Trane Air-Fi Security and Interference

The Trane Air-Fi system uses Wireless Communication Interface (WCI) modules to form the mesh network. The Trane WCI modules are certified as ZigBee Building Automation (ZBA) devices. ZigBee communications is based on the IEEE 802.15.4 standard. An IEEE 802.15.4 radio is required to communicate on an Air-Fi network. Commonly used Wi-Fi (IEEE 802.11) radios, tools and software will NOT work on a ZigBee network.

The ZigBee Building Automation (ZBA) security policy mandates that all communications must be secured using Advanced Encryption Standard AES-128 (FIPS Pub 197) and HMAC (FIPS Pub 198). The Trane WCI operating as a Trust Center will create a randomly generated 128-bit network security key for each ZigBee network. This network security key is required to decrypt communications from the network. In order to join the secured Air-Fi network, the network must first be "opened" or set to allow devices to join. A device requesting to join the network is given a transport key which must be decrypted by the joining device before it can communicate on the Air-Fi network. The Air-Fi network will automatically close or prevent new devices from joining the network 1 hour after it was opened.

Trane WCIs create a ZigBee network that is either a stand-alone network or connected to a Trane SC. The Trane SC coordinates the information from up to 8 Air-Fi networks. Tracer SC can be connected to a building IP LAN to provide remote information to building operators. Many security options are available at the IP network level and IP security policies are implemented and enforced by the customer's IT department. Many customers will put Tracer SC on their building LAN and secure access to their IP network using VPN (Virtual Private Network). Other customers will setup a VLAN (Virtual Local Area Network) for Tracer SC or use a separate IP network infrastructure from their building IP network. .

Air-Fi Product page: **http://www.trane.com//COMMERCIAL/Internal/View.aspx?i=2580**

- Up to 8 Air-Fi networks per Tracer SC
- Each Air-Fi network supports 30 devices.

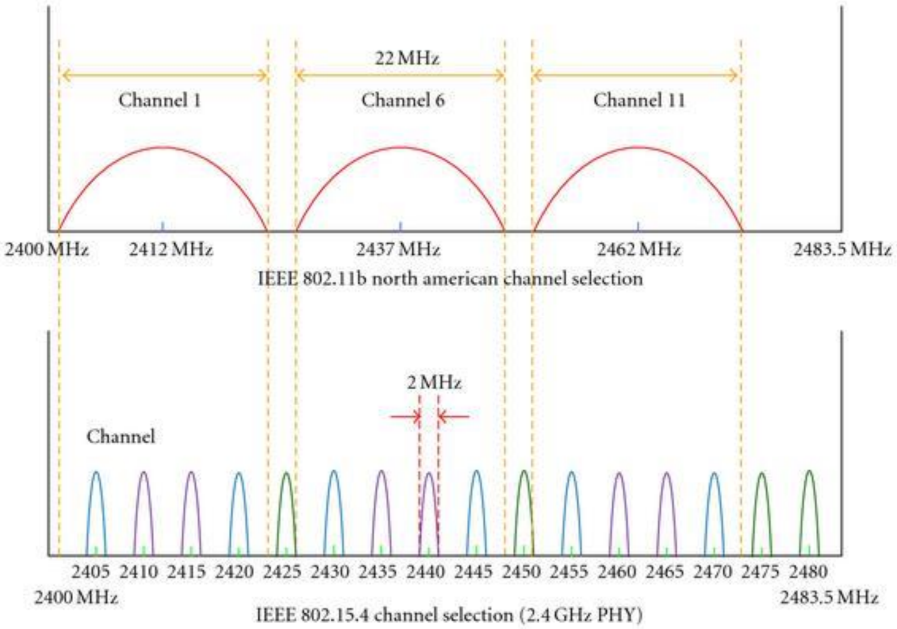
How secure is the WCI?

- Similar to Wi-Fi security
- Requires a 802.15.4 radio to connect to network
  - Not commonly available like Wi-Fi
- All wireless traffic is encrypted!
  - Coordinator creates a randomly generated 128-bit security key

- WCI will only allow BACnet/ZigBee communications
    - Cannot be used to communicate to business systems
- The network needs to be open to allow new devices to join and securely obtain the transport key (encrypted network key). The network will only stay open to allow new devices to join for 30 minutes

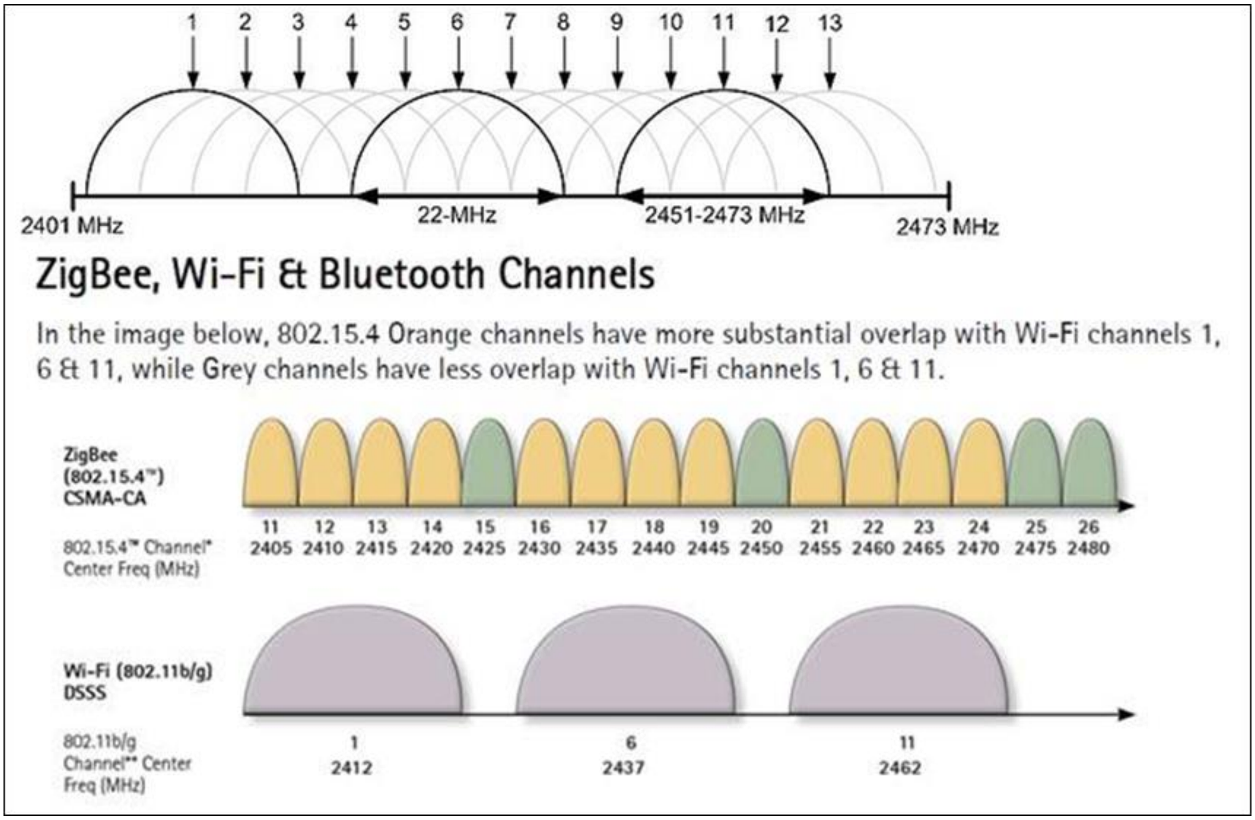
Will Air-Fi Interfere with Wi-FI?

Air-Fi operates at 2.4 GHz which is often used by Wi-Fi. However, since both Wi-Fi and Air-Fi use IEEE standards, there were designed to co-exist much like multiple Wi-Fi networks can operate in the same area. Furthermore, Air-Fi uses an IEEE 802.15.4 radio which operates at lower power and bandwidth which means it takes less of the 2.4 GHz spectrum to operate. The diagram below shows that Air-Fi (IEEE 802.15.4) only needs 2 MHz while a Wi-Fi (802.11) requires a 22 MHz band.



Wi-Fi channels overlap each other which can cause interference. IT department will setup Wi-Fi networks to use Wi-Fi channels that do not overlap. The diagram below shows the Wi-Fi channels and how they overlap. It is very common to use Wi-Fi channels (1, 6, and 11) to prevent Wi-Fi from interfering with other Wi-Fi networks.

Air-Fi (IEEE 802.15.4) channels do not overlap as shown below. Note that channels 15 and 20 fit between the commonly used Wi-Fi channels. This strategy is referred to as channel management.



ZigBee, Wi-Fi & Bluetooth Channels

In the image below, 802.15.4 Orange channels have more substantial overlap with Wi-Fi channels 1, 6 & 11, while Grey channels have less overlap with Wi-Fi channels 1, 6 & 11.

Note: Due to FCC regulations, channel 26 operates at a much lower power than the other channels making it not a viable channel to use. For the same reasons, Channel 25 operates at half the power of the other channels. Channel 25 can be used, but it will have a reduced range than the other channels.

Air-Fi also benefits from using CSMA/CA and a small 2MHz wide channel. By listening on the small channel for activity and only sending very small messages, Air-Fi can operate without issue even if it overlaps on the same frequency as a Wi-Fi network.

CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)
The WCI uses CSMA/CA which will first “listen” for an idle network before sending a message. If there is a collision, the WCI will resend its message again after a randomized amount of time elapses.

ZigBee Frequency Coexistence documentation:

ZigBee Wireless
Whitepaper.pdf

Air-Fi Mesh Reliability

Each WCI in the Air-Fi network maintains a neighbor table. The neighbor table is a list of the 10 nearby WCIs (neighbors) with the highest link quality. Every 30 seconds the WCI updates these table entries. The WCI will use the route with the best link quality, but if a message should fail to be delivered it will use its neighbor table and use the next best route.

Sensors send data on Change of Value (COV)

To reduce sensor battery usage, the sensor radio is an end device (sometimes called a reduced function device). The sensor radio cannot be a router or repeater and “wakes up” periodically to send data. Here is the

- The sensor will heartbeat the data every 15 minutes if the change in value is not exceeded.
- Humidity is sent on a delta of 1% with a 0.1% resolution
- Temperature is sent on a delta of .2 F with a 0.01 C resolution.