Revisting SDRs in the IoT Era

Revathy Narayanan, Swarun Kumar

Presented by Mike Hegarty

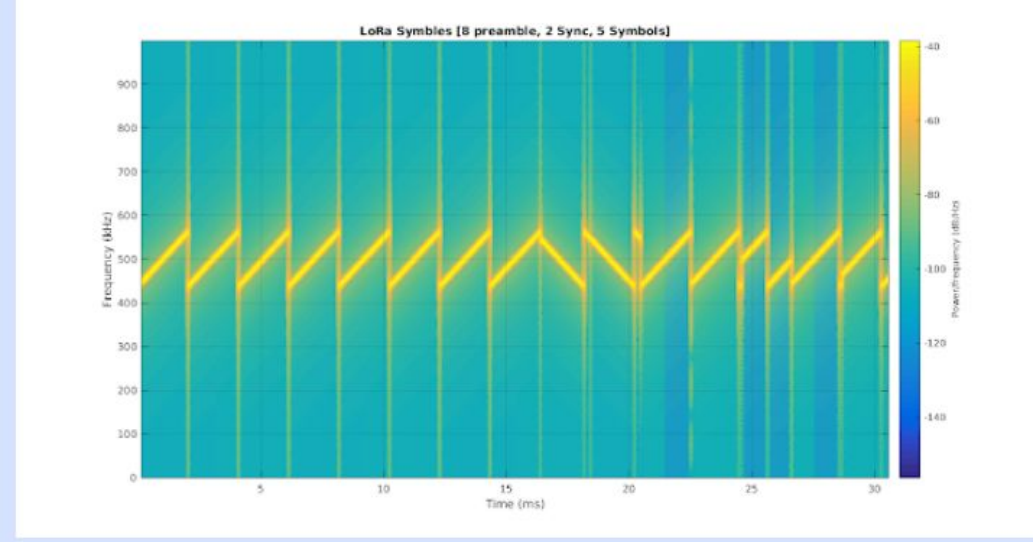
What is an Software Defined Radio?

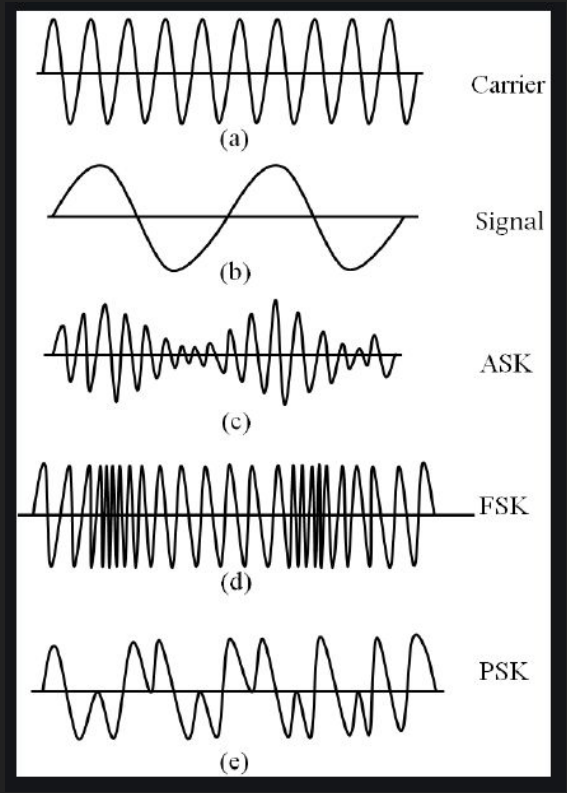
- A software defined radio(SDR) is a type of radio where the signal is demodulated in software rather than in hardware
- Functions very similar to how a sensor functions.
- Typical applications include:
  - Spectrum analysis
  - Network security testing/reverse engineering
  - RF prototyping
  - Defense industry

Modulation

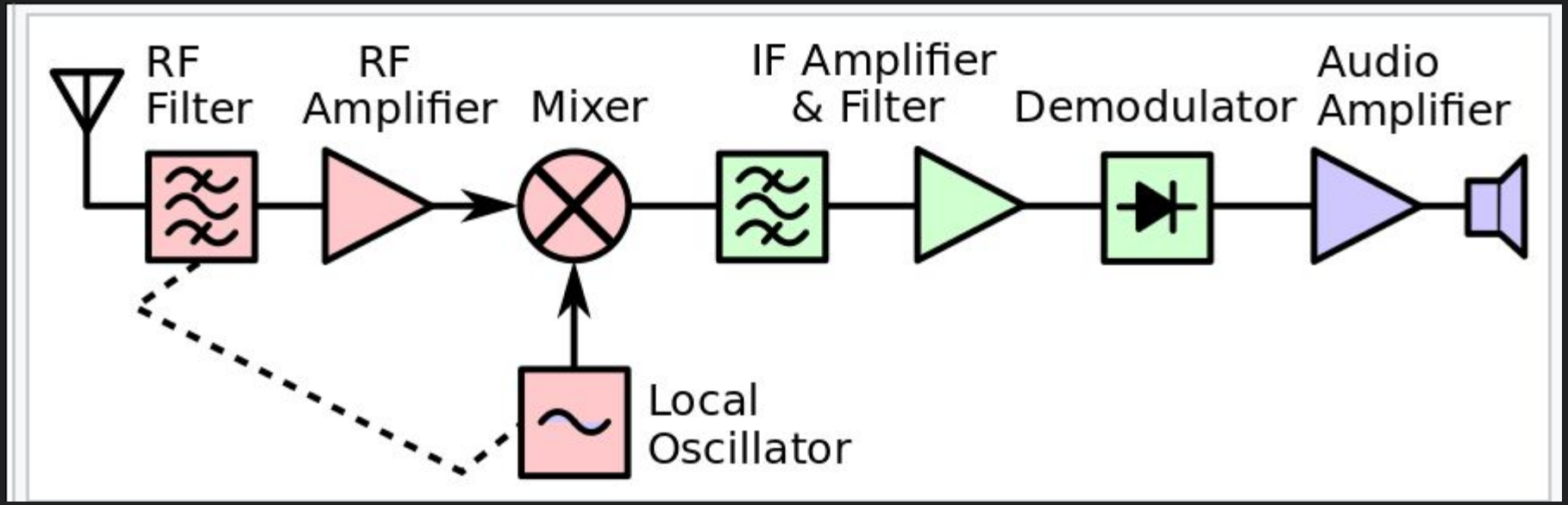
- Wireless communication happens via ElectroMagnetic waves
  - Information can be sent across these waves by altering one or more of the properties of the wave
    - Amplitude
    - Phase
    - Frequency
- Different modulation types have different bits per symbol and different bit error rates.

Some Modulation Types

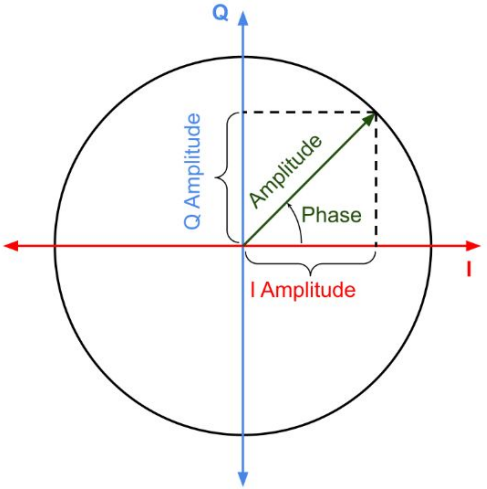


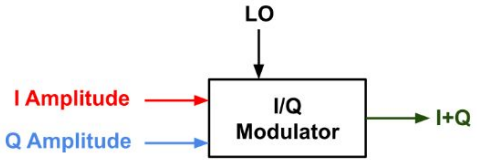


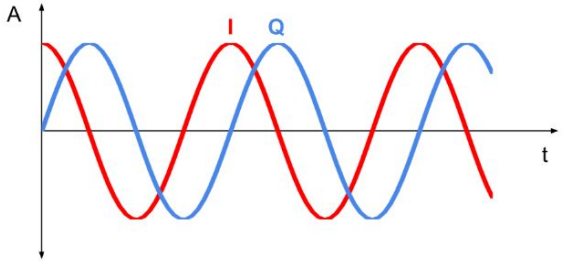
General RF background

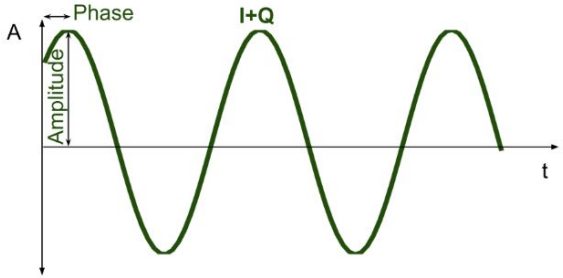


IQ Data









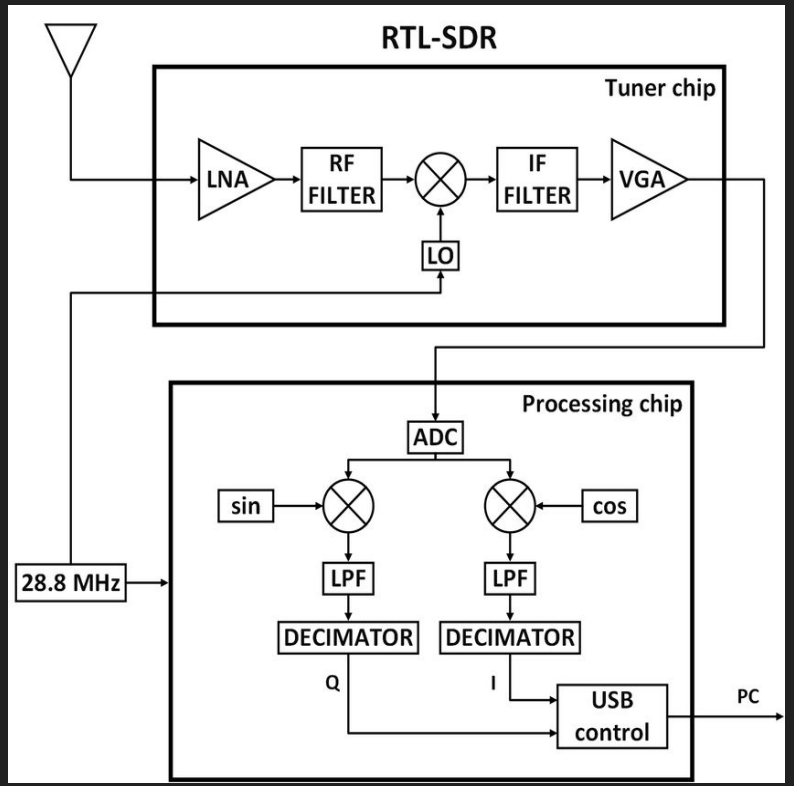
I Amplitude (V)	Q Amplitude (V)	I+Q	
		Amplitude (V)	Phase (°)
1	0	1	0
0	1	1	90
-1	0	1	180
0	-1	1	270

How SDRs work

- After initial processing, data is sampled by an analog to digital converter and passed along a data bus in the form of IQ data.
- Modulation and demodulation occurs in software rather than hardware
- As long as the sampling speed is fast enough any signal can be theoretically decoded.

RTL-SDR

- Very simple and cheap USB SDR
- Receive only
- Costs around $20
- Higher end SDRs can get kinda pricey
  - ~4,000s range
  - Higher sampling rate, more bits per sample, built in FPGA, etc.



What makes SDR suited for IoT

- Can support new technologies when they pop up
  - New modulation types
  - Or new techniques such as angle of arrival
- Can interface between different wireless technologies
- Software solutions to RF problems
  - processing starts at PHY layer

What is holding back SDRs

- No good commercial low cost SDR on the market ATM.
  - The one the paper uses is a hobbyist device
- Less optimized for speed than pure hardware system
  - CPU processing bottlenecks
- High throughput requirements for data buses
  - FPGA in the middle

GalioioT Gateway

- Proposed IoT framework that makes use of SDRs for networking to support multiple modulation types broadcasting in the same band.
- Universal Gateway
- Cloud Based Decoder
  - Can filter out different types to isolate the different modulation types
  - LoRa, XBee, Z-Wave
  - Less repeating transmissions = less power usage

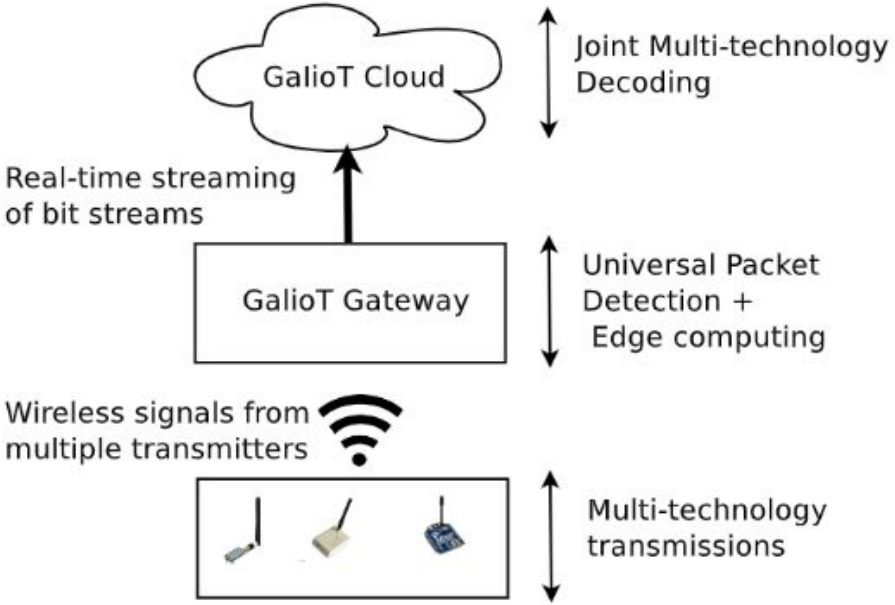


Figure 2: System overview of GalioT

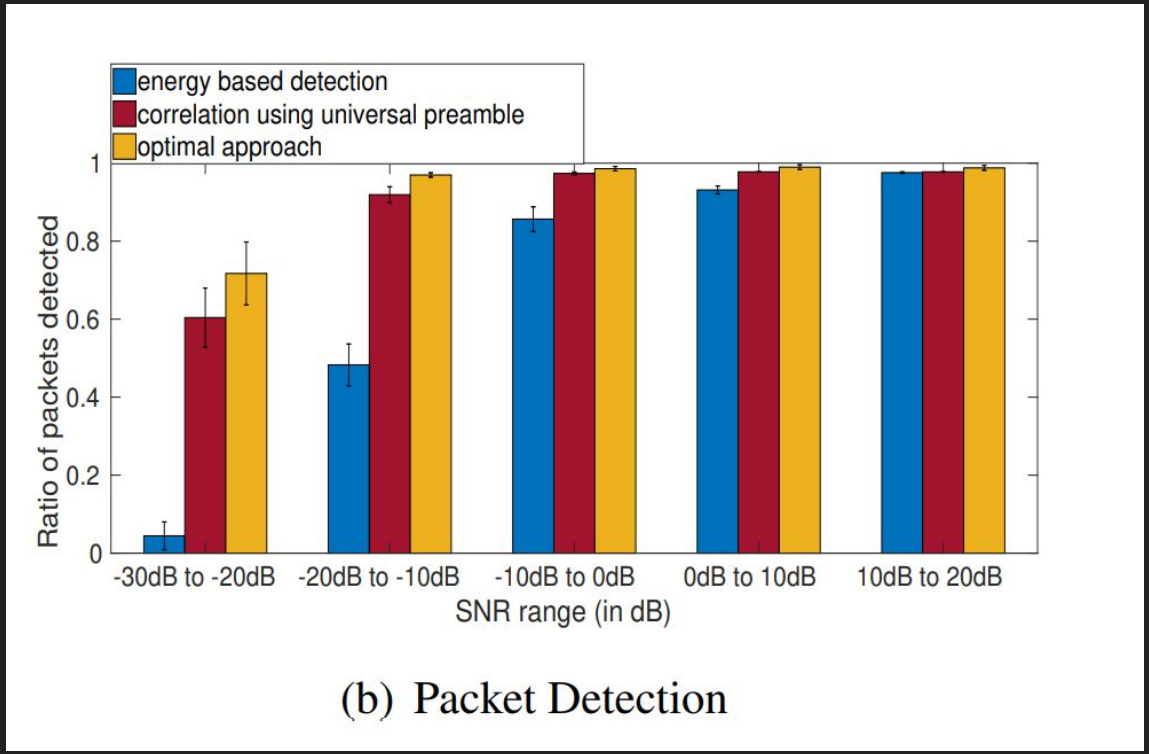
Universal Preamble

- A preamble is a section of the PHY layer that comes before the data packet typically in a very distinct pattern.
- Designed a universal preamble containing a sum of all of the different preambles wanted to be detected.
- If any of the preambles of the signals are detected, it passes the data around the preamble to the cloud for demodulation.

Multiple signal detection

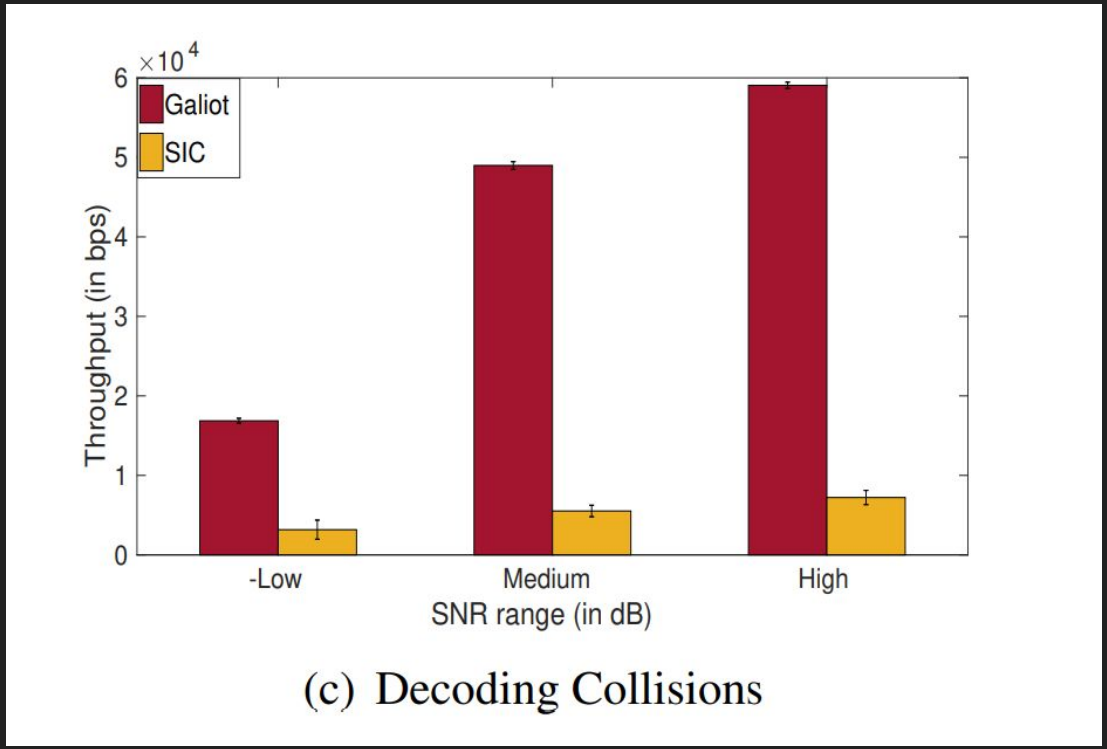
- Detected packets sent to cloud may contain one or more signals in them
- The authors design different digital filters for handling packet collisions
  - Alternative to Successive interference cancellation
  - Filtering center frequencies for Z-Wave/X-Bee
  - Downchirps for upchirp LoRa

Results



(b) Packet Detection

Results



(c) Decoding Collisions

Critiques

- Receiver only system
  - No acks
- Results section only talks about throughput of algorithm, not entire system.
  - No comparison to normal radio hardware.

Conclusion

- Interesting paper showing software solution to RF problem
- Would be interesting to see how scaleable this solution is in terms of throughput and adding more signals