附表1-2（工学类、理学类、艺术学类、教育学类等用）

Attached List 1-2（For Engineering class, Science class, Art class, Education Class etc.）

南京邮电大学毕业设计(论文)开题报告

Nanjing University of Posts and Telecommunications

Opening Proposal of Graduation Project/Thesis

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 题　　目Title of the project/ thesis | Design and Implementation of UAV Authentication System based on Proof‑of-History Blockchain Technology | | | | | |
| 学生姓名Student Name | MUNTASIR AL MAMUN | | 班级学号Student Number | F22040119 | 专业Major | Computer Science and Technology |
| **1. Introduction**  The global proliferation of Unmanned Aerial Vehicles (UAVs), or drones, has marked a pivotal shift across numerous sectors. The commercial drone market is indeed experiencing significant growth. Market valuations are projected to increase substantially, with estimates reaching USD 57.8 billion by 2030. Recent report even suggests a CAGR of 37% between 2024 and 2034, leading to a potential market size of USD 1,445.80 billion by 2034.  . This expansion is fueled by the unprecedented flexibility and reach that UAVs offer, transforming industries from precision agriculture and disaster response to logistics and last-mile delivery. However, as these autonomous systems become increasingly integrated into commercial and civilian airspace, they introduce significant security and privacy concerns. The very connectivity that makes them effective also renders them vulnerable to a host of cyber-physical threats, including unauthorized access, malicious data tampering, and identity spoofing, which can lead to loss of control, data breaches, or physical disruption.  Traditional security architectures for network devices often rely on centralized authorities for authentication. While straightforward, this model introduces a single point of failure, which is particularly risky in a distributed and dynamic UAV network. A compromised central server could incapacitate an entire fleet. In response, researchers have proposed leveraging blockchain technology, whose inherent features of decentralization, immutability, and transparency offer a promising alternative [2]. Despite its potential, applying conventional blockchain consensus mechanisms like Proof-of-Work (PoW) or Proof-of-Stake (PoS) to UAVs is problematic. These algorithms are computationally intensive and suffer from high energy consumption, significant transaction fees, and low throughput limitations that are incompatible with the resource-constrained nature of UAVs [1].  This research proposes a novel authentication framework designed to address these challenges directly. It centers on the design and implementation of a lightweight, blockchain-based authentication system tailored for UAV networks. The core of this system is an efficient consensus mechanism inspired by Proof-of-History (PoH), which operates within a permissioned consortium blockchain. By creating a verifiable, chronological record of events, this approach eliminates the heavy computational burden of traditional consensus protocols and the need for strict clock synchronization among devices. Paired with the efficiency of elliptic-curve cryptography for secure communications, this work lays the groundwork for a robust, scalable, and extensible authentication infrastructure that can safeguard the next generation of autonomous aerial systems.  **1.1 A Study and Understanding of Tasks Assigned by the Supervisor**  The assigned research task is to investigate and develop a high-performance, lightweight authentication scheme for UAV networks by addressing the known deficiencies in existing blockchain-based solutions. The primary challenge in this domain is that conventional blockchain protocols were not designed for the resource-constrained and high-speed nature of UAV operations, leading to issues like high resource consumption, low transaction throughput, and significant confirmation delays . This project will focus on designing, implementing, and rigorously evaluating a novel framework that overcomes these specific limitations.  The research will develop a solution founded on a consortium blockchain model, which is better suited for a semi-trusted environment like a UAV fleet than a fully public chain. A central component of this work is the creation of a novel leader election mechanism. Instead of relying on the economic incentives of traditional Proof-of-Stake systems, this research will explore a method where leader nodes are chosen based on their statistical network participation, specifically by tracking the volume of transactions they forward. To maintain the decentralized integrity of the system, the design will incorporate a "cooling-off" period to prevent any single node from continuously holding the leader role.  The core technical task is to implement and leverage a Proof-of-History (PoH) consensus mechanism. By using sequential hashing, this approach creates a verifiable, chronological proof of events, which crucially eliminates the need for complex and slow clock synchronization protocols across the network. A key objective is to validate the performance of this architecture, with the goal of achieving the high throughput and low latency necessary for real-world UAV applications. Finally, to ensure robust end-to-end security, the framework will integrate lightweight elliptic-curve cryptography to facilitate rapid and secure key agreement between UAVs and the network nodes.  **2. Related Work**  This section provides a comprehensive review of the existing literature pertinent to Unmanned Aerial Vehicle (UAV) security, the application of blockchain technology for decentralized authentication, and the evolution of consensus mechanisms toward high-performance, lightweight solutions suitable for resource-constrained environments.  **2.1 Security Vulnerabilities and Authentication in UAV Networks**  The operational environment of UAVs is inherently insecure, exposing them to a wide array of cyber-physical attacks. The wireless communication channels used for command and control (C2) and data telemetry are prime targets for malicious actors. Recent analyses from 2024 and 2025 consistently highlight major threats, including control channel tampering, data breaches, and Global Positioning System (GPS) spoofing, which can deceive a UAV about its true location, leading to mission failure or capture [3, 4]. These vulnerabilities jeopardize not only the integrity of the data collected by UAVs but also the physical safety of operations, underscoring the critical need for robust authentication mechanisms [5].  Traditional security solutions that rely on centralized servers are ill-suited for the distributed nature of modern UAV deployments, as they create a single point of failure that is an attractive target for attackers [6]. In response, significant research has focused on developing lightweight security solutions tailored for the limited computational power of UAVs. Proposals from 2024 explore computationally efficient authentication protocols using techniques like Hyper-Elliptic Curve Cryptography (HECC) to provide strong security with lower overhead than traditional methods like RSA [5]. Furthermore, recent studies emphasize the integration of Artificial Intelligence (AI) and Machine Learning (ML) for intrusion detection and real-time anomaly detection to actively defend against threats [3, 6]. Despite these advancements, the core challenge remains: establishing a decentralized, scalable, and resilient trust framework that can operate effectively in dynamic and potentially hostile environments without overburdening the resource-constrained UAVs [4].  **2.2 Blockchain for Decentralized Trust and Its Inherent Limitations**  Blockchain technology has emerged as a transformative solution for establishing decentralized trust, making it a compelling candidate for securing UAV networks [7]. Its core properties decentralization, immutability, and transparency directly address the single-point-of-failure problem and enhance data integrity [8]. Recent 2024 studies demonstrate the viability of using blockchain to create tamper-proof logs for UAV-collected data, secure communication in ad-hoc UAV networks, and provide privacy-preserving location authentication [7, 9]. By leveraging cryptographic hashing and smart contracts, blockchain can ensure that sensitive information remains secure and verifiable, fostering trust and transparency among network participants without a central intermediary [10, 11].  Despite its promise, the direct application of mainstream blockchain technologies to UAVs is fraught with challenges, primarily stemming from their consensus mechanisms. The first and most famous consensus algorithm, Proof-of-Work (PoW), requires nodes to solve computationally intensive puzzles. This process consumes vast amounts of energy and results in very low transaction throughput and high latency, making it entirely unsuitable for real-time UAV operations. Proof-of-Stake (PoS), while more energy-efficient, still suffers from scalability issues and often involves transaction fees (gas fees) that are impractical for the high-frequency, non-financial transactions typical of IoT devices. As highlighted in recent analyses, the computational and energy demands of these traditional consensus protocols are often prohibitive for resource-constrained devices like UAVs [12].  **2.3 Advancements in High-Performance and Lightweight Consensus**  Recognizing the shortcomings of PoW and PoS for the Internet of Things (IoT), the research community has developed numerous alternative consensus mechanisms designed to be both lightweight and efficient. Recent 2025 studies propose novel hybrid algorithms that minimize resource demands by using methods like distributed lotteries for fair block proposals and reputation-based voting, avoiding the need for specialized hardware or heavy computation [13, 14]. Other approaches focus on designing consensus logic that is inherently suited for IoT scenarios, where nodes have heterogeneous capabilities. For instance, the Hierarchical Proof-of-Capability (HPoC) mechanism aims to elect leader nodes based on their actual computing, storage, and communication resources rather than financial stake [15]. These efforts reflect a clear trend toward creating efficient, fair, and secure consensus protocols tailored for the unique constraints of decentralized device networks [12].  Among the most significant innovations for high-throughput systems is Proof-of-History (PoH), the mechanism popularized by the Solana blockchain. PoH is not a standalone consensus mechanism but rather a cryptographic clock that creates a verifiable, ordered log of events *before* consensus is reached . It works by using a Verifiable Delay Function (VDF) a sequential hash that requires a specific amount of time to compute to timestamp every transaction. This creates a standardized timeline that all nodes can trust without having to communicate back and forth to agree on the order of events. By decoupling ordering from consensus, PoH dramatically reduces messaging overhead and allows for massive parallelization, enabling high speeds and low latency. This approach directly addresses the throughput bottlenecks of previous systems, providing a strong foundation for building the high-performance, lightweight authentication protocol proposed in this research.  **3. System Design**  This section details the proposed system for a secure and efficient UAV authentication network. The design leverages a permissioned blockchain architecture and a novel consensus mechanism, Efficient Proof-of-History (EPOH), to overcome the limitations of traditional systems. The design is broken down into its overall architecture, the core consensus mechanism, and the specific protocol for authentication and key agreement.  **3.1 Overall System Architecture**  The system is designed as a decentralized network composed of two primary entities: the UAV fleet and the edge/authentication nodes that form a consortium blockchain. The UAV fleet acts as the user base of the system. Each UAV is pre-registered with a unique subscriber identity (SUPI) and holds the public key of the blockchain network's nodes (PKNode​) to initiate communication and perform authentication. The edge/authentication nodes constitute the backbone of the network, forming a permissioned consortium blockchain that serves as a distributed data storage and verification center.  While all nodes are equal at the hardware level, they assume one of two distinct roles during operation. A single, elected Leader Node is responsible for collecting user transactions, ordering them chronologically using a sequential hashing process, packaging them into a new block, and broadcasting this block to the network. All other nodes in the network act as Validator Nodes, which receive new blocks from the leader, verify the correctness of the transactions and the chronological proof, and append valid blocks to their local copy of the blockchain. This distributed architecture eliminates the single point of failure inherent in centralized authentication systems.  Figure 3.1 provides a clear visualization of the operational roles within this architecture. While all edge nodes are peers at the hardware level, they dynamically assume one of two critical functions during operation. A single node is elected as the Leader Node for a specific time period. This node acts as the central coordinator and the primary point of contact for the UAV fleet, as shown by the wireless authentication requests directed toward it.    Figure 3.1 System Architecture of the EPOH-based UAV Authentication Network  Its core responsibilities are to receive transactions from the UAVs, use the Proof-of-History process to order them chronologically into a new block, and broadcast this block to the rest of the network. The remaining nodes function as Validator Nodes, forming an interconnected mesh that underpins the network's security and resilience. Their collective duty is to receive blocks from the Leader, independently verify the validity of the transactions and the correctness of the chronological proof, and append the new block to their local copy of the ledger. This distributed architecture, with its clear separation of roles, effectively eliminates the single point of failure that plagues traditional centralized authentication systems, ensuring high availability and integrity.  **3.2 The EPOH Consensus Mechanism**  The core of the system is the Efficient Proof-of-History (EPOH) consensus algorithm, designed for high throughput and low latency. To avoid the need for cryptocurrency, EPOH uses a novel, traffic-based election process. Time is divided into Rounds, and the leader for the next Round is chosen based on network participation in the current one; specifically, the node that forwards the highest number of valid transactions to the current leader is elected. To ensure decentralization, a "cooling-off" period is enforced. If a node serves as the leader for six consecutive Rounds, it becomes ineligible for election for the next two. The block generation and verification process leverages Proof-of-History to create a verifiable timeline of events, which drastically speeds up consensus by eliminating the need for clock synchronization. The leader node continuously performs a sequential hashing function, and when it receives a transaction, it incorporates a hash of that transaction into the sequence. This cryptographically embeds the transaction into the timeline, proving it occurred at a specific point. This generation process is inherently sequential and cannot be accelerated with parallel processing. The time to generate a hash sequence is given by ​ where N is the total number of hashes and np​ is the number of hashes a single core can perform per second. Once the block is created, validators can verify the entire sequence in a highly parallelized manner by splitting the sequence into slices. The verification time is given by where n is the number of CPU cores the validator uses for verification. This significant speed difference ensures both security and high throughput.  **3.3 Authentication and Key Agreement Protocol**  The system employs a multi-step protocol for mutual authentication and the establishment of a secure session key (KTx​). During initialization, UAVs are pre-registered with their permanent identity (SUPI) and a long-term symmetric key (K), while the authentication nodes generate an asymmetric key pair using Elliptic Curve Cryptography (ECC) and share the public key (PKNode​) with the UAVs. The authentication flow begins when the UAV encrypts its SUPI to create a temporary, concealed identity (SUCI) and sends it to the service network. This request is forwarded to an authentication server, which uses the blockchain's smart contract to resolve the SUPI and generate an Authentication Vector (AV). This vector contains a random challenge (RAND), an authentication token (AUTN), and an expected response (XRES\*). The server calculates a preliminary session key (KTx​) and sends the RAND and AUTN values to the UAV. The UAV validates the AUTN token using its long-term key, computes its own response (RES\*), and derives the same session key, KTx​. It then sends RES\* back to the network as proof of key ownership. The network hashes this response and verifies that it matches its stored expected response. Once verified, the authentication is successful, and both parties share a secure session key for all subsequent communication.  **4. Plan for Implementation**  This section outlines a structured 14-week plan for the implementation, testing, and documentation of the proposed UAV authentication system. The plan is divided into four distinct phases: Foundation and Setup, Core EPOH Implementation, System Integration and Testing, and Final Analysis and Thesis Writing. Each week is assigned specific tasks and deliverables to ensure steady progress and timely completion of the project.  Phase 1: Foundation and Core Component Development (Weeks 1-4)  This initial phase focuses on establishing the development environment and implementing the fundamental building blocks of the system as identified in the literature review.  Week 1: Project Setup and Cryptographic Primitives  Tasks: Finalize the research proposal and literature review. Set up the development environment, including the chosen programming language, version control (Git), and necessary libraries for cryptography and networking. Implement the core Elliptic Curve Cryptography (ECC) functions for key pair generation, encryption, and decryption, which are essential for the authentication protocol.  Deliverable: A functional code module for ECC operations.  Week 2: Basic Blockchain Data Structures  Tasks: Design and implement the basic data structures for the blockchain, including the Block (with header and transaction list), Transaction, and Blockchain (a chain of blocks). Implement the core SHA-256 hashing function for block integrity.  Deliverable: A simple, functional local blockchain capable of adding and validating new blocks.  Week 3: Proof-of-History (PoH) Generator  Tasks: Implement the core Proof-of-History mechanism. This involves creating a sequential hashing loop that generates a verifiable timeline. Develop the logic to embed transaction hashes into this sequence at specific intervals.  Deliverable: A standalone PoH generator that can produce a verifiable hash sequence with embedded event data.  Week 4: P2P Network Layer  Tasks: Develop the peer-to-peer (P2P) networking layer for node communication. Implement basic message handling for broadcasting and receiving transactions and blocks across a network of nodes.  Deliverable: A network of nodes that can connect and exchange basic data packets.  Phase 2: EPOH Consensus and Protocol Implementation (Weeks 5-8)  This phase focuses on integrating the core components into the full EPOH consensus mechanism and implementing the authentication protocol.  Week 5: Leader Election Mechanism  Tasks: Implement the traffic-based leader election logic. This includes tracking the number of transactions forwarded by each node and selecting the next leader. Implement the "cooling-off" period to ensure decentralization.  Deliverable: A network of nodes that can dynamically elect a leader for each round.  Week 6: EPOH Consensus Integration  Tasks: Integrate the PoH generator with the leader node's functions. The elected leader must now generate blocks containing PoH proofs. Implement the parallel verification logic for validator nodes to quickly confirm the validity of new blocks.  Deliverable: A working blockchain network running the EPOH consensus mechanism.  Week 7: Authentication Protocol Implementation (Part 1)  Tasks: Begin implementing the authentication protocol on top of the blockchain. Implement the initial steps of the flow, including the UAV creating a SUCI and the network nodes handling the request and generating the Authentication Vector (AV).  Deliverable: A system where a UAV can initiate an authentication request and receive a valid challenge from the network.  Week 8: Authentication Protocol Implementation (Part 2)  Tasks: Complete the authentication flow. Implement the UAV's response validation (RES\*), the network's final verification, and the successful establishment of the session key (KTx​) on both sides.  Deliverable: A fully functional end-to-end authentication and key agreement protocol.  Phase 3: Simulation, Testing, and Refinement (Weeks 9-11)  This phase is dedicated to rigorously testing the implemented system for performance and security.  Week 9: Simulation Environment and Performance Benchmarking  Tasks: Develop a simulation environment to test the system at scale. Create scripts to simulate hundreds of UAVs and dozens of nodes. Conduct performance tests to measure key metrics like Transactions Per Second (TPS) and transaction confirmation latency.  Deliverable: Initial performance results and graphs comparing them to the claims in the source literature.  Week 10: Security Analysis and Testing  Tasks: Design and execute security tests based on the threats identified in the literature review. Simulate common attacks such as impersonation, replay attacks, and malicious fork attempts to verify the system's resilience.  Deliverable: A security analysis report detailing the system's performance against various attack vectors.  Week 11: System Refinement and Optimization  Tasks: Analyze the results from the performance and security tests. Identify and address any bottlenecks or vulnerabilities. Fine-tune system parameters (e.g., slot time, round duration) to optimize performance.  Deliverable: An optimized and robust version of the implemented system.  Phase 4: Documentation and Thesis Writing (Weeks 12-14)  The final phase is focused on documenting the work and completing the thesis.  Week 12: Writing Implementation and Results Chapters  Tasks: Begin writing the core chapters of the thesis. Document the system design, implementation details, experimental setup, and the results obtained from testing.  Deliverable: Draft of the implementation and results sections.  Week 13: Finalizing Analysis and Thesis Draft  Tasks: Complete the data analysis, generate final graphs and tables for the results chapter, and finish the first complete draft of the thesis, including the introduction, literature review, design, implementation, and conclusion.  Deliverable: A complete first draft of the thesis.  Week 14: Final Review and Submission  Tasks: Review and edit the entire thesis for clarity, consistency, and grammatical errors. Ensure all references are correctly formatted. Prepare the final document for submission to the supervisor for review.  Deliverable: Final, polished thesis document ready for submission.  **References** S. Javed et al., “An Efficient Authentication Scheme Using Blockchain as a Certificate Authority for the Internet of Drones,” Drones, vol. 6, no. 10, p. 264, Sept. 2022, doi: 10.3390/drones6100264.T. Alladi, V. Chamola, N. Sahu, and M. Guizani, “Applications of blockchain in unmanned aerial vehicles: A review,” Vehicular Communications, vol. 23, p. 100249, June 2020, doi: 10.1016/j.vehcom.2020.100249.Z. Yang et al., “AI-Driven Safety and Security for UAVs: From Machine Learning to Large Language Models,” Drones, vol. 9, no. 6, p. 392, May 2025, doi: 10.3390/drones9060392.Y. Renu and V. Sarveshwaran, “A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs),” ia, vol. 28, no. 75, pp. 199–219, Feb. 2025, doi: 10.4114/intartif.vol28iss75pp199-219.Choudhary, G., & Sharma, V. (2024). Securing UAV Networks: Exploring Computationally Efficient Authentication Protocols. *Preprint*.I. Chandran and K. Vipin, “Multi-UAV Networks for Disaster Monitoring: Challenges and Opportunities from a Network Perspective,” SN COMPUT. SCI., vol. 5, no. 5, May 2024, doi: 10.1007/s42979-024-02788-3.M. A. Alqarni, “Secure UAV adhoc network with blockchain technology,” PLoS ONE, vol. 19, no. 5, p. e0302513, May 2024, doi: 10.1371/journal.pone.0302513.H. Pan, Y. Wang, W. Wang, P. Cao, F. Ye, and Q. Wu, “Privacy-preserving location authentication for low-altitude UAVs: A blockchain-based approach,” Security and Safety, vol. 3, p. 2024004, 2024, doi: 10.1051/sands/2024004.S. Hafeez et al., “Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey,” IEEE Open J. Veh. Technol., vol. 4, pp. 558–580, 2023, doi: 10.1109/ojvt.2023.3295208.J. Akram, M. Umair, R. H. Jhaveri, M. N. Riaz, H. Chi, and S. Malebary, “Chained-Drones: Blockchain-based privacy-preserving framework for secure and intelligent service provisioning in Internet of Drone Things,” Computers and Electrical Engineering, vol. 110, p. 108772, Sept. 2023, doi: 10.1016/j.compeleceng.2023.108772.S. Sahraoui and A. Bachir, “Lightweight Consensus Mechanisms in the Internet of Blockchained Things: Thorough Analysis and Research Directions,” Digital Communications and Networks, Jan. 2025, doi: 10.1016/j.dcan.2024.12.007.S. Vavilis, H. Niavis, and K. Loupos, “A Fair and Lightweight Consensus Algorithm for IoT,” 2025, arXiv. doi: 10.48550/ARXIV.2503.08607.S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, “A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues,” IEEE Access, vol. 11, pp. 39066–39082, 2023, doi: 10.1109/access.2023.3267047.Z. Nie, M. Zhang, and Y. Lu, “HPoC: A Lightweight Blockchain Consensus Design for the IoT,” Applied Sciences, vol. 12, no. 24, p. 12866, Dec. 2022, doi: 10.3390/app122412866.Galaxy Research. (2024). *Protocol Overview: Solana 2024*. Galaxy Digital.Cointelegraph. (2024). What is proof-of-history, and how does it work?. *Cointelegraph Magazine*. | | | | | | |
| 指导教师批阅意见Supervisor’s Comments | | 指导教师(签名)： 年 月 日  Supervisor ( Signature)： Date: | | | | |

注：可另附A4纸

Remark: Additional A4 size papers could be attached.