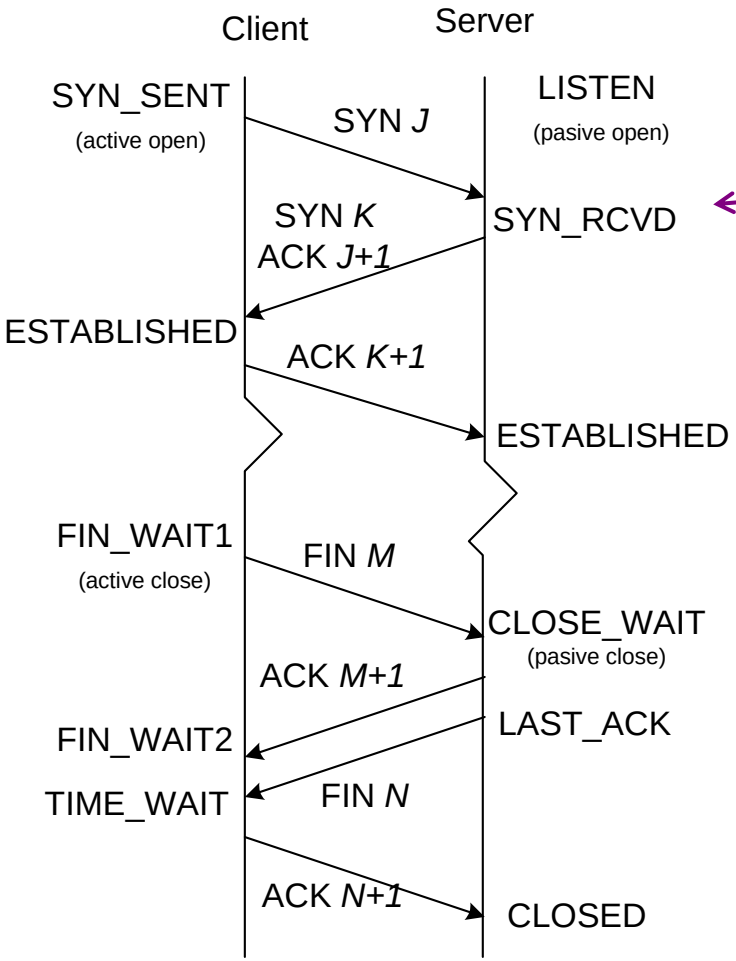
清華大學 Tsinghua University

A Novel Router-based Scheme to Mitigate SYN Flooding DDoS Attacks

Changhua Sun, Jindou Fan, Lei Shi, Bin Liu
Department of Computer Science and Technology, Tsinghua University, China

http://s-router.cs.tsinghua.edu.cn/~sunchanghua

What is SYN floods?



TCP three-way handshake

- In SYN_RCVD, the server allocates resources
- Then if the client does not send the final ACK, the server's resources can be easily exhausted → SYN Flood occurs

Defend SYN Floods

- SYN Cache
  - allocate minimal state in SYN_RCVD
  - allocate all the resources in ESTABLISHED
  - remove oldest entry when backlog is full
- SYN Cookie
  - allocate no state for half-open connections
  - encode most of states and encrypt them into the seq. no in SYN/ACK packet
  - reconstruct state from seq. no. of the last ACK

Problems of SYN Cookie

- not able to encode all TCP options
- never retransmit unacknowledged SYN/ACK packet

SYN Cache & Cookies

- Both do not handle application data piggybacked on the SYN segment
- not alleviate bandwidth exhaustion
- not decrease the normal traffic's delay resulting from SYN flooding

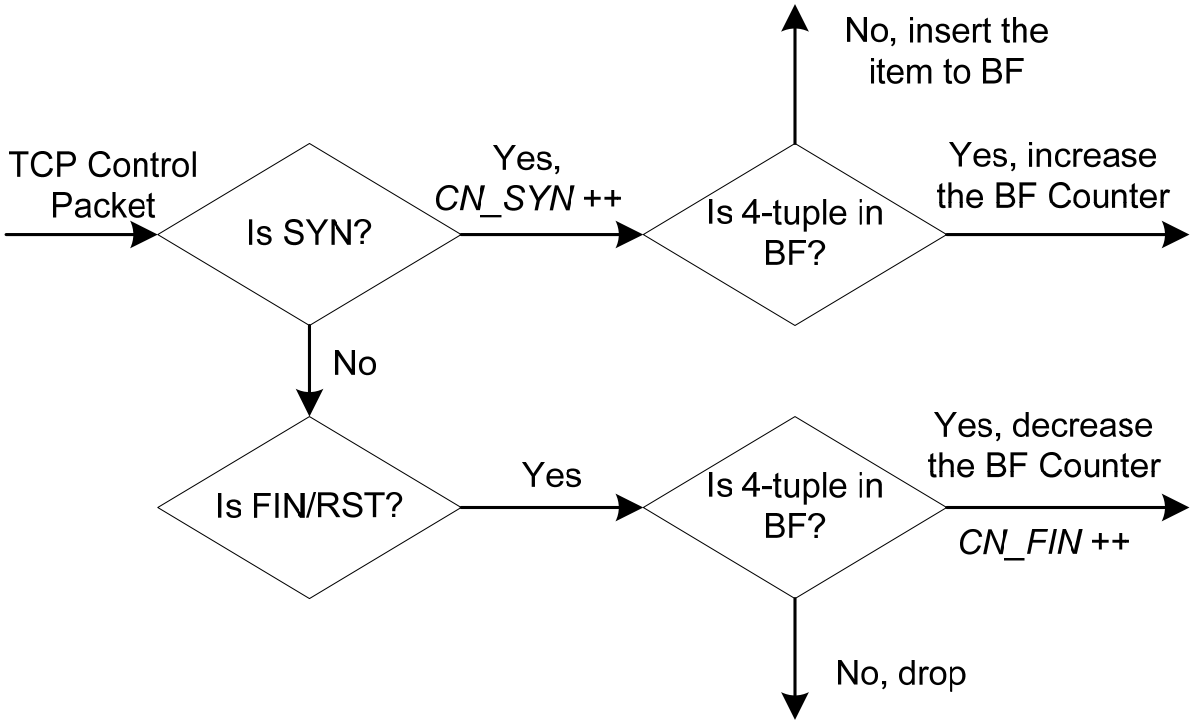
Router-based schemes

- Complementary
- Existing Schemes:
  - Wang et al. [3] based on SYN-FIN pairs
  - Al-Duwairi et al. [4] needs per TCP connection state

Our Scheme

- Router-based
- Two phases
  - detecting: inherent TCP valid SYN–FIN pairs behavior
  - mitigation: utilize the client's persistence
  - lightweight, stateless, but efficient and robust, and can be easily deployed

Detecting Scheme



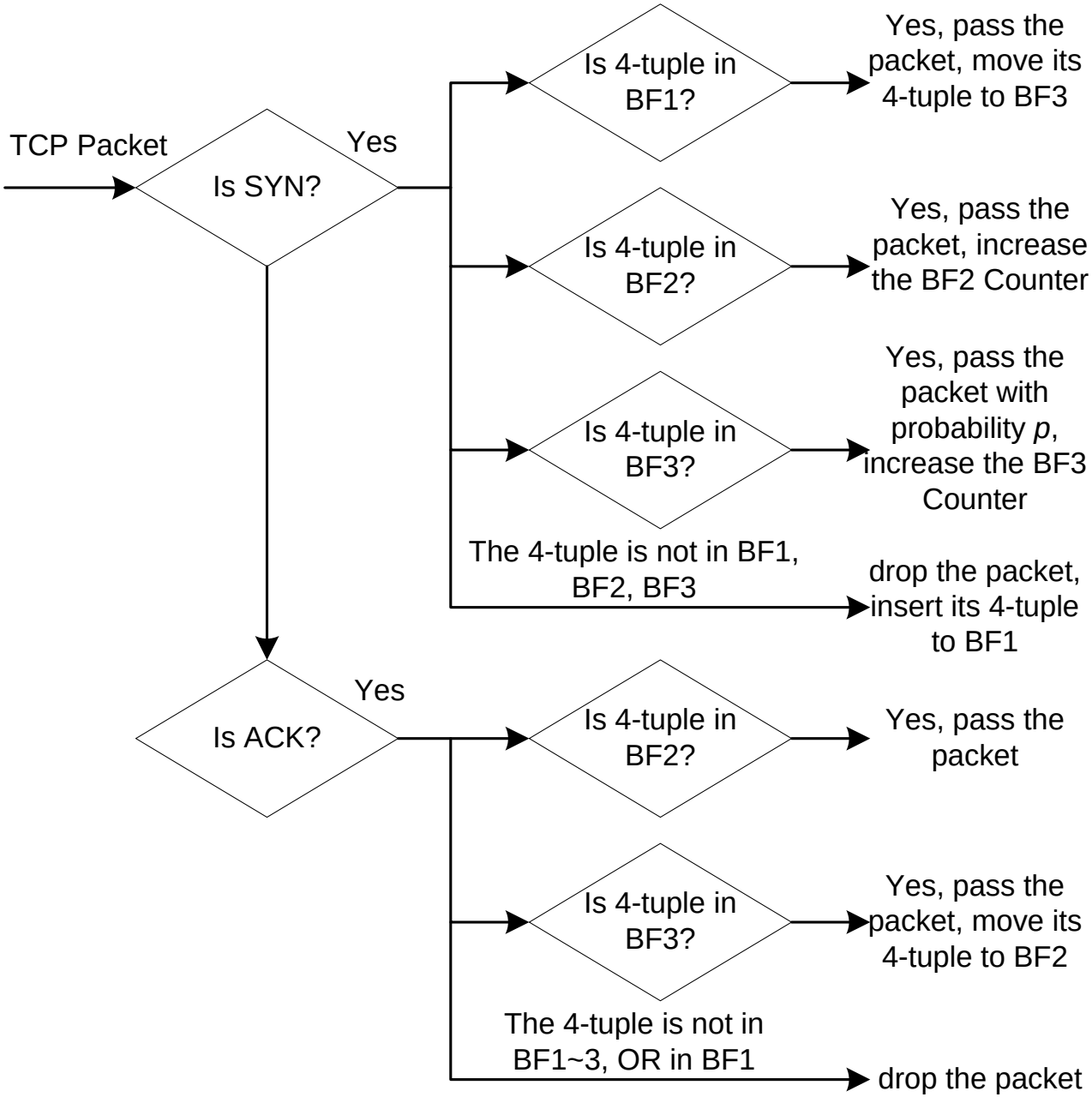
- Normally, a TCP connection begins with SYN, ends with FIN or RST;
- Attacker can avoid detection by sending a mixture FIN and SYN packets

- We use a counting Bloom Filter to count *void-FIN* packets

Mitigation Schemes

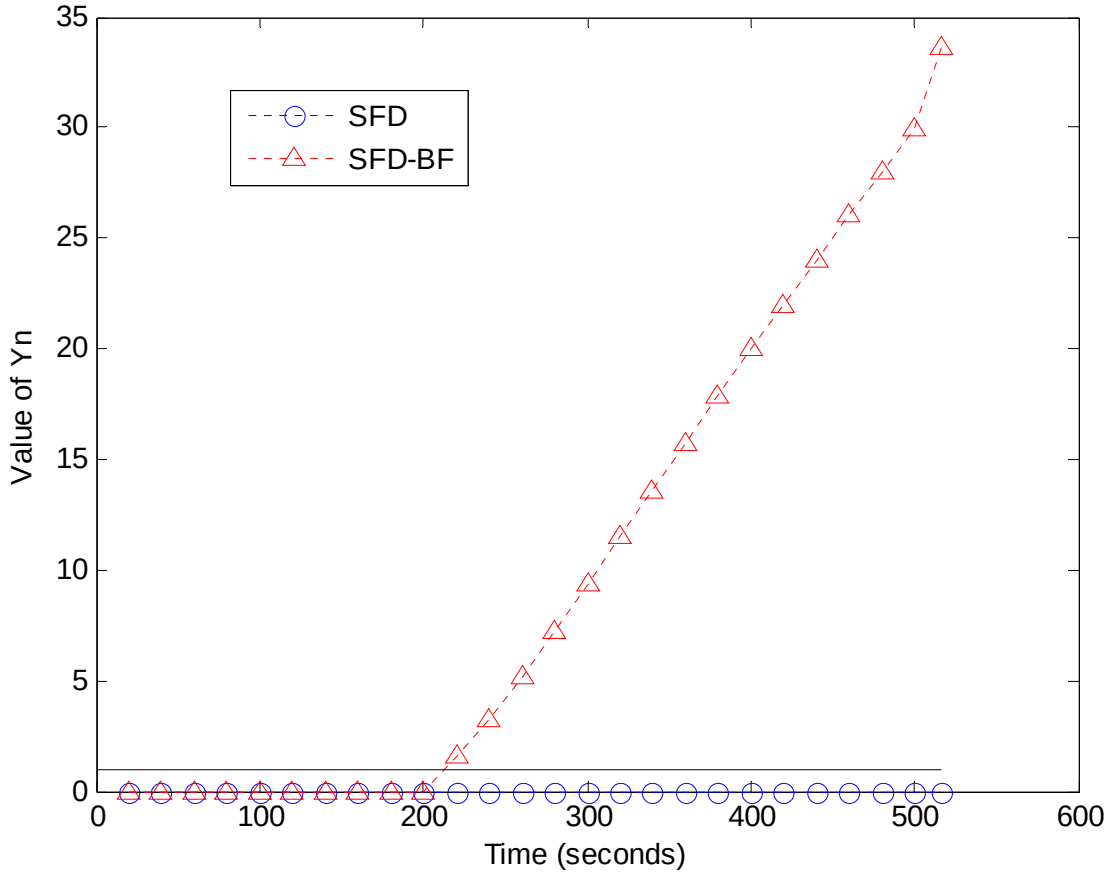
- Three counting Bloom filters are kept:

  - **BF-1**: to record the *4-tuple* of the first SYN packets of each connection;
  - **BF-2**: to record the *4-tuple* of SYN packets, whose connections have completed the three-way handshake;
  - **BF-3**: to record the *4-tuple* of other SYN packets.



- drop the first SYN packets when detecting SYN flooding
- drop other SYN packets with probability

Results with detecting scheme



- Based on real trace
- Add SYN flood attack traffic
- SFD-BF is our detecting scheme
- Yn > 1 indicates SYN flooding

Open Issues

- Evaluation the whole scheme in real Internet
- impacts on the performance of legit TCP connections
- More sophistic SYN flooding attacks
- On going work can be found:
  - http://s-router.cs.tsinghua.edu.cn/~sunchanghua/

References

[1] J. Lemon, "Resisting SYN flood DoS attacks with a SYN cache," in USENIX BSDCon, 2002.

[2] "SYN cookies." [Online]. Available: http://cr.yp.to/syncookies.html

[3] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in IEEE INFOCOM, 2002.

[4] B. Al-Duwairi and G. Manimaran, "Intentional dropping: A novel scheme for SYN flooding mitigation," in Global Internet Symposium, 2005.