Introduction

Goal:
- Allow residents in urban areas to make resources available to their neighbours through auctions over ad hoc networks.
  - Develop a suitable protocol.
  - Implement the protocol in an example application that allows users to make their parking spaces available to other road users when they are not in use.
  - Extend the protocol to allow the use of social network information to bias the auction.

Background:
- High prevalence of smartphones allows for the spontaneous creation of ad hoc networks in populated areas.
- People in the same location often share a common interest or goal.
- Combining these two ideas allows us to unite people to achieve their goal.

Biased Auctions

Auctions can be biased in favour of friends of the auctioneer.

Why?
- Encourages them to participate in the auction.
- Auctioneer may trust them more than other bidders.
- They may make other resources available through biased auctions themselves.

How?
- Share social network information through a new middleware, Yarta.
- Other applications store information about who an auctioneer knows.
- We can leverage that information to identify friends.

Protocol

Announcement

Seller announces auction. Interested parties reply.

Encrypted Bidding

Bidders send encrypted bids to the auctioneer.

At end of bidding auctioneer shares list of accepted bids.

Key Sharing + Winner Determination

Bidders flood their keys to the network.
Each participant makes independent decision on the winner.

Settlement

Auctioneer settles with a bidder and broadcasts winner to network for transparency.

Challenges

- High mobility of nodes presents communication and consistency challenges.
- Ad hoc network presents opportunities for bidders to act dishonestly.
- Seller cannot be trusted to run a fair auction.
- Vehicular ad hoc networks can span large geographical areas.

Results + Contribution

- Developed a hybrid network architecture with centralised and decentralised components.
- Developed a protocol suitable for urban areas with highly mobile nodes.
- Employed symmetric cryptography to prevent the seller from cheating and asymmetric cryptography for authentication and to ensure bidders do not act maliciously to gain an advantage.
- Implemented protocol in a sample Android application.
- One of the first mobile applications to use the Yarta middleware to share social data between applications.

Further Information

- Contact Information
  - Email: postgraduate@scss.tcd.ie