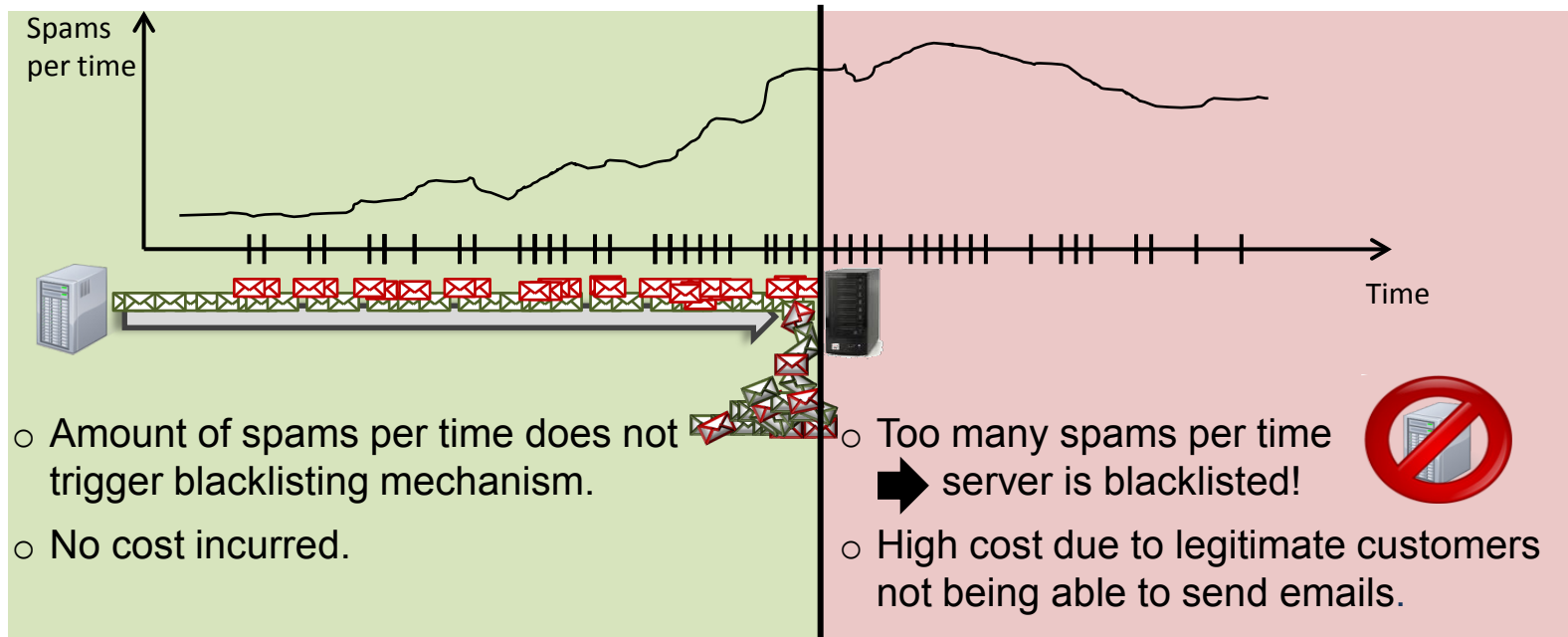


Throttling Poisson Processes

Dick, Haider, Vanck, Brückner, Scheffer

- Motivation: Filtering outbound email spam:
 - Denying legitimate emails from being sent incurs cost.
 - When sending spam messages, server may get blacklisted by other services — high costs!
 - Risk of being blacklisted increases with amount of spam sent per time unit.



Throttling Poisson Processes

- Sequential decision-making problems
 - events are generated by Poisson process,
 - loss may depend on number of false decisions per unit of time.
- Loss does not factorize over individual decisions.
- Common problem in IT security applications:
Attacks incur costs if number of unsuppressed hostile events per time exceeds certain capacity.

Throttling Poisson Processes

- Approach: Decision model employs parametric function
 - that takes sequence of events as input,
 - and outputs upper limit on passing (negative) decisions per time interval.

$$\pi(\text{seq}) = \begin{cases} -1 \text{ (“allow”)} & \text{if } (\# \text{events passed}) + 1 \leq f_{\theta}(\text{seq}) \\ +1 \text{ (“suppress”)} & \text{otherwise.} \end{cases}$$

Throttling Poisson Processes

- Result from queueing theory leads to closed-form, convex optimization problem.
- Experiments on throttling abusive email accounts.
- Currently in use for email service of large commercial European web hosting company.