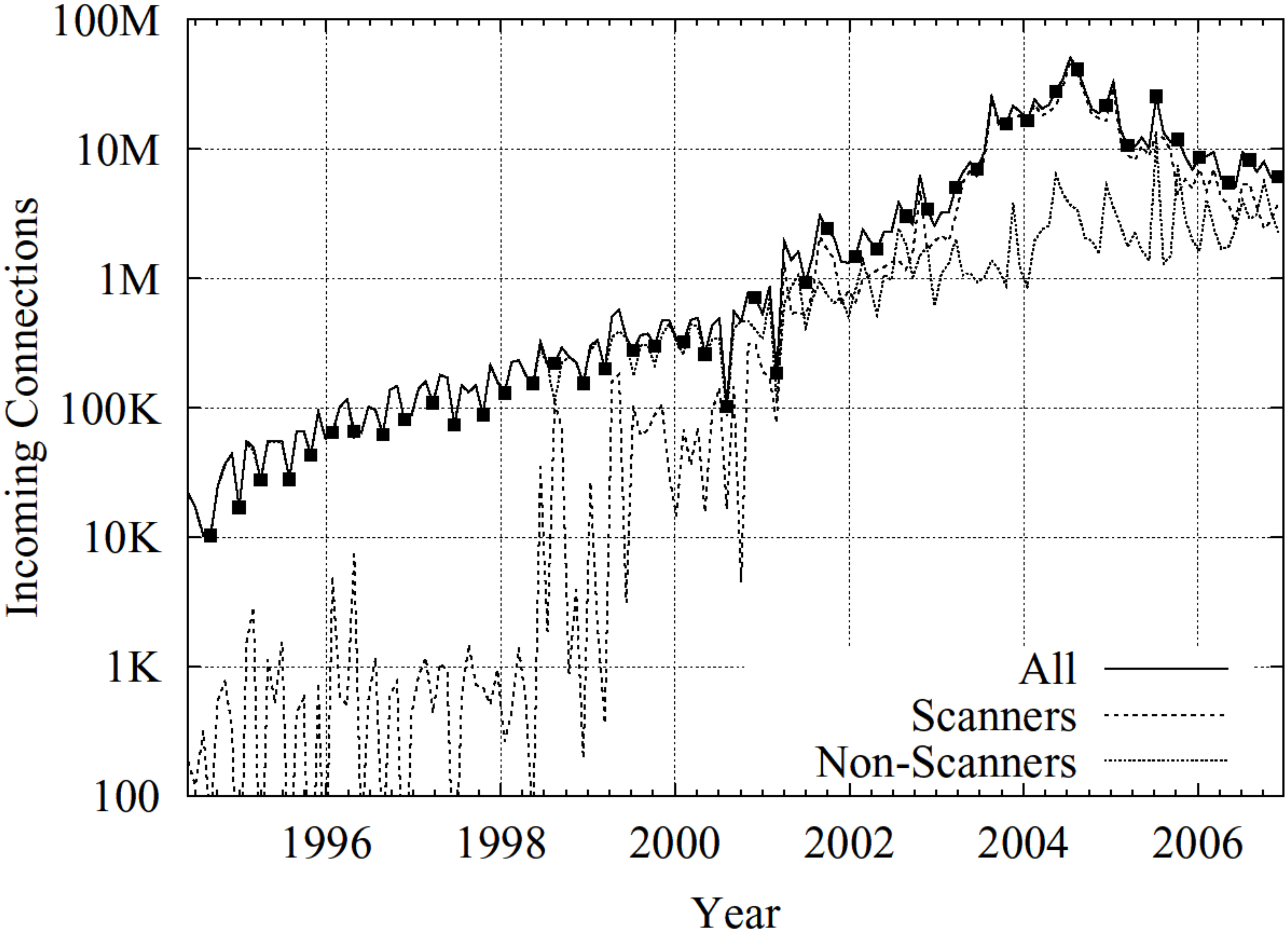
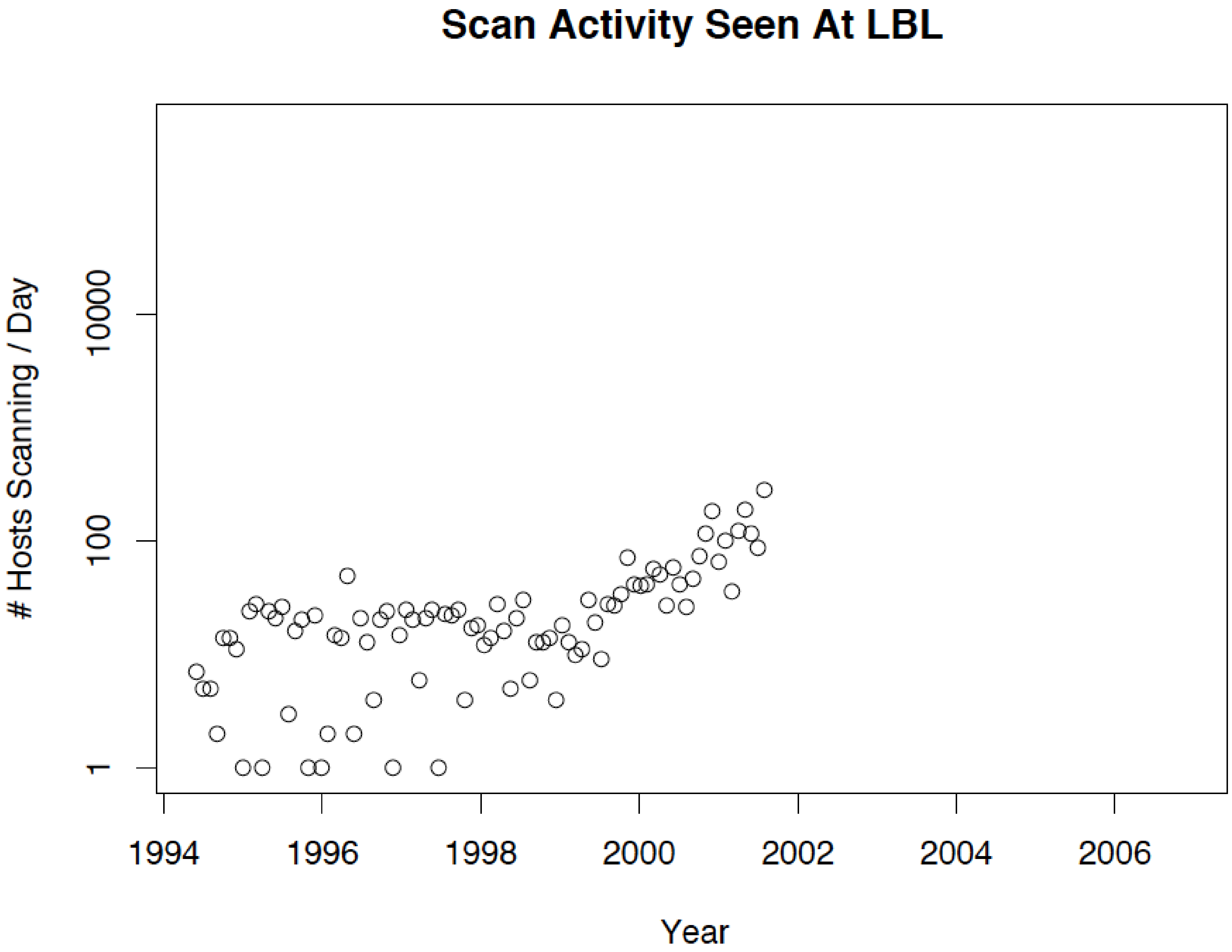
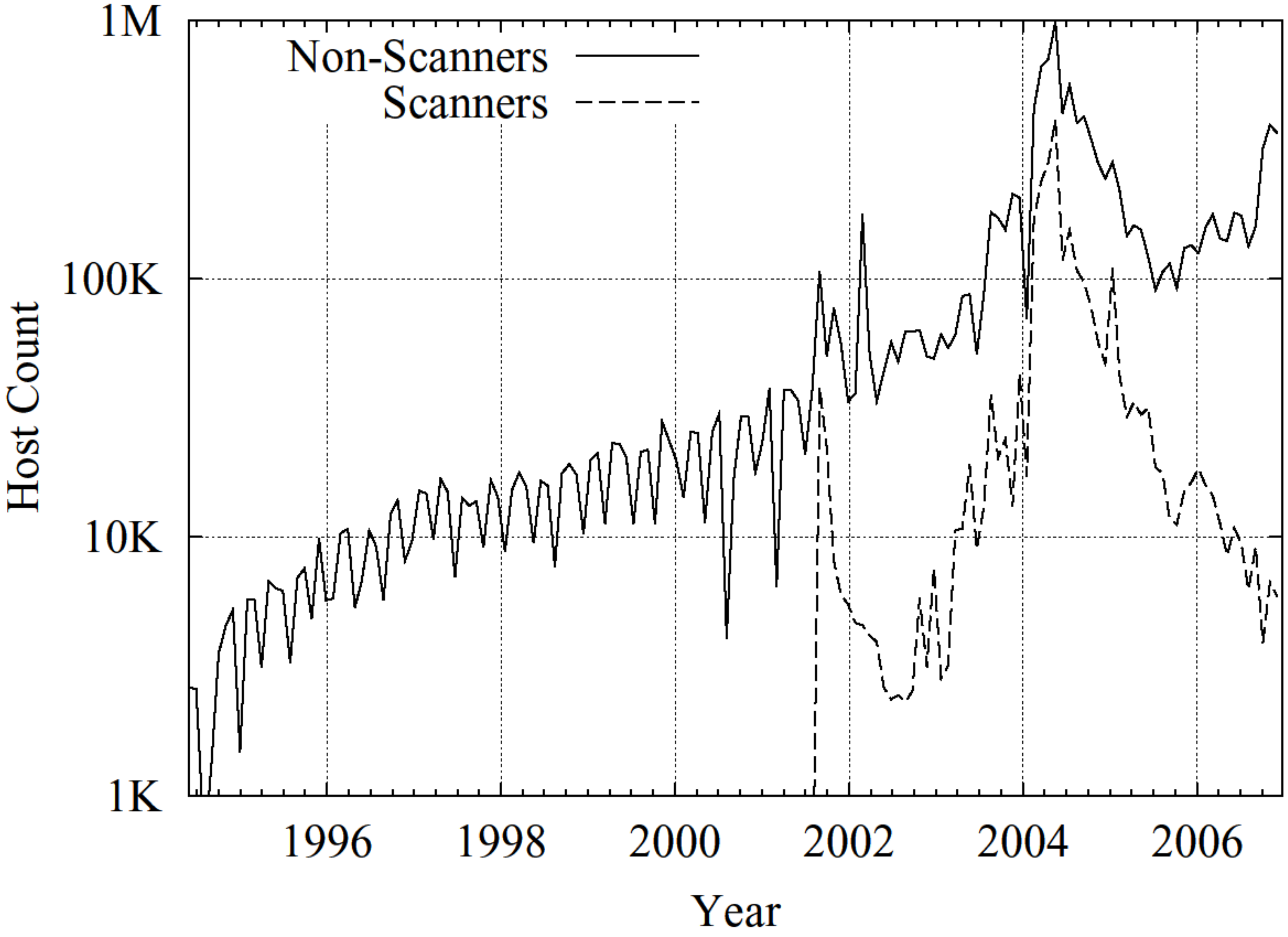
Scanning Activity Seen @ LBNL

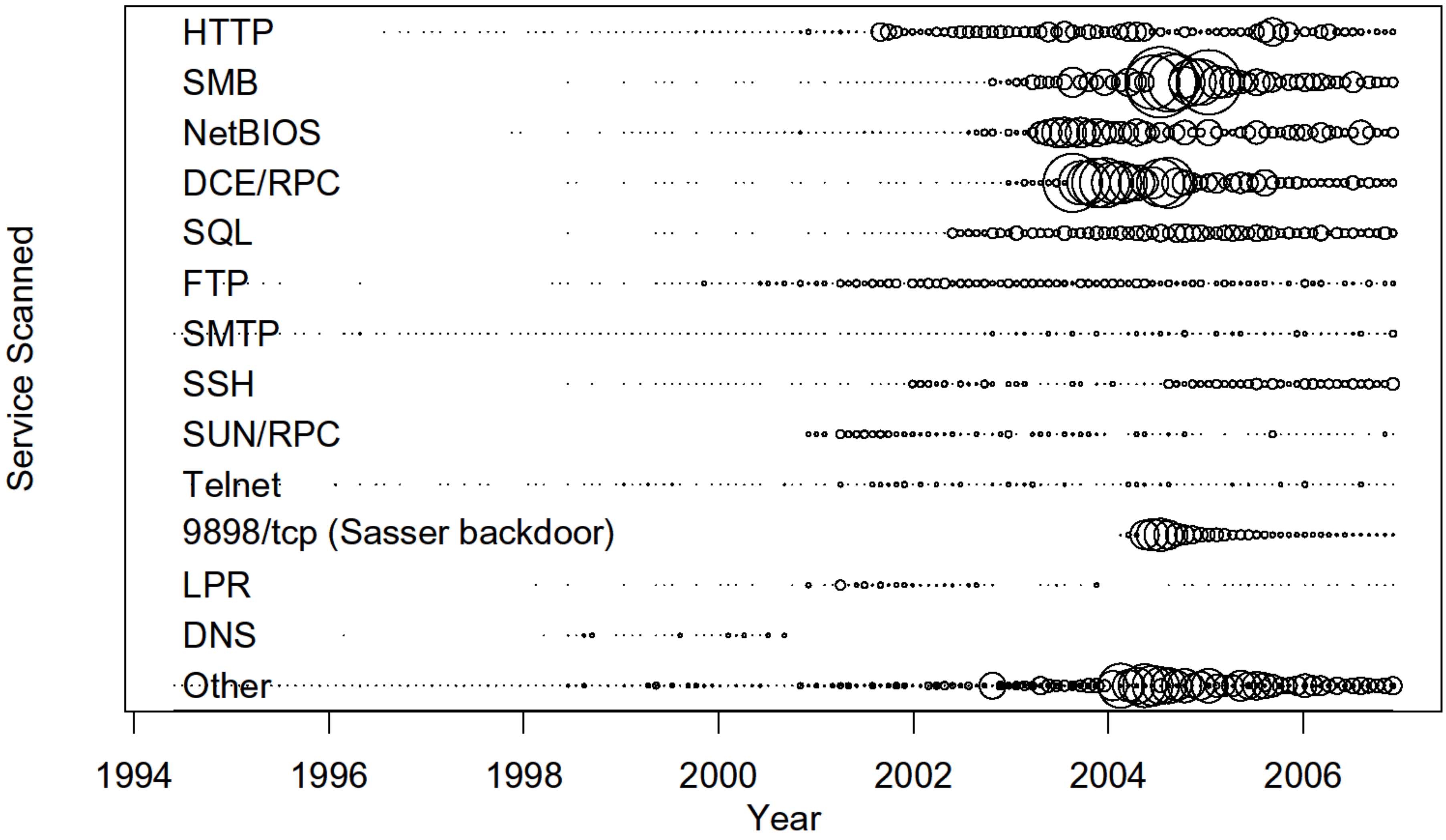


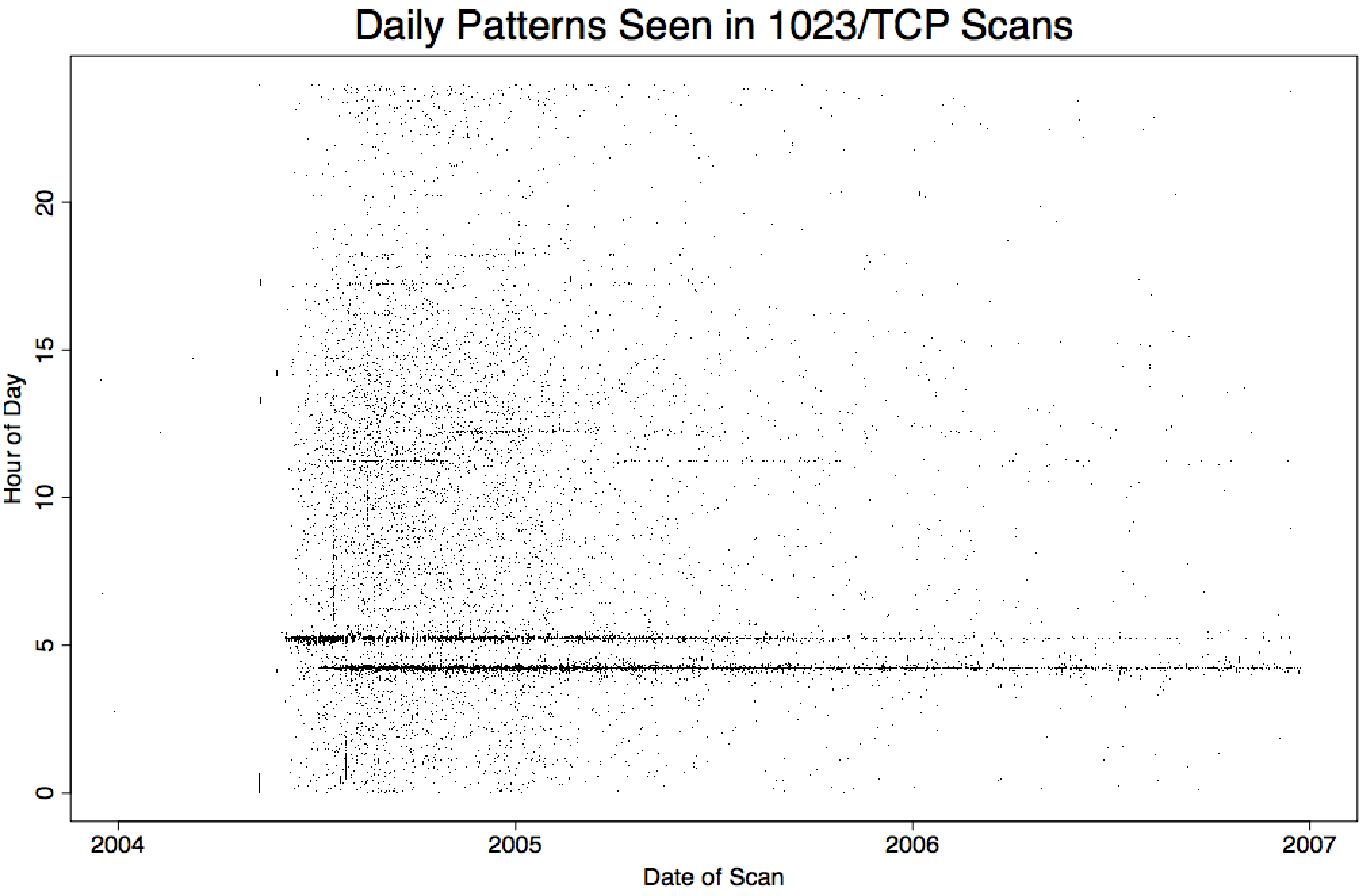

Scan Activity Seen At LBL
# Hosts Scanning / Day
10000
100
1
1994
1996
1998
2000
2002
2004
2006
Year

Scanning Hosts Seen @ LBNL



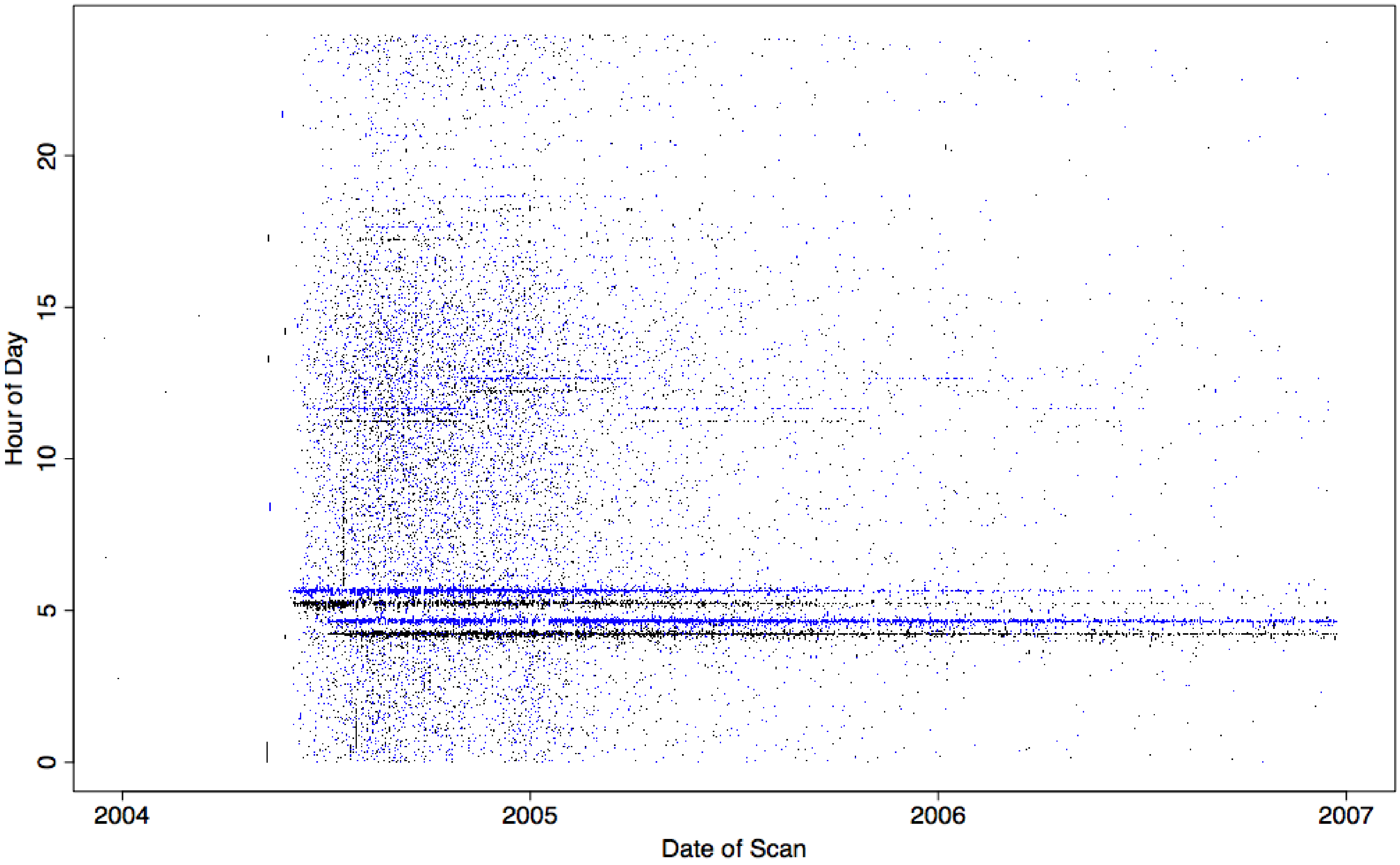
Services Scanned Over Time





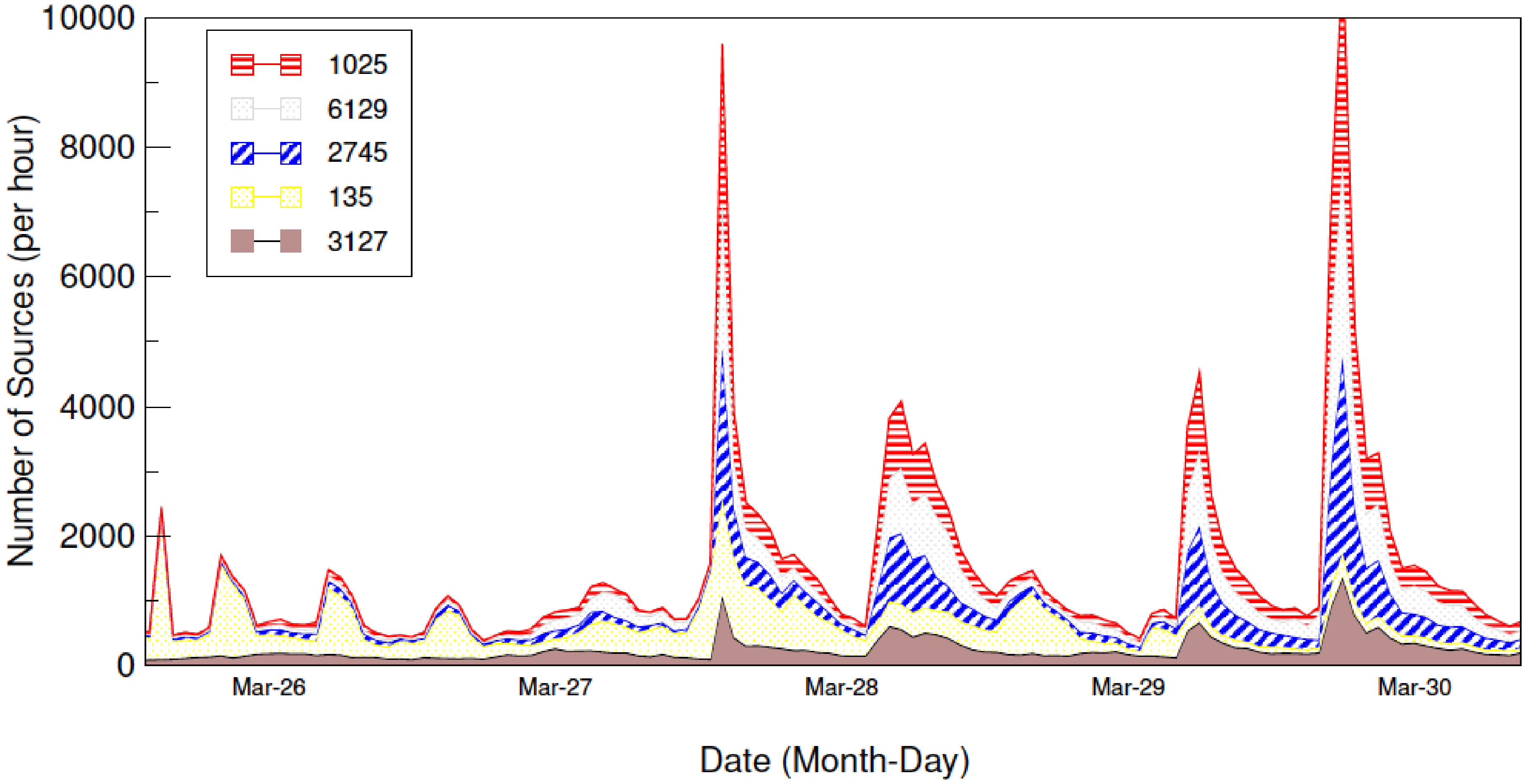
/16 at LBL, sampled 1-in-1K

Daily Patterns Seen in 1023/TCP Scans

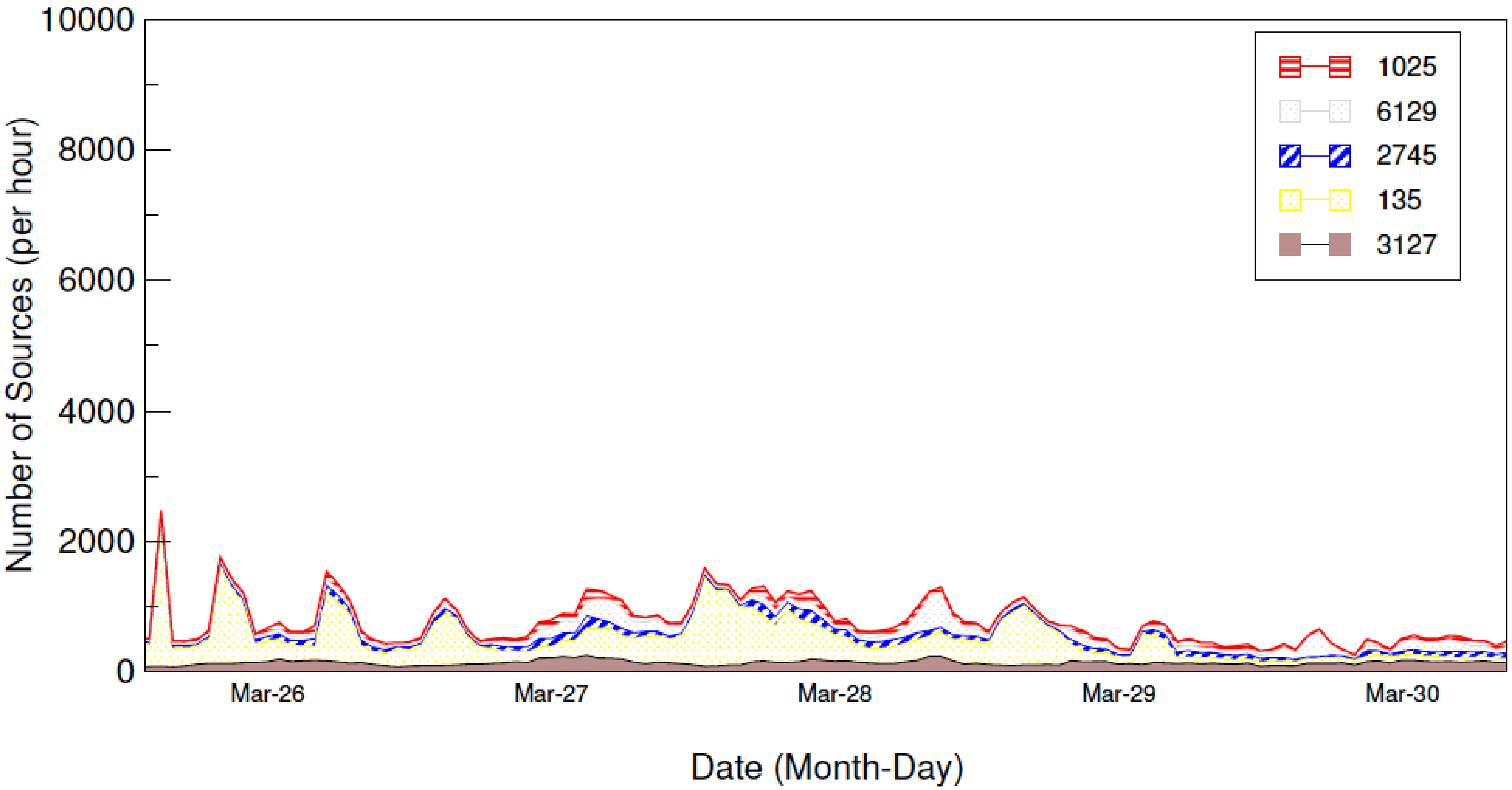


/16 at LBL, sampled 1-in-1K

2nd /16, sampled 1-in-1K

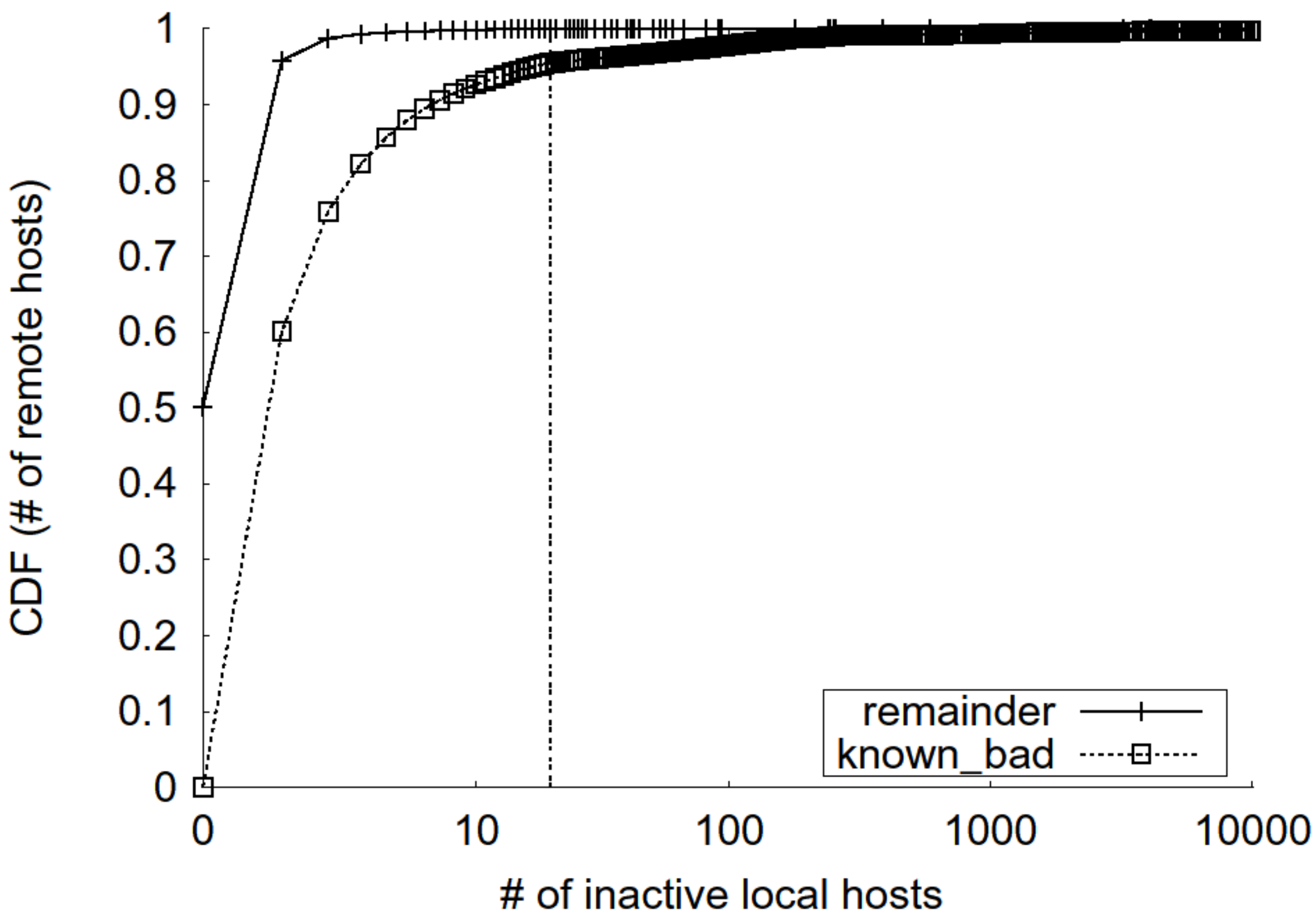


(a) Agobot Sources: UW I



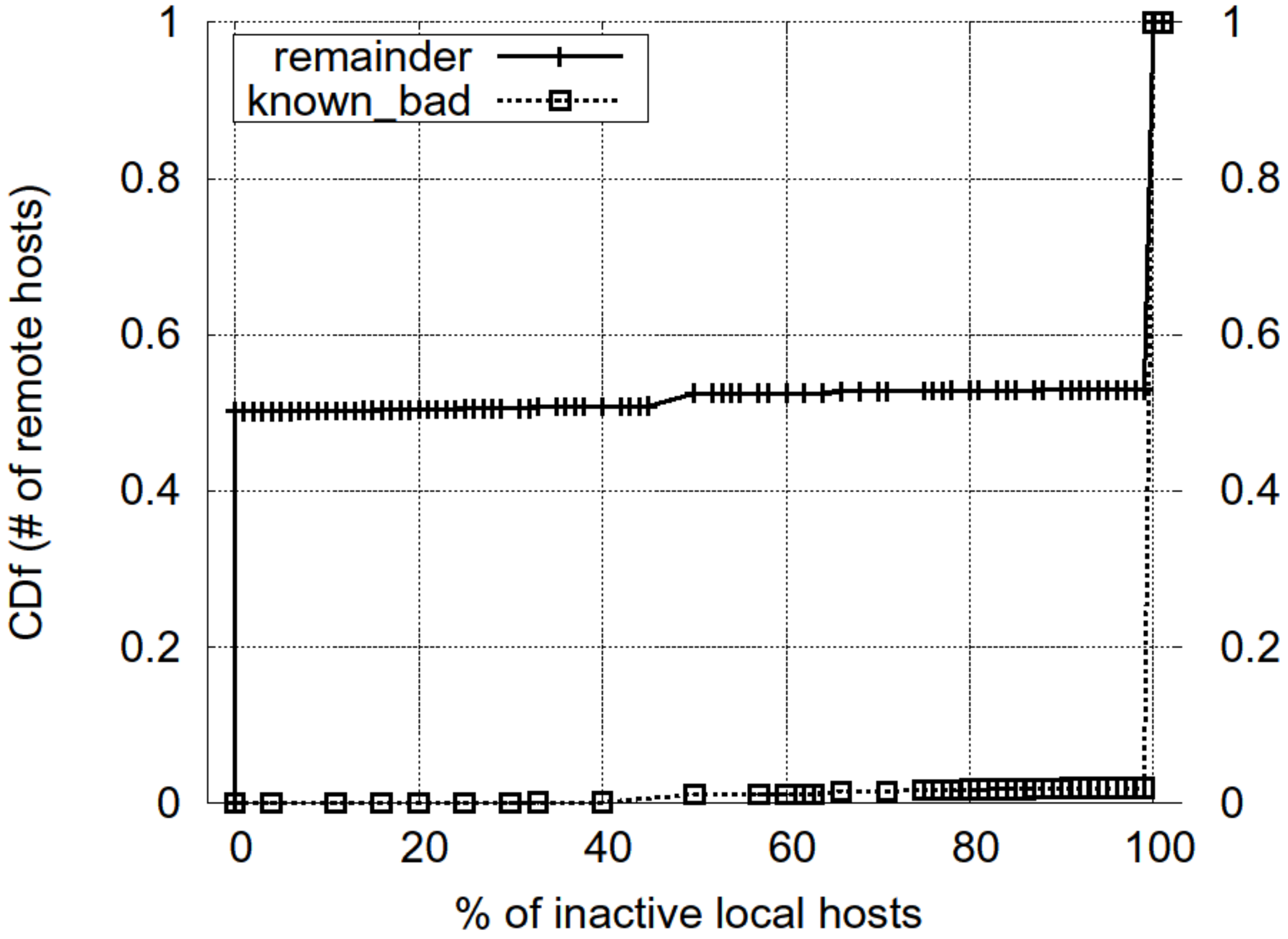
(b) Agobot Sources: UW II

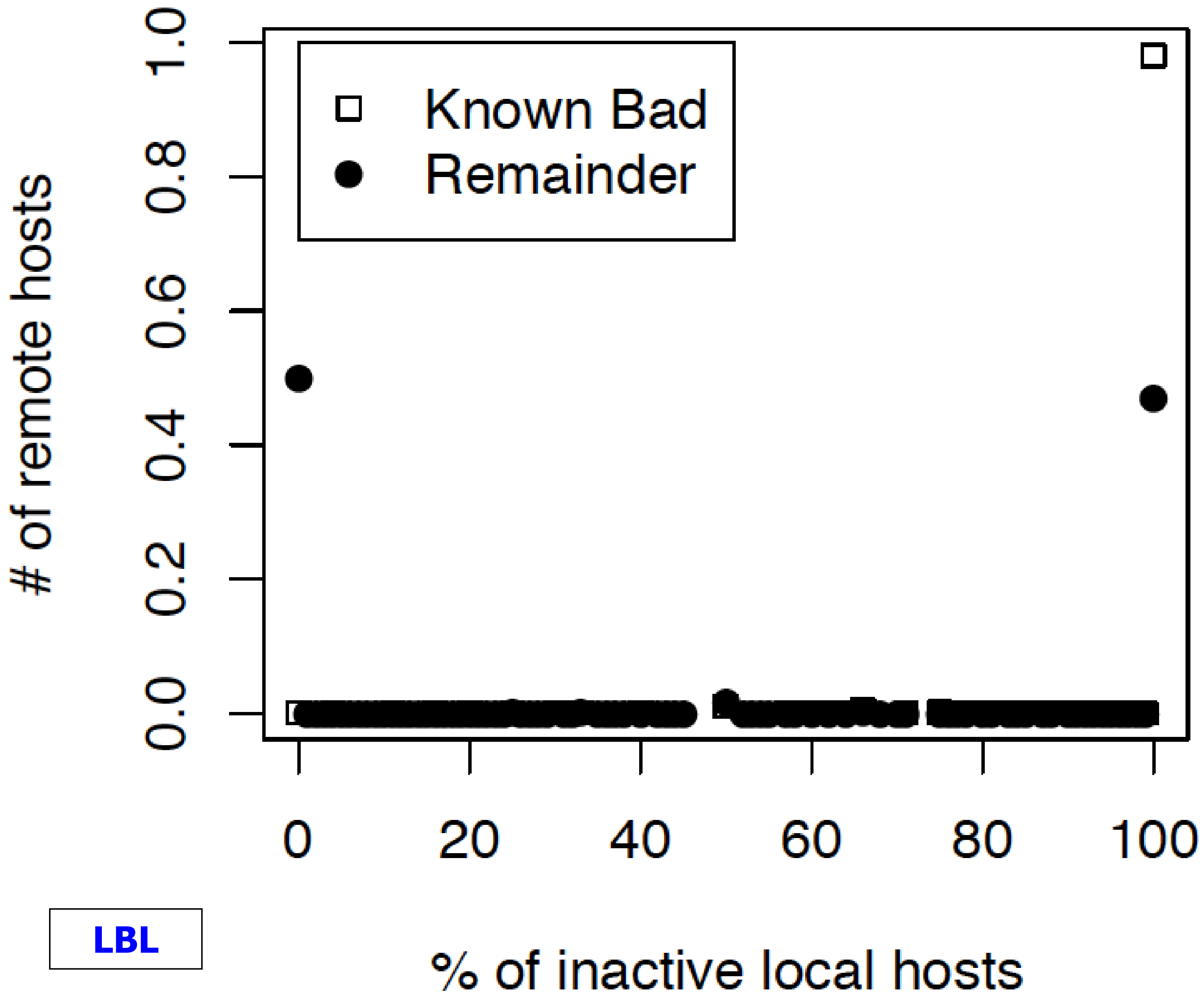
# Failed Conn's Not Enough Info



(a) LBL

Failure *Ratio* Much More Distinctive



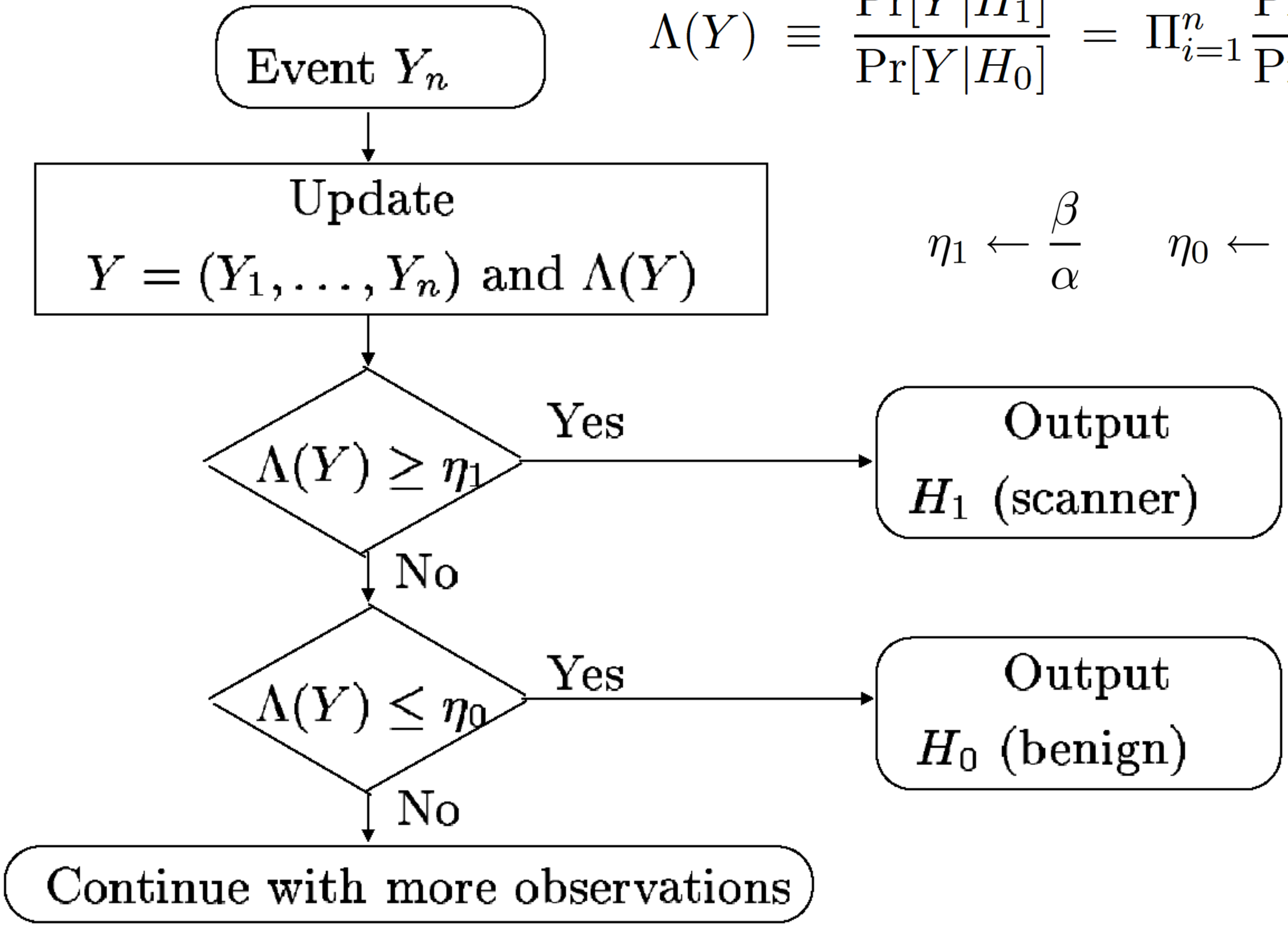


Known Bad
Remainder
# of remote hosts
0.0
0.2
0.4
0.6
0.8
1.0
0
20
40
60
80
100
% of inactive local hosts
LBL

Real-Time Detection

$$\Lambda(Y) \equiv \frac{\Pr[Y|H_1]}{\Pr[Y|H_0]} = \Pi_{i=1}^{n} \frac{\Pr[Y_i|H_1]}{\Pr[Y_i|H_0]}$$

$$\eta_1 \leftarrow \frac{\beta}{\alpha} \qquad \eta_0 \leftarrow \frac{1-\beta}{1-\alpha}$$



Event Y_n

Update

$Y = (Y_1, \ldots, Y_n)$ and $\Lambda(Y)$

$\Lambda(Y) \geq \eta_1$

Yes

Output

H_1 (scanner)

No

$\Lambda(Y) \leq \eta_0$

Yes

Output

H_0 (benign)

No

Continue with more observations

Expected Time Until Decision

$$E[N|H_0] = \frac{\alpha \ln \frac{\beta}{\alpha} + (1-\alpha) \ln \frac{1-\beta}{1-\alpha}}{\theta_0 \ln \frac{\theta_1}{\theta_0} + (1-\theta_0) \ln \frac{1-\theta_1}{1-\theta_0}},$$

$$E[N|H_1] = \frac{\beta \ln \frac{\beta}{\alpha} + (1-\beta) \ln \frac{1-\beta}{1-\alpha}}{\theta_1 \ln \frac{\theta_1}{\theta_0} + (1-\theta_1) \ln \frac{1-\theta_1}{1-\theta_0}}.$$