

# DoS Prevention in Shared Channels

Carl A. Gunter and Jose Meseguer, University of Illinois Urbana-Champaign  
Sanjeev Khanna and Santosh Venkatesh, University of Pennsylvania



## Denial of Service Protection

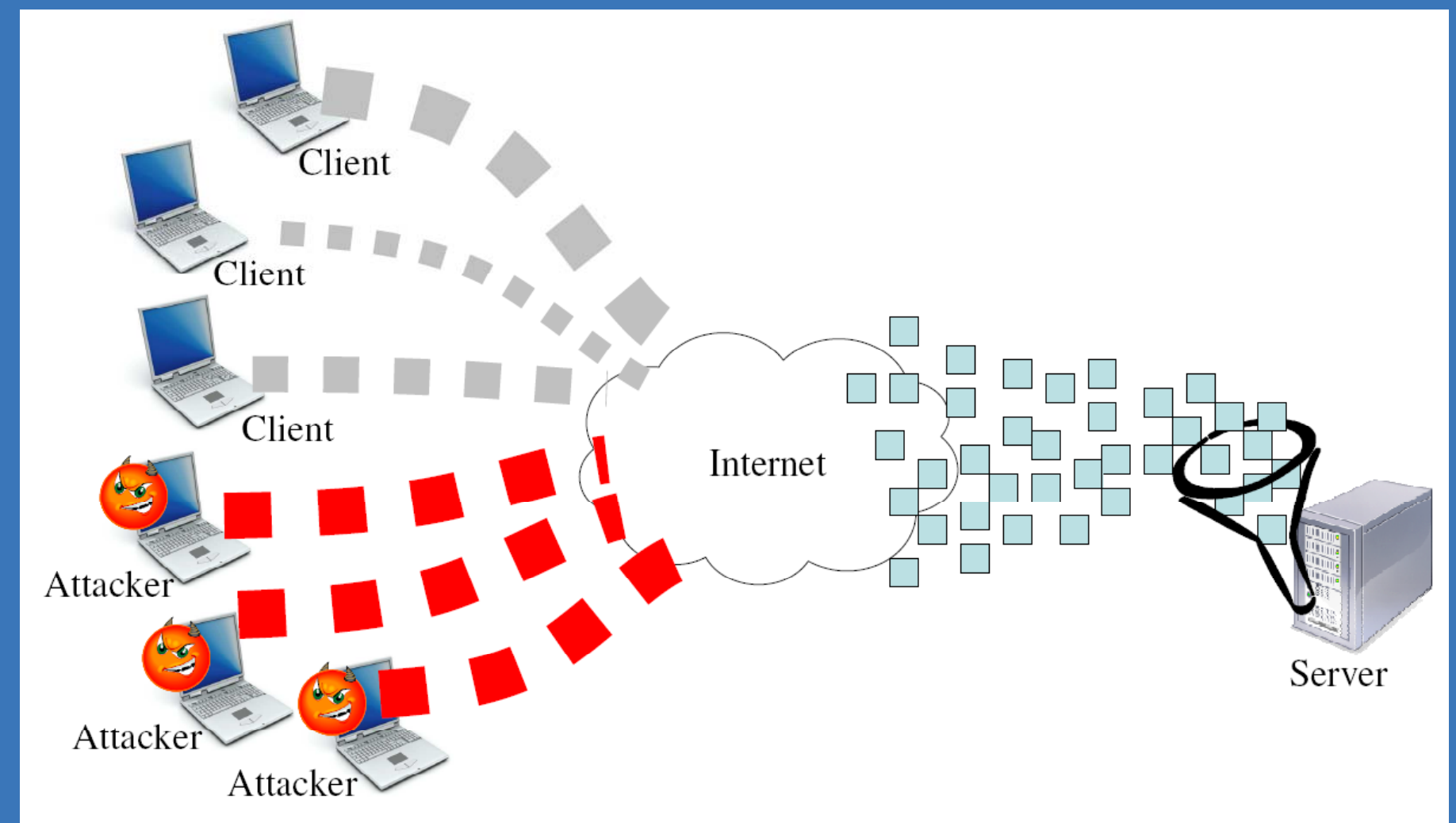
- We consider attacks that aim to deplete scarce resources of servers by generating illegitimate requests from one or many compromised hosts
- Potential attack targets: IKE key exchanges, digitally signed DNS, large file retrievals from web servers, computationally expensive query processing at database front-ends, *etc.*
- **Currency-based** defense mechanisms demand a payment (e.g. CPU cycles)
- Bandwidth as payment:
  - Selective verification (Gunter *et al.* '04): no adaptation mechanism
  - Bandwidth auctions (Walfish *et al.* '06): requires significant server state

## Adaptive Selective Verification (ASV)

- Research question:
  1. Is there an **adaptive** and **stateless** bandwidth-based defense mechanism?
  2. How to measure and control trade-offs?
- Our approach summary:
  - Shared channel model: attack rates are bounded; client rates vary within fixed bounds
  - Clients respond to an attack by boosting request rates
  - Server performs probabilistic random sampling
  - Theoretically and experimentally shown to be efficient in terms of bandwidth consumption
  - Requires limited state on the server

## Adaptation

- When should defense mechanism trigger?
- How should they be tuned?
- What are the trade-offs?
- Two possibilities for mechanisms:
  - Protection is intrinsic or has no cost (e.g. IPSec, SYN Cookies)
  - Protection has costs (e.g. client puzzles)
    - Need to control trade-offs
    - Need adaptation strategy



## Approach and Impact

### New approach

- Adaptive
- Stateless
- Bandwidth efficient

### Research Impact

- Advances bandwidth payment
- Underscores adaptation in DoS defense
- Introduces novel DoS analysis techniques

## Adaptive and Omniscient Protocols

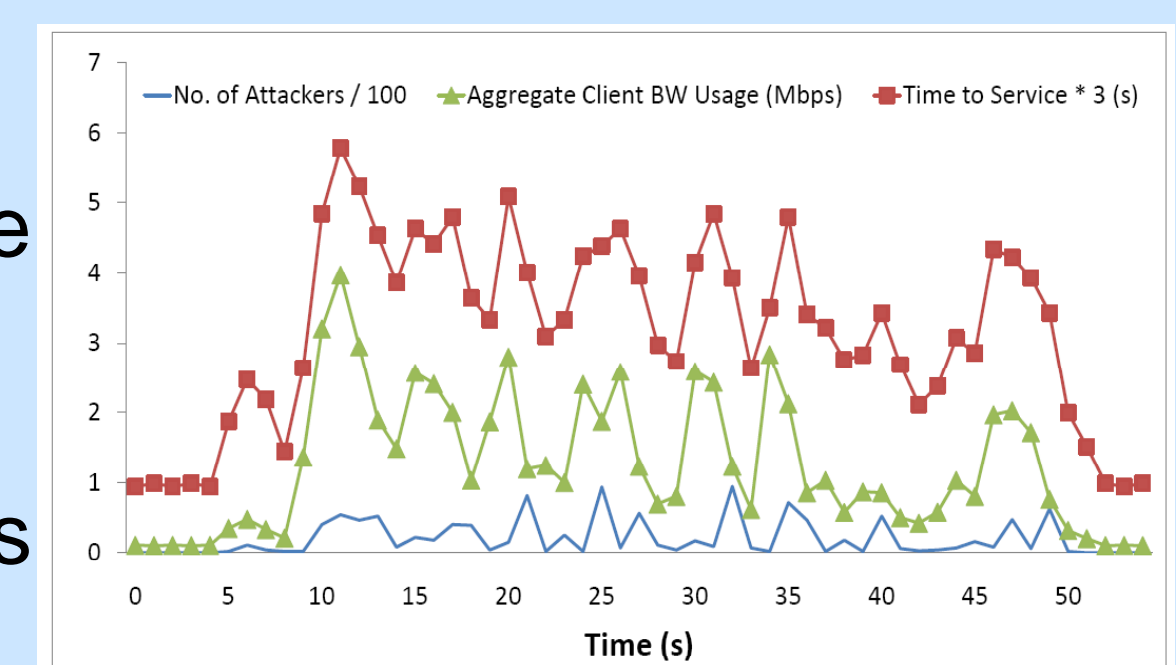
- Max client rate:  $\rho_{\max}$ , Max attack rate:  $\alpha_{\max}$
- Server processing rate  $S$ :  $\rho_{\max} \ll S \ll \alpha_{\max}$
- Clients double request rates after not getting service in one round ( $T$  sec.) for up to  $J$  rounds
- $J$  is the *retrial span*:  $\left\lceil \log\left(\frac{\alpha_{\max}}{\rho_{\max}}\right) / \log(2) \right\rceil$
- Server performs reservoir-based random sampling to sample from a sequence of incoming packets using *bounded state*
- **Omniscient protocol**: Clients and server have global knowledge about attack
- Measures for performance: success probability of each client and total bandwidth consumed by clients

## Analysis and Simulation Results

- Novel and intricate theoretical analysis shows that ASV closely approximates the performance of omniscient protocol
- Ratio of bandwidth consumption of the adaptive protocol to omniscient protocol:

$$O\left(\log(\alpha_{\max}) / \log\left(\frac{1}{\rho_{\max}}\right)\right)$$

- Extensive NS-2 simulations validate theoretical results and show how *quickly* ASV adjusts to attacks



Reference: Adaptive Selective Verification, Khanna, Venkatesh, Fatemeh, Khan, and Gunter, INFOCOM '08.

Learn more: Google "UIUC DoS Models"