GridStat Middleware Communication Framework: Systematic Adaptation

Rate-Based Failure Detection for Mission-Critical Data Delivery

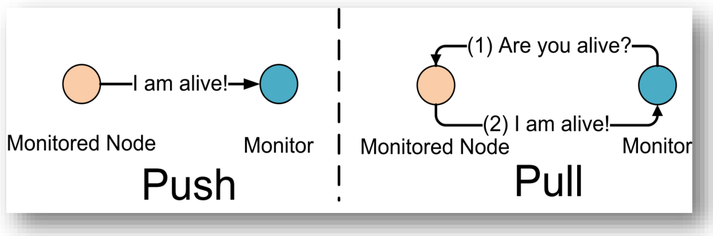
Brett Johnson, Thoshitha Gamage, and Dave Bakken

GOALS

- Enhance the resilience of wide-area power applications to both malicious cyber-attacks and non-malicious IT failures through systematic, dynamically adjustable, and extensible (GridStat) adaptation capabilities that respond faster and with high accuracy.
- Minimize the impact of adaptation ancillary services (instrumentation, failure detection) on core data delivery functionality by exploiting GridStat's rate-based semantics and complete knowledge of sensor flows at every location.

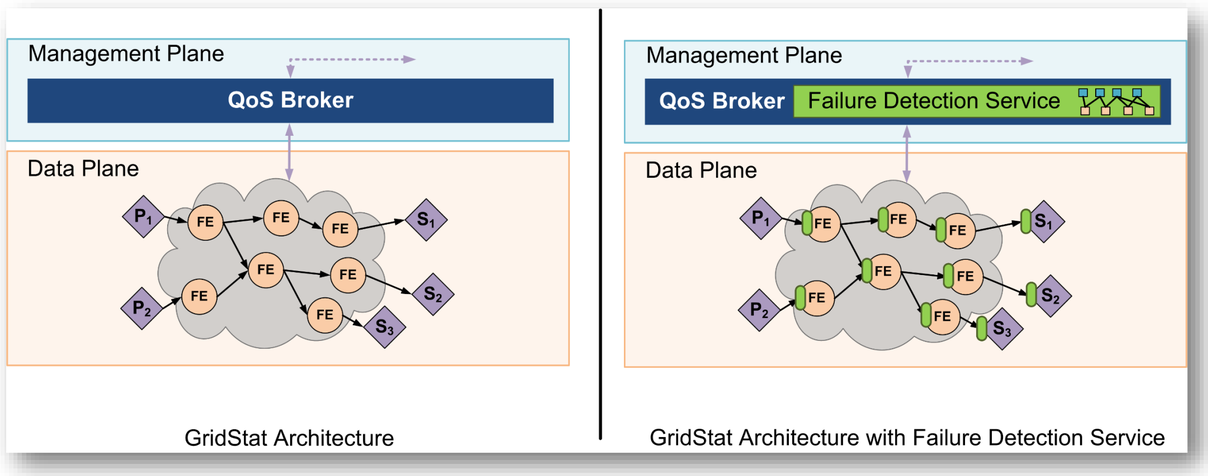
FUNDAMENTAL QUESTIONS/CHALLENGES

- Determine how to continuously maintain stringent QoS+ (low latency, high availability, rate, #paths) guarantees under adaptation with high assurance.
- Make fundamental design choices that have minimum instrumentation, failure detection, and adaptation footprints on the core data delivery guarantees and functionality.
  - Decide on the appropriate level of instrumentation that is necessary to capture the state of the data delivery network *accurately* and *sufficiently* under changing conditions with the lowest performance penalties.

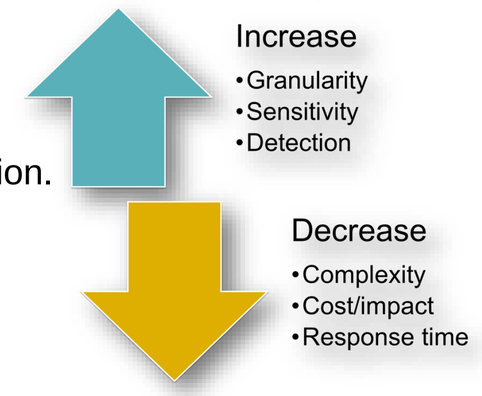


  - Minimize the total response time of adaptation (detection → diagnosis → identification) of an anomaly to trigger appropriate remedies in a timely fashion.
- Strike a principled balance between "*over-adapting*," which adversaries can try to exploit, and "*under-adapting*," which would affect delivery guarantees of most critical power applications.

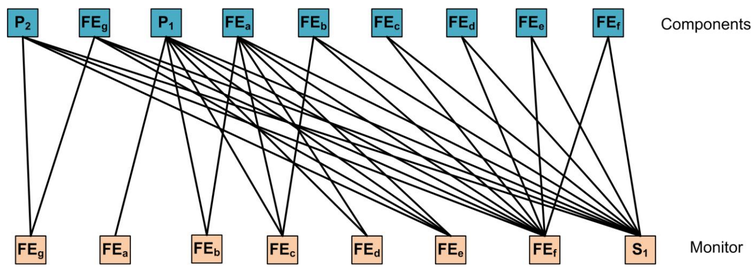
RESEARCH PLAN



- A <u>two-pronged monitoring approach</u> to failure detection that fully exploits GridStat's rate-based semantics:
  - **Heartbeat Failure Detection**
    - Used for link/node crash failure detection.
  - **Rate-based Failure Detection**
    - Used for in-network crash and QoS (latency, rate) failure detection.



- A <u>two-tier</u> architectural design: *Monitors* in the GS data plane observing individual flows for faults, *Service Logic* in the management plane.
- Use of *Exponential Weighted Moving Average* (EWMA) to monitor flow packet interval for abnormalities.
- Use of precalculated *Relationship Graphs* to identify the source of multiple failure events on demand.



RESEARCH RESULTS

- Techniques for localized and continuous detection for rate anomalies (both under- and over-rate events) in rate-based data delivery.

<u>EWMA Experiments</u>

- Raw data from a normal distribution with $\mu = 33$ and $\sigma = 2$
- EWMA

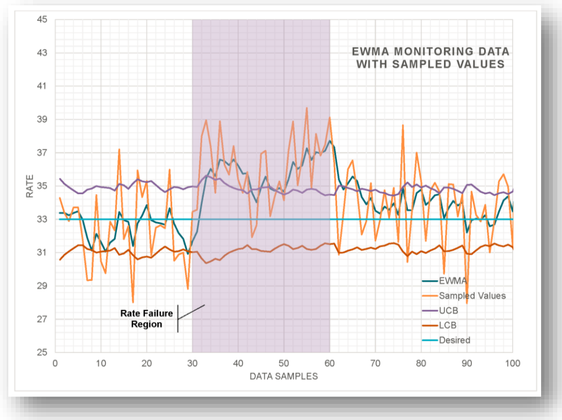
$$ave_k = \alpha * sample_k + (1-\alpha) * ave_{k-1}$$

- EWMA standard deviation

$$\sigma_k = \beta * (sample_k - ave_k) + (1-\beta) * \sigma_{k-1}$$

- Bounds

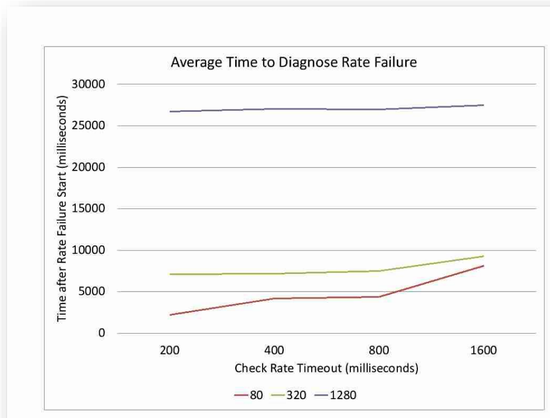
$$Bound = ave_k \pm Z * \sigma_k * \left(\sqrt{\frac{\alpha}{1-\alpha}}\right)$$

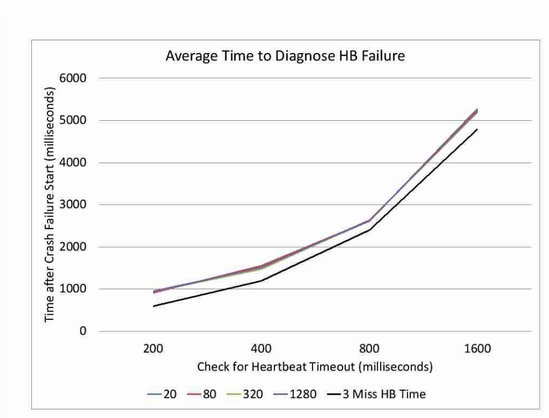


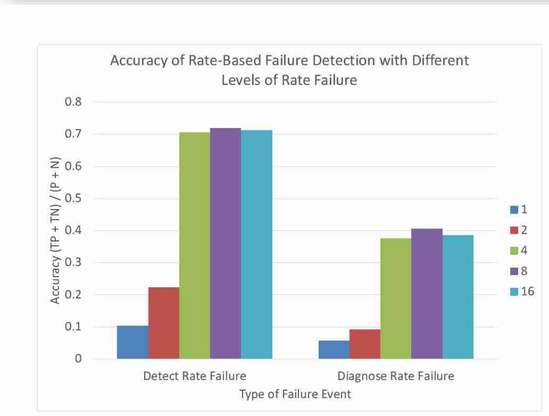
EWMA successfully detects rate anomalies in real-time.

<u>DETER Lab Experiments</u>

- Multiple setups used, from 4 to 16 forwarding nodes.
- Rate detection was evaluated against failures within milliseconds of the desired rate.







BROADER IMPACT

- Improves the resiliency of mission-critical data delivery for wide-area power applications.
- The novelty and the uniqueness of the rate-based failure detection concept.

INTERACTION WITH OTHER PROJECTS

- Experiments run on DeterLab.

FUTURE EFFORTS

- Development of the adaptation service for GridStat using failure detection input.
- Scalability testing using large-scale experiments involving ~150 nodes.
- Performance analysis of adaptation on GS topologies over real-world bus systems.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

gridstat.net