Sensor Networks Challenges for Intelligent Buildings

Alberto Eduardo Cerpa
University of California, Merced
acerpa@ucmerced.edu

1. Introduction

Sensor networks will play a fundamental role in future intelligent buildings. There are two basic areas that we envision this technology having a critical impact; these are energy conservation and security.

Most of the power consumption in most countries is done inside buildings. Furthermore, the largest consumers of energy are the richest, most developed countries, and the proportion of energy used inside buildings is much larger in those nations than the rest [1]. Regarding security, it is clear that having a large number of sensors in the building that can monitor human movement further increase the levels of security in the building. Having multiple sensing points can provide greater capability, as is leveraged commonly by sensor arrays such as in radar systems or binocular vision [2].

There are significant advantages for this technology to have an impact in intelligent buildings. First of all, sensor networks use small and non-intrusive devices. They have relatively low power consumption at the system level, which implies long lifetime per deployment. Second, it is possible to retrofit old buildings to do sensing and monitoring with minimal changes, and even integrate them with HVAC systems for finer grained distributed control in all new and old buildings –if they have one–, as long as these systems provide an open API. Finally, a large number of parameters could be measured to capture spatial and temporal distributions at a much finer granularity than other technologies available. For example, a sensor network system consisting thousands of sensors in a building could capture temperature, humidity, light and human mobility at a spatial and temporal granularity not available today.

2. Challenges

There are many research challenges to realize sensor network technology for intelligent buildings.

Hardware Cost: the current cost of each individual sensor unit is still very high. Commercially available platforms cost in the order of $100 per unit [3] with temperature, humidity and light sensors when bought in large quantities. Capable sensors able to track human mobility inside buildings are even more expensive, with research prototypes of low-power consumption cameras costing in the order of $200 per unit [4]. It is critical to reduce the per-unit cost at least one order of magnitude.

System Architecture: there is no unified system and networking architecture that is stable and mature enough to build different applications on top. Most of the applications and research prototypes are vertically integrated in order to maximize performance. This fact prevents further innovation at application layer, since currently each application has to reinvent the wheel at some portion of the lower levels of the stack.

Wireless Communication: one of the main strengths of sensor network technology is allowing sensor nodes to communicate and coordinate each other in a distributed manner completely un-tethered from the environment and the infrastructure. However, wireless communication in indoor environments is still quite unpredictable using low-power consumption RF transceivers, in particular in clutter environments common inside buildings, with many interfering electromagnetic fields, such as the ones produced by elevators, machinery and computers, among others [5,6].

Programmability: there are three main challenges regarding the programmability of the system. The first challenge is to achieve some network re-programmability capacity in an energy and communication conservative form. The second challenge is to allow the final user to easily task the network. Finally, as the number of nodes increases, there are scaling challenges regarding the programmability of the ensemble.

Security: there are security challenges at many levels. From the system point of view, it is critical that the information provided by the nodes is authenticated and the integrity verified, since this information provides the feedback loop to expensive equipment controlling power consumption in the building. From the users' point of view, it is also critical that this information cannot be easily spoofed and remains protected in the back end processor, since it may affect the privacy of users.

3. Research Needs

Each of the challenges above sets the direction for many of the information technology research needs. We believe the most important research needs for the next 5 to 10 years are the following:

Long Term SN Deployments: we think it is critical that we move to more stable long term deployments, in order to gain experience and insight with systems and applications. Building large scale, long term testbeds and deployments is a condition *sine qua non* to make progress in this area. One of the main problems with this vision is the individual cost of the sensor nodes. While some advances has been achieved with system integration and new designs, the most notable of them being the mote-in-a-chip 'spec' design [7], they remain at large research prototypes with limited programmability, mechanically fragile and still costly to obtain in large quantities. Innovations in hardware architecture or the fabrication of components may not be the most important need, but perhaps integration issues that push the cost of each node to at least less than $10 per unit. Another important issue is the packaging of these units. Packaging has been a no-man's land in the last 5 years, with ingenious graduate students finding ad-hoc solutions that do not necessarily work for real deployments. While many of these issues are not pure research issues and they may be a matter of economies of scale, they remain a critical roadblock to make progress in other areas.

System Architecture: it is *unclear* what should be done regarding the system and network architecture of this class of systems; to the point that some researchers argue there should be none. While most of the applications and research prototypes are vertically integrated in order to maximize performance, we strongly believe there should be some significant thought spent into analyzing a wide range of applications and stacks, and understanding what are the fundamental components and services necessary to a large range of applications. This exercise would allow a system architecture design based on common needs of a group of applications, and would also permit the synthesis of common functionality at the lower levels of the stack. There are researchers that propose very general and flexible architectures that could accommodate a wide range of applications' needs. We believe this is similar to the past history in computer architecture when researchers were designing micro-processors being instruction set independent. We also believe that there should be more research on tiered architectures with heterogeneous type of nodes [8], since one size does not fit all.

Wireless Communication: there are no accepted and implemented wireless simulation models in the sensor network community that are well understood, so algorithm and application researchers could at least get simulation results with more confidence and accuracy. This process is similar to the one experienced by simulations tools used by the internet networking community in wired networks [9,10], many of them still having problems when used to simulate wireless environments. Furthermore, as new more capable RF transceivers are introduced, there is a need to further improve upon previous work in other areas. For example, the effective nominal radio range of the new Zigbee 802.15.4 radios [11] significantly changes based on the bit rate used, so it is unclear how to perform link quality estimation for any parameter.

Security: while the community has produced several algorithms and schemes to provide cryptographic authentication and integrity at the packet transmission level under stringent energy constraints [12], the more general problems of system security has not been addressed extensively. These problems are critical if we are to move forward to real system deployments. For example, when the Soviet Union invaded Afghanistan in the '80s, they installed sensor motion detectors in the perimeters of all critical military bases. The Afghan rebels attacked the system by releasing large number of rabbits several weeks before the attacks. The soviet security officers were so exhausted with the false alarm rates, that they simply disconnected the systems.

Programming: There are many aspects regarding the programmability of the system that should be addressed. First of all, there is a need to establish an efficient way to perform low-level reprogramming. While TinyOS is the *de facto* OS standard for sensor nodes, it is not clear it is the best solution. Other OSes based on driver modules, virtual machines or even dynamic libraries [13,14] might be best suited. The second issue is user-level programming. It is unclear what paradigm should be the best suited for applications used in intelligent buildings. There are many options, including non-turning complete meta-languages, database languages, and parallel scripting languages. Finally, as the number of nodes increases in future application, there is a need to move to completely different programming paradigms, perhaps inspired in statistical mechanics with probabilistic bounds instead of deterministic ones.

REFERENCES

[1] P. Waide "Climate and Comfort: International Energy-Efficiency Policy and Air Conditioning", IEA Workshop'06, France.
[2] T. Kanade, M. Okutome, and T. Nakahara. "A Multiple Baseline Stereo Method." In Image Understanding Workshop, DARPA, 92.
[3] MoteIV. http://www.moteiv.com
[4] Cyclops. http://www.cyclopscamera.org
[5] A. Cerpa, J. Wong, L. Kuang, M. Potkonjak, D. Estrin. "Statistical Models of Lossy Links in Wireless Sensor Networks." In IPSN'05
[6] A. Cerpa, J. Wong, M. Potkonjak, D. Estrin. "Temporal Properties of Wireless Links: Modeling and Implications on Multi-Hop Routing." In MOBIHOC'05.
[7] SPEC. http://www.dustnetworks.com/
[8] L. Girod, J. Elson, A. Cerpa, N. Ramanathan T. Stathopoulos, and D. Estrin. "EmStar: a Software Environment for Developing and Deploying Wireless Sensor Networks." In USENIX'04.
[9] NS-2. http://www.isi.edu/nsnam/ns
[10] OPTNET. http://www.opnet.com
[11] 802.11.15 Standard. http://www.ieee802.org/15
[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar. "SPINS: Security Protocols for Sensor Networks." In MOBICOM'01.
[13] C. Han, R. Rengaswamy, R. Shea, E. Kohler and M. Srivastava. "SOS: A dynamic operating system for sensor networks." In MOBISYS'05.
[14] A. Dunkels, N. Finne, J. Eriksson, T. Voigt. "Run-time Dynamic Linking for Reprogramming Wireless Sensor Networks." In SENSYS'06.

Bio: Alberto E. Cerpa received the PhD degree in CS from UCLA (2005), the MSc degree in CS from USC (2000), the MSc degree in EE from USC (1998), and the engineer degree in EE from the Buenos Aires Institute of Technology, Argentina (1995). He is an assistant professor of computer science and engineering in the School of Engineering at the University of California, Merced. His interests lie broadly in the networking and distributed systems areas, with emphasis in wireless sensor networks. He is a member of the ACM and IEEE.