Wireless Sensor Networks Standards & Case Study

Prof. John McLeod

ECE9047/9407, Winter 2021

This lesson briefly introduces some standards and protocols for wireless communication in WSNs. This is hardly an exhaustive list, and may not even represent the dominant protocols in use today — this is a rapidly developing area and finding up-to-date information is difficult. Also, I am lazy. This lesson concludes with an example WSN used for habitat monitoring on "Great Duck Island". However, contrary to what you may think from the name, the actual animal monitored by the WSN is not a duck, but a petrel.

Wireless Communications Standards

It is almost certain that all of you use wireless communication every day, and probably all day too. There are lots of different kinds ofwireless networks — far too many to list here — but the ones most people are familiar with are not particularly well-suited for WSNs. Consider 3G, 4G, and LTE cellular networks, for example, or the IEEE 802.11 standard for WiFi, to name but a few. These networks tend to emphasize **data transmission speed**, [1] because people want stare at their phones to watch videos of people walking blindly into fire hydrants and telephone poles, while they themselves are walking outside. A typical UART serial connection may run a $96\,\mathrm{kbit/s}$, for example, while the twenty-year-old 3G network can (theoretically) reach $2\,\mathrm{Mbit/s}$. [2]
Communication speed isn't a bad thing for WSNs, but the priority is on reducing power consumption. This usually requires sacrificing transmission speed, and more importantly using specialized networks that use simplified communications protocols that minimize the amount of non-data bits in the **communications frame**.
Compared to WiFi and cellular networks, WSN communication is often over a much shorter range, significantly less data is transmitted, and data is only transmitted in occasional bursts.

[1] Really this is the same as the **baud rate** previously discussed for serial communications, but the term "baud" seems to have fallen out of favour in high-speed networks.

[2] And more recent updates to 3G claims to have even faster speeds, but I have yet to see them in Ontario.

IEEE 802.15.4

IEEE 802.15 is a broad collection of standards related to wireless personal area networks (WPANs). Within this broad group, **IEEE 802.15.4** is a standard for low-power WPANs (LP-WPAN).

- This standard commonly uses part of the same $2.4\,\mathrm{GHz}$ band used by typical WiFi, with 16 channels available. In North America the $902\,\mathrm{MHz}$ to $928\,\mathrm{MHz}$ band is also available for LP-WPAN, with 30 channels available, other areas may have different bands available.

- Transmission is typically at $250\,\mathrm{kbit/s}$ over a range of $10\,\mathrm{m}$. Often even lower transmission speeds are used.

- This standard defines two broad types of nodes: **full-function devices** (FFDs) which can communicate with each other and relay information in a multi-hop communication path, and **reduced-function devices** (RFDs) which can only communicate to a FFD.

This standard uses four basic **communications frames**: data, acknowledgements, beacon, and command. The data and acknowledgements frames should be self-explanatory. The beacon frame is used to synchronize sender and receiver hardware, while the command frame is used to identify the destination node for the transmitted data. If a FFD node is designated the network controller, it has the ability to set up *superframes*, wherein a given node can transmit 16 consecutive frames.

The **IEEE 802.15.4** standard uses **carrier-sense multiple access with collision avoidance** (CSMA/CA) for determining when a node is able communicate on the shared network. Compared to wired communications standards (like I^{2}C or the IEEE 802.3 standard used by ethernet), ensuring that only one device in a multi-node network is using the communications channel at a time is inherently problematic. [3] There are two main reasons for this, the first is the **hidden node problem**.

- Over a wired network, every device is aware of every other device: any device can communicate with any other device physically connected to the wired network.
- On a wireless network, the **hidden node problem** makes it possible (even probable) that some nodes will be "hidden" from each other. Two nodes may be in communication range of a hub, for example, but out of communication range from each other.

In the wireless network, there is no way for a given node to know what any other hidden nodes are doing, so it is impossible for that node to tell if the communications channel is free. The second major problem with wireless communications is from **signal attenuation**.

- Over a wired network, every device can accurately monitor the communications channel while transmitting, and the network will have roughly the same voltage at all points along the wire.

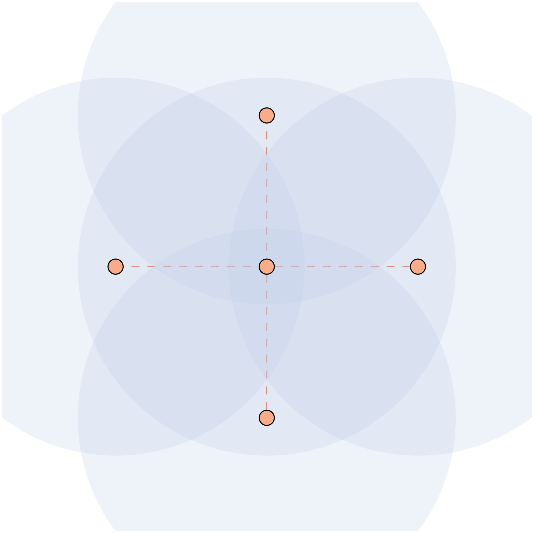

Figure 1: The **hidden node problem** in a star-topology WSN. All peripheral nodes can communicate with the central node, but none of the peripheral nodes are in communications range with each other.

[3] Ethernet uses the stronger **carrier-sense multiple access with collision detection** (CSMA/CD) method, for example.

A good wired communication protocol and hardware will prevent a short-circuit from occurring if one device tries to force the channel to high voltage simultaneously when another device is trying to force the channel to low voltage, so a node attempting to communicate on the channel can always simultaneously monitor that channel to see if it is carrying the correct signal.

- On a wireless network, the signal transmission strength **attenuates**, or decreases in strength, with increasing distance from the transmitting node.

Therefore, a wireless node cannot effectively monitor and transmit simultaneously, because its own transmission will always be much stronger than any other node's transmission. Even if a second node is not hidden, if both nodes start communicating at the same time they will be unaware of the interference in the channel. Only a third node can detect this communications overlap, and that third node will have to wait until the channel is clear again to inform the other two nodes of the problem.
The CSMA/CA method addresses these problems by having nodes exchange a **request-to-send** (RTS) and **clear-to-send** (CTS) signal before communicating their main data packet.

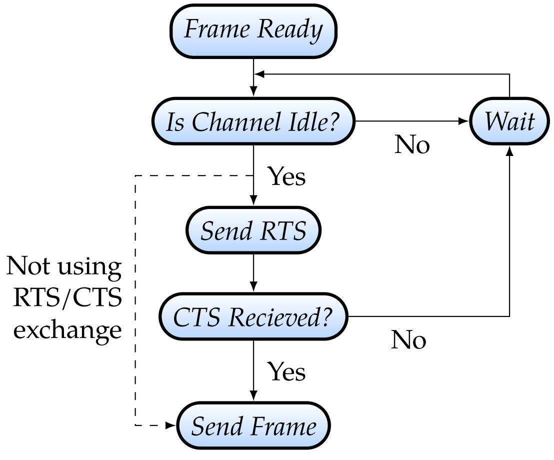

Figure 2: Simplified CSMA/CA process.

- When a node wants to communicate, it first listens to the channel to see if it is idle. [4]

- If the channel is clearly not idle, the node waits a while and listens again.

- If the channel appears idle, the node transmits a simple data frame containing a RTS.

[4] As discussed above, this does not guarantee the channel actually *is* idle due to the **hidden node problem**.

- If the destination node transmits a CTS back, then the channel is actually idle and the other node is available to receive the data. If no CTS is received, the node waits and tries again.

- Without a RTS/CTS exchange, the node would just transmit the data on the apparently idle channel and hope for the best. This always runs the risk that the data will be silently lost.

As implemented, **IEEE 802.15.4** only provides a basic framework for LP-WPANs. Many other standards, such as **Zigbee**, **ISA100.11a**, **WirelessHART**, **MiWi**, **6LoWPAN**, **Thread** and **SNAP** build off **IEEE 802.15.4** to provide a more functional standard for WSNs. Of all the **IEEE 802.15.4** standards, I will only briefly discuss **Zigbee** here.

Zigbee

As mentioned above, **Zigbee** is a communications standard based on IEEE 802.15.4. **Zigbee** is also the name of the hardware associated with this standard. **Zigbee** is designed for ad-hoc wireless networks with particular emphasis on low-power nodes, making it a good standard for WSNs. [5] A **Zigbee** network has the following characteristics:

- Short range communications. The maximum communication range under ideal conditions with increased power is around $100\,\mathrm{m}$, but the typical communications range for power-efficiency in real-world conditions is $10\,\mathrm{m}$.
- Uses the $2.4\,\mathrm{GHz}$ band. [6] Low-power transmissions at these frequencies have poor penetration depths, so reliable communications channels usually need to be line-of-sight, or through thin internal walls.
- Natively uses $128\,\mathrm{bit}$ encryption.
- Can be configured as a **beacon** network, where all devices idle in a low-power mode except for scheduled transmission periods. During these periods, nodes ready to receive transmissions will periodically transmit a beacon frame.

Zigbee networks are usually heterogeneous. There are three standard types of Zigbee hardware, depending on the requirements of the nodes. Of course, a Zigbee network does not necessarily have to

[5] Other variants of IEEE 802.15.4 are designed for smart devices and the "internet of things" (IoT), where transmissions do tend to be low-power, but optimizing power efficiency is less of a priority.

[6] Sometimes Zigbee devices are available for the other, country-specific IEEE 802.15.4 bands (like the $\sim\ 900\,\mathrm{MHz}$ band in North America), but these are rare.

be heterogeneous — every node can have fully functional hardware even it if does not self-configure to use that full functionality — but there is a savings in terms of both money and operating power efficiency by using a heterogeneous network.

- Every network needs a Zigbee coordinator (ZC) to act as a controller. ZC devices can communicate directly with other nodes, and can also act as relays.

- As each network should have only one ZC device, Zigbee routers (ZRs) can also communicate directly with other nodes and also act as relays.

- Zigbee end devices (ZEDs) can only communicate directly with other nodes (presumably a ZR or ZC, unless your network is really small). ZED hardware is comparatively cheap, with limited functionality.

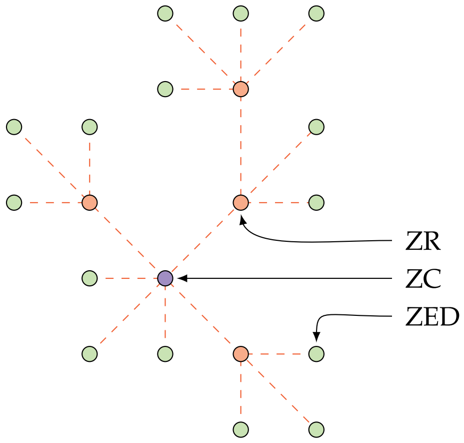

Figure 3: An example Zigbee network.

Once a Zigbee network is deployed and configured, transmissions can be relayed through ZR or ZC devices using just the Zigbee hardware, bypassing the node microcontroller. Because of this, ZR and ZC hardware includes on-chip memory for temporarily storing transmission data, this is one of the reasons why they are more expensive than ZED hardware. ZED nodes are also inherently more power efficient than ZRs and ZCs — they can typically have their transmitters turned off unless they want to send some data. ZRs and ZCs must keep monitoring the channel if the network is non-beaconed. Furthermore, even if the network is beaconed, ZRs and ZCs must regularly transmit beacon frames during the scheduled transmission times.

Bluetooth Low Energy

Most of you are probably familiar with **Bluetooth**, another WPAN technology in the 2.4 GHz band. **Bluetooth** is also a short-range network, again typically 10 m. However **Bluetooth** itself is not suitable for a WSN, as it typically is restricted to paired devices.

Bluetooth Low Energy (BLE) is an extension of the Bluetooth protocol that simplifies mesh communication between many BLE-enabled devices. BLE tends to have lower data transfer rates than regular Bluetooth. As the name suggests, BLE has lower power consumption than regular Bluetooth.

In previous years students used a BLE design kit as part of the laboratory component, but alas! That is not your fate. [7] Still, if you want to try building your own WSN or IoT-device, the BLE design kits are a good place to start: these kits are fairly cheap and have a reasonably user-friendly IDE.

- The manufacturer's website is here: www.cypress.com.
- Digikey sometimes has these kits as well (but seems to be out of stock right now), see here: www.digikey.ca.

There is a nifty phone app so you can interact with the BLE board using your cell phone.

[7] Honestly, the main reason why we don't use the BLE kit this year is because I don't know enough about it to design good labs. Otherwise I would have gone ahead and forced you to buy them!

Z-Wave

The final LP-WPAN protocol we will examine is **Z-wave**. This uses frequencies around 900 MHz, with the exact frequency being region-dependent. Consequently, **Z-wave** has a somewhat larger range than 2.4 GHz-based networks. The trade-off is lower data rates. A **Z-wave** network has the following characteristics:

- Typical communications range for power-efficiency in real-world conditions is 30 m, with increased power a 100 m range is possible.
- Typical transmission data rates are 40 kbit/s, the max data rate under ideal conditions is 100 kbit/s.
- Natively uses 128 bit encryption.

There is only kind of **Z-wave** hardware, allowing **Z-wave** networks to be naturally homogeneous. Of course, a Z-wave network can still be heterogeneous if different microcontroller or sensor hardware is used in different devices.

- One or more nodes will be designated as a controller (one primary, possibly several secondary, depending on the size of the network) during network deployment.
- Each node can communicate directly with other nodes and also act as relays.
- The network features automatic, active signal relaying, but only with a maximum of 4 hops.

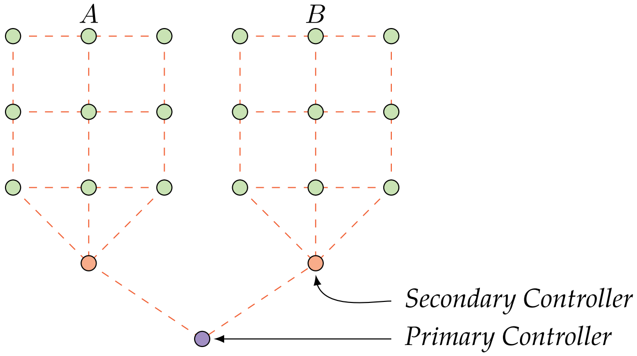

Figure 4: Example of a Z-wave network. Regular node A cannot communicate with regular node B using the communication channels shown, because they are 8 hops away from each other. Of course, depending on how the microcontrollers are programmed, A could communicate *indirectly* with B by communicating with its secondary controller, and including the instruction to pass the message on in the transmission.

Case Study

A neat case study of WSN for habitat monitoring is the 2003 deployment of **Mica** sensor nodes developed by UC Berkeley to Great Duck Island of the coast of Maine. The goal of this study was to determine nesting site selection and behaviour of Leach's Storm Petrels.

- These birds make nests and raise their young in underground burrows. Large flocks of birds form a nesting colony together.
- While incubating eggs or tending their young, adult birds only leave their burrows at night.
- While nesting, these birds are very sensitive to human interference and have been known to desert their colonies *en masse* if disturbed during the first week or so of nesting, and human interference leads to higher mortality among chicks.

Because Leach's Storm Petrels nest in relatively fixed areas (returning to the same set of burrows year after year), a WSN is a good way to non-invasively monitor the colony. The WSN was deployed before the start of the nesting season, and had to operate without servicing or replacement for at least 7 months.

- This WSN used an early version of the Berkeley **Mica** sensor node, powered by two AA batteries.
- The WSN was a **two-tiered heirarchical network**.

- The WSN used a combination of wireless technologies: WiFi and a custom 916 MHz wireless signal.

- The custom 916 MHz wireless signal was used to connect sensor nodes together and to the local hubs. One sensor node in each cluster had an larger external antennae to boost communication range to the hub.

- The local hubs were small computers, with large battery packs and solar panels. These connect to the primary hub using standard IEEE 802.11 WiFi.

- Each sensor node had six sensors: a light sensor, a humidity sensor, an atmospheric pressure sensor, and four different types of temperature sensor.

The WSN was deployed before the nesting season. 60 sensor nodes were deployed in existing burrows, approximately the same number were deployed on the surface. The study was reasonably successful, and the WSN was modified and expanded for a few years.

Reference: A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensors for Habitat Monitoring". *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 88–97 (2002). DOI:10.1145/570738.570751.

Reference: J. Anderson, "Micro- and Macro-Habitat Selection in Breeding Leach's Storm Petrels", poster at unknown conference, College of the Atlantic. Link: www.coa.edu.