16th International Conference on Network and Service Management 2010

Effective Acquaintance Management for Collaborative Intrusion Detection Networks

Carol Fung, Jie Zhang, and Raouf Boutaba

David R. Cheriton School of Computer Science,
University of Waterloo

Roadmap

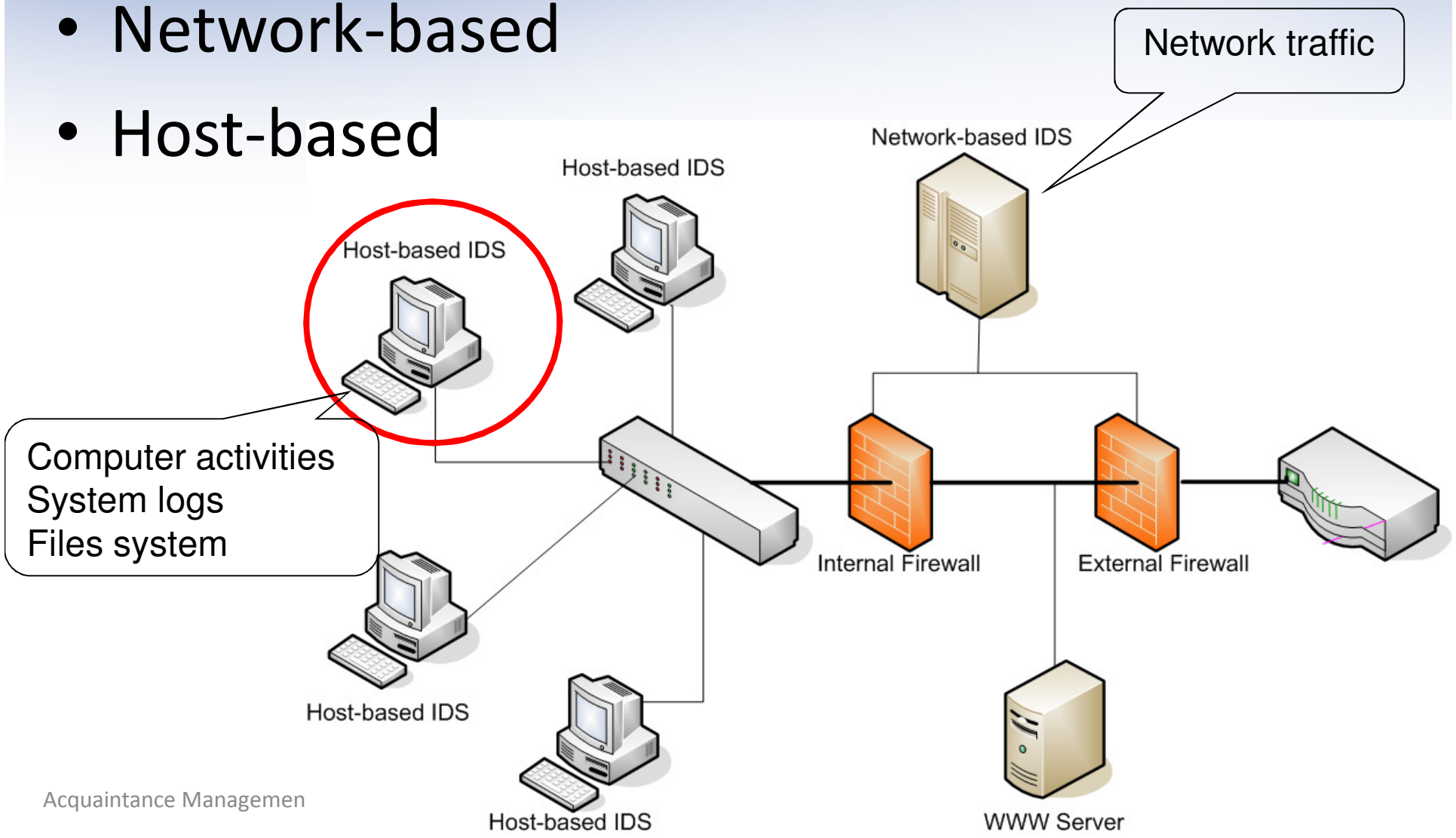
- Background
- Intrusion Detection and Collaboration
- Acquaintance Management
- Evaluation
- Conclusion

Network Intrusions

- Worms, Viruses, Malware
  - Storm worm (2007)
  - Conflicker (2008)
- Botnet
  - Zeus (2007-2010)
- Attack motivation
  - ID theft, Credit card , Privacy spying, Online account , Spamming, DoS, etc.

Intrusion Detection Systems

- Network-based
- Host-based

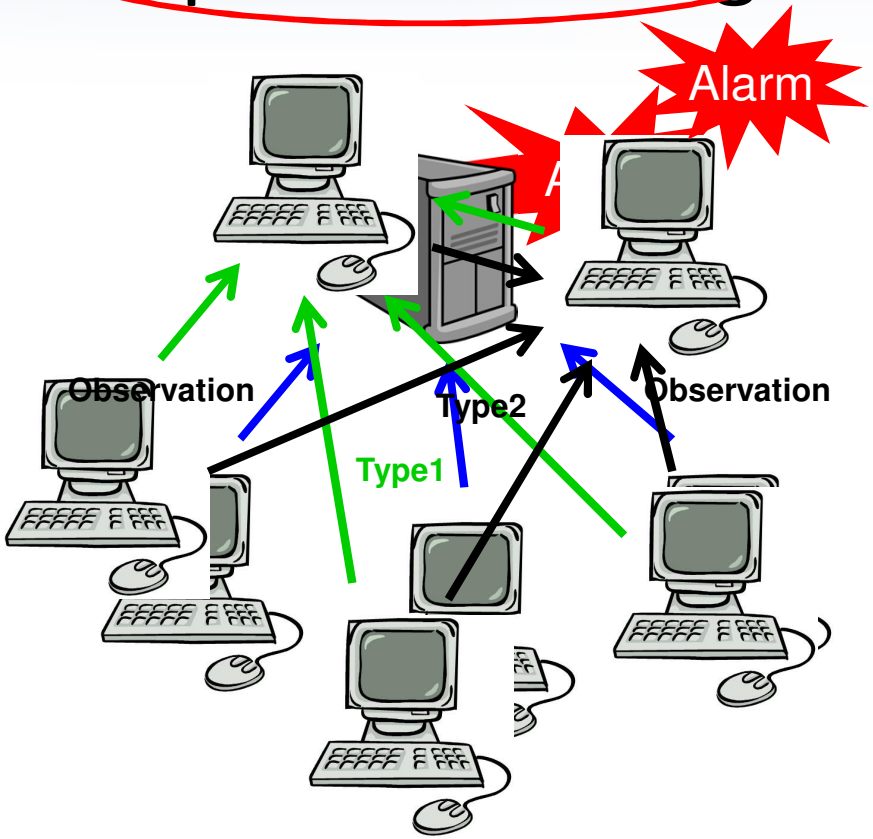


Host-based IDS (HIDS)

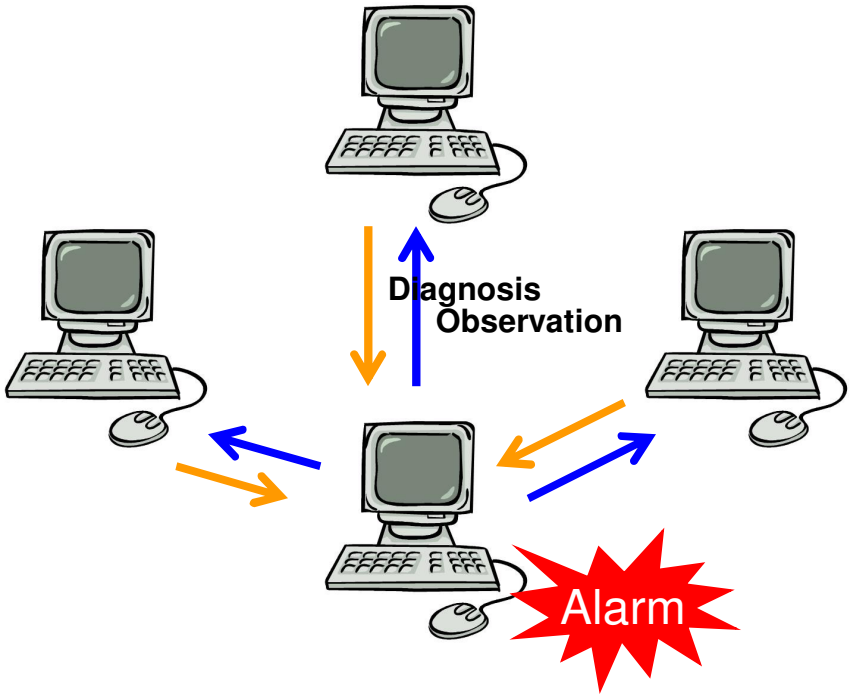
- Monitor computer activities, files, and compare against malicious patterns
  - Traditional HIDS such as OSSEC, Tripwire
  - Antivirus systems
- A single HIDS can be vulnerable to new attacks
  - Collaboration improves detection accuracy

Collaborative Intrusion Detection

- Information sharing (DShield, NetShield)
- Expertise sharing (Cloud-AV)



Information Sharing



Expertise Sharing

Who to collaborate with?

- Existing solutions
  - Fixed number
  - Fixed thresh-bar
- Our Contribution
  - An automatic acquaintance management
  - Cost efficient acquaintance selection

Our Approach

Step 1: Know your candidates

Step 2: Cost function modeling

Step 3: Consensus reaching

Know the Candidates

- Learn the quality of a candidate
  - False positive rate and True positive rate
  - Using test messages to gain experience
  - Bayesian learning

Cumulative evidences on false diagnosis

Cumulative evidences on true diagnosis

$$F \sim \frac{1}{B(\alpha,\beta)} x^{\alpha-1}(1-x)^{\beta-1}$$

Distribution of False Positive rate

Beta function

Cost Function Selection

- Cost on maintenance of collaborators
  - Increases with the number of collaborators
- Cost on false decisions
  - Cost of false positive and false negative decisions

$$C_{total} = M(\mathrm{A}) + R(\mathrm{A})$$

$$= C_m \mid \mathrm{A} \mid + \sum_{y \in \{0,1\}^{|\mathrm{A}|}} \min\{C_{fn}\pi_1 \prod_i T_i^{y_i}(1-T_i)^{1-y_i}, C_{fp}\pi_0 \prod_i F_i^{y_i}(1-F_i)^{1-y_i}\}$$

Maintenance cost

Cost on no alarm

Cost on raising alarm

Acquaintance Selection Algorithm

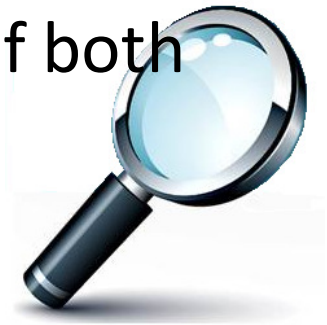
Algorithm1: Select the optimal acquaintance list with minimal cost

- Brute Force for a short candidate list and greedy for a long candidate list

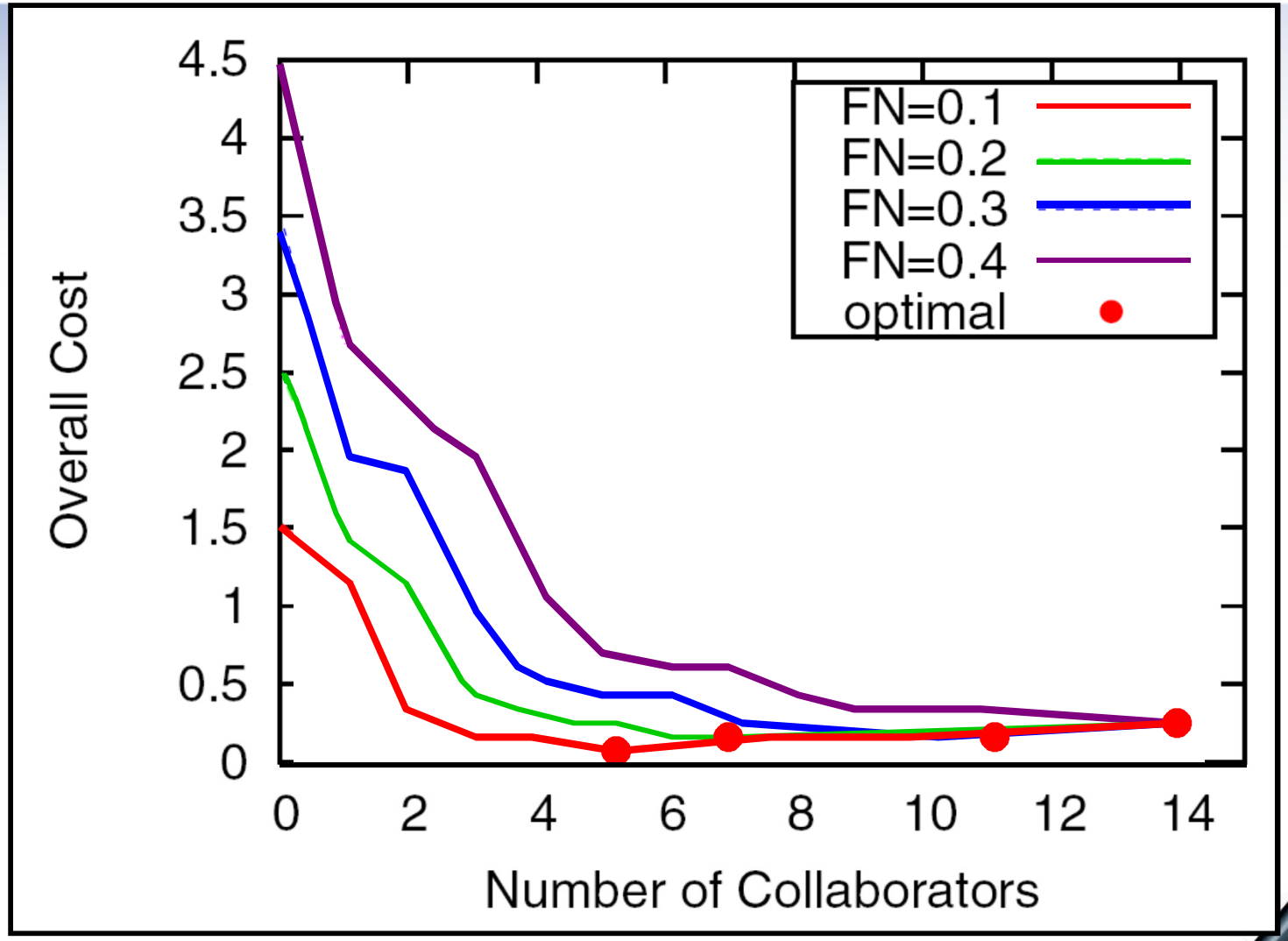
Algorithm2: Acquaintance management to find mutual agreement among nodes

- Probation period

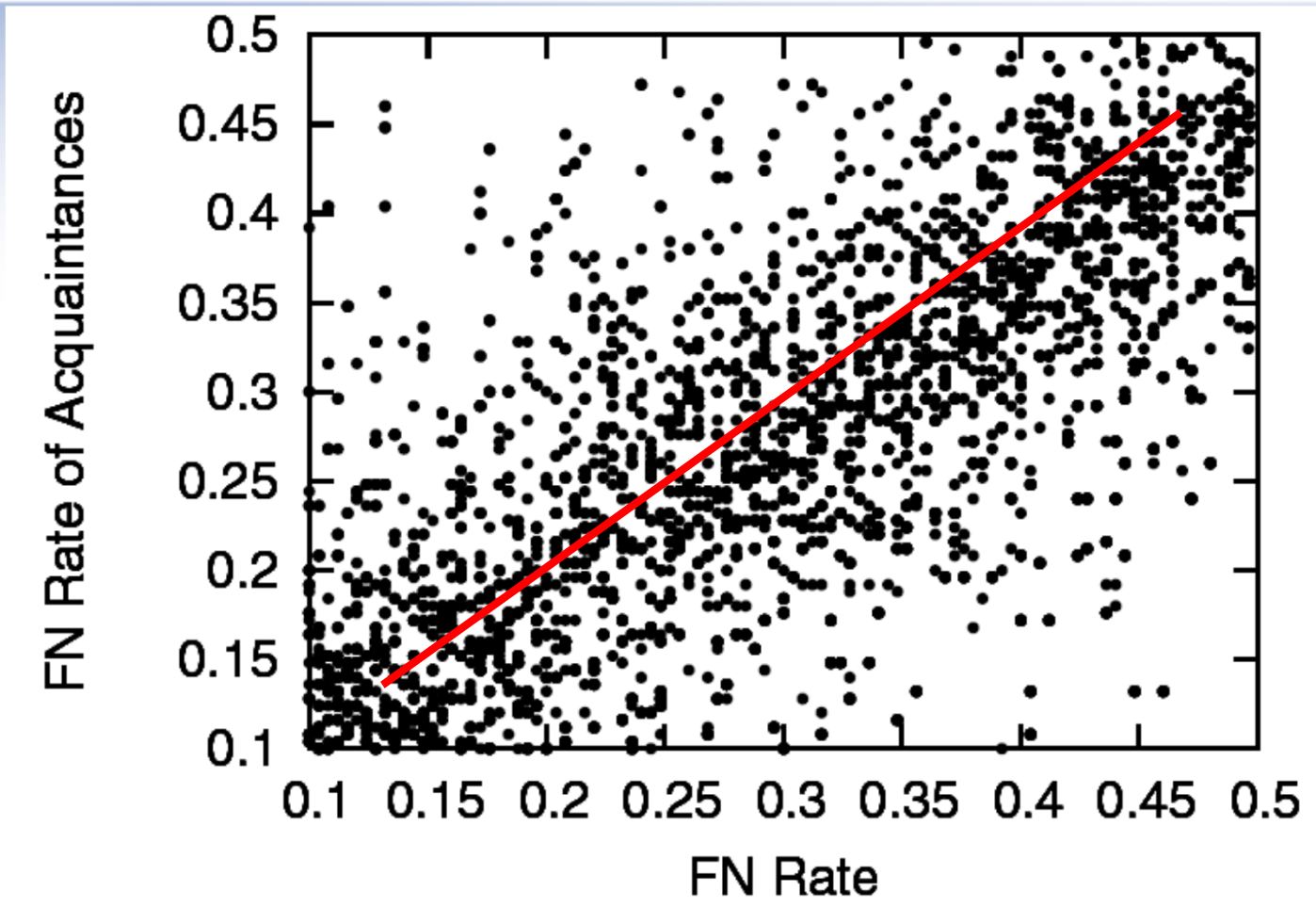
- Collaboration connection is established only if both peers select each other



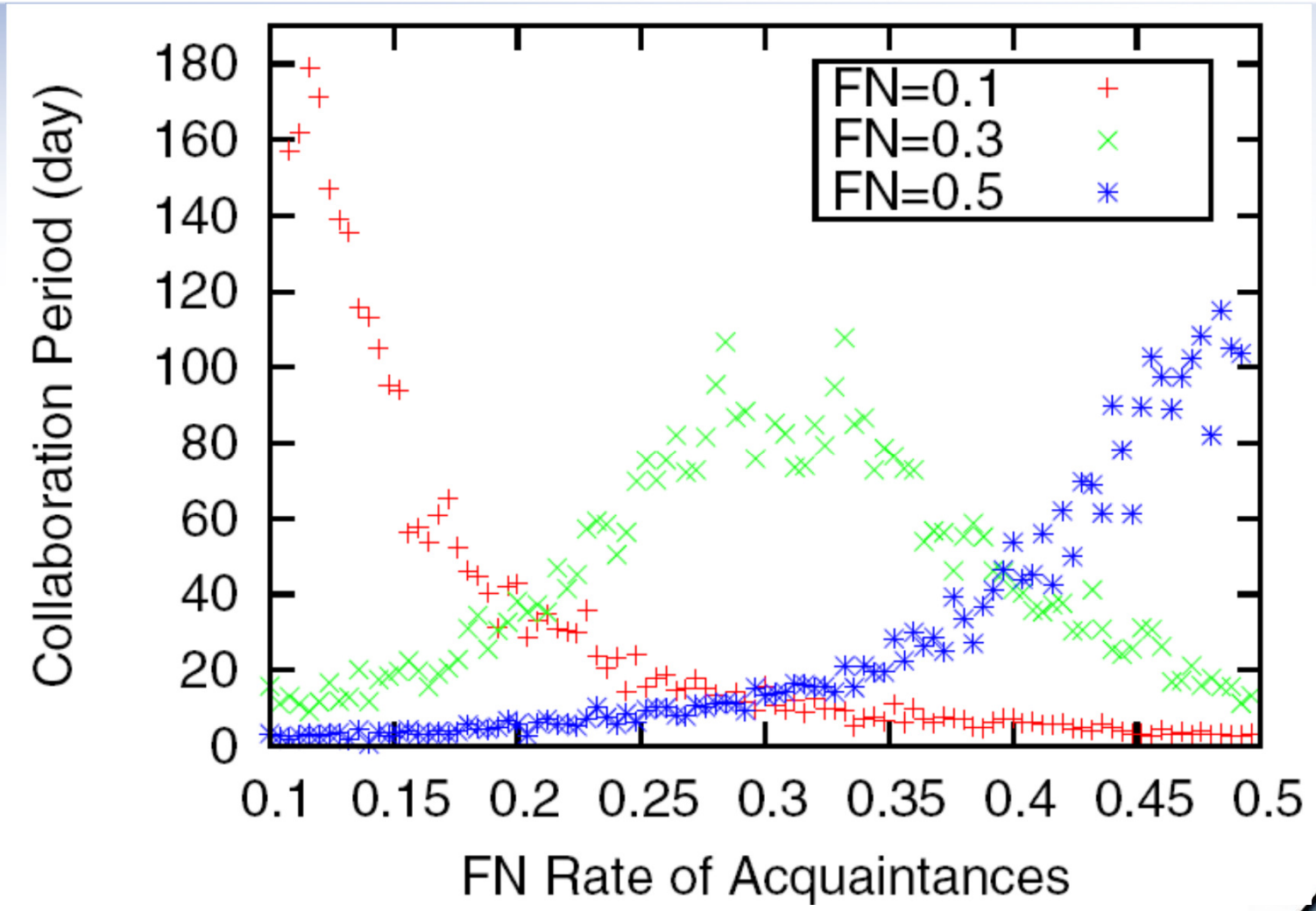
Evaluation - Cost Efficiency



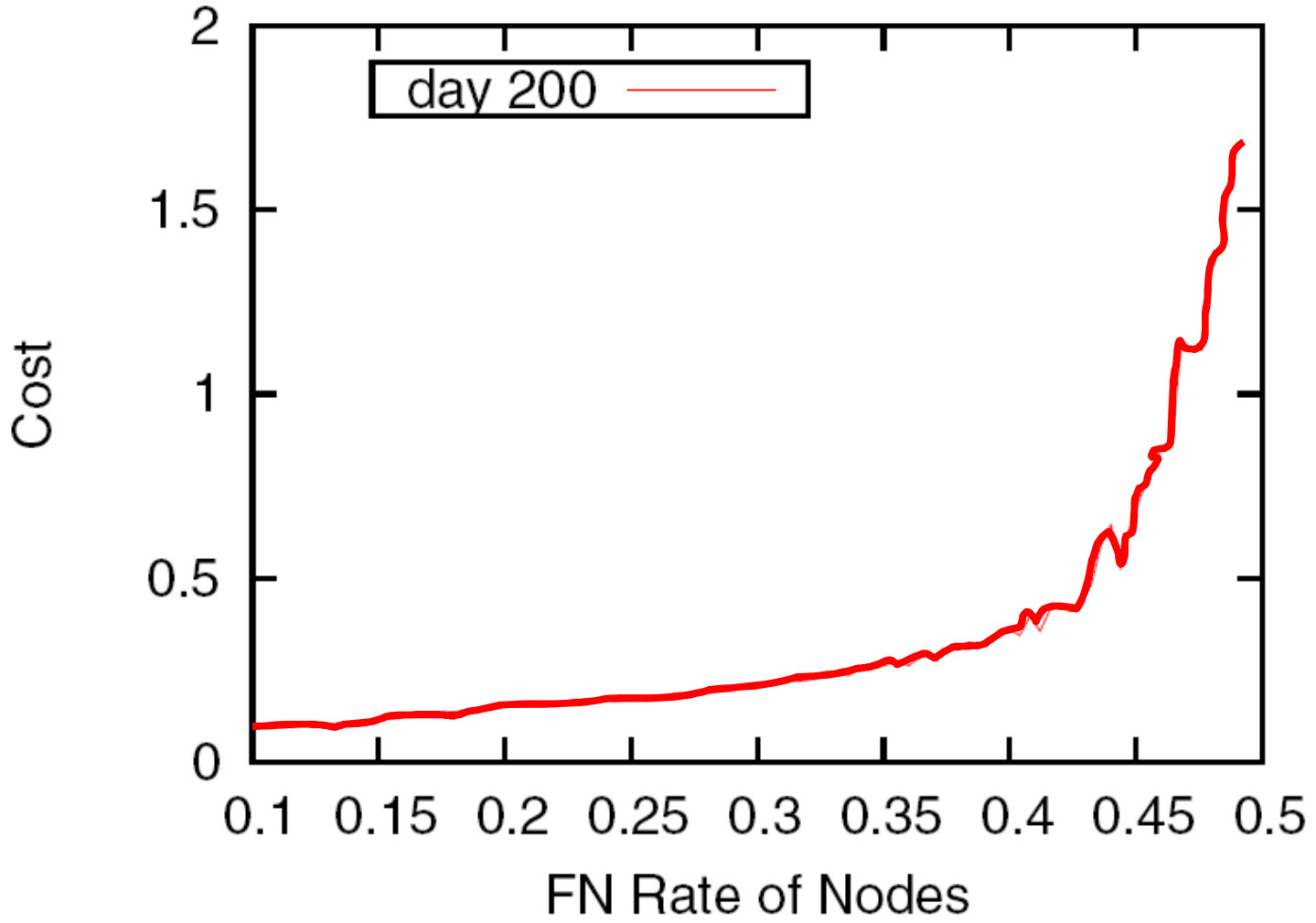
Evaluation - Convergence



Evaluation - Stability



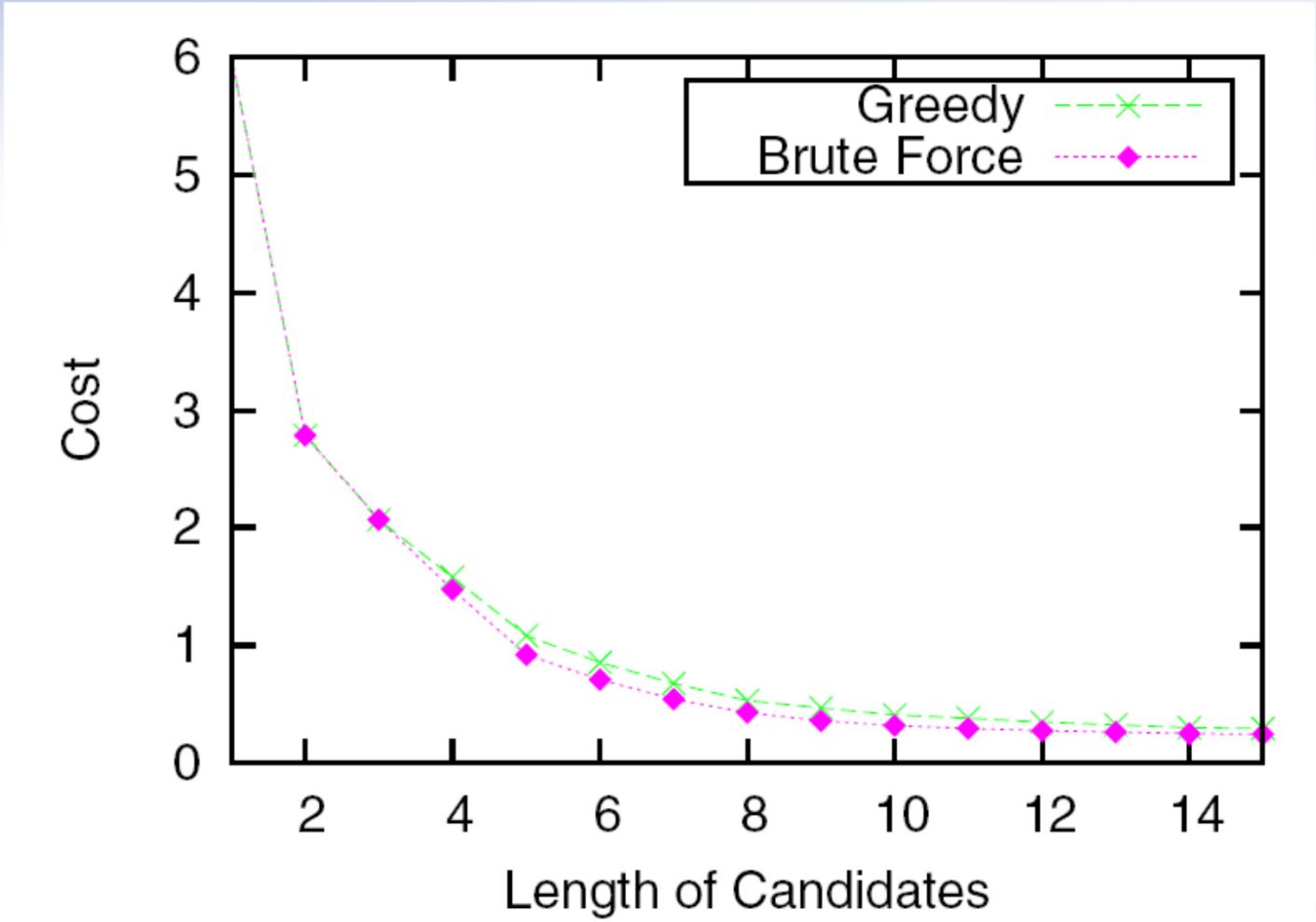
Evaluation – Incentive Compatibility

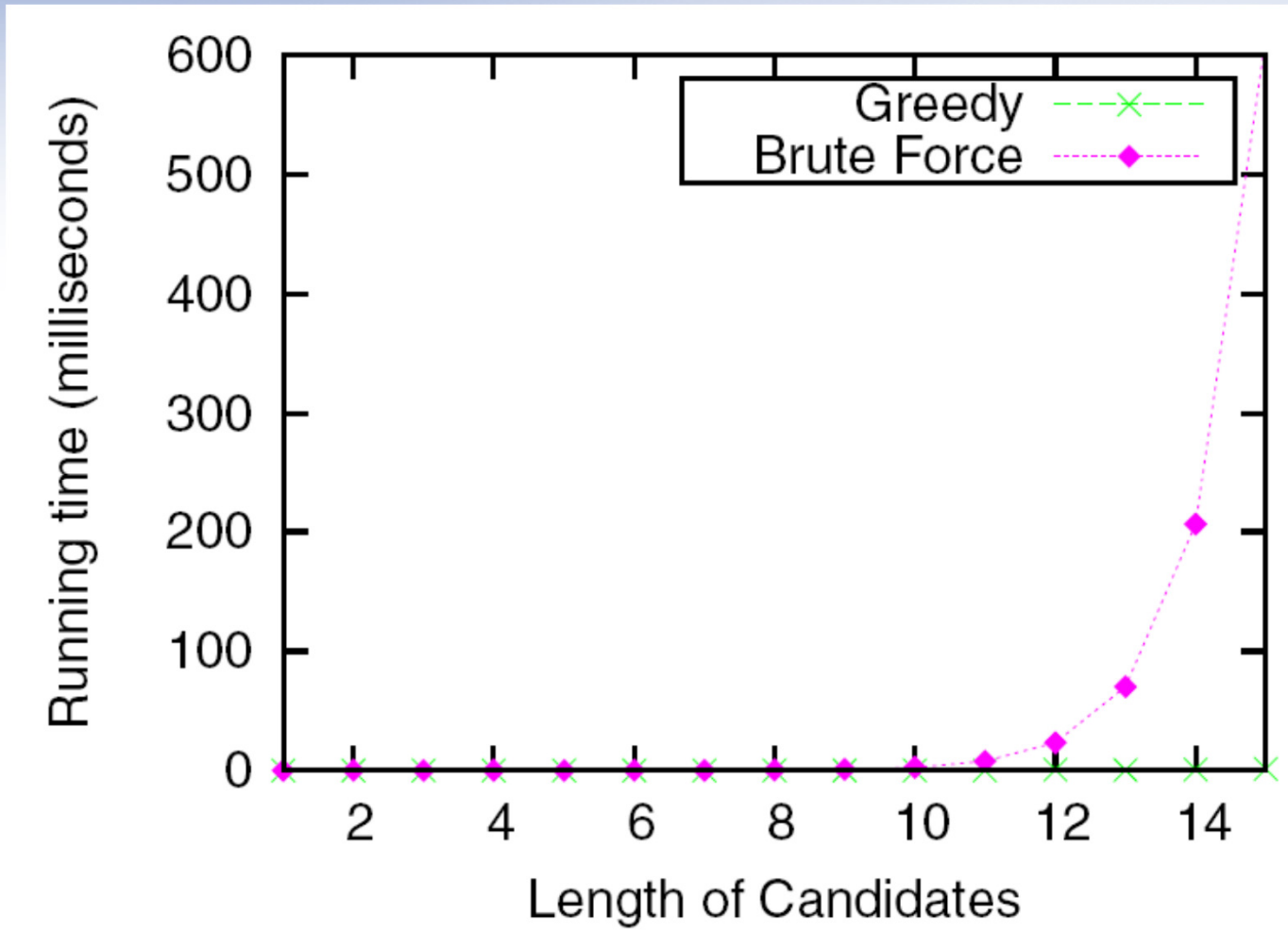


Conclusion

- Proposed an automatic acquaintance selection algorithm for collaborative intrusion detection networks
- Find optimal acquaintance list which leads to the minimum cost
- The acquaintance management algorithm holds the properties of efficiency, stability, and incentive-compatibility

Thank You


Greedy
Brute Force
Cost
Length of Candidates
0
1
2
3
4
5
6
2
4
6
8
10
12
14


Running time (milliseconds)
600
500
400
300
200
100
0
2
4
6
8
10
12
14
Length of Candidates
Greedy
Brute Force

Bayesian Learning

α: Cumulative evidences on false diagnosis
β: Cumulative evidences on true diagnosis