Sorcery: Could We Make P2P Content Sharing Systems Robust to Deceivers?

Ennan Zhai, Ruichuan Chen,
Zhuhua Cai, Long Zhang, Eng Keong Lua*,
Huiping Sun, Sihan Qing, Liyong Tang, and Zhong Chen

(Email: zhaien@infosec.pku.edu.cn)

*Peking University & *Carnegie Mellon University*

Background

What is the deceptive behavior in P2P content sharing systems ?

What are the existing solutions on this problem ?

Our approach ?

Background

What is the deceptive behavior in P2P content sharing systems ?

What are the existing solutions on this problem ?

Our approach ?

Deceptive Behavior

Individual or collusive attackers (deceivers) publish some polluted content items, and cast incorrect votes on them ... ...

Deceptive Behavior

Individual or collusive attackers (deceivers) publish some polluted content items, and cast incorrect votes on them ... ...

Normal users are deceived by votes and download these polluted content items.

Deceptive Behavior

Alice's Content items

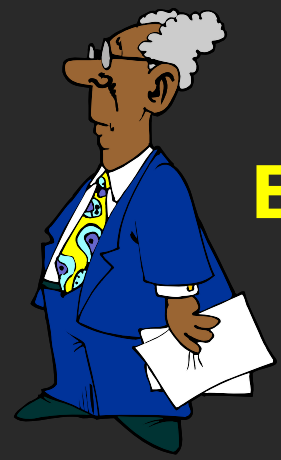
1 3 4

Alice's Votes

1 4

7 10 15

I would like to download File 4.



Bob

Deceptive Behavior

4

However, after downloading content 4, Bob finds this content item is polluted.

We say Bob is deceived by Alice's vote.

Bob

Background

What is the deceptive behavior in P2P content sharing systems ?

What are the existing solutions on this problem ?

Our approach ?

Existing Solutions

- Reputation Models:
  - ✓ Peer-based: EigenTrust, PeerTrust, Scrubber ...
  - ✓ Object-based: Credence, FileTrust ...
  - ✓ Hybrid: XRep, X^2Rep, Extended Scrubber...
- Micropayment Techniques: MojoNation.
- Exchange Protocol

... ...

Existing Solutions

- Reputation Models:
  - ✓ Peer-based: EigenTrust, PeerTrust, Scrubber ...
  - ✓ Object-based: Credence, FileTrust ...
  - ✓ Hybrid: XRep, X^2Rep, Extended Scrubber...
- Micropayment Techniques: MojoNation.
- Exchange Protocol

... ...

Some Problems!

Analysis

The above situation can be explained the attackers sit on the *dominant position*, and the solution is we need to achieve the conversion of the dominant position through constructing our own *dominant information.*

Analysis

The fundamental insight driving our work is social network can help the users construct the confidential and reliable friend-relationships, and we treat the confidential information of friends as the dominant information.

Background

What is the deceptive behavior in P2P content sharing systems ?

What are the existing solutions on this problem ?

Our approach ?

Sorcery

1. Introducing Social Network
2. Challenge-response Mechanism
3. Punishment Mechanism
4. Practical Issues

Sorcery

1. Introducing Social Network
2. Challenge-response Mechanism
3. Punishment Mechanism
4. Practical Issues

Introducing Social Network

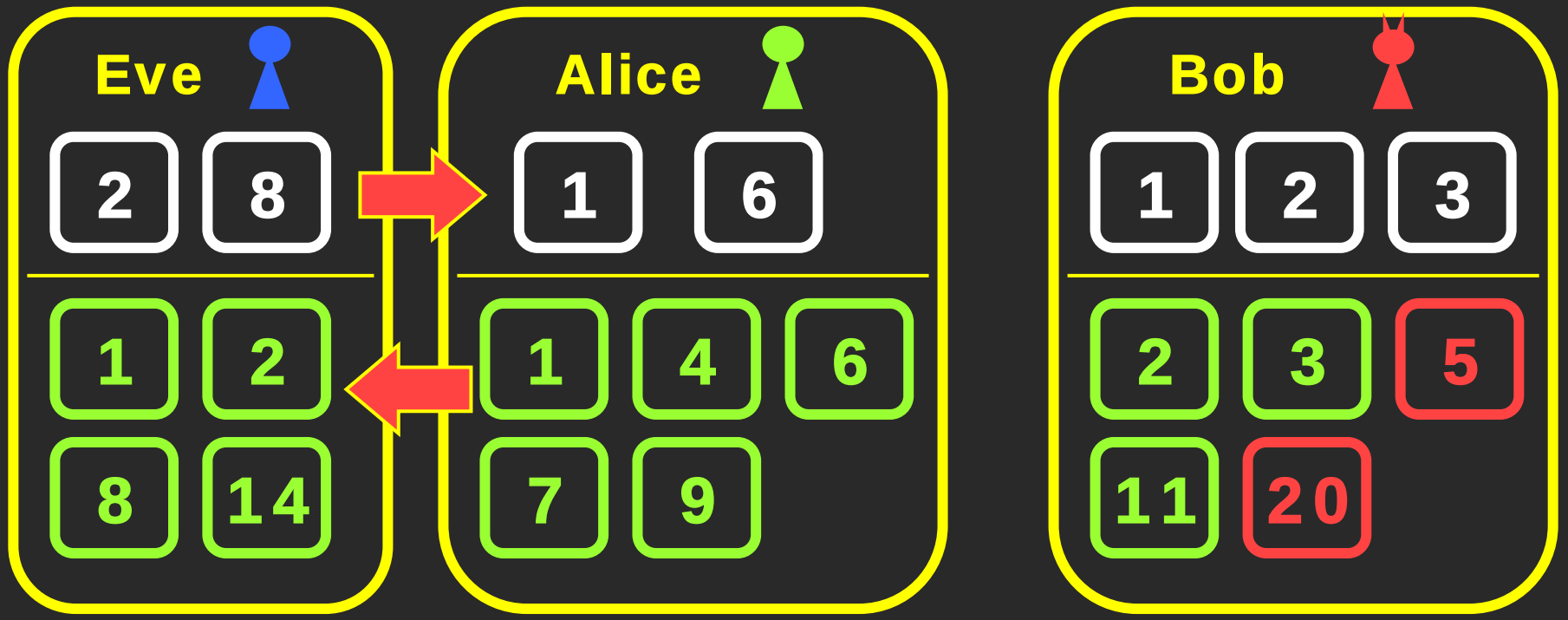
Sorcery client stores friends' information in his friend list. This friend list is confidential to other users in the system … …

Introducing Social Network

Sorcery client stores friends' information in his friend list. This friend list is confidential to other users in the system … …

This is the dominant information for the client

Introducing Social Network



Eve is Alice's friend, but Bob cannot know the friend-relationship between Alice and Eve.

Introducing Social Network

Because friends' experiences can be used, social network can address cold start problem which cannot be solved by the existing reputation models … …

Introducing Social Network

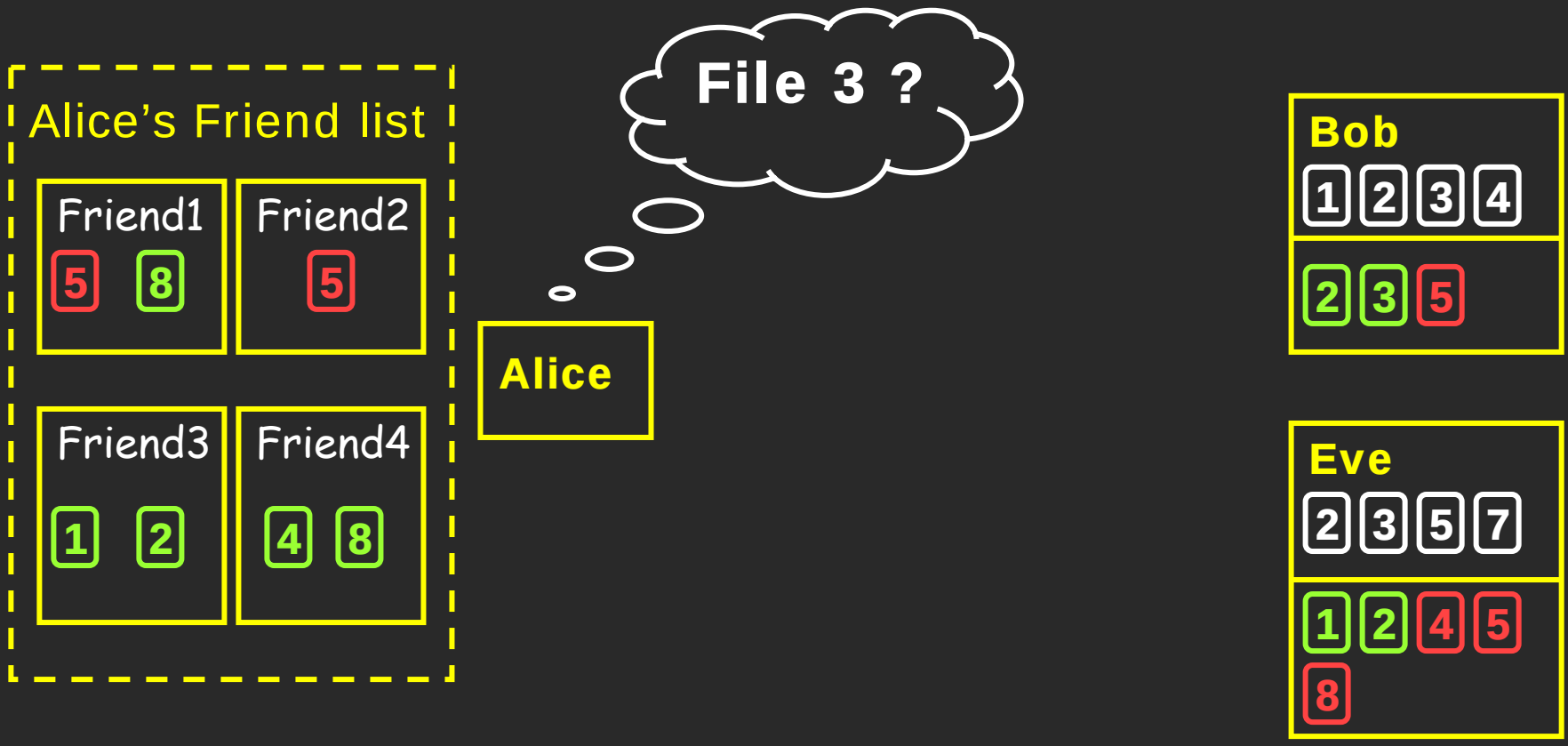
Because friends' experiences can be used, social network can address cold start problem which cannot be solved by the existing reputation models ... ...

New user joins in the system, he is easily to be deceived due to lack of experiences.

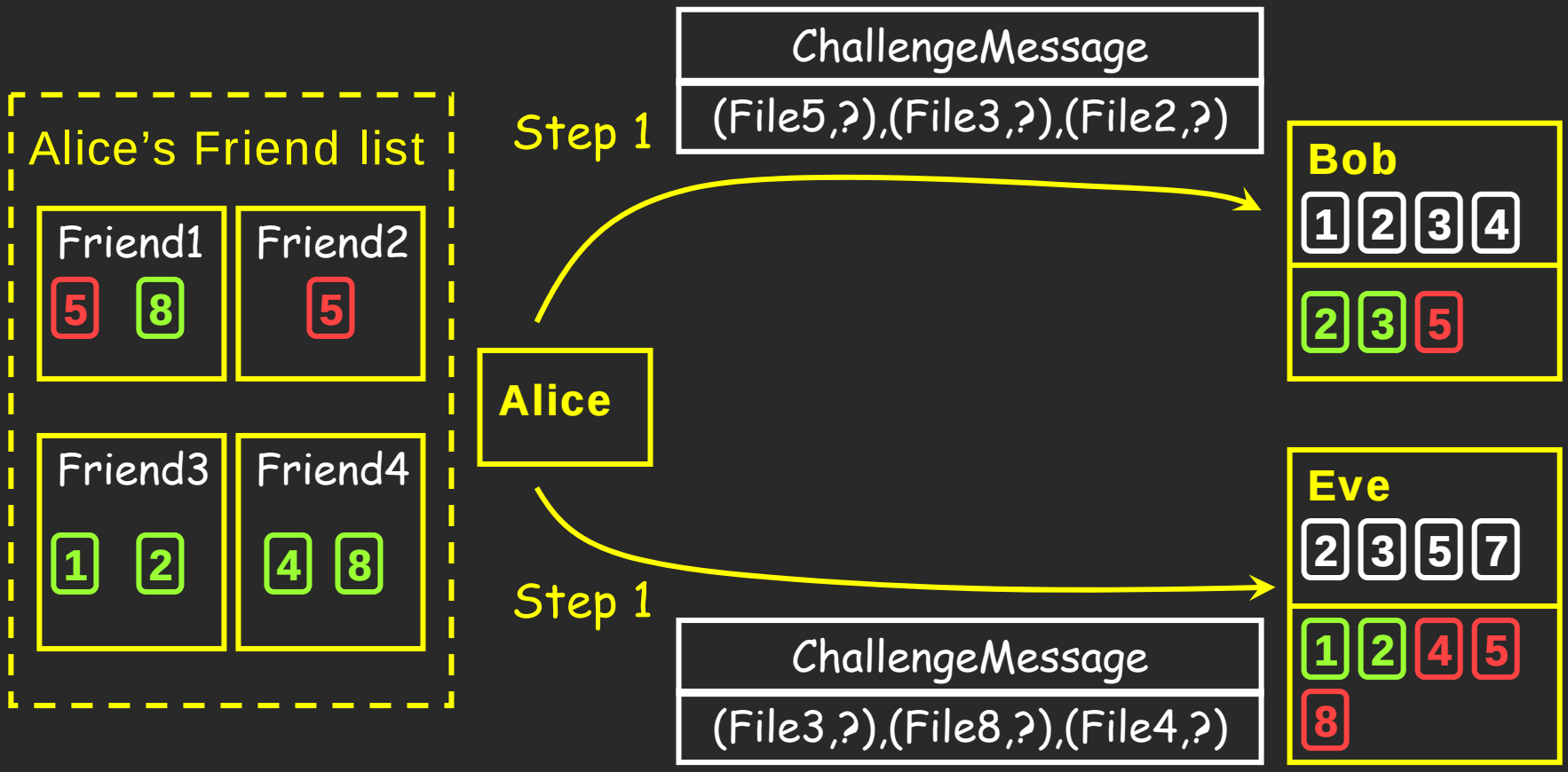
Sorcery

1. Introducing Social Network
2. Challenge-response Mechanism
3. Punishment Mechanism
4. Practical Issues

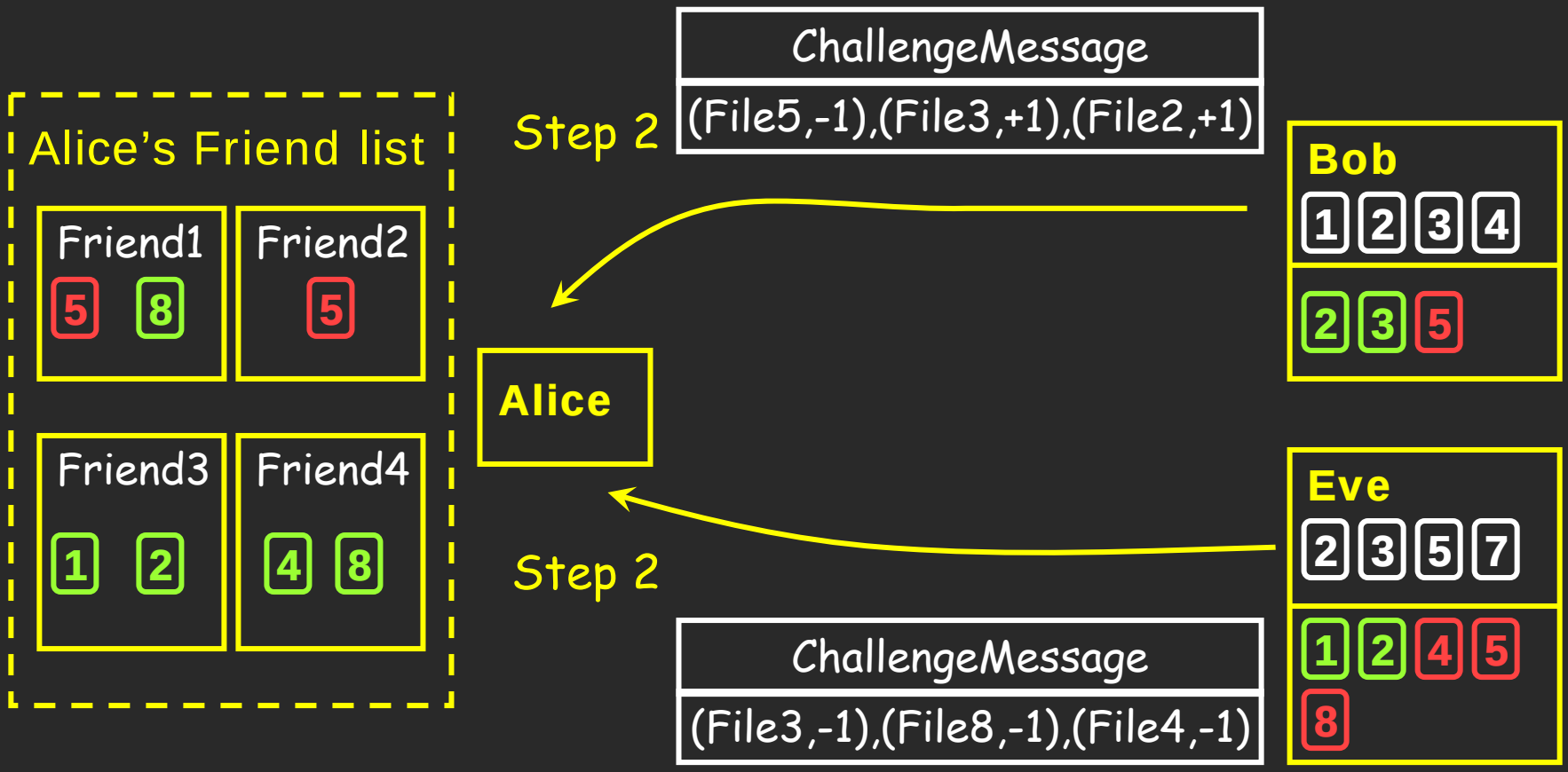
Challenge-response



Challenge-response



Challenge-response



Sorcery

1. Introducing Social Network
2. Challenge-response Mechanism
3. Punishment Mechanism
4. Practical Issues

Punishment Mechanism

Sorcery introduces reliability degree to punish deceivers, thus reducing the p-ossibility of impact brought by them ... ...

Punishment Mechanism

$$RD_{i(j)} = \begin{cases} \max(-1, RD_{i(j)} - pn^2) \\ \\ \min(1, RD_{i(j)} + r) \end{cases}$$

$RD_{i(j)}$: the reliability of i with respect to j;

p: the penalty factor;

r: the recompense factor;

n: the number of i being deceived by j.

Punishment Mechanism

$$RD_{i(j)} = \begin{cases} \max(-1, RD_{i(j)} - pn^2) \\ \min(1, RD_{i(j)} + r) \end{cases}$$

If *j* is a deceiver ... ...

Punishment Mechanism

$$RD_{i(j)} = \begin{cases} \max(-1,\ RD_{i(j)} - pn^2) \\ \min(1,\ RD_{i(j)} + r) \end{cases}$$

If *j* is not a deceiver, and *i* would like to upgrade $RD_{i(j)}$ ... ...

Sorcery

1. Introducing Social Network
2. Challenge-response Mechanism
3. Punishment Mechanism
4. Practical Issues

Practical Issues

- Lack of the Overlapping Votes
- Unreliable Friends

Practical Issues

- Lack of the Overlapping Votes
- Unreliable Friends

Non-overlapping Voting Histories

The studies in [J. Liang, INFOCOM'05] and [K. Walsh, NSDI'06] indicated it's a high probability that most peers have overlapping votes with the voters of any content item … …

Non-overlapping Voting Histories

The studies in [J. Liang, INFOCOM'05] and [K. Walsh, NSDI'06] indicated it's a high probability that most peers have overlapping votes with the voters of any content item … …

The client should challenge some of voters of the target content item (Details see paper please).

Practical Issues

- Lack of the Overlapping Votes
- Unreliable Friends

Unreliable Friends

In the practical applications, some friends may be online deceivers or compromised, Sorcery utilizes similarity based on cosine technique to filter those unreliable friends (The concrete equation see paper please) … …

Evaluation

I Simulation Setup

II Experimental Results

Evaluation

I **Simulation Setup**

II **Experimental Results**

Simulation Setup

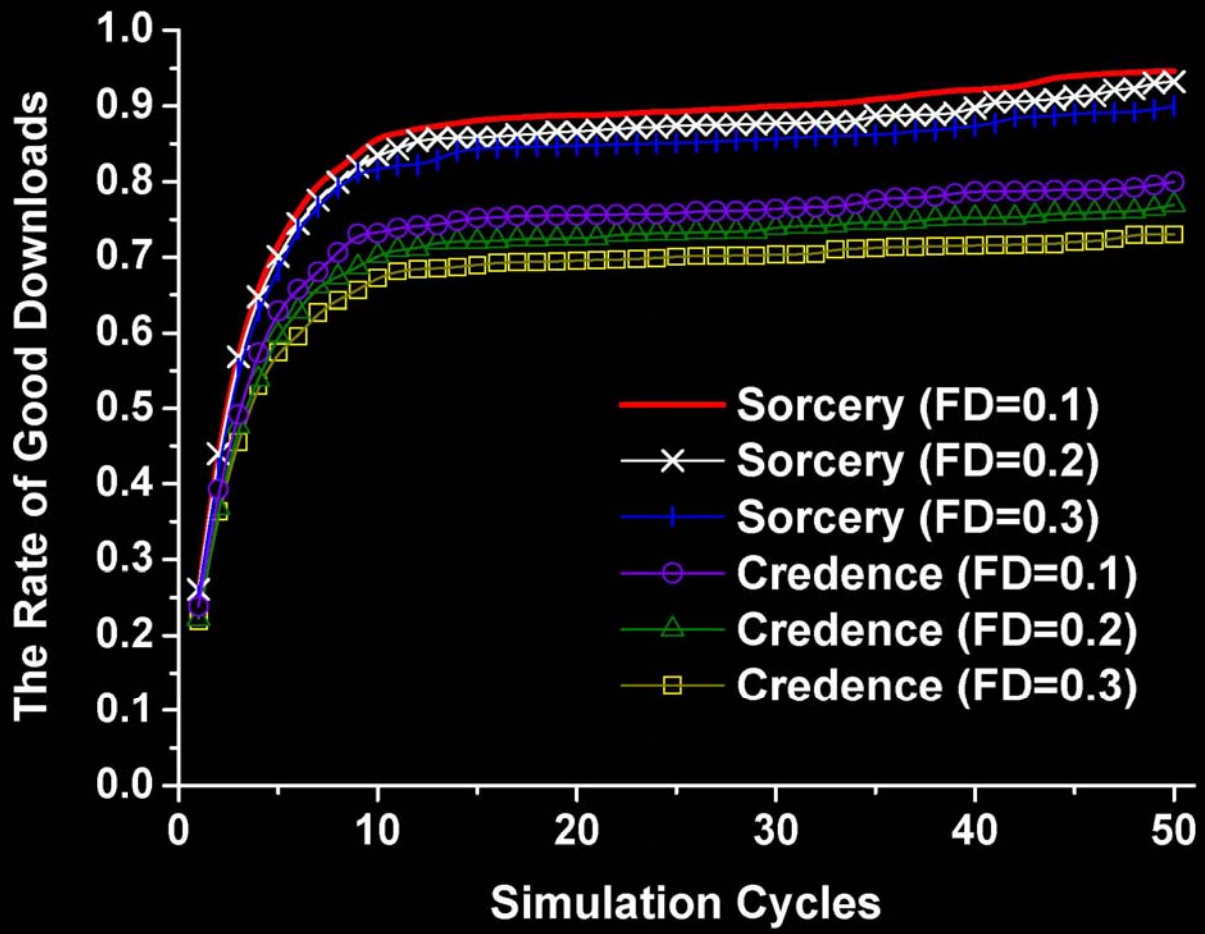
- Network Model: Gnutella Prototype
- Peer Model: 5, 000 Peers
- Social Model: Kleinberg Model
- Content Model:
  - 1,000 (Titles) X 500 (Versions) (50 good)
  - Zipf Distribution a=0.8

Evaluation

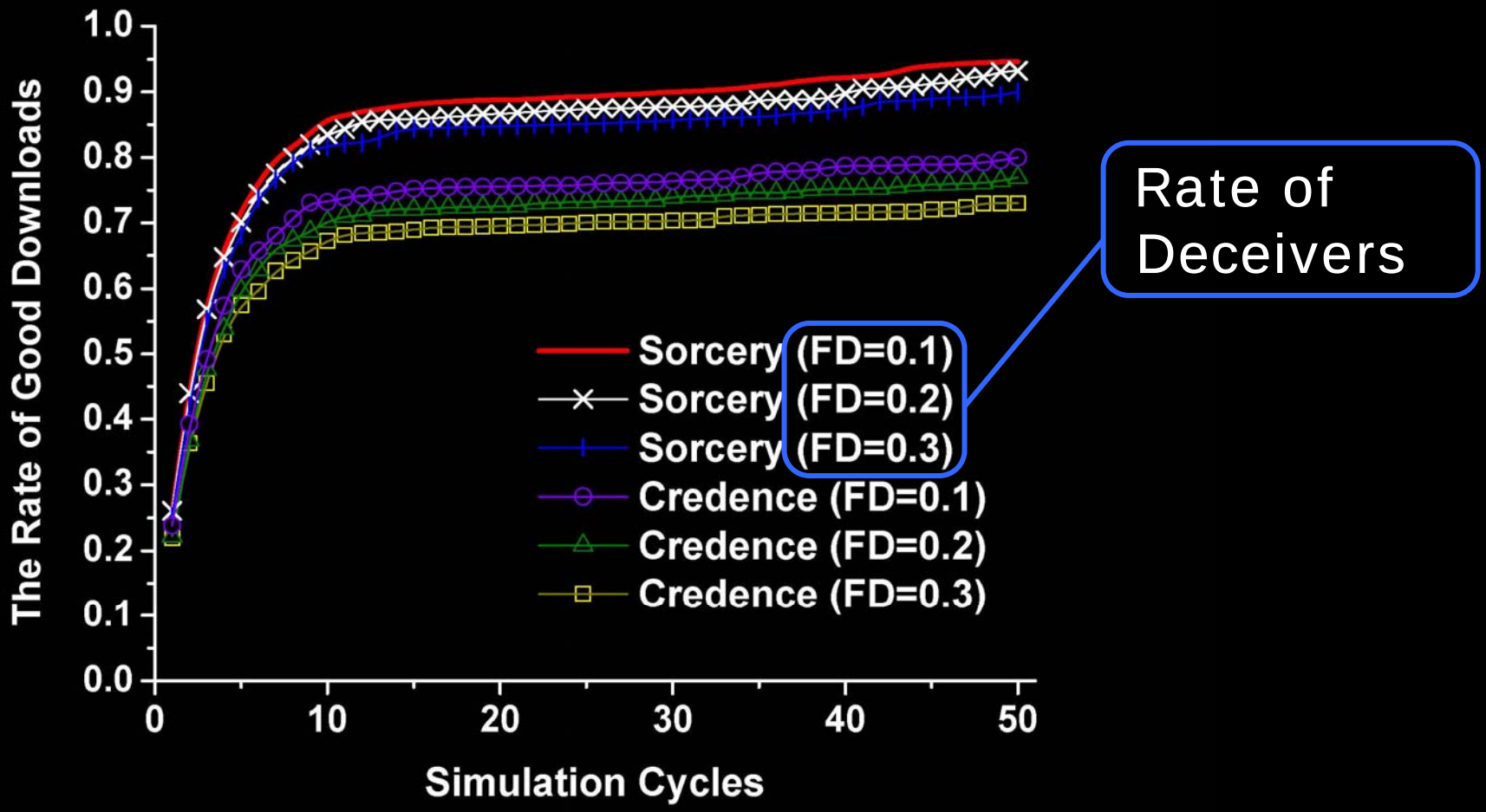
I Simulation Setup

II Experimental Results

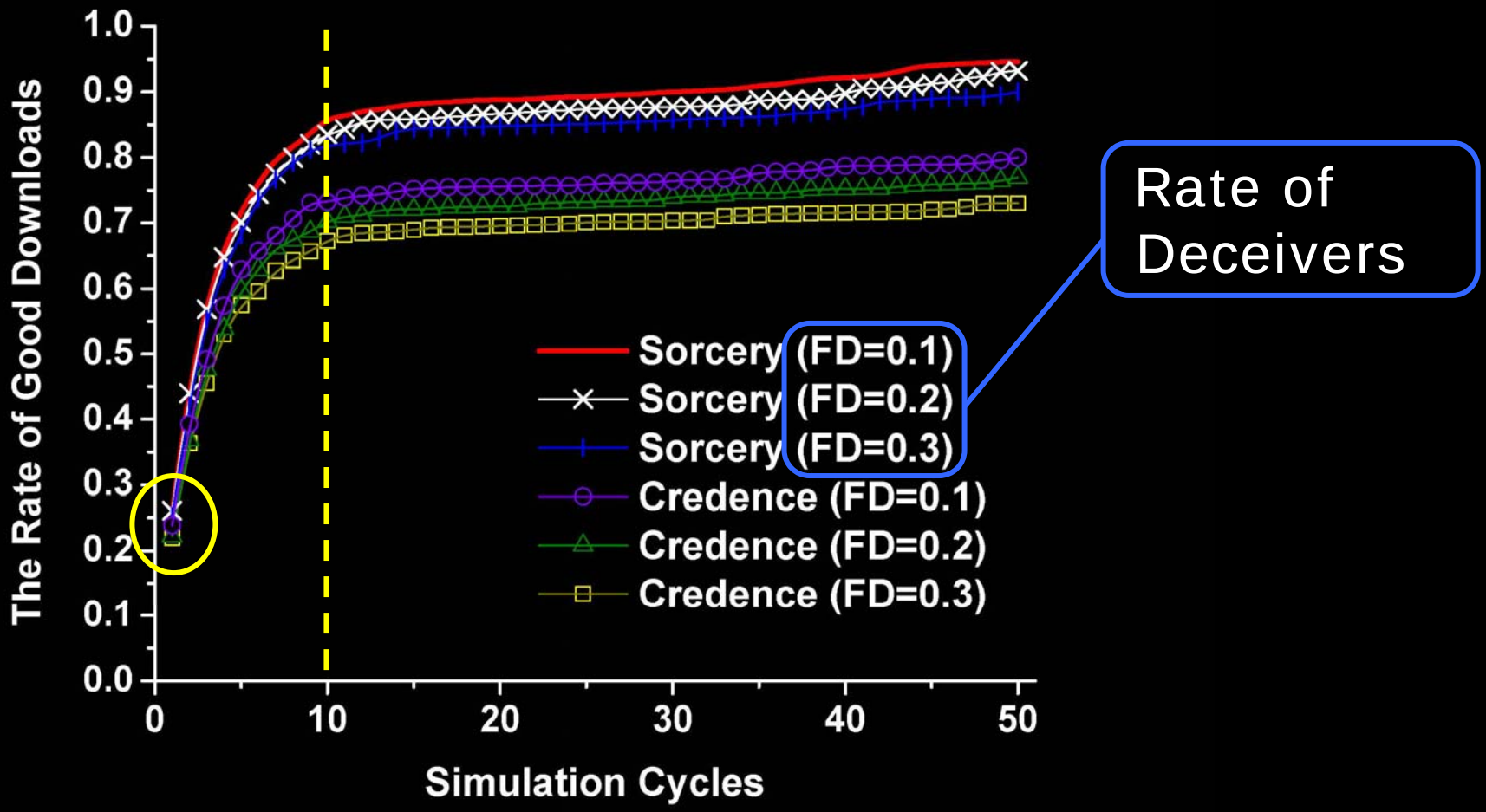
Normal Deceivers



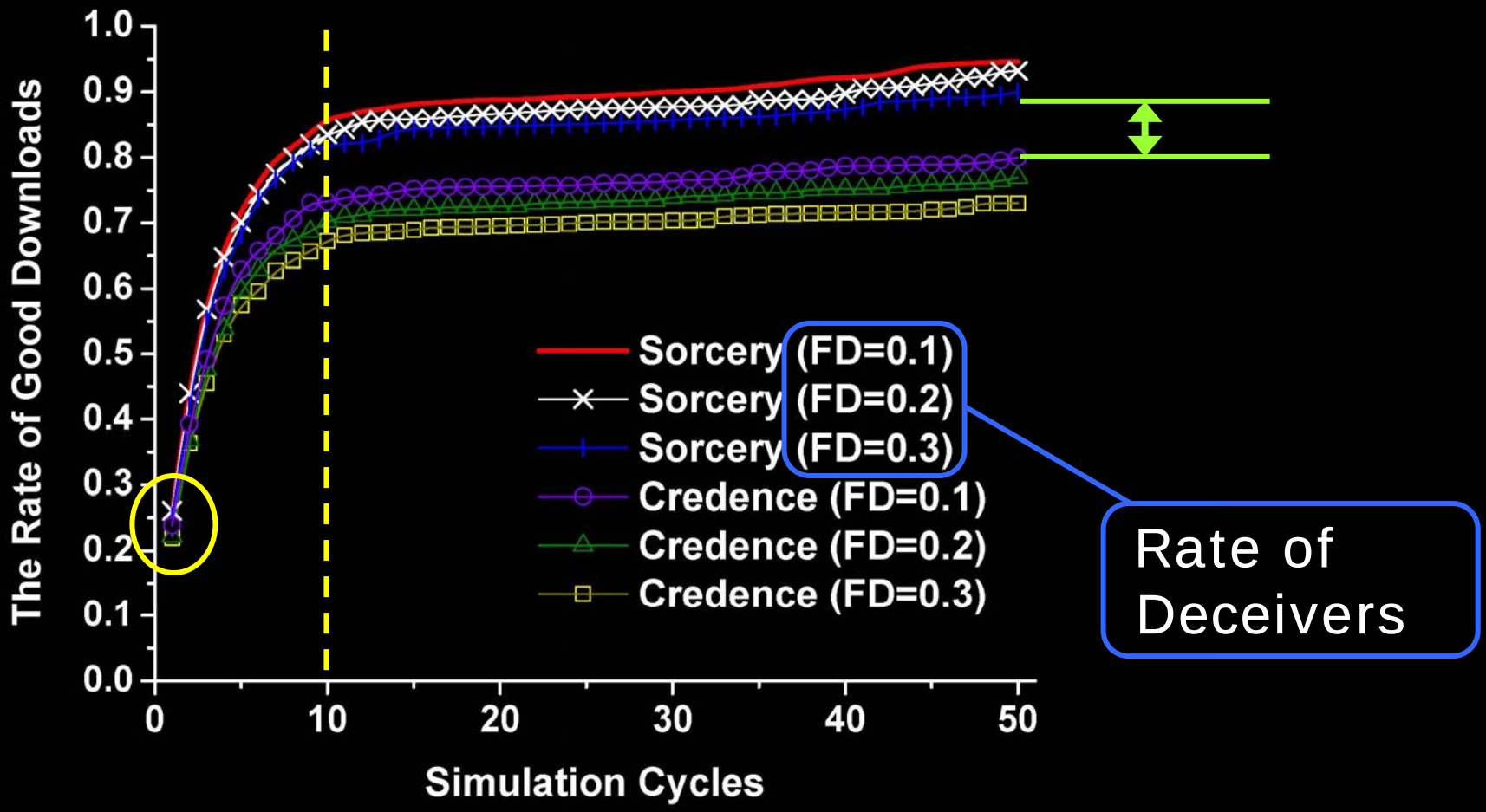
Normal Deceivers



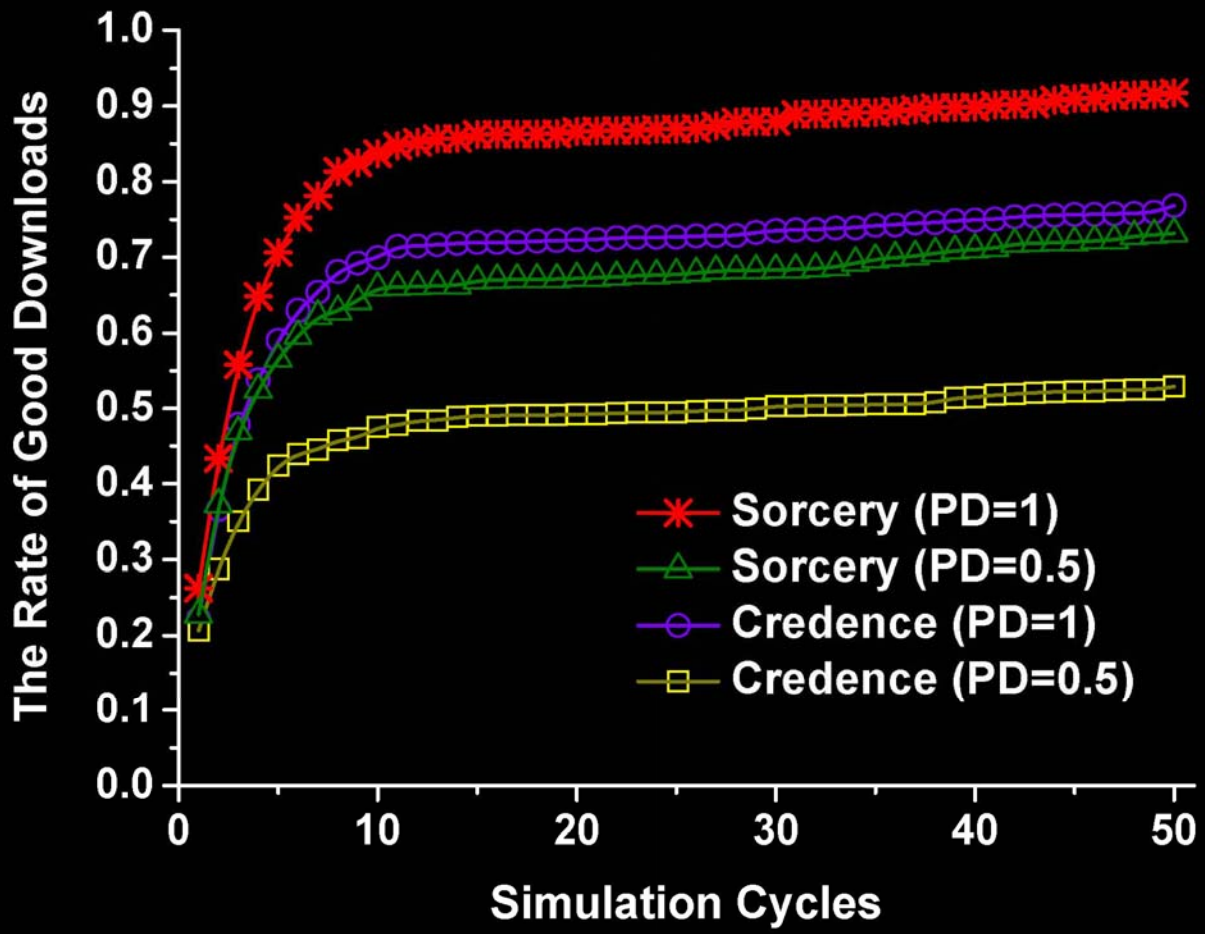
Normal Deceivers



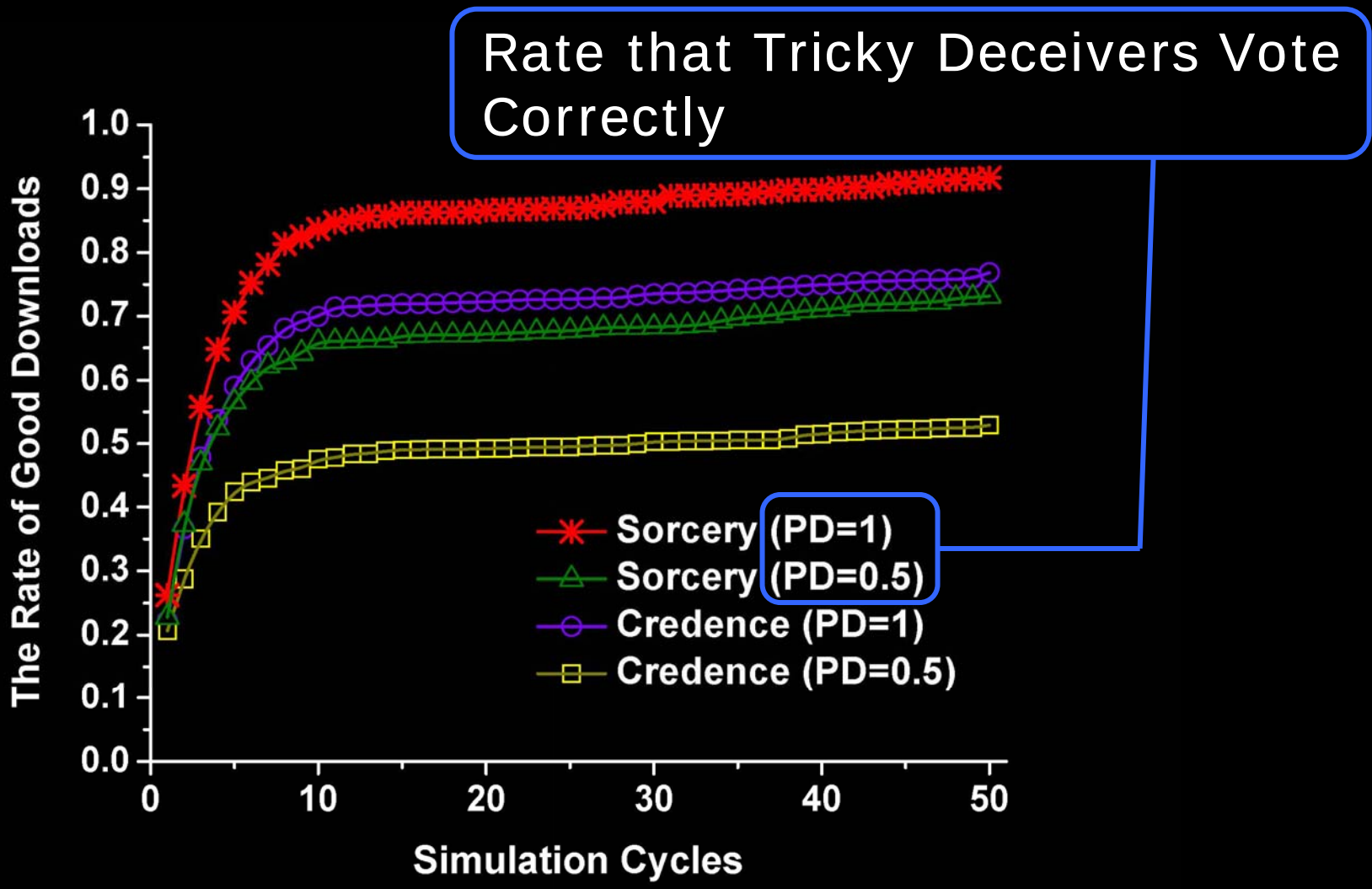
Normal Deceivers



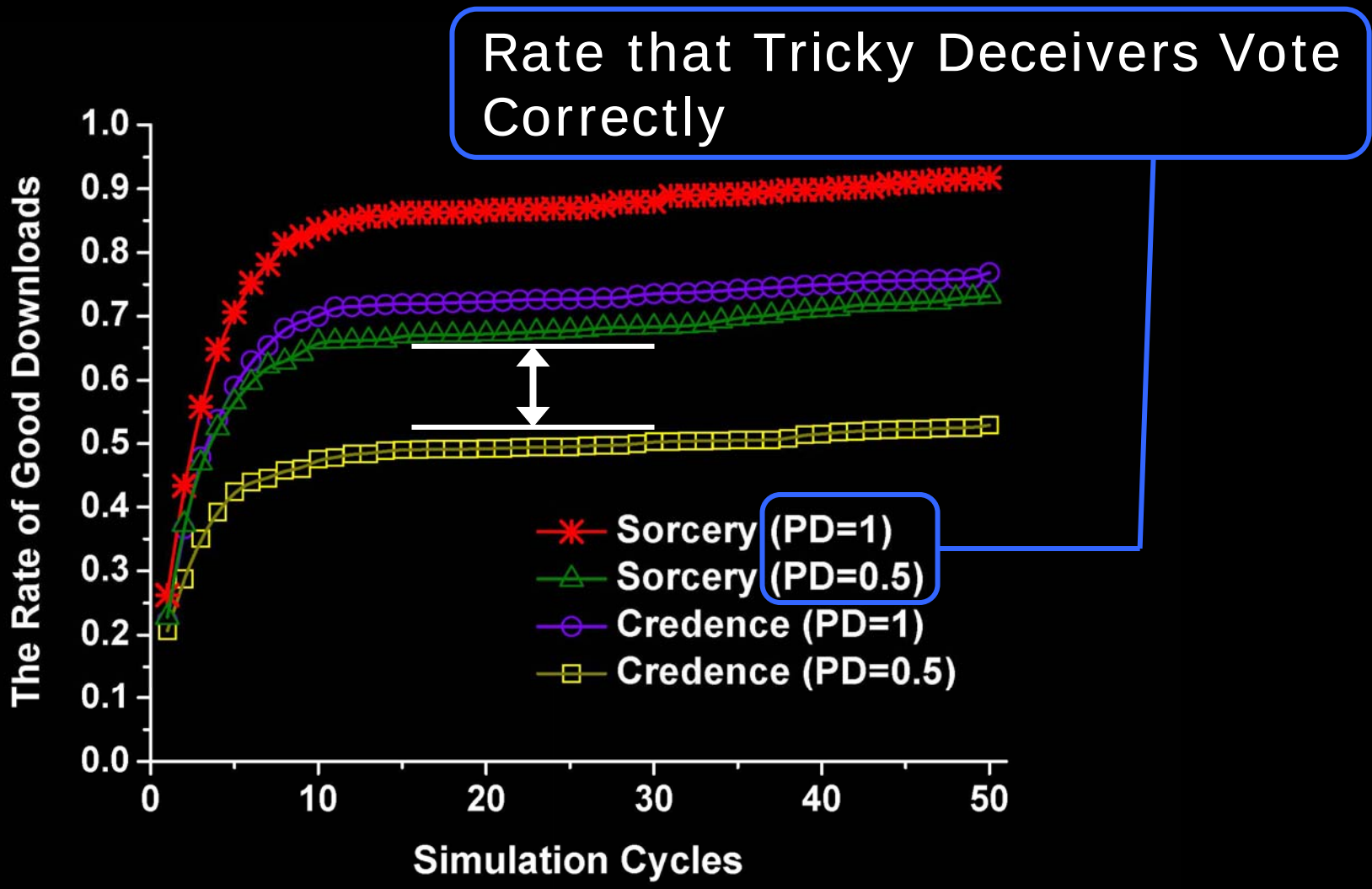
Tricky Deceivers



Tricky Deceivers



Tricky Deceivers



Conclusion and Discussion

- How to resist three types of attacks?
  - Man-in-the-Middle (MITM) Attack
  - Sybil Attack
  - Denial-of-Service (DoS) Attack

Q & A

Thank you !