分类号:　　密　　级：公开

学　号：20232008008　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于 PUF 的物联网中轻量级身份认证协议研究

学 位 申 请 人	**宋家全**
指 导 教 师	**王晓芳 副教授**
申 请 学 位 类 别	**工学硕士**
专 业 名 称	**网络空间安全**
研 究 领 域	**密码学及应用**
所 在 学 院	**信息科学与技术学院**

中国·新疆·石河子

2026 年 5 月

分类号:　　密　　级：公开

学　号：20232008008　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于 PUF 的物联网中轻量级身份认证协议研究

学 位 申 请 人	**宋家全**
指 导 教 师	**王晓芳 副教授**
申 请 学 位 类 别	**工学硕士**
专 业 名 称	**网络空间安全**
研 究 领 域	**密码学及应用**
所 在 学 院	**信息科学与技术学院**

中国·新疆·石河子

2026 年 5 月

A Research of Lightweight PUF-Enabled Authentication Protocols in IoT Networks

A Dissertation Submitted to

Shihezi University

In Partial Fulfillment of the Requirements

for the Degree of

Master of Engineering

By

Song Jiaquan

(Cyberspace Security)

Dissertation Supervisor: Prof. Wang Xiao-fang

May,2026

石河子大学学位论文独创性声明及使用授权声明

学位论文独创性声明

本人所呈交的学位论文是在我导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示谢意。

研究生签名：宋家全　　时间：　2026 年　05 月　20 日

使用授权声明

本人完全了解石河子大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或指定机构送交论文的电子版和纸质版。有权将学位论文在学校图书馆保存并允许被查阅。有权自行或许可他人将学位论文编入有关数据库提供检索服务。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

研究生签名：宋家全　　时间：　2026 年　05 月 20 日

导师签名：王晓芳　　时间：　2026 年　05 月 20 日

摘要

物联网的飞速发展推动智能化社会逐步成为现实，而海量智能设备在通信过程中面临着严峻的攻击与隐私泄漏风险。针对设备资源受限、现有协议效率低下且易受物理攻击的痛点，基于物理不可克隆函数（PUF, Physical Unclonable Function）的不可克隆特性成为破题关键。本文面向物联网三类典型场景，创新设计了三种高效的安全认证协议，在保障高安全性与强隐私性的同时，显著提升了协议运行效率。主要研究成果如下：

（1）针对无线体域网（WBAN, Wireless Body Area Network）节点资源受限、易受拒绝服务、中间人攻击及跟踪篡改等威胁的问题，提出一种高效的轻量级哈希与 PUF 混合认证协议。该协议利用 PUF 衍生响应的哈希值构建会话密钥，为合法用户建立安全通道，杜绝未授权访问；通过精简哈希运算频次与引入三方独立 PUF 机制，显著降低节点计算负担并增强传输安全性。特别地，密码更新阶段仅需用户参与，大幅简化操作流程。安全性分析与实验表明，该协议可抵御各类常见攻击，且在性能上优势显著：计算开销较传统方案降至 4.99 ms，通信开销缩降至 1856 Bytes，完美契合 WBAN 对低功耗、高安全的严苛需求。

（2）针对车载自组织网络（VANET, Vehicular Ad-hoc Network）开放环境中漏洞频发、节点资源受限及易泄露 PUF 挑战响应对（CRP, Challenge-Response Pair）、缺乏动态更新的痛点，提出一种去中心化动态 PUF 匿名身份验证协议。该协议融合椭圆曲线密码（ECC, Elliptic Curve Cryptography）与高可靠稳态逻辑（SDL, Stable Logic Delay）PUF，设计动态 CRP 混淆机制，将建模攻击预测成功率压制至 50%左右，通过匿名标识符与临时会话密钥实现身份不可追踪与会话独立性。经 ROR 模型与 AVISPA 工具验证，协议可抵御冒充、重放、中间人等典型攻击。SUMO 与 OMNeT++联合仿真表明，协议在 500 节点高密度场景下仍保持高效，单实体计算开销仅较同类最优方案降低 23.85%，通信开销较传统方案缩减 72.57%，端到端延迟控制在 25 ms 内，完美适配资源受限的实时车联网环境。

（3）针对无人机（UAV, Unmanned Aerial Vehicle）集群高动态拓扑、链路不稳定及节点资源严格受限的挑战，提出一种融合 SDL PUF 与后量子密码 Kyber 的算法，实现了高效密钥更新与抗量子攻击的安全通信，大幅降低节点计算与存储负荷。安全性分析表明，协议可抵御节点捕获、重放、仿冒、中间人等典型攻击，且满足前向/后向安全性。其仿真实验表明，在 100 架无人机的高密度动态拓扑下，协议计算开销仅 3200 ms，通信消耗低至 904 Bytes，端到端时延控制在 50 ms 以内，带宽占用率较同类方案降低超 60%，完美适配大规模高机动协同任务的严苛需求。

上述研究为 WBAN、VANET 及 UAV 等物联网关键场景提供了安全高效的解决方案，提升了物联网环境的安全性与健壮性，为物联网的部署奠定了基础，进一步推动了智能化社会的可持续发展。

关键词：物联网；双向认证；PUF；匿名身份；轻量级

Abstract

The rapid development of the Internet of Things (IoT) is gradually making the vision of an intelligent society a reality. However, the massive number of smart devices face severe risks of attacks and privacy leakage during communication. Addressing the pain points of resource-constrained devices, inefficient existing protocols, and vulnerability to physical attacks, the unclonable nature of Physical Unclonable Functions (PUFs) has emerged as a key solution. This paper focuses on three typical IoT scenarios and innovatively designs three efficient security authentication protocols, significantly improving protocol operational efficiency while ensuring high security and strong privacy. The main research achievements are as follows:

(1) To address the issues of resource constraints in Wireless Body Area Network (WBAN) nodes and their vulnerability to threats such as denial-of-service, man-in-the-middle attacks, and tracking/tampering, an efficient lightweight hybrid authentication protocol combining hash functions and PUFs is proposed. The protocol utilizes the hash value derived from PUF responses to construct session keys, establishing secure channels for legitimate users and preventing unauthorized access. By streamlining the frequency of hash operations and introducing a tripartite independent PUF mechanism, the protocol significantly reduces node computational burden and enhances transmission security. Notably, the password update phase only requires user participation, greatly simplifying the operational process. Security analysis and experiments demonstrate that the protocol can resist various common attacks and exhibits significant performance advantages: computational overhead is reduced to 4.99 ms compared to traditional schemes, and communication overhead is decreased to 1856 bytes, perfectly meeting the stringent low-power and high-security requirements of WBANs.

(2) To tackle the frequent vulnerabilities in open environments of Vehicular Ad-hoc Networks (VANETs), resource-constrained nodes, susceptibility to PUF Challenge-Response Pair (CRP) leakage, and lack of dynamic updates, a decentralized dynamic PUF anonymous authentication protocol is proposed. The protocol integrates Elliptic Curve Cryptography (ECC) with highly reliable Stable Logic Delay (SDL) PUF and designs a dynamic CRP obfuscation mechanism, suppressing the prediction success rate of modeling attacks to around 50%. Anonymous identifiers and temporary session keys are employed to achieve identity untraceability and session independence. Verified by the Real-or-Random (ROR) model and AVISPA tool, the protocol can resist typical attacks such as impersonation, replay, and man-in-the-middle attacks. SUMO and OMNeT++ co-simulation results show that the protocol remains efficient even in high-density scenarios with 500 nodes: the computational overhead per entity is reduced by 23.85% compared to the optimal existing

scheme, communication overhead is reduced by 72.57% compared to traditional schemes, and end-to-end delay is controlled within 25 ms, perfectly adapting to resource-constrained real-time vehicular network environments.

(3) To address the challenges of highly dynamic topology, unstable links, and strictly constrained node resources in Unmanned Aerial Vehicle (UAV) swarms, an algorithm fusing SDL PUF with the post-quantum cryptography Kyber is proposed. It achieves efficient key updates and quantum-resistant secure communication, significantly reducing node computational and storage loads. Security analysis indicates that the protocol can withstand typical attacks like node capture, replay, impersonation, and man-in-the-middle attacks, while satisfying forward and backward secrecy. Simulation experiments demonstrate that under the high-density dynamic topology of 100 UAVs, the protocol's computational overhead is only 3200 ms, communication consumption is as low as 904 bytes, end-to-end latency is controlled within 50 ms, and bandwidth occupancy is reduced by over 60% compared to similar schemes, perfectly suiting the rigorous demands of large-scale high-mobility cooperative missions.

The aforementioned research provides secure and efficient solutions for key IoT scenarios such as WBAN, VANET, and UAV, enhancing the security and robustness of the IoT environment, laying a foundation for IoT deployment, and further promoting the sustainable development of an intelligent society.

Key words: Internet of Things; Mutual Authentication; PUF; Anonymous Identity; Lightweight

目　录

第1章 绪论

1.1 研究背景及意义

物联网（Internet of Things，IoT）是指由实体设备、车辆、电器和其他实体对象组成的网络，这些实体对象内嵌传感器、软件和网络连接，可以收集和共享数据[1]。物联网设备范围广泛，包括简单的“智能无人机”设备、智能医疗芯片和支持车载单元（On Board Unit，OBU）等设备，以及更复杂的工业机械和运输[2]。技术专家甚至在设想以物联网技术为基础的整个智能城市环境。物联网使这些智能设备能够相互通信以及与其他支持互联网的设备通信。就像智能手机和网关一样，创建一个庞大的互联设备网络，可以交换数据并自主执行各种任务。而物联网的发展始于思想启蒙，1991 年马克·韦泽提出了一个泛在计算的理念，为其奠定了早期基础。而后 1999 年，麻省理工学院 Auto-ID 中心明确提出了基于射频识别技术的物联网构想，这被视为现代的物联网概念的正式起点。随后，产业影响力迅速扩大：2005 年，国际电信联盟（International Telecommunication Union，ITU）发布《ITU 互联网报告 2005：物联网》，标志着这一概念被正式推向全球舞台[3]；2008 年，IBM 又提出了一个智慧地球的战略，次年，我国政府提出了感知中国的概念，并建立无锡国家传感网络创新示范区，物联网由此上升为国家战略，进入规模化部署阶段。2025 年以来，在 5G、人工智能和边缘计算等技术的融合驱动下，物联网正从万物互联走向万物智联，开启智能协同的新阶段[4]。针对 IoT 体系架构，本研究聚焦于无线体域网、车联网与无人机网络三个具有代表性且应用前景广阔的物联网子领域，分别体现了 IoT 在个人健康监护、智能交通管理与广域空间作业等维度的深度落地。为系统呈现其技术构成与运行逻辑，本文构建如图 1-1 所示的物联网典型应用场景图，该图采用设备与感知层、传输与网络层、应用与服务层三层架构，横向对比三类场景的终端节点、通信协议与数据流向，纵向揭示其从物理感知到云端智能处理的完整链路。对于无线体域网部分采用可穿戴设备与植入式传感器为核心的生理数据采集 IoT 设备，通过 Zigbee/BLE 等短距离通信技术汇聚至医疗网关或智能手机，并进一步上传至云端，支撑远程健康监测、远程医疗等服务。而对于车联网部分基于 C-V2X、DSRC 等协议的车路协同架构，涵盖车载单元 OBU、路侧单元（Road Side Unit，RSU）等关键 IoT 设备，通过网络层与核心网、边缘计算平台互联，实现自动驾驶、智能交通调度等功能。最后，对于无人机网络部分则采用多机协同通信与地面控制站等 IoT 设备联动的架构，结合卫星链路与 5G/6G 通信，实现空中监视、精准农业、灾害救援等高动态场景。

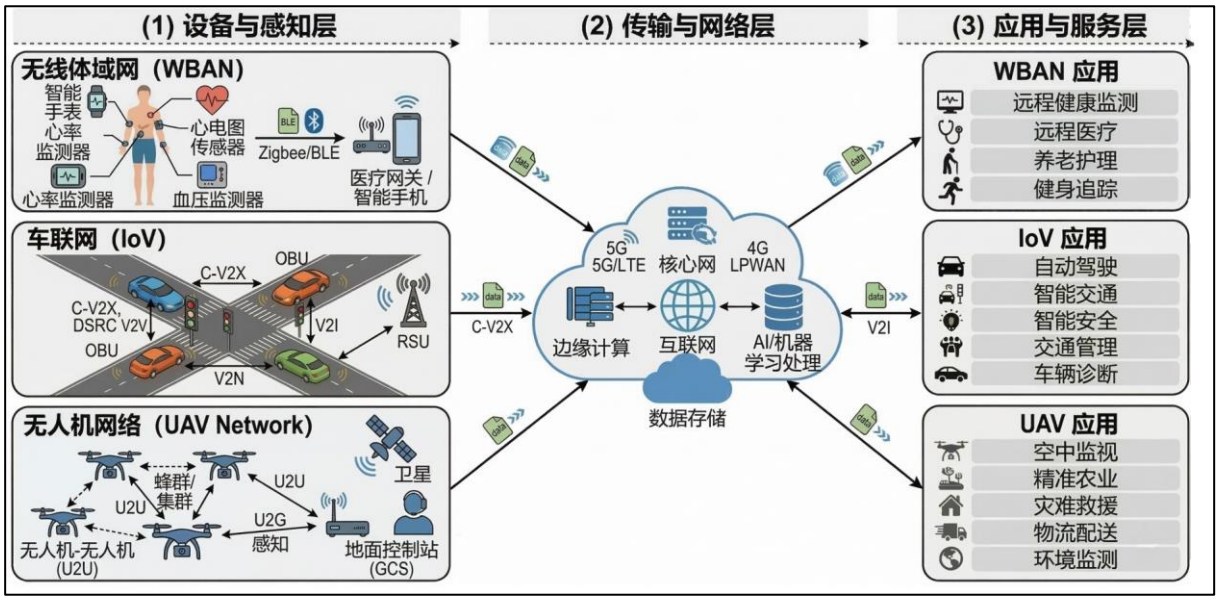

图 1-1 物联网典型应用场景图

Figure 1-1 Typical IoT Application Scenarios

然而随着 IoT 设备日益普及，虽然生活与工作变得越来越方便与快捷，但是安全和隐私却变得越来越重要。许多 IoT 设备很容易受到黑客和其他网络威胁的攻击，这可能会危及敏感数据的安全和隐私。IoT 设备还可以收集大量个人数据，引发了人们对隐私和数据保护的担忧。来自不同制造商的 IoT 设备通常使用不同的标准和协议，因此难以进行所谓的“机器对机器”通信。这可能会导致非法身份问题，并造成重要数据泄密。例如，在医疗保健领域，IoT 设备被攻击者操控会泄露病人生命体征数据，而对于智能汽车的非法身份参与会导致车载单元功能失效引发交通事故，而对于无人机网络目标篡改更会导致引发严重军事威胁等等。因此对于物联网系统而言，保证其安全与隐私尤其重要。在物联网系统中，数据完整性，数据可靠性，数据保密性与部分要求实时性是最基本的安全需求[4]，而像无线体域网络、车联网、无人机网络等 IoT 设备的计算与存储能力都比较低，难以搭载复杂的加密算法，而先进的人工智能和机器学习、区块链虽然最大限度地减少了数据安全泄漏问题，但并不适用于上述对实时性具有极高要求的物联网系统，目前学术界提出了大量认证协议，但这些协议存在安全性能较差、执行效率低下、无法满足多项安全需求，最近却又无法满足高安全性与实时性的平衡，因此，设计一个轻量级的针对物联网的安全认证协议迫在眉睫。

随着物理不可克隆函数（Physical Unclonable Function，PUF）的诞生，其作为一种硬件安全原语，它可以内置于无线体域网络、车联网、无人机网络等物理实体中，并基于其固有的制造随机性来工作。在制造过程中，芯片会因细微工艺差异为每个 PUF 生成独一无二的数字指纹。该技术具有稳定性、高随机性和抗物理攻击的特性，而探索如何以极低的硬件成本，显著增强整个系统的安全等级，正是 PUF 技术致力解决的主要问

题。因此在无线体域网络、车联网、无人机网络等典型网络的 IoT 设备中实现安全性与时效性的平衡，PUF 成为一个极好的解决办法。下面是其典型应用场景的国内外研究现状。

1.2 国内外研究现状

目前，学术界与互联网企业对物联网安全身份认证方面进行了积极探索。基本的轻量级通信协议是为了保证通信双方以共同的规则进行快速的数据交换与共享，而基于 PUF 的轻量级安全认证协议则是在此基础上，使用经过验证与实验的 PUF 设备，采用哈希函数、对称加密[5]、椭圆曲线密码学（Elliptic Curve Cryptography，ECC）[6]以及预着色密钥等，使数据交换在通过身份认证的实体之间进行，保证数据的完整性与可靠性，安全性与时效性的平衡。由于物联网的特点是能够在最小的人力干预下生成、交换和加密数据，其潜在应用广泛多样，涵盖多个领域。这些领域包括医疗保健、智能家居环境、军事无人机和智能车联网企业等。而其场景的系统结构不尽相同，相应地基于 PUF 的认证协议也有较大的区别，且 PUF 本身芯片的侧重也有差距。因此，针对不同系统的特点，为各种计算性能不同、存储性能不同、PUF 硬件设备侧重改进不同、适用场景不同的物联网系统设计相应的高安全性与时效性平衡的认证协议具有十分重要的现实意义。本节从与本文研究内容相关领域出发，分类对具体的国内外研究现状进行总结阐述。

1.2.1 无线体域网络系统安全认证协议相关研究

随着无线体域网络（Wireless Body Area Network，WBAN）在医疗健康等领域的广泛应用，其安全认证协议的研究备受关注。目前，针对资源受限的 WBAN 环境，研究者们提出了多种认证协议，主要可分为基于密码学、混合生物特征以及硬件安全原语等类型。2016 年，Mohammad Sabzinejad Farash 等人[7]提出了一种适用于物联网环境异质无线传感器网络的高效用户认证与密钥协商方案，但 Amin 等人[8]随后发现该协议存在身份欺骗和离线凭证破解等弱点。同年，Ruhul Amin 等人[8]设计了一种保护匿名的三因素认证密钥交换协议，以增强隐私性。2019 年，Mohammad Wazid 等人[9]提出了一种面向物联网边缘部署的轻量级设备认证与密钥管理机制，利用哈希函数和异或操作来保障流程安全。2020 年，Mahdi Fotouhi 等人[10]为医疗物联网设计了一个轻量级的安全因素认证方案，其安全性基于哈希序列，但可能面临拥有特殊访问权限的内部人员攻击风险。2021 年，Chunhua Jin 等人[11]提出了一种高效的生物特征身份基访问控制方案，采用混合加密技术，但需要相应生物特征采集设备的支持。2022 年，Jian Shen 等人[12]提出了一个适用于 WBAN 的轻量级、无证书的多接收者安全数据传输协议，其安全性基于椭

圆曲线离散对数问题，但较高的计算复杂度可能导致密钥泄漏。同年，Priyanka Mall 等人[13]对基于 PUF 的认证与密钥协商协议进行了全面综述。2023 年，Vikash Kumar Rai 等人[14]提出了一种轻量级的基于PUF的物联网设备认证机制，以提升实时性与轻量化；Daojing He 等人[15]设计了一个具备匿名性的轻量级物联网认证与密钥交换协议；而 Saeed Ullah Jan 等人[16]则探索了一种面向医疗设备的、高效的带宽与功率敏感的轻量级认证方案，但其中广泛的哈希函数运算可能不够轻量。此外，Amir Masoud Aminian Modarres 等人[17]系统分析了现有基于PUF的认证协议存在的漏洞，并提出了强化策略。

综上所述，WBAN 所使用的认证算法要不实现较复杂，成本较高，要不就是功耗较大。因此，缺乏一个所有实体全部采用 PUF 设备的 WBAN 身份认证协议，去满足常见的攻击，同时降低存储和计算消耗，同时可以实现离线更新，不需要第三方的参与。

1.2.2 基于车联网系统安全认证协议研究现状

随着智能交通系统的快速发展，车联网（Vehicular Ad Hoc Network，VANET）的安全认证与密钥协商协议研究备受关注。目前，针对车联网开放的无线环境、资源受限设备及高隐私要求的特点，研究者们提出了多种认证协议，其演进脉络从早期的公钥基础设施方案，逐步发展到融合硬件安全原语与轻量级密码学的混合方案。2007 年，Raya 和 Hubaux[18]提出了一种基于公钥基础设施（Public key Infrastructure，PKI）的聚合签名方案，以增强隐私保护，奠定了车联网安全的基础，但存在计算开销和证书管理复杂的问题。2008 年，Lu 等人[19]设计了一种匿名 PKI 身份保护方案。随着硬件安全原语的发展，Guajardo 等人[20]率先在基于现场可编程门阵列（Field Programmable Gate Array，FPGA）的环境中使用 SRAM PUF 进行隐私保护。2010 年，Sadeghi 等人[21]应用双线性配对技术保护 PUF 的挑战－响应对（Challenge Response Pair，CRP），对机器学习攻击有较强抵抗力，但计算成本较高。2015 年，He 等人[22]优化了基于 ECC 的车联网认证协议的批量验证延迟问题。2019 年，Gope 等人[23]提出了一种方案以避免显式存储 CRP，但仍面临内部威胁的风险。

近年来，研究趋势转向去中心化与混合方法。2022 年，Sutrala 等人[24]将生物特征融入双向认证协议，但因中心化设计导致效率不足。同年，Chen 等人[25]采用 ECC 加密的 CRP 来提升安全性，但增加了延迟且未解决参数更新问题。2023 年，Liang 等人[26]提出了一种无需可信机构（Trust Anchor，TA）的 PUF-ECC 密钥协商协议，但固定伪标识符存在位置可追踪风险。Xie 等人[27]则结合 PUF 与生物特征密钥，用于批量的车与基础设施/车与车（Vehicle To Vehicle/Infrastructure，V2I/V2V）认证。2024 年，Chaudhry 等人[28]开发了一种轻量级的基于 ECC 的协议，能防御常见攻击，但忽略了参数更新机制。最新的研究如 Men 等人[29]，2025 年引入了实时 CRP 生成以增强隐私，但可信机构 TA

的参与和参数更新的缺失影响了可扩展性。Li 等人[30]在车辆和路侧单元 RSU 中部署 PUF 以消除长期密钥存储，但仍面临机器学习（Machine Learning，ML）与深度学习（Deep Learning，DL）建模攻击的威胁。由此可见，现有的采用 PUF 设计的车联网身份认证协议无法有效抵御建模攻击，且常常忽略参数更新问题，且普遍使用的 PUF 的可靠性较低，需要纠错编码的参与，因此为本文研究提供了思路。

1.2.3 基于PUF的无人机群认证协议相关研究

基于 PUF 的无人机身份认证协议研究已持续多年，早期方案主要尝试将 PUF 作为硬件信任根来增强设备唯一性与防篡改能力。2019 年，Srinivas 等人[31]设计了一种面向无人机物联网环境的轻量认证协议，该协议采用 ECC 与生物特征，但仍需地面站存储全部无人机信息，无法抵抗物理捕获攻击，且缺乏完美前向保密性。紧随其后，2020 年，Alladi 等人[32]提出了支持无人机-无人机及无人机-地面站通信的新型认证协议，首次引入 PUF 机制，但由于 PUF 使用方式不当，导致信息传递错误，且未实现身份匿名与不可链接性，隐私泄漏风险突出。同年，Ali 等人[33]提出的生物特征认证方案虽然提升了用户身份验证强度，但无人机本身仍易受捕获与伪装攻击，且存在验证表窃取隐患。而随着无人机应用场景向动态化、群组化发展，认证协议需兼顾前向安全与高效密钥协商。2021 年，Bansal 等人[34]针对动态无人机群提出了可扩展的相互认证协议，但仍未保障完美前向保密性。Wu 等人[35]利用生物特征加密个人信息，却未解决无人机自身的物理脆弱性。这些方案普遍暴露出一个共性局限：依赖地面站集中存储验证信息，一旦节点被俘获，将引发系统性隐私泄漏。为此，部分研究开始探索 PUF 与轻量密码机制的深度融合。2022 年，Li 等人[36]设计了面向无人机网络的能效安全通信方案，采用 ECC 与双线性配对，虽实现跨域认证，但计算开销显著，且仍无法抵御物理捕获。Yu 等人[37]基于 PUF 的轻量认证协议聚焦于用户信息保护，却忽略了无人机本体的安全防护。2023 年，Zhang 等人[38]的 ECC 认证协议提升了运行效率，但同样未对抗物理入侵威胁。

近年来，研究者进一步将 PUF 嵌入跨域认证架构，以应对无人机多域漫游需求。Tian 等人[39]提出了面向多域环境的可靠 PUF 互认证协议，但每个地面站仍需维护全体无人机信息库，存在验证表泄漏风险。2024 年，Chandran 等人[40]设计了多无人机网络中基于 PUF 的轻量互认证协议，采用哈希与异或操作，但仍局限于单域场景。与此同时，区块链技术被引入以增强分布式信任，如 Akram 等人[41]基于区块链的隐私保护认证协议，可保障无人机在固定地面站的安全认证，但未充分考虑物理攻击威胁；Karmakar 等人[42]的区块链分布式智能集群认证协议亦仅适用于单域环境，难以满足多域协同需求。

在后量子时代，PUF 与后量子密码的结合又成为新兴的研究方向。而 Xu 等人[43]揭示了电磁选择密文攻击对 Kyber 的威胁；之后，2023 年，Jati 等人[44]提出可配置抗侧信

道 Kyber 实现虽提升安全性，但带来约 5%的额外开销；而后，2024 年以后，Nair 等人[45]开创性提出传统 PUF-Kyber 架构，但未考虑传统 PUF 在各种噪声条件下的可靠性，Zhang 等人[46]提出了一种高可靠性 SDL PUF，无需额外纠错码即可在假定环境下实现接近 100%可靠性，且 PUF-Kyber 构架的提出为 SDL PUF 与其结合，为本文提供了依据。而后，2025 年，梁飞燕等人[47]以及王雄等人[48]提出了更加轻量化的协议设计方案。2026 年，李志强等人[49]进一步优化协议将其做到了更加简洁低交互。

1.3 研究内容及创新点

本文的主要研究框架如图 1-2 所示，主要面向基于 PUF 的 IoT 中轻量级身份认证协议研究的典型应用领域，包括基于 WBAN 和 VANET 的认证协议改进、基于无人机身份认证协议认证方案，在充分调研国内外相关典型场景研究现状后，创新性地引入 SDL PUF、PUF-kyber、建模攻击以及传统加密算法等技术，重点解决 WBAN 的设备存储量小、车联网环境高速移动所带来的实时性以及无人机网络拓扑不断变化的高扩展性，以及 PUF 本身所有的容易遭受建模攻击等问题，本研究的主要内容以及创新如下：

（1）当前医疗行业快速发展，尤其是 WBAN 所涉及的物联网传感器，手机、网关等终端所具有的轻量存储特性，导致在 WBAN 中如何解决资源受限、易受安全威胁的问题成为重大难题，因此，提出了一种基于 PUF 的高效轻量级混合认证协议。本协议融合哈希函数与 PUF 技术，为合法用户建立安全信道，并通过哈希化 PUF 响应生成会话密钥，防止对物联网传感器的未授权访问，同时通过减少轻量级加密原语哈希的使用，降低节点的计算负担，并利用用户、网关和传感器三方不同的 PUF 来强化信息传输的安全性。与现有协议相比，该协议在通信与计算开销方面具有低消耗、高效率和新策略优势。同时，其密码更新阶段仅需用户参与，实际操作也更为便捷。

（2）面向新能源电车大量普及的大环境，PUF 的使用虽然解决了物理安全，但是随着人工智能（Artificial Intelligence，AI）的快速发展，海量的建模攻击正逐渐破解 PUF 安全性，但如何满足既保证轻量化，又抵御新进的建模攻击，且保证开放无线环境的安全效率的挑战。为此，提出了一种认证与密钥协商阶段去中心化的动态 PUF 匿名认证协议。该协议摒弃大多数基于 PUF 的认证方案，要么以明文暴露 CRP，要么依赖复杂的混淆方法，以及缺乏在重复用户认证过程中进行轻量化动态更新等缺点，采用 ECC 与高可靠性的 SDL PUF 相结合，引入了动态更新的 CRP 混淆机制，显著提升了抵御 ML 与 DL 攻击的能力。通过使用匿名标识符与临时会话密钥，实现了身份不可追踪性与会话独立性。协议的安全性在随机预言机模型（Random Oracle Model，ROR）的不可区分模型下进行了形式化验证，并利用 AVISPA 验证工具进行了检验。此外，在 SUMO 与