DDOS attack with TCP SYN flooding

SV: Đặng Việt An

Outline

- Tấn công DDOS TCP SYN-Flooding
  - Giới thiệu
  - Cơ chế tấn công
- Phương pháp phòng ngừa tấn công SYN-Flood và giảm thiểu tấn công DDOS
  - SFD
  - SFD-BF
  - Mô hình giảm thiểu thiệt hại

TCP SYN-Flooding Attack

Denial-Of-Service

- Flooding-based
- Send packets to victims
  - Network resources
  - System resources
- Traditional DOS
  - One attacker
- Distributed DOS
  - Countless attackers

TCP SYN-Flooding Attack

- Nguy cơ tấn công TCP SYN flooding được đề cập lần đầu bởi Bill Cheswick và Steve Bellovin vào năm 1994 trong cuốn sách "Firewalls and Internet Security: Repelling the Wily Hacker"
- Tấn công SYN flooding được công khai đầu tiên năm 1996 với sự mô tả một công cụ khai thác trong Phrack Magazine
- Vào tháng 11 năm 1996 tấn công SYN flooding lần đầu tiên được chú ý đến khi một mail server bị tấn công .

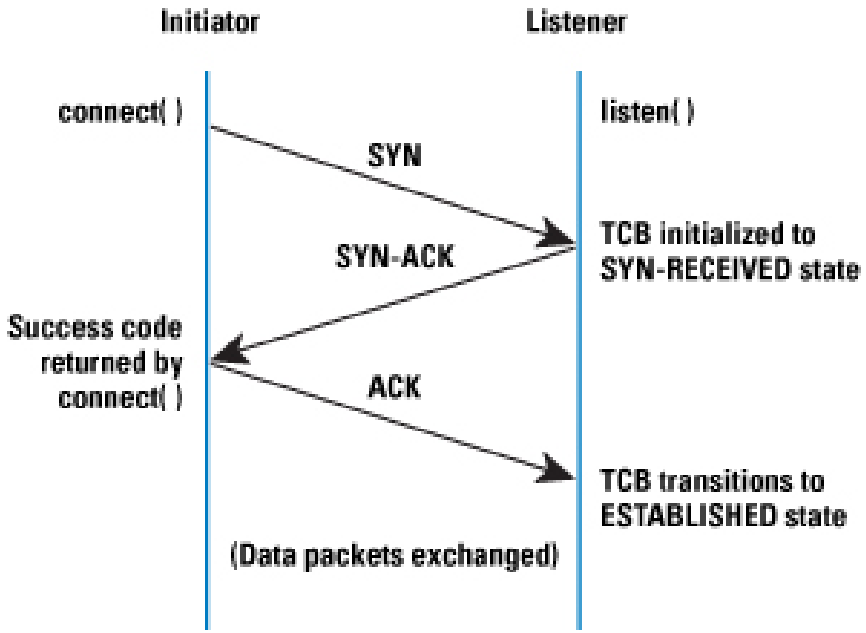
Attack Mechanism

Gói tin TCP

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset				Reserved				CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
128	Checksum																Urgent pointer															
160 ...	Options (if Data Offset > 5) ...																															

Attack Mechanism

- Transmission Control Block (TCB)
- Trạng thái TCP SYN-RECEIVED mô tả kết nối chỉ ở trạng thái half-open.
- Khi nhận được SYN segment TCB lưu giữ trạng thái này được lưu lại cho đến khi kết nối được thực hiện (ESTABLISHED).

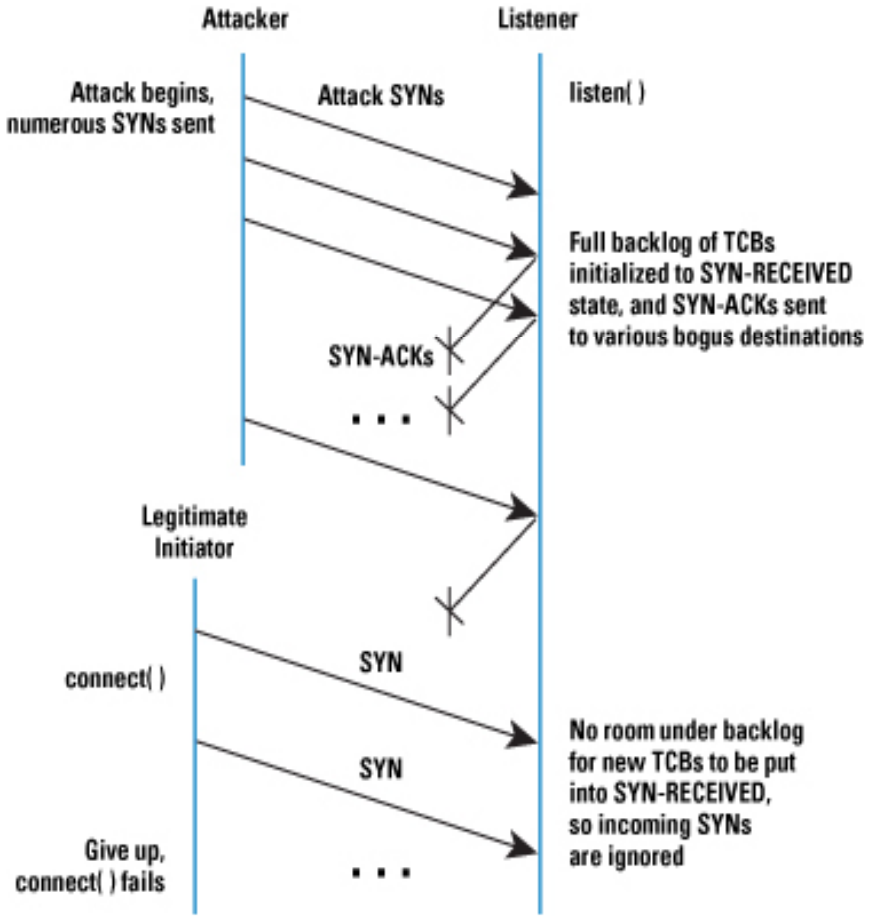


Attack Mechanism

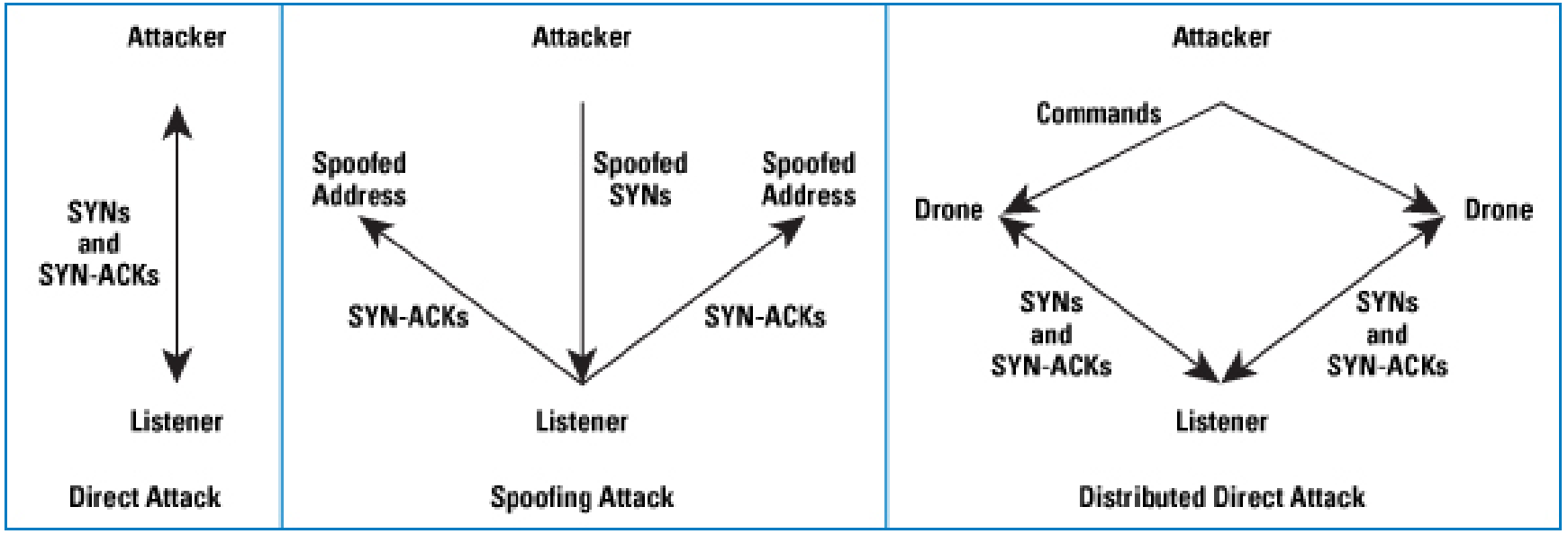
- Khi attacker gửi dòng lũ SYN dẫn đến tình trạng có quá nhiều TCB làm bộ nhớ của host bị can kiệt.
- Để phòng tránh việc bộ nhớ cạn kệt , hệ điều hành chỉ lưu giữ một số TCB xảy ra đồng thời ở trạng thái SYN-RECEIVED.
- Do hạn chế không gian lưu trữ nên khi có quá nhiều kết nối, một số kết nối hợp lệ có thể bị từ chối.

Attack Mechanism

- Kẻ tấn công gửi dòng lũ SYN segment nhằm gây cạn kiệt hệ thống



Method


Attacker
SYNs
and
SYN-ACKs
Listener
Direct Attack
Attacker
Spoofed
Address
Spoofed
SYNs
Spoofed
Address
SYN-ACKs
SYN-ACKs
Listener
Spoofing Attack
Attacker
Commands
Drone
Drone
SYNs
and
SYN-ACKs
SYNs
and
SYN-ACKs
Listener
Distributed Direct Attack

Phương pháp phòng ngừa và giảm thiểu tấn công SYN-Flood

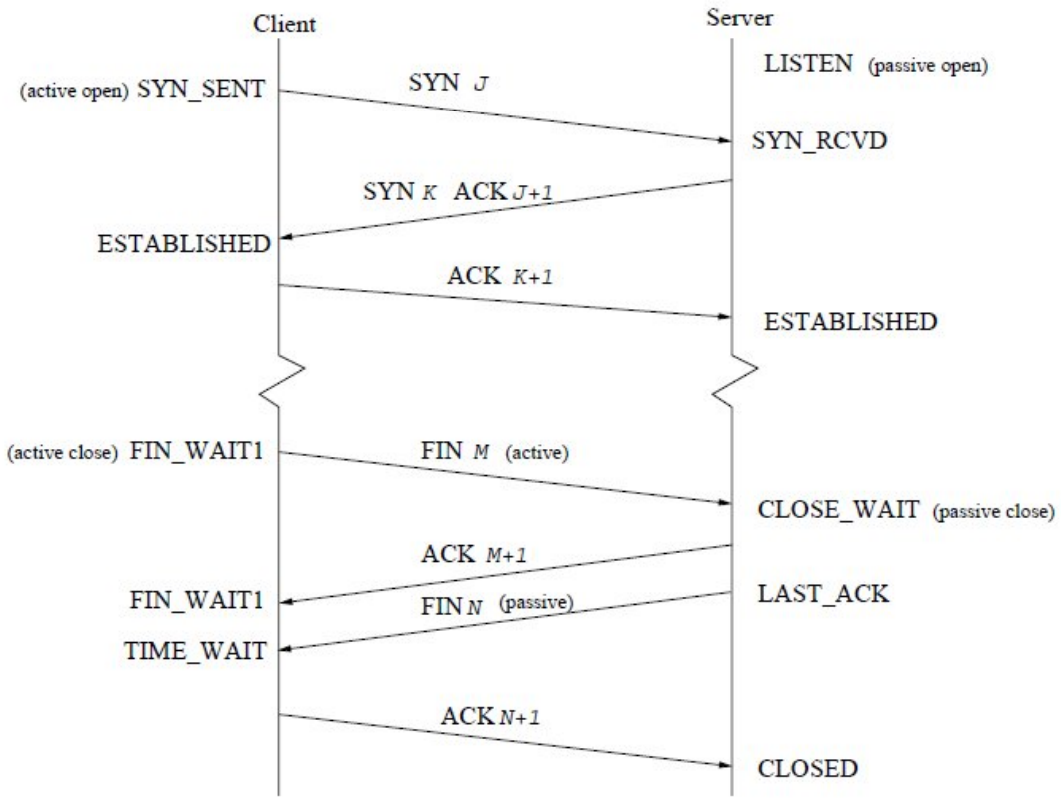
SFD

SFD

- Phương pháp phát hiện tấn công (Haining Wang ,Danlu Zhang Kang, G. Shin- EECS Department, The University of Michigan) SFD
- Phương pháp phát hiện tấn công sử dụng Bloom Filter (Changhua Sun, Jindou Fan, Bin Liu-Department of Computer Science and Technology, Tsinghua University, China) SFD-BF

Idea

- Sử dụng quan hệ vốn của cặp SYN-FIN.
- Trong một kết nối TCP thông thường mở đầu bằng một gói SYN thì kết thúc bằng một gói FIN (kết thúc kết nối) hoặc RST (reset kết nối).



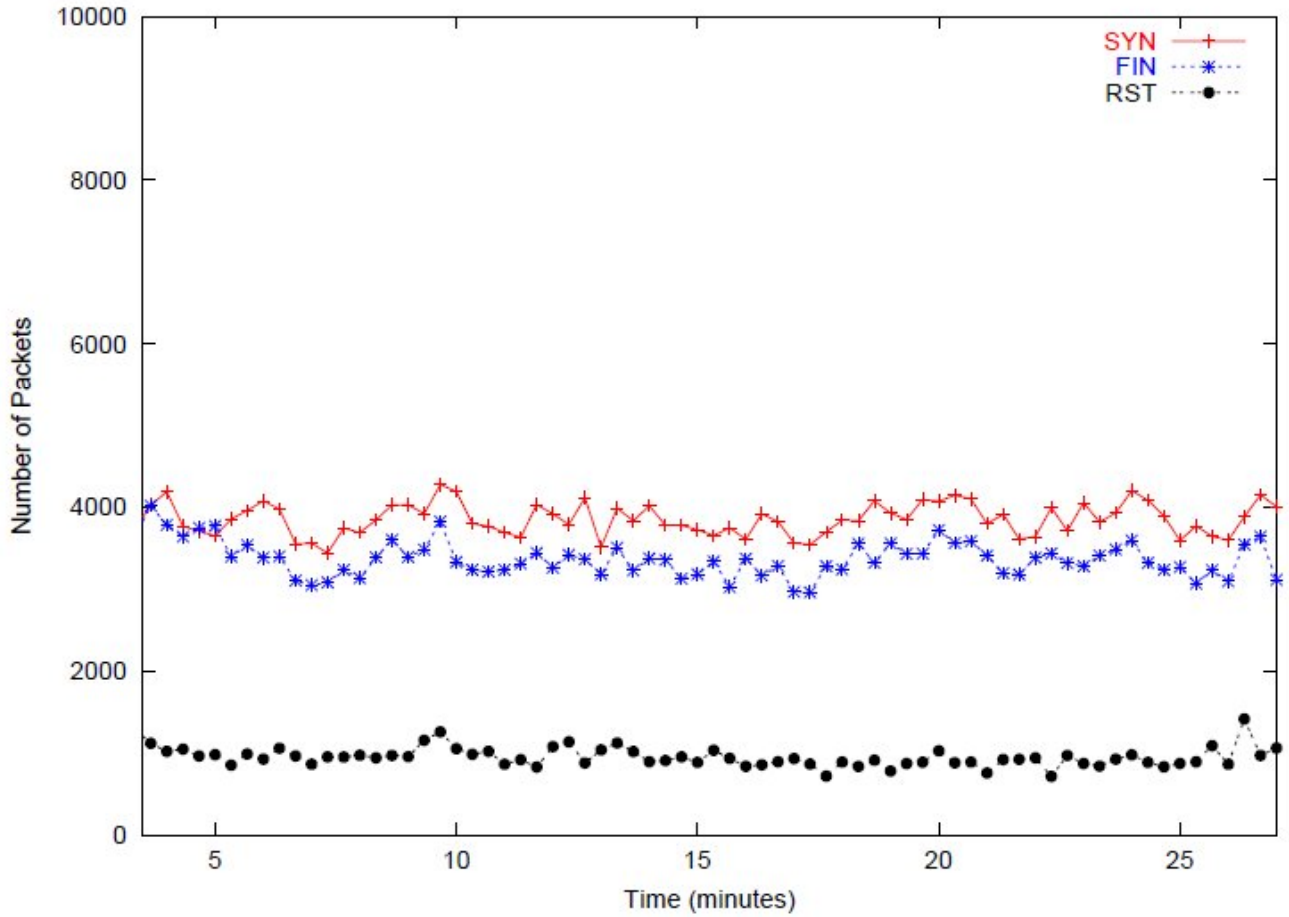
SYN – FIN Behavior

Generally every SYN has a FIN

RED – SYN

BLUE- FIN

BLACK- RST



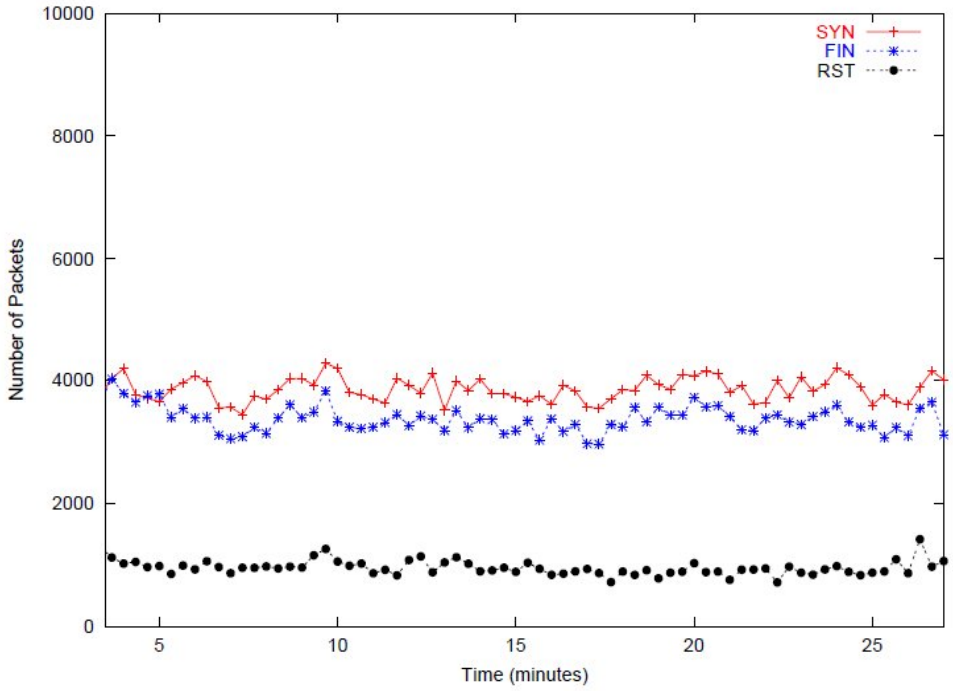
What to do about "RST"

- Phân loại:

  - RSTactive : khởi tạo kết nối khác

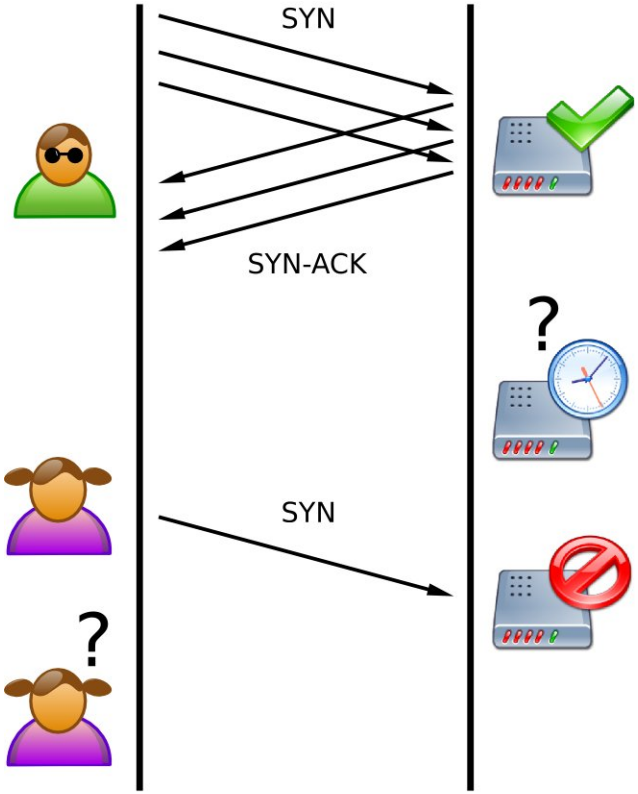
  - RSTpassive : phản hồi khi 1 gói tin tới một port đã bị đóng – không có giá trị để tính toán

- Trong phương pháp này ta lấy RSTactive ở ngưỡng 75% trên tổng số các gói tin.



Statistical Attack Detection

- There are very many SYN's necessary to accomplish a DoS attack
- At least 500 SYN/sec
- 1400 SYN/sec can overwhelm firewall
- 300,000 SYNs necessary to shut down server for 10 minutes



CUSUM Algorithm

- Xem xét mối quan hệ giữa số lượng 3 cặp (SYN, FIN), (SYN/ACK, FIN),(SYN,RSTactive)
- So sánh và kiểm tra sự thay đổi
- CUSUM = "cumulative sum"

Method

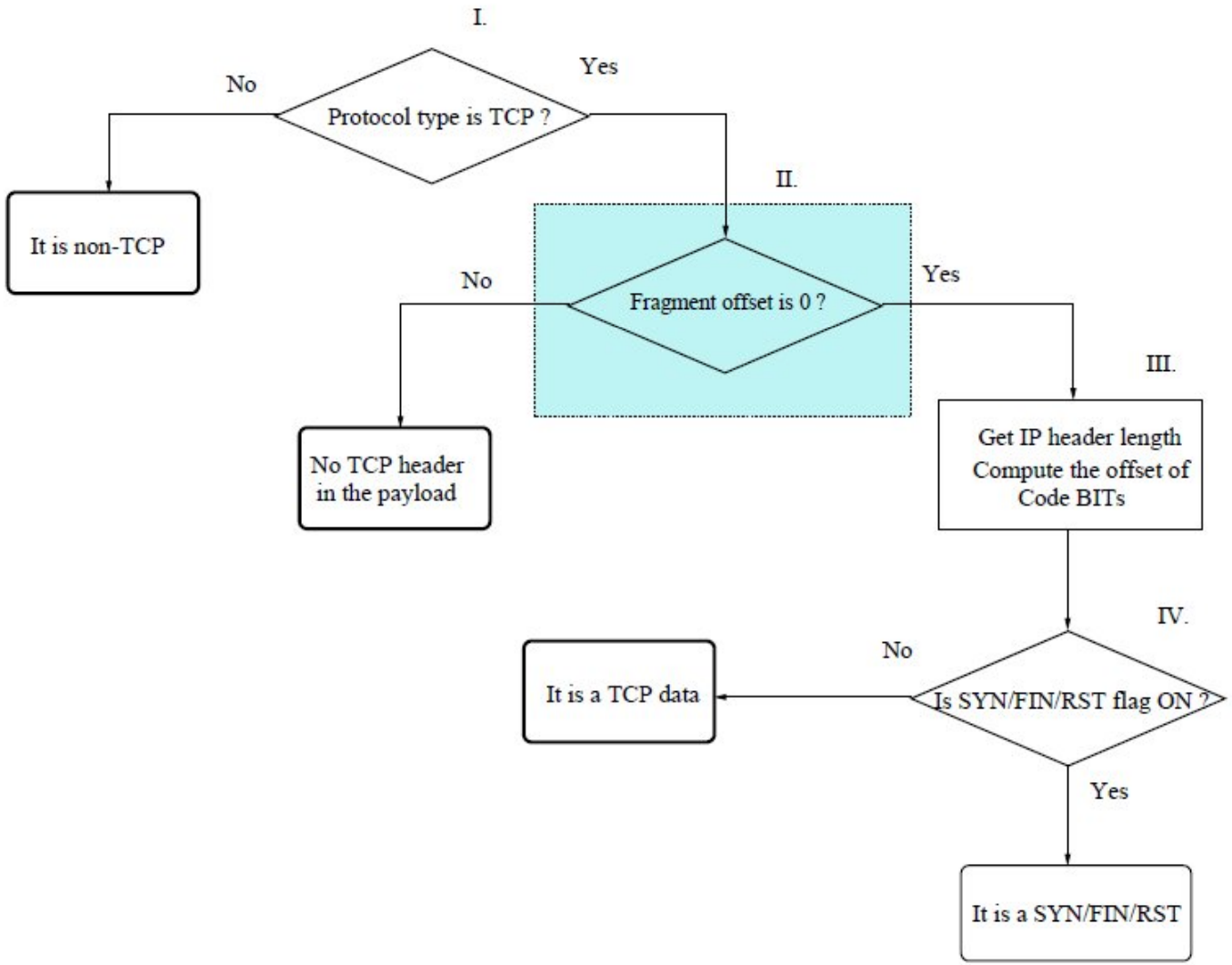
1- Phân loại gói tin

2-Tính số lượng gói tin SYN và FIN đi qua

3-Sử dụng giải thuật CUSUM phân tích cặp (SYN-FIN)

Method

- Phân loại gói tin



Method

- Lấy mẫu: Theo nghiên cứu mỗi kết nối TCP thường kéo dài từ 12s-19s nên ta thiết lập 2 tham số:
  - To: thời gian lấy mẫu To=20s
  - Td: thời gian trễ giữa lấy mẫu SYN và FIN. Td=10s

Phương pháp phòng ngừa và giảm thiểu tấn công SYN-Flood

SFD-BF

Idea

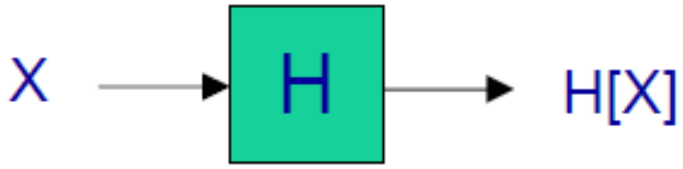
- Phương pháp này là cải tiến SFD. Ý tưởng chính là sử dụng Bloom Filter để truy vấn với tốc độ nhanh với xác suất chấp nhận được.
- Với mỗi gói tin TCP, ta quan tâm đến bộ tham số (4-tuple): (source and destination IP, source and destination Port).

Hash Function

Input : x

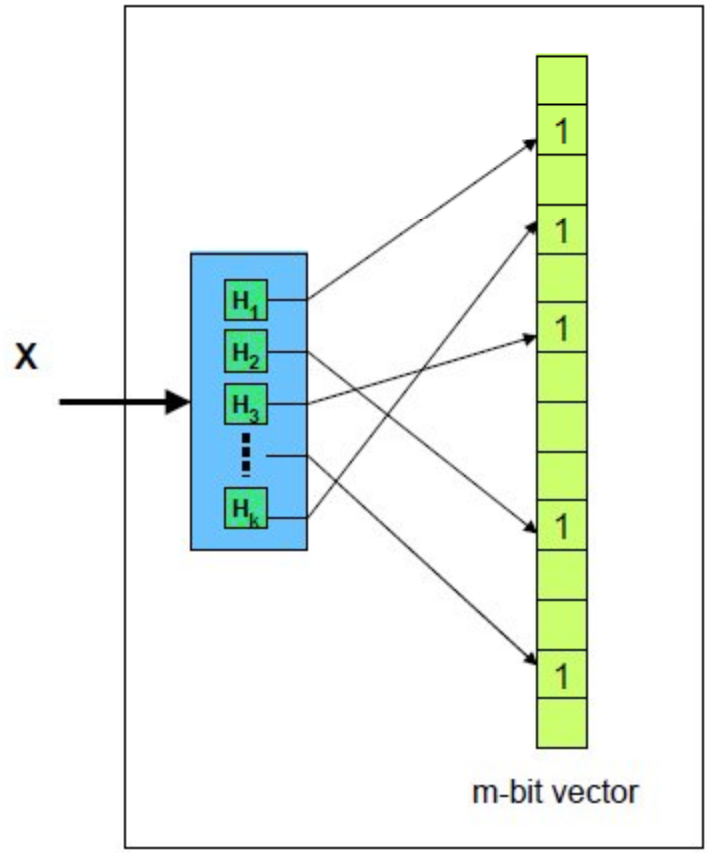
- Output : H[x]
- Properties
  - Each value of x maps to a value of H[x]
  - Typically: Size of (x) >> Size of (H[x])
- Implementation
  - Hash Function

XOR of bits, Shifting, rotates ..

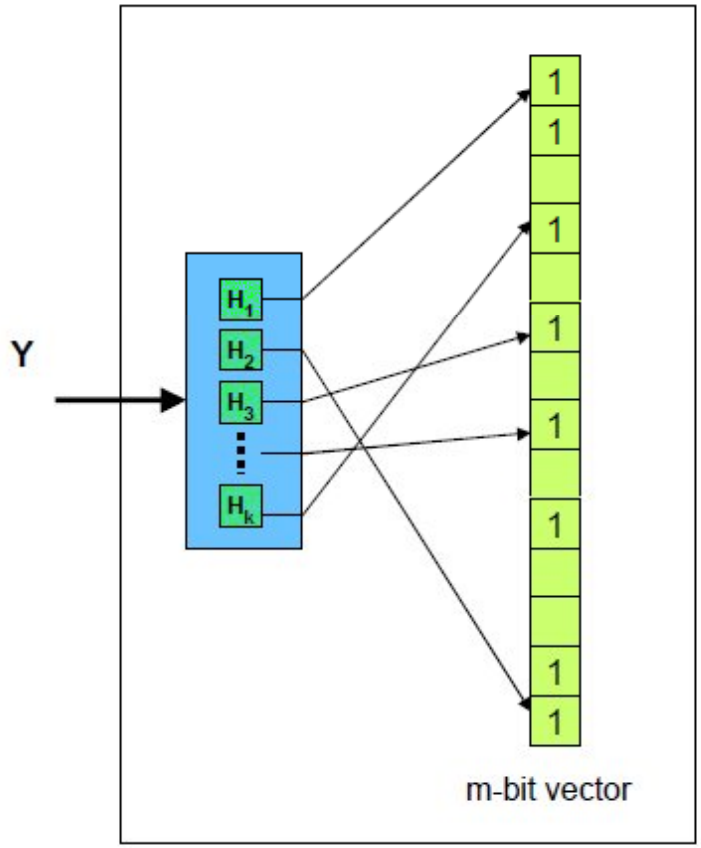


Bloom-Filter (BF)

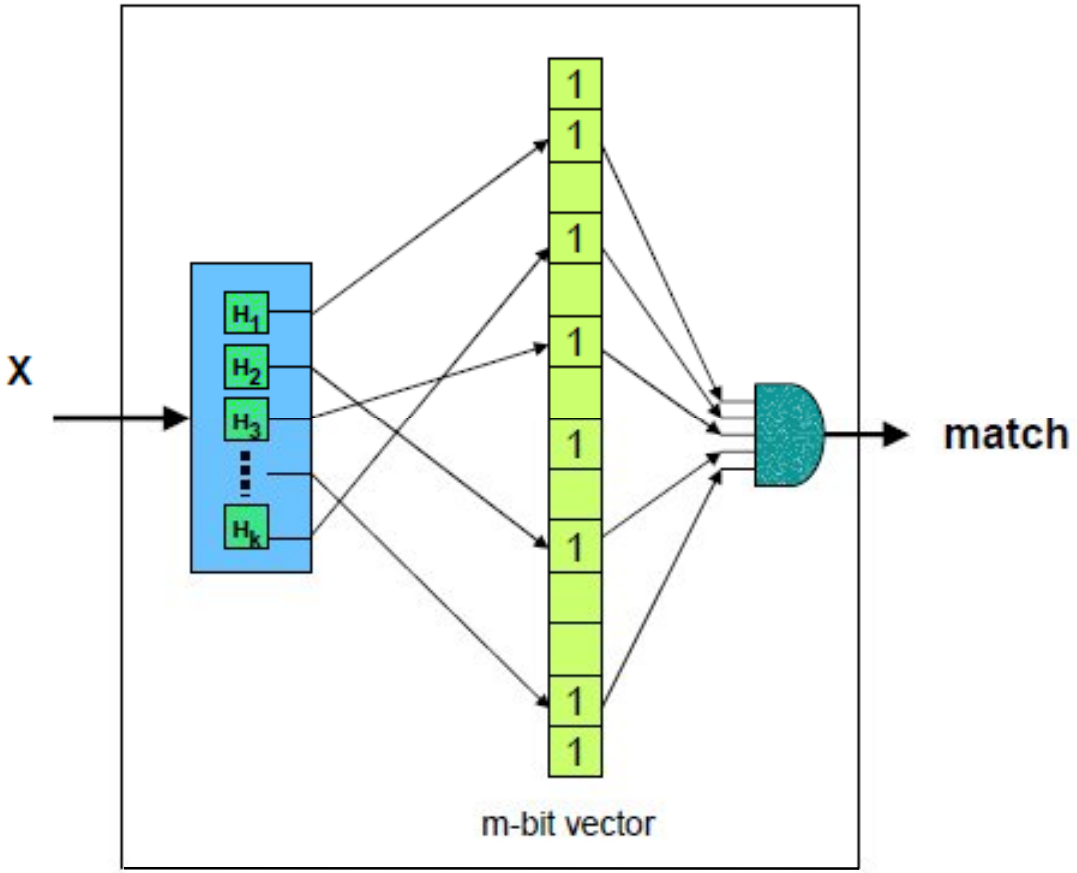
- Bloom Filter sử dung k hàm băm



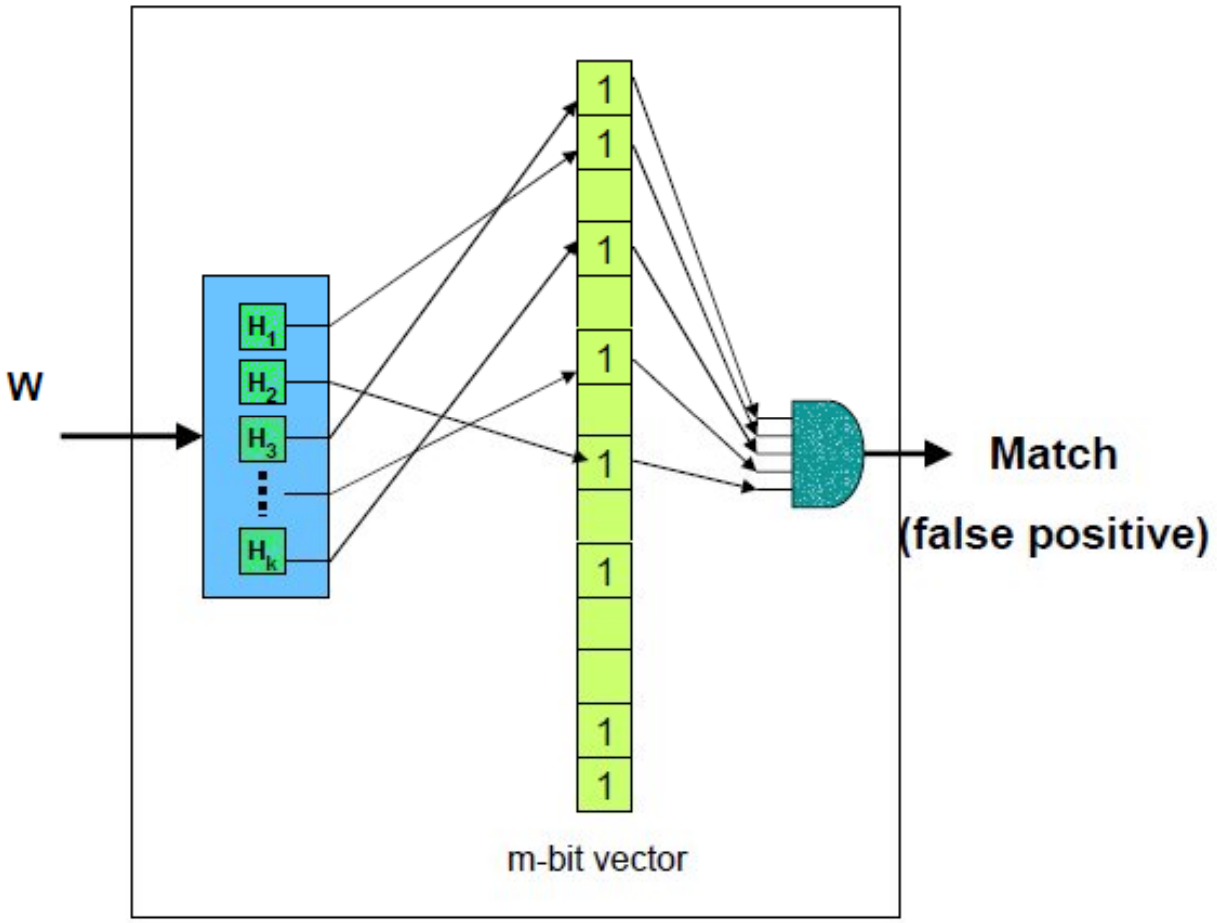
Bloom-Filter (BF)



Querying a Bloom Filter



Querying a Bloom Filter



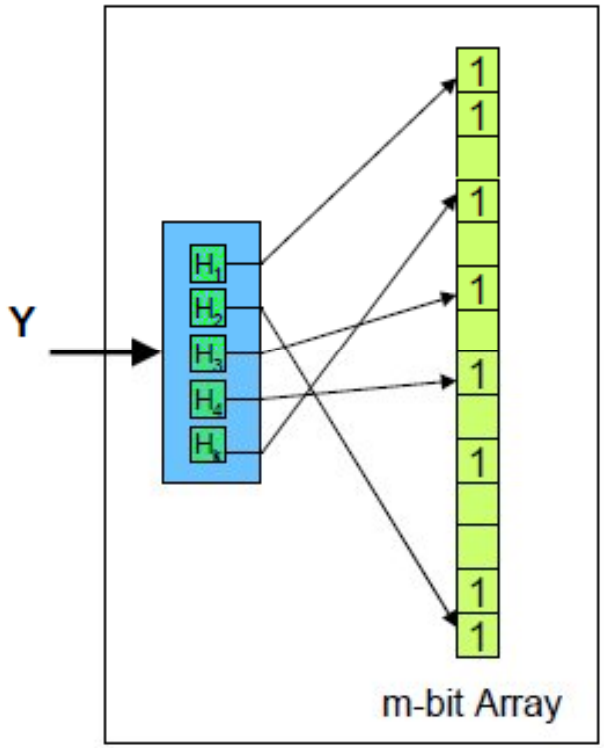
Optimal Parameters of a Bloom filter

- *n : number of Item to be stored*
- *k : number of hash functions*
- *m : the size of the bit-array (memory)*
- The false positive probability

  $f = (½)^k$

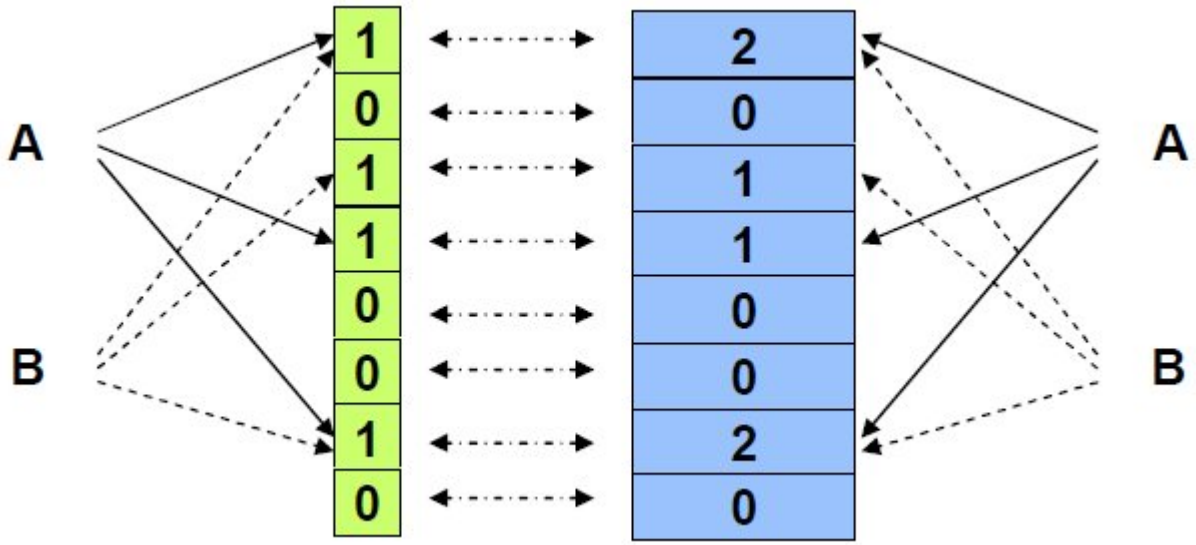
- The optimal value of hash functions, k,is:

  $k = \ln 2 \times m/n = 0.693 \times m/n$



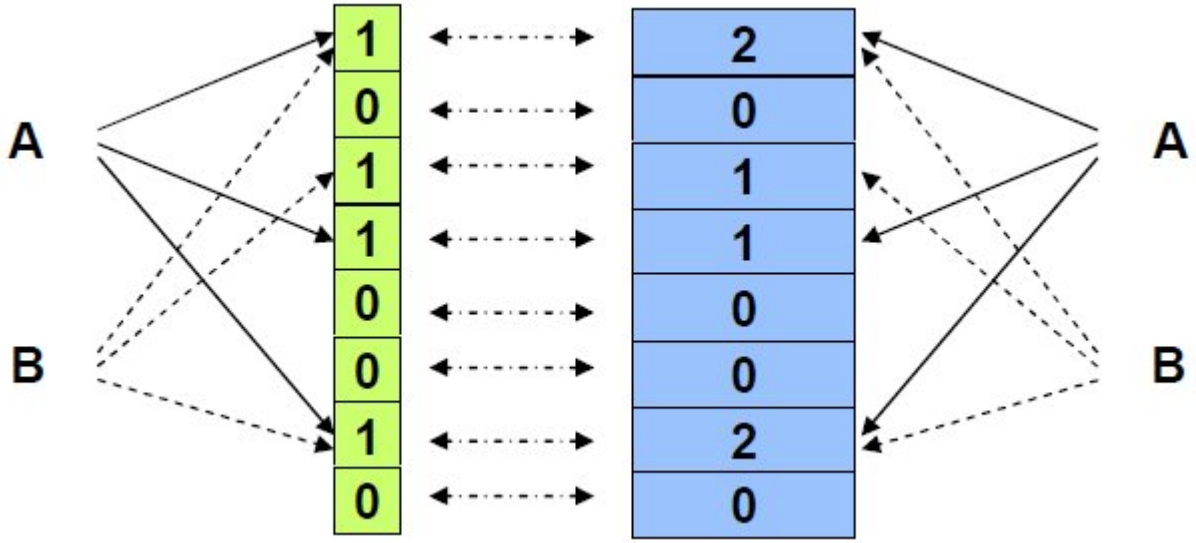
Counting Bloom Filters

- Trong bộ đếm được sử dụng, thay vì sử dụng m bit, ta sử dụng m bộ đếm nhỏ (small counter).
- Khi thêm hoặc xóa giá trị x ta tăng hoặc giảm giá trị bộ đếm tại vị trí tương ứng



Counting Bloom Filters

- Để đảm bảo xác suất truy vấn ta cho m/n=16. Xác suất truy vấn sai nhỏ hơn 0,000459
- Cấp phát cho mỗi bộ đếm nhỏ 8 bit.
- Khi số bộ đếm nhỏ có giá trị >= m/2 reset lại BF để đảm bảo độ chính xác của truy vấn.



SFD-Method

1- Phân loại gói tin

2-Tính số lượng gói tin SYN và FIN đi qua

3-Sử dụng giải thuật CUSUM phân tích cặp (SYN-FIN)

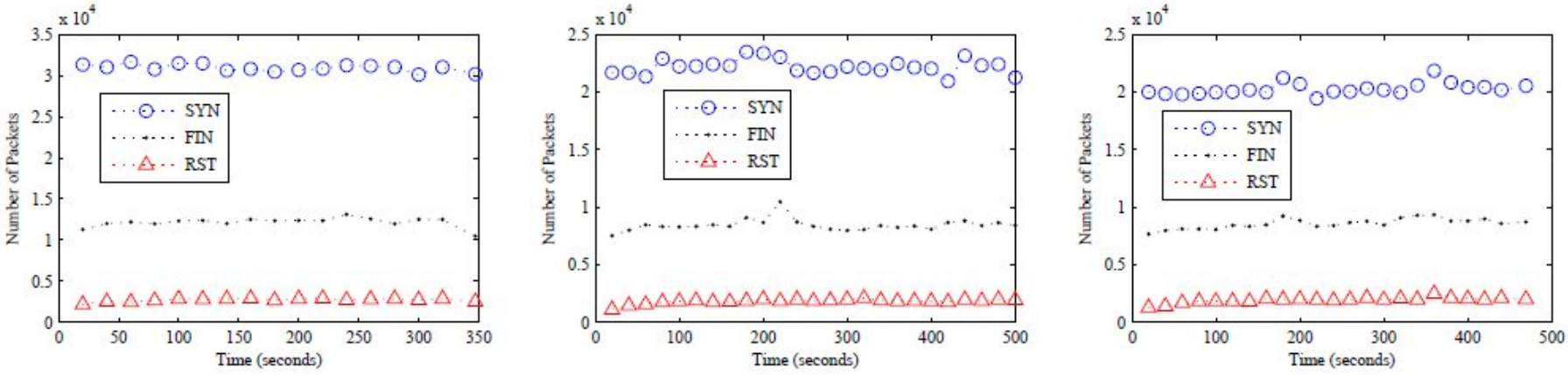
SFD-BF Method

- Cải tiến so với SFD:
  - Khi tính hiệu số giữa số gói tin SYN và FIN ta so khớp bộ 4 tham số nói trên bằng phương pháp sau:
    - Khi một gói SYN đi qua ta lấy bộ 4 tham số và insert vào BF. Ta tăng bộ đếm số gói SYN lên 1.
    - Khi một gói tin FIN hay RST đi qua, lấy bộ 4 tham số truy vấn với giá trị trong BF nếu bộ này có trong BF số gói FIN tăng lên 1 và ta xóa bộ gía trị tương ứng trong BF.

SFD-BF Method

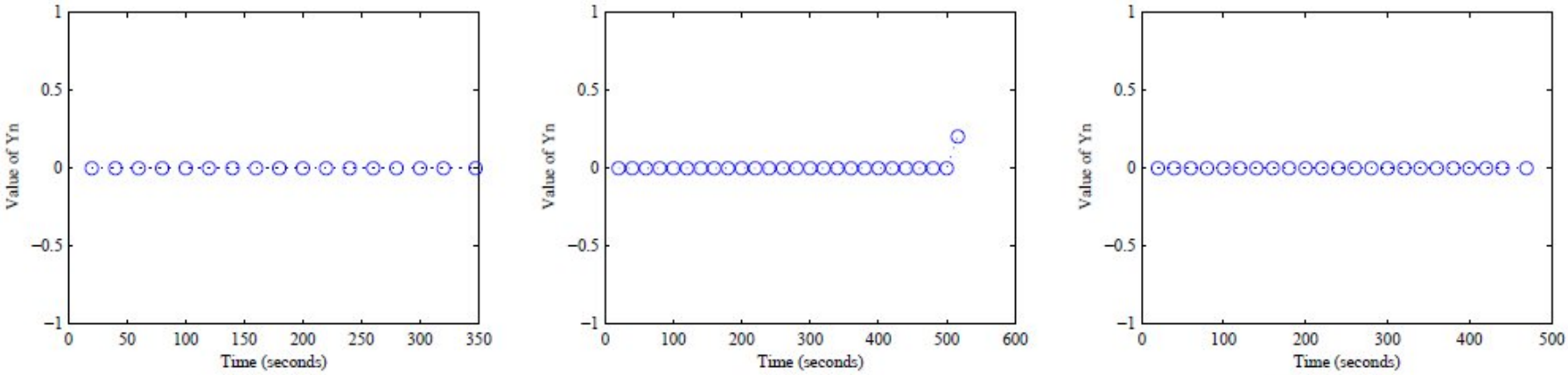
- Nhận xét:
  - Cải tiến này giúp tăng hiệu năng phương pháp do các FIN được so khớp bộ 4 tham số với các gói SYN thì mới được đếm. Vì vậy khi sử dụng CUSUM hiệu gói SYN và FIN sẽ đạt tới ngưỡng nhanh hơn khi bị tấn công.
  - Nhờ việc so khớp 4 tham số sẽ khắc phục được hạn chế của SFD khi attacker gửi các gói FIN kèm theo SYN.

Result



(a) THU-1 (b) THU-2 (c) THU-3

Fig. 2. The dynamics of *valid SYN and FIN packets*.



(a) THU-1 (b) THU-2 (c) THU-3

Result

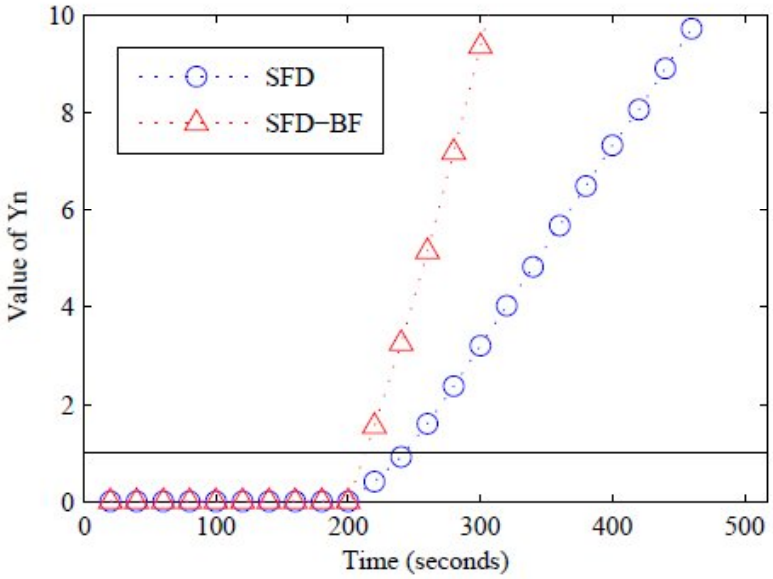


Fig. 4. SYN flooding detection under simple attacks.

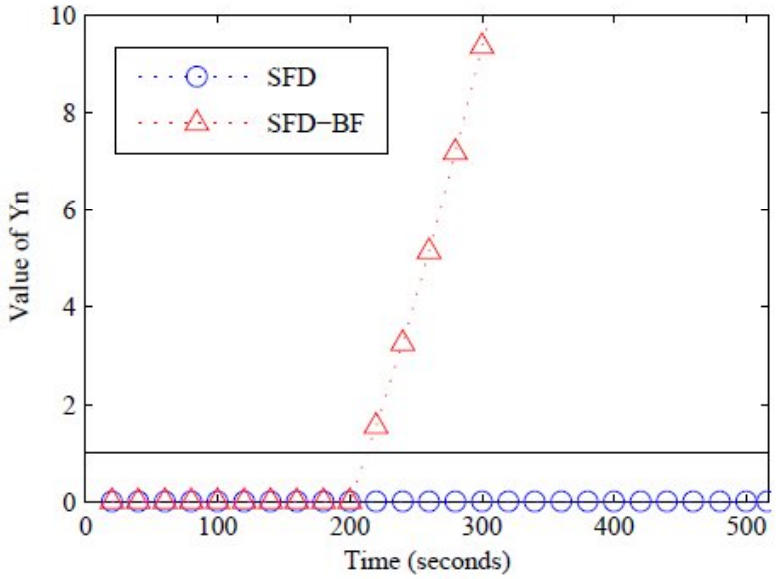


Fig. 5. SYN flooding detection under complex attacks.

Phương pháp phòng ngừa và giảm thiểu tấn công SYN-Flood

Mô hình giảm thiểu thiệt hại

Idea

- Trong điều kiện bình thường khi thực hiện kết nối TCP nếu trong thời gian xác định trước khi phía client gửi gói SYN mà server không phản hồi lại bằng gói SYN-ACK thì client sẽ tiếp tục gửi gói SYN cho đến khi kết nối được.
- Phương pháp này sử dụng hành vi trên bằng cách loại bỏ hết tất cả các gói SYN trong nhận được từ một địa chỉ nguồn trong lần đầu tiên.

Method

- Sử dụng 3 bộ đếm BF
  - BF1: lưu trữ các bộ 4 tham số của các gói SYN trong mỗi kết nối.
  - BF2: lưu trữ bộ 4 tham số của các gói SYN, khi các kết nối đã hoàn thành bắt tay 3 bước.
  - BF-3: Lưu trữ các bộ 4 tham số của các gói SYN còn lại.

Method

Khi một gói SYN được nhận, bộ 4 tham số được so sánh với giá trị trong 3 BF. Xảy ra 4 trường hợp sau:

- 1. Giá trị không nằm trong 3 BF, kết nối này là mới và bị drop, ta insert giá trị này vào BF1
- 2. Nếu giá trị này có trong BF-1, đây là gói SYN thứ 2 ta chuyển giá trị này từ BF1-BF3
- 3. Nếu trị nằm trong BF-2. Ta cho gói tin này đi qua.
- 4. Nếu giá trị này nằm trong BF-3 ta cho gói tín này đi qua với xác xuất p=1/n, với n là số giá trị nằm trong BF-3

Method

Nếu một gói ACK được nhận bộ 4 giá trị được so sánh với các giá trị trong BF. Xảy ra 3 trường hợp:

1. Giá trị không nằm trong 3 BF, drop gói tin
2. Giá trị này nằm trong BF-2. Cho gói tin đi qua
3. Giá trị này nằm trong BF-3. Kết nối hoàn thành, di chuyển bộ 4 tham số này từ BF3 sang BF-2

.

Result

- Khi một gói SYN được gửi đi từ một địa chỉ nguồn lần đầu tiên, gói này bị drop.
- Trong lần tiếp theo từ địa chỉ đó tiếp theo gói SYN này sẽ được đi qua
- Nếu địa chỉ nguồn này tiếp tục gửi gói tin SYN, xác suất được đi qua bằng 1/n với n là số lần gửi gói SYN. Với n tăng, xác suất gói tin đi qua sẽ nhỏ dần, do vậy số gói tin SYN đến được host bị tấn công sẽ được giảm bớt.

TLTK

[1] CERT Advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks. [Online]. Available: http://www.cert.org/advisories/CA-1996-21.html
[2] W. Eddy, "TCP SYN flooding attacks and common mitigations," February 2007. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-tcpm-syn-flood-02.txt
[3] J. Lemon, "Resisting SYN flood DoS attacks with a SYN cache," in *USENIX BSDCon, 2002.*
[4] "SYN cookies." [Online]. Available: http://cr.yp.to/syncookies.html
[5] B. Al-Duwairi and G. Manimaran, "Intentional dropping: A novel scheme for SYN flooding mitigation," in *Global Internet Symposium, 2005.*
[6] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in *IEEE INFOCOM, 2002.*
[7] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM, vol. 13, no. 7, pp. 422–426, 1970.*
[8] [Online]. Available: http://s-router.cs.tsinghua.edu.cn/%7Esunchanghua/publication/THUTR200703SYN.pdf
[9] M. V. Ramakrishna, E. Fu, and E. Bahcekapili, "Efficient hardware hashing functions for high performance computers," *IEEE Transactions on Computers, vol. 46, no. 12, pp. 1378–1381, 1997.*

Question???