

SYN Flooding Attack Detection by TCP Handshake Behaviour Observation

Martine Bellaïche

professor at École Polytechnique de Montréal

Jean-Charles Grégoire

professor at INRS-EMT

Goals

- **Detection of SYN flooding attack.**
- **On the victim's side.**
- **Monitoring TCP handshake behaviour.**
- **An architecture for a good detection.**

Agenda

- 1. Unusual Handshake Detection (UHD)**
- 2. TCP Handshake**
- 3. SYN Flooding Attack**
- 4. Usual and Unusual TCP Handshakes**
- 5. Detection Technique Architecture**
- 6. Evaluation of Detection Method**
- 7. Characteristics of DDoS Attacks**
- 8. Performance Evaluation**
- 9. Discussion and Conclusion**

Unusual Handshake Detection (UHD)

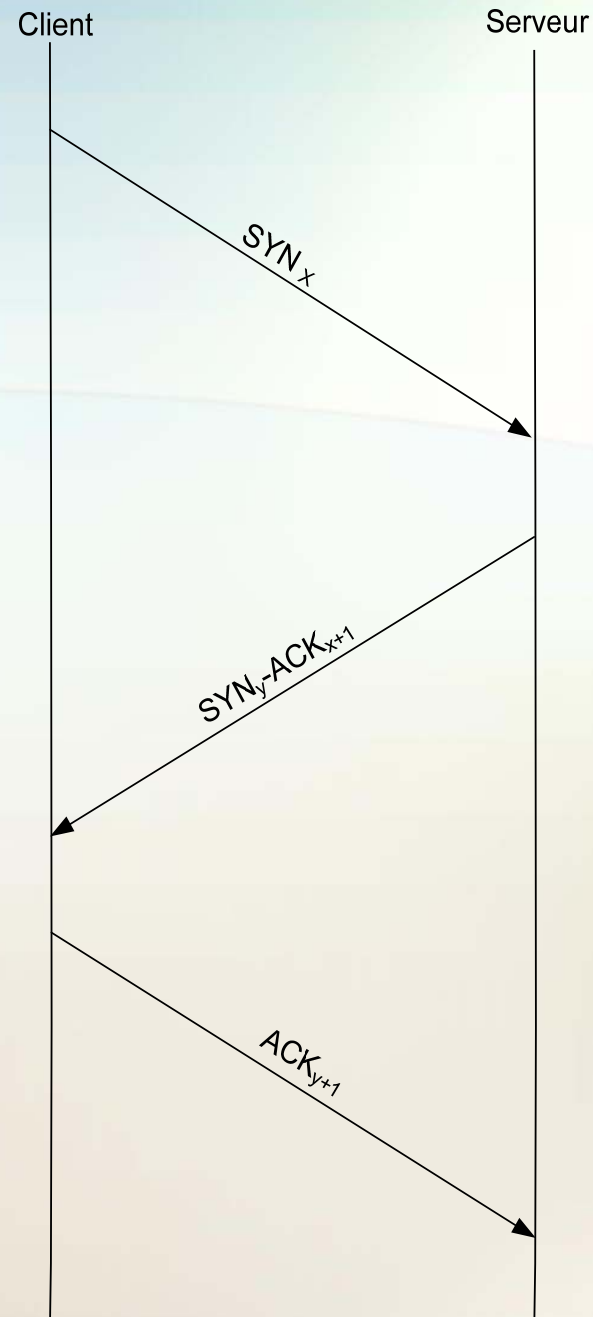
- **Their detection/collection/measure is used to detect DDoS.**
- **Used to classify the different forms of TCP handshakes during a connection setup between a client and a server.**
- **During a denial of service attack, some handshake sequences are unusual.**

TCP Handshake

A 3-way handshake:

Exchange of 3 packets.

Reserve and announce suitable resources at both ends before data exchange can proceed.

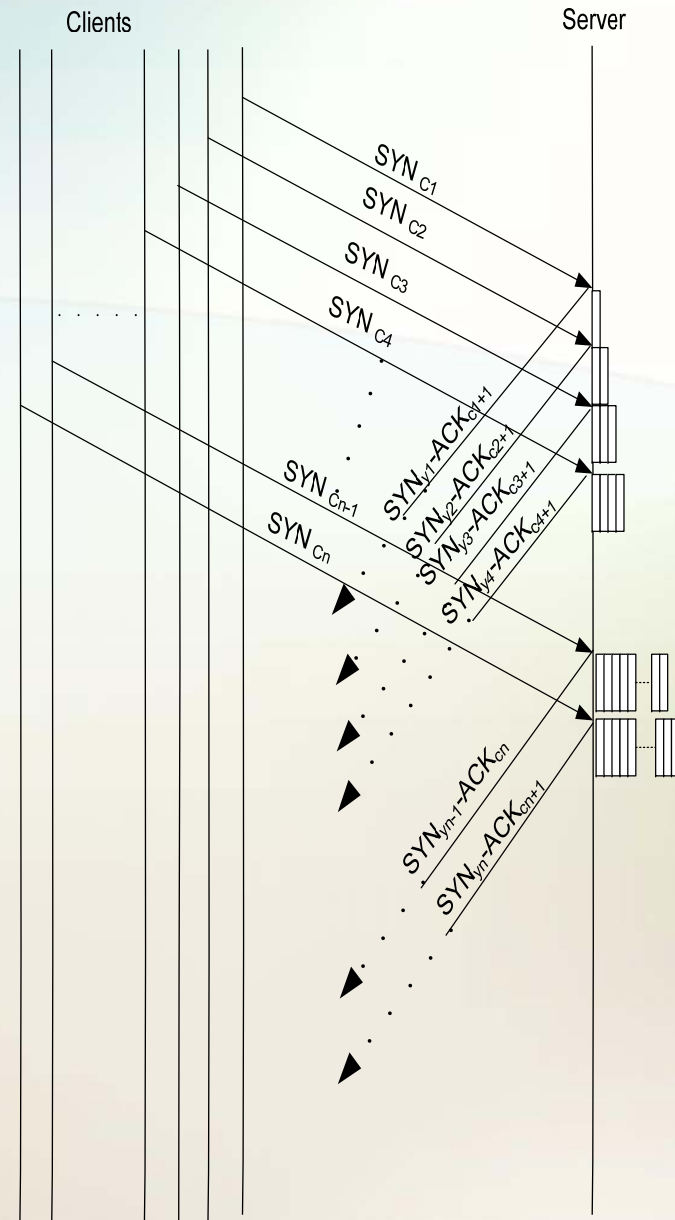


SYN flooding attack

- **90% of DDoS attacks.**
- **To submerge the victim with traffic pretending to open a new TCP connection, thus abusing the handshake mechanism.**
- **To tie the memory of server machines with half-open connections.**

SYN flooding DDoS attack

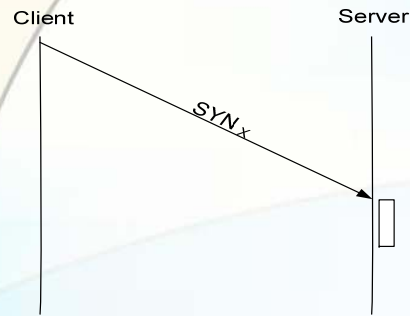
- Attackers send to the server a SYN packet with a forged (spoofed) address.
- This could be done by zombies.



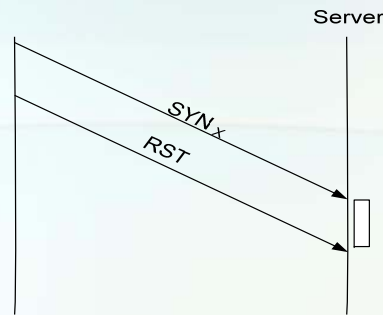
Usual and Unusual TCP Handshakes

- **TCP handshakes whose sequence does not follow the 3 steps standard.**
- **Not only SYN flooding.**
- **Unusual TCP handshakes result from:**
 - **Network congestion.**
 - **Router errors.**
 - **DDoS attack.**

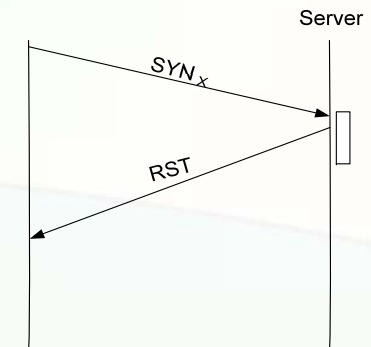
Handshake Sequences With Attack Sequence A, C, D, E



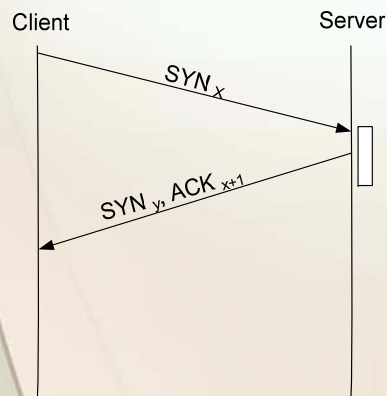
A



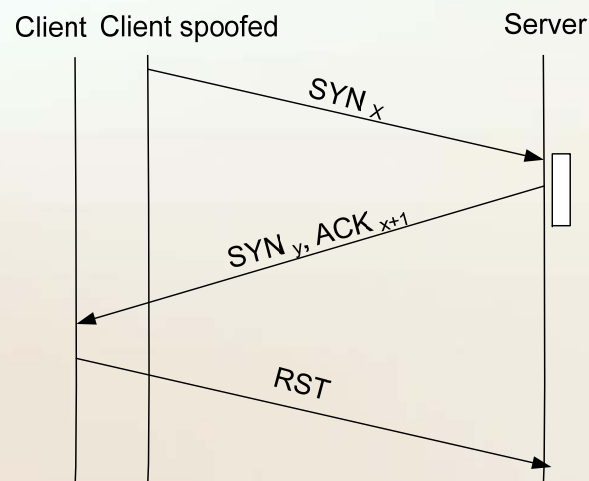
B



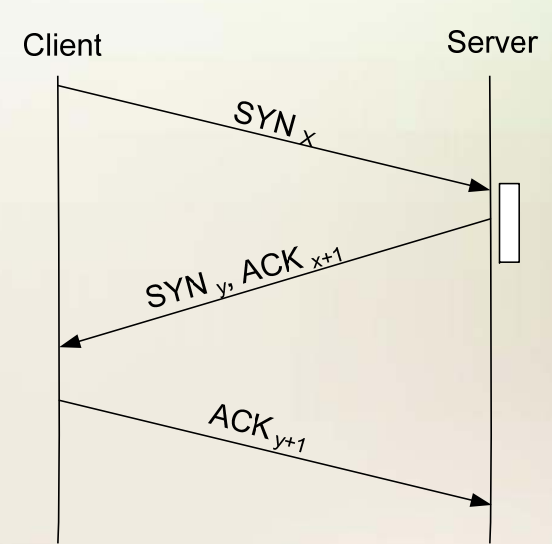
C



D



E



F

Handshake Sequences (cont'd)

(SYN, delay).

(SYN (Client, Server), RST (Server, Client)).

(SYN, SYN/ACK, delay).

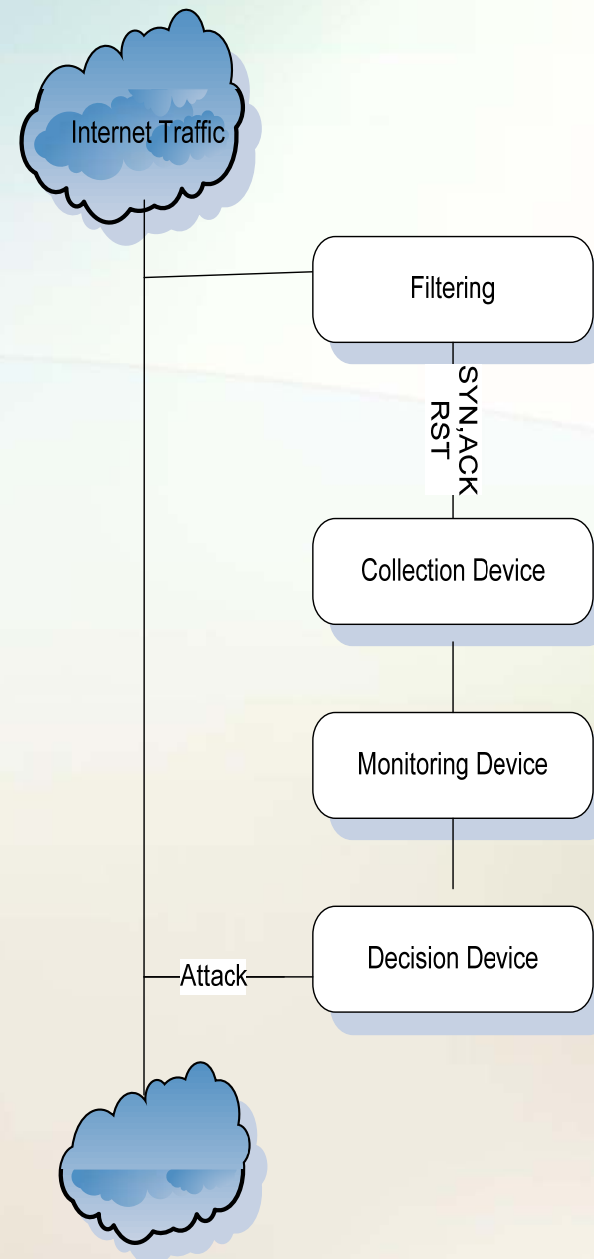
(SYN, SYN/ACK, RST).

Delay

- **the time--out of the server.**
- **Data structure for an estimate of TCP connection latency:**
 - ✓ RTT.
 - ✓ TCP data structure.

Detection Technique Architecture

A decomposition is necessary to identify all the detection aspects.



Collection Device

- **To filter TCP SYN, TCP ACK and TCP RST packets.**
- **Database of the TCP flow information.**
- **Database to estimate the detection delay for the unusual handshake.**

Decision Device: Anomaly Detection Algorithm

- **CUSUM Algorithm,**
 - a sequential change point.
 - a non-parametric method based on a monitored variable
- **Monitored variable**
 - An appropriate choice for the detection of SYN flooding attacks

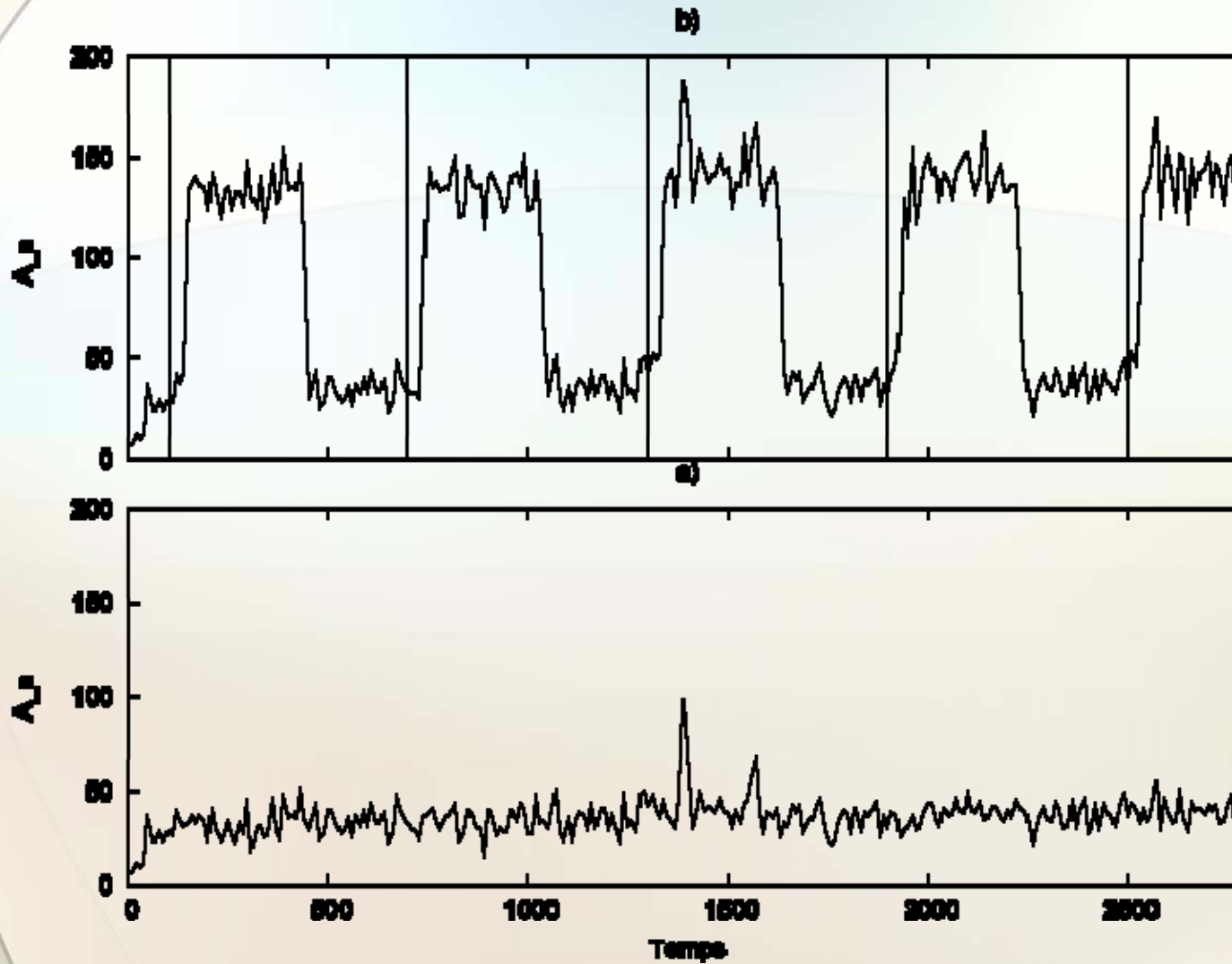
CUSUM Algorithm

- **To detect anomalies in real time, with small execution time.**
- **To detect a change based on the cumulative effect of changes in a monitored variable.**

Monitored variable

- **The observation of an instance of an unusual handshake sequence.**
- **It increases significantly and abruptly during a DDoS attack.**

Monitored variable (cont'd)



Monitored variable (cont'd)

- Unusually important increase of handshakes to detect a DoS attack.

B_n = usual handshakes.

A_n = unusual handshake.

\bar{A} = average calculated when there is no attack.

- CUSUM variable

$$X_n = \frac{|A_n - \bar{A}|}{A_n + B_n}$$

Please Note That

- **Under normal circumstances, the ratio of the unusual handshakes versus all handshakes is more or less constant. If not, we use the EWMA of A_n .**
- **Except for a SYN flooding attack a possible cause would be a simultaneous increase of congestion across the different transit networks.**
- **It is however extremely unlikely that such events would occur simultaneously. Unless the first results in the second.**

Evaluation of Detection Method

- **Performance Criteria:**
 - **Detection time.**
 - **Detection rate.**
 - **False positive rate.**
- **Require TCP link trace containing bidirectional traffic to represent normal traffic.**

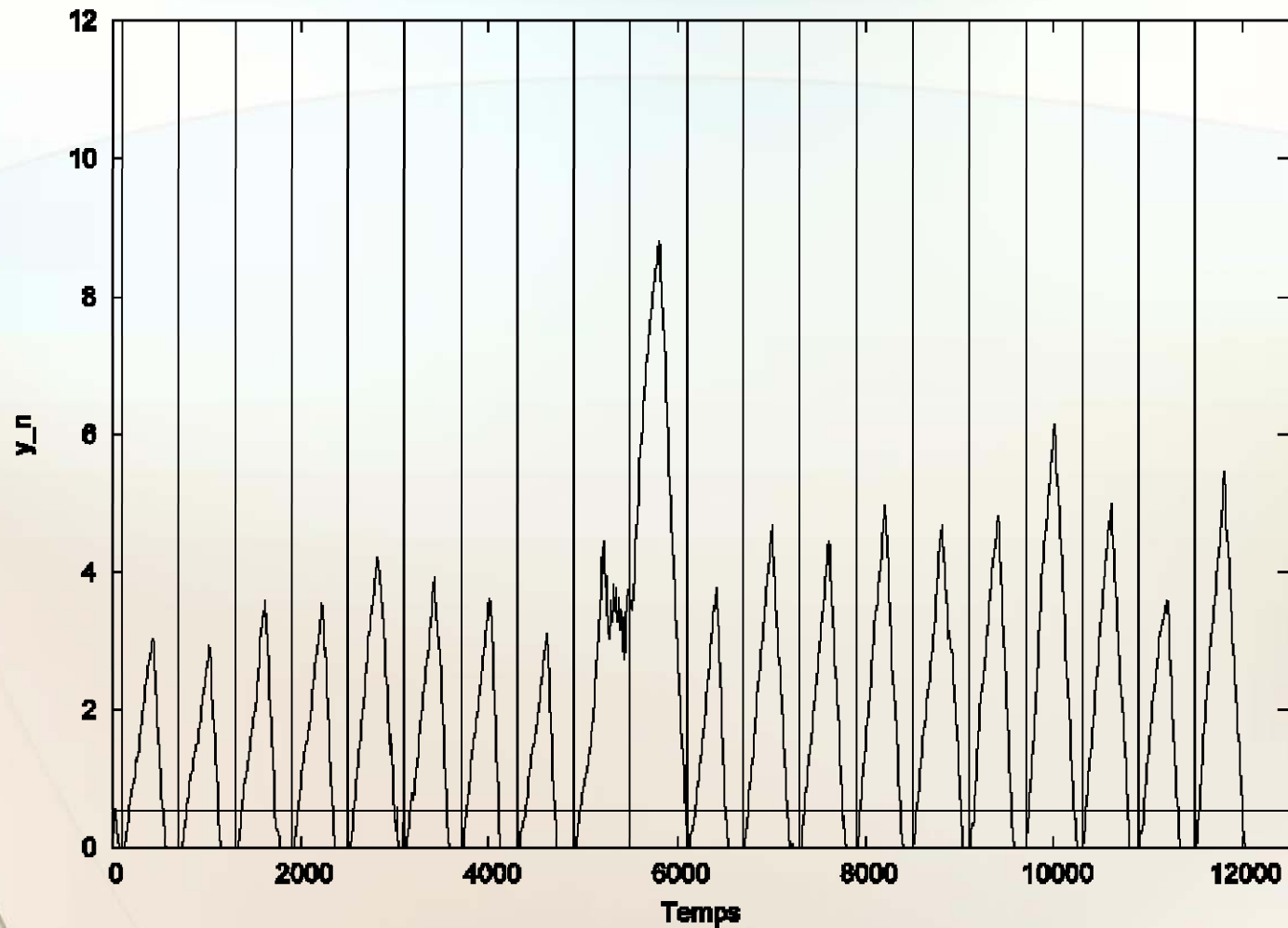
Characteristics of DDoS Attacks

- **To emulate a SYN flooding attack:**
 - **TCP SYN packets.**
 - **Rate of 25% of the mean SYN packet rate of normal traffic.**
 - **Source address and the source port of the attack packet are generated with a uniform distribution.**
 - **Other fields of the attack packets are assigned to arbitrary values.**
 - **Starts at 100s.**
 - **Duration and the inter-arrival time between two attacks have a constant value of 300s.**
 - **20 attacks in total (for the duration of the trace).**

Performance Evaluation

- **Merge attacks with the normal traffic trace.**
- **An attack is detected when the value of the CUSUM variable exceeds the value of the threshold N .**

Performance Evaluation (cont'd)



Performance Evaluation(cont'd)

- **Detection time:**
 - 5 to 8 observation periods of the monitoring device
 - fast detection (usually detection DDoS attack takes 30 observation periods)
- **Detection rate: 100%.**
- **False alarm rate: 0%.**

Note: fake attack at time 5500s is merged with the existing attack at time 5120s.

Discussion

- **UHD would preferably be implemented in the last mile routers. It is not recommended to install the UHD in core routers, as it could not then detect all flooding sources and protect the server victim.**
- **As the detection variable uses a CUSUM decision algorithm, based on the cumulative effect of the monitored variable change, it is not necessary that the attack rate is increasing or pulsing.**

Conclusion

- **Number of unusual handshakes: good choice for detection of the SYN flooding attack.**
- **It is independent from the traffic volume: no produce false alarms during flash crowd.**
- **It does not require a traffic pattern model: CUSUM, is non-parametric.**
- **It does not introduce additional traffic in the network**
- **It is independent of the attack packet attribute characteristics.**
- **It is autonomous: not need other information from other routers.**
- **It is stateful: store the TCP flow information.**
 - **Having more information to make its decision, detection of an attack is more precise with a stateful method and contains fewer false alarms than a stateless method, for example in the case of flash crowds.**