WIRELESS TECHNOLOGY INFILTRATION INTO HVAC AUTOMATION

Wireless networks are everywhere in 2014. I have on my person 3 wireless networks happening at any given moment (4G LTE, Bluetooth, and Wi-Fi). I am a walking source of radio everywhere I go. And this is only the beginning. As more wireless devices proliferate for personal and commercial use, the spectrum will only grow more crowded and complicated. Are you prepared as wireless technology penetrates the HVAC automation market? Do you understand how radio propagates with respect to data and networks? I hope to scratch the surface and share some of this with you in the following paragraphs.

The Spectrum and Adoption in HVAC Applications

Wireless networks have to contend with many points of failure. To communicate a set of standard radio frequencies are established (sometimes called channels) and every device of the same type will use the same set of channels. Because HVAC automation isn't a big enough industry to which a chunk of the limited radio spectrum is dedicated, most devices piggyback on existing wireless standards. There are two major wireless technologies currently being utilized in this arena – zigbee and enocean. Others include Bluetooth, Wi-Fi and Z-Wave.

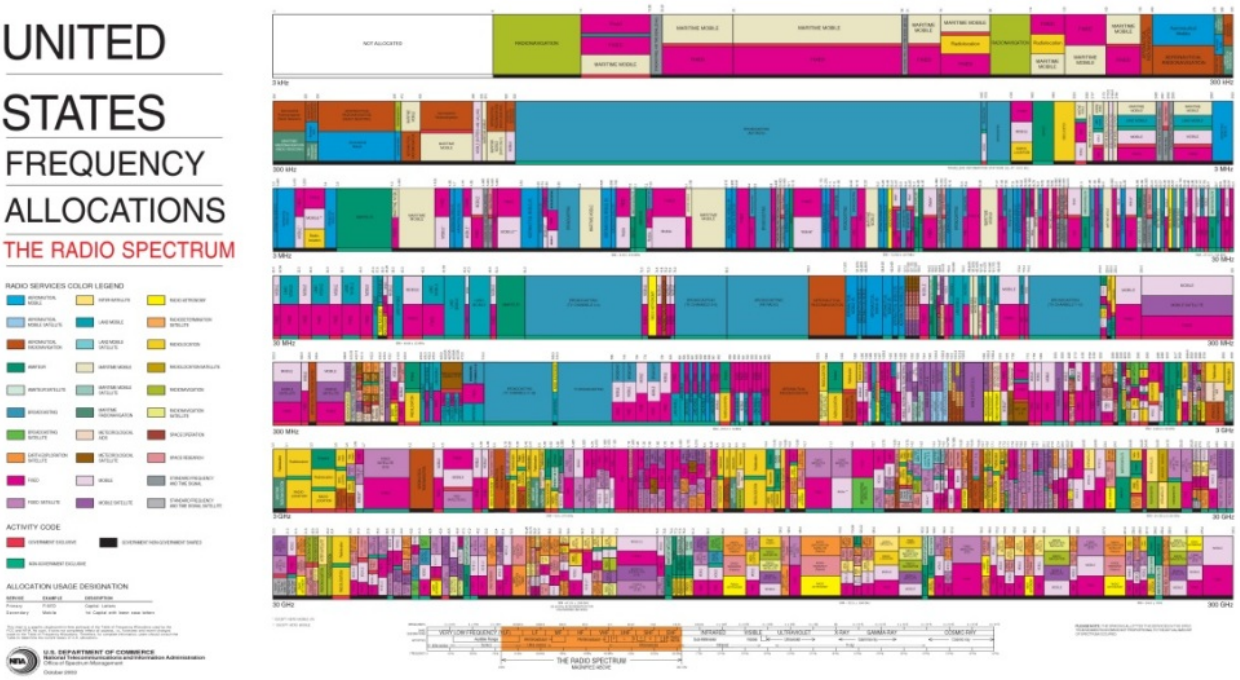


Image by US Dept. Of Commerce

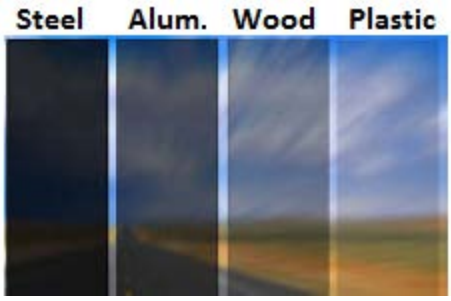
Zigbee is starting to see widespread adoption in the HVAC Controls market, and is already adopted in the smart meter market. So HVAC controls and Smart meters will be sharing the same channels, for two different applications. Scale out for the next 10 years, and add the Internet of Things to the mix, and you'll start to be able to predict how flooded with data these channels will become thus reducing throughput over time (even if there are some mechanisms built in to handle noisy channels).

Steep Learning Curve for Controls Contractors

A challenge presented by the adoption of wireless protocols in HVAC applications is that at present many controls contractors don't have formal training or experience with understanding how radio works, and expect it to 'just work.' The specifics of how radio works can be complicated, so I run through the same mental exercise when I teach people how to think about radio in simpler terms:

A Glass World

Imagine everything in the world was made of clear glass. Now imagine that all sources of radio are bright light bulbs. All communication is done via Morse code over the light bulbs through the glass (Morse code being analogous to software protocols like BACnet or Modbus). In our glass world, materials like aluminum, wood, sheetrock, and plastic are like tinted glass with various shades of darkness to them. Ferrous metals are such a dark tint of glass that they barely allow any light through. Take a moment and look around you, at the materials with which your building is constructed and think of how they might look in their various shades of tinted glass.



To send messages you want to see the light bulbs blinking with the greatest clarity. The preference then becomes that you try not to shine through any glass at all (hence line of sight). If you can't have line of sight, you'd want to make sure the barriers between you and the source are of the lightest tint possible and the distance is as short as needed per your bulb's brightness. Again, these are all factors to consider that affect throughput.

Security Issues

Now let's talk security. What happens if you look through your building to your neighbor's building? You can see all their communications; albeit slightly less bright as there are more barriers that the light needs to penetrate. This could give you the ability to snoop in on what is being said doesn't it? Let's take it one step further.

Philip Johnson's Glass House. Photo by Flicker user stewedpeas

Remember in this analogy, you, the person in this glass world, are the computer. The thing we might take for granted is our human ability to apply filters to unexpected data received. But computers need to be told what to accept and what to ignore. Using this train of thought, you can imagine how easy it might be to listen in or hack your neighbor in this glass world. Simply point your light bulb towards your neighbor (as close to them as possible) and tap out …. . .-.. .-.. — ("hello"). You might be surprised how easily you get a response. This is what hackers do all the time to probe unsecured wireless networks.

"Wardriving" – looking for unsecured networks. Photo by Flickr user groov3.

Wireless Technology Infiltration into HVAC Automation: Convenience With a Price

Wireless is a great convenience, but it can come at a cost. I have only scratched the surface of a multi-layered and sophisticated technology. As you consider wireless technology for your building's systems, don't let the issues of security, reliability, and throughput fall by the wayside. You should also always compare the cost of wireless against what it would cost to run a wire. Done correctly, a wireless BMS system can provide excellent service and convenience. But sometimes it's worth the extra cash just to keep your security exposure profile down and possibly increase the reliability of your BMS System.

Source : http://buildingenergy.cx-associates.com/2014/12/wireless-technology-infiltration-into-hvac-automation/