Simulation of Critical ICT Infrastructure for Municipal Crisis Management

Adam Kozakiewicz, adam.kozakiewicz@nask.pl
Anna Felkner, Tomasz Jordan Kruk

Crisis management benefits tremendously from simulation, especially during the planning and testing. At the same time an often overlooked aspect of crisis management is the key role of telecommunication. The following description presents the work done at NASK with the goal of implementing a simulator of the consequences of threats to the ICT (Information and Communication Technology) infrastructure, as a part of a large simulation environment for crisis management in a large urban area (specifically the Warsaw agglomeration).

Project background

Simulation is a very useful tool for crisis management. It can be used in the planning phase, to make sure that the proposed actions will be effective. In the training phase it can help verify the ability of decision makers to control disaster response. Finally, during an actual crisis, a simulator acts as a visualization tool for the observed threats, a prediction mechanism suggesting probable development of the crisis and a testing environment enabling comparison of different strategies.

In response to this need, a consortium of Polish research institutes was formed to research the crisis management problems, including preparation of a multi-aspect simulation environment for the Warsaw agglomeration. The simulation should include all kinds of threats: fires, floods, chemical or nuclear pollution, terrorism, military threats, etc. Institutes from respective fields were invited and work started as a research grant from the Ministry of Science and Higher Education "Models of threats to agglomeration and crisis management system – case study for the Capital City of Warsaw", coordinated by the Military University of Technology in Warsaw.

NASK, together with the National Institute of Telecommunications, was tasked with researching the often overlooked problem of critical ICT (Information and Communication Infrastructure) infrastructure.

One of the tasks handled by NASK was to prepare a concept of a simulator of the consequences of threats to the ICT infrastructure. This work has been completed and will be followed by the implementation of this simulator. Observations forming the basis for the project were made in Warsaw, but the same comments hold more or less true for many cities. The goal of the project was to build adaptable tools, which could be used in any city after minor changes and of course with new data.

Problem description

The main task of the simulation is to identify the consequences of damage to ICT infrastructure by different threats. The cause of damages only affects the probability of failures, but the state of system elements is basically binary. Internal threats, like viruses, worms, software misuse, etc. are also simulated, but are omitted here due to space constraints.

The ICT infrastructure of an agglomeration consists of cables, network nodes (routers, switches), wireless antennae, computers, etc., as well as information systems actually provided by the computers.Information is prioritized by means of a "criticality factor", which enables us to differentiate critical systems and links from those, whose functioning during a crisis is only preferred, and the rest.

The following elements must be incorporated in the design of a threat consequences simulator for ICT infrastructure:

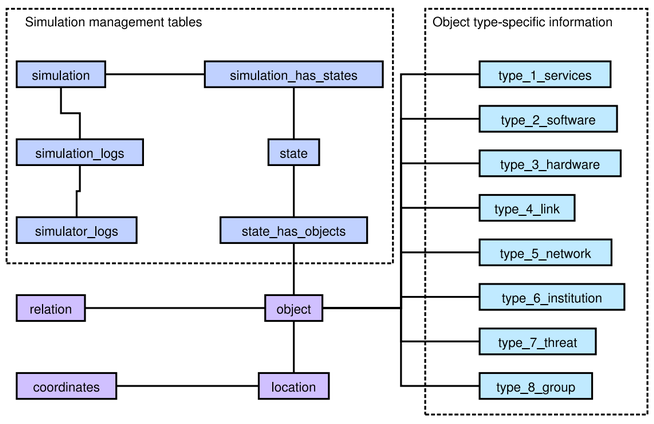
- a database of the city's most important computers, networks and communications equipment, of the important systems and key relationships between elements,
- identification of critical elements of the infrastructure,
- collecting information about external threats,
- computing the effects of these threats on the graph of the network, focusing on the critical elements.

System architecture

The simulator was designed to be used as a part of the multi-threat simulator, communicating with others and using the system's main GUI as its user interface. Due to the specification of the multi-simulator, the interface of the ICT simulator is specified as web services.

User interface of the multi-simulator is based on a digital map of the city. This digital map is also an important source of data for individual simulators. The ICT simulator will hold all the data locally for efficiency reasons, but a large part of that data is supplied by the map software at the start of a new simulation. Some kinds of information may be too task-specific to be stored in the central system, so the design is a hybrid one. The simulator can also function without the digital map module, if all necessary data can be loaded in a different way.

A database for this task has already been designed and, with the use scenarios and algorithms resulting from them, forms the engine of the simulator.

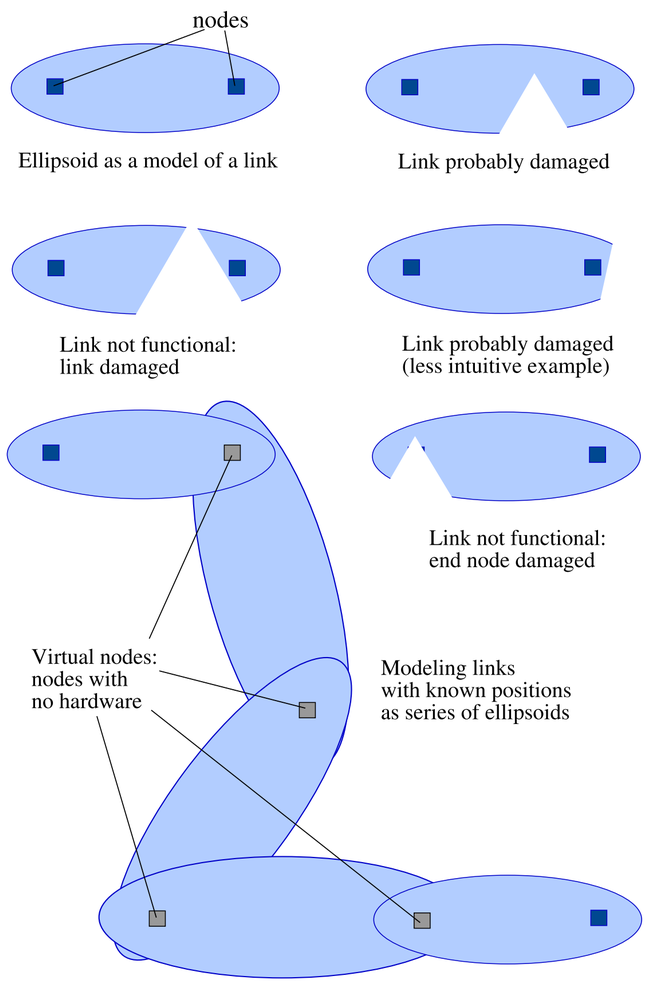


The database stores the following data:

- the network topology,
- positions of nodes and links in the network,
- positions of essential systems, which provide services,
- ranges of wireless communications,
- criticality levels,
- connections between nodes and links, defining the topology of the system,
- software and services – depending on relevance of offered services,
- tunnels – pairs of objects which need to communicate, defined when the connectivity is itself critical, but the route is not,
- dependencies (whether one object is necessary for the functioning of another).

The system is designed to work with low-quality data. The dependencies or location data need not be precise for the simulator to function and give meaningful results.

The hardware and software components are described as generic objects, with type-specific information stored separately. Objects may have defined locations. In case of node hardware (computers, switches, etc.) these are simply coordinates, while each link is defined as an ellipsoid. The precise location of links can in many cases be difficult to obtain. The ellipsoids allow at least estimation of probability of a link being damaged by a disaster near its estimated path. The tables defined for storing locations are also used to hold wireless ranges.



The objects in the database are organized using groups, defining sets of objects which are important as a whole. A special kind of group is used to store the tunnels mentioned above. The defined kinds of groups are as follows:

- If all elements of group are essential in implementation of key assignments, systems can be joined into *complementary groups*. The criticality of elements of the group is at least equal to the criticality of the entire group. If this is not given, the criticality is equal to that of the most critical element.
- Systems, links and nodes, can be joined into *replacement groups*, most often into pairs. The criticality of the group is then equal to the lowest criticality among the elements from that group. This type of groups has an additional property – the maximum switching time.
- A *tunnel group* can be assembled from pairs of resources, which need to have a connection assured. Such a tunnel has it's own criticality, not related to the criticality of the connected objects (in most cases it probably should not be higher than the lowest of those).

All groups are themselves objects and can be members of other groups. The groups are defined by a relation. There are more types of relations: a *topological relation* stores the connections between nodes and links, defining the structure of the network as a graph, a *dependency relation* stores the dependencies between objects and an *inclusion relation* is used to assign members to groups.

Other tables, not explained earlier, are necessary from the simulation point of view and are used to describe the passage of time and to store simulation run-specific information.

Use scenarios

Scenarios which should be accomplished by the simulator were divided into five groups: helper scenarios, simple scenarios, location scenarios, graph and group scenarios, and variant scenarios. These groups are listed in the following sections.

Helper scenarios

Helper scenarios do not perform any simulations. They are used only for preparation to future simulations. This group includes the following scenarios:

- Modify the object/list of objects.
- Connect network devices with a link.
- Modify the system (network devices, software, services and relations between them). Creates new objects and relations between the device, software and services.
- Modify the group.
- Add object(s) to the group.
- Add/remove relation.
- Change the criticality of the object.
- Move the network devices with all bindings.
- Define the new threat area and give it a name to simplify management.
- Change (or delete) the range of named threat.

Simple scenarios

The scenarios in this group do not demand any calculations and are used for data output from the system:

- What is the inherent criticality of the object?
  Scenario is used to show what criticality is assigned to the resource or group directly in its database record.
- Which connections are essential to realize a crisis management procedure?
  Scenario determines a procedure's requirements. A procedure is modeled as a group of systems, tunnels and links, without which the communication and management specified in the official procedure cannot be assured.

Location scenarios

These scenarios check if nodes and systems belong to a static threat area:

- Which critical resources are threatened?
- Which critical resources are available despite the threat?
  Scenario useful if the disaster causes a total collapse of the ICT system, when the list of operational system is actually much shorter than the list of damages. Lists only critical resources or all resources in the database.
- Is the resource/area vulnerable to threat?

Group and graph scenarios

In these scenarios the topology of the network has to be analyzed, which includes finding paths and processing the structure of the network. Note, that the scenarios concerning groups can also be used to ask about groups to which a given resource belongs. The group includes the following scenarios:

- What is the static level of the criticality of the resource/object?
- What is the level of the criticality of a group?
  These two scenarios determine the pessimistic estimation of the resource significance, taking into account its role in groups. In the second scenario the group can be identified either directly, or through a resource – in the latter case all groups to which the resource belongs are checked.
- How critical is the resource/area?
- What is the criticality of elements of the group?
- Which resources are critical at the moment?
- Is the connection between two points/nodes possible?
- Is the realization of given crisis management procedure possible (or realization of another group)?
- Does a given service work?
- What localization does the service have?
- Is the given service available from a certain point?
- Which crisis management procedures are possible/impossible to carry out in the current situation?
- Find a functioning path between two given points.

Variant scenarios

This group of scenarios has to compare the system state in at least two different simulation states. The following scenarios belong to this group:

- What consequences for connectivity would occur if a resource (or list of resources) was repaired/damaged in the context of existing threats?
- What consequences for criticality of resources would occur if a resource (or list of resources) was repaired/damaged in the context of existing threats?
- Which resources should be protected during the changing crisis situation?
- Prioritize the repair/replacement of damaged resources (after the crisis situation).

Further development

The ICT threat consequences simulator is already past the basic design phase. The functional specification for the project is complete. The technical specification is advanced – the architecture, database structure, choice of tools, etc. are completed, the only unfinished element of the specification is the design of some of the algorithms implementing the use scenarios. Until these are ready, the specification of web services is also considered volatile. As soon as this phase is completed, implementation will start.

About NASK

In 1991, NASK connected Poland to the Internet. Since December 1993, NASK has been a research & development organization and a leading Polish data networks operator. We offer state-of-the-art telecommunications and data solutions to business, administration and academic customers.

Comprehensive Solutions The NASK integrated service package comprises broadband Internet access, corporate networks, data transmission, collocation and hosting, videoconference, as well as network security services. Corporate networks of international range are built in cooperation with global operators: INFONET and TeliaSonera.

Scientific Activity NASK carries out scientific and research & development activities in cooperation with the Faculty of Electronics and Information Technology of Warsaw University of Technology. Projects centre on telecommunications & data quality (QoS – Quality of Service) and security of IT systems, with a particular focus on biometric identification methods. NASK is an active member of many international organizations and associations (FIRST, CENTR, TERENA, RIPE) and participate in European Union projects.

NASK's scientific activity is the domain of the Research Division that works on developing mechanisms and algorithms enabling better efficiency and reliability of modern telecommunications networks. Research focuses mainly on quality of service (QoS) assurance, optimized service pricing and enhancing security of both networks and network services. The chief topic is biometric methods in ensuring security of services.

Other NASK teams, for example CERT Polska, the Domain Department, the Legal Department, the Design Department, the Security and Service Integration Department, and the Polska.pl team, also conduct research and develop innovative projects.

The authors are members of the Network and Information Systems Security Methods Team of the Research Division.

CERT Polska A part of the NASK organization, CERT Polska is Polands first Computer Emergency Response Team that cooperates closely with other such teams worldwide.

Internet Domains NASK is the Polish national registry of Internet names in the .pl domain. On the initiative of NASK, the Polish Chamber of Information Technology and Telecommunications has established a court of arbitration that mediates in Internet domain name cases.

Polska.pl and Poland.pl For many years now, NASK has been collecting resources for the Polska.pl portal and its English language version – Poland.pl. The sites provide access to reliable sources of verified information about Poland.