Rate-Based Failure Detection for Critical-Infrastructure Sensor Networks

Brett Johnson, Thoshitha Gamage, David E. Bakken

Goals

- Exploit GridStat's rate-based semantics and its complete knowledge of sensor flows at every location in order to provide much quicker and more accurate failure detection.
- Enhance resilience of wide-area power applications with a systematic, dynamically adjustable, and extensible foundation to enable quicker and more accurate adaptations to both malicious cyber-attacks (sensor spoofing, denial of service) and benign IT failures.

Fundamental Questions/Challenges

- How to provide rich and fast per-flow failure detection without degrading the performance of GridStat's Forwarding Engines (FE) or overloading links.
- How to exploit the relatively static nature of GridStat subscriptions and a critical infrastructure environment while handling acute dynamic faults in the underlying IT infrastructure.
- How can rate-based application traffic supplant traditional failure detection algorithms using heartbeat messages as well as GridStat's existing end-to-end Subscriber-based QoS Exception detection?
- How can rate-based application traffic be used to quickly and locally detect unauthorized traffic?

Research Plan

- Identify requirements for an *adaptation service* supported by the failure detector.
- Survey the state of the art in failure detectors.
- Develop a suite of *adaptation use cases* to identify requirements for the failure detector.

7. Subscriber/Publisher Failure

Description	A crash failure of a Subscriber or Publisher.
Actors	• Domain QoS Broker • Forwarding Engine A • Subscriber S • Forwarding Engine Neighbors of S • Link AS that is in the domain controlled by the Broker
Assumptions	• All the actors in this case can be trusted. • The QoS Broker knows about the Subscriptions that S is subscribing/publishing
Input	Heartbeat messages between A, S, and the Broker.
Logic	**Problem** • The Subscriber S crash fails. **Diagnose** • FE A will notice a lack of heartbeat messages from S. They will then send a notification to the Broker that it cannot reach S. • The Broker will attempt to ping S to see if it can get a response. • After a timeout the Broker will check if any other neighbors of S can still reach S. **Act** • The Broker can only act by terminating Subscriptions to/from S because there is no other way to get messages to it. It can allow forwarding to continue for a moment in case S reconnects. The Broker also logs the disconnection of S.
Output	After some timeout period, termination of Subscriptions to/from S. Other domains with subscriptions to/from S are notified.
Issues	• Other domains may need to be notified of the subscription's failure in order to recover allocated resources.
Security Issues	• If S is malicious attacker can trick a majority of neighbors to think that S has failed then the Broker would be tricked into terminating Subscriptions. • What if S is malicious and says it can hear from A? How would the Adaptation service determine what is going on?
Policies	• How many dropped messages before notification of issue? • How long after a subscriber is disconnected do we wait before terminating the subscription? When do we free the resources?

Figure 1: Sample use case.

- Use the adaptation use cases to develop a decision tree of how to identify and diagnose faults. This provides the basis for the algorithm that will be used by the failure detector.

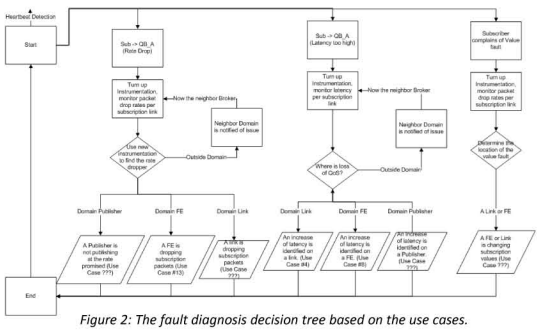

Figure 2: The fault diagnosis decision tree based on the use cases.

- Design and implement *bump-in-the-wire rate monitors* providing per-flow granularity in order to avoid impacting FE scalability.
- Design and implement a failure detector service to detect and trigger events when crash or rate anomalies are detected.
- Test the implemented architecture using the DETER Testbed to evaluate performance and scalability at a large scale.

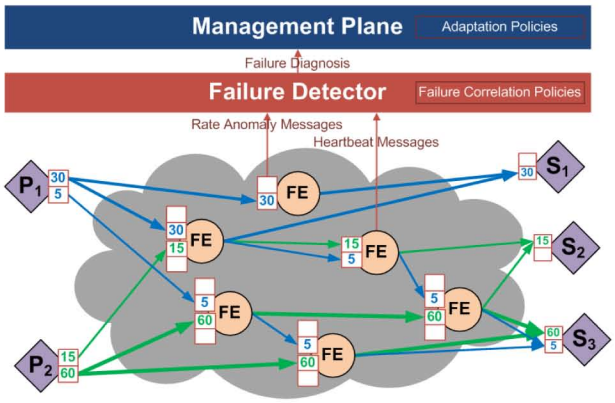

Figure 3: Example of a running GridStat Rate-Based fault detection system with no active failures. The bump-in-the-wire rate anomaly detectors are attached to each incoming link on a forwarding engine to monitor incoming sensor update flows.

Research Results

- **Technology Readiness Level:** Beginning research.
- Identification of a bump-in-the-wire rate detector as a fundamental building block for creating scalable rate-based failure detection.
- Techniques for localized and continual detection of rate anomalies (both under- and over-rate events) in rate-based data delivery systems.

Broader Impact

- Grid resilience will be enhanced by power applications that can operate at full efficacy despite suffering a much wider range and number of IT anomalies.
- These techniques will be useable by any communication framework where rates are known for each link. The monitoring will allow for much more accurate and localized detection of failures than possible with traditional heartbeat-based failure detection alone.
- A fine-grained and scaleable failure detector able to detect anomalies quickly and locally will enable much richer and more systematic coordinated adaptations. Such adaptations will be much more effective than today's per-flow, uncoordinated adaptations.

Interaction with Other Projects

- Other anomaly detection techniques TBD can be incorporated into this extensible failure detection framework.

Future Efforts

- Development of an Adaptation Service for GridStat using the failure detector presented in this research.
- Development of a *multi-level instrumentation service* for GridStat with more levels of inference and more programmability.