nano-tera.ch
swiss scientific initiative in health / security / environment systems

SEC-WEAR NTF

FNSNF

LEXCOMM: A Low Energy, Secure and Flexible Communication Protocol for A Heterogeneous Body Sensor Network

Bishal Lamichhane[§], Steven Mudda[¥], Francesco Regazzoni[¶] and Alessandro Puiatti[¥]

[§]ECED, SVNIT, Gujarat, India , [¥]University of Applied Sciences of Southern Switzerland, Manno, Switzerland, [¶]ALaRi Institute, University of Lugano, Lugano, Switzerland

University of Applied Sciences and Arts of Southern Switzerland
SUPSI

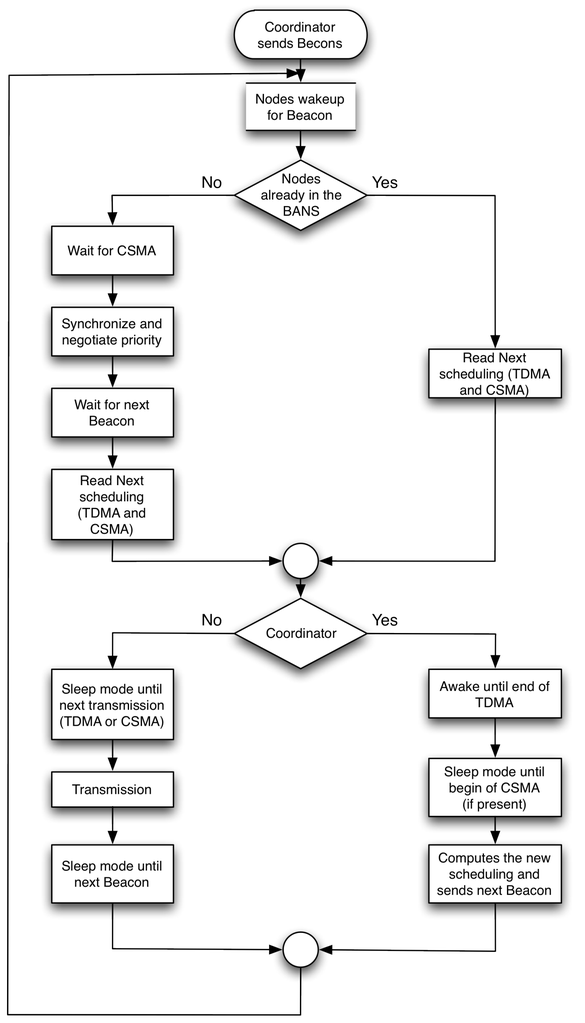
Why a new protocol?

- Lack of flexibility
- Only some issues addressed
- BASN Heterogeneity not addressed

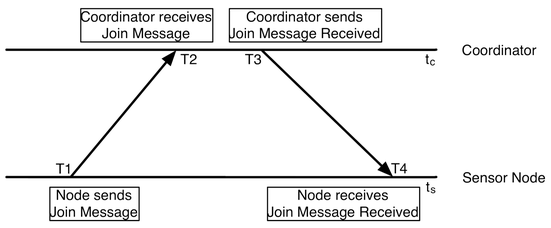
- The communication protocol has to:
  - Manage fixed periodicity, guarantee bandwidth and occasional transmissions;
  - Be flexible enough to operate for different set of sensors in the network
- Star topology for the network with a limited number of maximum node
- Address changes in the network structure without affecting energy consumption and bandwidth/ throughput

Considerations

- BASNs are intrinsically heterogeneous => different sampling frequencies, different transmission periodicity, asynchronous/synchronous data, different data rates
- The type of disease that has to be monitored governs the overall requirement of the BASN (number and kind of sensors)
- The nodes are deployed on the subject:
  - The distance from the nodes to a network coordinator (e.g. Smartphone), generally, does not require a multi hope scheme
  - The maximum number of nodes in the BASN is limited
- Multi hop/Mesh topology will just accrue the data rate requirements of nodes closer to the network coordinator
- Balance between flexibility (allow any new node to join at any time), and bandwidth degradation (listening for new connections when least expected)



Synchronization



$$\text{Transmission Delay} = \frac{(T2 - T1) + (T4 - T3)}{2}$$

$$\text{Clock Drift} = \frac{(T4 - T3) - (T2 - T1)}{2}$$

Protocol Description

Implementation and Results

Implemented on Shimmer Platinum Development Kit with the following sensors and parameters

Sensor	Sampling Rate (Hz)	Number of Channels	Number of encryption blocks per Beacon
ECG	144	2	36
EMG	480	1	60
GSR	16	1	2
Magnetometer Accelerometer	48	3*2	36
Temperature	2	1	-

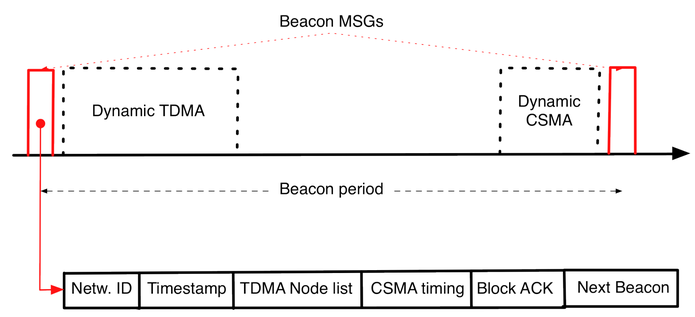
Data rate and encryption blocks per beacon for the different sensors used

- Hundreds of experiments with thousands of beacon periods in each run
- Slot allocation, acknowledgement and retransmissions tested and worked correctly
- Average throughput of 85.93% considering also TinyOS overhead
- Packet Delivery Ratio as follows

Sensor	PDR
ECG	98%
EMG	99.5%
GSR	100%
Magnetometer/Accelerometer	99.7%
Temperature	100%

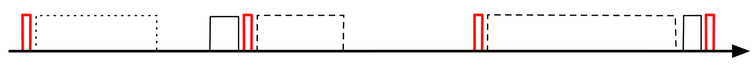
Packet delivery Ratio for different sensors

Beacon structure



Dynamic TDMA

Dynamic CSMA

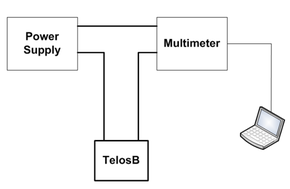


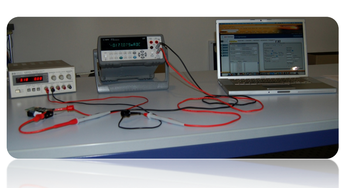
Node Priority

- Depends on the node constraints
- Determines the sequence in the TDMA
- In case of noisy channel (needs for retransmissions), nodes with low priority can be shifted from TMDA to CSMA

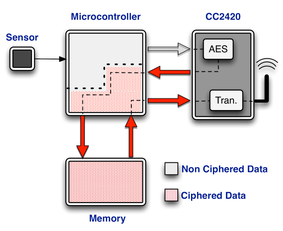
Security

Experimental Setup

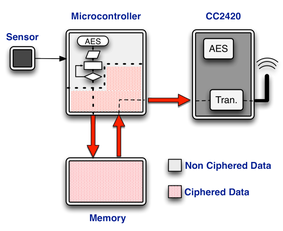




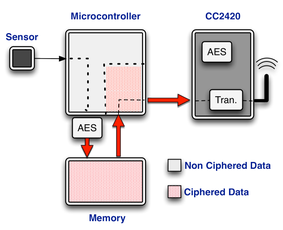
Encryption with AES in CC2420



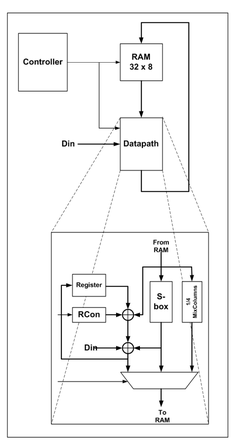
Software Encryption in Microcontroller



Dedicated Hardware Encryption Module



AES Architecture

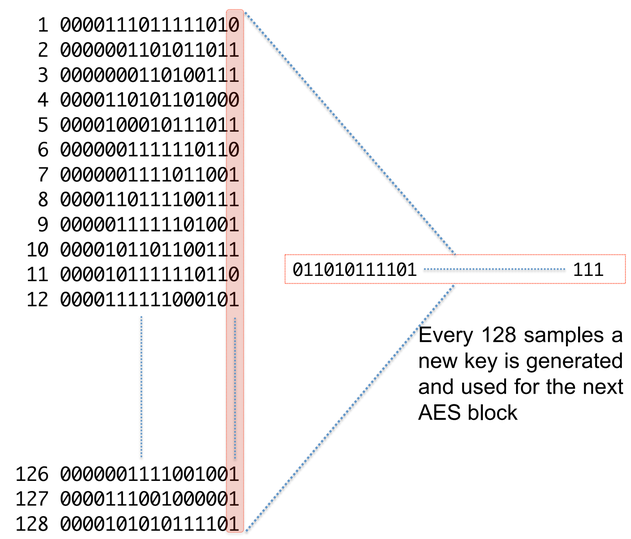


Parameter	Encryption CC2420	Software Encryption	Hardware Encryption (*)
Av. Current (mA)	10	1.9	0.065
Av. Energy (µJ)	273	241.68	4.63
Av. Power (mW)	30	5.7	0.065
Time (ms)	9.1	42.4	71.35

Data averaged over thousands of transmissions of 16 encrypted blocks per transmission

(*) Post place and route Synopsys NanoSim™ simulation

Key Generation



Every 128 samples a new key is generated and used for the next AES block

Data from sensors