# Firewalls and Intrusion Detection Systems: Part 8

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

# References

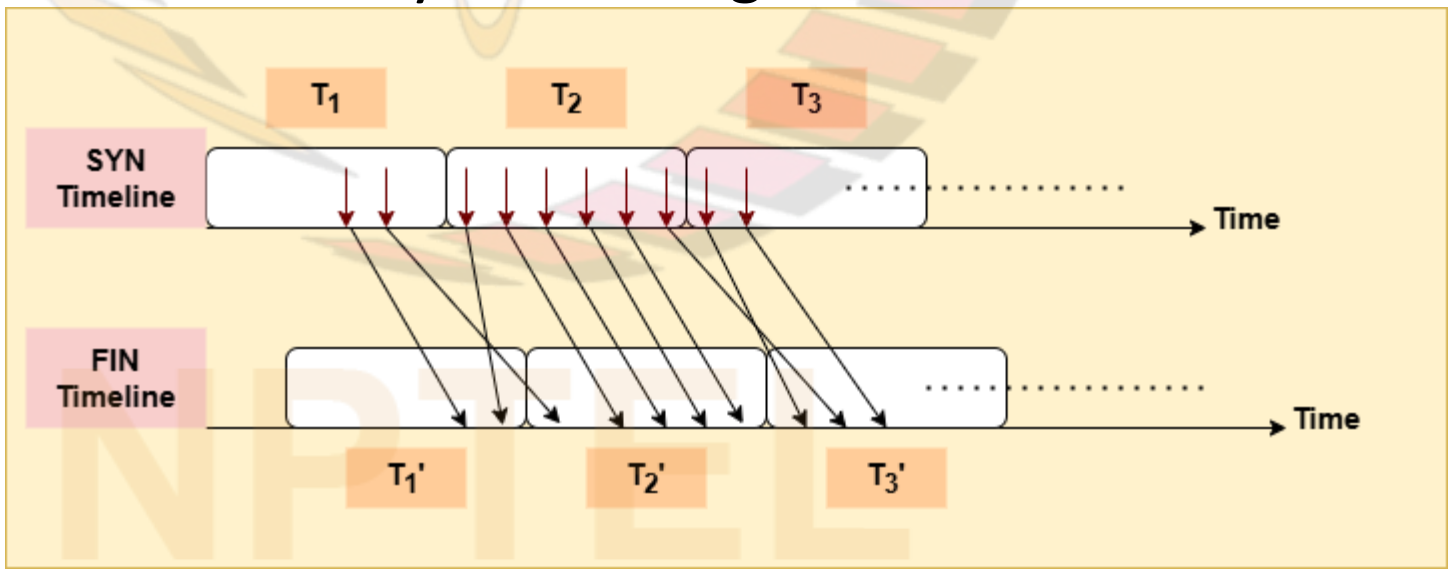

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2012
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt. Ltd., 2018
- C. Kaufman, R. Perlman, M. Speciner, "*Network Security: Private Communication in a Public World*", Pearson Education, 2nd edition, 2002

# DDoS Detection

- Egress filtering and DRF are preventive mechanisms
- Alternative approach: detect the onset of DoS and then take remedial action
- Recall:
  - TCP connection initiated by three-way handshake in which SYN, SYNACK, and ACK packets are sent
  - TCP connection closed by each side by sending a FIN, which is ACKed by other side
- So for legitimate connections, a server receives SYN packets and FIN packets in pairs
- But in a SYN flood attack, the victim receives much larger number of SYN packets than FIN packets
- This fact can be used to detect SYN flood attack by a victim as we explain next

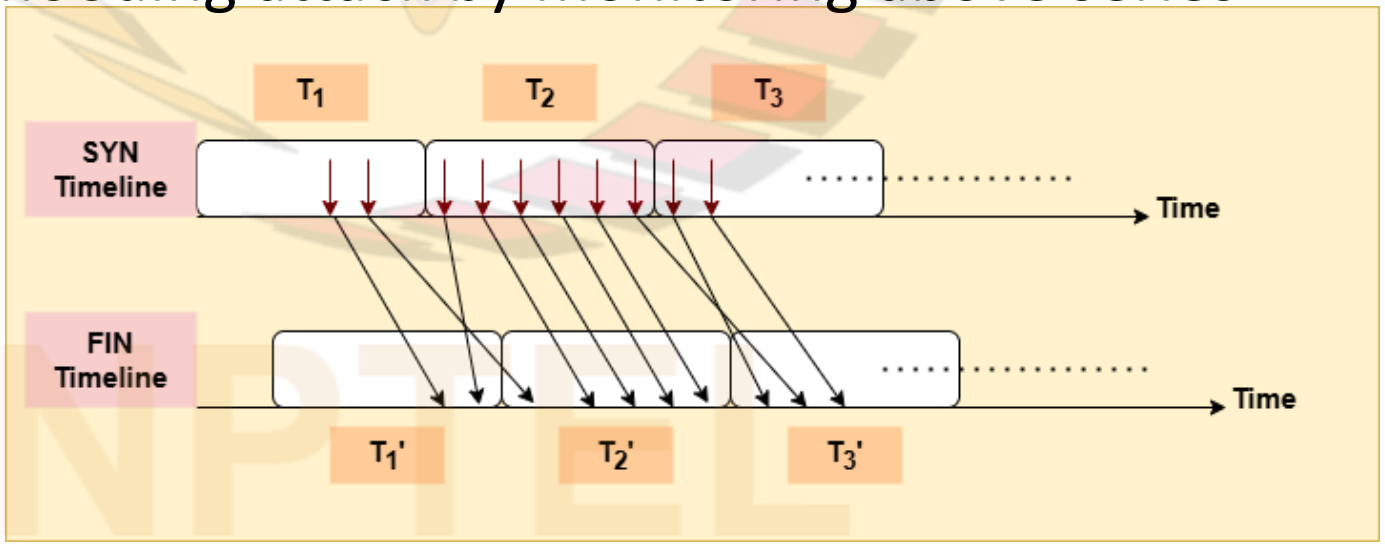
# DDoS Detection (contd.)

- Fig. shows two horizontal timelines:
  - top line shows the times of SYN packet arrivals
  - bottom line shows corresponding FIN arrivals
- Time is slotted into fixed-length "observation intervals":
  - $T_1, T_2, T_3, \ldots$ on the SYN timeline, during which we record the number of SYN arrivals
  - $T_1', T_2', T_3', \ldots$ on the FIN timeline, during which we record the number of FIN arrivals
- The observation intervals for FINs are shifted to the right relative to those for SYNs by the average duration of a TCP connection



# DDoS Detection (contd.)

- To construct an anomaly detection system, we define the following variables:
  - $S_i$: no. of SYN packet arrivals in $i$'th observation interval
  - $F_i$: no. of FIN packet arrivals in $i$'th observation interval
  - $D_i = \frac{S_i - F_i}{F_i}$
  - $\mathcal{T}$: threshold for detection
- Consider the time series:
  - $D_1, D_2, D_3, \ldots$
- Next, we discuss various algorithms that attempt to detect onset of a SYN flooding attack by monitoring above series

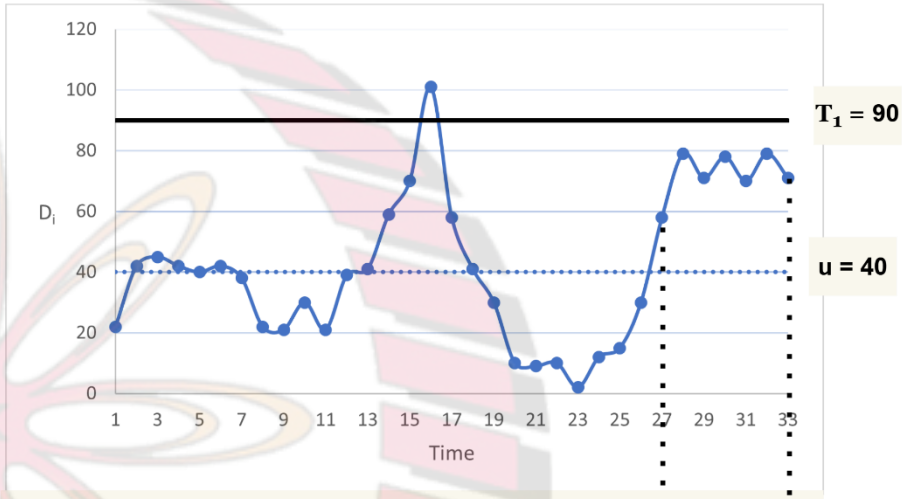


# DDoS Detection (contd.)

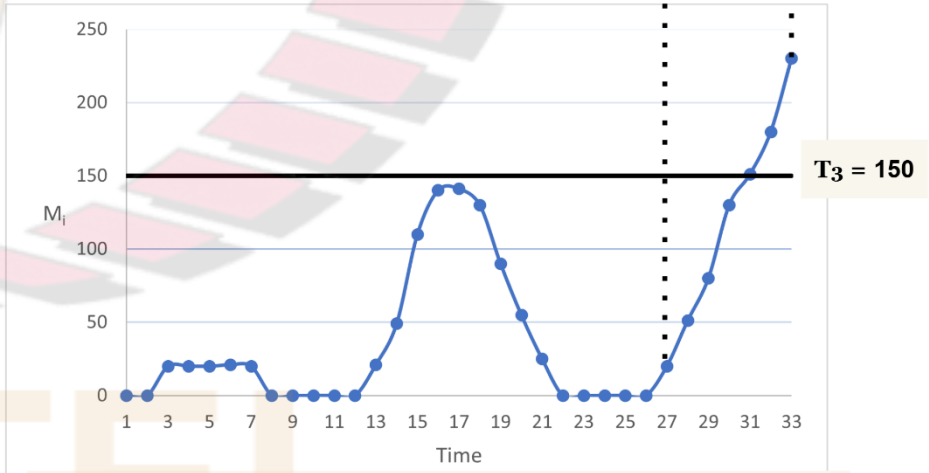
- **Algorithm 1**:
  - ❑ Raise an alert if the most recently computed decision variable $D_i$ exceeds the threshold, i.e., if $D_i > \mathcal{T}_1$
- Shortcomings of Algorithm 1:

❑ The IDS may raise many *false alarms* since it bases its decision on point values
- E.g., at time = $16$ in fig. (a), the value of $D_i$ rises to $102$, triggering an alarm
- However, this alarm is unwarranted since the $D_i$ values at neighboring points (around time = $16$) are well below the threshold $\mathcal{T}_1$
- A modest spike in $D_i$ at just one point is unlikely to result in memory exhaustion, but it causes IDS to raise an alarm

❑ The IDS may fail to raise alarms when an attack occurs
- In fig. (a), the values of $D_i$ between time $28$ and $33$ are just below the threshold $\mathcal{T}_1$
- Cumulative effect of the attack packets across the interval will result in memory exhaustion, but the algorithm does not raise an alarm



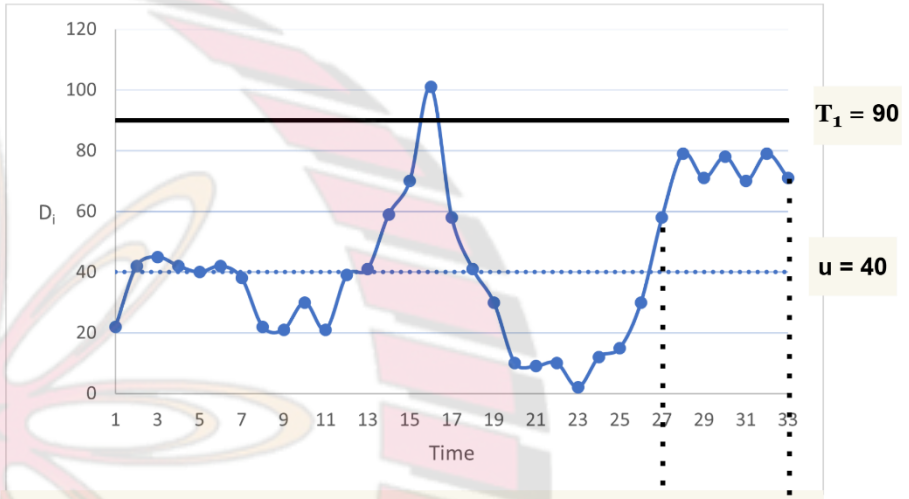

(a) $D_i$ versus time
$T_1$ = Threshold in Algorithm 1,
u = Upper bound on the mean of $D_i$ in Algorithm 3



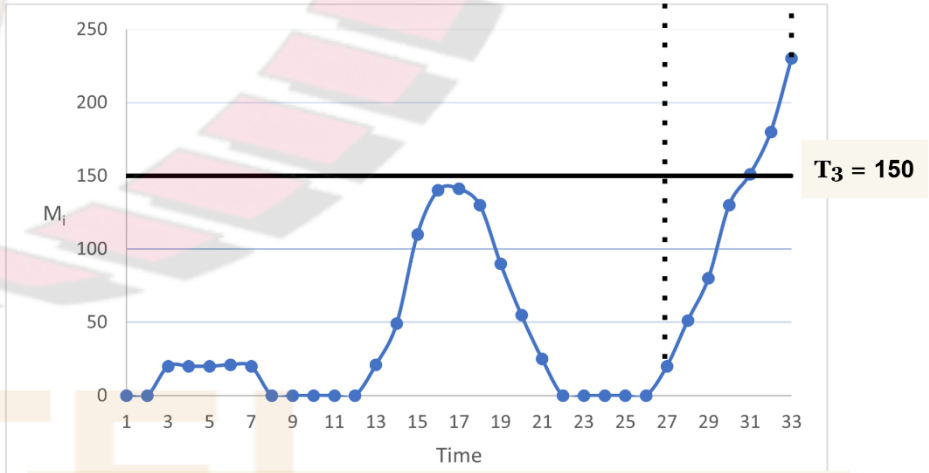

(b) $M_i$ versus time (Algorithm 3),
$T_3$ = Threshold in Algorithm 3.

# DDoS Detection (contd.)

- **Algorithm 2**:
  - ❑ Raise an alert if the *exponentially smoothed average* of the values of $D_i$ exceeds the threshold
- Let $S_i = \alpha D_i + (1 - \alpha) S_{i-1}$, where $\alpha \in (0,1)$, e.g., $\alpha = 0.4$
- An alarm will be raised if $S_i > \mathcal{T}_2$, where $\mathcal{T}_2$ is a threshold
- Value of $\mathcal{T}_2$ set based on empirical data
  - ❑ If it is set too low (respectively, high), then will result in a lot of false positives (respectively, false negatives)
- Another design parameter is $\alpha$:
  - ❑ If it is too close to 1, it will give disproportionate importance to the most recent value of $D_i$
  - ❑ The closer to zero it gets, the more even are the weights assigned to all values of $D_i$



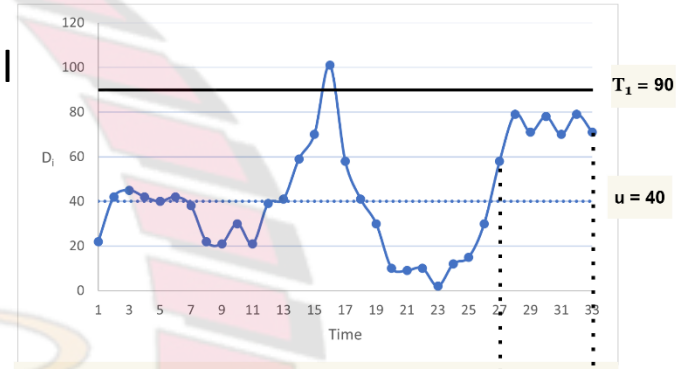

(a) $D_i$ versus time
$T_1$ = Threshold in Algorithm 1,
u = Upper bound on the mean of $D_i$ in Algorithm 3



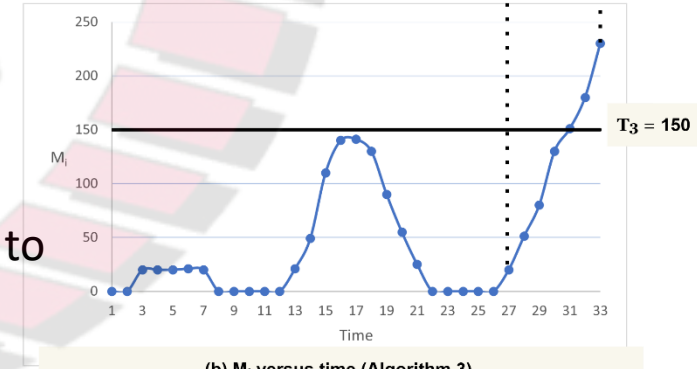

(b) $M_i$ versus time (Algorithm 3),
$T_3$ = Threshold in Algorithm 3.

# DDoS Detection (contd.)

- **Algorithm 3**:
  - Define a *modified cumulative sum* of the previous values of $D_i$
  - Raise an alert if this value exceeds a threshold
- During normal operation, the number of FINs will balance the number of SYNs and hence $D_i = \frac{S_i - F_i}{F_i}$ will be close to $0$
- Let $u$ be an upper bound on the mean of $D_i$ during normal operations
- Let $D_i' = D_i - u$
- Let $M_i = (M_{i-1} + D_i')^+$, with $M_0 = 0$,
  - where $x^+ = \begin{cases} x, & \text{if } x > 0, \\ 0, & \text{else.} \end{cases}$
- The IDS sounds an alarm at the end of the $j$'th interval if $M_j > \mathcal{T}_3$, where $\mathcal{T}_3$ is a threshold that is determined empirically
- Fig. (b) shows $M_i$ versus time with $\mathcal{T}_3 = 150$
- Between time $2$ and $6$, $D_i$ is slightly above $u$, so $M_i$ increases monotonically
- Between time $7$ and $12$, $D_i$ falls below $u$, so $M_i$ decreases to $0$ and remains there until time $12$
- Between time $27$ and $33$, $D_i$ is consistently above $u$, although it is below the threshold $\mathcal{T}_1 = 90$
- This causes $M_i$ to increase and it overshoots the threshold of $\mathcal{T}_3 = 150$; this causes an alarm to be raised
  - this is a true positive due to cumulative build-up of SYN attack packets
- Thus, false positive and false negative encountered with Algorithm 1 are both avoided with Algorithm 3




(a) $D_i$ versus time
$T_1$ = Threshold in Algorithm 1,
u = Upper bound on the mean of $D_i$ in Algorithm 3




(b) $M_i$ versus time (Algorithm 3),
$T_3$ = Threshold in Algorithm 3.