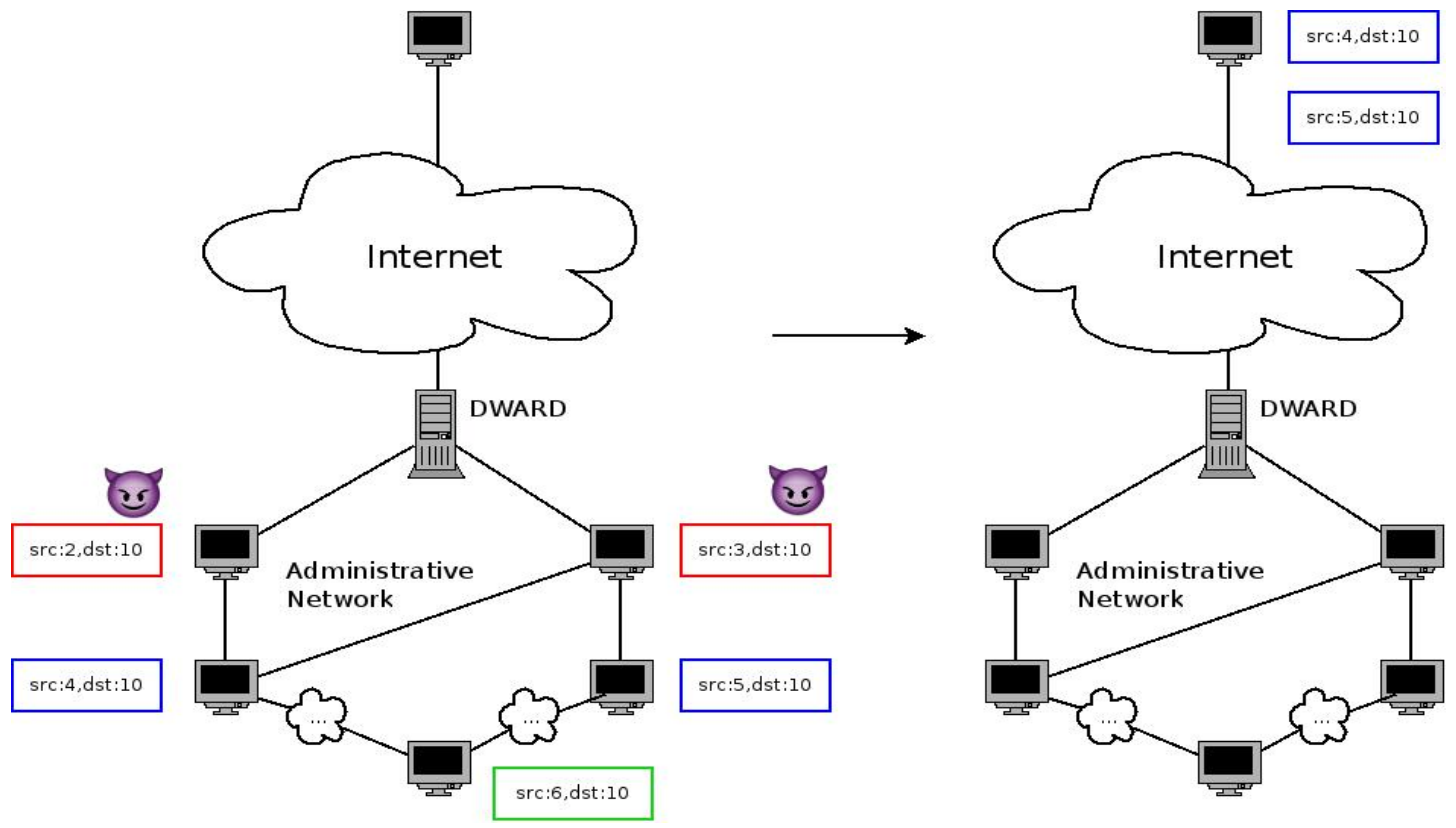
# Modifying Classic Source-End DDoS Defense for IoT Environments

Sam Mergendahl

## Motivation

- The number of connected IoT devices is projected to be near 50 billion by 2020.
- A home network is now becoming topologically similar to an administrative network.
- Typical source end defense solutions are deployed at the border gateway router in the administrative network.
- Instead of reinventing the wheel, maybe these solutions could be deployed at the home border router.

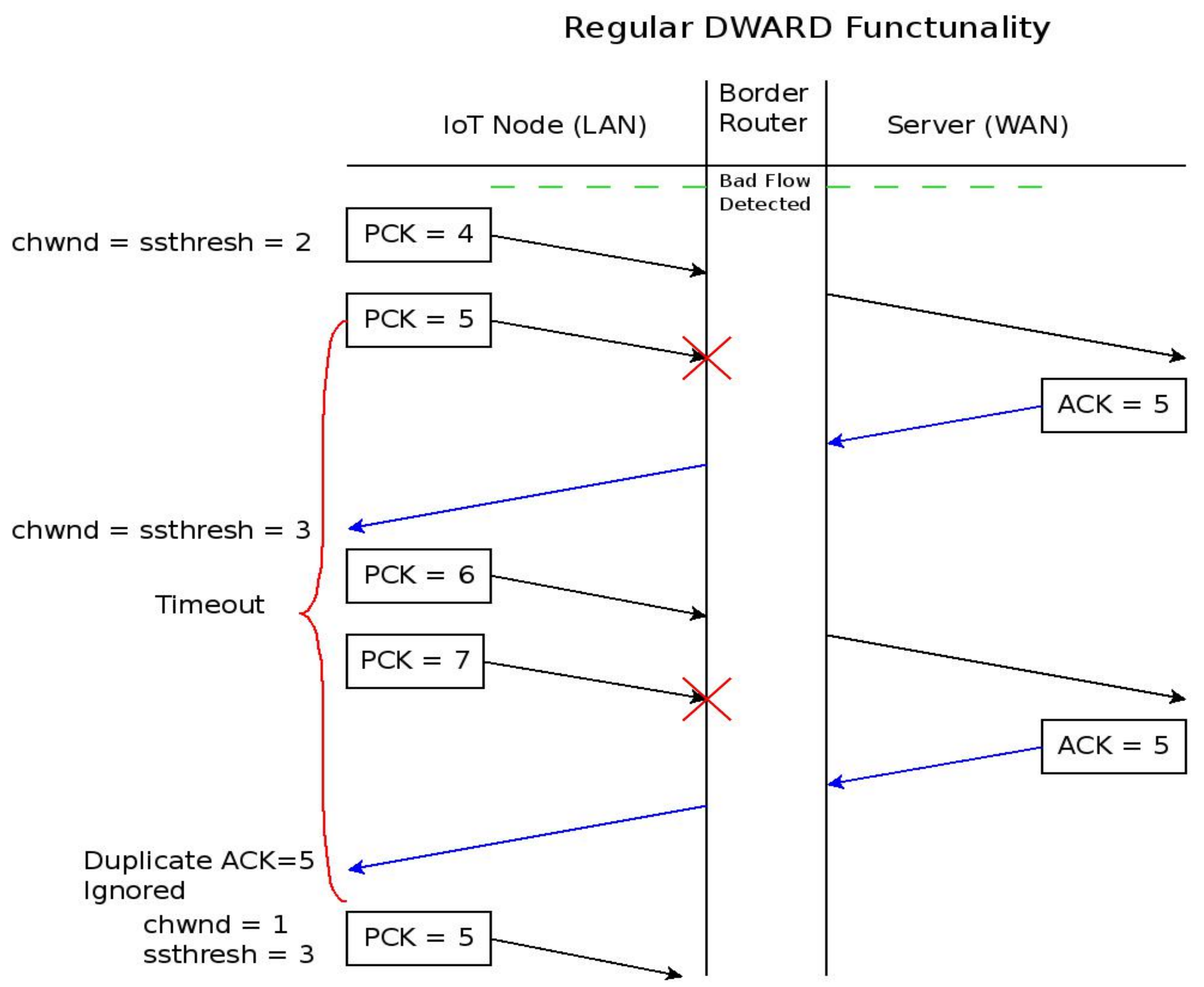
## DWARD

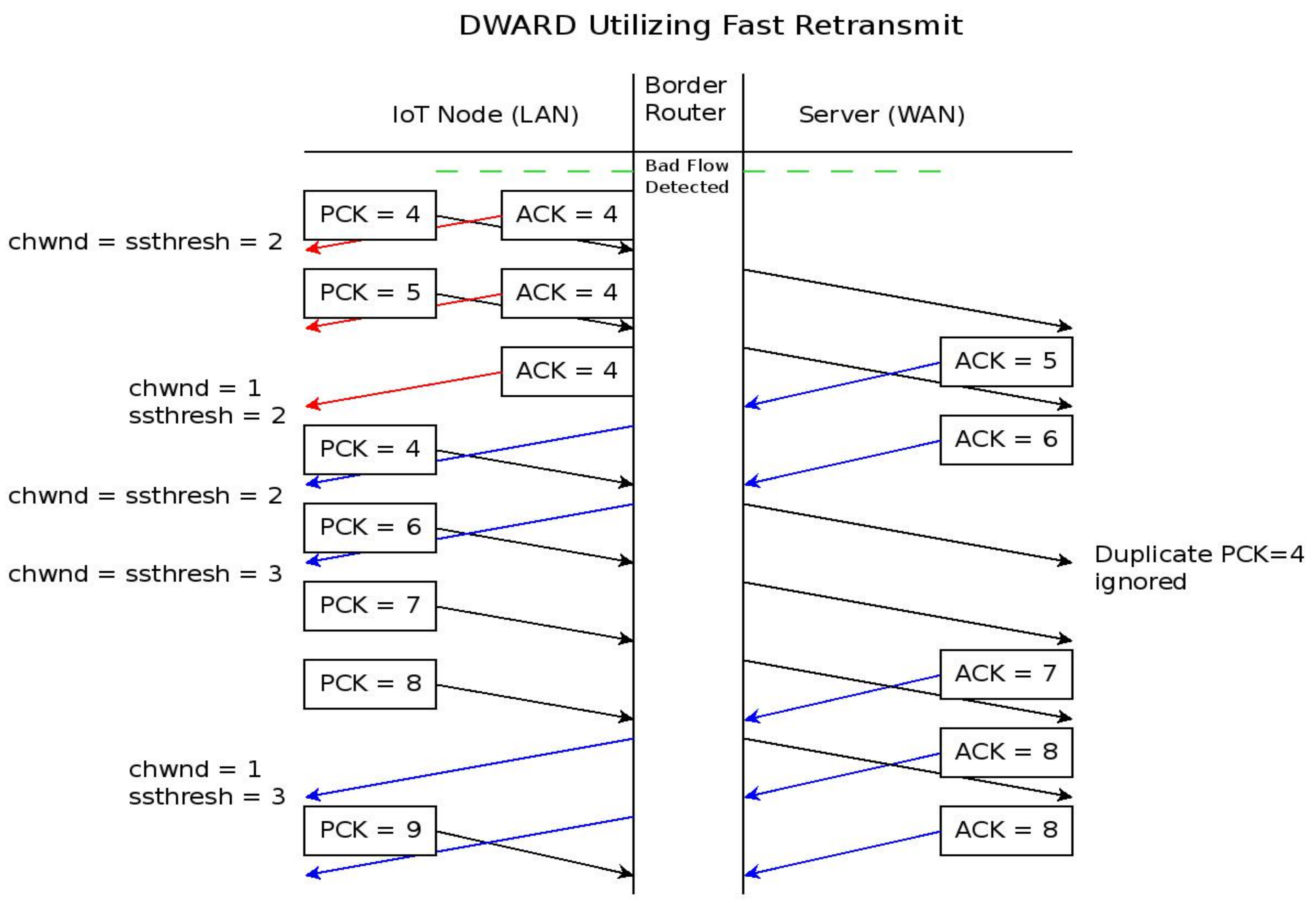


- DWARD filters out both bad connections (red) and the transient connections (green) increasing the possibility benign packet loss.

- Source end DDoS defense deployed at administrative gateway router.
- When a flow is labeled as an attack, DWARD throttles all bad and transient connections.
- Monitors connection to make sure source is following TCP congestion control.
- Need to cut back throttling transient traffic that is actually benign.
- Use TCP Fast Retransmit instead of timeout to test for good connection.

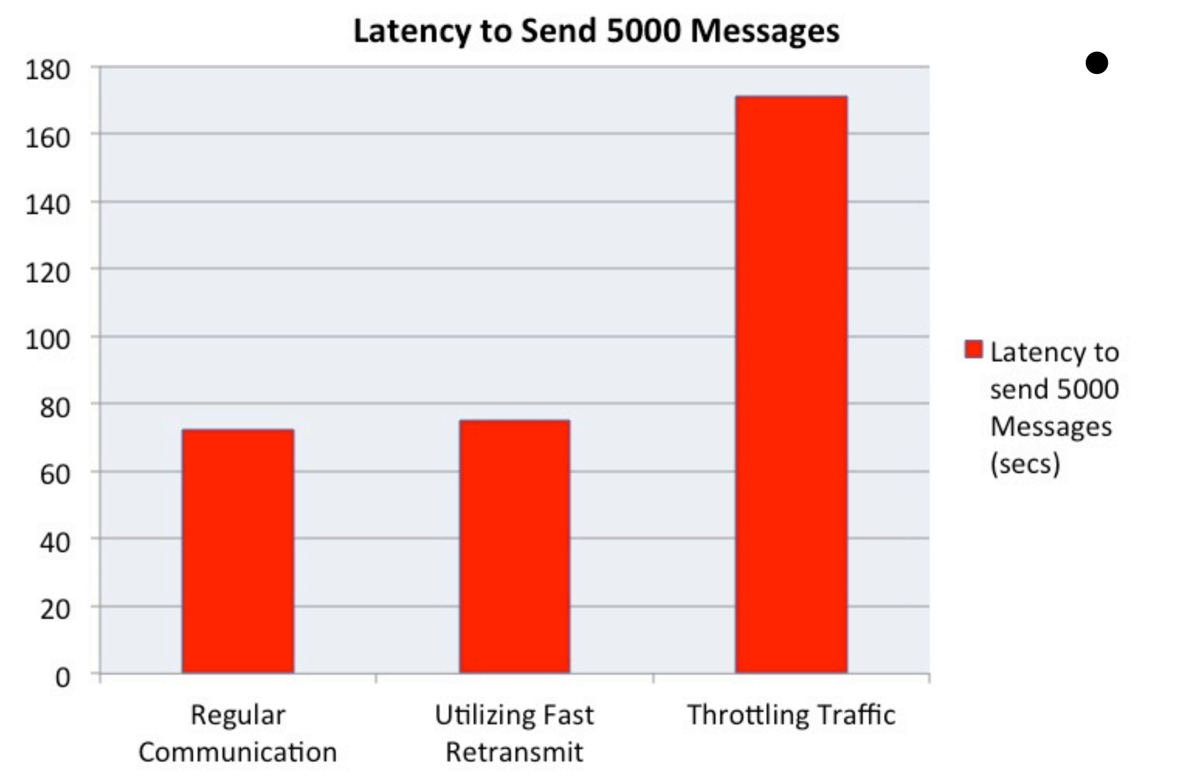
## Utilizing TCP Fast Retransmit

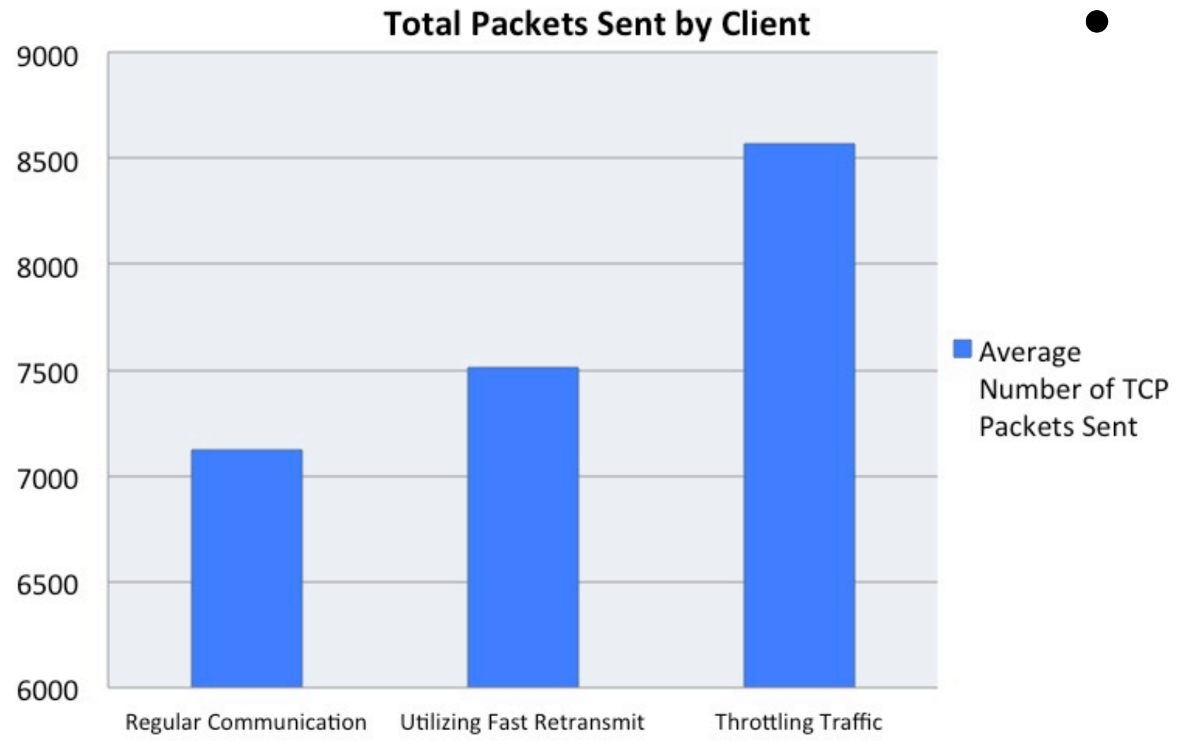




- If a benign sender receives three back-to-back ACK packets, they will follow congestion control and cut their sending rate in half.
- If there is no congestion control response, the connection can be assumed to be an attack connection.

## Results





- Using a Macbook Pro as a wireless router, the client and server opened a TCP connection and proceeded to send 5000 MTU messages.
- The graphs on the left represent the time to completely send all 5000 messages and the number of overall packets sent.