NCShield:

Securing Decentralized, Matrix Factorization-Based Network Coordinate Systems

Shining Wu[1], Yang Chen[2],
Xiaoming Fu[1], Jun Li[3]

[1] University of Goettingen, Germany
[2] Duke University, USA
[3] University of Oregon, USA

computer NETWORKS

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

Outline

- 1. Introduction (NC & MFNC)
- 2. Security Issues & Attack Modeling
- 3. NCShield & Evaluation
- 4. Summary & Future Work

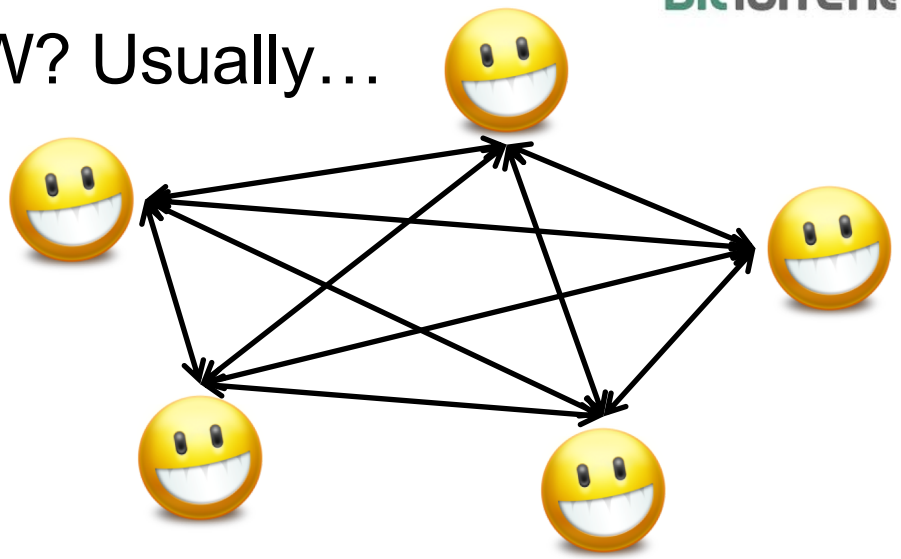
1.1 Network Coordinate (NC) Systems

- Network distances (round-trip times) are important
  - p2p streaming
  - online/mobile gaming
  - p2p file sharing
  - cloud server selection
  - etc.

BitTorrent

XBOX 360

- HOW? Usually…

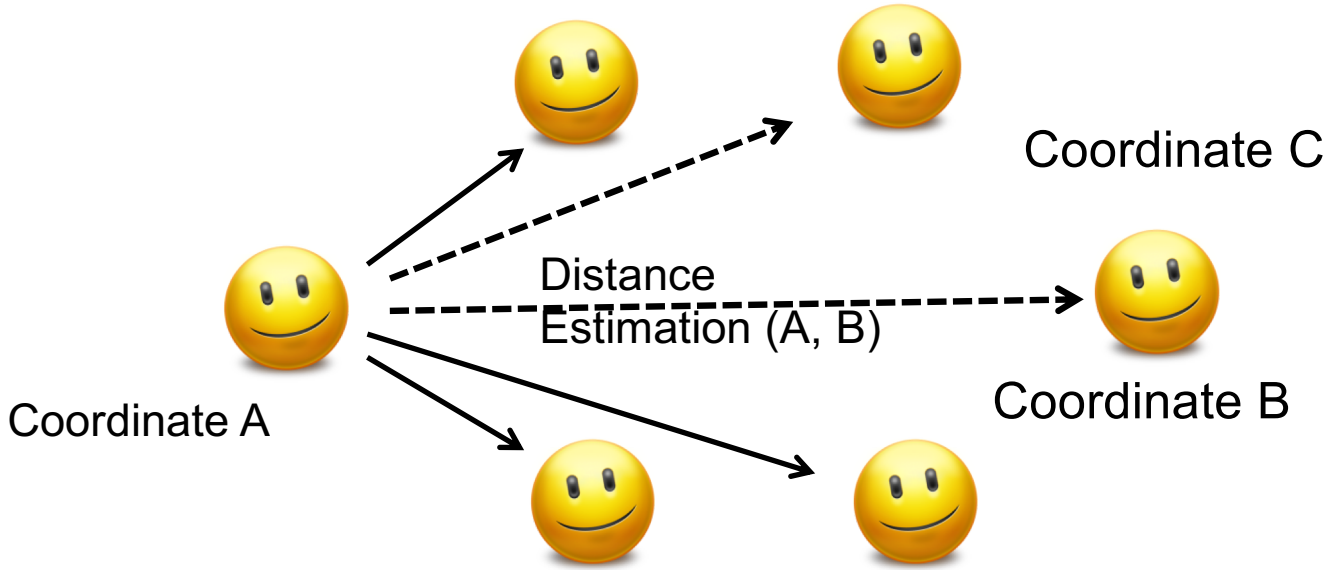


n-node network:
O(n^2) measurements !

1.1 Network Coordinate (NC) Systems

- NC: scalable way of estimating Internet distances (RTTs) with O(n) measurements!

Each node has a **Fixed** number of reference nodes (neighbors)



Constant * n: Not $O(n^2)$ measurements any more!

1.1 Network Coordinate (NC) Systems

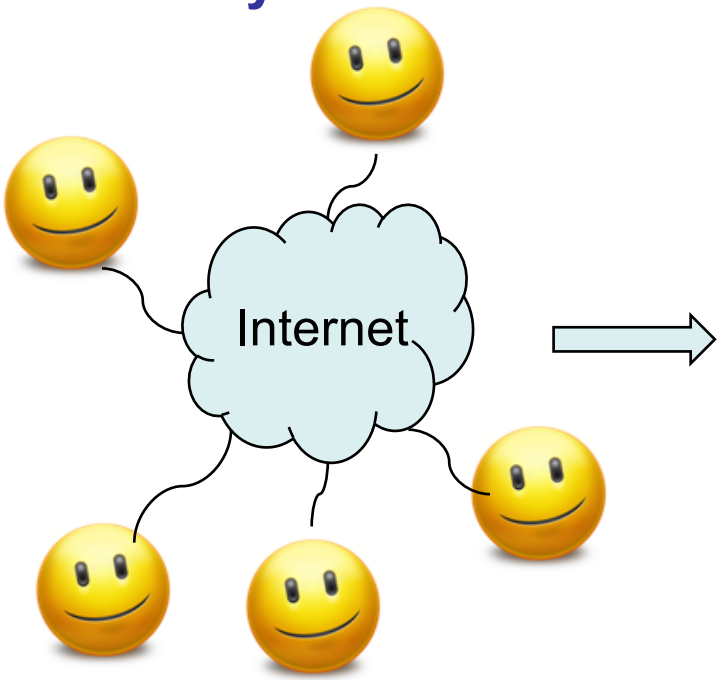
- System Structure
  - Centralized (landmark based)
  - **Decentralized (scalability)**

- Based on different mathematical models
  - Euclidean-based NC systems (ENC systems)
    - GNP, Vivaldi, PIC
    - ***Low prediction accuracy***
  - **Matrix factorization-based NC systems (MFNC systems)**
    - IDES, DMF, Phoenix

GNP: [T. S. E. Ng et al. INFOCOM'02]. PIC: [M. Costa et al. ICDCS'04]. Vivaldi: [F. Dabek et al. SIGCOMM'04].
IDES: [Y. Mao et al. JSAC'06]. DMF: Y. Liao et al. Networking'10]. Phoenix: [Y. Chen et al. TNSM'11].

1.2 MFNC Systems

- Matrix factorization-based NC systems
  - In a network of **n** nodes
  - Goal: to obtain or approximate n-by-n distance matrix D, **accurately**



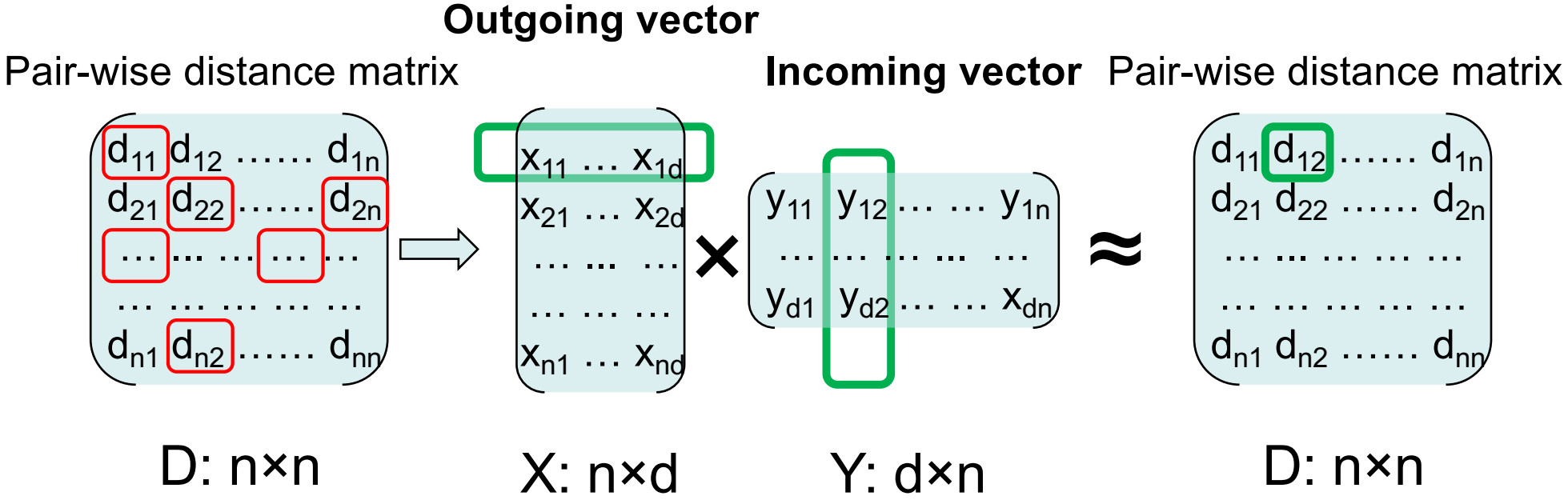
Pair-wise distance matrix

$$\begin{matrix} d_{11} & d_{12} & \cdots\cdots & d_{1n} \\ d_{21} & d_{22} & \cdots\cdots & d_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ d_{n1} & d_{n2} & \cdots\cdots & d_{nn} \end{matrix}$$

D: n×n

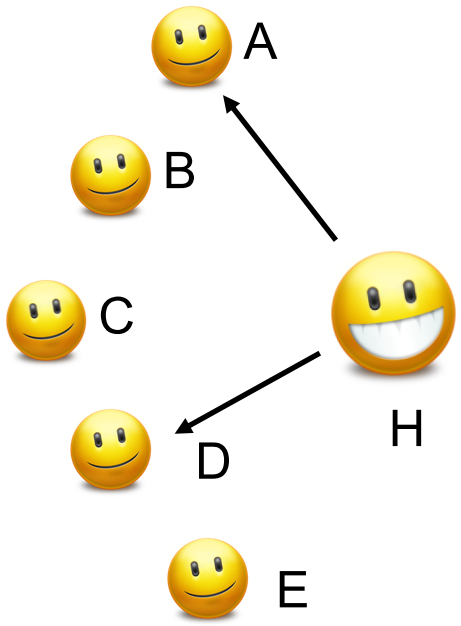
1.2 MFNC Systems

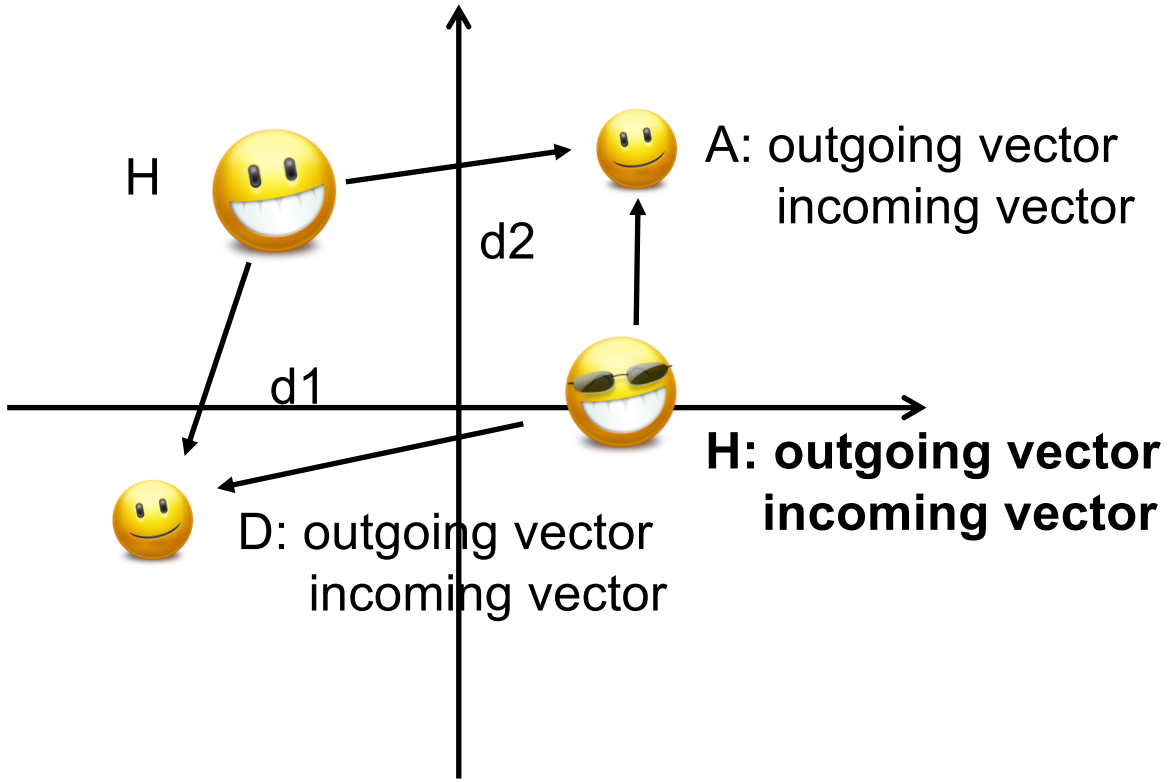
- Based on matrix factorization model
  - Each node has an **outgoing vector** and an **incoming vector**, both d-dimensional, as the **coordinates**. (d<<n)
  - Estimated distance: **dot product** calculation.



1.2 MFNC Systems

- How a newcomer node obtains its outgoing and incoming vectors?

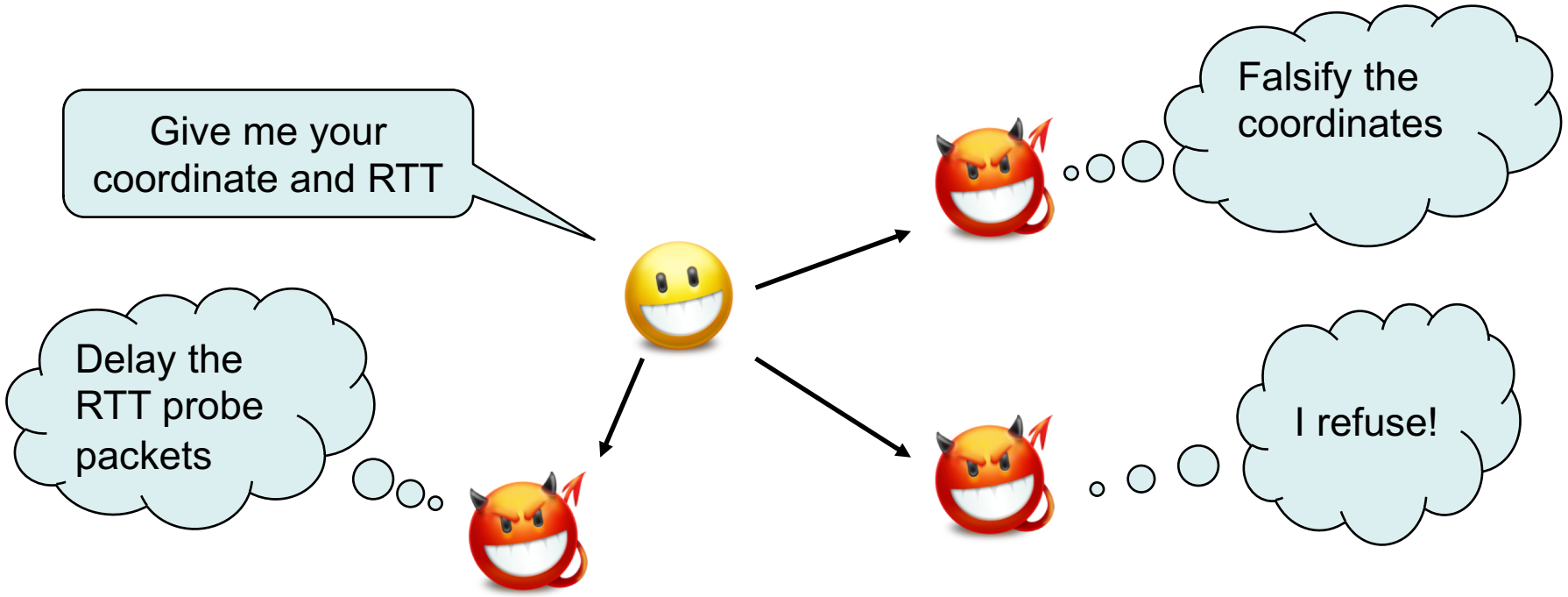




Distance(A,B) ≈ A(outgoing vec) · B(incoming vec)

2.1 Security Issues

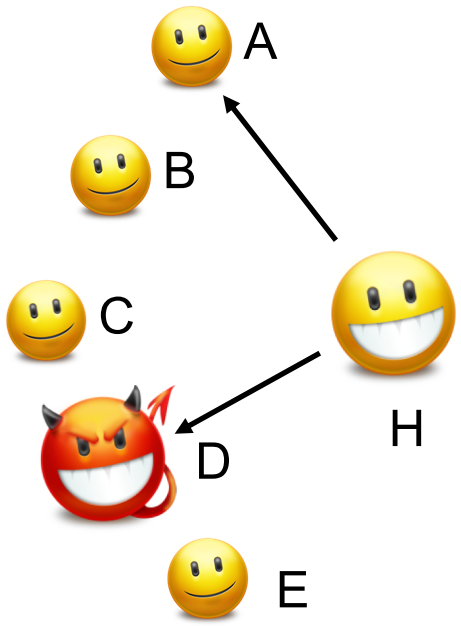
- Decentralized MFNC systems could suffer from insider attacks



[1]:[M. Kaafar et al. SIGCOMM Workshop on Large-Scale Attack Defense, 2006.].

2.1 Security Issues

- E.g. Decentralized MFNC systems face insider attacks.
  - Newcomer H, neighbor A and D.



	Outgoing	Incoming	Distance to H
A	(3,5)	(1,6)	31
D	(8,2)	(11,3)	26
H	(1,5)	(2,5)	

	Outgoing	Incoming	Distance to H
A	(3,5)	(1,6)	31
D	(4,4)	(4,2)	36
H	(7,4)	(7,2)	

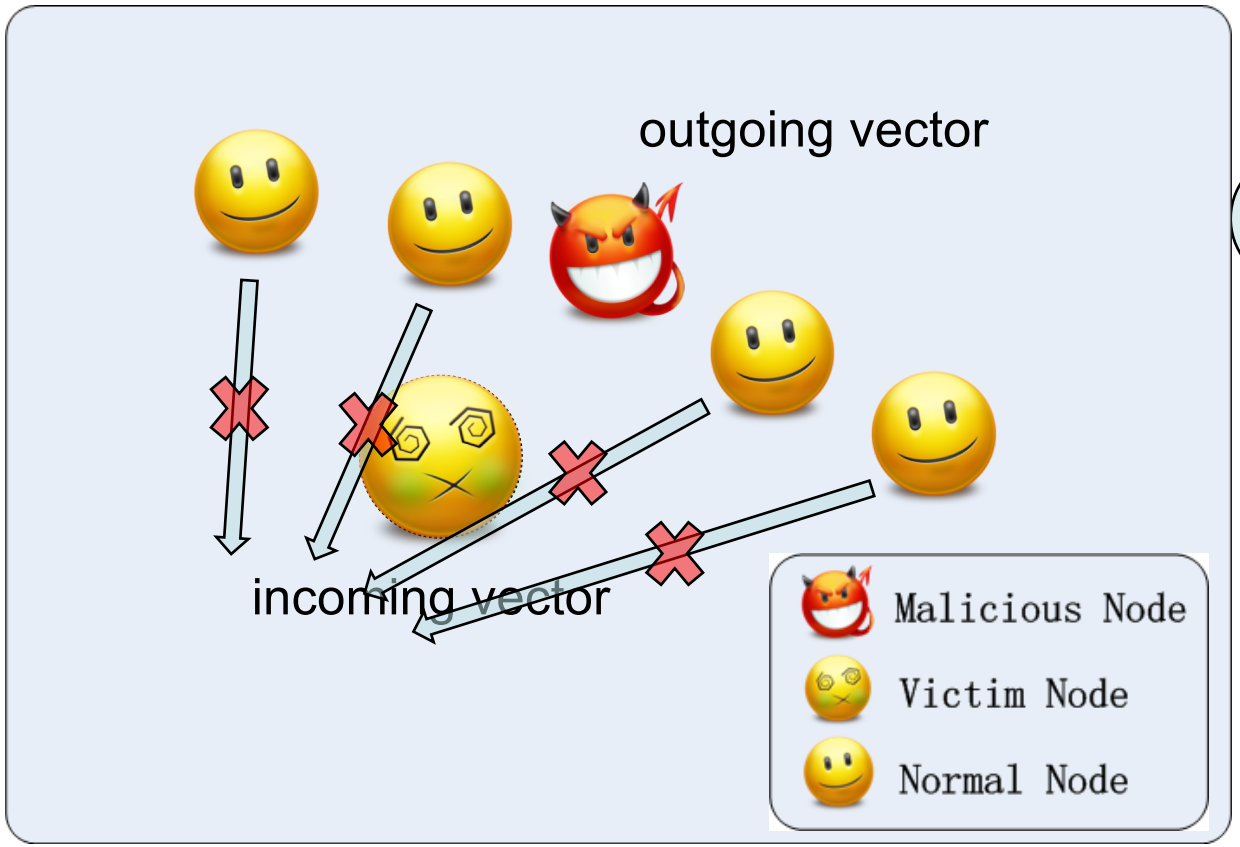
2.2 Attack Modeling

- Classifications of attacks (based on malicious purposes)
  - a. Disorder attack: To reduce the accuracy of entire system

My **outgoing** and **incoming** vectors are **not accurate** enough for distance estimation!

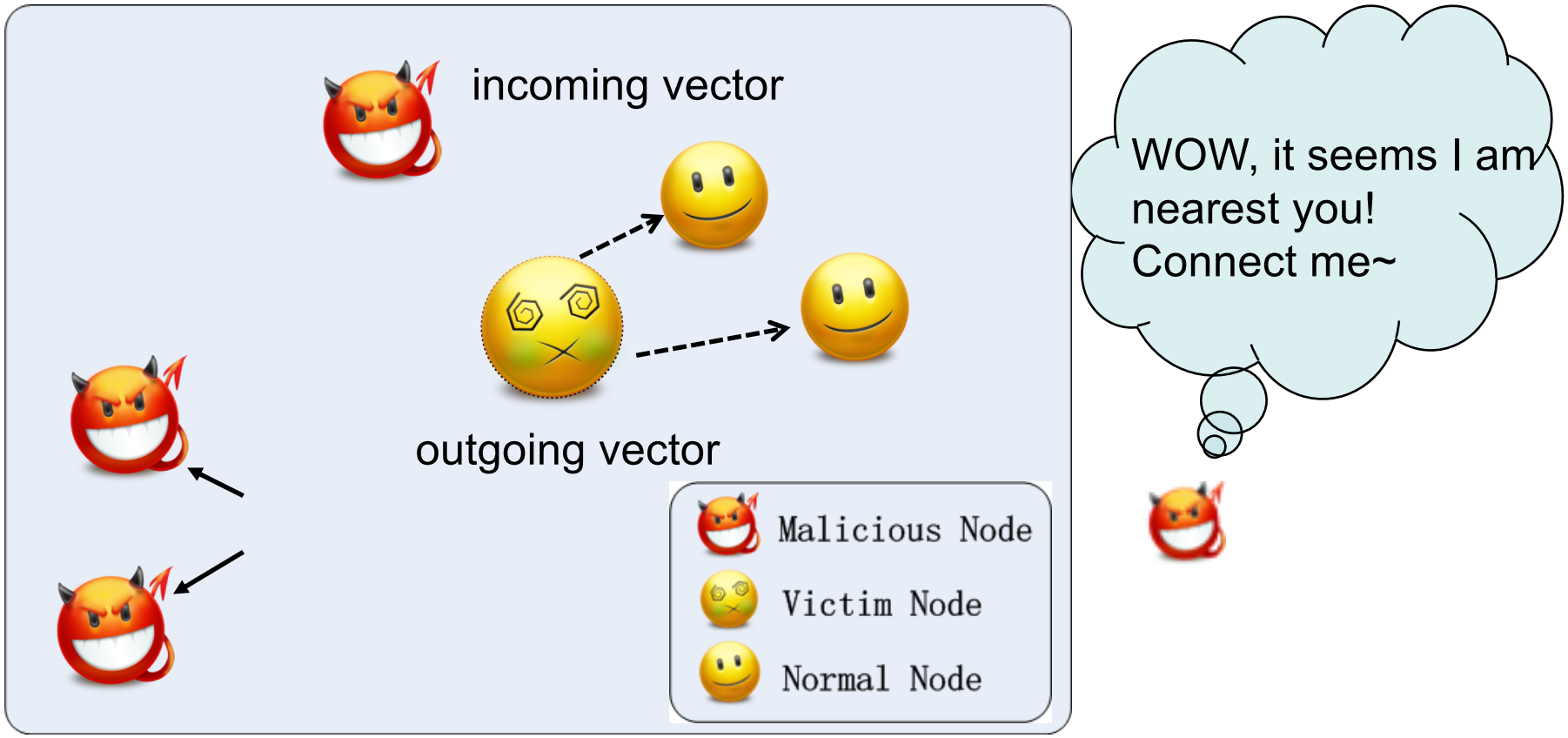
2.2 Attack Modeling

- Classifications of attacks (based on malicious purposes)
  - b. Repulsion attack: To make victims look far away, thus reducing their attractiveness



2.2 Attack Modeling

- Classifications of attacks (based on malicious purposes)
  - c. Isolation attack: To make victims in a certain area, where many malicious nodes may be around



3.1 NCShield

- How can we deal with the attacks above?
- A Defense approach is desired!

- Considerations of such defense approach:

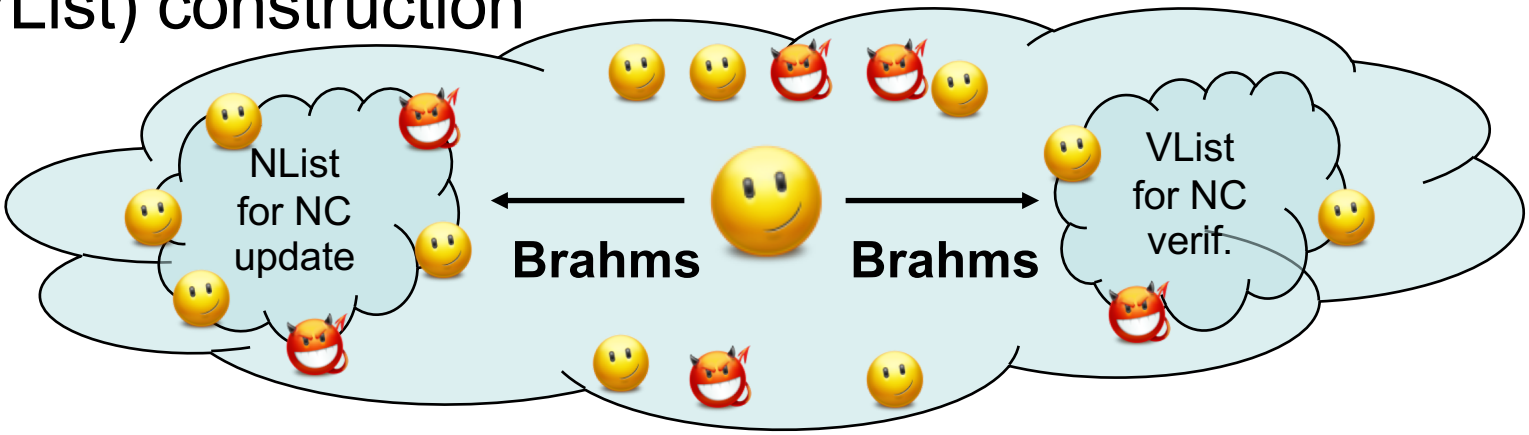
Item	Choice 1	Choice 2	Reason
Structure	Centralized	**Decentralized**	Scalability
Mechanism	History info	**Trust & reputation**	Node churn
Infrastructure	DHT	**Gossip algorithm**	Overhead
TRS model	Agent-Surveyor	**Score and vote**	Complexity

3.1 NCShield

- NCShield: A score and vote based approach

Work flow control		
a. node sampling algorithm	b. extra information model	c. coordinate verification model

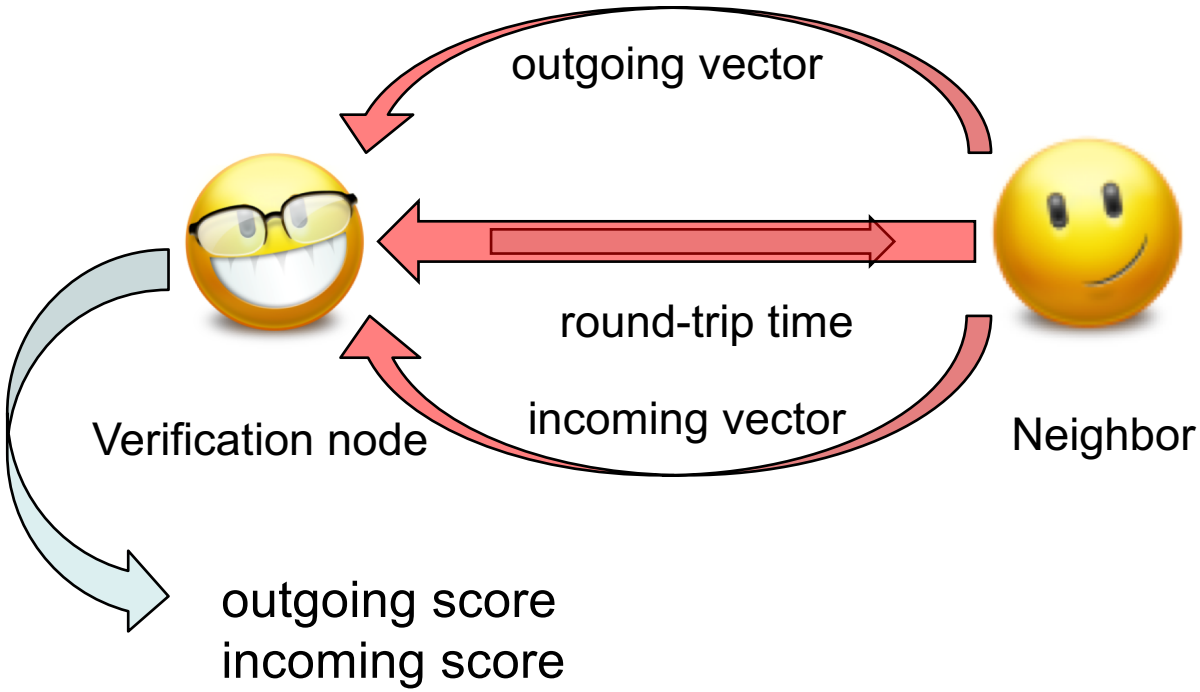
- Part a. Secure gossip algorithm (Brahms) for **unbiased** node sampling -- neighbor list (NList) and verification list (VList) construction



Brahms: [E. Bortnikov et al. PODC'08]

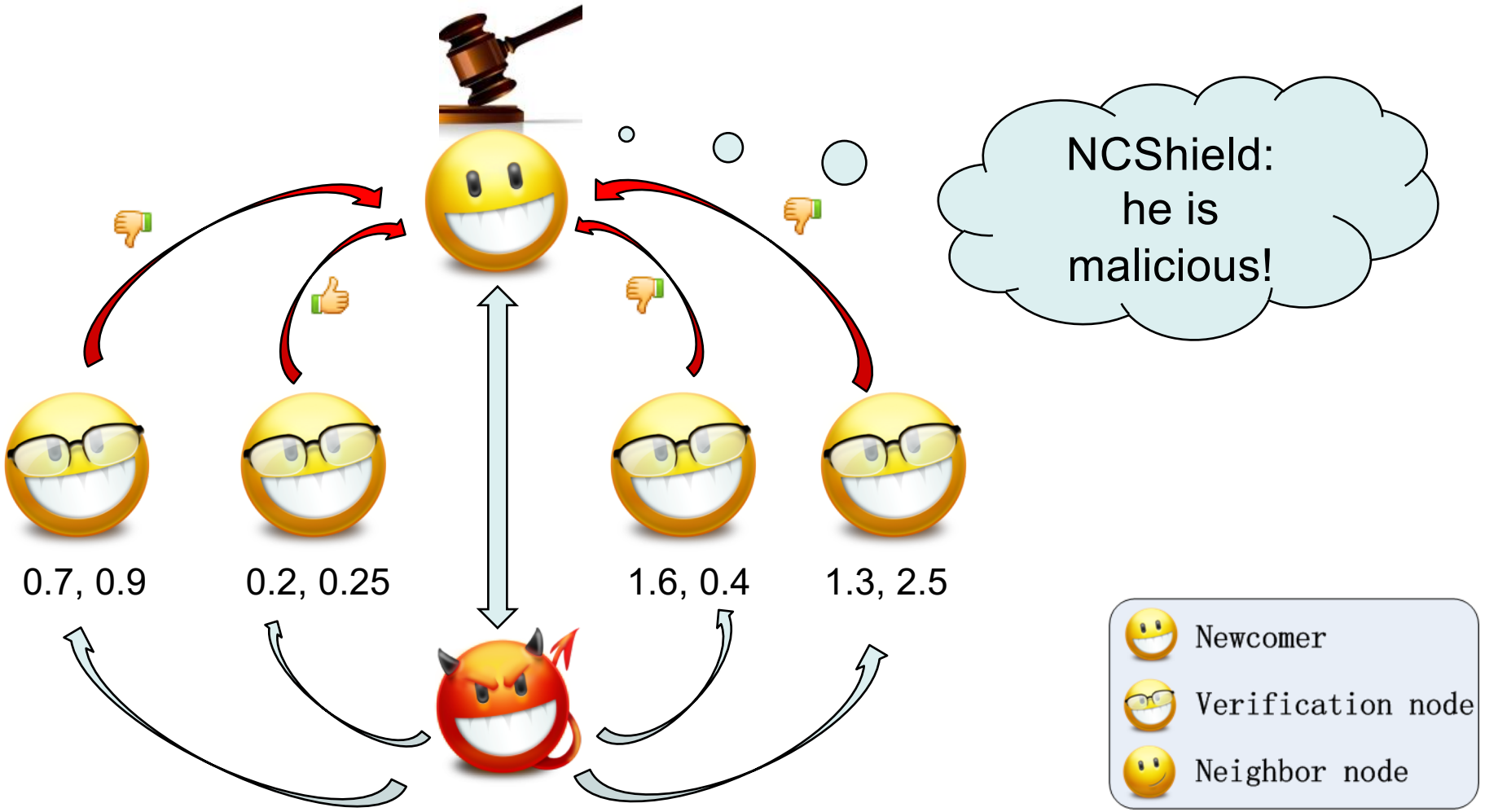
3.1 NCShield

- Part b. extra information model: dual-RE (relative error) model for **score calculation**



3.1 NCShield

- Part c. coordinate verification process: score, vote, judge



3.2 Evaluation Set-up

- NC system simulators:
  - DMF simulation environment
  - Phoenix simulation environment
- Data sets: real Internet traces
  - Aggregate data sets:
    - AMP: 110 nodes
    - PlanetLab: 335 nodes
    - King: 1740 nodes
  - ”k200-allpairs-1h” dynamic data set: 200 nodes, 99 snapshots
- Typical parameters as in Phoenix and DMF systems.

3.2 Evaluation Set-up

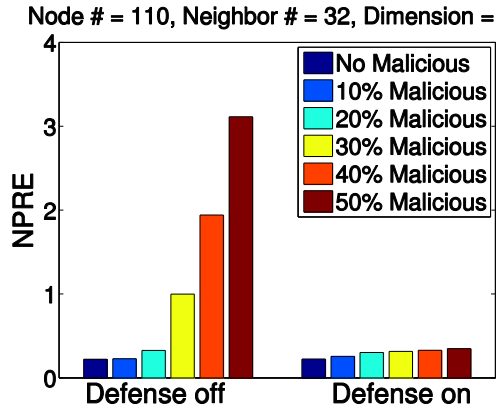
- Metrics:
  - Relative error (RE): for node i, j

$$RE = \frac{|D^E(i,j) - D(i,j)|}{\min(D^E(i,j), D(i,j))}$$

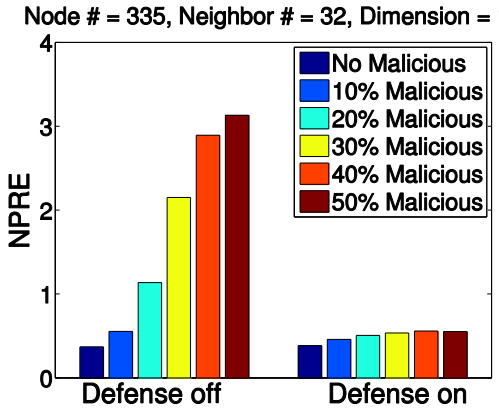
  - Ninetieth percentage relative error (**NPRE**): guarantees 90% of the links have lower RE values than it
    - NPRE = 0.4 means the RE of 90% of all evaluated links are smaller than 0.4
    - A global metric for performance evaluation of whole system
- All **3** attacks are evaluated in Phoenix and DMF systems, with aggregate data sets and dynamic data set.

3.3 Evaluations on Aggregate Data Sets

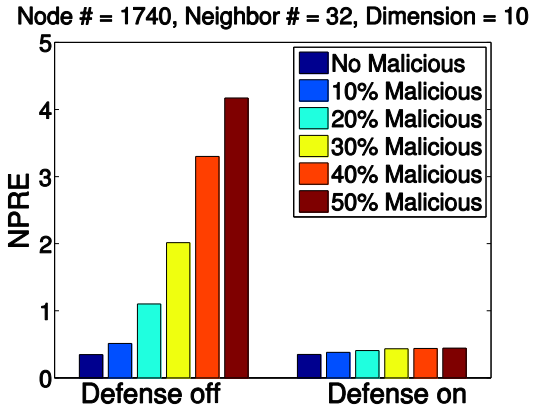
- Disorder attack



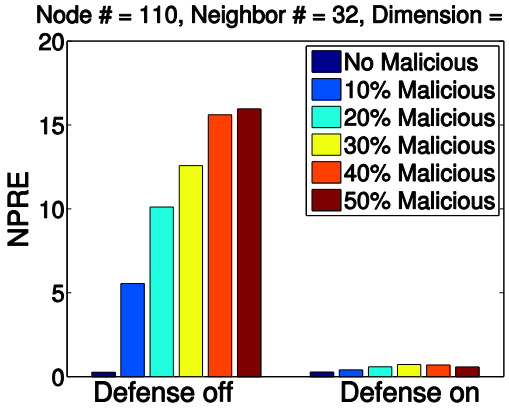
(a) Phoenix on AMP Data Set



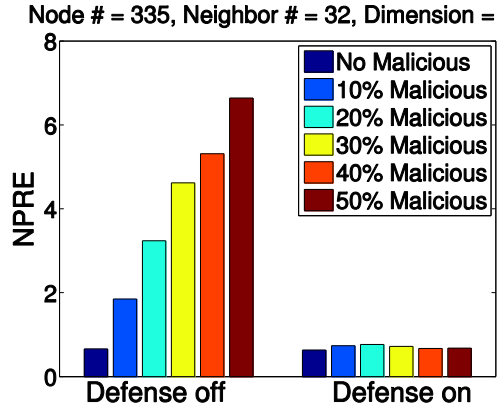
(b) Phoenix on PlanetLab Data Set



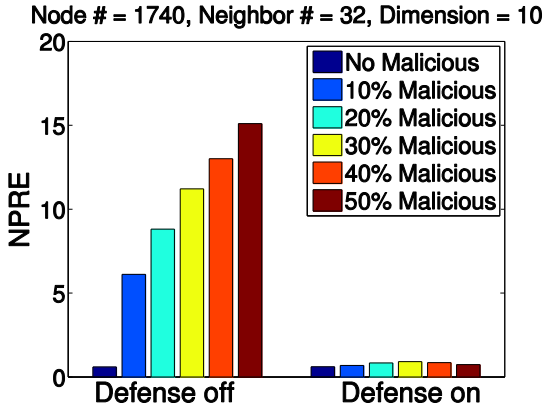
(c) Phoenix on King Data Set



(a) DMF on AMP Data Set



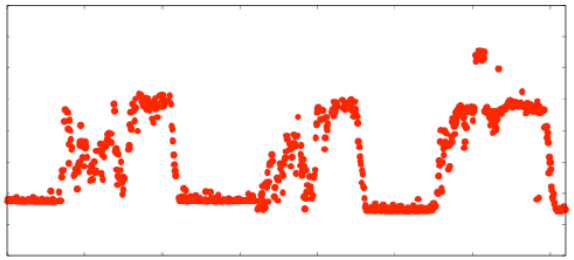
(b) DMF on PlanetLab Data Set



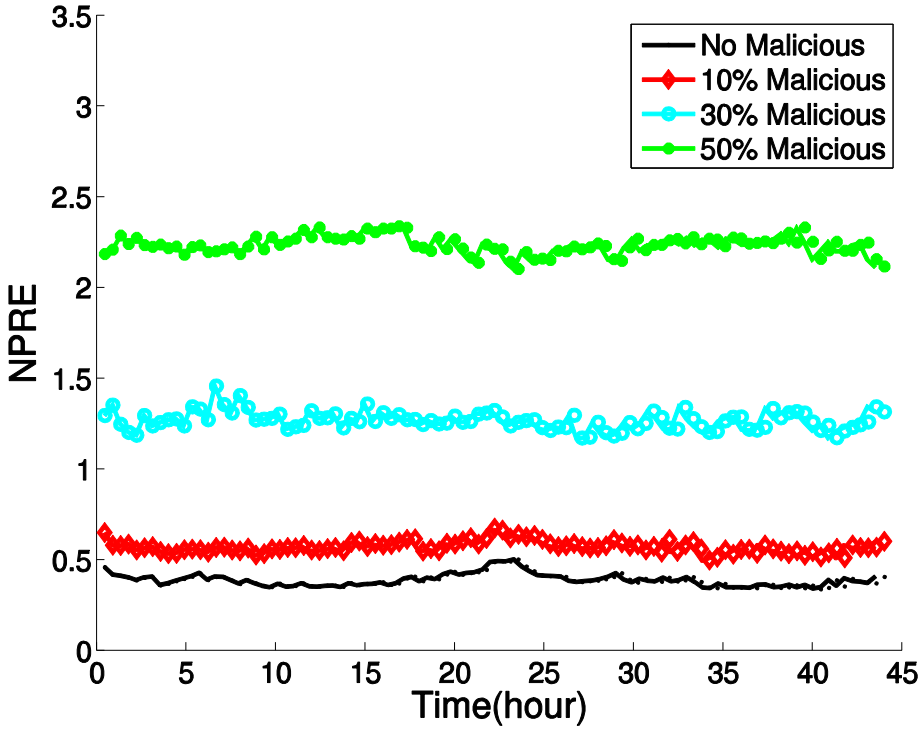
(c) DMF on King Data Set

3.4 Evaluations on Dynamic Data Set

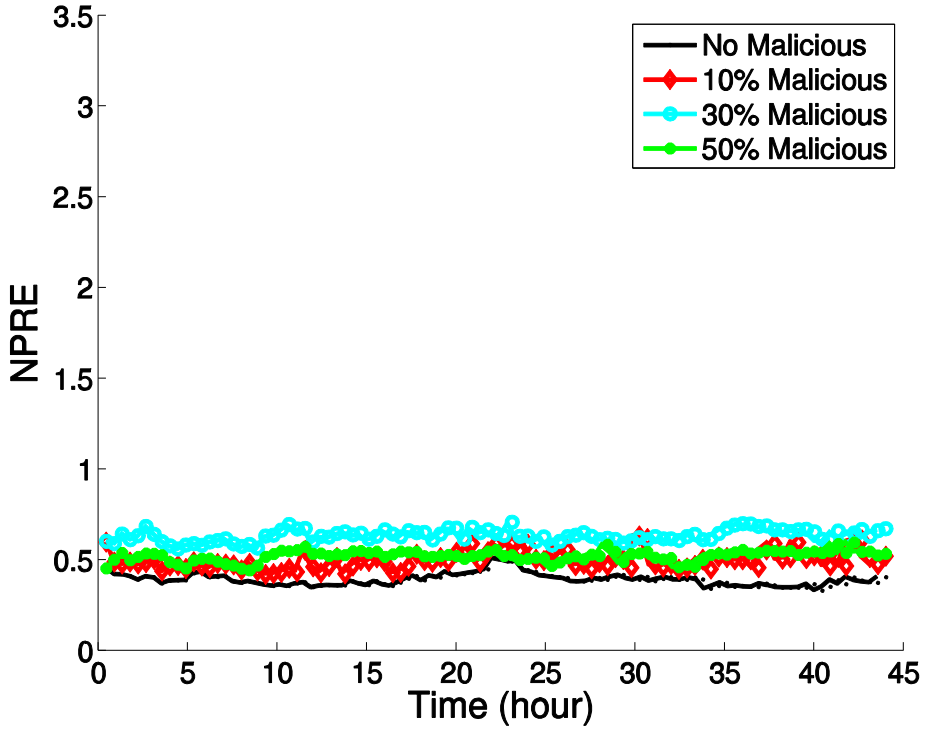
- Internet distances are time varying
- NCShield is adaptive to such variation
- Disorder attack in Phoenix system:



[P. Pietzuch et al. WORLDS'05]



w/o defense



w/ defense

3.5 Online Game Scenario Evaluation

- Identify links.RTT < **predefined threshold** (e.g. **100ms** for first-person perspective games)
- NC estimation for such link selection
- "Good" ("bad") link: a link whose measured RTT is below (above) the predefined threshold
- **Application-specified** metrics: false positive (negative) rate -- FPR and FNR

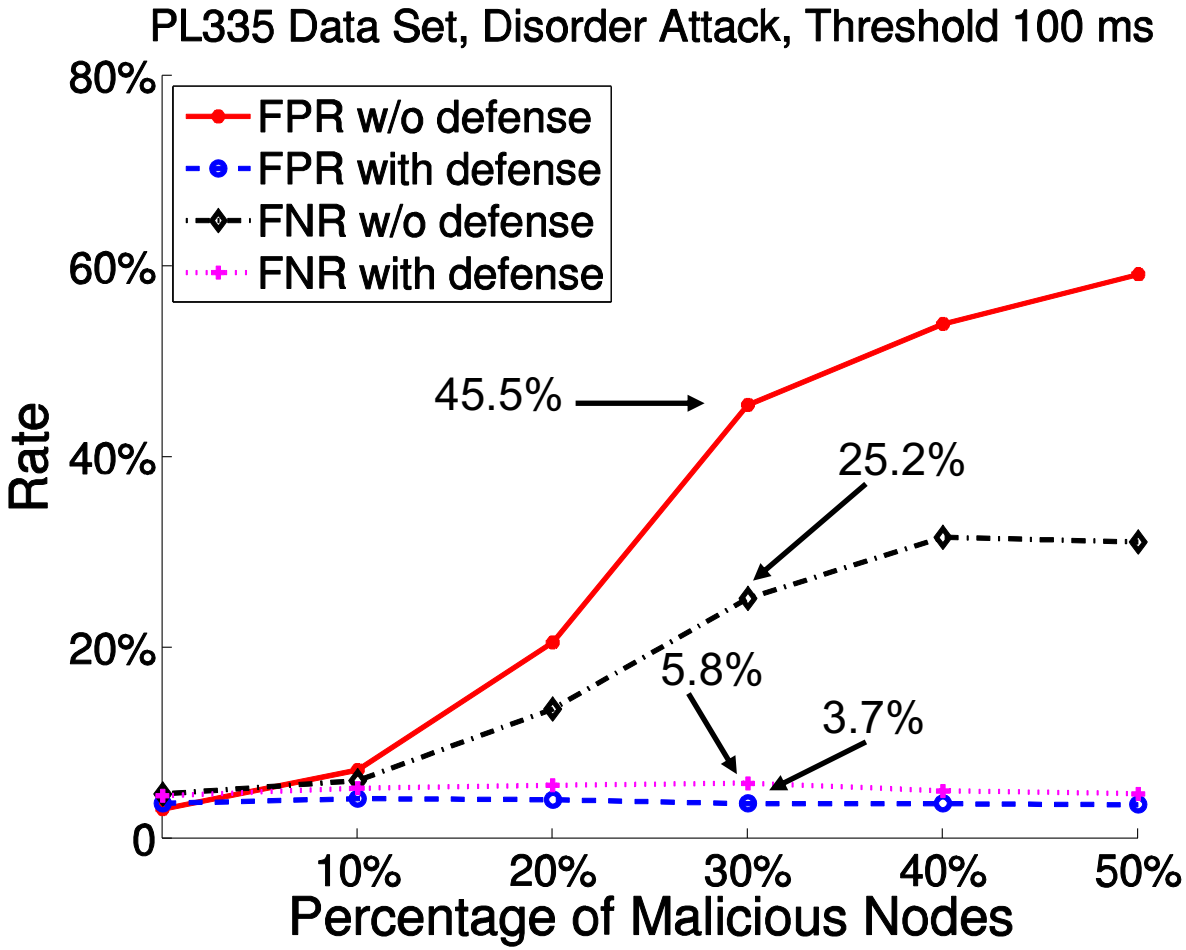
	Actual	Predicted
True Positive	good	"good"
False Positive	bad	"good"
True Negative	bad	"bad"
False Negative	good	"bad"

FPR = FP/(FP+TN)
FNR = FN/(TP+FN)

The lower, the better!

3.5 Online Game Scenario Evaluation

- Disorder attack in Phoenix system.



4. Summary & Future Work

- We modeled the attacks on decentralized MFNC systems, and showed the severity of such attacks.
- A score and vote based approach with an effective and scalable node sampling mechanism.
- **NCShield** is **practical** and **effective** according to evaluations on aggregate data sets, dynamic data set and online game scenario.
- Future work:
  - New emerging frog-boiling attacks[1]
  - Evaluations with Phoenix and DMF on a real network

[1]Frogboiling attack: [E. Chan-Tin et al. TISSEC 2011].

Thank you very much! Q&A!

Gänseliesel (*Goose girl*)

The most kissed girl in the world.

BAK: Relative Error

$$RE = \frac{|D^E(i,j) - D(i,j)|}{\min(D^E(i,j), D(i,j))}$$

Mostly used in NC research work!

$$RE = \frac{|D^E(i,j) - D(i,j)|}{D(i,j)}$$

Smaller prediction will not generate high RE!

BAK: Repulsion Aggregate

NPRE OF REPULSION ATTACK AND DEFENSE

NC	Data	Defense	Percentage of Malicious Nodes			
			0%	10%	30%	50%
Phoenix	AMP	OFF	0.144	0.161	0.628	2.628
		ON	0.181	0.182	0.219	0.244
	PL	OFF	0.346	0.391	0.636	2.861
		ON	0.343	0.402	0.491	0.538
	King	OFF	0.394	0.512	1.418	4.750
		ON	0.341	0.355	0.380	0.401
DMF	AMP	OFF	0.234	3.644	6.331	8.482
		ON	0.220	0.212	0.224	0.237
	PL	OFF	0.668	4.603	14.354	22.191
		ON	0.657	0.780	0.644	0.641
	King	OFF	0.611	13.585	35.903	50.113
		ON	0.614	0.613	0.614	0.610

BAK: Isolation Aggregate

NPRE OF ISOLATION ATTACK AND DEFENSE

NC	Data	Defense	Percentage of Malicious Nodes			
			0%	10%	30%	50%
Phoenix	AMP	OFF	0.167	0.225	0.923	2.249
		ON	0.159	0.214	0.197	0.200
	PL	OFF	0.315	0.475	0.715	4.679
		ON	0.320	0.382	0.499	0.447
	King	OFF	0.386	0.587	1.326	4.124
		ON	0.394	0.412	0.418	0.413
DMF	AMP	OFF	0.284	2.097	5.461	7.890
		ON	0.269	0.278	0.262	0.261
	PL	OFF	0.676	1.371	2.716	3.296
		ON	0.656	0.781	0.664	0.654
	King	OFF	0.657	3.970	8.430	15.431
		ON	0.513	0.516	0.523	0.524

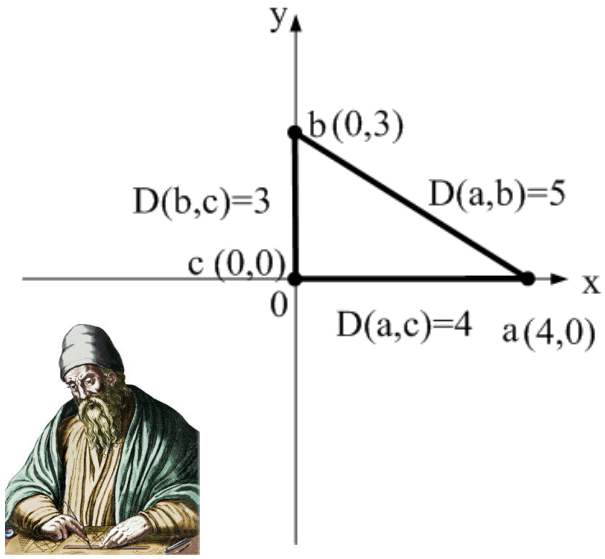
BAK: Full Dynamic Simulation Results

AVERAGE NPRE OF SIMULATION ON "K200-ALLPAIRS-1H" DATA SET

NC	Type	Defense	Percentage of Malicious Nodes			
			0%	10%	30%	50%
Phoenix	Dis.	OFF	0.389	0.574	1.270	2.237
		ON	0.393	0.499	0.636	0.523
	Rep.	OFF	0.389	0.526	1.691	2.450
		ON	0.393	0.424	0.540	0.454
	Iso.	OFF	0.389	0.505	1.509	3.553
		ON	0.393	0.417	0.511	0.442
DMF	Dis.	OFF	0.924	1.684	3.218	4.012
		ON	0.858	0.938	1.344	1.613
	Rep.	OFF	0.924	11.031	18.116	22.660
		ON	0.858	1.990	0.798	0.899
	Iso.	OFF	0.924	11.471	20.191	25.920
		ON	0.858	1.643	0.855	0.984

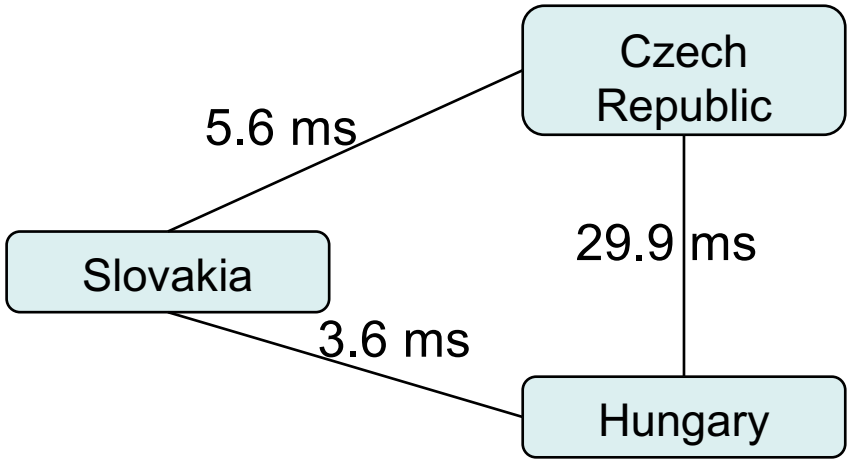
BAK: ENC Systems, TIV

- Euclidean-based NC systems (ENC systems)
  - Each node has a d-dimensional coordinate
  - Estimated distance: Euclidean distance calculation
  - Triangle inequality violations (TIVs) widely exist in Internet!



Triangle Inequality should hold!

29.9 > 5.6+3.6

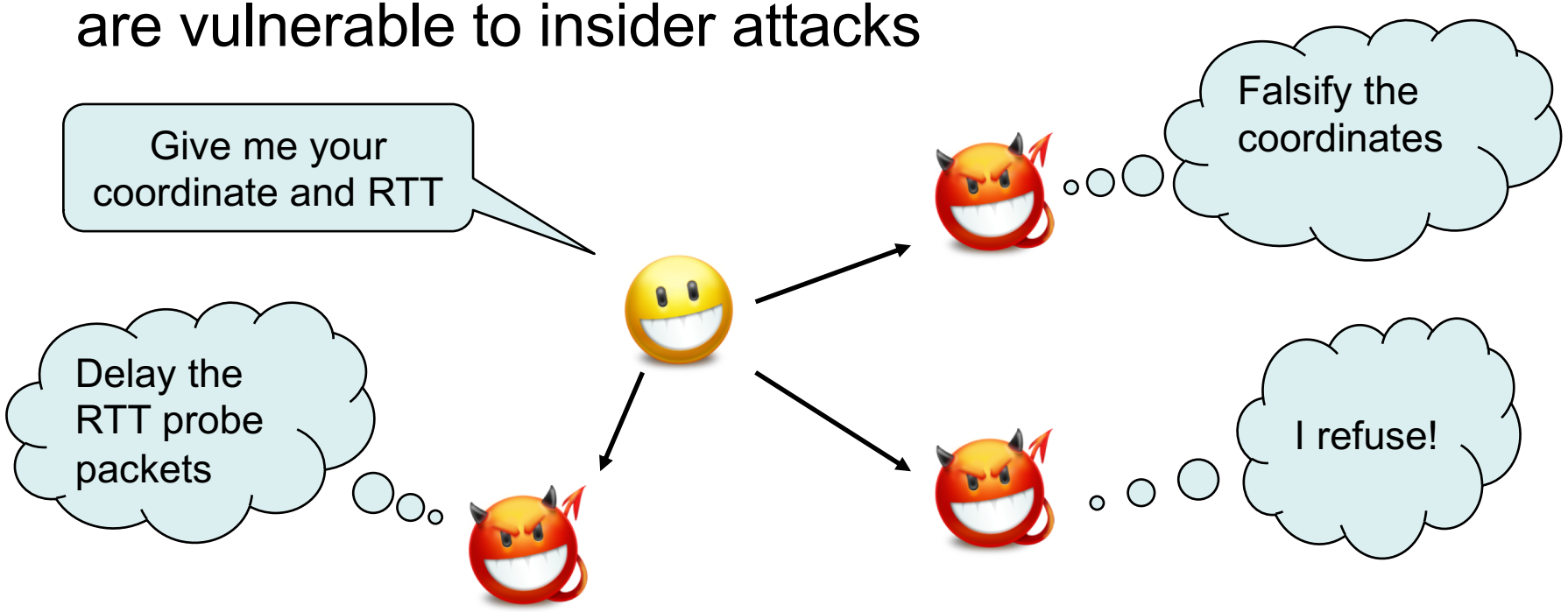


A TIV example in GEANT network[1]

[1]:[H Zheng et al. PAM'05]

BAK: Attacks on Decentralized ENC systems

- Early research[1] showed that decentralized ENC systems are vulnerable to insider attacks



[1]:[M. Kaafar et al. SIGCOMM Workshop on Large-Scale Attack Defense, 2006.].

BAK: Defense Approaches for ENC Systems

- Common idea: using extra information to determine whether a neighbor is trustworthy or not.
- Existing approaches for securing decentralized ENC systems:

Approach	Extra Info	Infrastructure	Drawback
Kalman Filter	Surveyors observation	Centralized	**Scalability**
Outlier Detection	History analysis	Decentralized	**Node churns**
RVivaldi	Trust and reputation sys.	Centralized	**Scalability**
Veracity	Information for vote	Decentralized	**Overhead**

Karman Filter: [M. A. Kaafar et al. SIGCOMM'07]. Outlier Detection: [D. Zage et al. CCS'07].
RVivaldi: [D. Saucez et al. DANS'07]. Veracity: [M. Sherr et al. ATC'09].

BAK Overhead: DHT vs. Gossip

- Overhead analysis
  - Typical DHT in an overlay network has **$O(\log_2 N)$** route length.
  - N: # of total participants.
  - Veracity using DHT and NCShield using gossip-based algorithm
    - 1024 nodes, 32 neighbors and 7 VList members, a update round of all nodes, for verification.
    - For detail analysis, please refer to the paper.

Mechanism	Veracity using DHT	NCShield using Gossip
# of messages needed	2674688	997376

62.7% overhead saved!