REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10/23/2019	Conference Briefing	

4. TITLE AND SUBTITLE
Mission Mapping and Robust Network Analysis Methods

5a. CONTRACT NUMBER
FA8702-19-C-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Becca Rousseau; Les Servi; (MITRE)
David Myers (AFRL)

5d. PROJECT NUMBER
03196CA0ZZ

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-19-3022

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Air Force (AFLCMC)

10. SPONSOR/MONITOR'S ACRONYM(S)
AFLCMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
https://www.abstractsonline.com/pp8/#!/6818/presentation/5485 INFORMS National Meeting, Seattle, WA
Sunday, October 20, 2019 - Wednesday, October 23, 2019

14. ABSTRACT
Mission mapping aims to identify the dependencies between a mission's components (e.g. activities and functions) and resources like applications, services and communication infrastructure. Using robust optimization methods and MILP we identify critical infrastructure nodes while hedging against imperfect dependency estimates in a mission map. The results and approach are illustrated with a numerical example.

15. SUBJECT TERMS
Strategic Planning; Information Security Architecture; mission mapping; robust network analysis; RDF; Resource Description Framework

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		40	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

Mission Mapping and Robust Network Analysis*

Becca Rousseau (becca@mitre.org, MITRE)

Les Servi (lservi@mitre.org, MITRE)

David Myers (david.myers.35@us.af.mil, AFRL)

23 October 2019

INFORMS National Meeting

Seattle, WA

* Approved for Public Release; Distribution Unlimited. Public Release Case Number 19-3302

MITRE

Challenge

Advanced nodal critically analysis methods requires mission mapping input and ties to required dependency parameters

BUT

the current subject matter experts (SMEs) approach is both very time consuming and expensive

Solution: Create an approach to (semi-) automate process and tested process with simulated data.

MITRE

Overview

- Generate RDF Mission Maps
- Generate dependency relationship parameters and uncertainty network
- Perform Robust Network Analysis

MITRE

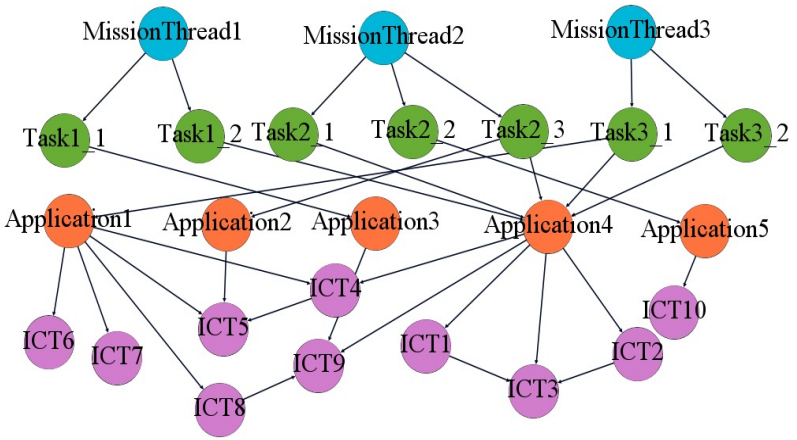
Overview

- **Generate RDF Mission Maps**
- Generate dependency relationship parameters and uncertainty network
- Perform Robust Network Analysis

MITRE

Generate RDF Mission Maps

- **Input:** Map out dependency relationships in a directed graph between
  - *Mission Threads*
  - *Tasks*
  - *Applications/Services*
  - *ICT Infrastructure*

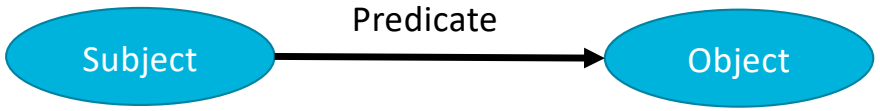


- **Goal:** Identify Cyber Key Terrain (CK-T) could be hardware/software, cables, data center, DNS, cloud service etc.

MITRE

What is the Resource Description Framework (RDF)?

- RDF
  - Data Model - Representation of data as a directed graph
  - Every statement is represented by a *TRIPLE (Subject, Predicate, Object)*



- Captures attributes of objects or relationships between objects

http://www.linkeddatatools.com

MITRE

Generate RDF Mission Maps

MITRE

Generate RDF Mission Maps

- **Python Scripts pull inputs from Excel workbook**
- **Constraints:**
  - Follow a given hierarchy/vocabulary and structure (adaptable)
  - Ensure graph is properly connected (ex: all tasks rely on some application)
  - Use .ttl syntax
- **Input:**
  - 1. Node Classes and their URI's for RDF triples
  - 2. Size (Number of nodes at each level/of each type)
  - 3. Density (probability of edges between/within levels)
  - 4. Predicates and their URI's for RDF triples

MITRE

Input 1: Node Classes and Information for RDF Graph

Determines how nodes are referenced in RDF triples

Class	NodeURIBase	ClassURI
MissionThread	http://example.org/nodes	http://example.org#MissionThread
Task	http://example.org/nodes	http://example.org#Task
Application	http://example.org/nodes	http://example.org#Application
ICT	http://example.org/nodes	http://example.org#ICT

"MissionThread1 is of the type MissionThread"

Example (in .ttl file):

…

<http://example.org/nodes#MissionThread1> a <http://example.org#MissionThread>

…

MITRE

Input 2: Number of Nodes in Each Class

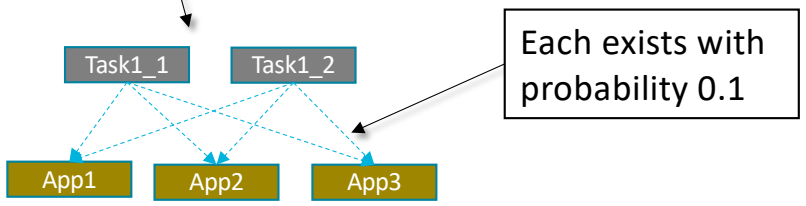
Class	addedByParent?	numTotal	minPerParent	maxPerParent	NodeType
MissionThread	None	3	NA	NA	Top
Task	MissionThread	NA	3	10	Middle
Application	None	40	NA	NA	Middle
ICT	None	50	NA	NA	Leaf

Top: Must depend on something
Leaf: Must be depended on
Middle: Both

MITRE

Input 3: Edge Probabilities (impacts density of graph)

DomainClass	RangeClass	addedByParent?	ProbOfEdge
MissionThread	Task	MissionThread	NA
Task	Application	None	0.05
Application	ICT	None	0.005
ICT	ICT	None	0

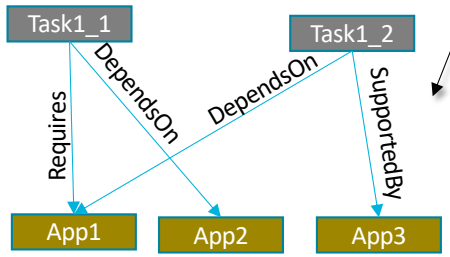


MITRE

Input 4: Predicates and Probabilities

How predicate appears in triple

DomainClass	RangeClass	addedByParent?	Predicate	Probability	PredURI	WhichIsDependent?
MissionThread	Task	MissionThread	CriticalTask	0.6	http://example.org#CriticalTask	Subject
MissionThread	Task	MissionThread	NonCriticalTask	0.4	http://example.org#NonCriticalTask	Subject
Task	Application	None	SupportedBy	0.25	http://example.org#SupportedBy	Subject
Task	Application	None	DependsOn	0.5	http://example.org#DependsOn	Subject
Task	Application	None	Requires	0.25	http://example.org#Requires	Subject
Application	ICT	None	SupportedBy	0.2	http://example.org#SupportedBy	Subject
Application	ICT	None	DependsOn	0.6	http://example.org#DependsOn	Subject
Application	ICT	None	Requires	0.2	http://example.org#Requires	Subject
Application	ICT	None	HostOption	0	http://example.org#HostOption	Subject
ICT	ICT	None	LowDataFlow	0.7	http://example.org#LowDataFlow	Object
ICT	ICT	None	HighDataFlow	0.3	http://example.org#HighDataFlow	Object



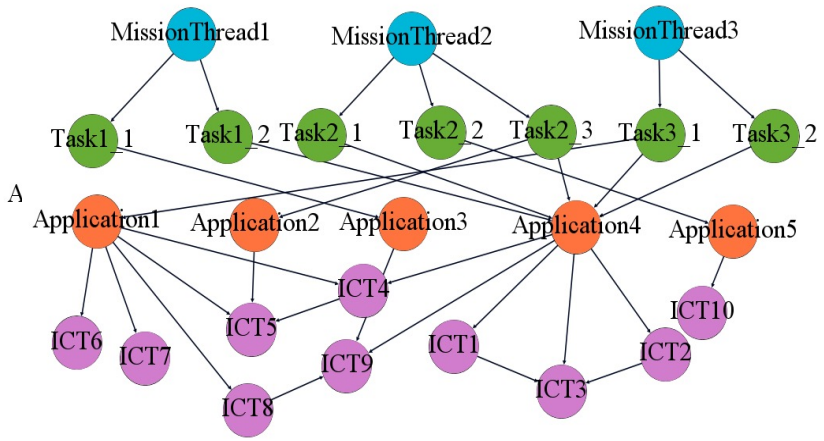
MITRE

Generate RDF Mission Maps: A Small Example

Output: RDF Graph (.ttl file)

```
...

<http://example.org/nodes#Application1> a ns1:Application ;
    ns1:DependsOn <http://example.org/nodes#ICT6>,
        <http://example.org/nodes#ICT7>,
        <http://example.org/nodes#ICT8> ;
    ns1:Requires <http://example.org/nodes#ICT5> ;
    ns1:SupportedBy <http://example.org/nodes#ICT4> .

<http://example.org/nodes#Application2> a ns1:Application ;
    ns1:SupportedBy <http://example.org/nodes#ICT5> .

<http://example.org/nodes#Application3> a ns1:Application ;
    ns1:SupportedBy <http://example.org/nodes#ICT9> .

<http://example.org/nodes#Application5> a ns1:Application ;
    ns1:DependsOn <http://example.org/nodes#ICT10> .

<http://example.org/nodes#ICT1> a ns1:ICT ;
    ns1:LowDataFlow <http://example.org/nodes#ICT3> .

<http://example.org/nodes#ICT10> a ns1:ICT .

...
```

Visualization
(without predicates or 'type' triples)



MITRE

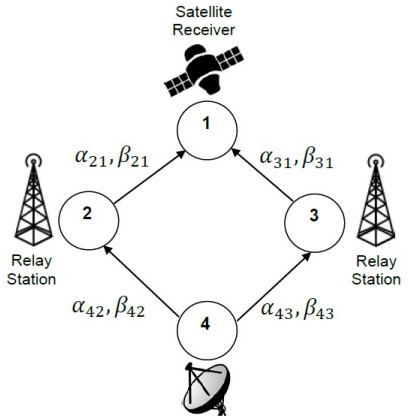
Overview

- Generate RDF Mission Maps
- **Generate dependency relationship parameters and uncertainty network**
- Perform Robust Network Analysis
-

MITRE

FDNA – An approach for capturing dependency

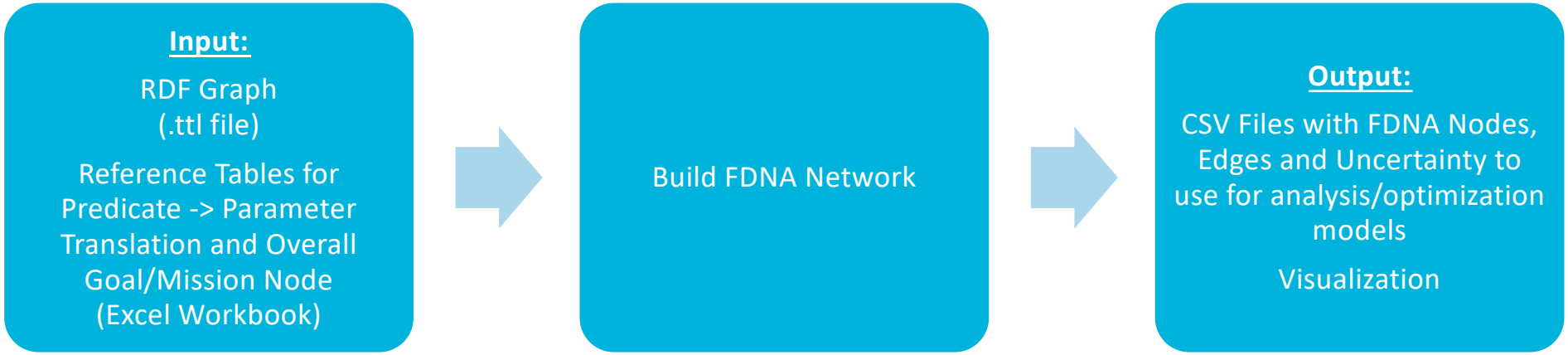
- **Mission/Network has an overall "Goal"**
- **Each node has operability level (0-100)**
- **Two parameters:**
  - Alpha (0-1): "Strength of Dependence"
  - Beta (0-100): "Criticality of Dependence"
- **Each parameter specified in an interval if there is uncertainty**



$$P_j = \min\left[\min_{i\in\mathcal{N}_j}[P_i + \beta_{ij}], 100 - \sum_{\ell\in\mathcal{N}_j}\frac{\alpha_{\ell j}}{|\mathcal{N}_j|}(P_\ell - 100)\right]$$

MITRE

Creating dependency network from RDF Mission Maps



MITRE

Creating dependency Network from RDF Mission Maps: Input

- **For each predicate:**
  - Alpha/Beta (Strength of Dependence and Criticality)
  - Uncertainty in Parameters
  - Direction of dependency
  - Type of relationship (parent = best/worst of children?)

- **For overall mission/goal**
  - Which nodes it depends on (for example, mission threads)
  - Parameters/uncertainty for each edge

MITRE

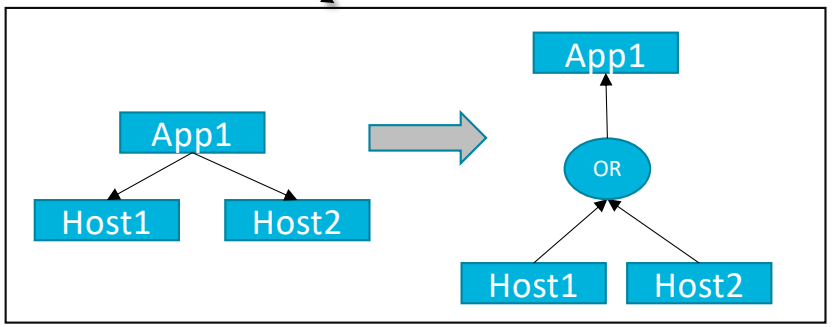
Input 1: Predicate -> FDNA Edges and Parameters

To identify predicate in RDF triple

Parameters and Uncertainty

Predicate	URI	Type	AND_OR	EdgeDirection	alpha	alphaMinus	alphaPlus	beta	betaMinus	betaPlus
CriticalTask	http://example.org#CriticalTask	Dependency	AND	obj-subj	0.8	0.1	0.1	10	5	5
NonCriticalTask	http://example.org#NonCriticalTask	Dependency	AND	obj-subj	0.8	0.2	0.1	75	3	5
SupportedBy	http://example.org#SupportedBy	Dependency	AND	obj-subj	0.75	0.05	0.2	90	10	10
DependsOn	http://example.org#DependsOn	Dependency	AND	obj-subj	0.85	0.1	0.15	50	5	5
Requires	http://example.org#Requires	Dependency	AND	obj-subj	0.85	0.05	0.05	10	2	2
HostOption	http://example.org#HostOption	Dependency	OR_Group	obj-subj	0.9	0.1	0.1	50	15	10
LowDataFlow	http://example.org#LowDataFlow	Dependency	AND	subj-obj	0.25	0.2	0.05	70	5	5
HighDataFlow	http://example.org#HighDataFlow	Dependency	AND	subj-obj	0.75	0.3	0.2	25	1	5
type	www.w3.org/1999/02/22-rdf-syntax-r	Attribute	None	None	None	None	None	None	None	None

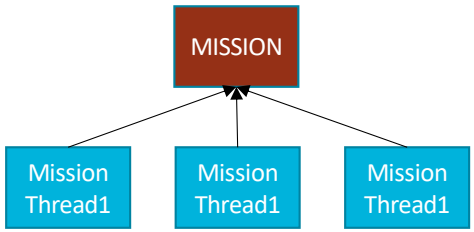
Does this predicate indicate dependency?



MITRE

Input 2: Nodes to Connect to Overall Goal/Mission (Optional, if there is already one "Top" node)

nodeName	alpha	alphaMinus	alphaPlus	beta	betaMinus	betaPlus
MissionThread1	0.5	0.01	0.01	55	5	5
MissionThread2	0.5	0.01	0.01	50	10	10
MissionThread3	0.75	0.1	0.1	25	5	5



MITRE

Creating Dependency Network from RDF Mission Maps - Small Example

Output:

Nodes

Label	ID
MissionThread2	0
Application4	1
Task3_1	2

...

Edges

Depen	Parent Name	Parent ID	Child Nam	Child ID	SOD	COD
0	Application4	1	ICT9	24	0.85	40
1	MissionThread	0	Task2_3	12	0.5	25
2	Task2_2	19	Applicatio	17	0.85	40

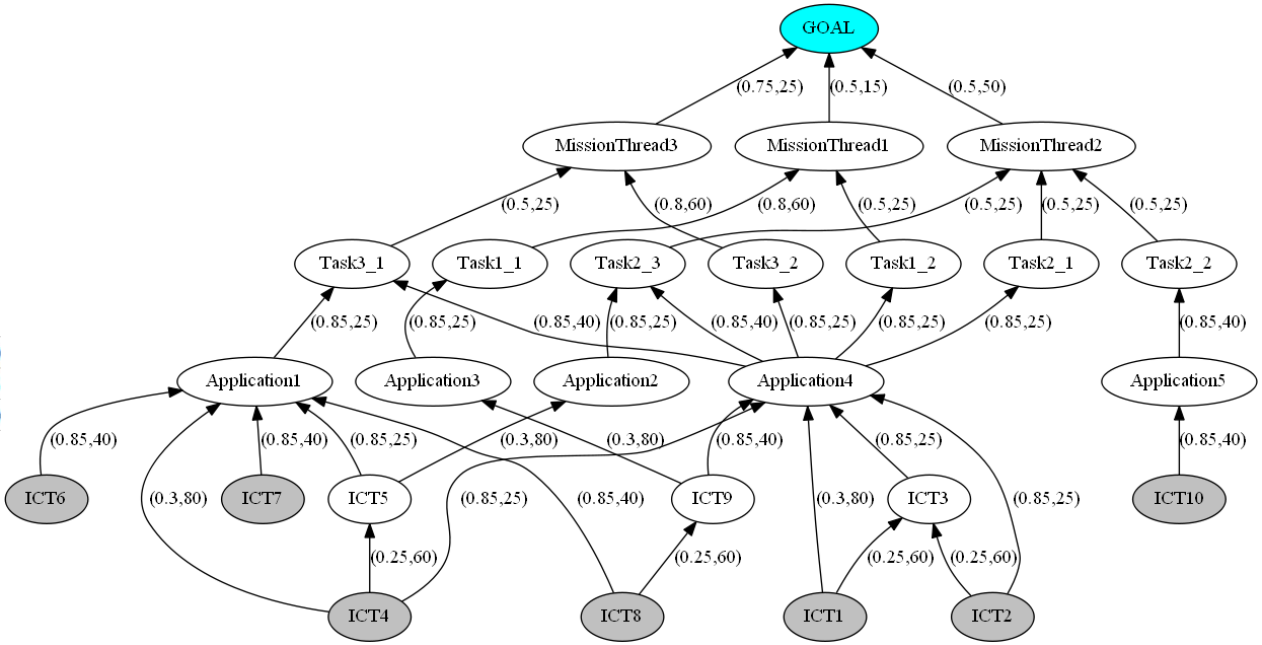
...

Uncertainty

#Alpha	AlphaH	Beta	BetaH
#Comment			
0.1	0.15	5	5
0.1	0.1	5	5
0.1	0.15	5	5

...

Visualization

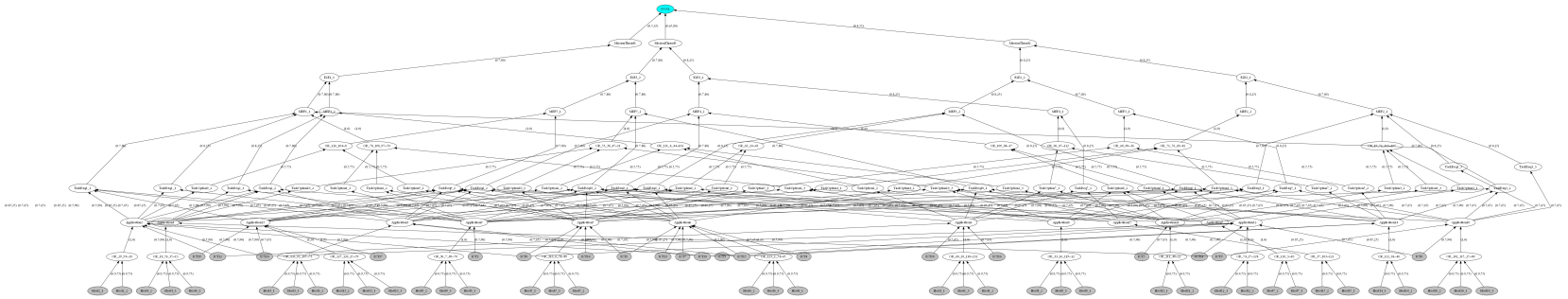


Jump to Demo

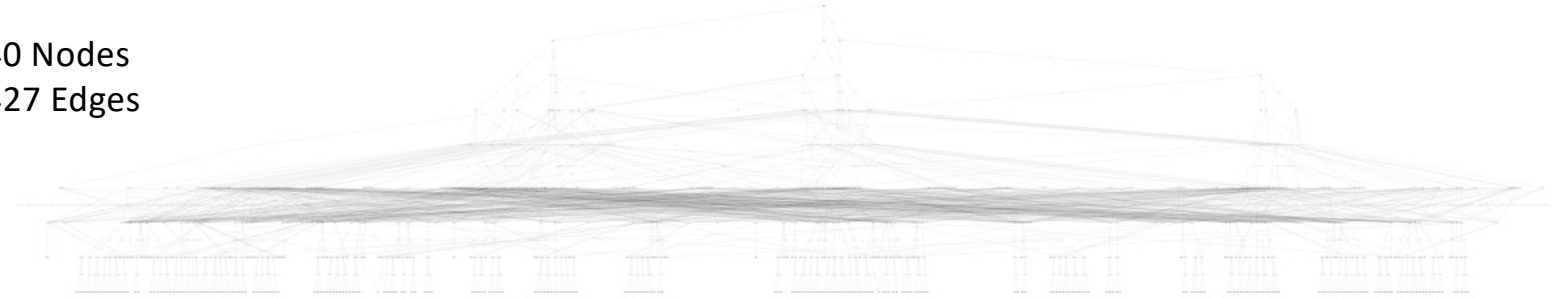
MITRE

Creating Dependency Network from RDF Mission Maps: Larger Examples

160 Nodes
252 Edges



740 Nodes
1427 Edges



MITRE

Overview

- Generate RDF Mission Maps
- Generate dependency relationship parameters and uncertainty network
- **Perform Robust Network Analysis**

MITRE

Robust Network Analysis

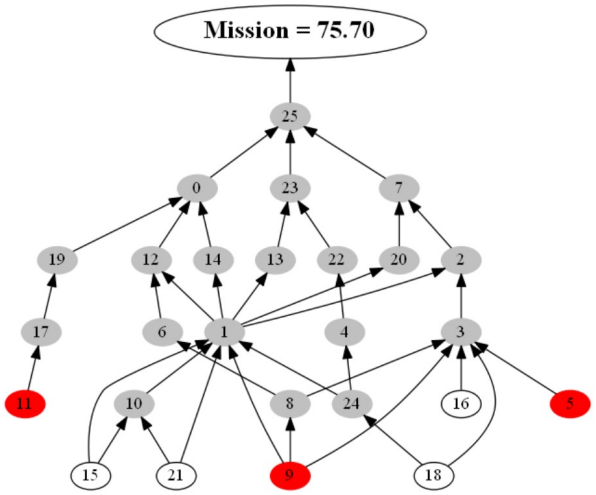
- **Capability previously developed at MITRE from its IRAD program**

- **Purpose: Identifying critical nodes while hedging against uncertainty in parameters**
  - An attacker can change the operability of "N" leaf nodes
  - Choose how many parameters might stray from their nominal values
  - Optimize while accounting for what is "known to be unknown"

MITRE

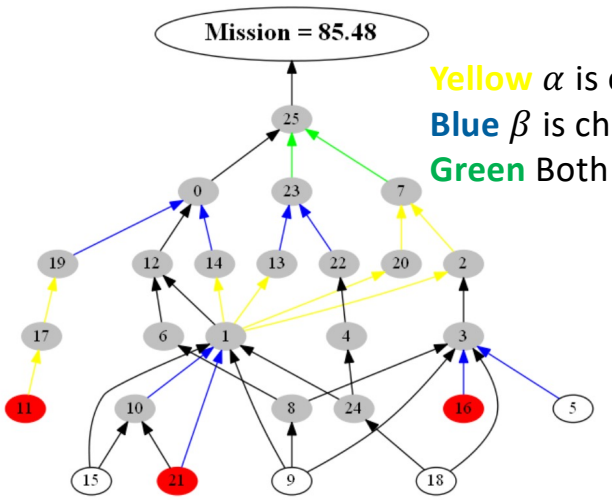
Robust Network Analysis: Small Example

Attack Budget = 3 Nodes
No Uncertainty



Attack***: ICT10****, ICT4, ICT6*

Attack Budget = 3 Nodes
Allowing 10 alpha/10 beta to change



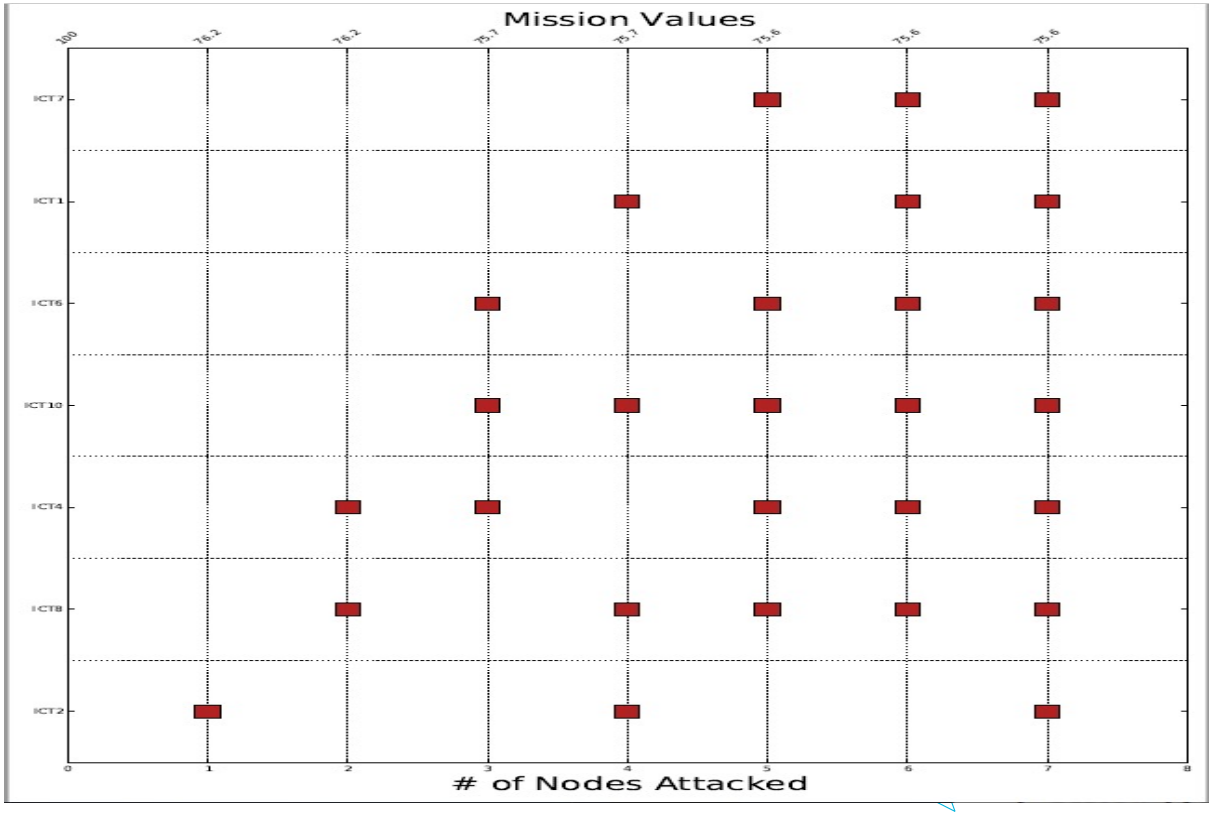
Yellow α is changed from nominal
Blue β is changed from nominal
Green Both α and β are changed nominal

Attack: ***ICT10***, *ICT2, ICT7*

OUTPUT FROM SOFTWARE PREVIOUSLY DEVELOPED AT MITRE

MITRE

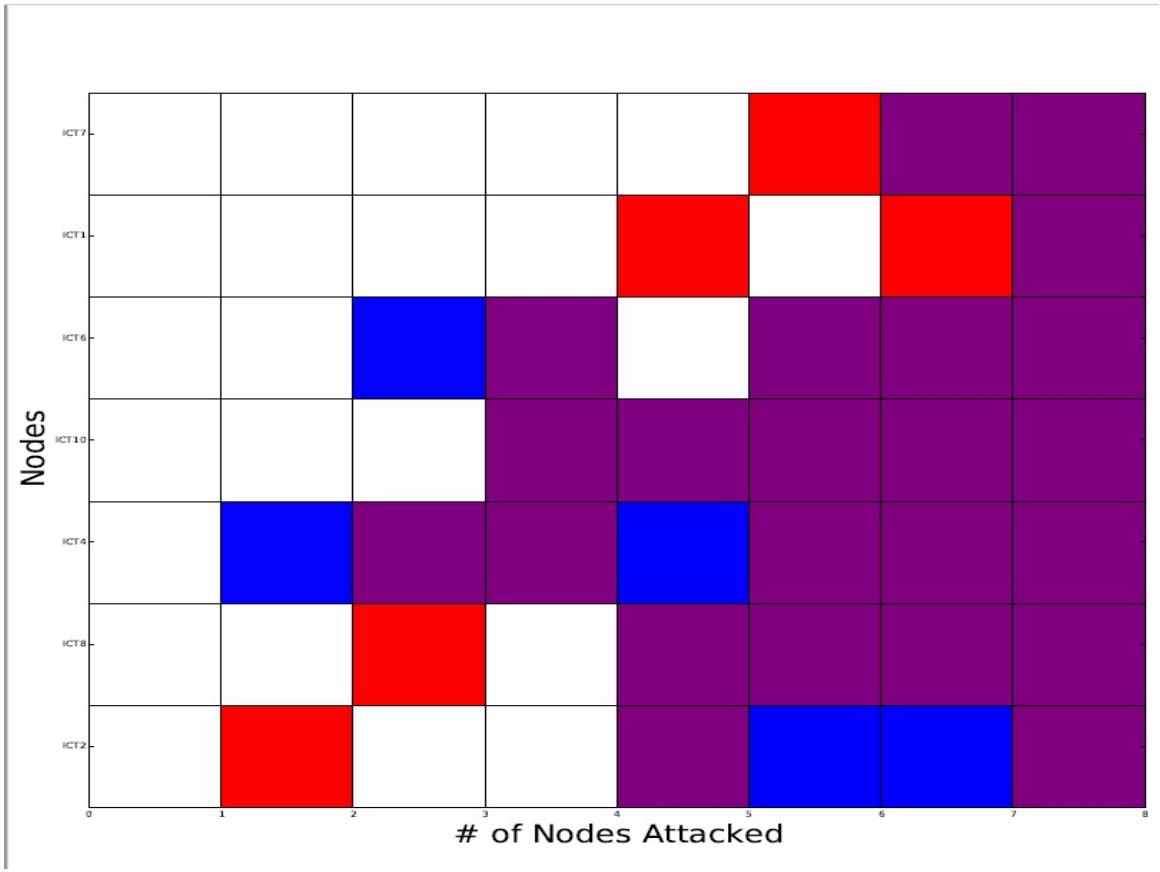
Increasing Attack Budget: Small Example



OUTPUT FROM SOFTWARE PREVIOUSLY DEVELOPED AT MITRE

MITRE

Comparing Robust/Non-Robust Strategy – Small Example



Non-Robust:
Assume all parameters certain
Robust:
Assume 10 alpha/10 beta uncertain

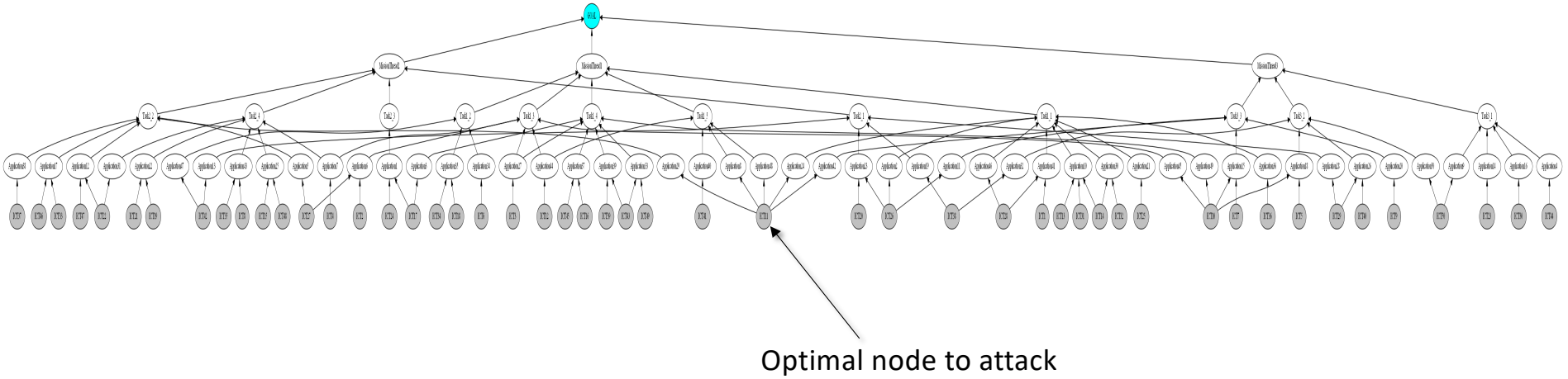
Red: Attacked in Non-Robust Case
Blue: Attacked in Robust Case
Purple: Both

OUTPUT FROM SOFTWARE PREVIOUSLY DEVELOPED AT MITRE

MITRE

More Examples

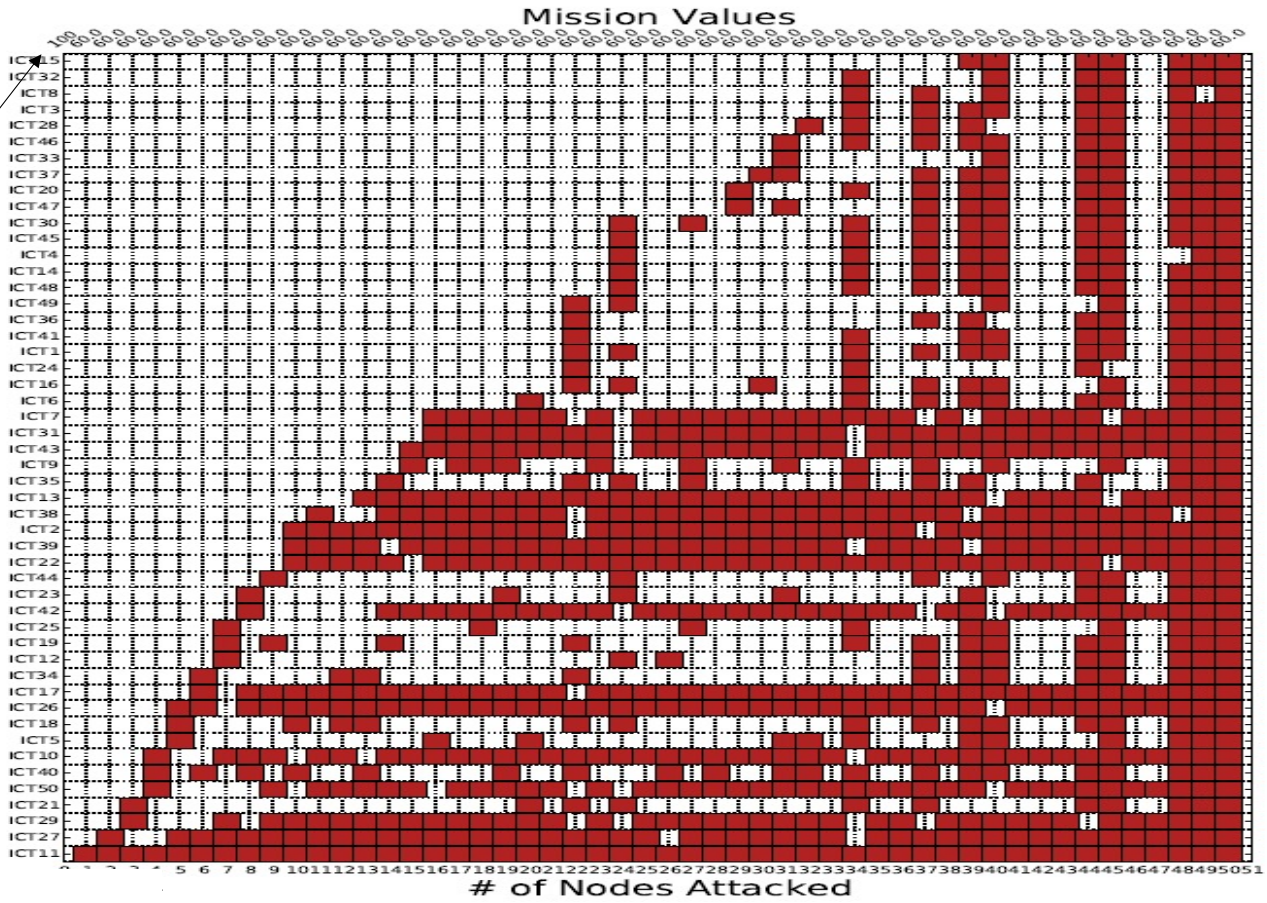
Robust Network Analysis: An Example with Little Resilience



MITRE

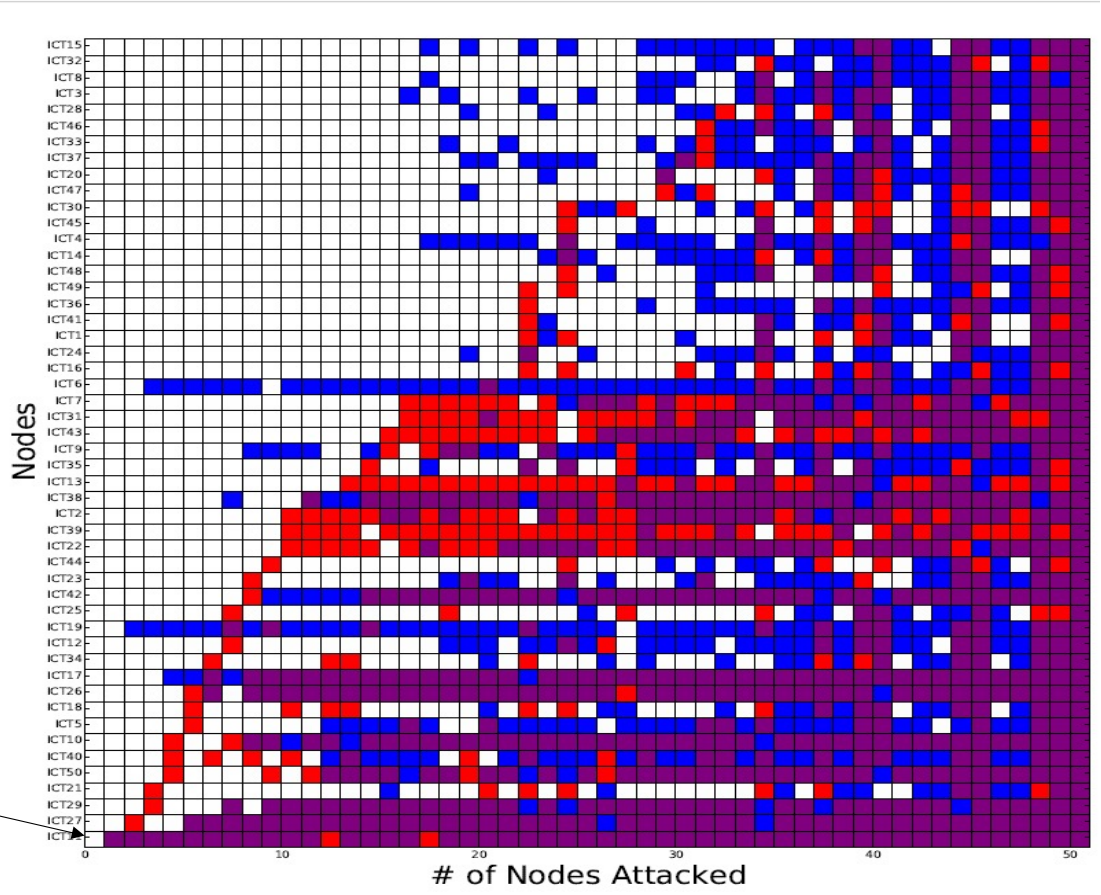
Attack Budget and Resulting Impact Policy:
No Resiliency

Attacking a single node brings the mission down as far as possible



MITRE

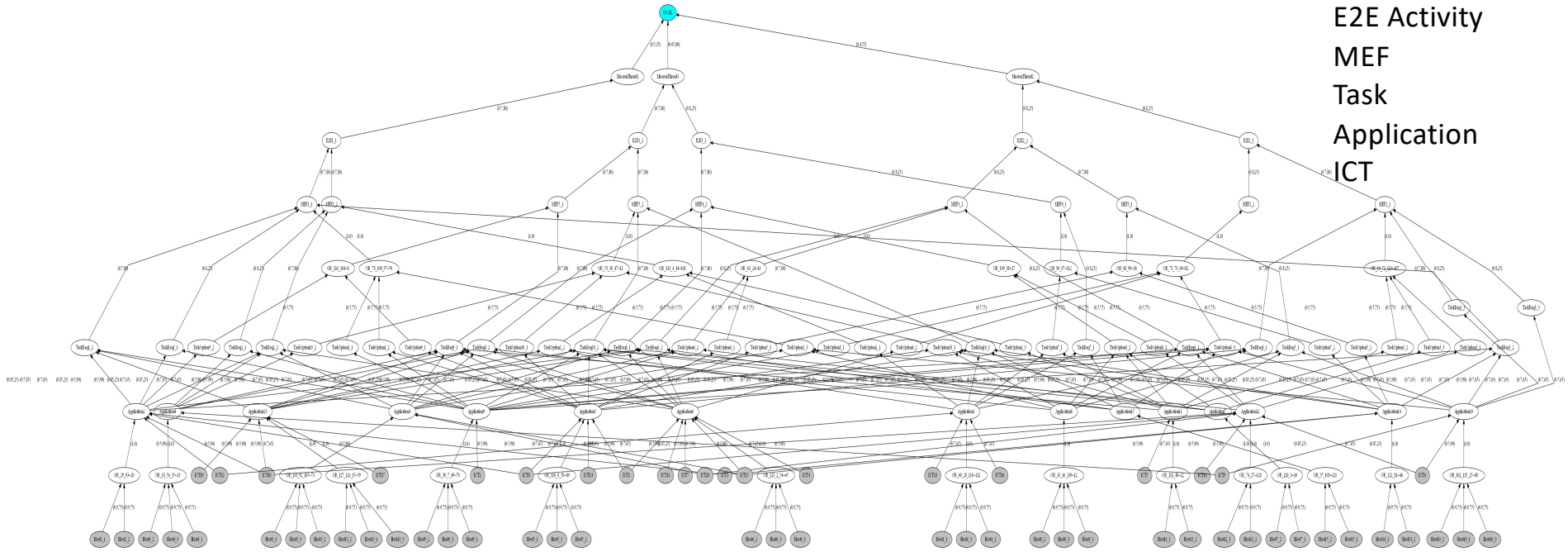
Attack Budget and Resulting Impact Policy:
Comparison of Robust/Non-Robust Analysis



ICT11 almost always Part of the Attack Strategy

MITRE

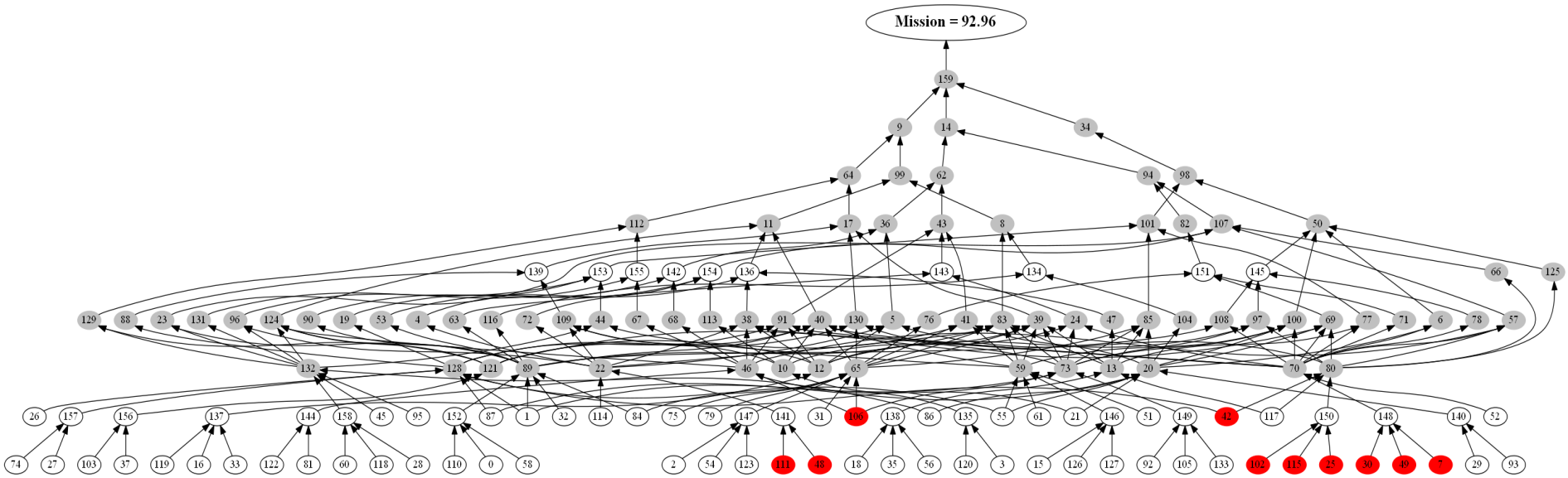
Example with More Resilience



More Node Classes:
MissionThread
E2E Activity
MEF
Task
Application
ICT

MITRE

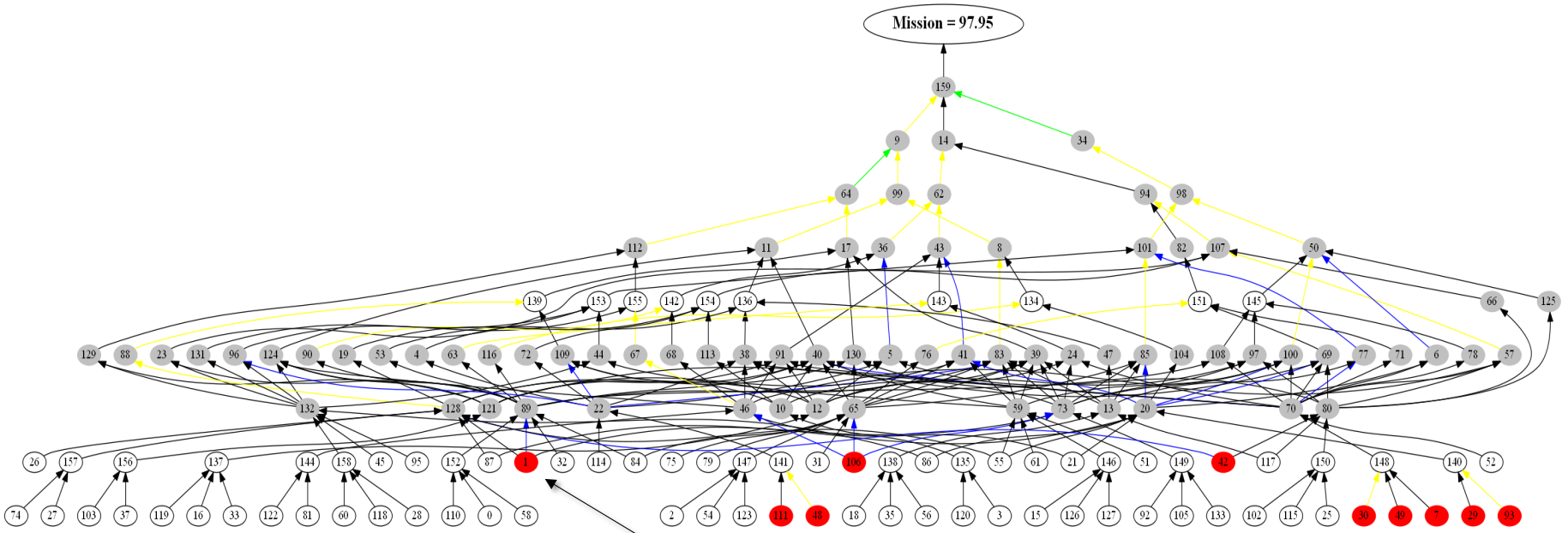
Example with More Resilience



Attacking 10 Nodes Assuming No Uncertainty

MITRE

Example with More Resilience

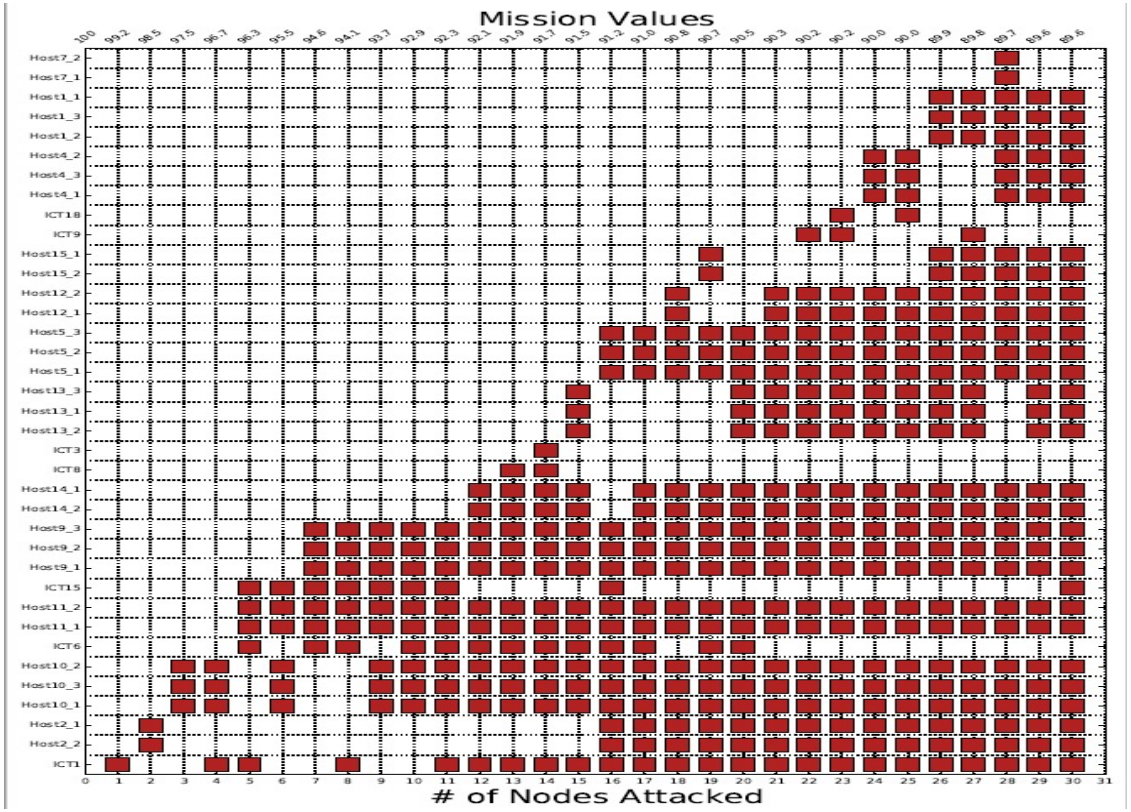


Attacking 10 Nodes Assuming Some Uncertainty (Letting at most 30 of each parameter stray from nominal value)

3 Nodes change in Attack Strategy

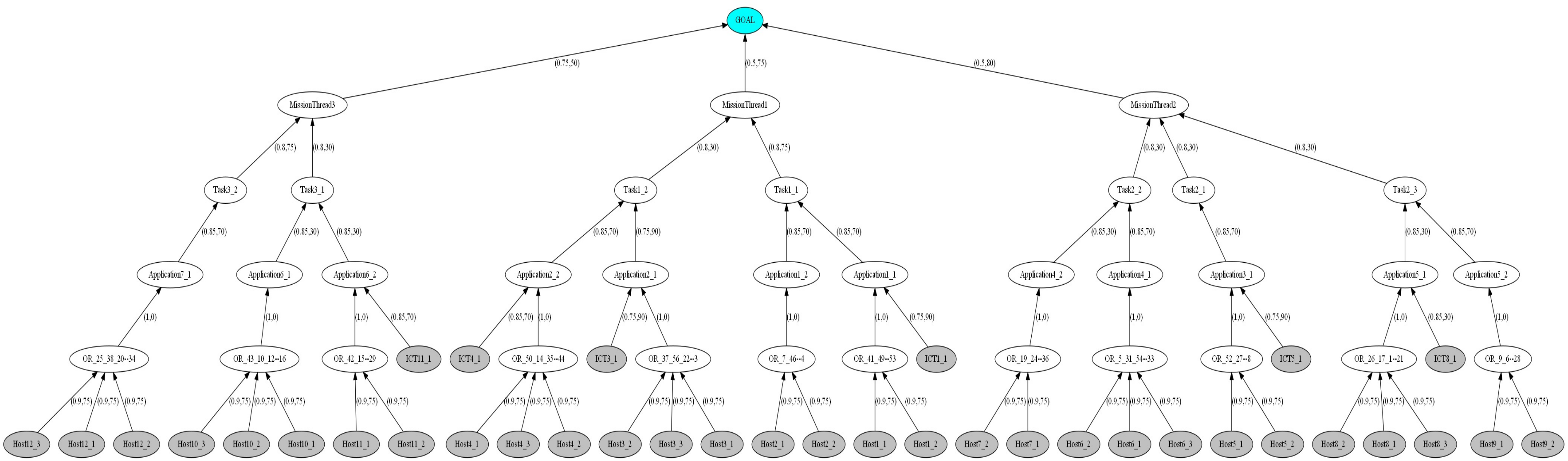
MITRE

Example with More Resilience



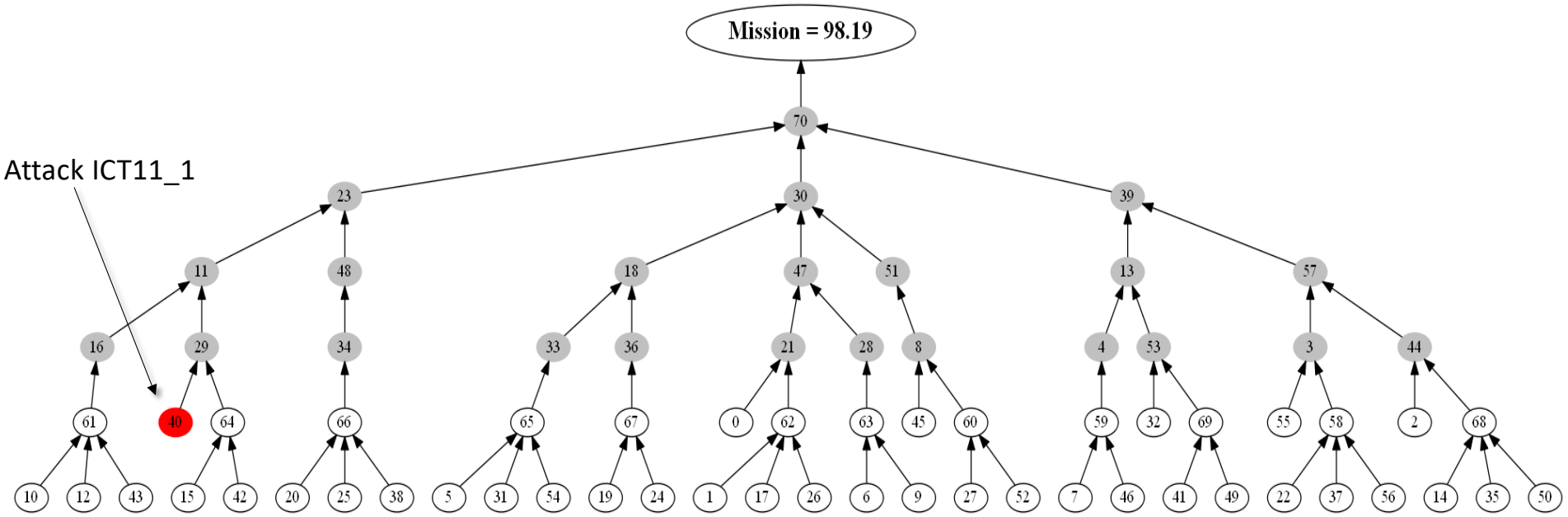
MITRE

Example with "Tree Like" Network with Some Resilience



MITRE

Example with “Tree Like” Network with Some Resilience

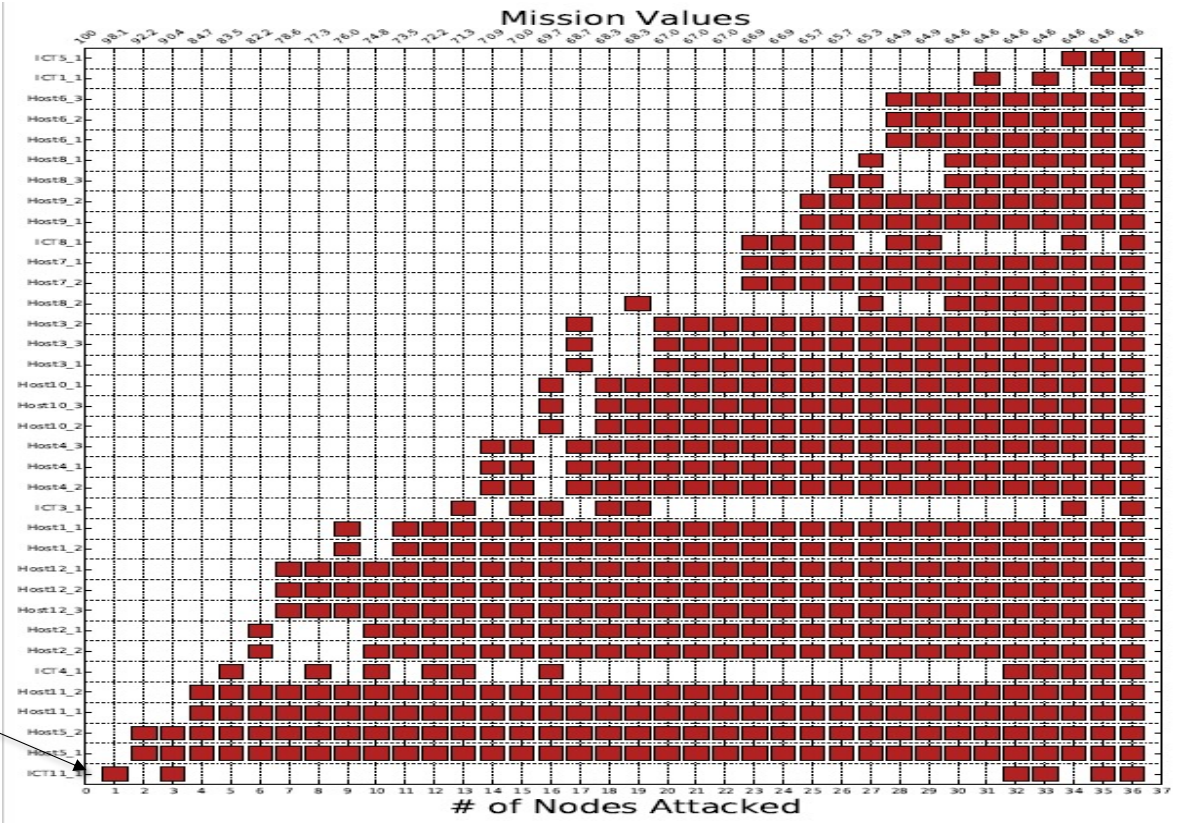


Attacking a single node assuming no uncertainty

MITRE

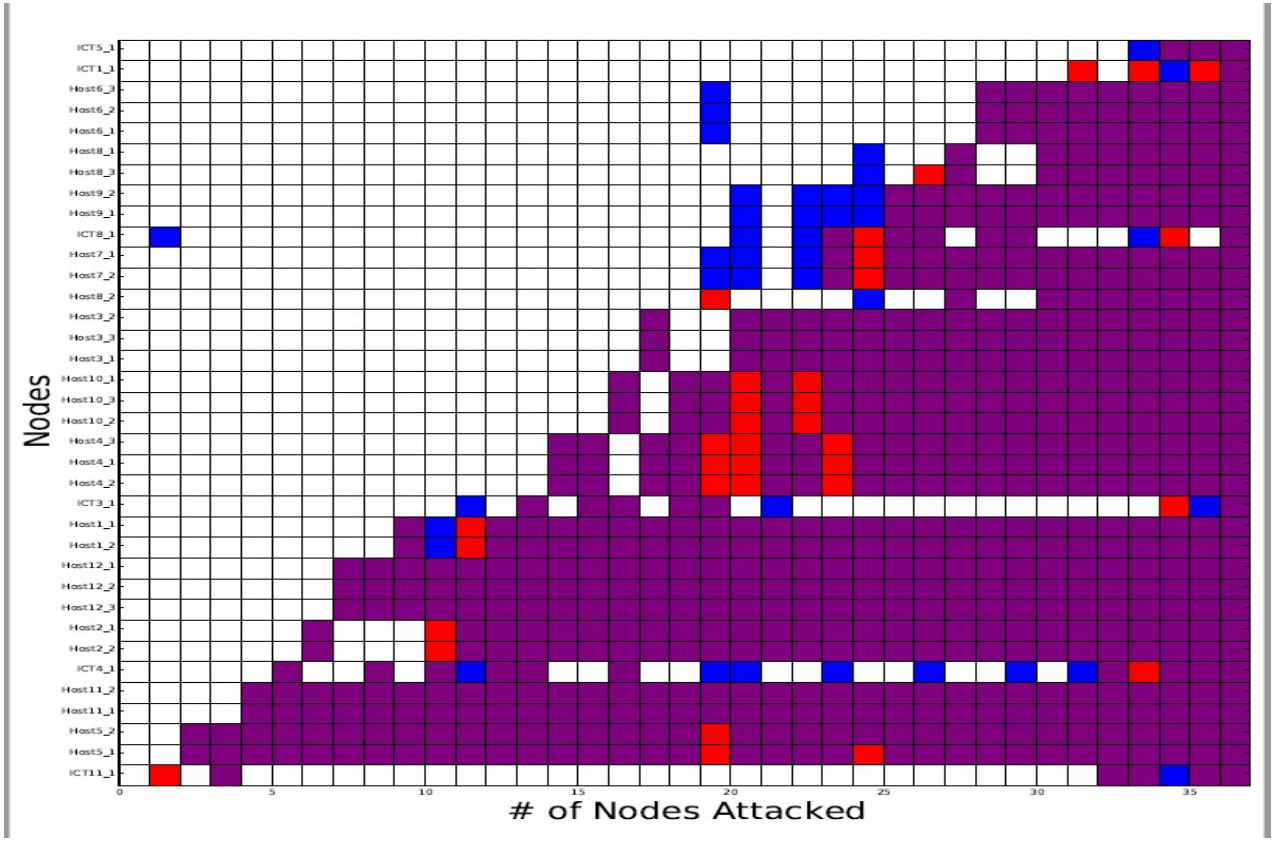
Example with “Tree Like” Network with Some Resilience

ICT11_1 leaves the solution when increasing the “Budget”. So, how critical is it?



MITRE

Example with “Tree Like” Network with Some Resilience: With and Without Uncertainty Assumption



MITRE

Conclusion

- **Demonstrated end-to-end process of incorporating robust network analysis starting with mission maps**
- **Illustrated by example the importance of analysis which accounts for uncertainty in the dependency parameters, i.e., what is known to be unknown**

MITRE

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org