On the safety & security analysis of critical networks: methodological challenges

B. Galván, D. Salazar & G. Winter
Evolutionary Computation and Applications division (CEANI)

University Institute for Computational Engineering (SIANI)
University of Las Palmas de Gran Canaria (ULPGC)
Canary Islands, Spain
bjgalvan@siani.es
Critical Infrastructures (CI) and Key Assets (KA)

• Definition
  • The meaning of CI and KA is still open to debate
    • 1970-90: “adequacy of the nation’s public work”
    • 1990-2002: “homeland security” (terrorism)
    • after 2002: “citizens rights” (cyber-attacks)

• The list of CI and KA
  • Evolves (economic changes, geopolitical influence, security policy,..)
  • Lack of precise descriptions: “Ambiguity increase vulnerability”
  • Includes many items: transportation (airports, roads, ...), energy (power grids, generation facilities, ...), Communications, chemical, nuclear, water, ..., etc.

• Some CI are networks (very sensible to terrorist attacks)
  • Communications (digital networks, ...)
  • Energy (grid power, ...)

Open Innovative Software Horizons Forum  University of Jyväskylä/Agora  March 12, 2010
Efforts related to Critical Infrastructures (CI) and Key Assets (KA)

• Some Initiatives

  • National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (USA)


  • The European Policy on Critical Information Infrastructure Protection (CIIP).

• Some Projects

  • CI2RCO. (http://www.ci2rco.org/9). the European co-ordination project on Critical Information Infrastructure Research Co-ordination

  • PSE PROMARES (MARYAM & SIROCO subprojects). Spanish MICINN.

  • INTERESTED. (www.interested-ip.eu). INTER-operable Embedded Systems Tool chain for Enhanced rapid Design
Critical Information Infrastructure Protection (CIIP): The European Policy

• Scope
  • Enhance Europe’s protection from large scale cyber-attacks
  • Promote security and resilience of CIIs as a first line of defense
  • Enhance preparedness and response capability in EU

• Approach
  • Build on national and private sector initiatives
  • Engage public and private sectors
  • Be multilateral, open and all inclusive

• Pillars
  • Preparedness and prevention
  • Detection and response
  • Mitigation and recovery
  • International cooperation and criteria for CIIP
Annual Work Programme 2010
Prevention, preparedness and consequence management of terrorism and other security related risk

• Budget (20420000 Euros)
  • Action grants (16080000), Public procurement (19000000), Actions with JRC (23400000)

• With regard to prevention and preparedness of risk (terrorism,.. )
  • Stimulating, promoting and supporting risk assessments and the development of methodologies (risk assessment)
  • Others: (promoting and supporting shared operational measures, security standards, exchange of know-how, cooperation,...)

• 2010 (Round II : Call for proposals scheduled for June 2010)

• Action grants: some priorities in 2010 call
  • Development/evaluation/propagation of tools and methods to design public spaces to improve protection against terrorist attacks (including simulation and testing). Improving information management and increasing protection capacity in the transport, energy, communications, chemical, nuclear, water....
Critical Networks examples

• General
  • Energy
  • Transport
  • Water
  • Communications
  • Digital
  • Many others …

• Mission-Critical
  • European Emergency Number Association EENA (112)
  • Federal Emergency Management Agency (USA)
Some problems

- Current analysis based on complexity theory considers only the topology of the network, but its mission and dynamic aspects remain scarcely studied.
- Some analyses require intensive computations, particularly for large and very large networks.
- Some features like “network fragmentation” are easy to calculate but difficult to interpret.
- Some networks are robust against random events but fragile against intentional attacks.

Several objectives and constraints

- Traditional: Availability, Reliability, Maintainability, Cost, Safety….
- New: Survivability, Risk, Security, ….
Critical Networks needs and methodologies

• needs
  • Conduct probabilistic risk assessment (PRA) from critical networks analyses.
  • Tools for evaluating the dynamic aspects of networks.
  • Cooperative R&D support software.

• current methodologies
  • Centrality measures: network diameter, shortest and longest paths, betweenness of links (number of paths containing a link)
  • Degree distributions (distributions of the number of links connecting a node): scale-free networks, random network, small-world networks.
  • Link analysis: determining existing interactions (links) among objects
  • single objective PRA
Critical Networks methodological challenges

• Modeling
  • Network structure is modeled frequently using graphs. **Network dynamics requires additional efforts** (e.g. Cellular Automata and Monte Carlo have been used to model spreading through networks)

• About MOEA in Critical Networks
  • To improve the efficient use of frontiers like “impact delivered” vs. “cost of attacking” (can be used to assess worst case scenarios and to devise robust protections against intentional attacks).
  • **To improve the use of Multicriteria analysis** that can be carried out to determine what nodes or links should be protected to interdict optimally criminal networks.
A Critical Network R&D example

• **How to allocate resources to interdict optimally a criminal network?** (Applications: border control, drug traffic control, etc.)

• Formulate objectives (e.g. minimize max flow, interdiction cost and recovery speed) and solve the multiobjective problem.

• You can use the same type of analysis to allocate robust protections (those that minimize the maximal impact) or to identify exploitable weaknesses in your network.

A R&D integration software platform for Mission-Critical Networks: Platea 4D (P4)

• Platea 4D is a R&D initiative to develop a platform for software integration in order to support cooperative R&D activities among several partners for large scale projects.

• **Platea 4D characteristics:** Platea4D Console (user application) compatible with Windows Vista or Windows 7 with .NET Framework 3.5. Requires 3D graphics card with OpenGL 2.1 support. Platea4D Services compatible with Windows Server 2008, Windows Vista or Windows 7. Real-time 2D & 3D Interactive graphical visualization. Supports multiple viewers. *(See Annex for a complete description)*

• Platea 4D is used in two Mission-Critical networks:
  
  • Real Time Risk Assessment (ships traffic control and emergency management in Canary Islands)
  
  • 112 emergencies control centers at Canary Islands (Forrest Fires and Adverse Meteorological Phenomena)

• **Platea 4D gives support to a R&D project:**
  
  • A “transport-related” project between our two Universities (ULP GC, ULL).

• **Platea 4D was selected to give support for two large projects in Spain (2010-2013)** (Multiphysics, Wind/current fields, Oil Spill simulation, Risk, Decision Making)
Platea4D Service Bus: A company solution example
Platea 4D results example (oil spill simulation) models executed (wind, currents, oil spill transport, oil spill chemical evolution)

The results of different chains of models (wind-currents-oil spill) can be showed under user demand (2D)(3D coming soon)(time control available on screen)
Platea 4D graphic capabilities example

Results of two coupled wind field models (regional – local)
Platea 4D stations on duty
Platea 4D is available for R&D projects support

• Platea 4D is useful for many types of projects (not only for Critical Networks)

• Platea 4D is not Open Source but is free for all the project partners if:
  • Platea 4D is used only for R&D and demonstration purposes.
  • CEANI is a project partner or external contractor (in charge, at least, of Platea 4D core services for the project).
  • At least one new feature of Platea 4D is developed under the project.
  • At least one new feature of Platea 4D developed under the project will be free. (can be included in the Platea 4D features for any other coming or previous projects). “The Platea 4D community get benefits from each new project supported”
  • The partners can not do business with the Platea 4D core without CEANI commercial license agreement.

• Under this conditions every project partner will receive the Platea 4D heritage (at the present time 1.2 Meuros invested in developing Platea 4D features)
Critical Networks Innovative software Horizons

Conclusions

- There is an increasing interest in safety and security
- Specific “calls for proposals” at European level for R&D projects
- Due to the large scale of the problems to solve (many variables, many objectives). The current methods might be inefficient. **Parallelization? New MOEAs?**
- To move from the current solution to an optimal solution frequently is not possible in only one step. **Efficient constraints management methods? new strategies?**
- Normally the whole Pareto Front is not needed. **Methods to converge to specific regions of the front?**
- Billions of dangerous scenarios are possible (only a few of them will be a priori computed). **How to assess risk for large/complex problems?**
- There are many sources of Uncertainty. **In deep analysis of Uncertainty management in Simulation and Optimization (MOEA)?**
- The Pareto Front before one event (attack) will be different from the one after that. **How to model and solve dynamic scenarios? game theory? MOEAs?**
- Software platforms (**Integration**) for cooperative R&D projects are needed
On the safety & security analysis of critical networks: methodological challenges

Thank you very much

B. Galván, D. Salazar & G. Winter
Evolutionary Computation and Applications division (CEANI)
University Institute for Computational Engineering (SIANI)
University of Las Palmas de Gran Canaria (ULPGC)
Canary Islands, Spain
bjgalvan@siani.es
Platea 4D Technical features and requirements

• Platea4D Console (user application) compatible with Windows Vista or Windows 7 with .NET Framework 3.5. Requires 3D graphics card with OpenGL 2.1 support.
• Platea4D Console designed for enhanced user experience. Touch systems friendly.
• Realtime 2D Interactive graphical visualization. Supports multiple viewers.
• (on progress) Realtime 3D interactive graphical visualization.
• Fully customizable workspaces and environment.
• Platea4D client application can work either standalone or as part of a distributed system of services and workstations (Service Bus).
• Follows Service Oriented Architecture (SOA) tenets.
• Distributed Transactional communications and concurrency management.
• Spatial data types based on OpenGIS specifications. Raster and Vector data supported.
• Databases on SQL Server 2008. Geospatial data uses Spatial SQL Server data types.
• Access control security based on users and roles. Allows fine grain control.
• Allows Load Balancing on multiple data services.
• Centralized administration service. Only centralized administration database optional.
• Time variable 3D spatial data management (includes height component). Any data element can have either spatial or temporal properties without limiting the use of data lacking these components.
• Flexible and modular design customizable for concrete uses with the addition of new modules that extend the systems features. Platea4D allows either new data modules or new processes modules for analysis, exploitation, evaluation …
Annex

Platea 4D Technical features and requirements

• Declarative data definition (XML) as main tool to define domain specific schemes and data descriptions. Hierarchical and category based data structures allowed.
• Supports relations of grouping, membership, ownership, category, type, composition and aggregation for allowing complex domain shapes and behaviors. Supports object oriented features for data definition and exploitation: abstraction, multiple inheritance and encapsulation. Also polymorphism.
• A property type supports all common primitive types (integer, float, double, boolean …) and also complex types (classes).
• Discrete data temporal interpolation supported.
• Processes modules can either be executed on frontend application or hosted on services.
• Both data and process services can be easily extended to allow complex system integration like exploitation of cluster or cloud computing resources.
• Software Development Kit (SDK) for the development of new processes and add-ons. Dependent processes of a concrete application domain are packed into process modules. Developer of a module focuses on domain logic; the platform is responsible for persistence, internal data representation and storage, communications, graphical representation, user interaction and error management. Available multiple extensions mechanisms for customization of workstation’s application (Platea4D Console, client application).
• SDK design guidelines are primarily ease of use for non programming experts and encapsulation of complex processes like concurrency management or data consistency preservation.
• Native support for metric units and conversion. Incorporates International System of Units. Extensible capacity for new units and conversions.