University of Missouri

VIMAN Lab
VIRTUALIZATION, MULTIMEDIA AND NETWORKING LAB

Multi-domain Internet Performance Measurement: *Sampling, Analysis and Security*

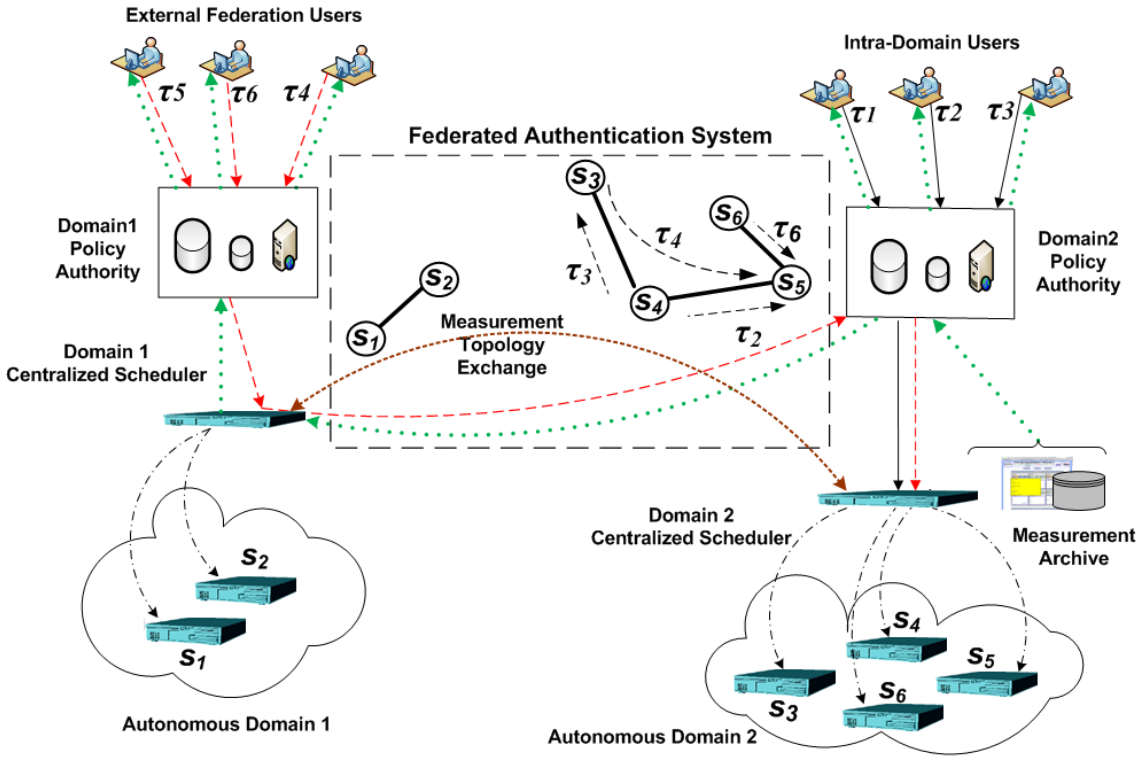
Prasad Calyam, Ph.D. (PI)
calyamp@missouri.edu
Saptarshi Debroy, Ph.D. (PostDoc)
debroysa@missouri.edu

Graduate Students: **Yuanxun Zhang** & **Ravi Akella**

Progress Update, Annual PI Meeting
September 2014

Multi-domain Measurement Federation

for meeting diverse user/operator monitoring objectives



Multi-domain Performance Measurement
- *Our R&D Highlights*

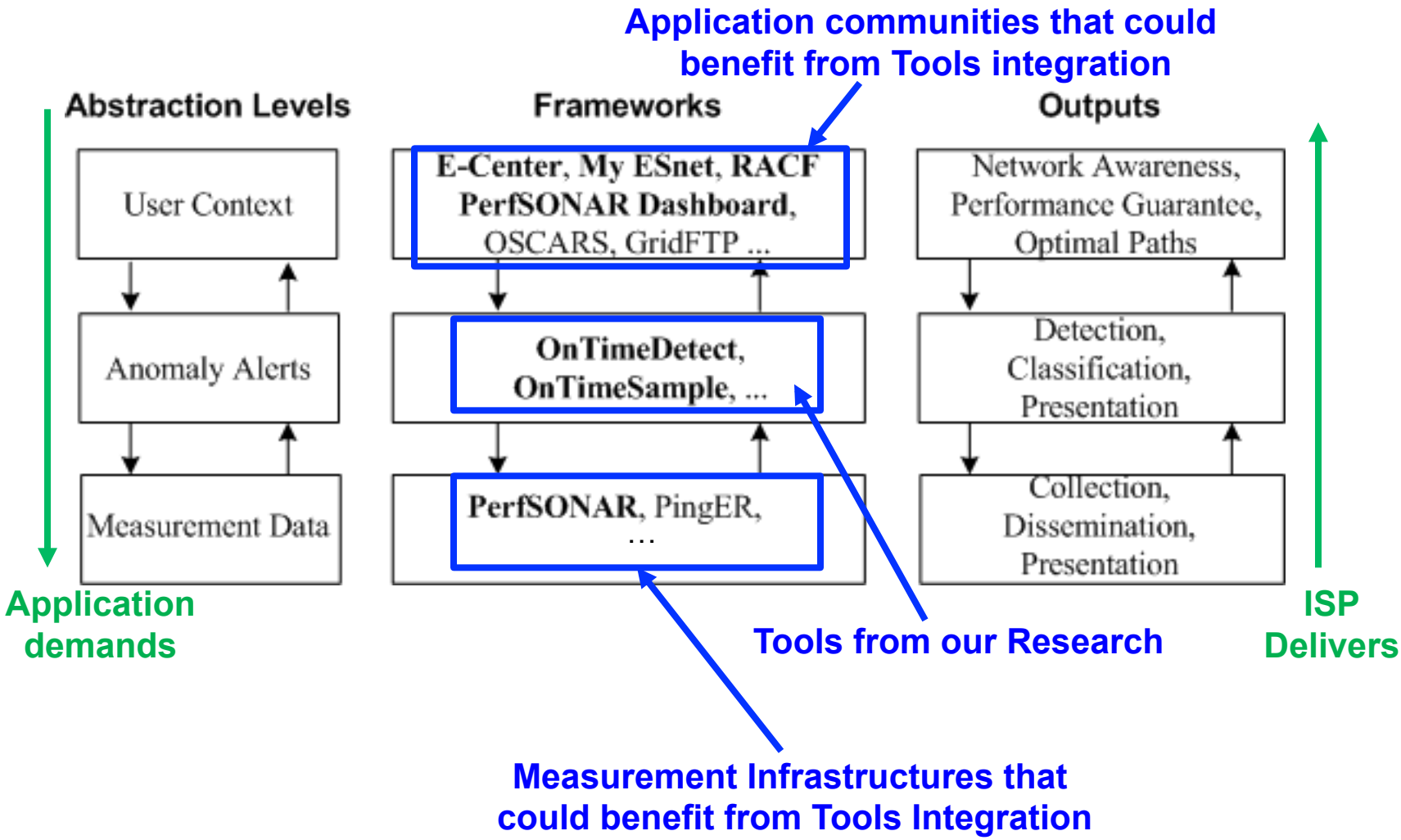
- Network-wide active measurement orchestration
  - Conflict-free measurement scheduling algorithms
  - *OnTimeSample Tool:* Semantic meta-scheduler and policy inference engine for perfSONAR-based multi-domain measurements

- Multi-domain measurement data analysis and bottleneck diagnosis
  - Correlated and uncorrelated network anomaly detection algorithms
  - *OnTimeDetect Tool:* Validated with perfSONAR data sets; includes detailed studies with DOE lab sites perfSONAR measurement archives

- 'Measurement Level Agreements' for federated network monitoring
  - Secured middleground for sharing measurement resources and data
  - *OnTimeSecure Tool:* Resource Protection Service that is integrated with Internet2 InCommon and evaluated in Science DMZ testbeds

Papers available at – http://cs.missouri.edu/~calyamp

Context of our Research and Development



Topics of Discussion

- Research and Development Context

- Latest Accomplishments
  - *Sampling & Analysis:* "OnTimeDetect" Algorithms/Tools for correlated anomaly detection and diagnosis

  - *Sampling & Security:* "OnTimeSecure" Algorithms/Tools for secured middleground in measurement federations

- One more thing…. Next Research Question? ☺

Topics of Discussion

- Research and Development Context

- Latest Accomplishments
  - *Sampling & Analysis:* "OnTimeDetect" Algorithms/Tools for correlated anomaly detection and diagnosis

  - *Sampling & Security:* "OnTimeSecure" Algorithms/Tools for secured middleground in measurement federations

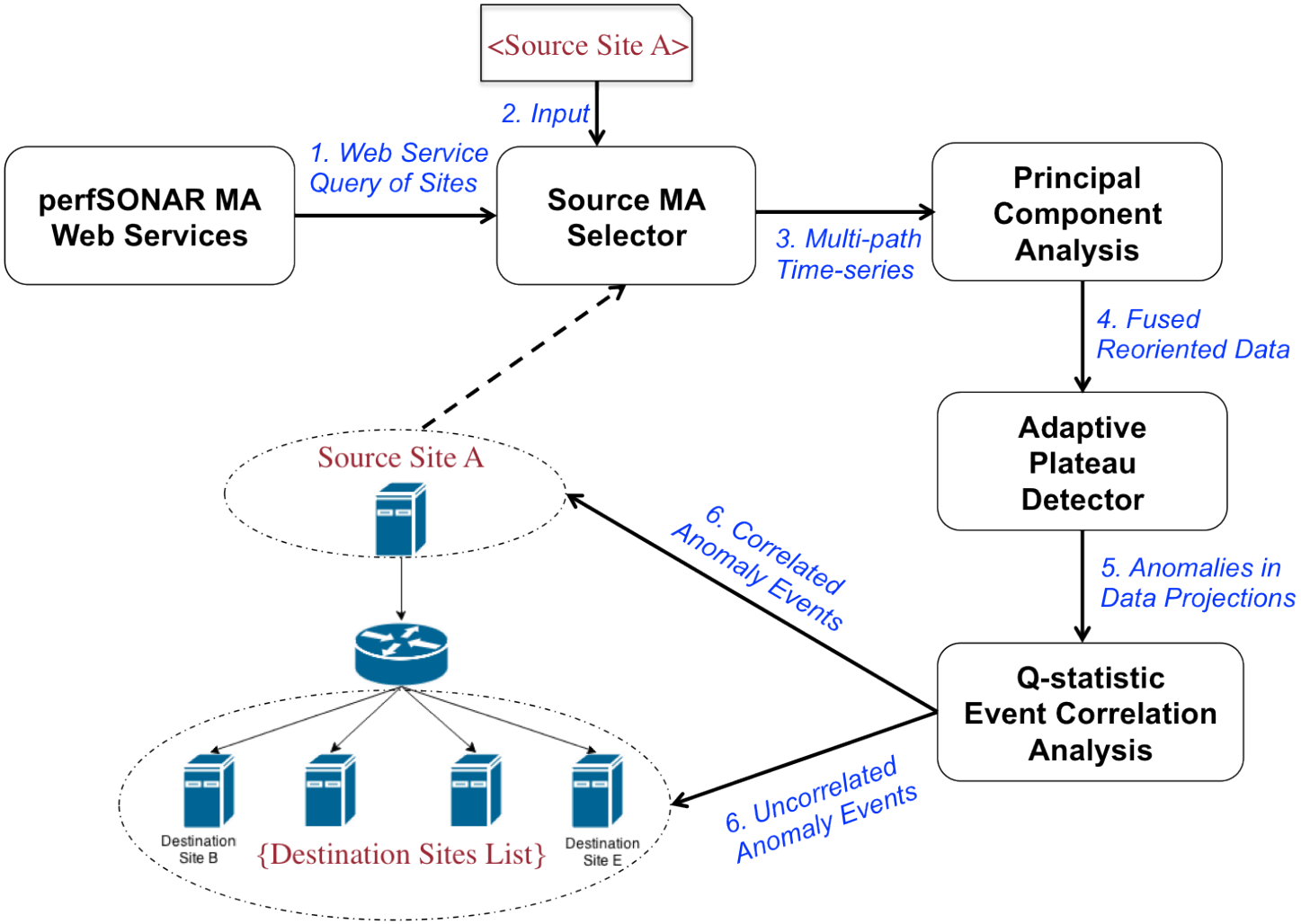
- One more thing…. Next Research Question? ☺

"OnTimeDetect" Algorithms and Tools

- Developed an adaptive anomaly detection (APD) algorithm that is more accurate (lower false alarms) than existing schemes (e.g., NLANR/SLAC plateau detector)
- Demonstrated how *adaptive* sampling can reduce anomaly detection times from several days to only a few hours in perfSONAR deployments
- Developed a network-wide topology-aware (NTA-APD) *correlated* anomaly detection algorithm to detect bottlenecks in paths between DOE labs
- Developing a principal component analysis (PCA-APD) based *correlated* anomaly detection algorithm that does not require complete topology

- P. Calyam, Y. Zhang, S. Debroy, M. Sridharan, "PCA-based Network-wide Correlated Anomaly Event Detection and Certainty Diagnosis", *Under Peer-review*, 2014.
- P. Calyam, L. Kumarasamy, C. -G. Lee, F. Ozguner, "Ontology-based Semantic Priority Scheduling for Multi-domain Active Measurements", *Springer Journal of Network and Systems Management (JNSM)*, 2014.
- P. Calyam, M. Dhanapalan, M. Sridharan, A. Krishnamurthy, R. Ramnath, "Topology-Aware Correlated Network Anomaly Event Detection and Diagnosis", *Springer Journal of Network and Systems Management (JNSM)*, 2013.
- P. Calyam, J. Pu, W. Mandrawa, A. Krishnamurthy, "OnTimeDetect: Dynamic Network Anomaly Notification in perfSONAR Deployments", *IEEE MASCOTS*, 2010.

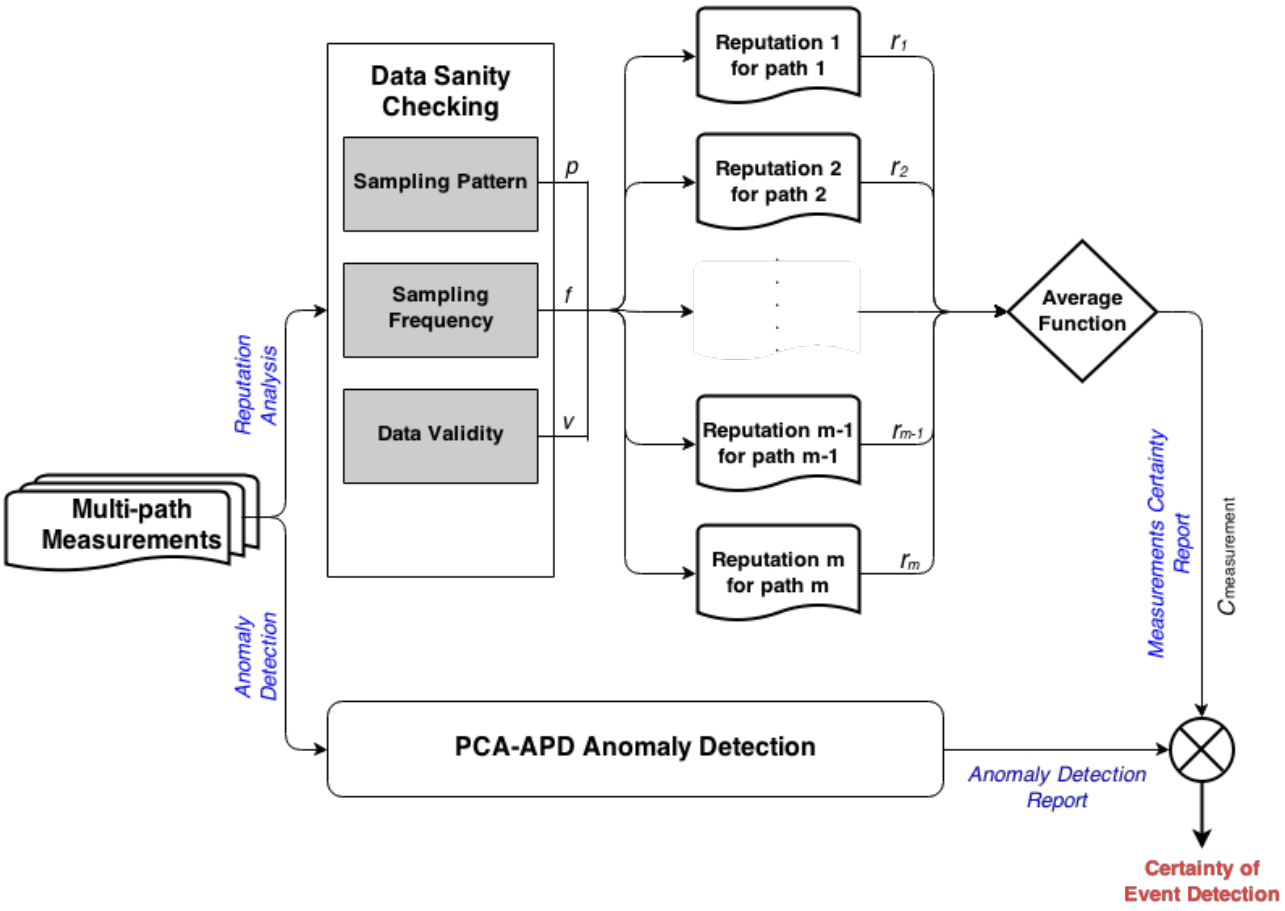
PCA-APD Workflow with perfSONAR Data

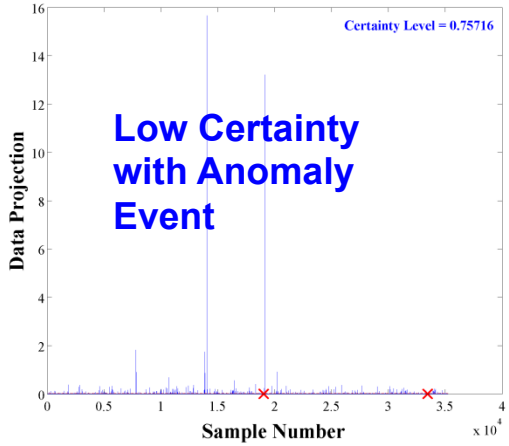


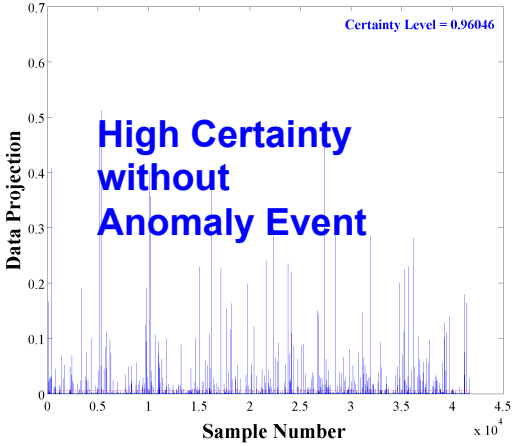
Data Sanity Checking and Certainty Analysis

- Measurement mis-calibration or improper sampling can lead to erroneous anomaly detection and/or useless diagnosis
- Factors for data sanity checking:
  - *Validity of the measured data*
    - E.g., no negative delay values
  - *Sampling pattern*
    - E.g., periodicity
  - *Sampling frequency*
    - E.g., once each hour
- Output of the sanity check quantifies the certainty of detected anomaly events
  - A weighted function is used that dynamically adapts with the nature of the collected traces

Data Sanity Checking and Certainty Analysis (2)







- Certainty verification in cases of presence/absence of anomaly events

Topics of Discussion

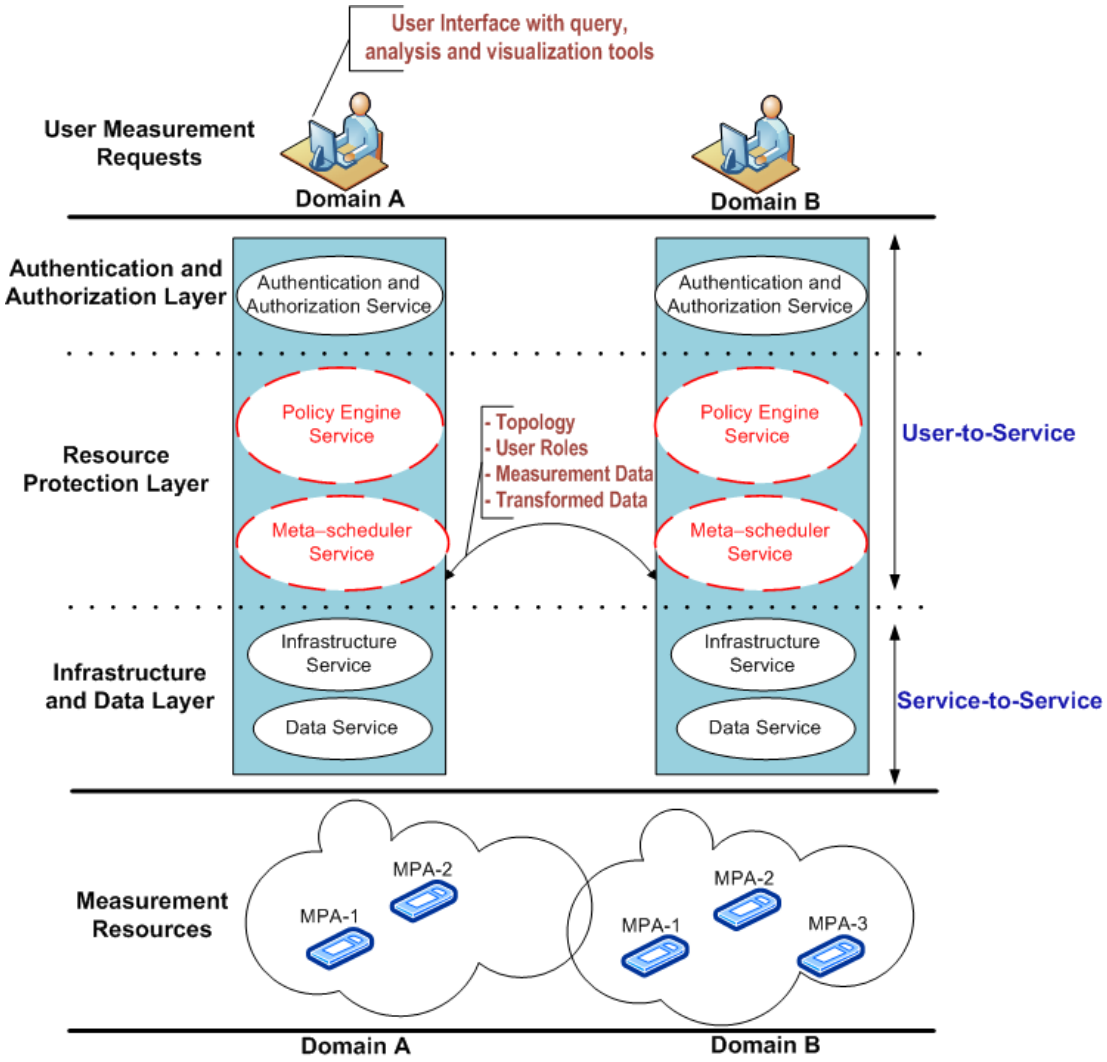
- Research and Development Context

- Latest Accomplishments
  - *Sampling & Analysis:* "OnTimeDetect" Algorithms/Tools for correlated anomaly detection and diagnosis

  - *Sampling & Security:* "OnTimeSecure" Algorithms/Tools for secured middleground in measurement federations

- One more thing…. Next Research Question? ☺

OnTimeSecure Resource Protection in perfSONAR



perfSONAR User and Service Integration

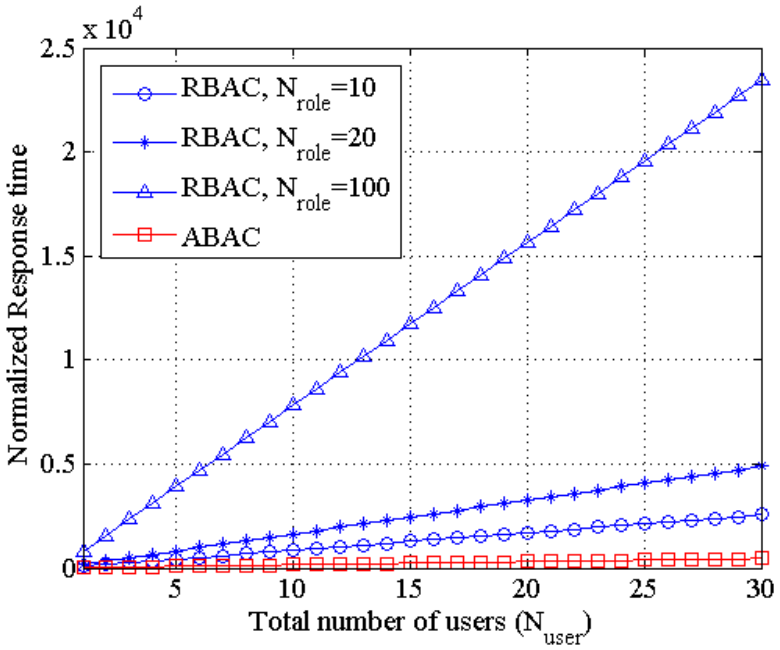
- Caters to unique security requirements of a multi-domain measurement federation
- Security requirements to be addressed:
  - Authentication
  - Authorization
  - Data and message integrity
  - Audit trail
- 'User-to-Service' case
  - User accessing measurement functions such as for e.g., graphing the measurement data, querying trends
- 'Service-to-Service' case
  - Secure communication of measurement services using REST API key authentication

- P. Calyam, R. Akella, S. Debroy, A. Berryman, T. Zhu, M. Sridharan, "Secured Middleground for User and Service Integration in Federated Network Monitoring", *Under Peer-review*, 2014.
- P. Calyam, A. Berryman, E. Saule, H. Subramoni, P. Schopis, G. Springer, U. Catalyurek, D. K. Panda, "Wide-area Overlay Networking to Manage Accelerated Science DMZ Flows", IEEE International Conf. on Computing, Networking and Communications (ICNC), 2014.
- P. Calyam, S. Kulkarni, A. Berryman, K. Zhu, M. Sridharan, R. Ramnath, G. Springer, "OnTimeSecure: Secure Middleware for Federated Network Performance Monitoring", IEEE Conf. on Network and Service Management (CNSM) (Short Paper), 2013.

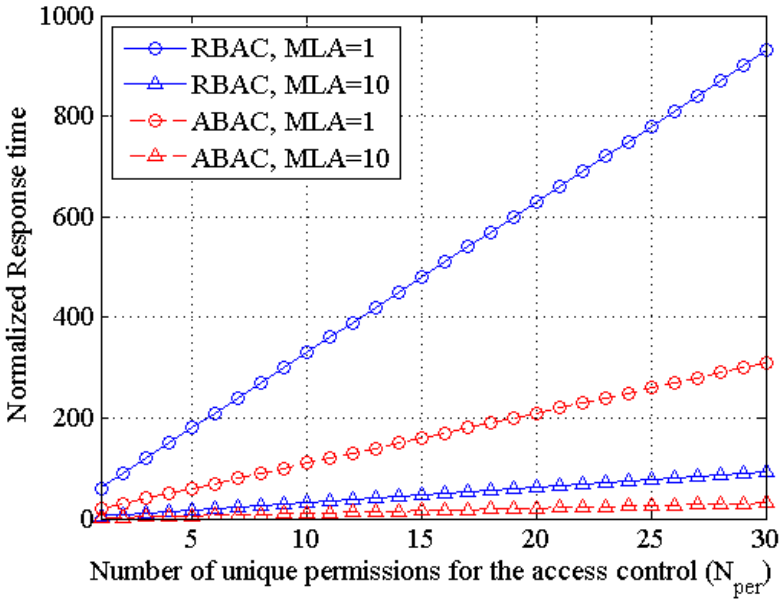
Middleground Solutions Considered

- Role Based Access Control (RBAC)
  - Hierarchical model of mapping
  - Users → Groups → Roles → Permissions
- Attribute Based Access Control (ABAC)
  - Direct mapping of users to permissions
- Modeling and comparison analysis using 5 novel metrics:
  - *Manageability*
  - *Vulnerability*
  - *Message overhead*
  - *Scalability*
  - *Response time*
- We address both Intra-domain and Inter-domain scenarios

Secured Middleground Response Time Comparison

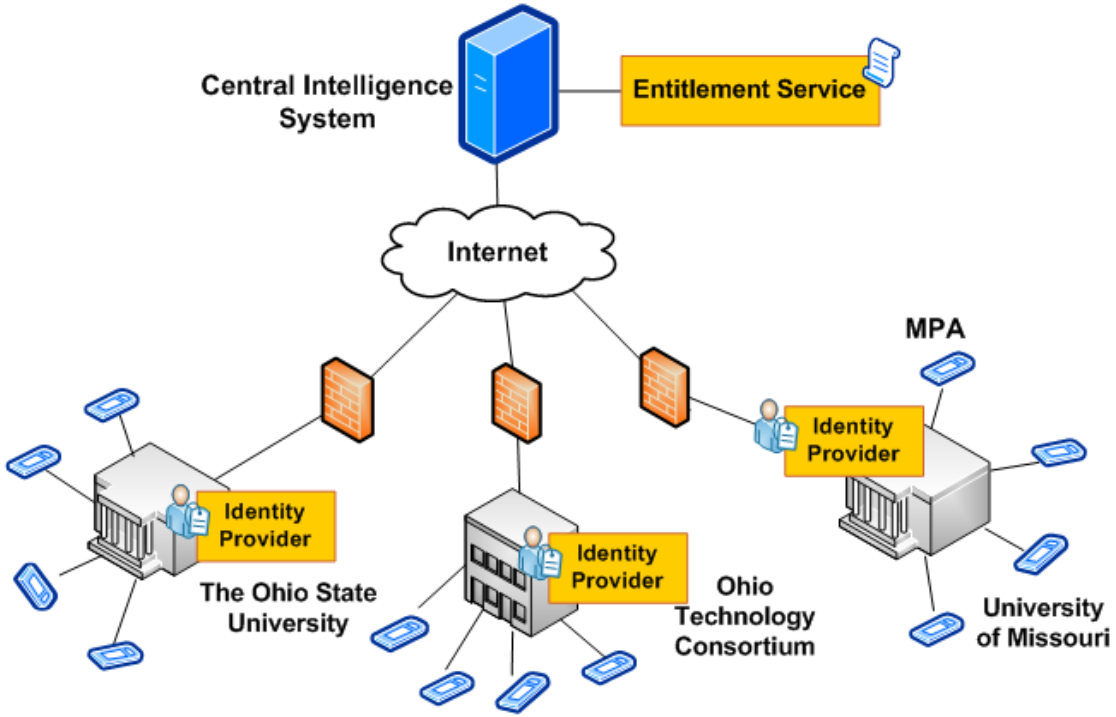


Sequential execution of measurement jobs



Effect of concurrent scheduling

Case Study: Secured Middleground in a Multi-campus Testbed



Risk Level	Risk Tolerance		
	Open-pS	RPS-pS	
		RBAC	ABAC
Low	73%	70%	69%
Moderate	88%	72%	70%
High	92%	74%	69%

- Measurement federation across campuses using Internet2 InCommon
- Risk assessment and threat modeling study using the NIST method
  - Open-pS compared with RPS-pS (RBAC and ABAC)

Topics of Discussion

- Research and Development Context
- Latest Accomplishments
  - *Sampling & Analysis:* "OnTimeDetect" Algorithms/Tools for correlated anomaly detection and diagnosis
  - *Sampling & Security:* "OnTimeSecure" Algorithms/Tools for secured middleground in measurement federations
- One more thing…. Next Research Question? ☺

One more thing… Next Research Question?

- *OnTimeSocial Tool* -
  - Could allow a Facebook-like portal for measurement data exchange among "friend domains"
    - Users and applications could 'subscribe' to measurement feeds
    - Trust assignment based on quality of the measurement data
    - Incentives for domains that are more disciplined in collecting and disseminating accurate measurement data

- Open questions:
  - Who will be the users?
    - Producers versus Consumers
  - How to manage trust?
    - Centralized versus Distributed
  - How reputations are established?
    - Objective Algorithms versus User Ratings

Thank you for your attention!