IFIP Network and Service Security Conference 2009

A simulation framework for Trust Model Evaluation in Intrusion Detection Networks

Carol Fung, Jie Zhang, Issam Aib, Raouf Boutaba, and Robin Cohen

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

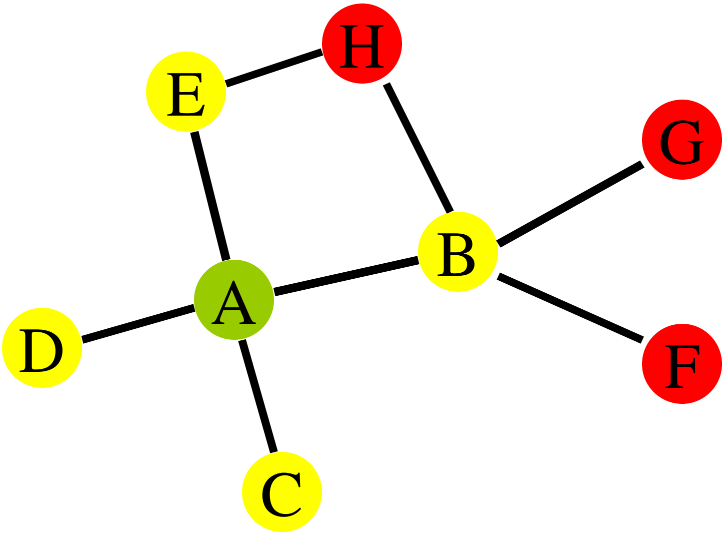
Outline

- Introduction
- Framework Design
- Demonstration Results
- Conclusion and Future Work

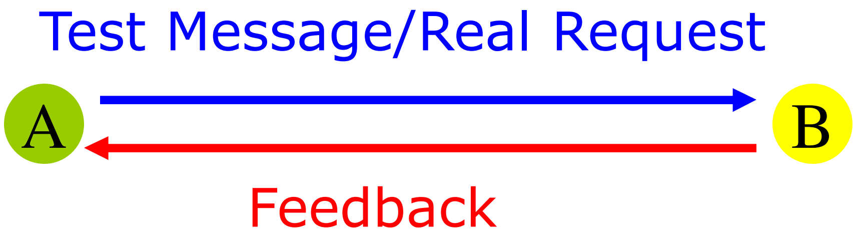
Cyber Threats and Intrusion Detection Systems (IDS)

- Cyber Threats
  - Viruses, Worms, Malware, and Denial of Service attacks
- Intrusion Detection Systems
  - Firewalls, Antivirus Software, Signature-based Intrusion Detection Systems, and Anomaly-based Intrusion Detection Systems

Collaboration Network Architecture



- Acquaintance (List)
- Test Message
- Real Request
- Feedback



Intrusion Detection Networks

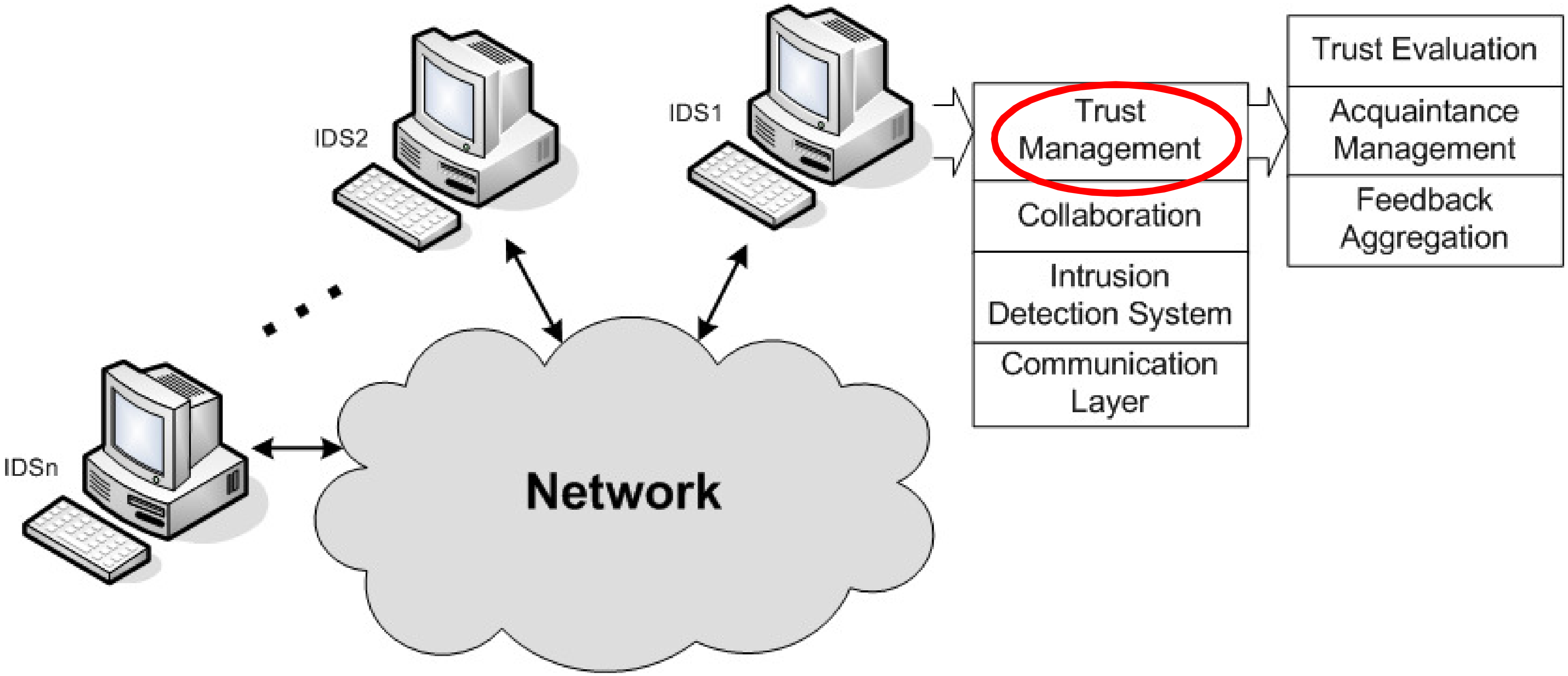


Figure1. Collaborative Intrusion Detection Networks

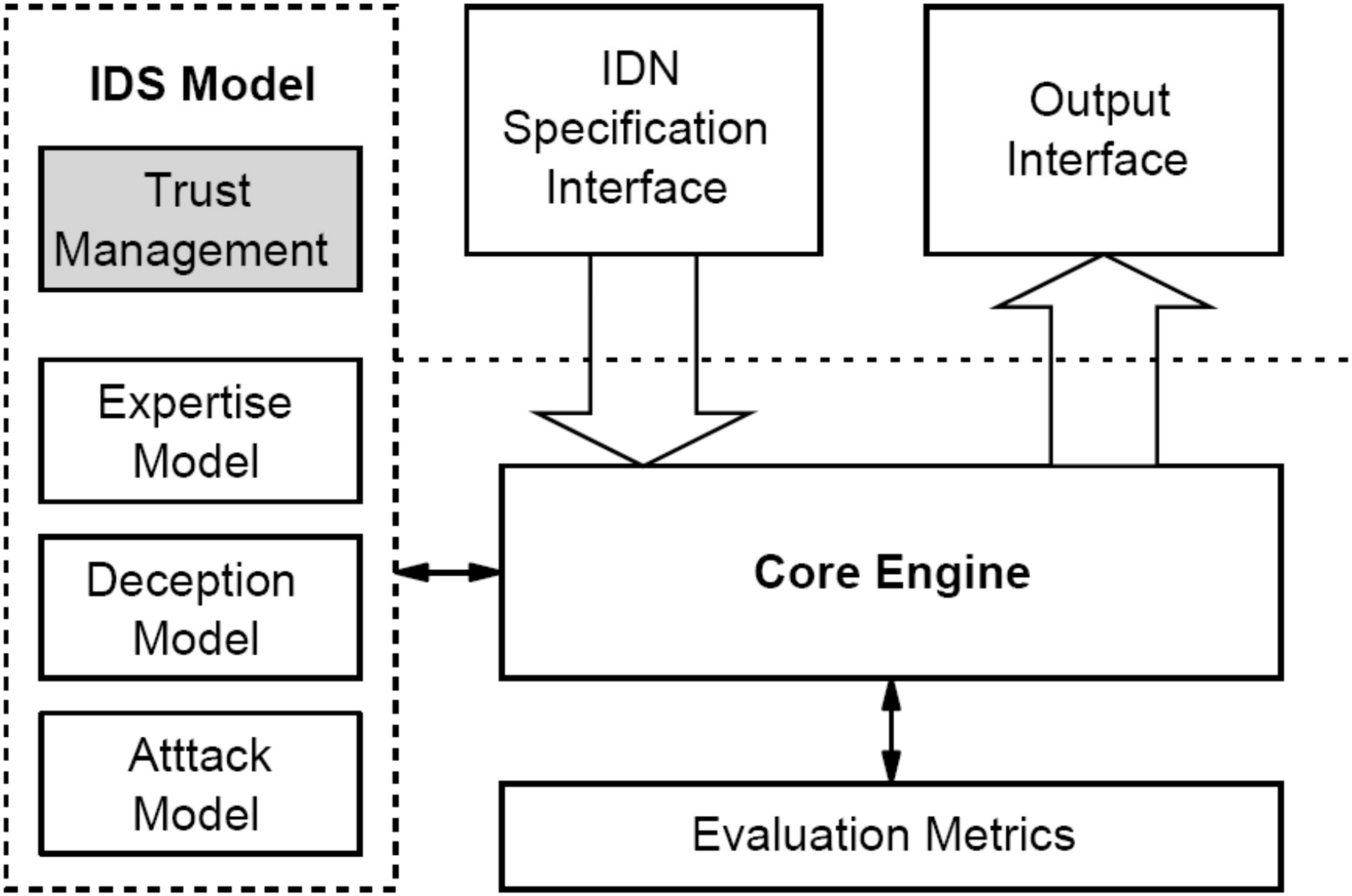
Existing Trust Models for IDN

- Duma et al. [DEXA 2006]
- Fung et al. [DSOM 2008]
- Dirichlet-based Model [IM 2009]

Motivation

- A testbed for researchers to compare their trust models against objective metrics
  - Provide conveniences for researchers
  - Create a neutral platform to compare models
- Repeatable experiments
- Can be a benchmark of IDN trust models evaluation

Architecture



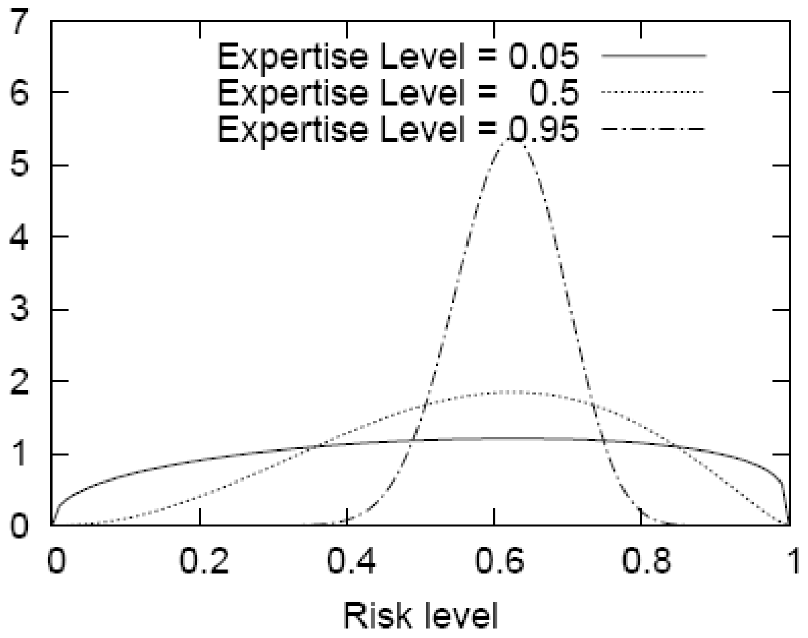
Components

- Modeling of single IDS (expertise model)
- Trust Model
- Acquaintance List Management Model
- Feedback Aggregation Model
- Deception Model
- Attack Model

Expertise Model

- Use a Beta density function to simulate the intrusion detection accuracy of a single IDS

- Use an expertise level parameter to control the detection accuracy



Deception Models

- Complement
- Exaggerate Positive
- Exaggerate Negative
- Maximal Harm

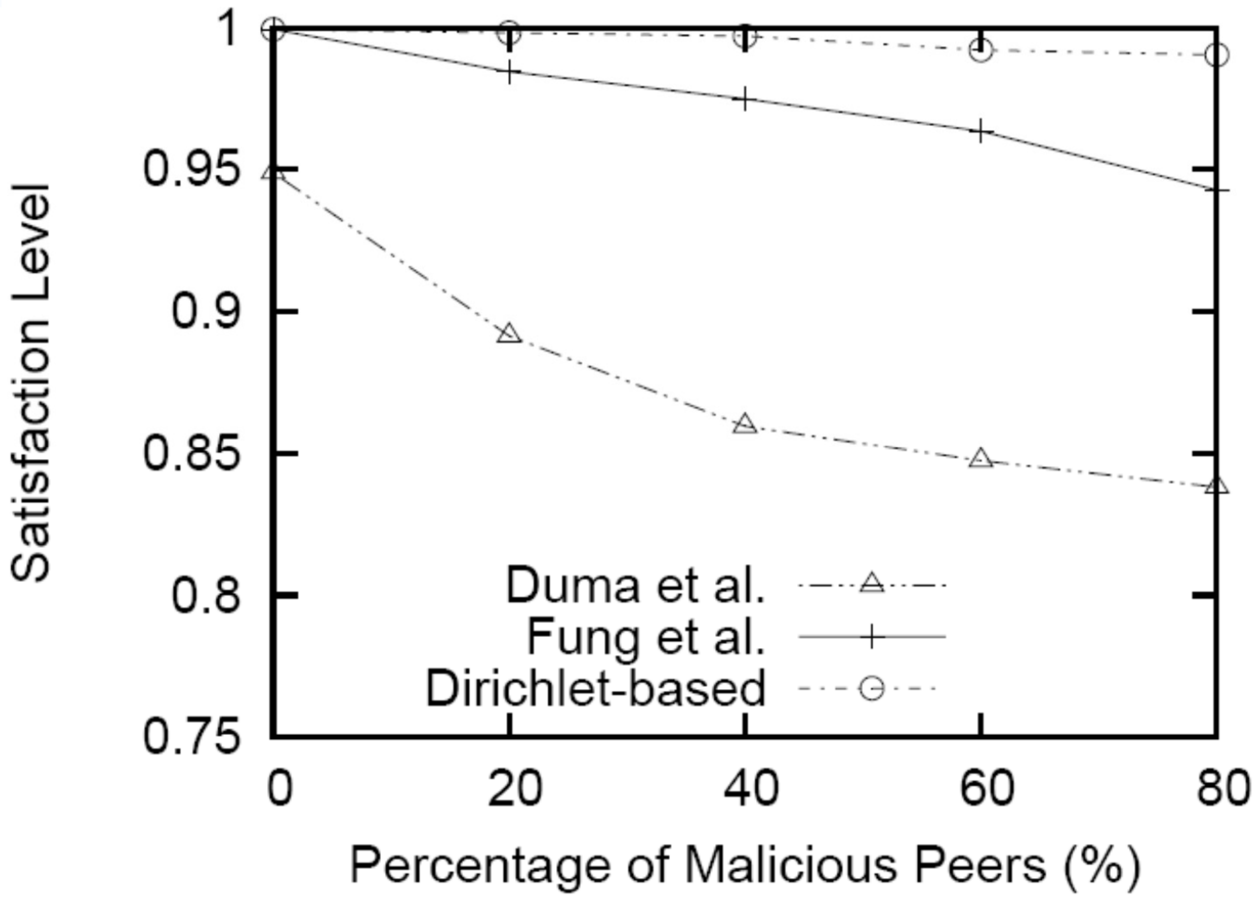
Attack Models

- Newcomer attack
- Betrayal attack
- Inconsistency attack
- Group attack

Metrics

- Intrusion Detection Accuracy
- Robustness against attacks
- Scalability

Demonstration (1)



Dirichlet-based

Fung et al.

Duma et al.

Fig 2. Results of Detection Accuracy

Demonstration (2)

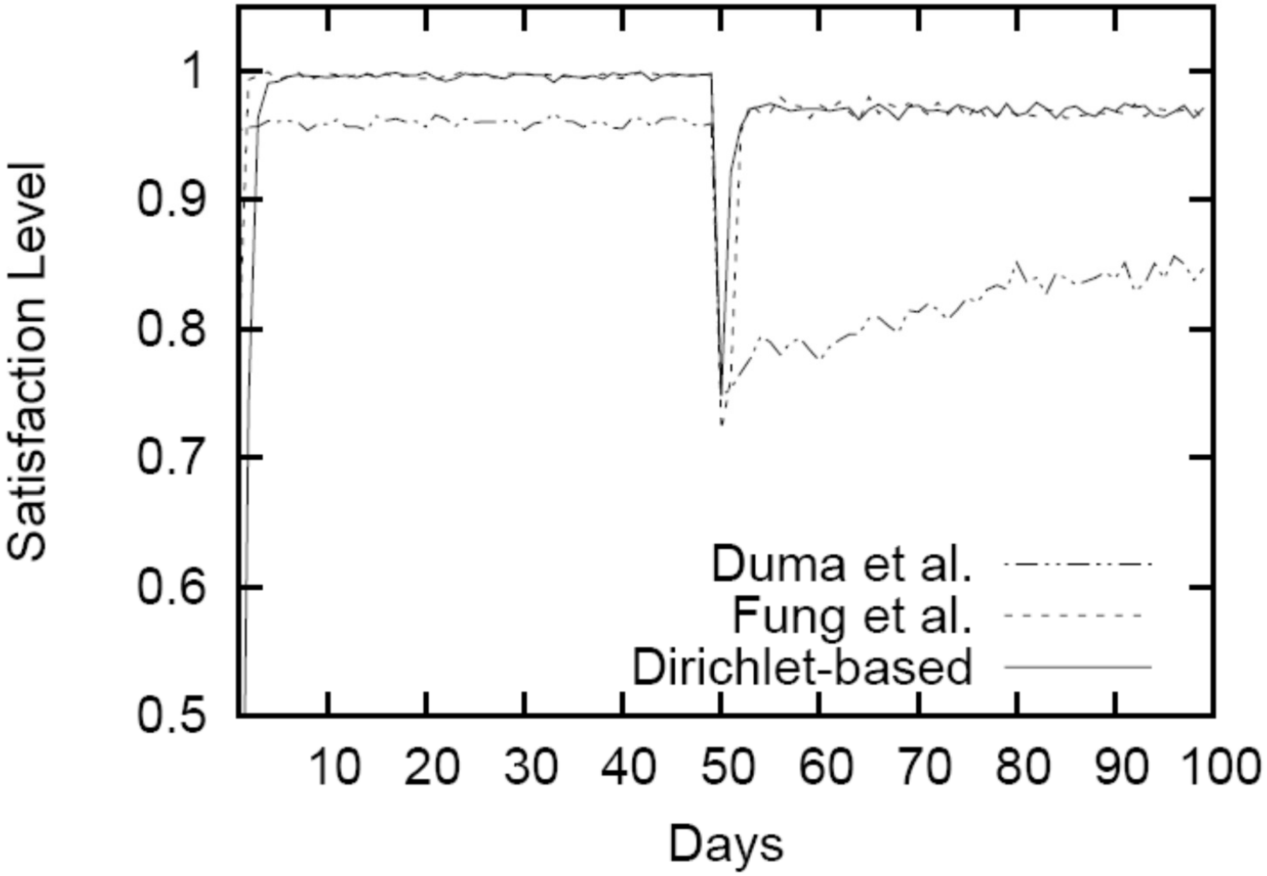


Fig 3. Robustness of Trust Models

Demonstration (3)

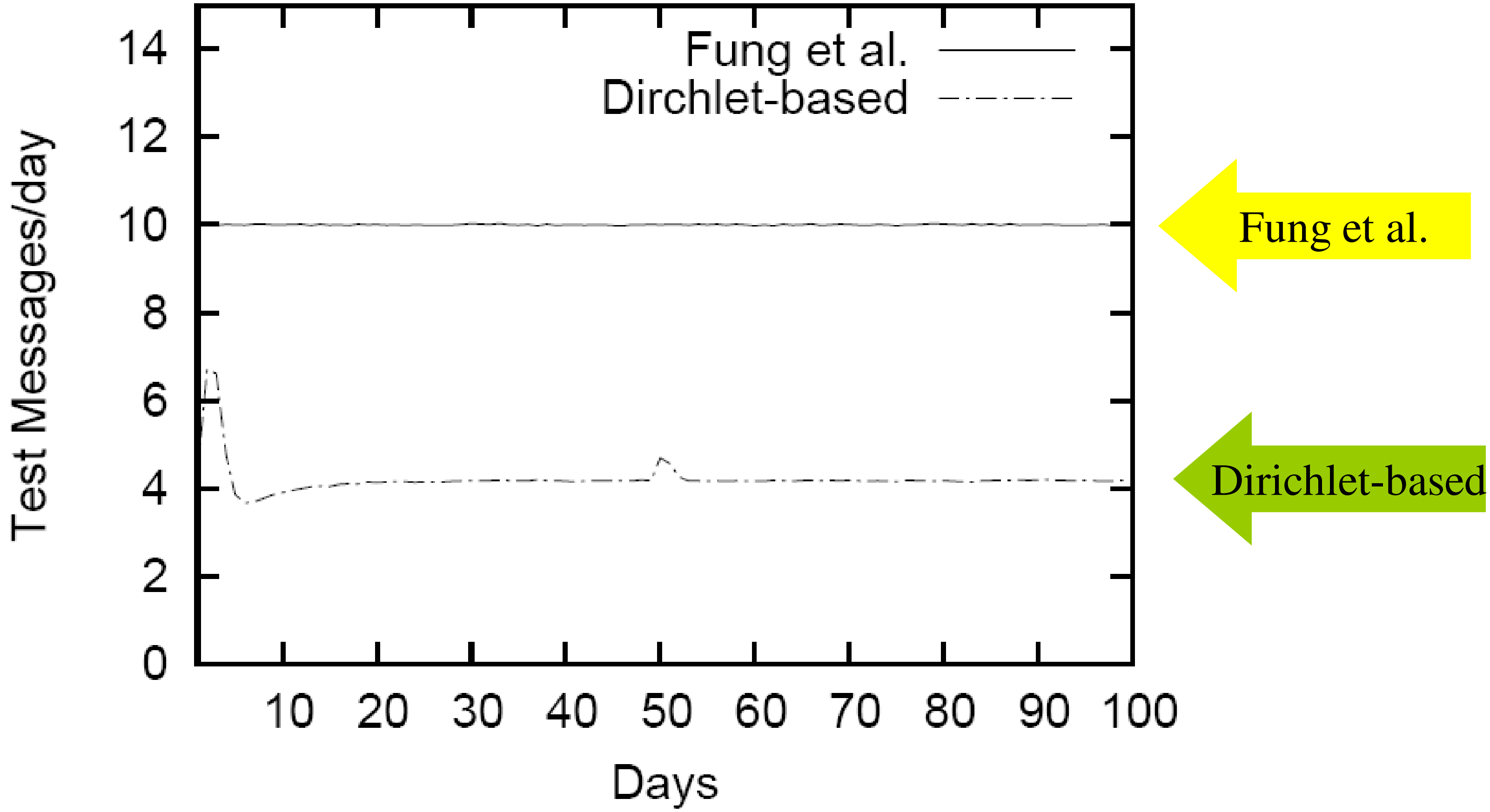


Fig 4. Test message rate under different models

Conclusion and Future Work

- Design a simulation framework for the purpose of comparing trust models in IDN
  - Single IDS model
  - Deception models
  - Attack models
  - Metrics
- Implementation of the simulation design

Thank You!