1000 days of UDP amplification DDoS attacks

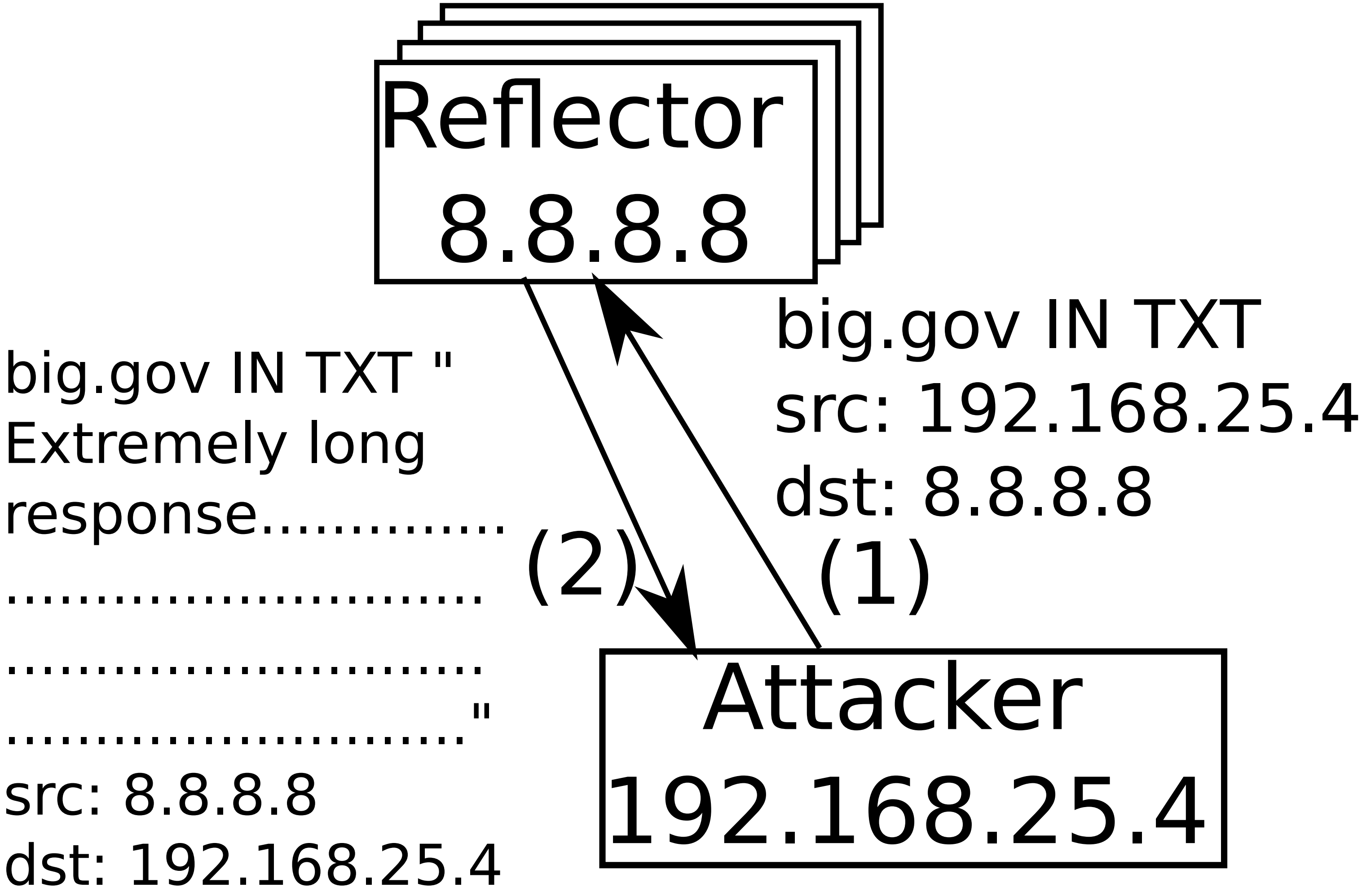
Daniel R. Thomas,
Richard Clayton,
Alastair R. Beresford

Firstname.Lastname@cl.cam.ac.uk

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Daniel:	5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Richard:	899A 94CE BFCE CCE2 5744 5ACE 3BBC CF52 A8B9 ECFB
Alastair:	9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3

UDP scanning



Reflector
8.8.8.8

big.gov IN TXT
src: 192.168.25.4
dst: 8.8.8.8

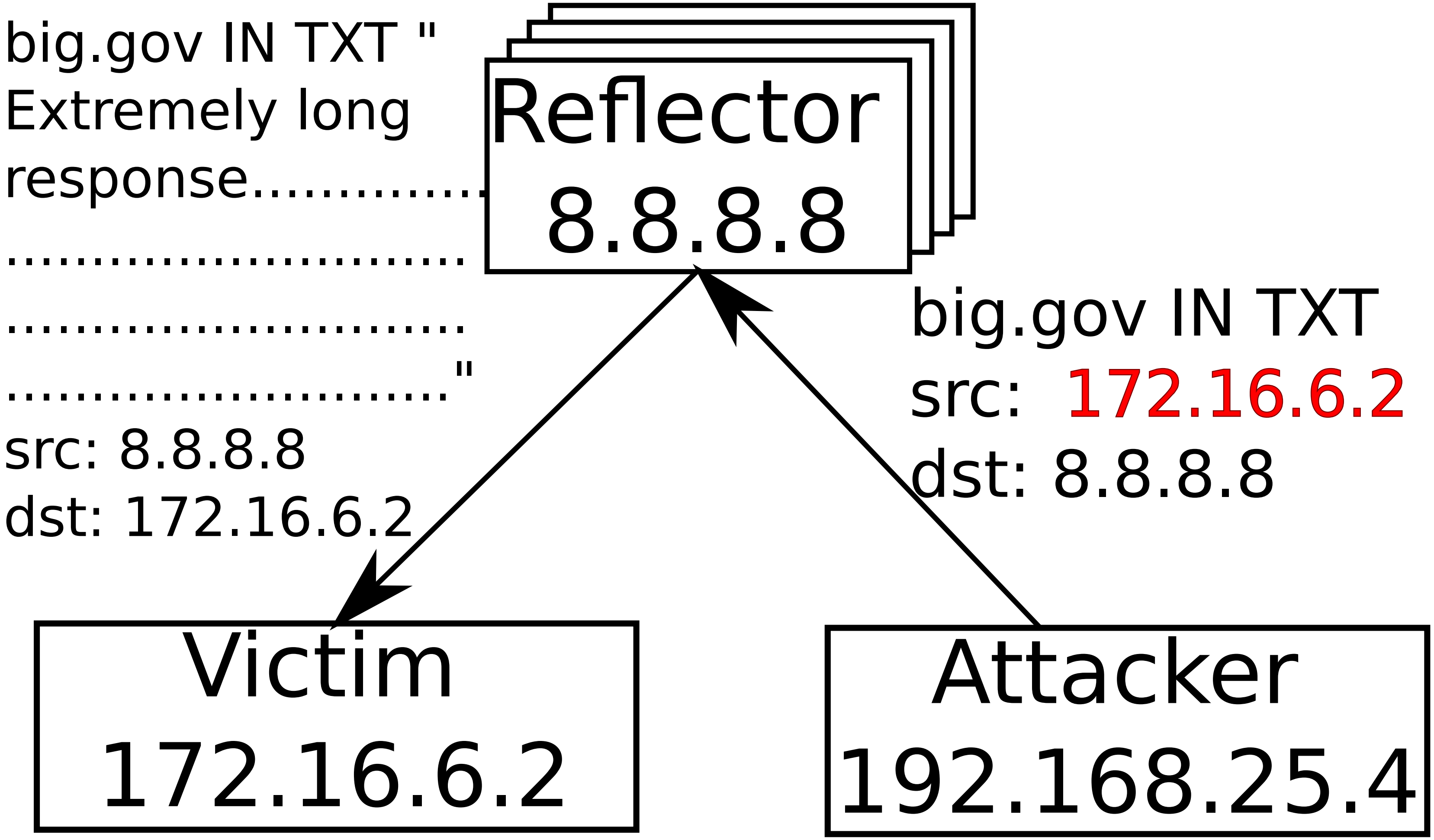
(1)

big.gov IN TXT "
Extremely long
response.............
....
....
........................."
src: 8.8.8.8
dst: 192.168.25.4

(2)

Attacker
192.168.25.4

UDP reflection DDoS attacks



big.gov IN TXT "
Extremely long
response.............
....
....
.........................."
src: 8.8.8.8
dst: 172.16.6.2

Reflector
8.8.8.8

big.gov IN TXT
src: 172.16.6.2
dst: 8.8.8.8

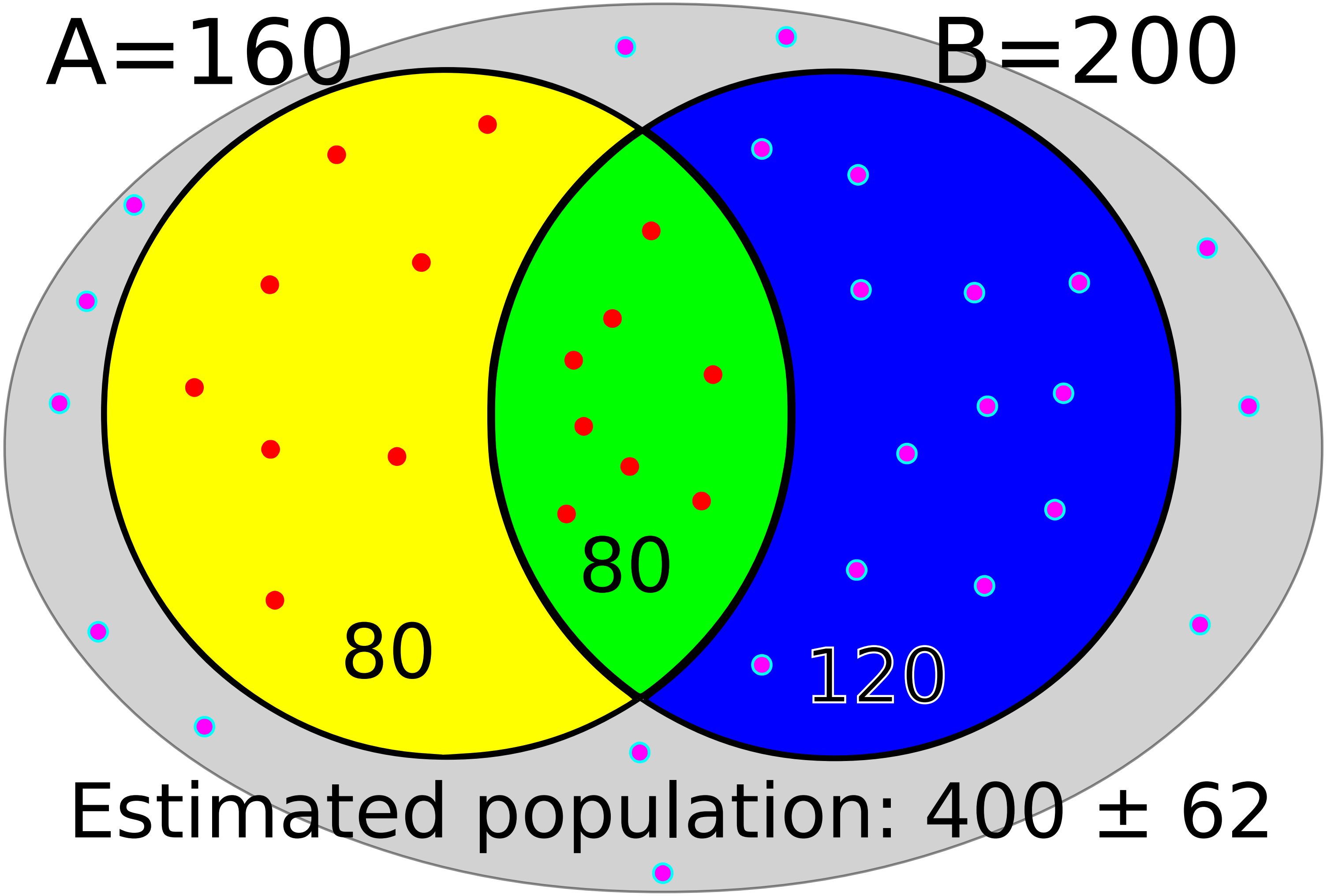
Victim
172.16.6.2

Attacker
192.168.25.4

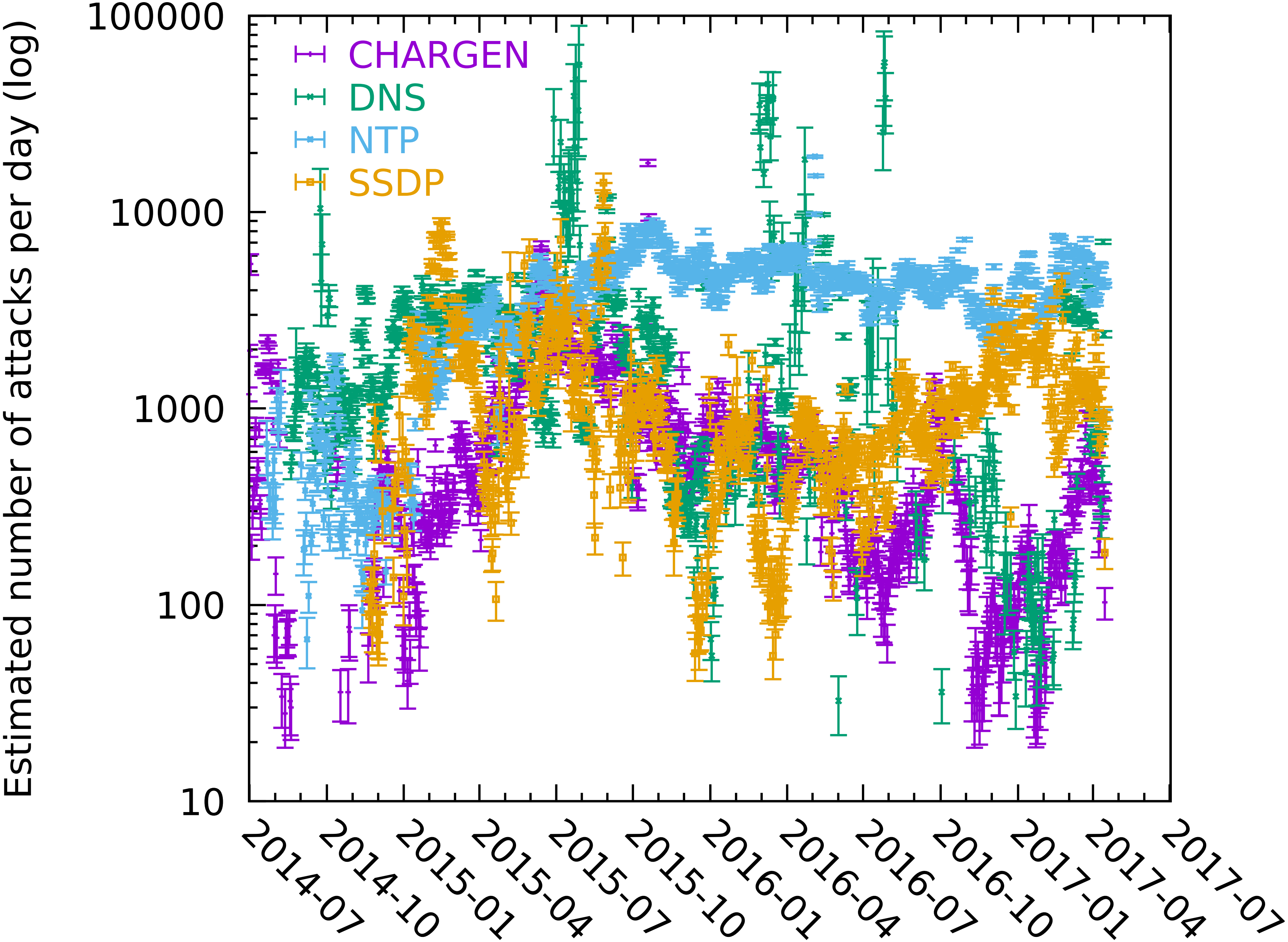
We run lots of UDP honeypots

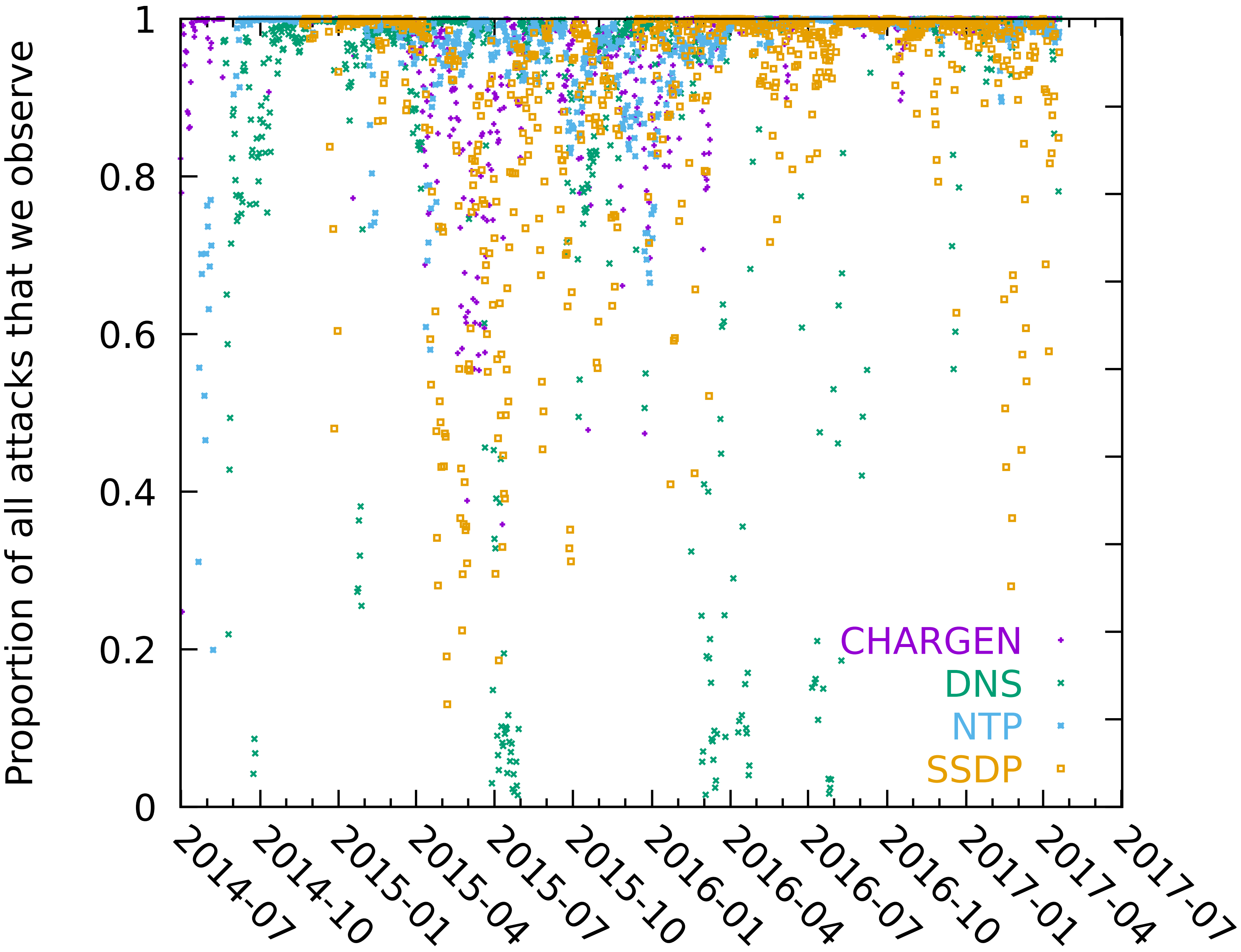
- Median 65 nodes since 2014
- Hopscotch emulates abused protocols
  - QOTD, CHARGEN, DNS, NTP, SSDP, SQLMon, Portmap, mDNS, LDAP
- Sniffer records all resulting UDP traffic
- (try to) Only reply to black hat scanners

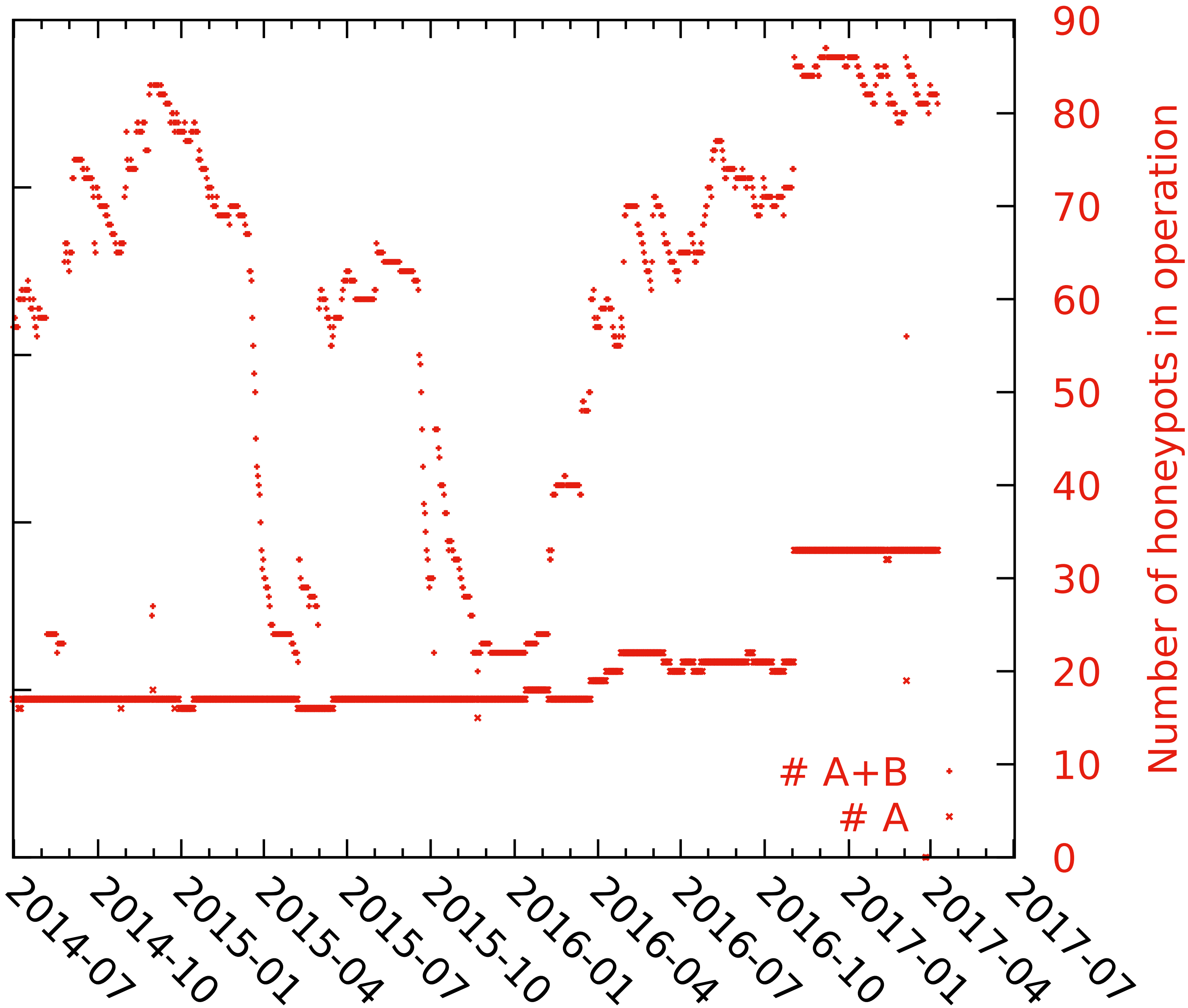
Estimating total attacks using capture-recapture

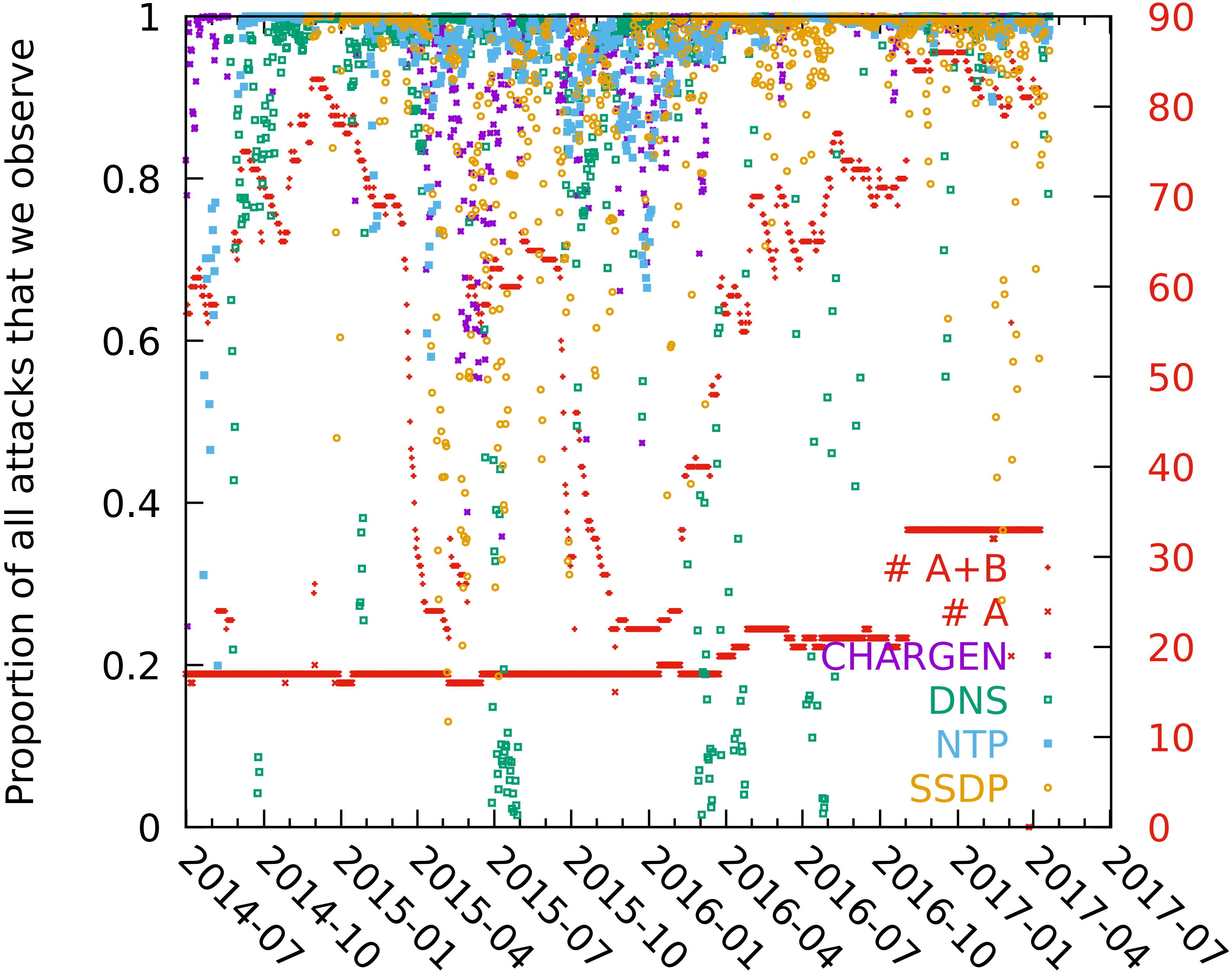


Estimated population: 400 ± 62


Estimated number of attacks per day (log)
100000
10000
1000
100
10
CHARGEN
DNS
NTP
SSDP
2014-07
2014-10
2015-01
2015-04
2015-07
2015-10
2016-01
2016-04
2016-07
2016-10
2017-01
2017-04
2017-07

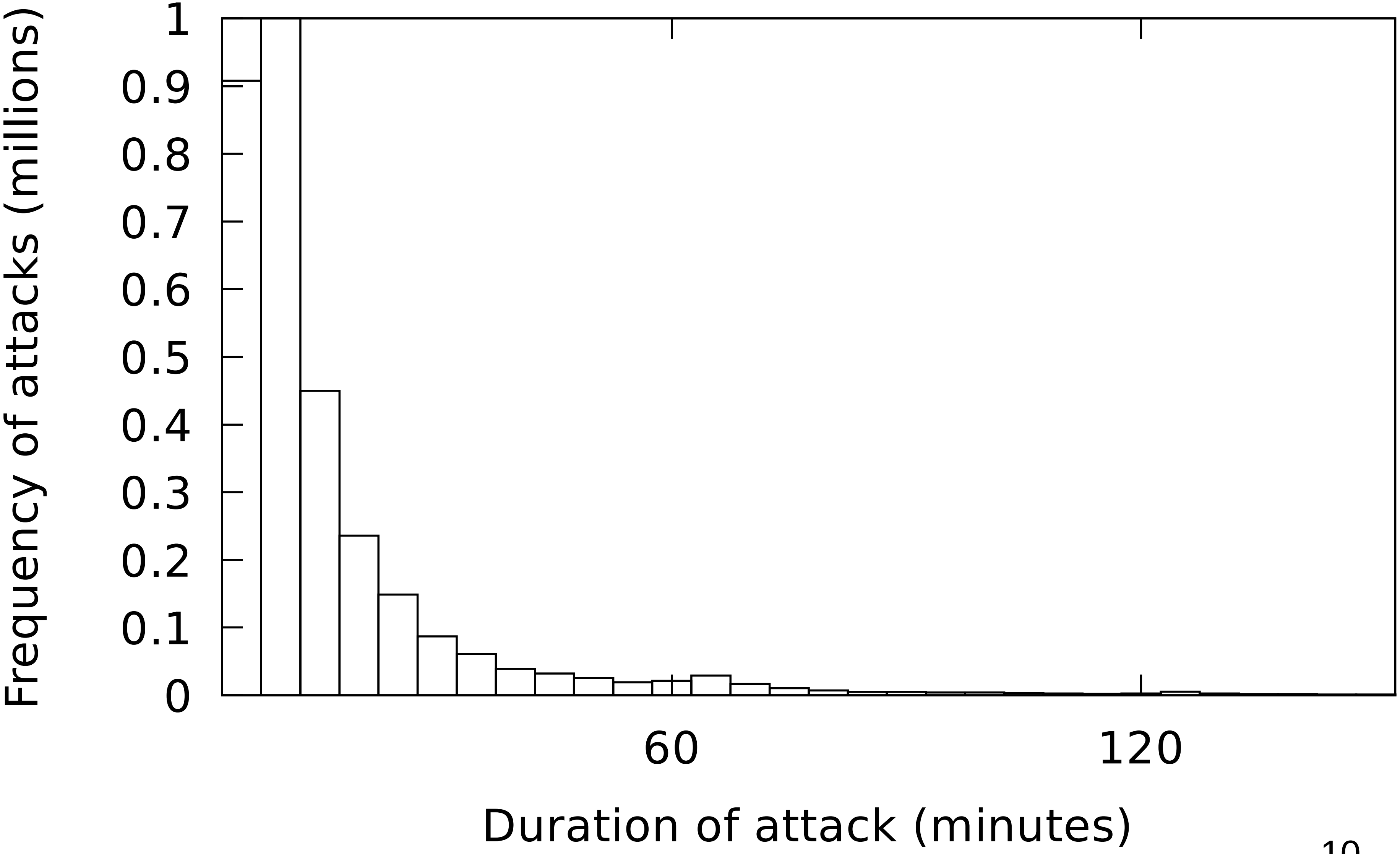

Proportion of all attacks that we observe
1
0.8
0.6
0.4
0.2
0
2014-07
2014-10
2015-01
2015-04
2015-07
2015-10
2016-01
2016-04
2016-07
2016-10
2017-01
2017-04
2017-07
CHARGEN
DNS
NTP
SSDP


90
80
70
60
50
40
30
20
10
0
Number of honeypots in operation
# A+B
# A
2014-07
2014-10
2015-01
2015-04
2015-07
2015-10
2016-01
2016-04
2016-07
2016-10
2017-01
2017-04
2017-07

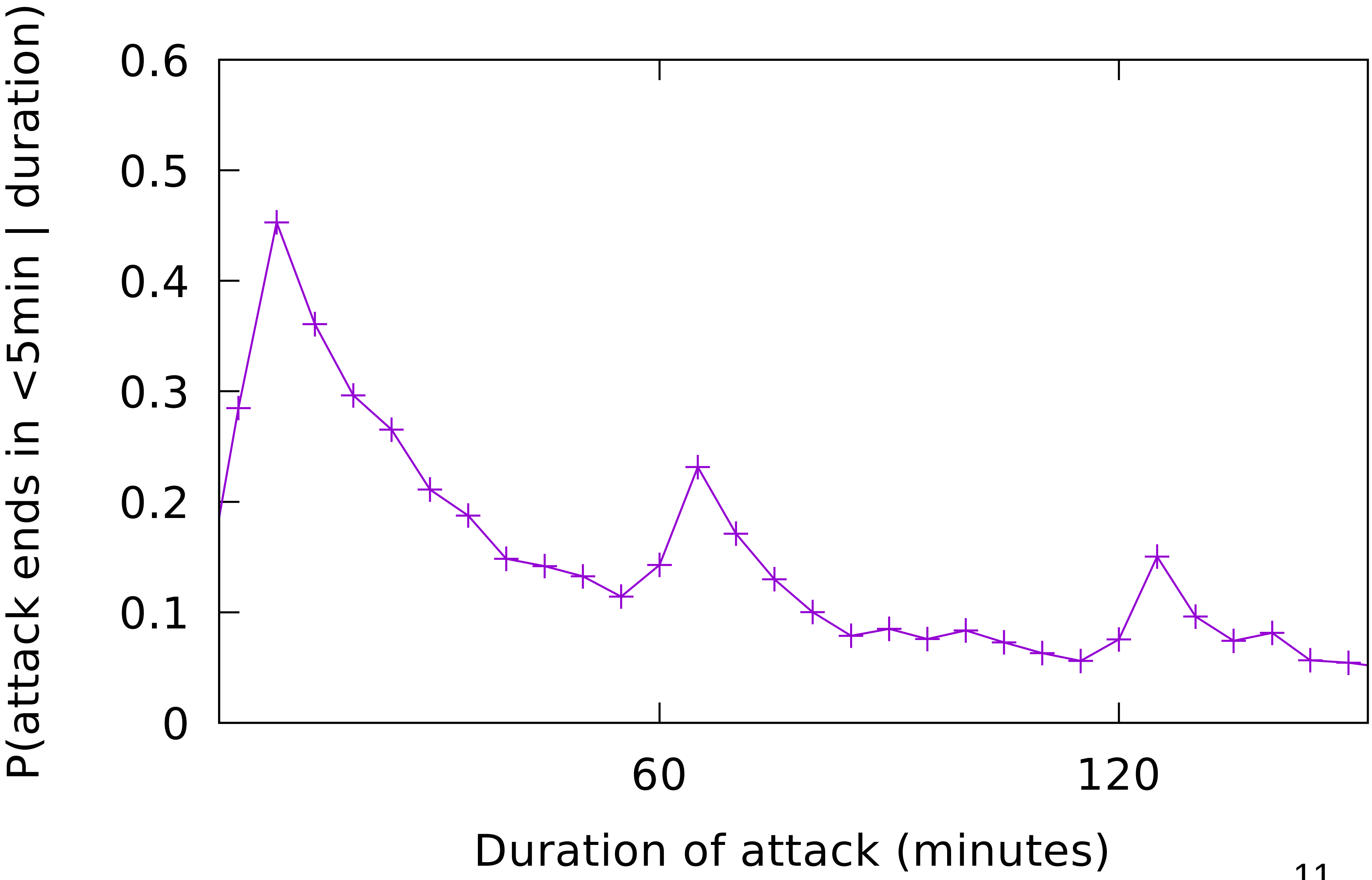


Proportion of all attacks that we observe
0
0.2
0.4
0.6
0.8
1
Number of honeypots in operation
0
10
20
30
40
50
60
70
80
90
2014-07
2014-10
2015-01
2015-04
2015-07
2015-10
2016-01
2016-04
2016-07
2016-10
2017-01
2017-04
2017-07
# A+B
# A
CHARGEN
DNS
NTP
SSDP

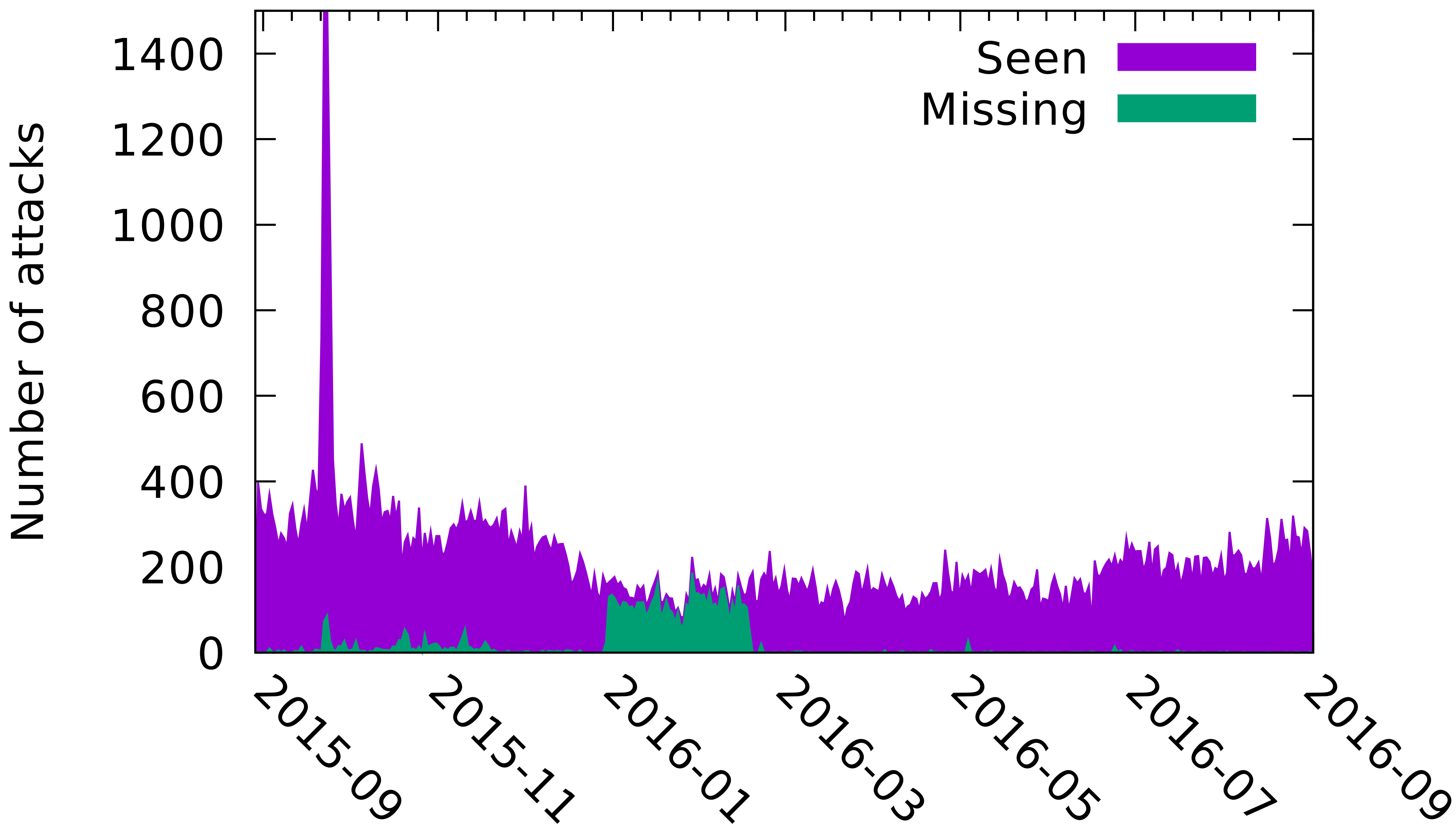
NTP


Frequency of attacks (millions)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
60
120
Duration of attack (minutes)

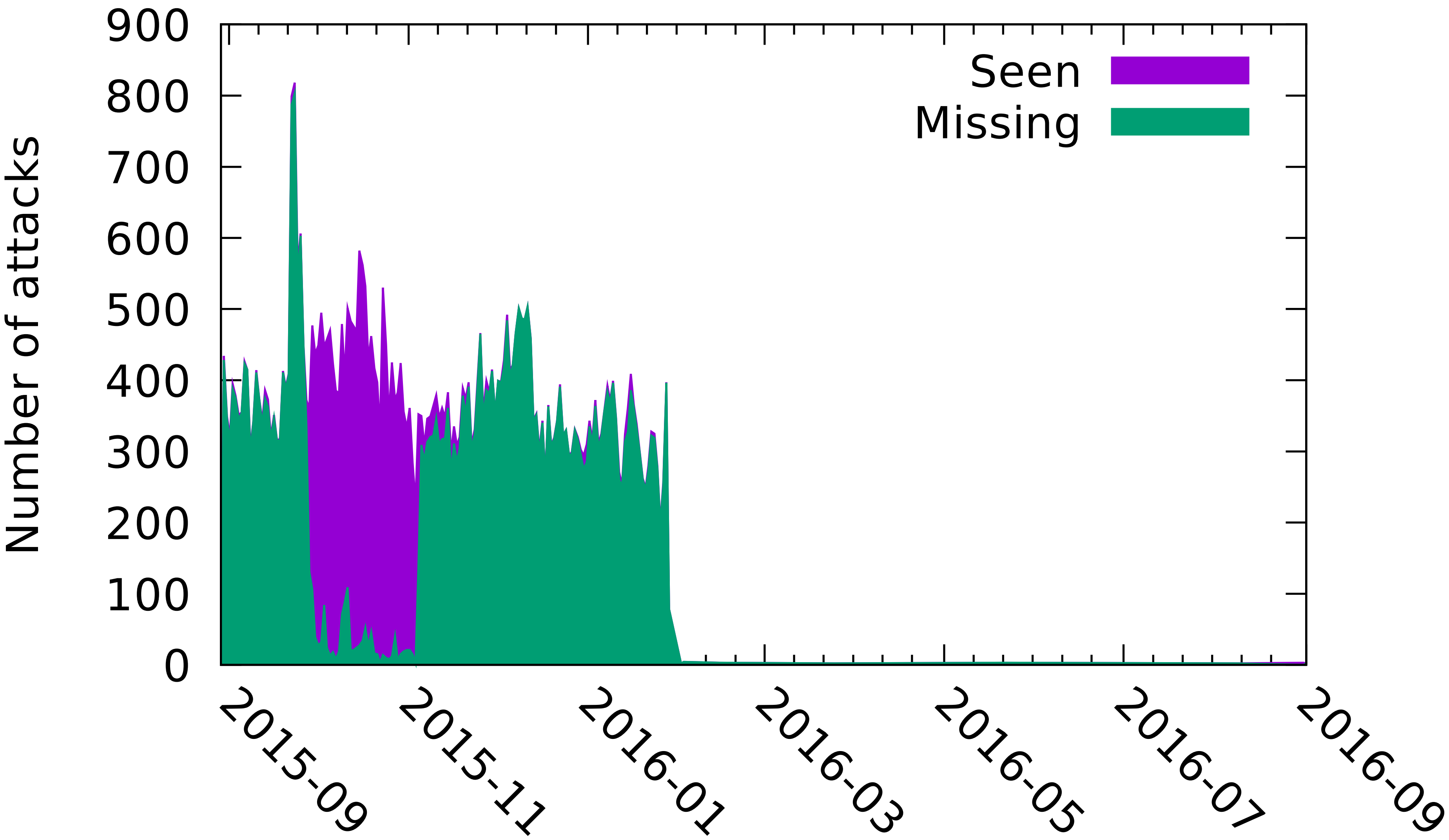
NTP


P(attack ends in <5min | duration)
0.6
0.5
0.4
0.3
0.2
0.1
0
60
120
Duration of attack (minutes)

Vdos coverage NTP



Vdos coverage SSDP



This was ethical

- We reduce harm by absorbing attack traffic
- We don't reply to white hat scanners (no timewasting)
- We used leaked data for validation, this was necessary and did not increase harm.
- We have a paper under submission on the ethics of using leaked data for research.

Running a honeypot network is cheap (but we do it for you)

- Median of 65 nodes.
- 200GB/month inbound per node.
- Hosting costs of $170/month (+staff costs)
- Need 10 to 100 sensors depending on protocol.
- Our collection is ongoing and you can use our data. You can also contribute.

This is a solvable problem

- BCP38/SAVE
- Follow the money
- Enforce the law
- Warn customers it is illegal

Ongoing work

- Selective reply (like Krupp et al. 2016)
- More cross validation
- Estimate attack volume
- Collaboration
  - What do you want to do with this data?
  - You can run our code.
  - Do you have ground truth for attack volumes?

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Data is available through the Cambridge Cybercrime Centre

https://cambridgecybercrime.uk/

Daniel R. Thomas
Richard Clayton
Alastair R. Beresford

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Firstname.Lastname@cl.cam.ac.uk

Daniel:	5017 A1EC 0B29 08E3 CF64 7CCD 5514 35D5 D749 33D9
Richard:	899A 94CE BFCE CCE2 5744 5ACE 3BBC CF52 A8B9 ECFB
Alastair:	9217 482D D647 8641 44BA 10D8 83F4 9FBF 1144 D9B3