Surveillance and Censorship resistant communication

Over the internet

Rishi’s part

Content

1. Introduction
2. Literature Review
3. Solution
4. Methodology & Implementation
5. Evaluation
6. Demonstration
7. Conclusion
8. Future works

Introduction

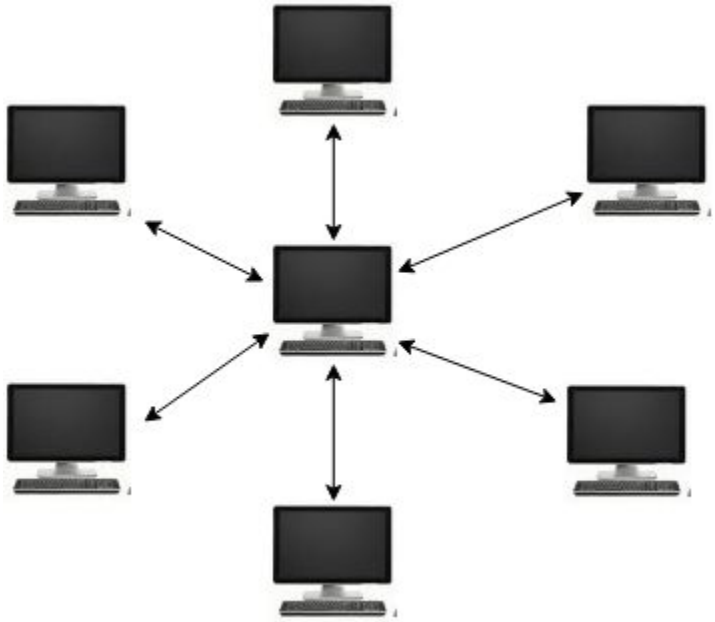
Background

Concerns of modern internet communication

- Privacy
- Surveillance
- Censorship
- Data tracking

Problem

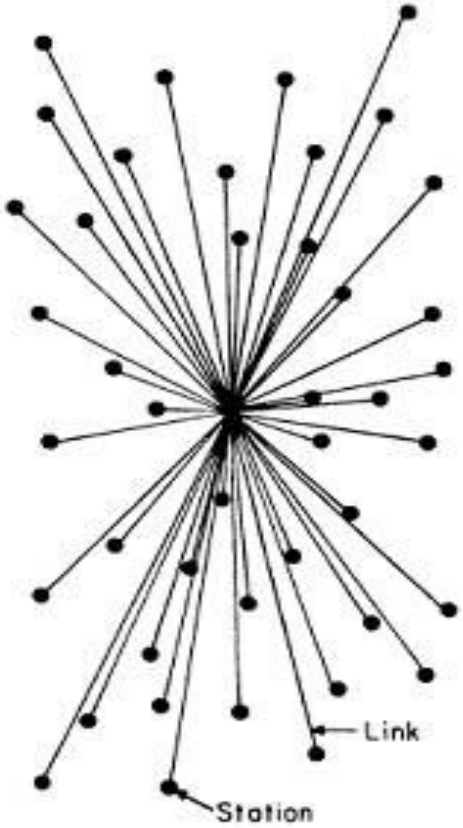
Centralized design architecture of services



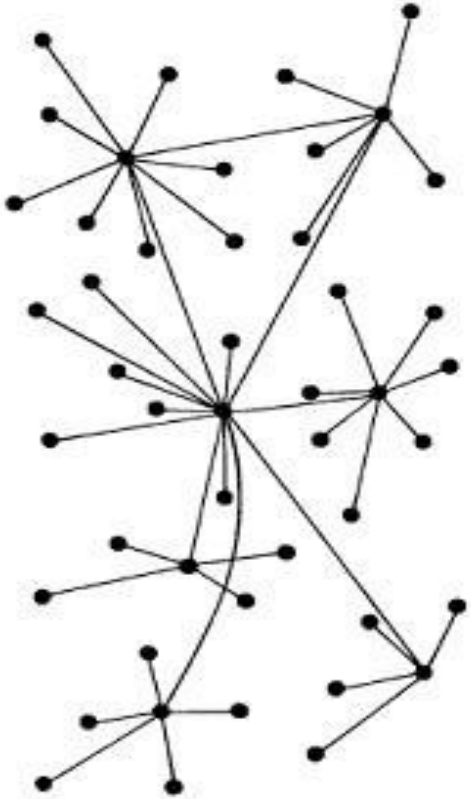
Literature Review

Alternative design architectures

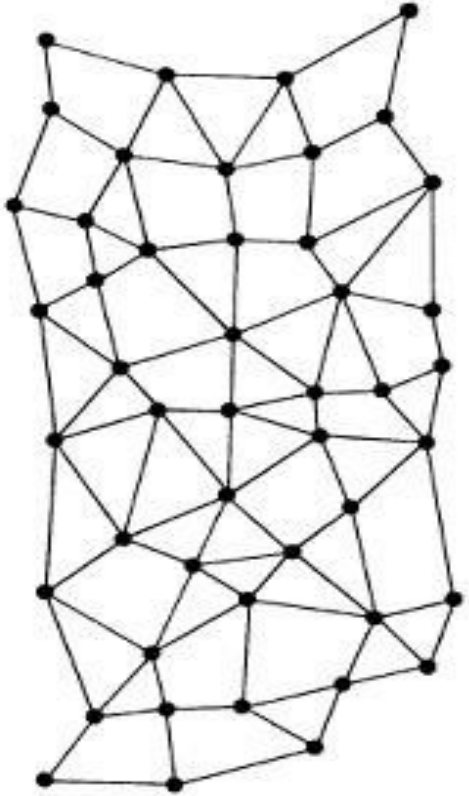
- Decentralized architecture
  - Peer to peer
  - Master slave architecture
- Distributed architecture
  - Peer to peer
  - Client server
  - N-tier architecture



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

Related Works

- TOR
  - Tor is free and open-source software for enabling anonymous communication.
  - Onion routing.
  - Decentralized master slave architecture.
  - Anonymity over privacy.
- Skype peer to peer
  - A peer-to-peer IP telephony network.
  - Decentralized master slave architecture.
  - Three types of nodes (Super node, Ordinary node, Login server).

- Bitcoin
  - Digital or virtual currency.
  - Distributed peer to peer architecture.
  - Blockchain technology.
  - Proof of Work consensus mechanism.
- Anonymous remailers
  - Mail servers that conceal the identity of users.
  - Distributed client server.
  - Four types (Cypherpunk, Mixmaster, Mixminion, Pseudonymous remailers).

Summary

	Decentralized	Federated	Interactive	Federatable
Torrents	Y	N	N	Y
BTC	Y	N	N	N
IPFS/Freenet	Y	N	N	N
TOR	N	N	N	N
Usenet	N	Y	N	N/A
Skype	Y*	Y*	Y	N/A
I2P	Y	Y	N	N
Remailers	Y	Y	N	Y
Our solution	Y	Y*	Y	Y

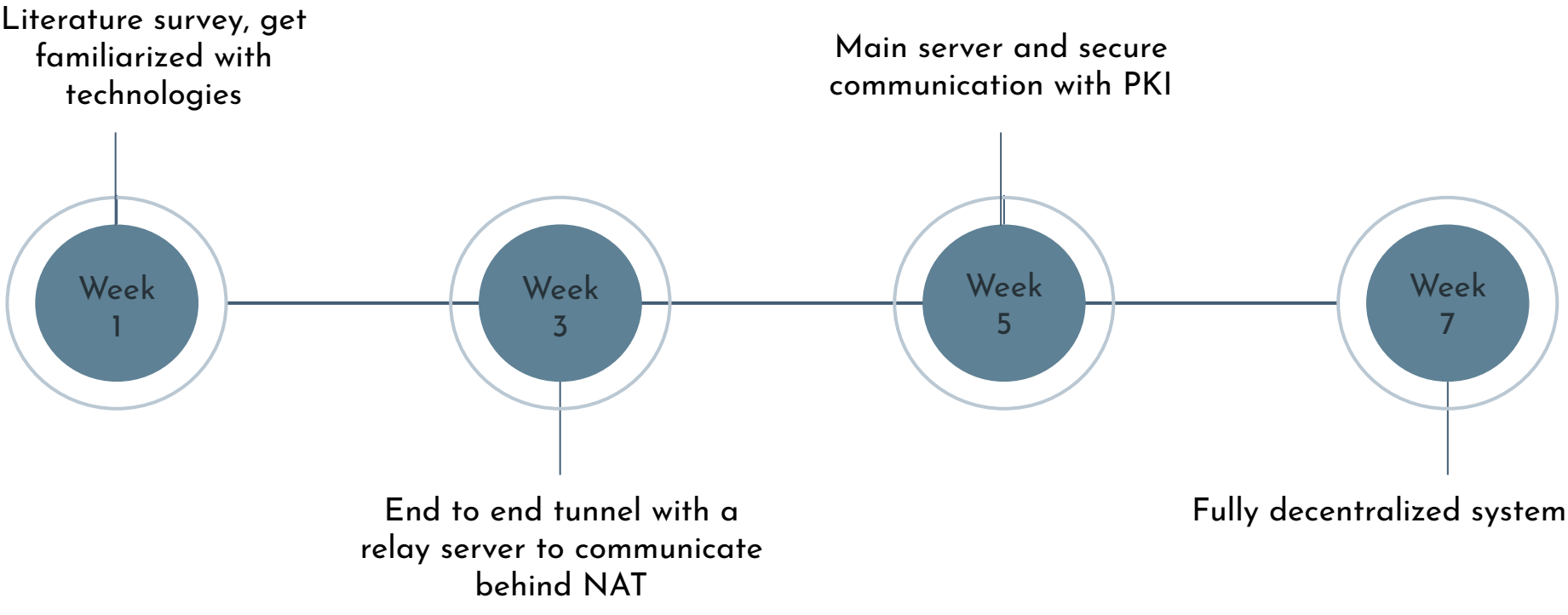
Solution

We explores a way of using a hybrid approach for decentralized communication and utilize this to establish DTLS tunnels to maintain connectivity among devices behind NAT.

Reasons for solution

- Avoid single point of failure.
- Exhaustive and inefficient connection establishment in purely distributed systems.
- Hybrid systems, provides
  - Search efficiency of centralized systems.
  - Maintain the reliability of decentralization.

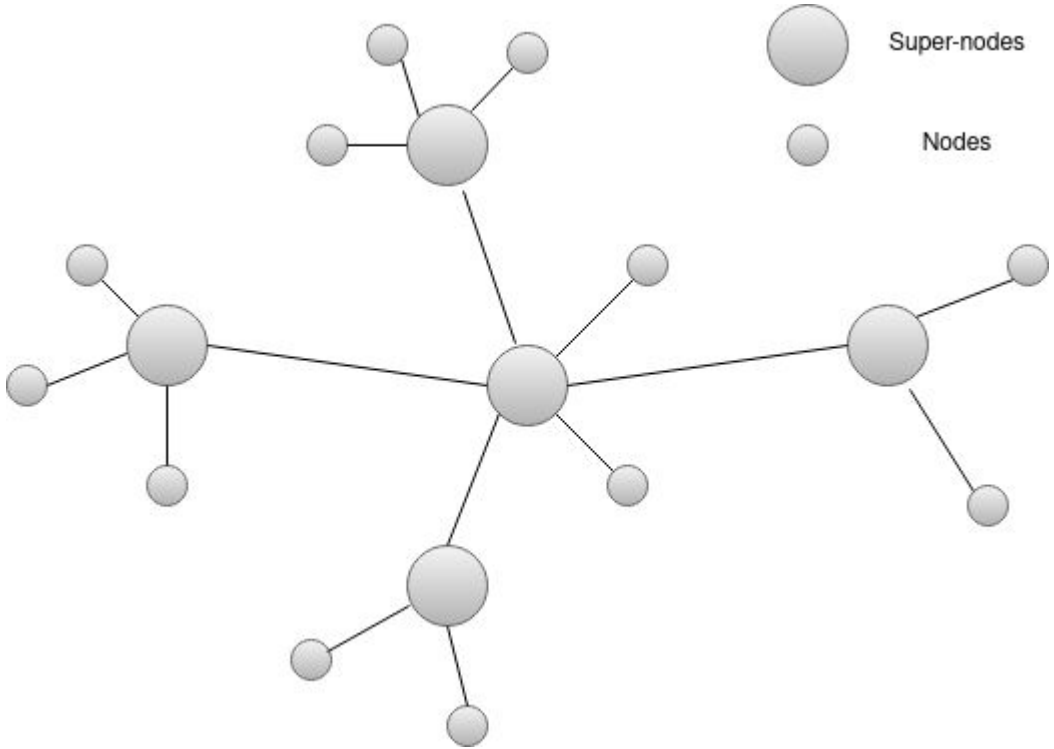
Timeline (as per proposal)



Methodology

Supipi’s part

Conceptual Design



Aims of this phase

- Handle dynamic behaviour of super-nodes.
- Decentralized and pseudonymous node discovery.
- NAT navigation of nodes.
- Protect confidentiality of node to node communication.

Implementation

Message Types

Message	Description
HELLO_S	A connection request from a super-node to another super-node. Sends when a super-node initiates
CHANGE_S	A super-node cannot directly connect to another super-node. A change in topology is required
END_S	To end the connection between two super-nodes. Sends when a change of neighbour-nodes is required.
SEARCH	Search for a node. This is sent when a Node requests a tunnel establishment.

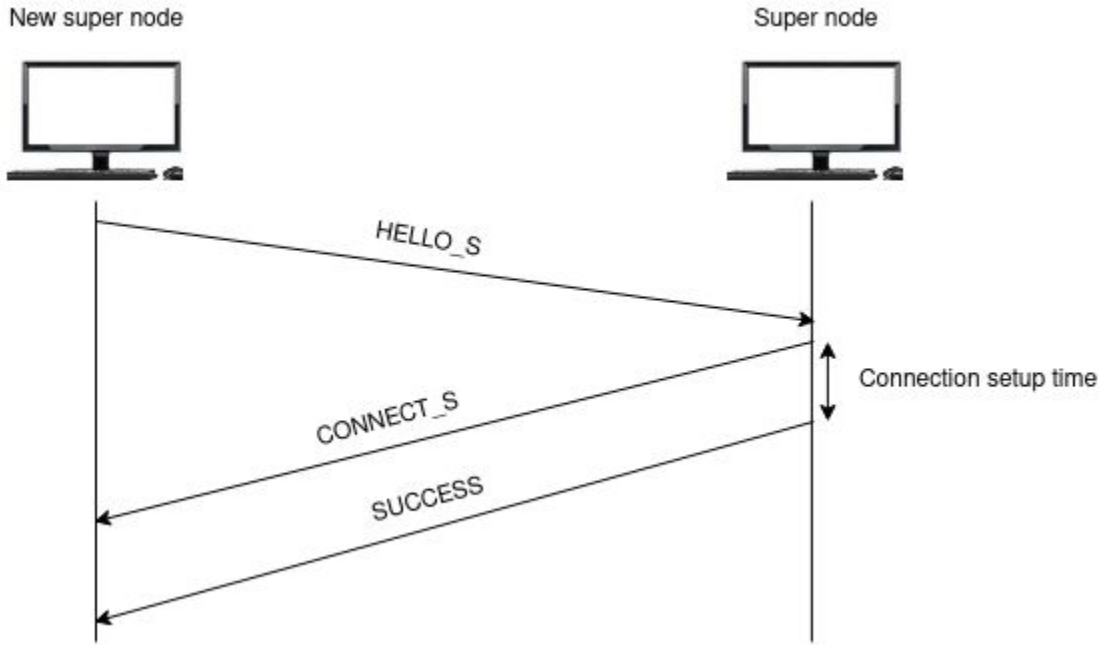
Message Types

Message	Description
INIT_P	A connection request from a node to a super-node.
FIND_P	A service request to find the location that holds a destination hashed key in a tunnel establishment scenario.
ANONYM_P	Inform a change of public key of a node. This can be utilized by nodes to obtain pseudonymity.
CONNECT_P	Tunnel establishment request sends from a node.

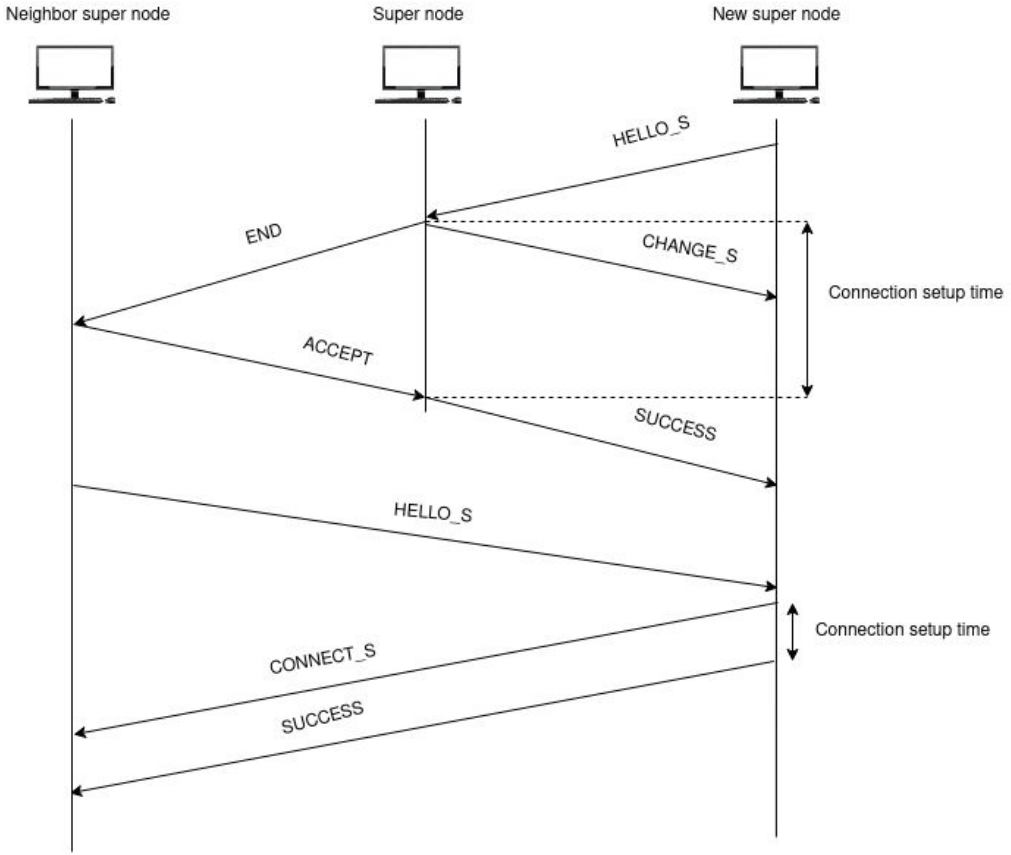
Message Types

- Other types of messages
  - CONNECT_S
  - EXIT_S
  - FOUND
  - LOCATE_P
  - LISTEN_P
  - ACCEPT / SUCCESS
  - REJECT / FAIL

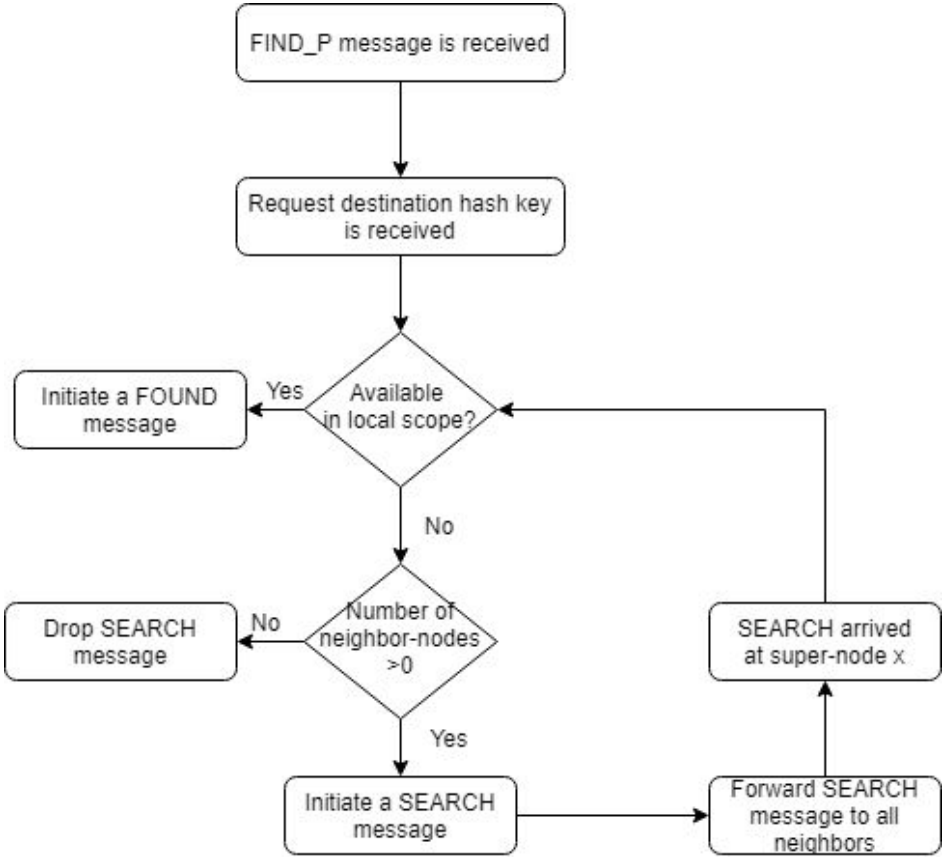
Connection establishment - 1



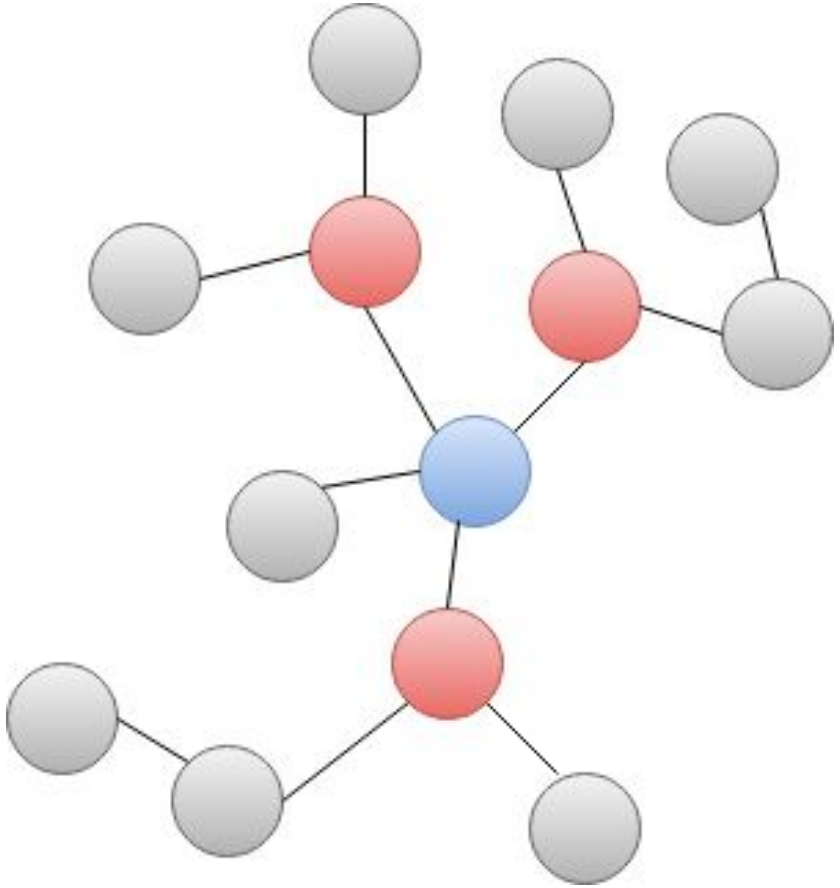
Connection establishment - 2



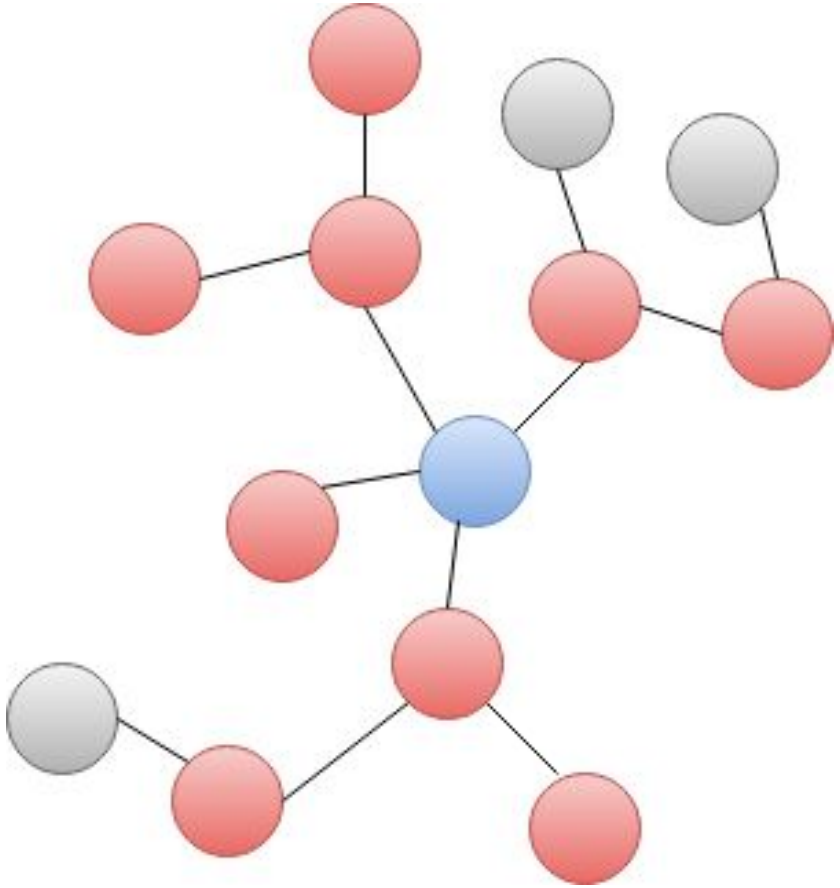
Node discovery - 1



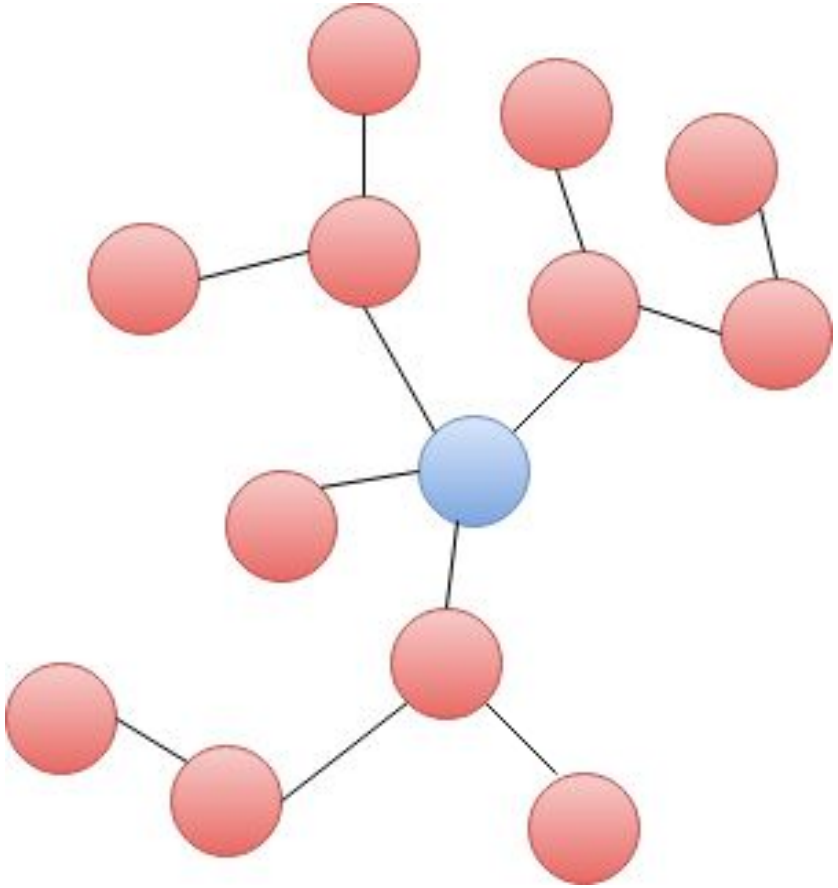
Node discovery - 2



Node discovery - 2



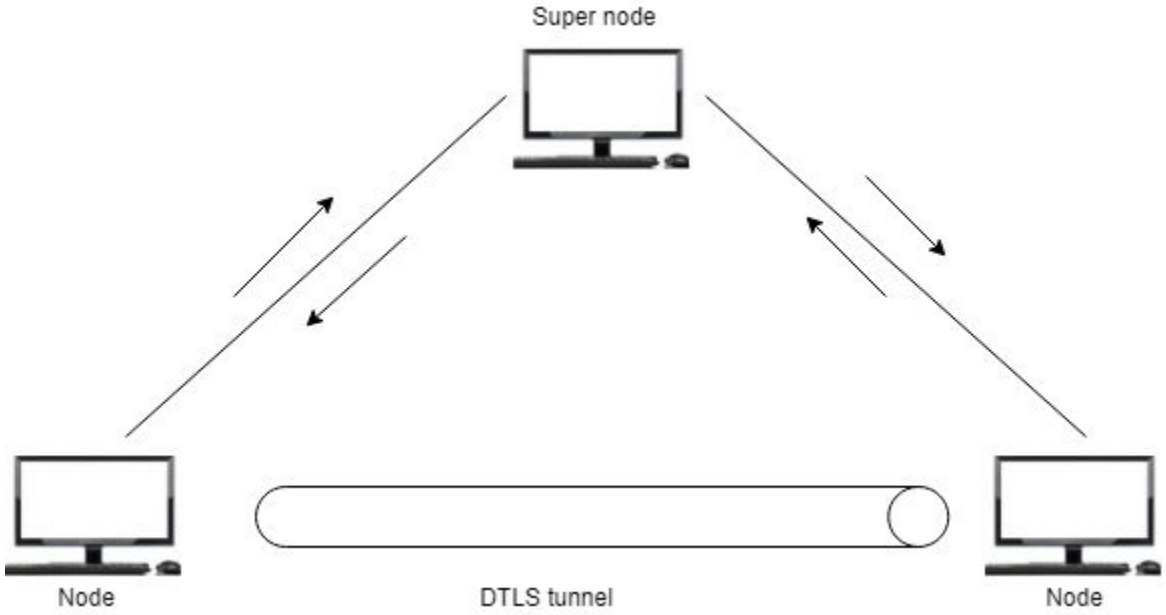
Node discovery - 2



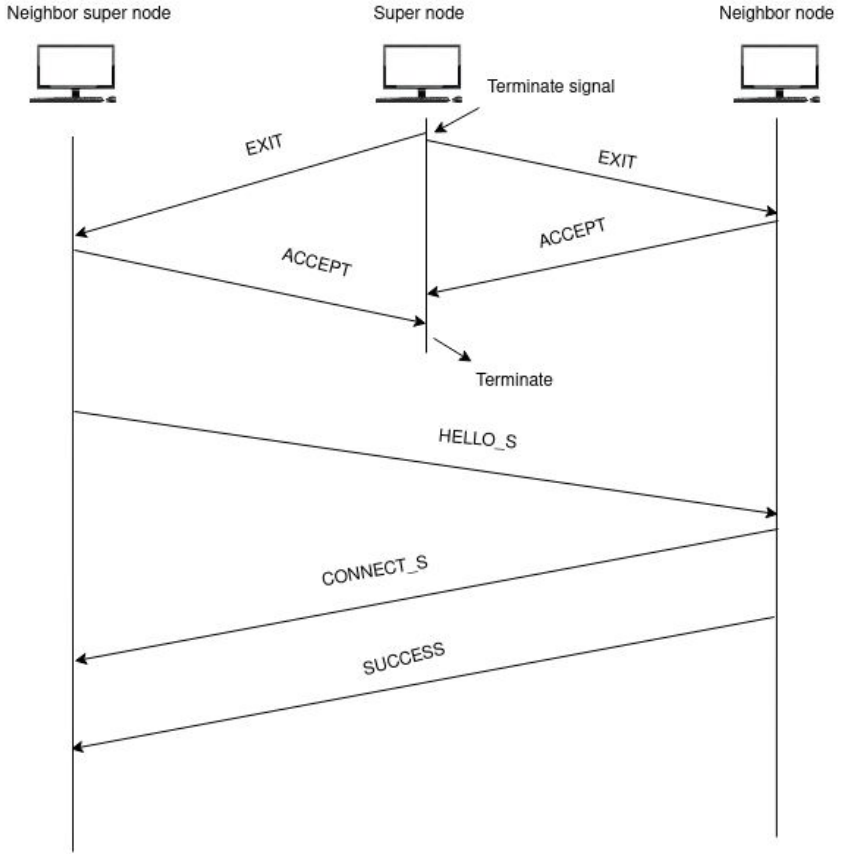
Tunnel establishment

1. Disconnects from the current super-node
2. Connects to the destination super-node
3. DTLS tunnel is established between the super-nodes utilizing the super-node as a relay agent.

Tunnel establishment

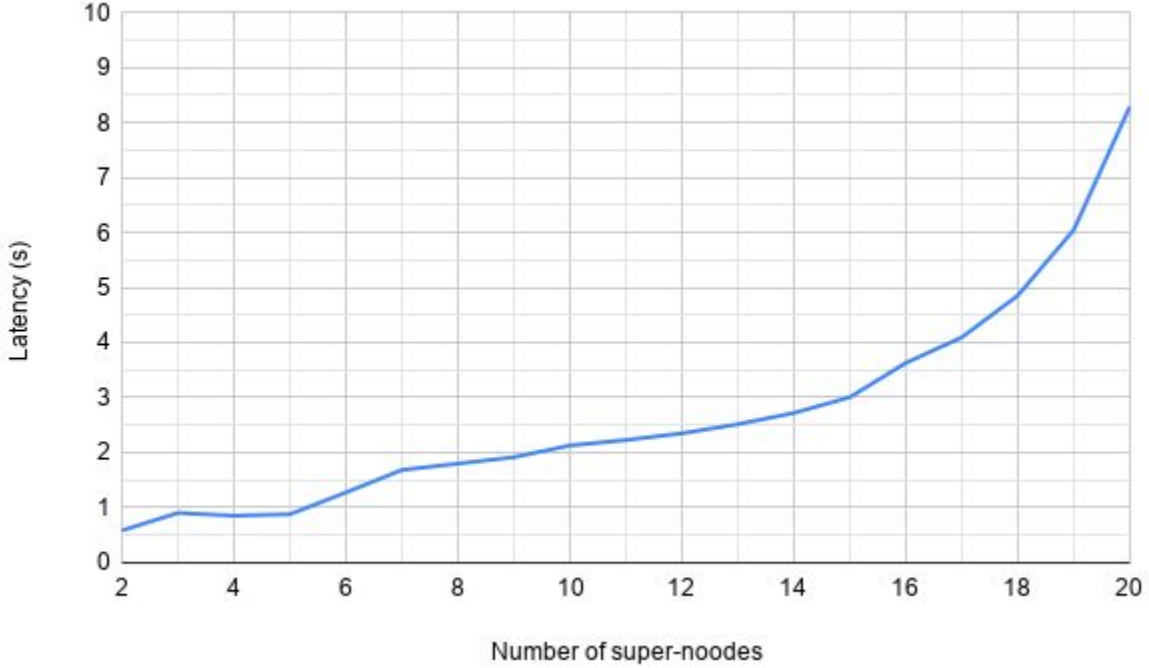


Connection termination

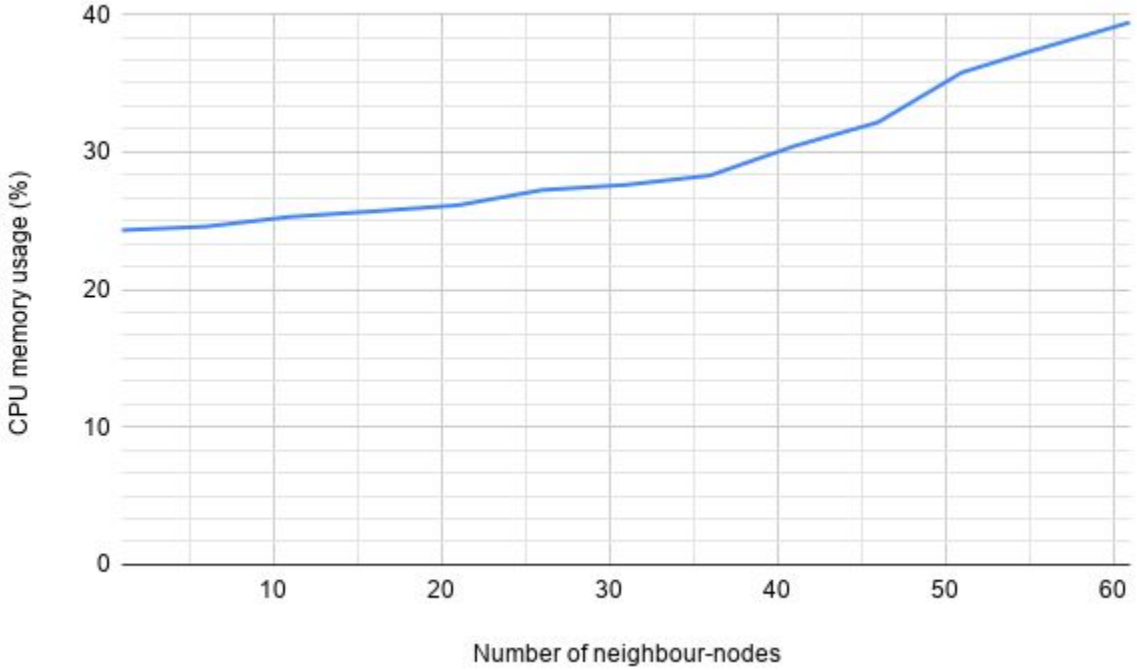


Evaluation

Performance of node discovery



Performance of super-nodes



Demonstration

Conclusions

- Distributes the control of information over multiple nodes.
- The super-node system improve the performance of the node discovery.
- Dynamically changing the topology of the network to keep the
- Allows a node to obtain pseudonymity.
- A node discovery can be done under five seconds, along 18 linearly connected super-nodes.
- The system assumes all super-nodes are trustworthy.

Future Works

Future Directions

- Improve efficiency of node discovery.
- Continuous communication during topology changes.
- Distributed authentication.
- Distributed authorization.

Distributed Authentication

Plan for 8th semester

Deliverable	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15
Literature review															
Design of a new Decentralized authentication mechanism															
Performance analysis															
Integrate with the decentralized communication system															

QnA