11TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS 2016

A Synthesis of Optimization Approaches for Tackling Critical Information Infrastructure Survivability

Annunziata Esposito Amideo[a], and Maria Paola Scaparra[a]

[a] Kent Business School, University of Kent, Canterbury, UK

Kent Business School

Summary

- Introductory Concepts on Critical Information Infrastructures (CII)
- Survivability-Oriented Interdiction Models
- Resource Allocation Strategy Models
  - for Protecting CII Physical Components
  - for CII Service Restoration
- Survivable Design Models
- Future Research Suggestions
- Conclusions
- References

Introductory Concepts on CII

<u>Critical Infrastructures (CI):</u> primary physical structures, technical facilities and systems which are socially, economically or operationally essential to the functioning of a society or community, both in routine circumstances and in the extreme circumstances of an emergency (UNISDR, 2009)

[Image Source: www.iprem.ca]

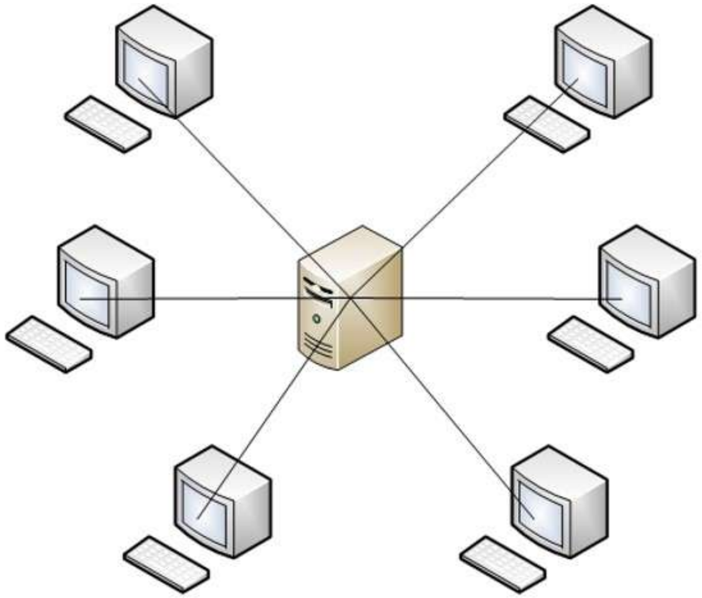
Introductory Concepts on CII

Critical Infrastructures (CII): those systems, belonging to the Information and Communication Technology (ICT), which are critical not just for their own sakes but for other CI that may rely on them (Theron, 2013)

Examples of CII (Patterson and Personick, 2003):

- the public telephone network
- the Internet
- terrestrial and satellite wireless networks

Physical or **logical** attacks may affect a CII



[Image Source: www.webexploits.co.uk]

Introductory Concepts on CII

Emerging issues

1. What are the most critical elements of the system whose disruption would significantly degrade the system's normal functioning?
2. How can such events be prevented or mitigated through a means of resource allocation plans, aimed at solving either protection or recovery issues?
3. Is it possible to build infrastructures which are intrinsically able to resist service breakdown when a disruption occurs?

Optimization models

1. Survivability-Oriented Interdiction Models
2. Resource Allocation Strategy Models
3. Survivable Design Models

(1, 2) → **Pre-existing Systems**

(3) → **New Systems**

Survivability-Oriented Interdiction Models

Aim of Interdiction Models

To identify the most critical network components, the ones whose disruption would inflict the most serious damage to the system

Impact metrics of Interdiction Models for CII

- Network reliability
- **Network survivability** (Murray, 2013)
  - **Physical survivability** (e.g., **maximal flow** (Wollmer, 1964), shortest path (Corley and David, 1982), connectivity (Soni et al., 1999; Lin et al., 2011), system flow (Myung and Kim, 2004; Murray et al., 2007))
  - Logical survivability

Survivability-Oriented Interdiction Models

CRITIS 2016

Survivability Interdiction Model (SIM)
(Myung and Kim, 2004; Murray et al., 2007)

$$max\ z = \sum_{o \in \Omega} \sum_{d \in \Delta} f_{od} X_{od}$$

Total Disrupted Flow Maximization

s.t.

$$\sum_{h \in \phi_p} S_h \geq X_{od} \quad \forall\, o \in \Omega, d \in \Delta, p \in N_{od}$$

Flow Disruption

$$\sum_{h \in H} S_h = r$$

Exactly *r* Arcs are Disrupted

$$S_h \in \{0,1\} \quad \forall\, h \in H$$

$$X_{od} \in \{0,1\} \quad \forall\, o \in \Omega, d \in \Delta$$

Binary Variables

Survivability-Oriented Interdiction Models

Insights on the SIM

- *Fixed Number of Components to be Disrupted (r)*
  - Difficult to choose a suitable r value in practice → models run for several values of r across different disruption scenarios

- *Natural Disasters VS Malicious Attacks*
  - Natural Disasters: Cardinality Constraint ("Exactly r Arcs are disrupted"), as in the SIM
  - **Malicious attacks**:
    - Resource Constraint (e.g., human, financial) in place of the Cardinality Constraint in the SIM
    - Optimization models to minimize the attacker's expenditure to achieve a given level of disruption (Lin et al., 2011) → Resource Allocation Strategy Models

- *Uncertainty of an attack outcome*
  - Interdiction successful with a given probability (Church and Scaparra, 2007)
  - Interdiction probability of success dependent upon disruption magnitude (Losada et al., 2012)
  - **Similar extensions for SIM to assess the survivability of physical networks to attacks with uncertain outcomes**

Resource Allocation Strategy Models

CRITIS 2016

Aim of Resource Allocation Strategy Models

To optimize the allocation of resources (i.e., budget) in order to deal with either **protection** or **recovery** issues

CII Protection (Viduto et al., 2012)

- Technical protection (e.g., security administration)
- Management protection (e.g., technical training)
- **Operational protection** (e.g., **physical security**)

Service Recovery builds on **System Survivability**

Resource Allocation Strategy Models

CRITIS 2016

Survivability Protection Problem (SPP)

$min\, H(z)$ — Highest Flow Loss Minimization

$s.t.$

$\sum_{h\in H} c_h Z_h \leq B$ — Budgetary Resources

$Z_h \in \{0,1\} \quad \forall\, h \in H$ — Binary Variables

$H(z) = max \sum_{o\in\Omega} \sum_{d\in\Delta} f_{od} X_{od}$ — Highest Flow Loss

$s.t.$

SIM Constraints:

$\sum_{h\in\phi_p} S_h \geq X_{od} \quad \forall\, o \in \Omega, d \in \Delta, p \in N_{od}$

$\sum_{h\in H} S_h = r$

$S_h \in \{0,1\} \quad \forall\, h \in H$

$X_{od} \in \{0,1\} \quad \forall\, o \in \Omega, d \in \Delta$

$S_h \leq 1 - Z_h \quad \forall\, h \in H$ — Component's Protection

Resource Allocation Strategy Models

CRITIS 2016

Networked Infrastructure Restoration Model (NIRM)
(Matisziw et al., 2010)

$$max \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{p\in N_{od}}\sum_{t\in T}\beta_t f_{od} Y_{pt}$$

System Flow Maximization

$$min \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{t\in T} C_{odt} W_{odt} + \sum_{o\in\Omega}\sum_{d\in\Delta}\sum_{p\in N_{od}}\sum_{t\in T} c_{pt} Y_{pt}$$

System Cost Minimization

s.t.

Budgetary Resources:

$\sum_{i\in\Gamma^n} \lambda_i V_{it}^n \leq H_t^n \quad \forall t \in T$

$\sum_{j\in\Gamma^l} \lambda_j V_{jt}^l \leq H_t^l \quad \forall t \in T$

Component's Repair:

$\sum_{t\in T} V_{it}^n \leq 1 \quad \forall i \in \Gamma^n$

$\sum_{t\in T} V_{jt}^l \leq 1 \quad \forall j \in \Gamma^l$

Path Availability:

$Y_{pt} - \sum_{\hat{t}\leq t} V_{i\hat{t}}^n \leq 0 \quad \forall p \in P, i \in \Phi_p^n, t \in T$

$Y_{pt} - \sum_{\hat{t}\leq t} V_{j\hat{t}}^l \leq 0 \quad \forall p \in P, j \in \Phi_p^l, t \in T$

Connectivity:

$\sum_{p\in N_{od}} Y_{pt} + W_{odt} = 1 \quad \forall o \in \Omega, d \in \Delta, t \in T$

Binary Variables:

$Y_{pt} \in \{0,1\} \quad \forall p \in P, t \in T$

$V_{it}^n \in \{0,1\} \quad \forall i \in \Gamma^n, t \in T$

$V_{jt}^l \in \{0,1\} \quad \forall j \in \Gamma^l, t \in T$

$W_{odt} = \{0,1\} \quad \forall o \in \Omega, d \in \Delta, t \in T$

Resource Allocation Strategy Models

Insights on Resource Allocation Strategy Models

- *CII Physical Components' Protection*
  - Protection investments over time (Starita and Scaparra, 2016, as an example within the transportation infrastructure context)
  - Element protection may reduce its probability of failure
  - Other issues:
    - Uncertainty in the number of simultaneous components' losses (Liberatore et al., 2011)
    - Correlation among components failures (Liberatore et al., 2012)

- *CII Service Restoration*
  - Component repair duration along with repair activities scheduling (Nurre et al., 2012)
  - Multiple interdependent infrastructure systems (e.g., power, telecommunication, water) restoration (Sharkey et al., 2015)
  - Relevance of information sharing and coordination among infrastructures (Sharkey et al., 2015)

Survivable Design Models

Aim of Design Models

To plan the design of a brand new system in order to meet some specific criteria

Features of Design Models for CII

- Connectivity requirements
- Path-length restrictions (Orlowski and Wessäly, 2006)
- Cost Minimization (Orlowski and Wessäly, 2005)
- Dedicated settings

Future Research Suggestions

To extend the current optimization models

- physical and logical survivability issues to be tackled together

To address the probabilistic behaviour of CII under disruptions

- uncertain parameters (e.g., arc/node availability, repair time)
- scenario-based modelling

To combine together the current optimization models

- protection and restoration
- design and restoration (Orlowski and Wessäly, 2005)

To develop cutting-edge solution methodologies

To incorporate interdependence among multiple CI

Conclusions

This contribution investigated three main research areas in CII Protection:

- Survivability-Oriented Interdiction Models
- Resource Allocation Strategy Models (aimed at either Protection or Recovery issues)
- Survivable Design Models

More work is needed in the CIIP field because CII are large-scale, heterogeneous, distributed systems whose complexity is continuously evolving in a risky environment

Further research directions have been identified and discussed