Unicomm: A Decentralized, Secure, and Anonymous Communication Network

liomuguchia@gmail.com

www.unicom.org

*This project is not intended for ownership by any entity or organization
Contribute to the open project on github.com/leomuguchia/unicomm*

Abstract

Unicom is a fully decentralized, anonymous, and secure communication network designed to support real-time communication such as messaging and voice calls. It achieves this through a combination of **Distributed Hash Tables (DHT)**, **Onion Routing**, **Secure Multi-Party Computation (SMPC)**, and advanced cryptographic techniques. The goal is to ensure privacy, security, and anonymity while maintaining high performance and scalability across a dynamic, peer-to-peer network of mobile devices.

Introduction

In today's world of mass data surveillance and privacy concerns, most communication systems rely on centralized servers, which are prone to censorship, breaches, and interception. Unicom addresses this by decentralizing communication, allowing peers to communicate without any reliance on central authorities. Every node in Unicom's network is both a client and a server, enabling direct peer-to-peer communication while preserving user privacy.

The core objectives of the Unicom network are:

- **Privacy**: All communications are end-to-end encrypted.
- **Anonymity**: Onion routing ensures that no single node knows the entire communication path.
- **Decentralization**: The network has no single point of failure or control.
- **Fault Tolerance**: The system is resilient to node churn, ensuring reliable communication even in dynamic environments.
- **Real-Time Communication**: Support for messaging and voice calls with efficient encryption and routing.

---

1. Key Components

1.1 Peer-to-Peer (P2P) Network

Unicom operates over a peer-to-peer network where each node (mobile phone,or computer) acts as both a **client** and a **server**. Every node:

- Sends and receives messages (client role).
- Routes other users' messages (server/relay role).

Each node connects to the network dynamically, and the system adapts in real-time to changes in the number of active nodes. Peers can share their encrypted session tokens instead of their direct addresses. Only peers that share a direct connection can decrypt these tokens to establish a link.

1.2 Distributed Hash Table (DHT) for Peer Lookup

The **DHT** serves as the backbone of Unicom's decentralized structure:

- **Peer Lookup**: DHT enables fast and decentralized lookup of peers without a central server.
- **Key-Value Storage**: Public keys (representing user identities) are stored in the DHT, mapping to session data (e.g., active routing paths or rendezvous points).

Technical Implementation:

- **Kademlia DHT** is a preferred choice due to its ability to handle network churn (nodes joining or leaving frequently). Each node is responsible for a portion of the DHT, and lookups are distributed efficiently across the network.
- **Node Registration**: When a node joins the network, it generates a unique cryptographic identifier, which is stored in the DHT along with its session data.

Challenges & Solutions:

- **Data Integrity**: Malicious nodes could potentially insert false data into the DHT. To address this, each entry in the DHT is signed cryptographically, ensuring only legitimate data is stored.
- **Dynamic Churn**: Frequent node departures (common in mobile environments) are handled by replicating DHT data across multiple nodes, ensuring redundancy.

1.3 Onion Routing for Anonymity

Unicom uses **Onion Routing** to guarantee user anonymity and privacy:

- **Multiple Layers of Encryption**: Messages are encrypted in layers, with each intermediary node (relay) decrypting only its own layer to forward the message. The final destination removes the last layer of encryption.
- **Relay Hopping**: Each communication route involves multiple intermediary nodes, so neither the sender nor the recipient is directly exposed to anyone except the next and previous hop.

Technical Implementation:

- Each communication session establishes a virtual circuit of intermediary nodes, chosen randomly.

- Messages are encrypted layer-by-layer, with each relay node responsible for decrypting its layer and forwarding the rest.

Dynamic Peer Connections

Users can initiate connections based on shared group keys or identifiers that do not reveal their individual addresses. If two peers wish to connect, they establish a temporary direct communication channel with ephemeral session keys that expire after use.

Obfuscating Current IP Address

To avoid exposing the user's current IP address, peers can utilize a relay system where a user's traffic is routed through multiple peers before reaching its final destination. This way, the endpoint is unaware of the original sender's location.

Optimization Strategy:

- **Latency Mitigation**: For real-time communication like voice calls, direct peer-to-peer connections are preferred, using Onion Routing only when anonymity is critical.
- **Reputation System**: Nodes with high up-time and reliability are prioritized for relay functions to ensure stable routing.

1.4 Secure Multi-Party Computation (SMPC)

SMPC is employed in Unicom for privacy-preserving computations, allowing nodes to collectively compute routing paths without revealing sensitive data:

- **Routing Path Discovery**: SMPC enables nodes to collaborate and determine the best route for messages without exposing IP addresses or connection metadata.

Technical Implementation:

- SMPC algorithms allow nodes to perform distributed computations, such as selecting intermediary relays, while maintaining the confidentiality of each node's data.
- **Threshold Cryptography** can be used within the SMPC framework to ensure data remains private unless a majority of nodes agree on its disclosure.

Challenges:

- **Performance Overhead**: SMPC can be computationally expensive. To mitigate this, it's only used for critical operations like initial peer discovery or establishing anonymous routes.
- **Mobile Environment**: Use lightweight cryptographic protocols that minimize computational burden on mobile nodes.

1.5 Encryption and Key Management

All communications within Unicom are secured using end-to-end encryption:

- **Elliptic-Curve Diffie-Hellman (ECDH)** is used for secure key exchange between nodes.

- **Ephemeral Session Keys**: For each communication session, a unique key is generated and discarded once the session ends, ensuring forward secrecy.

Key Management:

- **Public/Private Key Pair**: Each user has a long-term public/private key pair. The public key is shared for others to encrypt messages, while the private key decrypts incoming data.
- **Key Rotation**: Session keys are rotated frequently to limit exposure in case of compromise.

Implementation:

- **Zero-Knowledge Proofs (ZKP)** can be employed for node authentication, ensuring a node can prove its identity without revealing sensitive information.

---

2. Secure Communication Protocols

2.1 End-to-End Encryption

All communications are encrypted end-to-end using **Elliptic-Curve Cryptography (ECC)** for key exchange and **symmetric encryption** (e.g., AES) for data transmission. This ensures that no intermediary node can read the message content.

Encryption Process:

- **Key Exchange**: Nodes use **Elliptic-Curve Diffie-Hellman (ECDH)** to establish a shared secret without revealing their private keys.
- **Symmetric Encryption**: Once a shared secret is established, all communication between nodes is encrypted using AES (Advanced Encryption Standard).
- **Session Keys**: Each session generates unique keys that are discarded at the end of the communication session, reducing the risk of long-term key compromise.

2.2 Secure Multi-Party Computation (SMPC) for Routing

SMPC allows nodes to participate in routing and path finding computations without revealing sensitive information such as IP addresses.

SMPC Use Cases:

- **Routing Decisions**: Nodes collaborate to determine the best routing path without revealing their private data.
- **Private Information Retrieval (PIR)**: Nodes can query the DHT for lookup information without exposing which entry they are looking for.

2.3 Zero-Knowledge Proofs (ZKP)

ZKPs are used for node authentication and verification, allowing nodes to prove their identity without revealing their private information. This adds an additional layer of privacy by preventing metadata leaks during verification processes.

---

3. Network Architecture

3.1 Dynamic Node Behavior

Nodes in Unicom are highly dynamic, meaning they can frequently join and leave the network. To handle this, the architecture must account for:

- **Node Churn**: The system uses adaptive routing and replication to ensure that the network remains resilient, even as nodes frequently come and go.
- **Heartbeat Mechanism**: Nodes periodically send heartbeats to notify others of their presence. If a heartbeat is missed, the node is assumed to be offline, and the DHT is updated accordingly.

3.2 Fault Tolerance & Scalability

Unicom is designed to handle the dynamic nature of decentralized mobile networks:

- **Adaptive Routing**: If a node on the communication path goes offline, Unicom dynamically re-routes the message through alternative nodes.
- **Redundant Data Storage**: The DHT ensures data is replicated across multiple nodes to prevent data loss when peers disconnect.
- **Reputation System**: Nodes are scored based on their reliability. High-reputation nodes are preferred for relaying and routing.

3.3 Bootstrapping and Network Discovery

Initial Peer Discovery:

- When a node joins the network, it must discover other peers. This can be achieved via **predefined bootstrap nodes** (public seed servers or well-known entry points).
- Once connected to the network, the node can start interacting with the DHT and routing traffic.

Local Peer Discovery:

- In certain cases (e.g., local mesh networks), Unicom can use **Wi-Fi Direct** or **Bluetooth** for discovering nearby nodes and establishing direct communication.

---

4. Scalability and Performance

4.1 Load Balancing

The DHT allows for load distribution across the network, ensuring that no single node is overwhelmed by traffic. Nodes with more reliable resources (e.g., stable network connection, strong battery life) can be prioritized for handling higher traffic loads.

4.2 Latency Minimization

Although onion routing introduces some latency, Unicom will implement optimizations to reduce overhead:

- **Optimized Routing Algorithms**: Routing algorithms will be optimized to minimize the number of hops needed for communication, especially in high-latency scenarios like voice calls.
- **Relay Selection**: Nodes will dynamically select the best relays based on network conditions and latency.

---

5. Use Cases

5.1 Private Messaging

Unicom can be used for fully encrypted, anonymous messaging, where neither the sender nor the receiver’s IP addresses are known to each other or any intermediary nodes.

5.2 Real-Time Voice Calls

Unicom supports real-time voice communication using low-latency encryption methods and dynamic routing to maintain performance and anonymity.

5.3 Secure Data Transmission

Sensitive data (e.g., documents, files) can be securely transmitted across the network with full anonymity and encryption.

---

6. Security Model

6.1 Reputation System

To ensure the integrity and reliability of relay nodes, a **reputation system** will be implemented:

- Nodes earn reputation points based on successful message routing and participation in SMPC.
- Malicious nodes (e.g., those dropping packets or altering messages) are penalized, reducing their chances of being selected as relays.

6.2 Malicious Node Detection

Nodes that behave suspiciously (e.g., altering message content, tampering with routing paths) are identified and penalized by the reputation system. This ensures that the network remains secure, even in the presence of malicious actors.

6.3 Security Considerations

1. Attack Vectors:

- **Sybil Attacks**: A malicious actor creates many fake identities to overwhelm the network. Unicom's reputation system and **proof-of-work** for new identities can mitigate this risk.
- **DDoS Attacks**: Distributed attacks targeting nodes are mitigated by the decentralized nature of the network, where traffic is distributed across many nodes.

2. Data Integrity:

- All data entries in the DHT are signed using cryptographic keys to ensure their validity and prevent tampering by malicious nodes.

---

7. Future Work

7.1 Improved Routing Algorithms

Future iterations of Unicom will focus on optimizing routing algorithms to further reduce latency and improve the user experience, particularly for real-time communication.

7.2 Advanced Cryptographic Protocols

New cryptographic protocols, such as post-quantum encryption methods, will be explored to future-proof the network against emerging security threats.

7.3 Decentralized Governance

Implementing decentralized governance will allow network participants to vote on key changes to the network's protocol and security measures, ensuring that the network evolves based on community consensus.

Conclusion

Unicom represents a major step forward in decentralized, anonymous communication. By leveraging advanced cryptography, decentralized storage and routing methods, and dynamic fault tolerance, Unicom ensures secure, real-time communication without the need for centralized servers or trusted intermediaries. With its highly scalable architecture and emphasis on privacy, Unicom is poised to become a leading solution for secure, anonymous communication in an increasingly surveillance-driven world.