

Analyzing the Incentives in Community-based Security Systems

Pern Hui Chia

Centre for Quantifiable Quality of Service in Communication Systems (Q2S), NTNU

SESOC 2011, Seattle, 21 Mar 2011

This talk is

~~not about security in social networks~~

about social networks for security

Outline

- Background
- Basic model
- Simulation
 - social expectation / influence
 - nice users & dynamics
 - community structure
- Limitations, Future Work & Summary

Background

- Community-based Security System (CSS)
 - PhishTank
 - collator of user reporting and voting against potential phishing sites
 - Web Of Trust (WOT)
 - reputation system for trustworthiness / security / privacy of domains
- Benefits: advantage of scale, law of large number, catering user needs
- Concerns: reliability, economic feasibility, manipulation

- Evaluating the ‘wisdom of crowds for security’
 - PhishTank: less comprehensive, less timely than a commercial report [1]
 - WOT: more comprehensive in identifying ‘bad’ domains than automated services [2]
- Reliability depends on
 - User capability
 - Mitigation of gaming behavior
 - Incentives
 - Few contributors => outcomes may be biased or manipulated more easily
 - Skewed ratio => large impact if a few highly active users stop contributing
- This work focuses on incentives

Basic model

- n-player game
- utility: normalized total effort security [5]
 - Inputs from all players are equally important
 - If all contribute, utility = benefit of full protection – individual's cost of contribution
 - If Bob does not contribute, he gets utility = sum of contributing players / n * benefit
- a public provisioning problem
 - reverse of “the tragedy of the commons” [3]

- infinite repetition
 - n players evaluate a different target (e.g. domain) at each time t
 - δ -discounted average criterion
 - High δ : player values long term benefit of system or community
 - δ_i drawn uniformly between δ_{\min} and 1
- => An infinitely repeated n -person prisoner's dilemma
- More complex than the iterated 2-person PD
 - Cannot identify non-contributors w/o centralized monitoring

Simulation

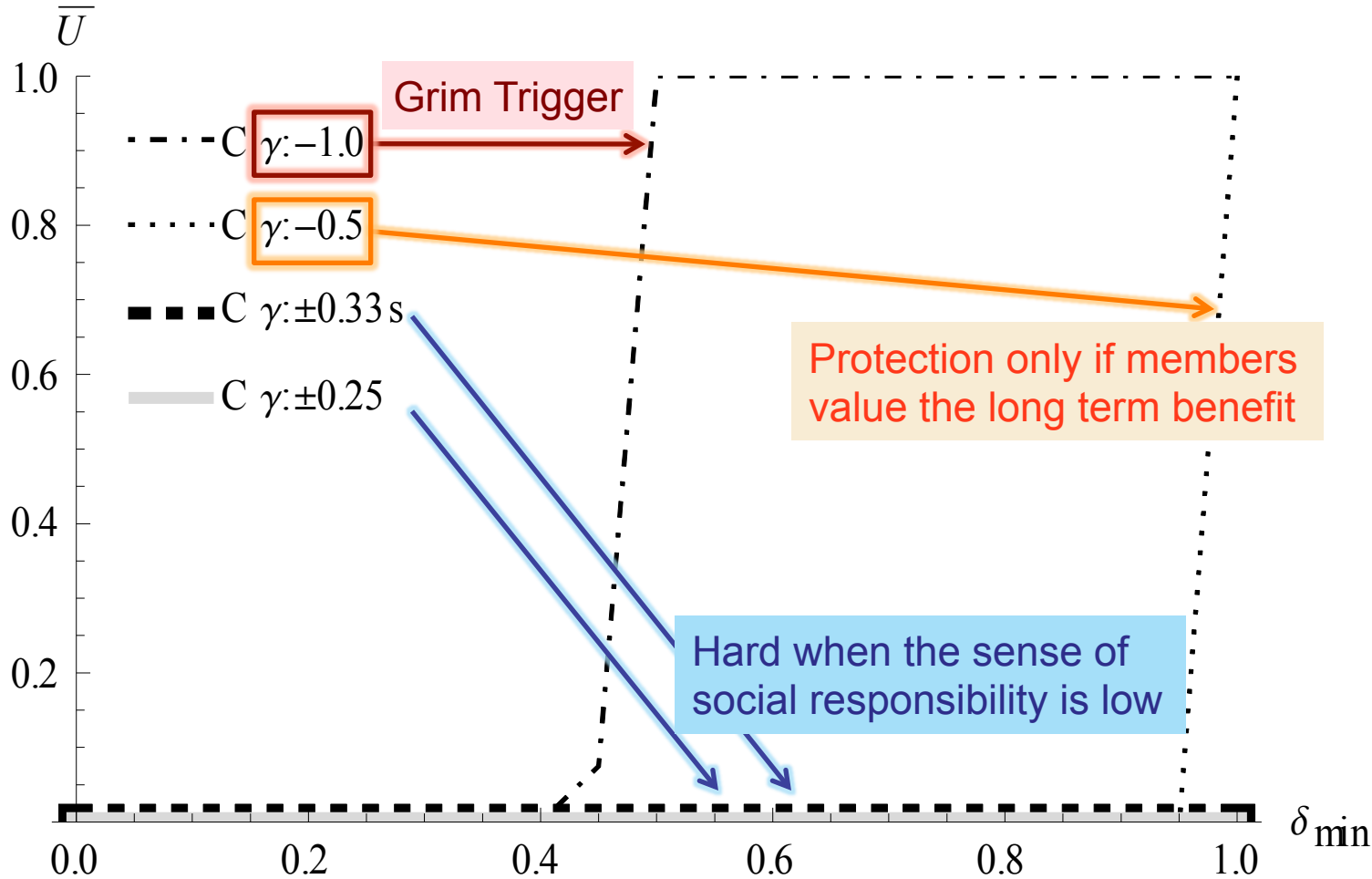
Simulation:

Social Expectation / Influence

- Complete graph community
 - $N = n = 100$, cost of contribution = 1, benefit of full protection = 2
- Modeling social influence
 - Assume players expect that
 - if he does not contribute: a fraction of others will follow suit, and vice-versa
 - if he contributes now, since his action will cause some positive influence, he would be better to contribute also in the future, and vice-versa
 - Influence updating rules: Linear, Sigmoid

Limited help with expectation on social influence

Average Utility



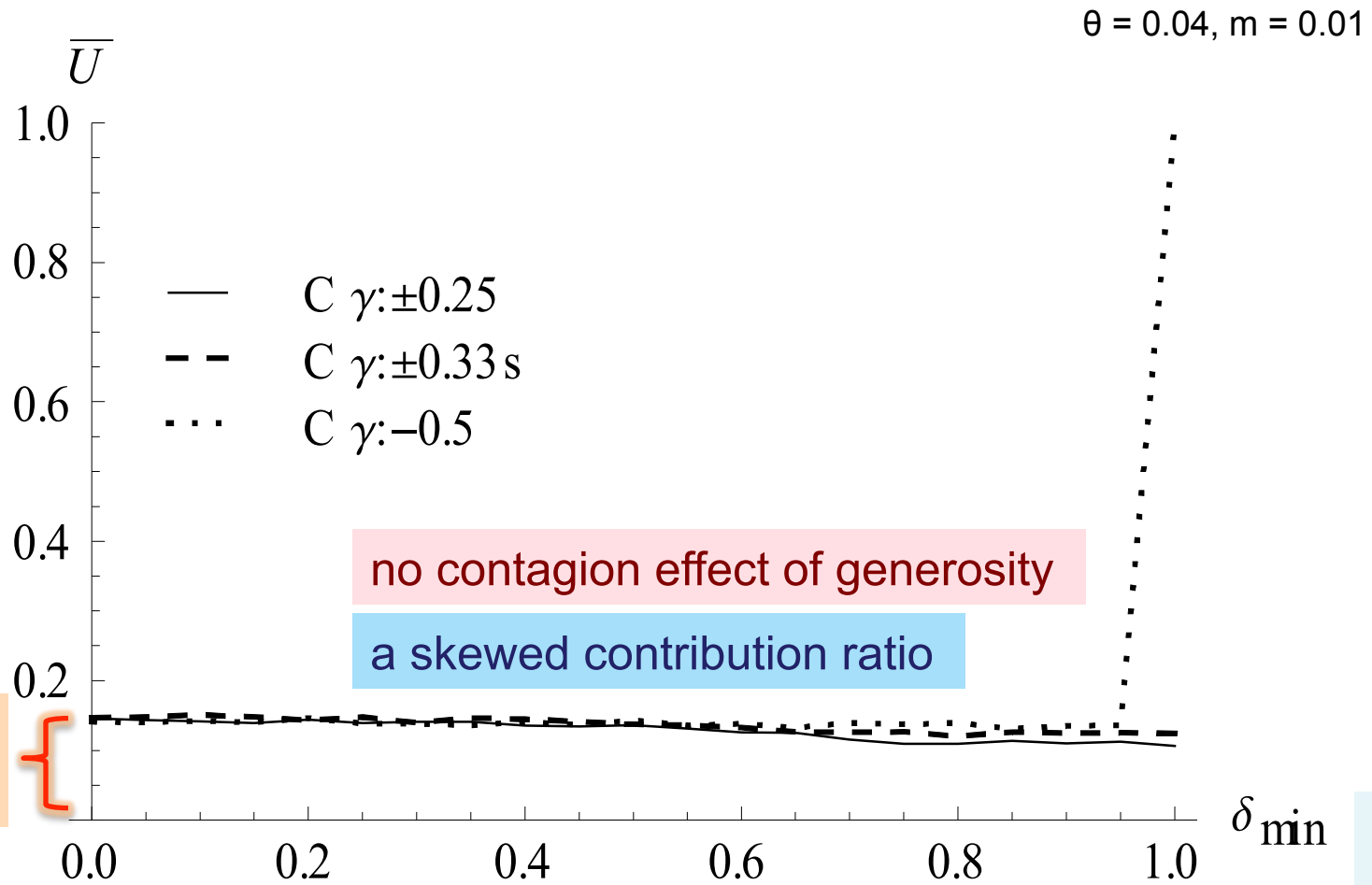
Simulation:

Effect of 'nice' players and user dynamics

- 'Nice' players
 - Assume a fraction θ of players who always contribute
- User dynamics
 - A fraction of m worst-performing users leave community, per game round
 - Same number of new users join

No contagion effect of generosity

Average Utility



no contagion effect of generosity

a skewed contribution ratio

a minimal level of utility

Minimum discounting

Simulation:



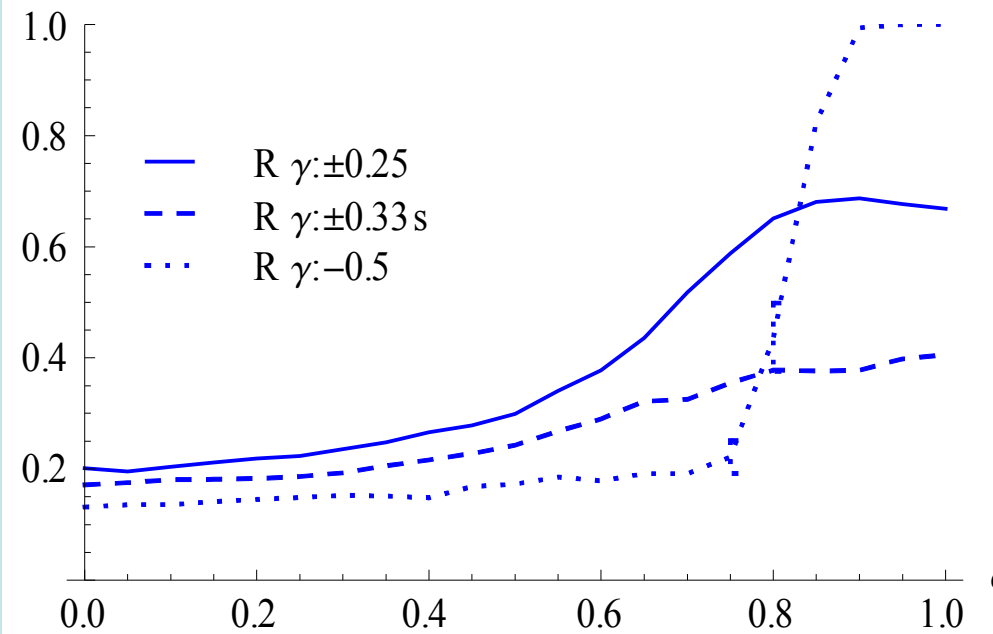
Random and Scale-free networks

- Organize players into ‘social networks’ topologies
- Random graph
 - For each player, assign ψ peers, selected with uniform probability
- Scale-free
 - Preferential peer selection [8]
 - Initialize $\psi+1$ fully connected players
 - For each subsq. player, assign ψ peers, selected with Pr (proportional to candidate’s degree)
- Each player engages with his peers
 - n varies

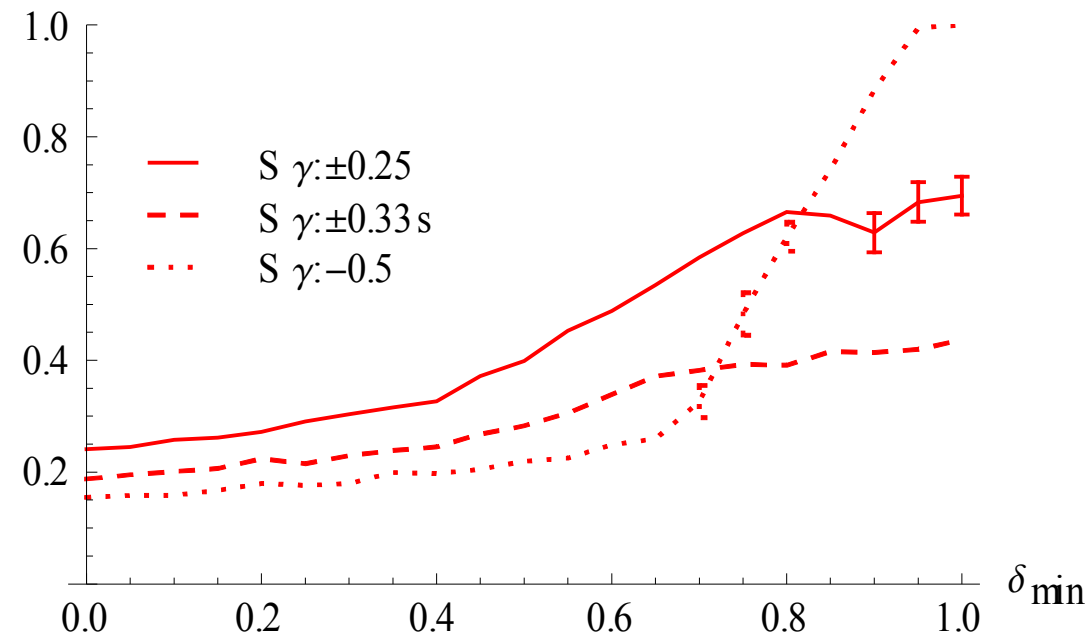
Random / scale-free community: Easier to encourage contribution

$\theta = 0.04, m = 0.01, \psi = 4$

Random network ($\psi=4$)



Scale-free network ($\psi=4$)



- A moderate level of cooperative behavior can emerge (also with $\psi=8$)
- Contagion effect of generosity as δ_{\min} increases
- Results for random and scale-free networks similar
 - likely due to limited structural variation given a small $N = 100$

Limitations & Future Investigation

- Best- k -effort game, if it suffices to have k inputs for full protection
 - adaptable from “best-shot” security games (used in [5][6][7])
- Budget constraint
- Endogenous δ discounting factor
- Heterogeneous cost / benefit

Summary

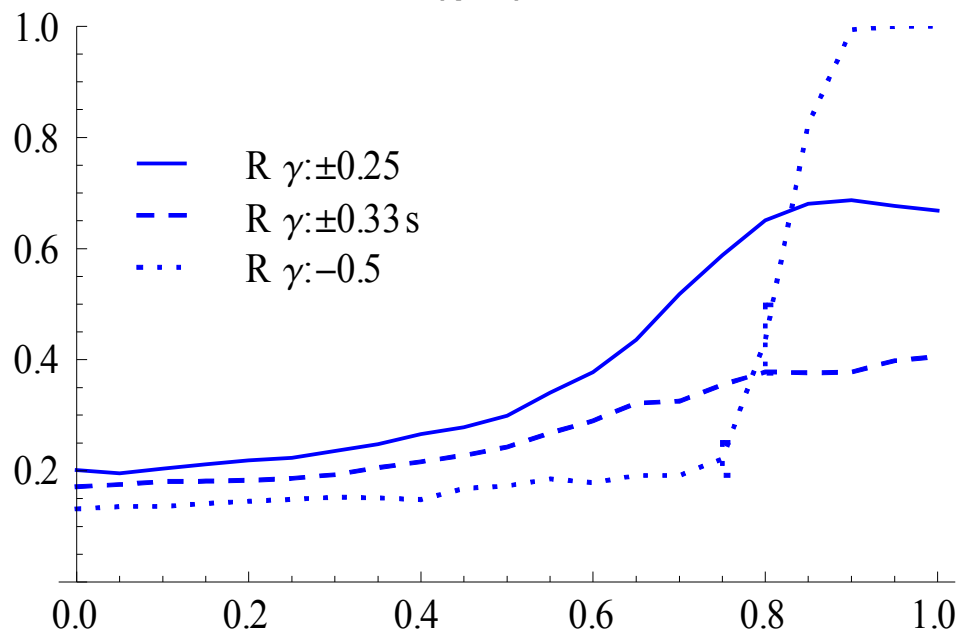
- Challenging to get active contribution in a complete-graph community
- But, does not imply economic infeasibility of CSS
 - Have not factored in any incentives schemes
 - Nor considered social capital (e.g., reputation)
- Community structure matters
 - Easier to cultivate cooperation in scale-free / random graphs
 - There could be challenges, e.g., ‘limited wisdom’ in separate local groups
 - Innovative ways to aggregate the output of separate groups would be helpful

1. Moore, T., and Clayton, R., “Evaluating the Wisdom of Crowds in Assessing Phishing Websites,” *FC 2008*.
2. Chia, P.H., and Knapskog, S.J., “Re-evaluating the Wisdom of Crowds in Assessing Web Security,” *FC 2011*.
3. G. Hardin, “The tragedy of the commons,” *Science*, vol. 162, pp. 1243–47, 1968.
4. N. S. Glance and B. A. Huberman, “The outbreak of cooperation,” *The Journal of Mathematical Sociology*, vol. 17, no. 2, pp. 281–302, 1993.
5. J. Grossklags, N. Christin, and J. Chuang, “Secure or insure? A game-theoretic analysis of information security games,” in *WWW 2008*.
6. H. Varian, “System reliability and free riding,” in *Economics of Info. Security*, ser. *Advances in Info. Security*, L. Camp and S. Lewis, Eds. Springer, 2004, vol. 12, pp. 1–15.
7. J. Hirshleifer, “From weakest-link to best-shot: The voluntary provision of public goods,” *Public Choice*, vol. 41, no. 3, pp. 371–386, 1983.
8. A.-L. Barabasi, “Scale-Free Networks: A Decade and Beyond,” *Science*, vol. 325, no. 5939, pp. 412–413, Jul 2009.

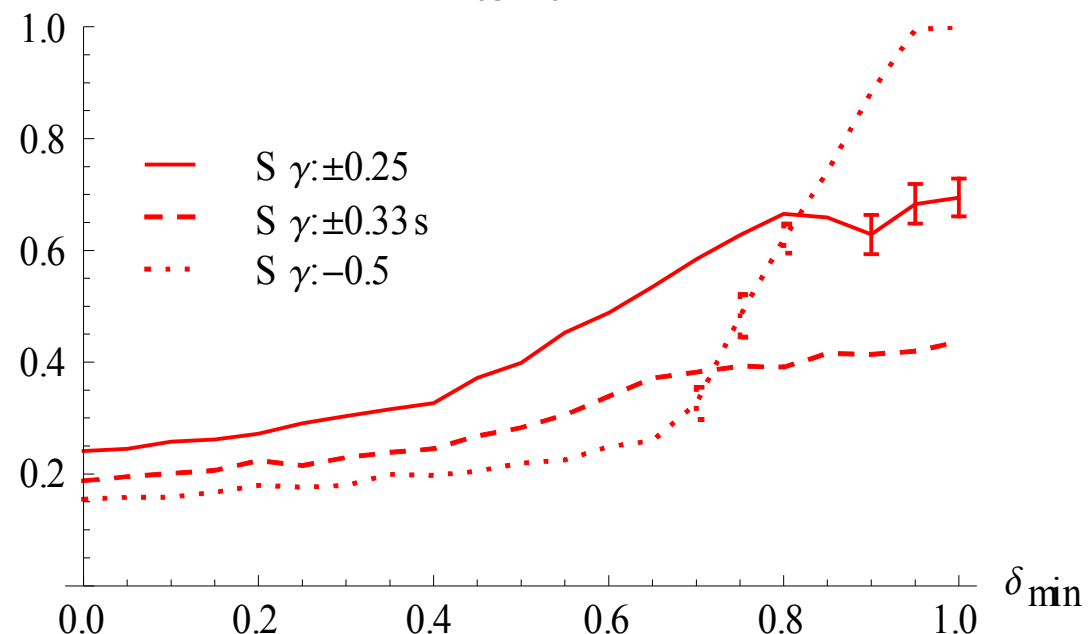
Thank you. Question?

Pern Hui Chia
chia@q2s.ntnu.no

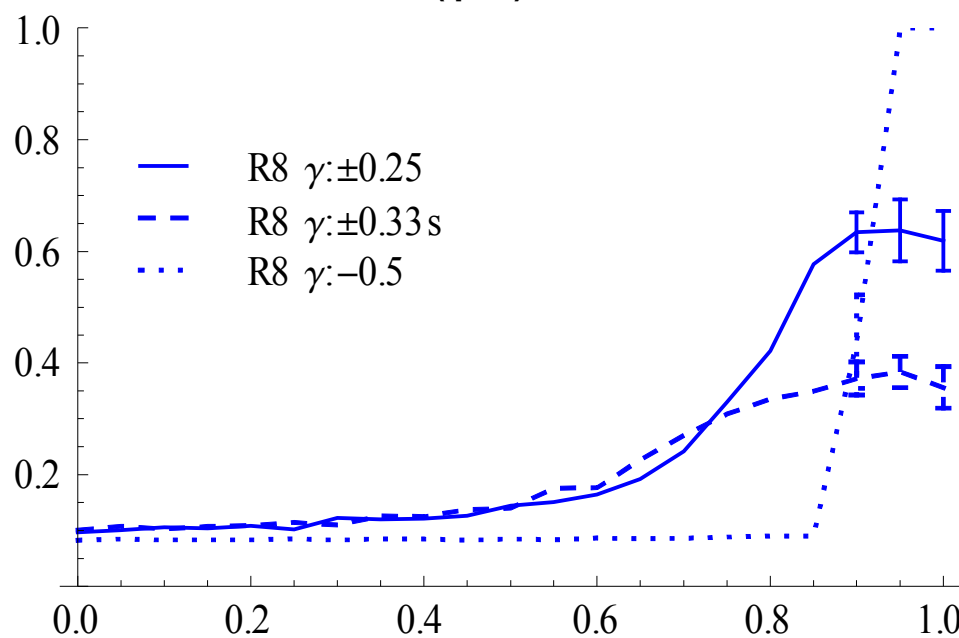
Random network ($\psi=4$)



Scale-free network ($\psi=4$)



Random network ($\psi=8$)



Scale-free network ($\psi=8$)

