NETWORKING: THE GROWING ROLE FOR ADVANCED SENSORS

BY RAMI ABIELMONA AND GEORGE DINARDO

A mobile network of robotic sensor agents able to provide reconnaissance when a bomb squad responds to a threat phoned in from a local school?

A biological network of sensors able to monitor a soldier's health from within the body and coordinate a response to fight off viruses?

Or a nanorobotic airborne sensor network able to swarm towards a disaster site or a hostile environment to provide a tactical team with audiovisual, real-time information?

No longer the fanciful product of military imagination, sensor networks are on the verge of becoming part of everyday life. As we become more and more technologically intertwined, sensors networks will shape the future of our scientific and industrial innovations.

Sensor networks have humble origins: us. Humans formed the very first networks, using them to forge relationships and share resources. Soon human networks connected to other such networks, igniting a global chain reaction that eventually found its way into our technology. Electrical networks were formed to distribute, share and manage power; phone networks followed to distribute, share and manage voice; and computer networks rapidly emerged to move and manage data between remote clusters, eventually interconnecting these clusters into a global structure.

Sensor networks became a feasible reality in the mid 1990s, when computing and communications capacities became economical at the higher ends of the spectrum.

Much like the rise of the internet from a military project (i.e., DARPANET), at the outset the technology presented abundant military applications due to the immediate need for scalable and robust surveillance systems. But as with most other technologies developed in the military, SNETs easily migrated into commercial applications, which coincided with the demand for personal and communal security (e.g., anti-civilian actions and threats), and the corresponding organizational restructuring to find solutions to these pressing concerns, such as the establishment of the Department of Homeland Security in the US.

Sensor networks are composed of multiple interconnected and distributed sensors that collect information on areas or objects of interest. Sensor nodes (SNODEs) make up each sensor network and consist of three major components: (i) parameter, event and object sensing, (ii) data processing and classification, and (iii) data communications.

A large number of sensor nodes working together, in a coordinated manner, form a network that can be represented as a single data source to higher-level processing levels. For example, hundreds of sensors scattered across an area to be monitored for enemy unit movement could provide individual positional, heading and speed measurements. The in-network processing provided by the SNET would also allow for analysis of a fused information stream describing the dynamic mobilization patterns of enemy units, and identifying possible holes in their clusters for a counterattack.

There are numerous taxonomies that differentiate and classify SNETs; however, there are five main areas that indiscriminately delineate one SNET from another:

1. Node services: the properties of the SNODE – sensing unit, processing unit, communications unit, power unit, localization, mobility and physical size.
2. Network services: the properties of the network – self-organization, self-discovery, network topology, security and network protocols.
3. Data-flow services: the properties of how the data flows through the SNET – aggregation, dissemination, classification, fusion, information processing and target tracking.
4. Control-flow services: the properties of how the data is controlled throughout the SNET – tasking and querying.
5. Environment services: the properties of the environment that the SNET resides in – deployment, landscape and survivability.

Sensor networks provide flexibility, fault-tolerance, high-sensing fidelity, low-cost and rapid deployment. They can be applied to myriad security areas such as area surveillance, path prediction, target detection/classification/tracking, integrated views and state estimation.

AS HOMELAND SECURITY is now a multi-national initiative, Canada must undertake and coordinate major projects to better root out illegal activities, along, as well as within, its borders. Sensor networks could best be applied in developing a national surveillance network able to mitigate the dangers of hostile threats, as well as effectively respond to national security events.

The late Mark Weiser from Xerox PARC once said: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." Our world has been transformed by the onset of the computer, migrating mundane and repetitive tasks into the realm of the machine, as well as passing down a certain level of trust in our everyday lives that the computer (and its derivatives) will partake in our decisions as much as our own conscience and intuition.

Soon enough, we will be interacting with smart garments, smart appliances, smart sensor networks, and even smart floor tiles. All of which have obvious applications for the soldier and law enforcement officer. Sensor networks will play an important part in taking the next step: making the computer disappear.

Dr. Rami Abielmona is chief research scientist and George DiNardo is president of Larus Technologies Corp (Rami.Abielmona@larus.com or George.DiNardo@larus.com).