

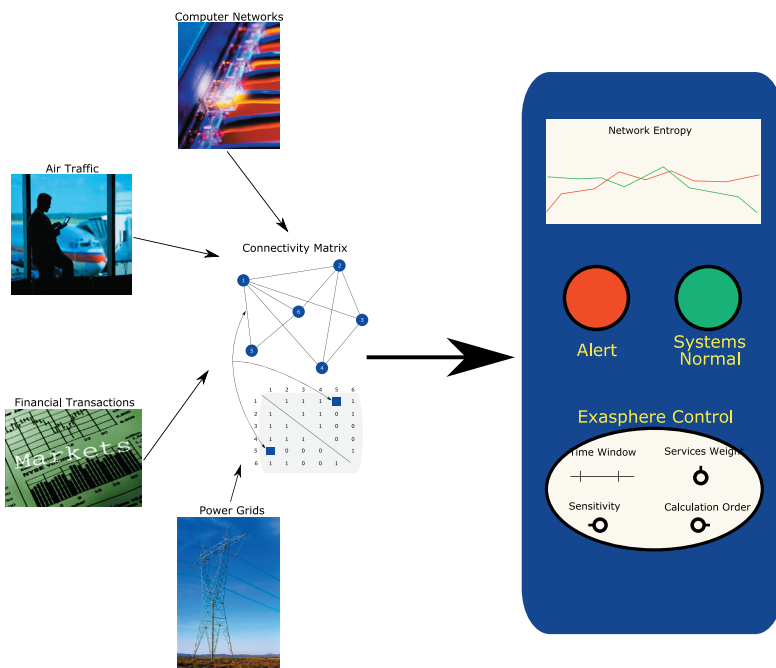
ExaSphere

Network Analysis Engine

Networks are so vast and complex and change so rapidly that until now there was no known method of tracking their behavior. Now there is a way!

ExaSphere

- Is the first and only completely generalized tool for network monitoring.
- Tracks a network entropy spectra over time, monitoring its behavior
- Identifies abnormal behaviors in networks – anomalies, attacks, & failures.
- Is a general-purpose engine for all types of networks



The Origin of ExaSphere

- The ExaSphere Network Analysis Engine software algorithms were developed under a DARPA research program to monitor the Internet.

What is a network?

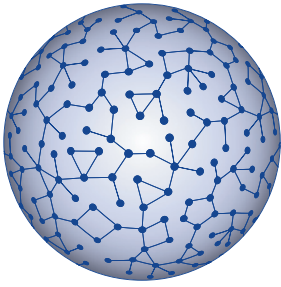
- A network is a set of points or nodes where some are connected.
- Examples
 - Internet networks: Computers are the nodes and information (emails, images, and documents) is transferred between them.

Airline networks: Airports are nodes and the number of connecting flights or number of passengers transported is the transfer.

Banking networks: People and companies are nodes and money is the transfer.

Why is this problem hard?

- Important networks involve millions of nodes and trillions of changing values.
 - All values are of equal importance and thus it is impossible to measure or track the network without reducing the problem to a manageable set of values.

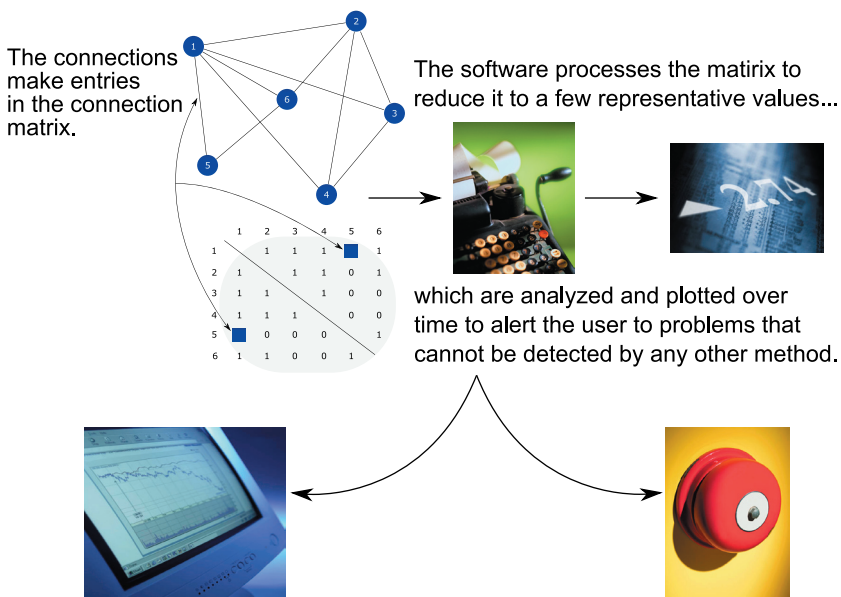


ExaSphere

Network Analysis Engine

How does it work?

- Four inputs are needed: (1) Time, (2) Node i, (3) Node j, (4) Transfer value
 - Transfer value can be money, passengers, or information from i to j where i & j are numbers (1, 2, ...) that distinguish the nodes, whether they are people, computers, or airports.
 - These four variables will be repeated in millions and millions of records corresponding to each data transfer.
- A window of time is defined to add up these transfers into a collection as a matrix.
 - For example, the financial transfers done between 8:00 and 9:00am, then next, those between 9:00 and 10:00am and so on.
 - The transfers are added up into a 'connection matrix' for each window: $C_{i,j}$ for that time.
 - There are a few user adjustable parameters depending on the application.
- The software processes C over time:
 - It reduces C to a few representative values for network monitoring, and plots as a graph.
 - Entropy levels for inputs and outputs of all nodes are computed and plotted.
 - The curves are correlated over time to summarize behavior.
 - Other analysis is performed on the entropy structures



Types of Networks That Can Be Tracked and Analyzed

- **Communication Networks**
 - Internet Traffic
 - Phone - wireless & wired
 - Mail, UPS, Fed-Ex
- **Transportation**
 - Air Traffic
 - Highway Traffic
 - Waterways
 - Railroads
 - Pipelines
- **Financial**
 - Banking Transactions
 - Accounting Flows
 - Ownership & Investment
 - Input-Output Economic Flows
- **Utility & Energy**
 - Electrical Grids
 - Water & Sewer Flows
 - Natural Gas Distribution
- **Social Networks**
 - Organizational Structures
 - Terrorist & Criminal Networks
- **Manufacturing Processes**
 - Process & Manufacturing Workflow
- **Biological & Ecological**
- **Disease & Health**