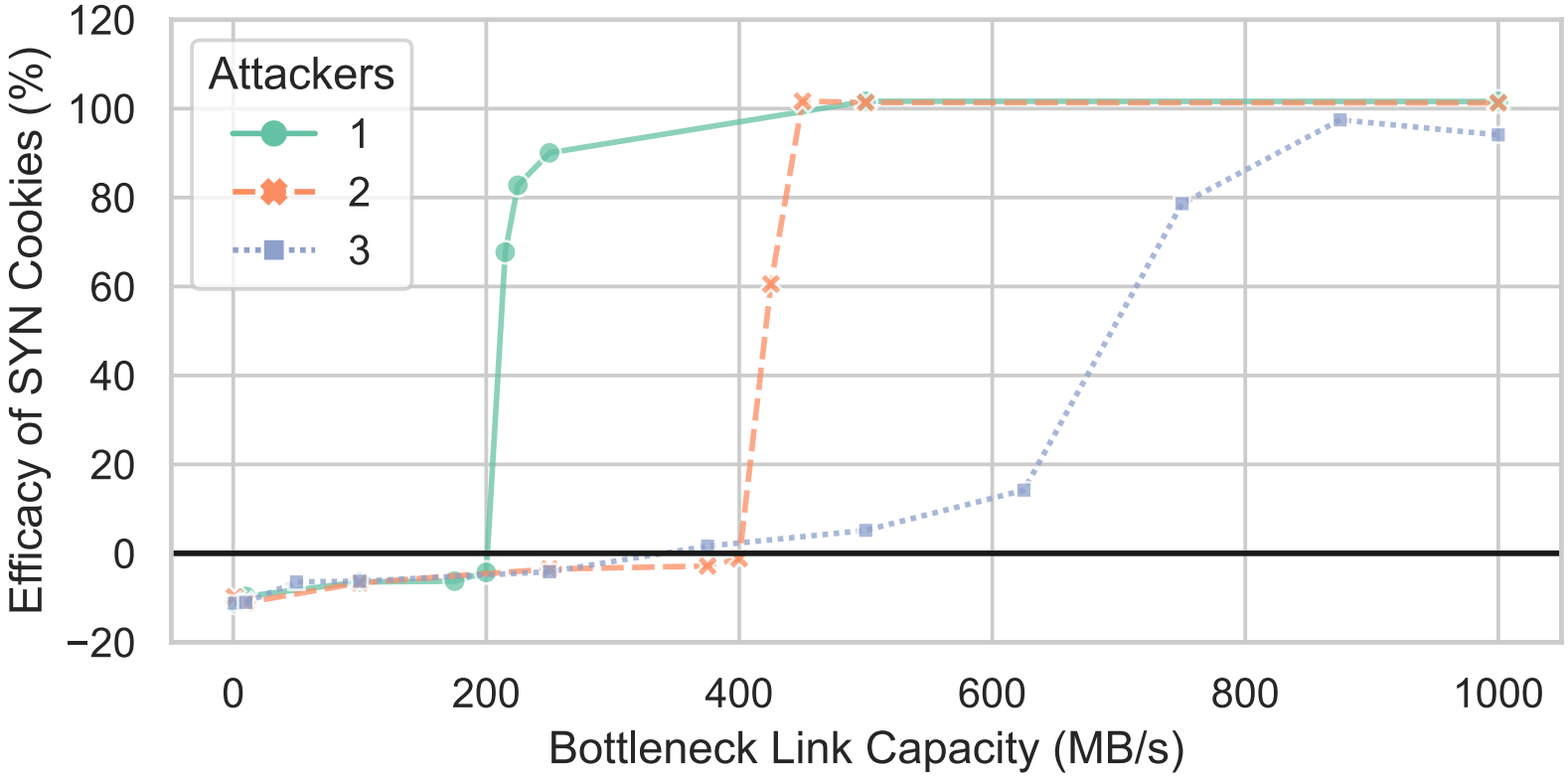
Context Matters: Accurately Measuring the Efficacy of Denial-of-Service Mitigations

Computer Science Experimentation and Test Workshop ‘22
August 8th, 2022

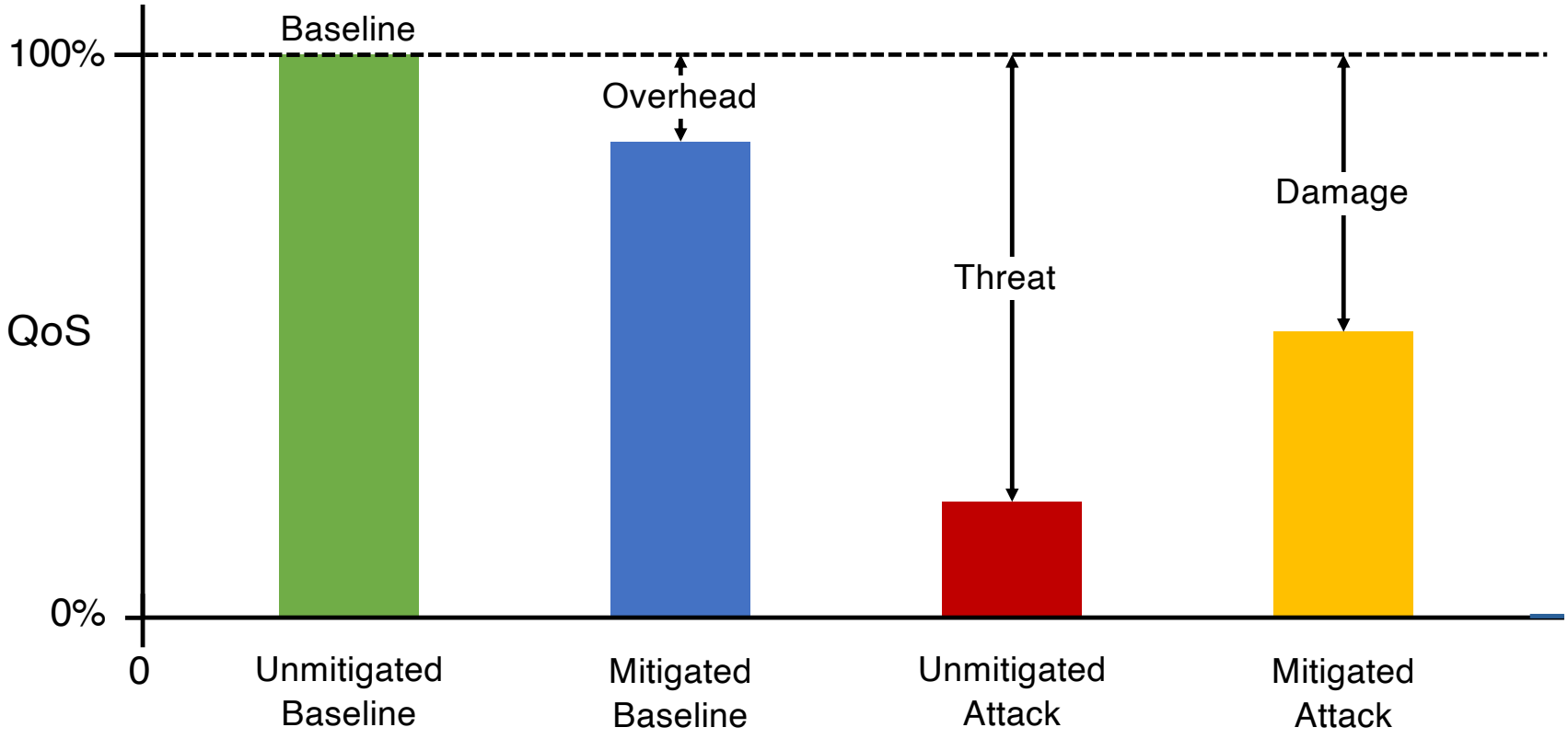
Samuel DeLaughter (samd@mit.edu)
Karen Sollins (sollins@csail.mit.edu)

Mitigation Efficacy is Context-Specific



Context-Specific Metrics

$$\% \text{ Efficacy} = \frac{\text{Threat} - \text{Damage}}{\text{Threat}} * 100$$



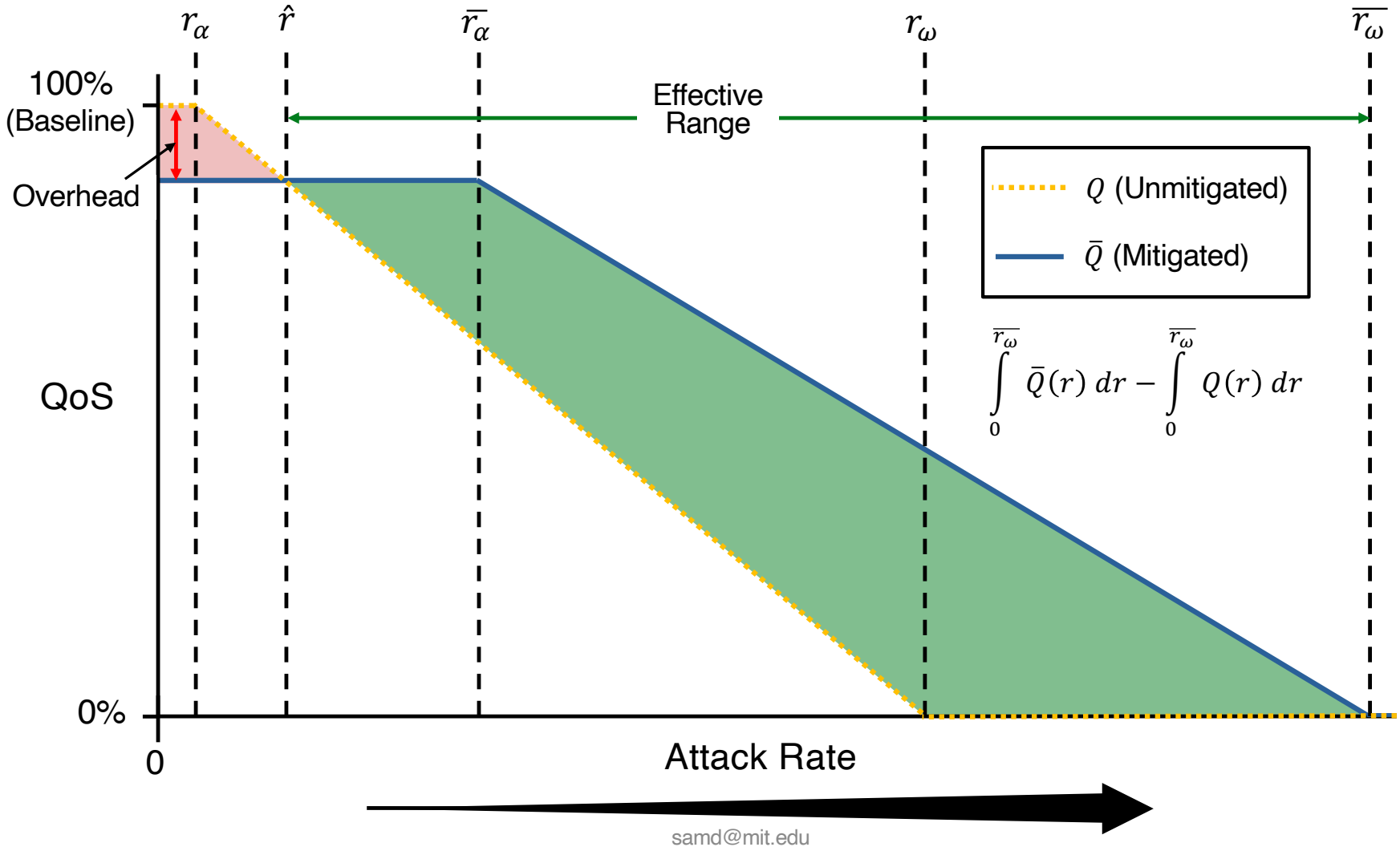
Defining a Context

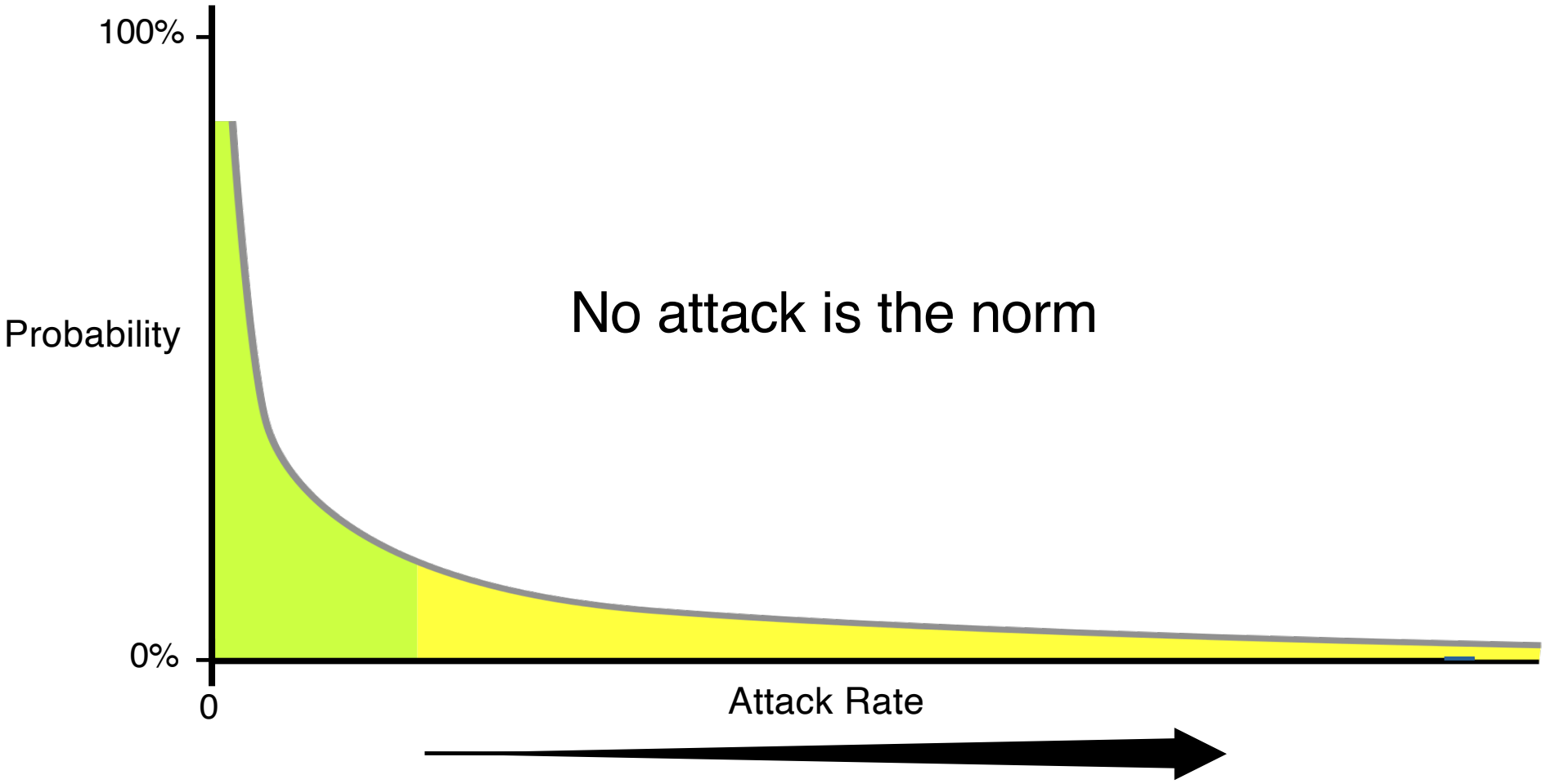
These metrics depend on categorical and numerical context variables:

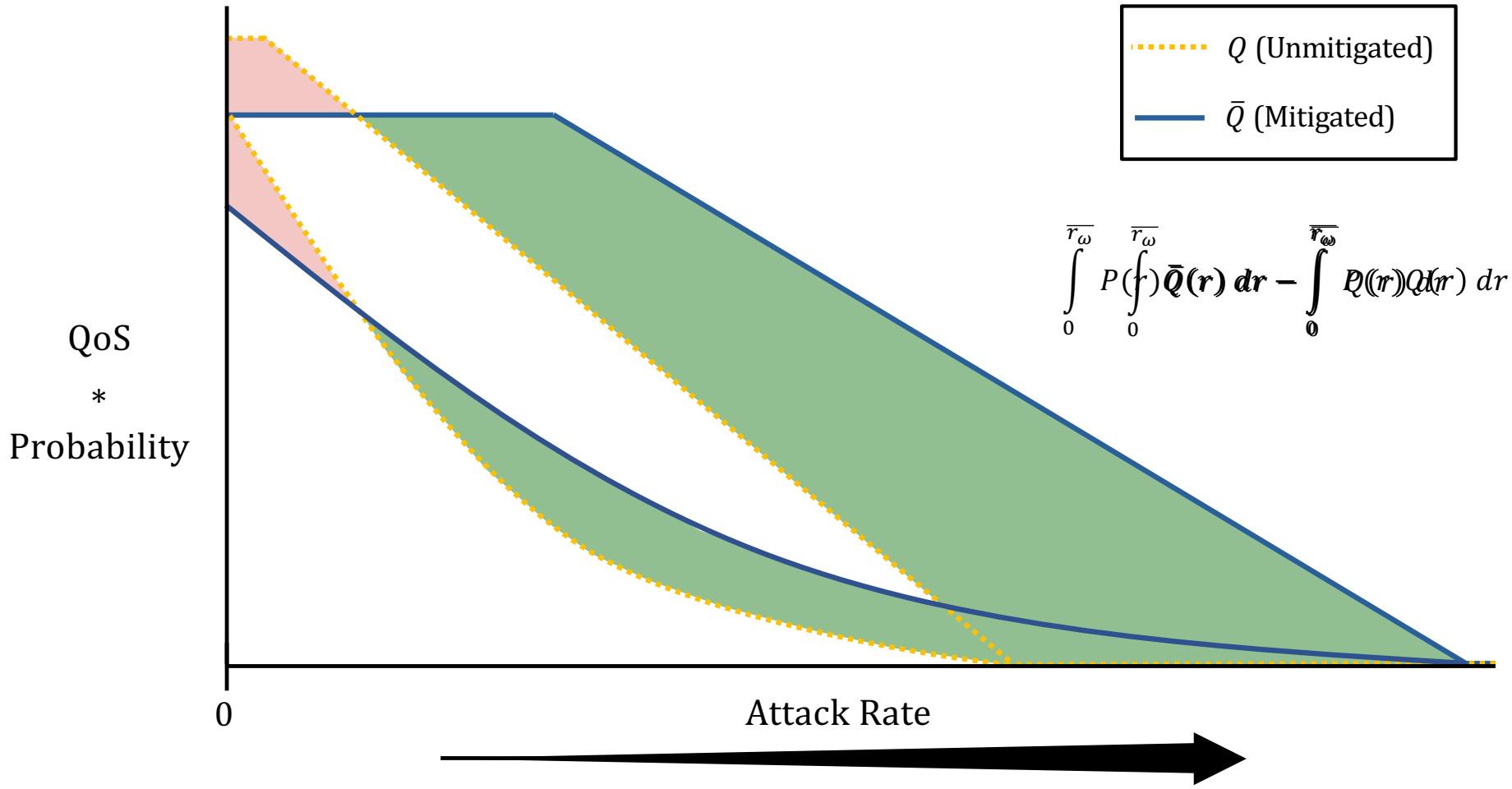
- Attack Vector
- Client Application
- Server OS
- Network Topology
- IP Version
- etc.

- Attack Rate
- Client Request Rate
- Server RAM / CPU Speed
- Client/Server RTT, Loss
- Bottleneck Link Capacity
- etc.

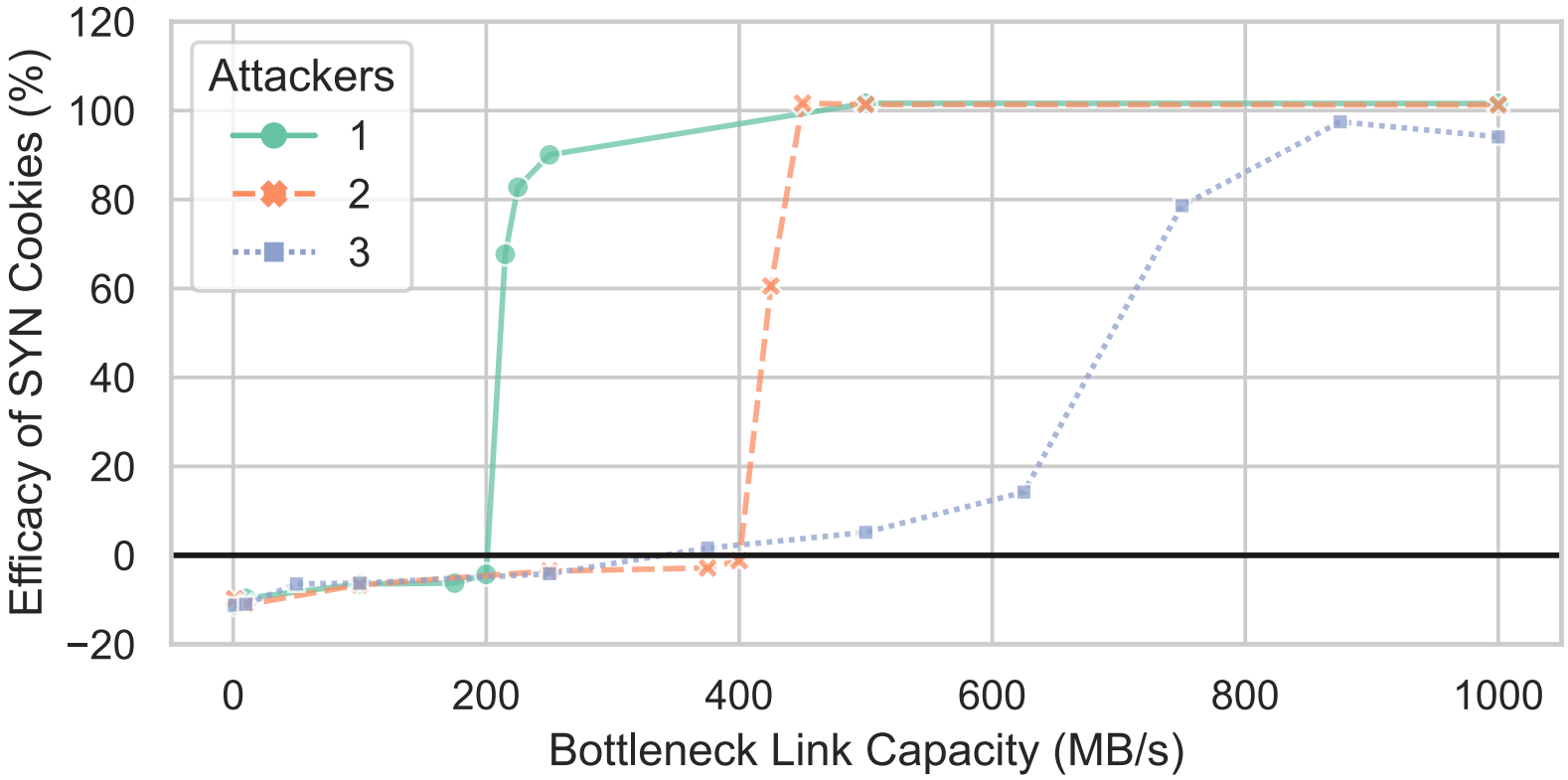
Minor changes in context can have a major impact on results


r_α
$\hat{r}$
$\overline{r_\alpha}$
r_ω
$\overline{r_\omega}$
100%
(Baseline)
Overhead
Effective
Range
Q (Unmitigated)
$\bar{Q}$ (Mitigated)
$\int_0^{\overline{r_\omega}} \bar{Q}(r)\,dr - \int_0^{\overline{r_\omega}} Q(r)\,dr$
QoS
0%
0
Attack Rate


100%
Probability
0%
0
No attack is the norm
Attack Rate


Q (Unmitigated)
$\bar{Q}$ (Mitigated)
$\int_0^{\overline{r_\omega}} P(r)\bar{Q}(r)\,dr - \int_0^{\overline{r_\omega}} P(r)Q(r)\,dr$
QoS
*
Probability
0
Attack Rate

Mitigation Efficacy is Context-Specific



Questions?

Experiments

- Run on DeterLab
  - Real hardware = real bottlenecks
- Clients repeatedly open and close TCP connections
- Attackers send SYN floods
  - ~90 MB/s per device
  - Spoofed source addresses
- Server toggles SYN Cookies
- SYN-ACKs routed to Sink
  - Prevent drop from Deter's sandboxing
  - Preserve backscatter effects