

Contessa at Penn December 2003

Carl A. Gunter
University of Pennsylvania

Overview of Projects

- Secure and Open Embedded Devices
 - Designing software for smart cards
- Models and protection measures for DoS
- Secure Routing
 - Management protocols for IPSec
 - Secure web services and workflow
 - Power-aware routing
- Privacy
 - Location-based services

Software for Smart Cards

- OpEm Project: Open APIs for Embedded Systems
 - Flexible extensions support interoperation
- PISCES: Protocols and Implementation for Smart Card Enabled Software
 - Middleware to address limitations
 - Security analysis techniques

Models and Protection for DoS

- Models needed to improve analysis techniques for DoS
 - Quantitative assessment is essential
 - Current models too conservative
- New protection measures can be discovered given better models
 - Selective verification
- Probabilistic techniques

Management Protocols for IPsec

- IPsec tunnels in widespread use for road warrior applications
- IPsec key exchange protocols in limited use, but revisions are on the way
- Potential for dynamic negotiation of security context is unsolved
- Our focus: formal requirements and design of configuration protocols

Secure Web Services and Workflow

- Security gateways can be built at higher protocol layers: security gateways and routing for web services
- Security for workflow is enabled
- Project aims to build a messaging system based on web services under a federated security framework
 - WSEmail

Privacy

- Define “use rules” for data collected on subjects
- Approach based on Digital Rights Management (DRM)
- Case study for Location-Based Services (LBS)
 - 802.11 sightings
 - Interrupt rights

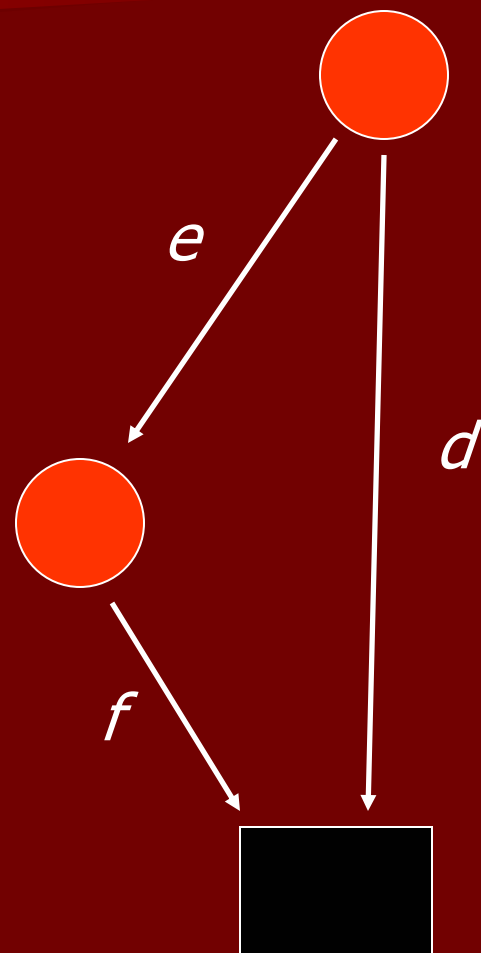
Focus Topic: Coalitions for Power Aware Routing

- Sharing between wireless nodes has well-proven benefits
 - Routing can yield two orders of magnitude in power savings
- Some sharing can be achieved by direct design
- Other sharing can be achieved by adapting to context and exploiting ad hoc opportunities for mutual benefit

Savings from Routing

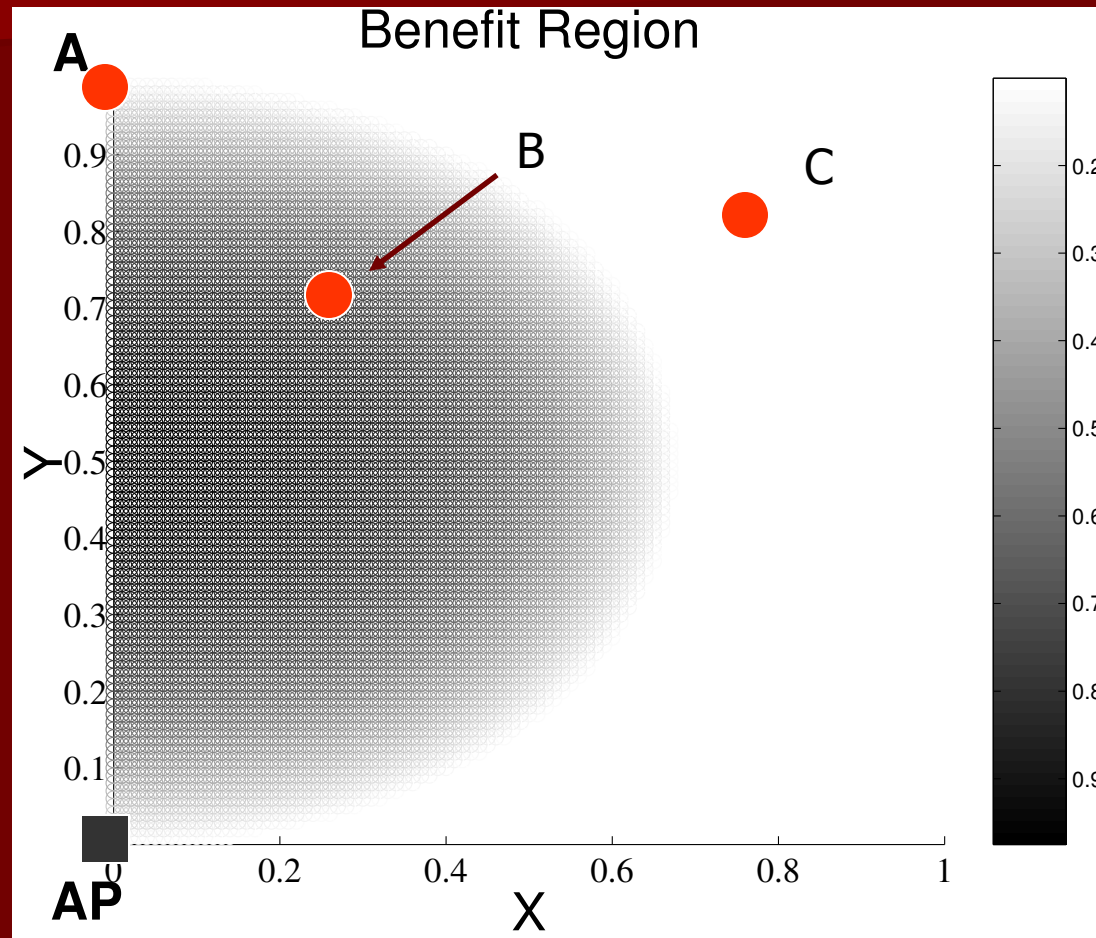
- Power costs for wireless transmission are proportional to a power of the distance over which the transmission must occur
- Transmitting a packet a distance of d is proportional to d^4

Example



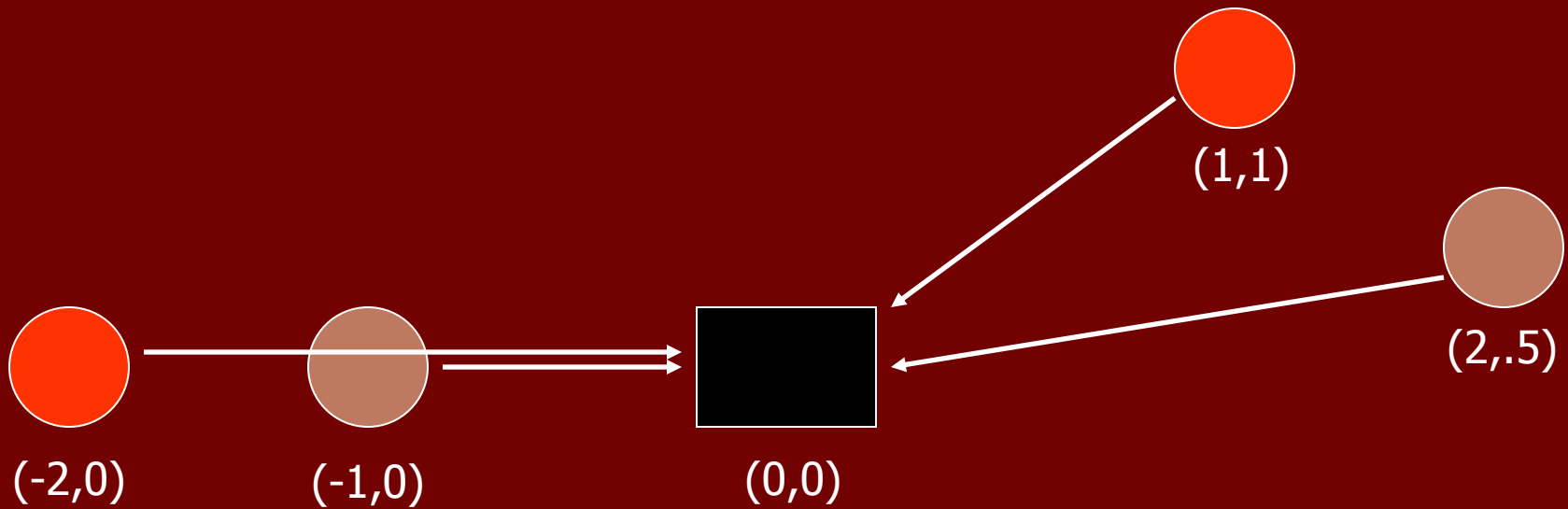
$$e^4 + 2f^4 < d^4$$

Benefit Region



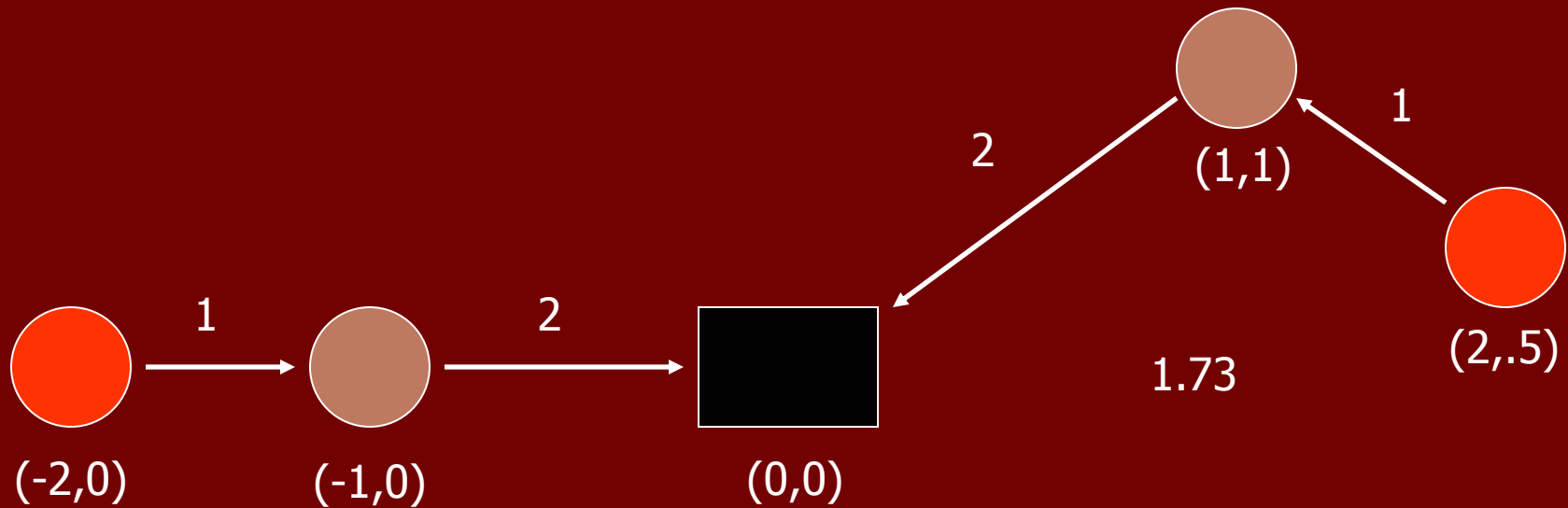
A benefits by routing through B but not by routing through C

Default Routing



Cost for red: 20
Cost for brown: 19

Optimal Power Aware Routing



Cost for red: 9
Cost for brown: 3.6

Benefit for red: $20-9=11$
Benefit for brown: $19-3.6=15.4$
Benefit for network: $11+15.4=26.4$

Coalitions

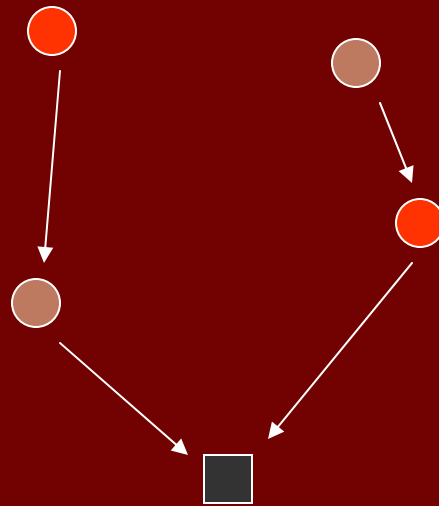
- Sharing between individual nodes may be beneficial because of a relationship between the nodes
 - Common owner
 - Common purpose
- Given a group of sharing nodes, when is it worthwhile to collaborate with another group?
- We refer to a sharing arrangement between two or more groups as a *coalition*

Coalitions do Not Benefit Pairs of One-Member Groups



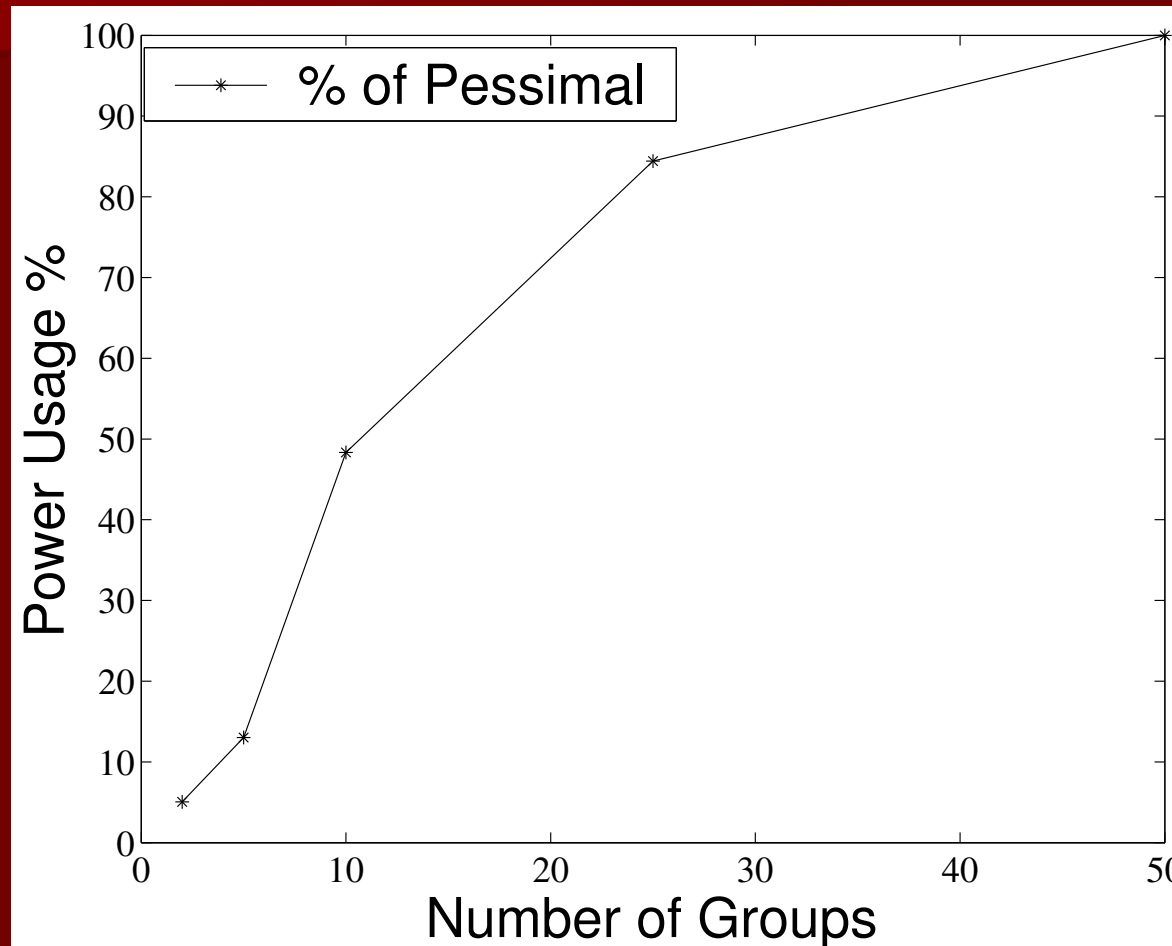
Only the red group can benefit from shared routing!

Multi-Member Groups May Benefit from Coalitions



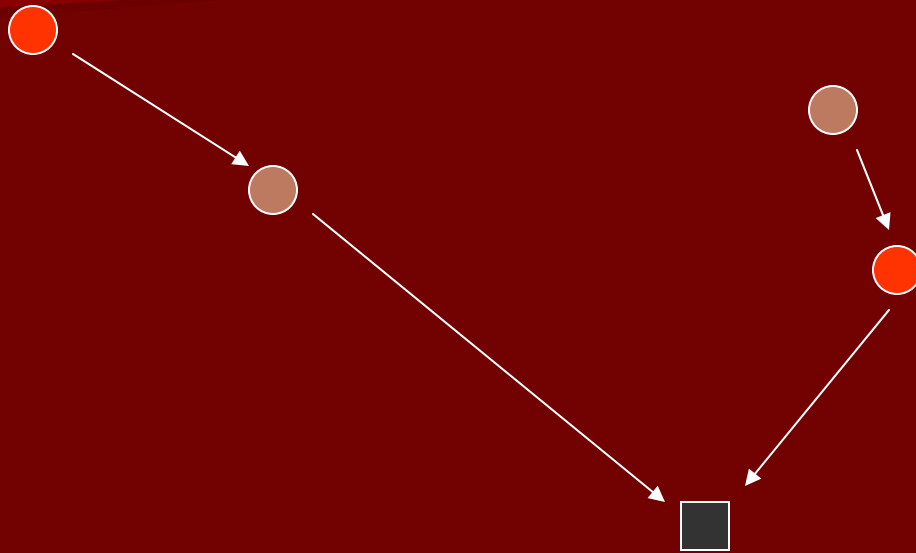
This routing allows both groups to benefit from shared routing.

This Benefit Can Be Substantial



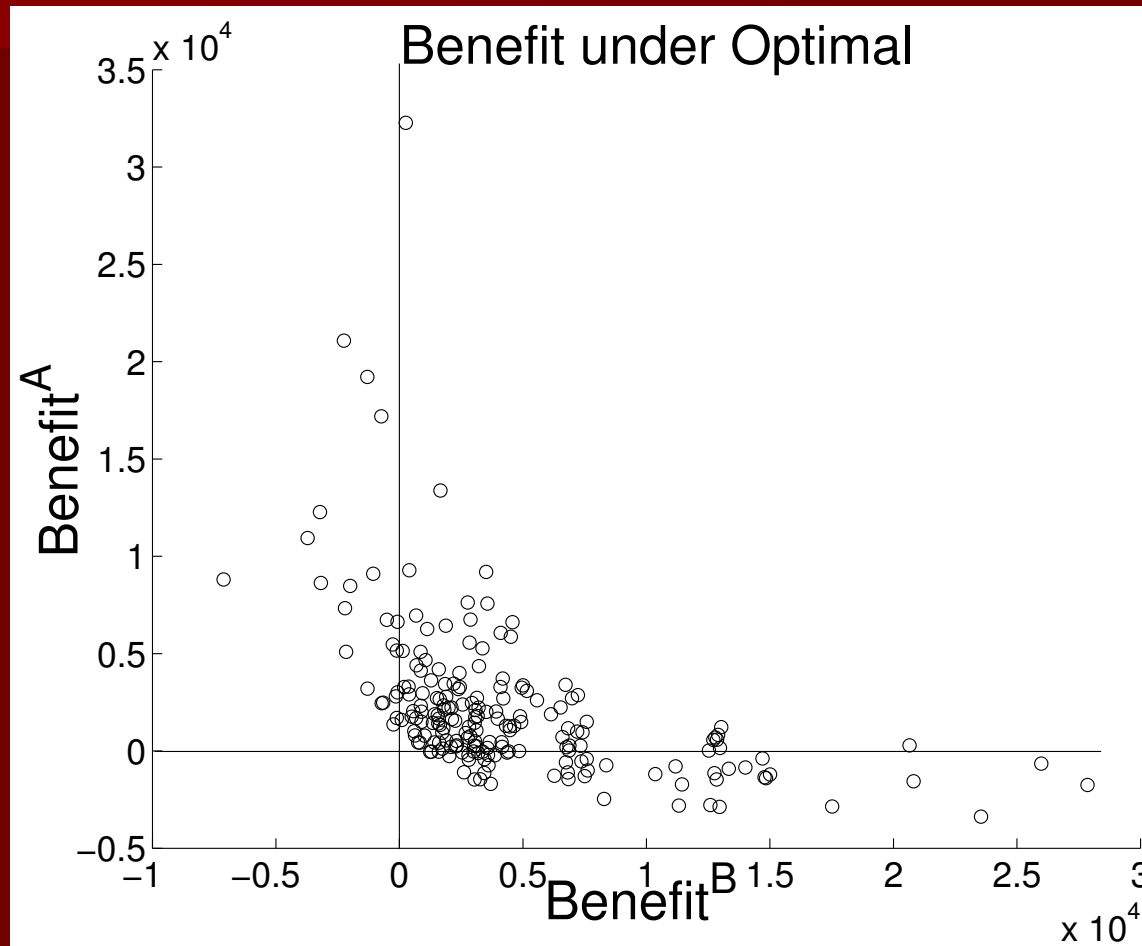
50 nodes randomly located and randomly formed into groups

But it May Not be Equal



This routing allows both groups to benefit from shared routing, but the red nodes have more opportunity to benefit.

Optimal Routing Provides Greatest Benefit to the Network at the Expense of Fairness



Units are in watts. Each axis represents the benefit for a group

But What is Fair?

- How should groups that can benefit from forming a coalition share the mutual benefit?
- Approach: use *max-min fairness*, an idea from fair routing developed for wireline networks.

Max-Min Fairness

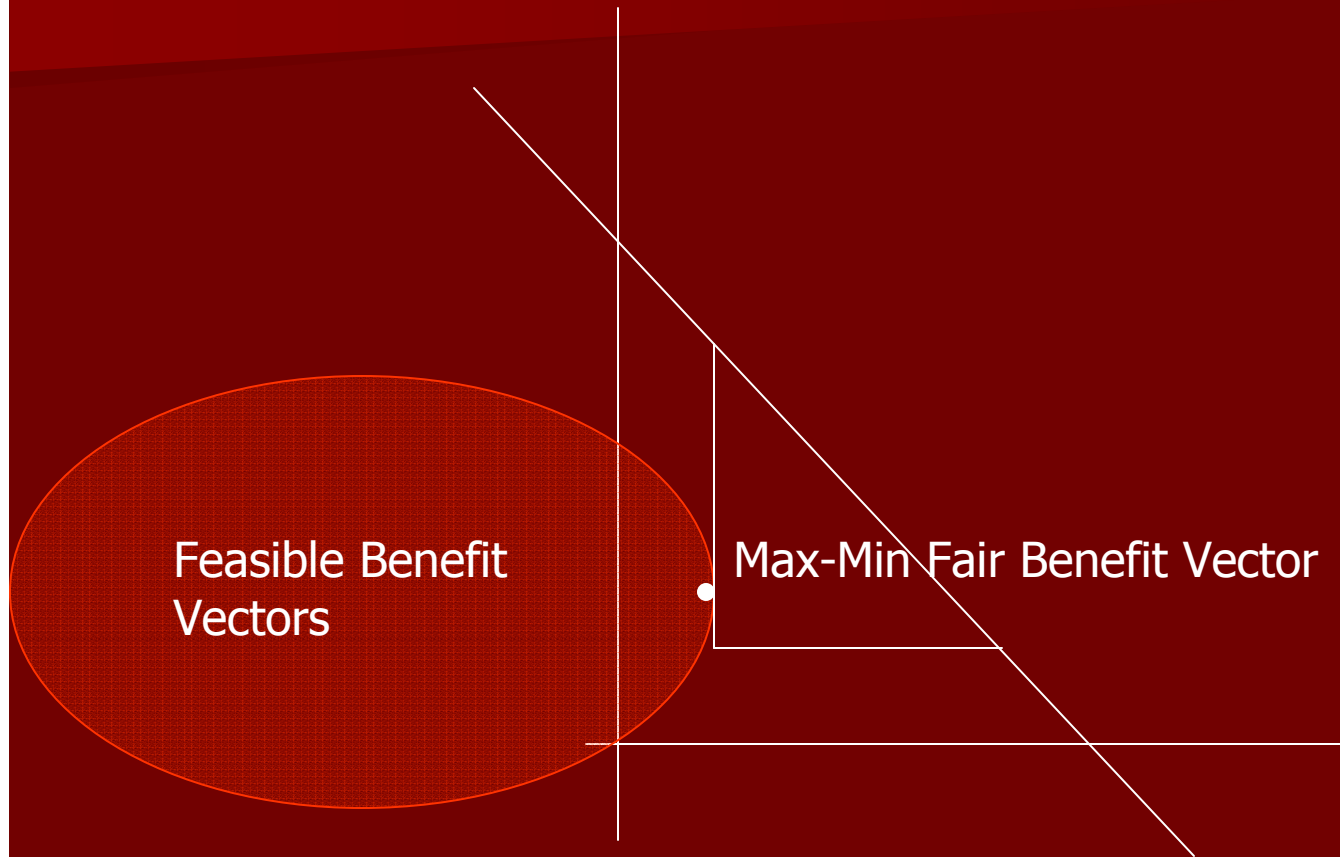
- A *benefit vector* is a pair (x_1, \dots, x_n) where x_i is a benefit to party i .
- A benefit vector is *feasible* if it can be realized by a possible sharing.
- A feasible benefit vector (x_1, \dots, x_n) is *max-min fair* if for each i , x_i cannot be increased while maintaining feasibility without decreasing x_j for some j for which $x_j \leq x_i$.
- A *fair coalition routing* is a routing that induces a max-min fair benefit vector.

Theorem

The following properties hold for fair coalition routing for any collection of groups:

1. There is always a unique max-min fair benefit vector.
2. This vector can be calculated efficiently using linear programming techniques.
3. When there are two groups the components of the benefit vector are equal.

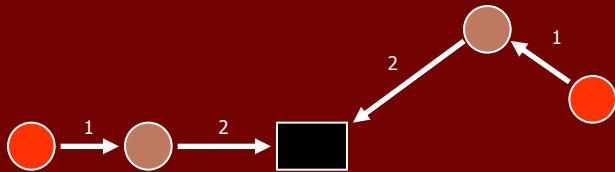
Max-Min Fair Geometry



Fair Coalition Routing

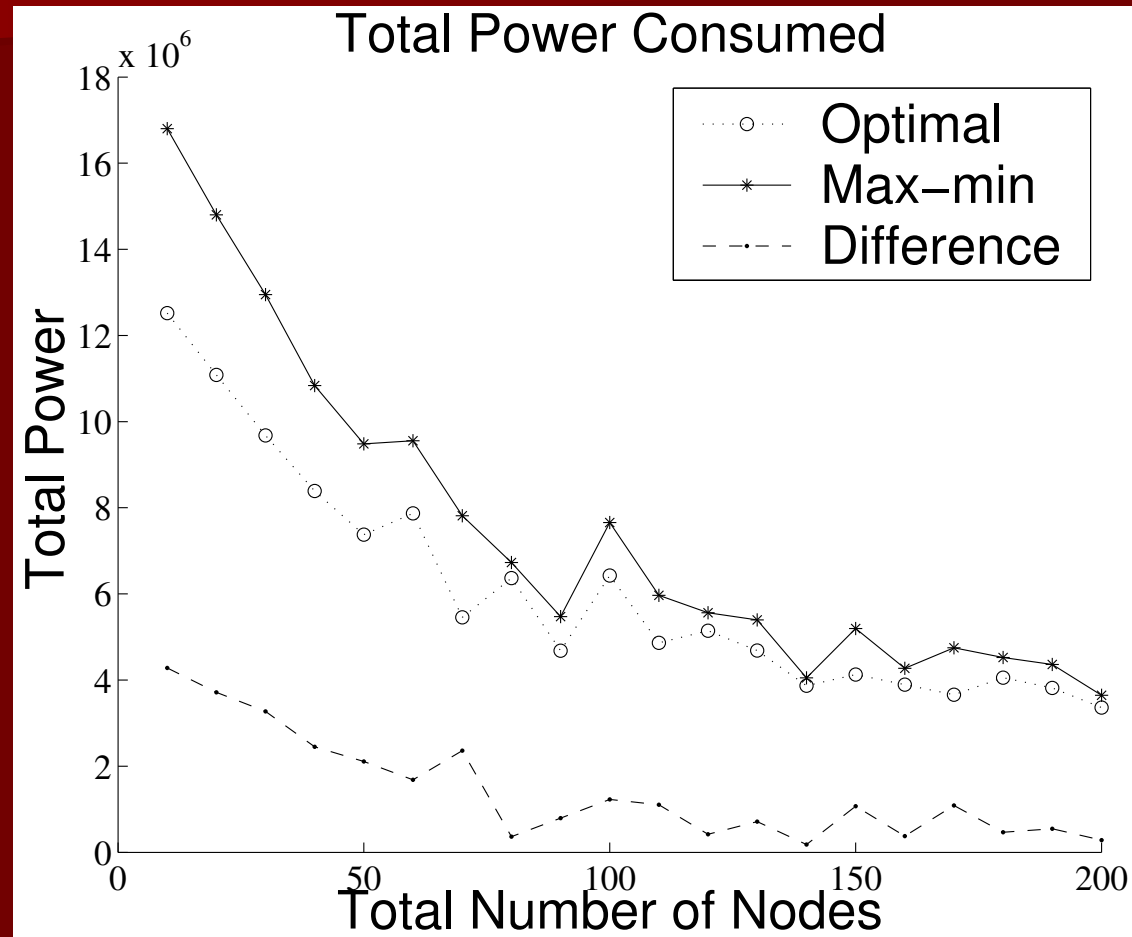
Cost for red: 9
 Cost for brown: 3.6

Opt Benefit for red: $20-9=11$
 Opt Benefit for brown: $19-3.6=15.4$
 Opt Benefit for network: $11+15.4=26.4$



Fair benefit for red: 11.9
 Fair benefit for brown: 11.9
 Fair benefit for the network: 23.8
 Cost of fairness: $26.4-23.8=2.6$

How Much Does Fairness Cost?

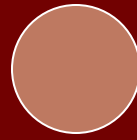


Average cost is 18% compared to the average benefit of 46%

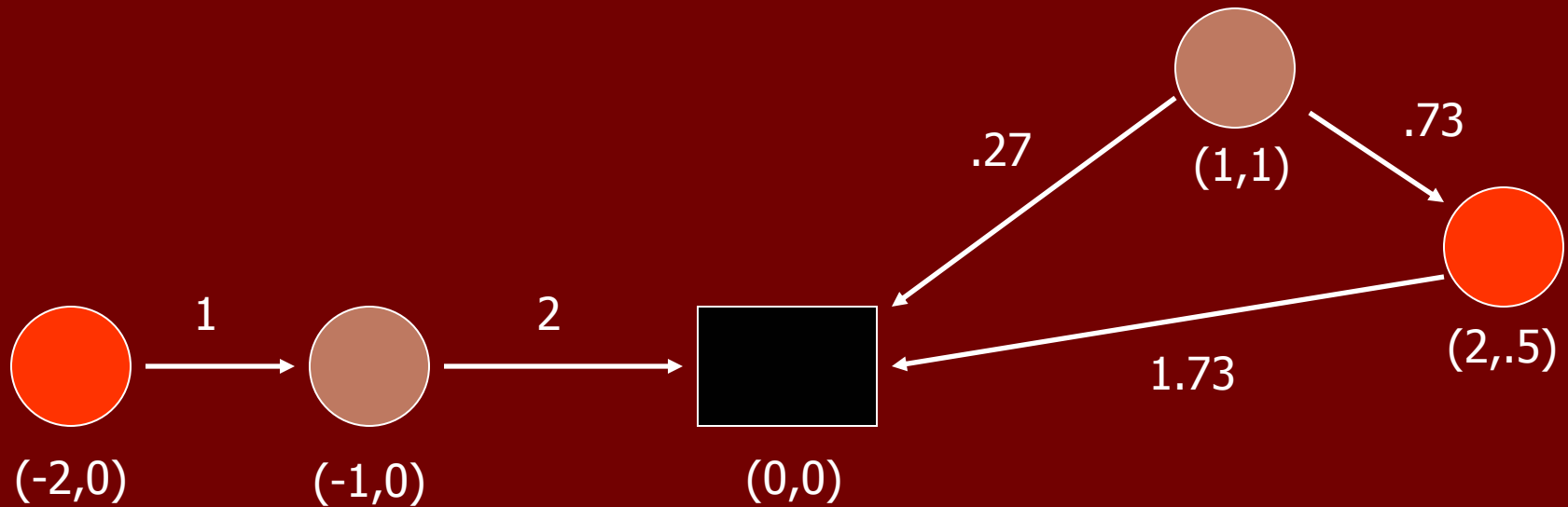
Two Counter-Intuitive Observations

- There are instances where three groups can form a beneficial coalition even when no pair of the groups can.
- Fairness sometimes entails routing away from the access point.

Three but Not Two

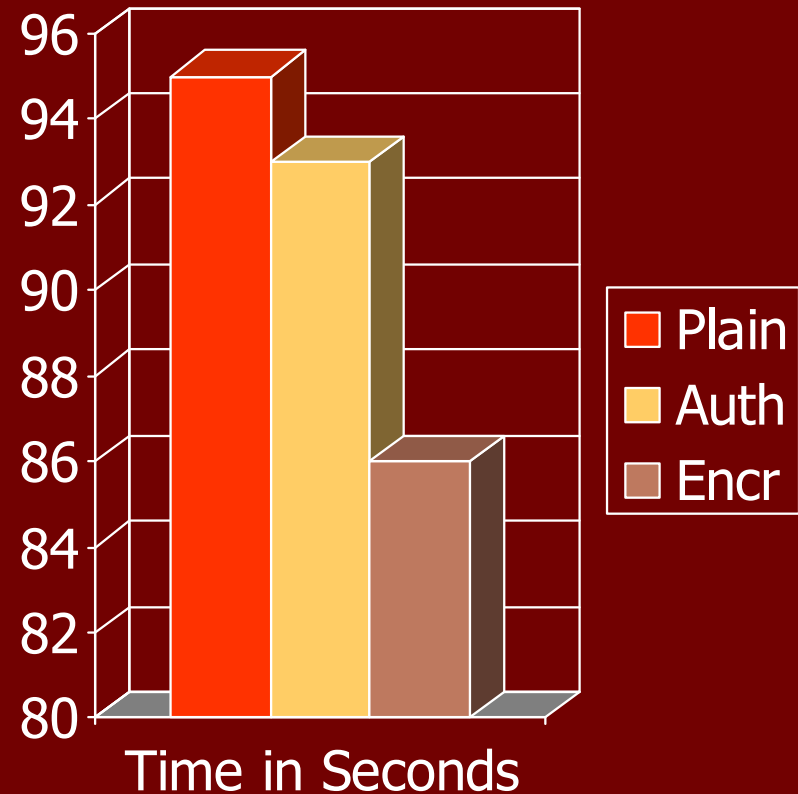


Routing Away from the Access Point



Trust Issues

- Groups must be able to economically enforce routing for their members and trusted coalition partners.
- How much does this cost?
- Experiment with IPSec on laptops



Future Work

- Negotiation and middleware.
- Mobility (incremental re-routing).
- Families of sensors.
- Other forms of sharing
 - Memory