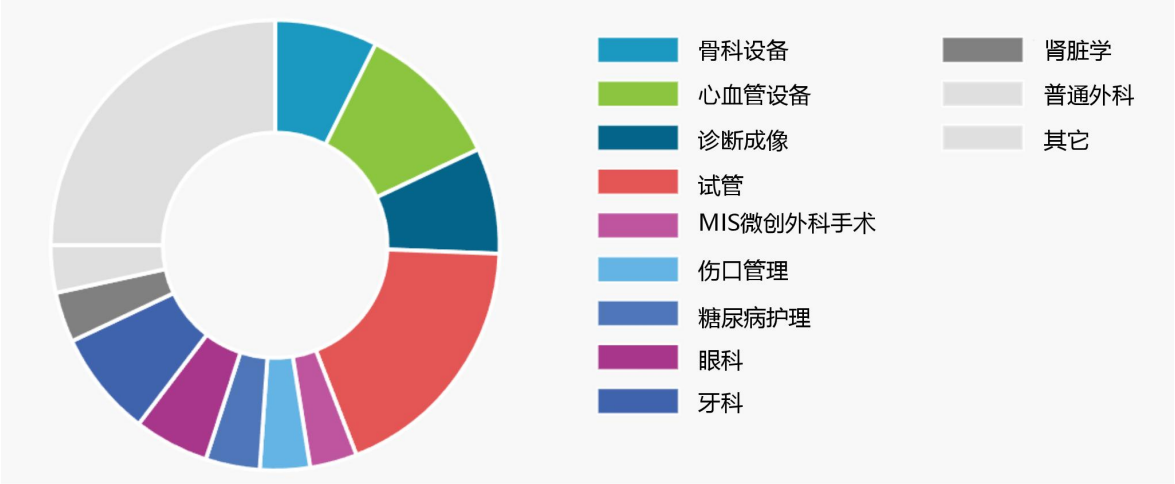


图1-3 2022全球各类型医疗器械市场份额图

本作品应用射频指纹和信道密钥技术能有效保障无线体域网内数据交互的安全：数据传输前依靠基于物理特性的射频指纹对通信双方进行身份认证，射频指纹从双方交互的信号中计算并提取，无法被克隆、伪造、篡改，攻击者即使窃听到用于生成指纹的相关信号，受限于其发射器、接收器硬件特征与合法双方不一致也难以获得相同指纹，无法实现仿冒攻击欺骗其他设备节点；在数据传输过程中利用无线信道的时变性和空间去相关性生成的会话密钥能实现“一次一密”的安全效果，能有效防范由于无线体域网使用的无线信道的开放性引发针对数据的窃取攻击或篡改攻击，保障病人数据安全；会话密钥生成后同步更新身份认证阶段所用密钥，信道时变性也天然地取得了会话密钥更新的优势，因此可以有效抵御重放攻击。本文提出的安全系统可在不对原有设备进行改装的条件下，极大提高无线体域网网络节点的身份认证和准入控制能力、减免会话密钥共享分配的繁琐环节，为无线体域网络提供物理层安全保障。该系统还有效解决传统身份认证需要复杂计算、额外传感器、特定用户模式、无法适用于Inter-WBAN层和传统密钥共享依赖于预分配和可信第三方、或依赖于摆放特定位置的传感器获得生理信号等问题，其轻量、安全、灵活的优势使得应用前景更为广阔。

此外，无线体域网是无线传感器网络（WSN）的重要分支网络，而WSN是物联网（IoT）的重要组成部分。基于物理层安全的无线体域网安全系统除了保障无线体域网的安全外还可以推广到物联网场景中，例如智能家居、智慧社区等。本作品支持目前市面上普遍使用的Wi-Fi信号，因此还可推广应用于使用局域网的多种场景，如电力局域网、企业局域网、银行政府机关等内网、涉密会议、大型安保等。由于不需要对信号发射或接收设备做出任何改动，仅需要软件获取信道状态信息即可实现安全性保障

因此基于物理层的身份认证和密钥共享方式不需要完全替换原有技术，可以叠加到传统的系统之上，实现现有安全机制的加固。

第二章 作品设计与实现

2.1 理论基础

2.1.1 基于射频指纹的身份认证

利用射频指纹实现身份认证的主要理由是考虑到设备在生产制造过程中元器件的差异以及发射机模拟元件的非线性，这些因素的叠加产生的独有特征都会寄生在Wi-Fi设备发出的无线信号当中，因而对信号进行处理理论上可获得用于唯一标识设备的特征，类比于人的指纹可以用于对人身份的认证。具体因素分析如下。

1. 设备内部电子元器件及与其相连的走线存在容差。Wi-Fi设备的射频电路中包含多张集成芯片以及众多的电阻、电容、电感等电子元器件，电子元器件存在制造容差和漂移容差，制造容差是指电子元器件出厂时的实际值与标称值之间的差值，生产仪器的精度决定了元器件的各项生产指标误差不可能正好为零，生产的各元器件之间必然存在着一定的指标差别。常见的Wi-Fi设备射频收发电路中，不同参数规格的元器件往往存在着±5%、±10%等不同的容差。漂移容差是指由于温度、湿度、压力、阳光、灰尘等外界因素以及装配工艺、老化等内在因素导致设备在工作过程中元器件指标值发生的变化。此外，电源供电电压存在不稳定性，在不同电压下，器件的工作状态会发生变化，能提供大量的指纹信息。电源电压转换电路中的变压器线圈在手工或机器绕制过程中无法做到完全一致，与元器件相连的印制电路板走线等所有硬件部分都有可能产生容差，这些差异也是网卡产生指纹的原因。Wi-Fi设备内部元器件的容差效应使得在同一设计指标下不同元器件以及相连电路的性能指标不同，并最终导致同一流水线上生产的无线设备的实际硬件参数存在差异，形成设备独特的射频指纹。

2. 晶体振荡器和锁相环电路引起载波相位噪声和时钟相位噪声。目前大多数Wi-Fi设备的本地振荡源由晶体锁相环构成，并由其产生载波频率和时钟频率。受晶体的精度和噪声等干扰的影响，在实际工作中振荡器的幅度和相位会发生变化，从而引起输出频率的波动，带来合成载频的差异。Wi-Fi芯片的频率合成器其中的锁相环电路中包含大量的数字分频电路以及模拟的晶体振荡器和压控电路，当需要产生较高的

频率时，需要通过分频器进行多次分频，分频也会花费一定时间，这就导致压控振荡器的输出频率是瞬时变化的，带来非高斯噪声的干扰，引起类似线谱的相位噪声，形成相噪指纹。

3. 无线发射机射频前端的模拟带通滤波器可形成暂态响应指纹。在发射信号过程中，数字基带信号经过重构滤波器时，会根据采样点数据重建恢复采样前的模拟信号，随后送入混频器。在射频前端，信号会通过模拟滤波器后经功率放大器发射到空中，模拟滤波器的生产制造差异使得其幅频特性曲线存在差异性，且在实际中信号无法在理想的截止频率处完全截止，滤波器的冲激响应过程即为产生暂态指纹的过程。接收信号过程中，天线感应到空间中的无线信号后经过低噪声放大器将信号放大便于解调，下变频到基带后通过增益滤波器解出I/Q两路数字基带信号。从信号发射到接收的整个过程中，会经过多个滤波器和放大器，这些非线性元器件使得发出的射频信号包含非线性成分，此外混频器的幅度偏差、I/Q两路间的相位差等都可能是引起射频信号非线性和时变性的因素，从而产生指纹信息。

通过上述分析可知，芯片内部元件的容差、PCB板的走线、锁相环晶振引起的相噪、变压器线圈的绕制、滤波器的滤波特性、功率放大器和混频器引起的射频信号非线性等因素都能产生射频指纹，通过对无线信号的采集和识别，理论上可辨别出每一台Wi-Fi设备，而伪造出硬件特征完全一致的设备是极其困难的，因此通过提取射频指纹进行设备认证识别具有可行性和较高的安全性。

2.1.2 基于信道互易性的密钥生成

基于信道互易性的密钥生成方案中，如图2-1所示通信双方可凭借一个高度相关的信道特征生成一致的密钥，且在此过程中由于信道的时间变化性和空间去相关性窃听者难以得到同样高度相关的信道特征，另一方面即使获得了部分协商信息也难以破解出双方使用的密钥，因此利用信道互易性实现密钥共享具有可行性，能有效保障通信安全，其具体理论依据及分析如下。

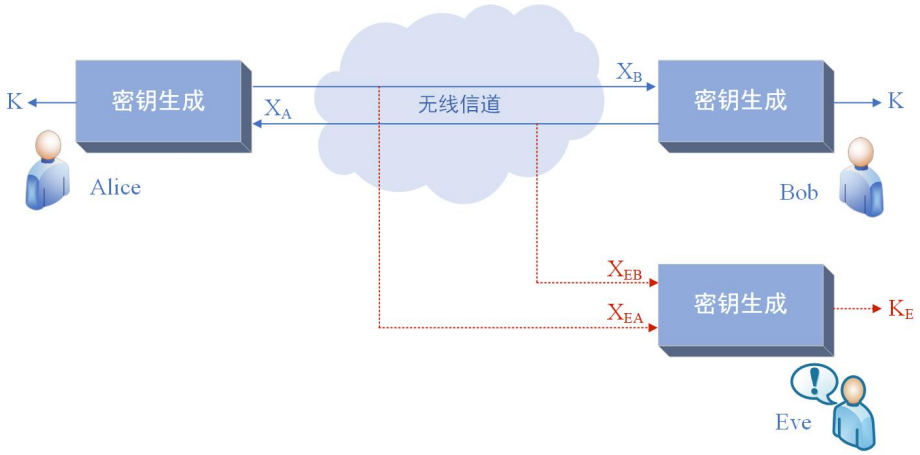


图2-1 基于信道互易性的密钥生成

基于信道互易性的密钥生成的理论依据来源于信道的三个特性。

1. **互易性**：当上行和下行信道以相同载波频率运行时，动态变化的信道在极短时间内如相干时间，可视为固定不变，则短时内双方的冲激响应是高度相关的，这一特性使得通信双方测量到的信道特征极具相似性，为后续双方使用信道特性测量值生成一致密钥奠定基础。

2. **时间变化性**：信号在通信环境中传播时遇到移动物体阻碍等将会经历不同的反射、折射等变化，严格意义上信道环境不是静止不变的，因此信道响应也是时刻动态变化且不可预测的，这一特性为密钥提供了随机性保障，还可实现“一次一密”的安全效果。

3. **空间去相关性**：根据Jakes模型[34]，在一定环境约束条件下，通信各方信号不相关的距离为半波长，也称该距离为“安全距离”。即当攻击者与任一合法通信方的距离超过半波长时，他则无法获得高度相关的信道响应。对窃听者而言将自身放置于合法用户的安全距离内是不现实的，因为这无疑增加了暴露风险。这一特性为密钥安全性提供了第二重保障，能有效防止密钥被泄漏。

2.2 系统架构设计

2.2.1 系统概述

本作品提出了一个基于物理层安全的无线体域网安全系统，主要用于无线体域网的Inter-WBAN层的控制器节点CN和移动节点MN进行双向身份认证和会话密钥生成共享。本系统的工作原理为：对接入移动节点的控制器节点进行抗信道干扰的指纹提取，

将其纳入指纹库在后续接入时进行比对，若分类模型输出结果与CN声明身份一致则MN对CN合法性验证通过，反之则判别该CN为非法设备。MN再将包含CN设备指纹信息的数据加密传输给CN，CN解密与自身比对，若一致则MN身份合法。双向身份认证完成后，双方可通过信道探测、信道特征量化及协商获得一致密钥，用于后续的数据加密传输并更新身份认证阶段所用的密钥。其工作流程如图2-2所示。

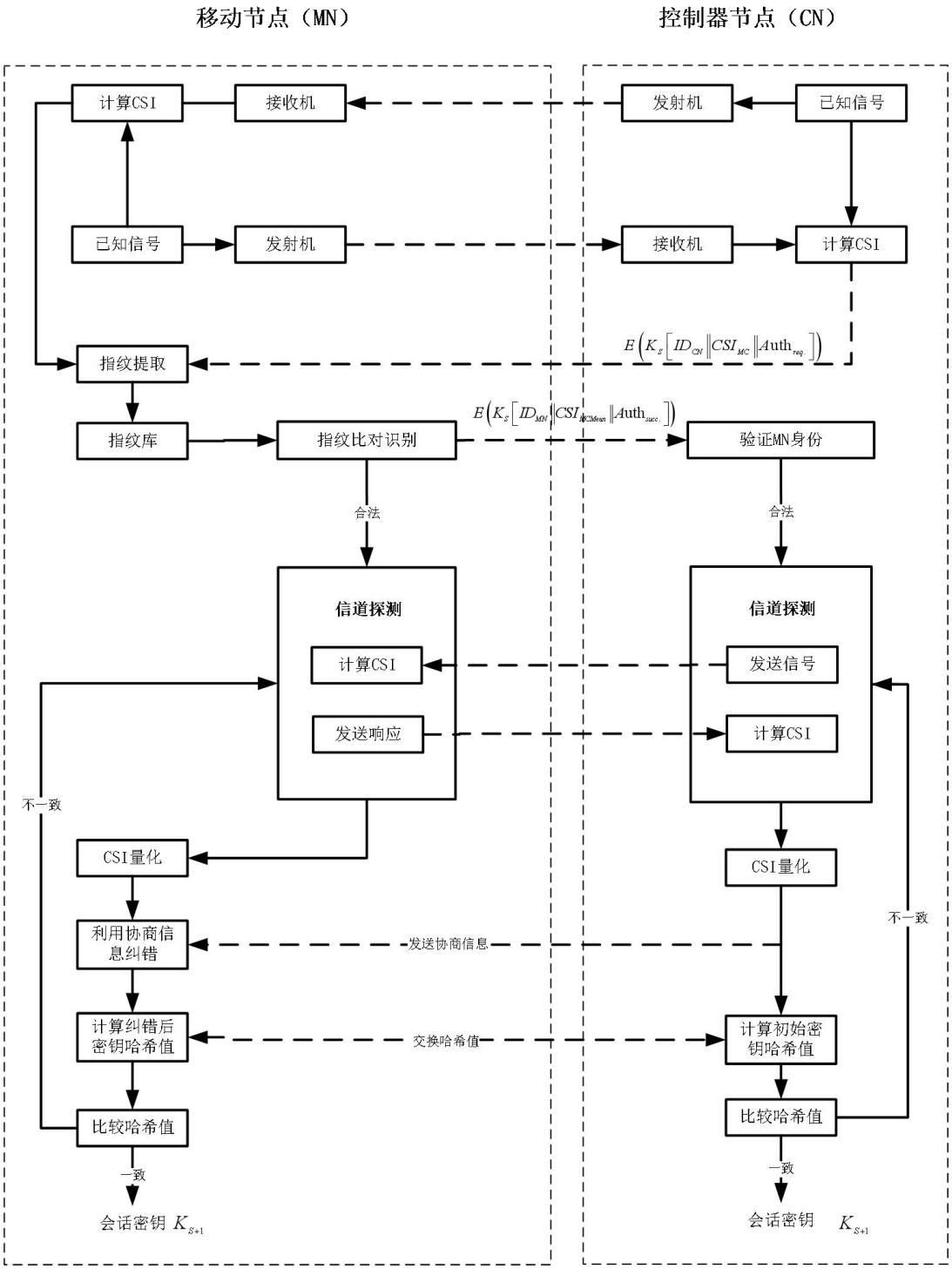


图2-2 系统工作原理流程图

2.2.2 系统结构

从逻辑架构来看，系统部署于移动节点一端，从移动节点的视角出发管理身份认证和密钥共享，系统可分为三层，分别是：表现层、业务逻辑层、数据服务层，如图2-3所示。

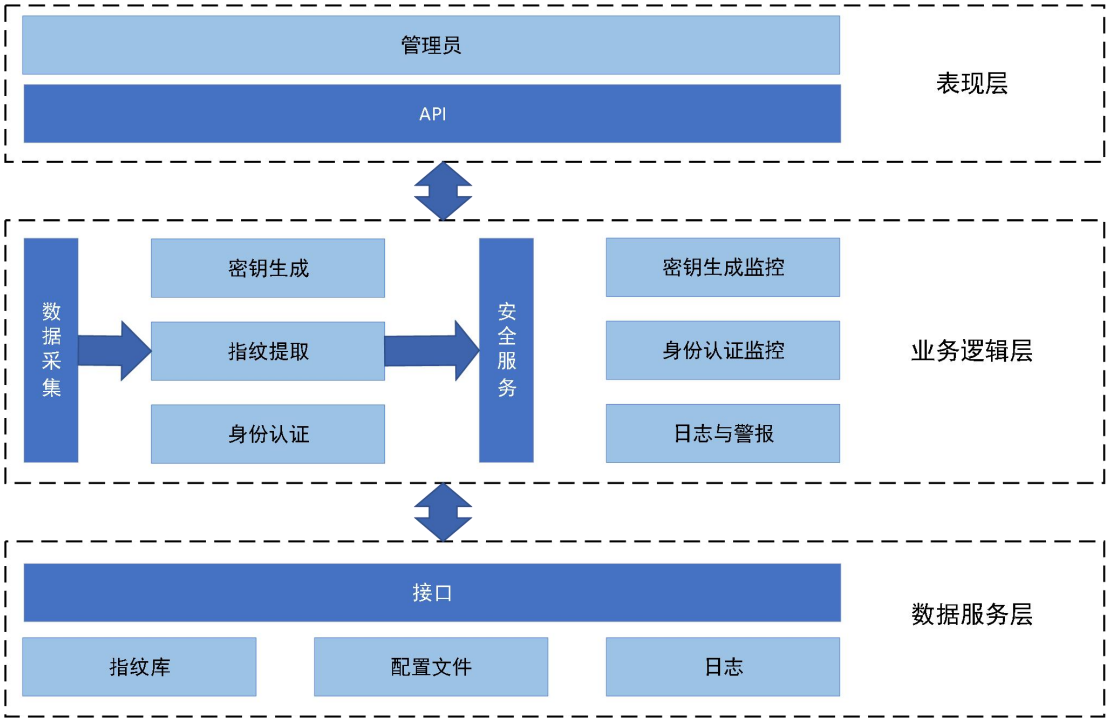


图2-3 系统三层架构图

- **表现层：**主要完成用户交互功能，页面主要基于由HTML与JavaScript写成，功能主要由状态展示、审计、配置三大模块构成。
- **业务逻辑层：**业务逻辑层主要进行业务处理，这些业务功能根据数据服务层的配置文件进行，包含了指纹提取、身份认证、密钥生成、安全服务等。
- **数据服务层：**数据服务层根据控制层的解析结果负责数据库的存取，配置文件的存储、读取和校验。

从功能实现来看系统由六大模块：数据采集模块、指纹提取模块、身份认证模块、密钥生成模块、安全服务模块和可视化界面组成，具体说明如下：

- **数据采集模块：**提取信道状态信息，用于后续指纹提取与密钥生成。
- **指纹提取模块：**主要目标是对数据采集模块传过来的数据进行设备指纹提取。该模块旨在MN接收到CN的信息后解密其传输的信息，获得身份识别请求、CN

声明自己的身份ID和CSI_{MC}，利用MN到CN的信道状态信息CSI_{MC}与CN到MN的信道状态信息CSI_{CM}计算得到CN的指纹特征，纳入设备指纹数据库。该信号特征分析也将可以为识别新增的设备提供相关的信息和依据。

- **身份认证模块**：采用前馈神经网络实现设备识别分类。对合法设备提取一定数量的指纹后，训练分类模型。训练好的模型的轻量级版本部署在MN上， MN提取到CN的指纹后将其输入分类模型得出分类结果，若结果与CN声明的身份ID一致则对CN的身份认证通过。而后MN向CN发送加密信息（包含MN的身份ID、从CN发来信息中解密获取的CSI_{MC}的均值、认证成功标识），CN接收后解密与自身存储的CSI的均值对比，若一致说明MN合法。双向身份认证成功。
- **密钥生成模块**：在设备CN和MN双向身份认证通过后，由CN向MN发起信道探测请求，双方信道探测完毕后各自量化得到初始密钥，再利用初始密钥得到协商信息，CN向MN发送协商信息，MN收到后对自己的密钥进行纠错，之后计算哈希值并比对，确认双方密钥已经协商一致。
- **安全服务模块**：提供辅助的安全服务如设备指纹数据库、身份认证实时监控、密钥生成实时监控、日志与警报等。
- **可视化平台**：为管理员提供MN视角的可视化操作界面，提供各类接口对接各功能单元，例如供用户查询设备安全状态信息、密钥源可视化等。

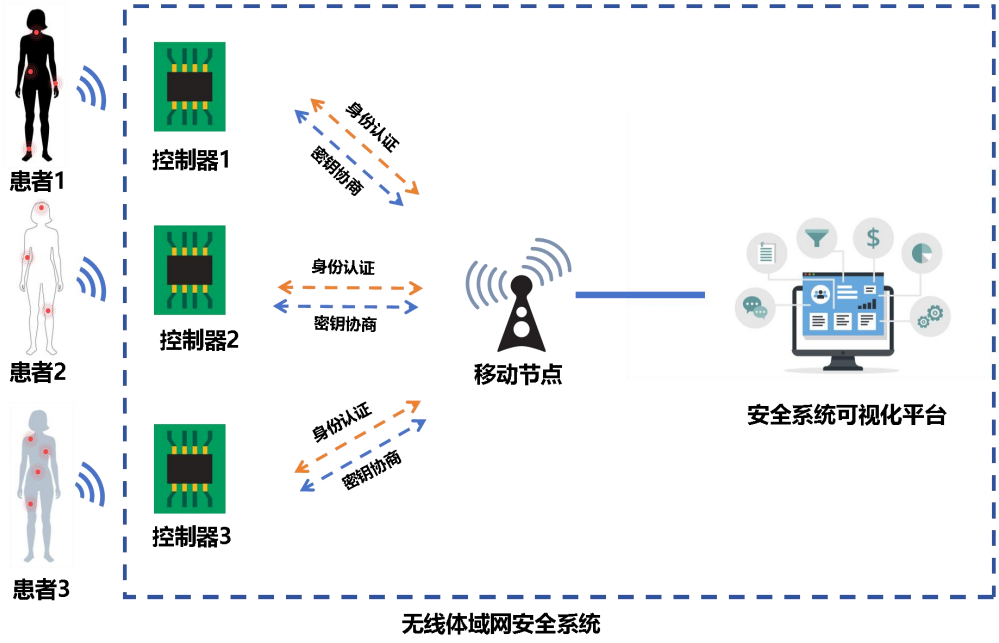


图2-4 系统物理架构图

从物理架构来看，本系统由一组待认证控制器节点、一个移动节点和一台安装了本安全系统可视化平台的计算机组成，如图2-4所示。作为控制器节点和移动节点的设备具体为乐鑫科技旗下的ESP32-DevKitC-v4开发板（分别设置为终端模式和接入点模式），其搭载ESP32-WROOM-32U模组，模组的核心是ESP32-DOWD芯片，具有可扩展、自适应的特点，ESP32-WROOM-32U模组集成了传统蓝牙、低功耗蓝牙和 Wi-Fi，其中Wi-Fi支持协议802.11 b/g/n（802.11n，速度高达 150 Mbps），工作信道中心频率范围为2412 ~ 2484 MHz，能够满足常用的CSI提取场景所需频点要求，利用该模组提供的接口可连接移动节点与运行可视化平台的电脑满足可视化需求。

2.2.3 系统功能

基于物理层安全的无线体域网安全系统在上述六个一级模块的基础上，以七个功能单元共同实现系统所需的身份认证、密钥共享、安全管理、安全服务四大目标，功能单元关系如图2-5所示。

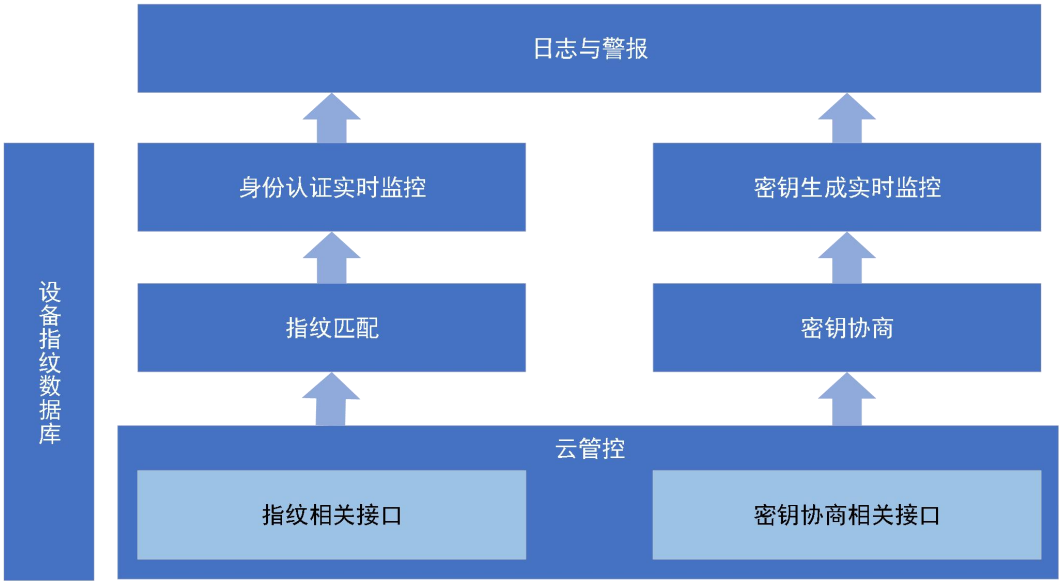


图2-5 功能单元关系图

各功能单元的说明如下：

- **设备指纹数据库：**新增、删除、查询数据库数据，用于后续合法设备指纹分类模型的训练。登记合法设备指纹入库，解析合法设备指纹数据，将有效信息记入数据库。根据指纹库的信息对设备指纹进行分类识别，对比分类结果与设备声明身份，进而认证设备身份与判别设备身份合法状态。

- **身份认证实时监控：**统计汇总接入移动节点的不同设备的身份认证结果，例如合法次数、非法次数、合法比例等。
- **密钥协商：**身份认证后调用信道探测程序，接收来自控制器节点的探测请求并发回响应；接收控制器节点发送的协商信息并完成密钥纠错计算纠错后密钥的哈希值，完成哈希值比对，得到一致密钥。
- **密钥生成实时监控：**统计汇总MN和不同CN设备协商生成密钥的时间、协商结果和对应密钥信息。
- **指纹匹配：**将待认证设备的提取的指纹输入由指纹数据库中的已录入指纹训练得出的分类模型，输入的指纹信息匹配出分类模型中的一个设备，根据分类结果与声称身份是否一致对设备的合法与否进行状态标记。
- **云管控：**包含指纹识别结果查询接口、指纹识别参数查询接口、指纹识别参数设置接口、CSI原始数值查询接口、密钥协商结果查询接口、合法设备登记接口、合法设备取消登记接口、数据库查询接口、数据库增加接口、数据库修改接口、数据库删除接口。当用户拥有使用该功能的权限时，指纹识别参数查询/设置接口独立用于通过设置身份认证的参数，进而查询身份认证的结果；而其他接口为其余六个功能单元服务使其可以对合法设备进行登记、取消合法设备的登记，管控设备的状态信息，查询密钥生成情况、导出需要的密钥相关信息，新增、删除、查询数据库数据等。
- **日志与警报：**记录并更新身份认证日志、密钥协商日志，用于数据维护。当用户具有使用该功能的权限时，身份认证日志或密钥协商日志进行显示，供用户查看。

2.3 系统性能指标

2.3.1 信道互易性

利用信道互易性消除信道干扰的射频指纹提取和基于信道互易性的密钥生成方案的可行性取决于数据体现信道互易性的程度，如果数据不能体现信道互易性则无法实现减除信道干扰以及双方经过量化后的初始密钥会出现严重不一致需要进一步的协商，这一过程则可能存在信息泄漏的安全风险。因此对信道互易性进行评估是密钥生成方案的首要任务。

通信双方对信道的测量值被称为信道估计，我们首先想到，通信双方所获的信道估计可以看为两个向量，信道互易性高则反映为两个向量高度相似或一致，而欧几里德距离是常见的相似度的计算方式。向量的相似度由两者间距离衡量，距离越小则越相似。但随后的实验中我们对所获信道测量值进行作图比较时发现，远距离实验时会出现两组数据趋势大致相同而数值相差较大的情况，即双方图像平行。因此简单地以欧氏距离衡量信道互易性可能出现误判的情况。

在进行调研时我们发现Christan Zenger和Hendrik Vogt等[35]在对窃听者距离合法用户较近时的被动窃听风险进行分析时利用了皮尔逊相关系数来衡量窃听者所获信道特征与合法用户的相似性。文献[36]也指出通过对信道估计的相似性使用相关系数进行定量评估可以得到对信道互易性好坏的直观描述。

皮尔逊相关系数（Pearson Correlation）是衡量向量相似度的一种方式。其计算原理如下：

$$\rho_{xy}=\frac{\sum_{i=0}^{N-1}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=0}^{N-1}(x_i-\bar{x})^2}\sqrt{\sum_{i=0}^{N-1}(y_i-\bar{y})^2}}, \tag{2.1}$$

上式中，N为样本数量，X_i和Y_i是变量X，Y对应的i点观测值，$\bar{x}=\frac{1}{N}\sum_{j=0}^{N-1}x_j$，$\bar{y}=\frac{1}{N}\sum_{j=0}^{N-1}y_j$。结果大小范围为$[-1,+1]$，其中0代表无相关性，负值代表负相关，正值代表正相关。皮尔逊相关系数描述的是线性相关关系，因此对应于信道互易性衡量过程而言，通信双方Alice和Bob所获的信道测量值其样本称为X和Y的话，如果X和Y高度相似，则X和Y应该呈现$Y\approx X$的关系，即斜率为1的正比例函数。反映于皮尔逊相关系数则是数值越接近1则互易性越高。

因此，本文中定义互易性系数$\rho(CSI_{AP},CSI_{STA})$来衡量互易性好坏，其定义如下：

$$\rho(CSI_{AP},CSI_{STA})=\frac{\sum_{i=0}^{N-1}\left(CSI_{AP_i}-\overline{CSI_{AP_i}}\right)\left(CSI_{STA_i}-\overline{CSI_{STA_i}}\right)}{\sqrt{\sum_{i=0}^{N-1}\left(CSI_{AP_i}-\overline{CSI_{AP_i}}\right)^2}\sqrt{\sum_{i=0}^{N-1}\left(CSI_{STA_i}-\overline{CSI_{STA_i}}\right)^2}} \tag{2.2}$$

上式中CSI_{AP_i}和CSI_{STA_i}分别指AP和STA的第i个子载波的CSI信息。同时，为取得实

验结果的普遍性意义，定义互易性系数的平均值如下：

$$\overline{\rho\left(CSI_{AP},CSI_{STA}\right)}=\frac{\sum_{i=1}^{10}\rho\left(CSI_{AP},CSI_{STA}\right)_i}{10} \tag{2.3}$$

上式$\rho\left(CSI_{AP},CSI_{STA}\right)_i$表示AP和STA间第i组CSI信息的互易性系数，$i=n\cdot 100$，n为从1到10的整数。

2.3.2 指纹唯一性

类比于人类身份认证中的指纹信息，用于设备身份认证的物理指纹应当具有唯一性。相同厂商、相同批次、相同型号的设备其由于物理硬件不可能完全一致，从Wi-Fi设备发出的无线信号当中提取的射频指纹也应当各不相同。所提取的射频指纹应当能反映每个设备各不相同的芯片内部元件的容差、PCB板的走线、锁相环晶振引起的相噪、变压器线圈的绕制、滤波器的滤波特性、功率放大器和混频器引起的射频信号非线性等因素的叠加产生的唯一特征。具体表征在指纹的图像上时，各个设备的指纹曲线应当互不重合。

2.3.3 指纹稳定性

用于设备身份识别的射频指纹应当具有稳定性。具体而言，从Wi-Fi信号中提取的设备射频指纹，不应当受信噪比变化、时间变化、位置变化、信号传播过程中有无障碍物阻隔、信道变化等因素的影响。在不同信噪比、不同时间段、不同环境（如视距或非视距）的信道环境中提取的射频指纹应当一致。具体表征在指纹的图像上时，不同环境下设备的指纹曲线应当完全重合。

2.3.4 身份识别准确率

对发起身份认证请求的CN设备进行指纹提取后，分类模型对其准确识别分类得出正确的设备标签将影响身份认证的完成。本系统对设备身份合法性的验证依赖于分类模型输出结果与CN声明的身份标签一致，若一致则MN判别CN为合法设备，反正为非法设备，MN对CN的身份认证不予通过。因此设备识别准确率将直接影响身份认证的正确

率。身份识别准确率将按认证次数中正确判别为合法的比例计算。

2.3.5 密钥协商成功率

对称密钥的首要要求即是双方使用一致的密钥，然而由于噪声和硬件不对称等量化后所得原始密钥可能不一致。而密钥的一致性可以由密钥不一致率（Key Disagreement Rate，KDR）来衡量，其定义为合法通信双方相同密钥位对应的密钥值不一致位数总和占密钥总长度的比值。鉴于通信双方的密钥为0,1序列，则可以通过相同位置上计算两者密钥值差值的绝对值再进行累加，最后除以密钥总长得到，计算公式如下：

$$KDR = \frac{\sum_i |K_A(i) - K_B(i)|}{l_K} \tag{2.4}$$

上式中$K_A(i)$和$K_B(i)$分别表示Alice和Bob的第i位密钥位对应的密钥值，l_K表示密钥总长度。密钥不一致率越低，密钥协商环节压力越小，双方用于协商获得一致密钥带来的密钥泄露风险越低。

当密钥不一致率超过纠错限制，则双方在一定的时间和资源限制下无法协商成功，我们定义密钥协商成功率（Key Agreement Success Rate，KASR）为如下：

$$KASR = \frac{N_S}{N} \tag{2.5}$$

上式中N_S表示协商成功次数，N表示协商总次数。协商成功率越高，证明本作品提出的会话密钥协商方案越有效。

2.3.6 密钥随机性

一个好的密钥生成方案应该在指定时间内生成数量满足要求且符合随机分布要求的密钥。通常使用美国国家标准与技术研究院（National Institute of Standards and Technology， NIST）的随机性测试来检验生成的密钥是否符合随机性要求。NIST测试套件包含了15种测试的统计软件包，目的是测试数据是否在数学上符合随机性的要求。15种测试为频数测试、块内频数测试、游程测试等，使用时可以自行选择测试数据长度和组数以及测试种类，所测得的P-value大于0.01即表示该项测试通过。以下是几种常用测试项目的介绍：

1. 频数检验：判定序列中0和1各自所占序列元素总数的比例是否相近，该检验

的通过是其余随机性检验项目的基础。

2. 块内频数检验：在频数检验基础上，将序列划分为M位的小数据块，针对每个数据块检验块内的0和1比例是否相当。
3. 游程检验：判定不同长度的“1”游程的数目以及“0”游程的数目是否跟理想的随机序列的期望值相一致。
4. 累加和检验：判定序列的累加和相对于预期的累加和过大还是过小。可将累加和视为随机游动，当其偏离在0附近时符合随机序列的特征。
5. 近似熵检验：测试整个序列中所有可能的重叠 m bit 模式的频率。目的是将两相邻长度m和m+1的重叠子块的频数与随机情况下预期的频数相比较。
6. 序列检验：设置欲检验的模式大小为m bit，判定2^m个重叠模式的出现频率是否与理论上的随机序列的出现频率的值相当。

2.3.7 安全性

身份认证常面临以下攻击：模仿攻击、中间人攻击、重放攻击、主动和被动的窃听攻击等，一个有效安全的身份认证机制应当能抵御上述攻击。

密钥的使用目的是为了有效保障数据的保密性，因而密钥必须防范泄漏的风险。被动窃听攻击是一种常见的攻击方式，好的密钥生成方案应该能有效抵御此类攻击，即防止攻击者能通过窃听合法通信双方的协商信息或者由数据包获得信道测量值来破解出密钥。具体而言可以通过设置被动窃听场景，将窃听者捕获到的信道状态信息与合法用户的进行比较，如果高度不相关则论证了此密钥生成方案的防窃听性。

2.4 系统实现方案

2.4.1 密钥源选择

2.4.1.1 接收信号强度RSS

RSS有时也称接收信号强度指示（Received Signal Strength Indication，RSSI），是无线传输层用来衡量链接质量的重要指标，传输层根据RSS判断是否需要增大发送端的发送强度。其计算公式为：

$$RSS(d)=P_{\mathrm{r}}(\mathrm{d})=P_t-P_L(\mathrm{d}) \tag{2.6}$$

其中P_{t}是发射功率，$P_r(\mathrm{d})$是距离发射源d 米远处的接收功率，$P_L(\mathrm{d})$为在距离d处的路径损耗。根据自由空间传播模型，距离辐射源d 米处的天线接收功率$P_r(\mathrm{d})$计算公式如下：

$$P_{\mathrm{r}}(d)=\frac{P_{\mathrm{t}}G_{\mathrm{t}}G_{\mathrm{r}}\lambda^2}{(4\pi)^2d^2L} \tag{2.7}$$

上式中P_{t}为发射功率，$P_r(\mathrm{d})$是接收功率，G_t是发射天线增益，G_r是接收天线增益，d 是发射机和接收机之间的距离，L 为与传播无关的系统损耗因子，λ 是信号波长。

自由空间的路径损耗P_L按下式计算：

$$P_L=10\log\frac{P_t}{P_r}=-10\log\left[\frac{G_tG_r\lambda^2}{(4\pi)^2d^2}\right] \tag{2.8}$$

在实际应用中，一般采用对数正态距离路径损耗（Log-normal Distance Path Loss，LDPL）模型对路径损耗进行建模：

$$P_L(d)=\overline{P_L}(d_0)+10n\log\left(\frac{d}{d_0}\right)+X_\sigma \tag{2.9}$$

其中$P_L(\mathrm{d})$为在距离d 处的路径损耗，d_0为参考点与发射点的距离，通常选为1，n为路径损耗指数（表明路径损耗随距离增长的速率，依赖于周围环境和建筑物类型），X_σ为方差为σ的零均值高斯分布随机变量，表示环境引起的信号阴影衰落。

2.4.1.2 信道状态信息CSI

尽管RSS已经在无线信道密钥生成领域被广泛研究，并取得较多成果，但RSS所反映的是粗粒度的无线信道信息，其密钥生成容量较低。在无线感知领域，RSS受多径效应影响不再随着距离增加而单调衰减且稳定性差，另一个缺陷是RSS无法刻画多径传播。CSI克服了这一局限，通常认为CSI主要指信道冲激响应（Channel Impulse Response，CIR）和信道频率响应（Channel Frequency Response，CFR），CIR和CFR互为傅里叶变换。CIR为时域上多径传播的表现，根据相关文献，在时不变假设下，CIR

可以表示为：

$$\mathrm{h}(\tau)=\sum_{i=1}^{N}a_i e^{-j\theta_i}\delta\left(\tau-\tau_i\right) \tag{2.10}$$

上式中α_i表示第i条传播的路径的幅度衰减，θ_i表示第i条路径的相位偏移，τ_i表示第i条路径的时间延迟，N表示传播路径总数，$\delta(\tau)$为狄克拉脉冲函数。

CFR为频域上多径传播的表现，CFR一般包含幅度/频率和相位/频率两种响应，可表示为：

$$H(f,t)=\int_0^{\tau_{\max}}h(\tau,t)e^{-j2\pi f\tau}d\tau \tag{2.11}$$

其中，$\tau_{\max}$为最大的信道延迟。

CSI是一个用于刻画无线传输链路的信道状态的指标，从信号传输的过程和CSI的定义来看，如果以Y表示接收端的信号向量，X表示发送端的信号向量，H表示信道状态矩阵，N表示高斯白噪声，数学表示为：

$$Y=HX+N \tag{2.12}$$

CSI即信道状态矩阵H，$H=\left[H_1,H_2,H_3,\ldots,H_K\right]^T$其中$i\in[1,K]$，$K$为子载波个数。其中每个$H_i$以复数形式表示。另一方面，CSI也可以理解为CFR在不同子载波的离散采样。从CSI数值的组成来看，设CSI_i表示对应于第i个OFDM子载波的CSI流，则可以描述如下：

$$\mathrm{CSI}_i=\left|\mathrm{CSI}_i\right|\mathrm{e}^{j(\angle\mathrm{CSI}_i)} \tag{2.13}$$

其中$\left|\mathrm{CSI}_i\right|$和$\angle\mathrm{CSI}_i$分别代表幅度和相位，目前的研究中常利用CSI的幅度和相位作为特征。综上，CSI能反映多个子载波的状态变化，其分辨率层次为子载波层次，对环境更为敏感，所提供的数据更加丰富且细粒度。

2.4.1.3 RSS与CSI间的对比

在无线信道密钥生成方案中，初期使用RSS的原因是RSS的实用性。RSS属于MAC层信息，可以依赖于现有的网络设施实现简单的密钥生成，而不用对物理层设备有所更

改。CSI则属于物理层信息，尽管目前测量CSI是Wi-Fi接收器的一个标准功能，但对CSI的访问仍不具普适性，对CSI的获取依赖于Linux 802.11n CSI工具、Atheros CSI工具以及基于博通芯片组开发的Nexmon CSI工具等特定硬件或开源固件。另一方面，基于CSI的密钥生成如果使用的信道特征为相位信息，则需要合法通信双方紧密同步，进而对双方的硬件同步和互易性校准提出了较高要求。

但基于RSS的密钥生成最为突出的弱点即是粗粒度数据导致的低密钥生成速率和小密钥容量，以及需要额外的随机性补充。而CSI不仅反映了各个子载波的状态，还将单值的RSS扩展至多维度的频域空间，能提供更细粒度的信息。随着物联网迅速发展，MIMO技术背景下多用户的密钥生成、OFDM系统中的密钥生成、无线体域网中的密钥生成等场景，CSI则更为适合，因此本作品中将利用CSI作为密钥源。对RSS和CSI进行对比，结果概括如下表：

表2-1 RSS和CSI对比表

类别	RSS	CSI
所属网络层次	MAC层	物理层
能否刻画反映多径传播	否	能
分辨率层次	无	子载波
数值粒度	粗	细
采集设备	几乎所有设备	部分特定设备
稳定性	低	高
实现复杂度	低	高

2.4.2 信道特征提取

2.4.2.1 信道特征提取工具调研

目前的研究中有许多得益于CSI，比如室内定位、人体姿态识别、呼吸检测、信道密钥生成等，Wi-Fi接收器也会视CSI为标准特征对其进行测量，但是对其进行直接获取和记录的工具则较少。根据调研，目前主要使用的CSI提取工具有以下四种：基于Intel Wi-Fi 5300网卡的Linux 802.11n CSI工具，基于Atheros 系列网卡的 Atheros CSI 工具，基于Broadcom 和Cypress Wi-Fi 芯片组的Nexmon CSI提取工具以及

基于ESP32开发板的ESP CSI Toolkit。

1. 基于 Intel Wi-Fi 5300网卡的Linux 802.11n CSI工具

早在2011年，华盛顿大学的Daniel Halperin和Wenjun Hu等[37]开发了一个适用于Ubuntu系统的 CSI提取工具，能够在Intel Wi-Fi 5300无线网卡上完成CSI提取。该工具由为此工具定制的Intel闭源固件和开源 iwl Wi-Fi 无线驱动程序、用于控制链路两端的接入点功能的用户工具以及用于数据分析的Matlab（或 Octave)脚本共同组成。该工具能够采集到30个有效子载波的CSI信息，支持的信道带宽为20MHz和40MHz，其数据实部和虚部分辨率均为8 bit。

2. 基于Atheros 系列网卡的 Atheros CSI 工具

谢亚雄和李镇江等[38]提出了该种可以提取到非分组CSI的工具，此工具以开源的Linux内核驱动程序ath9k为基础，能够在Qualcomm Atheros 802.11n Wi-Fi芯片组（包括 AR9580、AR9590、AR9344和QCA9558）上实现CSI提取，支持的工作频段包含2.4和5GHz，能够对20和40 MHz信道上的每个子载波进行CSI提取，即能采集到至少56个有效子载波的CSI信息，暂不支持802.11ac标准下的80MHz信道带宽，其数据实部和虚部分辨率均为10bit。

3. 基于 Broadcom 和 Cypress Wi-Fi 芯片的Nexmon CSI提取工具

Francesco Gringoli和Matthias Schulz等[39]为了解决在商用设备上难以获取CSI的问题以及前两种CSI提取工具不够灵活难以推广的限制，开发了Nexmon CSI提取工具。此工具主体为Nexmon固件补丁框架，原理为通过此开源代码由用户对含Broadcom和Cypress芯片组的设备进行固件的修改，因此其存在着损坏硬件的可能。支持的工作平台涵盖了树莓派3B+、树莓派4B以及Nexus 智能手机，支持2.4GHz和5 GHz 频段，具有高达80 MHz 的带宽，能采集到242个子载波的CSI信息，其数据分辨率实部和虚部均为14bit。

4. 基于ESP32的CSI提取工具

考虑到前三种工具依赖于特定网卡不能独立工作、缺乏灵活性或者是需要对硬件本身进行修改存在破坏风险，Steven M. Hernandez等人使用ESP32开发板设计并实现了一个简便、轻量级、可独立工作的CSI提取工具ESP CSI Toolkit[40]。该工具依托于ESP32开发板，利用了拓展性强的Espressif物联网开发框架且无需对固件进行更改，既能独立工作也能移植到用户开发的程序中，还允许用户将搭载工具的ESP32连接到

一般的智能手机从而实现由智能手机直接访问CSI，能采集到64个子载波的信息，其数据实部和虚部分辨率均为8 bit与其他工具相当。此外该工具极其轻便、移动性强，其实现代码也避免了许多冗余功能，仅1000行左右。

对于上述调研，以表格汇总便于直观清晰的对比，表格如下：

表2-2 CSI提取工具的比较

工具	Intel 5300 (+笔记本)	Atheros (+笔记本)	Nexmon	ESP32
使用该工具的论文	92.5%	6.8%	＜1%	N/A
是否开源	否	是	是	是
支持设备	PCI	路由，PCIE	Nexus5/6P，RPi3B+/4B	智能手机
能否独立工作	否	否	需对固件修改	是
能否与智能手机连接	否	否	需对固件修改	是
最大带宽	40MHz	40MHz	80MHz	40MHz
子载波组数	30	56或114	242	64或128
分辨率（虚部/实部）	8	10	14	8
带宽（帧/s）	1000	1000	1000	650
实现层次	内核	内核	Wi-Fi特定固件	用户
天线	3	3	1	1至16
支持协议	HT/11n	HT/11n	VHT/11ac	HT/11n
成本	$10 + 电脑	$10 + 电脑	＞$100	＜$10
重量	＞1kg	＞1kg	＞100g	＜10g

2.4.2.2 信道特征提取方案

■ **方案简述**

依附于ESP32本身提供的CSI提取接口，采用开源的ESP CSI Toolkit加以改造作为信道特征提取工具。

■ **具体流程**

1. 软硬件环境搭建

(1) 硬件选择

硬件上我们选择ESP32开发板分别作为控制器节点CN和移动接入节点MN，一台搭载Ubuntu 20.04系统的笔记本用于运行系统实时监视捕获的CSI数据。

具体地，根据工具硬件环境需求，选择了乐鑫科技旗下的ESP32-DevKitC-v4开发板，搭载ESP32-WROOM-32U模组，模组的核心是ESP32-DOWD芯片，具有可扩展、自适应的特点，两个CPU核可以被单独控制。ESP32的模组及其开发板在以下五点提供了使用其开发CSI提取工具乃至研究多用户接入场景下基于信道互易性和Wi-Fi技术的无线信道密钥生成方案的实施基础：

① 支持Wi-Fi功能

ESP32-WROOM-32U模组集成了传统蓝牙、低功耗蓝牙和 Wi-Fi，其中Wi-Fi支持协议802.11 b/g/n（802.11n，速度高达 150 Mbps），工作信道中心频率范围为2412 ~ 2484 MHz，能够满足常用的CSI提取场景所需频点要求。

② 支持数据导出

ESP32-WROOM-32U模组集成了丰富的外设，包括电容式触摸传感器、霍尔传感器，SD 卡接口、以太网接口、UART等，其中USB接口方便将开发板与电脑直连对CSI提取工具进行开发和调试，SD卡则为CSI提取时导出数据提供了可能。

③ 支持多种工作模式

ESP32支持三种工作模式：仅 station 模式、仅 AP 模式和station/AP 共存模式，在研究多用户接入一个接入点场景下的密钥生成时，可以将其中一个开发板设置为AP模式作为移动接入节点MN，其余开发板设置为station模式作为控制器节点CN。同时这一特性也提供了智能手机等常规终端接入实验所设置AP的可能。

④ 提供Wi-Fi 信道状态信息API

ESP32中CSI由子载波的信道频率响应组成，获取CSI的原理为在发送端接收数据包时进行计算。每个子载波的CSI信息由两个字节大小的签名字符组成，其中第一字节为虚部，第二字节为实部。EPS32的菜单配置中提供了组件配置 - > Wi-Fi - >Wi-Fi CSI(Channel State Information)的选项，ESP32 硬件开发的软件环境为乐鑫 IoT 开发框架 (esp-idf) ，此开发框架中提供了Wi-Fi 信道状态信息相关的API，例如：调用esp_Wi-Fi_set_csi_rx_cb()可以设置 CSI 接收回调函数，调用esp_Wi-Fi_set_csi_config()能配置 CSI，调用esp_Wi-Fi_set_csi()启用CSI采集功能。对于提取CSI时相关的信道参数如信号模式、信道带宽等ESP32提供了数据结构 Wi-Fi_cs

i_info_t 方便研究人员根据需求开发使用。

⑤ 提供Wi-Fi Sniffer 模式API

ESP32的Wi-Fi Sniffer模式可以通过 esp_Wi-Fi_set_promiscuous()启用。在此模式下，可以向应用程序转储802.11的管理帧、数据帧、控制帧等数据包。这一功能使得我们可以利用ESP32开发具有窃听同一信道内其余设备CSI信息功能的CSI提取工具。

(2) 软件环境搭建

软件环境搭建流程如图2-6所示。首先设置了Linux平台工具链，安装所需的python3、cmake等软件包。然后将乐鑫提供的ESP-IDF软件开发框架克隆到本地，实验时我们选择了ESP-IDF release/v4.3。随后，运行安装脚本完成相关编译构建工具的安装。至此，基于ESP-IDF开发和运行的项目所需的软件环境搭建完毕。使用时，需要在项目所在终端设置环境变量，以此来激活IDF虚拟环境。

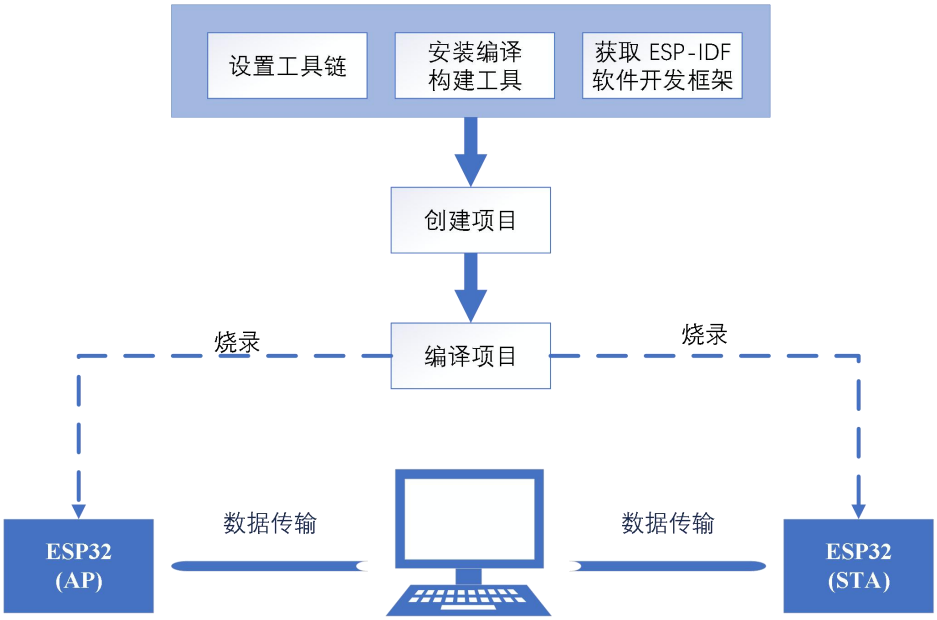


图2-6 软件环境搭建流程图

2. 部署ESP CSI Toolkit

使用开源的ESP CSI Toolkit工具包，选用4个ESP32开发板中一个设置为AP模式作为移动节点，其余3个设置为STA模式作为控制器节点，按上一节完成硬件准备、软件环境配置后，将ESP CSI Toolkit资源包克隆到本地，选择对应模式将提取程序烧录至相应开发板。编写脚本完成提取程序的启动运行和信道特征提取及数据导出存储。

(1) 设置工具

ESP32 CSI Toolkit中有三种模式可供选择：active_sta、active_ap、passive。每个模式的main.c中均调用相关函数设置了ESP32的工作模式。首先进入active_ap对应目录，在终端设置环境变量后，进入菜单栏按以下步骤完成配置：

① 在Serial flasher config中设置Custom baud rate value为115200。这个数值决定了串行端口的传输速率。实验时我们发现烧录波特率过高如：1152000或155200将会导致输出结果乱码，波特率过低则可能导致采样率有滞后，最终选用了适中的115200。

② 在Channel for console output中选择Custom UART并设置其UART console baud rate为相同的115200。这样设置的目的是将提取到的CSI数据通过串口导出到笔记本电脑进行保存和后续处理。

③ 在Wi-Fi中设置 Wi-Fi CSI(Channel State Information),具体实验时选择环境中信道干扰数较低的信道。

④ 在FreeRTOS 中设置Tick rate (Hz)为1000。

⑤ 在ESP32 CSI Tool Config中设置AP的SSID和PASSWORD。目的是和环境中其它接入点区分，并且使得STA能和指定AP建立连接。

⑥ 在ESP32 CSI Tool Config中设置允许捕获CSI并且导出到串口。

对于STA模式，上述步骤基本相同，但步骤5需要设置其欲连接的AP的SSID和PASSWORD，此处我们将其设置为与AP一致，否则无法连接上AP。完成上述配置后，清空项目中已有编译结果，重新编译。根据MN和CN与笔记本相连的端口号，将编译后的项目烧录到对应的ESP32开发板。

(2) 采集数据

将编译后的项目烧录到对应的ESP32开发板后，后续可在程序中需要采集数据时调用对应信道探测脚本进行软件环境激活以及对项目监视输出。

■ 可行性分析

1. 提取功能测试

在完成提取环境搭建后，本文初步检验了ESP CSI Toolkit这一基于ESP32开发的CSI提取工具的可行性。对作为MN和CN的ESP32，分别使用ESP CSI Toolkit目录下的AP和STA程序，设置AP对应SSID及密码，选择信道13，进行获取CSI的相关组件设置，

最后分别烧录，于终端观察工具运行情况。将两个ESP32开发板摆放于室内，相距约1米，启用脚本使其同时工作，如图2-7所示，由已经完成软件环境搭建的笔记本电脑进行MN和CN间CSI数据提取开始和终止的调控、监视数据的输出，并导出捕获的CSI。

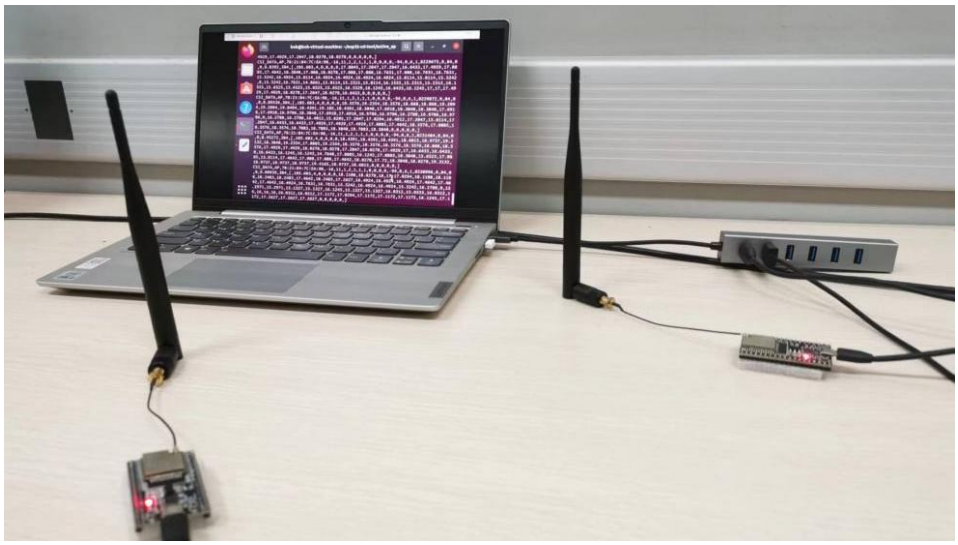
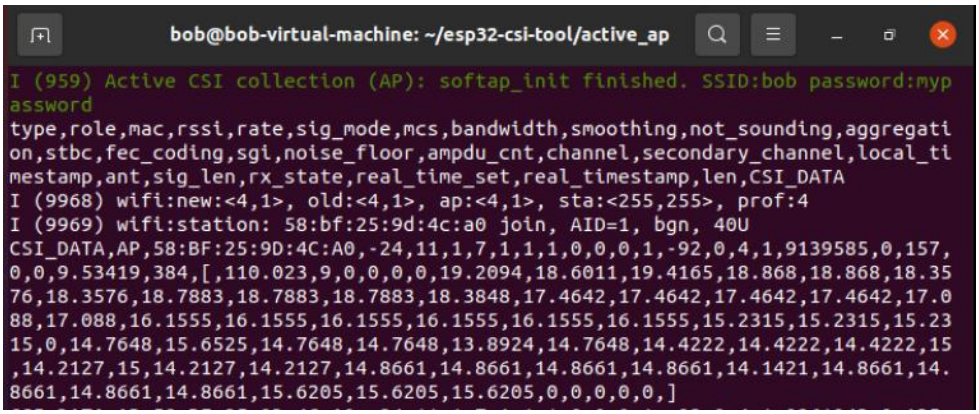
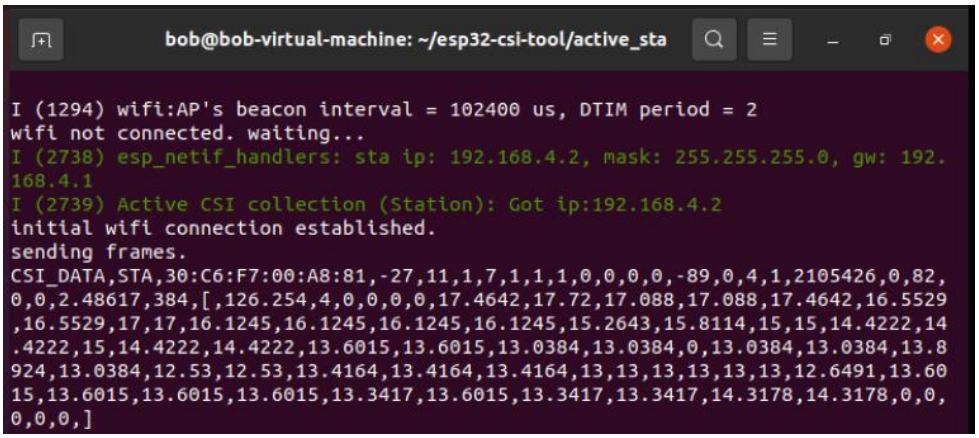


图2-7 基于ESP32的CSI提取环境示意图



(a) 移动节点MN端捕获数据输出图



(b) 控制器节点CN捕获数据输出图

图2-8 ESP CSI Toolkit测试结果图

如图2-8所示，此工具可以使得MN和CN进行相互的CSI提取，并且给出了对应设备的MAC地址、RSS、时间戳、带宽等信息。

2. 多用户接入可行性测试

根据ESP32的使用指导文档，ESP32工作模式为AP时，最多可接入10个设备，随后选择了7个ESP32开发板，按上一节完成提取环境搭建，其中一个作为MN，其余6个作为CN，分别烧录对应程序，使用脚本使得7个设备同时运行CSI提取工具，结果显示MN能正常连接6个CN，且实现对应CSI的提取，各个终端也能通过来自MN的数据包成功提取到CSI。这一工作为后续实现多个用户对应的CN接入一个MN的场景中的身份认证和密钥生成奠定了实践基础。

2.4.3 设备指纹提取

■ 方案简述

通信双方控制器节点CN向移动节点MN发送双方已知的信号，MN接收后利用上述的信道特征提取工具从中提取CN到MN的传输特性信号的频谱即信道状态信息，而后MN向CN发送已知信号，CN接收后利用上述的信道特征提取工具从中提取MN到CN的信道状态信息，并加密传输给MN，MN接收后计算两个信道状态信息的比值，在信道互易性理想的情况下可以直接获得包含CN设备物理特性的指纹信息。

■ 具体流程

处于无线体域网络中的通信双方CN和MN，控制器节点CN向移动节点MN发送双方已知的信号$x(n)$，该信号的频谱为$X(z)$：移动节点MN获得接收信号$y_M(n)$，该信号的频谱为$Y_M(z)$；

$$\mathrm{Y_M(z)=X(z)\cdot H_{TC}(z)\cdot H_{CM}(z)\cdot H_{RM}(z)} \tag{2.14}$$

移动节点MN将已知信号$x(n)$作为应答信号直接发送。CN接收到MN发送的应答信号获得信号$y_C(n)$；控制器节点CN获得的信号的频谱$Y_C(z)$满足：

$$\mathrm{Y_C(z)=X(z)\cdot H_{TM}(z)\cdot H_{MC}(z)\cdot H_{RC}(z)} \tag{2.15}$$

CN接收到接收信号后求取MN到CN传输特性信号，同时将MN到CN的传输特性信号

$v_{MC}(n)$不失真传输给MN。在频域，根据接收信号$y_C(n)$的频谱$Y_C(z)$除以已知信号$x(n)$的频谱$X(z)$，得到MN到CN传输特性信号的频谱：

$$V_{MC}(z)=\frac{Y_C(z)}{X(z)}=H_{TM}(z)\cdot H_{MC}(z)\cdot H_{RC}(z)=CSI_{MC} \tag{2.16}$$

$H_{TM}(z)$为移动节点MN发射机的传递函数，$H_{MC}(z)$为MN到CN信道的传递函数，$H_{RC}(z)$为控制器节点CN接收机的传递函数，特别地此处CSI_{MC}代表实际应用中提取的信道状态信息，因此包含了发射机和接收机的特征，与理论定义上的信道状态信息即信道传递函数$H_{CM}(z)$和$H_{MC}(z)$应有所区分；再计算$V_{MC}(z)$和$V_{CM}(z)$的幅度商，即：

$$RFF_C(z)=|V_{CM}(z)/V_{MC}(z)|=\frac{H_{TC}(z)\cdot H_{RM}(z)\cdot H_{CM}(z)}{H_{TM}(z)\cdot H_{RC}(z)\cdot H_{MC}(z)} \tag{2.17}$$

$V_{CM}(z)$为CN到MN传输特性信号$v_{CM}(n)$的频谱，用控制器节点CN发射机的传递函数$H_{TC}(z)$，CN到MN信道的传递函数$H_{CM}(z)$和移动节点MN接收机的传递函数$H_{RM}(z)$表示为：

$$V_{CM}(z)=H_{TC}(z)\cdot H_{RM}(z)\cdot H_{CM}(z)=CSI_{CM} \tag{2.18}$$

又由于信道传递函数$H_{CM}(z)$和$H_{MC}(z)$满足信道互易性，即：

$$H_{CM}(z)\approx H_{MC}(z) \tag{2.19}$$

在忽略接收信号中的噪声干扰时，最终提取到包含CN设备信息的指纹特征表示为

$$RFF_C(z)=\frac{CSI_{CM}}{CSI_{MC}}=H_{TC}(z)\cdot\frac{H_{RM}(z)}{H_{TM}(z)\cdot H_{RC}(z)} \tag{2.20}$$

实际应用中无法避免噪声的干扰，使用符号堆叠法减少影响， Wi-Fi信号中一个64点长导码符号仅包含52个子载波，最终对应提取的CSI包含52个有效数值，对第k个子载波而言，从中提取的包含设备物理特性的指纹信息具体表示

$$\overline{RFF_C}(k)=\frac{\frac{1}{N}\sum_{l=1}^{N}TC^l(k)H_{CM}^l(k)RM^l(k)+\frac{1}{N}\sum_{l=1}^{N}Z_1^l(k)}{\frac{1}{N}\sum_{l=1}^{N}TM^l(k)H_{MC|}^l(k)RC^l(k)+\frac{1}{N}\sum_{l=1}^{N}Z_2^l(k)} \tag{2.21}$$

考虑到噪声服从复高斯分布，因此最终第k个子载波而言，从中提取的包含设备

物理特性的指纹信息具体表示为：

$$\overline{RFF_C}(k) = \frac{\frac{1}{N}\sum_{l=1}^{N} TC(k)H_{CA}(k)RM(k)}{\frac{1}{N}\sum_{k=1}^{N} TA(k)H_{MC}(k)RC(k)} = \frac{TC(k)RM(k)}{TM(k)RC(k)} \qquad (2.22)$$

由于CSI可表征为幅度和相位，又可以分别应用得到基于幅度值表示的指纹与基于相位值表示的指纹。

■ 可行性分析

为初步验证此设备指纹提取方案是否有效，选用5个型号一致的ESP32开发板作为5个CN设备，对其进行指纹提取。考虑到CSI具有幅度和相位信息，最终可在两种维度提取到指纹如图2-9所示，从图2-9可知，此方法能提取出具有区分度、唯一性的指纹。

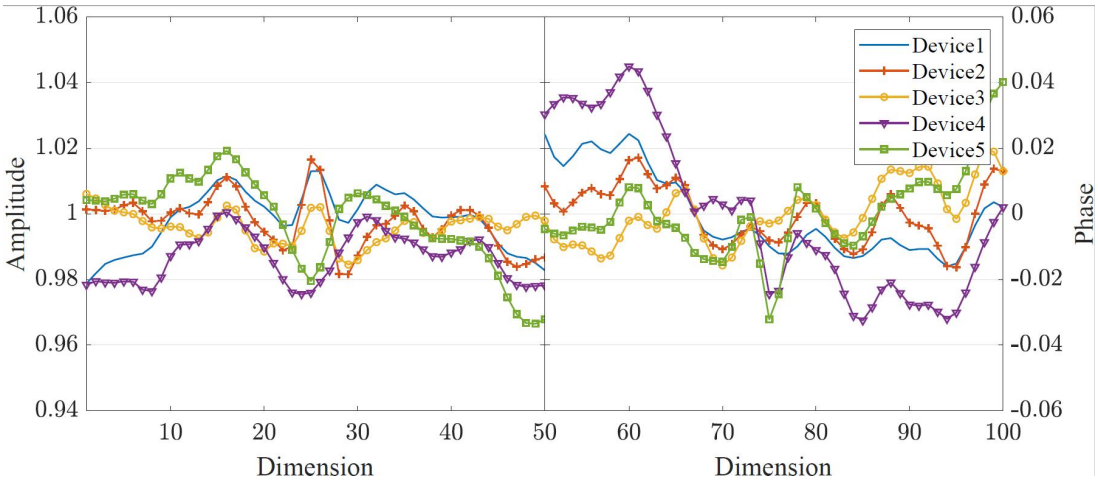


图2-9 设备指纹图

2.4.4 设备身份认证

■ 方案简述

基于射频指纹的身份认证方案中，MN对欲接入的多个合法CN按上述设备指纹提取原理计算取得各自的指纹信息纳入指纹库并训练分类模型。当一CN发起认证请求时，MN按上述方法计算取得指纹输入分类模型，分类模型对该设备指纹进行识别，若分类结果与CN声称的身份标识一致则CN身份合法。MN再将获得的MN到CN信道状态信息均值和自己的身份信息及认证成功段发给CN，CN与自己存储的数据均值作比对若一致则MN

合法性验证通过，至此双向身份认证完成。

■ 具体流程

利用前馈神经网络，使用监督学习方法，根据用户标记的目标集对提取的指纹特征进行分类。前馈神经网络其基本结构由神经元组成，以前馈形式连接成输入层、隐藏层和输出层。前馈神经网络的优点是由于其优良的函数逼近性，具有更好的模式检测性能，以及可以很容易地模拟复杂和非线性关系。

本系统考虑的前馈神经网络由三层组成：一个输入层、一个包含50个隐藏神经元的隐藏层和一个输出层。在训练阶段，将指纹信息设置为训练输入，被提取指纹的设备身份设置为训练目标，每一个隐层中的每个神经元都接收来自前一层的输入，通过权重和偏差的连接来处理，并将结果传递给下一层。然后，在隐层和输出层上，将前一层的结果通过激活函数归一化为概率分布。

我们定义四个主要的方法：前向传播方法forward，反向传播方法backward和预测方法predict和训练方法train。在前向传播方法forward中，使用权重和偏置计算加权和，然后通过tanh函数计算激活值。在输出层，直接计算加权和和输出值。在反向传播方法backward中，首先计算误差，然后计算参数的梯度，并使用梯度下降法更新参数。在训练方法train中，进行前向传播和反向传播的交替训练。在预测方法predict中，使用训练好的模型进行预测并返回具有最大值的输出作为预测类别。以下为前馈神经网络训练过程的详细步骤：

第一步：初始化参数

训练前馈神经网络前，首先对其参数进行初始化，本系统选择了随机初始化权重矩阵和偏置向量。

第二步：前向传播

调用前向传播方法forward，首先计算了隐藏层的加权输入z1，然后将其输入到tanh激活函数中，得到了隐藏层的激活输出a1。接下来计算了输出层的加权输入z2，并将其输入到softmax函数中，得到了输出层的激活输出output。

第三步：计算代价函数

利用均方误差（MSE）最小化代价函数。

第四步：反向传播

前馈神经网络训练的核心在于参数的更新，选用梯度下降法进行优化。其基本思

想是通过计算代价函数对参数的偏导数来更新参数。

第五步：更新参数

在反向传播求解梯度信息后，根据梯度信息对网络中的参数进行更新。

第六步：重复以上过程

最后，在模型训练中重复以上过程，直到达到指定迭代次数。

■ 可行性验证

为初步验证设备身份识别方案是否有效，利用上一小节5个型号一致的ESP32开发板作为5个CN设备提取的指纹作为数据集，其中80%作为训练集20%作为测试集，训练模型后用测试集验证已训练好的模型分类准确率，结果如图2-10所示，可以看到此方案具有较高的识别准确率。

图2-10 分类结果混淆矩阵

2.4.5 信道特征量化

■ 方案简述

此模块将在设备完成信道探测后，对所获CSI幅度进行归一化处理，然后按分块格雷算法进行量化。

■ 具体流程

1. 选择量化算法

常用的量化算法有无门限的2比特量化、选用中位数的单阈值量化、选用均值和方差的双阈值量化、分块格雷量化等。本方案中采用了对互易性要求一般，综合性能较好的分块格雷法，本方案最终选择的20MHz带宽能捕获到64个子载波的信道特征，根据802.11n协议相关说明，最终含有效数据的子载波序号为-26至-1和1至26，共52个。分块格雷量化算法的流程为：

① 设备对所获一轮信道探测的一组信道测量值按升序或降序排列。

② 设备将排序后的信道测量值尽可能均分为个数据块，k为格雷编码位数。每个数据块按顺序标上序号，数据块里的元素其标号与所属块序号一致。

③ 按原有信道测量值分布顺序使用k位的格雷编码将每个数据元素量化为0,1序列。

2. 按需调整量化方案

当所需密钥长度与当前单个数据包生成的密钥长度不匹配时，可按需调整，为此本方案进一步设想了“间隔取样，多组量化”这一机制。间隔取样指间隔一定数据包数来对所获信道测量值进行量化，多组量化则是指根据所需密钥长度和密钥的随机性表现选择拼接的组数。另一方面，取样间隔极小时，信道环境变化不明显，密钥较为相似，取样间隔过大时生成一组所需长密钥时间过长，因此取样间隔最终定为100个数据包。综上，量化方案具体流程如图2-11所示。

具体步骤描述如下：

① MN和CN各自对所获一轮信道探测的一组64个子载波CSI幅度值（共64字节），去除前两字节硬件缺陷造成的无效数据，再去除802.11.n协议中规定的不承载有效信息的子载波以及0号子载波对应的空数据。获得52个子载波的CSI幅度值。

② 对52个子载波的CSI幅度值进行归一化处理并从小到大排列。

③ MN和CN各自将其52个值均分为4个数据块，每个数据块按顺序标上序号，数据块里的元素其标号与所属块序号一致。

④ 按原有的子载波CSI分布顺序（-26至-1,1至26）使用格雷编码将每个数据元素量化为2位的0,1序列，获得长度为104位的原始密钥。

⑤ 间隔100组，再取一组64个子载波CSI幅度值，重复步骤1至4的操作，获得第2组长度为104位的原始密钥。若仍不满足拼接成的长密钥的位数要求，则重复步骤5。

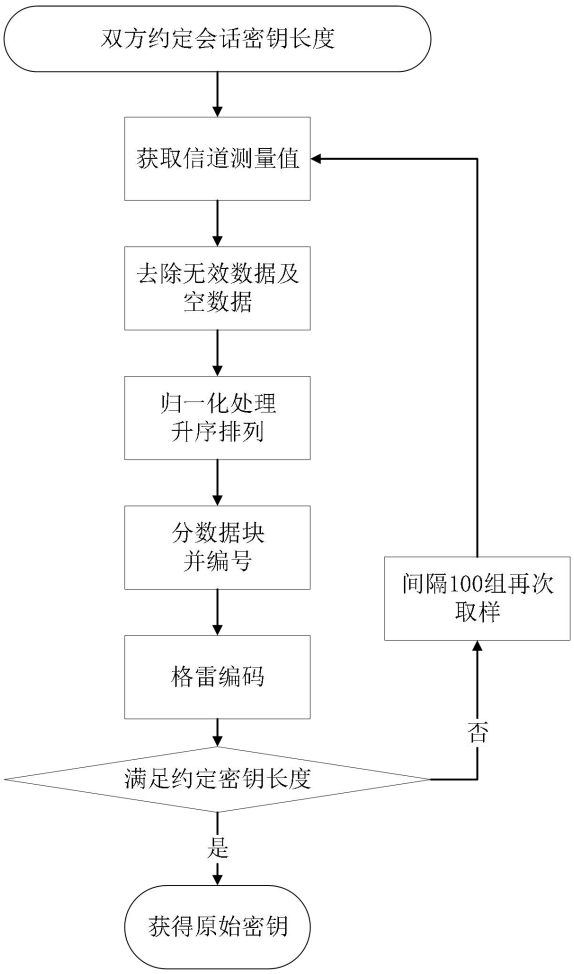


图2-11 量化方案流程图

■ 可行性分析

信道测量值可保存为csv文件，在python中提供了相关的读取csv文件的函数、去除矩阵特定列的函数、归一化的函数等，编写其余函数实现数据分块编号以及格雷编码也较为容易实现。综上，此方案可行。

2.4.6 会话密钥协商

■ 方案简述

MN和某一个CN在各自完成信道特征量化后，由CN生成一协商信息发送给MN，之后双方通过BCH纠错码完成密钥协商，如果双方的原始密钥不一致位数在阈值以内，则可以协商成功生成一致密钥，否则提示用户重新选择数据。

■ 具体流程

受硬件不对称等影响，双方信道测量值经过量化后仍可能有不相同的密钥位，如果双方不同的密钥位数目较少，则可以等同于噪声对一般性通信过程的影响，可以使用纠错算法来纠正。密钥协商通常使用纠错码（Error Correction Codes ，ECCs）来实现。根据BCH纠错码原理，以及上文中量化所得原始密钥长度，我们设想不一致率不能超过20%，以免因为频繁协商增加信息泄漏风险，因而将纠错位数上限设置为22位。

具体步骤如下：

① 首先由CN生成一个随机的原始消息c并执行BCH编码和密钥 K_A 一起处理后生成协商信息 s。

② 假设MN无差错地收到协商信息 s，然后将协商信息与自身密钥 K_B 一同经过BCH译码得到 c_B。

③ 根据 c_B 定位不一致位置还原c。

④ MN由协商信息 s 和还原的c得到纠错后的密钥。

■ 可行性分析

对于通信双方Alice和Bob，其通常的工作机制为Alice从ECC的代码集中随机选择一个码字c,再将码字c与自己的密钥 K_A 进行异或得到秘密信息 s 发送给Bob，即：

$$s = K_A \oplus \mathrm{c} \tag{2.23}$$

假设Bob无差错地接收到 s，则计算 K_B 和 s 的异或得到 c_B 即：

$$c_B = s \oplus K_B \tag{2.24}$$

如果 c_B 和 c 的汉明距离在纠错范围内，则Bob可以通过 c_B 解密得到 c，再通过计算

$$K_B = c \oplus \mathrm{s} \tag{2.25}$$

就能得到和Alice相同的密钥。

BCH纠错码（Bose－Chaudhuri－Hocquenghem codes）是常用纠错码的一种，能够利用不同的本原多项式实现多位纠错。将通信双方称为Alice和Bob，其纠错的基本原理为：令Alice欲发送的原始消息为 $m(\mathrm{x})$，根据纠错位数 t 设计一个编码多项式

$Q(x)$，$Q(x)$为通信双方提前共同商量好，其标准形式为：

$$Q(x)=p(x)p_3(x)p_5(x)\cdots p_{2t-1}(x) \tag{2.26}$$

其中$p(\mathrm{x})$是本原多项式，而其余各式需满足以下关系：

$$p_{2i-1}\left(x^{2i-1}\right)=0 \pmod{p(x)},1\le i\le t \tag{2.27}$$

然后使用上述的编码多项式$Q(x)$，计算出发送的消息s：

$$s=m(x)\bullet Q(\mathrm{x}) \tag{2.28}$$

传输过程中受到噪声等干扰，令其为$e(x)$，则Bob收到的消息为：

$$\mathrm{c(x)=m(x)\bullet}Q\mathrm{(x)+e(x)} \tag{2.29}$$

Bob按下式计算：

$$\frac{\mathrm{c(x)}}{p(x)}=m(\mathrm{x})\ldots\frac{\mathrm{e(x)}}{p(\mathrm{x})} \tag{2.30}$$

则Bob可以根据上式的余项来定位何处与Alice欲发送的原始信息不同从而纠正。根据上述原理分析，此方案可行。

第三章 作品测试与分析

3.1 测试方案

系统的功能模块包含数据采集模块、指纹提取模块、设备识别模块、密钥协商模块、安全服务模块以及可视化平台。数据采集、设备指纹特征的提取与选择以及识别算法的设计都与最终识别的准确率紧密相关。设备识别的准确率关系到系统误报率的高低，设备的指纹作为设备的标记能使我们区分设备身份是否合法，而合法性的确认决定了后续对无线体域网内设备的访问控制。密钥协商模块则为已经确认合法的设备之间提供会话安全保障。密钥的高一致性将能减轻信息协商时的压力，避免因为协商频繁泄露更多信息。而密钥的随机性也影响着密钥的安全性。在用户端完成身份认证以及会话加密后，系统还通过安全服务模块提供辅助的安全服务如身份认证监控、密钥生成监控、日志与警报等。系统提供可视化界面展示各功能单元的运作效果，五大模块共同完成了设备间身份认证、设备间密钥共享、系统安全管理和为用户提供安全服务的目标。系统测试将从两方面展开：性能测试、功能测试。

3.1.1 性能测试

性能测试主要为了测试以下两个方面：一是验证系统是否能在实际应用中利用信道特性提取出用于身份识别的设备指纹并正确识别设备身份是否属实进而判别设备是否合法；二是验证系统所生成的会话密钥能否满足基本的性能需求，即密钥一致性、密钥随机性、密钥安全性。具体而言：

1. **信道互易性**：设置5米×4米的矩形空间，四周有桌椅，仿照真实的使用环境。实验环境变量设置包含是否静态（实验人员是否走动）、控制器节点与移动节点间距离远近、控制器节点与移动节点间有无墙体阻隔，全方位地观察各种环境中数据所体现的互易性。具体地，为使得数据有普遍意义，采集1000组信道状态信息数据，以标号100的数据包为起始，间隔100组计算一次互易性系数。最后取MN-CN1、MN-CN2、MN-CN3的平均值作为该实验场景下信道互易性测试的结果。

2. **指纹唯一性**：选取相同的实验环境，使用相同型号的不同设备模拟实际场景

中的CN，与MN交互生成设备指纹，对比不同设备生成的指纹是否具有显著差异性，以验证指纹唯一性。

3. 指纹稳定性：在不同信噪比、不同时间段、不同环境（如视距或非视距）的信道环境中对同一设备进行指纹生成，对比多次实验生成的指纹是否一致，以验证指纹稳定性。

4. 身份识别准确率：设置5米×4米的矩形空间，四周有桌椅，仿照真实的使用环境。实验环境变量设置包含是否静态（实验人员是否走动）、控制器节点与移动节点间距离远近、控制器节点与移动节点间有无墙体阻隔。测试在不同场景中，同一型号的不同CN设备重新接入MN向其发起认证请求时被正确识别分类进而合法性被认证通过的比例。

5. 密钥协商成功率：为使得数据有普遍意义，在不同的实验环境中采集1000组信道状态信息数据，以标号100的数据包为起始，间隔100组统计双方利用该组数据生成的原始密钥不一致位数最后取均值并计算不一致率，代表该场景下的密钥一致性情况。再按密钥协商方案进行协商仿真，计算密钥协商成功率最后取均值得到该场景下的平均密钥协商成功率。

6. 密钥随机性：使用美国国家标准与技术研究院（National Institute of Standards and Technology， NIST）的随机性测试来检验生成的密钥是否符合随机性要求。考虑到NIST随机性测试对待测数据的容量要求，选用了6种测试项目，对视距和非视距的不同距离下的场景所得密钥进行随机性检验。

7. 密钥安全性：通过设置被动窃听场景，将窃听者捕获到的信道状态信息与合法用户的进行比较，如果高度不相关则论证了此密钥生成方案的防窃听性。选取3个ESP32分别作为MN、CN、Eve，MN与CN视距1米左右。在使用2.4GHz的频段时，对应半波长约为12厘米，实验中使Eve距离CN约30厘米，超过半波长。对比Eve捕获到的MAC地址为CN的CSI数据与MN、CN端的CSI数据。计算MN和CN, Eve和CN间的互易性系数，并进行比较。

3.1.2 功能测试

功能测试主要是为了测试平台各功能单元的实现效果，具体功能单元如下：

1.设备指纹数据库：目的是通过合法设备登记接口、合法设备取消登记接口、数

据库查询接口、数据库增加接口、数据库修改接口、数据库删除接口检测能否实现新增、删除、查询数据库数据。完成合法设备指纹数据的登记和解析，将有效信息记录数据库。根据指纹库的信息对设备进行分类识别，对比分类结果与声明身份，判别设备身份合法状态。

2.身份认证实时监控：目的是通过身份认证监控接口观察能否获取设备指纹与数据库中合法设备的指纹进行比较，判断是否合法，达到对接入设备的合法性进行实时监控的目的。

3.密钥协商：目的是调用信道探测程序，接收来自控制器节点的探测请求并发回响应;接收控制器节点发送的协商信息并完成密钥纠错计算纠错后密钥的哈希值，完成哈希值比对，得到一致密钥。

4.密钥生成实时监控：目的是统计汇总和不同设备协商生成密钥的时间、协商结果和对应密钥信息。

5.指纹匹配：目的是根据指纹数据库中的合法设备指纹训练得出的分类模型，比对合法设备指纹信息和待认证设备的指纹信息，根据分类结果与声称身份是否一致对设备的合法与否进行状态标记。

6.云管控：目的是通过指纹识别结果查询接口、指纹识别参数查询接口、指纹识别参数设置接口，检验当前用户拥有使用该功能的权限时，能否设置指纹识别的参数，进而查询指纹识别的结果的参数。

7.日志与警报：目的是记录并更新身份认证日志、密钥协商日志，用于数据维护。当用户具有使用该功能的权限时，身份认证日志或密钥协商日志进行显示，供用户查看。

3.2 测试设备

为了验证在体域网应用中的身份认证和密钥协商功能的可行性和稳定性，我们用4个乐鑫科技旗下同一型号的搭载ESP32-WROOM-32U模组的ESP32-DevKitC-v4开发板，其中3个作为CN（设置为Station模式，简记为CN1,CN2,CN3）和1个作为MN（设置为AP模式）来验证身份认证和密钥协商两大基本功能，以一台电脑运行验证可视化平台辅助验证其余功能。

(a)MN (b)CN1 (c)CN2 (d)CN3

图3-1 测试用ESP开发板一览

ESP32开发板相关参数如表3.1所示。

表3-1 测试所用ESP32开发板参数设置

设备编号	工作模式	MAC地址	频段带宽
MN	AP模式	78:21:84:7C:EA:99	20MHz
CN1	Station模式	78:21:84:7C:F5:70	20MHz
CN2	Station模式	58:BF:25:18:BF:30	20MHz
CN3	Station模式	58:BF:25:18:99:AC	20MHz

3.3 测试环境搭建

控制器节点CN一般可位于患者身体上或位于患者身体附近，本作品为模拟更复杂的使用环境，将CN固定于实验人员手臂。在无线体域网的实际应用中，患者可能静卧于某个位置或在房间内自由走动，据此我们以理想的相对静止的静态环境和符合现实的有人体移动的动态环境作为两大测试方向，又考虑到实际使用中MN和CN存在距离远近、受墙体阻隔等情况，设置了视距与非视距下不同距离的场景，测试场景汇总如表3.2所示。

表3-2 测试场景汇总

场景编号	场景内容
1	静态视距1米
2	静态非视距1米
3	静态视距3米
4	静态非视距3米
5	动态视距1米
6	动态视距3米

测试场景均设置于室内，以模拟无线体域网多为在室内使用的情景。场地选为一个5米×4米的矩形房间，室内四周有墙壁桌椅阻挡，实验环境如图3-2，3-3所示。以一个实验人员视角为例，实验人员佩戴CN，视距环境下时同移动节点MN位于同一室内，

非视距环境下时移动节点与实验人员分属于房间内外，搭载可视化平台的电脑与MN相连接用于接收来自MN的数据提供相关安全服务，供操作人员选择各个功能按钮调用运行相关程序。静态场景中实验人员几乎保持不动，动态场景中实验人员可自由走动、站立、坐下。

图3-2 静态实验场景实拍图

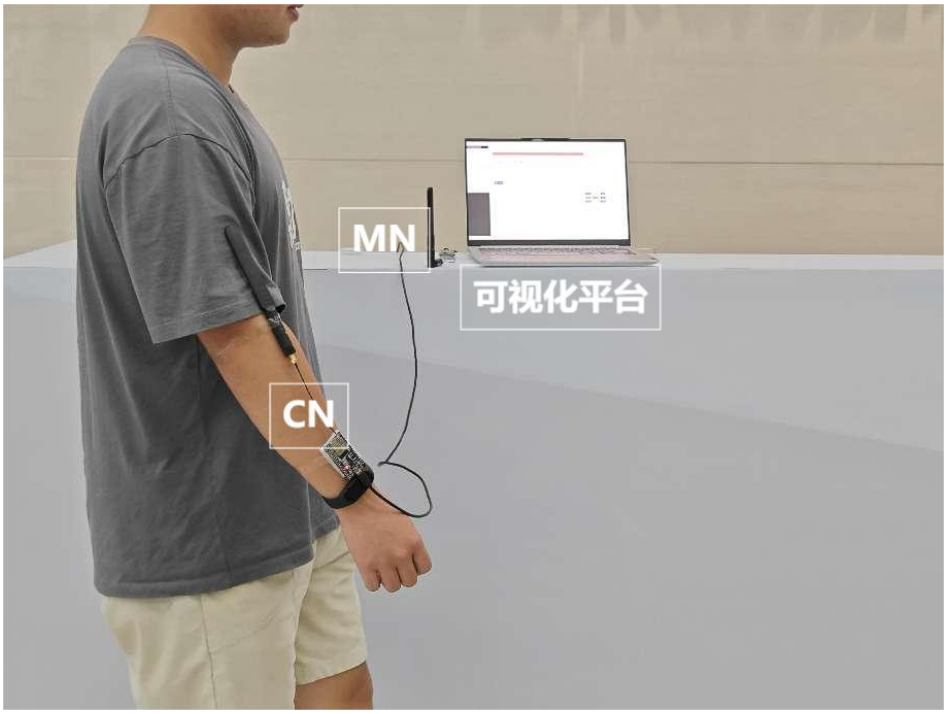


图3-3 动态视距实验场景实拍图

3.4 测试数据及分析

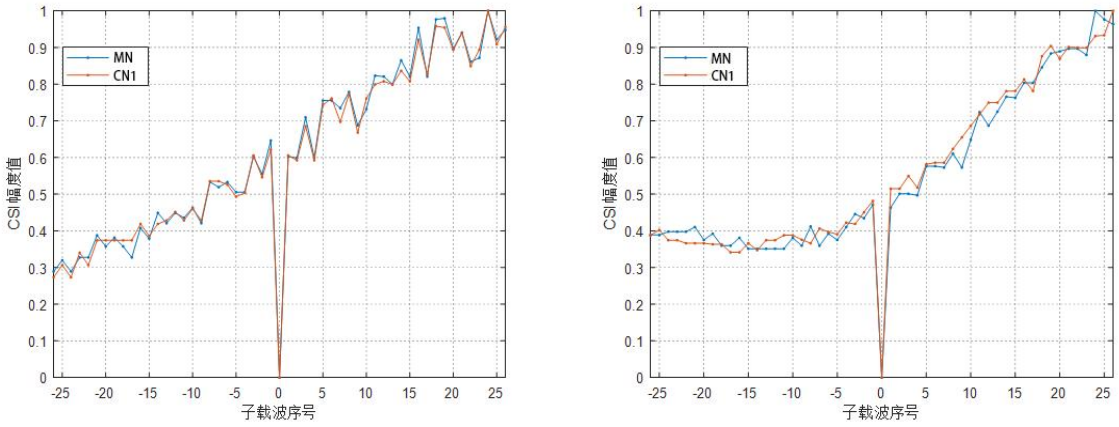
3.4.1 性能测试

3.4.1.1 信道互易性

1. 静态视距测试

首先进行静态视距1米的实验：将MN放置在距离3个CN约1米处，各个CN间相距约0.8米，保持环境的相对静止，避免实验人员的走动和设备的移动，如图3-2所示。让MN和3个CN同时工作，进行1000轮信道探测，采集1000组MN和对应CN间的CSI幅度值数据分别导出，图3-4(a)展示了视距1米时MN与对应CN1间的CSI幅度值对比图。

然后移动MN，使其距离3个CN约3米，各个CN间保持相距约1米，环境仍保持相对静止，进行静态视距3米的实验。同样让MN和3个CN同时工作，采集1000组以上MN和对应CN间的CSI幅度值数据，图3-4(b)展示了视距3米时MN与对应CN1间的CSI幅度值对比图，与图3-4(a)对比，可看出设备间距离的增长会对测量值的相似程度有所影响，尽管MN和CN的数据整体趋势相似，但有更多子载波数据点趋势不同，曲线重合度略有降低。



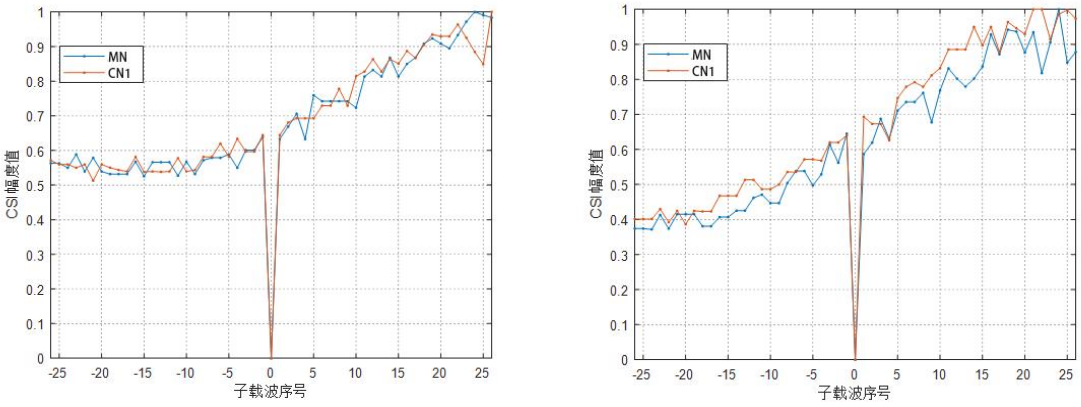
(a) 视距1米：MN与CN1　　(b) 视距3米：MN与CN1

图3-4 静态视距1米与3米CSI幅度值对比图

2. 动态视距测试

我们重新按视距1米时的实验设置摆放MN和CN，但在实验开始后，让佩戴控制器

节点的实验人员以普通步速在移动节点MN半径1米范围内自由行走，如图3-3所示，进行动态视距1米的实验。



(a) 视距1米：MN与CN1　　(b) 视距3米：MN与CN1

图3-5 动态视距1米与3米CSI幅度值对比图

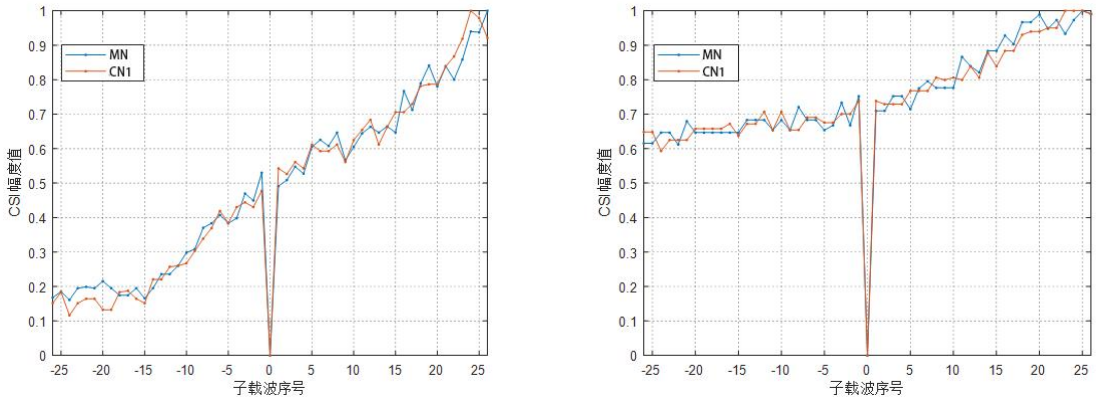
作出MN和对应CN间的CSI幅度图，如图3-5(a)所示。可以看出同一设备组合且设备间视距相同时在静态环境中所获数据比动态环境互易性更好，其原因是环境中有人体移动，信号所经历的散射、折射等更为丰富，多径效应一定程度上影响了信道测量值的相似程度，使其有所下降。

我们重新按视距3米时的实验设置摆放MN和CN，实验人员于实验开始后到实验终止时以普通步速在移动节点MN半径3米范围内自由行走。作MN和对应CN间的CSI幅度图直接对比观察，对比图3-4(a)与图3-5(b),可知距离与移动障碍物的双重影响使得所获数据相似程度更低，但通信双方数据基本走势仍然相同。

3. 静态非视距测试

在分别验证了距离和环境中有无移动障碍物对互易性的影响后，分别测试了静态非视距1米和静态非视距3米两种场景下CSI提取工具的短时互易性效果，目的是检验墙体阻隔是否会影响数据相似性。在静态非视距1米的测试中，将MN放置于室外，3个CN端放置于室内，中间有厚度约10厘米的墙体作为阻隔，MN与各个CN间距为1米左右，各个CN间相距0.8米左右。测试过程与数据组数要求同视距1米。

如图3-6(a)所示，墙体的阻隔轻微地降低了所获信道测量值的相似程度，这是由于信号在穿墙传输的过程中发生反射、散射等。



(a) 非视距1米：MN与CN1　　(b) 非视距3米：MN与CN1

图3-6 静态非视距1米与3米CSI幅度值对比图

在静态非视距3米的测试中，墙体阻隔同上，MN与CN间距约3米，各个CN间仍间距约1米。测试流程依然不变。如图3-6(b)所示，与静态视距1米时相对比可以发现墙体和距离的双重影响使得互易性受到一定影响。

为取得更为直观的对比和衡量，按2.3.1中所提出的互易性系数对上述实验场景的结果进行分析。为保证结果具有普遍性和稳定性，对MN和对应CN间所获的1000组CSI幅度值数据，从标号100的数据起，间隔100组计算一次互易性系数。最后再计算MN和对应CN间的$\overline{\rho(CSI_{AP},CSI_{STA})}$作为本次探测的信道测量值相似程度的定量描述。最后取MN-CN1、MN-CN2、MN-CN3的平均值作为该实验场景下互易性测试的结果。

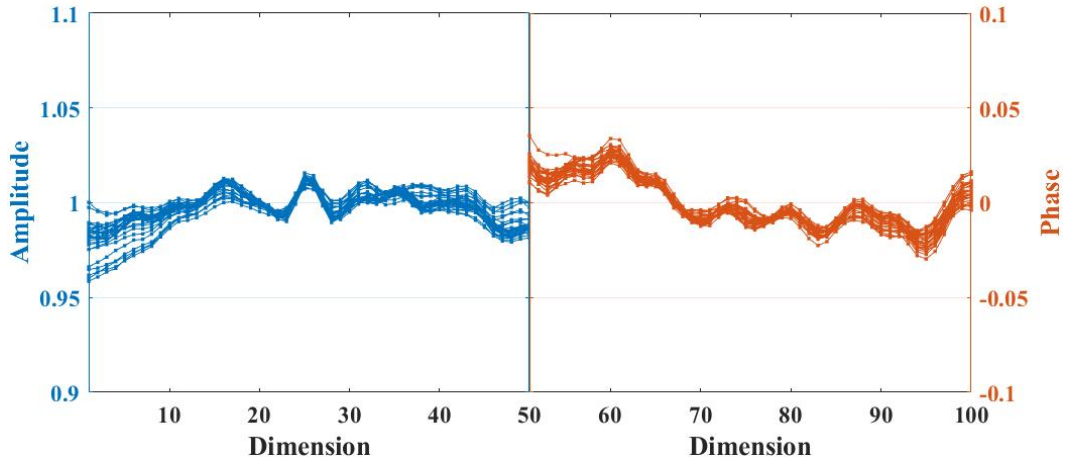
表3-3 不同实验场景的互易性系数

	MN-CN1	MN-CN2	MN-CN3	平均值
静态视距1米	0.993372199	0.994007502	0.991618317	0.992999339
静态非视距1米	0.986267135	0.987657146	0.975788798	0.983237693
静态视距3米	0.992123368	0.974880560	0.990022782	0.985675570
静态非视距3米	0.969491052	0.991994491	0.988183474	0.983223005
动态视距1米	0.977435483	0.991106167	0.959720184	0.976087278
动态视距3米	0.965021010	0.953290031	0.975557617	0.964622886

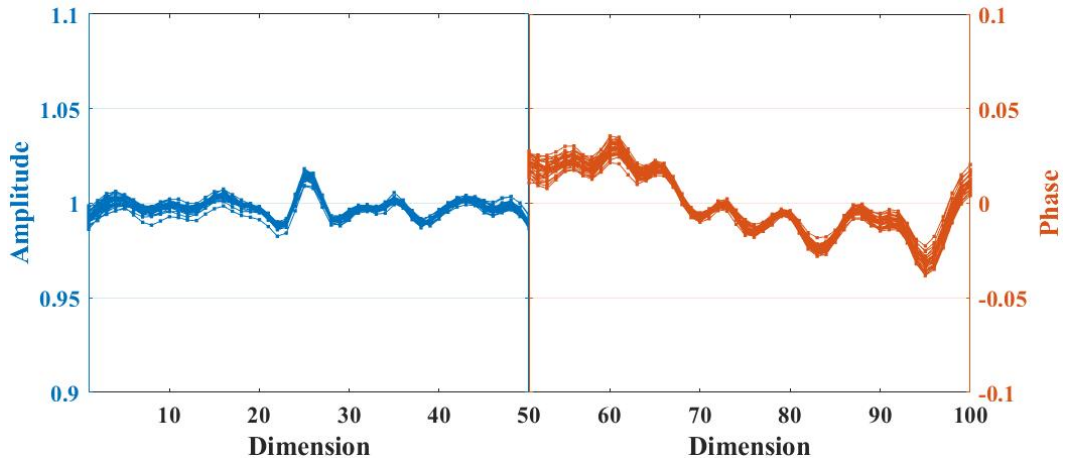
由表3-3可知距离的增加、墙体的阻隔、人体移动均会使互易性略有降低，但是六种场景中每一个MN-CN组合其互易性系数$\rho(CSI_{AP},CSI_{STA})$平均值均超过了0.95，各个场景的平均值都超过了0.96，这说明本作品提出的信道特征提取方案能获得互易性良好的数据，能适应实际应用中可能出现的多种场景，能为量化为一致密钥、提取设备指纹时减除信道干扰影响提供坚实基础，性能良好。

3.4.1.2 指纹唯一性

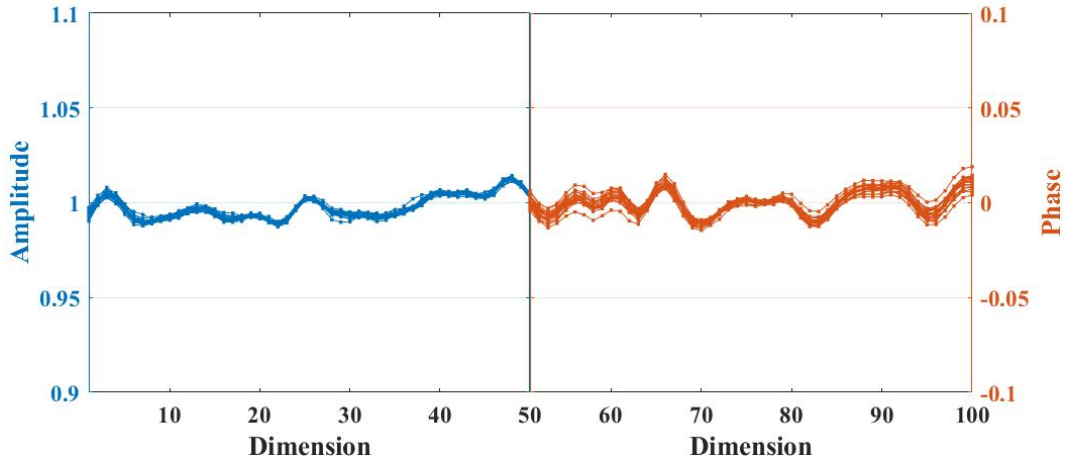
为验证指纹唯一性，我们控制实验环境变量相同，尽可能减少环境中的噪声对指纹生成的影响。实验环境选取为静态视距1米的实验场景下，选用设备型号均相同的设备CN1,CN2,CN3分别与MN进行交互。MN分别接收到CN1，CN2，CN3的信息后解密其传输的信息，获得身份识别请求、CN声明自己的身份ID和CSI_{MC}，利用MN到CN的信道状态信息CSI_{MC}与CN到MN的信道状态信息CSI_{CM}计算得到每台设备对应的射频指纹。生成的射频指纹如图所示：



(a) CN1生成的射频指纹



(b) CN2生成的射频指纹



(c) CN3生成的射频指纹

图3-7 静态视距1米不同设备生成的射频指纹对比图

由图3-7可知，不同的设备生成的设备指纹具有明显的差异性，证明该系统生成的设备指纹具有唯一性。

3.4.1.3 指纹稳定性

指纹稳定性指从Wi-Fi信号中提取的设备射频指纹，不应当受信噪比变化、时间变化、位置变化、信号传播过程中有无障碍物阻隔、信道变化等因素的影响。

为验证在不同信噪比的情况下指纹的稳定性，我们在静态的场景下，使用同一个设备CN与MN生成射频指纹。逐次加强实验的信噪比，多次实验生成两种类型的射频指纹（由CSI幅值生成的指纹和由CSI相位生成的指纹），进行对比。

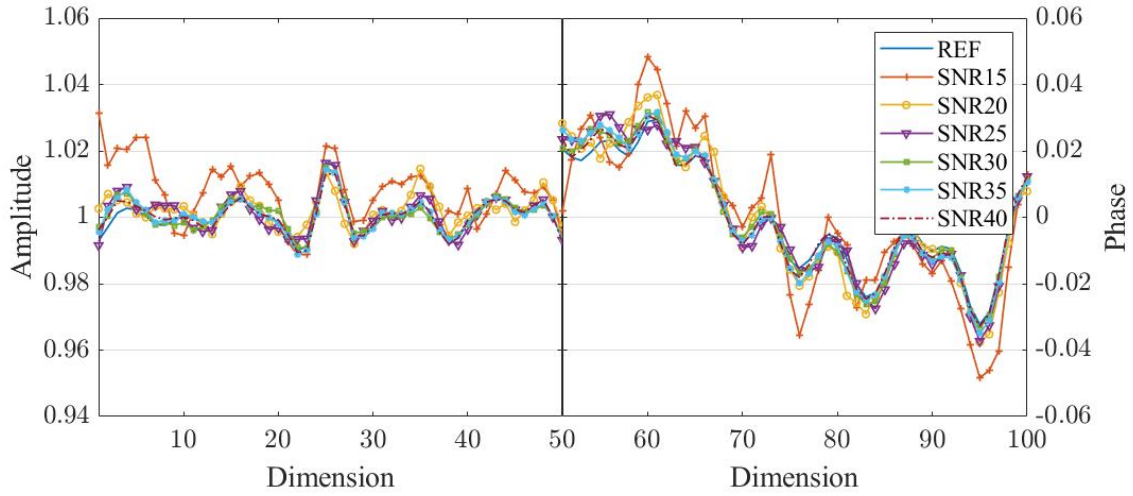


图3-8 静态视距1米CN1不同信噪比下生成的射频指纹对比图

从图3-8可知，虽然环境中的信噪比存在较大差异，但CN1生成的射频指纹高度一

致，不受信噪比变化的影响。

为进一步探究在位置变化的情况下指纹生成的稳定性，我们分别在动态和静态的场景下，使用同一个CN与MN生成射频指纹，进行对比。

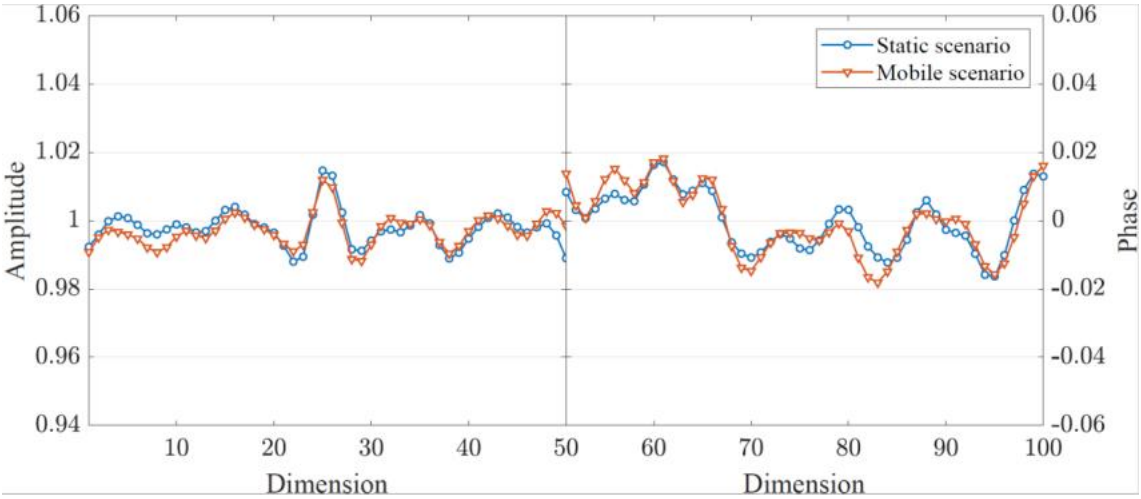


图3-9 静态和动态场景下CN1生成的射频指纹对比图

从图3-9可知，在动态和静态的场景下，CN1生成的射频指纹高度一致，说明指纹不受位置变化的影响。证明该系统生成的射频指纹具有稳定性。

3.4.1.4 身份识别准确率

为验证系统对身份识别的准确率，在不同场景下分别进行多次实验，由CN向MN发起认证请求后进行多次信号交互，提取足量指纹用于训练分类模型，在模型训练结束后断开CN与MN的连接，之后不断让CN多次发起接入MN的请求，MN将应用训练好的模型对其身份进行识别认证，利用可视化平台查看该段时间内的总的识别次数和合法比例，合法比例即为该段时间的识别准确率。

1. 场景一：静态视距1米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-02 9:41:13	75	75	0	100%	0%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-02 10:05:08	98	97	1	98.98%	1.02%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-02 10:45:15	80	80	0	100%	0%

图3-10 场景1-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到，经过初期采集、训练后，每隔一段时间运行CN向MN发起认证请求，并进行识别后，CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）

识别率均在98%以上，其中CN1与CN3识别率达到了100%。这一测试表明了本系统可以实现对合法设备的精确识别。

2.场景二：静态非视距1米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-02 11:02:27	64	63	1	98.44%	1.56%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-02 12:05:19	95	94	1	98.95%	1.05%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-02 13:45:19	80	80	0	100%	0%

图3-11 场景2-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到，尽管将CN与MN分处于室内外，存在其他设备收发数据、墙体阻隔等干扰，在已有训练基础上对识别率是可视为微弱影响的，CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）识别率均在98%以上。从CN1到CN3的识别率的提高是因为前期我们在室内近距离采集了其数据并进行了足量训练，因此继续增大训练量减弱了设备运行初期提取的到的特征不稳定的影响。本系统随着运行周期的增长和设备的平稳运行，所提取到用于匹配的特征会更利于匹配，因而识别率会有所提高，理想环境下且表现好时达到100%。

3.场景三：静态视距3米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-04 13:59:20	75	71	4	94.67%	5.33%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-04 16:56:44	130	125	5	96.15%	3.85%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-04 07:59:35	120	117	3	97.50%	2.50%

图3-12 场景3-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到，我们将CN与MN处于同一空间内，增大两者间距，CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）识别率略有波动，但均在97%以上。

4.场景四：静态非视距3米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-06 09:12:37	75	73	2	97.33%	2.67%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-06 10:07:39	130	127	3	97.69%	2.31%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-06 11:45:21	120	119	1	99.17%	0.83%

图3-13 场景4-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到，尽管将CN与MN间距离增大且分处于室内外，存在其他设备收发数据、墙体阻隔等干扰，在已有训练基础上对识别率是可视为影响微弱，CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）识别率均在98%以上。体现了本系统在有墙体阻隔等复杂的实际应用场景中，也能精确识别合法设备。

5.场景五：动态视距1米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-06 14:31:25	120	118	2	98.33%	1.67%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-06 15:11:34	130	130	0	100%	0%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-06 16:25:21	90	89	1	98.89%	1.11%

图3-14 场景5-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到，在各个实验人员走动的动态场景下，CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）也能被正确识别，识别率均在98%以上。说明在动态场景下，本系统也能对合法设备做出精确识别。

6.场景六：动态视距3米

设备名	mac地址	厂商	最后识别时间	识别次数	合法次数	非法次数	合法比例	非法比例
CN1	78:21:84:7C:F5:70	ESPRESSIF	2023-09-07 13:21:15	115	113	2	98.26%	1.74%
CN2	58:BF:25:18:BF:30	ESPRESSIF	2023-09-07 14:03:44	130	128	2	98.46%	1.54%
CN3	58:BF:25:18:99:AC	ESPRESSIF	2023-09-07 15:37:01	75	74	1	98.67%	1.33%

图3-15 场景6-设备CN_1 /CN_2 /CN_3识别率

从身份认证实时监控接口处可以查看到， CN1（对应MAC地址为78:21:84:7C:F5:70）、CN2（对应MAC地址为58:BF:25:18:BF:30）、CN3（对应MAC地址为58:BF:25:18:99:AC）在摆放于同一室内，距离达到3米且实验人员来回走动的动态场景下，对于合法设备的识别率也能达到98%以上。同厂商、相同型号的设备即同款但编号不同的设备测试凸显了本系统基于射频指纹对设备身份进行识别的优势，这是传统的只基于加密认证方案或者生理信号或用户运动模式识别不能达到的。凭借射频电路等的微小差异对最终的信号特征造成影响，使得每台设备的射频指纹完全不同，所以即便攻击者采用同一型号设备甚至还伪造MAC地址本系统也能因为其指纹与MAC的二元组匹配不上发现问题。

3.4.1.5 密钥协商成功率

为准确对比密钥协商前后的情况，在6种测试场景下各采集1000组MN和CN的CSI数据分别导出处理。对于MN和对应CN间所获1000组的CSI信息，间隔100组取样一次进行量化，得到10组原始密钥来分析一致性高低。分别统计不同CN与MN之间10组原始密钥密钥协商前双方的不一致位数均值，进而得到某个实验场景中三个设备组合的不一致位数均值，并计算该场景下的密钥不一致率，而后按照2.4.6节所述的协商原理进行协商仿真，统计协商成功次数计算得到平均协商成功率。例如，静态视距1米下，MN和CN1的10组原始密钥经过对比得到平均不一致位数为5.2位，MN和CN2，MN和CN3的数据同理，该场景下不一致位数均值为（5.2+3.3+4.2）/3=4.23位，一组含52个有效子载波的CSI幅度值信息可量化为104位，该场景下不一致率为4.23/104=4.07%。对设备组合MN和CN1，按协商原理进行协商仿真，10组密钥协商10次，成功10次，平均协商成功率为100%。

表3-4 各场景密钥协商前后情况统计

	密钥协商前					密钥协商后	
	MN-CN1	MN-CN2	MN-CN3	不一致位平均值	平均不一致率	各组合协商成功次数	平均协商成功率
静态视距1米	5.2	3.3	4.2	4.23	4.07%	10	100%
静态非视距1米	4.7	5.4	7.4	5.83	5.61%	10	100%
静态视距3米	6.3	10.6	3.9	6.93	6.67%	10	100%
静态非视距3米	14.9	5.6	9.9	10.13	9.74%	10	100%
动态视距1米	11.8	6.2	11.8	9.93	9.55%	10	100%
动态视距3米	11.5	14.4	7.2	11.03	10.61%	10	100%

如表3-4，可看出墙体的阻隔、设备间距离的增加以及移动障碍物的出现都会加剧多径效应进而使得所获CSI幅度数据互易性下降，最终导致密钥不一致率增高。静态视距1米时MN与对应CN间密钥高度一致，KDR平均值仅为4.07%，而动态视距3米时密钥不一致情况最为严重，KDR平均值高达10.61%，但整体而言六个实验场景中密钥不

一致率均在可协商纠错范围。对上述原始密钥按协商方案进行协商，最终平均协商成功率为100%。以MN与CN2间为例，双方在经过信息协商后可获得一致密钥。

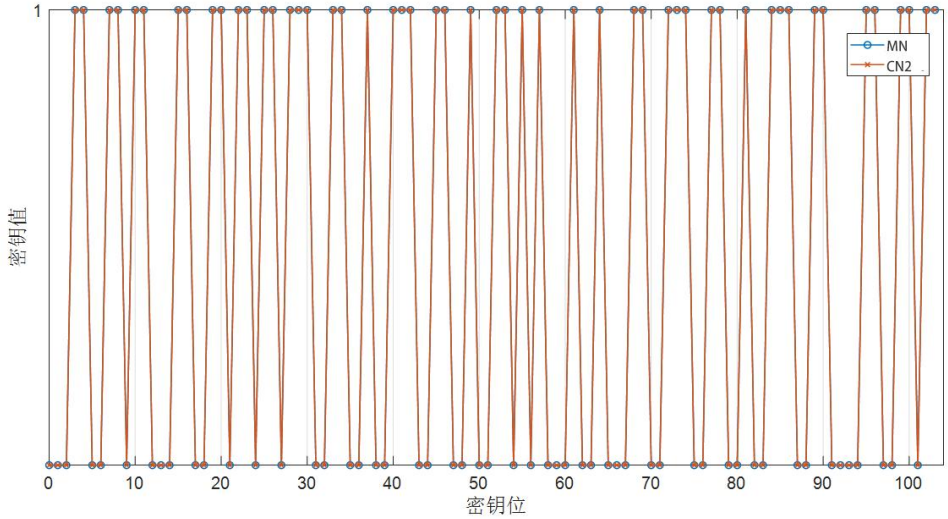


图3-16 MN-CN2视距1米初始密钥对比图

3.4.1.6 密钥随机性

对于一组MN和CN的10组初始密钥，拼接成1040位的待测序列，取前1000位进行随机性测试，考虑到NIST随机性测试对待测数据的容量要求，本实验中仅选用了6种测试项目，对视距和非视距的不同距离下的场景所得初始密钥进行了随机性检验。

结果如表3-5至表3-8所示，可以看到所生成的密钥各项测试P值均大于0.01，即均能通过随机性检验。此处需说明的是：累加和检验会将待测序列分为两个方向进行检测，即前向和反向分别输出1个P值。序列检验中我们将数据块大小设为2，目的是检验每个2bit模式出现的概率，测试程序将计算不同位数子块的频数与预期随机序列的频数的匹配程度得到两个检验统计量，再由不完全伽马函数计算最终输出两个P值。

表3-5 视距1米密钥随机性测试P值

检验方法	MN-CN1	MN-CN2	MN-CN3
频数检验	0.657969	1.000000	0.704336
块内频数检验	0.978885	0.995317	0.989730
游程检验	0.653428	0.704336	0.803775
累加和检验	0.994708 ，0.971736	0.999994 ，0.999994	0.982178 ，0.958243
近似熵检验	0.151523	0.019486	0.066901
序列检验	0.843665 ，0.704336	0.930531 ，0.704336	0.901225 ，0.800282

表3-6 非视距1米密钥随机性测试P值

检验方法	MN-CN1	MN-CN2	MN-CN3
频数检验	0.949571	0.486616	0.704336
块内频数检验	0.966434	0.98439	0.998848
游程检验	0.375850	0.987783	0.803775
累加和检验	0.999140 ，0.994708	0.79473 ，0.823133	0.958243 ，0.999140
近似熵检验	0.118111	0.035297	0.168452
序列检验	0.674354 ，0.375921	0.785056 ，1.000000	0.901225 ，0.800282

表3-7 视距3米密钥随机性测试P值

检验方法	MN-CN1	MN-CN2	MN-CN3
频数检验	0.899343	0.89934	0.087705
块内频数检验	0.993756	0.99932	0.76891
游程检验	0.999596	0.94997	0.777351
累加和检验	0.999140 ，1.000000	0.99995 ，1.000000	0.17540 ，0.133272
近似熵检验	0.142032	0.82743	0.976333
序列检验	0.992032 ，1.000000	0.98412 ，0.899343	0.230847 ，0.899343

表3-8 非视距3米密钥随机性测试P值

检验方法	MN-CN1	MN-CN2	MN-CN3
频数检验	0.527089	0.205903	0.447884
块内频数检验	0.981208	0.94265	0.988934
游程检验	0.201224	0.80977	0.436799
累加和检验	0.765607 ，0.765607	0.38938 ，0.389382	0.765607 ，0.850473
近似熵检验	0.992883	0.05823	0.750136
序列检验	0.36787 ，0.205903	0.44574 ，0.899343	0.562142 ，0.447884

3.4.1.7 安全性

对本文所提的身份认证机制的安全性分析如下：

仿冒攻击：攻击者冒充CN时，假设其拥有伪造CSI的能力，不知道MN和CN间的K_S，则攻击者只能发送一个未加密的认证请求或伪造一个密钥，MN按约定密钥解密，但对解密所得的CSI所提取的设备指纹将与指纹库中合法设备的不一致，分类结果与攻击者声明身份无法对应，MN将发现攻击者身份，攻击无效。

仿冒攻击：攻击者冒充MN时，假设其拥有伪造CSI的能力，不知道MN和CN间的K_S，则攻击者只能发送一个未加密的认证请求，MN按约定密钥解密，但攻击者伪造CSI得到的均值与合法CN本身的值无法相同，CN将发现MN身份，攻击无效。

中间人攻击：假设攻击者可伪造CN和MN的身份，拦截从CN到MN的消息，反之亦然，并试图作为中间人将它们修改。当攻击者先截获CN发给MN的消息，然后使用自己随机生成的会话密钥伪造类似的消息，但是 MN收到后将无法解密，反向同理，攻击无效。

重放攻击：假设攻击者重放来自CN发往MN的消息。每当MN认证了CN的合法性则会进入密钥协商环节并利用所得密钥更新密钥，因此下一轮认证中会使用最新的密钥，重放的消息MN无法使用最新密钥正确解密，攻击无效。

窃听攻击：假设攻击者可以窃听无线信道，获得所有传输的信息。合法CN和MN间的交互的信息均使用密钥加密，攻击者不知道密钥无法解密，攻击无效。

对本文提出的密钥协商机制，选取3个ESP32分别作为MN、CN、Eve，Eve模拟实际应用场景中的攻击者，对系统进行窃听并伪造成合法设备。MN与CN视距1米左右。在使用2.4GHz的频段时，对应半波长约为12厘米，实验中使Eve距离CN约30厘米，超过半波长。对比Eve捕获到的MAC地址为CN的CSI数据与MN、CN端的CSI数据。作CSI幅度值对比图如图3-17所示。

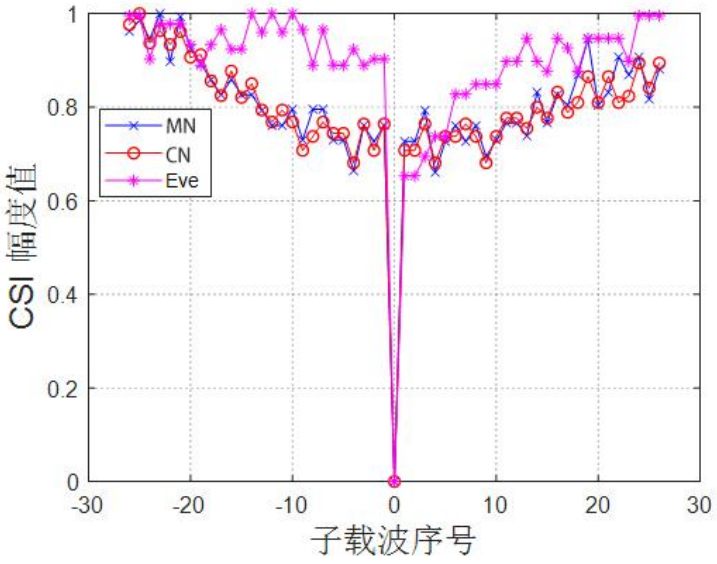


图3-17 MN-CN-Eve CSI幅度值对比图

可以看到MN和CN的数据高度相似互易性极好，而Eve监听到的包对应生成的CSI与它们差异极大。经计算，$\rho(CSI_{MN},CSI_{CN})=0.94180$，$\rho(CSI_{Eve},CSI_{CN})=0.55953$，进一步证明了合法通信双方间信道测量值高度相似，而窃听者所获数据反之。综上，若窃听者冒充MN欲和CN协商生成密钥则无法通过互易性要求，量化后所得密钥与合法双方所得密钥严重不一致，无法攻击成功。由上述测试可知，该密钥生成方案能够防范

被动窃听攻击，具有较高的安全性。

3.4.2 功能单元实现效果

系统可视化界面将主要按登录前后区分，分为登录界面和主界面。其中登录界面完成使用者基本的身份认证；主界面分为左右栏，其中左栏为各个功能单元一览。用户使用时应该完成：由登录界面进入系统，完成基本身份认证。登录成功后，进入主界面，界面中包含“设备指纹数据库”、“密钥协商”、“身份认证实时监控”、“密钥生成实时监控”等功能按钮。

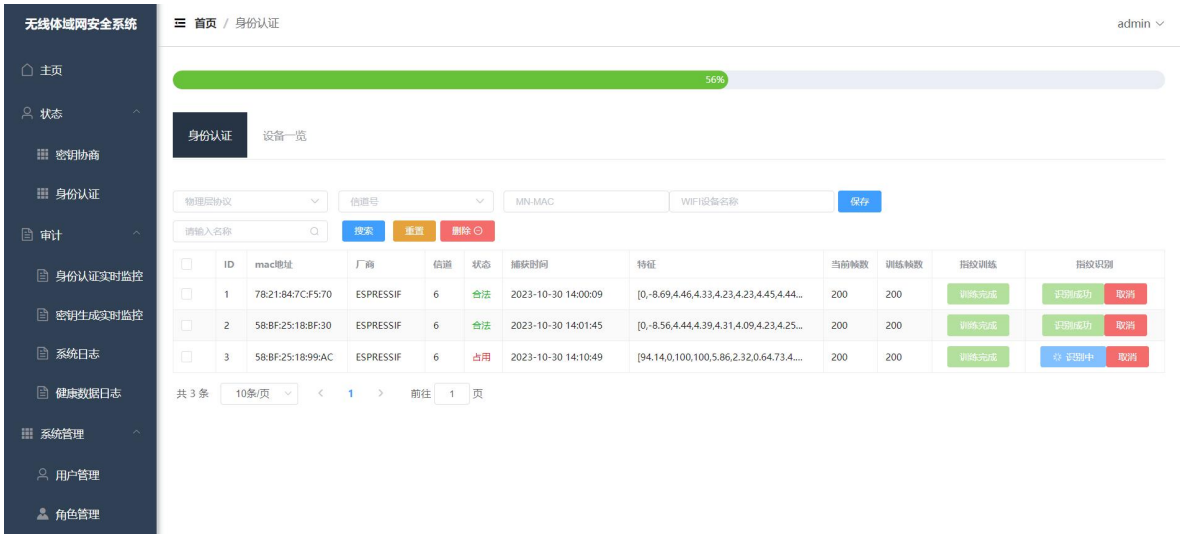


图3-18 主界面

用户点击对应位置可实现功能说明如下：

- **设备指纹数据库：**完成信息展示、合法设备登入与取消与数据库增删。具体而言，展示被系统扫描的设备信息（MAC地址、厂商）及采集状态。选择“训练”根据已提取特征做识别前的模型训练，选择“取消”进行合法设备的取消登记并在数据库中删去其对应数据，选择“识别”对重新接入MN的CN设备应用训练好的分类模型进行身份认证。其中被识别状态分为“等待”未加入白名单待识别，“合法”识别完毕判为合法设备，“非法”识别完毕判为非法设备。
- **密钥协商：**选择“密钥协商”，身份认证后调用信道探测程序，接收来自控制器节点的探测请求并发回响应；接收控制器节点发送的协商信息并完成密

钥纠错计算纠错后密钥的哈希值，完成哈希值比对，得到一致密钥。其中可以预览并导出CSI幅值图和协商一致的密钥。

- **身份认证实时监控：**展示欲识别设备信息，截止目前识别次数、合法/非法次数、合法/非法时长以及对应合法/非法比例。
- **密钥生成实时监控：**统计汇总MN和不同 CN设备协商生成密钥的次数、协商成功比例。
- **系统日志：**包含和不同CN设备进行身份认证的时间及对应状态判别为合法或非法的记录；和不同CN设备进行密钥协商的时间及密钥协商成功或失败的记录。

1. 设备指纹数据库：

① 合法设备登记和数据库增加：点击“身份认证”，可观察到信号的具体设备为哪些；点击“训练”按钮，采集及提取模块首先自动运行，页面显示当前采集数据帧数，当用于训练模型的数据量不足训练帧数要求时，显示“训练中”，达到要求时利用指纹数据集进行分类模型训练，其纳入数据库的是指纹和设备信息的组合，相当于对一个合法设备在数据库中的登记过程，并如图于可视化平台展示出。如图3-19，设备CN1、CN2是预先进行训练登记入库的合法设备，断开连接后重新接入，设备CN3是第一次接入需要进行设备登记的合法设备。

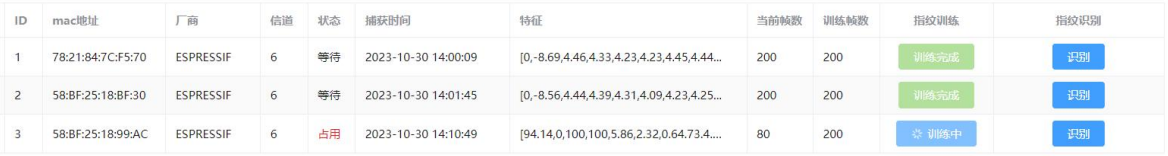


图3-19 设备登记界面

② 合法设备取消登记及数据库删除：对完成识别后确认为合法的设备可点击“取消”，可将已经在数据库中设备指纹移除，并且重新训练分类模型。

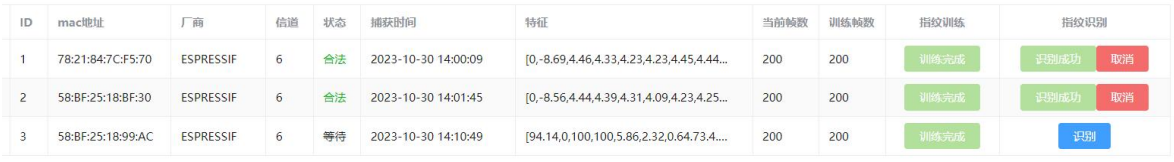


图3-20 设备取消登记界面

③ 数据库查询：对应窗口左侧列出的“状态”“MAC地址”等信息展出区域，查询设备名称、合法性信息。

ID	mac地址	厂商	信道	状态	捕获时间	特征
1	78:21:84:7C:F5:70	ESPRESSIF	6	等待	2023-10-30 14:00:09	[0,-8.69,4.46,4.33,4.23,4.23,4.45,4.44...
2	58:BF:25:18:BF:30	ESPRESSIF	6	等待	2023-10-30 14:01:45	[0,-8.56,4.44,4.39,4.31,4.09,4.23,4.25...
3	58:BF:25:18:99:AC	ESPRESSIF	6	等待	2023-10-30 14:10:49	[94.14,0,100,100,5.86,2.32,0.64.73.4....

图3-21 设备指纹库查询界面

2. **身份认证实时监控：**认证结果展示，全部设备的合法次数、非法次数、合法比例等。其中第一列合法比例指MN对CN指纹登记入库后CN再次接入时，正确识别为对应CN身份标签次数占总识别次数的多少；非法比例指合法CN被分类错误进而与其声明的身份标签不一致，被系统认为是非法设备的次数占总识别次数的多少。

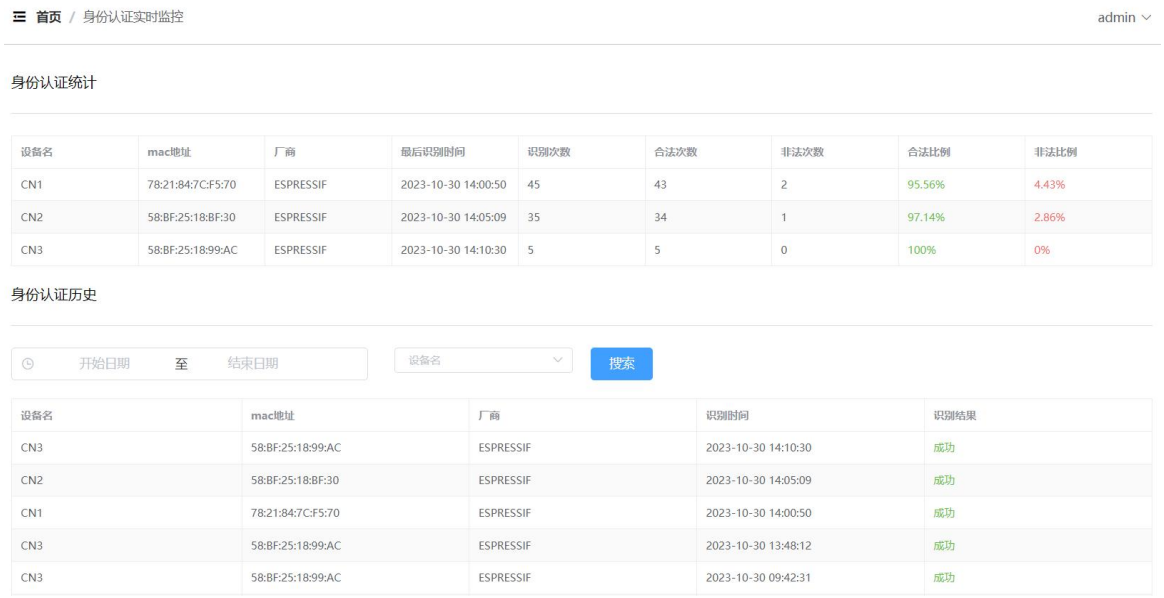


图3-22 身份认证实时监控界面

3. **密钥协商：**选择“密钥协商”，在完成身份认证后调用信道探测程序，接收来自控制器节点的探测请求并发回响应；接收控制器节点发送的协商信息并完成密钥纠错；计算纠错后密钥的哈希值，完成哈希值比对，得到一致密钥。根据进程的不同状态，在密钥协商栏显示“密钥协商”与“协商中”；状态栏显示“等待”表示未进行协商，显示“占用”表示协商中，“成功”表示密钥协商成功。

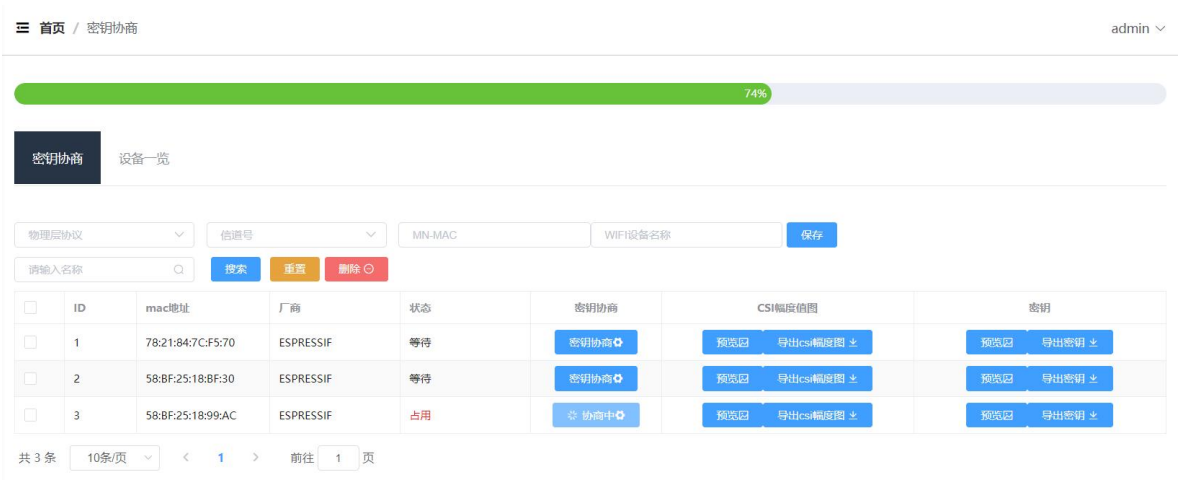


图3-23 密钥协商界面

对于协商成功后的设备，可以通过点击“预览”或“导出”查看对应的CSI幅值图和生成的一致密钥。

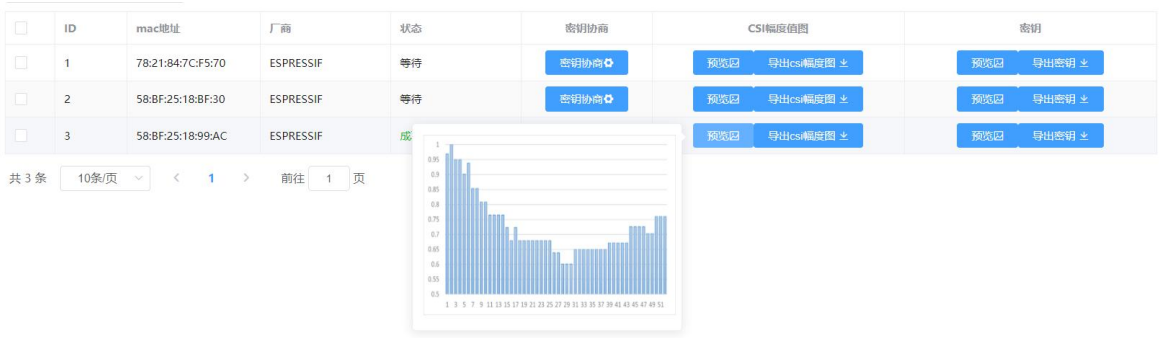


图3-24 预览CSI幅值图

图3-25 预览生成的一致密钥

4. **密钥生成实时监控：**统计汇总一段指定时间内MN和不同CN设备协商生成密钥的情况，包括最后一次协商时间、协商次数、成功次数和协商成功比例。

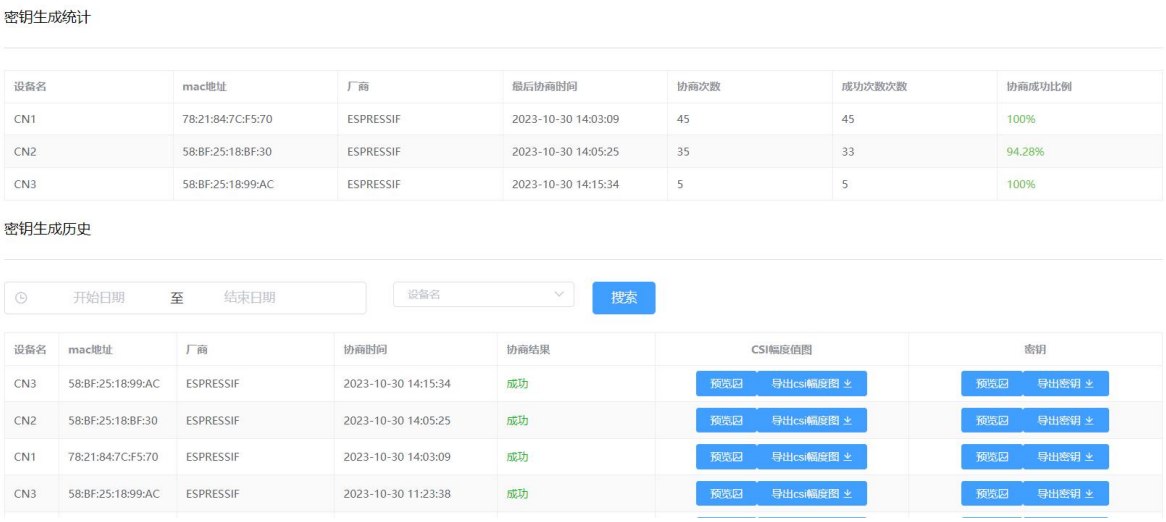


图3-26 密钥生成实时监控界面

5. **指纹匹配：**设置合法与非法设备的对照组，检验是否能匹配合法设备指纹，并对非法设备进行标记。非法设备即MAC地址与用户纳入训练并获得特征的设备相同但其特征匹配度低的设备。例如下图中被标记为非法的设备58:BF:25:18:99:AC，其MAC地址与一先前已登记指纹入库的CN相同，但其实际是我们人为改造出的非法设备冒用了该MAC地址，依据指纹匹配我们验证了其非法性。指纹匹配结束后，MN将包含CN设备指纹信息的数据加密传输给CN，CN解密与自身比对，若一致则MN身份合法，同时CN收到MN的认证通过信息将不再向MN发送用于生成指纹的探测信号。

ID	mac地址	厂商	信道	状态	捕获时间	特征
1	78:21:84:7C:F5:70	ESPRESSIF	6	合法	2023-10-30 14:00:09	[0,-8.69,4.46,4.33,4.23,4.23,4.45,4.44...
2	58:BF:25:18:BF:30	ESPRESSIF	6	合法	2023-10-30 14:01:45	[0,-8.56,4.44,4.39,4.31,4.09,4.23,4.25...
3	58:BF:25:18:99:AC	ESPRESSIF	6	非法	2023-10-30 14:19:34	[94.14,0,100,100,5.86,2.32,0.64.73.4....

图3-27 指纹匹配界面

6. **云管控：**指纹识别参数查询：查询设置身份认证使用的相关的协议、信道号、设备名称等参数。

图3-28 云管控界面

7. **日志与警报：** 记录并更新身份认证监控日志，用于数据维护。当用户具有使用

该功能的权限时，日志进行显示，供用户查看。

图3-29 身份认证监控日志查询界面

第四章 创新性说明

- **物理指纹在无线体域网身份认证领域的创新应用**

传统的无线体域网身份认证方案依赖于加密计算的复杂性或相同型号的传感器采集生理特征、或用户特定的行为模式、或体内外信道的区别。但本作品创造性利用无线设备发射的信号中包含设备本身的细微身份特征，通过对接收无线信号的分析，从设备“物理特性”中提取出数据特征作为设备指纹，将设备指纹首次用于无线体域网内Inter-WBAN层的身份认证。利用设备指纹这一物理特性的认证方案，无需复杂计算、无需特定硬件、无需用户特定行为模式。

- **利用物理指纹的唯一性和不可克隆性克服现有安全机制的缺陷**

当前主流应用的无线体域网认证机制可分为加密认证方案和非加密认证方案，但基于传统密码理论的加密认证方法计算量大不适用于资源有限的Inter-WBAN层设备，或健壮性不足不能抵御模仿攻击；基于非加密的认证方案常需要专用传感器、硬件实现较为复杂；两者共同的缺点是部分认证方案都只针对Intra-WBAN层，无法应用于Inter-WBAN层的身份认证。以无线接入设备的物理指纹特征形成的身份标识，利用了设备物理指纹的唯一性和不可克隆性，有效克服了当前认证方案对仿冒攻击防护的局限性，使得应用防护效果产生了本质的飞跃。在无线体域网数量快速增长、接入无线体域网设备爆发式增长、对无线体域网安全要求较高的场景下相比其他安全技术拥有绝对的优势。

- **解决基于无线信道特征同时实现设备认证和密钥协商的难题**

基于无线信道特征同时实现设备认证和密钥协商的难点在于设备认证基于通信信道的稳定性与快速的密钥生成基于信道衰落过程中的不稳定性是矛盾的。因此，鲜有研究能同时实现无线体域网中设备认证和密钥协商，本作品针对这一挑战提出了解决方案：从通信双方交互过程中的信道状态信息中提取设备指纹时利用信道的互易性在计算过程中去除信道不稳定性的影响；利用信道的不稳定性得到变化丰富的信道状态信息作为满足随机性要求的密钥源，基于信道互易性双方获得的密钥源同样互易实现了共享一致密钥的基础。

- **利用信道互易性实现轻量、安全的密钥共享**

无线体域网中常用的密钥协商方案是通过预先部署密钥参数来实现密钥协商，该方案资源消耗少，但不具备灵活性；使用密钥管理体系则需要一个可信任的第三方存储密钥；基于人体生理信号特征的密钥协商方案则局限于Intra-WBAN层。利用信道互易性生成密钥，克服了密钥协商共享轻量与安全的难题：双方无需预先配置或第三方参与，在互易性理想的情况下双方仅需一次协商确认密钥一致。密钥源来自于通信双方交互的信号，获取简单方便；生成密钥仅需按约定的量化算法将信道特征转化为0,1序列，操作容易；密钥生成的过程计算仅涉及一次编码与一次哈希；由于无线信道的时间变化性、空间去相关性，信道特征值具有天然的随机性和不可重复性，因而所得密钥可实现近乎“一次一密”的安全效果。

第五章 总结

当前世界老龄化加剧、医疗资源分布不均，与年龄密切相关的疾病的绝对数字持续增加，传统的人工监测模式已无法满足当今社会的健康需求，另一方面研究发现可通过长期生理观察减少慢性疾病的致死率。由传感器节点、控制器节点、移动节点、医疗服务中心等组成的无线体域网是上述问题较好的解决方案。但无线信道中传输的患者生理特征和健康数据一旦被窃听或篡改，或设备身份被冒充，不仅会泄露用户的隐私敏感信息，甚至会对用户的生命健康造成威胁。据此，本文提出了一种基于物理层安全的无线体域网安全系统。该系统具有两大技术特色：利用物理特性实现身份认证和利用信道互易性实现密钥共享。特别地，物理指纹抗伪造防篡改、不可克隆、不需要对终端改造、无需复杂计算；信道密钥无需预先配置、无需第三方参与、无需硬件修改、具有天然安全性。

基于物理层安全的无线体域网安全系统整合了数据采集、指纹提取、设备识别、密钥生成、安全服务六大模块，提供移动节点管理视角的可视化界面。在数据采集模块，捕获信道状态信息无需硬件修改、无需外设电脑、程序轻量、计算资源消耗少、成本低较好地满足了无线体域网的资源需求。在指纹提取模块创新使用双方信道状态信息提取设备指纹排除信道干扰，相较于使用瞬态信号特征提取方法减少了信道干扰，相较于稳态信号特征提取方法减少了指纹信息损失。在设备识别模块利用前馈神经网络优良的函数逼近性、更好的模式检测性能，以及易模拟复杂和非线性关系的优势搭建并训练设备识别分类模型，模型训练后的轻量版本可预配置在MN设备上。在密钥生成模块，利用信道的不稳定性得到变化丰富的信道状态信息作为满足随机性要求的密钥源，利用信道互易性解决了无线体域网中密钥分发协商需要可信第三方或预先配置的难题。在安全服务模块，提供了身份认证监控、密钥生成监控等功能方便移动节点管理员掌握无线体域网内各设备的身份认证、密钥协商情况。

整个系统由表现层、业务逻辑层和数据服务层三层架构共同组成，在此基础上根据安全需求设计了无线设备指纹库、身份认证监控、密钥协商、密钥生成监控、指纹匹配、云管控、日志与警报七个功能单元，实现了身份认证和密钥共享的目标。最后设计静态、动态、不同距离、障碍物阻隔等多个场景，检验了身份认证识别率和密钥

协商成功率、密钥随机性、密钥安全性，论证了本系统能够实现安全准确的身份认证和密钥共享。

本作品具有轻量级、安全性、灵活性三大优势，在医疗行业对无线体域网依赖增加、无线体域网内数据交互剧增、病患数据安全亟需保障的应用场景下具有极大的实用价值和商业前景。

参考文献

[1]Al-Janabi S, Al-Shourbaji I, Shojafar M, et al.Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications[J].Egyptian Informatics Journal, 2017, 18(2): 113-122.

[2]Wu X, Xu J, Huang W, et al.A new mutual authentication and key agreement protocol in wireless body area network[C]//2020 IEEE International Conference on Smart Cloud(SmartCloud).IEEE,2020.DOI:10.1109/SmartCloud49737.2020.00045.

[3]Preethichandra D M G, Piyathilaka L, Izhar U, et al.Wireless Body Area Networks and Their Applications—A Review[J].IEEE Access, 11[2023-09-01].DOI:10.1109/ACCESS.2023.3239008.

[4]李战国,祝啸.无线体域网在医疗领域的运用综述[J].中国医疗设备,2023,38(06):168-174.

[5]D.Dewkhaid and S.C.Sahana, "A Comparative Study on Performance and Security issues on authentication and key-agreement schemes for Internet of Things (IoT) based wireless body area network," 2023 4th International Conference on Computing and Communication Systems (I3CS), Shillong, India, 2023, pp.1-6, doi: 10.1109/I3CS58314.2023.10127345.

[6]Huang Y,Wang W,Wang H, et al.Authenticating On-Body IoT Devices: An Adversarial Learning Approach[J].IEEE Transactions on Wireless Communications,2020,PP(99).

[7]Rottenberg F, Nguyen T H, Dricot J M, et al.CSI-based versus RSS-based Secret-Key Generation under Correlated Eavesdropping[J].2020.

[8]Li X, Ibrahim M H, Kumari S, et al.Anonymous Mutual Authentication and Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks [J].Computer Networks, 2017:S1389128617301044.DOI:10.1016/j.comnet.2017.03.013.

[9]Pandi,Vijayakumar,Mohammad,et al.Efficient and Secure Anonymous Authentication With Location Privacy for IoT-Based WBANs[J].IEEE Transactions on Industrial Informatics，2019，16(4):2603-2611.DOI:10.1109/TII.2019.2925071.

[10]Liu J，Zhang Z，Chen X，et al.Certificateless remote anonymous authentication schemes for wirelessbody area networks[J].IEEE Transactions on parallel and distributed systems，2013，25(2)：332- 342.

[11]Zhao Z.An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem[J].Journal of medical systems，2014，38(2)：13.

[12]He D，Zeadally S，Kumar N，et al.H.Anonymous authentication for wireless body area networks with provable security IEEE Systems Journal[J].2016.

[13]Arfaoui A，Kribeche A，Senouci S M .Context-Aware Anonymous Authentication Protocols in the Internet of Things Dedicated to e-Health Applications[J].Computer Networks，2019，159(AUG.4):23-36.DOI:10.1016/j.comnet.2019.04.031.

[14]Umar M，Wu Z，Liao X .Channel characteristics aware zero knowledge proof based authentication scheme in body area networks[J].Ad Hoc Networks，2021，112(9):102374.DOI:10.1016/j.adhoc.2020.102374.

[15]Biometric Authentication Using Noisy Electrocardiograms Acquired by Mobile Sensors Choi H.-S.， Lee B.， Yoon S.(2016) IEEE Access，4， art.no.7444130， pp.1266-1273.

[16]Peris-Lopez P，Lorena González-Manzano，Camara C，et al.Effect of attacker characterization in ECG-based continuous authentication mechanisms for Internet of Things[J].Future generations computer systems：FGCS，2018.

[17]Choi G H，Jung J H，Moon H M，et al.User Authentication System Based on Baseline-corrected ECG for Biometrics[J].Intelligent automation and soft computing，2019，25(1):193-204.DOI:10.31209/2018.100000055.

[18]Revadigar G, Javali C, Xu W, et al.Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables[J]. IEEE Transactions on Information Forensics & Security, 2017:2467-2482.DOI: 10.1109/TIFS.2017.2708690.

[19]Sun Y, Lo B .An Artificial Neural Network Framework for Gait Based Biometrics[J].IEEE Journal of Biomedical and Health Informatics,2018,PP(99): 1-1.DOI:10.1109/jbhi.2018.2860780.

[20]Zhao N, Zhang Z, Rehman M U, et al.Authentication in Millimeter-Wave Body-Centric Networks Through Wireless Channel Characterization[J].IEEE Transactions on Antennas & Propagation, 2017, PP(99):1-1.DOI:10.1109/TAP.2017.2681462.

[21]Huang Y,Wang W,Wang H, et al.Authenticating On-Body IoT Devices：An Adversarial Learning Approach[J].IEEE Transactions on Wireless Communications,2020,PP(99).

[22]DIFFLE W, H-ELLMAN M.New directions in cryptography[J].IEEETransactions on Information Theory,1976, 22(6):644-654.

[23]BLASS, E,ZITTERBART M.Efficient implementation ofelliptic curve cryptography for wireless sensor networks[R].Technical report.Universitat Karlsruhe, 2005：1-16.

[24]CHERUKURI S, VENKATASUBRAMANIAN K K, GUPTA SK S.Biosec：a biometric based approach for securing commu-nication in wireless networks of biosensors implanted in thehuman body[C].11 Proceedings of Parallel Processing work-shops.Piscataway：IEEE Press,2003:432-439.

[25]POON CC Y,ZHANG Y T,BAO S D.A novel biometricsmethod to secure wireless body area sensor networks for tele-medicine and m-health[J].IEEE Communications Magazine,2006,44(4):73-81.

[26]VENKATASUBRAMANIAN K K,BANERJEE A,GUPTA SK S.EKG-based key agreement in Body Sensor Net-works[C/Proceedings of IEEE INFOCOM Workshops 2008.Piscataway：IEEE Press, 2008:1-6.

[27]OVILLA-MARTINEZB，DiAZ-PEREZ.A，GARZA-SALDANAJJ.Key establishment protocol for a patient monitoring systembased on PUF and PKG[C]V/Proceedings of 2013 10th Interna-tional Conference and Expo on Emerging Technologies for aSmarter World(CEWIT).Piscataway:IEEE Press,2013：1-6.
[28]VENKATASUBRAMANIAN K K，BANERJEE A，GUPTA sK S.PSKA：usable and secure key agreement scheme for bodyarea networks[J].IEEE Transactions on Information Technolo-gy in Biomedicine，2010,14(1):60-68.
[29]WU Y,Sun Y M，ZHAN L，et al.Low mismatch key generationbased on wavelet-transform trend and fuzzy vault in body areanetwork[EBJ.2013.
[30]Zhang Z , Wang H , Vasilakos A V ,et al.Channel Information based Cryptography and Authentication in Wireless Body Area Networks[C]//Proceedings of the 8th International Conference on Body Area Networks.2013.DOI:10.4108/icst.bodynets.2013.253689.
[31]Revadigar, Girish, et al."Mobility Independent Secret Key Generation for Wearable Health-care Devices.”Proc.BodyNets (2015).
[32]Javali, Chitra, et al."SeAK：secure authentication and key generation protocol based on dual antennas for wireless body area networks."Radio Frequency ldentification：Security and PrivacyIssues.Springer International Publishing, 2014.74-89.
[33]Lai, Lifeng,Yingbin Liang,and Wenliang Du."Cooperative key generation in wireless networks.”Selected Areas in Communications,IEEEJournal on 30.8 (2012):1578-1588.
[34]JAKES W C，COX D C.Microwave Mobile Communications[M].Wiley-IEEE Press，1994.https://dl.acm.org/doi/book/10.5555/561302.
[35]Zenger C， Vogt H， Zimmer J，et al.The Passive Eavesdropper Affects my Channel：Secret-Key Rates under Real-World Conditions (Extended Version)[J].IEEE，2017.
[36]郭登科,熊俊,高玉威,等.基于无线信道状态信息的密钥提取方案设计与实现[J].信号处理.

[37]Halperirr D， Hu W， Sheth A，et al.Tool release：gathering 802.11n traces with channel state information[J].Acm Sigcomm Computer Communication Review，2011，41(1):53-53.
[38]Xie Y， Li Z， Li M .Precise Power Delay Profiling with Commodity Wi-Fi[J].IEEE Transactions on Mobile Computing，2015.
[39]Schulz M，D Wegemer，Hollick M .The Nexmon Firmware Analysis and Modification Framework：Empowering Researchers to Enhance Wi-Fi Devices[J].Computer Communications，2018，129(SEP.):269-285.
[40]Hernandez S M， Bulut E .Lightweight and Standalone IoT Based Wi-Fi Sensing for Active Repositioning and Mobility[C]// 2020 IEEE 21st International Symposium on "A World of Wireless，Mobile and Multimedia Networks" (WoWMoM).IEEE，2020.