

# Detecting SYN Flooding Attacks



Haining Wang, Dandle Zhang, Kang G.  
Shin

---

Presented By  
Hareesh Pattipati



# Outline

---

- Introduction
- Related Issues
- Attack Detection
- Performance Evaluation
- Future Work
- Conclusion



# Introduction

---

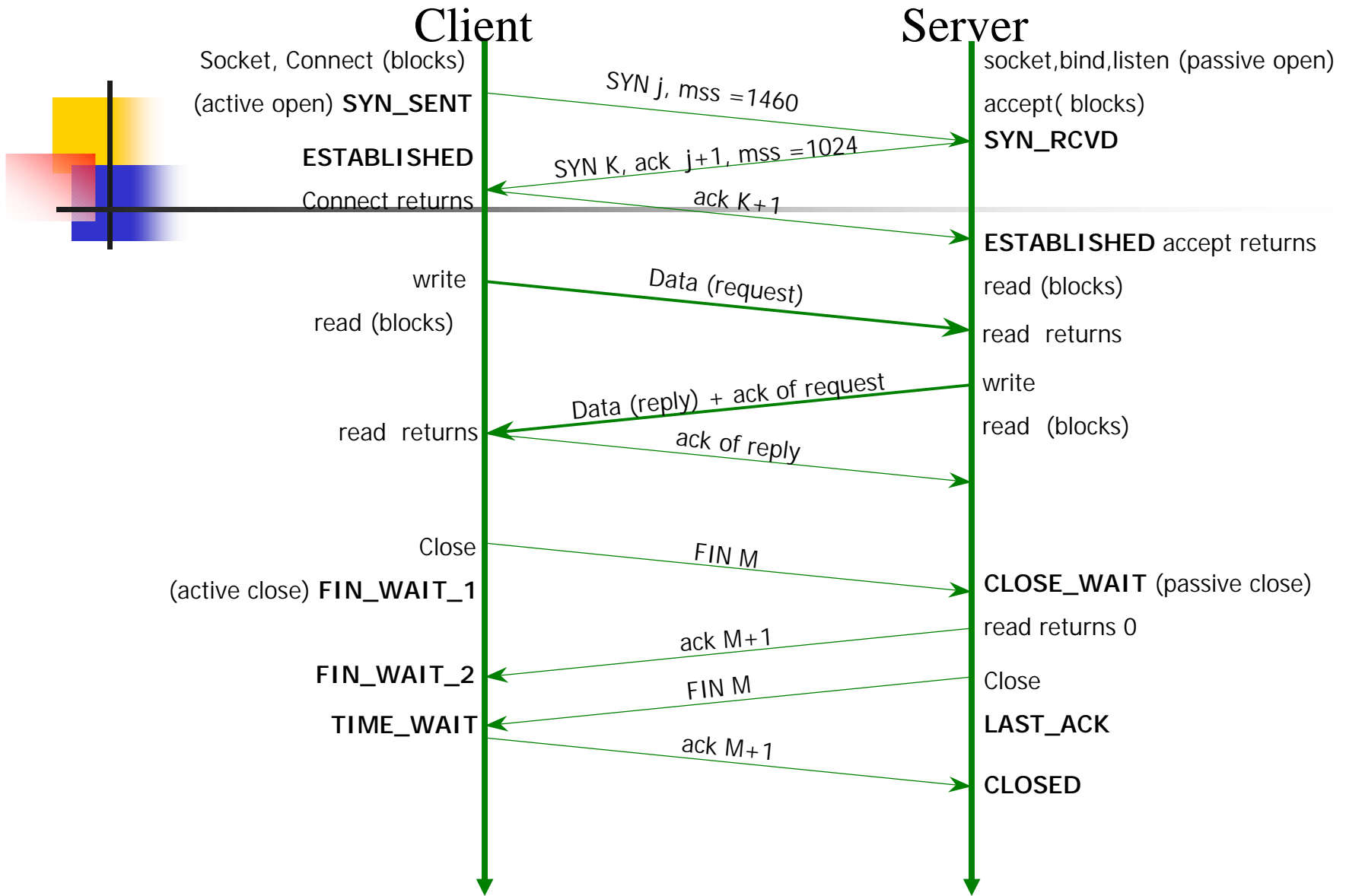
- Attacks on popular sites
- Most of them are DoS using TCP
- SYN Flooding exploits TCP 3-way handshake
- Syn Cache, Syn cookies, SynDefender, Syn Proxying and SynKill
- Installed on firewall or victim server

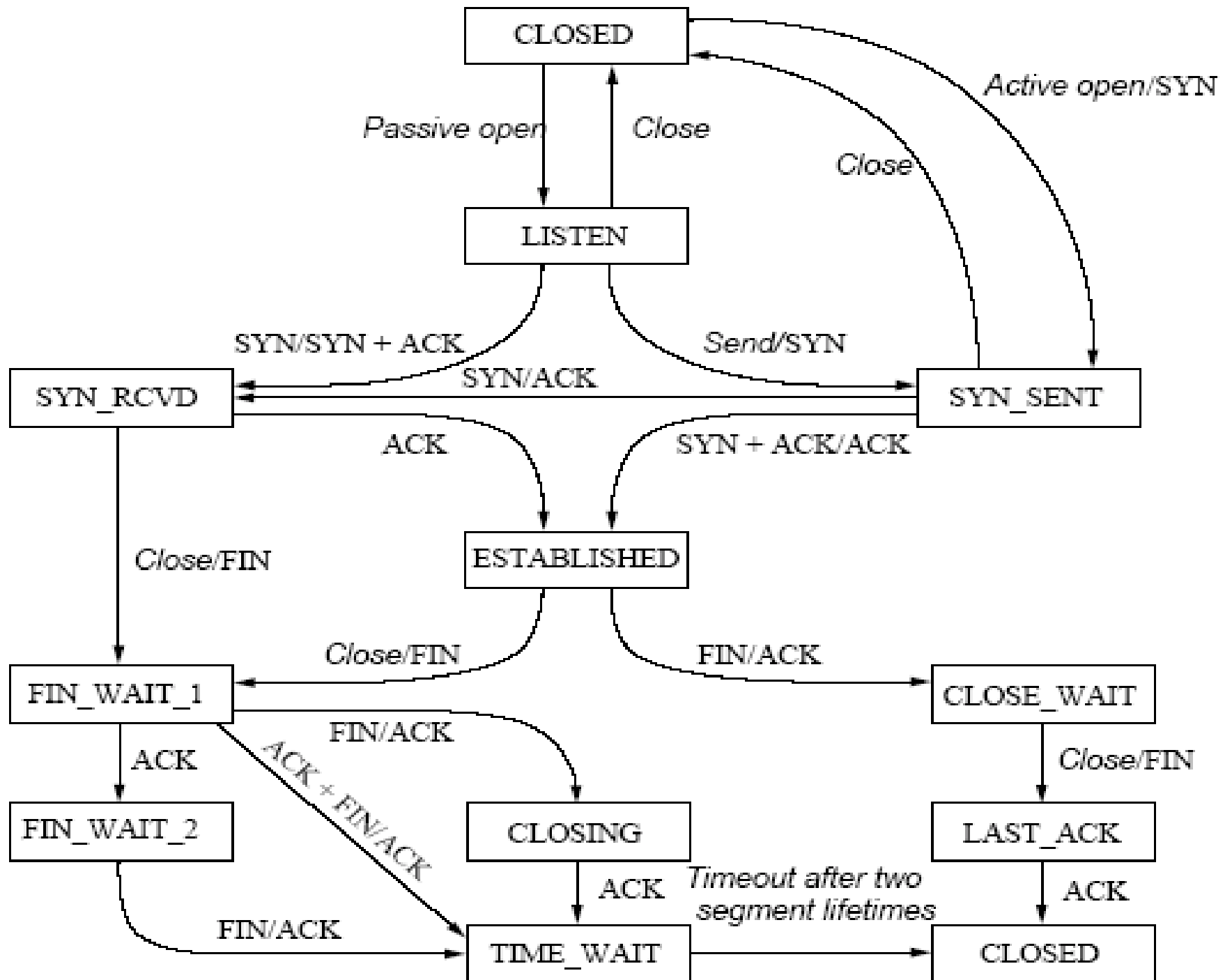


## Introduction (cont)

---

- Specialized firewalls become worthless with 14000 packets per sec.
- FDS – Flooding Detection System
- Installed on leaf routers (First-mile or Last-mile routers)
- FDS uses key feature of TCP SYN-FIN pairs behavior.







## Introduction (cont)

---

- TCP packet classification is done at leaf router
- SYN (beginning) FIN (END) for each TCP connection
- No means to distinguish active FIN and passive FIN
- RST violates the SYN-FIN pairs
- Three new variables introduced to count SYN, FIN, and RST



# Related Issues

---

- Packet Classification
- Placement of Detection Mechanism
- Discrepancy between SYN's and FIN's



# Packet classification

---

- Packet Classification is done at the leaf router

$$IPoffset = Hdr\_length^{IP} + TCPoffset.$$

- First two steps confirm that it is a TCP packet
- Code Bits in IP packet equals the sum of the length of IP header and offset of code BIT's in TCP

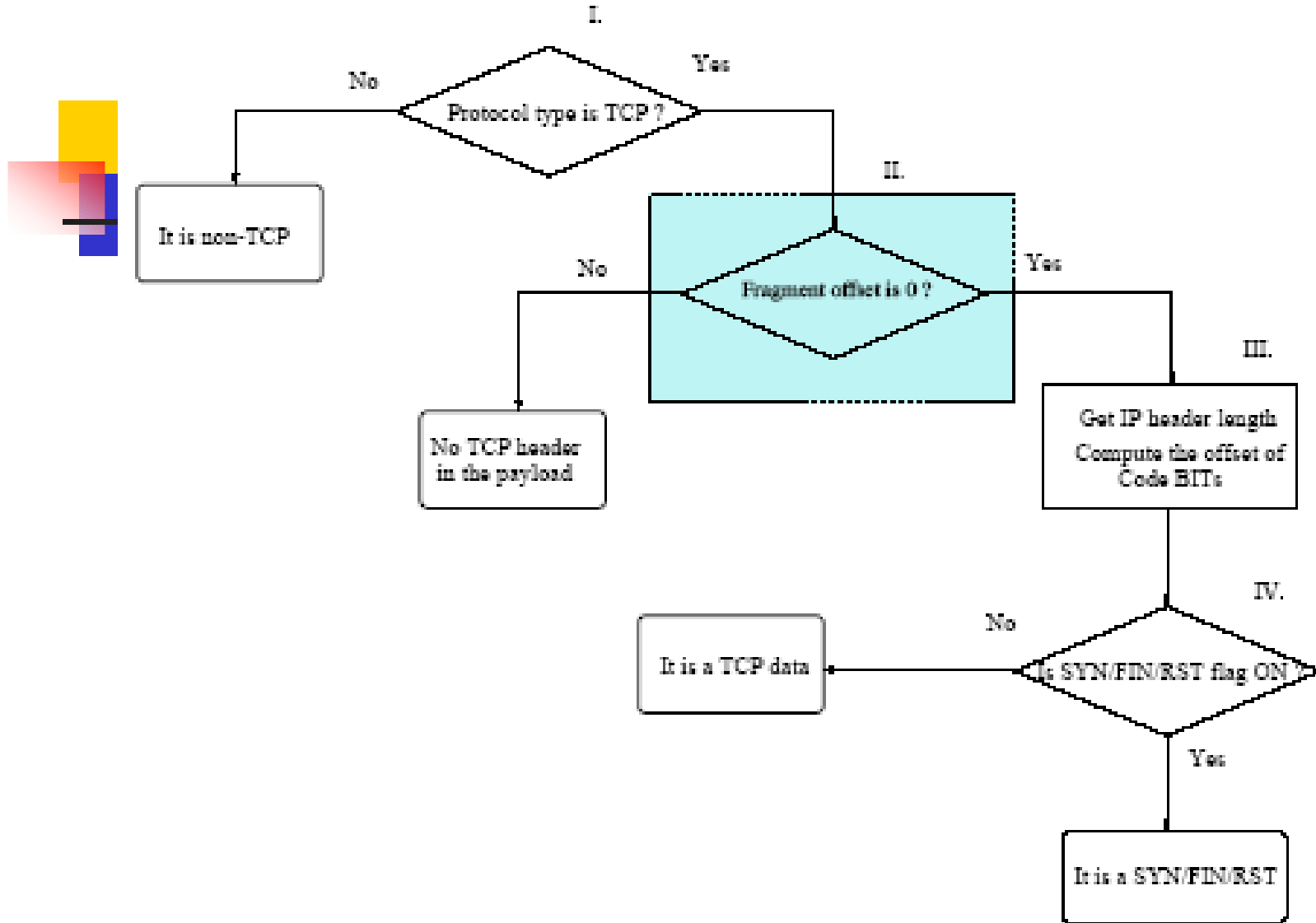


Fig. 2. The flowchart of the packet classification at leaf routers



# Placement of Detection Mechanism

---

- FDS is installed at the first-mile and last mile router
- First-mile is more likely to catch flooding detection due to proximity to sources.
- Last-mile quickly detects the flooding but cant provide hint about flooding sources
- FDS is not installed at core due to a) it is close to neither flooding sources not the victim b) packets of the same flow could traverse different paths

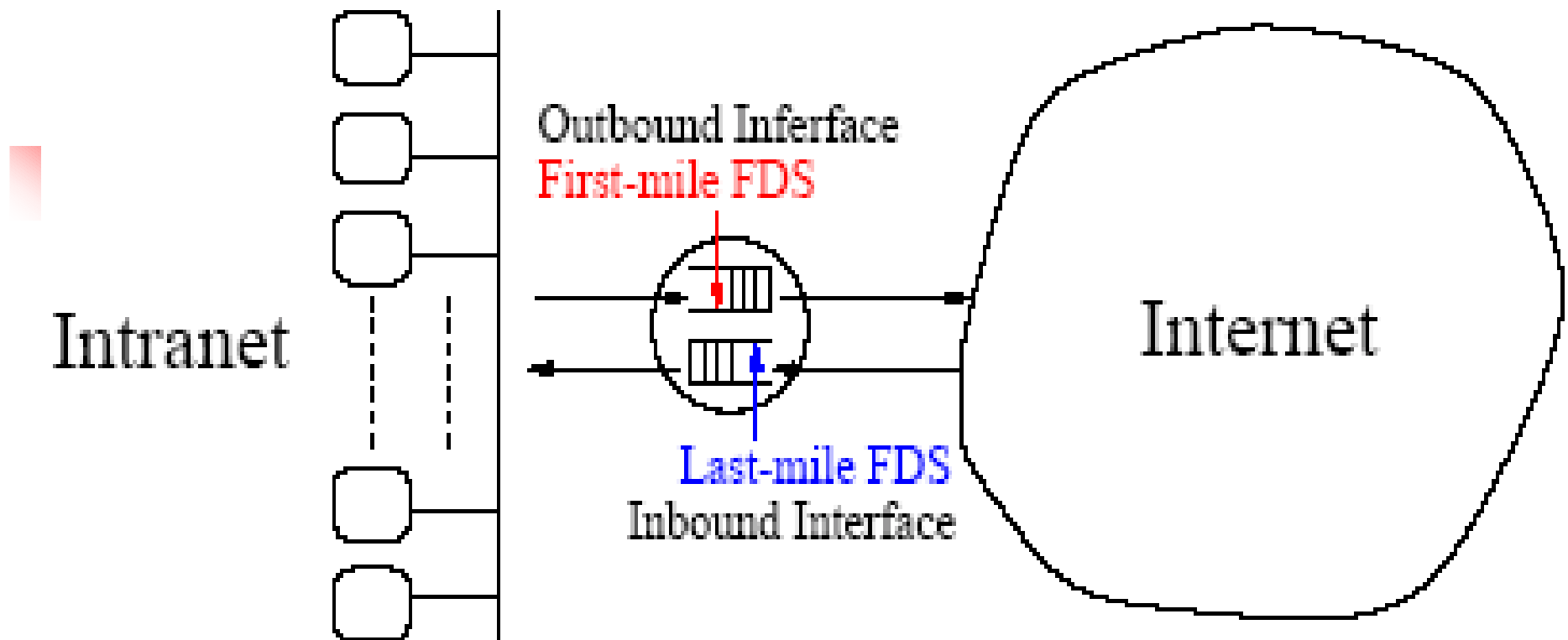


Fig. 3. The installation of FDS at a leaf router



# Discrepancy btw SYN's and FIN's

---

- Single RST packet can terminate a TCP session
- Passive RST transmitted in response to close the port
- Active RST transmitted in response to abort a TCP connection and associated with a SYN
- Normal behavior of TCP: (SYN, FIN), (SYN/ACK, FIN) and (SYN, RST<sub>active</sub>)
- FDS cannot differentiate between active and passive RST



## Discrepancy btw SYN's and FIN's

---

- Normal Conditions :
  - 1) SYN and RST have a strong correlation
  - 2) Difference between SYNs and FINs is equal to RSTs
- Threshold is set at 75%, i.e., 3 out of 4 RSTs are active



# Attack Detection

---

- Data Sampling and Detection Mechanism
  - SYN and FIN packets collected over time  $t_0$
  - Sampling time of FIN(RST)  $t_d$  later than SYN
  - Recent study : TCP Connections 12-19 sec
  - $t_d$  set to 10 sec and  $t_0$  is set to 20 sec
- The CUSUM algorithm
  - $\{\Delta_n, n=0, 1, \dots\}$  Number of SYNs-FINs.
  - $\{\Delta_n\}$  is Normalized by average number of F of FINs(RSTs)

$$\bar{F}(n) = \alpha \bar{F}(n-1) + (1-\alpha) \text{FIN (RST)}(n),$$



# Attack Detection

---

- $X_n = \Delta_n / F$ .  $X_n$  denoted as  $C$  and ranges between 0 and 1.

$$y_n = S_n - \min_{1 \leq k \leq n} S_k,$$

$$S_k = \sum_{i=1}^k \bar{X}_i.$$

- $\{y_n\}$  large value indicates of an attack.

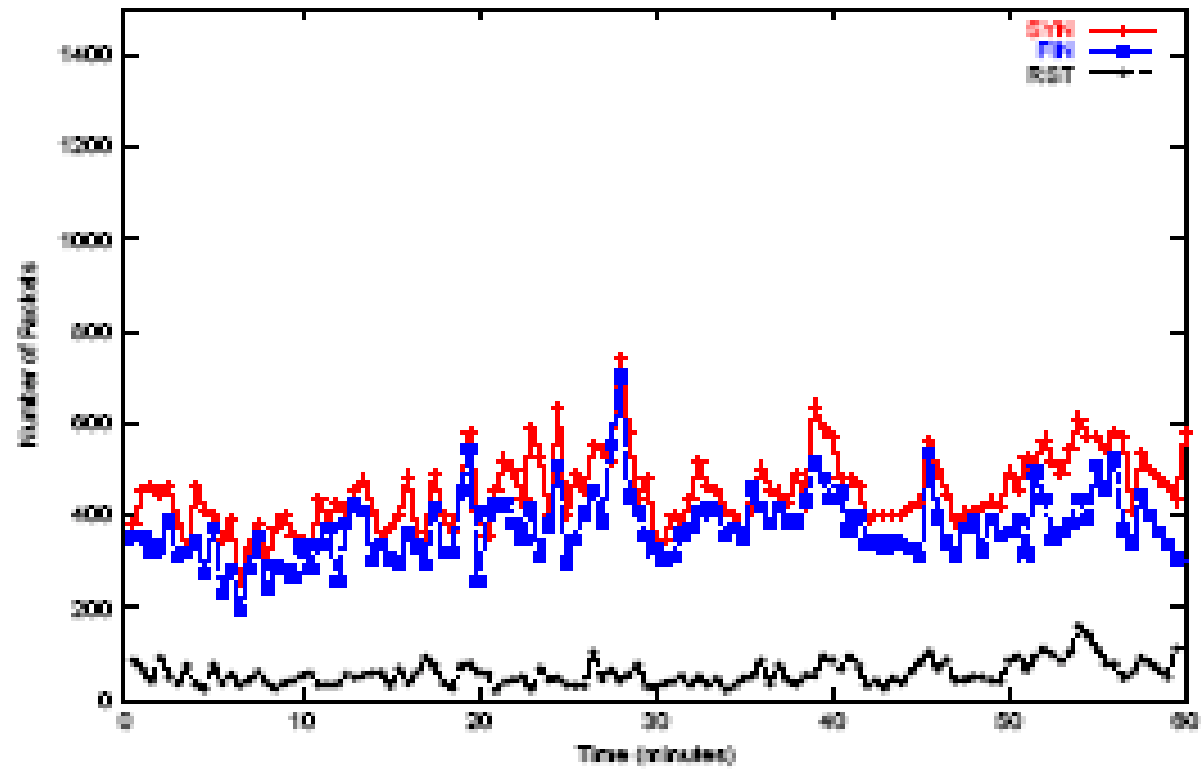
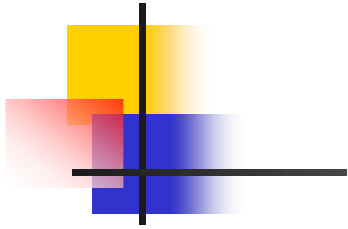


# Performance Evaluation

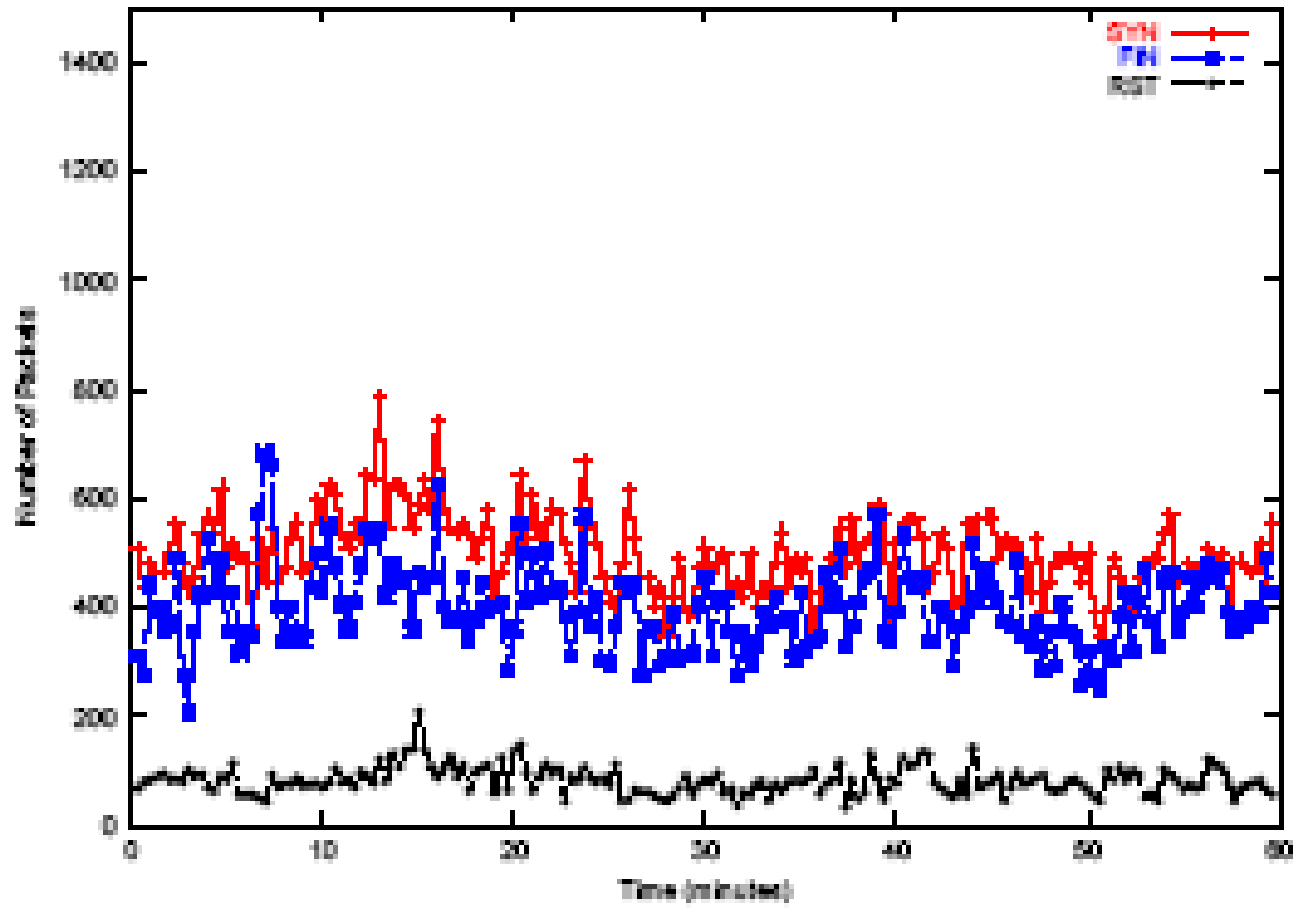
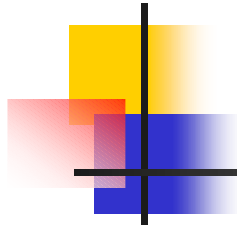
TABLE I

A SUMMARY OF THE TRACE FEATURES

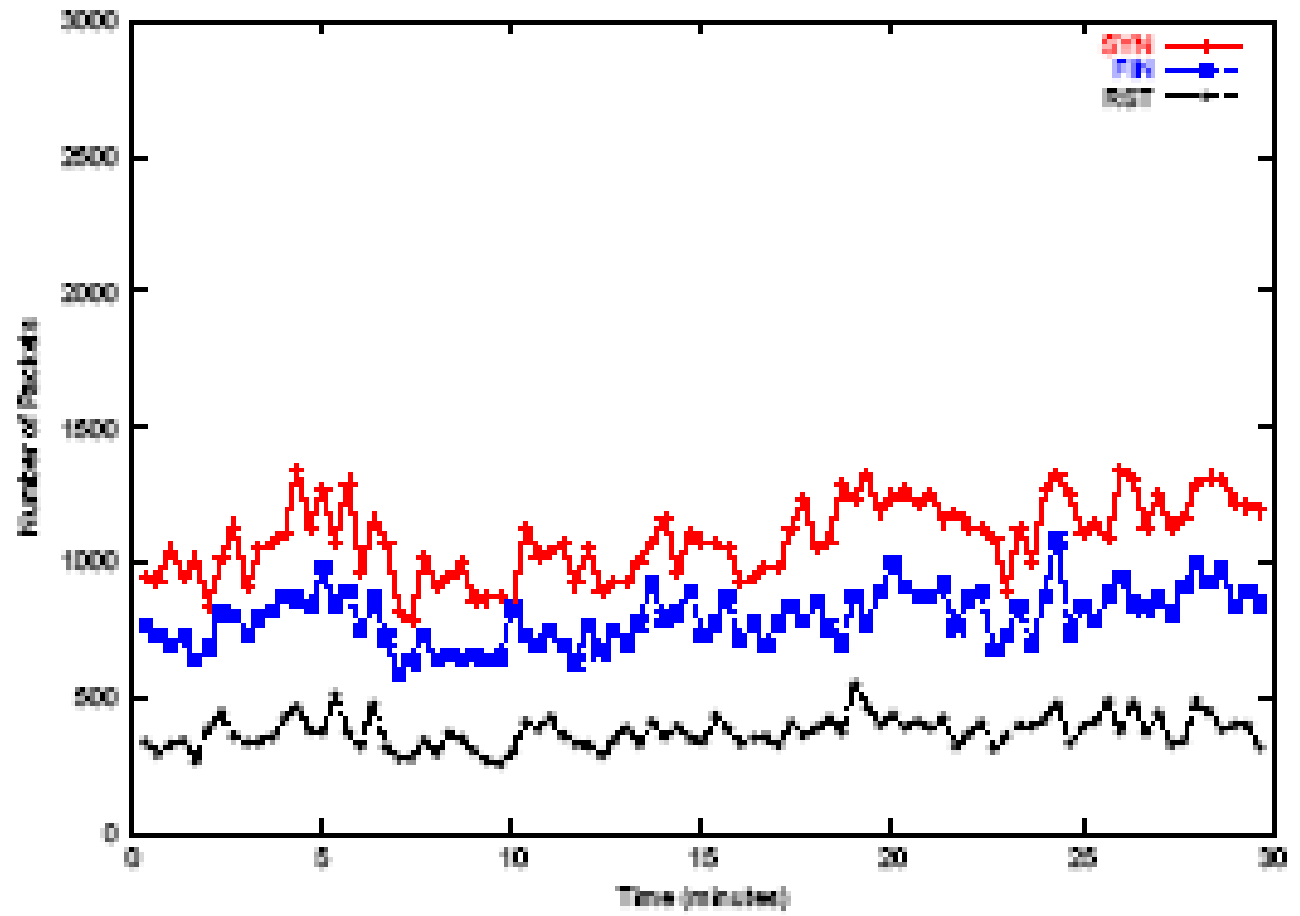
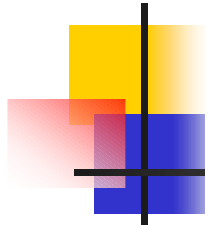
Trace	Starting time	Traffic type
DEC-1	2:00, Thu Mar 9, 95	Bi-directional
DEC-2	10:00, Thu Mar 9, 95	Bi-directional
Harvard-1	12:39, Thu Mar 13, 97	Bi-directional
Harvard-2	16:39, Thu Mar 13, 97	Bi-directional
UNC-in	19:30, Wed Sept 27, 00	Uni-directional
UNC-out	19:30, Wed Sept 27, 00	Uni-directional

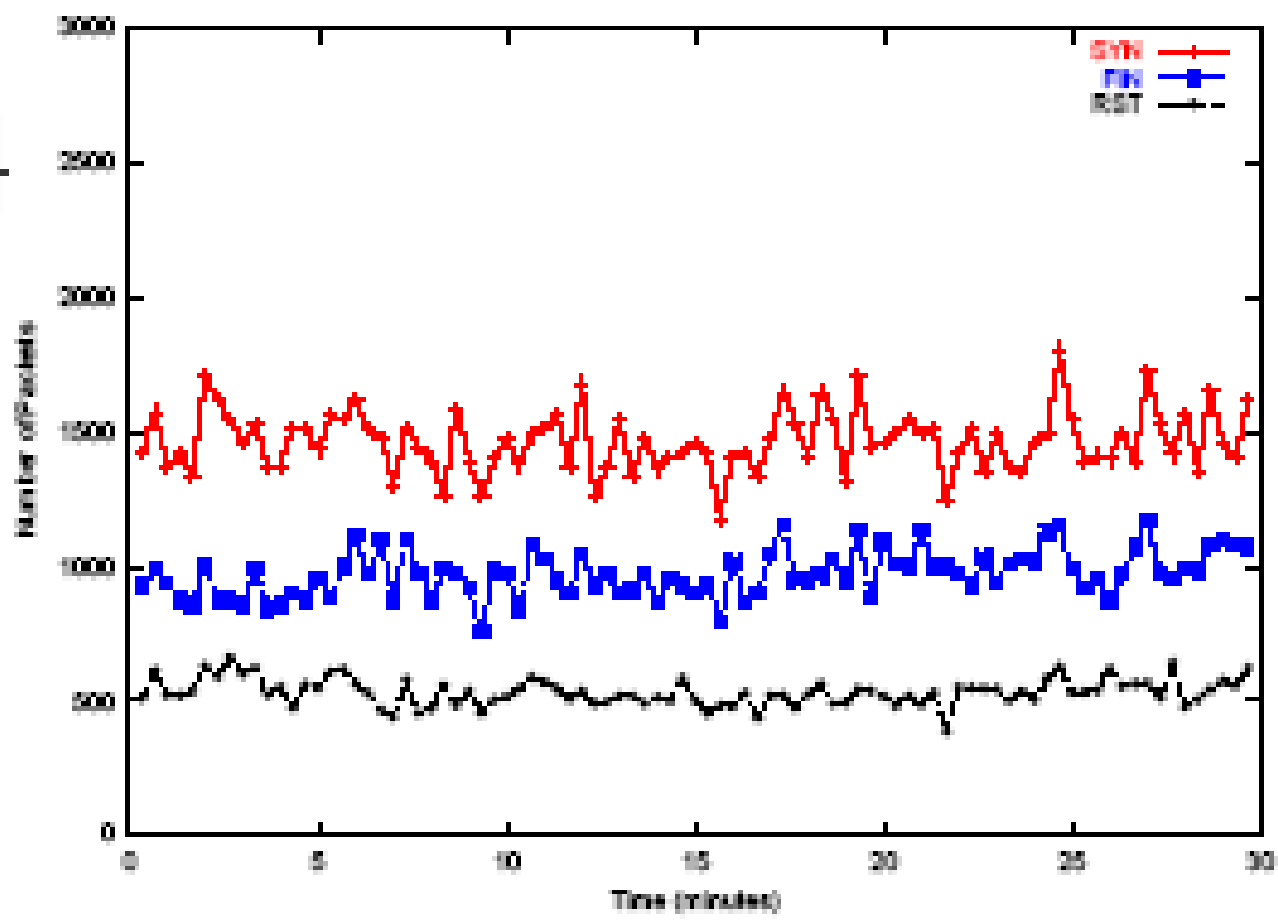
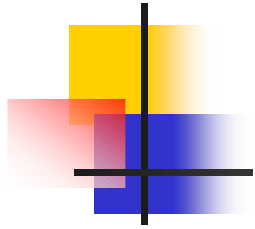


(a) DEC-1

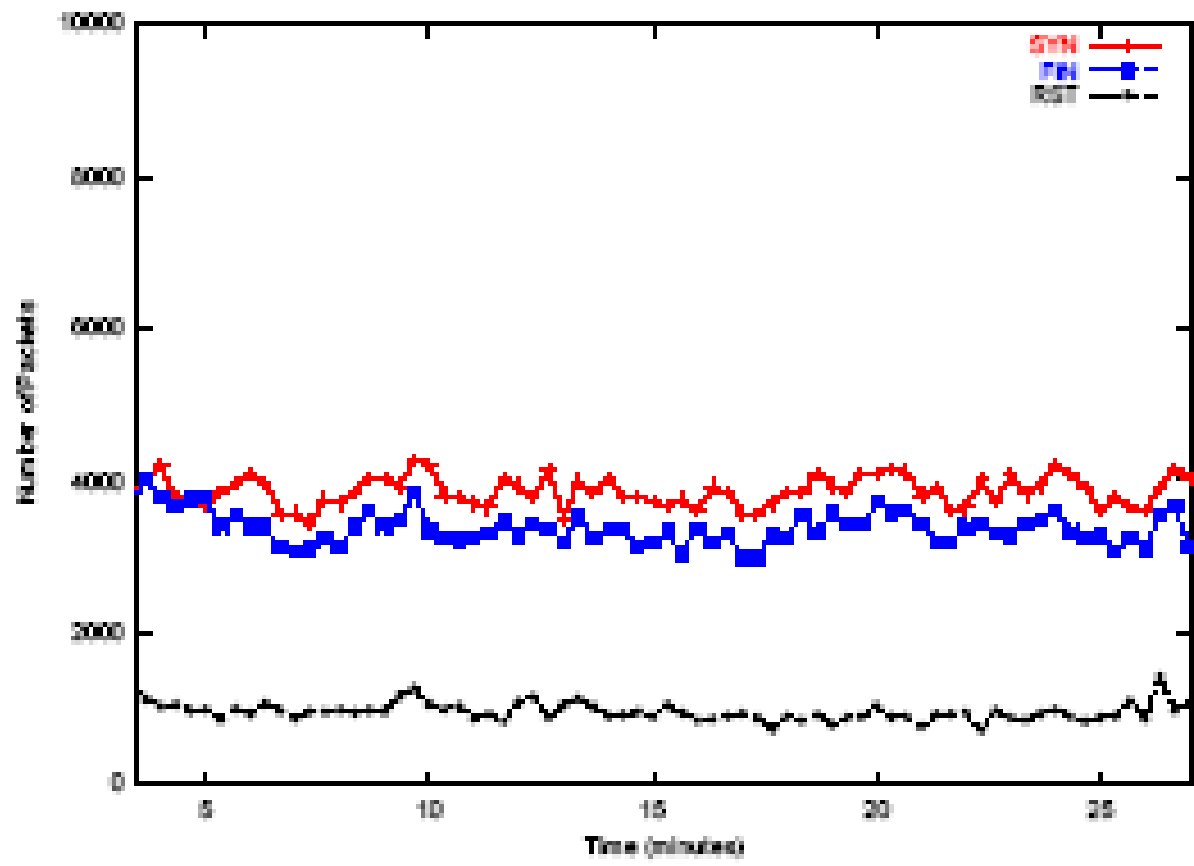
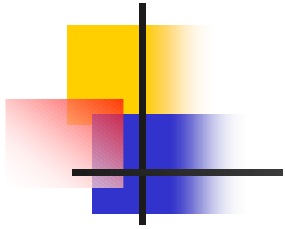


(b) DEC-2

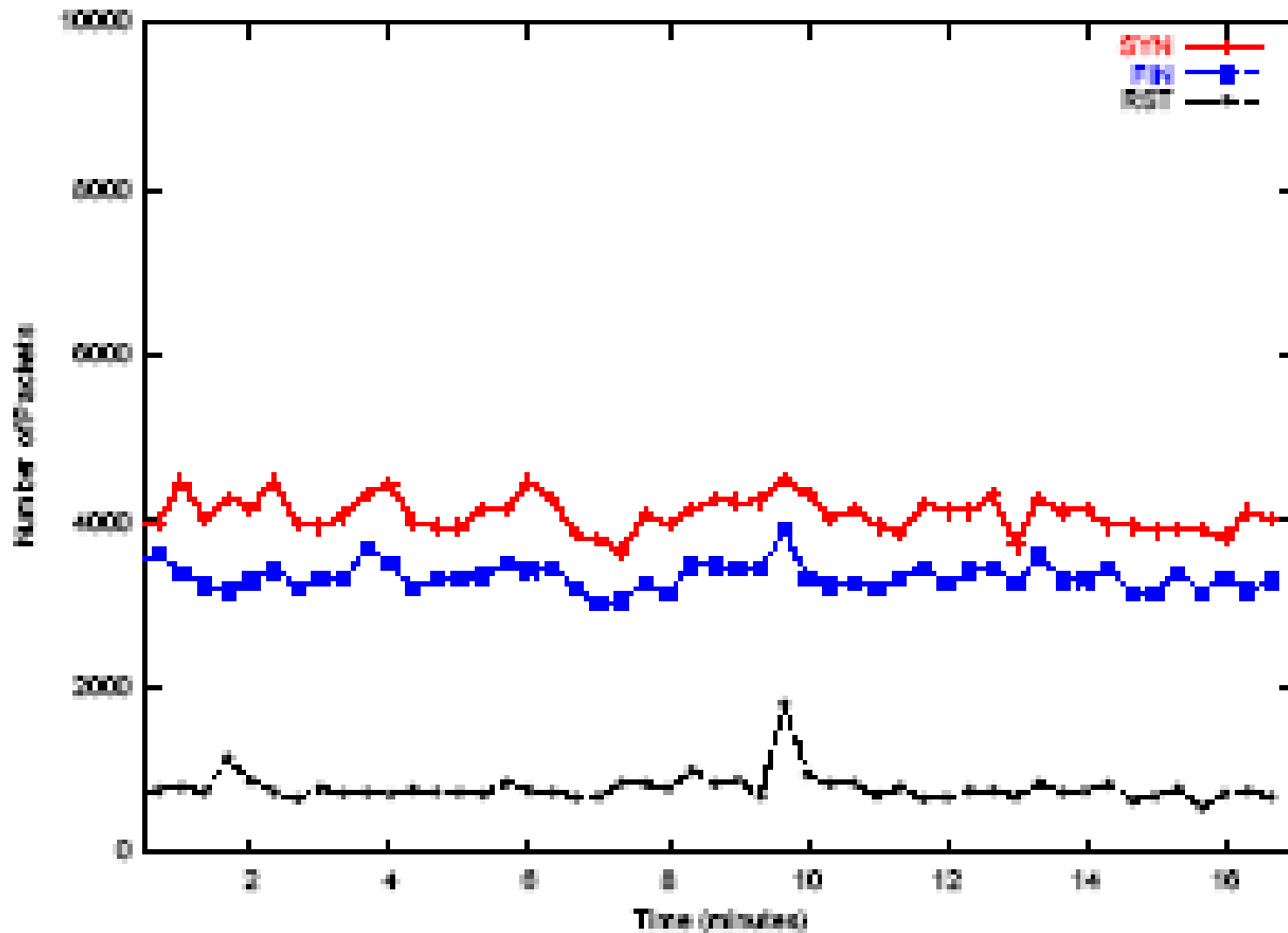


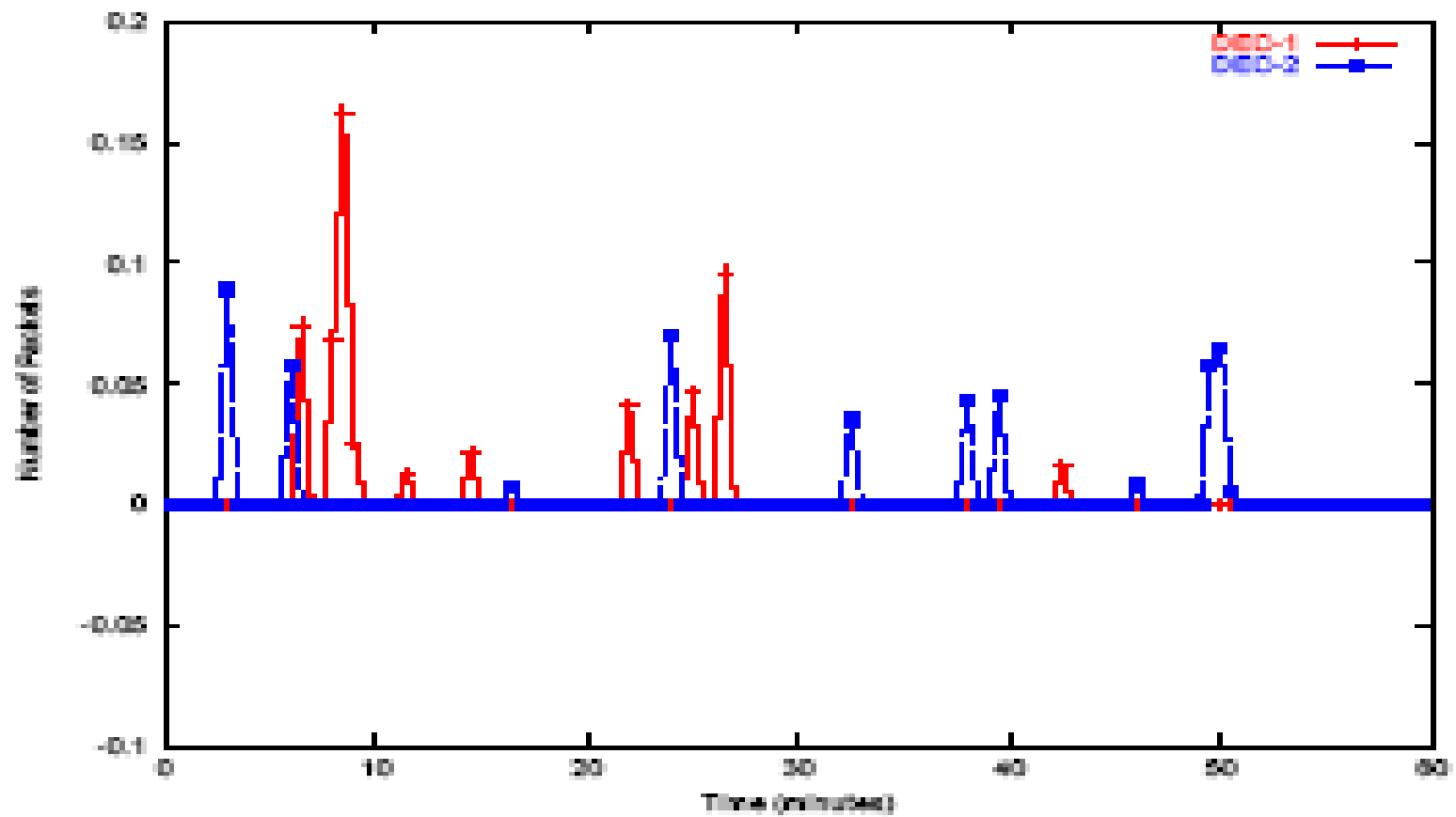


(a) Harvard-2

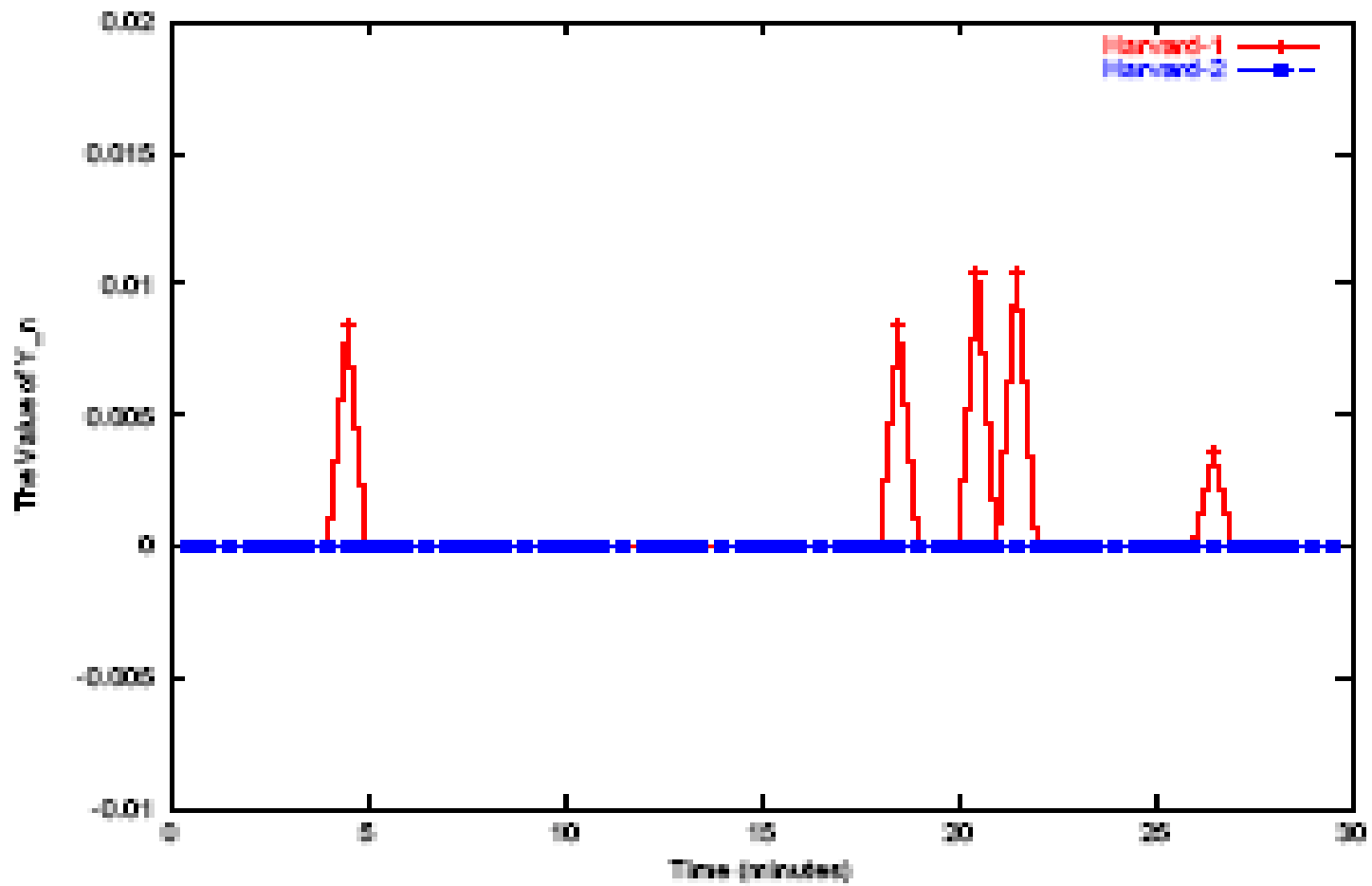


(b) UNC-in

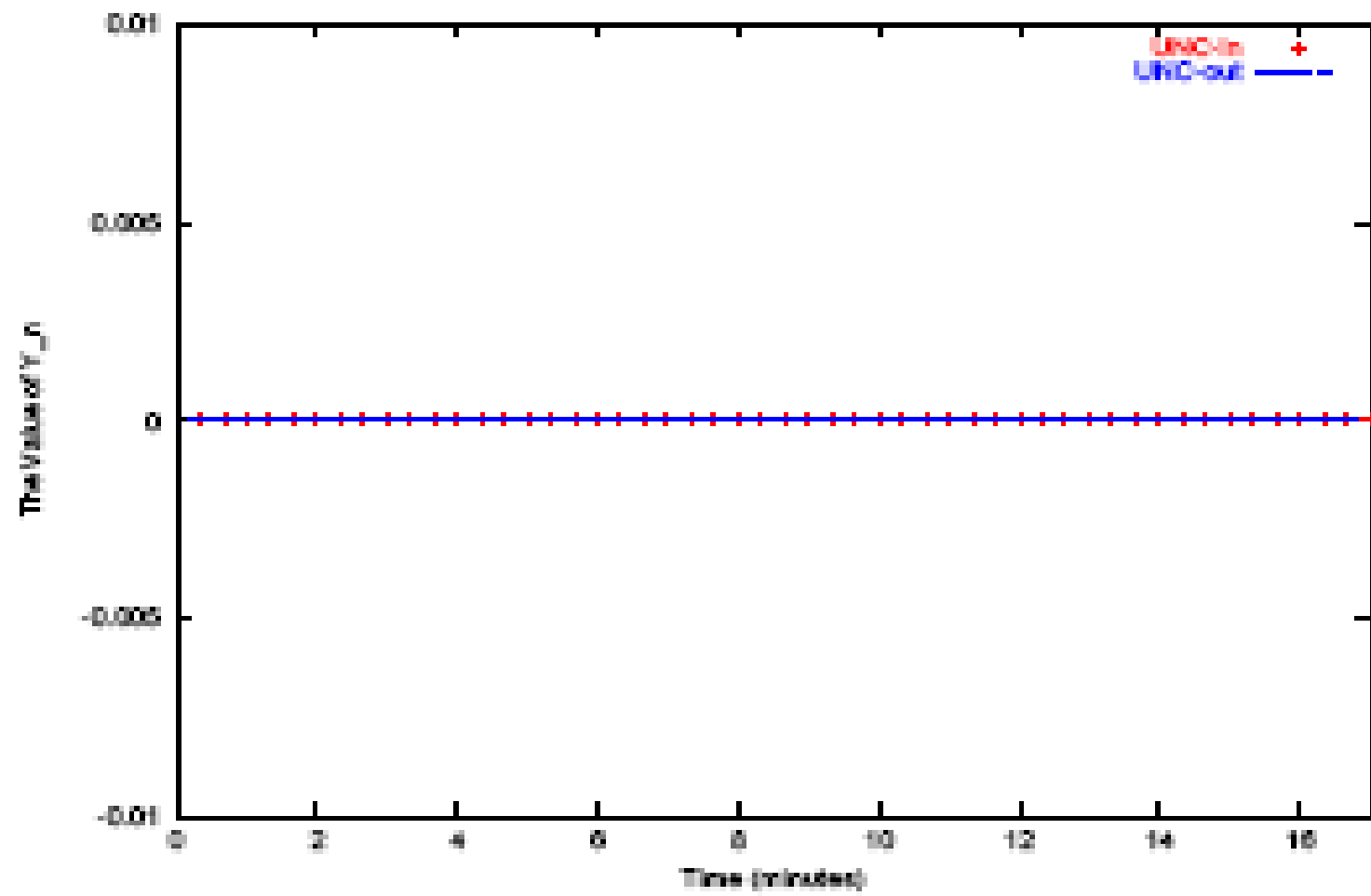




(a) DEC



(b) Harvard



(c) UNC



# SYN Flooding Detection

---

- UNC 2000 used a normal traffic
- UNC\_in inbound as Last-mile monitoring
- UNC\_out outbound as First-mile monitoring
- Flooded traffic is mixed and FDS is simulated at the leaf router

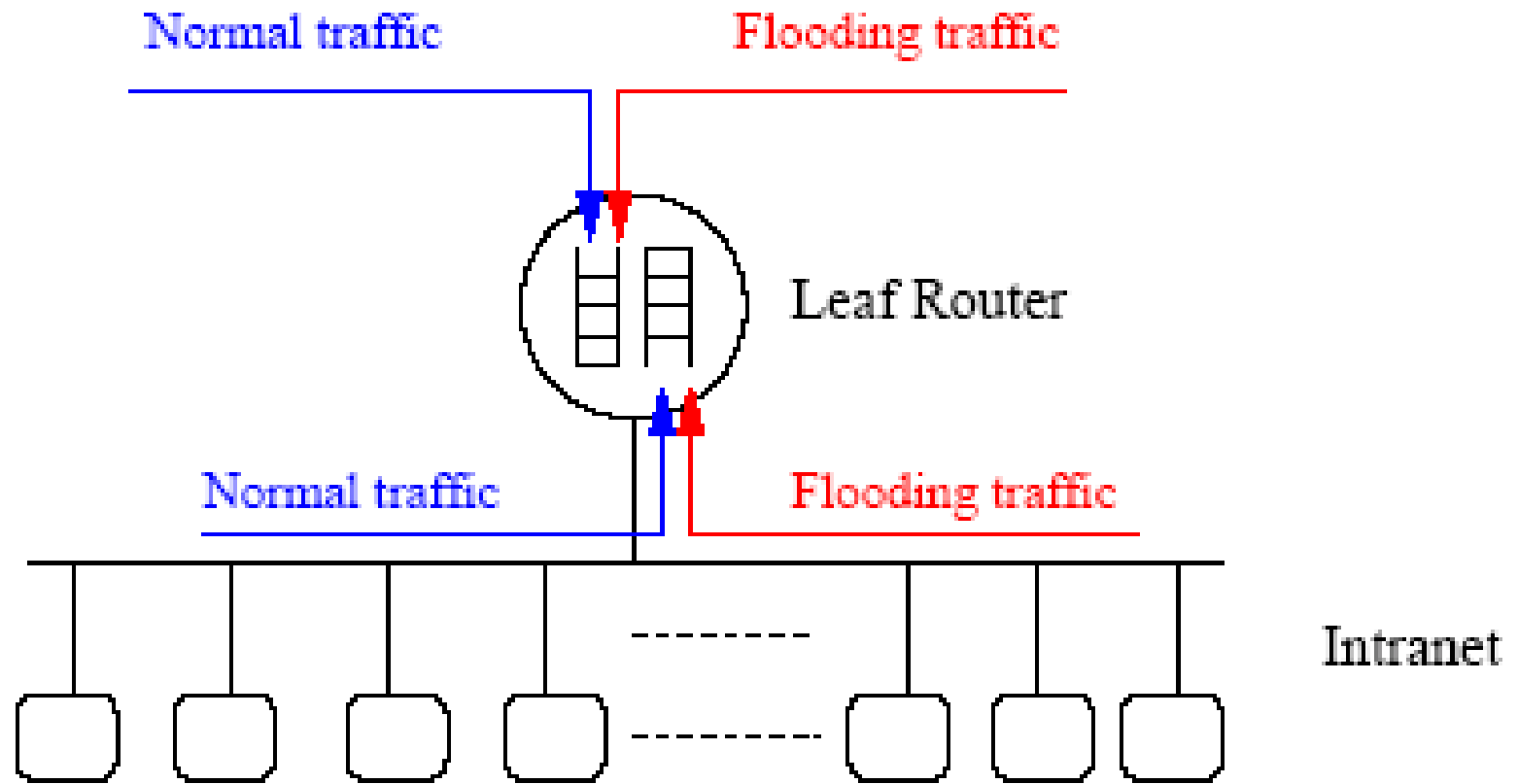
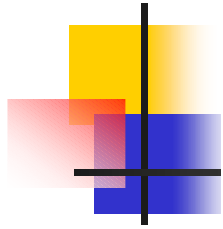
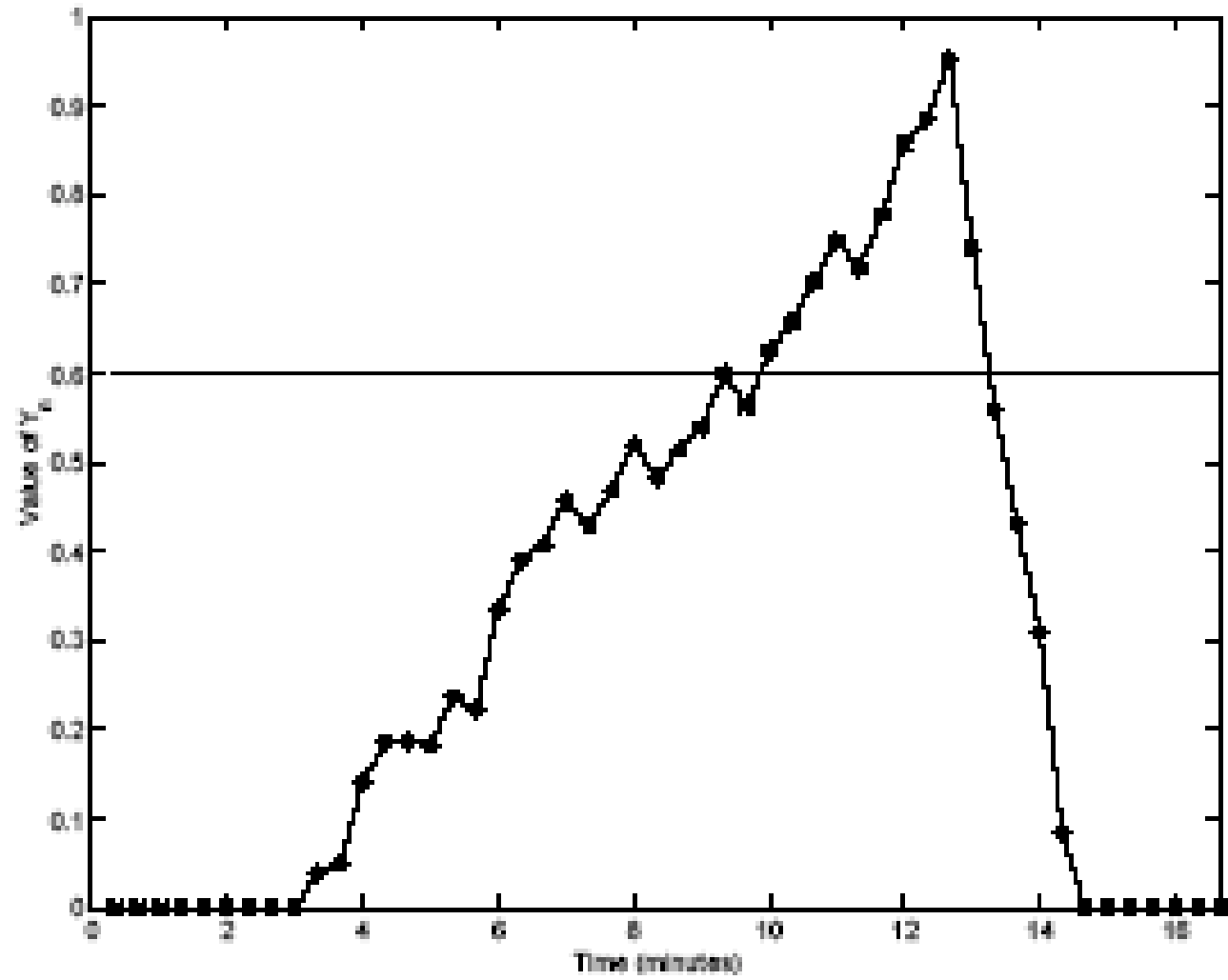
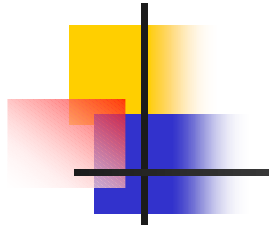
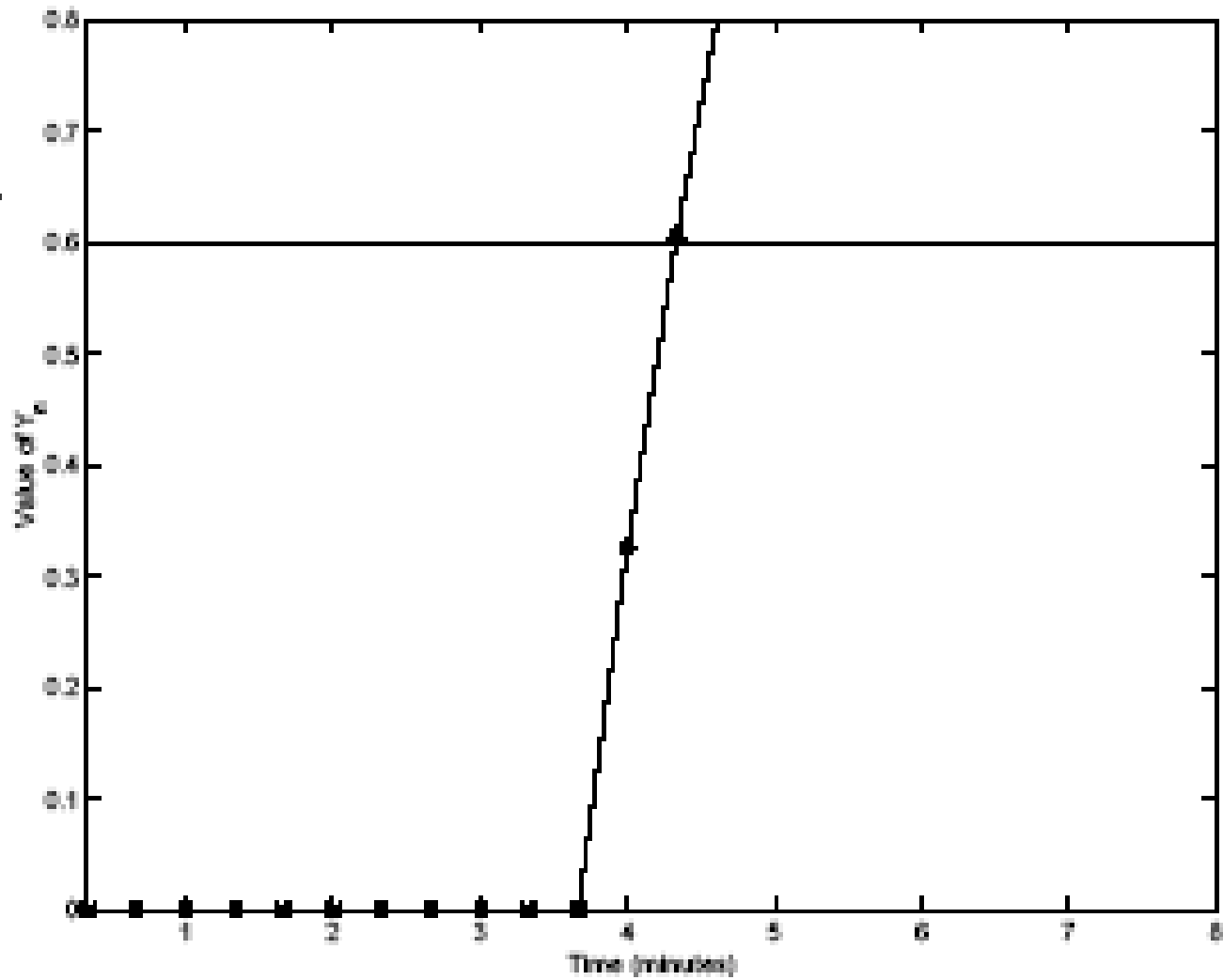
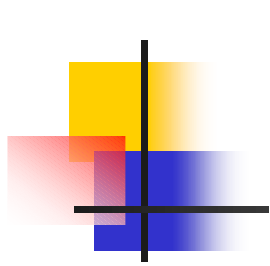


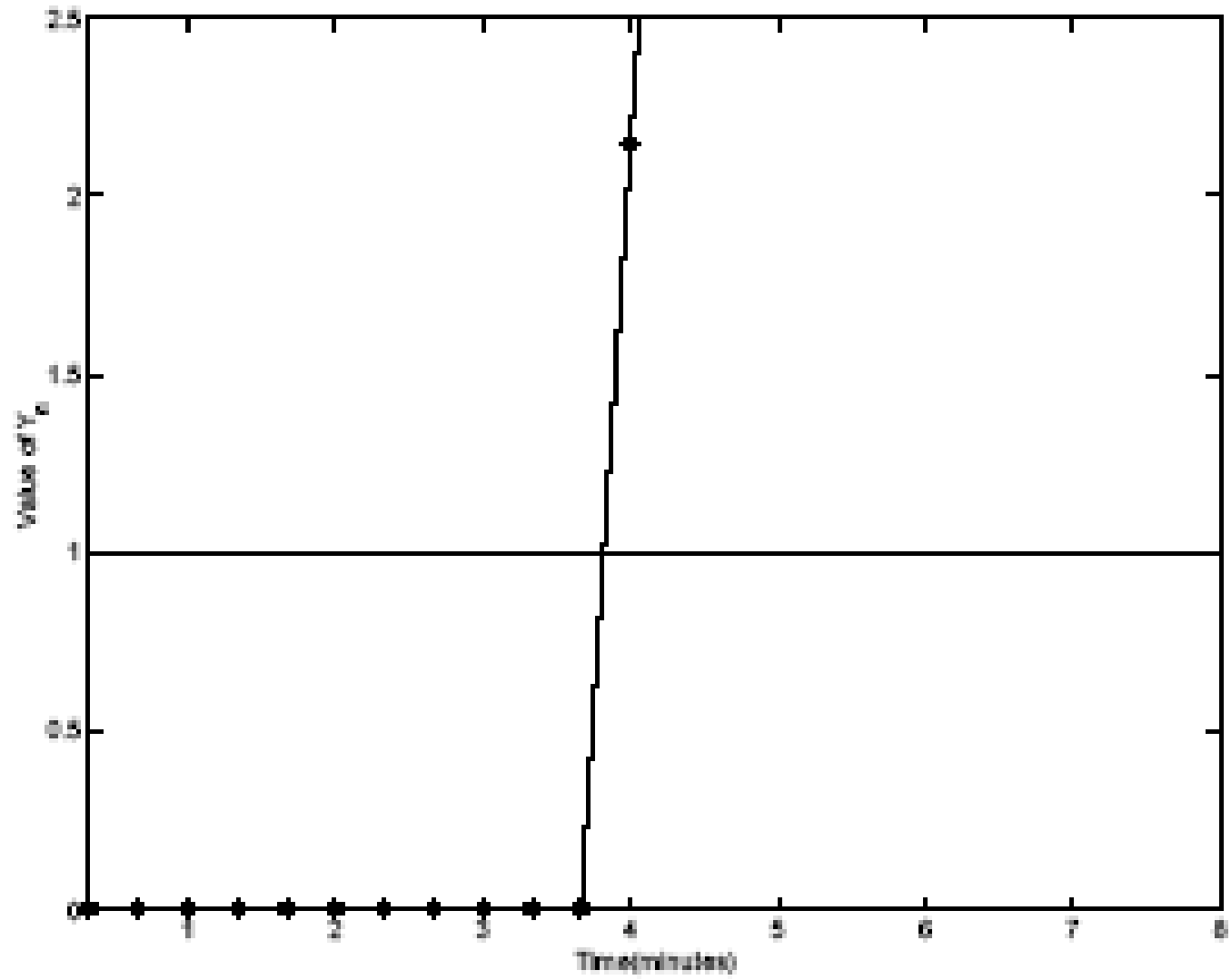
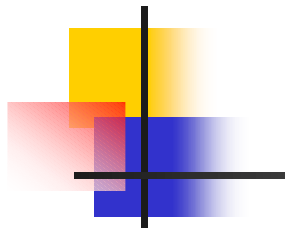
Fig. 8. The trace-simulation flooding attack experiment



(a) 35 SYNs per second



(b) 80 SYNs per second



(c) 500 SYNs per second

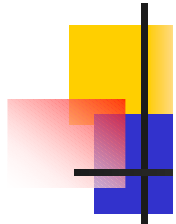


TABLE II  
DETECTION PERFORMANCE OF THE FIRST-MILE FDS

$f_i$ (SYNs/s)	Detection Prob.	Detection Time
33	70%	24.36
35	100%	17.25
40	100%	9.2
50	100%	4.75
60	100%	3.0
70	100%	2.4
80	100%	1.8
90	100%	1.2
100	100%	1.0



## Future Work

---

- SYN-FIN detection paralyzed is the attacker sends SYNs and FINs



# Conclusion

---

- SYN flooding detection installed at leaf router
- FDS is stateless and low computation overhead
- In-sensitive to the site
- Does not under mine the end-to-end TCP performance.