Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

SPIFFY: Inducing Cost-Detectability Tradeoffs for Persistent Link-Flooding Attacks

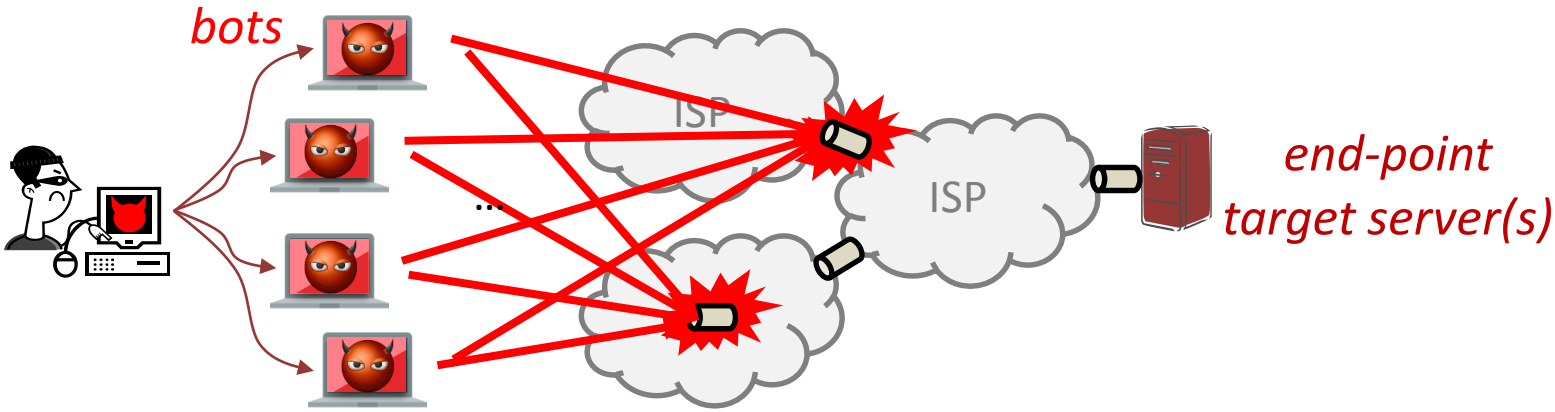
Min Suk Kang **Virgil D. Gligor** **Vyas Sekar**

ECE Department and CyLab,
Carnegie Mellon University

Feb 22, 2016

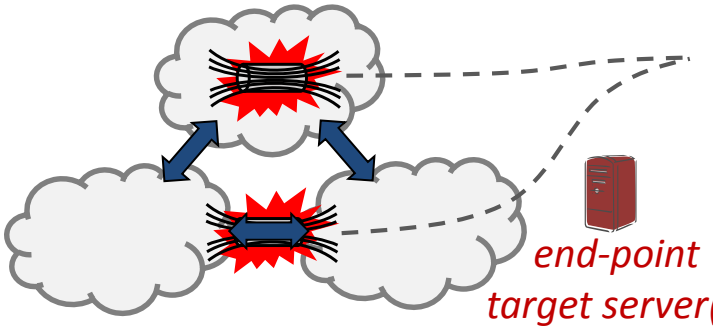
Large-scale *link-flooding* attacks

Massive DDoS attacks against *chosen target links* in *Internet Infrastructure*



- *Real-world examples*
  - ✓ Spamhaus (March 2013), ProtonMail (Nov 2015)
- *"**Indistinguishability**"* of attack flows
  - ✓ *Bot-to-bot* or *bot-to-server* attack flows (e.g., Coremelt [ESORICS'09], Crossfire [S&P'13])

Fundamental defense approach requires *inter-ISP coordination*



"Routing Bottlenecks" [CCS'14]
become the *vulnerabilities exploitable* by link-flooding attacks

Removing routing bottlenecks **=> inter-ISP coordination**

Inter-ISP coordination requires global deployment of new protocols, bilateral agreement, and added infrastructure

=> Thus, we need a first-line of defense that can be offered by a single ISP and can be immediately deployed

First-line of defense

without inter-ISP coordination

Goal: attack deterrence

Deter ***rational*** Indistinguishable link-flooding adversaries

rational: ***cost-sensitive*** and **stealthy**

- ✓ Majority of DDoS adversaries are rational [Png et al. 2008]

Sketch of solution

- ✓ **Bot detection** at **local ISP**
  exploiting adversary's ***cost-sensitive behavior***
- ✓ **Bot detection** can be **circumvented**
  when adversary **accepts significant cost increase**
- ✓ **Bot detection =>** ***cost-detectability tradeoff***

Problem statement and solutions

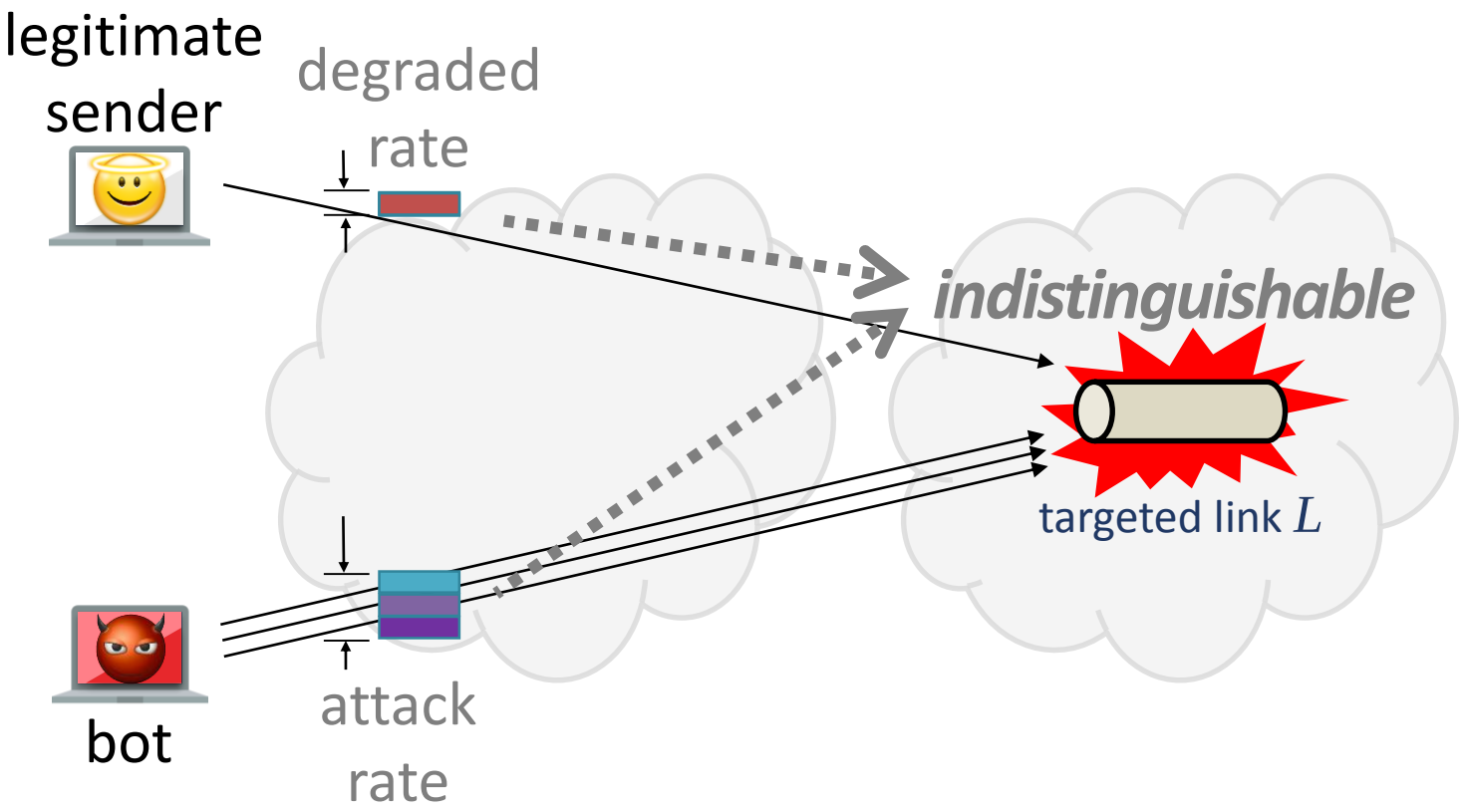
Problem: First-line of defense for link-flooding attacks

Solutions: Deterrence of rational link-flooding adversaries

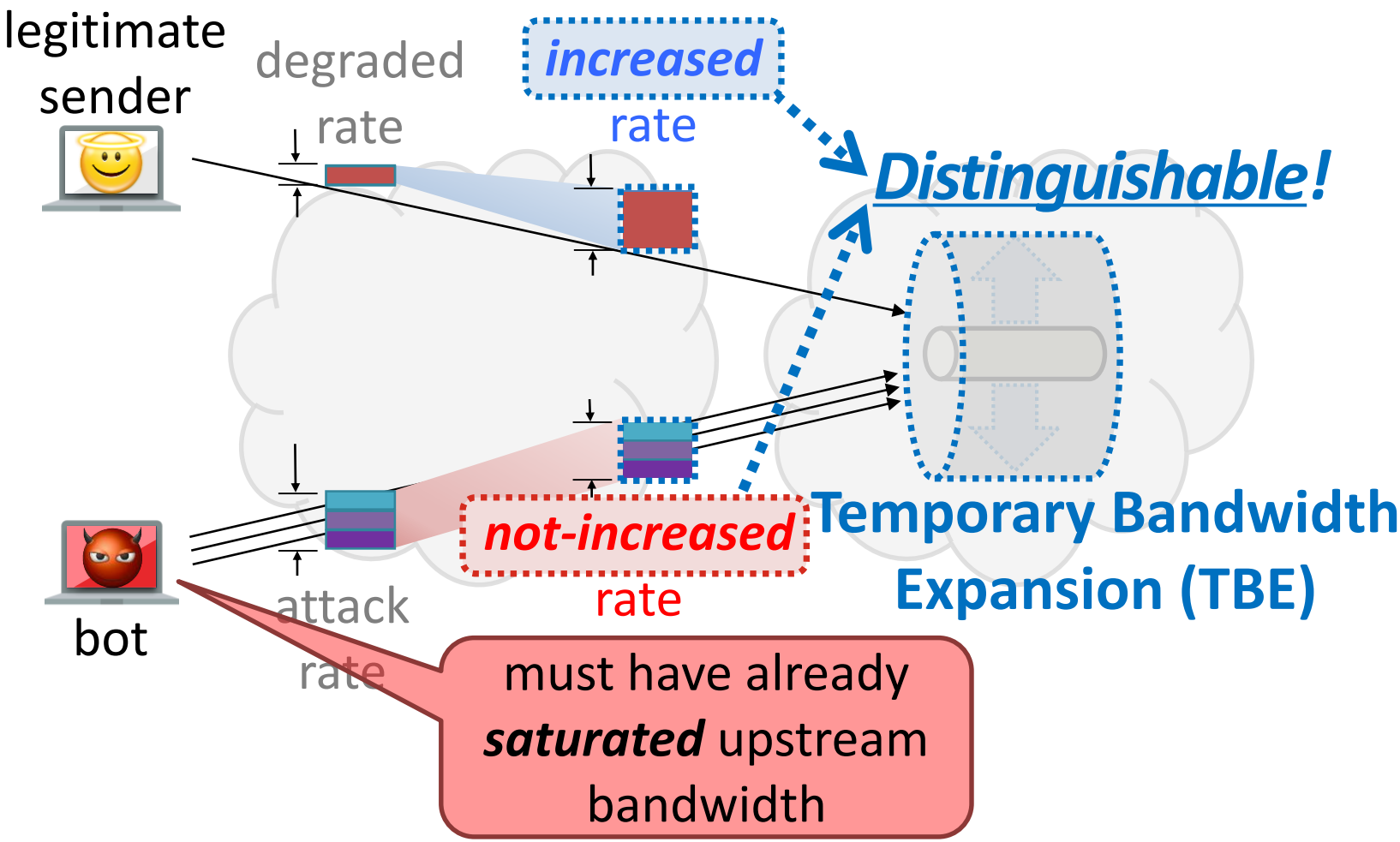
Cost-detectability tradeoffs based on bot detection

SPIFFY: system design for ISP networks

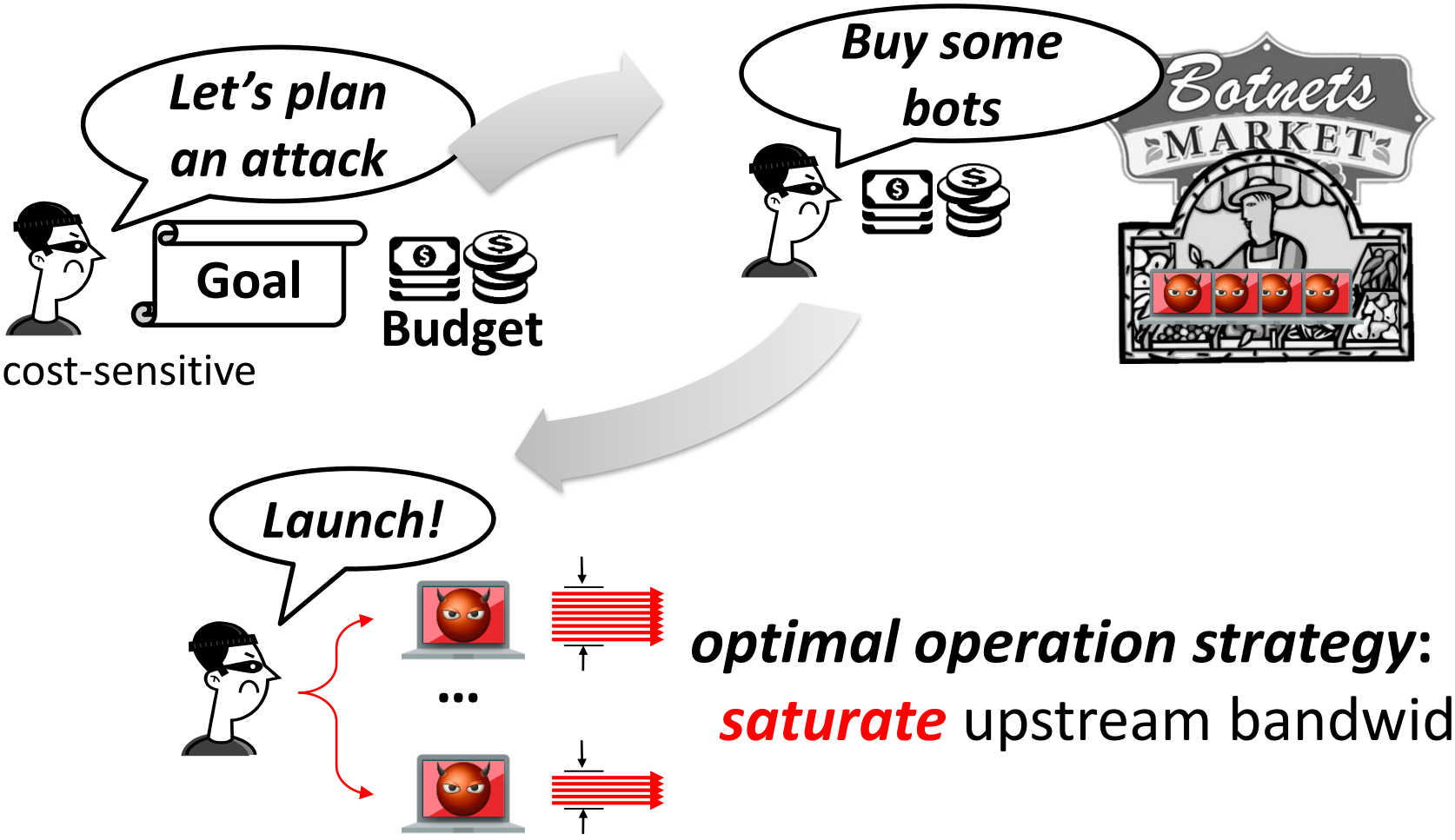
SPIFFY's *bot detection* mechanism



SPIFFY's *bot detection* mechanism

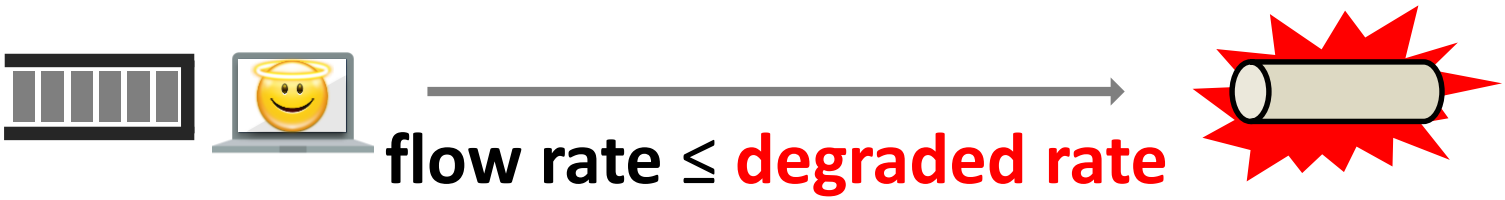


Why bots are supposed to be ***saturated***?

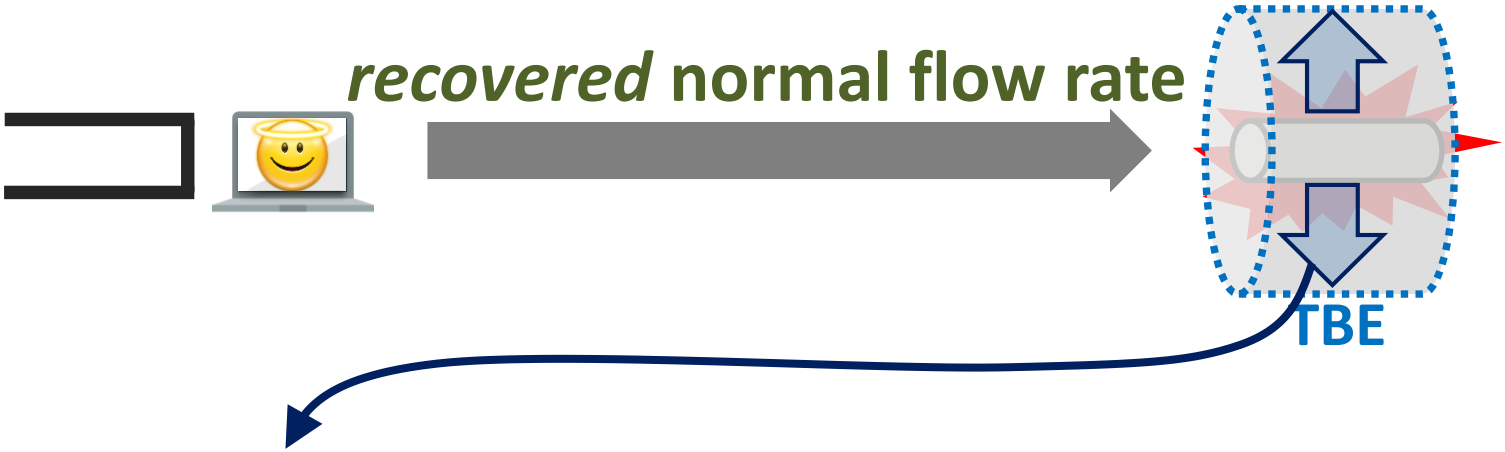


optimal operation strategy:
saturate upstream bandwidth

Why legitimate senders would ***increase rates*** in response to TBE?



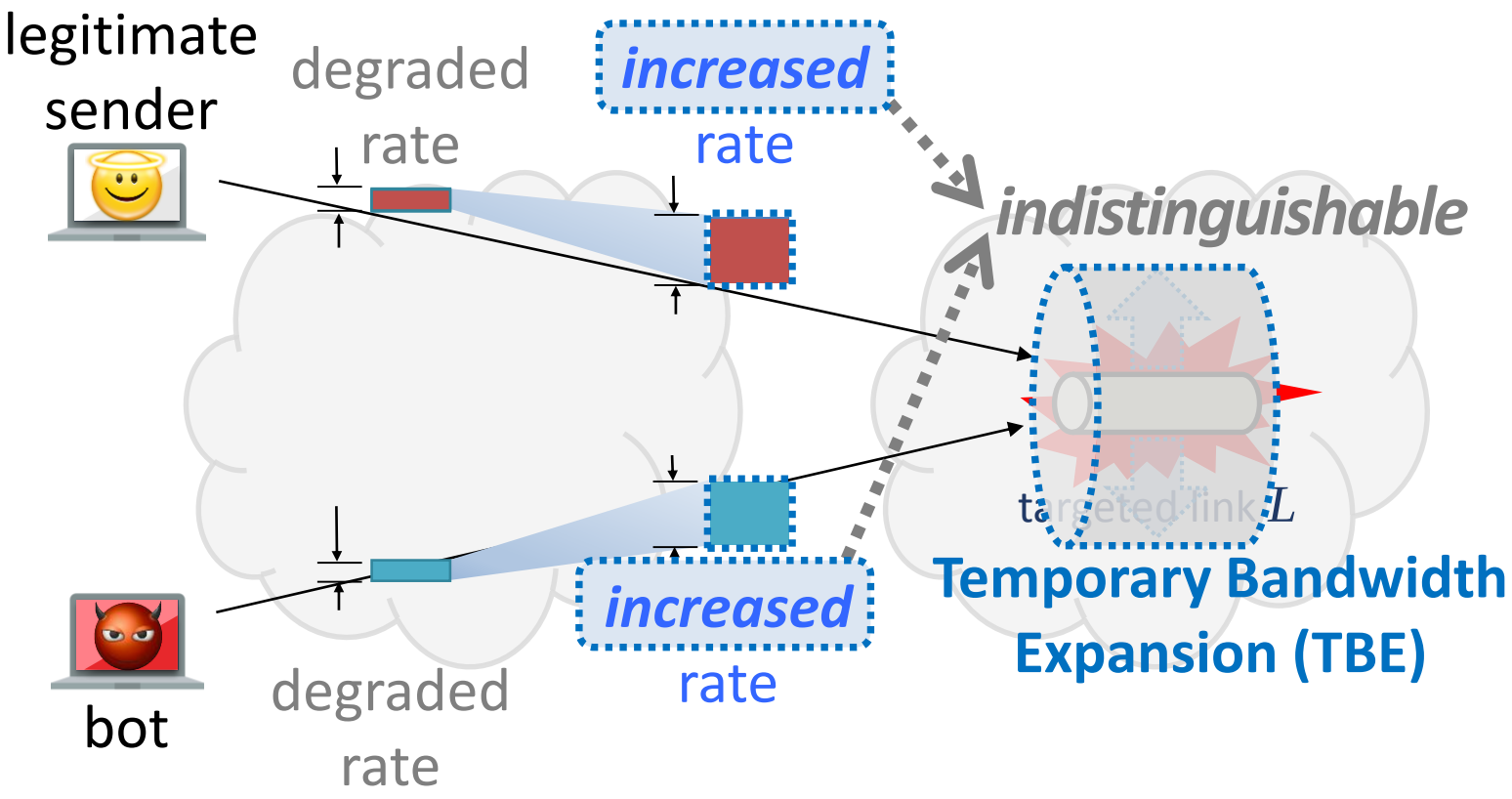
Why legitimate senders would ***increase rates*** in response to TBE?



$$\mathbf{BEF_{ideal}} = \frac{\textbf{(guaranteed) normal rate}}{\textbf{degraded rate}}$$

(*Ideal* Bandwidth Expansion Factor)

Bot detection *circumvention* => highly *increased attack cost*

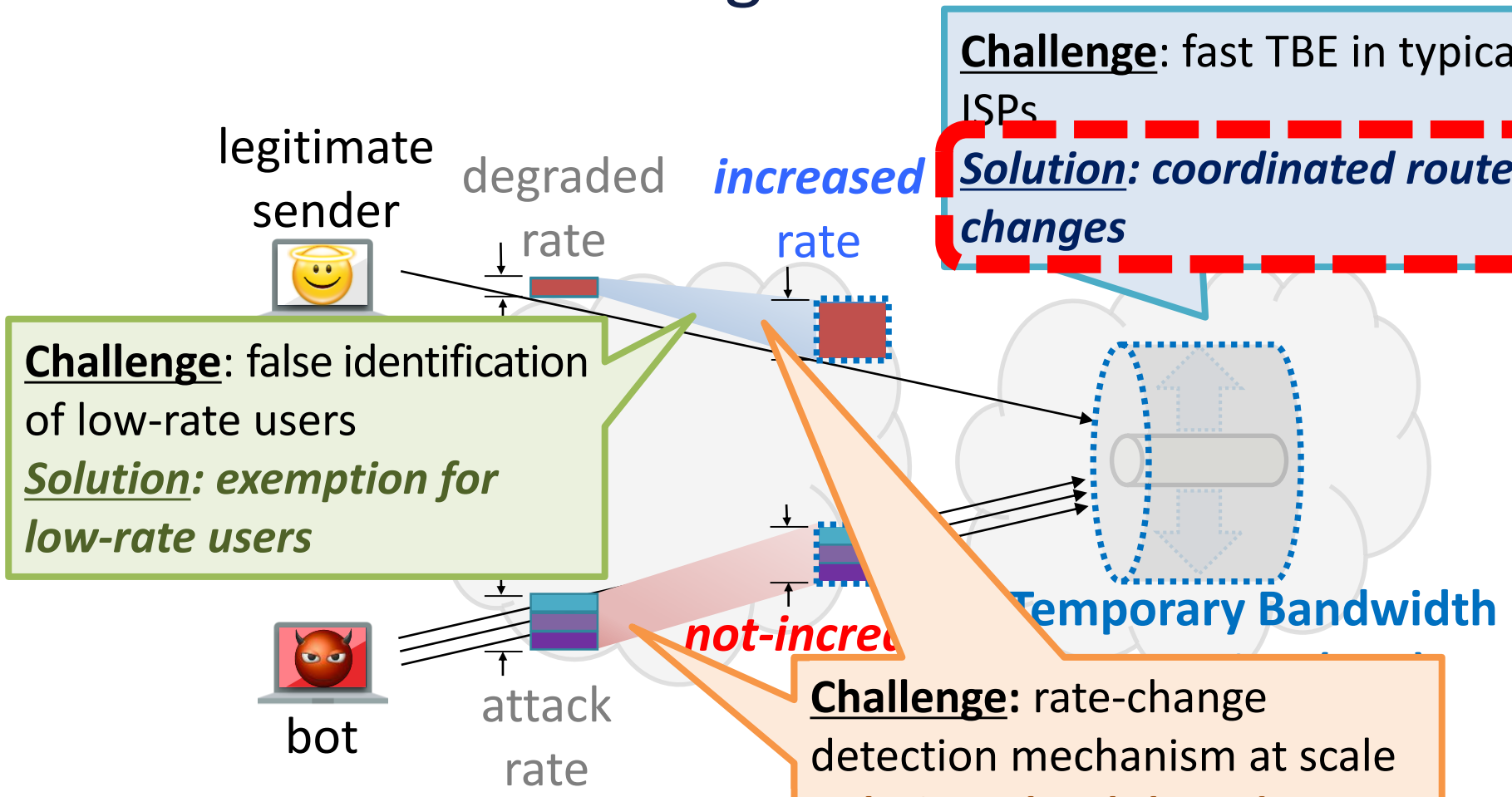


Bot detection *circumvention* => highly *increased attack cost*

Strategy => massive reduction of bots' *bandwidth utilization*
=> ***massive increase** in **the number of required bots***
(by a factor of BEF_{ideal})

SPIFFY forces unpleasant ***tradeoff***:
(1) ***undetectability*** but at highly increased cost;
(2) ***low cost*** but easily detectable

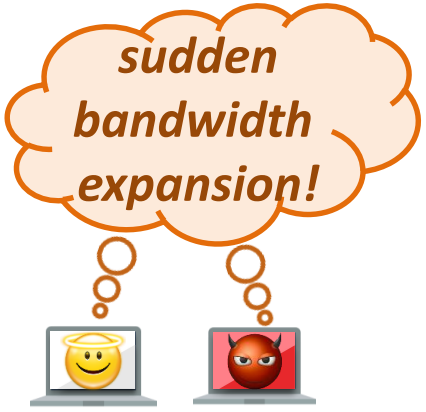
SPIFFY challenges and solutions

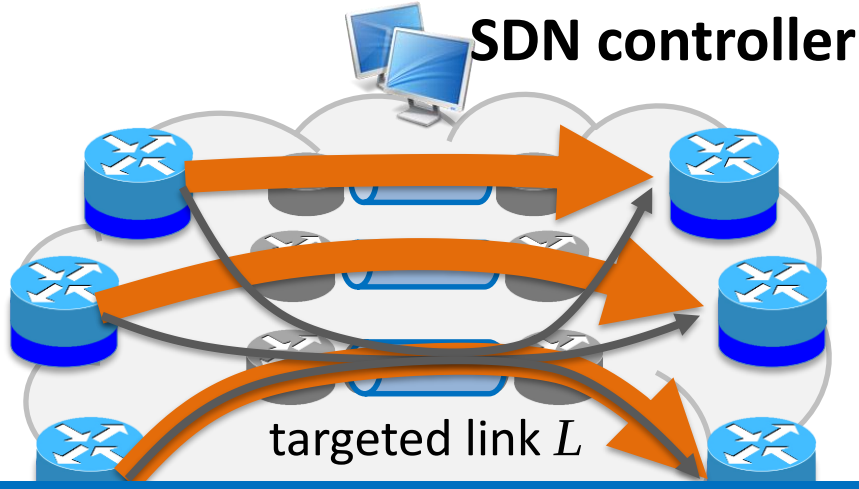


Design of temporary bandwidth expansion

Solution: coordinated, sudden ***route changes*** that handle large bandwidth expansion

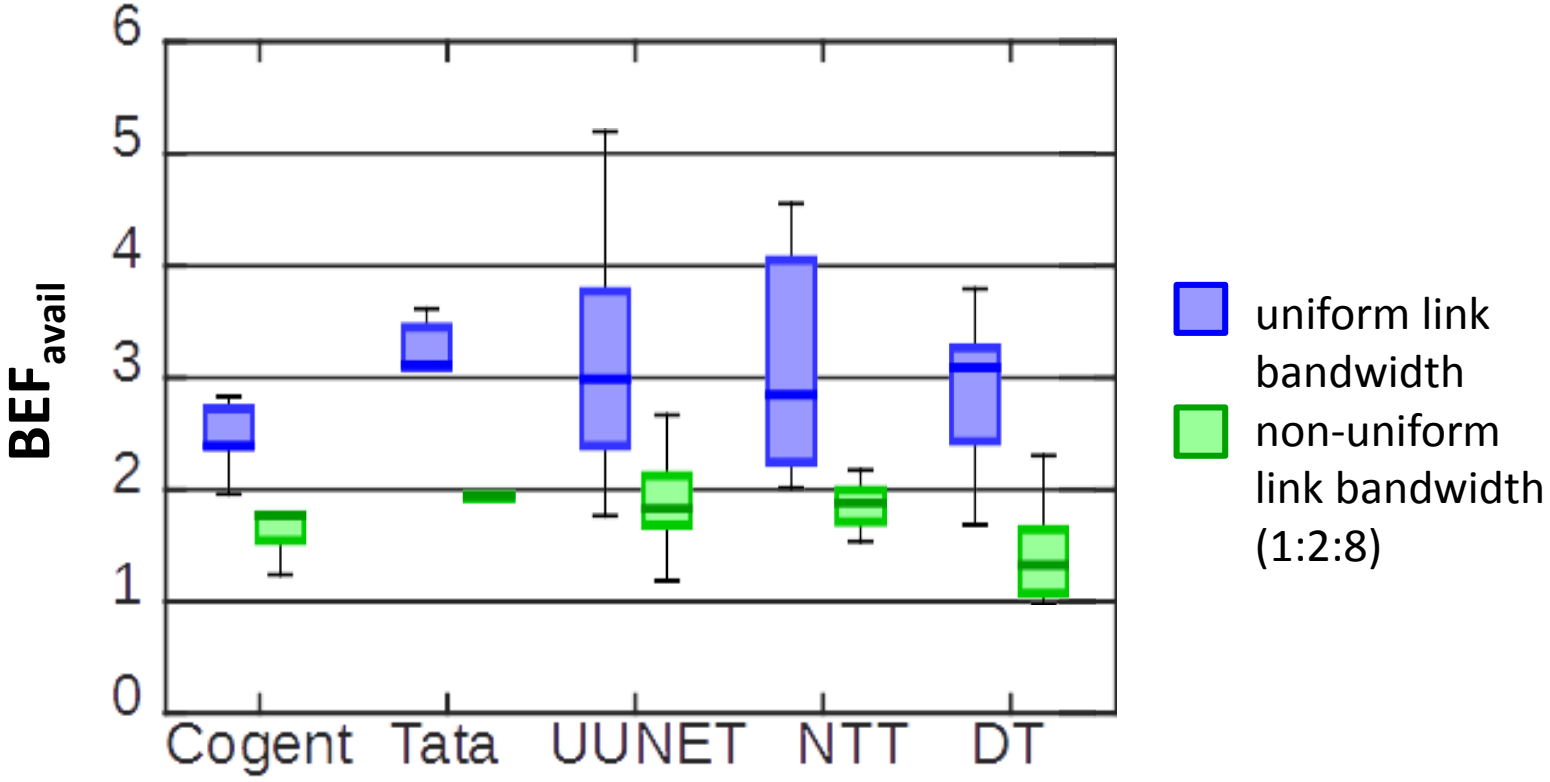
✓ **Software-defined networking (SDN)** provides *centralized control* and *traffic visibility*





Linear programming formulation:
We find the ***maximum available bandwidth expansion factor*** (***BEF_{avail}***) and ***new routes*** for a ***target link*** and a ***given network topology***

Maximum available bandwidth expansion factor (BEF_{avail}) for 5 ISP networks

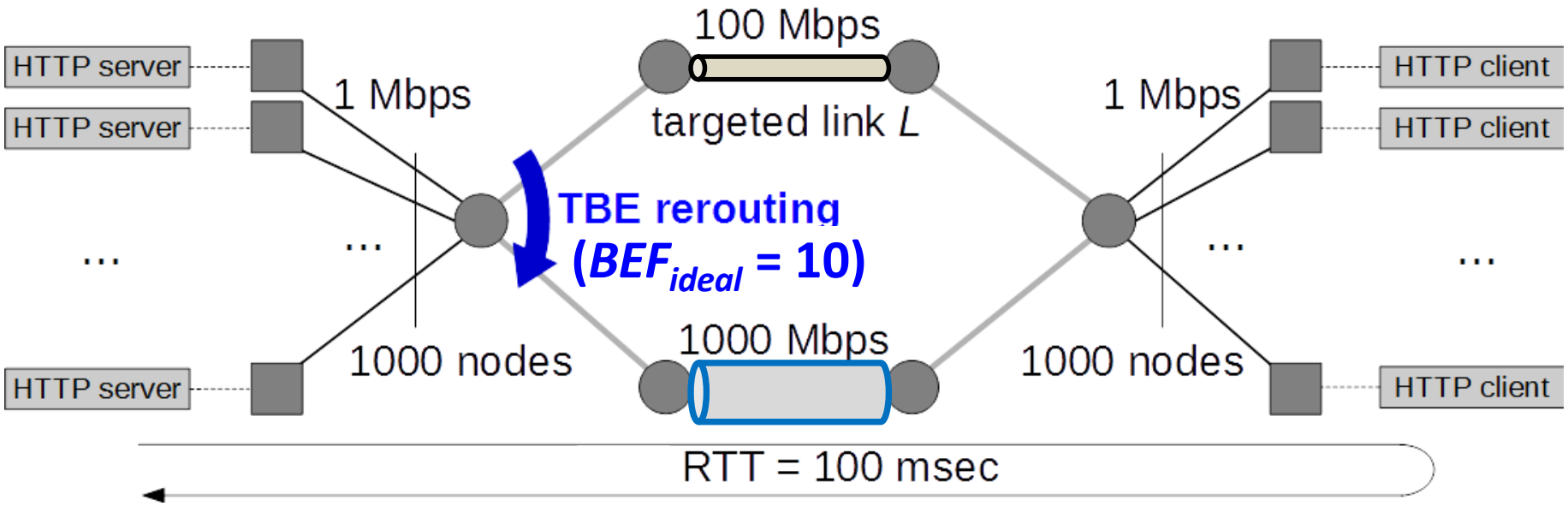


How to implement ***TBE with large BEF_{ideal}*** *when* ***BEF_{avail} < BEF_{ideal}***?

- ✓ **randomized sequential TBE:** we sequentially test only a random subset of senders at each TBE, providing them the ideal bandwidth expansion factor ***BEF_{ideal}***

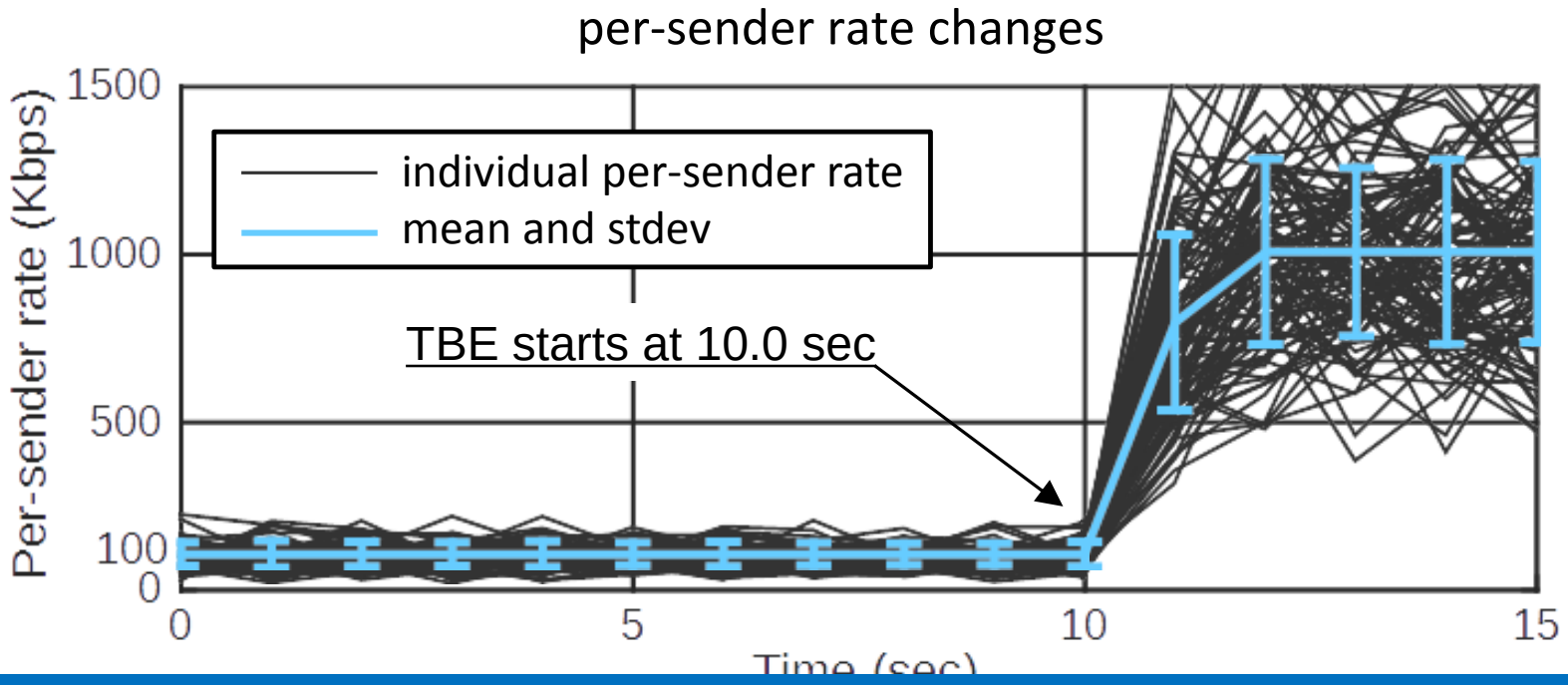
Simulation for rate change behaviors

Topology



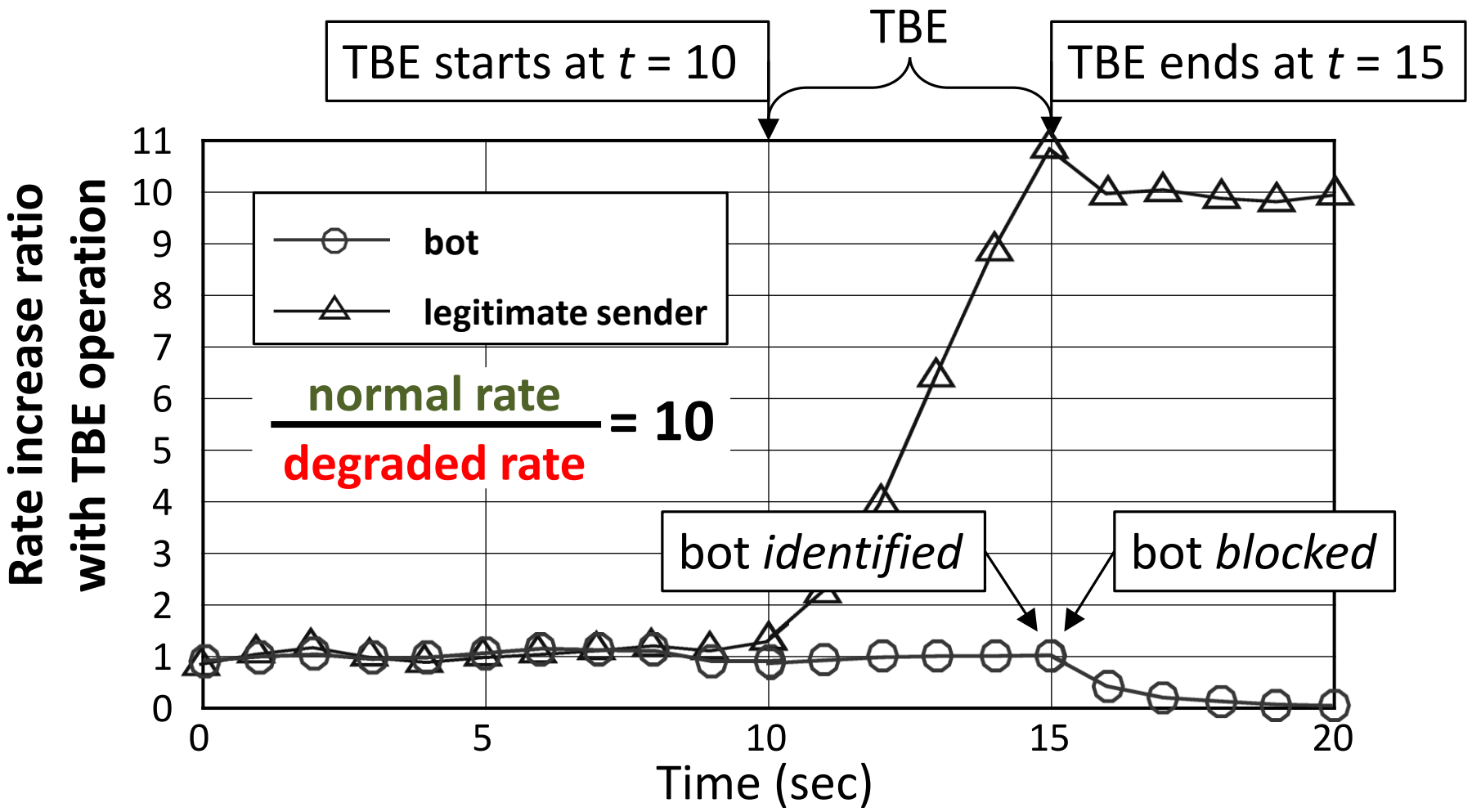
*ns*2 simulator with HTTP traffic generator (PackMime)

Simulation for rate change behaviors



- ✓ Large rate-change ratio can be quickly measured (e.g., < 5 sec)
- ✓ ***Robust rate change behavior*** of legitimate senders in various environments (e.g., TCP variants, RTT changes, short flows)

Rate-increase ratios of bot and legitimate sender in SDN testbed



Conclusion

- **First-line of defense** for **indistinguishable** link-flooding attacks
  - **Attack deterrence** of **rational** adversaries
  - **Cheaper/easier** than **inter-ISP coordination** based defenses

- **SPIFFY: system design for cost-detectability tradeoffs**
  - Practical **bot detection** mechanism for large ISPs
  - **SDN-based** design for temporary bandwidth expansion

Thank you

minsukkang@cmu.edu