

All pull together!

Wireless technology is having a profound impact on embedded systems. Low cost, low power, easy to implement, large scale wireless sensor networks are enabling innovative applications, as well as significant improvements in existing systems.

Generating the most interest and potential are wireless sensor networks that can assemble and reconfigure themselves. Consider a wireless sensor network that can run without a human administrator that will reconfigure itself automatically if nodes on the network fail. It might comprise tens of thousands of nodes spread over a huge area, yet will operate for years with minimal maintenance. Or consider an ad hoc network that builds or reconfigures itself, as required, from any suitable devices in range or which move into range.

Self assembling wireless sensor networks are enabling new applications.

By Louise Joselyn.

Autonomous, semi autonomous, self building reconfigurable wireless sensor networks are quite different from domestic or office wireless networks. The building blocks of a wireless sensor network can be extremely simple devices, sometimes called sensor motes, typically comprising a sensor, microcontroller and radio – effectively a miniature embedded system. Power may be via a battery or, increasingly, via energy harvesting. Typically small, low cost and low power, they do their own routing and can communicate across a potentially vast network by forwarding messages via nearby nodes.

The design challenge is for self building, self managing reconfigurable networks to operate reliably at very low power, inexpensively and on a large scale. The nodes are typically resource constrained and might use different operating systems,

connected through different types of network interfaces. Ad hoc networks, accessing mobile nodes, need to be adaptive to changing conditions based on context awareness.

Designers are beginning to recognise that cognitive radio – being developed today as an ancillary feature of software defined radio (sdr) – is the tip of a technology iceberg. Extending the concept to wireless sensor network nodes has the potential to enable wireless systems to use machine learning and decision theory methods to self configure, to produce an optimal and predictable response to a changing environment. Cognitive wireless systems can exploit sensor networks to obtain the large amount of environmental data they need to make context sensitive decisions.

Middleware is an important aspect of these network systems, providing a link between the basic operating system used by the wireless sensor nodes and high level applications software.



A EU funded project called Runes, completed last year, resulted in a range of middleware, mostly available on an open source basis. The Contiki operating system, for example, is designed for networked embedded systems with small amounts of memory. It is equally at home on a desktop running complex Java routines as in a resource constrained sensor mote.

Application nirvana

In the healthcare sector, wireless sensor networks are being used to monitor the elderly and infirm in a residential environment, facilitating care in the community schemes and providing confidence and security for patients and carers. France Telecom Orange has launched a ZigBee based scheme that monitors patient location, alerting carers if they stray too far or if they detect movement or lack of movement that might indicate a medical problem. The self organising, self healing network links to cellular and internet protocols to provide alerts and alarm calls, as necessary.

Medical applications are under development for the continuous monitoring of vital signs, such as heart rate, blood sugar levels and blood pressure. A range of non invasive and implantable devices is emerging for diagnosis, treatment (release of accurate doses of drugs in a precise location), health monitoring, and therapeutic

treatments. Communication links directly to the doctor, clinic or hospital can save time, hospital beds and money and the comfort and patient lifestyle is improved.

In the home, applications include room lighting that adjusts automatically to the people present, their movements or activation of a home cinema system, for example. Home networks will be able to check for gas or carbon monoxide leaks, provide surveillance and transfer security and other information, such as insurance data, to a mobile phone or maps to a car navigation system.

Wireless sensor networks will revolutionise tactical and surveillance security applications, with impromptu networks assembling themselves to meet specific demands. Nodes will be reconfigured dynamically to adapt to device failure or gaps in coverage, with data rerouted to where it is needed.

In the industrial sector, rfid tagging systems for warehouse and retail management will be extended to inventory tags on shelves, bays or containers, which can then report their own inventory status and initiate reordering and replenishment. Factory automation will benefit, particularly from increased efficiency, improved material flow and waste management, through real time control, increased robotics and reconfiguration of processes to adapt to demand. In an often noisy environment, wireless sensor networks need robustness (to resist failure), resilience (for self healing) and reliability for continuous operation.

A host of other applications include systems for power distribution, traffic management and smart buildings; the last, monitoring light, heat, humidity, noise and vibration to save energy as well

as increase comfort and promote productivity. Self healing networks are ideal for environmental monitoring, while self managing networks can reroute around physical obstacles, and areas with rf interference, for example.

Monitoring emergencies

Emergency disaster management is one of the most exciting applications for self assembling wireless sensor networks. The ability to collect data from, and pass data to, reconfigurable fixed or mobile sensors could make a vital difference.

The Runes project describes the scenario of a road tunnel fire (www.ist-runes.org/scenario.html).

Imagine the tunnel is fitted with a sensor network monitoring temperature, humidity, air quality and gases. Data is available to central control and to car passengers with devices designed to receive it. All vehicles containing potentially hazardous materials are tagged so data is available on what they are carrying and their location. All vehicles (and many people) carry transceivers capable of communicating, when necessary, with other mobile or infrastructure devices.

In the event of a fire, the control centre and emergency services are alerted and the precise location, number of vehicles involved and nature of the incident is known. Where sensor nodes are destroyed or fail, others nearby pass messages. Devices not normally on the network – maybe even mobile phones – can be reconfigured to join, guaranteeing and improving data flow.

Rescue teams receive detailed maps of the safest available access and exit routes, based on changing, real time data. Paramedics will attach monitoring devices to the injured, alerting waiting ambulances and hospitals to prepare appropriately.

But whilst self assembling wireless networks may enable new applications, they will bring with them issues and challenges, including authentication, security and even civil liberties. ■

