Sakernas säkerhet

SUSEC Östersund
2013-04-18
Robert Olsson UU/KTH

Usage-Security Meditation Needed

- Many new technologies
- Many new standards
- Covering new areas PAN, BAN

  Freedom/integrety human needs vs business models.

Contiki Programming Experiences

IoT enablers:

MCU microcontrollers with radio tranceivers
Radio & Antennas
Operating system / Contiki etc
Networking / IETF, IEEE
Sensor technology / I2C etc
Energy effiency / Capacitors possible

Contiki Programming Experiences

Technology moves forwards...
Sometimes a jump.

Not only legacy IP networking

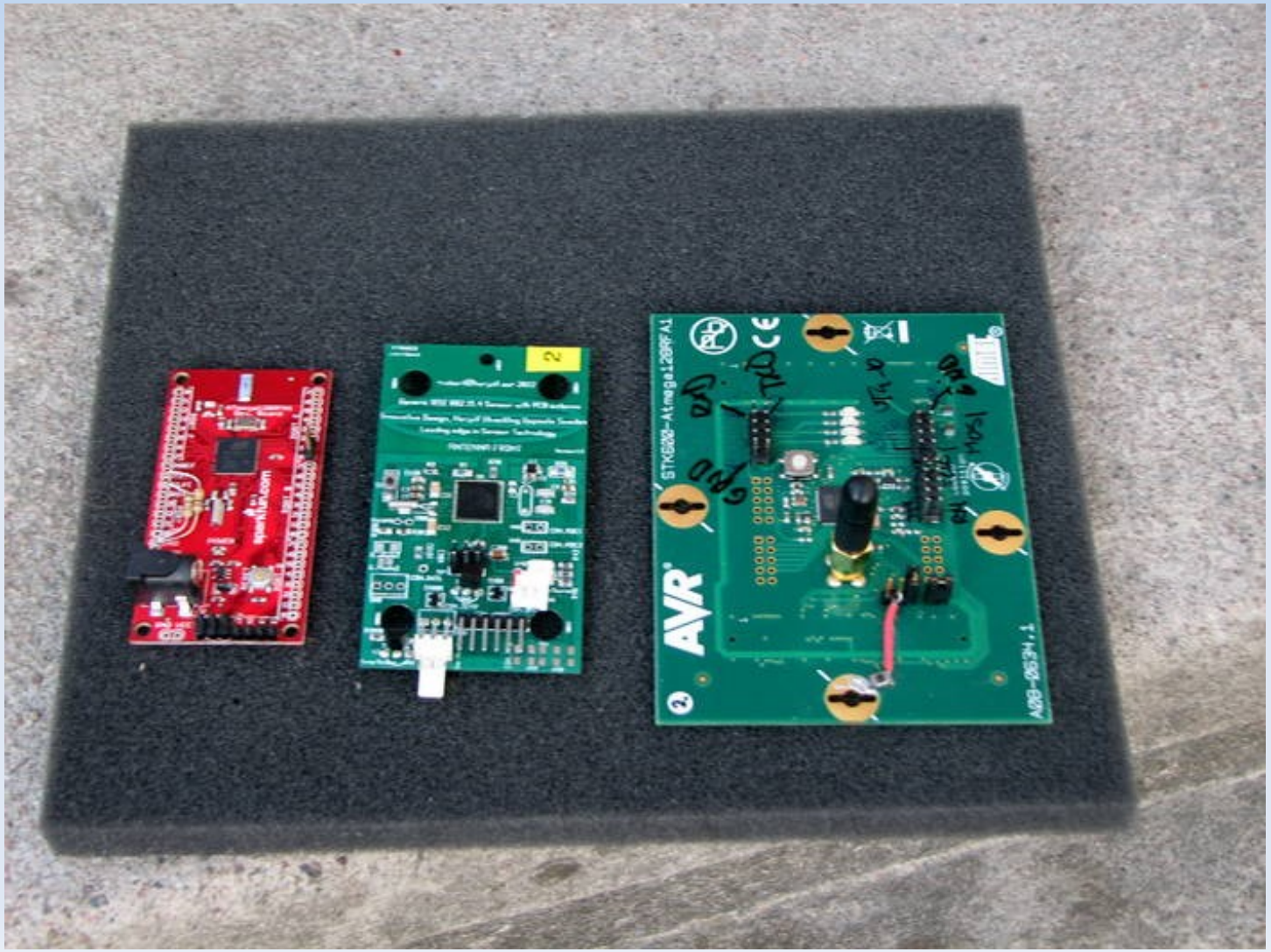
Keyword: Connectivity (rather than bandwidh)

Communication to solve new problems:

- Environmental
- Health, buildings, home
- Agricultural, industri
- etc

Contiki Programming AtMega128rfa1 boards

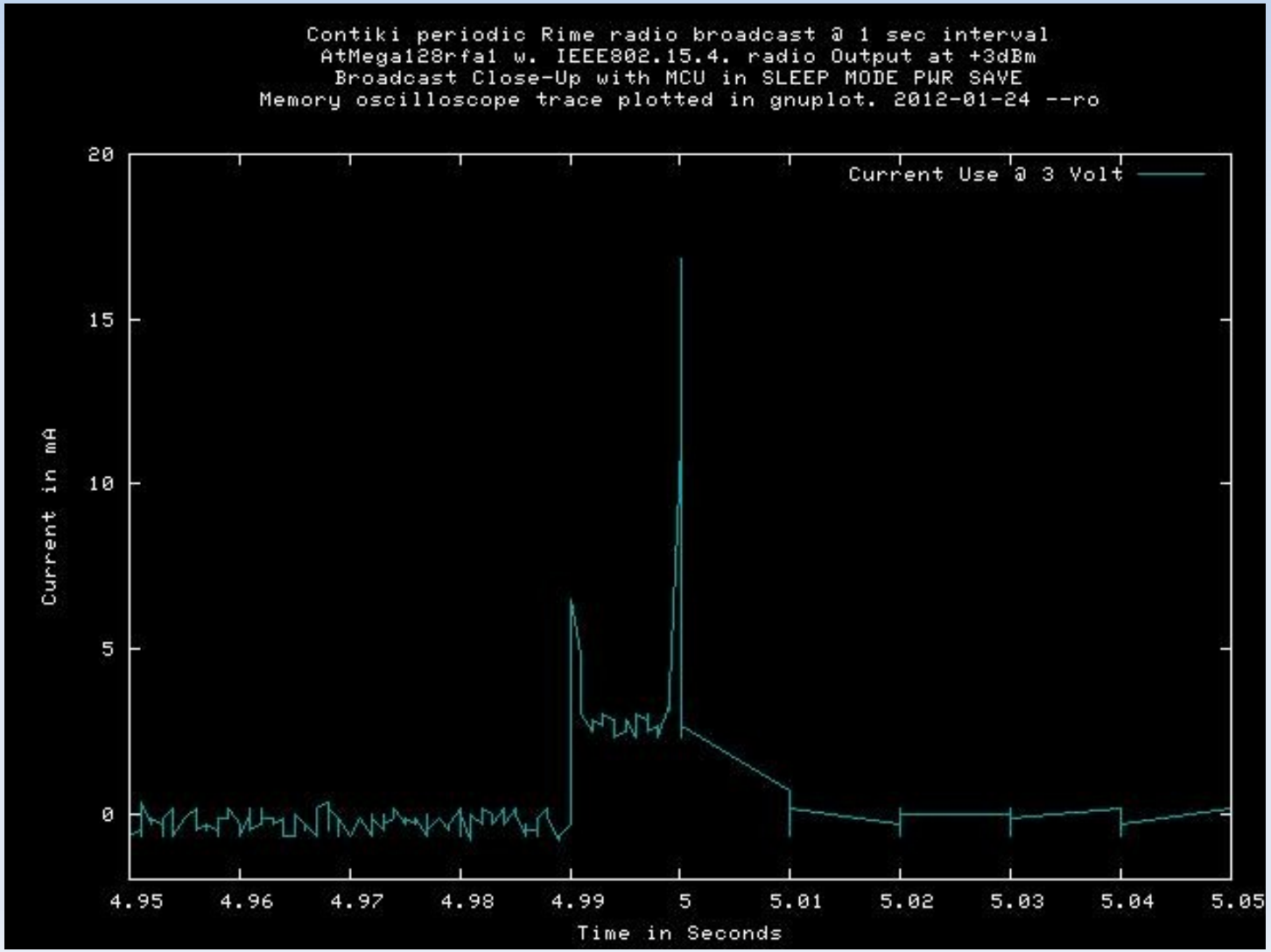
MCU boards w. Builtin IEEE202.15.4 radio tranceiver
Note! Different antenna design on boards



st32w similar w. tranceiver.

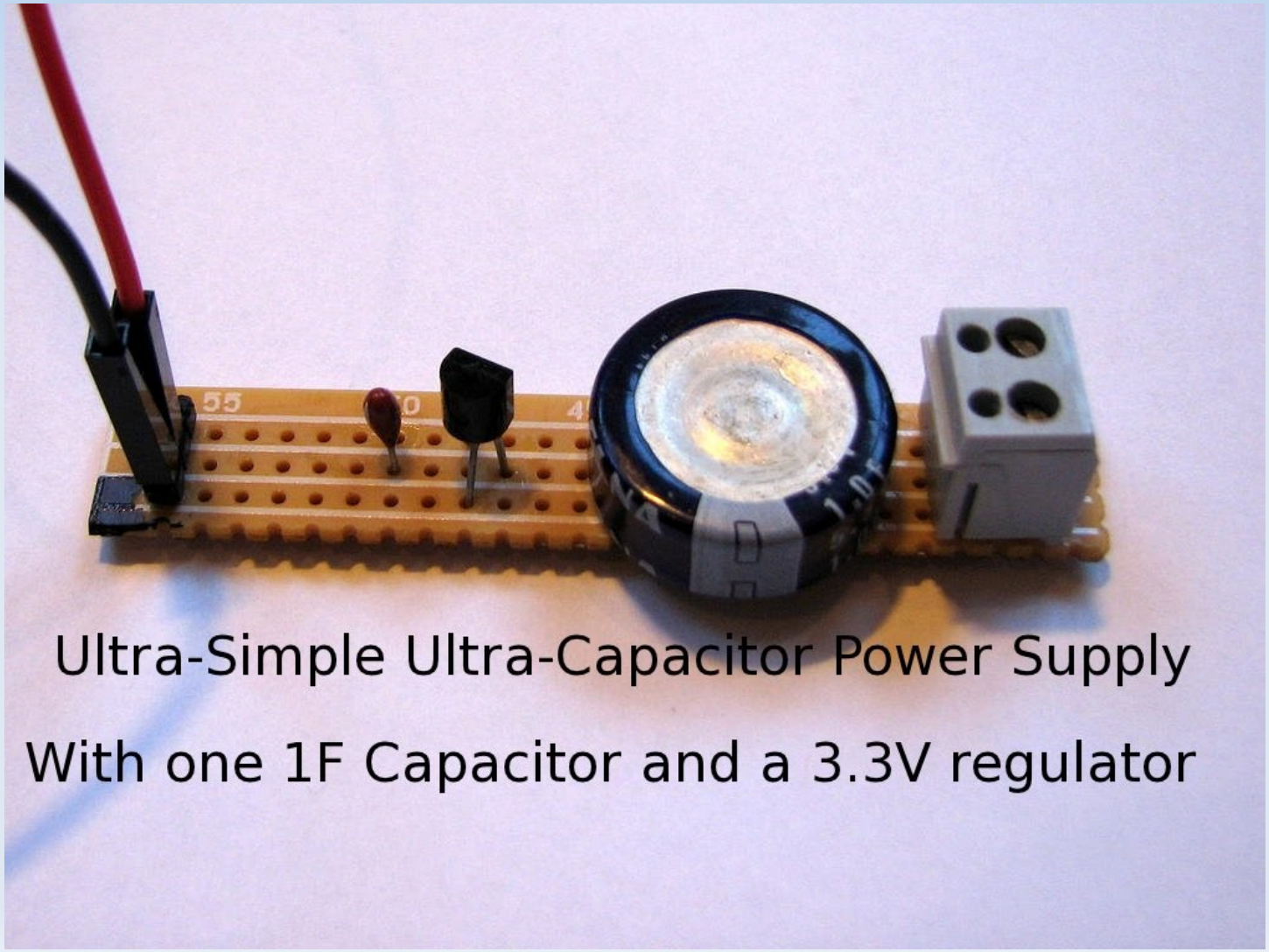
Contiki Programming Experiences

Hacked version contiki rime broadcast program
Radio broast every sec. Current monitored.



Contiki Programming Experiences

Capacitor experiment.



IEEE 802.15.4 groups/standards

- WPAN Low Rate Alternative PHY (4a)
- Revision and Enhancement (4b)
- PHY Amendment for China (4c)
- PHY and MAC Amendment for Japan (4d)
- MAC Amendment for Industrial Applications (4e)
  Frequencehopping

IEEE 802.15.4 groups/standards

- PHY and MAC Amendment for Active RFID (4f)
- PHY Amendment for Smart Utility Network (4g) Smartgrid
- Positive Train Control (PTC) (4p)
- IEEE 802.15.6 Body Area Networks (BAN)
- IEEE 802.15.7 Visable Light

IEEE 802.15.4 radio capabilies

Initial 250kbit/s range 10m

Atmega128rfa1 example:

- TX

-16.5 dBm (0.02 mW) – 3.5 dBm (2,24 mW)

- RX @ 250 kbit/s

-100 dBm – 10 pW PER <= 1% PSDU 20 bytes

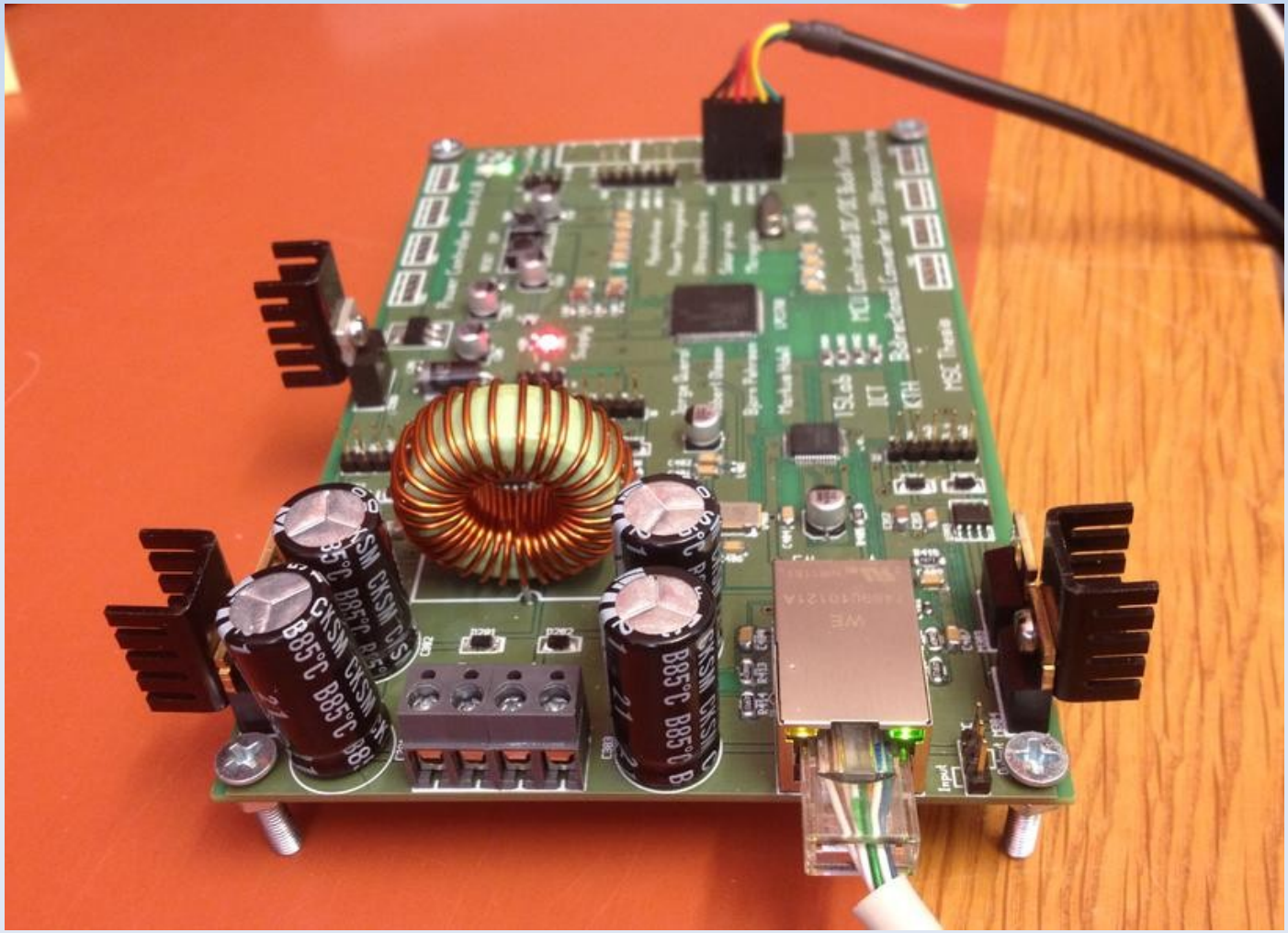
Good antenna design line-of-sight coverage
> 300 m @ 2.24 mW @ 250 kbit/s

IEEE 802.15.4 channels

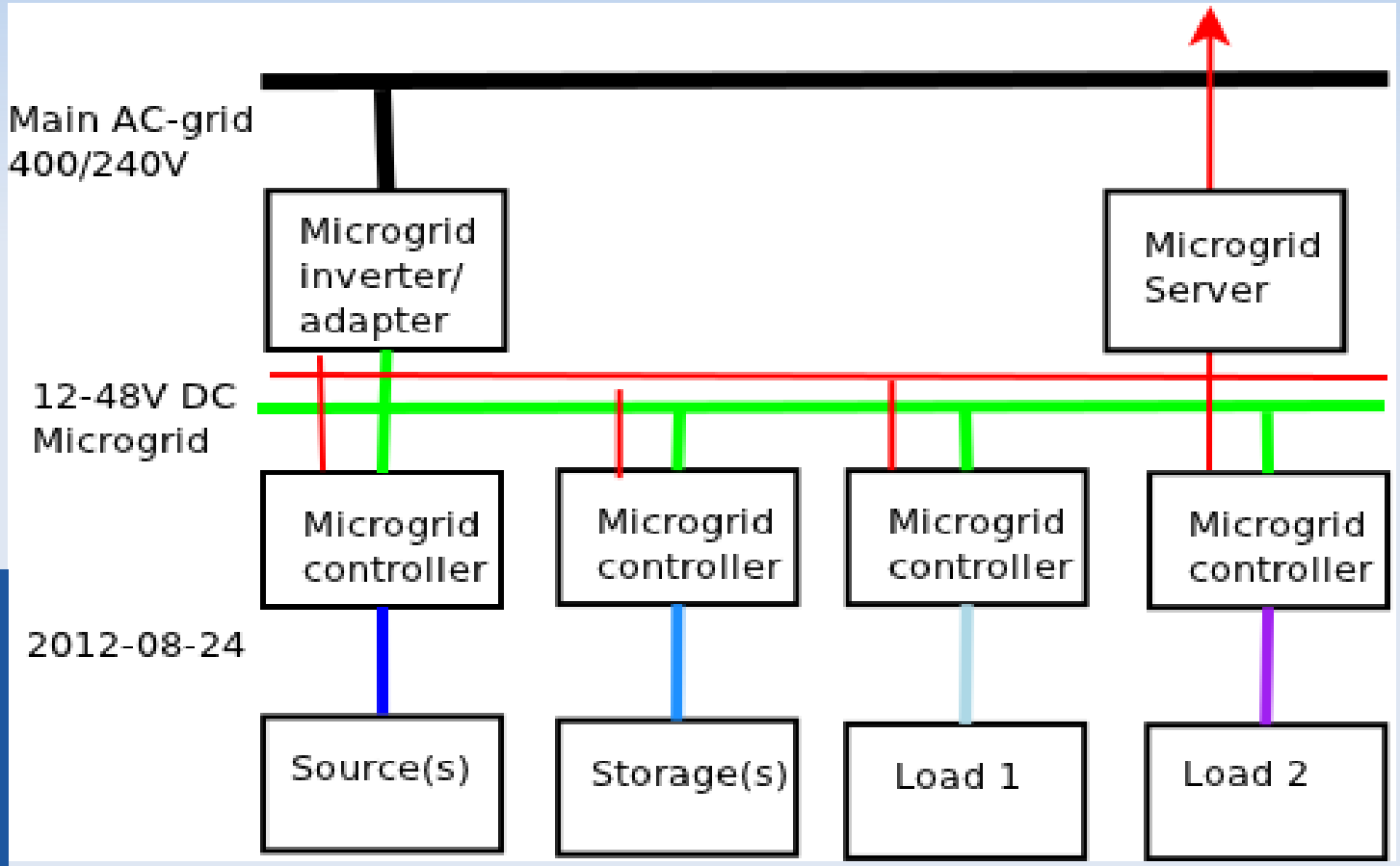
- 12 2410
- 13 2415
- 14 2420
- 15 2425
- 16 2430
- 17 2435
- 18 2440
- 19 2445
- 20 2450
- 21 2455
- 22 2460
- 23 2465
- 24 2470
- 25 2475
- 26 2480
- 11 2405 MHz

IoT-grid control unit

ARM Bidir. Step-Up/down-DC-DC converter/Contiki/CoAP/Ethetnet



IoT-grid/CoAP app.



Usage-Security Meditation standard track

- IEEE 802.15.4
- 6LowPAN
- CoAP
- DTLS

Usage-Security Meditation simple/small track

- IEEE 802.15.4
- Broadcast Network
- Sink Node → USB → sensd → URI
  - AES-128 optional

herjulf.se:8080/WSN1-GW2

RPi with 802.15.4 sensors each with 64-bit ID

CoAP/transport

- Default UDP but required

  DTLS (Datagram TLS)
- TCP SCTP is discussed

UDP Port 5683 (mandatory)

UDP Ports 61616-61631 compressed 6lowPAN

CoAP/protocol header

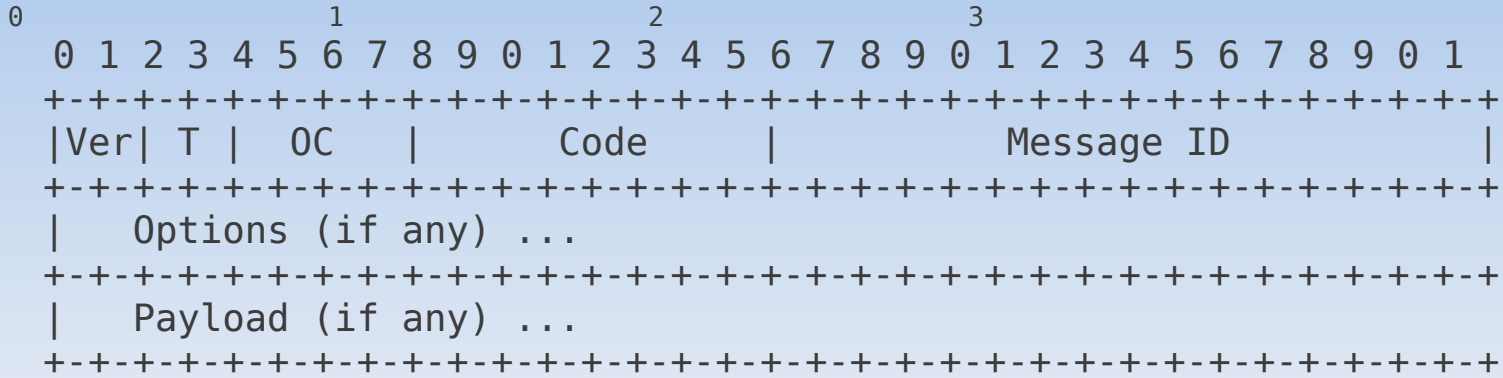


Figure 7: Message Format

3.1. Header Format

The fields in the header are defined as follows:

Version (Ver): 2-bit unsigned integer. Indicates the CoAP version number. Implementations of this specification MUST set this field to 1. Other values are reserved for future versions.

Type (T): 2-bit unsigned integer. Indicates if this message is of type Confirmable (0), Non-Confirmable (1), Acknowledgement (2) or Reset (3). See Section 4 for the semantics of these message types.

Option Count (OC): 4-bit unsigned integer. Indicates the number of options after the header (0-14). If set to 0, there are no options and the payload (if any) immediately follows the header. If set to 15, then an end-of-options marker is used to indicate the end of options and the start of the payload. The format of options is defined below.

CoAP/implementations

- Contiki-2.6
  - ETH Zurich
    - 8.5 kB ROM
    - 1.5 kB RAM
- Linux → libcoap
- TinyOs (libcoap)
- Firefox CoAP plugin – install an test.
- Wikipedia has an upated list. Check it!

CoAP/URI

coap URI

coap://example.se:5683/~sensors./temp1.xml

coaps URI

coaps://example.se:XXXX/~sensors./temp1.xml

CoAP/Secure

- DTLS (Datagram TLS) RFC4347
- IPSEC alternative (has problems)
  - DTLS as-is has problems. For normal network
  - Compressed DTLS proposed
  - Different implemenations
  - DTLS i Contiki
  - Propitary stack from sensinode.

    White paper good summary.
- Crucial f. function & understanding. Project?

IEEE 802.15.4 Monitor/Snoop

- Project?

  Hack Contiki to monitor activity?

    sensd should be a good start...

References

- The Contiki OS. http://www.contiki-os.org/

- draft-ietf-core-coap-12 https://datatracker.ietf.org/doc/draft-ietf-core-coap/
- draft-ietf-core-block-10 https://datatracker.ietf.org/doc/draft-ietf-core-block/
- draft-ietf-core-observe-07 https://datatracker.ietf.org/doc/draft-ietf-core-observe/
- draft-ietf-core-link-format-14 https://datatracker.ietf.org/doc/draft-ietf-core-link-format/

- M. Kovatsch, S. Duquennoy, and A. Dunkels, A Low-Power CoAP for Contikiâ in Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on, 2011, pp. 855-860, DOI:10.1109/MASS.2011.100.

- 6LowPAN, Zach Shelby, Carsten Borman (2009)

- IANA: RFCUniform Resource Identifier (URI) Schemes. [RFC4395]

- Nanoservice. Sensinode.Security Whitepaper www.sensinode.com

- R. Olsson and J. Laas, Sensd. http://github.com/herjulf/sensd.