Wireless networks that build themselves

March 7 2008

From traffic lights to mobile phones, small computers are all around us. Enabling these 'embedded systems' to create wireless communications networks automatically will have profound effects in areas from emergency management to healthcare and traffic control.

Networks of mobile sensors and other small electronic devices have huge potential. Applications include emergency management, security, helping vulnerable people to live independently, traffic control, warehouse management, and environmental monitoring.

One scenario investigated by European researchers was a road-tunnel fire. With fixed communications destroyed and the tunnel full of smoke, emergency crews would normally struggle to locate the seat of the blaze and people trapped in the tunnel.

Wireless sensors could cut through the chaos by providing the incident control room with information on visibility, temperatures, and the locations of vehicles and people. Firefighters inside the tunnel could then receive maps and instructions through handheld terminals or helmet-mounted displays.

For this vision to become reality, mobile devices have to be capable of forming self-organising wireless networks spanning a wide variety of communications technologies. Developing software tools to make this possible was the task of the RUNES project.

Intelligent networking

‘Ad-hoc’ mobile networks are very different from the wireless computer networks in homes and offices, explains Dr Lesley Hanna, a consultant and dissemination manager for RUNES. Without a human administrator, an ad-hoc network must assemble itself from any devices that happen to be nearby, and adapt as devices move in and out of wireless range. And where office networks use powerful computers with separate routers, the building blocks of ad-hoc mobile networks are low-power devices that must do their own wireless routing, forwarding signals from other devices that would otherwise be out of radio range.

A typical network could contain tens or even hundreds of these ‘embedded systems’, ranging from handheld computers down to ‘motes’: tiny units each equipped with a sensor, a microcontroller and a radio that can be scattered around an area to be monitored. Other devices could be mounted at fixed points, carried by robots, or worn as ‘smart clothing’ or ‘body area networks’.

Wireless standards are not the issue: most mobile devices use common protocols, such as GSM, Wi-Fi, Bluetooth and ZigBee. The real challenge, suggests Hanna, is to build self-managing networks that work reliably on a large scale, with a variety of operating systems and low-power consumption.

Middleware and more

The EU-funded RUNES (Reconfigurable Ubiquitous Networked Embedded Systems) covered 21 partners in nine countries. Although RUNES was led by Ericsson, it had an academic bias, with twice as many universities as industrial partners, and most of the resulting software is publicly available.

RUNES set out to create middleware: software that bridges the gap

between the operating systems used by the mobile sensor nodes, and high-level applications that make use of data from the sensors. RUNES middleware is modular and flexible, allowing programmers to create applications without having to know much about the detailed working of the network devices supplying the data. This also makes it easy to incorporate new kinds of mobile device, and to re-use applications.

Interoperability was a challenge, partly because embedded systems themselves are so varied. At one end of the spectrum are powerful environments, such as Java, while at the other are simple systems designed for wireless sensors. For devices with small memories, RUNES developed middleware modules that can be uploaded, used to carry out specific tasks, and then overwritten.

Project partners also worked on an operating system and a simulator. Contiki is an open-source operating system designed for networked, embedded systems with small amounts of memory. Simics, a simulator allowing large networks to be tested in ways that are impractical with real hardware, is commercially available from project partner Virtutech.

Taking the plunge

The tunnel fire scenario was valuable in demonstrating what networks of this kind can achieve. Using real sensor nodes, routers, gateways and robots developed during the project, a demonstration setup showed how, for instance, a robot router can manoeuvre itself to cover a gap in the network's wireless coverage.

"A lot of people have been looking at embedded systems networking, but so far there has been a reluctance to take the plunge commercially," says Hanna. "RUNES' open-source model is an excellent way to stimulate progress, and it should generate plenty of consultancy work for the academic partners."

Source: ICT Results