Are we on the right track to achieve survivable computer networks

by Yvo Desmedt and Mike Burmester

Florida State University, USA

and Yongge Wang

Karthika Technologies Inc., Canada

© Yvo Desmedt

The research as well as the text predate the September 11, 2001 terrorist attack.

- Introduction
- The economics of the enemy
- Communication versus computation
- The economics of the designer
- Conclusions

Introduction

- **Why models?**
  - describe world mathematically
  - abstract away details
  - allows us to focus
- **Why do models get outdated?**
  - world changes
  - details are no longer details
  - may have focused on wrong aspects

© Yvo Desmedt

Introduction

- **Why we must update: otherwise:**
  - heuristics only may lead to incorrect results, waste of resources, dangerous, ...

© Yvo Desmedt

Introduction

- **Survivable computer aspects:**
  - 1970-1980: secure computers possible.
    - Problems: e.g.: computer viruses, sloppy designed software, inexpensive and large OS.
    - Solution: distributed computers
    - Model: Byzantine: homogeneous

© Yvo Desmedt

Introduction

- **Survivable computer aspects:**
  - Critical Infrastructure: certain computers are more critical a priori. This is not the case in Byzantine model.
  - Isolated WWW server: distributed aspect not explained by Byzantine model: our model will.

© Yvo Desmedt

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

© Yvo Desmedt

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

© Yvo Desmedt

The economics of the enemy

- **What can the enemy attack?**
  - Analysis of the 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.

© Yvo Desmedt

The economics of the enemy

- Problems of the linear aspect:
  - too linear:
    - cost to break into k computers is not k * 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

© Yvo Desmedt

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:

$$c_{S,E} =< B_E$$

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

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

call this the Byzantine cost assumption.

© Yvo Desmedt

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 $c_{S,E} =< B_E$
  - This defines an access structure of the enemy: Gamma.

© Yvo Desmedt

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?

© Yvo Desmedt

The economics of the enemy

- **Introduction**
- **What can the enemy attack?**
- **Optimizing the attack**

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

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

© Yvo Desmedt

The economics of the enemy

- **Optimizing the attack**

  There are:

  - units of applications and several computers are involved. Natural to talk about a flow.
  - attacking different flow units has a different impact. So we have an impact factor.

© Yvo Desmedt

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.

© Yvo Desmedt

The economics of the enemy

- More realistic: total impact of the reduction in flow (f_s) > critical value.

  Impact: does not to be linear.

© Yvo Desmedt

The economics of the enemy

- Different goals: if given the budget of the enemy the total impact of the reduction in flow is for all possible strategies (for all possible subsets in Gamma) < critical value, then the enemy lost (will loose).

  So then the enemy can only maximize the impact.

© Yvo Desmedt

Communication versus computation

- **Problems with the communication model:**

  network model:

  - too homogeneous: computers do not play similar roles: good only for theoretical results
  - certain distributed computation (e.g. transactions require that all sub-transactions have taken place: well known in mechanical world.

© Yvo Desmedt

Communication versus computation

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

© Yvo Desmedt

Communication versus computation

- **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

© Yvo Desmedt

Secure distributed computation needs a different model

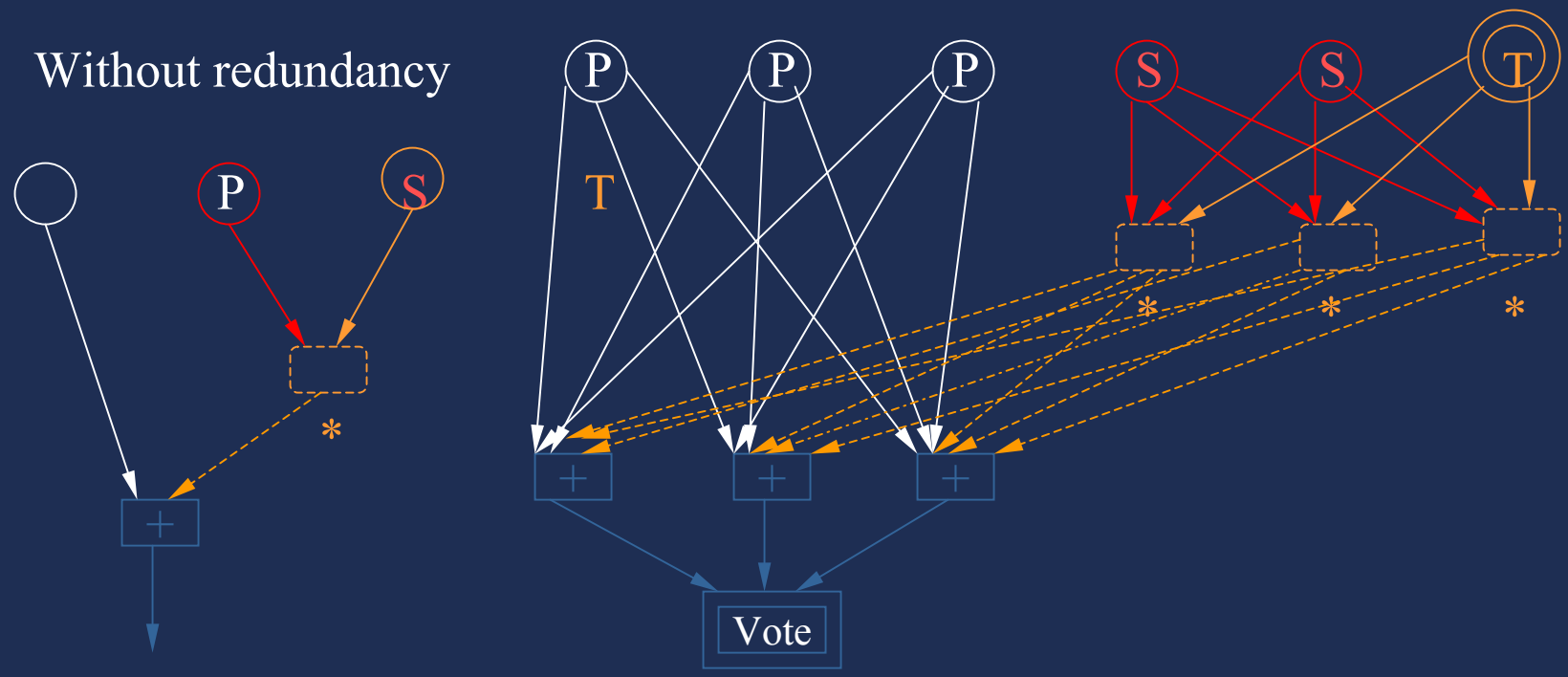
The airplane's next position $s = s_0 + v \times t + 1/2\, a \times t^2$

- $s0$: current position
- v : speed

a : acceleration, here $a = 0$

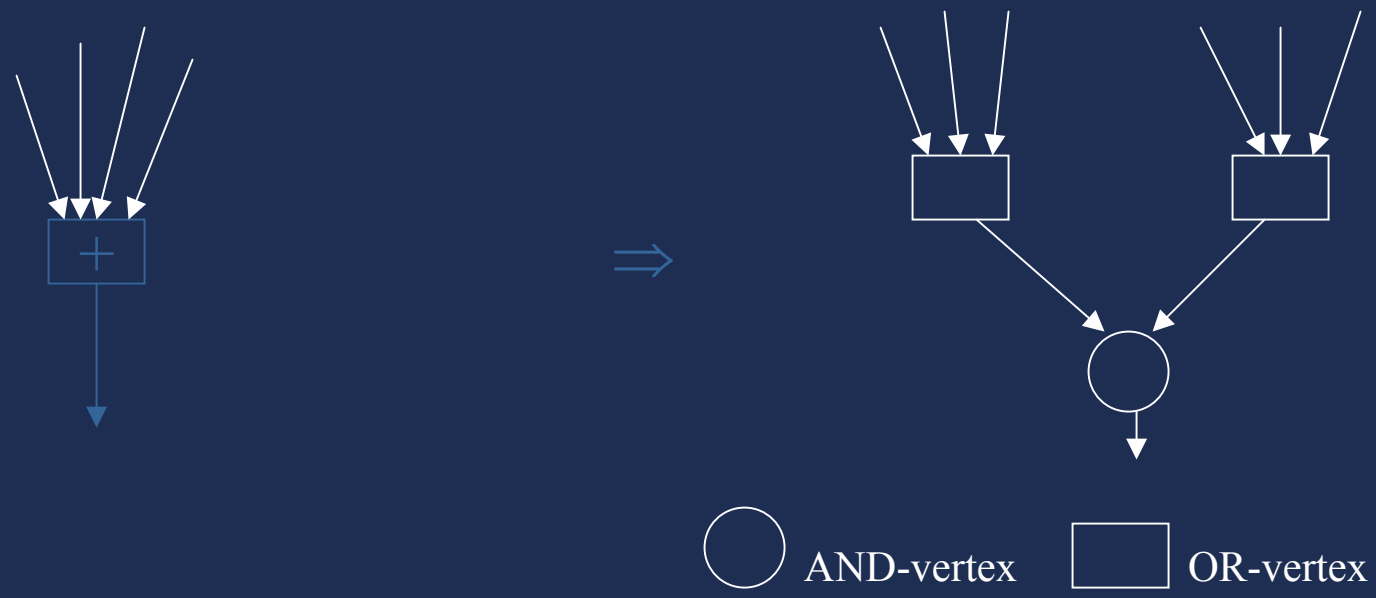
with redundancy

Without redundancy



P The airplane's position sensor; S The airplane's speed sensor; T The time interval (input);

Wang-Desmedt-Burmester use an AI concept :



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

The economics of the designer

Given (at least):

- B_D: budget of designer
- C_D: minimum required total capacity (expressed as a total impact factor)
- F_T: maximum tolerable impact flow reduction
- B_E: budget of the enemy
- others: maintenance, user friendliness, etc.

© Yvo Desmedt

The economics of the designer

Question: design a graph G of computers:

- cost(G) =< B_D
- total impact flow >= C_D
- the enemy cannot win: for all S:
  - $c_{S,E} > B_E$ or
  - $f_S =< F_T$

If possible: designer won, else the enemy will.

© Yvo Desmedt

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.

© Yvo Desmedt

Conclusions

- **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

© Yvo Desmedt

Conclusions

- time survivability condition:

(time to repair the system) +

(time to detect an attack)

<

(the time of no return) +

(the time the stock will last)

© Yvo Desmedt

Conclusions

- **Impact**

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

© Yvo Desmedt

Conclusions

- **Call for interdisciplinary effort:**
  - Byzantine model is too linear and too unrealistic
  - heuristics to design systems do not follow Byzantine model
  - in physics billions of dollars have been spent to make good models
  - alternative models are worth studying

© Yvo Desmedt

Conclusions

- **Call for interdisciplinary effort:**

  economists, control engineers, information security engineers, war strategists and other experts should join in an effort to better understand how survivable computer networks should be designed.

© Yvo Desmedt