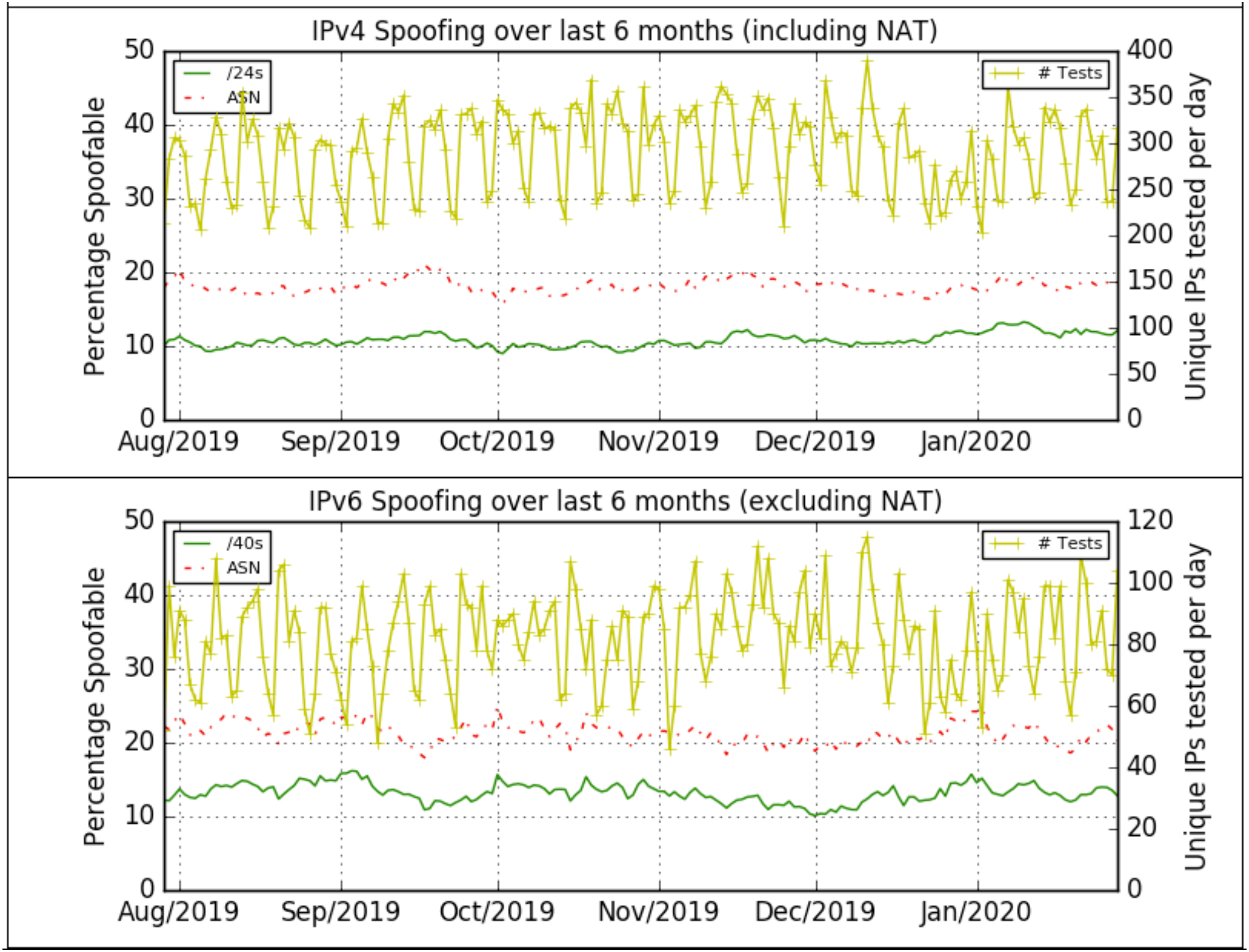
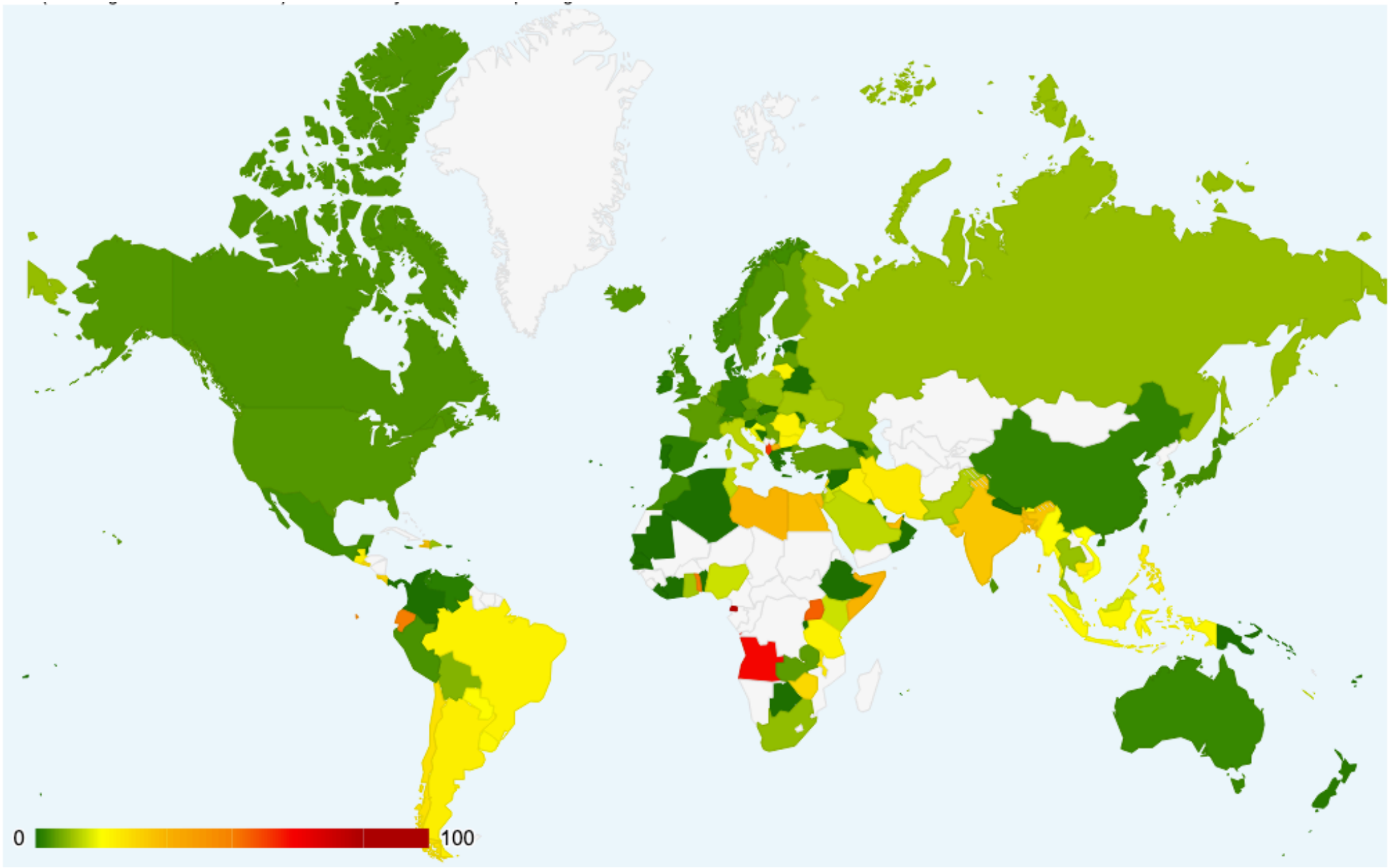
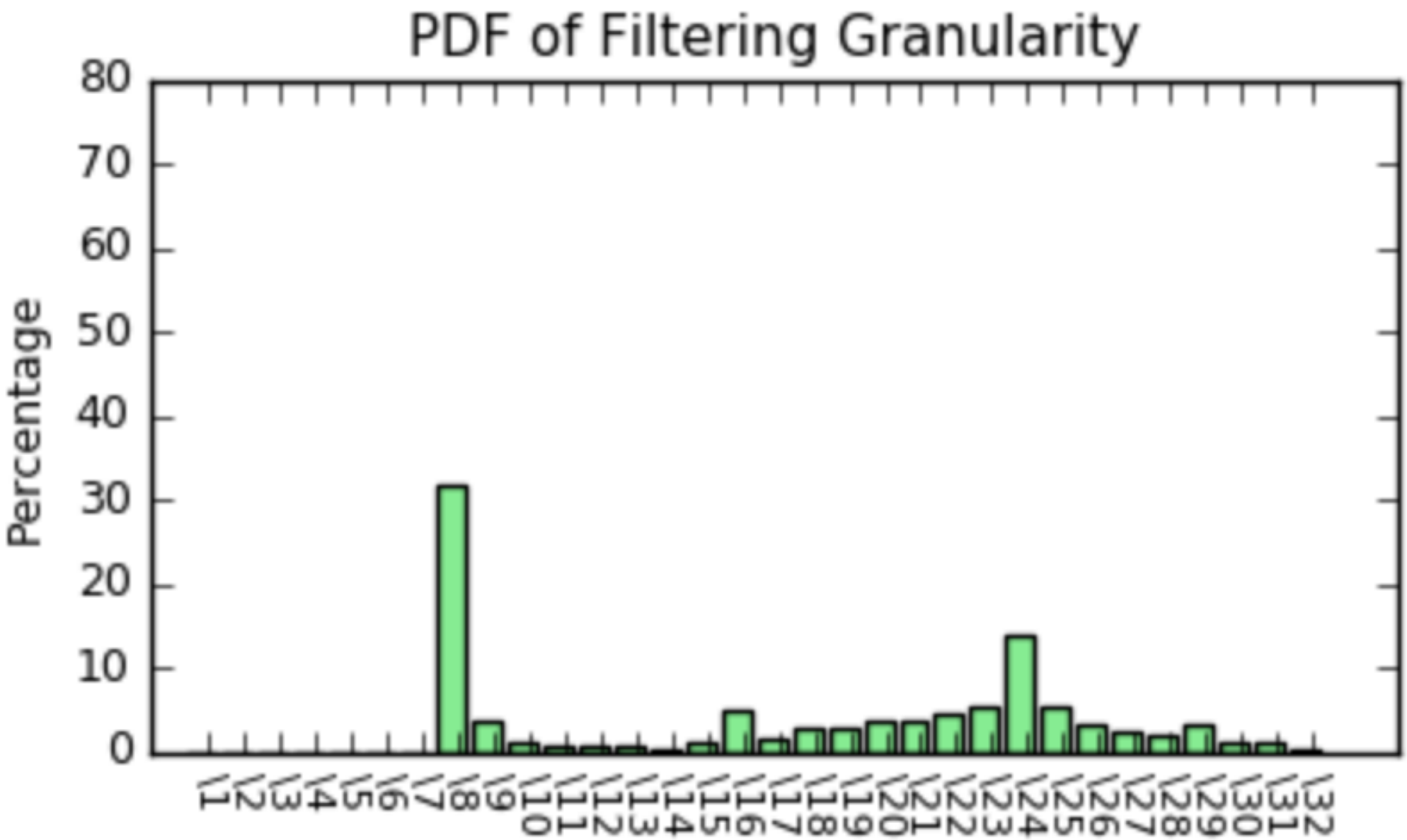
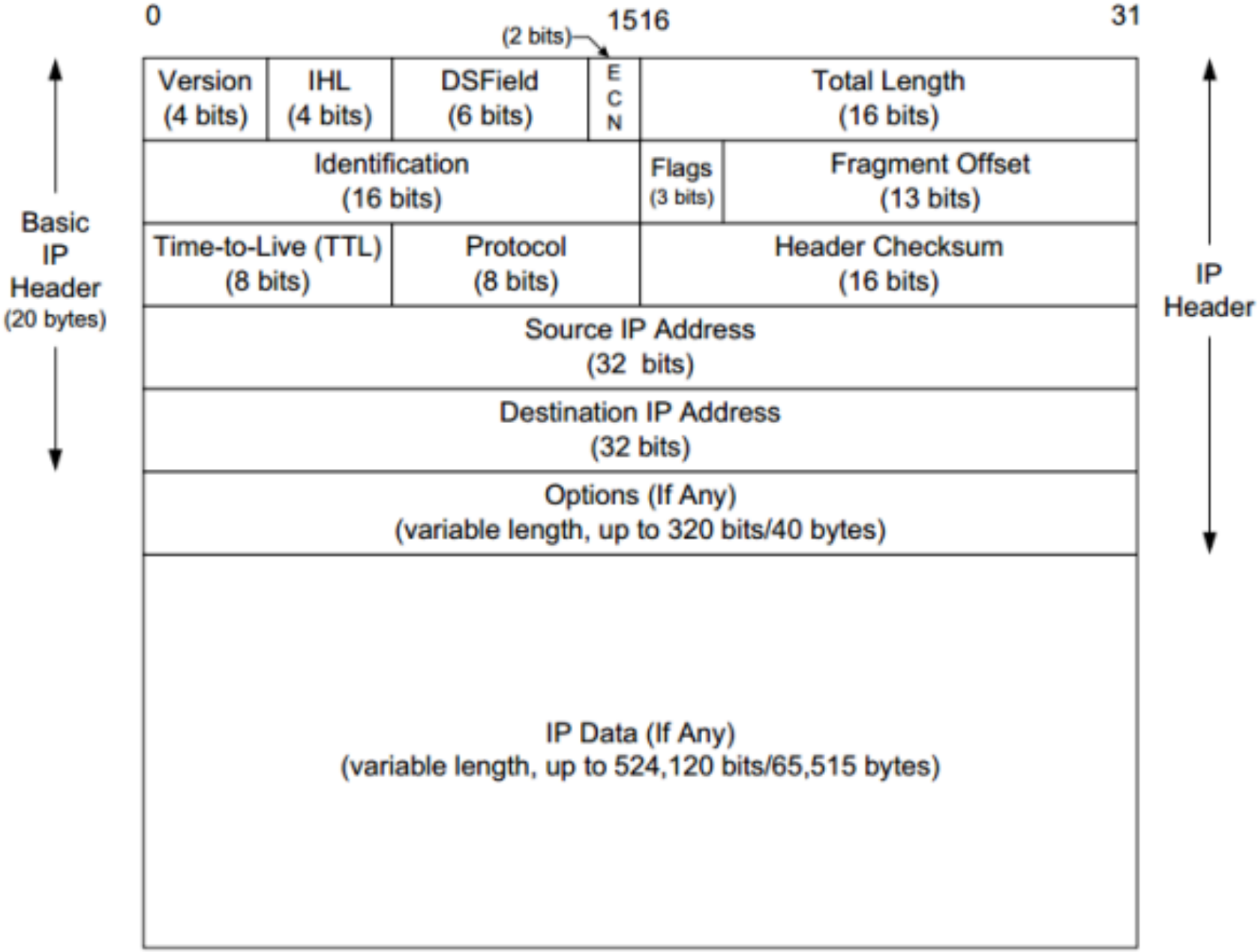
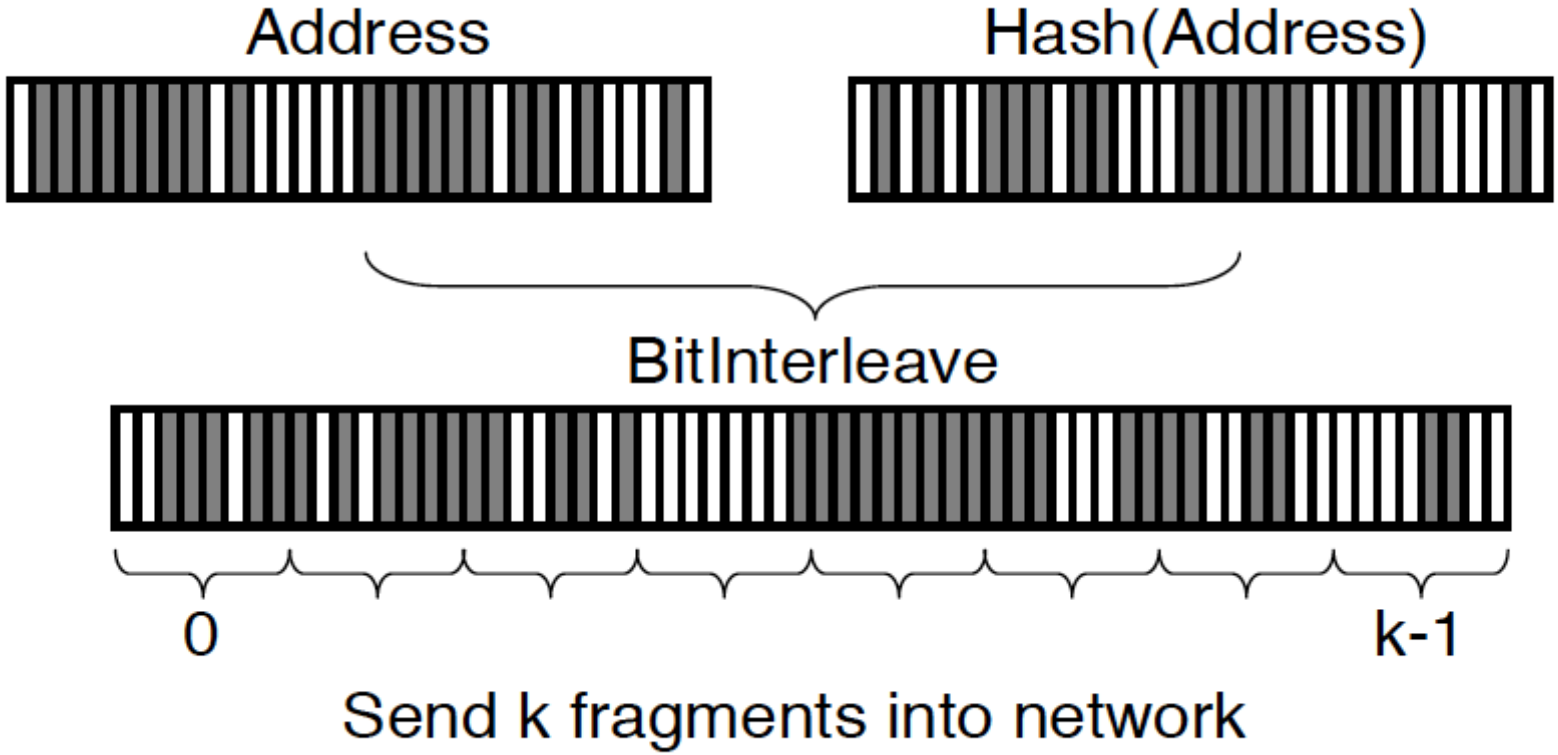

IPv4 Spoofing over last 6 months (including NAT)
Percentage Spoofable
Unique IPs tested per day
/24s
ASN
Tests
0
10
20
30
40
50
0
50
100
150
200
250
300
350
400
Aug/2019
Sep/2019
Oct/2019
Nov/2019
Dec/2019
Jan/2020
IPv6 Spoofing over last 6 months (excluding NAT)
Percentage Spoofable
Unique IPs tested per day
/40s
ASN
Tests
0
10
20
30
40
50
0
20
40
60
80
100
120
Aug/2019
Sep/2019
Oct/2019
Nov/2019
Dec/2019
Jan/2020

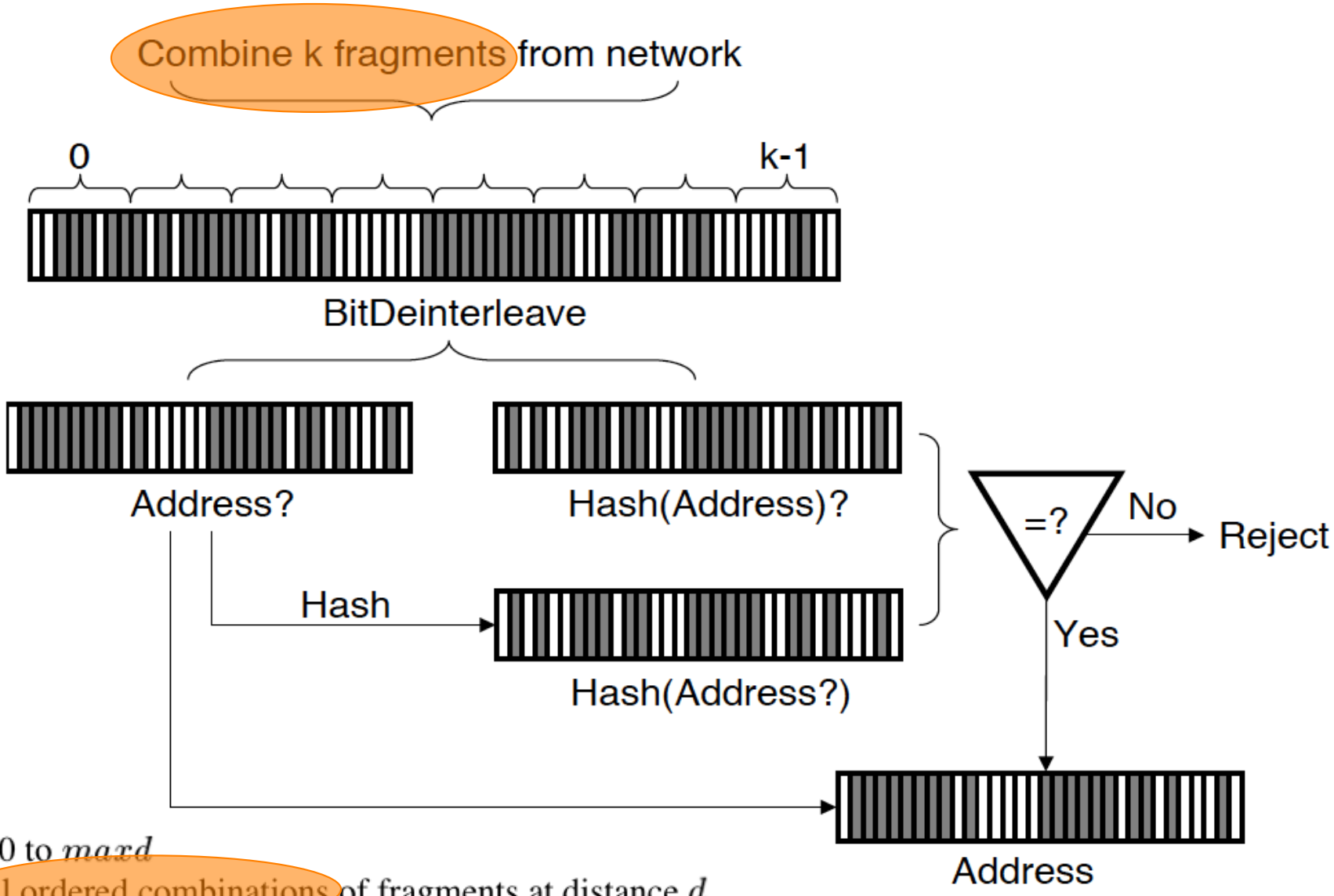

0
100


PDF of Filtering Granularity
Percentage
80
70
60
50
40
30
20
10
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

We define the *approximate traceback* problem as finding a candidate attack path for each attacker that contains the true attack path as a suffix. We call this the *valid suffix* of the candidate path.


0
15
16
31
(2 bits)
Version (4 bits)
IHL (4 bits)
DSField (6 bits)
ECN
Total Length (16 bits)
Identification (16 bits)
Flags (3 bits)
Fragment Offset (13 bits)
Time-to-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)
Options (If Any) (variable length, up to 320 bits/40 bytes)
IP Data (If Any) (variable length, up to 524,120 bits/65,515 bytes)
Basic IP Header (20 bytes)
IP Header


Address
Hash(Address)
BitInterleave
0
k-1
Send k fragments into network




```
for d := 0 to maxd
    for all ordered combinations of fragments at distance d
        construct edge z
        if d ≠ 0 then
            z := z ⊕ last
        if Hash(EvenBits(z)) = OddBits(z) then
            insert edge (z,EvenBits(z),d) into G
            last := EvenBits(z);
```

	Management overhead	Network overhead	Router overhead	Distributed capability	Post-mortem capability	Preventative/ reactive
Ingress filtering	Moderate	Low	Moderate	N/A	N/A	Preventative
Link testing						
Input debugging	High	Low	High	Good	Poor	Reactive
Controlled flooding	Low	High	Low	Poor	Poor	Reactive
Logging	High	Low	High	Excellent	Excellent	Reactive
ICMP Traceback	Low	Low	Low	Good	Excellent	Reactive
Marking	Low	Low	Low	Good	Excellent	Reactive

Table 1: Qualitative comparison of existing schemes for combating anonymous attacks and the probabilistic marking approach we propose.