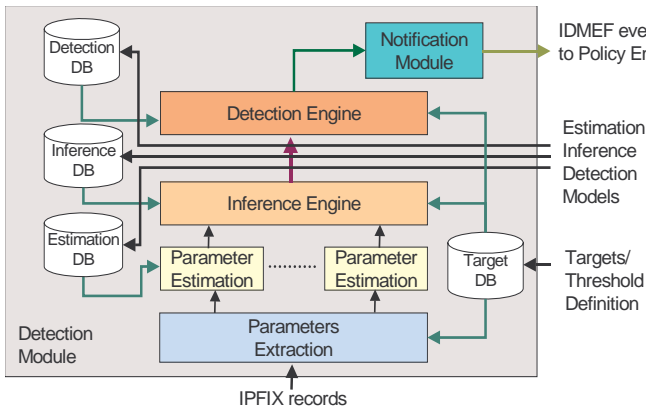


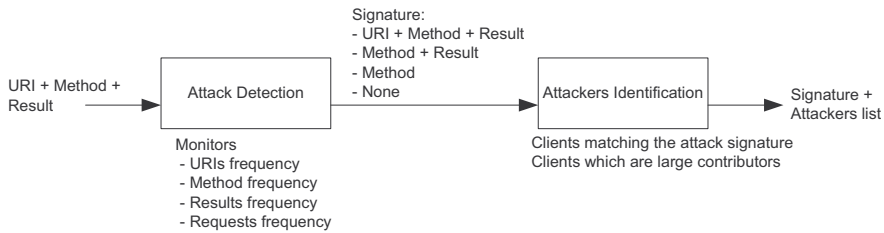
Problem: Improve mitigation against web server floodings

- Mitigation often **takes to much time**.
- Mitigation **affects** attackers as well as **legitimate users**.

Idea: Monitor changes in application-level behavior



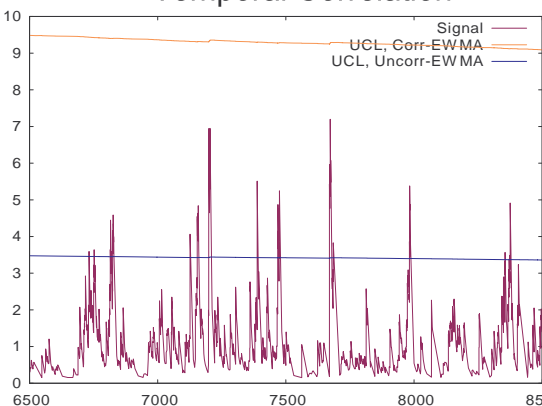
- Idea: DDoS = **change** in the **frequency** of requests.
- Most saturation attacks use a **fixed set of requests**.



- **Earlier attack detection** by monitoring **less frequent events**.
- Attack **signature** includes **application level information**.

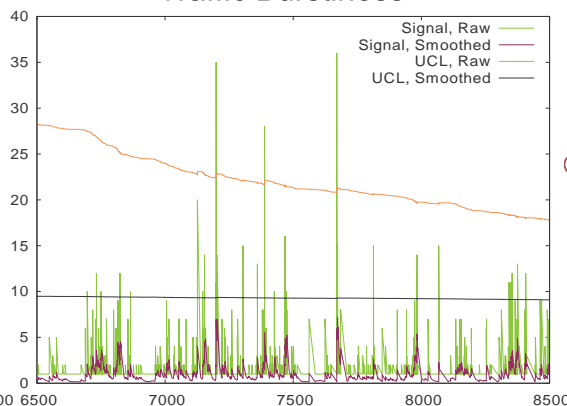
Tools: Models to detect changes in correlated parameters

Temporal Correlation



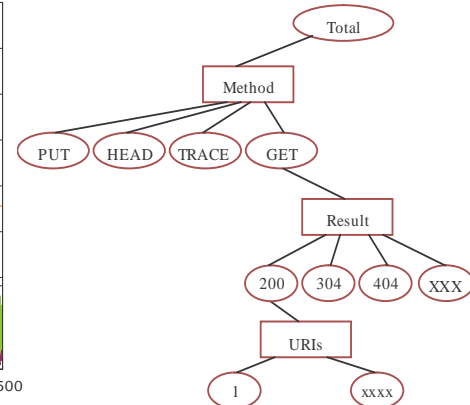
EWMA for correlated signals

Traffic Burstiness



Signal Smoothing

Inter-parameters Correlation



Results: Improvements for focused Attacks

Tests with an internal web server, ~15k objects, 10k monthly access

Reduced reaction delay

Reduced collateral impact

Benefit/Cost on FP/TP rates

Reaction Delay comparison

Blocked users comparison

