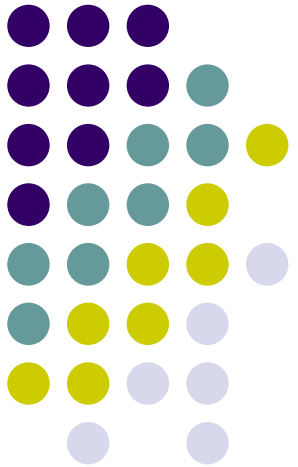
# Protecting Internet Threat Monitors: A Statistical Filtering Approach

Yoichi Shinoda
JAIST

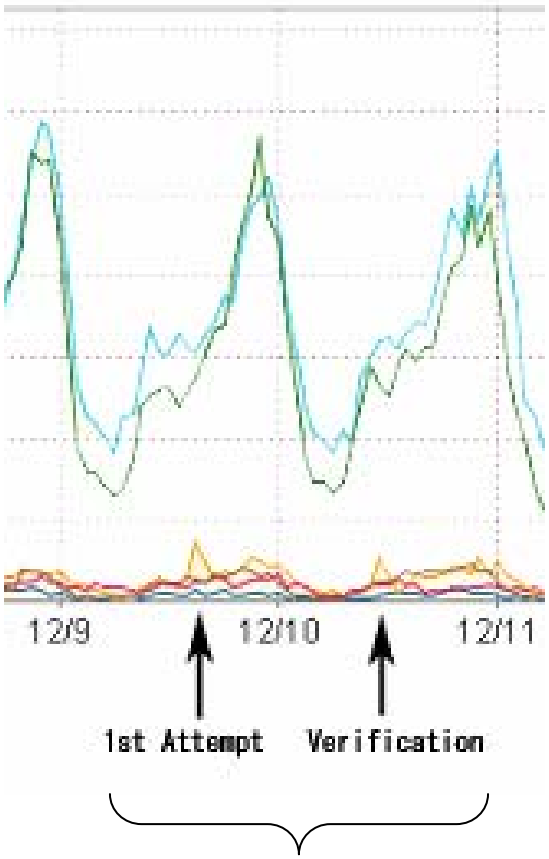


# Mapping Internet Monitors

- Two papers were presented/published at the 14th USENIX Security Symposium (Aug. 2005).
  - **Mapping Internet Sensors with Probe Response Attacks**
    *John Bethencourt, Jason Franklin, and Mary Vernon, University of Wisconsin, Madison*
  - **Vulnerabilities of Passive Internet Threat Monitors**
    *Yoichi Shinoda, Japan Advanced Institute of Science and Technology; Ko Ikai, National Police Agency of Japan; Motomu Itoh, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)*

# Mapping example: ISDAS marking & feedback

- Marking design
  - Range: Address blocks assigned to 3 IXes.
  - Marker: UDP/137
    - Was in the top-5.
    - Low dynamic range.
  - Algorithm: Time-series
  - Velocity: Each /24 block in an hour
  - Intensity: Each address were marked with 90 markers (to make 3 unit high spike in the graph of avg. count per sensor, where there are 30 sensors).

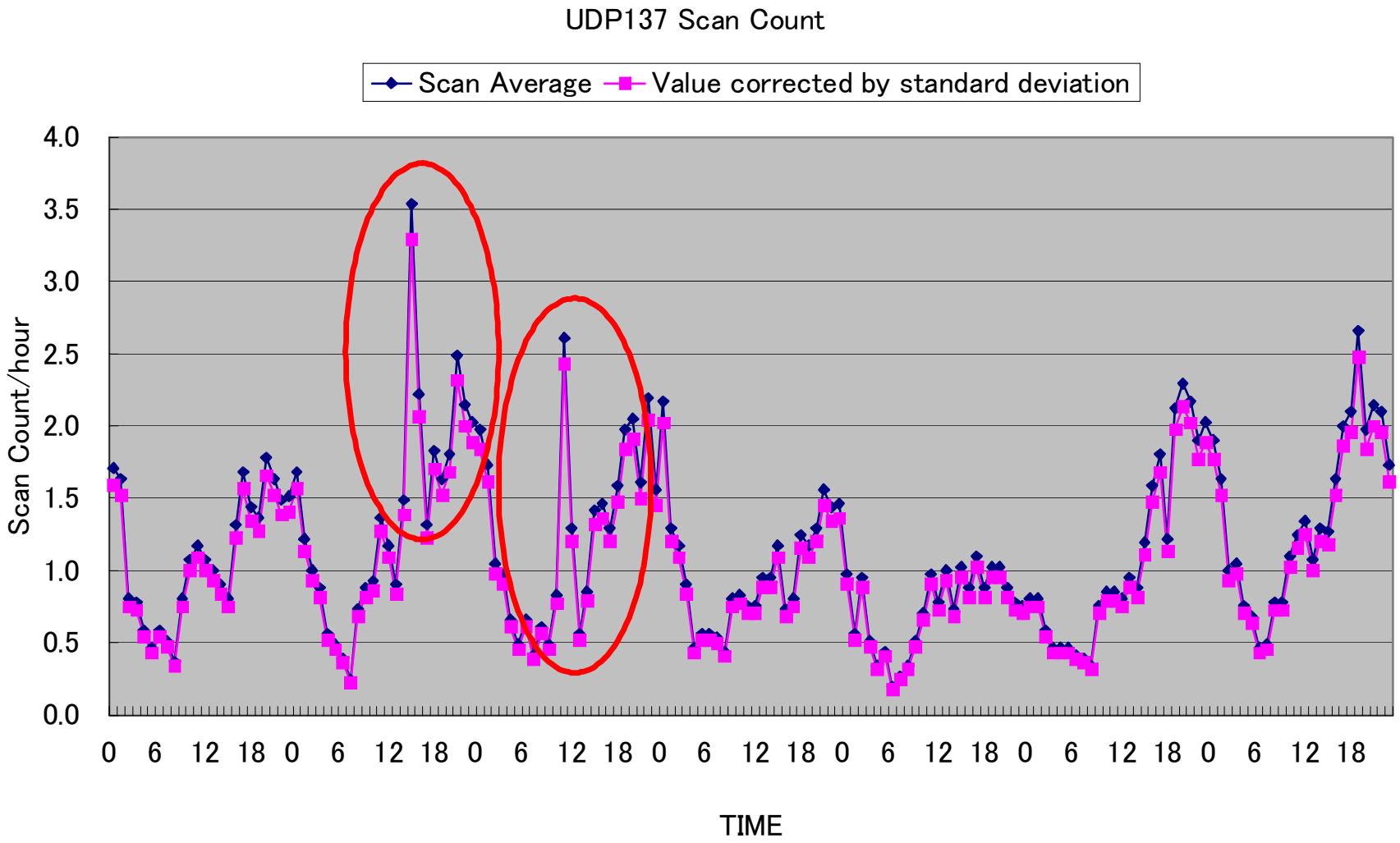



One /24 block hosting one sensor was identified

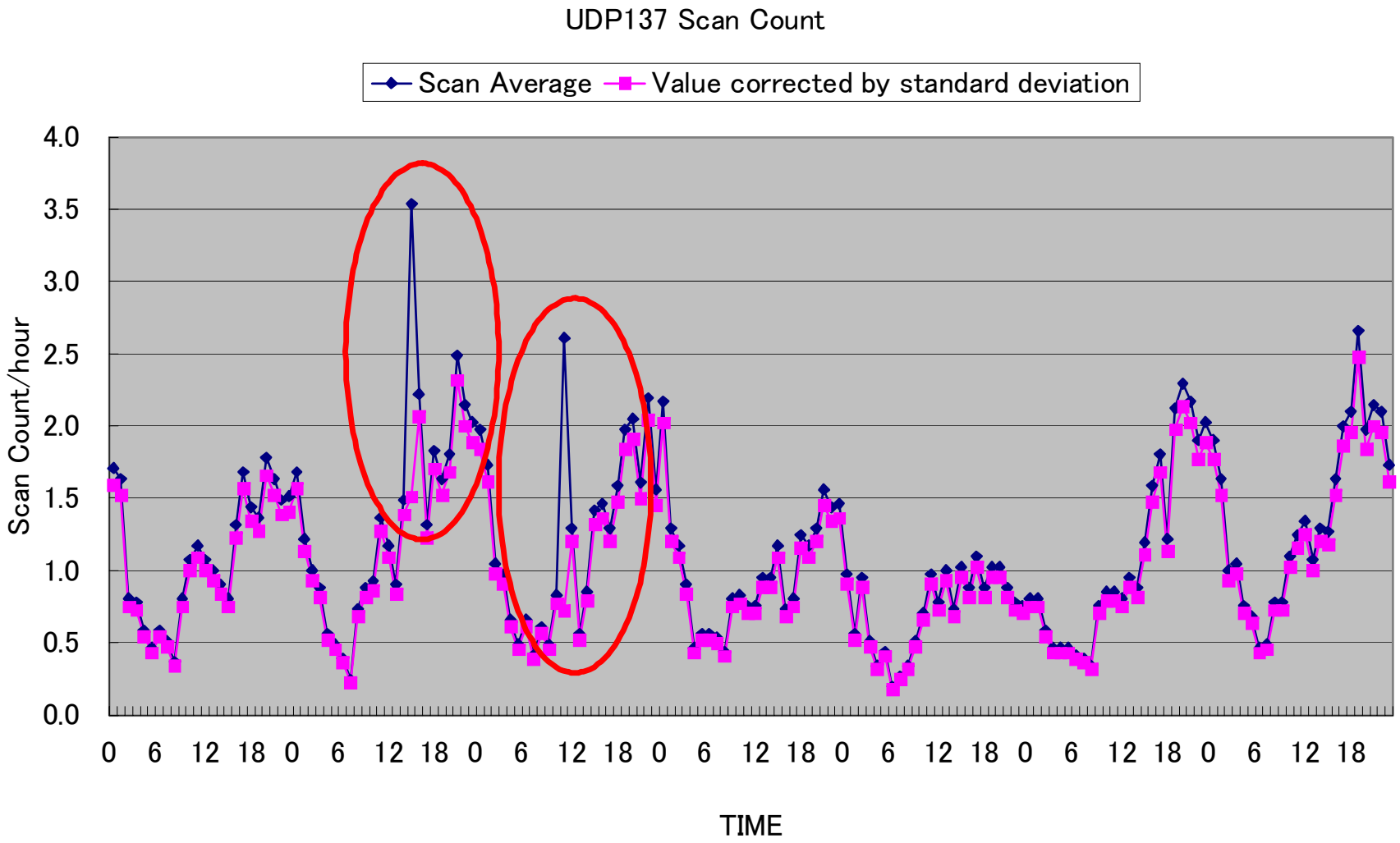
# SD Filtering

- Omit counts from sensors reporting “unusual counts”:
  - **if (count > $m + \rho \times \sigma$) then drop; where**
    - ***m* = avg of all sensor counts**
    - **$\sigma$ = stddev of all sensor counts**
    - **$\rho$ = magic multiplier**
  - **The magic value is in the range 5.0 – 6.0 (and sometimes up to 7.0) for several different distributed architecture monitors.**

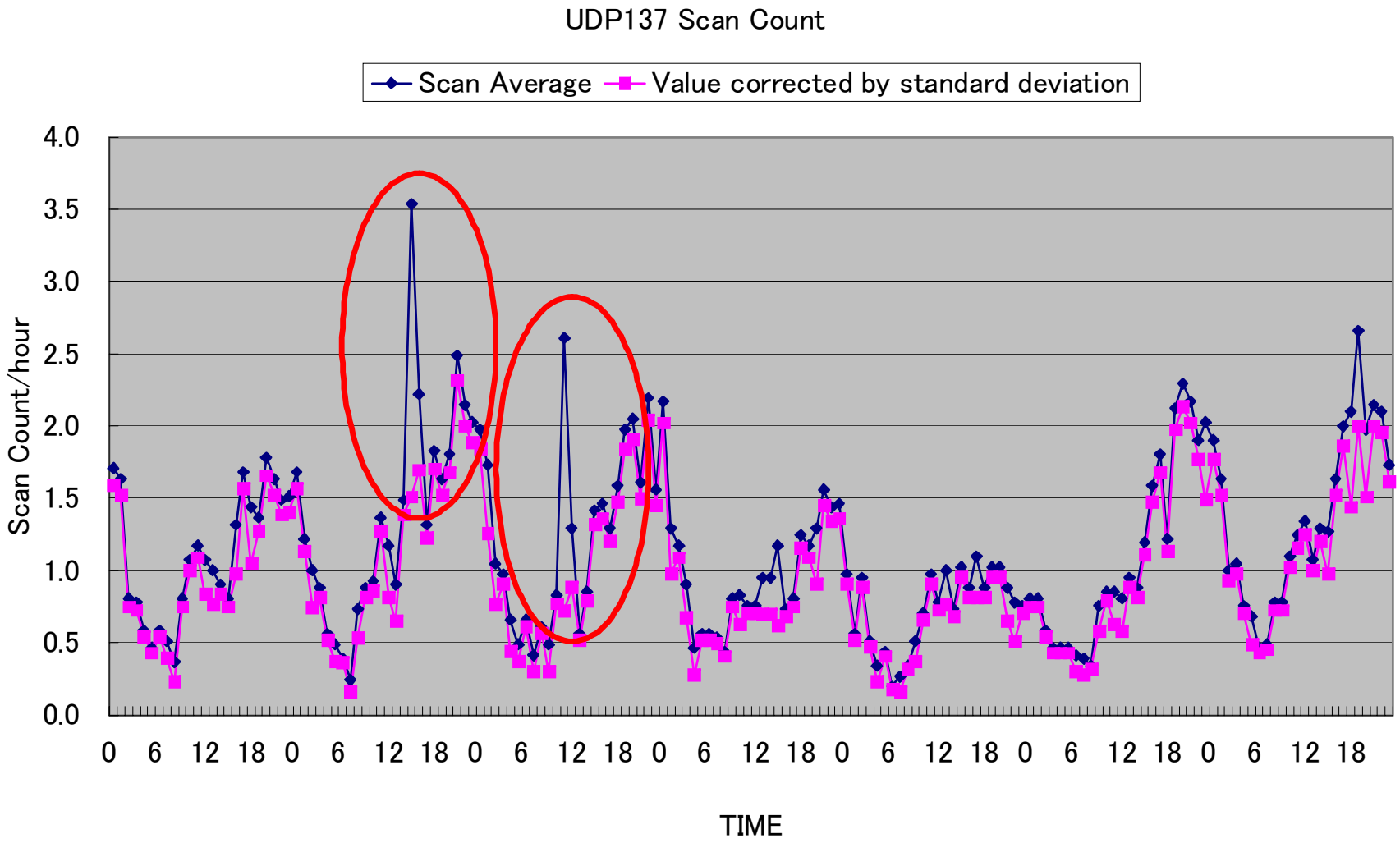
# SD filtering @ 6.5σ



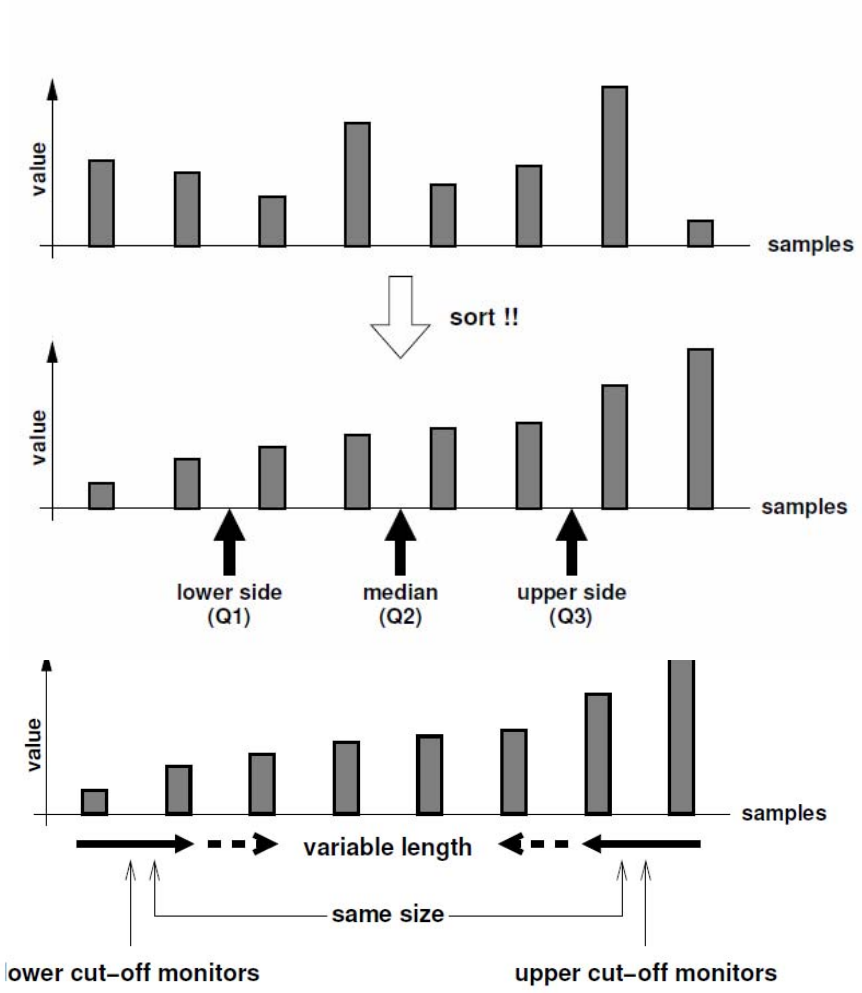
# SD Filtering @ 6.2σ



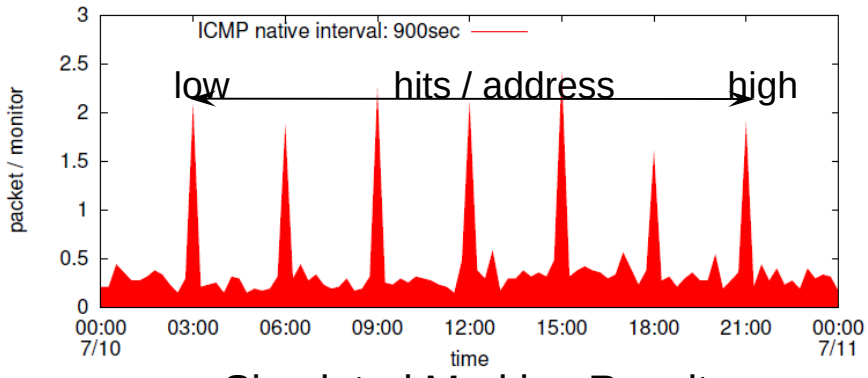
# SD Filtering @ 4.5σ



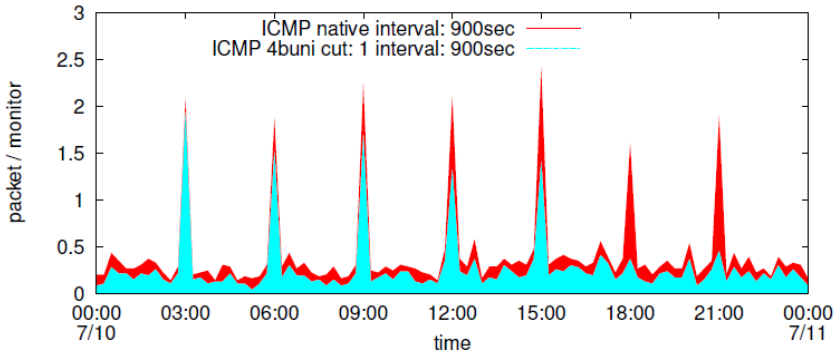
# Quartile Filtering



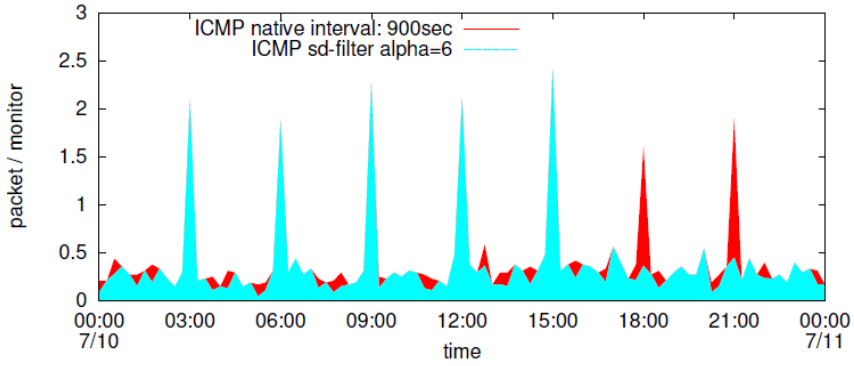
# Some Results



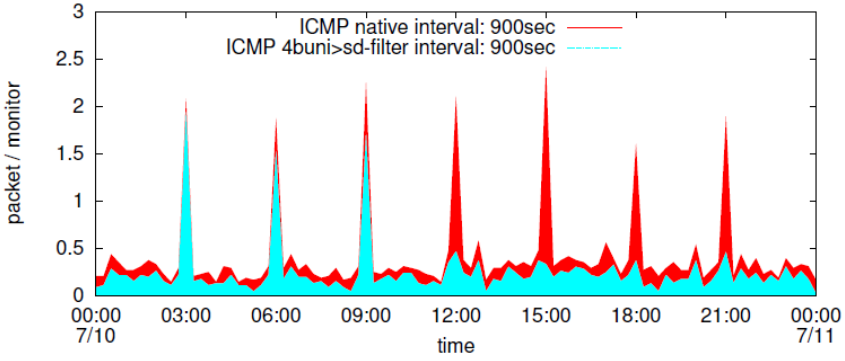

Simulated Marking Result




Quartile (cutoff = 1) Filtered




SD ( $\rho$ =6.0) Filtered




Quartile (cutoff = 1) then
SD ( $\rho$ =6.0) Filtered