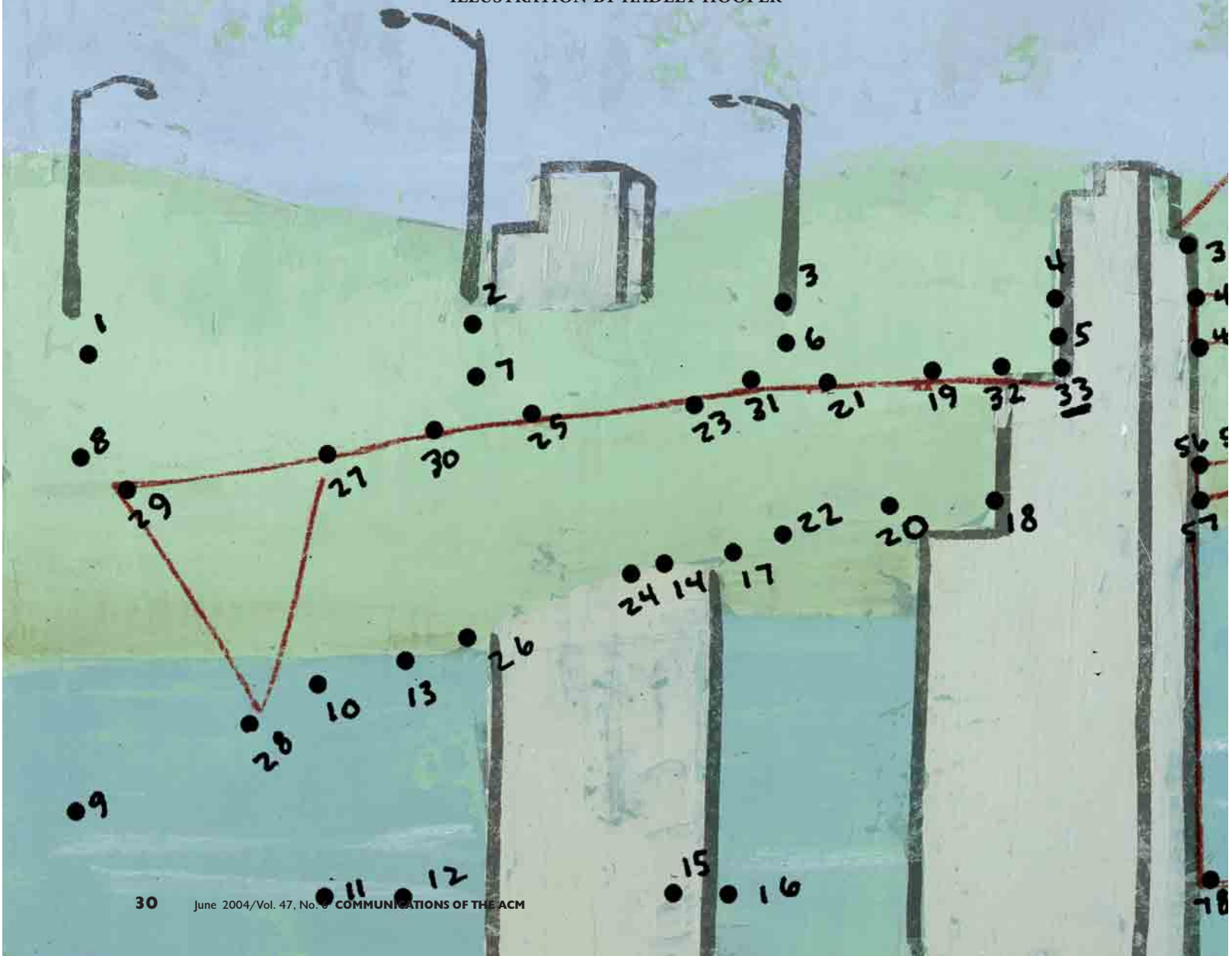
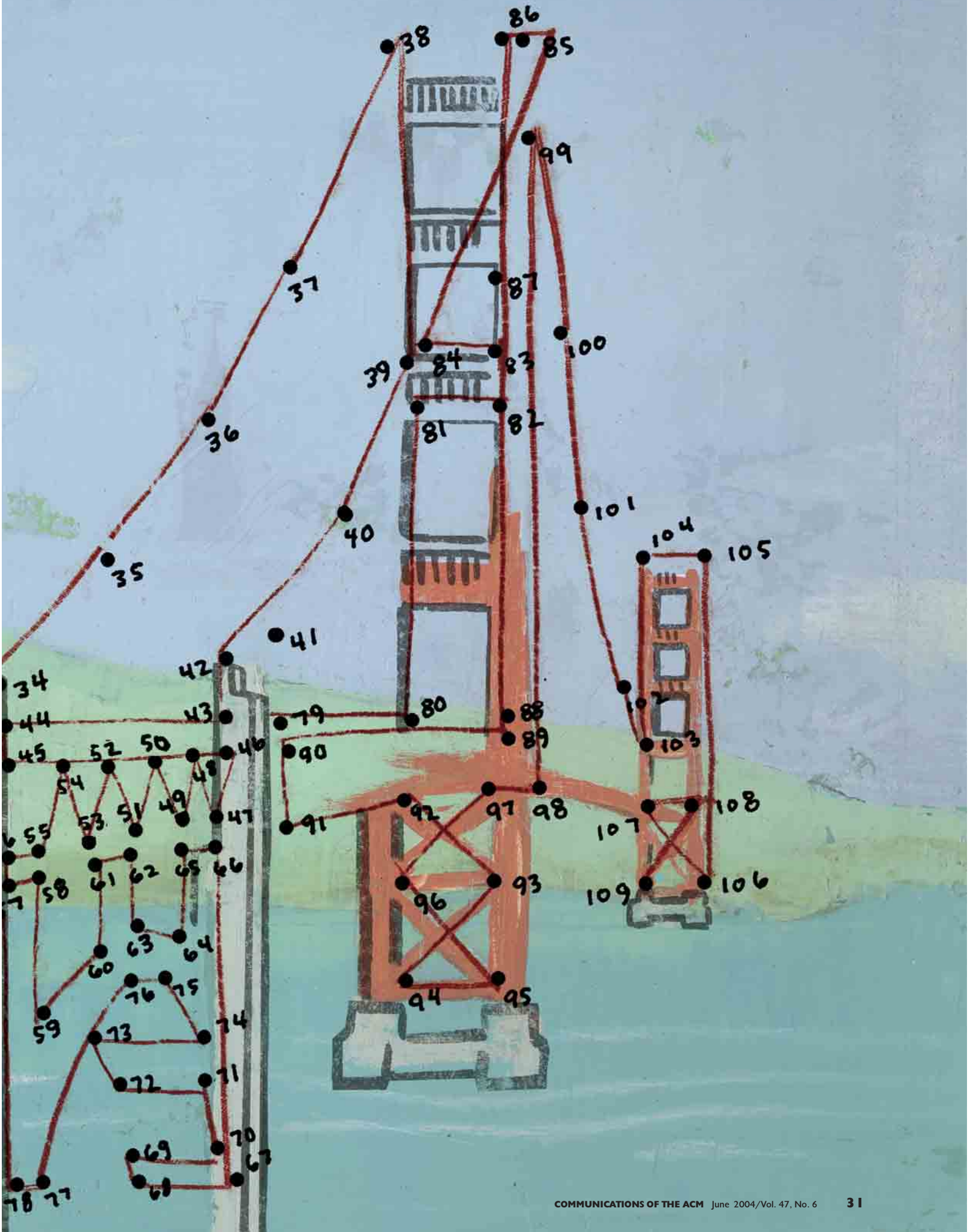
WIRELESS SENSOR NETWORKS

By DAVID E. CULLER *and* WEI HONG, GUEST EDITORS

Thousands of tiny low-power devices spread over large physical spaces collaboratively monitor the environment, guide vehicles, and predict potential faults in buildings, bridges, roads, and rails.

ILLUSTRATION BY HADLEY HOOPER




86
38
85
99
37
87
100
39
84
83
36
81
82
101
40
104
105
35
41
42
34
44
43
79
80
88
89
45
52
50
46
90
54
48
49
53
51
47
91
92
97
98
108
55
107
61
62
65
66
58
93
96
109
106
63
64
60
76
75
59
73
74
72
71
70
69
68
61
78
77

Wireless sensor networks are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security, and social factors. They are beginning to realize the vision of an embedded Internet, in which networks of interconnected computing devices deeply embedded into the physical environment transform whole fields of science, engineering, and manufacturing by providing detailed instrumentation of many points over large spaces, both natural and artificial.

Sensor networks provide a new kind of instrument—call it a macroscope—that enables us to observe and interact with physical phenomena in real time at a fidelity that was previously unobtainable. Such pervasive instrumentation will be of great value in a range of applications, including understanding ecosystem dynamics, setting land-use policy, protecting property, efficiently operating and managing machinery and vehicles, establishing perimeter and building security, protecting packages and containers, monitoring supply chain management, and helping deliver health care. Sensor networks readily extend to monitoring interactions among many objects within these domains, ensuring asset management, ubiquitous computing environments, and emergency response. Moreover, they help feed information into autonomous distributed control actions in, say, building temperature control and precision agriculture systems.

To fully realize the vision of the embedded Internet, the related devices must be small, unobtrusive, and expendable, and the network of potentially thousands of nodes must be cost-effective to develop, deploy, program, utilize, and maintain. Thus, sensor networks present significant systems challenges involving the use of large numbers of resource-constrained nodes operating essentially unattended and exposed to the elements and to the potential for malicious attack for years at a time while dealing with the noise, uncertainty, and asynchrony of the real world. They need to be largely self-organizing, self-regulating, and self-repairing, programmable in place, and easily utilized as an ensemble.

Over the past few years, various platforms, including the Berkeley wireless Mica mote, have been developed to allow researchers to address these challenges in concrete, not just conceptual, terms. Meanwhile, important applications in the natural environment and in smart structures have helped identify the practical limits and prioritize future directions in the problem domain.

This special section addresses the lessons being learned through direct experience in realizing several important facets of the embedded Internet vision. Each of the four articles represents a substantial thrust in translating that vision into reality, including the design and development of applications, hardware and software needed to collect ubiquitous physical data, distributed algorithms for gathering and analyzing this information, and methods for robust and secure operation. We challenged each group to address three key aspects of their research: the state of the art, a common framework in which to understand their approaches, and an image of likely paths for future development.

Environmental monitoring has emerged as an especially important initial proving ground. Its long-term outdoor deployments stress reliability, low-power operation, network protocols, data quality, and new experimental processes. For example, in monitoring bird nesting habits, devices must be placed in small underground burrows before the birds arrive and last throughout the nesting season without disturbing their activity. Szewczyk et al. chronicle how a number of habitat-monitoring applications focus and drive their computer systems research toward developing an overall network architecture for dense monitoring of regions of physical space, power conservation, real-time network-performance monitoring, robust data collection despite intermittent connectivity, and verification of novel empirical data. Their experience monitoring environmental conditions, along with those conditions' effects on living organisms, sheds light on key systems issues, including routing, power management, and long-term network performance.

The underlying hardware technology for wireless sensor networks, consisting of perhaps thousands of integrated devices, with built-in processing, storage, and sensors with RF transceiver, energy storage, and antenna, is evolving quickly and gaining a signature style of design. That design involves many energy-constrained, resource-limited devices operating in concert as a result of application requirements demanding long-term operation, up-close monitoring, and constraints on size and available power. Hill et al. articulate this new class of computer system and the range of design points it comprises, including

specks of a few square millimeters of silicon, commodity microcontroller-based devices about the size of a coin, and more-powerful microprocessor-based embedded nodes. They also represent a road map of future developments, including deep integration and specialized accelerators to reduce power, extrapolating from several current devices, including the Berkeley motes, the Intel iMote, the Stargate Xscale-based server, and tiny integrated devices, along with such technology trends as improved radios and emerging standards.

Applications extract and process information as it flows across a distributed collection of the sensing, storage, processing, and communication resources that form wireless sensor networks. Thus, classical networking issues and query-processing issues become deeply intertwined, as queries are continuously processed within the network. Woo et al. explore this emerging interplay of historically distinct domains. Drawing from their experience implementing query processing in environment- and building-monitoring applications, they describe the TinyDB and Diffusion architectures, identifying a set of novel networking mechanisms that includes query-informed routing, efficient rendezvous, and virtual coordinate systems. They suggest how the networking interface might evolve to better serve the needs of in-network query processing.

As progress is made on the technical challenges of long-term, adaptive deployments, effective platforms, and efficient in-network query processing, the possibility looms that adoption of wireless sensor networks might be paced largely by competing social factors, or how they directly affect the personal private lives of individual people worldwide. To provide effective security and meaningful privacy, the technical aspects of these issues must be addressed from the start of any system's design process in the context of their end applications. Also needed is guidance derived from the social dialogue taking place among system architects, developers, users, and policy makers. Perrig et al. identify the main security goals, and risks, of this emerging class of system, including trust establishment, key management, secrecy, authentication, and robustness to various forms of denial of service. They recommend ways to use them to formulate a set of key security services, including effective defense strategies against the most likely attack scenarios.

These articles represent an exciting, insightful glimpse into the state of the art, as well as emerging future directions, in this important new area of computer systems research, turning the vision of pervasive instrumentation of the physical world into everyday reality. C

SENSOR networks provide a new kind of instrument—call it a macroscope—that enables us to observe and interact with physical phenomena in real time at a fidelity that was previously unobtainable.

DAVID E. CULLER (culler@cs.berkeley.edu) is a professor of computer science at the University of California, Berkeley.
WEI HONG (whong@intel-research.net) is a senior researcher and the principal investigator of sensor networks at Intel Research Laboratory in Berkeley, CA.