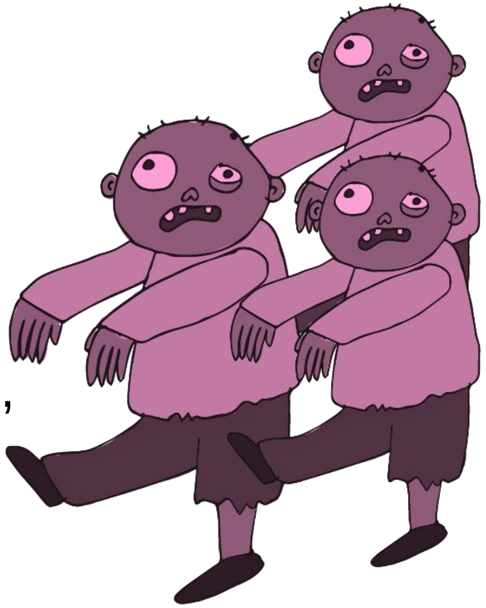
I Trust My Zombies: A Trust-Enabled Botnet



Emmanouil Vasilomanolakis, Jan Helge Wolf, **Leon Böck**,
Shankar Karuppayah, Max Mühlhäuser

Introduction #1

researchers botmaster

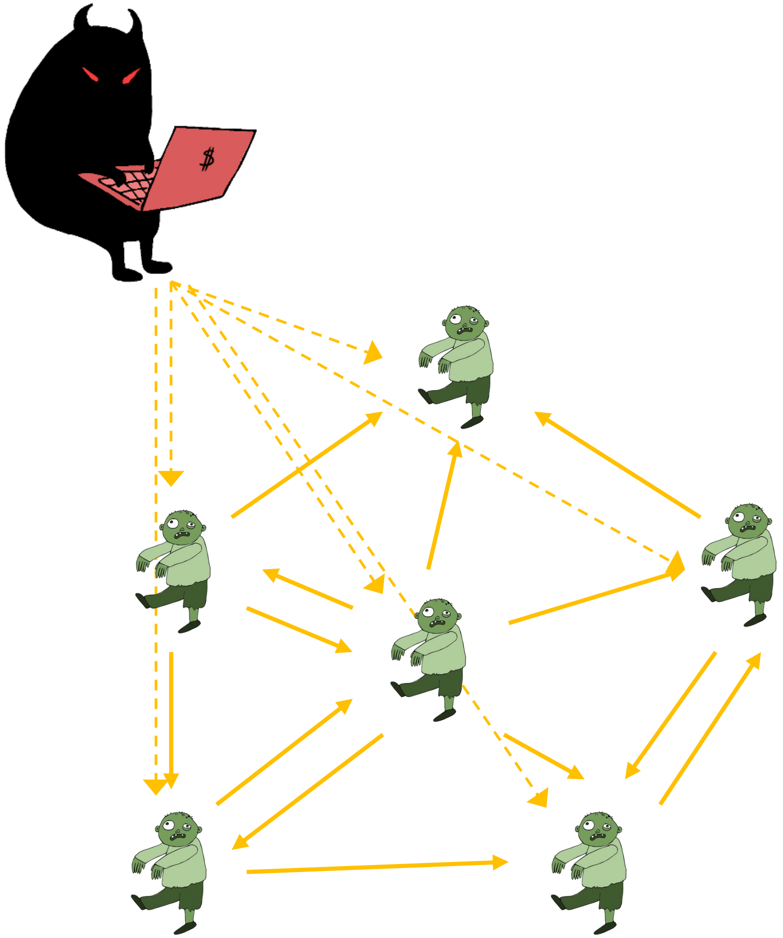
- Botnet monitoring is turning into a **cat** and **mouse** game…
- What if we start thinking like the bad guys?

Introduction #2

- Think as the attacker
- Envision the botnets of the future
  - ❑Exploit the limitations of defenders
  - ❑Mechanism for detecting the presence of sophisticated defenders

- Research Goal:
  - ❑Botnet in which monitoring is difficult/infeasible

Terminology #1



P2P Botnet:
a number of bots that communicate in a P2P fashion
and in which a botmaster can issue commands

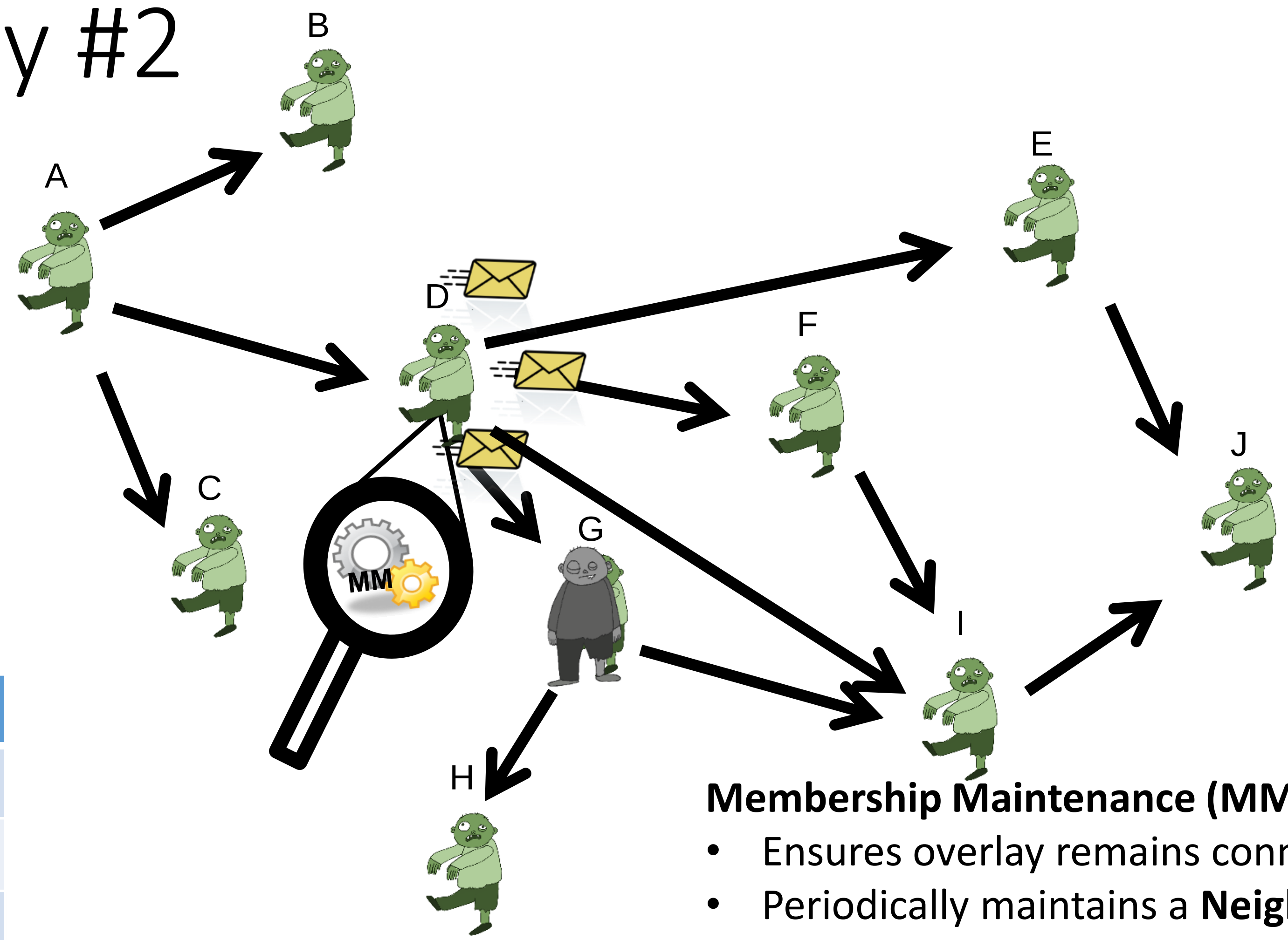
Bots behind NAT

Hi! I am a zombie
(Bot)

I am the evil Botmaster!

I am the good guy!

Terminology #2



Bot D	
No.	Neighbor
1	E
2	F
3	I

*The size of an NL ranges between 50-1000 entries

Membership Maintenance (MM) mechanism

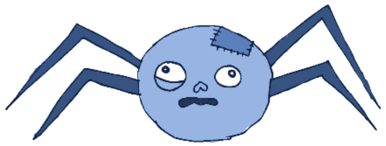
- Ensures overlay remains connected
- Periodically maintains a **Neighborlist** (NL)
  - ❑ Probes responsiveness frequently
  - ❑ Update/Replace entries as needed
  - ❑ Request additional neighbors

How can P2P botnets be taken down?

Reverse engineering

Analysis

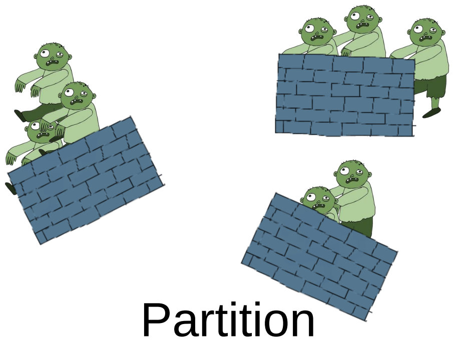
Preliminaries



Crawlers

Sensors

Monitoring

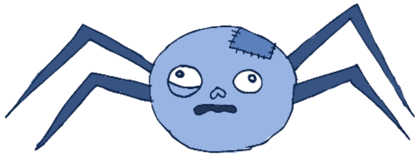


Partition

Sinkhole/Disarm

Disrupt

Background: crawlers & sensors



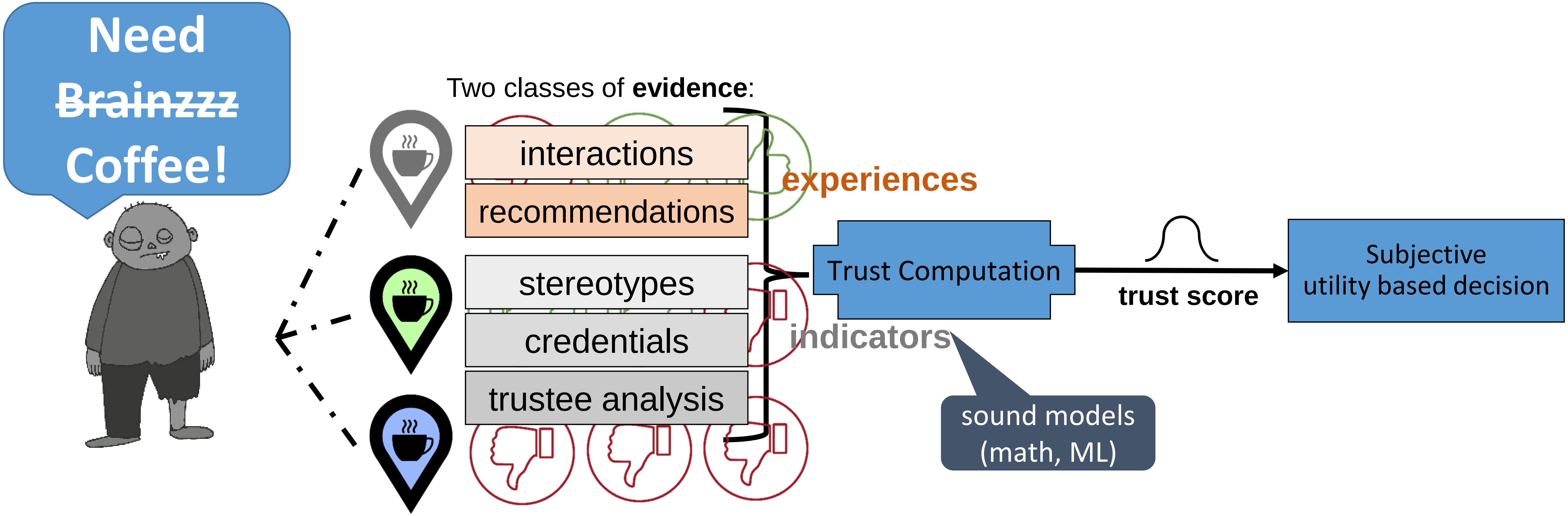
Crawler

- Aggressively crawls the botnet
- Attempts to create a holistic image of the botnet asap
- Can be **easily** detected and contended

Sensor

- Acts like a normal bot and builds up its knowledge (slowly)
- Harder to create a holistic view of the botnet
- Very passive compared to crawlers
- **Cannot** be easily detected and contended

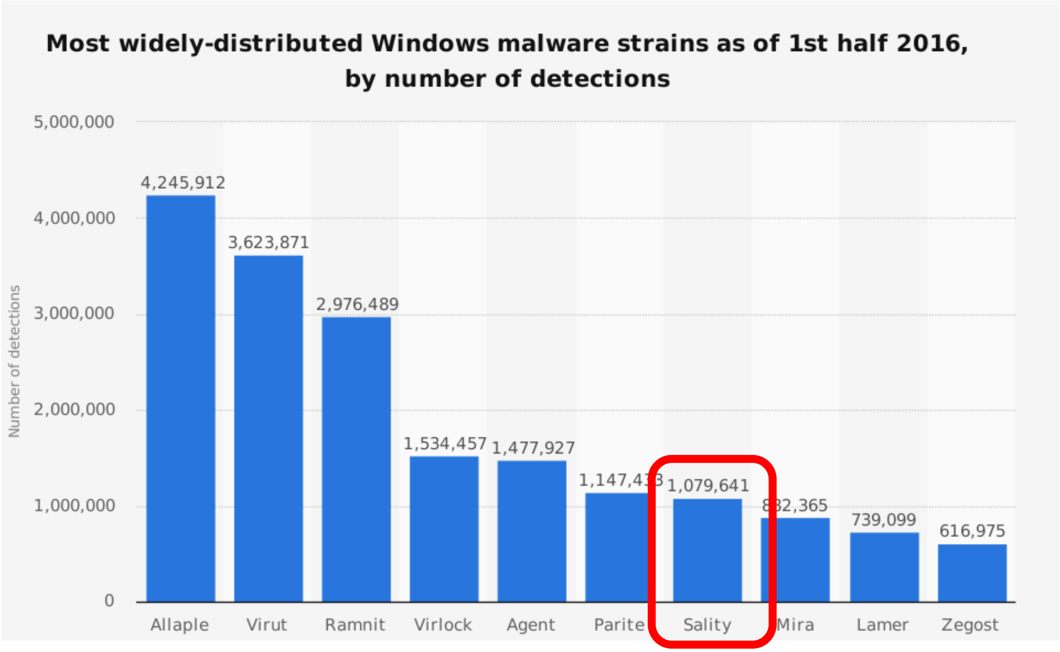
Background: Computational Trust



Background: the Sality P2P Botnet

- Early versions: 2003-2004!
- Very sophisticated all-around malware
- **P2P** since 2008
- Extremely resilient

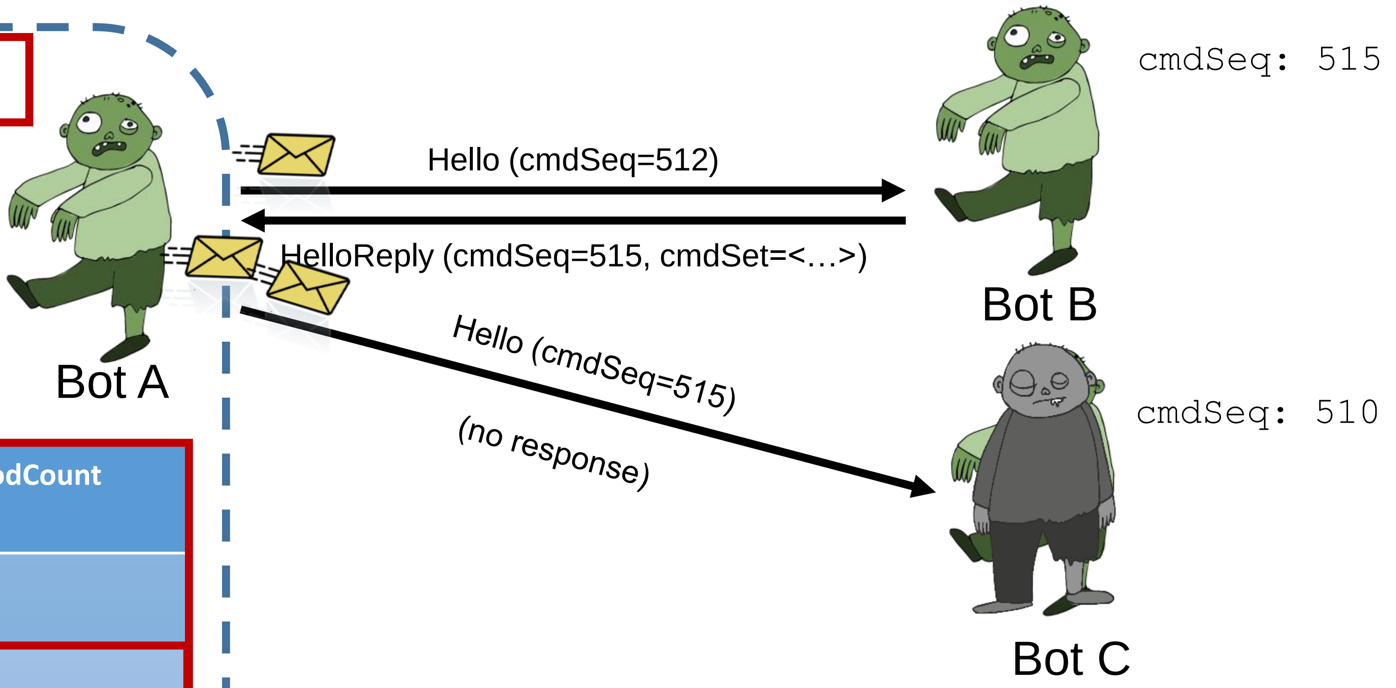
- Communication protocol
  - ❑ Membership maintenance
  - ❑ Command dissemination
- Basic trust management
  - ❑ *goodCount*



Worldwide, 1st half **2016** (Source: Statista)

Background: Sality “Hello” messages

`cmdSeq: 512`



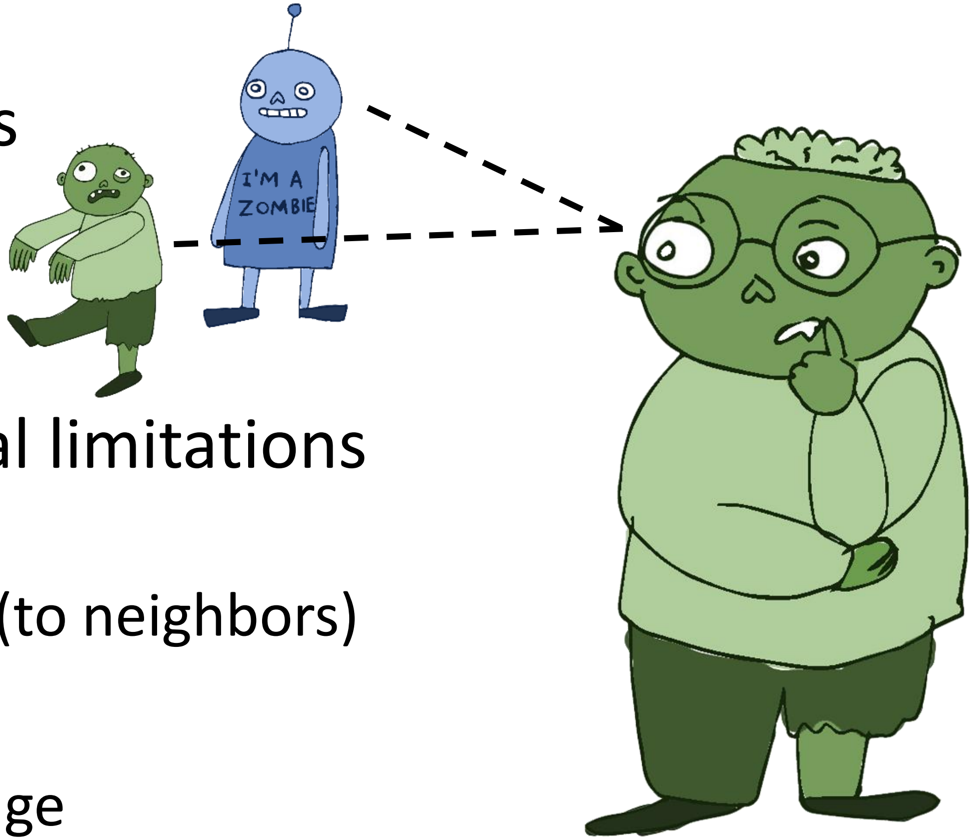
Id	IP	lastOnline	goodCount
B	1.2.3.4	2017-10-05 13:38:03	1
C	2.3.4.5	0000-00-00 00:00:00	5
…	…	…	…

cmdSeq (*command sequence*)**:**

- **an identifier of the latest command (simplified: the (internal) malware version)**

Meet our Botnet

- Cautious: careful to whom you talk to
- Smart: learn from your past experiences

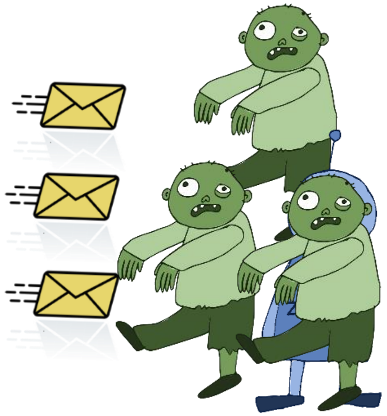


Core idea

- Defenders are bound to legal and ethical limitations
  - ❑They should not forward commands
  - ❑Exploitation via sending special messages (to neighbors)
- Utilization of computational trust
  - ❑Calculation and modeling of local knowledge

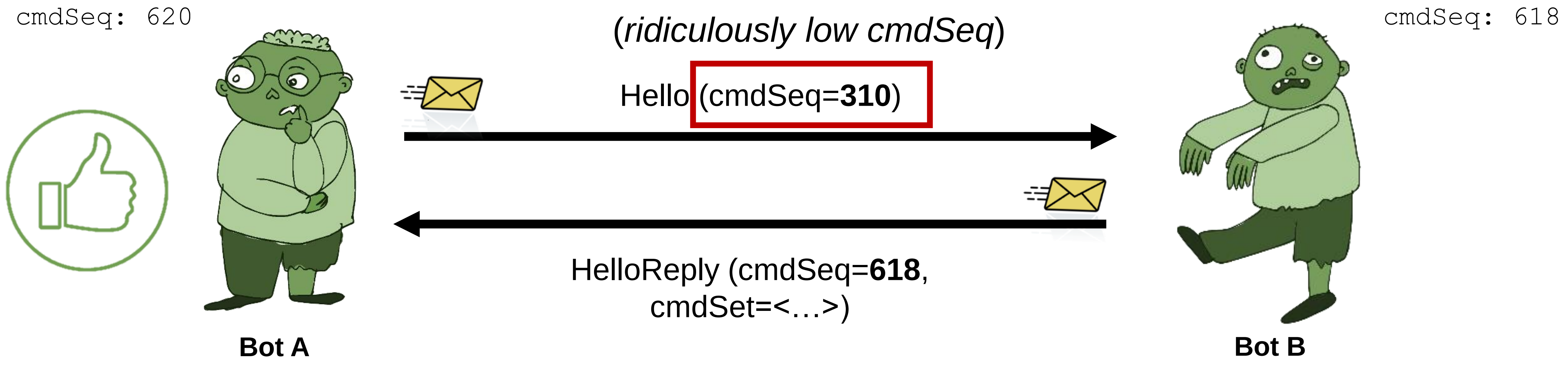
Meet our Botnet:
Bogus Command Sequence (BCS) Messages

- Extend basic botnet protocol
- Introduce a novel type of message
  - ❑Based on the ethical/legal limitations of sensors/crawlers
  - ❑BCS message: indistinguishable from common *hello messages*
  - ❑Forces zombies to reveal their true self



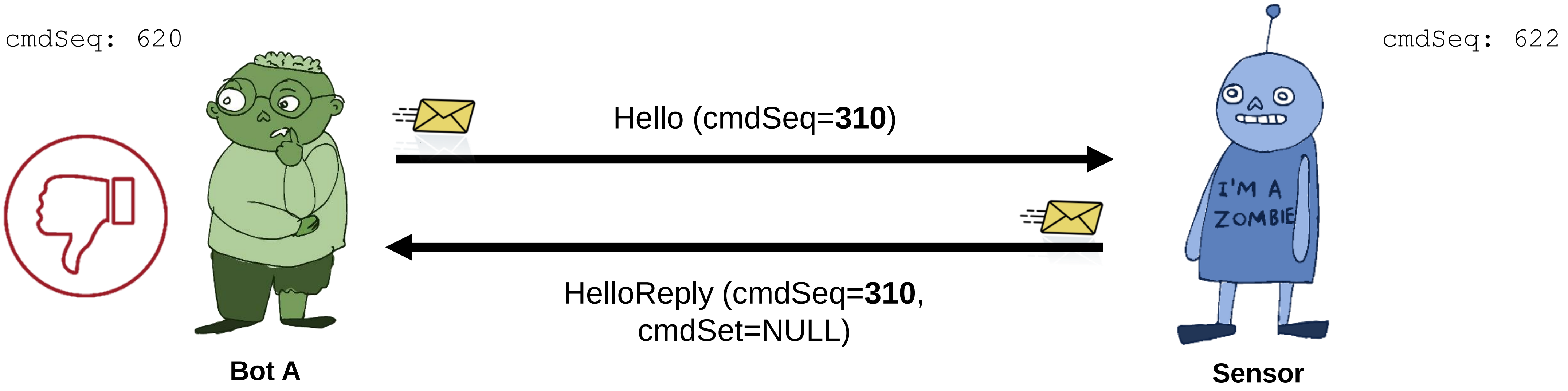
Meet our Botnet:

BCS Messages #1



Meet our Botnet:

BCS Messages #2

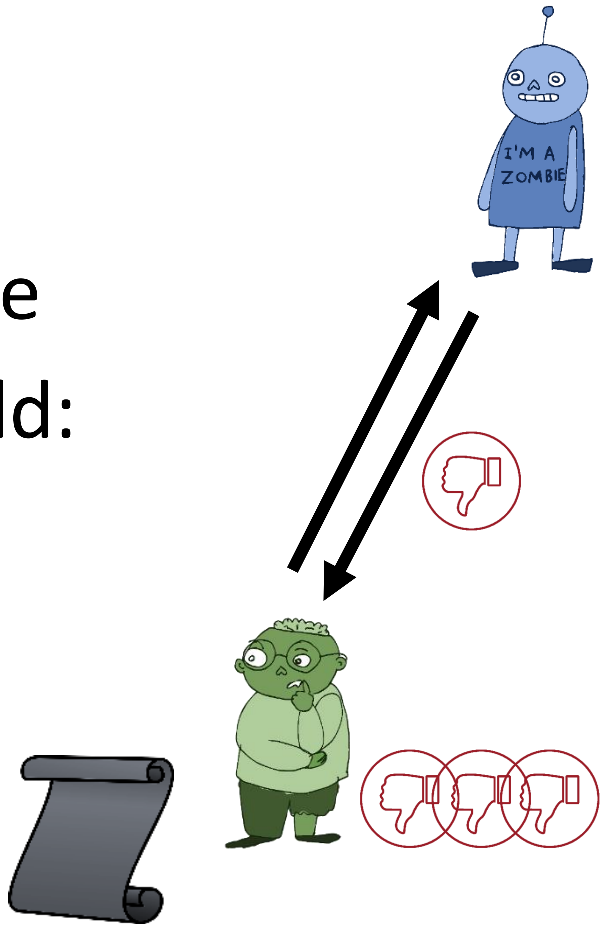


Meet our Botnet:

Trust Threshold and Blacklisting

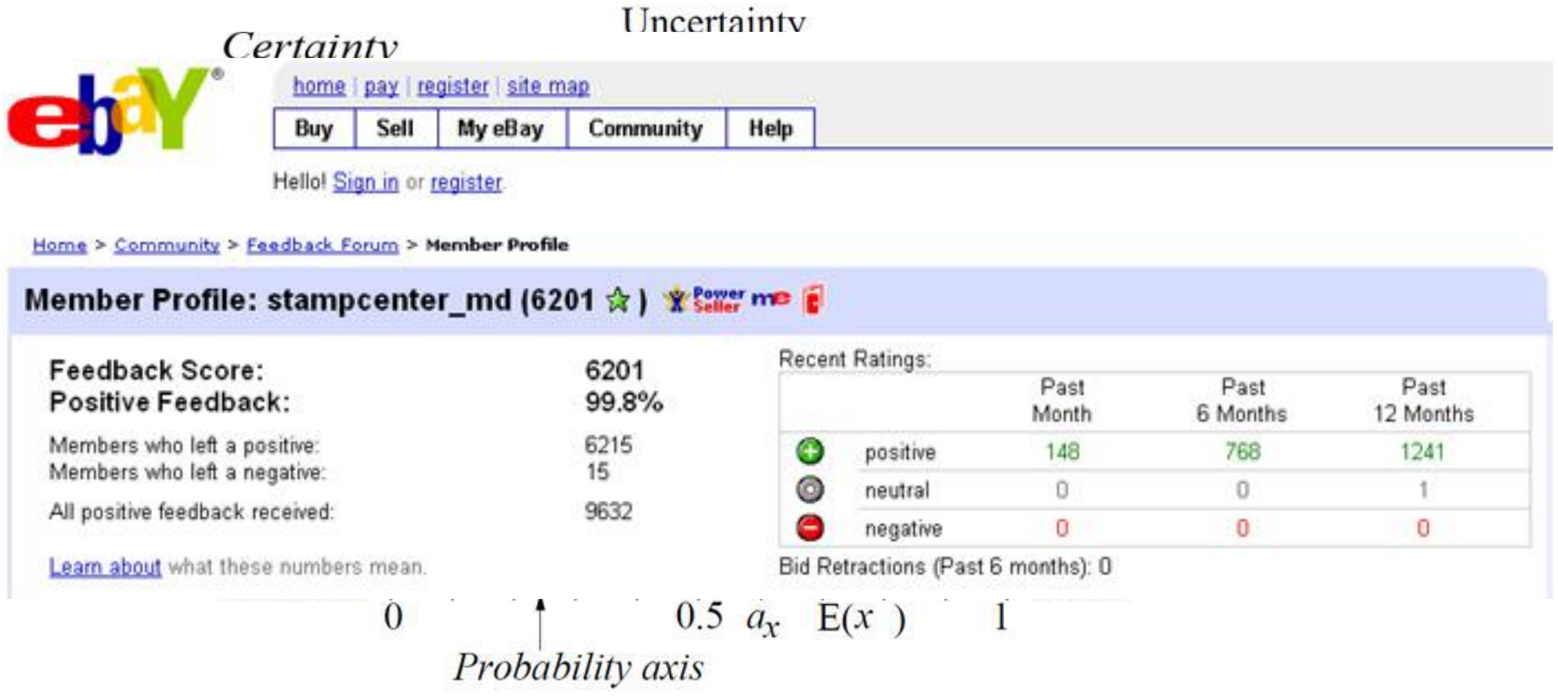
- Autonomous trust score calculation
- Trust score check after every new experience
- Trust score below pre-defined trust threshold:
  - ❑ Remove peer from neighborlist
  - ❑ Add to blacklist
    - Prevent re-adding to neighborlist
    - Drop all incoming messages
- Irreversible decision

„blacklisting“



Meet our Botnet:
Utilized Botnet Trust Models

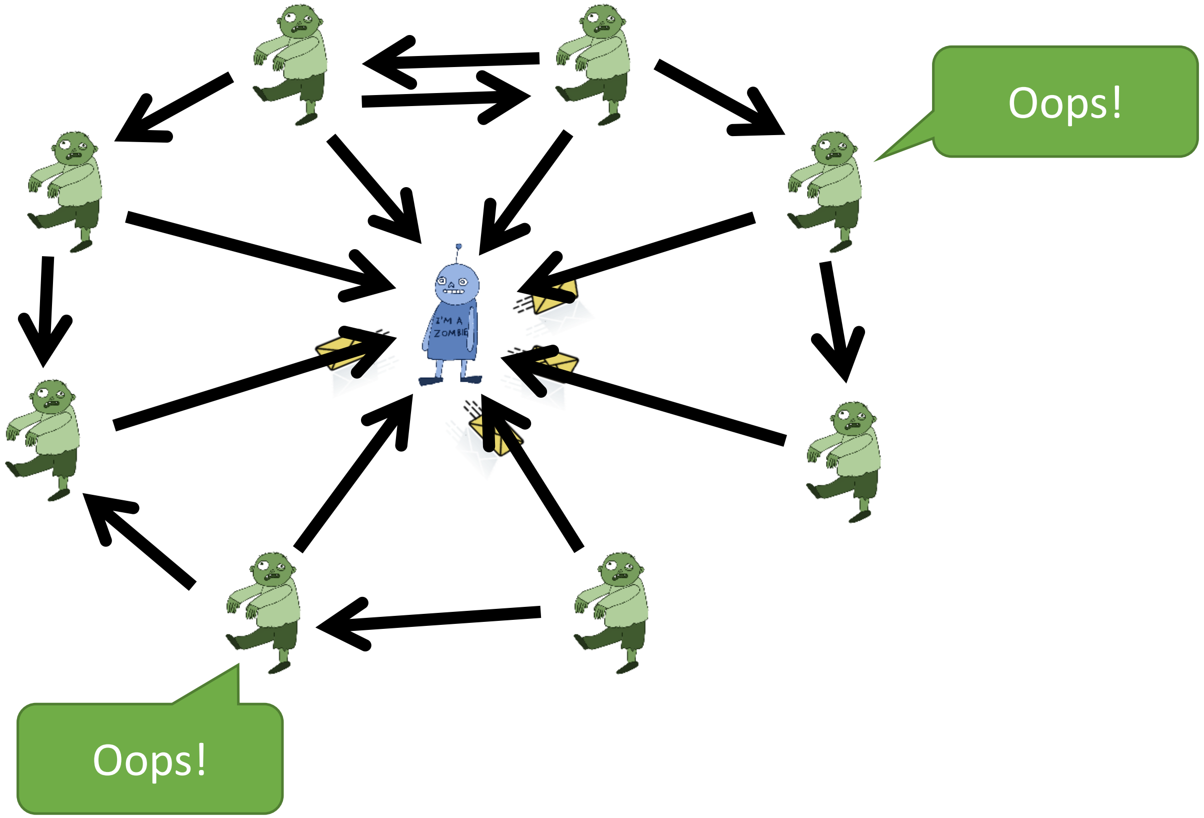
- Four trust models
  - ❑ EbayUserRating
  - ❑ BetaDistribution
  - ❑ SubjectiveLogic
  - ❑ CertainTrust



Experiments: objectives of monitoring

- Enumeration of the botnet
  - ❑ Sensor **popularity** (indegree)

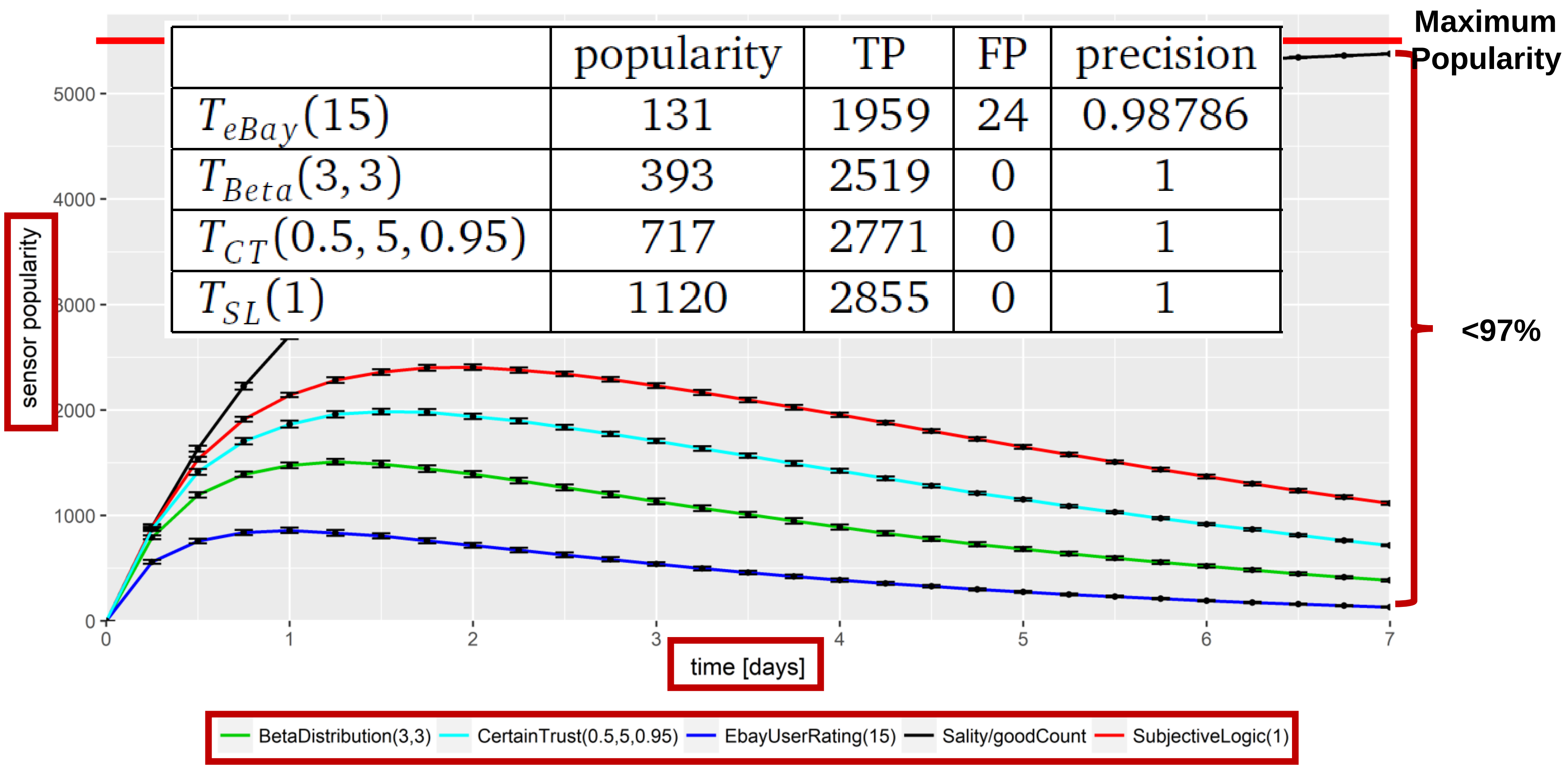
- Decrease sensor popularity
- Blacklisting precision
  - ❑ $p = \frac{TP}{TP+FP}$



Experiments: setup

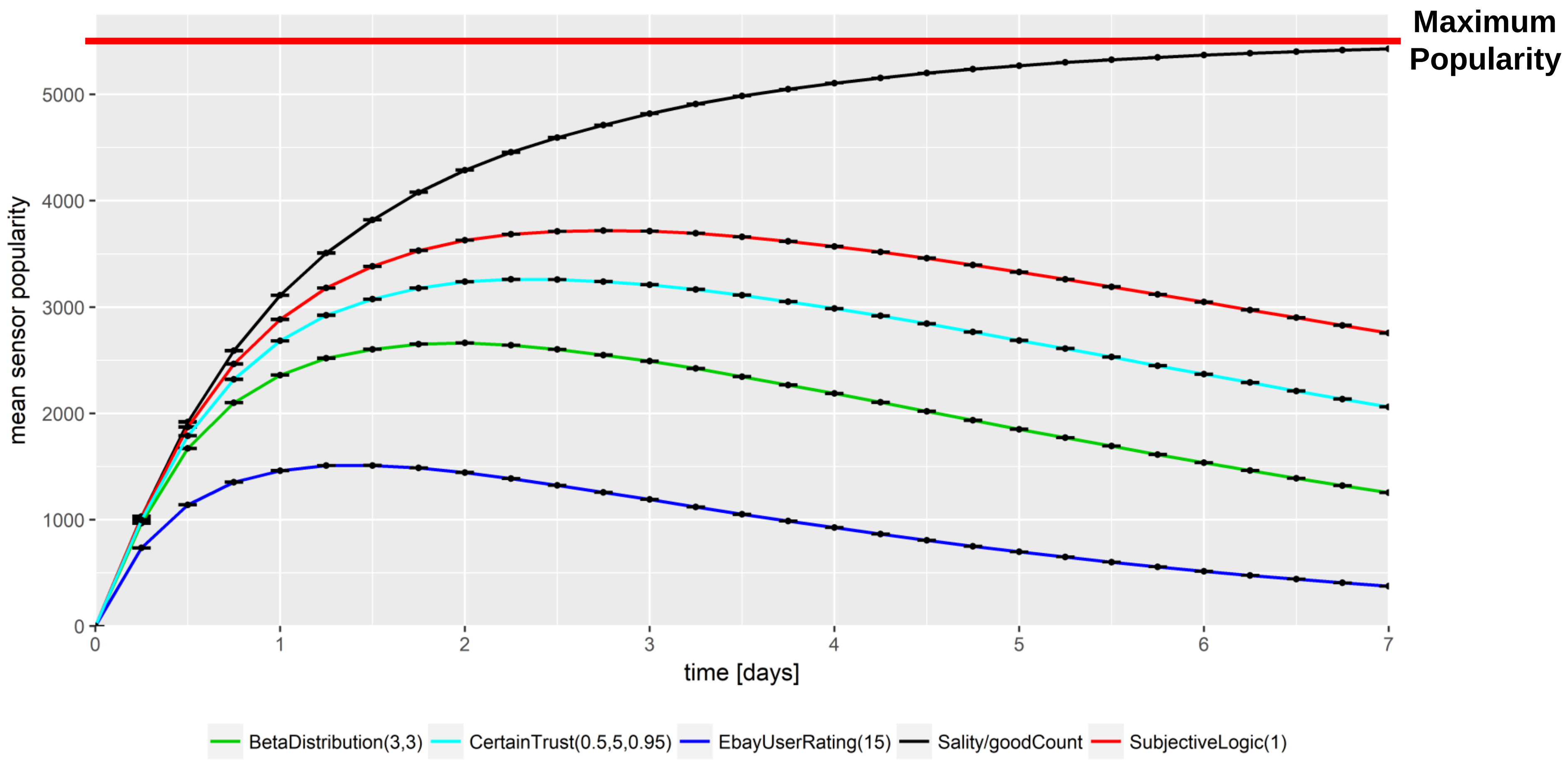
- Simulation environment
  - ❑ Botnet Simulation Framework (BSF) based on OMNeT++
- 5500 benign nodes
  - ❑ Churn
- 1/10/50 sensors
  - ❑ Permanently online
  - ❑ Cooperation among sensors
- Simulation time: 7 days
- 16 simulations per experiment

Experiments: Results – single-sensor

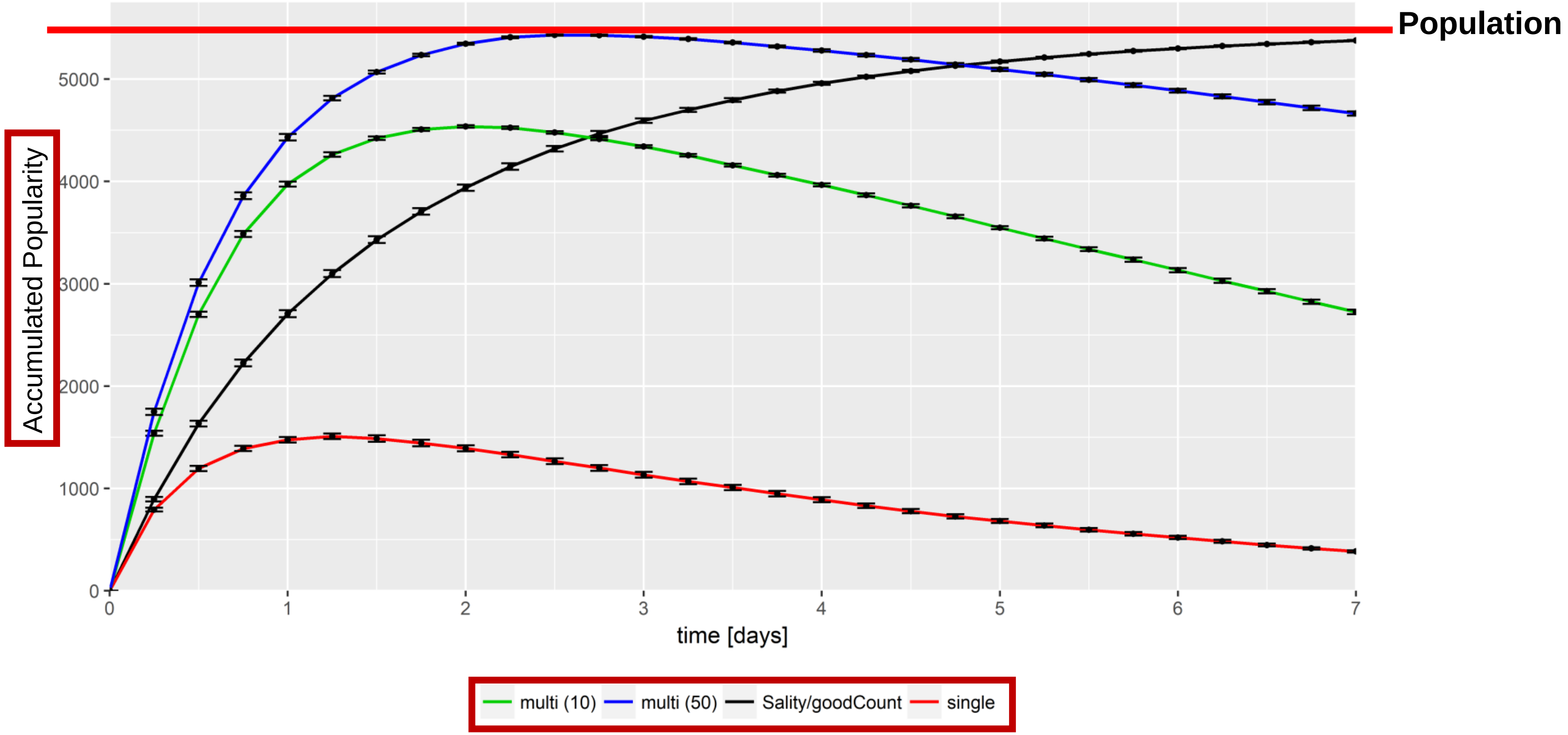


	popularity	TP	FP	precision
$T_{eBay}(15)$	131	1959	24	0.98786
$T_{Beta}(3,3)$	393	2519	0	1
$T_{CT}(0.5,5,0.95)$	717	2771	0	1
$T_{SL}(1)$	1120	2855	0	1

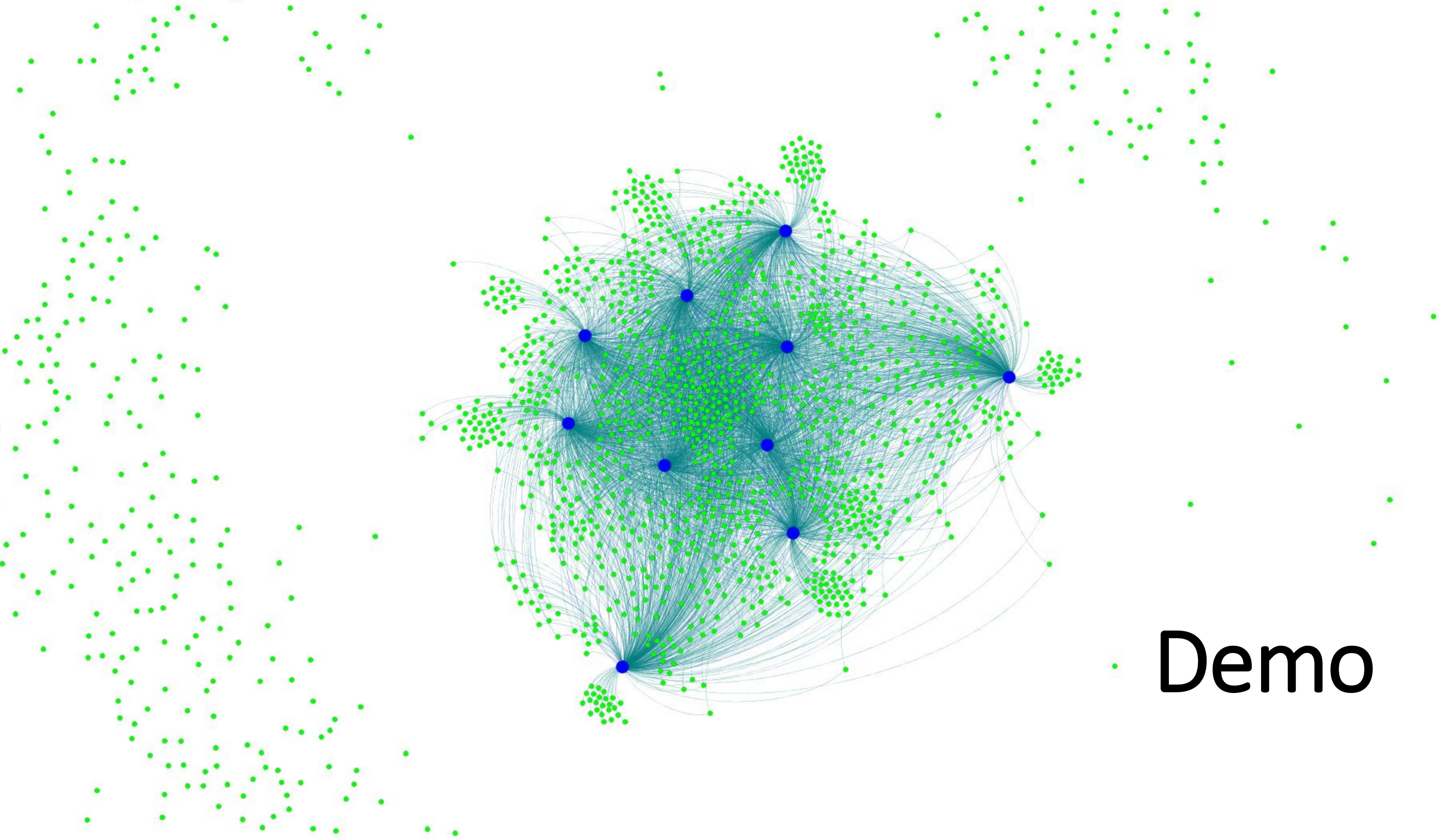
Experiments: Results – multi-sensor (10)



Experiments: Results – colluding sensors



comparison by number of sensors (BetaDistribution(3,3))



Demo

Conclusion

- The ***cat and mouse*** game will always benefit the mouse
  - ❑Infinite ways to improve botnets
  - ❑Cannot predict them all
- Monitoring P2P Botnets might become infeasible (soon)
  - ❑We have shown how to **decrease sensor effectiveness** by **up to 97**%
- The war is still not lost: **collaboration** might be the key
  - ❑Colluding sensors can provide an answer

Thank you!

Questions?