InSight2

Angel Kodituwakku & **Jens Gregor**, UTK
Alex Keller & **John Gerth**, Stanford University
Buseung Cho, KISTI
Carter Bullard, Qosient

IRNC: AMI: Advanced Measurements and Instrumentation

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What is InSight2 ?

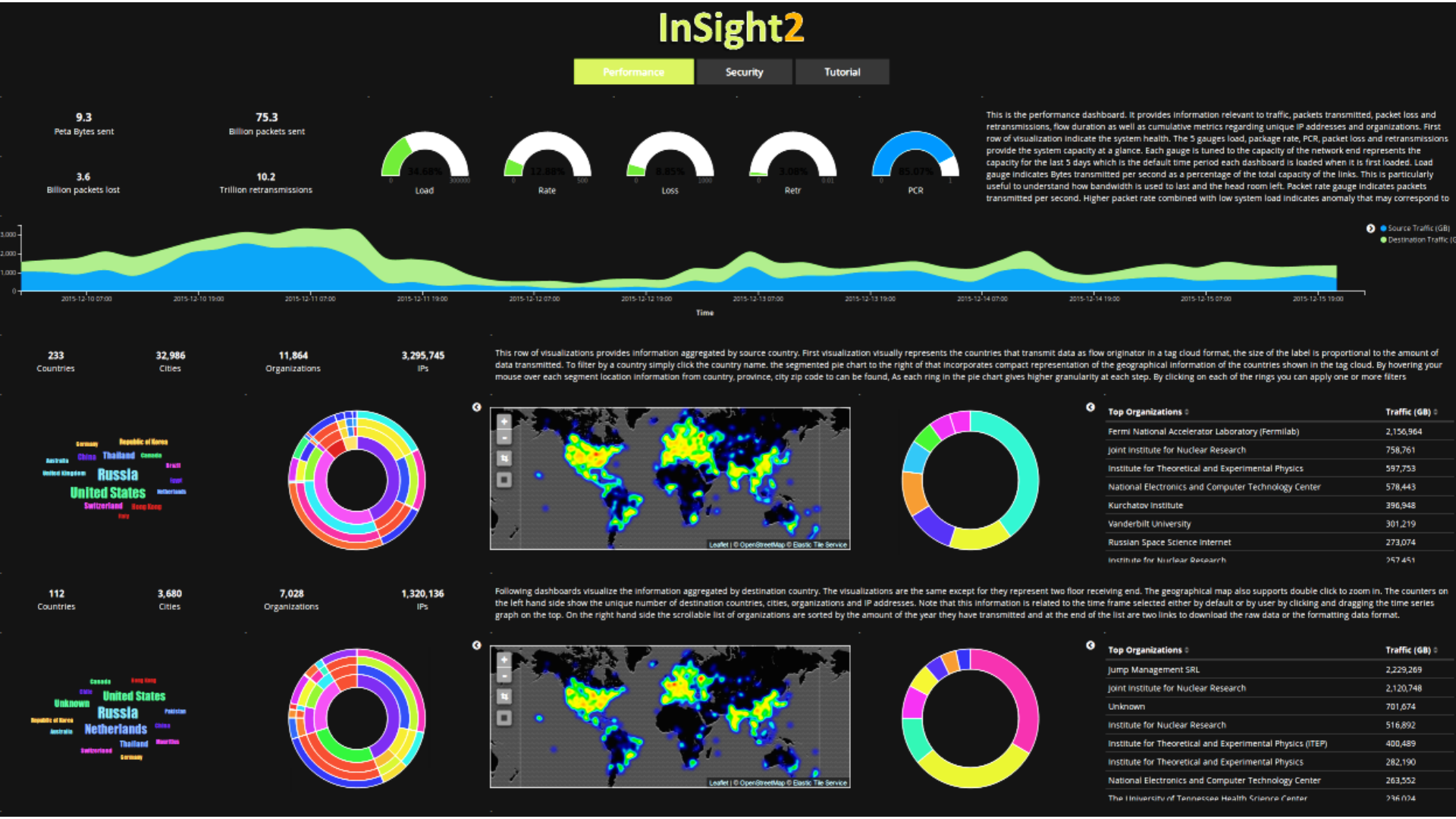
- Interactive situational awareness and analytics platform for real-time network traffic modeling and analysis.
- Argus flow data enriched with GeoIP, bad actor, and Global Science Registry (GSR) information.
- Multi-threaded, scalable, extendible architecture.
- Simple virtualized deployment.
- Plugin-based analytics modules.

Who is it for?

- Network managers and operators
  - Make proactive planning decisions
  - Determine optimum times for large data transfers

- Network analysts
  - Live and historic data enrichment
  - Real-time data visualization
  - Anomaly detection
  - Intuitive dashboards for detailed drill-down to flow level

InSight2 Dashboards

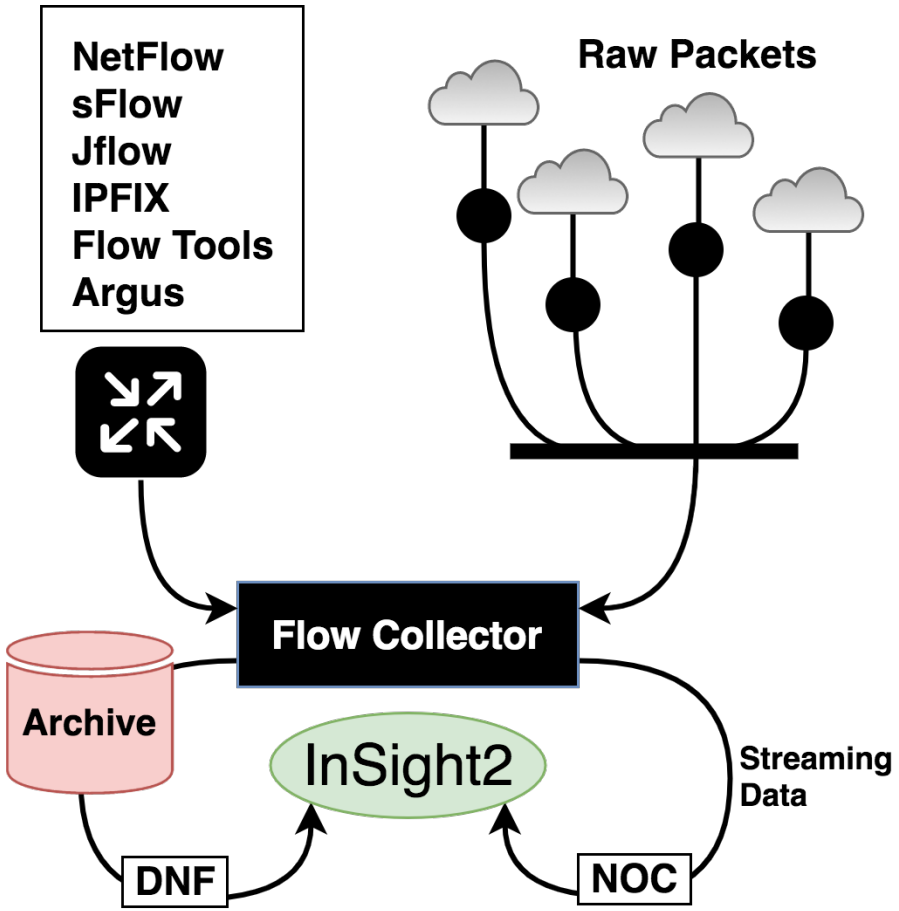


Capabilities

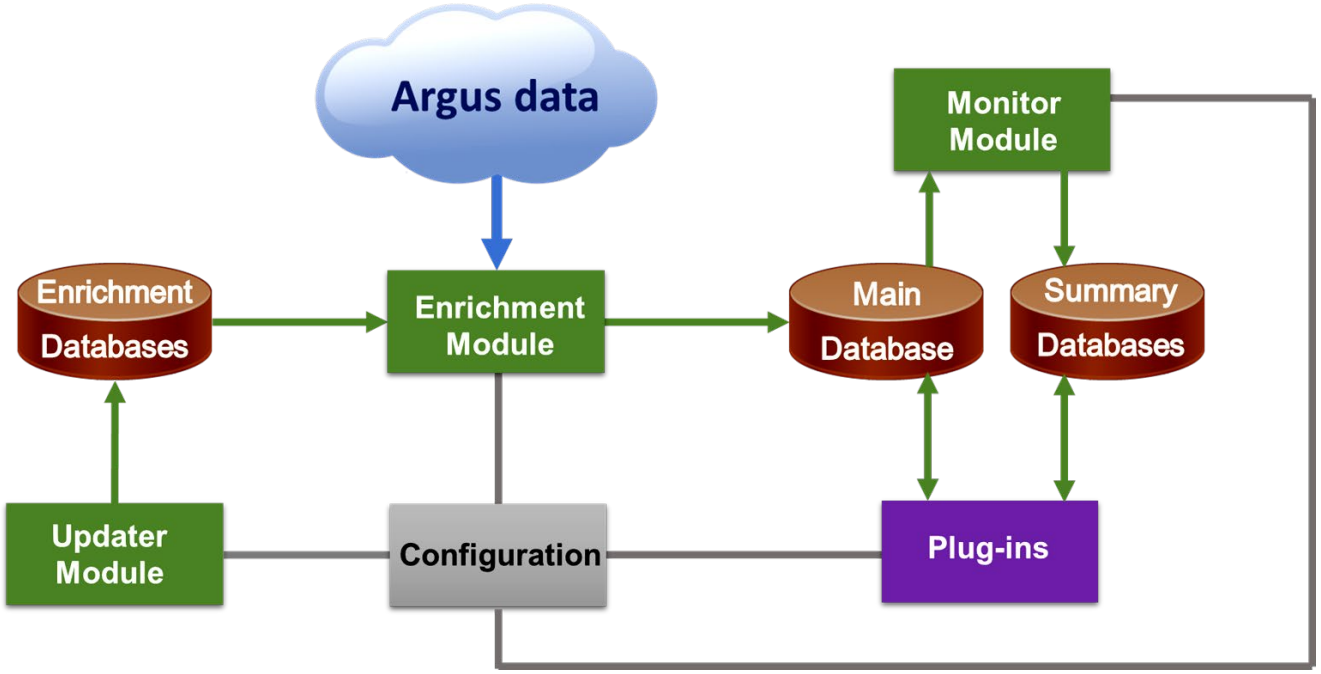
- Flow Data Measurements
  - Network statistics (load, packets dropped, retransmitted)
  - Usage statistics (countries, organizations, ISPs)
  - Diagnostics (jitter, packet size, hops, delay)
- Advanced Analytics
  - Traffic prediction
  - Event detection (automatic reporting)
- Visualizations
  - Critical activity gauges
  - Advanced metrics
  - Connection graphs (top users)

Flow Data Ingestion

- Multiple flow standards supporting existing infrastructure
- SPAN / mirror port support for direct live data



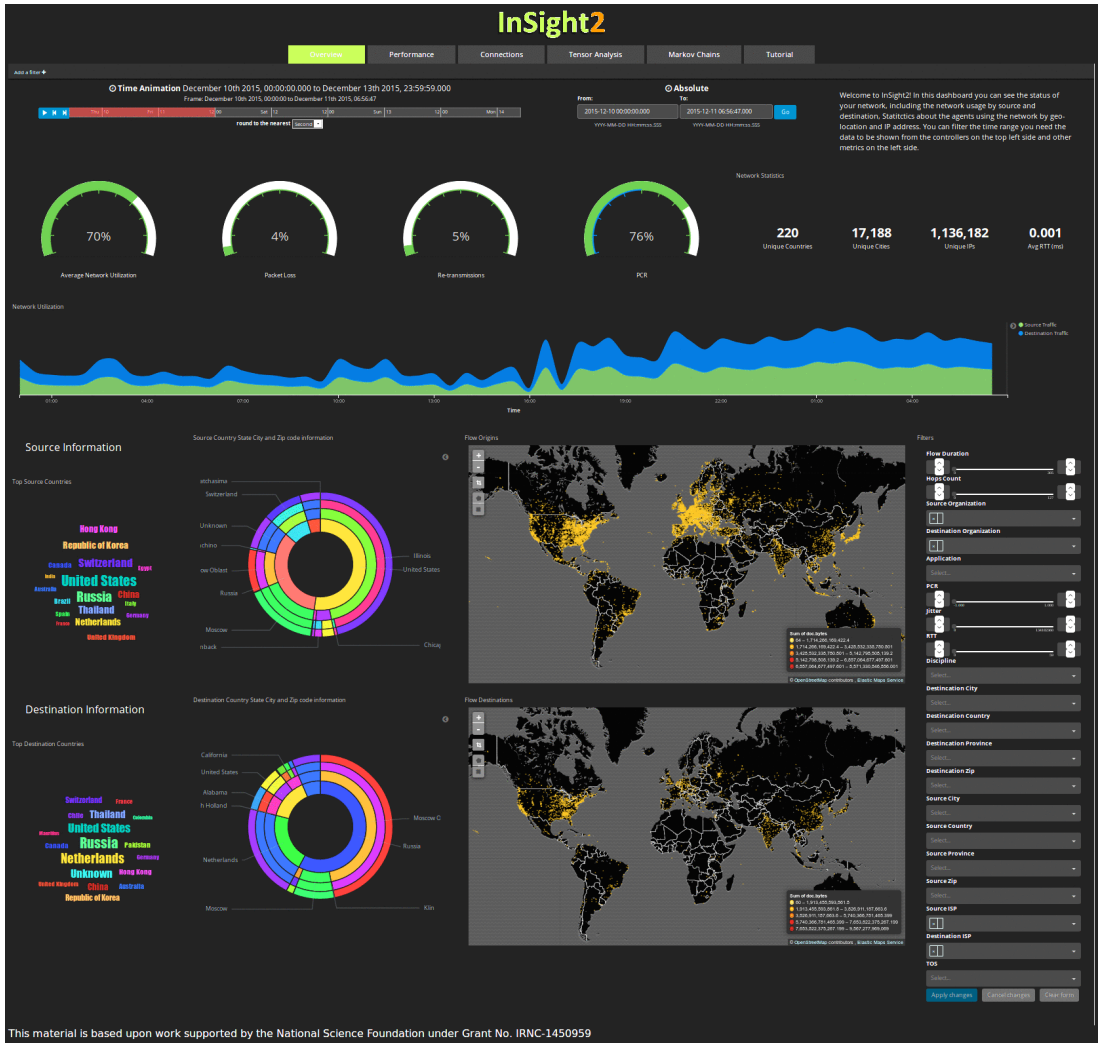
Software Architecture



- Robust, extensible system architecture
- Supporting modular collaborative development
- Development by academia, deployment by everyone

Performance Measurements

- Main Dashboard
- Activity Gauges
- Country Tag Cloud
- Geo Map
- Intuitive filters

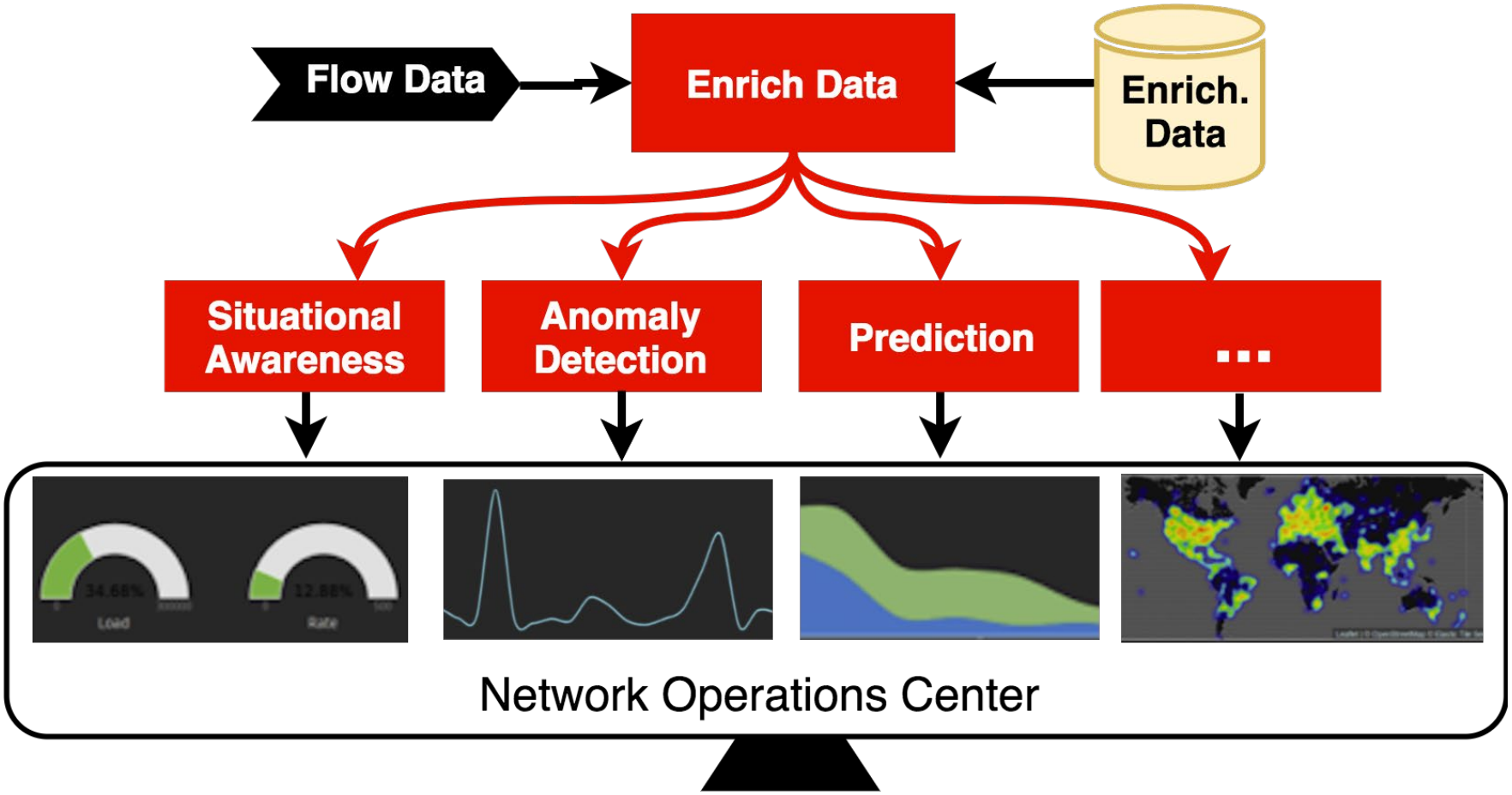


THE UNIVERSITY OF TENNESSEE KNOXVILLE

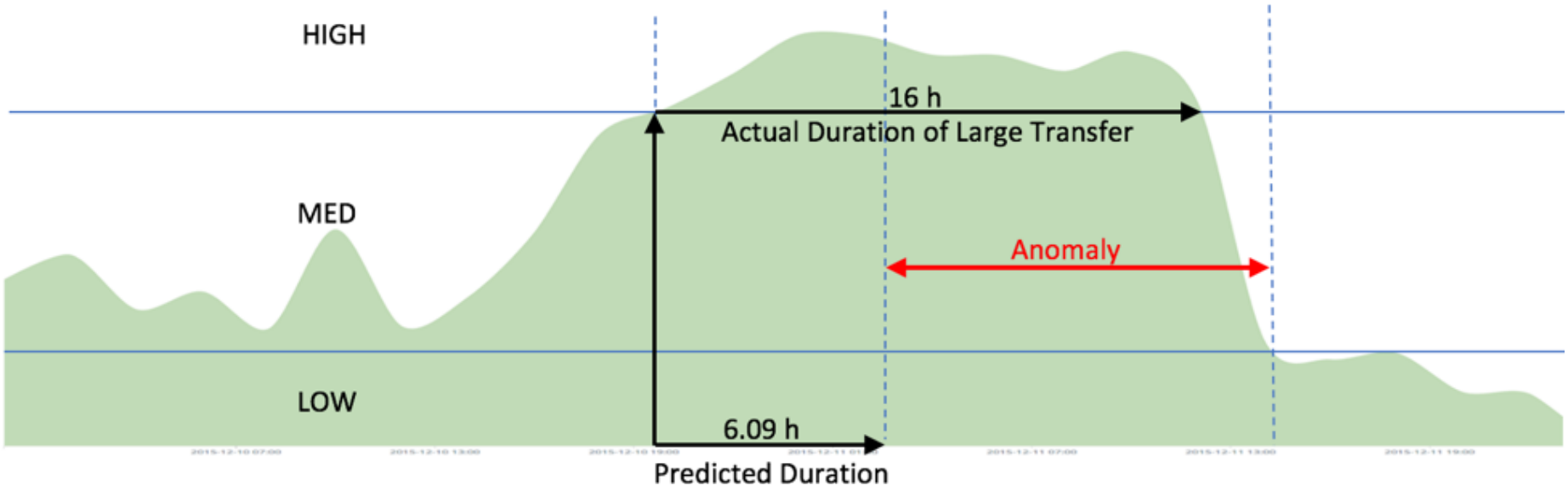
Performance Metrics

- Traffic ratios
- PCR
- TCP timers
- Path hops
- Packet sizes
- Jitter
- Inter-packet arrival time

Modular Analytics



Prediction of Large Data-transfers



Demonstration using flow data from GLORIAD network from 2012 - 2015

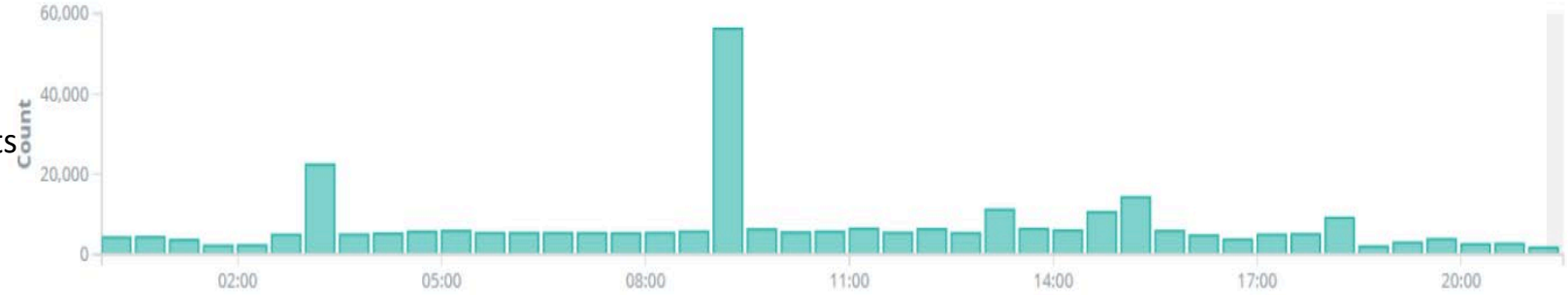
Prediction of Large Data-transfers

- Markov chain
  - Deterministic finite-state machine where, given the present state, future transitions only depend on the current state: $P(i_n|i_0, \ldots i_{n-1}) = P(i_n|i_{n-1}) \equiv P_{i,j}$
- Steady-state probabilities
  - Expected number of times each state contributes to infinitely long realization: Solve $\pi P = \pi$
- Mean first passage time
  - Expected number of transitions from given state till another state is reached: $m_{i,j} = 1 + \sum_{k \neq j} P_{i,k} m_{k,j}$

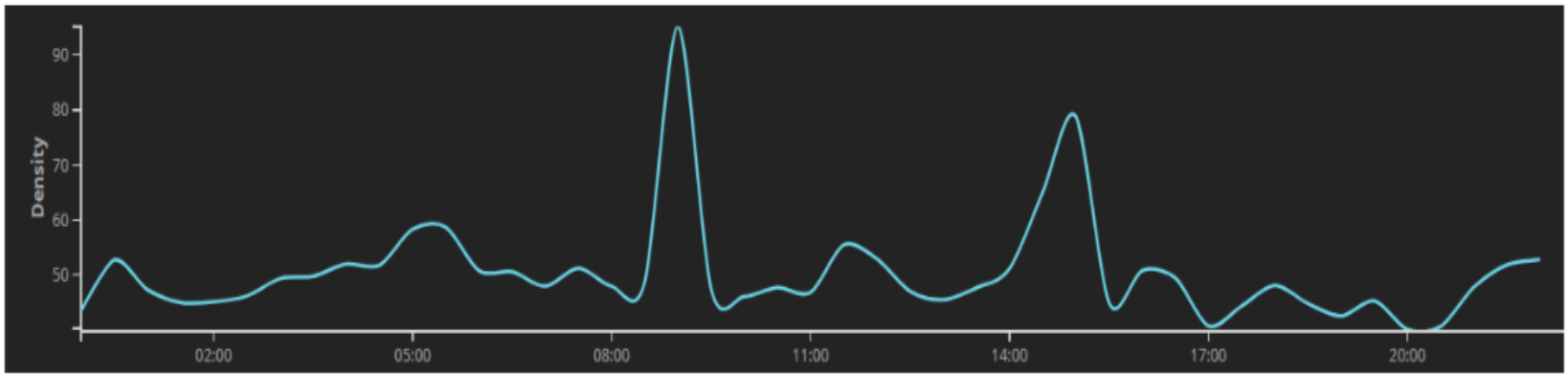
Botnet Detection

- RED Alert Algorithm (Recursive Event Detection).
- Uses tensors as storage containers for data.
- Based on multi-linear algebra theory.

Num. active known Botnets

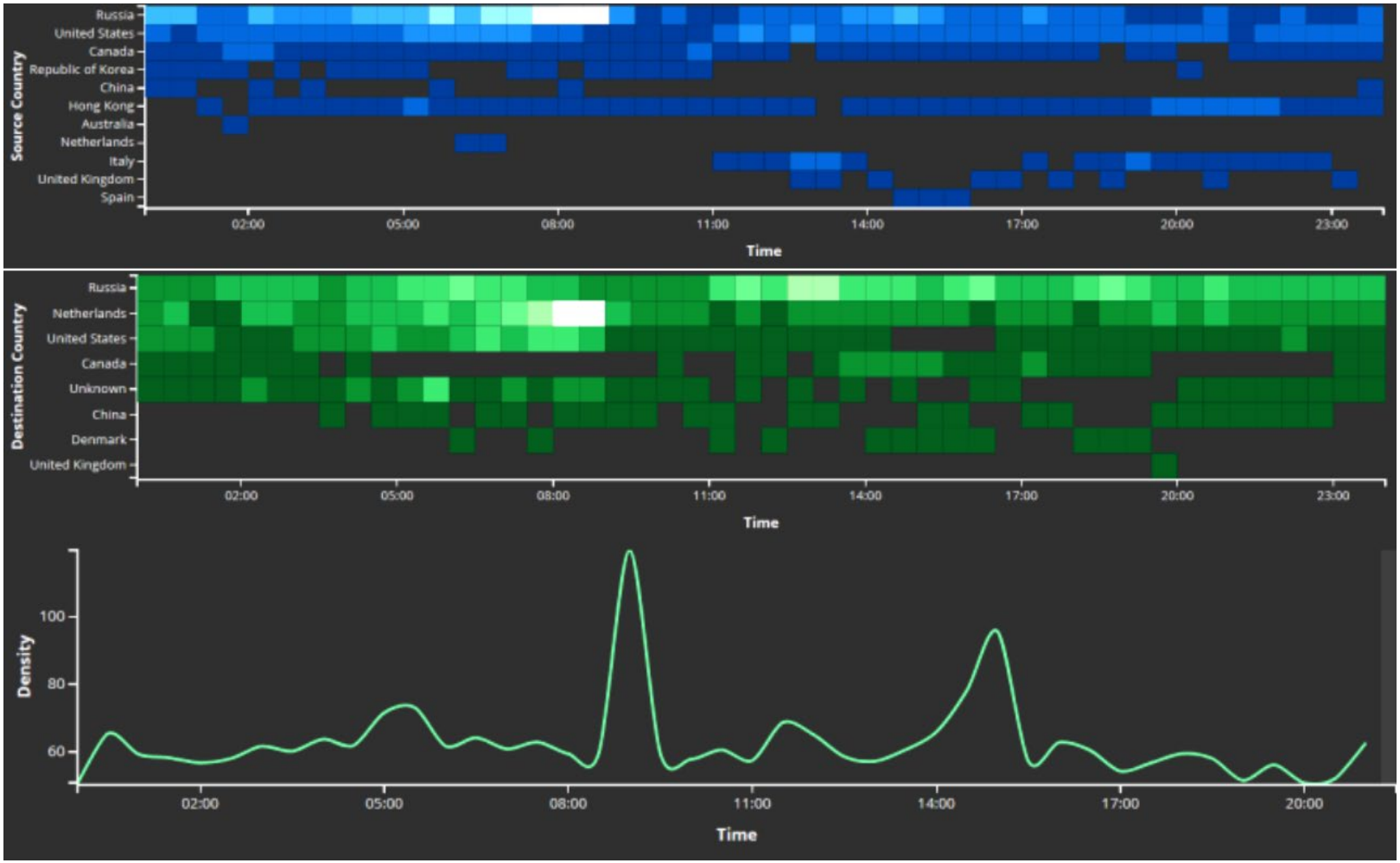


Botnet presence estimate based on num. conn.



Host IPs identified by automatically filtering data

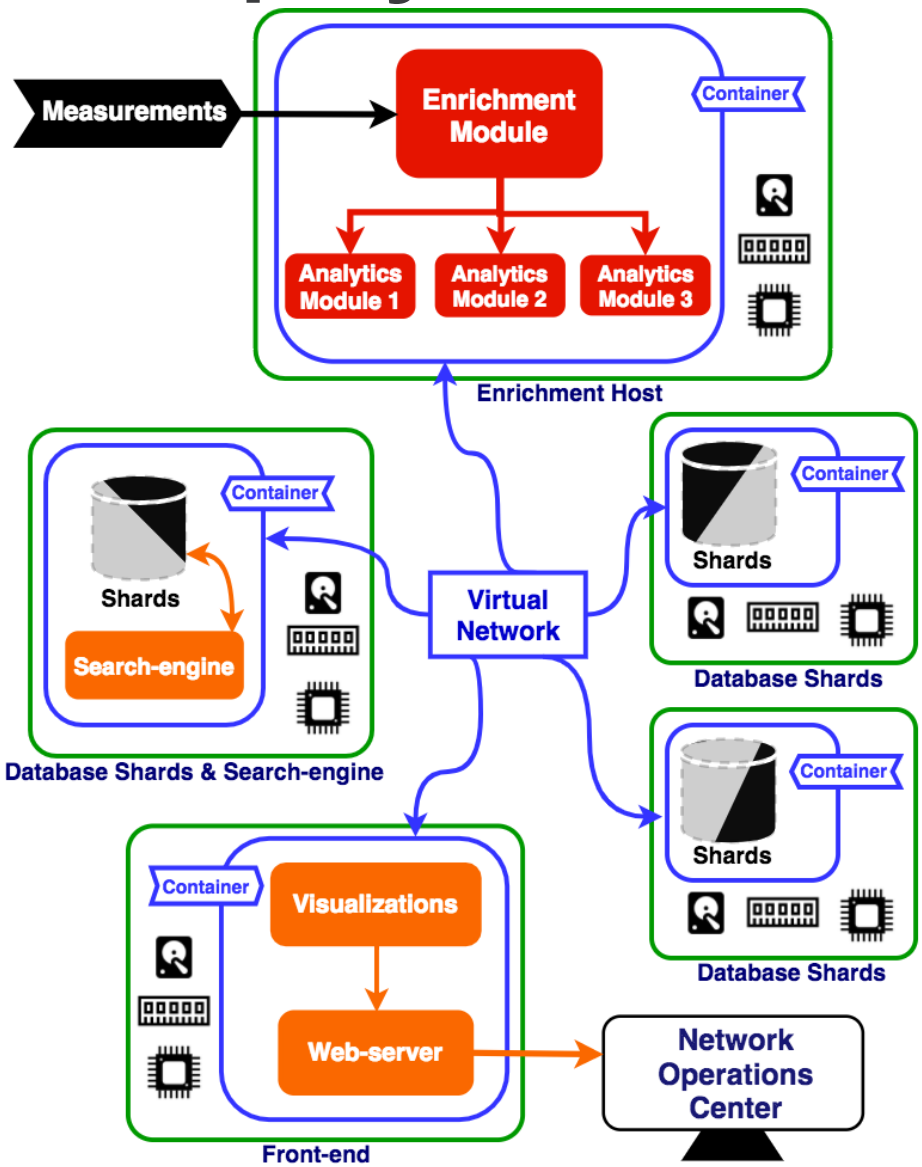
Botnet Detection



Botnet activity detected by RED Alert

Virtualized Deployment

- Extensibility via modularized deployment
- Third-party plugin support
- Docker based distribution
- Available via GitHub



More Information

- Contact information:
  - Angel Kodituwakku
    - Email: angelk@utk.edu
    - LinkedIn: **angelkdev**
  - Jens Gregor
    - Email: jgregor@utk.edu
- Download at GitHub
  - https://github.com/**angelkdev**/InSight2
- InSight2 usage demo
  https://youtu.be/jcc7Bk9BHpM