TRONE: Trustworthy and Resilient Operations in a Network Environment

P. Veríssimo (FCUL), F. Araújo (FCT/UC), J. Alegria (PT), P. Narasimhan (CMU), A. Casimiro (FCUL)

The Telecom industry is going through rapid changes leading to what are commonly designated as Next Generation Networks (NGN): different technologies converging into a network tissue able to provide multiple services with on-demand provisioning, in a seamless and technology-independent manner.

The introduction of new technologies and new services, especially at higher levels of abstraction, pushes the infrastructure to new levels of demand, increasing the likelihood of failures, either accidental or malicious. On the other hand, users are each day more demanding in terms of the quality of the service they get: the trend is deviating from sheer performance ("fast") to meeting expectations about how well the service is provided against what was promised ("trustworthy").

This evolution will lead to a new reality of decoupled services and multi-tenant architectures, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Such a reality, if nothing is done in the way networks are deployed and network operations are managed today, will create an inevitable trend to increase operational risk, specially relevant as operators engage in added-value services such as cloud computing, supported by increasingly binding SLAs.

It is our proposition that this challenges the way operators manage and operate their infrastructures today. Competitiveness of a telecom operator is drastically influenced by the way it masters a few key factors: fast service innovation, high quality of service (QoS), quality of protection (QoP), and, finally, high operational efficiency and agility.

In order to achieve these objectives in the near and mid-term future, we emphasize the need for reducing hazards, both proactively, by increasing architecture robustness, and reactively, by improving the means for detection and recovery from anomalous situations like faults and attacks. Amongst the latter we propose that automated or semi-automated reconfiguration and adaptation dynamics should be introduced, in order to preserve stability of network operation against unexpected events (accidents or attacks).

Given the global scenario above, the TRONE project proposes to address a set of well-defined and focused critical problems related to trustworthy network operation, faced today by the commonly designated area of Network Operation, Administration and Management (OAM), whose solutions we believe will have a fast and strong impact in terms of the CMU|Portugal program objectives, and in the international competitiveness of the industrial partner involved.

Under an operators' perspective, we believe that a crucial condition for survivability in the NGN arena, is the capacity of ensuring trustworthy network operation, in a way so as to

provide a seamless and dynamic enforcement of the dependability and security of network services. The more stable the infrastructure is against accidental and malicious faults, the lighter OAM tasks become. This is key to obtain operational efficiency and quality of service and protection guarantees, and we propose to address these through the investigation of innovative ways to apply fault/failure diagnosis, detection and prevention/tolerance techniques, in symbiosis with automatic reconfiguration mechanisms. With this we mean that quality of service and quality of protection are enforced as a first line, but any degradation thereof is detected, measured, and adaptation mechanisms deployed as a last line of defense. Like a spring, such network must be able to accommodate attacks, but it will eventually return to its original rest position mostly by itself.

We can find many symptoms of the problems described above, in the daily operation of telecom operators: the Internet peering infra-structure; the BGP and DNS "public" infrastructure; main DMZ's protecting resident (hosted by operator) customer's systems; managed "secure" communication services for large corporate customers. However, as NGN services tend to flow beyond a single operator's boundaries, supported on polymorphic and multi-tenant networks, those symptoms will be amplified, since the different ownership of the parts of an infrastructure involved in the provision of a service may dramatically increase management and stability problems. This vouches for the realistic nature of the scientific and technical problems we raise.

In order to achieve the intended objectives, the TRONE project will apply the foreseen scientific and technical results to a selected use case supported on the industrial partner's infrastructure reality.