On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack

IEEE INFOCOM 2001

Kihong Park, Heejo Lee

Outline

- What is Denial of Service Attack?
- What is IP Traceback?
- Related Work
- New Contribution
- PPM and Traceback
- Analysis of Single-source DoS Attack
- Distributed DoS Attack
- Conclusion

What is Denial of Service Attack?

- The attacks used several techniques to crash, hang up, or overwhelm servers with malformed packets or large volumes of traffic.

What is IP Traceback?

- Identified the machines that directly generate attack traffic and the network path this traffic subsequently follows.

Related Work

- IP Traceback Scheme:
  - Ingress Filtering
  - Link Testing
  - Logging
  - ICMP Traceback
  - PPM(Probabilistic Packet Marking)

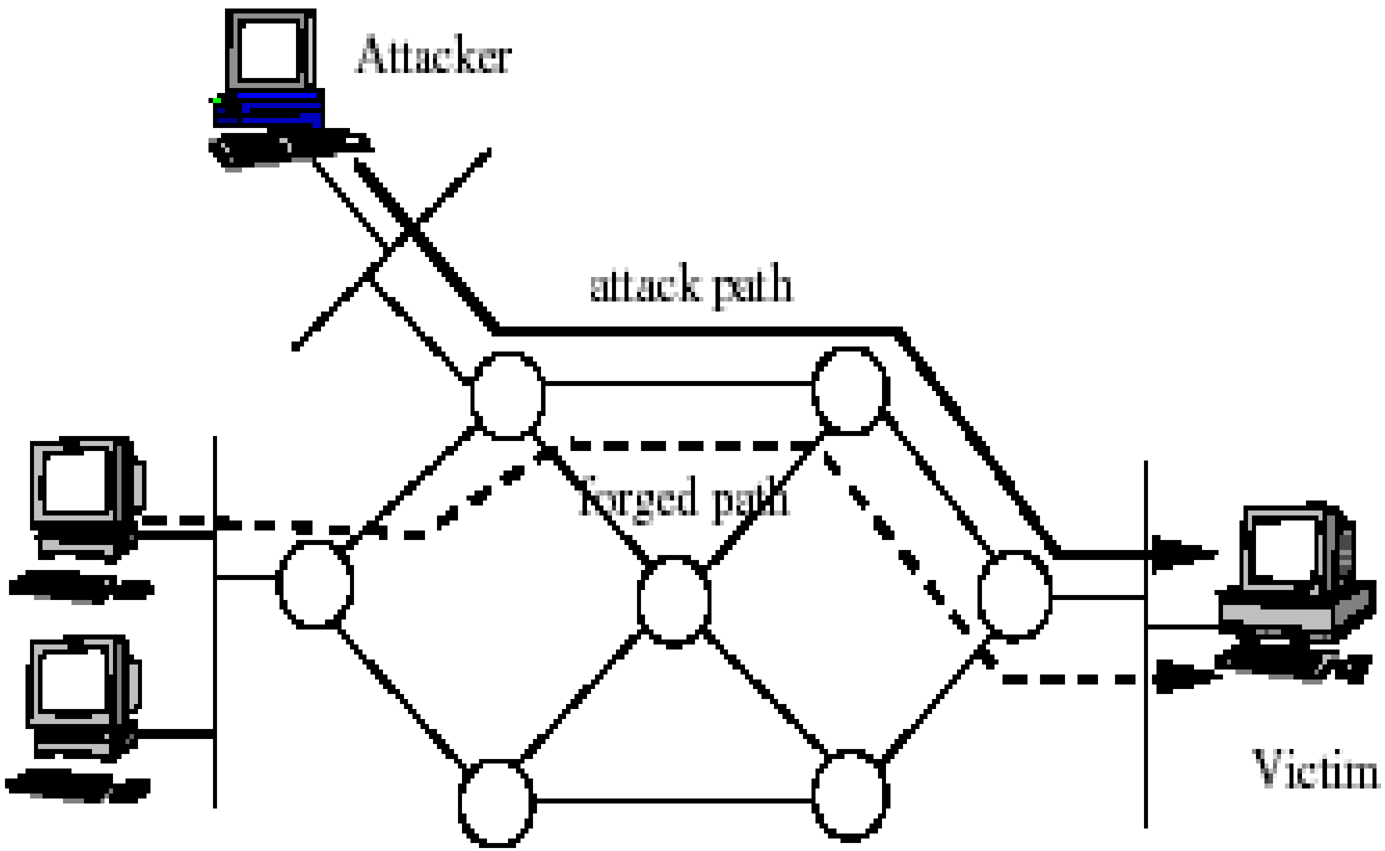
New Contributions

- This paper analyze the effectiveness of probabilistic packet marking for IP traceback under DoS attack

PPM and Traceback

- Network Model
  - Directed graph G = (V,E)
    - V : the set of nodes
    - E : the set of edges
    - S : attackers
    - t : victim (V\S)
  - Attack path
    - A = (s,v1,v2,…,vd,t)

Attack Path and Forgeable Path



Probabilistic Marking

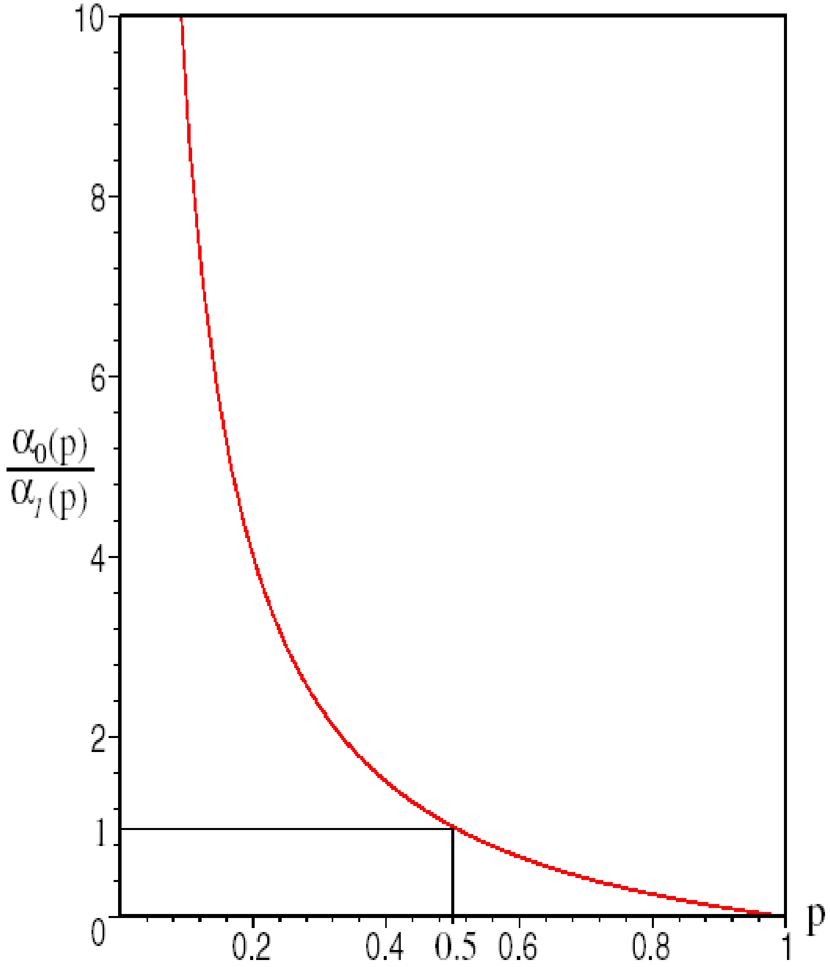
- Definition
- Path Sampling

$$\alpha_i(p) = \Pr\{x_d = (v_{i-1}, v_i)\} = p(1-p)^{d-i}.$$

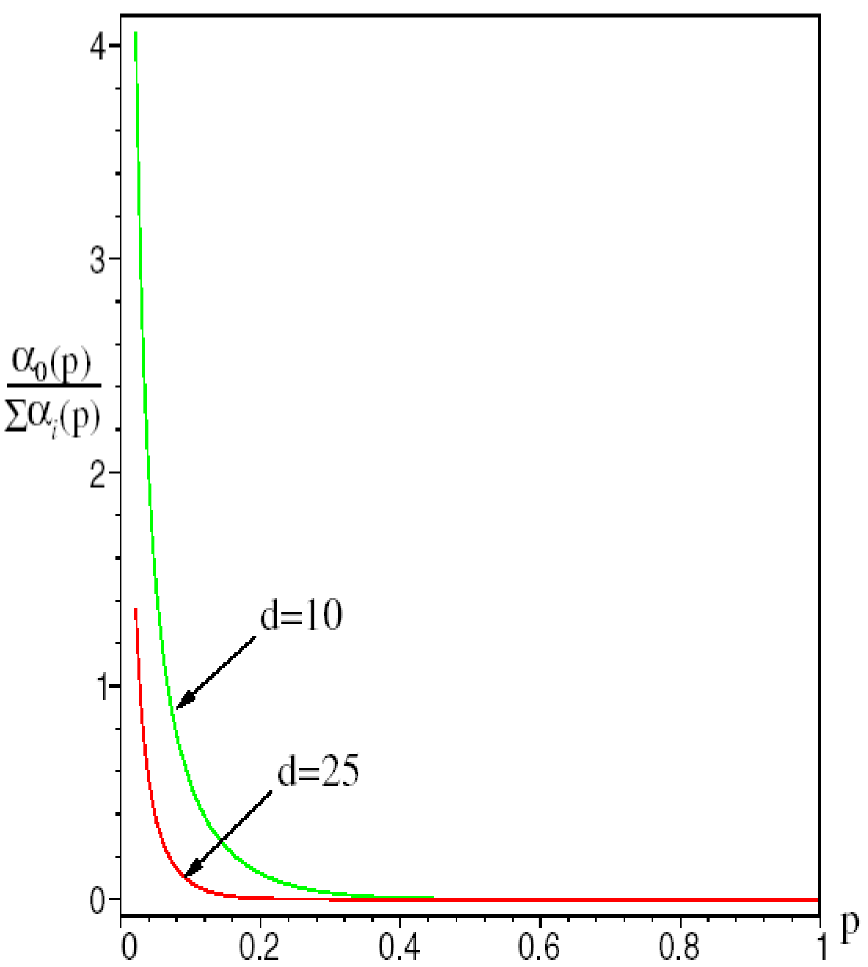
- Marking Field Spoofing

$$\begin{aligned} n_0(p) \geq n_1(p) \quad &\Leftrightarrow \quad \alpha_0(p) \geq \alpha_1(p) \\ &\Leftrightarrow \quad (1-p)^d \geq p(1-p)^{d-1} \end{aligned} \qquad \text{(III.1)}$$

$$\alpha_0(p) \geq \sum_{i=1}^{d} \alpha_i(p) \quad \Leftrightarrow \quad (1-p)^d \geq 1-(1-p)^d$$



$\frac{\alpha_0(p)}{\alpha_l(p)}$
10
8
6
4
2
1
0
0.2
0.4
0.5
0.6
0.8
1
p



$\frac{\alpha_0(p)}{\Sigma\alpha_l(p)}$
4
3
2
1
0
d=10
d=25
0
0.2
0.4
0.6
0.8
1
p

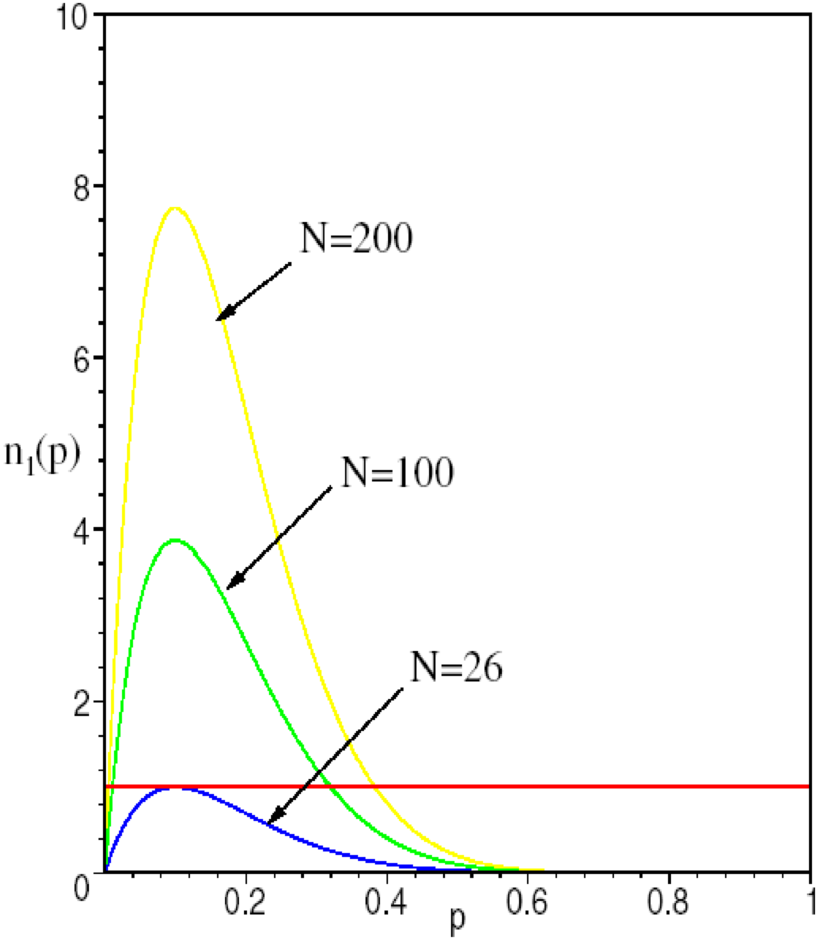
Probabilistic Marking(cont.)

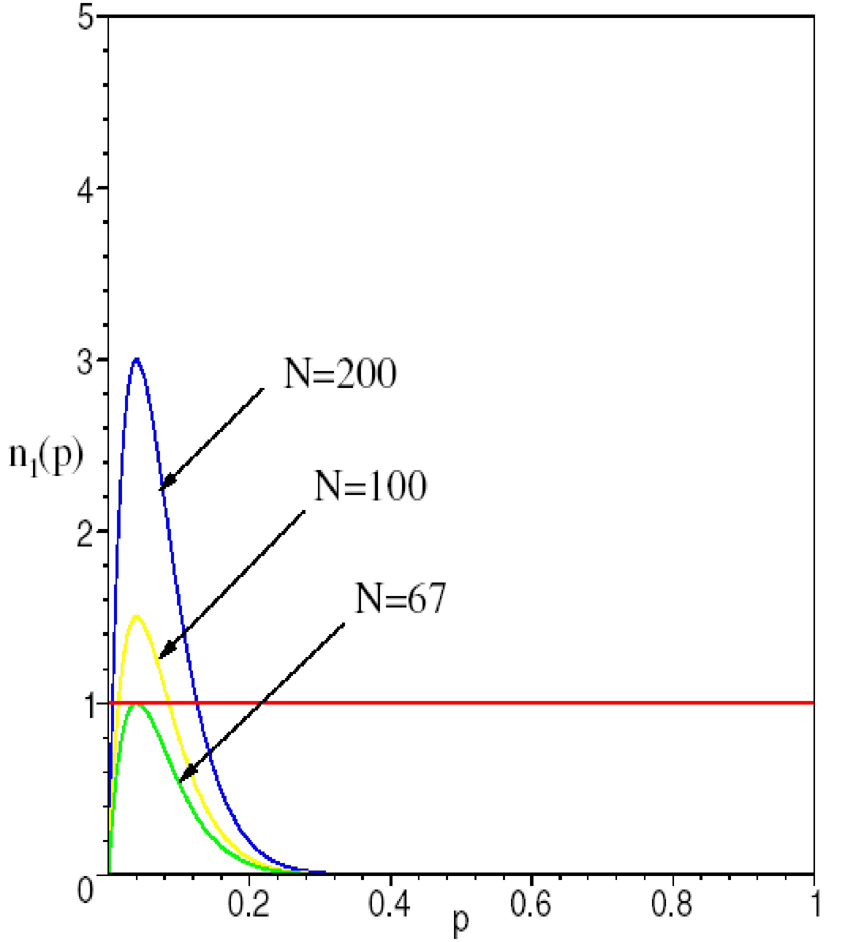
- Traceback Problem

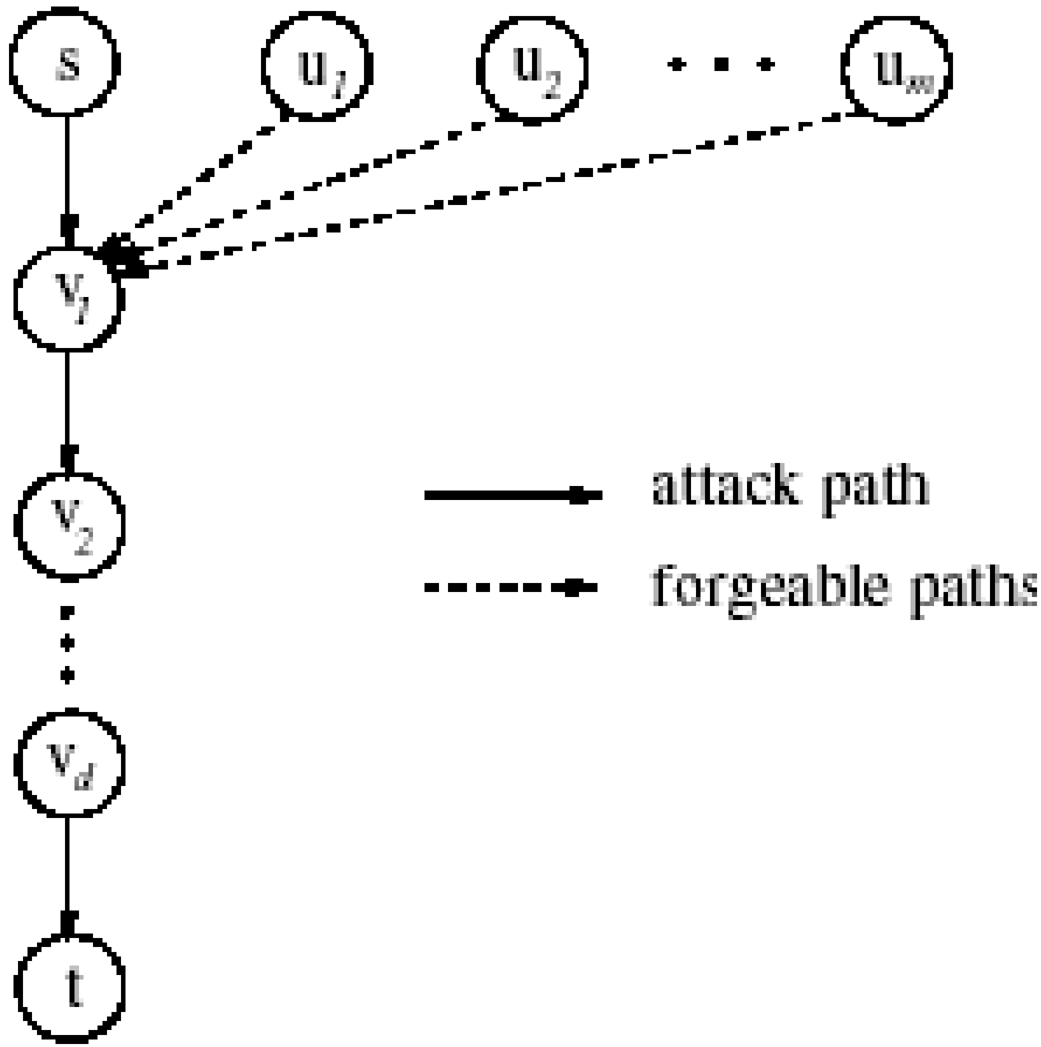
$$\alpha_1(p) = \alpha_1^s(p) = \alpha_2^s(p) = \ldots = \alpha_m^s(p)$$

$$N\alpha_1(p) = Np(1-p)^{d-1} \geq 1.$$

$$\min_{p} \max_{x_0, N} m(p, x_0)$$


10
8
6
4
2
0
0.2
0.4
0.6
0.8
1
p
$n_1(p)$
N=200
N=100
N=26


5
4
3
2
1
0
0.2
0.4
0.6
0.8
1
p
$n_1(p)$
N=200
N=100
N=67


s
u1
u2
um
v1
v2
vd
t
attack path
forgeable paths

Analysis of Single-Source DoS Attack

$$\Pr\{x_0 = (u_i, v_1)\} = \frac{1}{m}, \qquad i = 1, 2, \ldots, m.$$

$$\begin{aligned} m\,\alpha_1(p) = \alpha_0(p) \quad &\Leftrightarrow \quad m\,p(1-p)^{d-1} = (1-p)^d \\ &\Leftrightarrow \quad m = \frac{1}{p} - 1 \end{aligned}$$

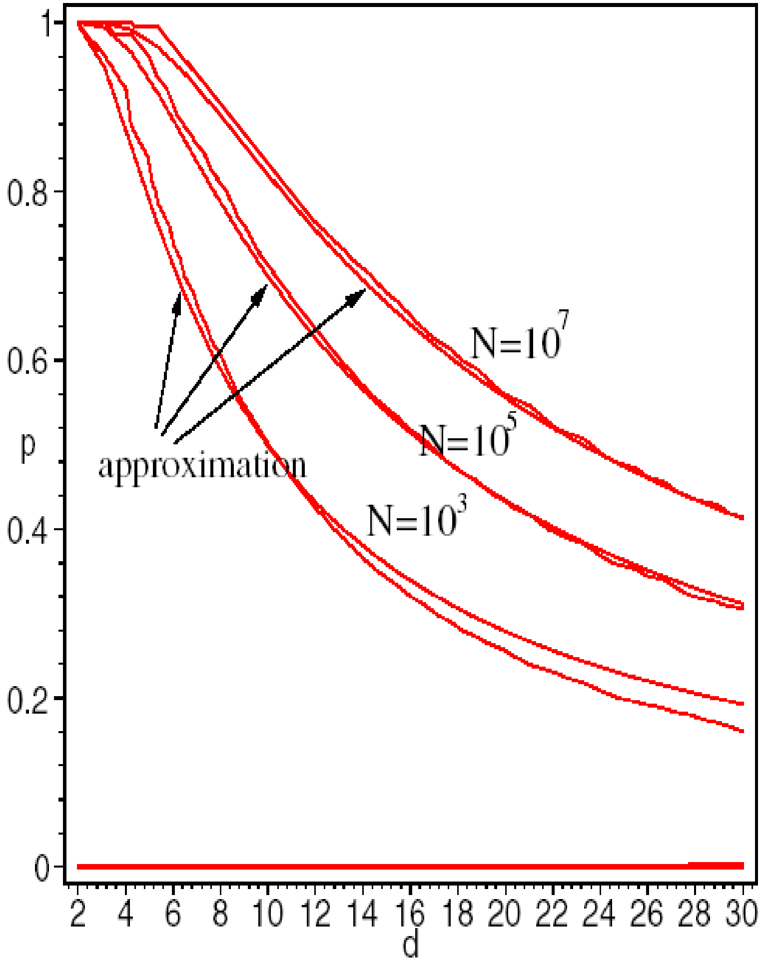
Approximation of Uncertainty Factor

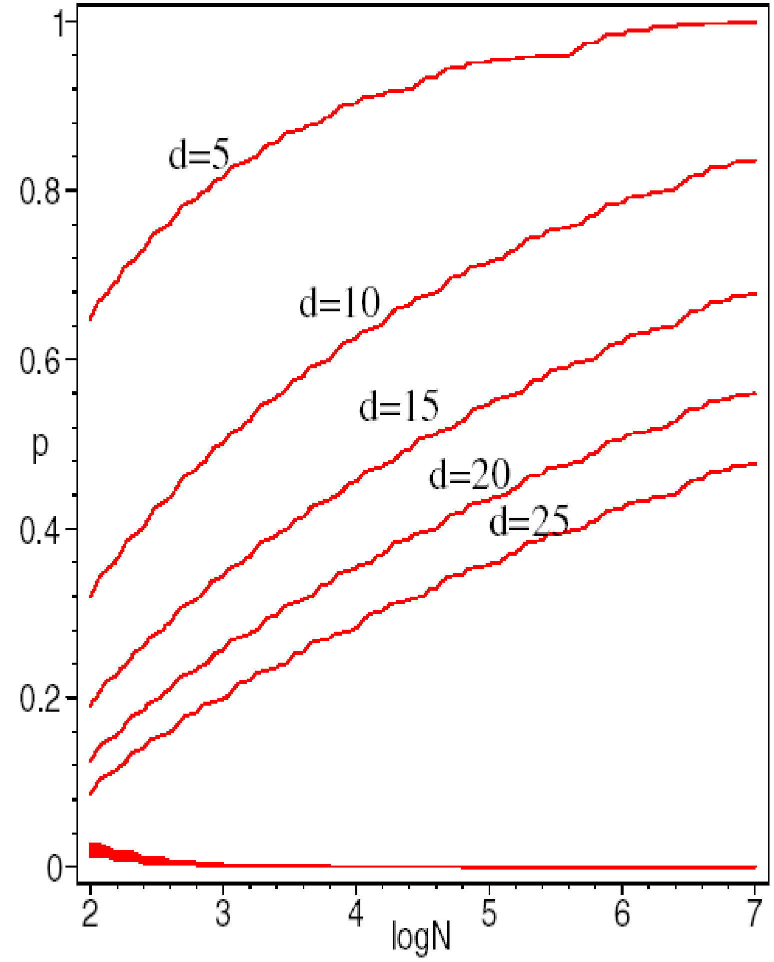
$Np(1-p)^{d-1} \geq 1$:

$$\frac{1}{N} \leq p \leq 1 - \left(\frac{1}{N}\right)^{\frac{1}{d-1}}.$$

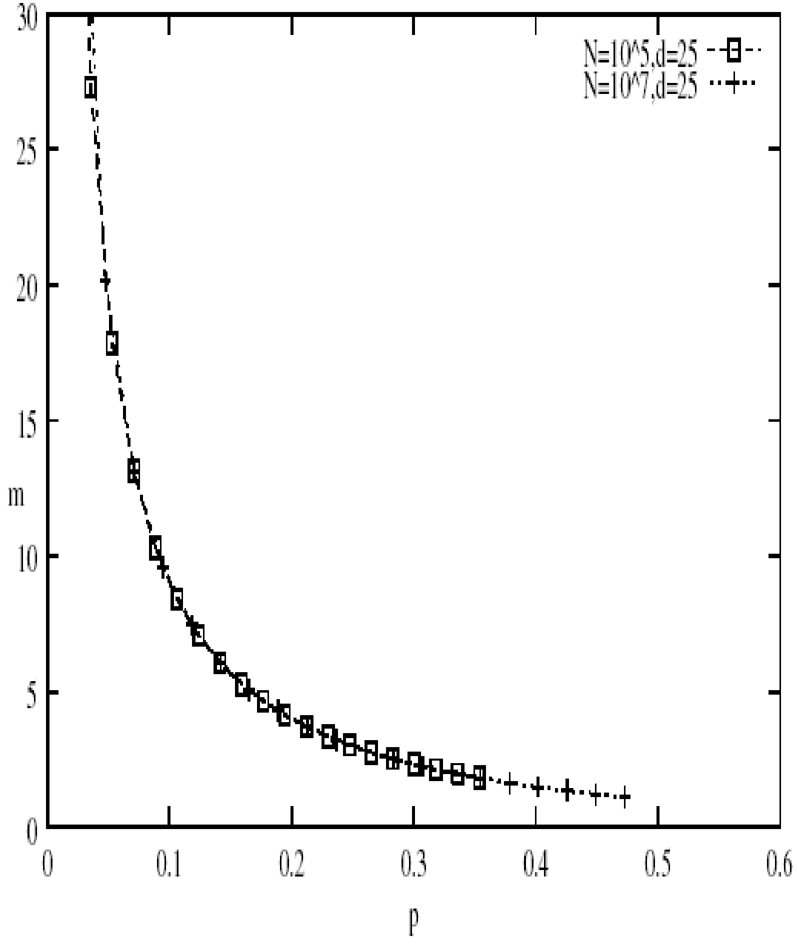
$$m \approx \frac{N^{-\frac{1}{d-1}}}{1 - N^{-\frac{1}{d-1}}}.$$

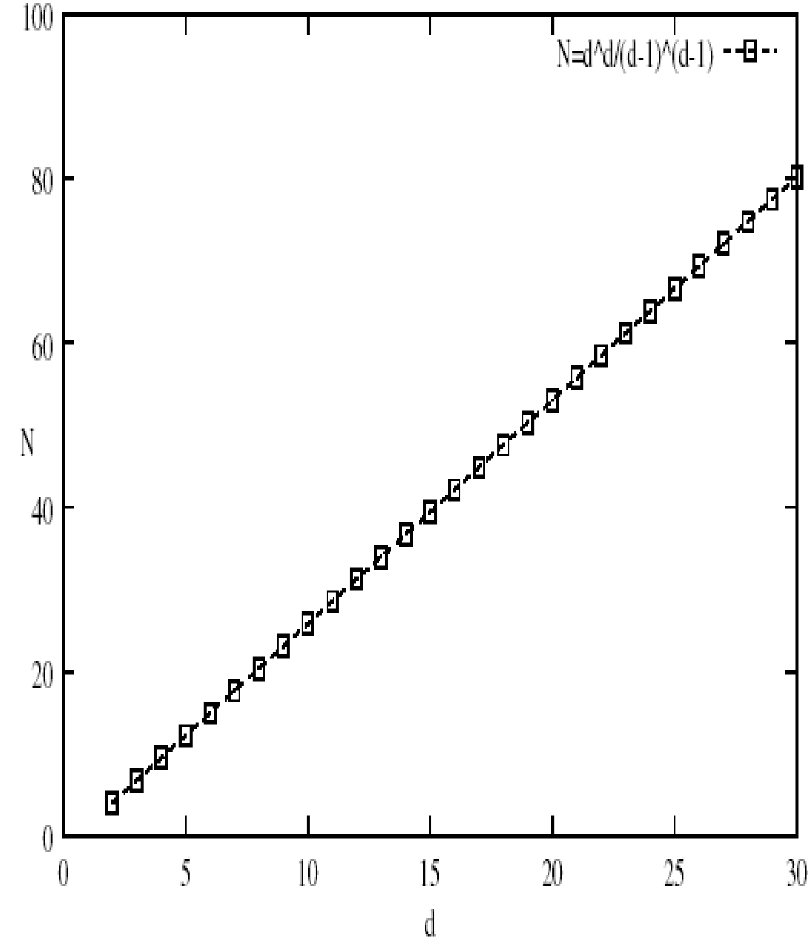
Numerical Evaluation



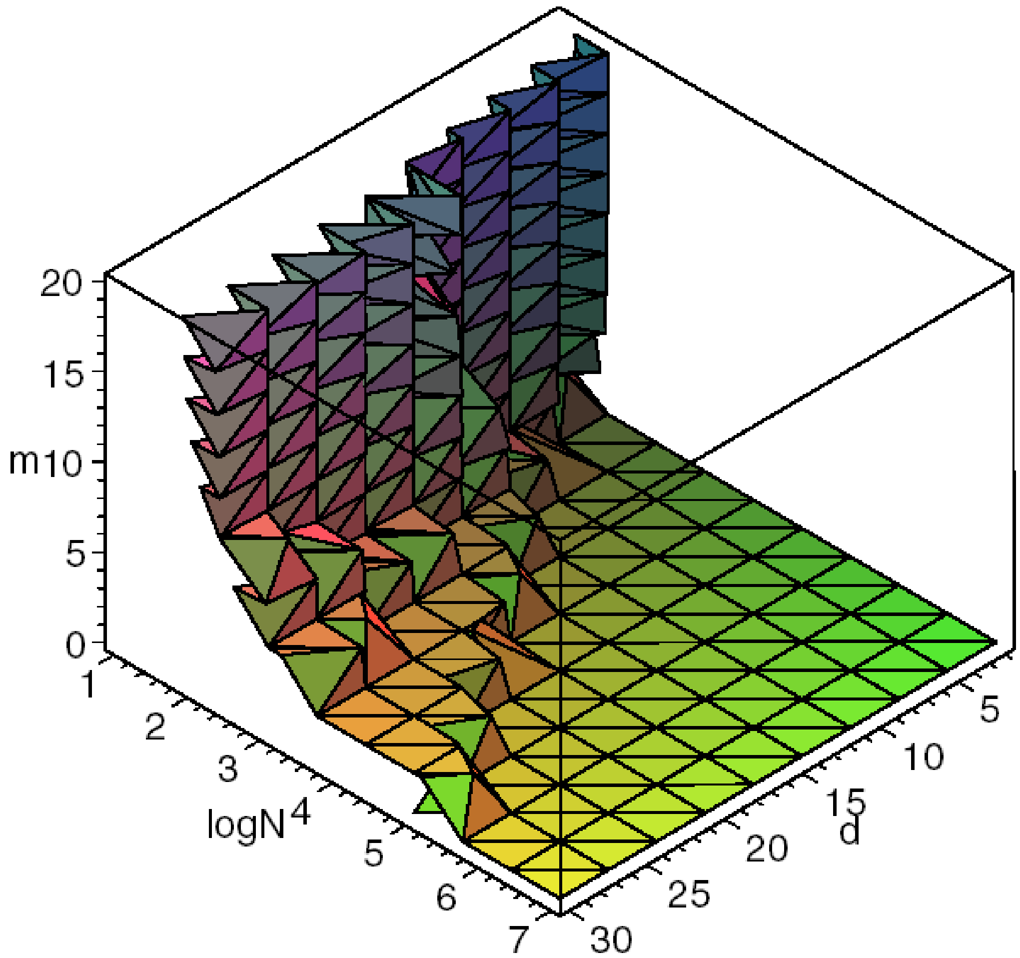


Numerical Evaluation





Numerical Evaluation



Distributed DoS Attack

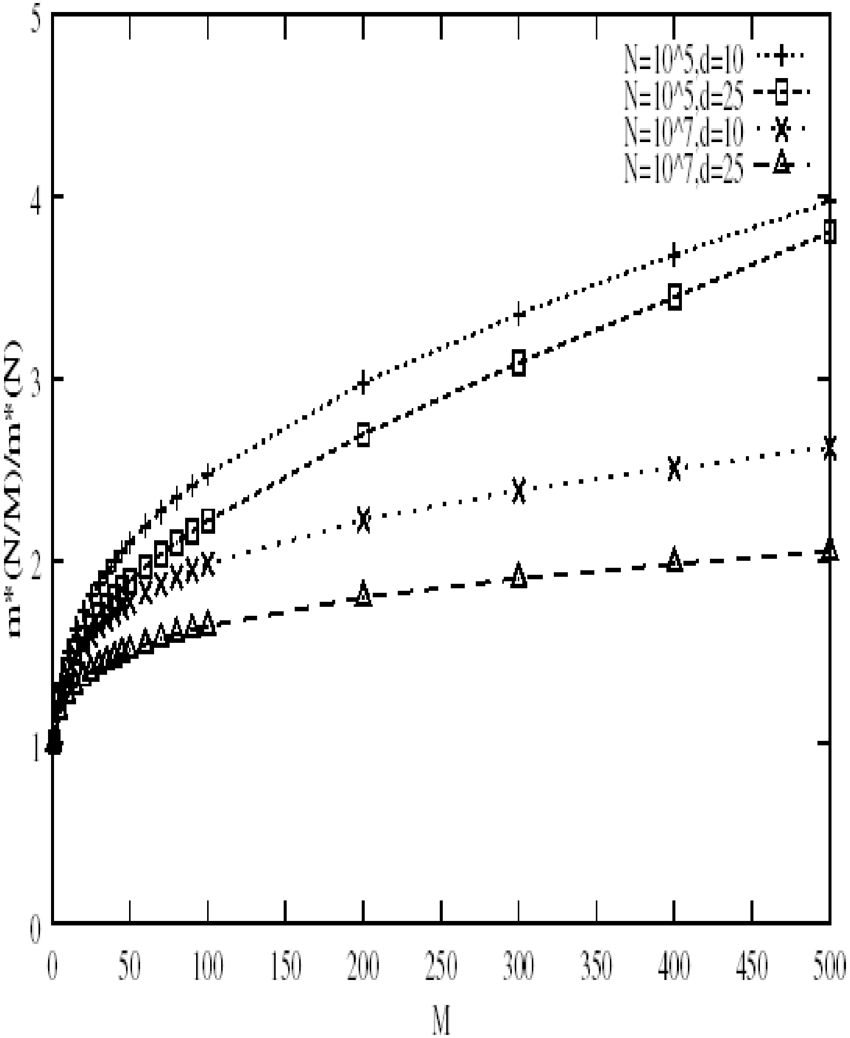
- Any-source traceback

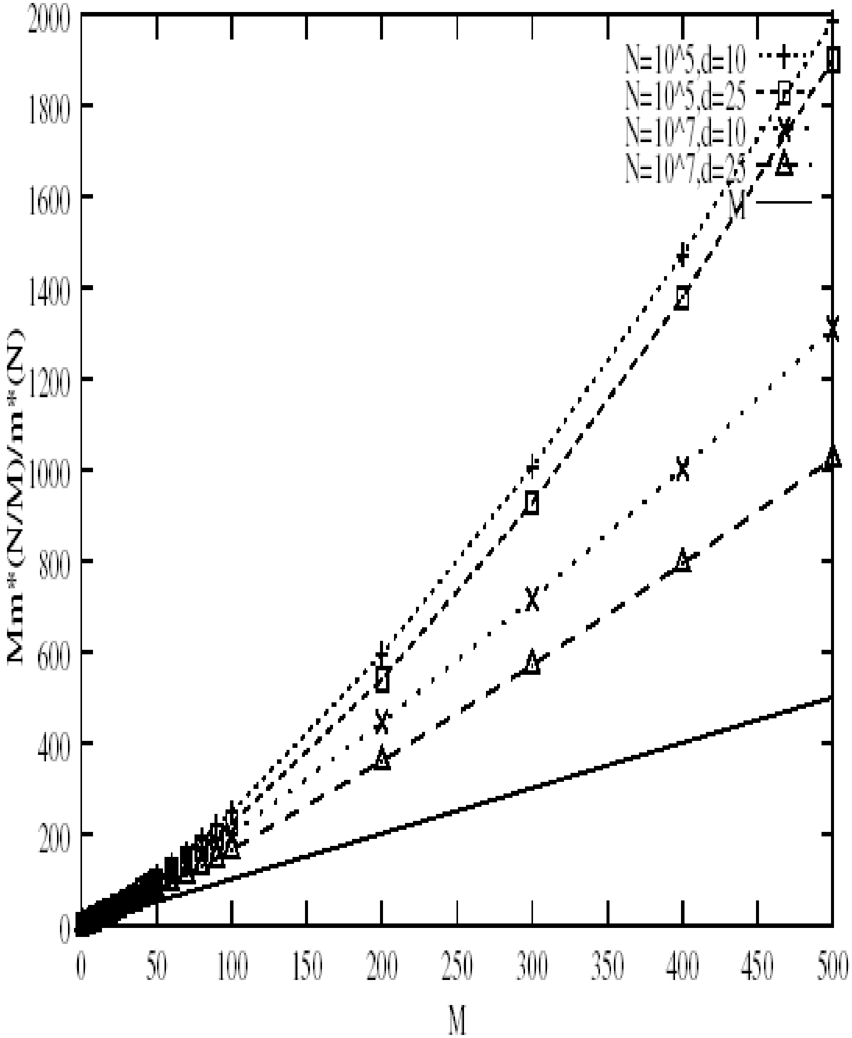
$$\min_{1 \le i \le M} \left\{ \frac{\alpha_{i,0}(p)}{\alpha_{i,1}(p)} \right\} = \min_{1 \le i \le M} \left\{ \frac{(1-p)^{d_i}}{p(1-p)^{d_i - 1}} \right\} = \frac{1}{p} - 1.$$

- All-source traceback

$$\sum_{i=1}^{M} m^i = \sum_{i=1}^{M} \frac{\alpha_{i,0}(p)}{\alpha_{i,1}(p)} = \sum_{i=1}^{M} \frac{(1-p)^{d_i}}{p(1-p)^{d_i - 1}} = M\left(\frac{1}{p} - 1\right)$$

Numerical Result





Conclusion

- This paper analyzed the effectiveness of PPM in a minimax adversarial context where the attacker is allowed to spoof the marking field to achieve maximum confusion at the victim.
- We can Choose a suitable marking probability to limit the attacker's ability.

Conclusion

- If we use different marking scheme,we may get different result.
- We can consider decreasing the marking probability by hop count.