TU Clausthal
Clausthal University of Technology

Markovian Modeling and Security Measure Analysis for Networks under Flooding DoS Attacks

Hendrik Baumann, Werner Sandmann
Department of Applied Stochastics and Operations Research,
Clausthal University of Technology

15 February 2012

Flooding DoS Attacks

- Flooding DoS attacks aim at obstructing regular service provisioning.
- Malicious attackers send large number of requests.
- Requests of legitimate users cannot be efficiently handled as designated.
- Aim: Give a Markov model for DoS attacks, incorporate 'Random Dropping Strategy' and compute security measures using special techniques for Quasi-Birth-Death processes.

Model assumptions (1)

- One server with N connection channels
- Basic model: Requests arrive according to Poisson processes with different rates λ_0 (regular requests) and λ_1 (attack requests), service times are exponentially distributed with rates β_0 (regular requests) and β_1 (attack requests), usually $\beta_1 << \beta_0$.
- Basic model yields two-dimensional Markov chain.

Model assumptions (2)

- Consider randomly changing environment: arrival rates and service completion rates are not constant but depend on some environmental state $v \in \{1, \ldots, m\}$.
- Switching rates σ_{vw} for change of environmental state.
- Together: Three-dimensional Markov chain, $X_t = (R_t, A_t, E_t)$.
- State space $\mathcal{S} = \{(i, j, v) \in \mathbb{N}^3 : \ i + j \leq N, \ v \in \{1, \ldots, m\}\}$.

Random dropping strategy

- Define threshold $t(N)$, use random dropping for $i + j > t(N)$.
- Use dropping rate $\delta(i + j) = d \cdot (i + j - t(N))$ for $i + j > t(N)$ with some 'dropping constant' d.
- The request to be dropped is chosen randomly.
- Result: specified dropping rates $\delta_0(i, j) = \frac{i}{i+j}\delta(i + j)$ (regular requests) and $\delta_1(i, j) = \frac{j}{i+j}\delta(i + j)$ (attack requests).

Markov chain model – Transitions

from	to	rate	condition
(i,j,v)	$(i+1,j,v)$	$\lambda_0(v)$	$i+j \leq N$
(i,j,v)	$(i,j+1,v)$	$\lambda_1(v)$	$i+j \leq N$
(i,j,v)	$(i-1,j,v)$	$\beta_0(v) \cdot i$	$i > 0,\ i+j \leq t(N)$
(i,j,v)	$(i,j-1,v)$	$\beta_1(v) \cdot j$	$j > 0,\ i+j \leq t(N)$
(i,j,v)	$(i-1,j,v)$	$\beta_0(v) \cdot i + d \cdot \frac{i+j-t(N)}{i+j} \cdot i$	$i > 0,\ i+j > t(N)$
(i,j,v)	$(i,j-1,v)$	$\beta_1(v) \cdot j + d \cdot \frac{i+j-t(N)}{i+j} \cdot j$	$j > 0,\ i+j > t(N)$
(i,j,v)	(i,j,w)	σ_{vw}	

QBD model

- Define *level* ℓ: $\mathcal{S}^{(\ell)} = \{(i,j,v) \in \mathcal{S} : \ i+j=\ell\}$, $\left|\mathcal{S}^{(\ell)}\right| = (\ell+1)\cdot m$.
- Transitions change the level at most by 1, resulting in Quasi-Birth-Death-Process (QBD).
- By appropriate ordering of states the generator is a block tridiagonal matrix:

$$Q = \begin{pmatrix} \tilde{Q}_{00} & \tilde{Q}_{01} & & & \\ \tilde{Q}_{10} & \tilde{Q}_{11} & \tilde{Q}_{12} & & \\ \ddots & \ddots & \ddots & \ddots & \\ & \tilde{Q}_{N-1,N-2} & \tilde{Q}_{N-1,N-1} & \tilde{Q}_{N-1,N} & \\ & & \tilde{Q}_{N,N-1} & \tilde{Q}_{NN} & \end{pmatrix}$$

Solution method – algorithm

Matrix analytic method for computing stationary distribution $\pi = (\tilde{\pi}_0\ \tilde{\pi}_1\ \ldots\ \tilde{\pi}_N)$:

- Compute $R_{N-1} = -\tilde{Q}_{N-1,N}\tilde{Q}_{NN}^{-1}$.
- For $\ell = N-1, N-2, \ldots, 1$: Iterate
  $R_{\ell-1} = -\tilde{Q}_{\ell-1,\ell}\left(\tilde{Q}_{\ell\ell} + R_\ell \tilde{Q}_{\ell+1,\ell}\right)^{-1}$.
- Obtain a solution $\tilde{\pi}_0 \neq 0$ from $\tilde{\pi}_0\left(\tilde{Q}_{00} + R_0\tilde{Q}_{10}\right) = 0$.
- For $\ell = 0, 1, \ldots, N-1$: Iterate $\tilde{\pi}_{\ell+1} = \tilde{\pi}_\ell R_\ell$.
- Normalize $\tilde{\pi}$.

Considered security measures (1)

- Stationary probability for i channels working on regular requests, j channels working on attack requests: $\pi(i,j) = \sum_{v=1}^{m} \pi(i,j,v)$.
- Ratio of channels occupied by regular requests to total number of channels:

$$p_r = \frac{1}{N} \sum_{\substack{i,j \\ i+j \leq N}} i \cdot \pi(i,j).$$

- Ratio of channels occupied by attack requests to total number of channels:

$$p_a = \frac{1}{N} \sum_{\substack{i,j \\ i+j \leq N}} j \cdot \pi(i,j).$$

Considered security measures (2)

- Probability of loss, that is rejection of regular request

$$p_{loss} = \sum_{i+j=N} \pi(i,j).$$

- Probablitiy for dropping regular requests rather than serving them successfully

$$p_{drop} = \frac{\sum \pi(i,j) \frac{i}{i+j} \delta(i+j)}{\sum \pi(i,j) \left(\beta_0 i + \frac{i}{i+j} \delta(i+j) \right)}.$$

- Probability for successfully serving an incoming regular request

$$p_{succ} = (1 - p_{loss})(1 - p_{drop}).$$

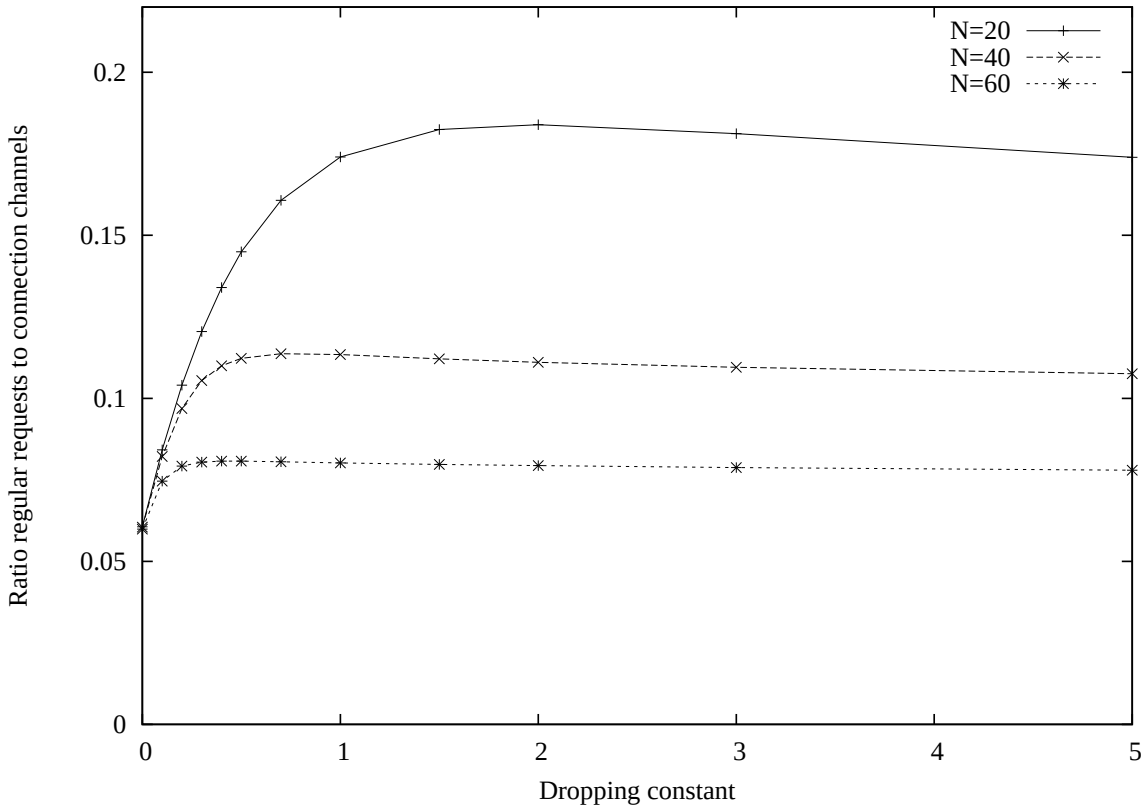
Parameter setting

- $m = 3$ environment states with switching rates

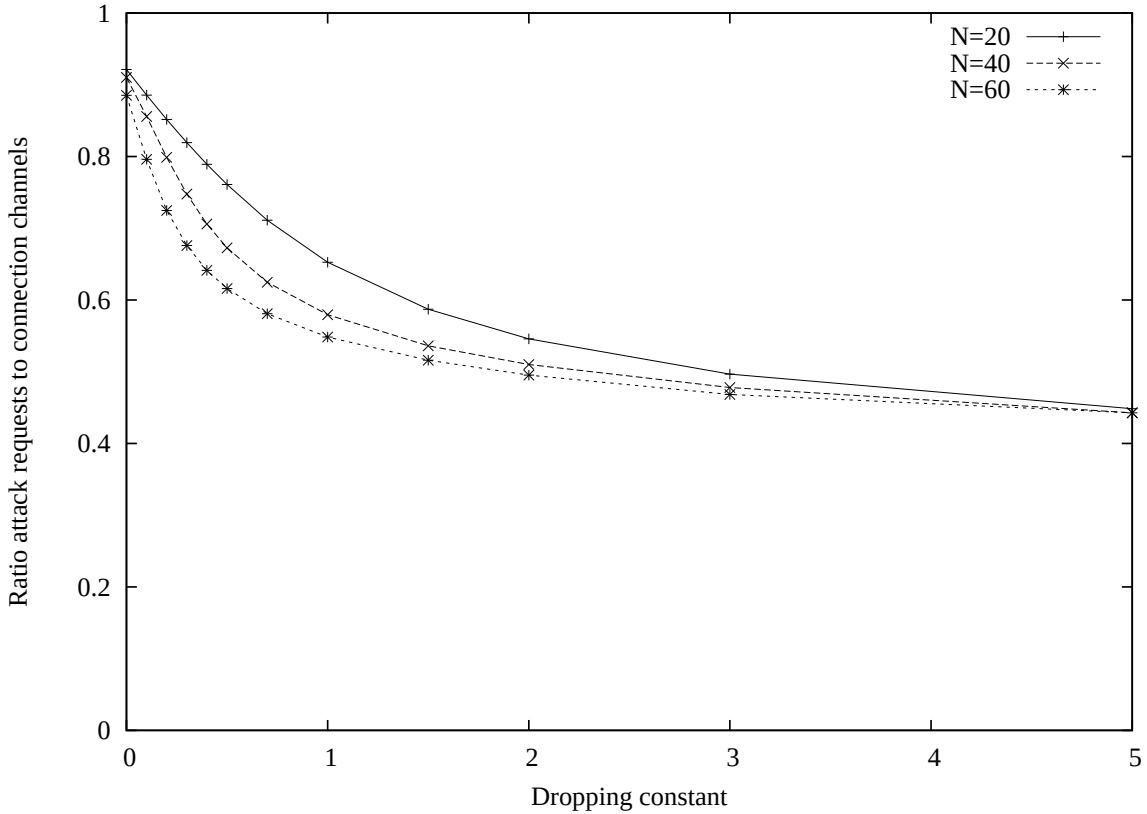
$v \mid w$	1	2	3
1		0.2	0.1
2	0.4		0.1
3	0.6	0.2	

- $\lambda_0(1) = \lambda_0(2) = 5$, $\lambda_0(3) = 25$.
- $\lambda_1(1) = \lambda_1(3) = 6$, $\lambda_1(2) = 60$.
- $\beta_0(v) = 2$, $\beta_1(v) = 0.1$.
- $t(N) = \frac{N}{2}$.
- Variate dropping rate d between 0 (no dropping) and 5 for $N = 20, 40, 60$.

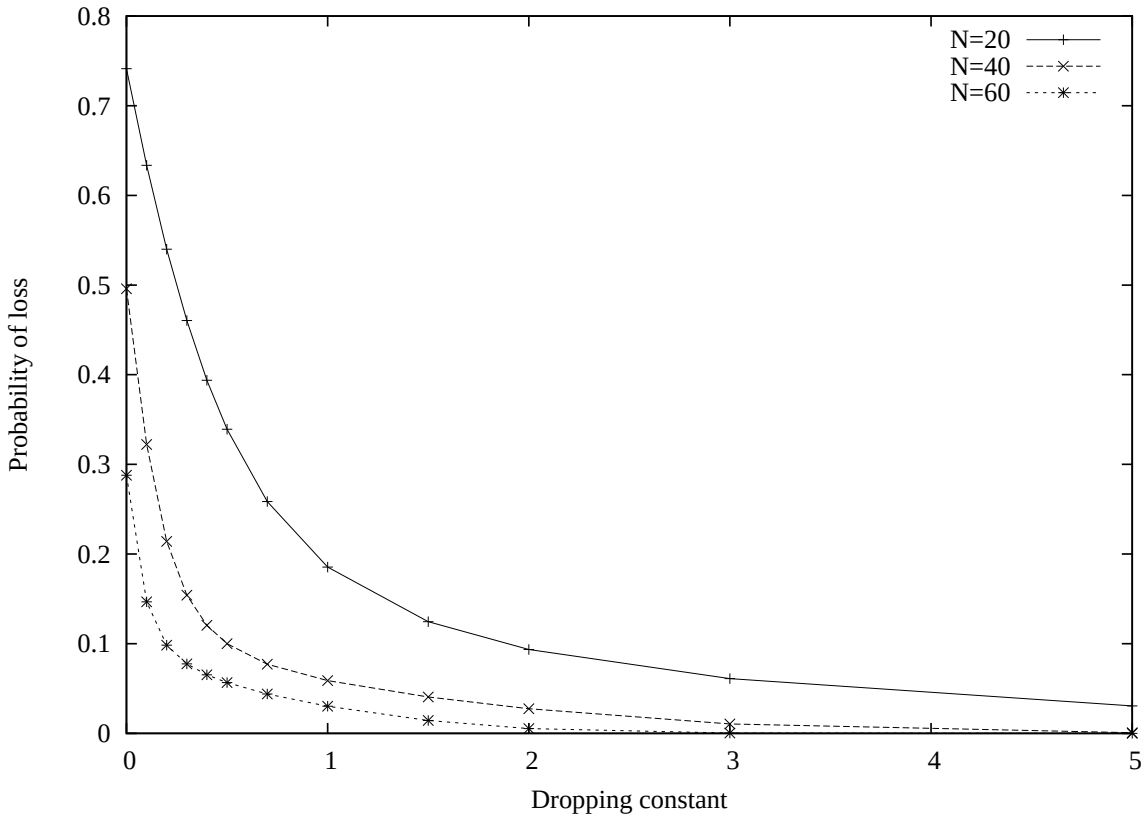
Numerical results (1)



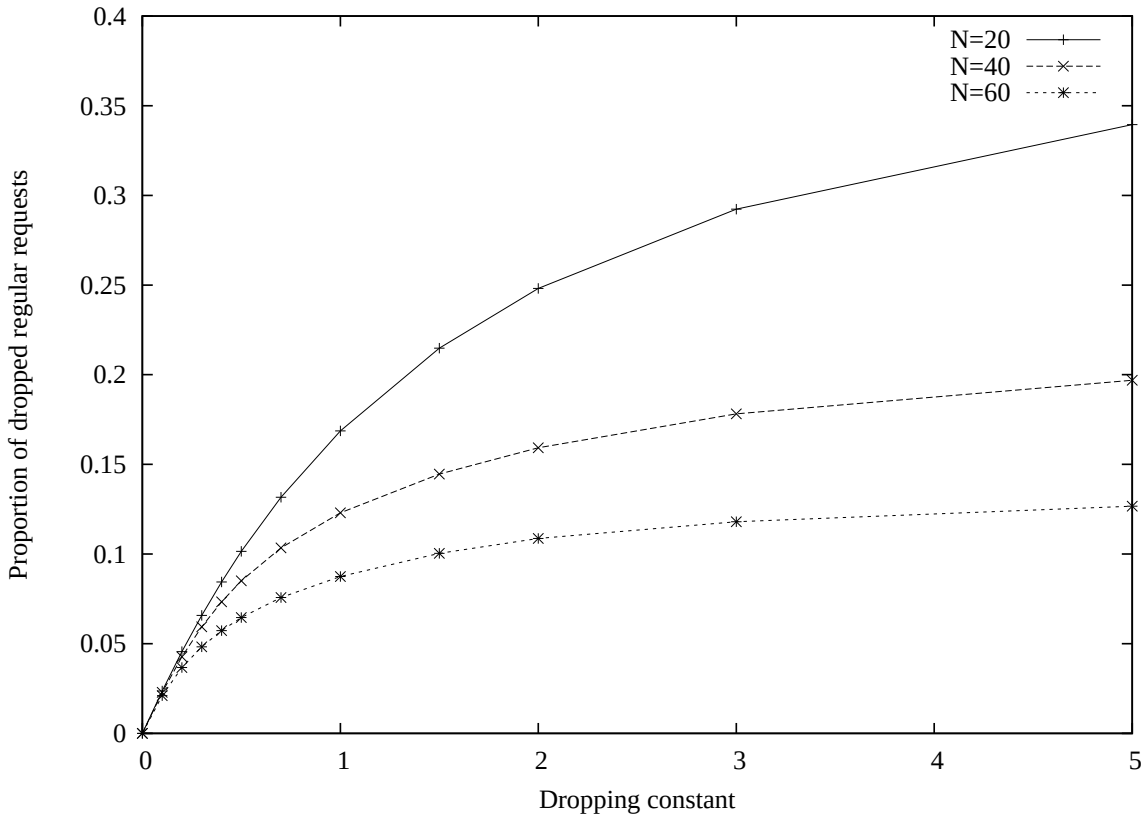
Numerical results (2)



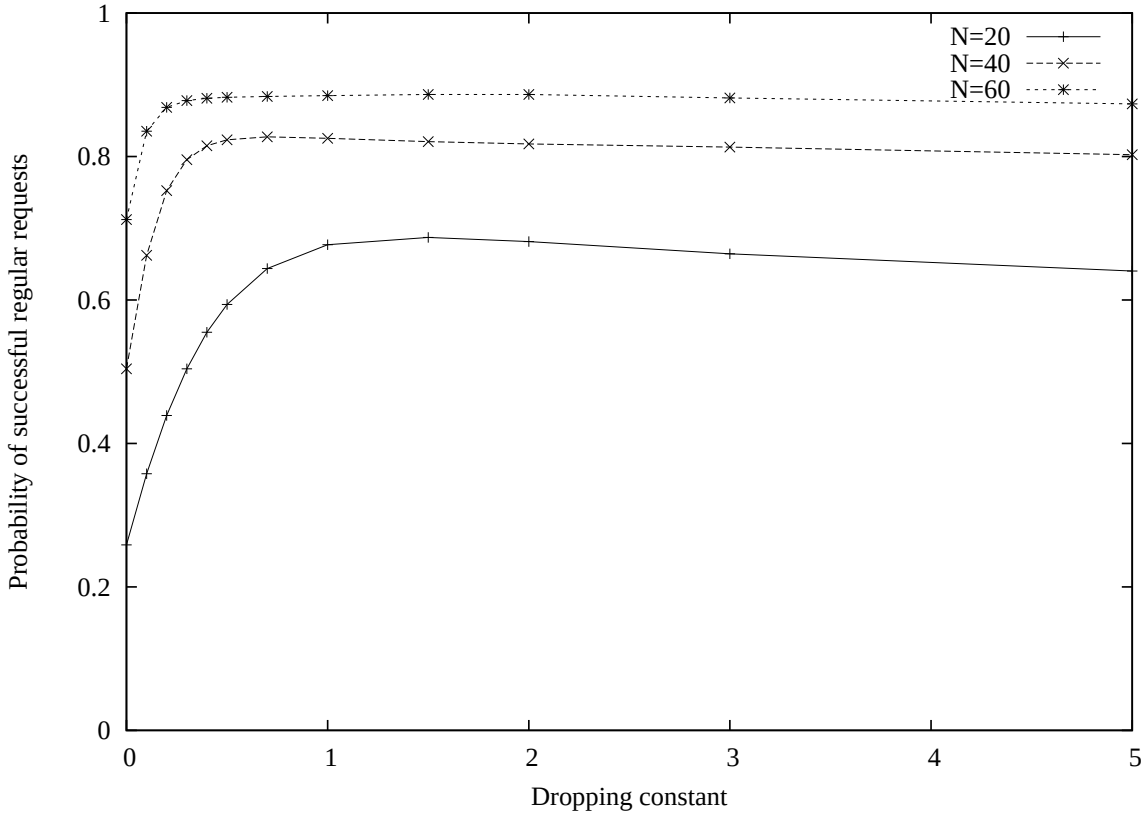
Numerical results (3)



Numerical results (4)



Numerical results (5)



Conclusions

- We have modelled flooding DoS-Attacks in a Markov chain including a random environment.
- We have analyzed them by efficient matrix analytic methods.
- Incorporation of random dropping improves the service significantly.

Future work

- Analysis of transient behaviour.
- Memory-efficient direct computation of stationary security measures.
- Consideration of BMAPs for arrivals instead of mere Markov modulated Poisson processes.
- Consideration of other service times distributions, approximation by PH-distributions.