10 Years ago @ Berkeley

- Post-PC age had arrived
  - The Palm Pilot in hand, massive computing clusters in the infrastructure, and Bluetooth "any day now"

- Smart Dust “vision”
  - complete (albeit very limit) computing system in mm³ expected in 10 – 15 years

- The “Systems” Urgency
  - Only 10 years to get the systems & networking right!
  - Power profile of embedded PCs / Laptops / PDAs / Cells orders of magnitude off from where we needed to be.
  - None of the Mobile Ad Hoc networks worked, ...

- Results streaming in from the world beyond
  - Estrin PC104-WiFi Testbed
    - None of the beautiful networking ideas mattered because ALL the energy went into idle listening of 802.11 MAC.
  - Many researchers solving imaginary problems
The Mote Platform

A World of Systems and Networking
Reliable, Low-Power Wireless “Routing”

Communication Power – Passive Vigilance

- **Sleep**: ~10 µA
- **Transmit**: ~20 mA x 1-5 ms
  - [20 - 100 uAs]
- **Listen**: ~20 mA
- **Receive**: ~20 mA x 2-6 ms
3 Basic Listening Techniques

Goal: listen only when there is likely to be something useful to hear.

- **Listen during scheduled time slots**
  - Arrange a schedule of possible communication opportunities
  - Maintain appropriately coordinated clocks and schedule
  - Only listen during specific “slots”
  - Many variants: Token-Ring, TDMA, Beacons, Bluetooth piconets, ... TSMP, ...

- **Sampled Listening**
  - Listen for very short intervals to detect eminent transmissions
  - On detection, listen actively to receive

- **Listen after send (with powered infrastructure)**
  - Generally, device is not listening and will not receive.
  - After it transmits to a receptive device, it listens for a time window
  - Many variants: 802.11 AMAT, Key fobs, remote modems, ...

---

Meanwhile... in the internet
The Next few billion network nodes

THE Question
If Wireless Sensor Networks represent a future of “billions of information devices embedded in the physical world,... why don’t they run THE standard internetworking protocol?

Web Services
- XML / RPC / REST / SOAP / OSGI
- HTTP / FTP / SNMP
- TCP / UDP
- IP
- Serial
- Ethernet
- Sonet
- 802.11
- GPRS

Plugs and People
Self-Contained

RFM, CC10k, 802.15.4
The Answer

They should

- Substantially advances the state-of-the-art in both domains.
- Implementing IP requires tackling the general case, not just a specific operational slice
  - Interoperability with all other potential IP network links
  - Potential to name and route to IP devices within security domain
  - Robust operation despite external factors
    - Coexistence, interference, errant devices, ...
- While meeting the critical embedded wireless requirements
  - High reliability and adaptability
  - Long lifetime on limited energy
  - Manageability of many devices
  - Within highly constrained resources

Internet Standards

- The Internet Engineering Task Force (IETF), formed in 1986, “is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet”
- Layered architecture provides interoperability for diverse applications across broad and evolving communications technology
- Today: Half a billion to a billion IP hosts → demonstrated scale
Many Advantages of IP

- Demonstrated scaling (up, down, over time, technologies, applications)
- Extensive interoperability
  - Other wireless embedded 802.15.4 network devices (entire goal of Zigbee, …)
  - Devices on any other IP network link (WiFi, Ethernet, GPRS, Serial lines, …)
- Established security
  - Authentication, access control, and firewall mechanisms
  - Network design and policy determines access, not the technology
- Established naming, addressing, translation, lookup, discovery
- Established proxy architectures for higher-level services
  - NAT, load balancing, caching, mobility
- Established application level data model and services
  - HTTP/HTML/XML/SOAP/REST, Application profiles
- Established network management tools
  - Ping, Traceroute, SNMP, … OpenView, NetManager, Ganglia, …
- Transport protocols
  - End-to-end reliability in addition to link reliability
- Most “industrial” (wired and wireless) standards support an IP option

Long road toward sensor integration

- 1950: 4-20 mA “current loop”
  - Common signal wiring, ADC, and calibration
  - Vast diversity in excitation, configuration, interpretation
- 1980: HART (Highway Addressable Remote Transducer)
  - 1200 baud, half-duplex digital communication over 4-20 wiring
  - Rosemount proprietary protocol => “open” => Fieldbus
  - Fixed packet format for command / response
    » Process Variable, Host->Device Commands, Status & Diagnostic Alerts, Device Id, Calibration and Limits
- 1987: BACnet (Building Automation and Control Network)
  - RS232, RS485, ARCnet, ethernet, LONTalk, … BACnet/IP
  - Device = Collection of Objects; 23 “object types”
  - Data types, packet formats, and object defined in Abstract Syntax (ASN.1)
  - Protocol services, Data Sharing, Alarm and Events, Trending, Scheduling, Remote Device and Network Management
- 1994: CIP (Common Industrial Protocol)
  - Device Net (CAN), ControlNet, … EtherNet/IP
  - Devices as physical instances of classes.
  - Communication between objects is independent of physical links providing transport
  - Fixed binary encodings of data types, object types, classes
- 200x: Zigbee, ZWave, Wireless HART, SP100.11a, …
  - IEEE 802.15.4 radio …
**IP-Based Instrumentation and Control**

**Critical Success Factors**

- Application profiles
- Non-mixing profiles
- Local scope only
- Closed sub-system

- Monolithic stack
- Radio dependent
- Local scope only
- Not future proof

**Internet Architecture**

- Diversity and fast innovation in application services
- Reliability and scalability through protocol layering
- Coexistence and fast innovation in link technologies
- Diversity and fast innovation in device types

**Zigbee, …**

**Relationship to Industrial Interconnects**

- **BACnet**
  - RS-232 & RS-485 => IEEE 802.3 via BACnet/IP

- **LONworks**
  - Twisted Pair & Power Line => LonTalk/IP

- **Common Industrial Protocol (CIP)**
  - CAN & ControlNet => EtherNet/IP

- **SCADA**
  - Prop. RS-485 & Leased Line & Prop. Radios => ModBUS => Ethernet => TCP/IP

- **FieldBus**
  - Modbus, Profibus, Ind. Ethernet, Foundation HSE, H1, …SP100.11a?

In 2000, ODVA and CI introduced another member of the CIP family: EtherNet/IP, where “IP” stands for “Industrial Protocol.” In this network adaptation, CIP runs over TCP/IP and therefore can be deployed over any TCP/IP supported data link and physical layers, the most popular of which is IEEE 802.311, commonly known as Ethernet. The universal principles of CIP easily lend themselves to possible future implementations on new physical/data link layers. [The Common Industrial Protocol (CIP) and the Family of CIP Networks (Pub 123)]
But, …

• isn’t IP too heavyweight for low-power, wireless, microcontroller based devices?

• No!

• 6lowpan compression with high quality multihop routing
  – Reliability and lifetime of the best mesh
  – Interoperability of IP

Making sensor nets make sense

LoWPAN – 802.15.4
• 1% of 802.11 power, easier to embed, as easy to use.
• 8-16 bit MCUs with KBs, not MBs.
• Off 99% of the time
Key Factors for IP over 802.15.4

- **Header**
  - Standard IPv6 header is 40 bytes [RFC 2460]
  - Entire 802.15.4 MTU is 127 bytes [IEEE]
  - Often data payload is small
- **Fragmentation**
  - Interoperability means that applications need not know the constraints of physical links that might carry their packets
  - IP packets may be large, compared to 802.15.4 max frame size
  - IPv6 requires all links support 1280 byte packets [RFC 2460]
- **Allow link-layer mesh routing under IP topology**
  - 802.15.4 subnets may utilize multiple radio hops per IP hop
  - Similar to LAN switching within IP routing domain in Ethernet
- **Allow IP routing over a mesh of 802.15.4 nodes**
  - Options and capabilities already well-defined
  - Various protocols to establish routing tables

IEEE 802.15.4 — The Low Power Wireless Link Standard

- **Low bandwidth (250 kbps), low power (1 mW) radio**
- **Moderately spread spectrum (QPSK) for robustness**
- **Small packets for lower error rates and media sharing**
- **Simple MAC allows diversity of networking protocols**
  - TinyOS-based protocols (MintRoute, LQI, BVR, …), TinyAODV, Zigbee, SP100.11, Wireless HART, …
  - New recommended choice for interoperability: IP with 6LoWPAN
- **HW choice now available with many semiconductor suppliers**
6LoWPAN: IPv6 over IEEE 802.15.4

- Deep compression by breaking the layering abstraction and putting it all back together again.

6LoWPAN – Format Design

- Orthogonal stackable header format
- Almost no overhead for the ability to interoperate over radio
- Pay for only what you use

IEEE 802.15.4 Frame Format

IETF 6LoWPAN Format

Uncompressed IPv6 address [RFC2460] 40 bytes

Fully compressed: 1 byte

Source address: derived from link address
Destination address: derived from link address
Traffic Class & Flow Label: zero
Next header: UDP, TCP, or ICMP

Mesh (L2) routing

Message > Frame fragmentation
What’s the energy Cost?

Energy Cost of Packet Communication vs. Data Size

- Global Internet Scope: Overhead < 20%
- Pay when needed!

Leverage what doesn’t need inventing

- RFC 768 UDP - User Datagram Protocol [1980]
- RFC 791 IPv4 - Internet Protocol [1981]
- RFC 792 ICMPv4 - Internet Control Message Protocol [1981]
- RFC 862 Echo Protocol [1983]
- RFC 1101 DNS encoding of network names and other types [1989]
- RFC 1191 IPv4 Path MTU Discovery [1990]
- RFC 2131 DHCPv4 - Dynamic Host Configuration Protocol [1997]
- RFC 2375 IPv6 Multicast Address Assignments [1998]
- RFC 2460 IPv6 [1998]
- RFC 2463 ICMPv6 - Internet Control Message Protocol for IPv6
- RFC 2765 Stateless IPv6/ICMPV6 Translation Algorithm (SIIT) [2000]
- RFC 3068 An Anycast Prefix for 6to4 Relay Routers [2001]
- RFC 3307 Allocation Guidelines for IPv6 Multicast Addresses [2002]
- RFC 3315 DHCPv6 - Dynamic Host Configuration Protocol for IPv6 [2003]
- RFC 3484 Default Address Selection for IPv6 [2003]
- RFC 3587 IPv6 global Unicast Address Format [2003]
- RFC 3819 Advice for Internet Subnetwork Designers [2004]
- RFC 4007 IPv6 Scoped Address Architecture [2005]
- RFC 4193 Unique Local IPv6 Unicast Addresses [2005]
- RFC 4291 IPv6 Addressing Architecture [2006]
- And --- in RFC4944 - "Transmission of IPv6 Packets over IEEE 802.15.4 Networks"
Connecting IP Networks to Wireless Embedded Devices

RFC 4944: 6LoWPAN (IPv6 for Low Power Wireless Personal Area Networks) Adapts full-fledged IPv6 to run over embedded wireless networks

IP Devices Directly Configure and Control Embedded Nodes
Embedded Nodes Send Data to Servers Across IP Networks

IP Firewalls and Security Models are Understood and Proven

128-Bit AES Link-Layer Encryption

LoWPAN-Extended IP Network

IP/6LoWPAN Border Router

IPv6/6LoWPAN Sensor Router

IPv6/6LoWPAN Border Router

IP Network (powered)

IP Device

Internal Firewalls

Border Firewalls

IP Network (powered)
Embedded IP Gives You a Choice: Proxies and Routers

Sensor Node

Proxy Gateway Server

Router

Web, HTTP, XML, SNMP, SMS, Email

Ping, Telnet, Sockets
TCP, UDP, ICMP
IPv4, IPv6
Ethernet, WiFi

IP6LoWPAN

Proxy Gateway Server

Sensor Node

Embedded IPv6 programming

sockaddr_in6_t m_dest;
uint8_t m_buf[BUFLEN];
call IPv6Addresses.pton( "fd01::1234", &m_dest.sin6_addr );
m_dest.sin6_port = 2724;
call UdpSend.sendto( m_buf, BUFLEN, &m_dest );

event void Tcp.connected() {
    call Tcp.send( m_buf, BUFLEN );
    call Tcp.close( TRUE );
}
What it means for you

• Reliable, low-power forwarding on 802.15.4 links now understood and demonstrated
  – Requires attention to detail, Continuous monitoring of link quality
  – Multiple forms of diversity (temporal, spatial, frequency)
  – Requires retransmission, rerouting, …
  – With radios off 99.5% of the time

• None of these issues are dictated by the “application profile”
  – HART, BACNet, Zigbee, … XML, …

• Wireless sensor networks are “not an Island”
  – Work with other networks, other kinds of devices
  – Cannot afford to return to the N^2 problem

• Internet architecture allows link technology and applications to improve
  – additional defensive measures for reliability in the face of change and imperfection

• Allows vast body of existing tools and standards to be applied to Wireless Sensor Networks

• Just one more member of the family