Application Requirements

Number, geometry, and topology

Deployment, Binding, Commissioning

Deployment is often overlooked in early discussions of applications, but if ignored it can lead to disaster. Who will put the sensors in place, and what configuration will they need to do? Will they need to write down the location and ID of each sensor, or type in a network ID or security code? How will the motes in my deployment know that they shouldn't talk to the ones in yours? For example, a single building may contain a network for HVAC, lighting control, building security, fire detection, and asset management. In fact, each floor may have different tenants, some of whom have their own networks for the same function. Some networks will be supplied by a single manufacturer, but many will be made up of products from a variety of manufacturers.

The early vision of Smart Dust led people to think that it would be sprinkled throughout an environment more or less randomly. Some deployments did this [29Palms], but for the vast majority of sensor network applications today the sensors are individually installed where they are needed.

Some systems will be installed by trained technicians and others by doctoral students, both of whom can be counted on to have some sophistication and ability. But the majority will be installed by people who may have no technical background whatsoever. In one application, a customer told me that the only tools his installers would bring to bear on the installation problem were a blowtorch and a sledgehammer. In another, we used an LED that would change from red to green when the mote had joined the network successfully – and our first installer was colorblind!

Gateways and Internetworking

In the late aughts ('09), most sensor networks are not connected to the internet. Access points are generally plugged into a system which uses the data locally, and the information flows in the network do not extend beyond the sensor network itself.

This is likely to change dramatically over the next decade, during which IP-based sensor networking is likely to take off. Many sensor networks will still not connect to the internet, however, due to tradition, politics, or concern over security.

Mobility

Localization

Data flows

There is such a wide range of applications of sensor networks that virtually any type of data flow that can be imagined can be ascribed to some type of network, real or conjectured. Here we describe the most common examples, and use "N" to represent all

of the nodes in our network, and "k" as some number of motes less than or equal to N. In most networks there is at least one "special node", which we will call an access point, which connects to some other information system.

Periodic and Event-driven reporting

Most reporting in sensor networks is periodic. The period may vary from milliseconds to days, but the sweet spot for current technology ranges from seconds to minutes.

Events may trigger the flow of data in an N-to-1 flow, as in a home alarm system where a door or window opening causes a packet to be sent to the alarm control box. Fault conditions on a mote, or evidence of a security attack may also generate packets to be sent to the AP.

Some systems use report by exception, where the data is sampled on a regular period, but is only reported if it falls outside of some specified range.

N-to-AP

By far the most common data flow in existing sensor networks is the regular collection of data from many points to one collection point. This is such a common flow that we will assume it as a baseline in all of our discussions, and call-out its absence in those rare cases where it doesn't appear.

In pharmaceutical monitoring, temperature data from dozens or hundreds of sensors is sent back to the data logger attached to the AP. Network and mote health and status information is often sent to the AP, either to enable network control in a centrally managed network, or for diagnostic purposes in a distributed management system.

AP-to-N, AP-to-k

Broadcast commands from the AP to some or all of the motes in the network is used for over-the-air programming (OTAP), changing network parameters such as ID and data-link-layer keys, and synchronous sampling or actuation commands.

AP-to-1, 1-to-AP

File-transfer to or from a mote ideally uses a higher-data-rate flow than would normally be used for data collection. When people troubleshoot or configure a mote over the network they generally want a shorter response time (lower latency) than might otherwise be available.

1-to-1

Pair-wise communication between motes occurs in control applications. A light switch sending a packet to a light fixture is an example of open-loop control. A tank level sensor sending a packet to a valve is an example of closed-loop control. Most of these flows are short geographically. If you can think of an application where mote needs to have a pair-wise flow to a mote more than 10 km away, let me know.

Latency-bounded reliability

The sole purpose of the *networking* piece of wireless sensor networks is to deliver data. It is the reliability of that delivery on each of the data flows that sets most of the requirements on the network. Reliability is the fraction of packets introduced to the network that successfully get to their destination. For some applications, a reliability of 90% may be acceptable. For others, the probability that even a single packet is lost out of millions sent must be a tiny fraction of a percent. Usually, if someone tells you that reliability isn't important to them, then there is probably an opportunity to redefine the data flow in a more mote-amenable way. If 50% reliability is acceptable on a flow of 1 packet per second, then the application would probably be just as happy with 1 packet every two seconds with 99.9% reliability.

For most data flows, reliability is tied directly to latency. Most applications will not tolerate a network which delivers 100% of the packets after a one year delay. Some applications will be sensitive to the mean latency, and others will be more concerned with worst-case latency. For example, people are willing to tolerate the occasional long response time as long as the average is reasonably low, whereas a feedback control system may not care about the mean as long as the worst-case latency is bounded.

Lifetime, cost, and size

For the WSN discussed in this text, wireless means no wires, which means that energy is going to be a scarce commodity. For a given topology, flow, radio, and protocol, the lifetime of a mote is going to be related to the amount of energy it can store or scavenge. Storage and scavenging require both cost and size in a mote. In most applications, cost is the driver rather than size. For example, if C-cell batteries were free, most sensor network applications would use them even though they are somewhat ungainly. In general, the reason that people want small batteries is because they are cheaper. Given the choice between equal cost C-cell and coin-cell batteries, the decision is likely to be made first based on lifetime, and then finally size. If the coin cell only gives the required lifetime in 80% of the desired deployments, then the larger C-cell is likely to be used. Only when the lifetime and cost are both satisfied is size likely to be the deciding factor.

Clearly there are exceptions to this. If car batteries were free, they would be too big for most applications. For medical sensors worn on the body, a C-cell is not going to be acceptable for almost any application.

Scavenging systems also take up size, either as volume for vibrational scavengers, or area for solar cells.

Line-powered devices make many of the networking challenges a lot easier, but they incur their own expense. For home automation, it may be perfectly acceptable for all routing motes to be plugged into an outlet or extension cord. For industrial automation and building automation, wired power can not come from outlets, it must be run in dedicated conduit.

Security

Most people don't have the nefarious disposition necessary to truly appreciate the need for security. Security people tend to think in terms of the worst-case scenario, and how to exploit weakness and improbable events.

Technologists and entrepreneurs very naturally tend to think about the benefits of their technologies. Embrace that, and imagine that your application is wildly success, and that people are using it in ways that go beyond even what you initially thought. Sadly, even foolish people are using it in ways that it probably shouldn't be used.

Now try to think like a crook, a hacker, a terrorist. Imagine that you have a lot of resources behind you, and try to come up with a set of worst-case scenarios.

Wireless Options

There are many existing wireless solutions to choose from. The research community has rightly tried to shoehorn every application into wireless mesh, but the marketplace will decide which ones make commercial sense. Some of the other options to consider when recommending wireless for a given application are listed below.

Single-hop Point-to-point

This is the traditional approach to wireless sensor networking, used probably since the days of Marconi. Cordless phones, RC toys, Nike shoes and Ipods, and TV and broadcast radio all use this approach with remarkable success. The biggest advantage is cost. A simple digital radio can be integrated into a product for well under a dollar.

The disadvantages can be subtle, and largely the purpose of this class is to explain why something more than point-to-point is needed, and how to do it. The short answer is that it is very difficult to guarantee reliability at low power in a point to point system.

Cellular

Cellular networks are almost ubiquitous, and our cell phones work almost anywhere. Obvious exceptions are remote areas where people often put industrial facilities, power plants, etc.

Many companies sell low-cost cellular modems which allow very low bit rate data communication at pricing well below traditional voice services. The power consumption of a cellular modem is much higher than what we'd expect from a typical mote radio, but for low-rate reporting (e.g. once per hour or less, as in utility meter reading) years of battery life are still possible. Latency for reporting urgent events can be quite low, since the cellular infrastructure is always listening.

Some of the challenges with cellular are the downstream latency, and the non-ubiquity of cellular coverage.

WiFi

WiFi enjoys some of the same benefits as cellular: nearly ubiquitous pre-existing powered infrastructure in many environments, and low cost access (zero if you own the

network). There is now a small industry growing up around low power WiFi for sensor networks, with companies like Gainspan and G2 Microsystems selling battery operated modules with years of lifetime.

Mesh

Let's see!

Case Studies & Examples:

Name	Make it catchy!	Industrial process monitoring
Traffic type(s)	• Regular collection to gateway(s) • Alarms/events to gateway(s) • Burst/batch to/from gateway(s) • Distributed/local-area processing	Regular collection Human query/response Alarms 50kB file upload
Data rate		1/s to 1/hour regular reporting
Scale	How many nodes? What different types? What geographic distribution?	10 to one thousand temperature, pressure, flow, etc. sensors in a metallic environment covering tens of meters to kilometers.
Topology, Spacing	1D, 2D, or 3D Regular, random, clusters, Min/mean/max separation between motes	2D and 3D random with clusters. 1m/20m/100m
Mobility	How many, how fast?	Wireless workers
Powered infrastructure	Is it available? Everywhere?	Occasional/sparse
Lifetime	How long, what batteries or other power supply?	3-10 years on C-cell lithium
Reliability	What fraction of the data needs to get through.	>90% to nine 9s.
Latency	Average? Upper bound?	Varies, from <1hour average to <100ms 99.9%
Security	Certification, encryption, integrity, authentication	Varies from "don't want it" to "if someone breaks in people could die"
Size/cost	Is there a magic number where the application becomes attractive? A lower limit below which it doesn't matter?	Anything under a deck of cards in size is fine. Cost < $100

Pharma

Industrial monitoring, w/ tank level control

Solar field monitoring

Home lighting

Commercial HVAC

RTLS/Asset tracking

Military: original smart dust vision

Problems

1. Pick an example application for wireless sensor networks, and fill in your own version of the table above.
2. You have purchased a wireless home security system. There's a box that plugs into the wall, your phone line, and your PC. You also picked 10 sensors from several different vendors that you will put around your house: open/close sensors on doors, open/break sensors on windows, and motion sensors. How much time and effort are you willing to put in to commissioning, security, and binding in this network? What would you want the user interface to look like?
3. What kind of reliability and latency would you want to see from a home security sensor network? What about a lighting control network (with wireless light switches and motion detectors)?