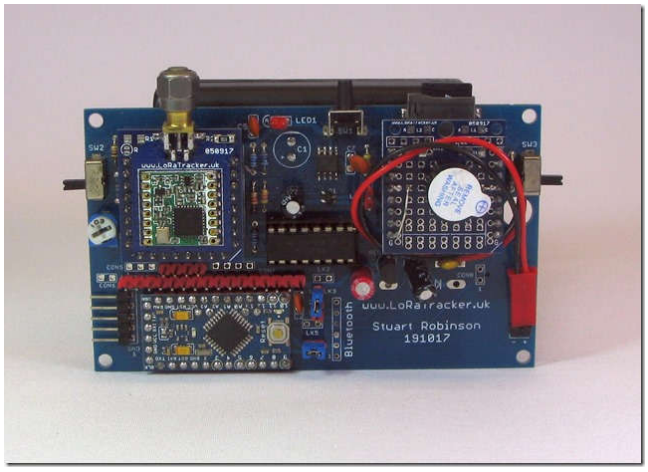
A LoRa Mystery 1 - Phantom Packets

I had noticed while testing LoRa links at 868Mhz with different receiver types that I was seeing a number of ‘phantom’ packets that I did not recognise. I initially thought these were just LoRa packets from the surrounding environment.

The receiver I was using was listening on Bandwidth 500Khz and spreading factor 7, which is not the typical packet settings used by LoRa for Internet of things applications. I was using these settings as I needed a fast data rate and only a hundread meters or so of range. These phantom packets being quite short range I thought must be coming from somewhere nearby.

I used some LoRa SD card logging software I had written to check out the details of these phantom packets. I could leave the receiver running for long periods to see how many packets were received. I did fing a bug in the software which explained some odd RSSI and SNR values I had been seeing but I was still curious as to where the packets were coming from.



With the receiver running on the bench with an antenna I was getting around 5 to 10 phantom packets per hour, these were a mixture of packets with valid CRC and those where the CRC check had failed. Packets varied in length from a few bytes up to 200+. The reported RSSI and SNR was always around –110dBm and –10dB respectively which suggested a single source of the packets.

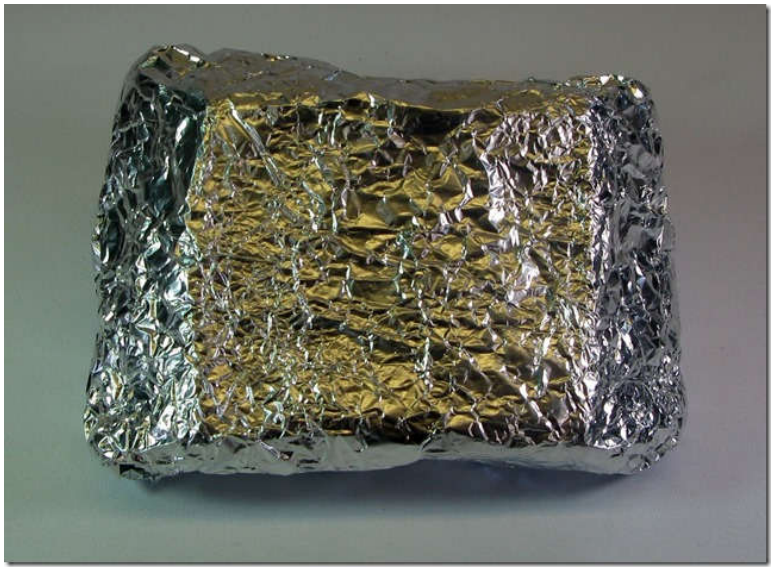
I put an SMA terminator in place of the antenna and was surprised to see that I got around the same results, 5 to 10 packets per hour and similar RSSI and SNR values.

As a check to see if these phantom packets were actually coming from the great wide world I put my reference 868Mhz antenna (1/4 wave vertical with radials) on top of the 8.5m mast attached to my workshop. I got the same results as I had when the receiver was sat on the bench with an SMA terminator on it. The assumption might be that the source of the phantom packets was therefore very local, interference from my PC or the lights perhaps ? That however would not explain why I origionally seen these packets in the middle of a large field.

For some of the LoRa link testing I had been doing recently I needed to cut the range of the LoRa transmitter (at spreading factor 12) to just 50m or so. Fitting an SMA terminator in place of the antenna was not enough. Even putting the receiver in a die-cast aluminium box was not enough. What did work very well was wrapping the transmitter in aluminium foil. That cut the reception range to 10m or so and it was easy to adjust the range out to 50m by using a pin to put small holes in the aluminium foil.

If the aluminium foil was so effective at preventing the RF getting out, it ought to be effective at preventing RF getting in. So I wrapped a LoRa receiver in foil and also put it in an aluminium box. A LoRa transmitter sending packets at

17dBm (50mW) had to be within 5cm of the box for the receiver to pick up the packets, there was a buzzer on the receiver so I could tell when packets were received. So if real world packets were getting through all that shielding they had to be very powerful indeed.



With the receiver now wrapped in foil and consequently very well screened I was still receiving phantom packets and with the similar RSSI and SNR values as before. Perhaps the phantom packets were a result of electro magnetic interference (EMI) coming from the receiver itself, but if so how could the CRCs be valid ?

I modified my logger software to put the Arduino Pro Mini to sleep and have it wake up when a packet was received using an interrupt from the LoRa devices DIO0 pin. I even powered down the SD card. Thus the only active electronics running (and thus possibly generating EMI) was the LoRa device itself listening for a packet.

With only the LoRa device itself active and with it heavily screened from the outside world, still the phantom packets appeared.

These phantom packets do seem to be coming from the receiver itself; when I ran two identical receivers next to each other on the bench, each would receive phantom packets but not at the same time. If the source of the packets was external then you might expect at least some duplicate receptions.

This does not appear to be just an issue with the 500khz bandwidth setting, IO have also seen phantom packets when the 125khz bandwidth setting is used.

Maybe the LoRa receiver is fooled into starting packet reception by noise but then why does reception complete with a valid payload CRC and a valid header CRC as well?

A LoRa mystery 2 – Phantom packets but deeper

Despite the shielding of my LoRa receivers being able to resist 50mW at 5cm it was possible that there could be a Megawatt LoRa transmitter somewhere close that was the cause of the phantom LoRa packets I was seeing at 868Mhz bandwidth 500khz and spreading factor 7. It’s unlikely there would be such a powerful transmitter nearby that I did not know about, but it seemed a good idea to eliminate it as a possibility.

What I needed was a test area that was in a relatively remote, was underground and with no openings to the outside world. Fortunately up in the hills nearby is a disused railway tunnel, it's at a height of 439m AGL, the tunnel is 600m long and curved so that in the middle there is no line of sight to the outside world. The tunnel is some 40m underground in the middle. There is a quiet road nearby with a few cars, the nearest building is 1km away. There are a few further buildings 3km away.

I went to the tunnel on a wet afternoon with my brother (Neil) to see if there would be any difference in the number of phantom packets received and their signal strengths in the middle of this tunnel. I used two receivers heavily screened as before and took the precaution of eliminating all possible EMI producing gadgets, phones off, cameras off, I even took the battery out of my car key fob.

With the two receivers on the floor I could still hear the beeps indicating phantom packets at the same rate as I had been getting in my workshop and local field. Looking at the logs the receivers produced later it was clear that the signal strengths in the workshop were the same as I was seeing deep underground and a very long way from any LoRa transmitters.

Log

ReqIrqFlags 0x50
CRC and Header OK
SNR,-11dB,RSSI,-114dBm,Length,153
Packet data 9E,62,C8,7C,55,B2,6F,E1,40,8A,F8,D4,B1,99,0C,33,EA,E1,58,
(packet data truncated)
Valid Packets 7 CRC Errors 2 Header Errors 0

Reported signal strength in all the tests, with an antenna on a tall mast, with small antenna on the bench, with an SMA terminator on the antenna socket on the bench, heavily screened on the bench and now with a heavily screened receiver deep underground were always the same, –112dBm to –114dBm and with SNRs of –11dB or –12dB. My assumption would be that the source of the phantom packets was the receiver itself.

With the microprocessor in use (ATMEGA328) being put to sleep this suggests the source of the phantom LoRa packets may be the LoRa device. If that is the case how can it be that the CRC is valid for about 70% of the phantom packets? My logging software was printing out the contents of the ReqIrqFlags register and that indicates a valid header (which has its own CRC) as well.

What are the chances of the CRCs for header and payload being valid in a packet that's some sort of random occurrence of noise?

Phantom Packets 3 - Is this the reason ?

After consulting Semtech, the reason why these phantom packets are seen becomes clear.

This is my current understanding of the issue but testing is continuing …….

The LoRa receiver will occasionally falsely see noise from the receiver itself as a packet preamble and header. Since its noise from the receiver this explains why the phantom packets are seen even in heavily screened receivers underground.

The header is protected with only a 6 bit CRC so there is a 1:64 chance that this noise will pass a valid header check.

When sending LoRa packets you have the option of using a payload CRC (16 bit) or not. If there is a payload CRC enabled a flag bit is set in the header. When receiving the packet the LoRa receiver tests for this payload CRC enabled flag and carries out the CRC check on the payload.

The trap you can fall into is in assuming that since your application only sends packets with CRC on the payload enabled, on packet receipt you only

need to check the RegIrqFlags register PayloadCrcError bit. If its set there is a CRC error, if it clear then you assume your packet is valid. But it may not be.

When one of the phantom packets is received (which are just noise remember) there is a probability that the false header both passes the header CRC check and does not have the payload CRC enabled bit set. If this bit is not set in the header then the LoRa receiver does not carry out a payload CRC check and the CRC error flag is left clear.

There are some LoRa software libraries that on packet receipt appear to check the header for the payload CRC enabled flag and then check the payload PayloadCrcError flag as appropriate. This makes sense if your receiver software is designed to automatically cope with packets that use a payload CRC and those that do not.

So in summary to ensure that you do not read phantom packets as valid, you should consider;

1. Sending packets with the payload CRC enabled.

2. Checking the RegHopChannel register RxPayloadCrcOn bit, if its is clear, dump the packet, it could be a phantom.

3. If the RegHopChannel register RxPayloadCrcOn bit is set, check the RegIrqFlags register for the PayloadCrcError bit, if that is set dump the packet, it could be a phantom.

Stuart Robinson

June 2018