Sensor Networks: Evolution, Opportunities, and Challenges

CHEE-YEE CHONG, MEMBER, IEEE AND SRIKANTA P. KUMAR, SENIOR MEMBER, IEEE

Invited Paper

Wireless microsensor networks have been identified as one of the most important technologies for the 21st century. This paper traces the history of research in sensor networks over the past three decades, including two important programs of the Defense Advanced Research Projects Agency (DARPA) spanning this period: the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SensIT) programs. Technology trends that impact the development of sensor networks are reviewed, and new applications such as infrastructure security, habitat monitoring, and traffic control are presented. Technical challenges in sensor network development include network discovery, control and routing, collaborative signal and information processing, tasking and querying, and security. The paper concludes by presenting some recent research results in sensor network algorithms, including localized algorithms and directed diffusion, distributed tracking in wireless ad hoc networks, and distributed classification using local agents.

Keywords**—***Collaborative signal processing, microsensors, network routing and control, querying and tasking, sensor networks, tracking and classification, wireless networks.*

I. Introduction

Networked microsensors technology is a key technology for the future. In September 1999 [1], *Business Week* heralded it as one of the 21 most important technologies for the 21st century. Cheap, smart devices with multiple onboard sensors, networked through wireless links and the Internet and deployed in large numbers, provide unprecedented opportunities for instrumenting and controlling homes, cities, and the environment. In addition, networked microsensors provide the technology for a broad spectrum of systems in the defense arena, generating new capabilities for reconnaissance and surveillance as well as other tactical applications.

Smart disposable microsensors can be deployed on the ground, in the air, under water, on bodies, in vehicles, and inside buildings. A system of networked sensors can detect and track threats (e.g., winged and wheeled vehicles, personnel, chemical and biological agents) and be used for weapon targeting and area denial. Each sensor node will have embedded processing capability, and will potentially have multiple onboard sensors, operating in the acoustic, seismic, infrared (IR), and magnetic modes, as well as imagers and microradars. Also onboard will be storage, wireless links to neighboring nodes, and location and positioning knowledge through the global positioning system (GPS) or local positioning algorithms.

Networked microsensors belong to the general family of sensor networks that use multiple distributed sensors to collect information on entities of interest. Table 1 summarizes the range of possible attributes in general sensor networks.

Current and potential applications of sensor networks include: military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, distributed robotics, environment monitoring, and building and structures monitoring. The sensors in these applications may be small or large, and the networks may be wired or wireless. However, ubiquitous wireless networks of microsensors probably offer the most potential in changing the world of sensing [2].

While sensor networks for various applications may be quite different, they share common technical issues. This paper will present a history of research in sensor networks (Section II), technology trends (Section III), new applications (Section IV), research issues and hard problems (Section V), and some examples of research results (Section VI).

II. History of Research in Sensor Networks

The development of sensor networks requires technologies from three different research areas: sensing, communication, and computing (including hardware, software, and

Manuscript received January 7, 2003; revised March 17, 2003.

C.-Y. Chong was with Booz Allen Hamilton, San Francisco, CA 94111 USA. He is now with Alphatech, Inc. San Diego, CA 92121 USA (e-mail: cchong@alphatech.com, cychong@ieee.org).

S. Kumar is with the Defense Advanced Research Projects Agency, Arlington, VA 22203 USA (e-mail: skumar@ darpa.mil).

Digital Object Identifier 10.1109/JPROC.2003.814918

0018-9219/03$17.00 © 2003 IEEE

Table 1
Attributes of Sensor Networks

Sensors	*Size*: small (e.g., micro-electro mechanical systems (MEMS)), large (e.g., radars, satellites) *Number*: small, large *Type*: passive (e.g., acoustic, seismic, video, IR, magnetic), active (e.g., radar, ladar) *Composition or mix*: homogeneous (same types of sensors), heterogeneous (different types of sensors) *Spatial coverage*: dense, sparse *Deployment*: fixed and planned (e.g., factory networks), ad hoc (e.g., air-dropped) *Dynamics*: stationary (e.g., seismic sensors), mobile (e.g., on robot vehicles)
Sensing entities of interest	*Extent*: distributed (e.g., environmental monitoring), localized (e.g., target tracking) *Mobility*: static, dynamic *Nature*: cooperative (e.g., air traffic control), non-cooperative (e.g., military targets)
Operating environment	Benign (factory floor), adverse (battlefield)
Communication	*Networking*: wired, wireless *Bandwidth*: high, low
Processing architecture	Centralized (all data sent to central site), distributed (located at sensor or other sites), hybrid
Energy availability	Constrained (e.g., in small sensors), unconstrained (e.g., in large sensors)

algorithms). Thus, combined and separate advancements in each of these areas have driven research in sensor networks. Examples of early sensor networks include the radar networks used in air traffic control. The national power grid, with its many sensors, can be viewed as one large sensor network. These systems were developed with specialized computers and communication capabilities, and before the term "sensor networks" came into vogue.

A. *Early Research on Military Sensor Networks*

As with many technologies, defense applications have been a driver for research and development in sensor networks. During the Cold War, the Sound Surveillance System (SOSUS), a system of acoustic sensors (hydrophones) on the ocean bottom, was deployed at strategic locations to detect and track quiet Soviet submarines. Over the years, other more sophisticated acoustic networks have been developed for submarine surveillance. SOSUS is now used by the National Oceanographic and Atmospheric Administration (NOAA) for monitoring events in the ocean, e.g., seismic and animal activity [3]. Also during the Cold War, networks of air defense radars were developed and deployed to defend the continental United States and Canada. This air defense system has evolved over the years to include aerostats as sensors and Airborne Warning and Control System (AWACS) planes, and is also used for drug interdiction.

These sensor networks generally adopt a hierarchical processing structure where processing occurs at consecutive levels until the information about events of interest reaches the user. In many cases, human operators play a key role in the system. Even though research was focused on satisfying mission needs, e.g., acoustic signal processing and interpretation, tracking, and fusion, it provided some key processing technologies for modern sensor networks.

B. *Distributed Sensor Networks Program at the Defense Advanced Research Projects Agency*

Modern research on sensor networks started around 1980 with the Distributed Sensor Networks (DSN) program at the Defense Advanced Research Projects Agency (DARPA). By this time, the Arpanet (predecessor of the Internet) had been operational for a number of years, with about 200 hosts at universities and research institutes. R. Kahn, who was coinventor of the TCP/IP protocols and played a key role in developing the Internet, was director of the Information Processing Techniques Office (IPTO) at DARPA. He wanted to know whether the Arpanet approach for communication could be extended to sensor networks. The network was assumed to have many spatially distributed low-cost sensing nodes that collaborate with each other but operate autonomously, with information being routed to whichever node can best use the information.

It was an ambitious program given the state of the art. This was the time before personal computers and workstations; processing was done mostly on minicomputers such as PDP-11 and VAX machines running Unix and VMS. Modems were operating at 300 to 9600 Bd, and Ethernet was just becoming popular.

Technology components for a DSN were identified in a Distributed Sensor Nets workshop in 1978 [4]. These included sensors (acoustic), communication (high-level protocols that link processes working on a common application in a resource-sharing network [5]), processing techniques and algorithms (including self-location algorithms for sensors), and distributed software (dynamically modifiable distributed systems and language design). Since DARPA was sponsoring much artificial intelligence (AI) research at the time, the workshop also included talks on the use of AI for understanding signals and assessing situations [6], as well as various distributed problem-solving techniques [7]–[9]. Since very few technology components were available off the shelf, the resulting DSN program had to address distributed computing support, signal processing, tracking, and test beds. Distributed acoustic tracking was chosen as the target problem for demonstration.

Researchers at Carnegie Mellon University (CMU), Pittsburgh, PA, focused on providing a network operating system that allows flexible, transparent access to distributed resources needed for a fault-tolerant DSN. They developed

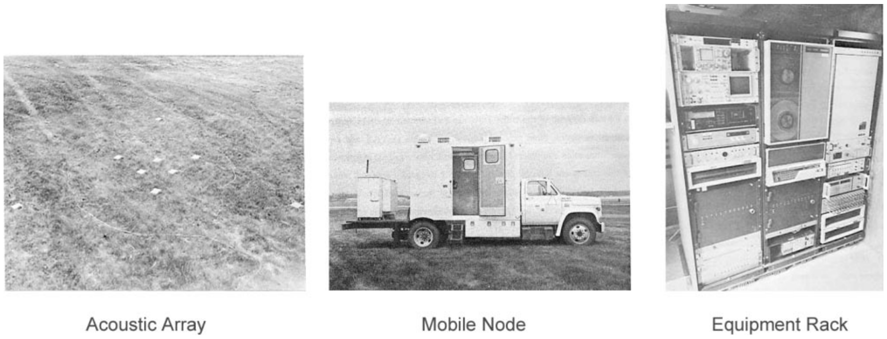

Fig. 1. Components in the DSN test bed around 1985.

a communication-oriented operating system called Accent [10], whose primitives support transparent networking, system reconfiguration, and rebinding. Accent evolved into the Mach operating system [11], which found considerable commercial acceptance. Other efforts at CMU included protocols for network interprocess communication to support dynamic rebinding of active communicating computations, an interface specification language for building distributed system software, and a system for dynamic load balancing and fault reconfiguration of DSN software. All this was demonstrated in an indoor test bed with signal sources, acoustic sensors, and VAX computers connected by Ethernet.

Researchers at the Massachusetts Institute of Technology (MIT), Cambridge, focused on knowledge-based signal processing techniques [12] for tracking helicopters using a distributed array of acoustic microphones by means of signal abstractions and matching techniques. Signal abstractions view signals as consisting of multiple levels, with higher levels of abstraction (e.g., peaks) obtained by suppressing detailed information in lower levels (e.g., spectrum). They provide a conceptual framework for thinking about signal processing systems that resemble what people use when interactively processing and interpreting real-world signals. By incorporating human heuristics, this approach was designed for high signal-to-noise ratio situations where models are lacking. In addition, MIT also developed the Signal Processing Language and Interactive Computing Environment (SPLICE) for DSN data analysis and algorithm development, and Pitch Director's Assistant for interactively estimating fundamental frequency using domain knowledge.

Moving up the processing chain, tracking multiple targets in a distributed environment is significantly more difficult than centralized tracking. The association of measurements to tracks and estimation of target states (position and velocity) given associations have to be distributed over the sensor nodes. In the 1980s, Advanced Decision Systems (ADS), Mountain View, CA, developed a multiple-hypothesis tracking algorithm to deal with difficult situations involving high target density, missing detections, and false alarms, and decomposed the algorithm for distributed implementation [13], [14]. Multiple-hypothesis tracking is now a standard approach for difficult tracking problems.

For demonstration, MIT Lincoln Laboratory developed the real-time test bed for acoustic tracking of low-flying aircraft [15]. The sensors were acoustic arrays (nine microphones arranged in three concentric triangles with the largest being 6 m across). A PDP11/34 computer and an array processor processed the acoustic signals. The nodal computer (for target tracking) consists of three MC68000 processors with 256-kB memory and 512-kB shared memory, and a custom operating system. Communication was by Ethernet and microwave radio. Fig. 1 (extracted from [16]) shows the acoustic array (nine white microphones), the mobile vehicle node with an acoustically quiet generator in the back, and the equipment rack with the acoustic/tracking node and gateway node in the vehicle. Note the size of the system and that practically all components in the network were custom built. That was the state of the art in the early 1980s. The DSN test bed was demonstrated with low-flying aircraft, which was successfully tracked with acoustic sensors as well as TV cameras. The tracking algorithm was fairly sophisticated, since the acoustic propagation delay is significant relative to the speed of the aircraft.

Another test bed in the DSN program was the distributed vehicle monitoring test bed at the University of Massachusetts, Amherst. This was a research tool for empirically investigating distributed problem solving in networks. The distributed knowledge-based problem solving approach used a functionally accurate, cooperative architecture consisting of a network of Hearsay-II nodes (blackboard architecture with knowledge sources). Different local node control approaches were explored [17].

C. Military Sensor Networks in the 1980s and 1990s

Even though early researchers on sensor networks had in mind large numbers of small sensors, the technology for small sensors was not quite ready. However, planners of military systems quickly recognized the benefits of sensor networks, which become a crucial component of network-centric warfare [18]. In platform-centric warfare, platforms "own" specific weapons, which in turn own sensors in a fairly rigid architecture. In other words, sensors and weapons are mounted with and controlled by separate platforms that operate independently. In network-centric warfare, sensors do not necessarily belong to weapons or platforms. Instead, they collaborate with each other over a communication network, and information is sent to the appropriate "shooters." Sensor networks can improve detection and tracking performance through multiple observations, geometric and phenomenological diversity, extended detection range, and faster response time. Also, the development cost is lower by exploiting commercial network technology and common network interfaces.

An example of network-centric warfare is the Cooperative Engagement Capability (CEC) [19] developed by the U.S. Navy. This system consists of multiple radars collecting data on air targets. Measurements are associated by a processing node "with reporting responsibility" and shared with other nodes that process all measurements of interest. Since all nodes have access to essentially the same information, a "common operating picture" essential for consistent military operations is obtained. Other military sensor networks include acoustic sensor arrays for antisubmarine warfare such as the Fixed Distributed System (FDS) and the Advanced Deployable System (ADS), and unattended ground sensors (UGS) [20] such as the Remote Battlefield Sensor System (REMBASS) and the Tactical Remote Sensor System (TRSS).

D. *Sensor Network Research in the 21st Century*

Recent advances in computing and communication have caused a significant shift in sensor network research and brought it closer to achieving the original vision. Small and inexpensive sensors based upon microelectromechanical system (MEMS) [21] technology, wireless networking, and inexpensive low-power processors allow the deployment of wireless ad hoc networks for various applications. Again, DARPA started a research program on sensor networks to leverage the latest technological advances.

The recently concluded DARPA Sensor Information Technology (SensIT) program [22] pursued two key research and development thrusts. First, it developed new networking techniques. In the battlefield context, these sensor devices or nodes should be ready for rapid deployment, in an *ad hoc* fashion, and in highly dynamic environments. Today's networking techniques, developed for voice and data and relying on a fixed infrastructure, will not suffice for battlefield use. Thus, the program developed new networking techniques suitable for highly dynamic *ad hoc* environments. The second thrust was networked information processing, i.e., how to extract useful, reliable, and timely information from the deployed sensor network. This implies leveraging the distributed computing environment created by these sensors for signal and information processing in the network, and for dynamic and interactive querying and tasking the sensor network.

SensIT generated new capabilities relative to today's sensors. Current systems such as the Tactical Automated Security System (TASS) [23] for perimeter security are dedicated rather than programmable. They use technologies based on transmit-only nodes and a long-range detection paradigm. SensIT networks have new capabilities. The networks are interactive and programmable with dynamic tasking and querying. A multitasking feature in the system allows multiple simultaneous users. Finally, since detection ranges are much shorter in a sensor system, the software and algorithms can exploit the proximity of devices to threats to drastically improve the accuracy of detection and tracking. The software and the overall system design supports low latency, energy-efficient operation, built-in autonomy and survivability, and low probability of detection of operation. As a result, a network of SensIT nodes can support detection, identification, and tracking of threats, as well as targeting and communication, both within the network and to outside the network, such as an overhead asset.

III. Technology Trends

Current sensor networks can exploit technologies not available 20 years ago and perform functions that were not even dreamed of at that time. Sensors, processors, and communication devices are all getting much smaller and cheaper. Commercial companies such as Ember, Crossbow, and Sensoria are now building and deploying small sensor nodes and systems. These companies provide a vision of how our daily lives will be enhanced through a network of small, embedded sensor nodes. In addition to products from these companies, commercial off-the-shelf personal digital assistants (PDAs) using Palm or Pocket PC operating systems contain significant computing power in a small package. These can easily be "ruggedized" to become processing nodes in a sensor network. Some of these devices even have built-in sensing capabilities, such as cameras. These powerful processors can be hooked to MEMS devices and machines along with extensive databases and communication platforms to bring about a new era of technologically sophisticated sensor nets.

Wireless networks based upon IEEE 802.11 standards can now provide bandwidth approaching those of wired networks. At the same time, the IEEE has noticed the low expense and high capabilities that sensor networks offer. The organization has defined the IEEE 802.15 standard for personal area networks (PANs), with "personal networks" defined to have a radius of 5 to 10 m. Networks of short-range sensors are the ideal technology to be employed in PANs. The IEEE encouragement of the development of technologies and algorithms for such short ranges ensures continued development of low-cost sensor nets [24]. Furthermore, increases in chip capacity and processor production capabilities have reduced the energy per bit requirement for both computing and communication. Sensing, computing, and communications can now be performed on a single chip, further reducing the cost and allowing deployment in ever larger numbers.

Looking into the future, we predict that advances in MEMS technology will produce sensors that are even more capable and versatile. For example, Dust Inc., Berkeley, CA, a company that sprung from the late 1990s Smart Dust research project [25] at the University of California, Berkeley, is building MEMS sensors that can sense and communicate and yet are tiny enough to fit inside a cubic millimeter. A Smart Dust optical mote uses MEMS to aim submillimeter-sized mirrors for communications. Smart Dust sensors can be deployed using a 3 × 10 mm "wavelet"

Table 2
Three Generations of Sensor Nodes

	Yesterday (1980's – 1990's)	Today (2000 – 2003)	Tomorrow (2010)
Manufacturer	Custom contractors, e.g., for TRSS	Commercial: Crossbow Technology, Inc. Sensoria Corp., Ember Corp.	Dust, Inc. and others to be formed
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particle
Weight	Kilograms	Grams	Negligible
Node architecture	Separate sensing, processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client server, peer to peer	Peer to peer
Power supply lifetime	Large batteries; hours, days and longer	AA batteries; days to weeks	Solar; months to years
Deployment	Vehicle-placed or air-drop single sensors	Hand-emplaced	Embedded, "sprinkled" left-behind

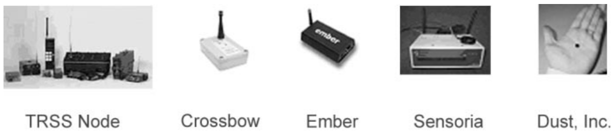

Fig. 2. Three generations of sensor nodes.

shaped like a maple tree seed and dropped to float to the ground. A wireless network of these ubiquitous, low-cost, disposable microsensors can provide close-in sensing capabilities in many novel applications (as discussed in Section IV).

Table 2 compares three generations of sensor nodes; Fig. 2 shows their sizes.

IV. New Applications

Research on sensor networks was originally motivated by military applications. Examples of military sensor networks range from large-scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection. However, the availability of low-cost sensors and communication networks has resulted in the development of many other potential applications, from infrastructure security to industrial sensing. The following are a few examples.

A. *Infrastructure Security*

Sensor networks can be used for infrastructure security and counterterrorism applications. Critical buildings and facilities such as power plants and communication centers have to be protected from potential terrorists. Networks of video, acoustic, and other sensors can be deployed around these facilities. These sensors provide early detection of possible threats. Improved coverage and detection and a reduced false alarm rate can be achieved by fusing the data from multiple sensors. Even though fixed sensors connected by a fixed communication network protect most facilities, wireless ad hoc networks can provide more flexibility and additional coverage when needed. Sensor networks can also be used to detect biological, chemical, and nuclear attacks. Examples of such networks can be found in [26], which also describes other uses of sensor networks.

B. *Environment and Habitat Monitoring*

Environment and habitat monitoring [27] is a natural candidate for applying sensor networks, since the variables to be monitored, e.g., temperature, are usually distributed over a large region. The recently started Center for Embedded Network Sensing (CENS) [28], Los Angeles, CA, has a focus on environmental and habitat monitoring. Environmental sensors are used to study vegetation response to climatic trends and diseases, and acoustic and imaging sensors can identify, track, and measure the population of birds and other species. On a very large scale, the System for the Vigilance of the Amazon (SIVAM) [29] provides environmental monitoring, drug trafficking monitoring, and air traffic control for the Amazon Basin. Sponsored by the government of Brazil, this large sensor network consists of different types of interconnected sensors including radar, imagery, and environmental sensors. The imagery sensors are space based, radars are located on aircraft, and environmental sensors are mostly on the ground. The communication network connecting the sensors operates at different speeds. For example, high-speed networks connect sensors on satellites and aircraft, while low-speed networks connect the ground-based sensors.

C. *Industrial Sensing*

Commercial industry has long been interested in sensing as a means of lowering cost and improving machine (and perhaps user) performance and maintainability. Monitoring machine "health" through determination of vibration or wear and lubrication levels, and the insertion of sensors into regions inaccessible by humans, are just two examples of industrial applications of sensors. Several years ago, the IEEE and the National Institute for Standards and Technology (NIST) launched the P1451 Smart Transducer

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**