The following author(s) request authority to disclose the following presentation in the MORSS Final Report, for inclusion on the MORSS CD and/or posting on the MORS web site.

Name of Principal Author and all other author(s): A. Shaw, R. Mills, B. Mullins, and K. Hopkinson

Principal Author's Organization and address:

R.F. Mills
Air Force Institute of Technology
AFIT/ENG
2950 Hobson Way
Wright-Patterson AFB OH 45433

Phone: 937-255-3636 x4527
Fax:
Email: robert.mills@afit.edu

Original title on 712 A/B: A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact

Revised title: no change

Presented in (input and Bold one): (WG 6/8, CG___, Special Session ___, Poster, Demo, or Tutorial):

This presentation is believed to be: UNCLASSIFIED AND APPROVED FOR PUBLIC RELEASE
# A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact

## Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. **REPORT DATE**  
   01 JUL 2008  

2. **REPORT TYPE**  
   N/A  

3. **DATES COVERED**  
   -  

4. **TITLE AND SUBTITLE**  
   A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact  
   
5a. **CONTRACT NUMBER**  

5b. **GRANT NUMBER**  

5c. **PROGRAM ELEMENT NUMBER**  

5d. **PROJECT NUMBER**  

5e. **TASK NUMBER**  

5f. **WORK UNIT NUMBER**  

6. **AUTHOR(S)**  

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**  
   Air Force Institute of Technology AFIT/ENG Wright-Patterson AFB, OH 45433  

8. **PERFORMING ORGANIZATION REPORT NUMBER**  

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**  

10. **SPONSOR/MONITOR’S ACRONYM(S)**  

11. **SPONSOR/MONITOR’S REPORT NUMBER(S)**  

12. **DISTRIBUTION/AVAILABILITY STATEMENT**  
   Approved for public release, distribution unlimited  

13. **SUPPLEMENTARY NOTES**  

14. **ABSTRACT**  

15. **SUBJECT TERMS**  

16. **SECURITY CLASSIFICATION OF:**  
   a. **REPORT**  
   unclassified  
   b. **ABSTRACT**  
   unclassified  
   c. **THIS PAGE**  
   unclassified  

17. **LIMITATION OF ABSTRACT**  
   UU  

18. **NUMBER OF PAGES**  
   28  

19a. **NAME OF RESPONSIBLE PERSON**  

Standard Form 298 (Rev. 8-98)  
Prescribed by ANSI Std Z39-18
A Multilayer Graph Approach to Correlating Network Events with Operational Mission Impact

Al Shaw
Robert Mills
Barry Mullins
Kenneth Hopkinson

Center for Cyberspace Research
Air Force Institute of Technology
robert.mills@afit.edu

Educating the Future Leaders of America’s Armed Forces
Overview

• The research problem
• Objectives
• Approach
• Completed and ongoing research
• Future research
The Problem

• Provide automated support in detecting computer network outages and degradations
  – Not enough to know there’s a problem…need to know the effect on the customer’s mission
  – Often called the “holy grail” of network management

• Current methods for this type of problem are mostly manual in nature
  – Network management tools focus on the network rather than the mission
  – First indications of mission impact are when people start calling the help desk
  – Even when we know there’s an outage, it’s difficult to explain the “so what?” factor to the commander
Limitations of Current NMS Technology

• Network Management Technology Survey
  – Network Auto-Discovery, Service Auto-Discovery
  – Correlation & Root-cause analysis techniques
  – Traffic Flow Analysis, Independent Agent Systems
  – Host-based Intrusion detection, Artificial Immune Systems
  – Active Networks

• Observations
  – NMS technologies allow increased visibility and control but cannot relate network status to mission capabilities
  – This information is simply not present in the network
Why Is This Important?

• If we can’t do this now, how will we do it when everyone and everything is networked into the GIG?

• Increased Reliance on IT Raises Stakes for IT Service Providers
  – E-Business and E-Commerce
  – Network Centric Warfare
  – Capabilities that are enabled by IT resources
  – Is there any other kind??

• Bottom line: we need to know what kind of info is traversing the network
The Problem

Currently no automated way to tie IT status to the mission

Customers

IT Providers

IT-enabled Capabilities

Traditional Network Management focused “below the water-line”

Mission Impact Analysis…need to automate link between IT and mission

Debra Curtis, Gartner Group 2004
Research Goals

• Framework for establishing traceability between systems, processes, and operational tasks and missions
  – Compatible with existing COP and DoD products
  – Practical, feasible, maintainable, complete, usable and accurate…
  – Self awareness, autopopulating

• Extensible
  – Build a cyberspace common operational picture
Need clear mapping of cyber assets to physical world missions, tasks, organizations, etc.
Approach

- **DoD Architecture Framework (DODAF)**
  - Guidance for developing / presenting architecture descriptions
  - Used in describing DoD systems and processes

- **Operational View (OV)**
  - Business process modeling
  - Operational tasks and activities, information flows
  - Organizational relationships

- **Systems View (SV)**
  - Physical entities that make up an architecture
  - Computer systems, networks & system functions
  - Data exchanges and communication paths
  - Link systems to capabilities
Approach

• Use multi-layer graph model based on DODAF
  – Mission View
  – Operational View
  – Systems View

• Linkages between layers establish traceability
  – Top down – facilitates comm planning and targeting
  – Bottom up – facilitates response and attack mitigation
Layered Complex Networks

- Marciej Kurant and Patrick Thiran, “Layered Complex Networks”
- Used to study complex systems
  - Multi-layered
  - Accounts for the interactions between and dependencies between physical and logical layers
- The two-layer model with the mapping $M(E_1^\lambda)$ of the logical graph $G^\lambda$ on the physical graph $G^\Phi$. The logical edge $e_1^\lambda$ is mapped on $G^\Phi$ as the path $M(E_1^\lambda) = (v_1^\Phi, v_2^\Phi, v_3^\Phi)$

- “Logical” Layer = City Pairs
- “Traffic Route” Mapping = Route through Stations
- “Physical” Layer = Train Stations

Method for Incorporating Structure of the Underlying Network
Multi-Layer Model of NCO

- Wong-Jiru – 2006
- Net Centric Operations represent complex systems with many different interacting elements
  - To measure net centricity, the complexity and interactive nature of NCO must be modeled
- Multi-layer model of NCO
  - Each layer represents major contributors to NCO
  - Relationships are graphically represented
  - Node and Edge definitions tailored to each layer

<table>
<thead>
<tr>
<th>Layer</th>
<th>Node</th>
<th>Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Task</td>
<td>Transition</td>
</tr>
<tr>
<td>People</td>
<td>Position</td>
<td>Information path, working relationship</td>
</tr>
<tr>
<td>Application</td>
<td>Application</td>
<td>Data-specific Interoperability</td>
</tr>
<tr>
<td>System</td>
<td>Application support node/platform</td>
<td>Communication Interoperability</td>
</tr>
<tr>
<td>Physical Network</td>
<td>Infrastructure entities</td>
<td>Communication pathways, wired or wireless</td>
</tr>
</tbody>
</table>
Multi-Layer Model of NCO: Interlayer Relationships

• Layers interact with each other
• Any failures or successes that occur at the lower layers may contribute (negatively or positively) upon the completion of mission objectives
• Interlayer relationships represented by mappings

<table>
<thead>
<tr>
<th>Mapping</th>
<th>Node to Node Mapping</th>
<th>Edge to Edge Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process-People</td>
<td>Allocates task to people</td>
<td>Order or route of process tasks through people</td>
</tr>
<tr>
<td>People-Applications</td>
<td>Identifies the applications used by people</td>
<td>Route of information transactions through applications</td>
</tr>
<tr>
<td>Applications-Systems</td>
<td>Identifies which systems support which applications. For some, the system and application are the same</td>
<td>Route of information from application to application through supporting systems</td>
</tr>
<tr>
<td>Systems-Physical Network</td>
<td>Identifies which entry points into the communications infrastructure is accessed by which system</td>
<td>Route of communications from one system to another.</td>
</tr>
</tbody>
</table>
Air Operations Center Model

Mission Layer
- Mission
- METL

OV Layer
- Organizations
- Operational Nodes
- Tasks
- Informational Needlines

SV Layer
- Systems/Servers
- Networks/Links
- Functions
- Data Exchange Requirements
### Table 6a. ATO Production Operational Tasks

<table>
<thead>
<tr>
<th>Description</th>
<th>Operational Node</th>
<th>Required Inputs</th>
<th>Output</th>
<th>Mission Essential Tasks Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan and Schedule Tanker Missions</td>
<td>Air Refueling</td>
<td>MAAP, SPINS, Intel Assessment, Airlift Requirements</td>
<td>Tanker Schedule</td>
<td>OP 2.1.4, OP 6.1.1, ST 4.3.1</td>
</tr>
<tr>
<td>Prepare MAAP Inputs</td>
<td>Air Refueling</td>
<td>Tanker Schedule</td>
<td>MAAP Inputs</td>
<td>OP 2.1.4, OP 6.1.1, ST 4.3.1</td>
</tr>
<tr>
<td>Plan and Schedule Airlift Missions</td>
<td>AME</td>
<td>Intel Assessment, Weather Forecast, Airfield Capability Assessment, ACO and SPINS</td>
<td>Airlift Schedule</td>
<td>ST 4.3.1</td>
</tr>
</tbody>
</table>

### Table 12a. Operational Task/System Function Associations

<table>
<thead>
<tr>
<th>Operational Task</th>
<th>System Functions</th>
</tr>
</thead>
</table>
| Plan and Schedule Tanker Missions | 1. Retrieve Airlift Requirements  
2. Plan Tanker Missions  
3. Schedule Tanker Missions       |
| Prepare MAAP Inputs (Air Refueling) | 1. Retrieve Airlift Requirements  
2. Plan Tanker Missions  
3. Generate Component MAAP Inputs |
| Plan and Schedule Airlift Missions | 1. Generate Weather Forecast  
2. Retrieve Strategic Mobility Information  
3. Schedule Airlift Missions       |
Multilayer Model Problem Domain

**Mission View**
- Mission
  - METL
    - Mission Essential Tasks
      - Composed of
      - Complete

**Operational View**
- Organizations
  - Operational nodes
    - Composed of
    - Perform
    - Complete
    - Operational Tasks
      - Complete

**Systems View**
- Server, Systems, Networks
  - Use
  - Perform
  - System Functions
  - Perform
OV Layer

METL

Organization

Name
Organizational Scope

1 Parent

* Child

Composed of ▼

* Supervises

Operational Node

Name
Description
Node Criticality
Network Scope

1 Performs

* ▼

Task

Description
Criticality

Device

Organizational Needline

Description
Criticality
Information Exchange
Time Frame

Information Requirement

Depends on ▲
Top-Down Analysis

- Starts at the mission layer
- Identifies all operational tasks and system functions that help complete a mission essential task
- Supporting operational nodes, systems, and networks are also identified
ST 4.3.1: Establish and Coordinate Movement Services within Theater

- MAAP Team
- MAAP Inputs
- External Airlift
- Prepare MAAP Inputs
- Import External Airlift
- Plan and Schedule Airlift Missions
- Import Airlift Missions
- Import Airlift Missions into AODB
- Export Airlift Missions
- Schedule Airlift Missions
- Retrieve Strategic Mobility Information
- AME
- AMC Reach-back Server
- AMC Reach-back Server
- JWICS
- JWICS
- U.S. Secret Network
- SIPRNET
- SIPRNET
- ABP Data
- ABP Data
- ABP Data
- ABP Data
- IRIS Messaging
- C2IPS
- PACE SIPRNET
- PACE JWICS
- MAAP Inputs
- TBMCS TAP
- TBMCS AIM
- AODB
- U.S. Secret Network
Bottom-up Analysis

• Starts at a network device (server, router, etc.)
• Identifies affected system functions (either on server or receive inputs from server)
• Affected operational and mission essential tasks can then be identified
OP 6.1.1: Process/Allocate Operational Aerospace Targets

OP 3.1.5: Publish Air Tasking Order(s)

ST 4.3.1: Establish and Coordinate Movement Services within Theater

MAAP Team

Prepare MAAP

Generate MAAP

MAAP Inputs

MAAP Inputs

Generate ATO with SPINS

Generate ATO

Generate Component MAAP Inputs

Prepare MAAP

Generate and Disseminate ATO

External Airlift

Import External Airlift

Import External Airlift

MAE

TBMCS

TAP

AODB

External Airlift

ABP Data

U.S. Secret Network

Retrieve Airlift Missions From AODB

Generate and Disseminate ATO

Generate MAAP Inputs

External Airlift

TBMCS AIM

ABP

OP 3.1.5: Publish Air Tasking Order(s)
Results

- Mission impact of network and system outages clearly demonstrated
  - All operational nodes, systems, tasks, and functions clearly identified
  - Operational and mission essential tasks affected by an outage completely identified
- Traceability through all layers of the model
- Usable for top-down and bottom-up analysis
- General methodology with broad applicability
Areas for Future Research

• Automating data input…cannot rely on manual inputs
  – Self-awareness

• How to handle degradation?
  – Network connectivity degradation, but services are available locally
  – Specific service may be down, but the network is green

• Determining Resource Criticality
  – Different users, different times, different priorities
  – Weighting and probabilities of degradation / destruction

• New Architectures
  – Modeling Network Virtualization
  – Service Oriented Architectures

• Cyberspace situational awareness
Map & Mission Context

• What does cyberspace “look like”
  – Common Operational Picture
  – Traceability to real world missions

• Cyberspace changes depending on how you look at it
  – Is multi-dimensional…has many aspects
  – Is a medium of operations (like air, land, and sea)
  – Supports operations in the physical domain (air, land, sea)

• Cyberspace is all about collecting, processing, and exchange of information
  – Has various layers of abstraction…just like information
  – The value / nature of information depends on where you sit and why you need it
Cyberspace Situational Awareness

Depending on your function, your desired “map” of cyberspace (i.e., what you care about) is different.

- **Cyberspace as domain of ops** (attack/defend) – each layer is an avenue for attack and we need to understand linkages for targeting, damage assessment, etc.
- **Cyberspace as supporting infrastructure** – need clear mapping of cyber assets to physical world missions, tasks, organizations, etc.
Questions?