school of Computer Science & Statistics

An Anonymous Decentralised Messaging Application Utilising the Whisper Protocol

Student: Seán Durban **Supervisor:** Donal O'Mahony

Motivation

- Web 3.0 movement
  Building a new decentralised web
- Global surveillance
- Security concerns with current applications
  Centralised servers and no anonymity
  Compromising information leaked from metadata

The Chat Application

- Supports direct and group messaging
- Decentralised Peer-to-Peer network
- Conceals a user's identity
- End-to-End encryption
- Uses Whisper messaging protocol

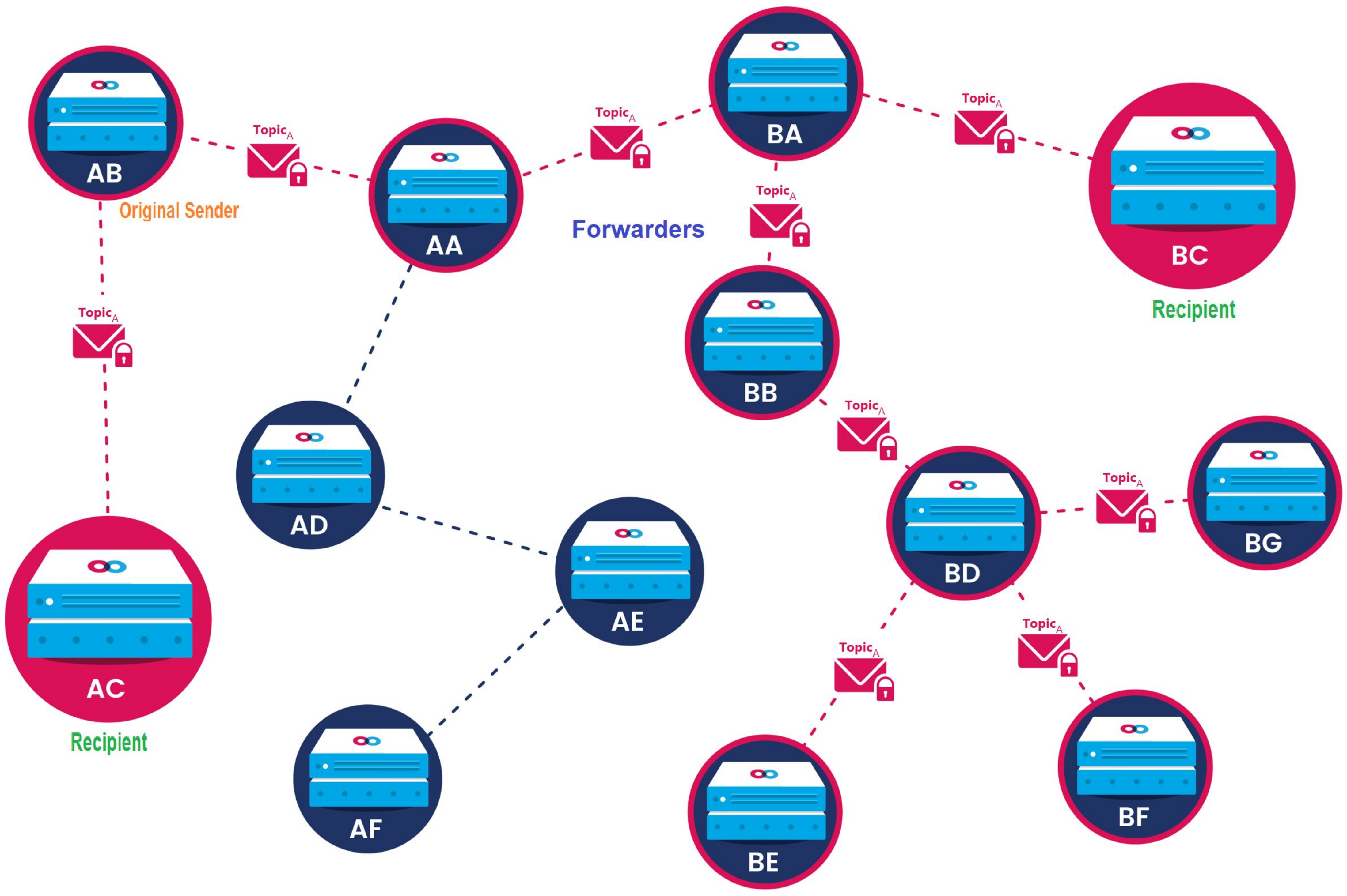
Application Features

- Backward and forward secrecy
- Spam prevention from proof of work
- Achieves *darkness*

> *"A truly dark system is one that is utterly uncompromising in information leakage from metadata."*

How does it Work?

1. Messages are broadcast to the entire network
2. Nodes continuously receive and forward on messages (even if intended recipient)
3. Identity of original sender and recipients is unknown to forwarder nodes
4. Must have decryption key to view message



B.A.(Mod.) Computer Science

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin