ETH zürich

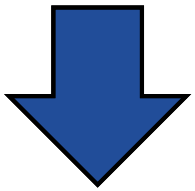
DITET

Stalk Me If You Can – The Anatomy of Sybil Attacks in Opportunistic Networks

Sacha Trifunovic, Andreea Hossmann-Picu
ETH Zurich, Switzerland

Opportunistic Networks

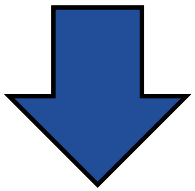
- **Cooperation** among mobile phone users
- Communicate when in *contact* (physical proximity),



- Complement wireless communication (cell, Wi-Fi)
- Communicate during failure/lack of infrastructure (disaster, remote areas)

Opportunistic Networks

- **Cooperation** among mobile phone users
- Communicate when in *contact* (physical proximity),



- Complement wireless communication (cell, Wi-Fi)
- Communicate during failure/lack of infrastructure (disaster, remote areas)

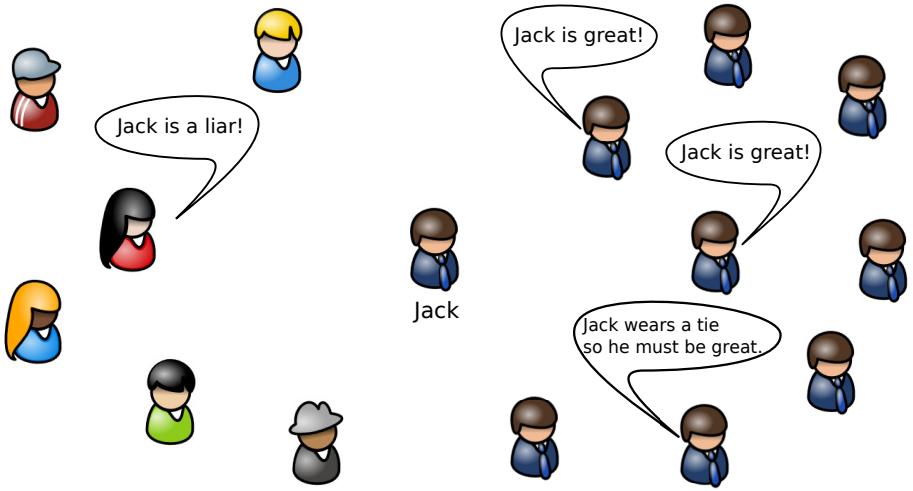
Honest node cooperation is key!

Threats to Honest Cooperation

I. Benign selfishness
   - effects of selfishness [Li'10, Sermpezis'14]
   - incentive systems [Chen'10, Krifa'11]

II. Malicious nodes
   - generate congestion (DDoS)
   - silent packet dropping (black holes)
   - Sybil attacks

Sybil attack



Fake identities to . . .

- increase resource allocation
- outvote recommendation systems
- “spread the blame”

Sybil attack in OppNets

OppNets are *easy* targets:

- highly distributed and dynamic nature
- no centralized user certification

OppNets are *challenging* targets:

- attack edges require co-location
- attacker must follow target node(s)

Sybil attack in OppNets

OppNets are *easy* targets:

- highly distributed and dynamic nature
- no centralized user certification

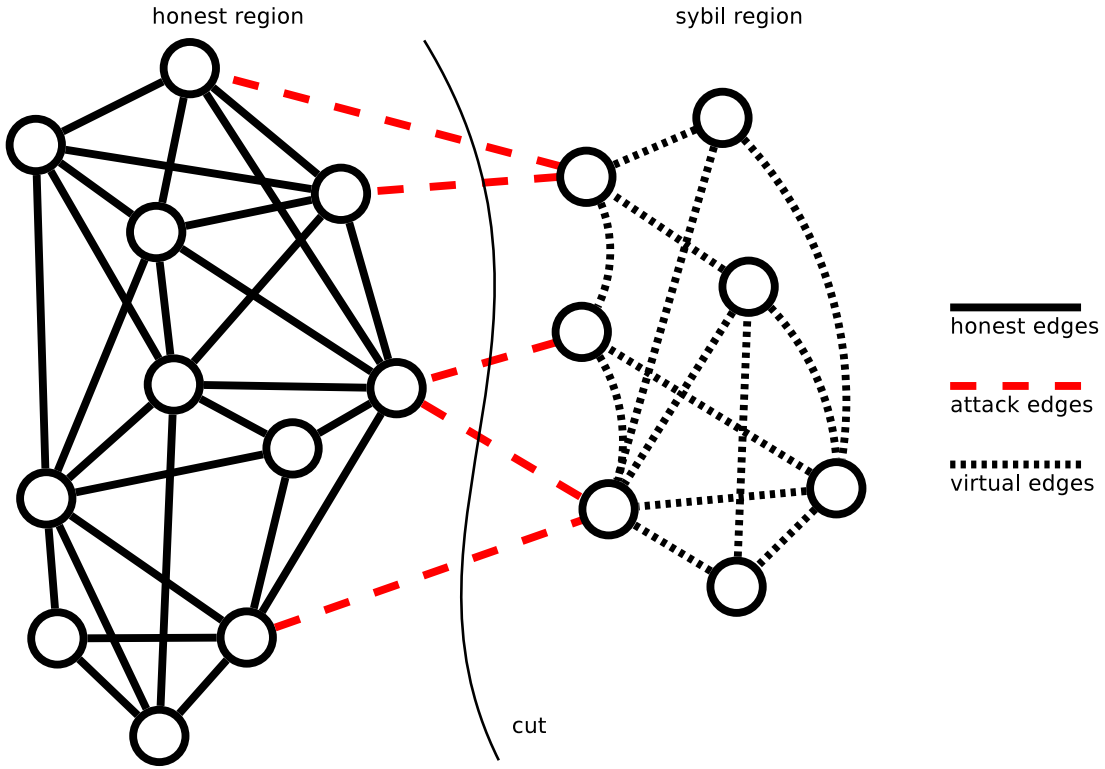
OppNets are *challenging* targets:

- attack edges require co-location
- attacker must follow target node(s)

Sybil attack on Oppnets: easy OR challenging???

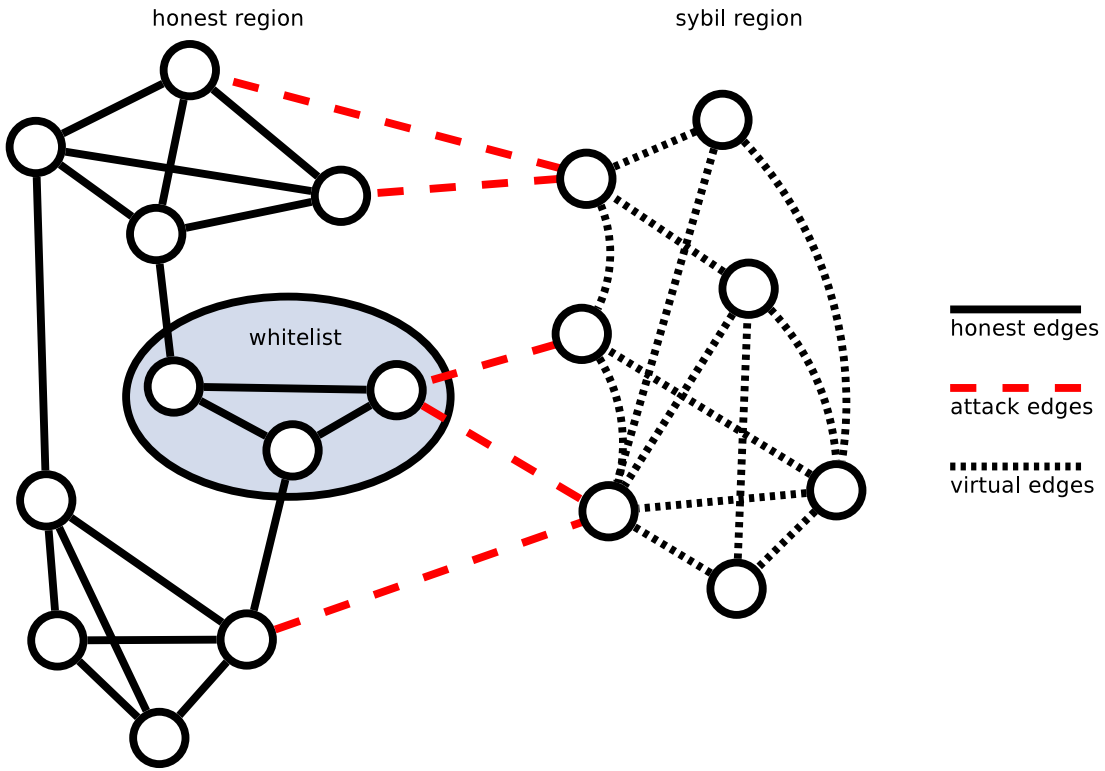
Sybil Detection/Defense

Initially: global defence [Yu'08]



Sybil Detection/Defense

State of the art: local whitelisting [Alvisi'13]



Application to OppNets

- Need *static graph*!
- Aggregate contacts to weighted graph [Hossmann'10]
  - contact frequency
  - contact duration
  - contact age
- Adapt latest Sybil defense algorithm

Ingredients of Sybil Attacks

I. Creating attack edges
   - edge weights are *crucial*!
   - total contact duration – most resilient
   - requires constant engagement

II. Node ID fabrication
   - Simultaneously broadcast multiple IDs
   - Advertise manipulated neighbor lists

Measuring Sybil Effectiveness

Metrics based on the local whitelisting algorithm

I. Trust rank of the attacker
   - Normalized rank – within target community

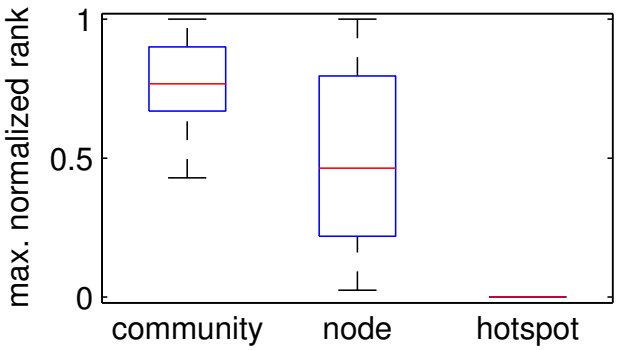
II. Amount of whitelisted Sybils
   - Influence – % of target community
   - Total influence – # of nodes in the network

Mobility traces

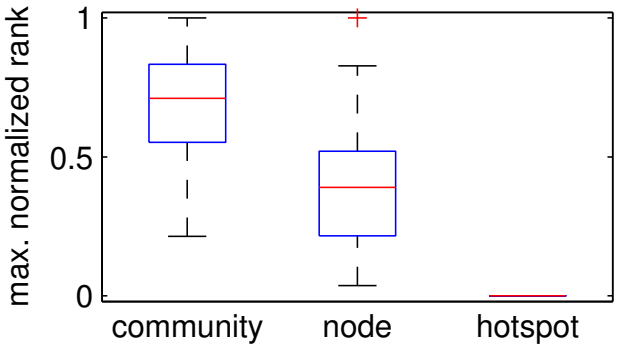
	TVCM	ETH	DART
# Nodes	505	294	1045
Time Period	72 hours	14.6 weeks	16.9 weeks
Type	Coordinates	AP assoc.	AP assoc.
# Contacts Total	3’822’531	101’805	5’177’521
# Contacts/Node	7’569	346	4’954
# Communities	34	26	65
Modularity	0.89	0.77	0.61

Finding the Optimal Target

ETH

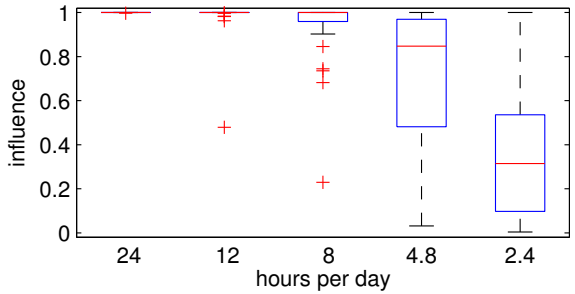


DART

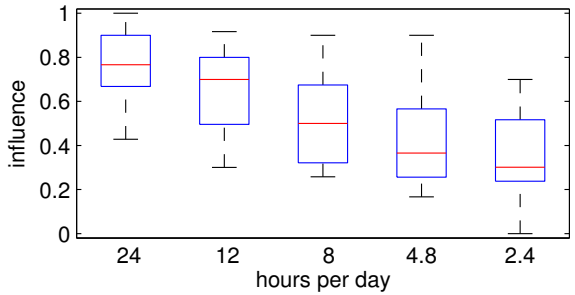


Required Time Investment

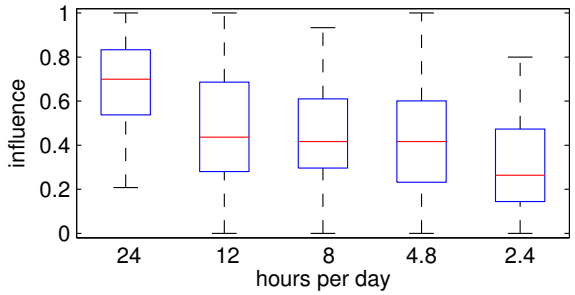
TVCM



ETH

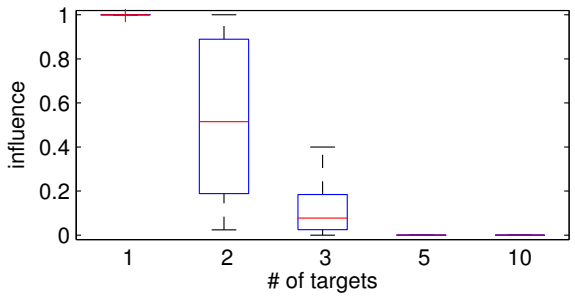


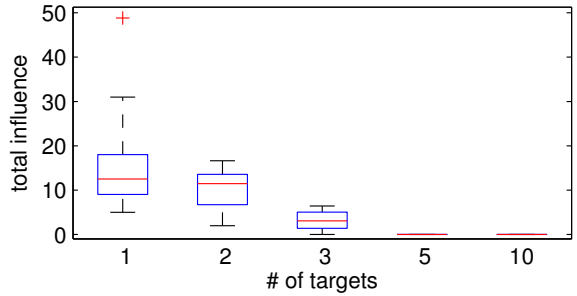
DART



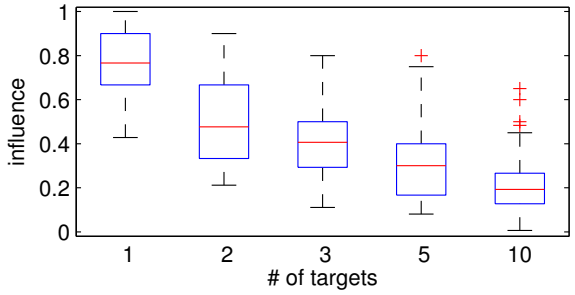
Attacking Multiple Targets

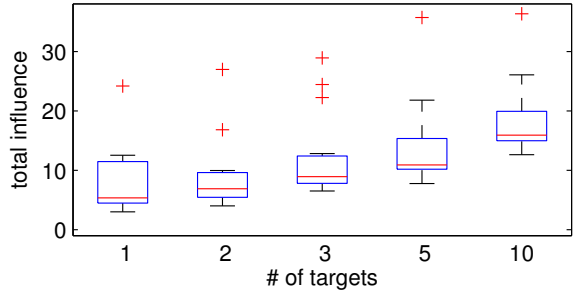
TVCM



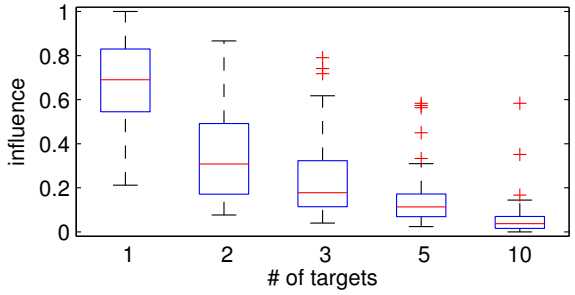


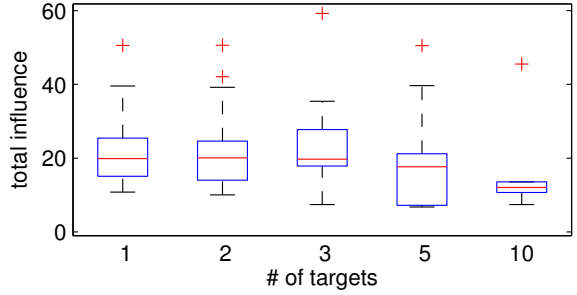
ETH





DART





Conclusion

I. First in-depth analysis of a Sybil Attack in OppNets

II. Lack of central authority allows for easy ID creation

III. Distributed nature of OppNet is also an opportunity
   - Implicit social structure hamper attack edge creation
   - Targets need to be continuously followed
   - Attack is limited to target communities

Conclusion

I. First in-depth analysis of a Sybil Attack in OppNets
II. Lack of central authority allows for easy ID creation
III. Distributed nature of OppNet is also an opportunity
   - Implicit social structure hamper attack edge creation
   - Targets need to be continuously followed
   - Attack is limited to target communities

Questions?