

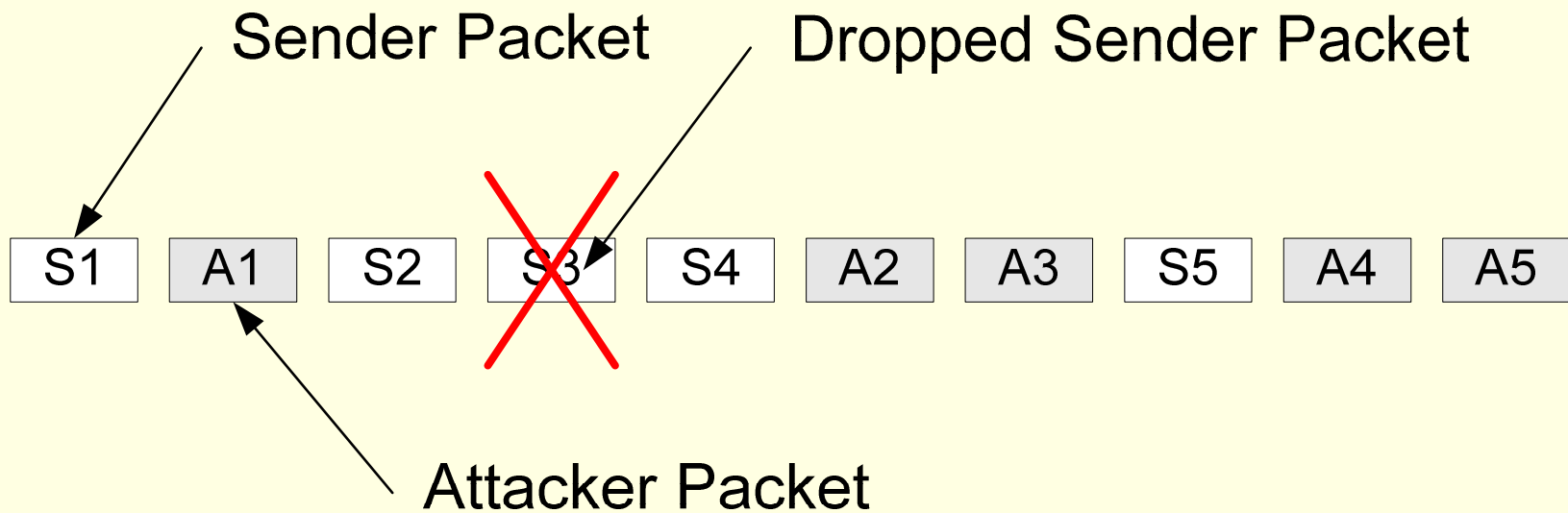
Shared Channel Model

- Adversary can replay and insert packets.
- Legitimate sender sends packets with a maximum and minimum bandwidth.
- Legitimate sender experiences loss, but not deliberate modification.
- Model is a four-tuple (W_0, W_1, A, p) .
 - W_0, W_1 min and max sender b/w
 - A attacker max b/w
 - p loss rate of sender

Probabilistic Techniques for DoS Models

- Work on probabilistic techniques is also being done at Penn by Gunter's group.
- The work provides for a model, the shared channel model, and techniques for DoS protection that it can analyze, viz. selective sequential verification.
- Possible future work: integrate probabilistic rewriting system with this work.

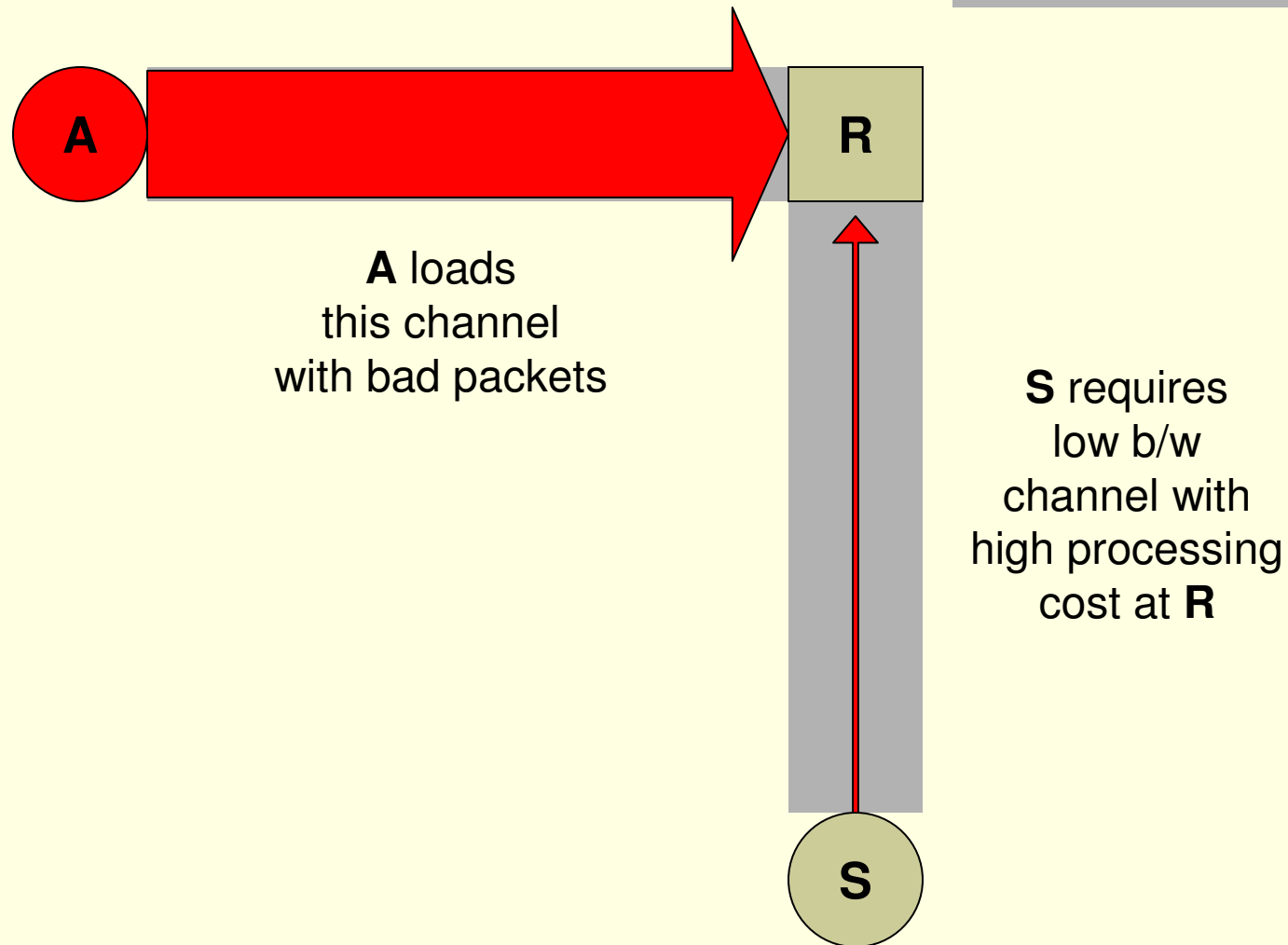
Shared Channel Model Example



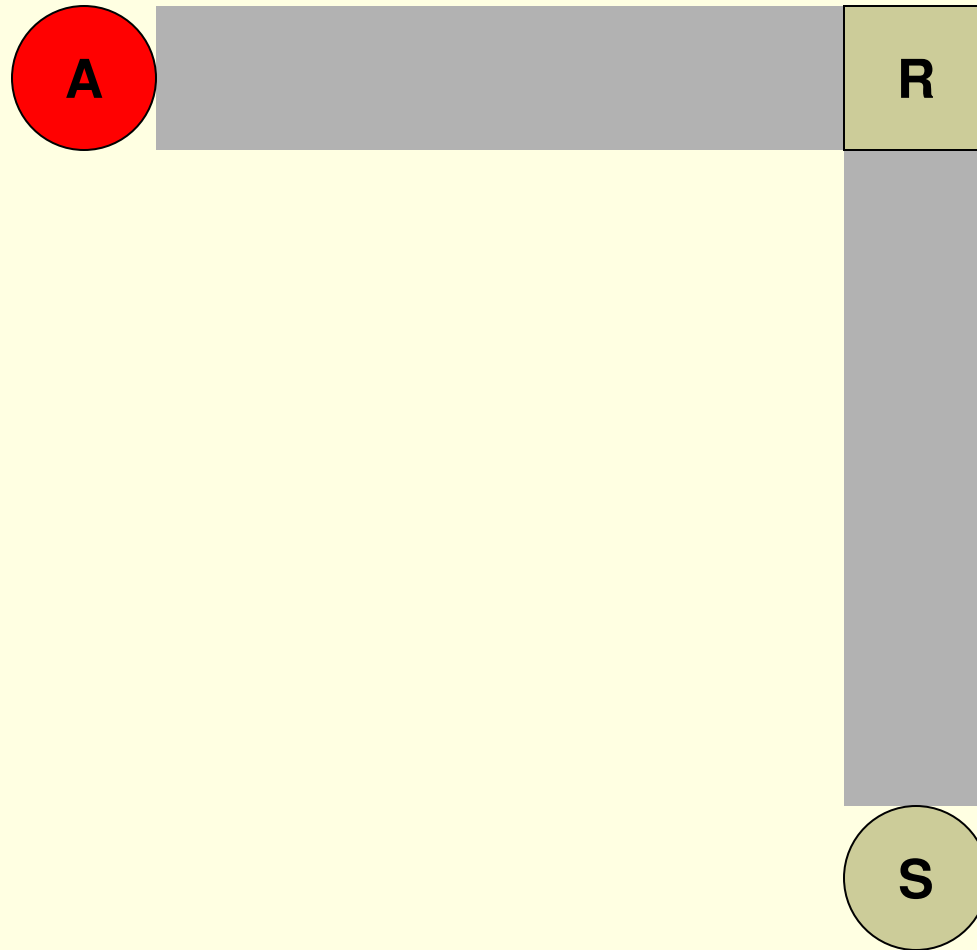
Selective Sequential Verification

- Channels can be protected from DoS by the use of probabilistic techniques.
- Sample countermeasure for signature floods in authenticated broadcast:
 - Valid sender sends multiple copies of the signature packet.
 - receiver checks each incoming signature packet with some probability (say, 25% or 1%).

Attack Profile

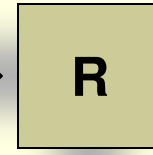
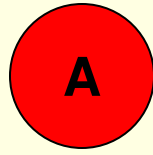


Selective Verification

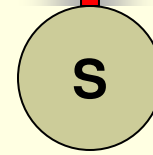


Selective Verification

A gets
reduced
channel



R makes
channels
lossy



S adds
redundancy

**Tradeoff:
bandwidth vs. processing**