Problem: How to provide robust, anonymous communication which is resistant to traffic analysis and DoS attacks?

Existing methods are prone to various types of traffic-analysis, and denial-of-service attacks; require mandatory generation of fake cover traffic between nodes, which cannot always be enforced.

Proposed solution in Ra:
The Ra Anonymizer protects recipient anonymity using the following techniques:
- **Secret sharing** for creating multiple, redundant shares, which are sent along different paths. A subset of the shares are sent to the destination; the other shares are sent to random destinations
- **Probabilistic dropping** allows intentional dropping of shares at random nodes along the route
- **Probabilistic forwarding** is used at the real destination; it randomly forwards some of the received shares to scapegoats

Messages are layer encrypted using onions in typical mix-network fashion

Advantages
1. Sending shares via multiple routes increases protection against denial of service attacks on nodes the route 2. Sending to fake recipients provides cover traffic 3. Probabilistic forwarding prevents most types of traffic analysis attacks 4. Probabilistic dropping increases anonymity set and prevents timing attacks

Applications
Ra can be used for sending sensitive messages where the recipient identity needs to be secret (anonymous email, transactions, etc.) It can also be integrated over existing mix-networks with minimal change

Current status: Work in progress, implementation and security analysis phase

An example scenario