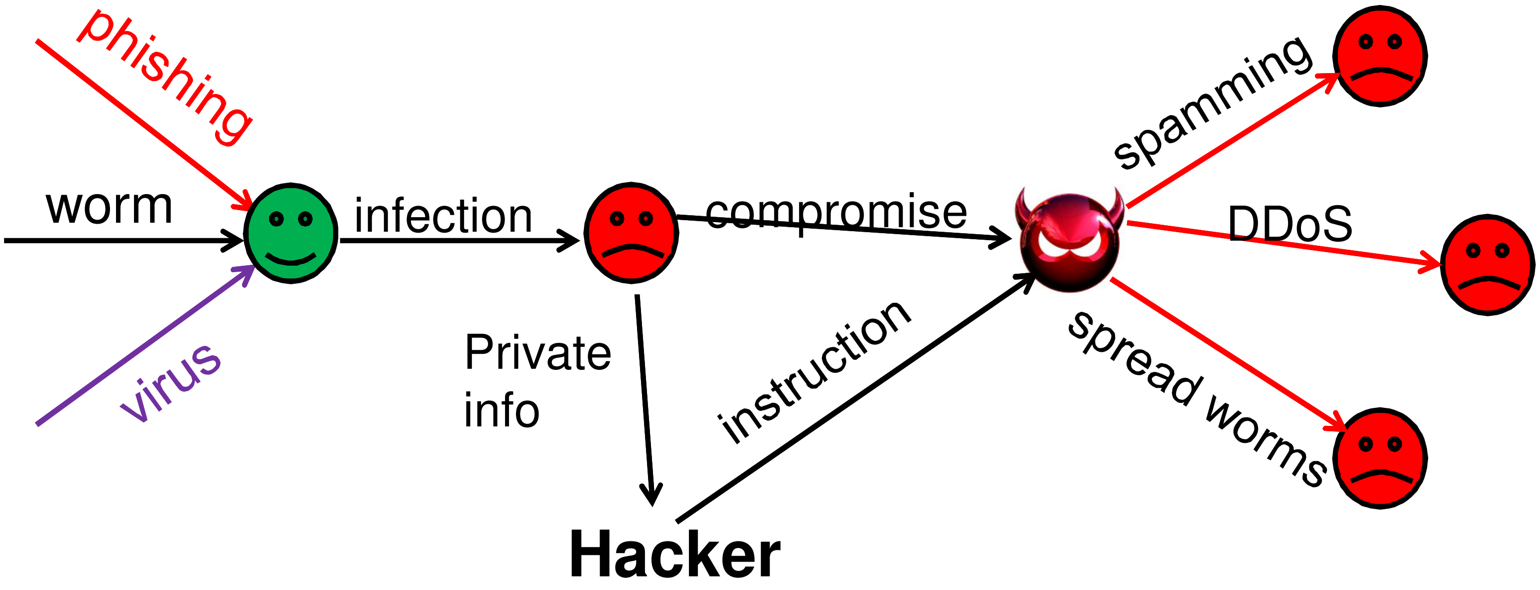
SMURFEN: A System Framework for Rule Sharing Collaborative Intrusion Detection

Carol Fung, Quanyan Zhu,
Raouf Boutaba, and Tamer Başar
David Cheriton School of Computer Science,
University of Waterloo
Department of Electrical and Computer Engineering
University of Illinois at Urbana Champaign

Motivation

- **Cyber intrusions are more sophisticated and harder to detect**
  - **Phishing, Malware, Botnet, Spam, DDoS**
  - **2 M new malware per month (McCafe)**



Intrusion Detection

- Intrusion Detection System (IDS)
  - Host-based and Network-based
  - Signature-based and Anomaly-based

- Collaborative Intrusion Detection
  - Share alerts (Indra)
  - Share data, logs (DShiled)
  - Share knowledge (blacklists, signatures and detection rules)

Why Share Detection Knowledge?

- Data Sharing
  - Information breaching
  - Privacy concern
- Knowledge Sharing
  - No security vendor has full knowledge
  - Exchange knowledge to increase detection rate
  - less privacy concern

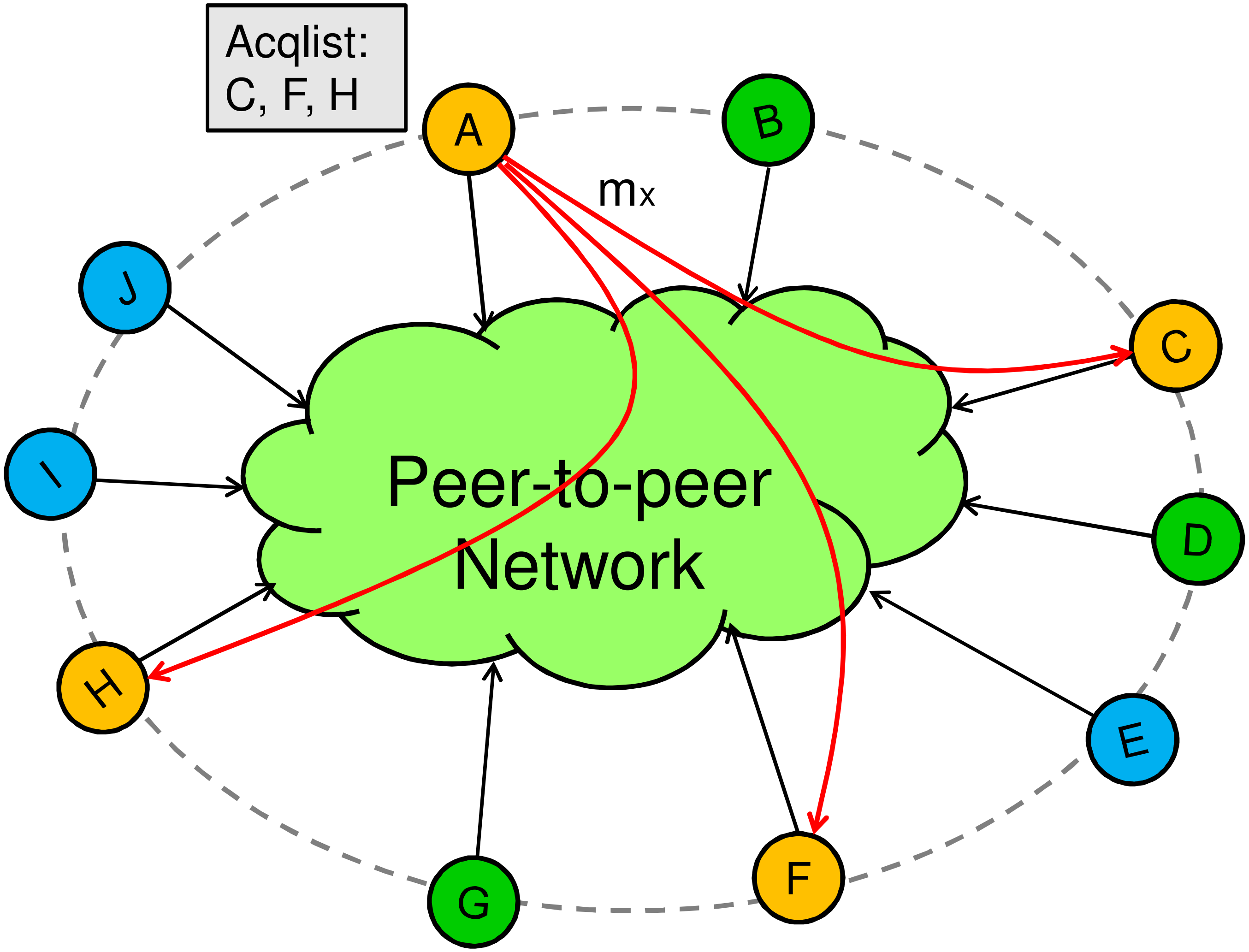
Challenges

- Propagation efficiency
  - Knowledge sent to nodes with similar interests?
- Scalability
  - Work well for large network size?
- Robustness
  - Resist to common insider attacks?
- Fairness and incentive
  - Similar credits, similar benefit
  - More contribution, more benefit

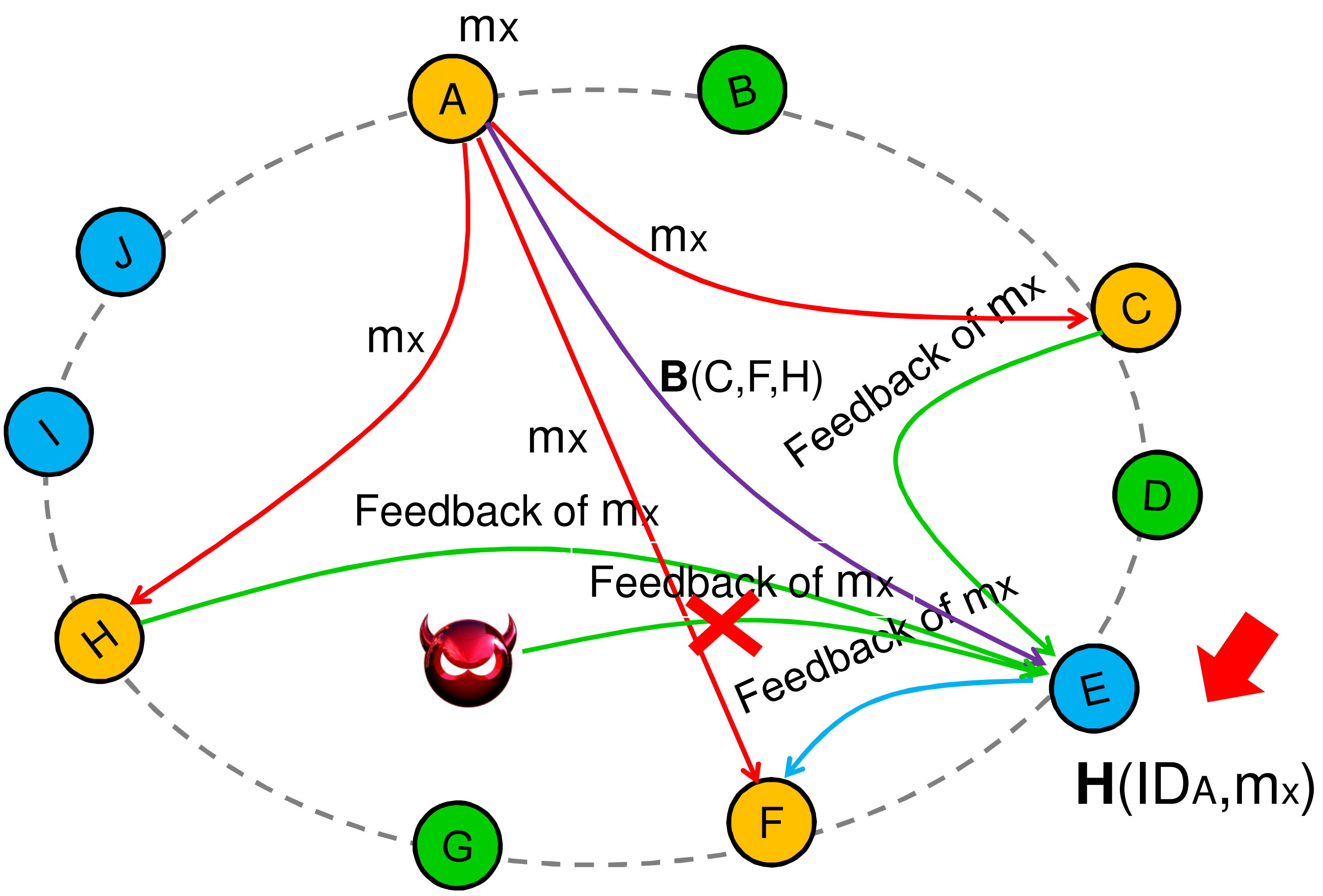
SMURFEN

- A knowledge sharing system for intrusion detection networks
  - Peer-to-peer topology
  - Knowledge sharing
  - Feedback collecting
  - Mutual consensus convergence

Architecture



Feedback Collection



Propagation Design

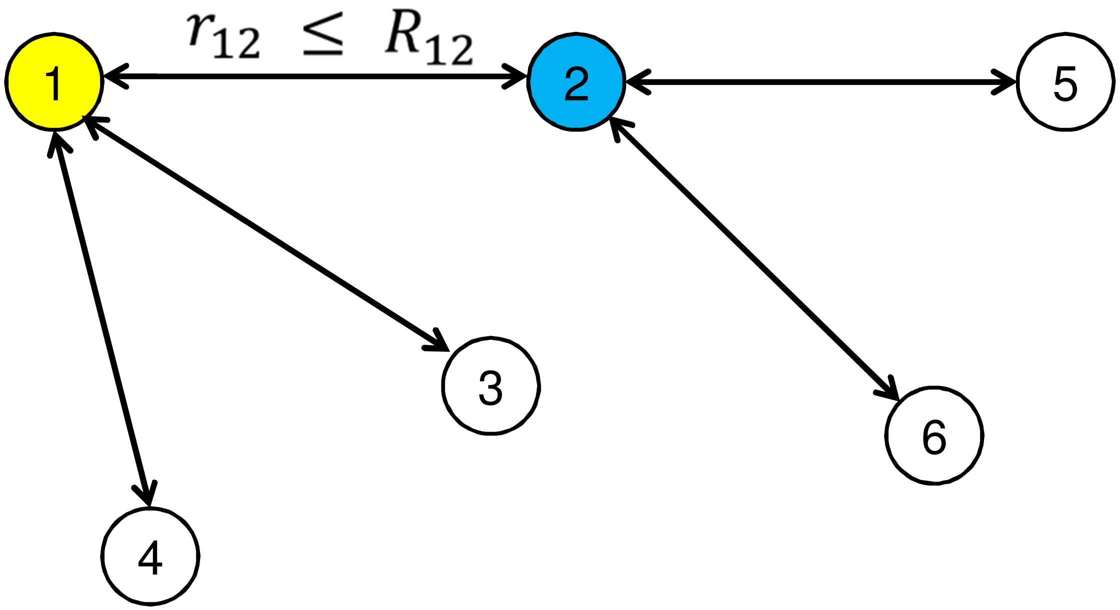
- A Two level game design
  - Low level - a public wareface
  - High level - a private wareface
  - Control variables are sending rate and requesting rate
  - Connection between public and private wareface

An Example

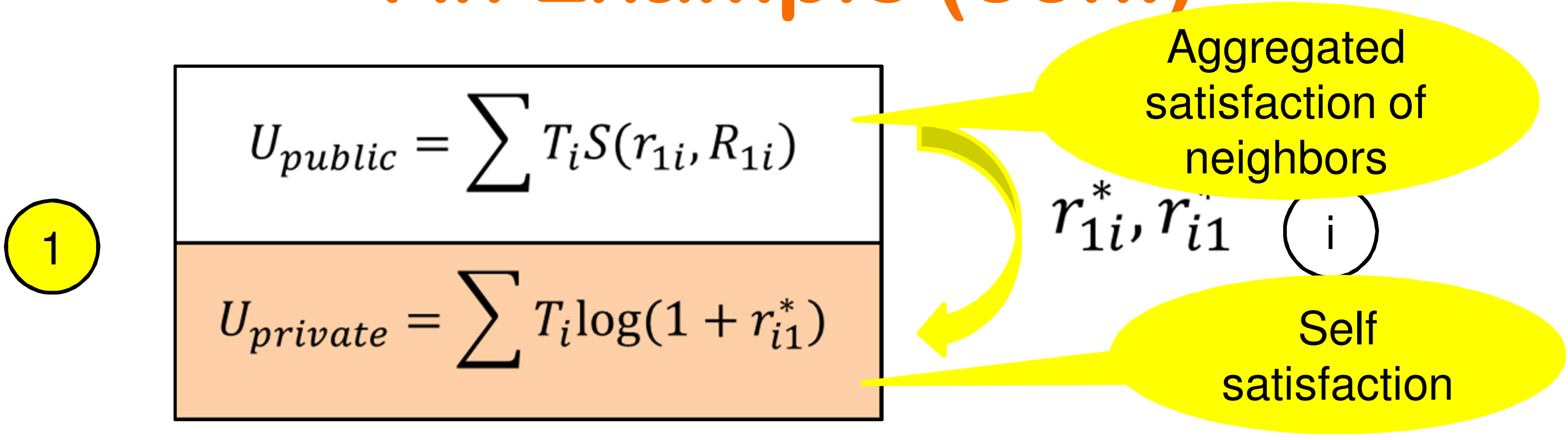
1

Propagation rate $\overrightarrow{r_1} = \{r_{12,} r_{13,} r_{14}\}$

Requesting rate $\overrightarrow{R_1} = \{R_{21,} R_{31,} R_{41}\}$



An Example (con.)



$$U_{public} = \sum T_i S(r_{1i}, R_{1i})$$

$$U_{private} = \sum T_i \log(1 + r_{i1}^*)$$

r_{1i}^*, r_{i1}^*

The two level game posses a Nash Equilibrium

Evaluation – Efficiency

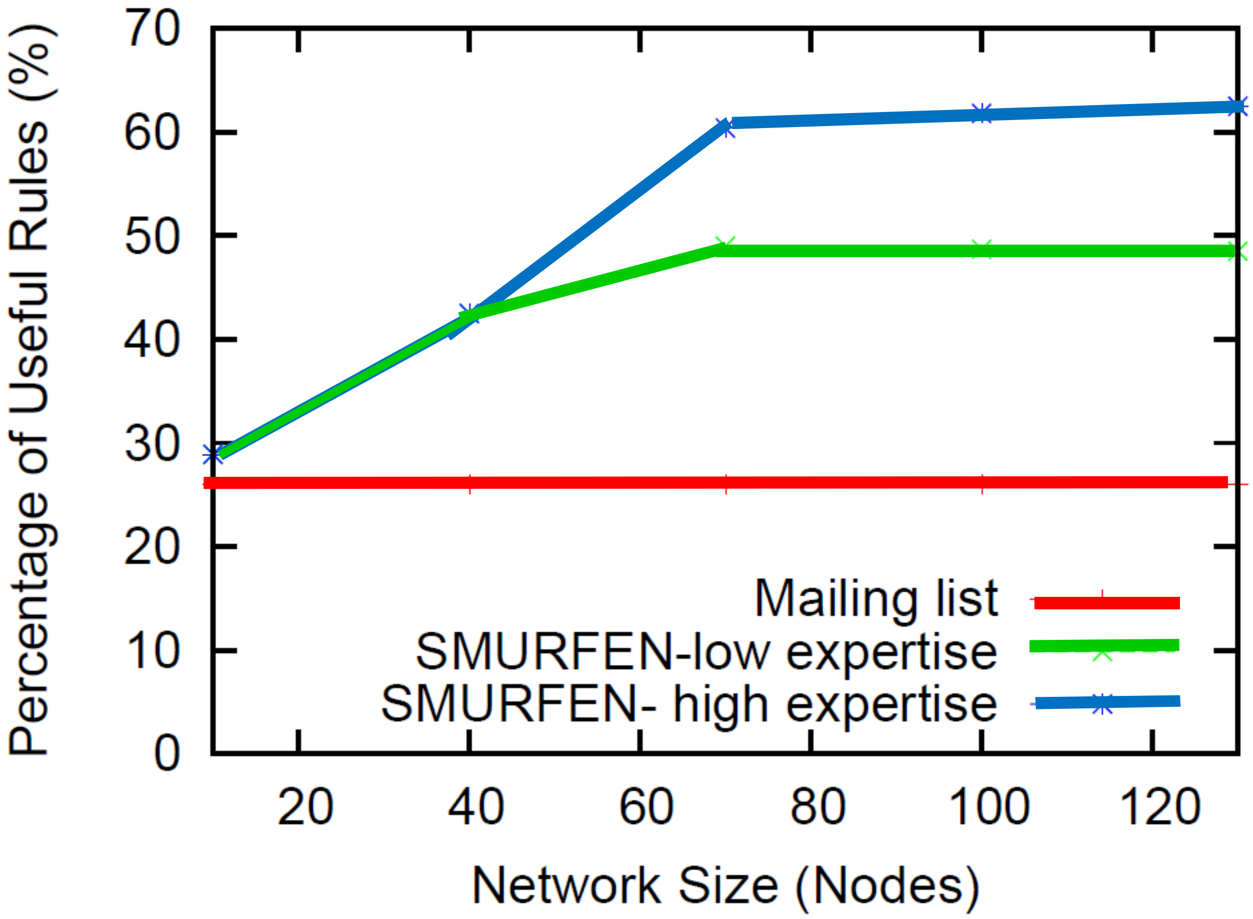


Figure 1. Efficiency of Rule Propagation

Evaluation – Fairness

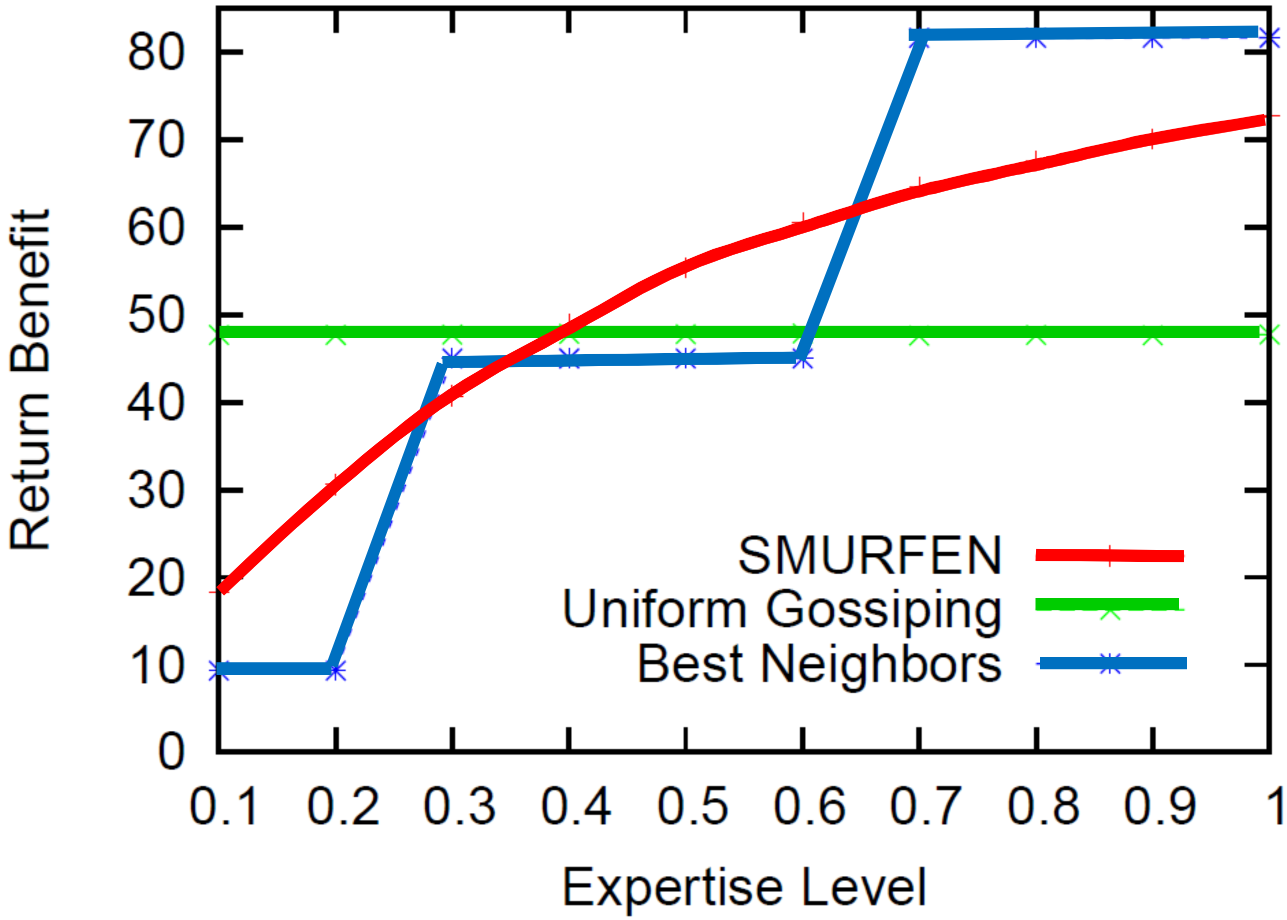


Figure 2. Fairness of Rule Propagation

Evaluation – Robustness

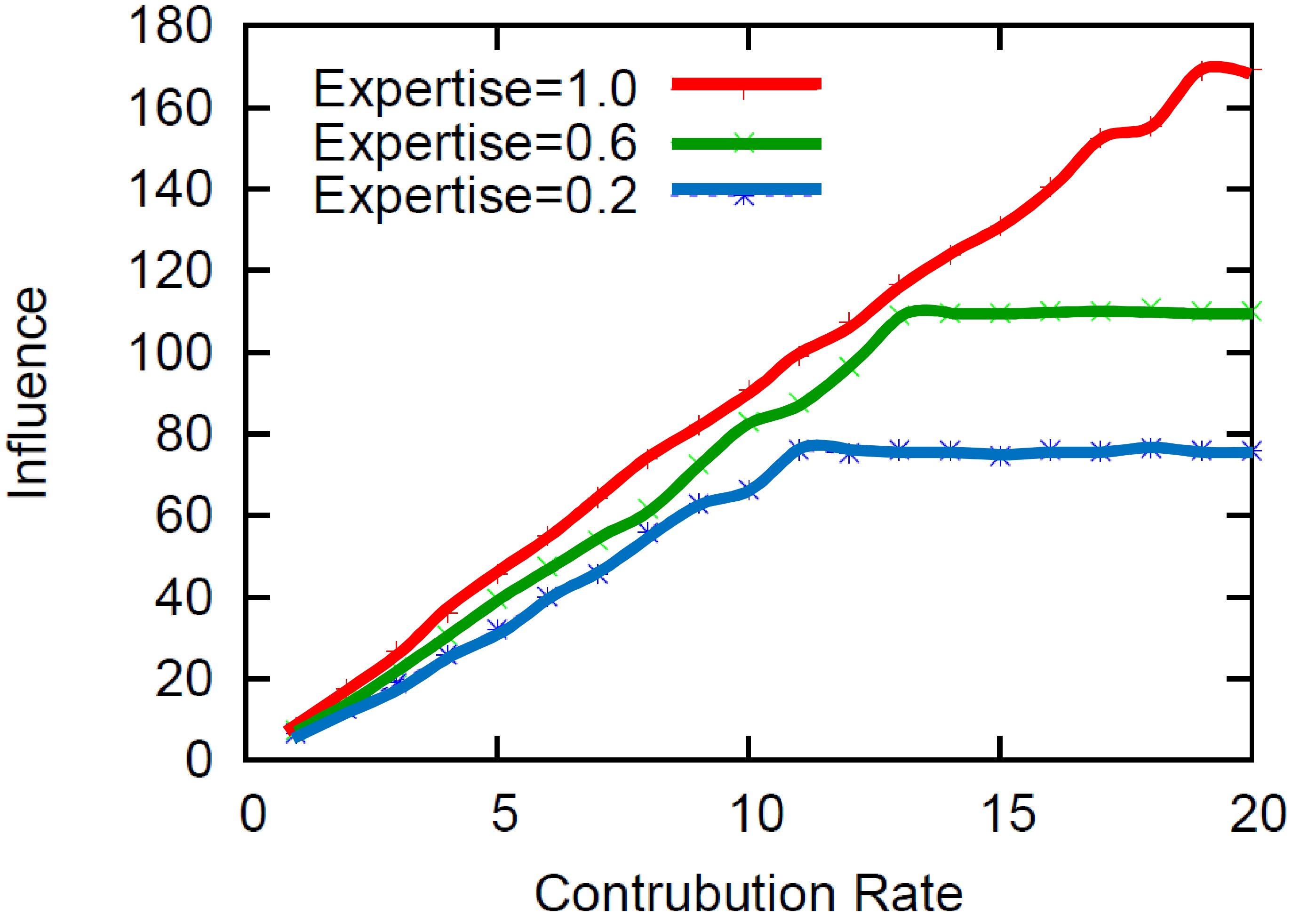


Figure 3. Robustness of Rule Propagation

Conclusion and Future Work

- Propose a framework for knowledge sharing collaborative intrusion detection
- A rule propagation model based on a multiplayer game
  - Achieve the properties of efficiency, scalability, fairness, and robustness
- As future work, we intend to show more insider attacks and defenses

Thank You!