Making Eigenvector-based Reputation Systems Robust to Collusion

Hui Zhang[1], Ashish Goel[2], Ramesh Govindan[1], Kahn Mason[2], Benjamin Van Roy[2]

[1]University of Southern California

[2]Stanford University

Outline

- Research motivation.
- PageRank algorithm : a brief introduction.
- Study of PageRank's robustness to collusion.
- Adaptive-resetting: make PageRank robust to collusion.
- Conclusion & future works.

Research motivation

- Build reputation in large-scale systems
  - P2P file sharing systems
  - Blogging communities
  - Networked gaming, …, etc.
- Collusion-proofness is an essential criterion in evaluating a rating scheme.

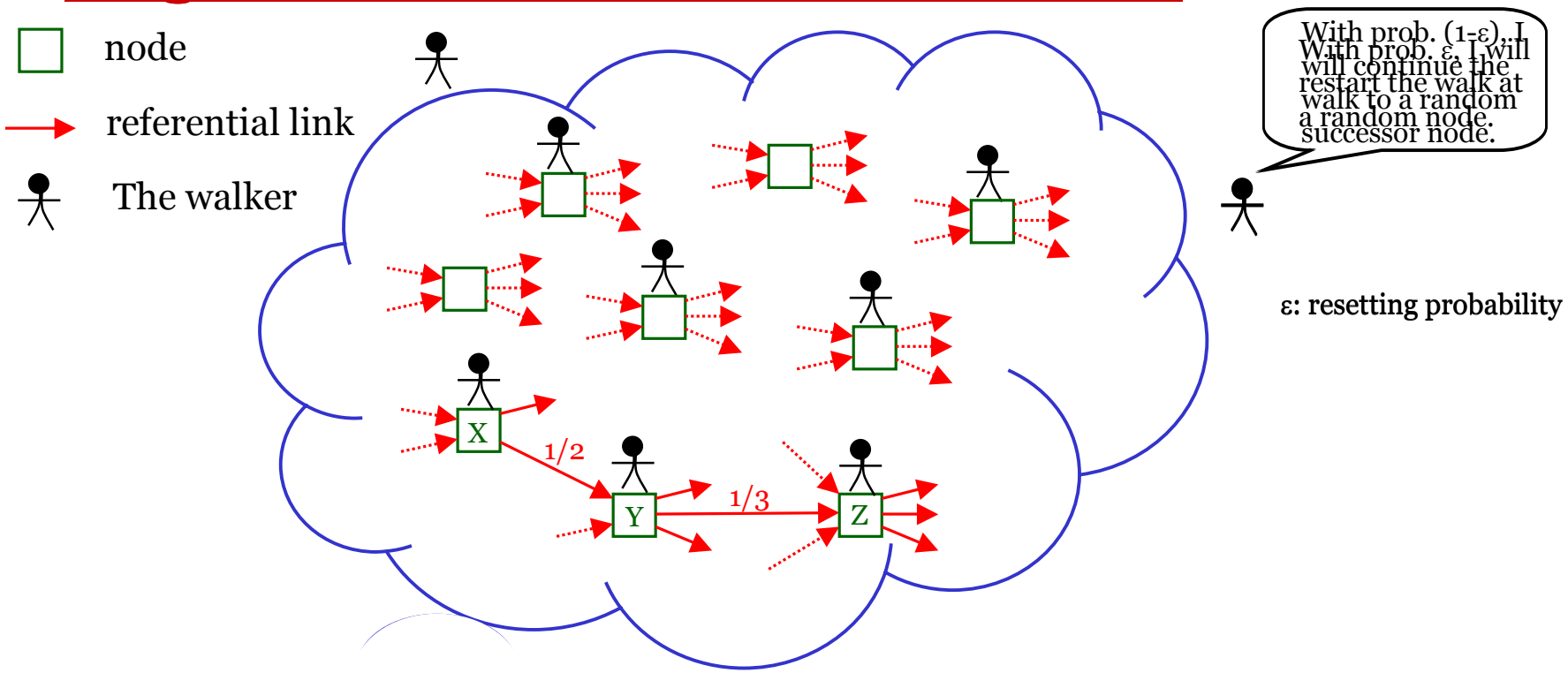
PageRank [Brin1998]

- An ***eigenvector-based*** rating scheme to rank hypertext documents on the WWW.

- An iterative algorithm to calculate the importance of a web page based on the importance of its parent pages.

- Can be applied to other systems than WWW.

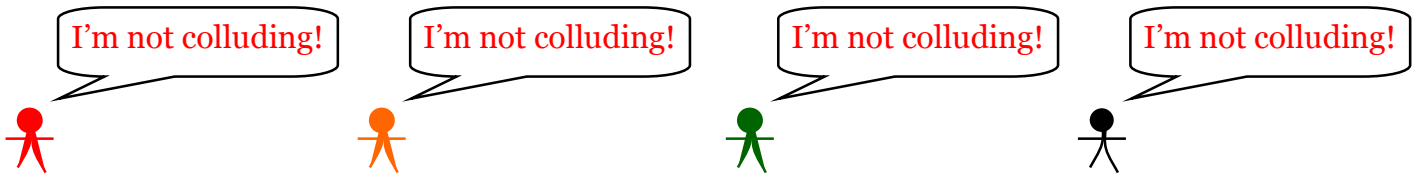
PageRank: random walk model



- As time goes on, the expected percentage of steps the walker is at each node *v* converges to the PageRank weight PR(*v*).

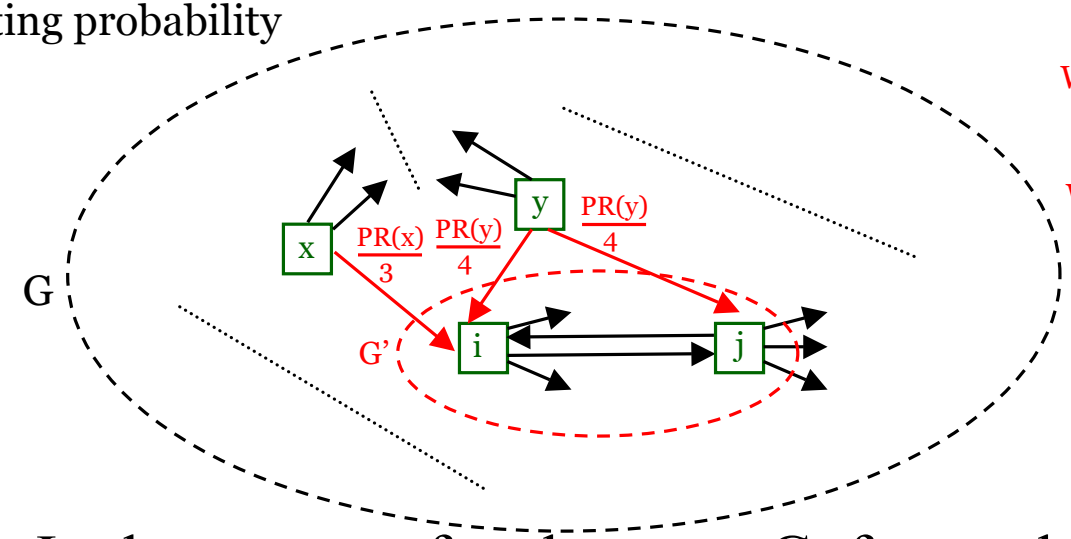
PageRank: is it collusion-proof?

- Can a node easily boost its rank by manipulating its out-going links with others'?



Amp(G): a metric on group collusion

ε: resetting probability



$W_G(G') = PR(i)+PR(j)$ ← real group weight

$W_{in}(G') = \frac{PR(x)}{3}(1-\varepsilon) + \frac{PR(y)}{2}(1-\varepsilon) + \frac{2}{N}(1-W(G'))\varepsilon$ ← "actual" group weight

- In the system of node group G, for a subgroup G',

  the amplification factor $Amp(G') = \frac{W_G(G')}{W_{in}(G')}$

  - $W_G(G') = \sum_{i:\ i\in G'} PR(i)$

  - $W_{in}(G') = \sum_{(i,j):\ i\notin G',\ j\in G',\ \exists i\to j} \frac{PR(i)}{out(i)}(1-\varepsilon) + \frac{|G'|}{|G|}(1-W_G(G'))\varepsilon$

Theorem on Amp

- In the original PageRank system,

$$\forall G' \subseteq G, Amp(G') \leq \frac{2}{\varepsilon}$$

where ε is the resetting probability.

$$Specifically, \quad when \quad \frac{|G'|}{|G|} << 1, Amp(G') \leq \frac{1}{\varepsilon}$$

Two experimental topologies

- *W*, a Web link topology
  - Contains the link structure of upwards of 80 million URLs.
  - Source: the Stanford WebBase.
- *B*, a weblog blogrolling topology
  - Contains the blogrolling structure of upwards of 72,000 blogs.
  - Source: *www.blogstreet.com*, the XML -RPC webblog service.

Experiment 1: *Collusion200*

- Model a small number of web pages ***simultaneously*** colluding.
- Methodology:
  - 100 colluding groups of 200 nodes;
  - Each colluding group has the circle topology consisting of two nodes with adjacent ranks;
  - Arbitrarily chose node pairs originally ranked around 1000^{th}, 2000^{th}, …, 100000^{th}.
  - $\varepsilon = 0.15$.

Experiment result of *Collusion200* (I)

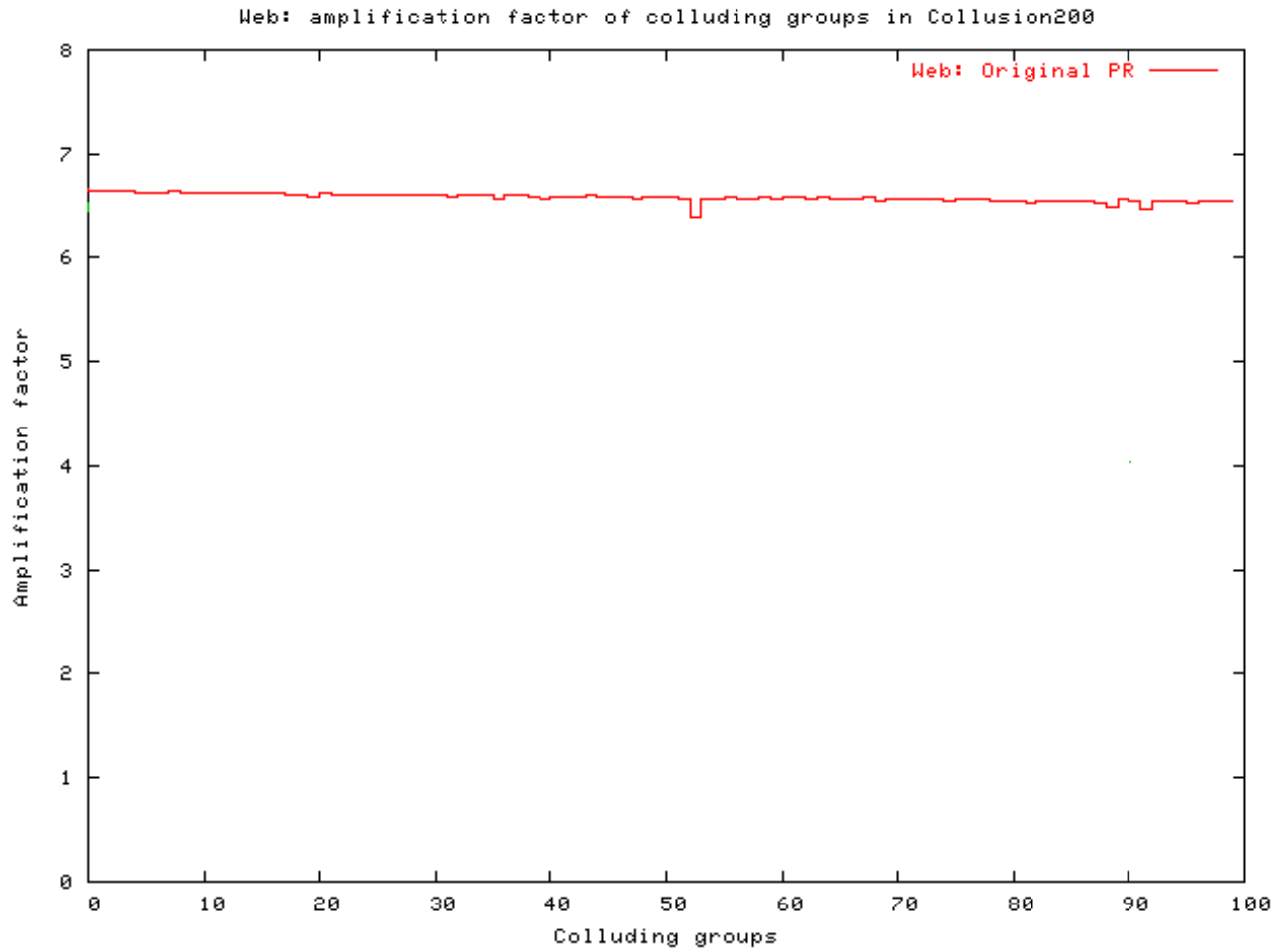


Figure 1: *W* - Amplification factors of the 100 colluding groups in *Collusion200*.

Experiment result of *Collusion200* (III)

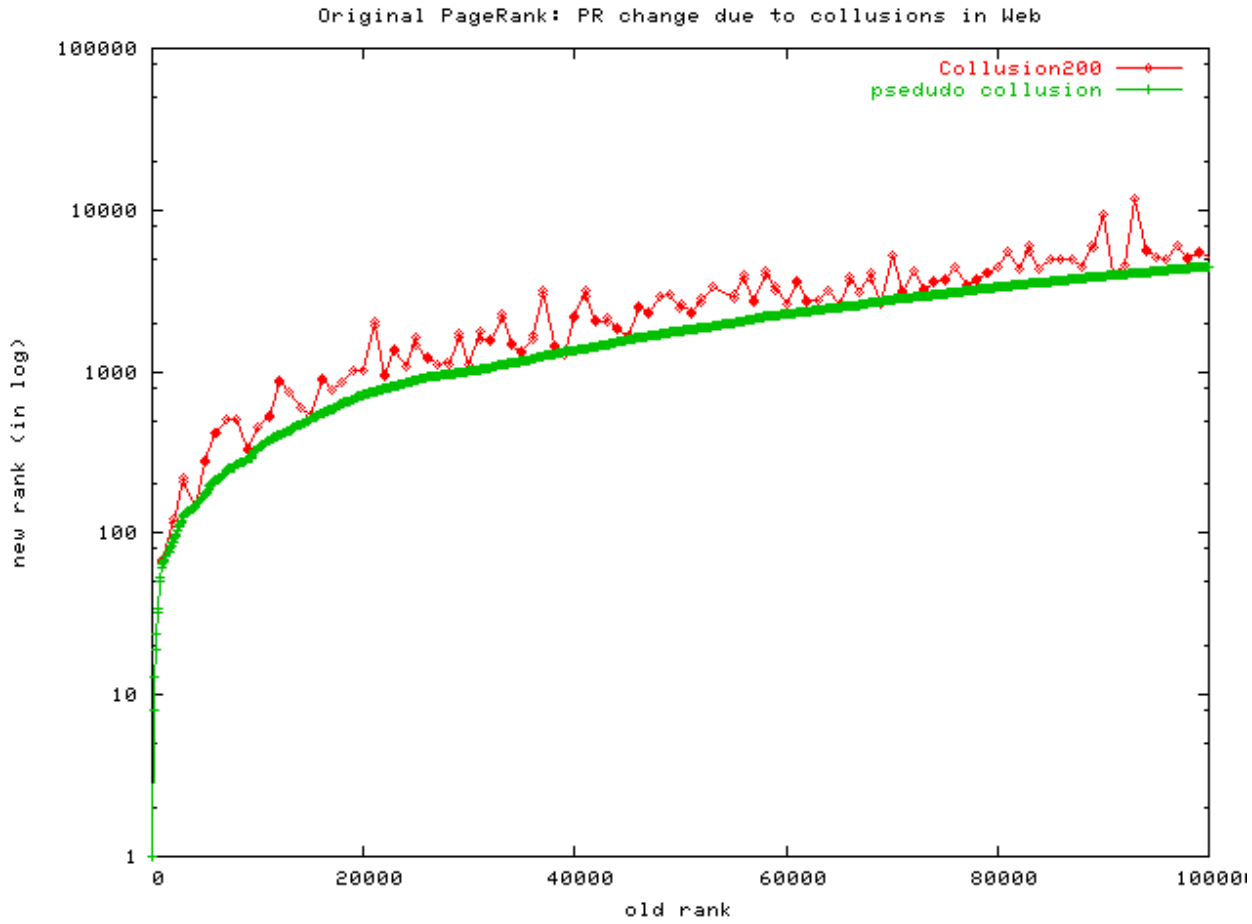


Figure 2: *W* – new PR rank after *Collusion200*.

There is a long flat portion…

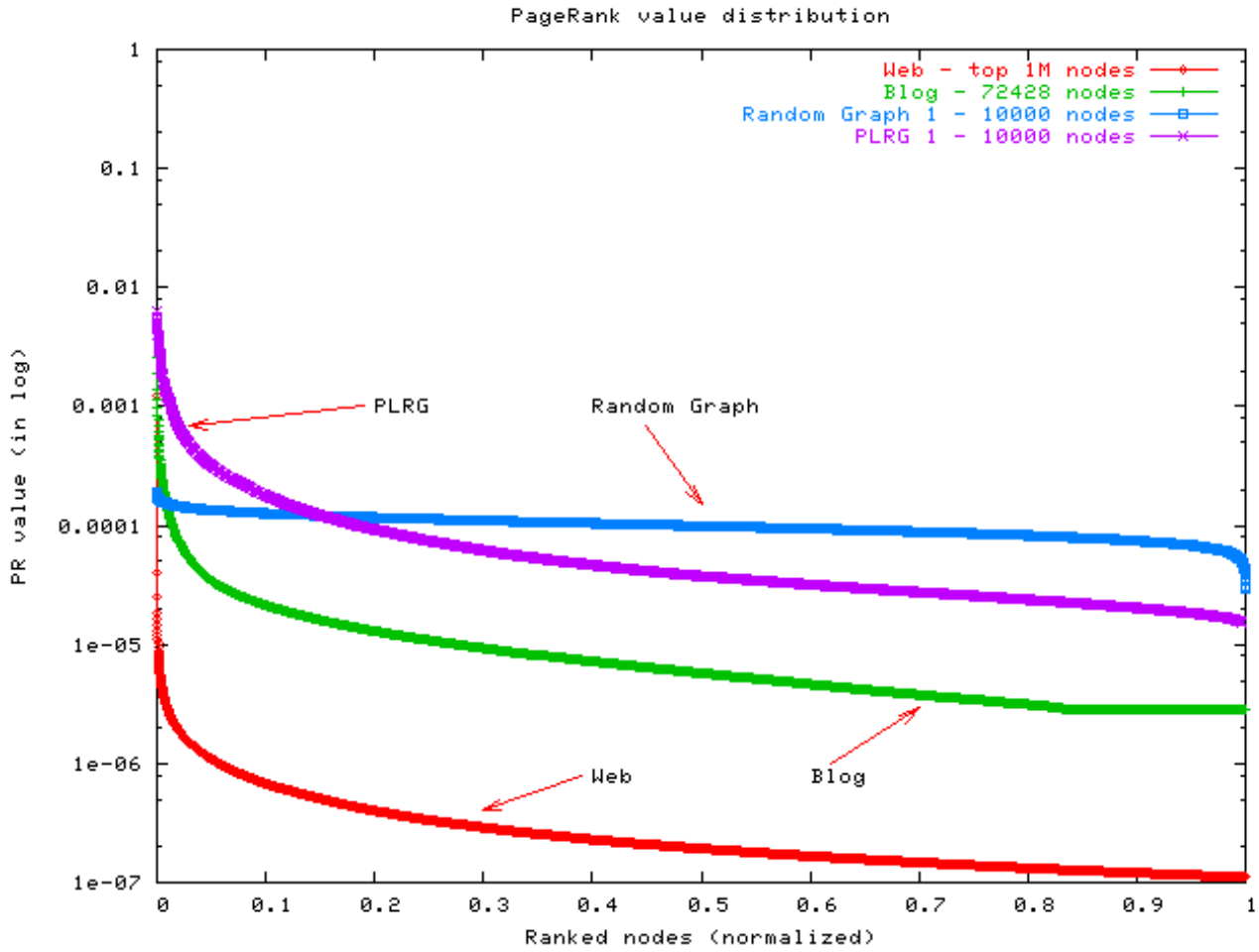


Figure 3: The PR weight distribution of 4 topologies.

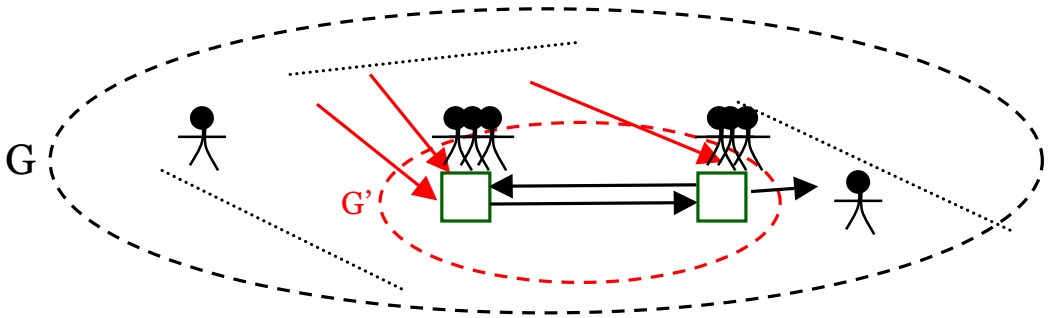
Next step: how to detect collusions?

- Theorem on Hardness.

$$Max_{G' \subseteq G} Amp(G') \text{ is a NP-Hard problem.}$$

An observation on collusion behaviors

- To increase their PR weight, i.e., the stationary weight in the random walk, the colluding nodes will stall the random walk.

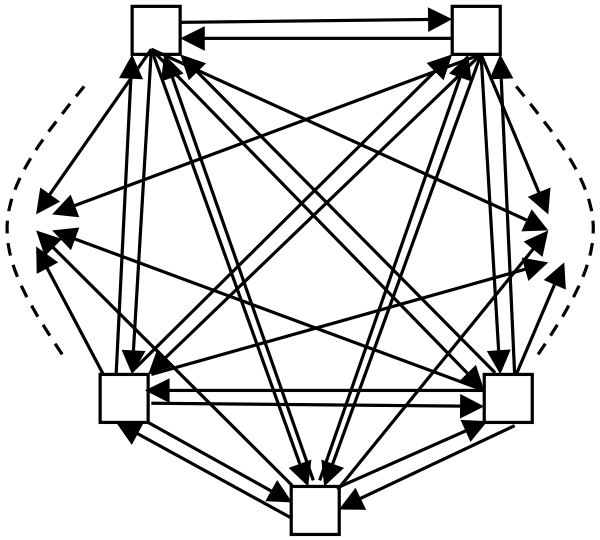


- When the resetting probability ε increases, the colluding nodes must suffer a significant drop in PR weight.
- Therefore, we expect the PR weight of colluding nodes to be highly correlated with 1/ ε (the average walk length), while that of non-colluding nodes is relatively insensitive to the change in ε.

An intuitive example

node

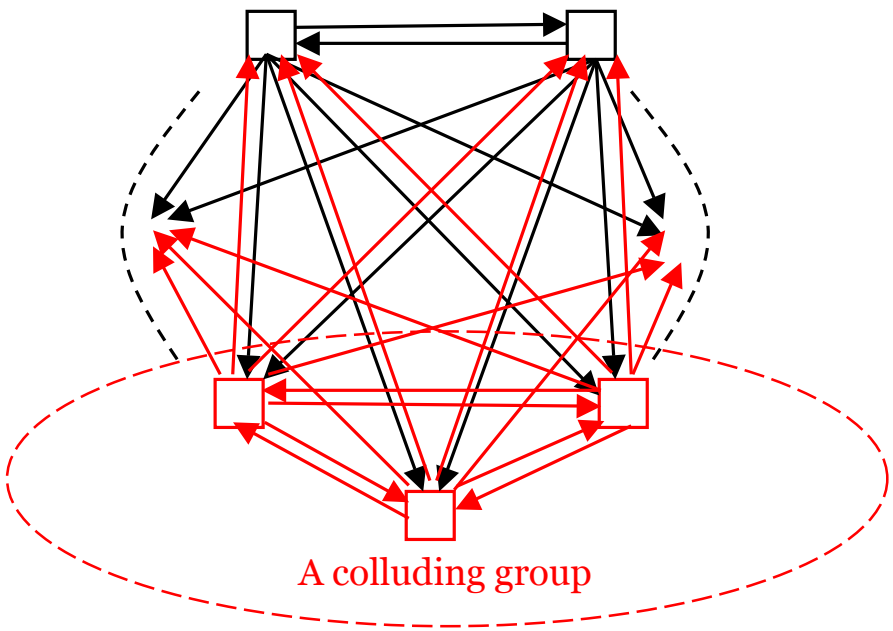
referential link



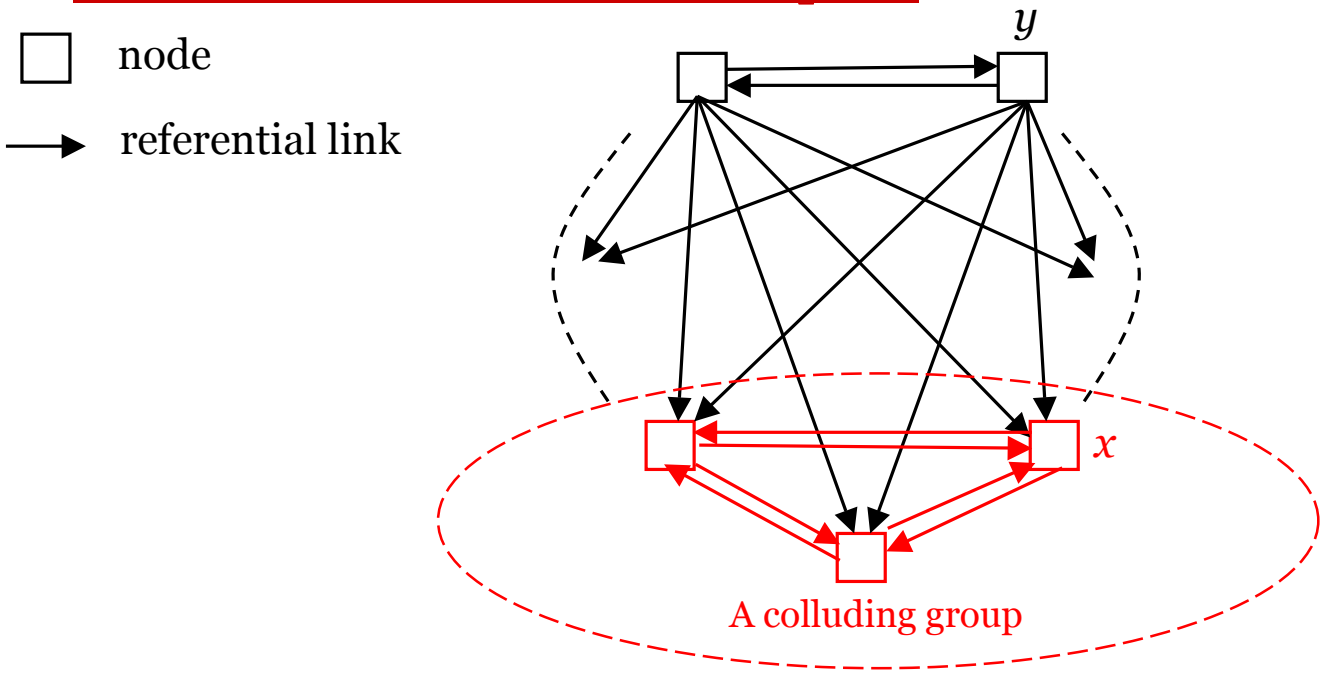
An intuitive example

node

referential link



An intuitive example



- A colluding node x: $PR(x) = \frac{1}{K+(N-K)\varepsilon} \approx \frac{1}{N\varepsilon}$, and co-co(PR($x$), 1/ε) ≈ 1. (co-co: correlation coefficient)
- A non-colluding node y: $PR(x) = \frac{\varepsilon}{K+(N-K)\varepsilon} \approx \frac{1}{N}$, and co-co(PR($y$), 1/ε) ≈ 0.

N: the system size; K: the colluding group size; K << N.

Adaptive-resetting scheme

- Part I – collusion detection:
  - Given the topology, calculate the PR vector under different ε values.
    - $\{\varepsilon\} = \{0.0375, 0.05, 0.075, 0.15, 0.3, 0.45, 0.6\}$, $\varepsilon_{default} = 0.15$.
  - Calculate the correlation coefficient between the curve of each node *x*'s PR weight and the curve of 1/ ε. Label it as *co-co(x)*.
- Part II – ε personalization:
  - Calculate each node *x*'s out-link personalized-ε = $F(\varepsilon_{default}, co\text{-}co(x))$.
    - Exponential function $F_{Exp} = \varepsilon_{default}^{(1.0-co-co(x))}$.
    - Linear function $F_{Linear} = \varepsilon_{default} + (0.5-\varepsilon_{default}) * co\text{-}co(x)$
  - The final PR weight vector is calculated with these personalized resetting values.

Experiment result of *Collusion200* (IV)

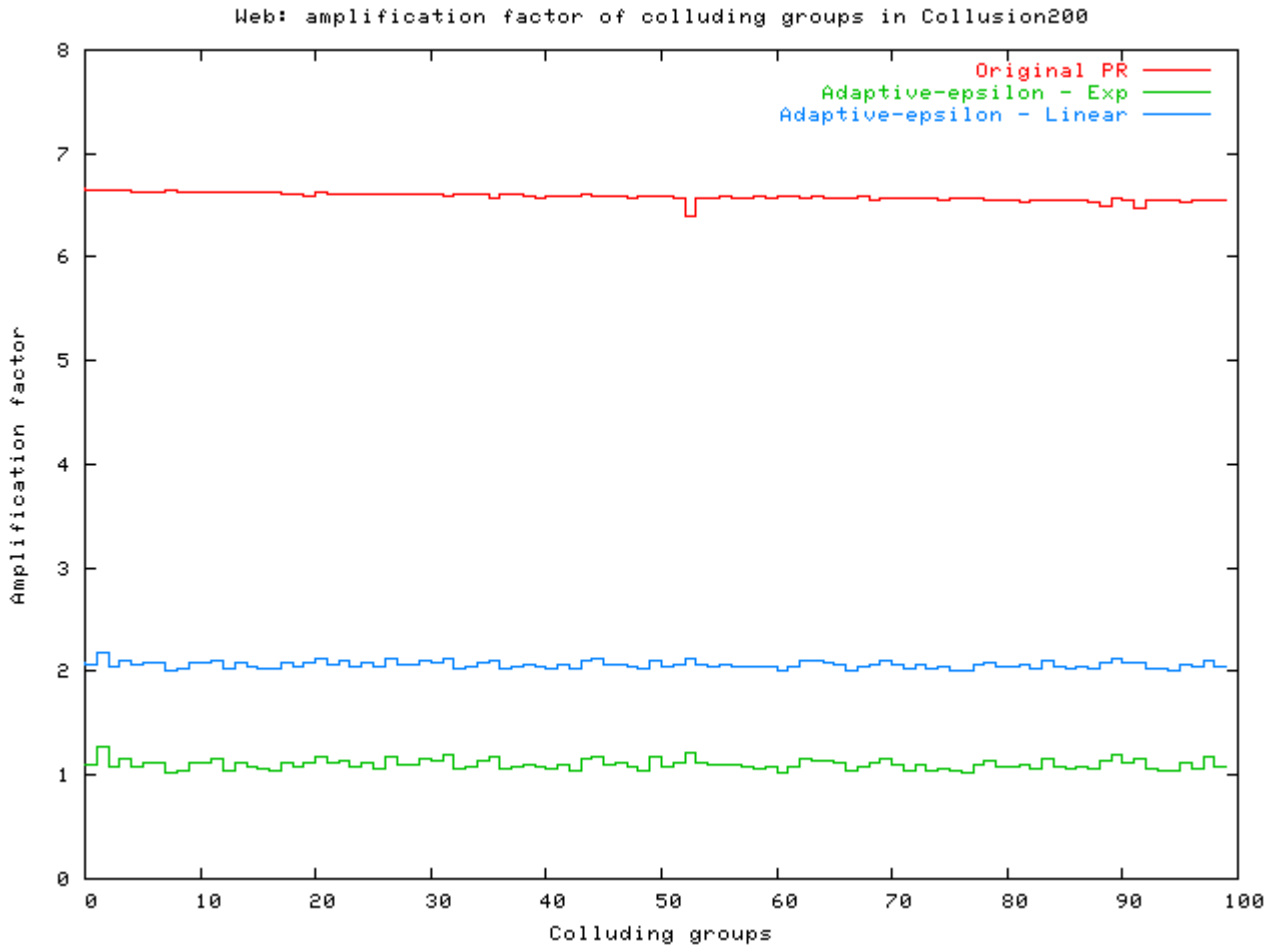


Figure 5: *W* - Amplification factors of the 100 colluding groups in *Collusion200*.

Experiment result of *Collusion200* (VI)

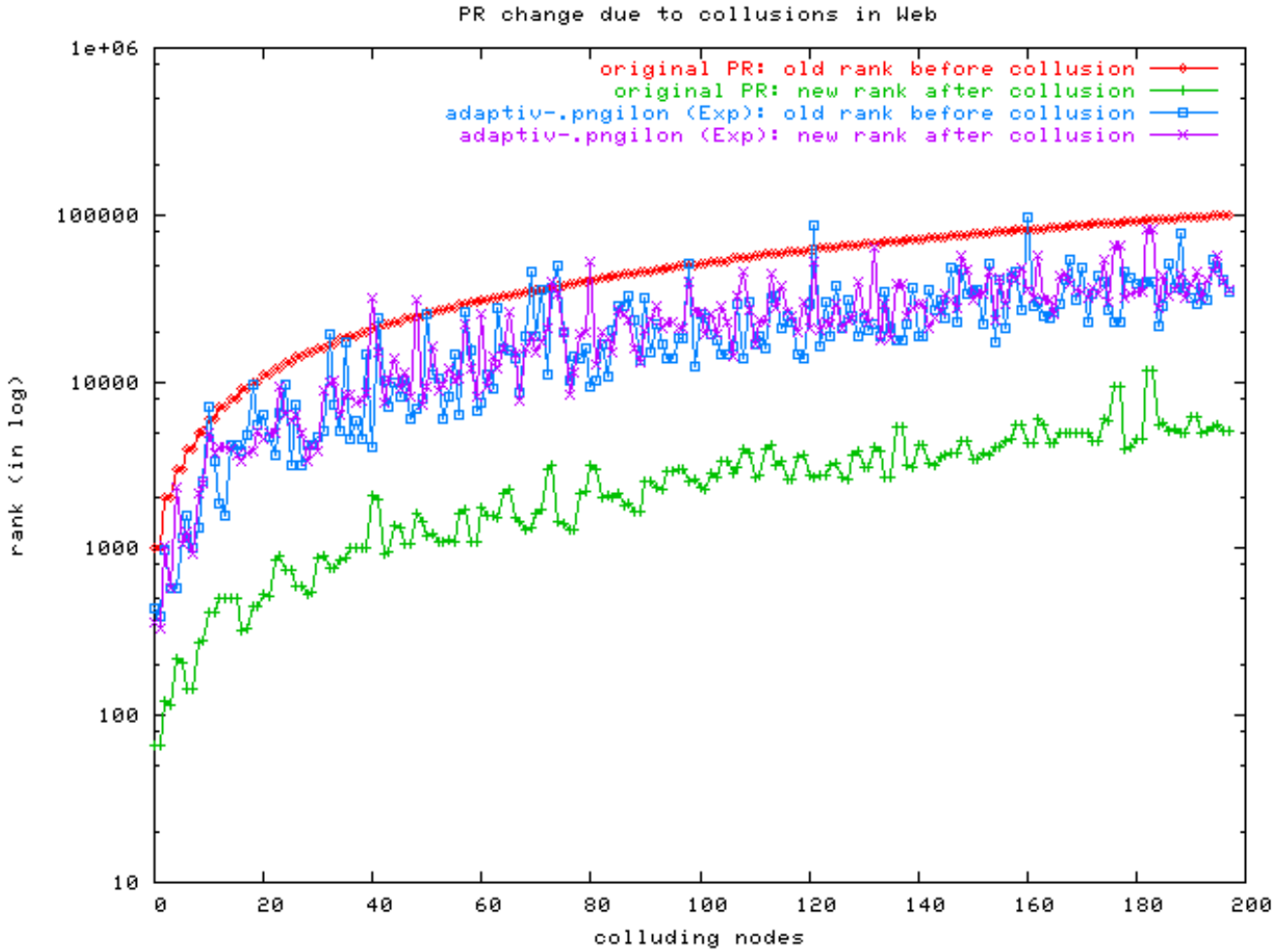
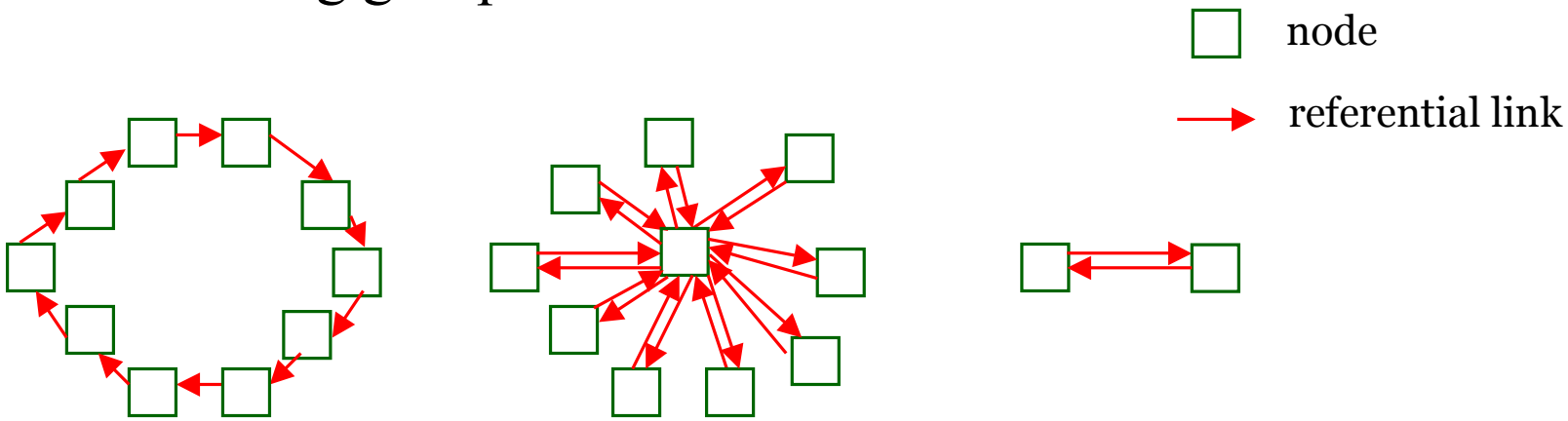


Figure 6: *W* – new PR rank after *Collusion200*.

Experiment 2: *Collusion22*

- Model various colluding subgraphs.
- Methodology:
  - 3 colluding groups:



G1: 10-node ring

G2: 10-node star topology

G3: 2-node ring

Experiment result of *Collusion22* (I)

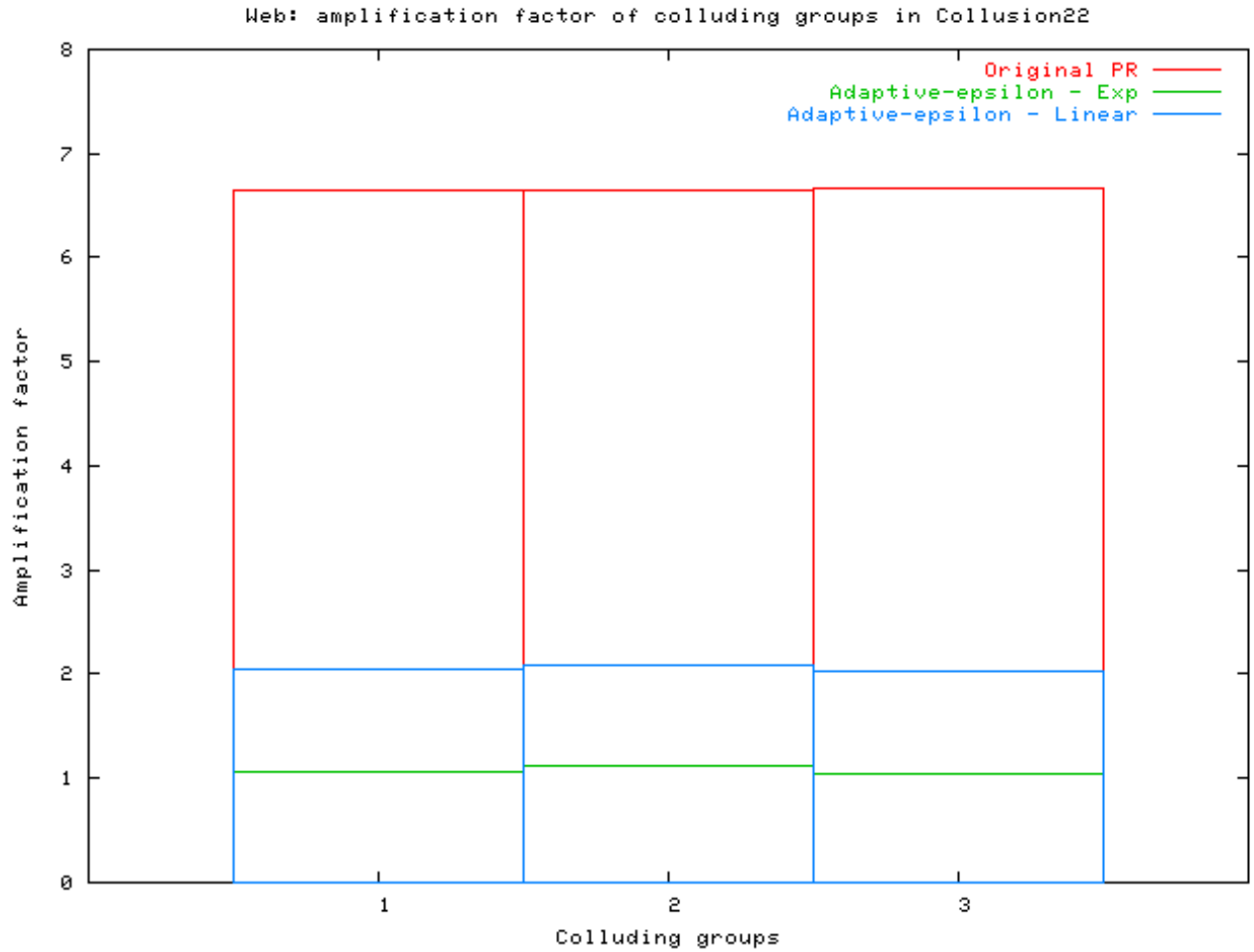


Figure 7: Amplification factors of the 3 colluding groups in *Collusion22*.

Experiment result of *Collusion22* (II)

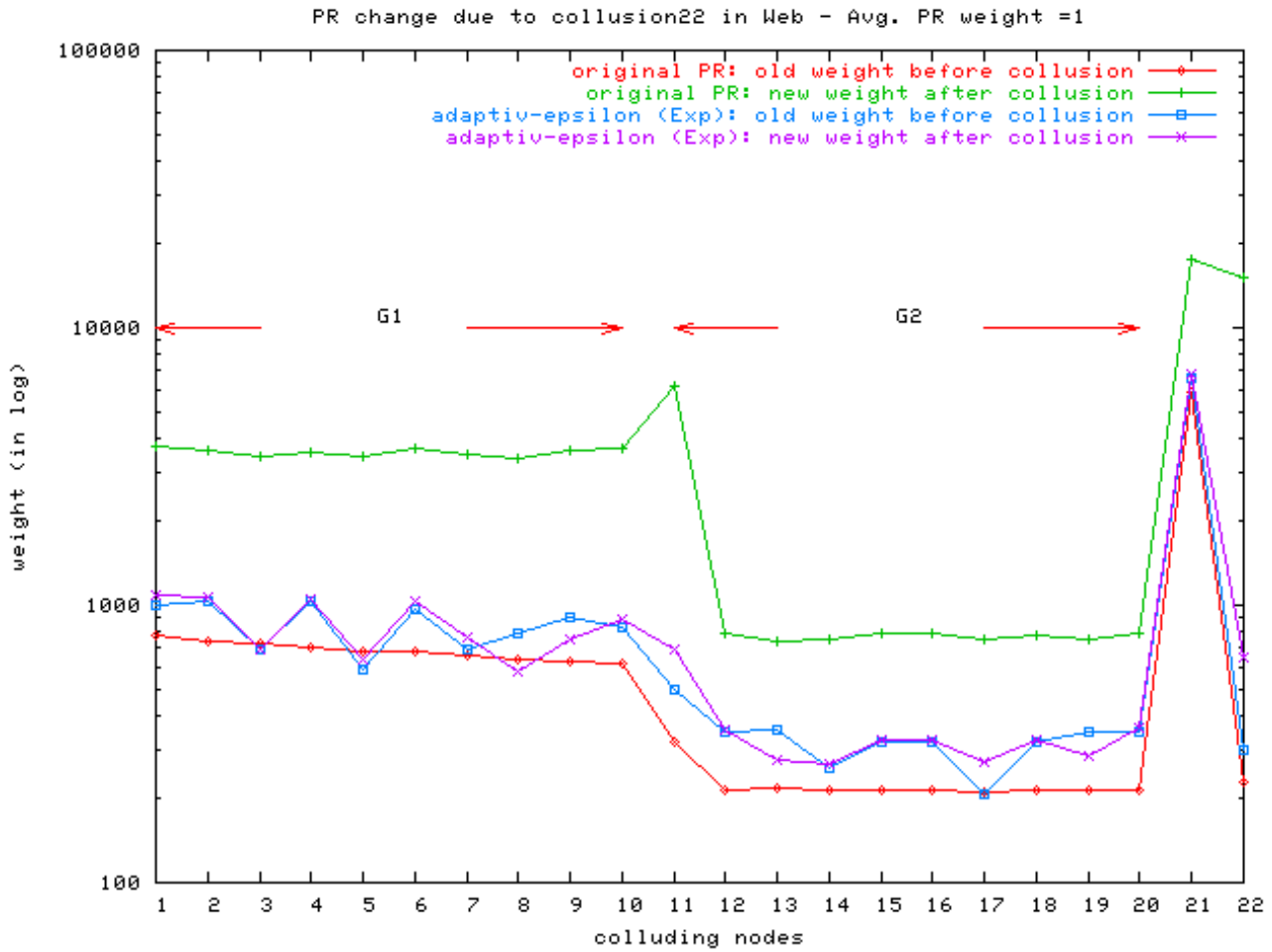


Figure 8: *W* – new PR weight after *Collusion22*.

New top-25 URL list in *W*

Dropped out
Dropping
New

Rank	Old list	New list
1	http://www.yahoo.com/	http://www.tucows.com/
2	http://www.msn.com/	http://www.yahoo.com/
3	http://www.tucows.com/	http://www.domaindirect.com/
4	http://www.domaindirect.com/	http://news.tucows.com/
5	http://news.tucows.com/	http://ispcentral.tucows.com/
6	http://ispcentral.tucows.com/	http://www.microsoft.com/
7	http://www.microsoft.com/	http://www.acme.com/software/thttpd
8	http://www.microsoft.com/info/privacy.htm	http://www.adobe.com/products/acrobat/readstep.html
9	http://www.adobe.com/products/acrobat/readstep.html	http://home.netscape.com/
10	http://home.netscape.com/	http://www.thecounter.com/
11	http://www.lycos.com/	http://www.gendex.com/ged2html
12	http://www.worldwidemart.com/scripts/	http://www.adobe.com/
13	http://www.acme.com/software/thttpd	http://www.worldwidemart.com/scripts/
14	http://search.internet.com/	http://upload.tucows.com/contactus.html
15	http://upload.tucows.com/contactus.html	http://www.w3.org/
16	http://www.thecounter.com/	http://www.listbot.com/
17	http://www.listbot.com/	http://www.tucows.com/privacy.html
18	http://www.w3.org/	http://www.worldwidemart.com/scripts/counter.html
19	http://www.adobe.com/	http://www.microsoft.com/windows/ie/default.htm
20	http://www.lycos.com/search.html	http://www.nsf.gov/
21	http://www.tucows.com/privacy.html	http://www.loc.gov/
22	http://www.gendex.com/ged2html	http://www.nsa.gov/
23	http://ds.internic.net/ds/dspg0intro.html	http://search.internet.com/
24	http://www.adobe.com/misc/privacy.html	http://www.nasa.gov/
25	http://www.adobe.com/homepage.html	http://ds.internic.net/ds/dspg0intro.html

Table 1: The old and new top-25 list of $\mathcal{W}$

Conclusion & future works

- A collusion-proof rating scheme based on PageRank algorithm.

- Future works:
  - Formal analysis of the adaptive-resetting scheme.
  - Study of Web link structure evolution under PageRankwithin the framework of game theory.