SIP DoS Attack Detection

An Ontological Approach

PTSN

v

PSN

SIP as the VoIP Control System

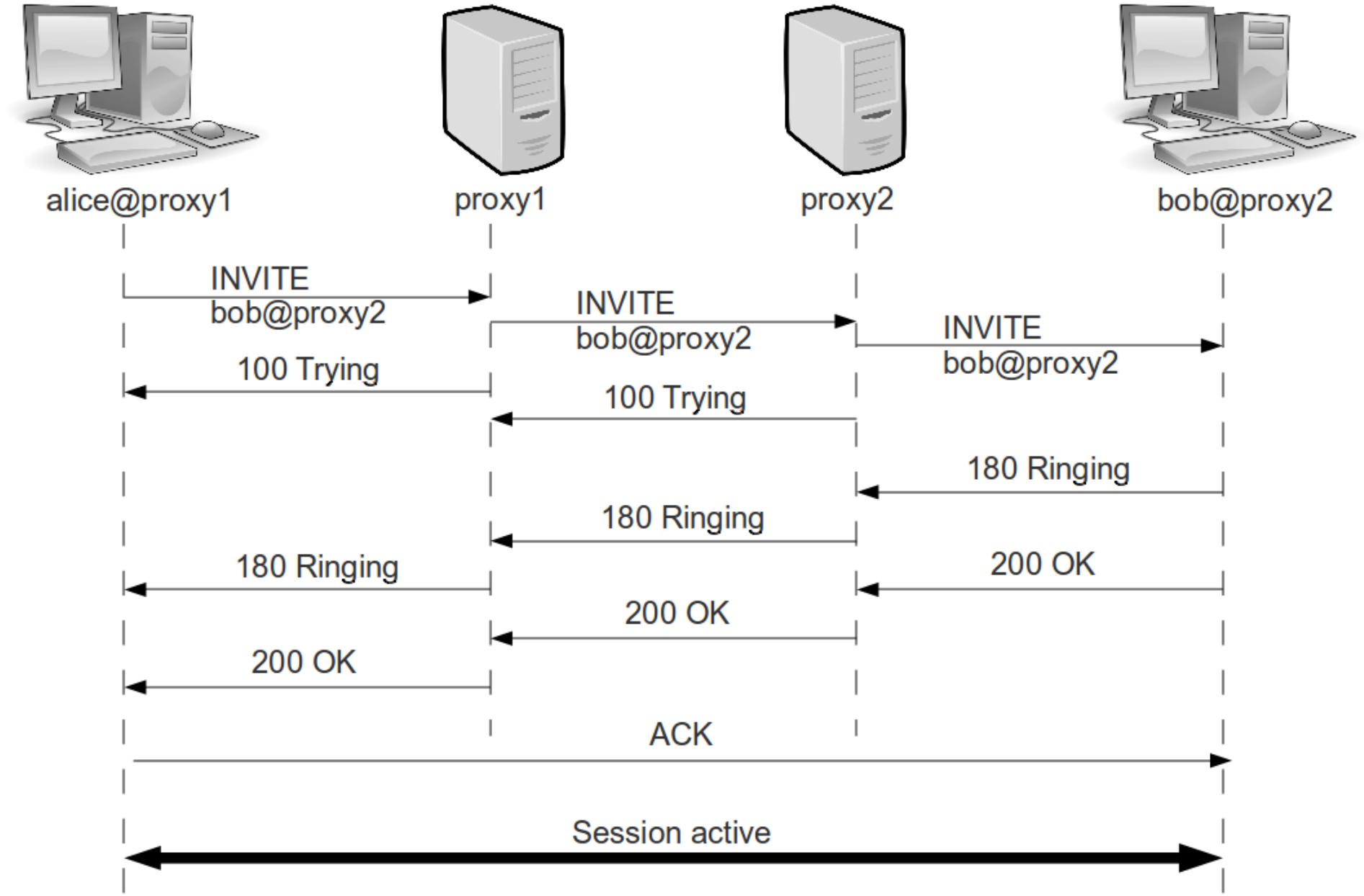
SIP Format

SIP Request Message

```
INVITE sip:happy@193.11.155.123 SIP/2.0
Via: SIP/2.0/UDP 193.11.155.93:5063
To: happy <sip:happy@193.11.155.123>
From: dopey <sip:dopey@193.11.155.93>
Contact: <sip:dopey@193.11.155.93:5061>
Call-ID: 1-3207@127.0.1.1
CSeq: 1 INVITE
Max-Forwards: 70
```

SIP Response Message

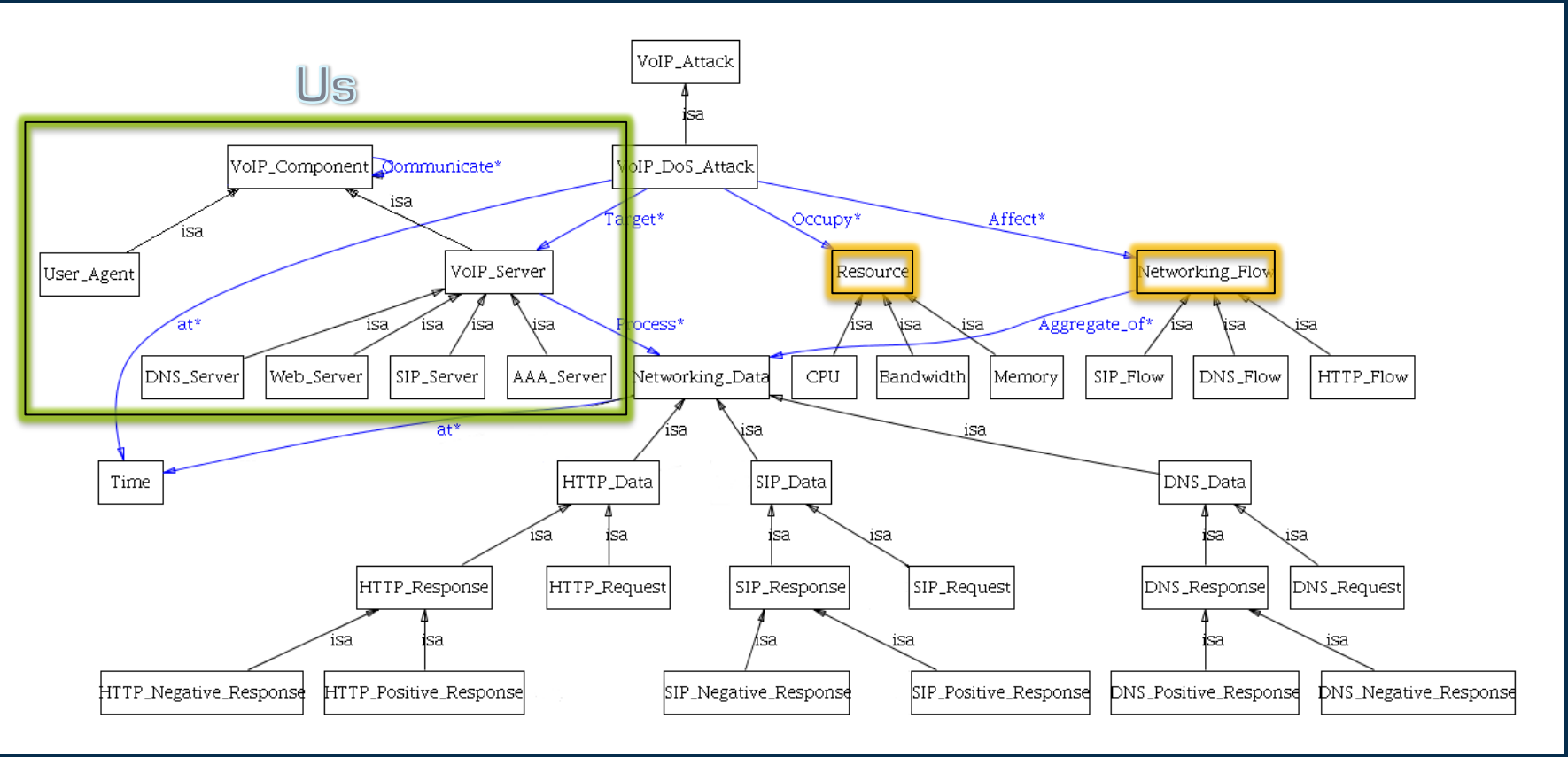
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 193.11.155.93;
     SIP/2.0/UDP 127.0.1.1:5061
From: snowwhite <sip:snowwhite@193.11.155.93:5061>
To: sut <sip:princecharming@193.11.155.123:5060>
Call-ID: 785-3206@127.0.1.1
CSeq: 2 INVITE
Contact: <sip:127.0.1.1:5061;transport=UDP>
```


alice@proxy1
proxy1
proxy2
bob@proxy2
INVITE
bob@proxy2
INVITE
bob@proxy2
INVITE
bob@proxy2
100 Trying
100 Trying
180 Ringing
180 Ringing
180 Ringing
200 OK
200 OK
200 OK
ACK
Session active

DoS Attacks

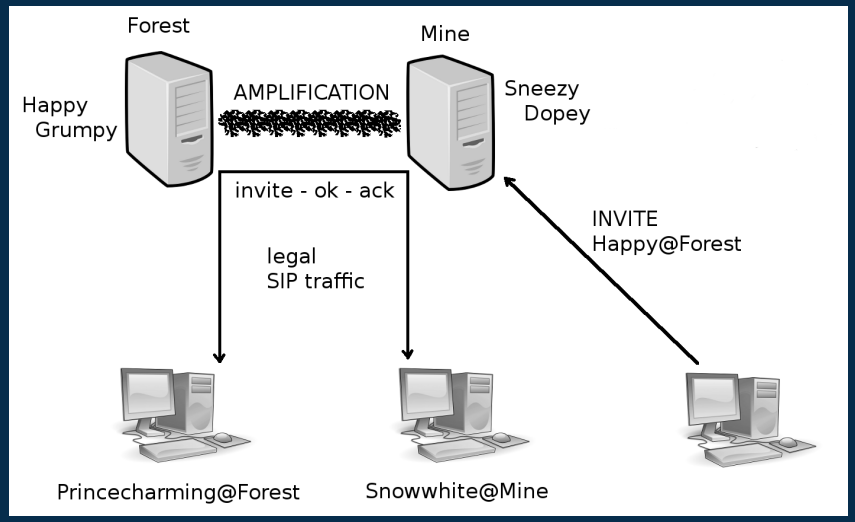
- Web Delay
- DNS Delay
- Malformed Message
- Invite Flood
- Amplification

SIP DoS Attack Ontology

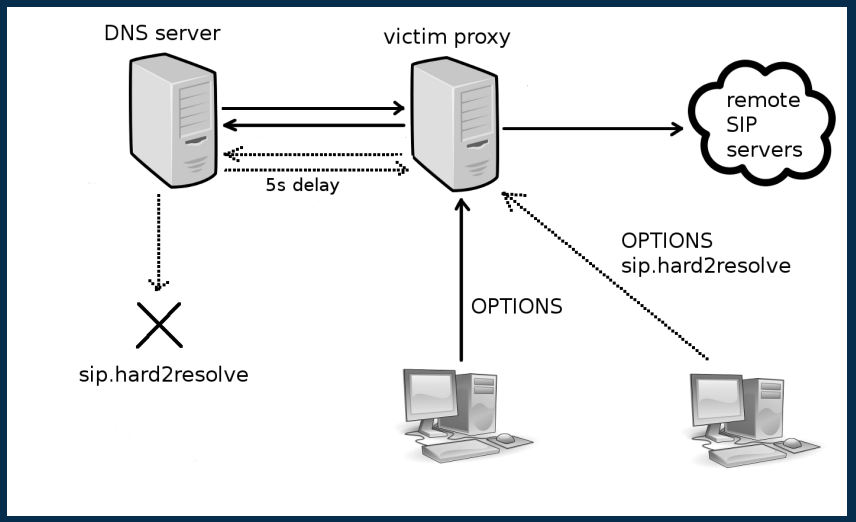


Testbed Setup

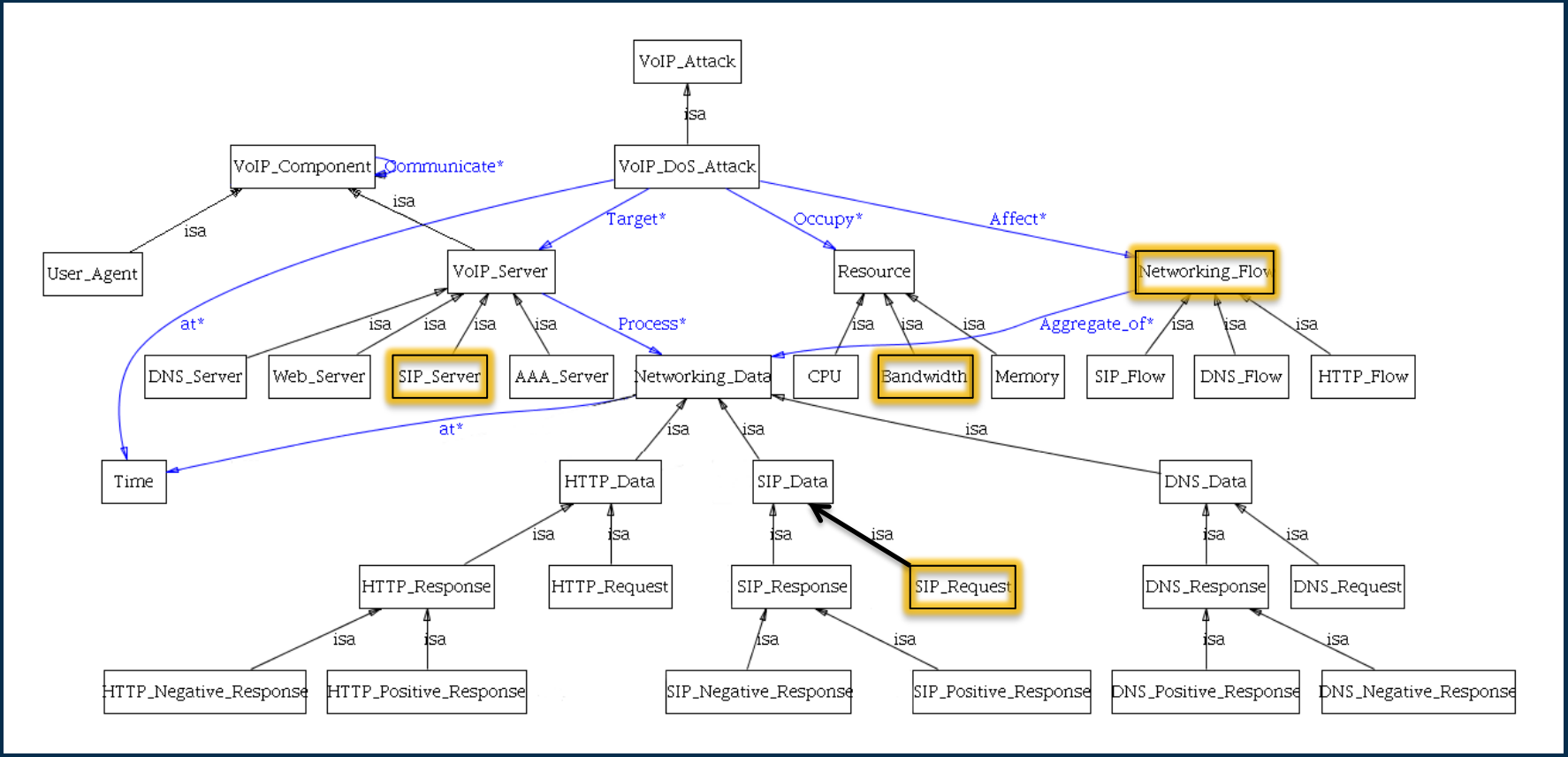
Amp Attack

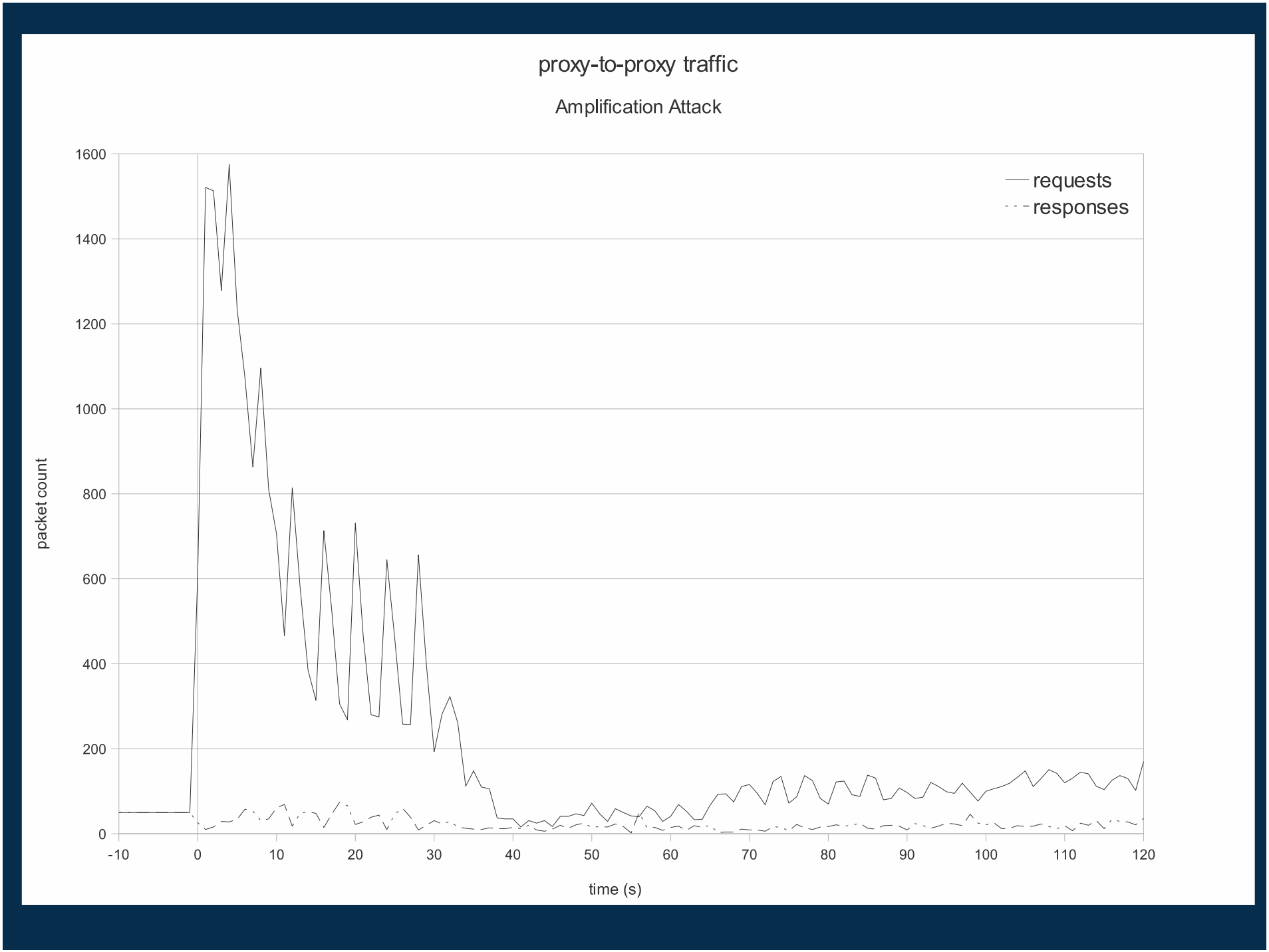


DNS Delay Attack

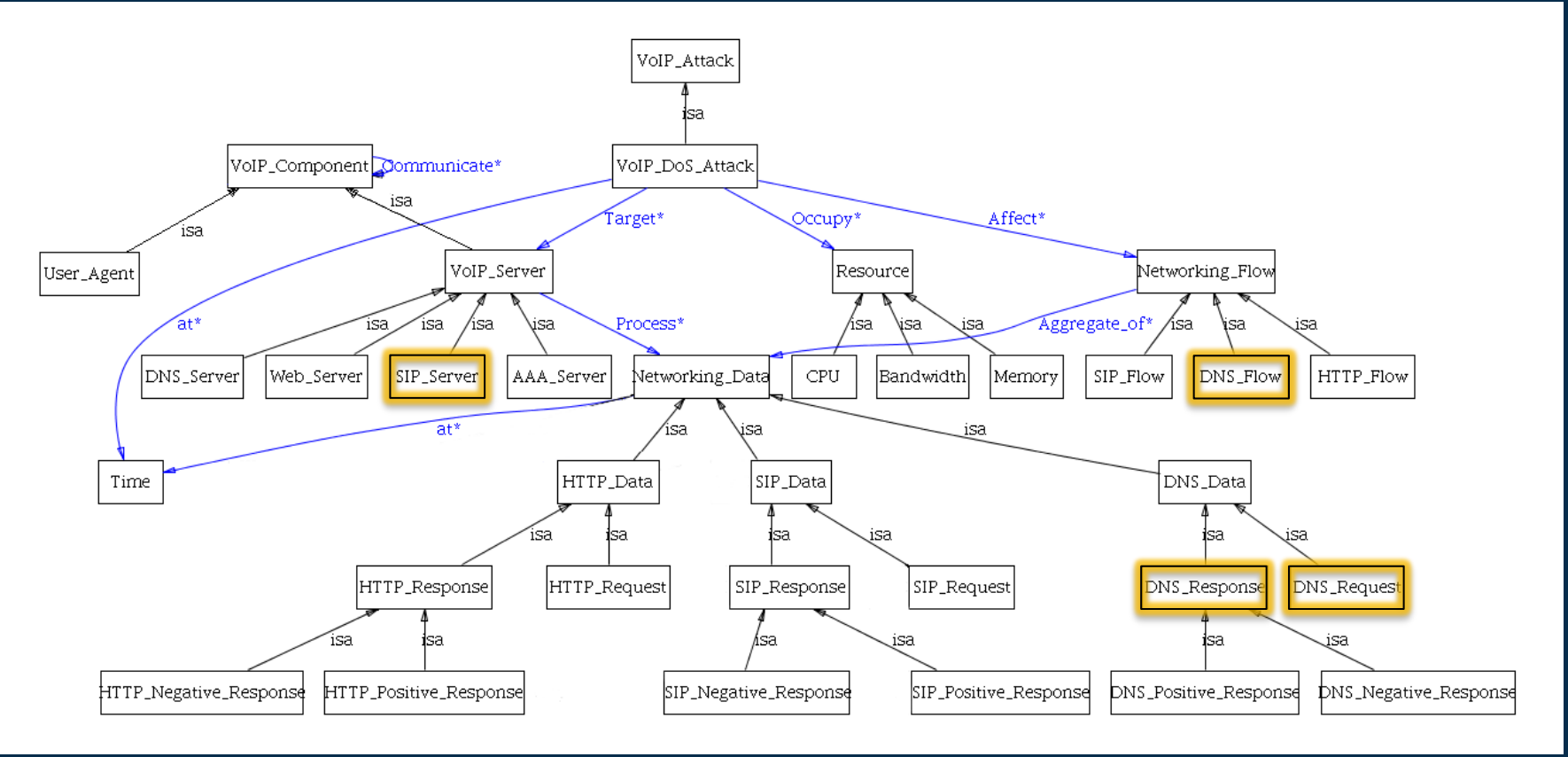


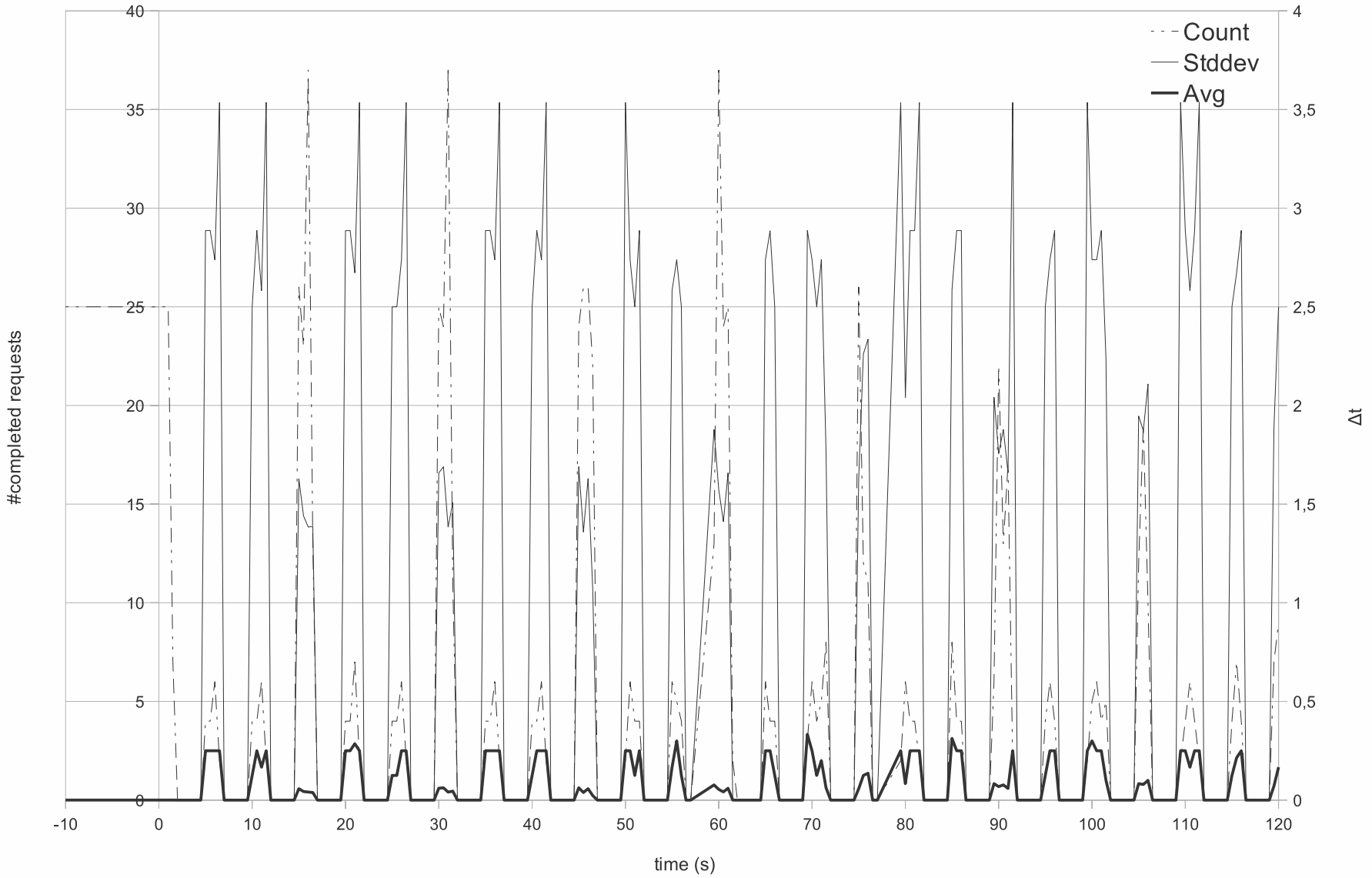
Amplification Attack



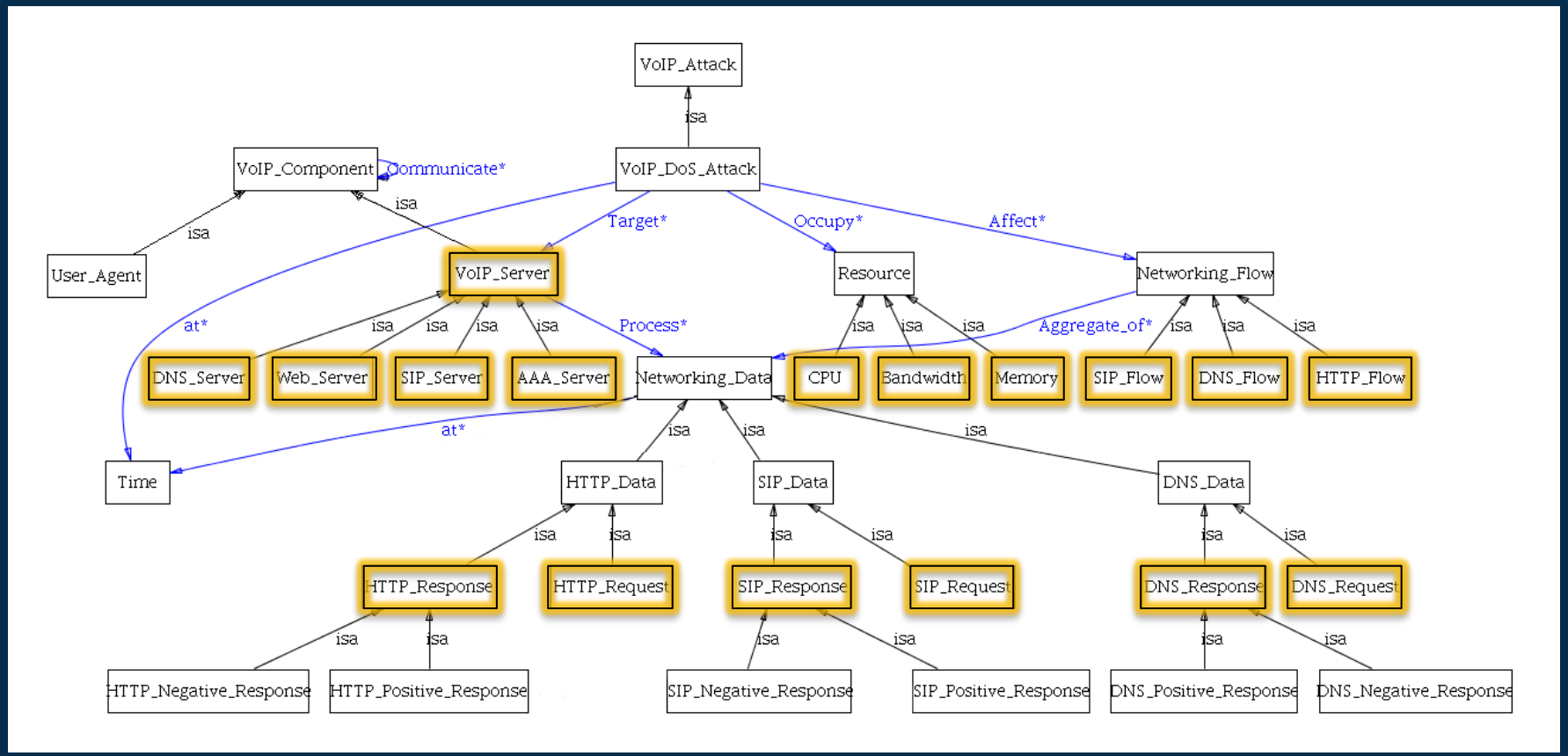

proxy-to-proxy traffic
Amplification Attack
requests
responses
packet count
time (s)
1600
1400
1200
1000
800
600
400
200
0
-10
0
10
20
30
40
50
60
70
80
90
100
110
120

DNS Delay Attack




DNS Response Graph
5 hard2resolve requests/s
Count
Stddev
Avg
#completed requests
Δt
time (s)
40
35
30
25
20
15
10
5
0
4
3,5
3
2,5
2
1,5
1
0,5
0
-10
0
10
20
30
40
50
60
70
80
90
100
110
120

Malformed Message Attack?
Invite flood attack a subset?



Conclusions

- Once we have an ontology, it is easier to distinguish between DoS Attacks, but…
- Creating an ontology that properly captures the attack can be difficult without distinguishing characteristics
- Sometimes, different attacks look very similar without deep packet inspection.