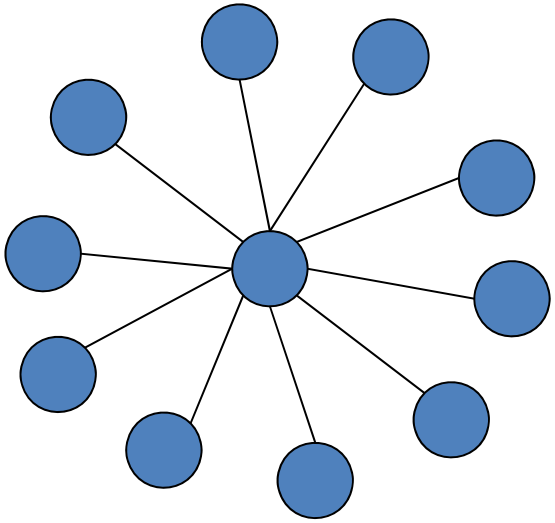
Network Resilience



Sanjeev Goyal

Christ's College

University of Cambridge

Indian Institute of Science

Bangalore

1. Introduction

Connections between individuals facilitate exchange of goods, services and information but are costly to set up and may expose nodes to threats faced by others.

Examples:

Transportation: node/link failure blocks flows.

Crime: capture of node triggers others…

Computer networks: viral attacks/botnet herders.

Finance: links smooth shocks, systemic risks.

Epidemiology: vaccination and interaction

Modelling Issues

Three dimensions

- Nature of shocks: *strategic vs. random*
- Nature of attack: *contagion vs. static*
- Decisions*: centralized vs. decentralized*

Capture different applications… and trace out an ensemble of models.

Examples

	Random attacks	Intelligent Adversary
Planner/ Designer	Infrastructure vs. nature	Criminal gangs vs. police Infrastructure
Decentralized choices	Vaccination vs. virus Inter-bank networks	Airports vs. terrorists Computers vs. hackers

Research Questions

1. Optimal attack strategy: who to target.
2. Network design to minimize damage.
3. Random versus strategic attack
4. Optimal defense & network design.
5. Centralized vs. decentralized decisions: trade-offs and role of policy intervention.

Planner's Problem Framework

- Two players: a *network designer D* and an *adversary A.*
- Designer chooses network and defence on nodes.
- Attack: Adversary observes choice, allocates attack resources. Alternative: random attack.
- Technology of shocks: how shock affects a node and how it spreads via neighbours

Strategic adversary: study equilibrium of game of conflict
Random attack: study optimal networks and defence.

2. Defence, attack and design

Dziubinski and Goyal 2011

- Two players: The Designer (D) and the Adversary (A).
- Stage 1: Designer chooses network and defence. One link costs L, defence of a node costs F.
- Stage 2: Adversary attacks nodes; budget is K nodes.

- Conflict technology: node removed if & only if undefended.
- Residual network: g – X\d.

- Payoffs:
- Designer f(g-X\d) - |g|.C – d.F

  Adversary: -f(g-X\d).

Defence and Design
General Payoffs

- Payoffs from g is component additive:

$$\sum_{C_i \in C(g)} f(|C_i|)$$

- f is increasing and convex.

- Examples: connections model (Goyal 1993, Jackson and Wolinsky, 1996), trading, communication.
- Designer maximizes this sum *less* costs of links/defence
- Adversary seeks to minimize this payoff.

Equilibrium

Theorem

In equilibrium designer chooses either

-- 0 defence and empty, (k+1) connected network among others. OR

-- 1 unit of defence and star network with protected hub.

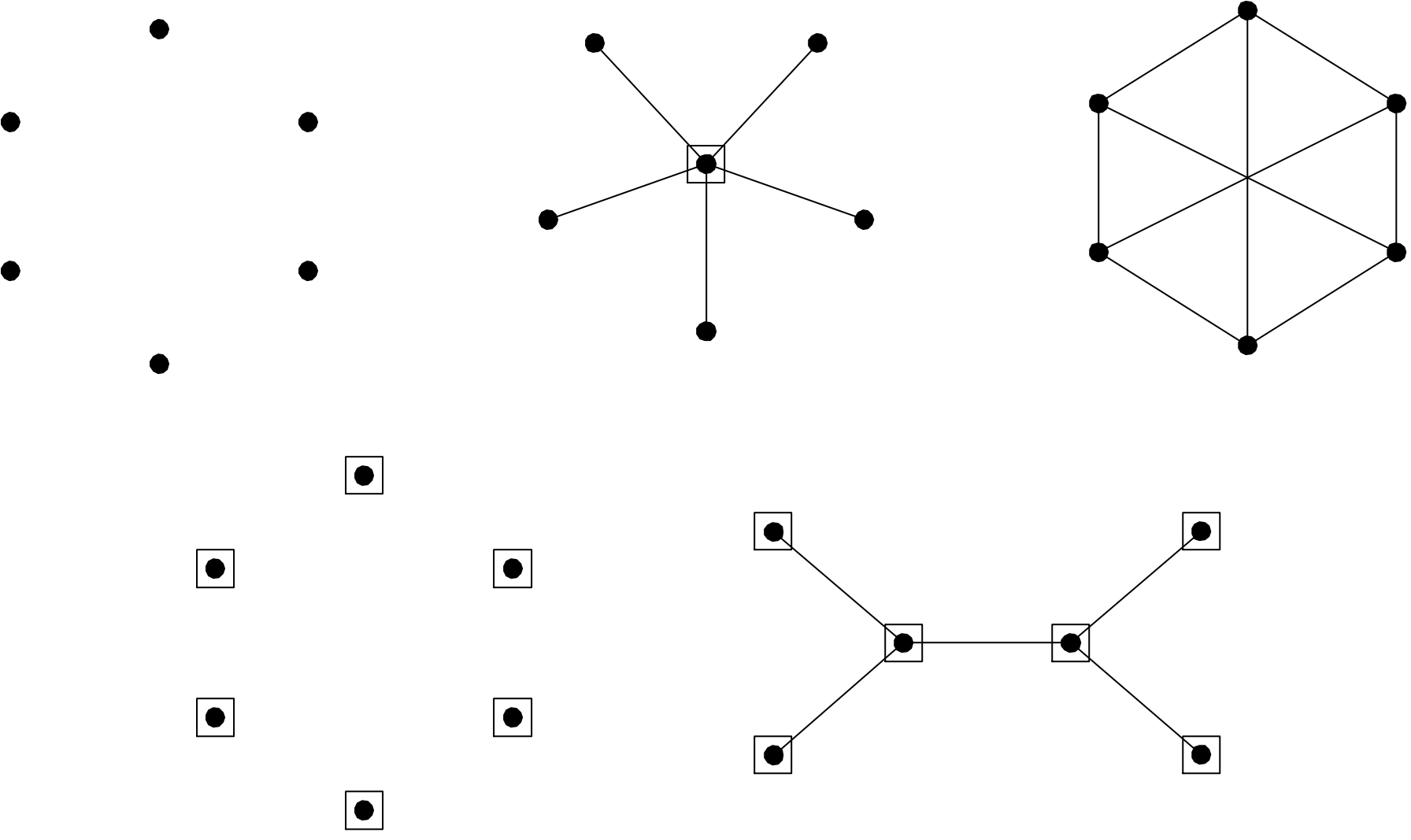
-- n units of defence and empty network or a tree.

Ideas:

0 defence: different networks arise, depend on costs of link

Intermediate defence unattractive: due to convexity of f(.)

In case of 1 defence: notice that single protected hub guarantees connectivity of residual network.



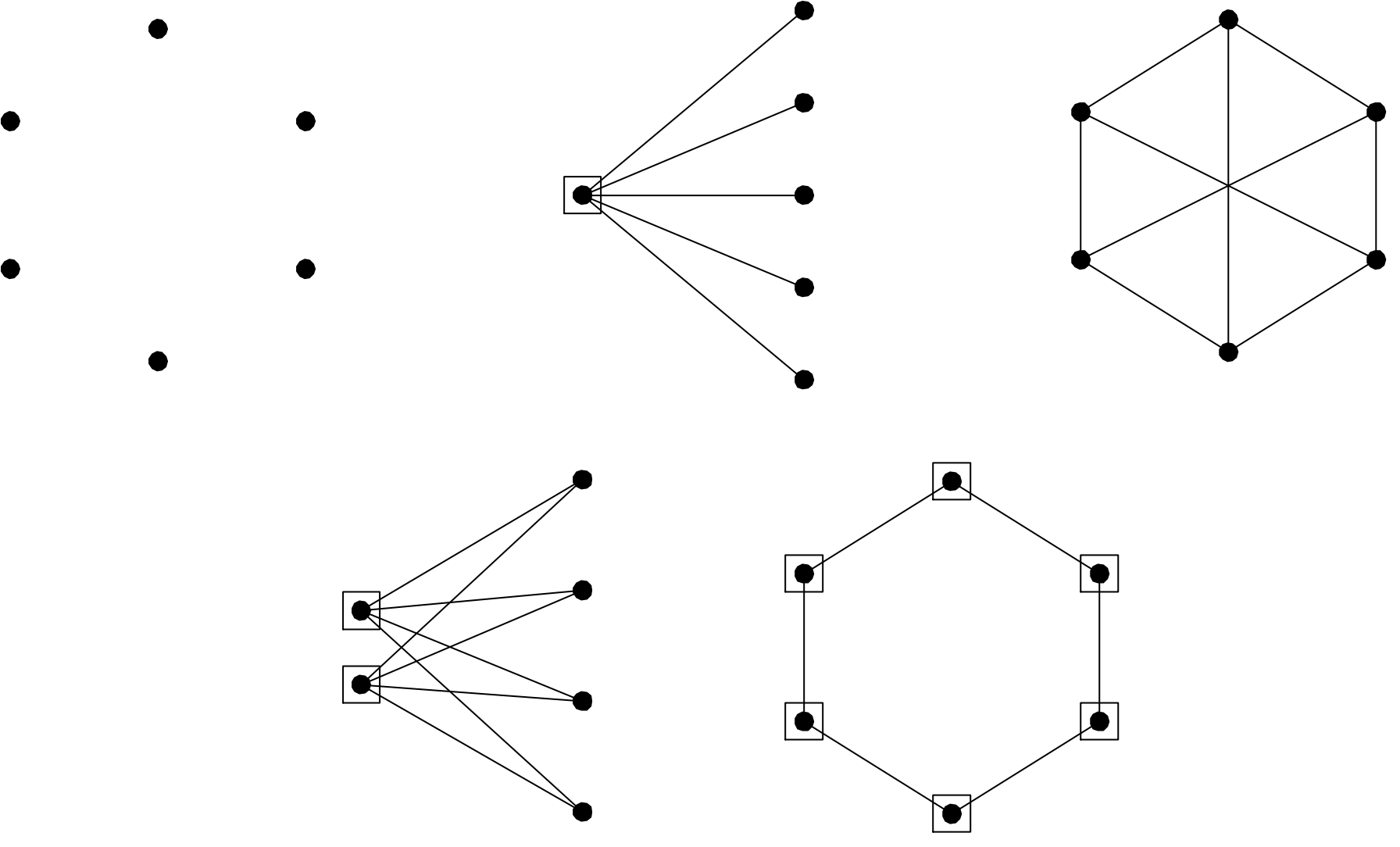
Imperfect defence

Probability P that defended node can be eliminated by attack. How do networks and defence depend on the value of P. This is a complicated problem.

- Two observations:

1. As defence becomes less reliable: optimal to protect multiple nodes and create bi-partite networks, with one side protected.

2. Richer defence and networks -- all nodes protected in a cycle network -- which trade off the costs of defence against the cost of linking, may arise in equilibrium.



Summary

In a setting with costly linking and defence and no contagion:

--- if defence is affordable and reliable then resilient networks are sparse, have heterogeneous linking, a few `central' nodes are protected.

--- if defence is costly then dense and homogeneous networks arise.

3. Contagion and Resilience

Goyal and Vigier 2010

Designer chooses network and allocates D units on network. Adversary allocates A units to attack the network.

Two new features:

1. Contests: Attack/defence probability of elimination
2. Contagion: attack spreads through links in network

Assumption A.1: Payoff to designer from network g is

$$\sum_{C_i \in C(g)} f(|C_i|)$$

where f(.) is increasing and convex.

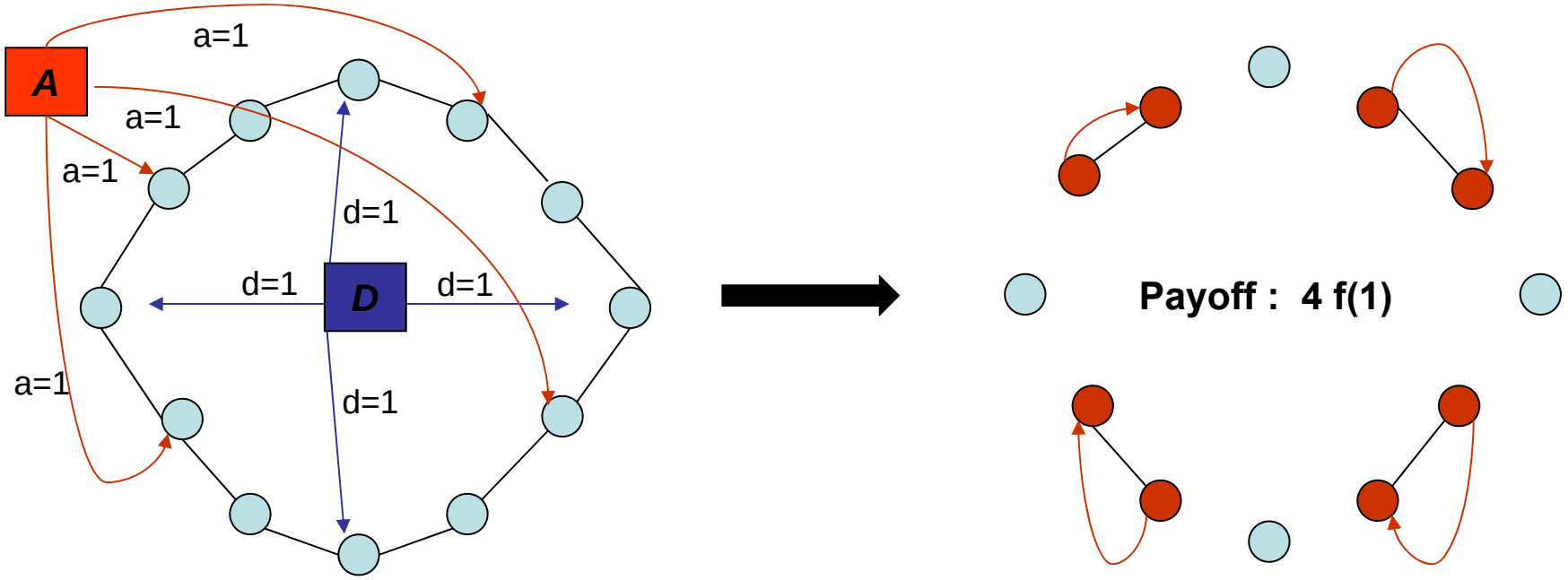
Contagion and Resilience
Contests and spread

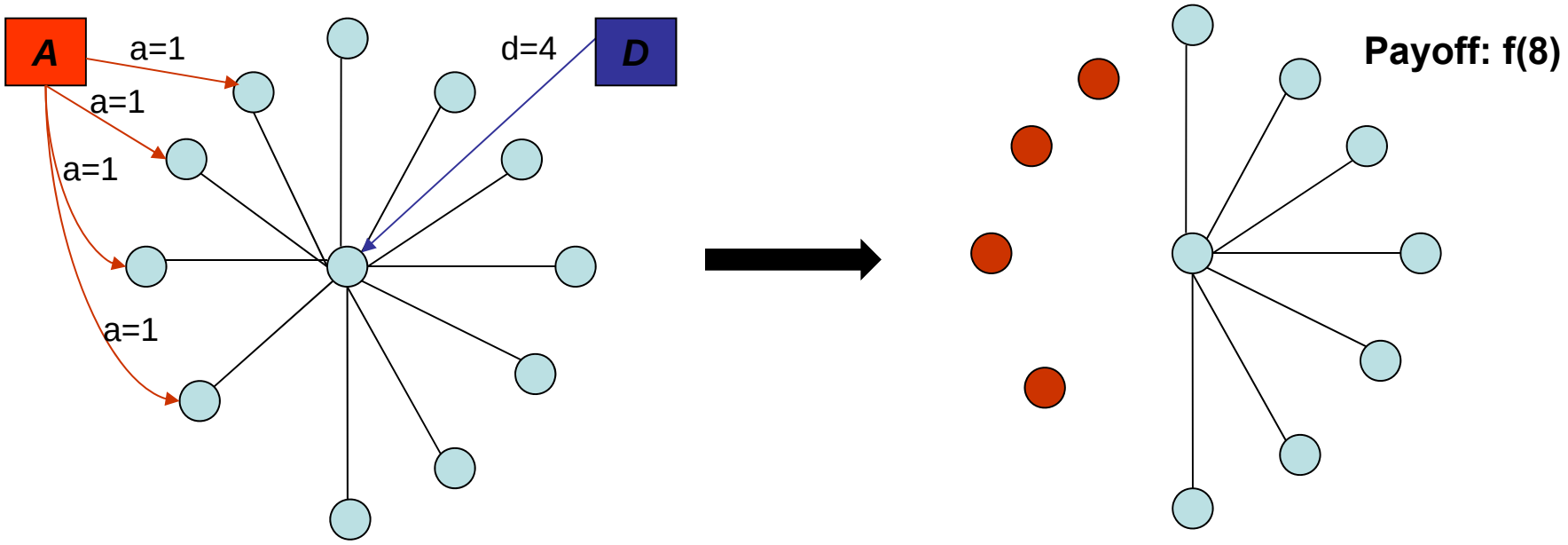
A canonical model of contests due to Tullock (1980):

Assumption A.2: Probability of successful attack on node *is increasing in attack and falling in defense allocation. Marginal returns from defense and attack are falling and symmetric.*

Assumption A.3: *Attack spreads across neighbors who are poorly defended.*

Threshold model: a path between *i* and *j* is *weak* if every node k on path has defense less than some threshold.


A
a=1
a=1
a=1
a=1
d=1
d=1
D
d=1
d=1
Payoff : 4 f(1)


A
a=1
a=1
a=1
a=1
d=4
D
Payoff: f(8)

Contagion and Resilience
Payoffs

Given a network ***g***, defence **d** and attack strategy **a,**

A.2 and **A.3** yield a probability distribution on networks:

$$P(g' \mid g, d, a)$$

The expected rewards to designer are:

$$\sum_{g'} P(g' \mid g, d, a) \sum_{C_k \in C(g')} f(\mid C_k(g') \mid)$$

We study zero sum games.

Pure Design Problem

Theorem

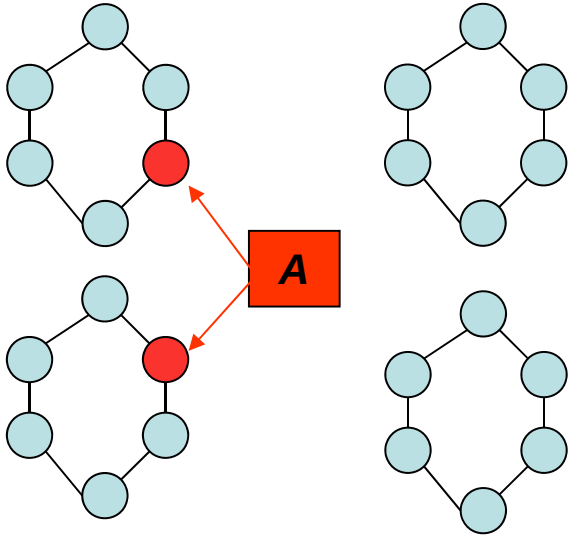
Assume zero defense budget. In equilibrium

-- *adversary targets at most one node in each component*

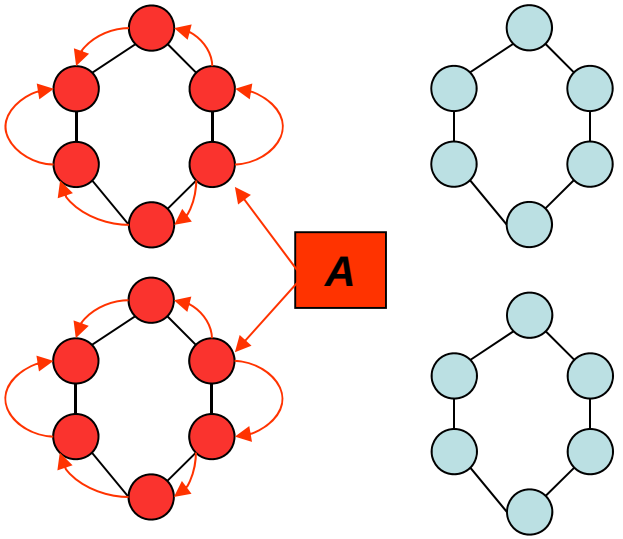
-- *Designer chooses network with equal size components*

-- *# components grows (and size falls) in adversary budget).*

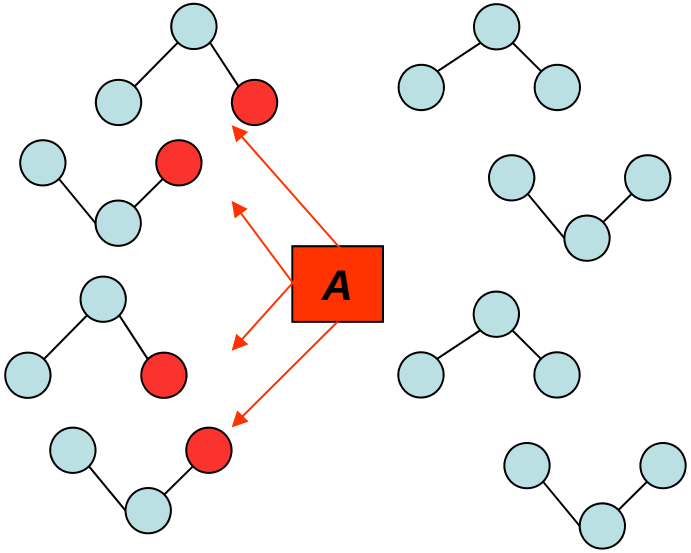
Remark: If attack is random, optimal network consists of fewer and unequal components.

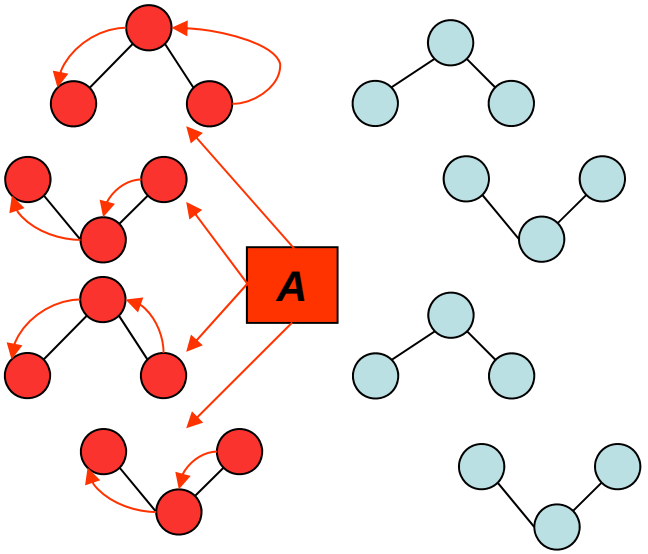


Effects:
adversary
budget

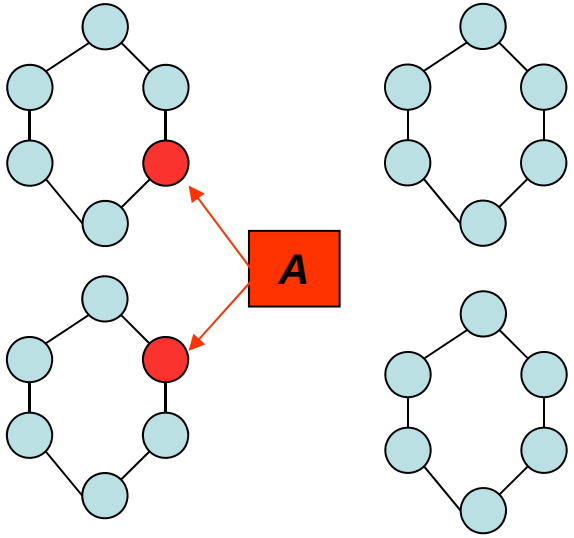


n=24 α=2 a=2: k=4

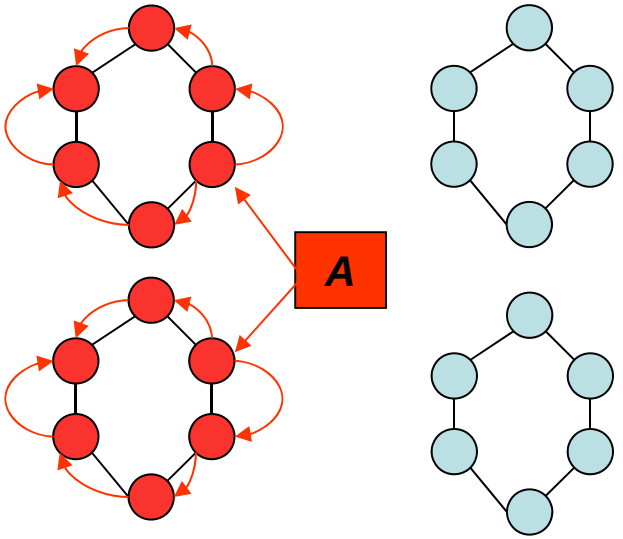




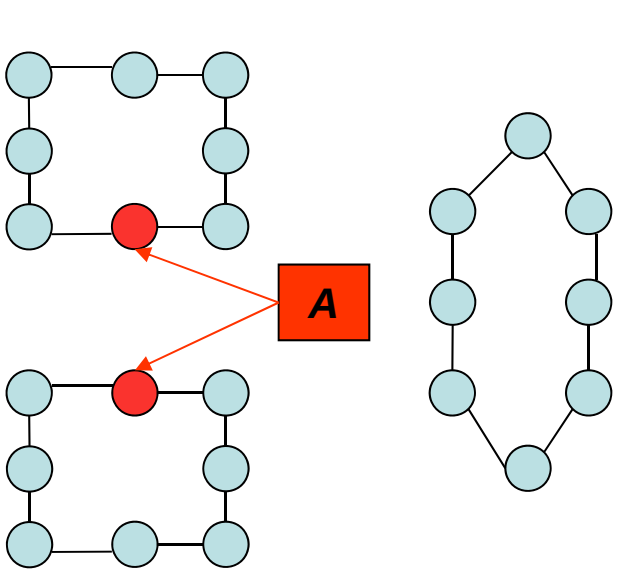
n=24 α=2 a=4: k=8

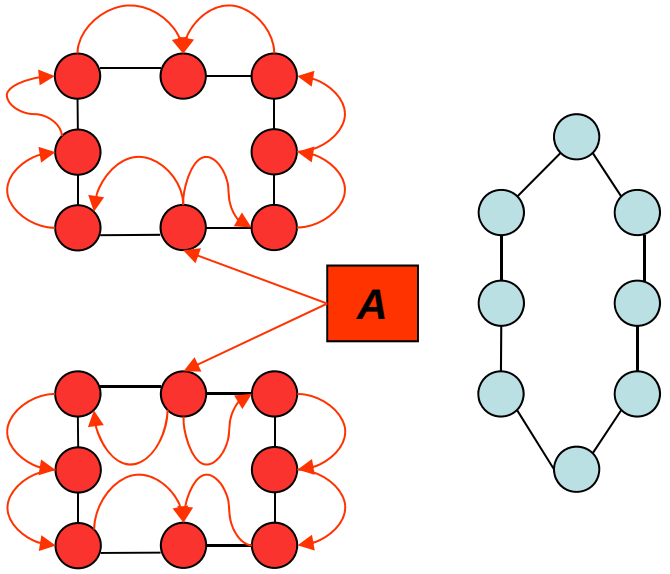


Effects of Convexity



n=24 α=2 a=2: k=4





n=24 α=3 a=2: k=3

Contagion and resilience

Random vs. strategic attack

Example: Fix a=1. Random attack q=a/n. Independent and identical across nodes.

As n gets large, optimal network is connected. Payoff to designer is

$$[1-1/n]^n = 0.38$$

Under intelligent attack resilient network contains two equal components and payoff is 0.25, irresp. of number of nodes.

Thus # components differ: 1 vs. 2.
Mistaking intelligent adversary for random attack leads to zero payoff!

Design and defence

Theorem

Suppose budgets of defense and attack are small relative to number of nodes. There is an equilibrium with

--- designer choosing a star network and assigns all defense to hub node.

--- adversary allocating entire budget to attack hub

Remark: when defence resources are large relative to nodes, dense network with dispersed defence is optimal.

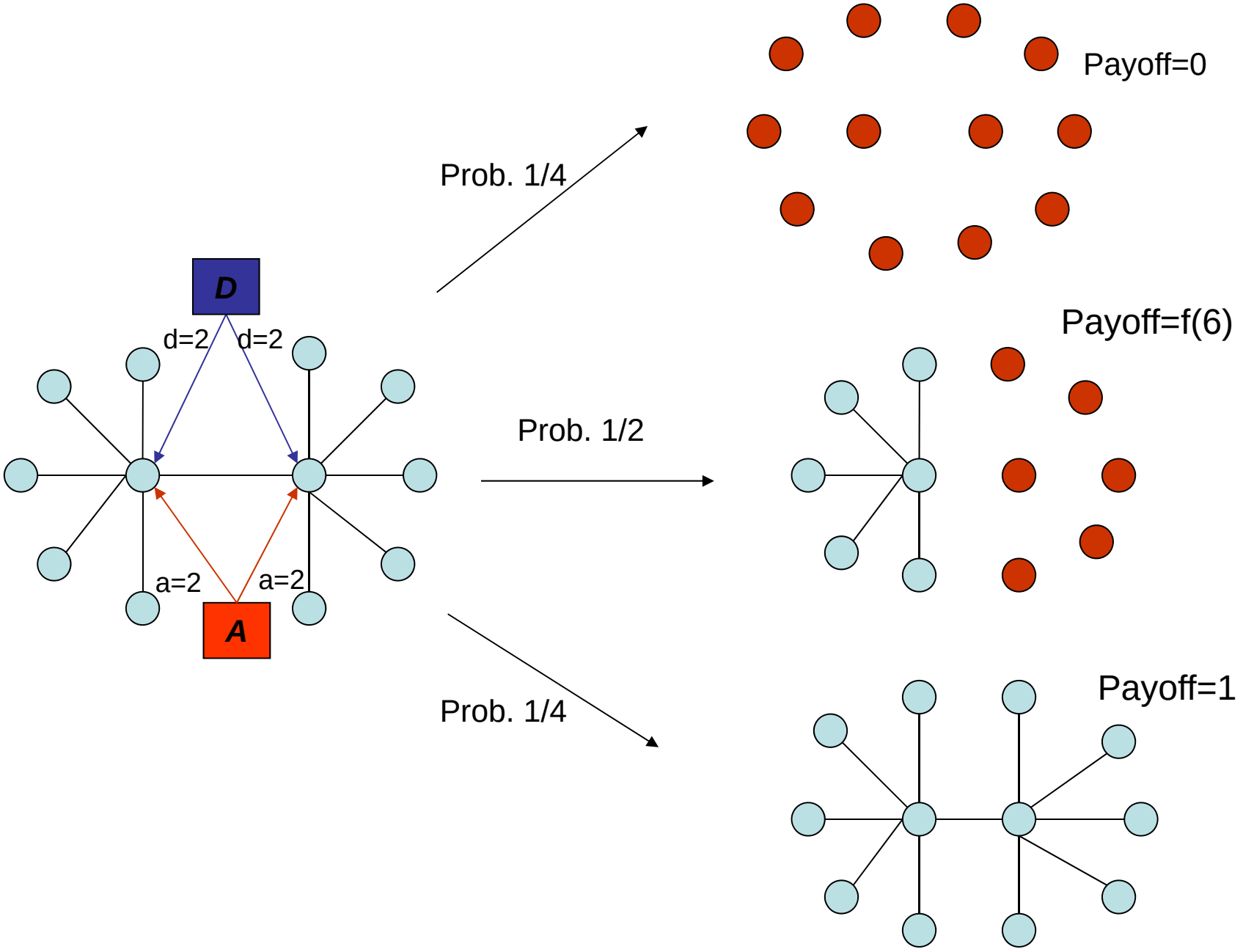
Proof: Ideas

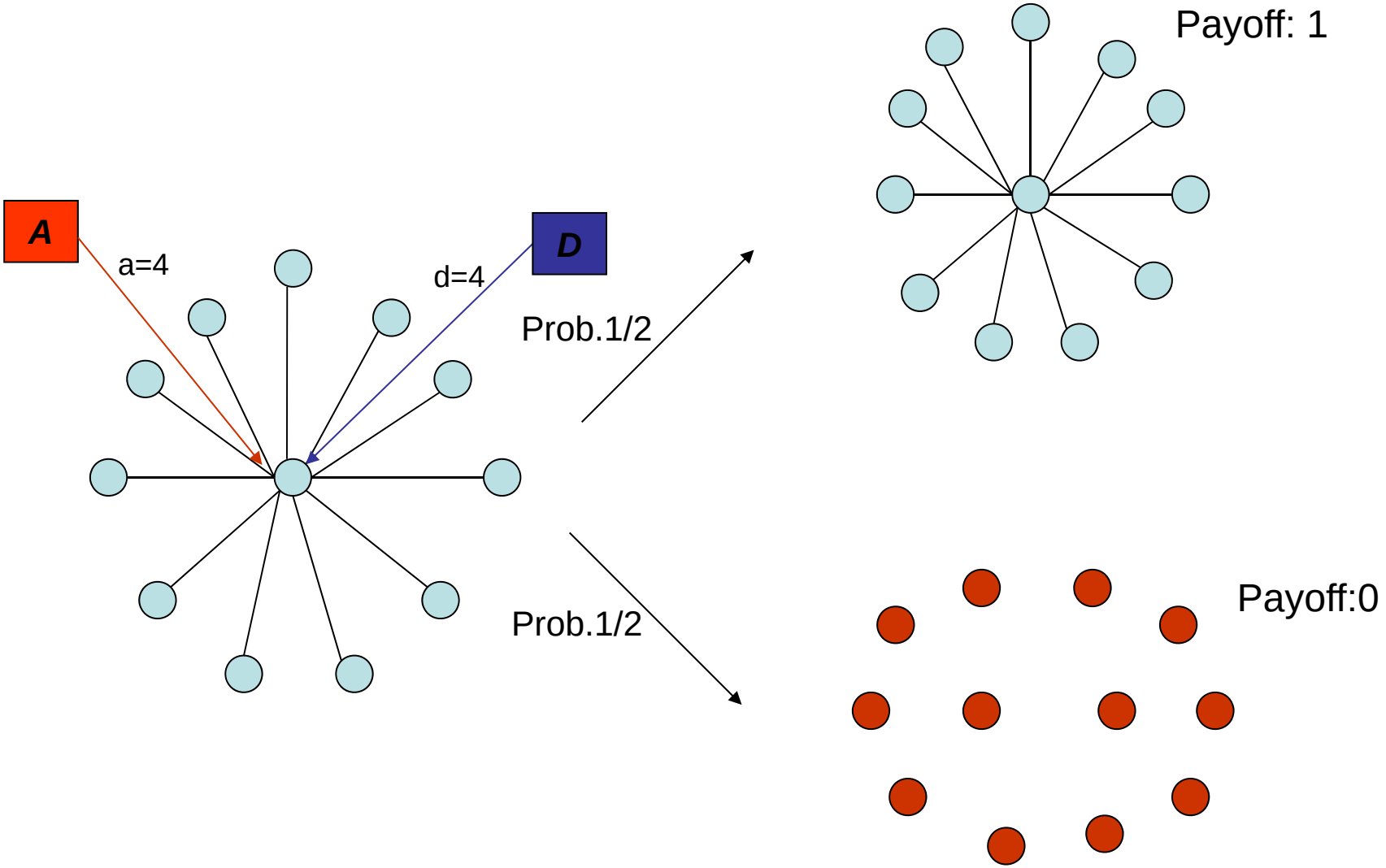
1. Protect and attack central node: convex f(.) and large n.
2. Payoff in star is bounded ***below by***

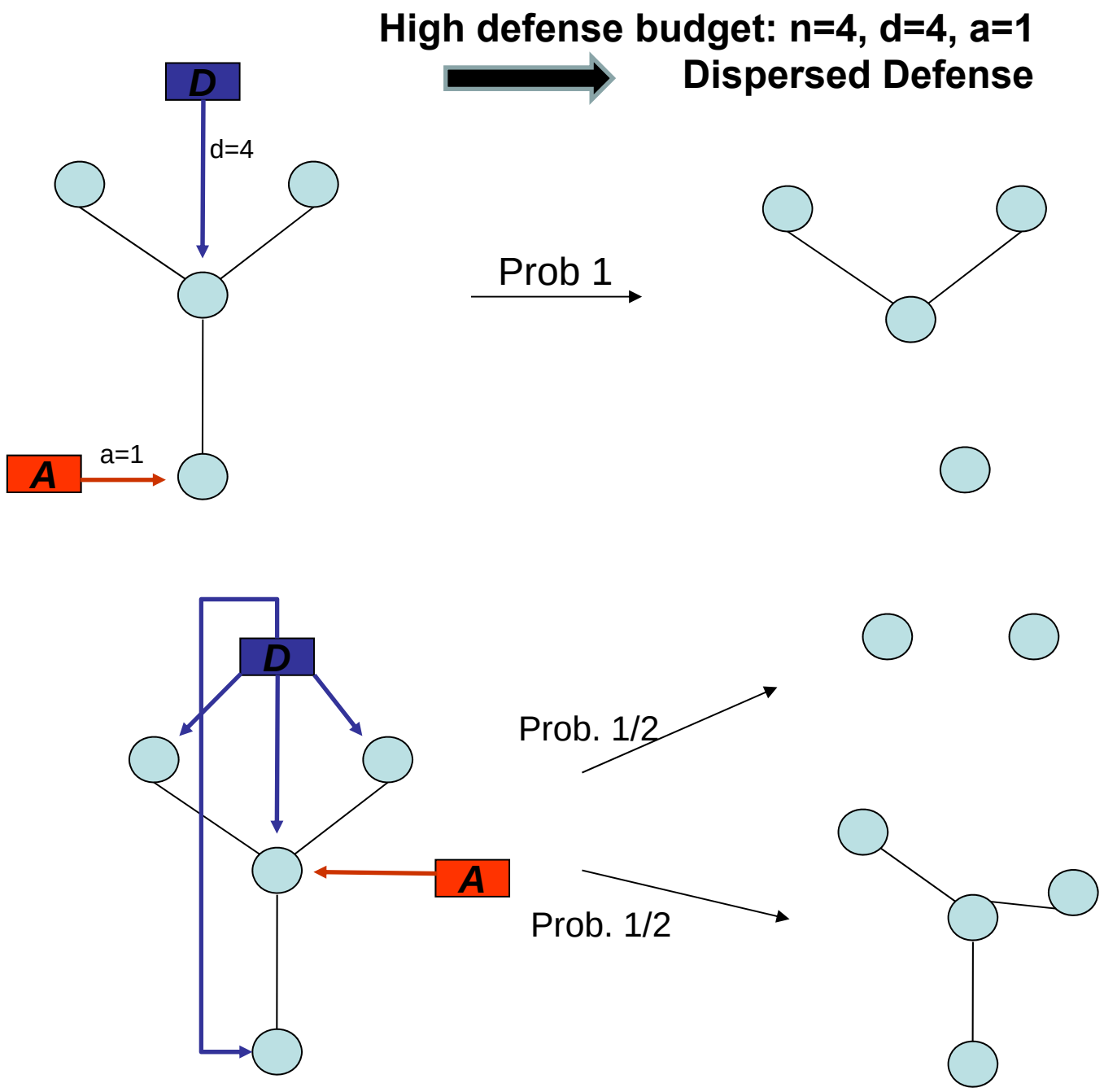
$$\chi = \frac{d}{d+(a-x)} f(n-x)$$

3. Single hub better than multiple hubs: many protected hubs allows adversary to mimic conflict in star.

   Key: distribution of surviving network is second order stochastically dominant relative to star. Since *f(.) is convex*, payoff bounded ***above*** by χ
4. K core-periphery network better than other networks with K protected nodes: minimizes attack contagion

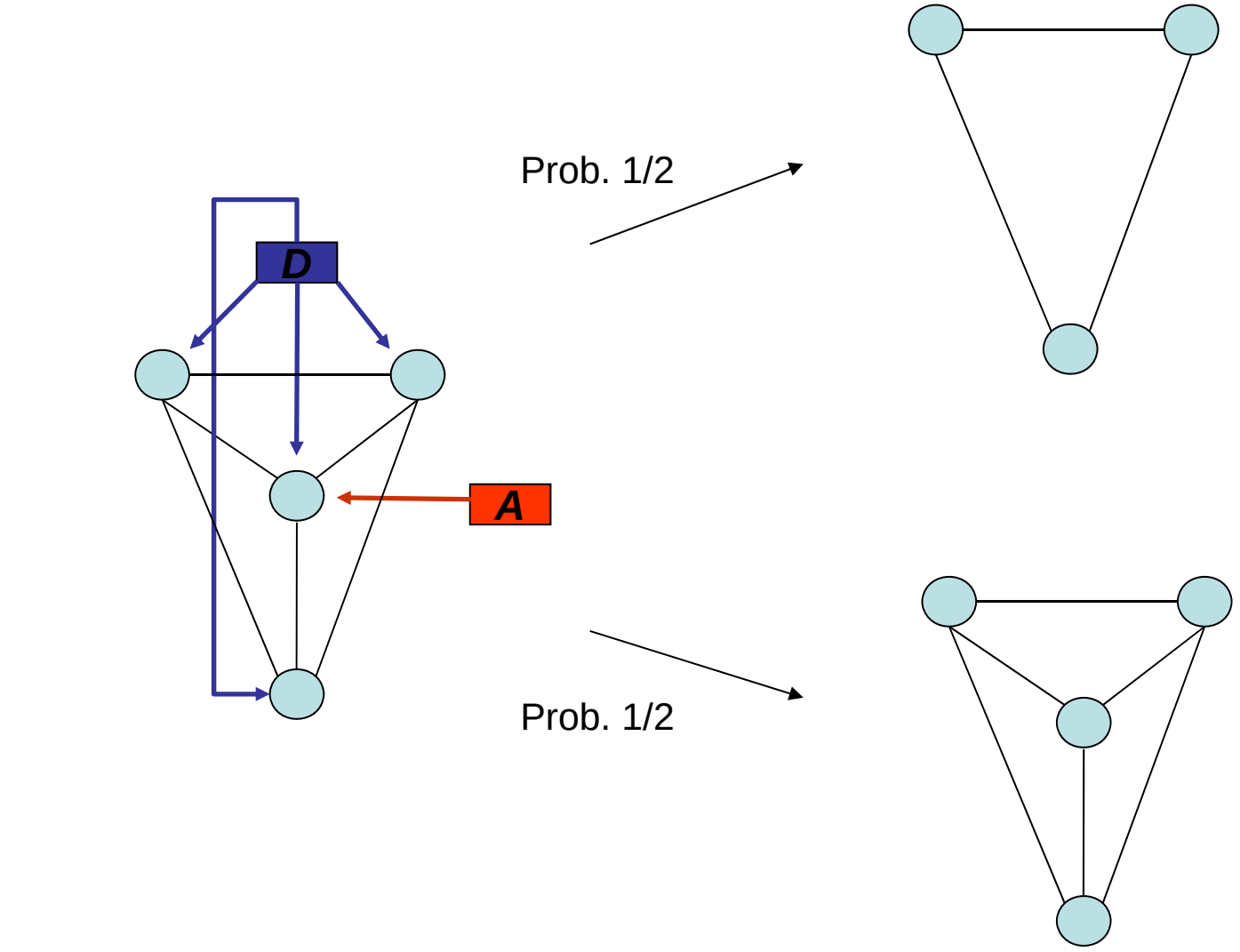

D
d=2
d=2
a=2
a=2
A
Prob. 1/4
Prob. 1/2
Prob. 1/4
Payoff=0
Payoff=f(6)
Payoff=1


A
a=4
D
d=4
Prob.1/2
Prob.1/2
Payoff: 1
Payoff:0


High defense budget: n=4, d=4, a=1
Dispersed Defense
D
d=4
A
a=1
Prob 1
D
A
Prob. 1/2
Prob. 1/2

High defense budget: n=4, d=4, a=1

Dense Networks



4. Concluding Remarks

Connections facilitate the exchange of goods, resources and information but links are costly and they also expose an individual node to threats faced by other nodes.

We studied research questions:

1. Optimal attack strategy: who to target
2. Network design to minimize damage.
3. Random versus strategic attack.
4. Optimally combine defense & network design

Summary

Compare optimal design with and without contagion

- Zero defense: dense connected homogenous networks optimal with no contagion; multiple components are optimal with contagion.
- Defended nodes: protected hub with heterogeneous and sparse networks in both cases.

5. On-going work

1. Competing for security: Higher security diverts attack to other nodes… and so individuals invest too much in security and exhaust all surplus.

Open problem: how does network location affect security choice? How does optimal centralized design compare to optimal design when security is decentralized?

5. On-going work

2. Decentralized security and linking: In many applications, agents form links and also choose security. E.g., Banks, social interaction, travel and vaccination.

Open problem: what is the emerging network and how secure are they? What is the role of public policy?

References

V. Bala and S. Goyal (2000), A strategic analysis of network reliability. *Review of Economic Design.*

S. Goyal and A. Vigier (2010), Robust networks.

M. Dziubinski and S. Goyal (2012), Network defence and design.

Y. Bacharach, M. Draeif and S. Goyal (2011), Competing for security

S. Goyal and J. Kovarik (2012), Network resilience: an empirical study

M. Baccra and H. Bar-Issac (2008), How to organize crime? *Review of Economic Studies.*

D. Kovenock and B. Roberson (2011), Conflicts with Multiple Battlefields.

Milind Tambe (2010), *Security and Game theory.*