HOW RPMA HANDLES

INTERFERENCE

A WHITE PAPER BY INGENU

INGENU
simply genius

HOW DOES RPMA HANDLE INTERFERENCE?

Imagine a highway that goes straight around the entire world, oceans and all, with speed limits that vary, and the entire route is toll-free. Who wouldn't want to use it? Imagine the savings commercial trucking lines would achieve! In the wireless world, an analogous highway exists: the 2.4 GHz frequency band.

RPMA's designers strategically chose to use the 2.4 GHz frequency band not just because it is globally available and cost-free. It also offers 80 MHz of bandwidth to work with and favorable regulations for those technologies using direct-sequence spread spectrum. But Ingenu isn't the only organization that sees these features and has leveraged them for its wireless technology. Bluetooth, WiFi, cordless phones, and even baby monitors utilize the 2.4 GHz band. It's no secret, then, that the 2.4 GHz band has some traffic running through it. This was no surprise to the inventors of RPMA and has been dealt with on every level of the technology stack. But Ingenu also believes in being good neighbors and has designed RPMA to minimally affect fellow 2.4 GHz band users. This white paper will describe how RPMA robustly operates in the 2.4 GHz band while minimally interfering with others in the same space.

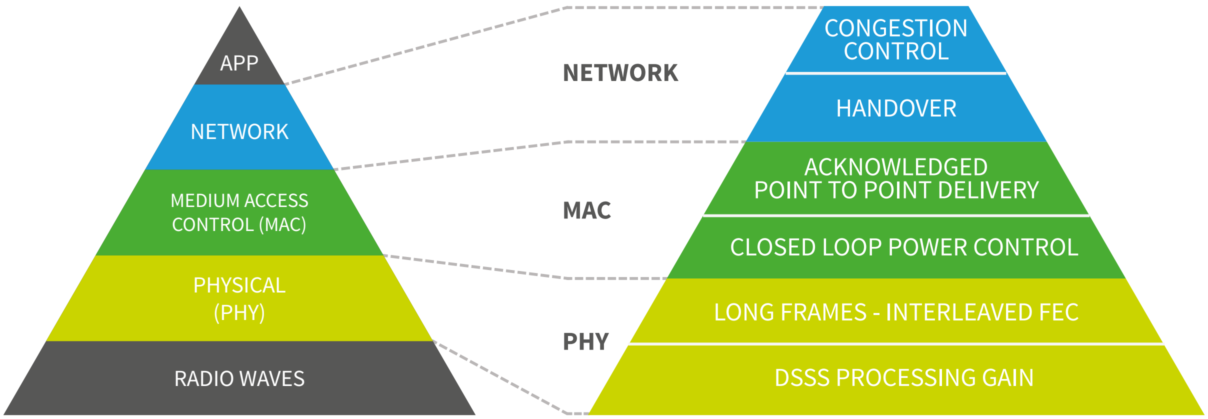
WHAT IS INTERFERENCE?

Imagine two people are talking and a third person tries to talk at the same time making it difficult for the original two to understand each other. This is interference. Similarly, if a device is sending a signal to the access point (AP), or the AP to the endpoint (both possible with RPMA), and another signal at the same frequency broadcasts so that the AP and endpoint can hear it, that is interference.

> In short, interference is defined as anytime unwanted signals are added to wanted signals.

HOW DOES RPMA HANDLE INTERFERENCE?

RPMA deals with others' interference at each level of the technology stack: the physical layer (PHY or hardware), the Media Access Control layer (MAC or firmware/software), and the network layer.



Physical Layer

When wireless signals are sent, they are often translated from digital to analog and back again. Then on the other end, the receiver, or transceiver if the antenna both receives and sends signal, tunes in to a certain frequency predetermined by that system, and looks for those waveforms. Interference is when other signals are also sending on the same frequency making it difficult to detect the waveforms the transceiver is looking for. Those signals represent energy, so signal could be thought of as energy signatures, and RPMA or other technologies, are looking for certain energy signatures. Those signatures can be written, or built up by either lots of power over a short time, or less power over a longer time.

Dealing with Sustained Interference

For dealing with constant interference either on the same channel, or adjacent channels spilling over, RPMA uses direct-sequence spread spectrum (DSSS). The DSSS technique builds a signal using less power over a longer time. Long, of course, being relative, as microseconds in the wireless world is a long time. If RPMA were to just blindly up the power and blast the signal through, it would waste precious battery power, and be unfriendly to neighboring technologies. RPMA's physical layer, using DSSS, is capable of finding signal in interference that is actually louder, or has more power, than the wanted RPMA signal even when sending in the same channel (or exact same frequency); this is called co-channel rejection.

RPMA will reject unwanted signals (i.e., interference) even when that interference is louder in the same channel by 1 dBc (dBc = decibels relative to carrier). A positive dBc is where the magic is here. Most non-RPMA technologies have a negative dBc, or in other words, the wanted signal can only be heard if the interfering signal is quieter than the wanted signal. This is an incredible feat! Imagine being able to clearly understand somebody whispering to you while another person is talking loudly to you as well. This is what it is like to have a positive dBc like RPMA. And as soon as you move even a short distance away from the same channel, those interfering signals can get even louder and RPMA is still able to detect the wanted signal. For instance, if there is interference coming from a channel 2 MHz away, RPMA will rightly reject it even if it is 73 dBc stronger than the wanted signal. RPMA's co-channel and adjacent channel rejection capabilities provide incredible robustness to sustained interference.

> Imagine being able to clearly understand somebody whispering to you while another person is talking loudly

Dealing with Strong Bursts of Interference

RPMA is also designed to deal with shorter bursts of signal that are stronger than the wanted signal by a limitless amount. RPMA is designed with long and flexible frame durations coupled with interleaved Forward Error Correction (FEC). Interleaving, using a simplified explanation, is like scrambling it in a special way that adds efficient redundancy so that if any packet is blasted by abnormally strong interference, the message can still be decoded. For example, RPMA can demodulate signal in the presence of a limitlessly strong 250 microsecond 50% duty cycle pulse jammer. RPMA only experiences a 3dB drop in receiver sensitivity. This kind of interference would cripple most other technologies.

In the end, RPMA has industry leading PHY layer interference protections not only for sustained interference that is louder than even the wanted signal itself, but can withstand even bursts of limitlessly powerful interference. And the interference protection continues at the next layer.

Medium Access Control (MAC) Layer

Interference conditions change all the time. A naïve way to prepare against interference on the MAC layer would be to blast the full signal at the maximum power each time. But this naïve approach is inefficient.

Real-time Feedback

Blasting the entire message at full power all the time drains battery life unnecessarily, and it wastes capacity. RPMA takes a more sophisticated approach with a closed loop power control scheme that adapts to changing interference. A real-time feedback loop from the AP tells the endpoint the signal conditions before it sends. Then the endpoint only uses the minimum amount of power for the shortest time necessary to close the link.

Intelligent Message Acknowledgement

After the message has been sent and received by the AP, it reports back to the endpoint that it has received the message. Using information from our advanced forward error correction scheme described earlier, the APs also communicate those parts of the message, if any, that were interfered with. Ingenu's smart endpoints then resend only those packets that are needed to complete the message, if there are any. RPMA utilizes several methods together for a sophisticated approach that in the end, allows messages to get through successfully with a 50%+ packet error rate (PER). This is incredibly robust as many other protocols would fail at even a 10% PER.

Network Layer

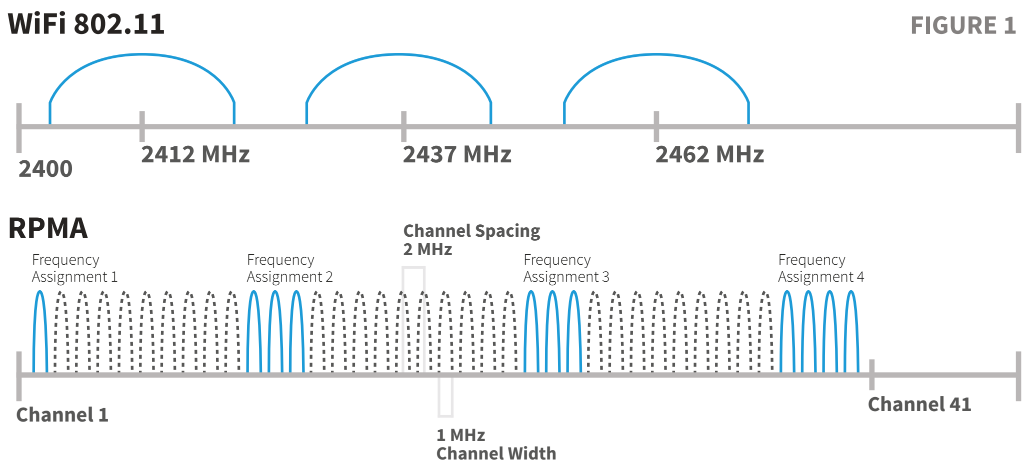
Finally, RPMA intelligently monitors conditions at the network level and handover to other APs is built in. RPMA can determine if a weak link with a clear channel is better than a congested channel with a strong link and is designed to choose the best one. This provides extreme resilience should an AP experience unusually high localized interference.

In addition, our network has sophisticated congestion management. This is important because many machine-to-machine users will most likely need their network to function during events where every device suddenly needs to communicate. This is how smart grids use RPMA. When an outage occurs, thousands to tens of thousands of devices want to suddenly report that the power line they are resting on is no longer powered. This sudden burst would overwhelm other networks as the multitude of signals pour in, essentially interfering with each other and overwhelming the network infrastructure. RPMA, naturally aided by its star topology, has sophisticated mechanisms for accommodating such "flood events" and is being used by many smart grids for this very purpose.

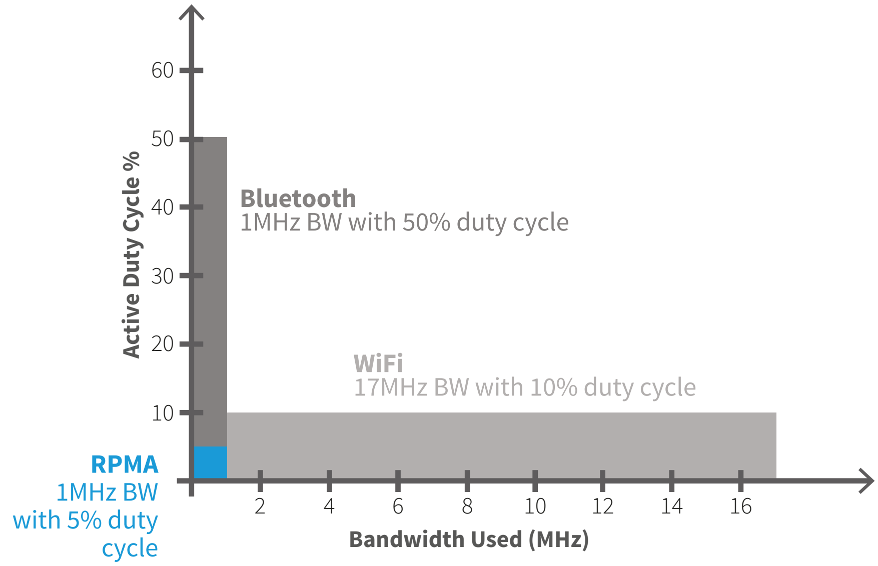
HOW DOES RPMA INTERFERE WITH OTHERS?

We've seen how RPMA robustly handles interference from other sources, but it is also designed to play nicely with other wireless technologies. Because of the 80 MHz of bandwidth that the 2.4 GHz band offers, RPMA can nestle nicely between commonly known congested areas. For example, WiFi is centered around 2412 MHz, 2437 MHz, and 2462 MHz (**see figure 1**). That leaves a single 1 MHz channel to the far left of the 2412 MHz channel open, with three 1 MHz channels between each of the WiFi channels, and then an additional four 1 MHz channels to the right of the WiFi channels. That means RPMA has 11 total channels available for use outside of the WiFi bands. Ingenu can deploy an entire network on a single channel, and even with an 8-channel setup RPMA has three degrees of freedom for placing those channels to be extra-friendly to other technologies.

FIGURE 1



The RPMA signal also has an incredibly small footprint compared to some of its neighbors. Bluetooth, for instance, has a 50% duty cycle, but the same 1 MHz bandwidth. This is like having a person talking 50% of the time right next to you. WiFi has a 10% duty cycle but uses 17 MHz of frequency, which is like having someone talk 10% of the time but having the sound coming from all around you when it does come. RPMA's interference footprint is shorter in time (active duty cycle) than WiFi by half. RPMA only uses a 1 MHz band (like Bluetooth)



but has 1/10th the active duty cycle. So compared to two common standards, its interference footprint is very polite. And because of its closed loop feedback mechanism, RPMA sends signal with only the minimum amount of power necessary.

In summary, RPMA handles interference on every level of the technology stack:

Physical Layer (PHY)

- For dealing with constant interference either on the same channel, or adjacent channels spilling over, RPMA uses direct-sequence spread spectrum (DSSS).
- For shorter bursts of signal that are much stronger than the wanted signal, RPMA is designed to have long frame durations coupled with interleaved Forward Error Correction (FEC).

Media Access Control (MAC) Layer

- For changing interference conditions Ingenu's APs update the endpoints on conditions and the endpoints transmit at the minimum power needed for a successful transmission.
- The APs and endpoints provide intelligent message acknowledgement so that if any information is lost, only that information is resent.

Network Layer

- RPMA can determine if a weak link with a clear channel is better than a congested channel with a strong link and choose the best one.
- RPMA, naturally aided by its star topology, also has sophisticated congestion management for accommodating "flood events" where many endpoints compete to transmit a message.

RPMA is stacked top to bottom with advanced mechanisms for handling not only typical but extreme interference while also playing very nicely with other technologies using the 2.4 GHz band.

To learn more about how RPMA can get you connected to the Internet of Things, contact us at info@ingenu.com