Intelligent Infrastructure Futures

Users and services in intelligent networks

Technology and intelligent systems are of limited value if they bring no value to human users. Intelligent networks can improve communications, enhancing our cultural environment, health, transportation and social life. Through intelligent networks, users could ubiquitously and harmoniously connect to, offer or receive many services, including transport.

Without effective and reliable communications networks, society is unlikely to allow intelligent infrastructure systems to manage many aspects of daily life, including transport activities. Traditionally, communications technology has relied on centralised networks with users connecting to networks to access services. The Internet has begun to break down this centralised model, becoming an immense organism of highly distributed, pervasive, communication intensive services.

Future networks will enable an intelligent dialogue between users and services, adapting to users' needs, based on mutual observation, network and user self-observation, and on-line distributed feedback control which responds to the events being controlled.

Autonomous adaptation

Services will need to autonomously adapt to the human, social and technical environment. They should improve our ability to interact with the world by providing us with any needed information about our surrounding physical environment.

To operate effectively, these services need to 'understand' the physical, human user based and social context. Autonomous 'intelligent' networks would, at an affordable cost, offer television broadcasts, voice or video telephony, messaging, libraries and documentation, live theatre and entertainment, and other services based on content, data and information. When it comes to transport, these networks would also offer intelligent transport systems with just-in-time or need based vehicles for children and the elderly, and intelligent traffic control systems for traffic regulation and control, based on distributed sensing and communications. Ad hoc wireless networks, based on adaptive networking technologies, will co-ordinate flocks of unmanned aerial vehicles for goods transport.

Future services raise major challenges for today's networks, including mismatches between protocol and differences at the service level between networks in terms of operational and behavioural semantics. Intelligent networks will need new kinds of architectures that will connect mostly lightweight user terminals, which may be as simple as personal digital assistants or mobile phones, or as complex as intelligent network routers (INRs). Vehicles will incorporate hundreds of network nodes to manage fuel efficiency, security, passenger monitoring and passenger comfort, as well as inter-vehicle distances and optimal vehicle speeds.

In this scenario, users connect to the intelligent network via INRs, or directly to a 'network cloud'. Network clouds are collections of routers, internally

interconnected by wire or wireless. Users and services do not actually know who and what is inside a network cloud. Clouds may refuse traffic, or control and shape the traffic that wishes to access them, depending on the cloud's own perception of the traffic.

Complex services

Services will be much more complex and may reside on one or more INRs, or they may own one or more INRs for their needs. When some other user or service asks something of a user, the chances are that there will be an automatic answer saying "sorry no; I am just a simple user". On the other hand, services will often carry authentication schemes to recognise whoever makes a request, billing schemes that collect payments, schemes allowing a service to be used simultaneously by many users, and so on, depending on the complexity of the service.

An intelligent network can be seen as an overlay of INRs with advanced features for search, quality of service (QoS), including pricing and billing, that links communities of users and services. The networked environment of the future will include numerous intelligent networks, perhaps with specific networks whose role is to find the best network for a particular user.

Networks could be small, for a single extended family, for example, while others would be very large, such as networks providing multimedia entertainment, or educational content.

New architectures

Effective management of the quality of service (QoS) and routing underpin this vision of a flexible and self-organising communications environment for users and services. Networks will need virtual regulating agencies to control who has access to, and who can supply, which services. The architecture must also handle situations when the goals of individual users and services conflict with the collective goals of the system.

Such a system must be scalable, so that it can grow to include new services and to meet rising demands. Here one solution is to make each INR responsible only for local users and services, much as a local telephone exchange handles local users.

The development of intelligent self-organising networks will also depend upon new ways of dealing with such issues as denial of service (DoS) attacks, already familiar to internet hosts, e-commerce sites and corporate networks, for example. An intelligent network should incorporate an autonomic approach to DoS defence, with the network monitoring itself, detecting attacks, assessing their severity and reacting to prevent an attack. One approach is to use 'smart packets' to search for services, and to offer QoS using on-line dynamic sensing and dynamically adaptive control.

This Research Brief is based on the Research Review written by Professor Erol Gelenbe of the Electrical & Electronic Engineering Department at Imperial College London for the Foresight Project on Intelligent Infrastructure Systems. Series editors Professors Phil Blythe, Glenn Lyons, Will Stewart and John Urry. Editor Michael Kenward.

The full version of this review is at www.foresight.gov.uk