CS144r/244r
Network Design Project
on
Secure and Intelligent Internet of Things
(iot networking)
2/26/2014

Instructor: Professor HT Kung
Harvard School of Engineering and Applied Sciences
Announcements

• Questions for next Monday’s class will be posted Saturday evening
  – Readings will be posted on Friday evening
• On March 12, Dr. Trevor Blackwell will give a guest lecture on hardware startups and robotics programming
• For course projects, students should do their best in coming up something interesting with intellectual content. Try to address one or more of the following aspects: sensing, machine learning, security, programming and novel application ideas
• This Friday from 10am-11:30am we will have an open session to discuss project ideas you may have. This will be non-mandatory meeting for informal discussion. The meeting location will be posted
• For those teams who need parts to be ordered, please let TFs know
• As said before, various labs/companies are hiring for summer interns. We will post some information Friday
**What Is New in the News?**

- **“Try Radar for Your Next Project”** (2/24/2014)
  - ... The low-end stuff that we can get our hands on usually suffers from poor range, lack of sensitivity, and no way to characterize what the target is. But today we can use the good stuff that, until recently, was only available to military: radar...Few off-shelf small radar options exist as of today
  
  - See [http://hackaday.com/2014/02/24/guest-post-try-radar-for-your-next-project/](http://hackaday.com/2014/02/24/guest-post-try-radar-for-your-next-project/)

- **“Can We Secure the Internet of Things?”** (2/25/2014)
  - Since the bad guys are already way out in front of the good guys today, why discuss the implications of future technologies?
  - Abraham Lincoln once said, “You cannot escape the responsibility of tomorrow by evading it today.”
Recap: Inertial Sensors

Widely used MEMS inertial sensors

• Accelerometers
  – Measure **acceleration** in x, y, directions

• Gyroscopes (or simply, gyros)
  – Measure **angular velocity** in yaw, pitch and roll directions

They complement each other in sensor fusion
Recap: Recognize a Gesture in a Set

• A user provides one template gesture for each of the eight vocabulary gestures offline (actually two templates are kept for each gesture; see the last slide of this lecture)

• Then online the user gives a sample gesture. Based on Dynamic Time Warping (DTW) The system will match the sample against the eight stored templates, and find the best match

The Nokia vocabulary of eight simple gestures:

The dot denotes the start and the arrow the end
Recap: Machine Learning Basics

• Supervised learning
  – Prediction
    • Linear regression
    • Polynomial curve fitting
  – Classification
    • Decision tree
    • Logistic regression
    • SVM

• Unsupervised learning
  – K-means
  – Gaussian mixture model

Generally speaking, supervised learning methods require ground-truth samples. Otherwise they are unsupervised
Recap: IoT Programming

- IoT has become interesting in recent years mainly because of new perspectives in networking and software components.
- With cloud and web, devices can provide services over the network.
- With Rest API, JavaScript (Nodejs), Web socket and HTML, we can readily do IoT programming.
- We can use event-based call back upon blocking. This can avoid complex multi-thread programming.
Today’s Topic: IoT Networking

• Long-term vision
  – All Things (sensors/actuators with microcontrollers) will connect to the Internet using Internet Protocols (IP), perhaps via gateways
  – Existing sensors will be joined by many, many, millions more, so that anything worth measuring can be measured ... and then managed

• For such scaling, we must re-think about IP based networking. This is the topic we will discuss today

• We will follow the current thinking of IETF in this area under the IPv6 framework, i.e., 6LoWPAN for constrained networks and RPL for their routing. (Note that IPv6 addresses are 128 bits long!)
Talking About Scale, In Addition to Sensors We Have Covered So Far, We Have Barcode, RFID and NFC

- **Universal Product Code (Barcode)**
  - Also 2D Quick Response Code (QR code)

- **Radio-frequency identification (RFID)**
  - ~5 million 802.15.4 RFICs per month
  - Volumes are now increasing in an exponential fashion due to the installed bases including smart meters

- **Based on RFID, Near Field Communication (NFC) standards cover communications protocols and data exchange formats for two-way communication between endpoints in proximity of few inches. It has been used in devices such as Google Nexus**

![Barcode Image](image1)

![RFID Chip Image](image2)

![NFC Image](image3)
How To Look At IoT Connectivity

• Lots of sensors to be connected
• They need to be stand-alone, communicate wirelessly and can go years between battery replacements (or are "scavenger-class" devices that work on solar or wind power)
• There are hundreds or more wireless networking standards on network edge
• A general and generic way of looking at IoT communication at large scale is to treat it as a routing problem
• This means interoperating with traditional IP routing, and even better, leveraging the existing and future IP infrastructure (naming, addressing, security, management, etc.). But how?
High-level Review of the Internet

• The Internet is composed of local area networks (LANs) and wide area networks (WANs)

• On a LAN, packets are sent over a broadcast domain (e.g., Wi-Fi, Ethernet, 802.15.4 and DOCSIS) to reach a default IP gateway, and then IP routing is used to route packets over WANs
We have been working on low-layer protocols for a decade or longer. New opportunities and challenges are mostly at higher layers for the purpose of connecting billions of devices on numerous heterogeneous edge networks.
IEEE 802.15.4: An Example of Lower-Layer Protocol Standard

- IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs)
- Several standardized and proprietary networks (or mesh) layer protocols run over 802.15.4-based networks, including IEEE 802.15.5, ZigBee, 6LoWPAN, WirelessHART, and ISA100.11a
# Wireless Solutions

## Supported standards

<table>
<thead>
<tr>
<th>13.4KHz / 13.56MHz</th>
<th>Sub 1GHz</th>
<th>2.4GHz to 5GHz</th>
<th>Satellite</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID NFC ISO14443A/B ISO15693</td>
<td>SimpliciTI 6LoWPAN W-MBus</td>
<td>SimpliciTI PurePath Wireless</td>
<td>ZigBee® 6LoWPAN RF4CE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Wi-Fi</td>
</tr>
</tbody>
</table>

## Example applications

![Wireless Solutions](image-url)
## Wireless Links

<table>
<thead>
<tr>
<th></th>
<th>802.15.4</th>
<th>802.15.1</th>
<th>802.15.3</th>
<th>802.11</th>
<th>802.3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Class</strong></td>
<td>WPAN</td>
<td>WPAN</td>
<td>WPAN</td>
<td>WLAN</td>
<td>LAN</td>
</tr>
<tr>
<td><strong>Lifetime (days)</strong></td>
<td>100-1000+</td>
<td>1-7</td>
<td>Powered</td>
<td>0.1-5</td>
<td>Powered</td>
</tr>
<tr>
<td><strong>Net Size</strong></td>
<td>65535</td>
<td>7</td>
<td>243</td>
<td>30</td>
<td>1024</td>
</tr>
<tr>
<td><strong>BW (kbps)</strong></td>
<td>20-250</td>
<td>720</td>
<td>11,000+</td>
<td>11,000+</td>
<td>100,000+</td>
</tr>
<tr>
<td><strong>Range (m)</strong></td>
<td>1-75+</td>
<td>1-10+</td>
<td>10</td>
<td>1-100</td>
<td>185 (wired)</td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>Low Power, Large Scale, Low Cost</td>
<td>Cable Replacement</td>
<td>Cable Replacement</td>
<td>Throughput</td>
<td>Throughput</td>
</tr>
</tbody>
</table>
Choosing the Right Technology

**Range**

- Zigbee
- RF4CE
- BLE
- WiFi
- Bluetooth
- 2.4GHz Proprietary
- Sub-1GHz

- Range (m)
  - 10
  - 100
  - 10,000+

**Throughput**

- 20 Mbps
- <2 Mbps
- <250 kbps

**Technology**

- WiFi
- BLE
- Zigbee
- RF4CE
- Sub-1GHz
- Bluetooth
- 2.4GHz prop

**Typical power source**

- Li-Ion
- AAA
- Coin Cell

- BLE
- Sub-1GHz
- 2.4GHz Proprietary
- Zigbee
- RF4CE
- Bluetooth
- WiFi

**Typical Topology**

- Mesh
- Star
- P2P

- Zigbee
- Prop Sub 1Ghz, Prop 2.4Ghz
- WiFi, Bluetooth
- RF4CE
The “Internet of Things” Three Major Hubs

- **Mobile Hub**
  - Bluetooth®
  - Bluetooth low energy

- **Wi-Fi Access Point**
  - Wi-Fi

- **Mesh Gateway**
  - ZigBee®
  - 6LoWPAN
  - 802.15.4
  - Sub-1GHz
The Real Challenge With IoT Networking Is Related to Its Large Scale

• A flat LAN that supports broadcasting cannot work for thousands of sensors. This means that we will need to segment LAN perhaps using IP routing

• To conserve energy, power-constrained sensors cannot communicate most of the time. They must wake up infrequently to send/receive data

• Wireless communication is subject to signal attenuation (strength $\propto \frac{1}{\text{distance}^2}$ in free space or $\frac{1}{\text{distance}^3}$ on the ground). In addition, there are radio interferences. For example, you cannot transmit and receive at the same time

• Bandwidth for a wireless spectrum is much smaller than that of wirelines. It cannot afford control protocols which require frequent route updates

• Wireless networking is lossy for good reasons such as allowing lowered transmit power to reduce interference

• Must be self-managed (auto-discovery, self-organizing networks), and live with many wireless standards

• Node mobility and node disconnect make things even more challenging
A Direction Under IETF Study: Destination Oriented Directed Acyclic Graph (DODAG) Networks

• A DAG is formed by a collection of vertices (nodes) and edges (links), each edge connecting one node to another (directed) in such a way that it is not possible to start at Node X and follow a directed path that cycles back to Node X (acyclic)

• A Destination Oriented DAG (DODAG) is a DAG that comprises a single root node

• Under DODAG routing and traffic management is much simplified. 6LoWPAN uses an adaption layer (layer 2.5) to support fragmentation and header compression
A DODAG is a simple hierarchical model. Any DODAG has only one “gateway” referred to as the root, is number one in the hierarchy. Anything that finds itself with a direct path to the root has Rank 2. Anything that can only see Rank 2 devices is a Rank 3 device, and so on.

Sensor nets may have different performance and security requirements. For example, sensors which merely ambient temperature don’t need not be treated the same as medical sensors.

The rule by which the DODAG is built is called the **Objective Function**.
Sampled Listening with Optimization

- Receiver monitors the channel using short periodic receive checks to determine if a neighboring node is currently transmitting.
- A node transmits frames by first transmitting a wakeup signal at least as long as the receiver’s sample period.
- By **learning neighbor’s sample schedules**, a node can nearly eliminate the need for wakeup signals. If the destination’s schedule is known, the wakeup signal is reduced to a small synchronization guard time, as shown.
Node Objects

- The *Node State and Attributes Object* – nodes can signal whether they have capacity to pass messages (the “A” flag, for available) or not (“O” flag, for overloaded)
- The *Node Energy Object* – indicating whether the node is on mains power, battery power, or “scavenger” power (solar or wind), along with flags to indicate remaining power, and whether this node can be included in networks
- The *Hop Count Object* – which is either a metric (how many hops) or a constraint (maximum number of hops).
Link Objects

- The *Throughput Object*;
- The *Latency Object*
- The *Link Reliability Object*
- The *Link Colour Object* – for user-selectable link characteristics
Use of Object Functions to Build DODAG

• The upshot of applying these object functions to the job of building the DODAG is that the table doesn't only reflect physical topology

• The DODAG might reflect rules such as “avoiding overloaded nodes”, or “try to find nodes connected to AC power” by using the following objects:
  – Avoid overloaded nodes;
  – Prefer ac-powered nodes over battery-powered nodes

• Vendor latitude: Vendors may create their own OFs, and bake them into devices at manufacture. When installed into a network, a device would determine if its OF is available – and if not, it will simply default to the default Objective Function (OF)
Summary

• The central issue for IoT networking is scaling
• Good work has been done over the years for local networking at lower layers
• An exciting new area of investigation is about how to connect millions of these local networks or devices at the network layer
• The IETF DODAG work based on IPv6 offers a promising approach to achieving such scaling