

Robust Operations Research II: Production Networks

by **Yvo Desmedt**

University College London, UK



This presentation is based on joint works with:

- Yongge Wang (University of North Carolina, Charlotte)
- Mike Burmester (Florida State University)



How to approach?

Approach:

- In our model terrorist can destroy parts of our infrastructure (micro or macro) without specifying how.



- Using an AI model
- The economics of the enemy
- Discussion and extensions

Using an AI model

Problems with the communication model:

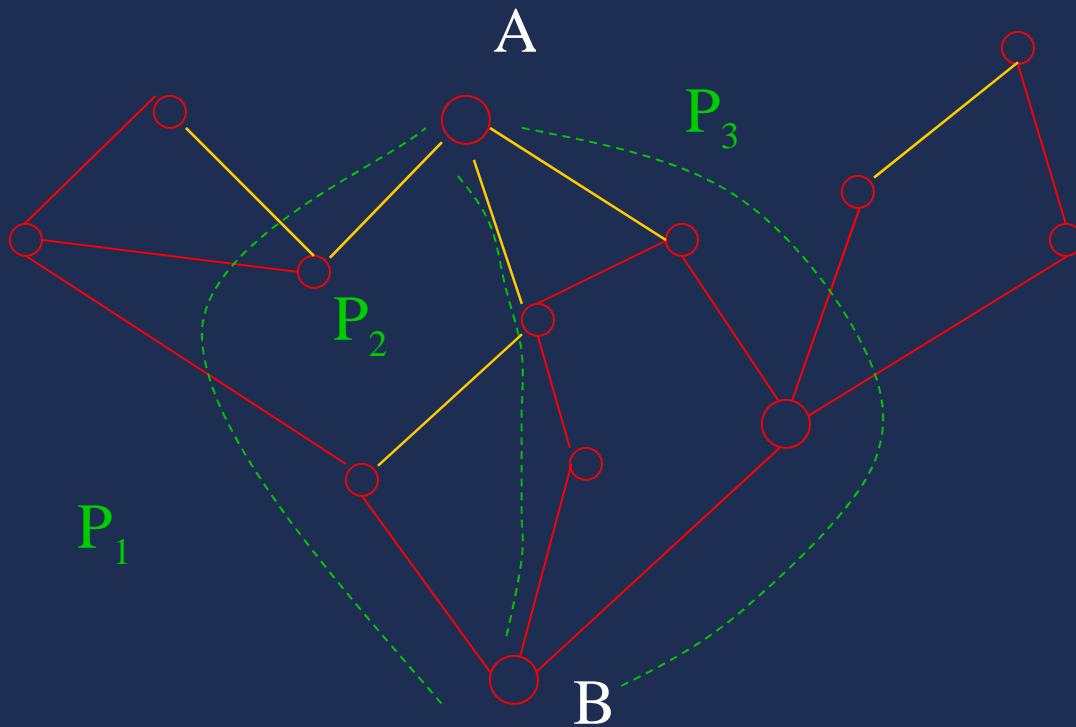
network model:

too homogeneous: computers do not play
similar roles: good only for
theoretical results



Using an AI model

Network graph: reliable
communication



information : can go
via P₁ or P₂ or P₃



Using an AI model

Problems with the communication model:

network model:

certain distributed computation (e.g. transactions require that all sub-transactions have taken place: well known in mechanical world.

Mechanical world uses PERT graph



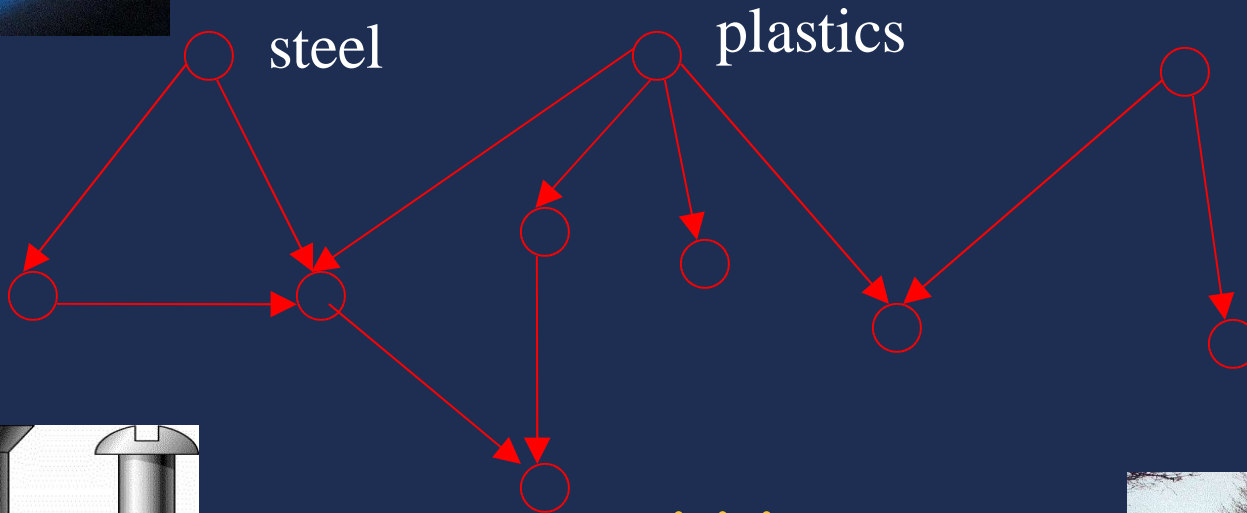
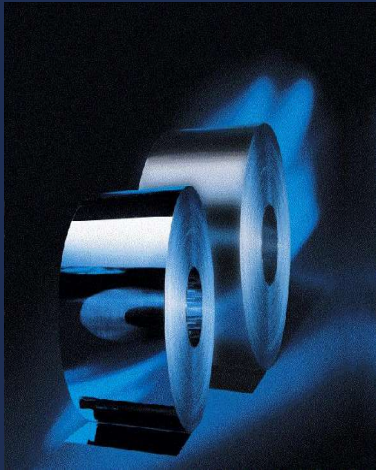
Using an AI model

PERT graph (Program Evaluation and Review Technique): Directed acyclic graph

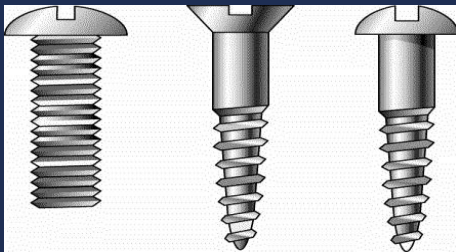
for car/truck manufacturing system



Using an AI model



screw



March 8, 2006

© Yvo Desmedt

David E. Miller Collection

Using an AI model

Impact goes beyond computers. So we need to have a model that integrates mechanical and computer world.



Using an AI model

AND/OR graphs as a model for distributed computation

- AND/OR graphs: acyclic directed graph: vertices labeled: AND or OR
- AND:
 - PERT aspect, i.e. multiple inputs
- OR:
 - network aspect
 - redundancy
- allow to integrate computer and mechanical aspects



Using an AI model

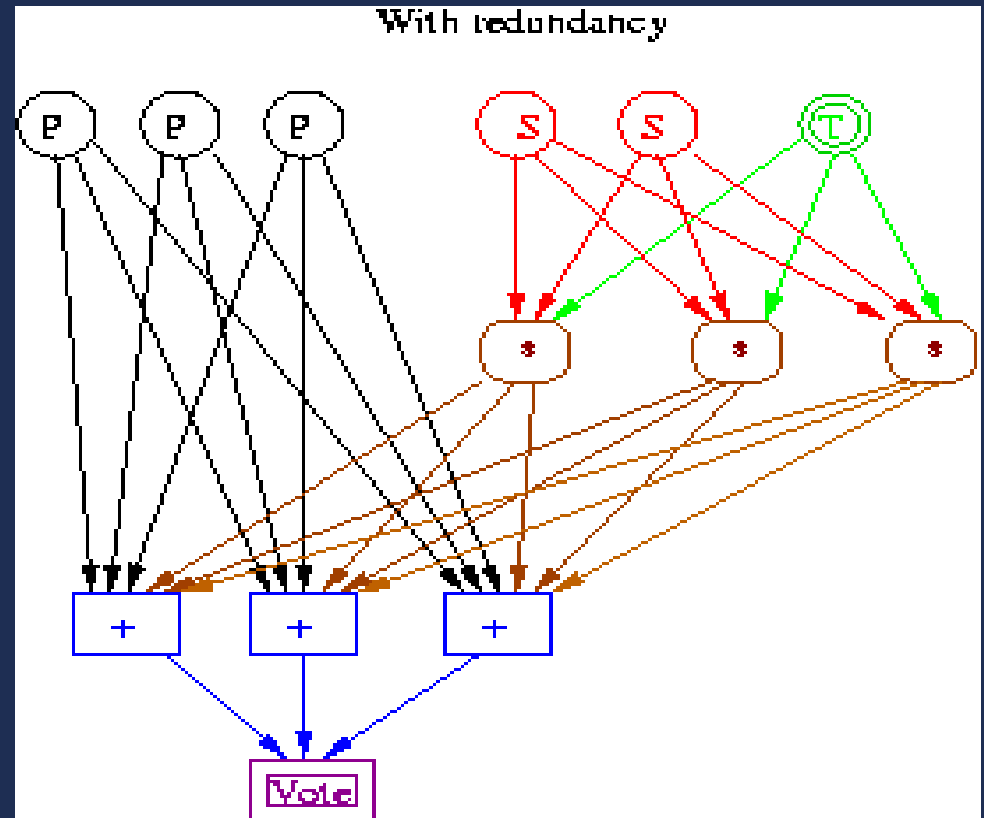
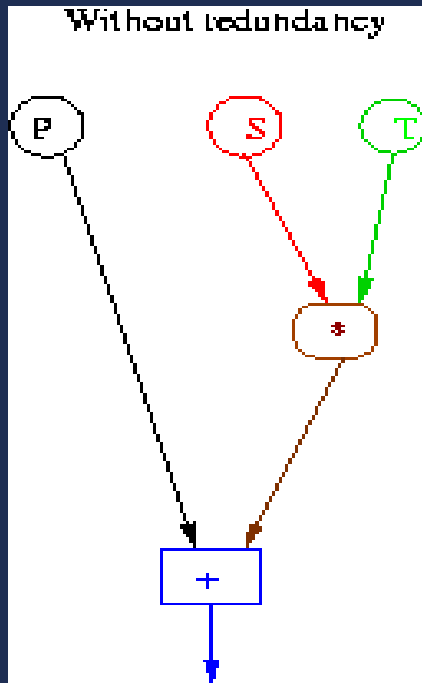
Secure distributed computation needs a different model

The airplane's next position $P' = P + S \cdot T + 1/2 a \cdot T^2$

· P : current position

· S : speed

a : acceleration, here $a = 0$



Wang-Desmedt-Burmester use an AI concept :



a vertex is: a sensor, or a process, or a dedicated computer

AND-vertex

OR-vertex



Using an AI model

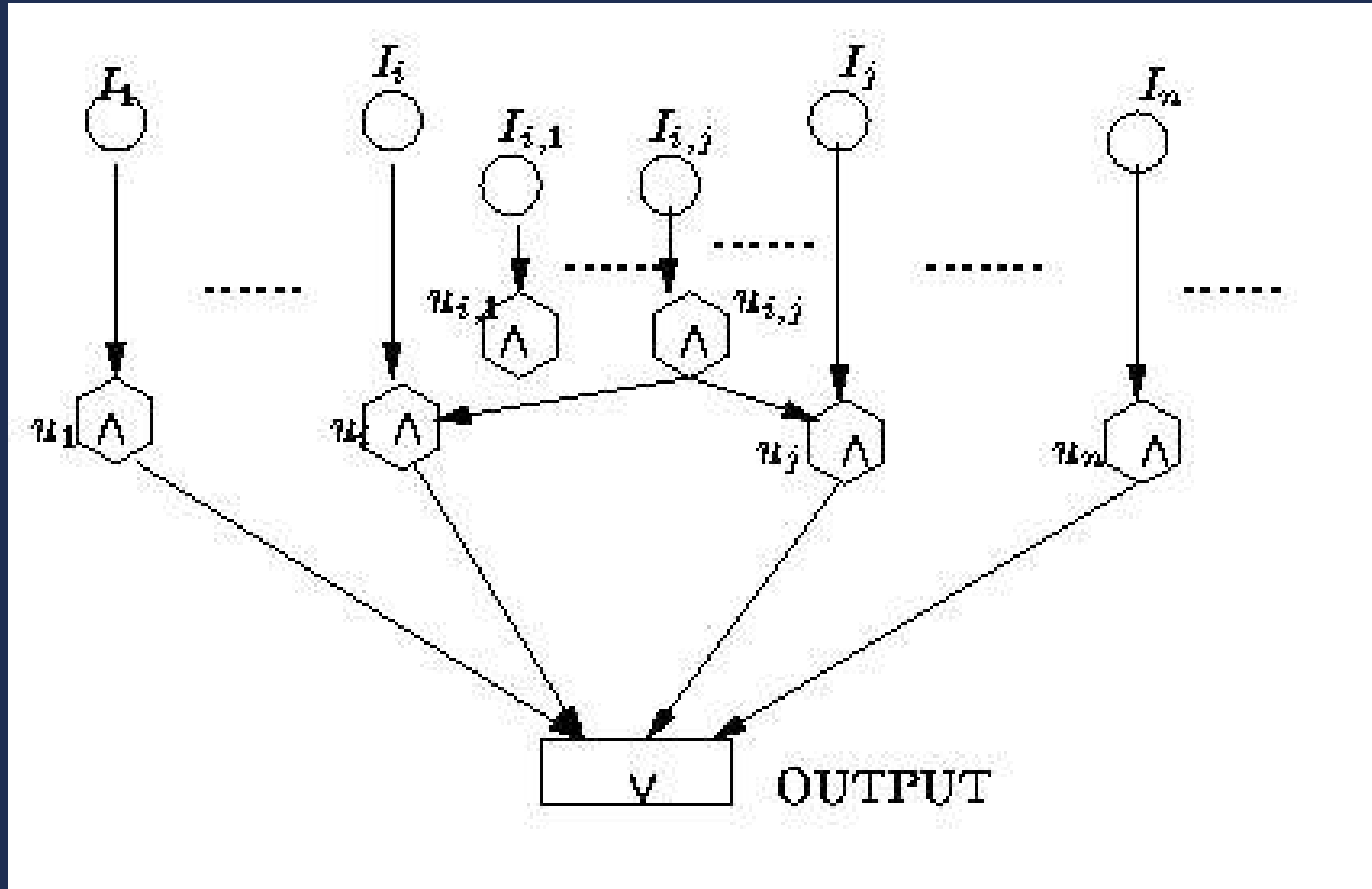
- **Disadvantage of AND/OR graph:**

— Deciding whether a given graph is k -connected is in **P**,

— however equivalent problem in AND/OR graph is **NP**-complete.



Using an AI model



Using an AI model

- Adding impact factor

flow: Preliminary question: Given:

AND/OR graph G ,
capacity function
positive integer z

Question: Is there a flow f (additive) such that the flow at the output is at least z ?

Is already NP-complete for the case $z=1$.



Using an AI model

- Adding impact factor:

flow: critical vertices:

— Set U , $|U| < k$: removed from graph (no input/output vertices)

— for all U' , $|U'| < k$:

maximal flow $_U \leq$ maximal flow $_{U'}$

Given: AND/OR graph G , capacity function, set U

Question: Is U critical?

Is **NP-hard**, and L is not in NP and not in co-NP (if P is different from NP).

Using an AI model

- **Adding impact factor:**

flow: below critical flow:

Given: AND/OR graph G , capacity function, integers k and p .

Question: Does there exist a vertex set U such that:

$$|U| < k$$

$$\text{maximal flow}_U < p$$

Is **NP-hard**, and L is not in NP and not in co-NP (if P is different from NP).



The economics of the enemy

Introduction:

- Seems hard to model since different opponents have different goals:

war: undermine economy, military output

terrorist: visible targets or targets with large impact

hacker: e.g. show that a system is insecure



The economics of the enemy

Introduction:

- Assume the enemy has a budget B_E : **not necessarily expressed in \$.**
- Optimization of the attack: may be, may be not



The economics of the enemy

Feasible attacks?

- Analysis of the threshold Byzantine model

Breaking into:

any k machines: feasible

any $k+1$ machines: infeasible

First economic model:

- uniform (same price to attack any machine), implies that the cost is linear.



The economics of the enemy

- Problems of the linear aspect:

too linear:

- cost to break into k computers is not $k * \text{cost to break into one}$, due to:

automated attacks

availability of attack on WWW

same platform, ...

not homogeneous:

- some computers are better protected than others



The economics of the enemy

- A first alternative:

To each subset S of the nodes we assign

$$c_{S,E}$$

as the cost of the enemy E to break into all nodes in S .

Still Byzantine iff:

- for each subset S of at most k nodes:

$$c_{S,E} \leq B_E$$

- for each subset S of $k+1$ nodes or more:

$$c_{S,E} > B_E$$

call this the Byzantine cost assumption.

The economics of the enemy

- A more realistic model:

Enemy can attack nodes and links

S: a subset of these

To each subset corresponds a cost:

$$c_{S,E}$$

Enemy can attack iff $c_{S,E} \leq B_E$

This defines an **adversary structure** of the enemy: Γ .



The economics of the enemy

- Difficulties:

 - Too many subsets!

 - How to estimate the costs?

- Possible solution:

 - cost of attacking $m+1$ machines using the same operating system (platform)

=

 - cost of attacking m machines using the same operating system (platform).

- Stability?



The economics of the enemy

Introduction

Feasible attacks?

Optimizing the attack

The enemy can attack any subset of computers/links in Gamma.

Good viewpoint for hacker, not for terrorists and information warfare.



The economics of the enemy

Optimizing the attack

– for an application “a” several computers/links T_a are involved.

Natural to talk about a flow f_{T_a} .

– Maximum flow: capacity: C_{T_a}

– attacking different flow units has a different impact. So we have an

impact factor I_a .

The economics of the enemy

Optimizing the attack

Total impact of the application:

$f_{T_a} * I_a$. This gives:

- a weighted total flow F (warning not necessarily linear), and
- a weighted total capacity C .



The economics of the enemy

Optimizing the attack

BIG QUESTION: which nodes/links are the most optimal for the enemy to take over?



The economics of the enemy

Optimizing the attack

- When enemy takes over a set S in Γ the weighted total capacity is reduced from C to C_S^-
- Enemy will choose S such that:
 - C_S^- is minimal, or
 - $C_S^- < C_{crit}$ (winning strategy)



The economics of the enemy

– Analysis of the Byzantine case
under:

Byzantine cost assumption

each unit of flow has the same impact

when optimized gives: enemy should
attack k disjoint paths.



The economics of the designer

Given (at least):

- B_D : budget of designer
- C_D : minimum required weighted total capacity
- F_T : maximum tolerable impact flow reduction
- B_E : budget of the enemy
- others: maintenance, user friendliness, etc.



The economics of the designer

Question: design a graph G of computers:

- $\text{cost}(G) \leq B_D$
- total impact capacity $\geq C_D$
- the enemy cannot win

If possible: designer won, else the enemy will.



The economics of the designer

Note:

- This is very general!
- We need a relation between the cost of setting up computer and the cost to attack, etc.



Discussion and extensions

Byzantine model had its time

Our models can be improved by
including:

control theory aspects, such as:

- time parameters, e.g.:

 - between attack and detection of attack

 - time to recover from an attack

 - time of no return



Discussion and extensions

- time survivability condition:
(time to repair the system) +
(time to detect an attack)
<
(the time of no return) +
(the time the stock will last)



Discussion and extensions

Impact

Byzantine model implies expensive redundant hardware. However, if the cost to attack a node is prohibitive: no redundancy is needed.

