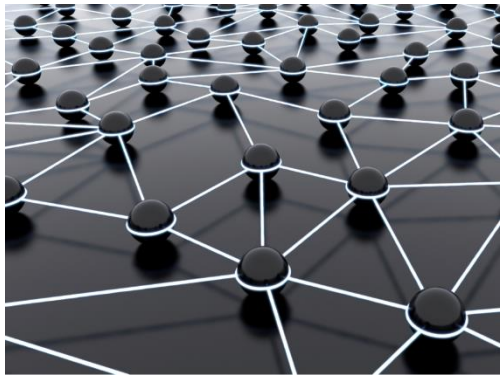
A jövő internete, BMEVITMAV74

BME-VIK és DE-IK közös szabadon választható tárgya

Szenzor hálózatok

Gál Zoltán PhD

Debreceni Egyetem



Debrecen, 2017. tavasz

Tartalom

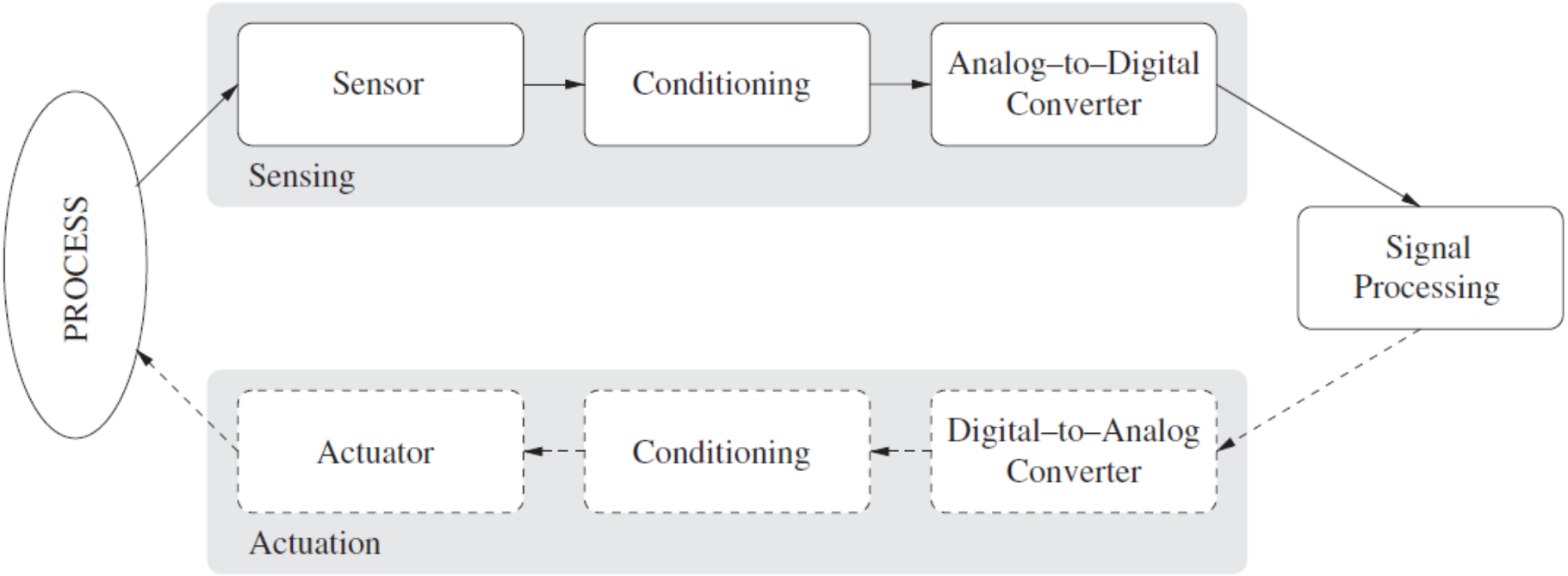
1.) Érzékelés és vezérlés alapok
2.) Alkalmazási példák
3.) Csomópont architektúra
4.) Operációs rendszer és referencia modell
5.) Fizikai réteg
6.) Közeghozzáférés vezérlési réteg
7.) Hálózati réteg
8.) Energia menedzsment
9.) Idő szinkronizálás
10.) Biztonság

1.) Érzékelés és vezérlés alapok

- Jelenség:
  - Esemény (event), folyamat (process)
  - Rendszer (system)
- Átalakító (transducer):
  - Eszköz, amely az energiát egyik formából a másikba alakítja át
- **Szenzor (sensor):**
  - Érzékelést végző objektum (fizikai vagy virtuális)
  - Eszköz: a fizikai világ jellemzőjét vagy eseményét mérhető és elemezhető jellé alakítja
  - Speciális átalakító: a fizikai világ energiáját elektromos energiává alakítja, ami számítógéphez vagy kontrollerhez küldhető
- **Beavatkozó (actuator)**:
  - Speciális átalakító, amely az elekt. vezérlő energiát a folyamat számára más fajta energiává alakítja át

1.) Érzékelés és vezérlés alapok

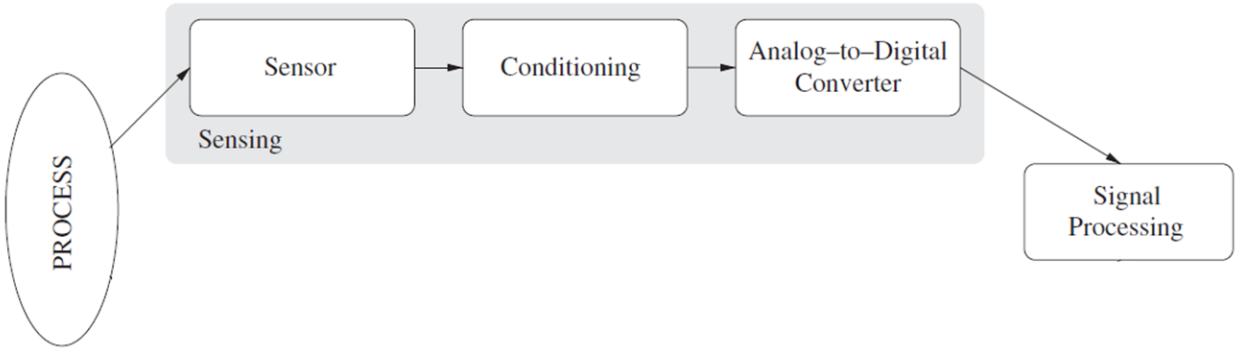
- Érzékelés:
  - Adatbegyűjtési technika folyamatról
- Vezérlés:
  - Hatás kifejtése folyamat számára



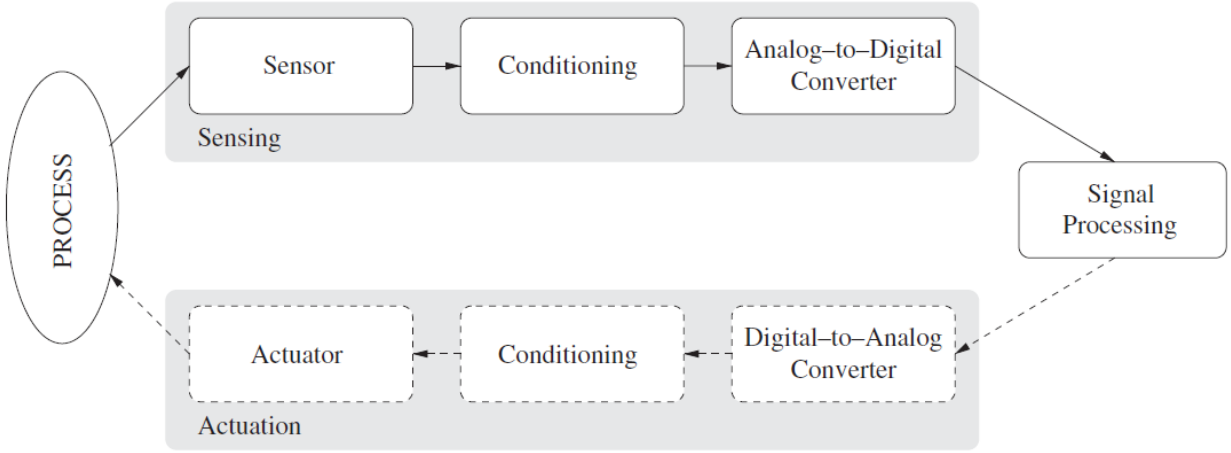
- Szabályozás (conditioning):
  - Erősítés/gyengítés, szűrés, módosítás, stb.

1.) Érzékelés és vezérlés alapok

- Szenzor hálózat (SN – Sensor Network): makroszkóp
  - Érzékelésre alkalmas kommunikációs rendszer



- Szenzor és aktuátor hálózat (SAN – Sensor and Actuator N.)
  - Érzékelésre és vezérlésre alkalmas komm. rendszer



1.) Érzékelés és vezérlés alapok

- **Szenzorok osztályozása**:
  - Alkalmazott érzékelési módszer szerint:
    - Rezisztív (hőmérséklet, nyomás, fényerő, nedvesség)
    - Kapacitív (mozgás, közelség, gyorsulás, nyomás, elektromos térerő, kémiai összetétel, folyadék vastagság)
    - Induktív (közelség, pozíció, erő, nyomás, hőmérséklet, gyorsulás)
    - Piezoelektromos (nyomás, erő, feszítés, gyorsulás) (nem érzékeny az EM térerőre és a sugárzásra)
  - Energiaforrás szerint:
    - Aktív: külső energiával működő
    - Passzív: környezetéből táplálkozó
      (pl. PIR – Passive Infrared)

1.) Érzékelés és vezérlés alapok

- Szenzorok:

Koncentráció

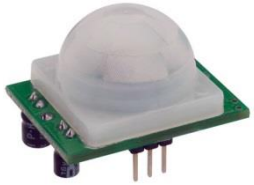
Hang

Rezgés

Fény

Sebesség

Közelség



Mozgás

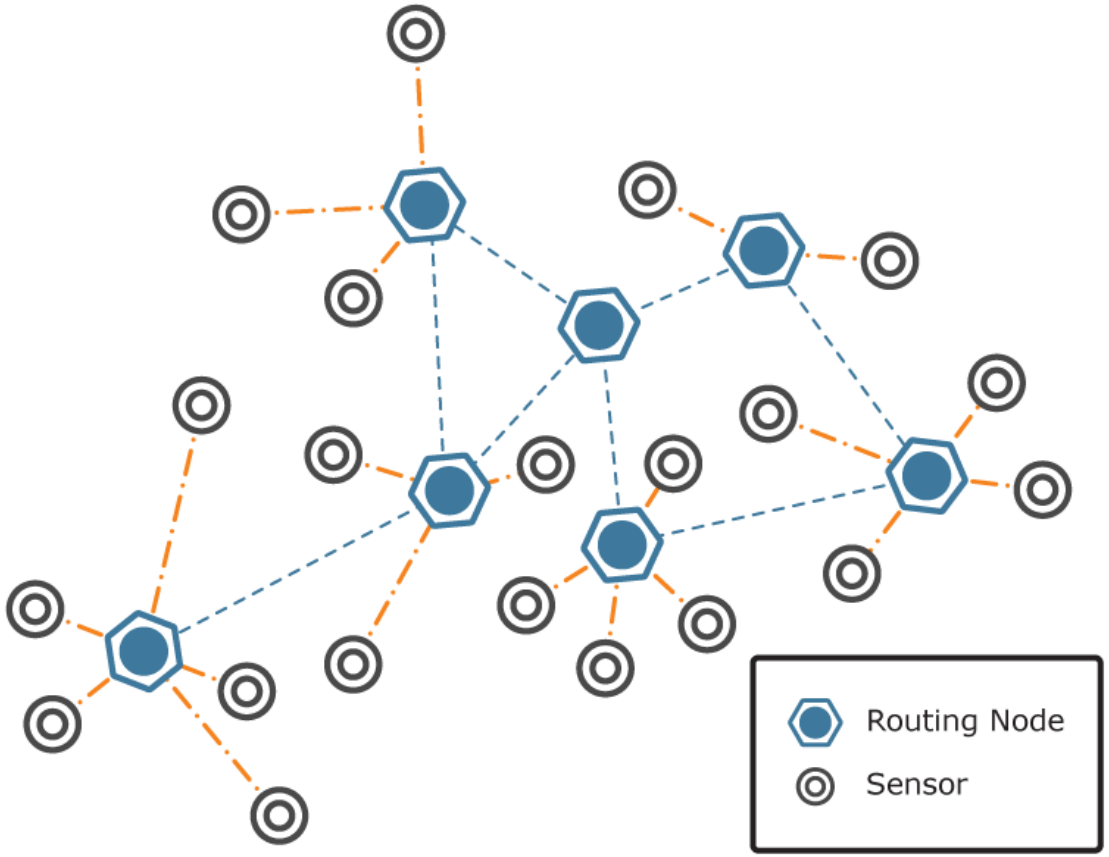
Elmozdulás

Ütközés

Erő

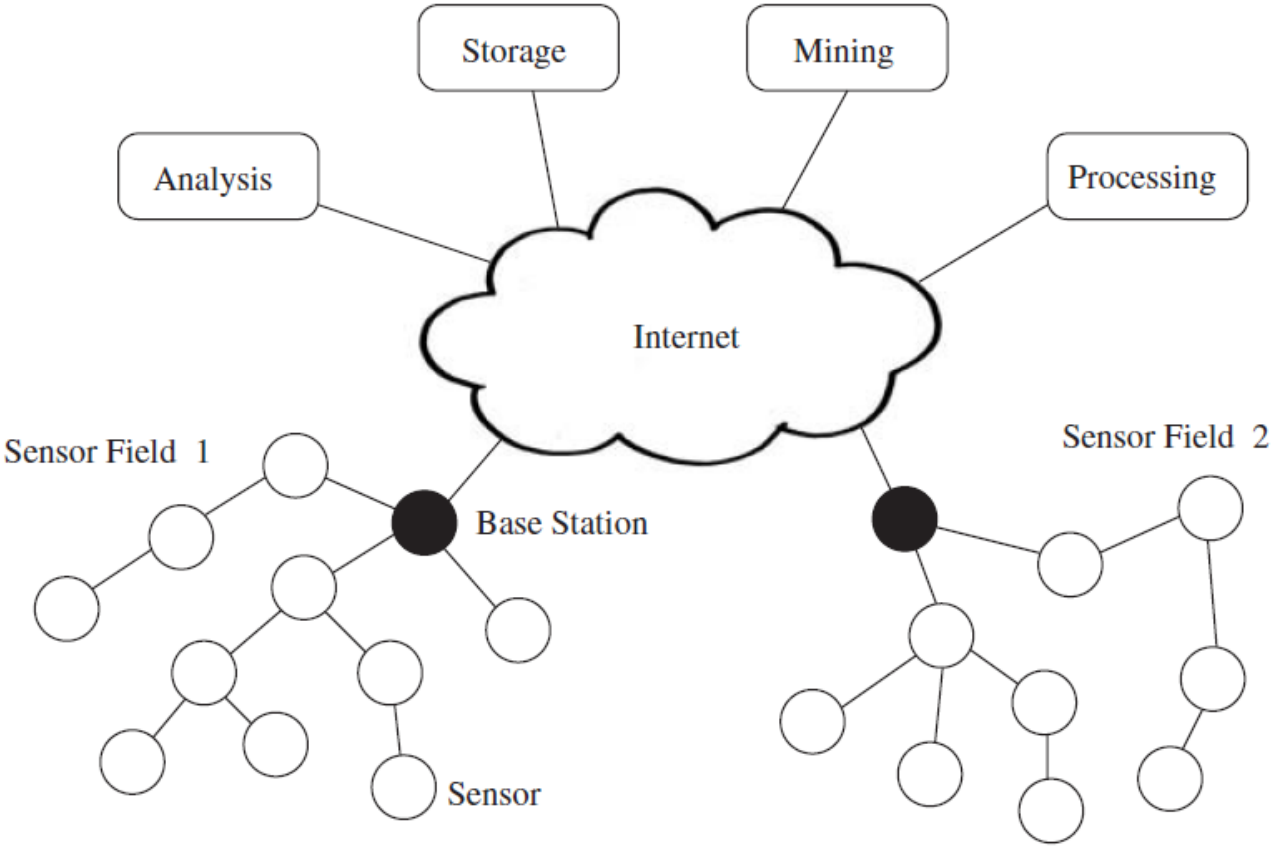
1.) Érzékelés és vezérlés alapok

- **Szenzor hálózat típusok**:
  - Vezetékes: rögzített
  - Vezetéknélküli (WSN): mobil, legelterjedtebb
  - Vegyes, hibrid (HSN)



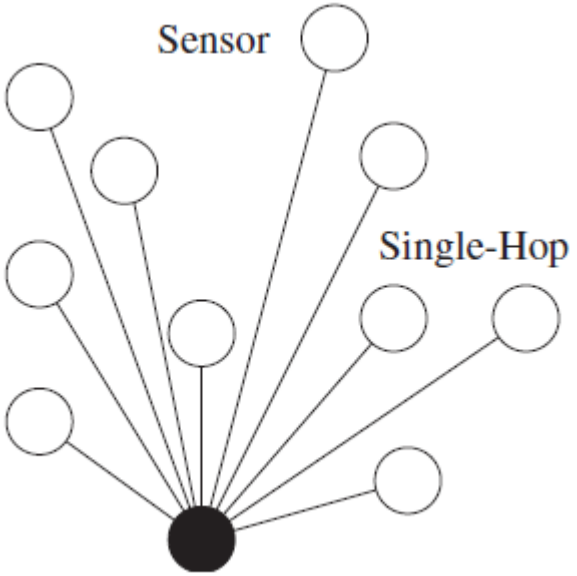
1.) Érzékelés és vezérlés alapok

- **WSN rendszer felépítése**:
  - Szenzor csomópont: érzékelés és kommunikáció
  - Bázisállomás (Base Station/Sink): kommunikáció
  - (Elemző, Tároló, Értelmező, Feldolgozó)

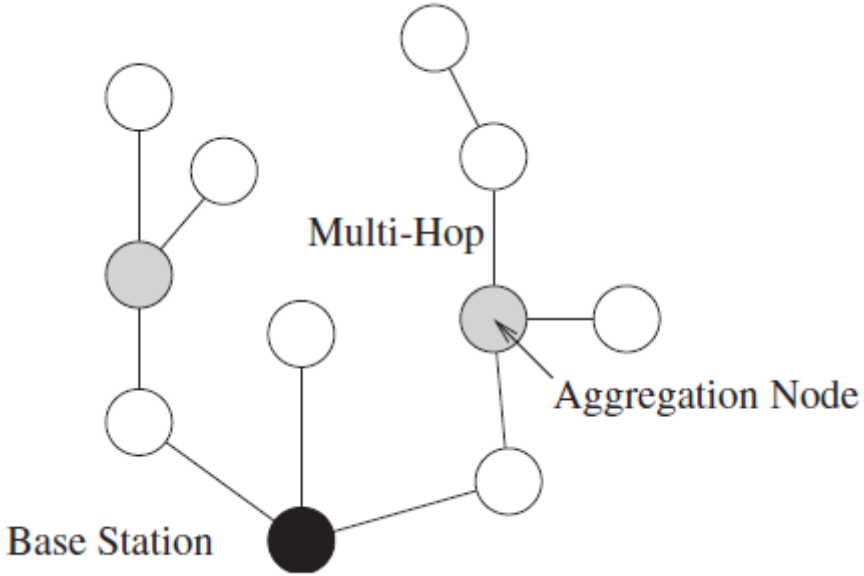


1.) Érzékelés és vezérlés alapok

- **WSN rendszer kommunikációja**:
  - Közvetlen kommunikáció (pl. IEEE 802.11)
  - Közvetett kommunikáció (pl. IEEE 802.15.4)



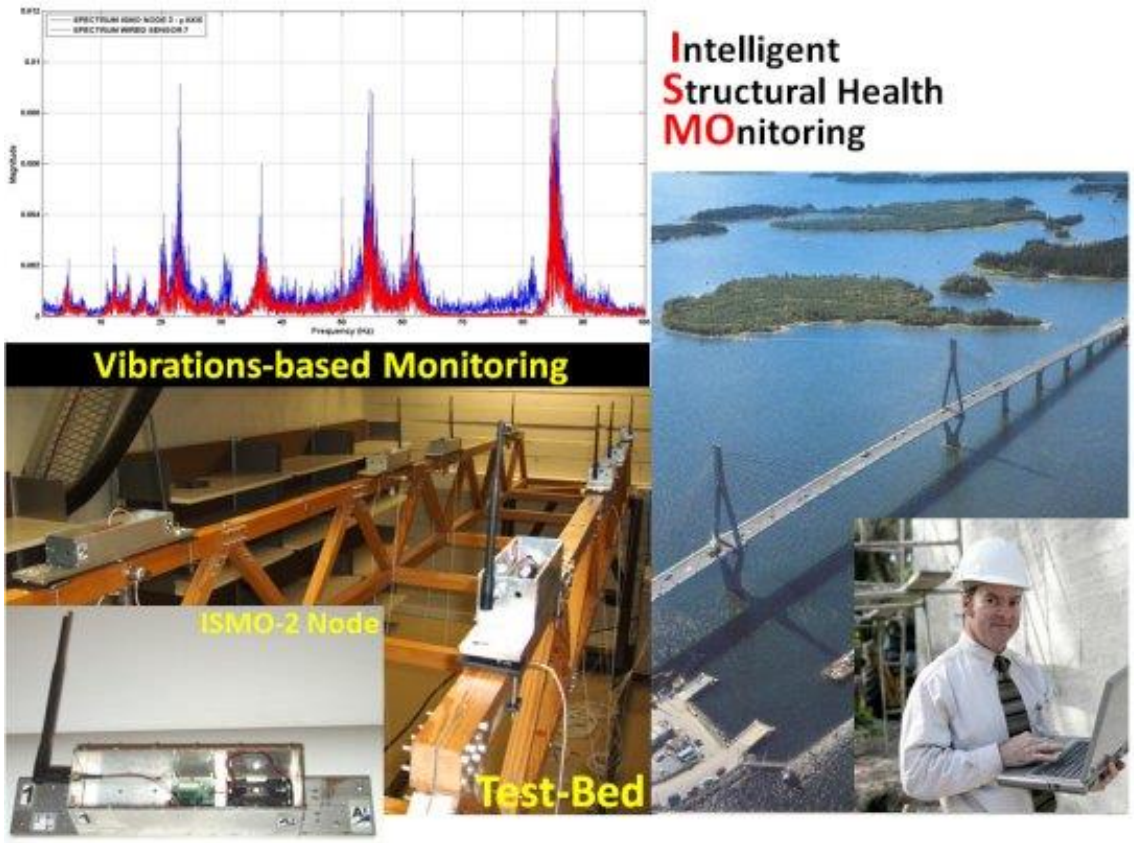
egyszerű routing



komplex routing

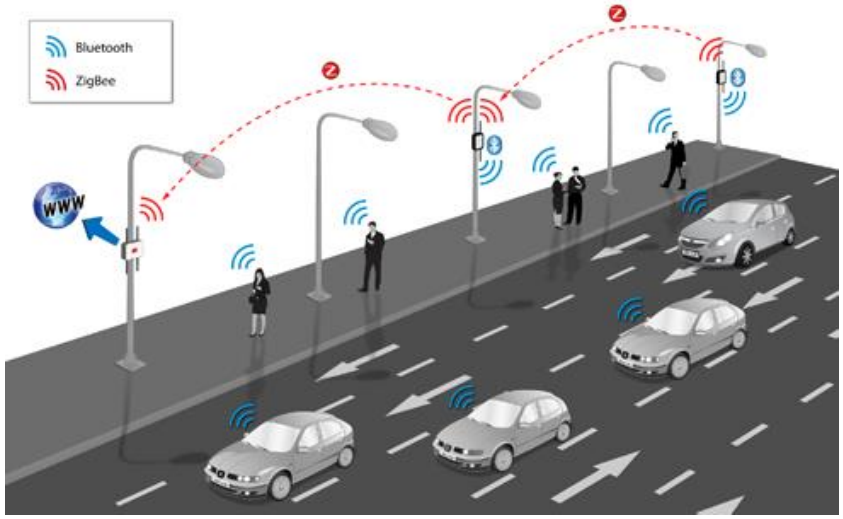
2.) Alkalmazási példák

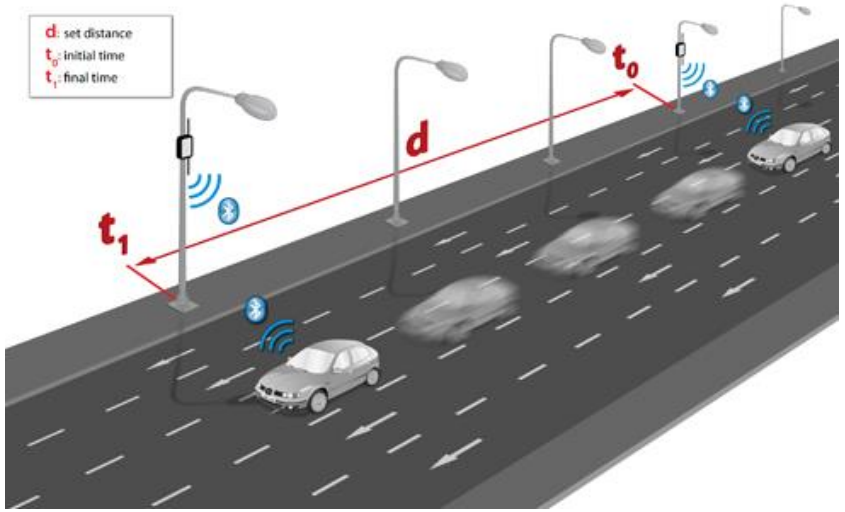
- Épületek (hidak, toronyházak, gátak) állagának ellenőrzése:
  - Hozzá nem férhető helyeken elhelyezés
  - Válaszok apró, teszt-rezgésekre



2.) Alkalmazási példák

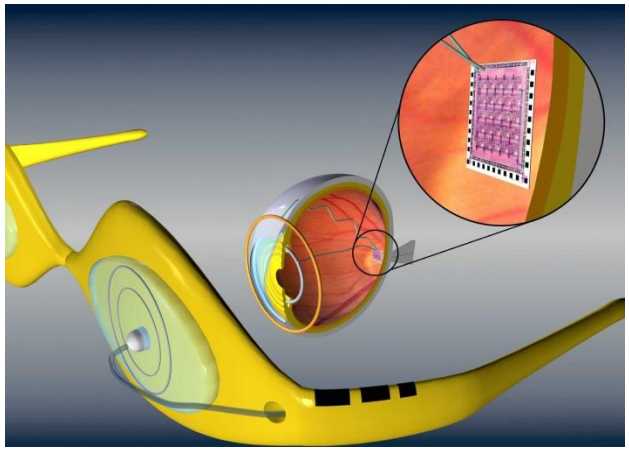
- Közúti forgalom szabályozása:

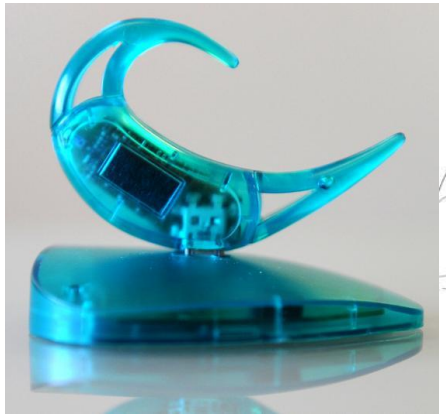


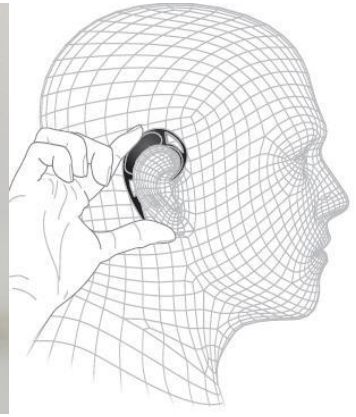


2.) Alkalmazási példák

- Egészség gondozása:
  - Mesterséges retina
  - Parkinson-kór monitorozás, stb.

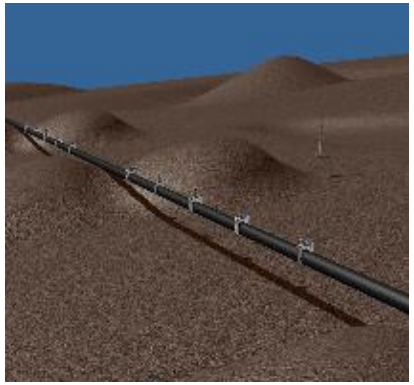


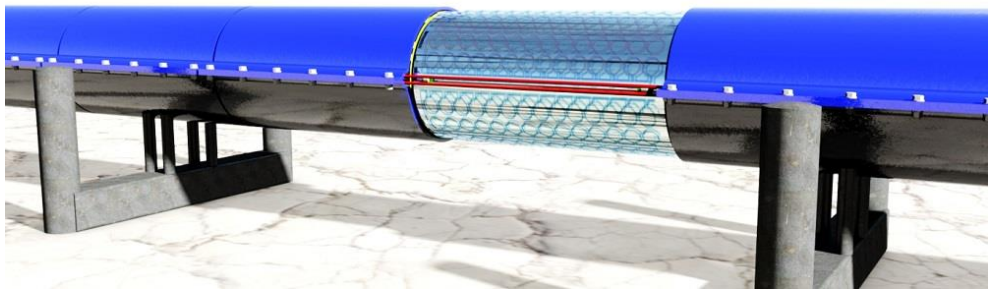




2.) Alkalmazási példák

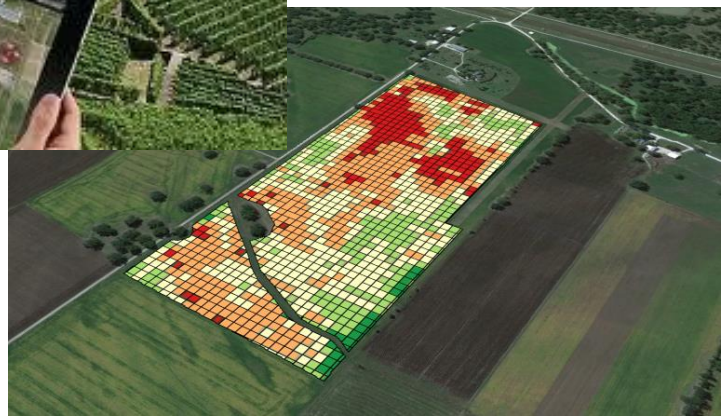
- Csőrendszer (víz, csatorna, gáz) monitorozása





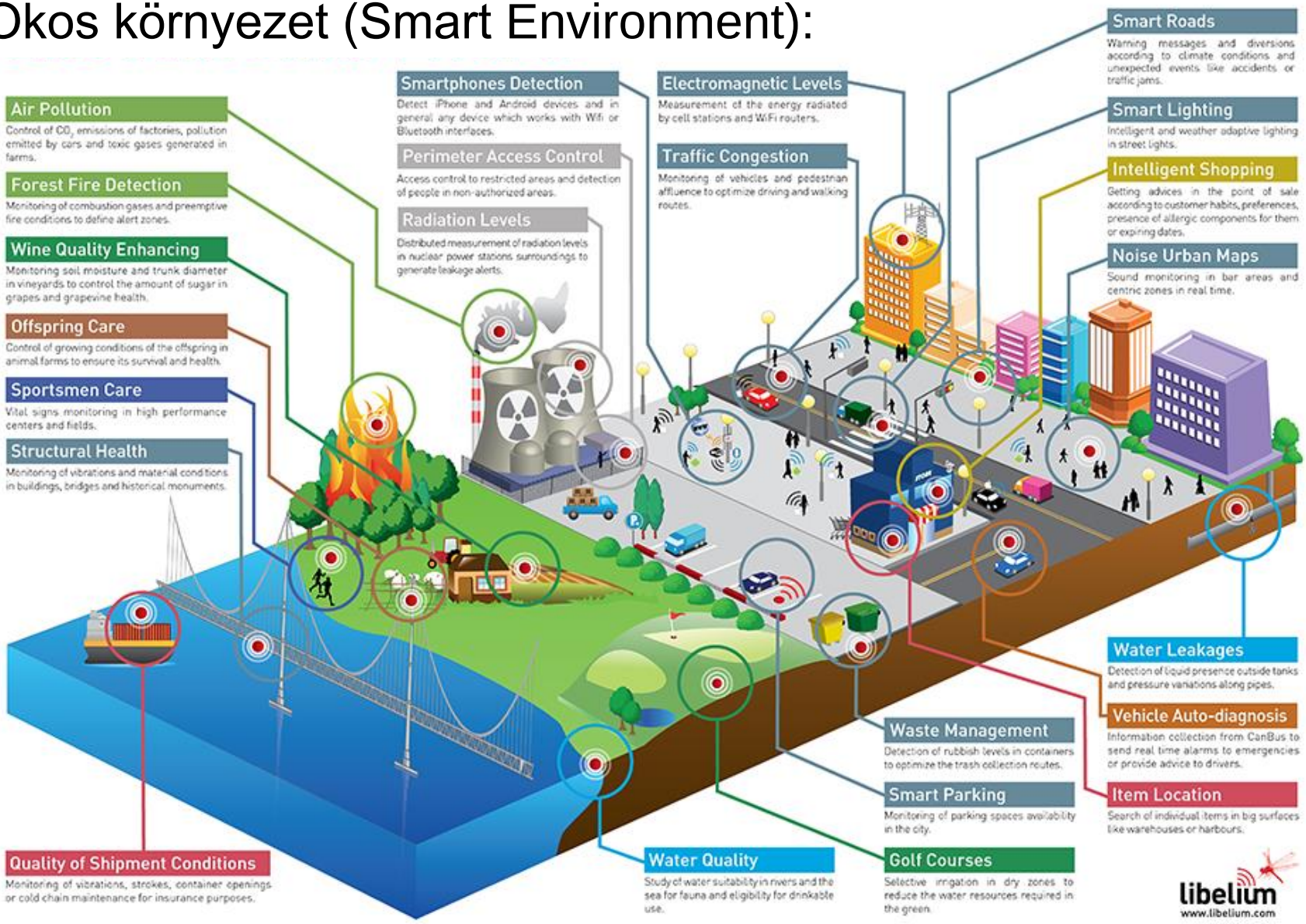
2.) Alkalmazási példák

- Precíziós mezőgazdaság:
  - Növény monitorozás
  - Igény szerinti trágyázás
  - Igény szerinti öntözés
  - Pozicionálás



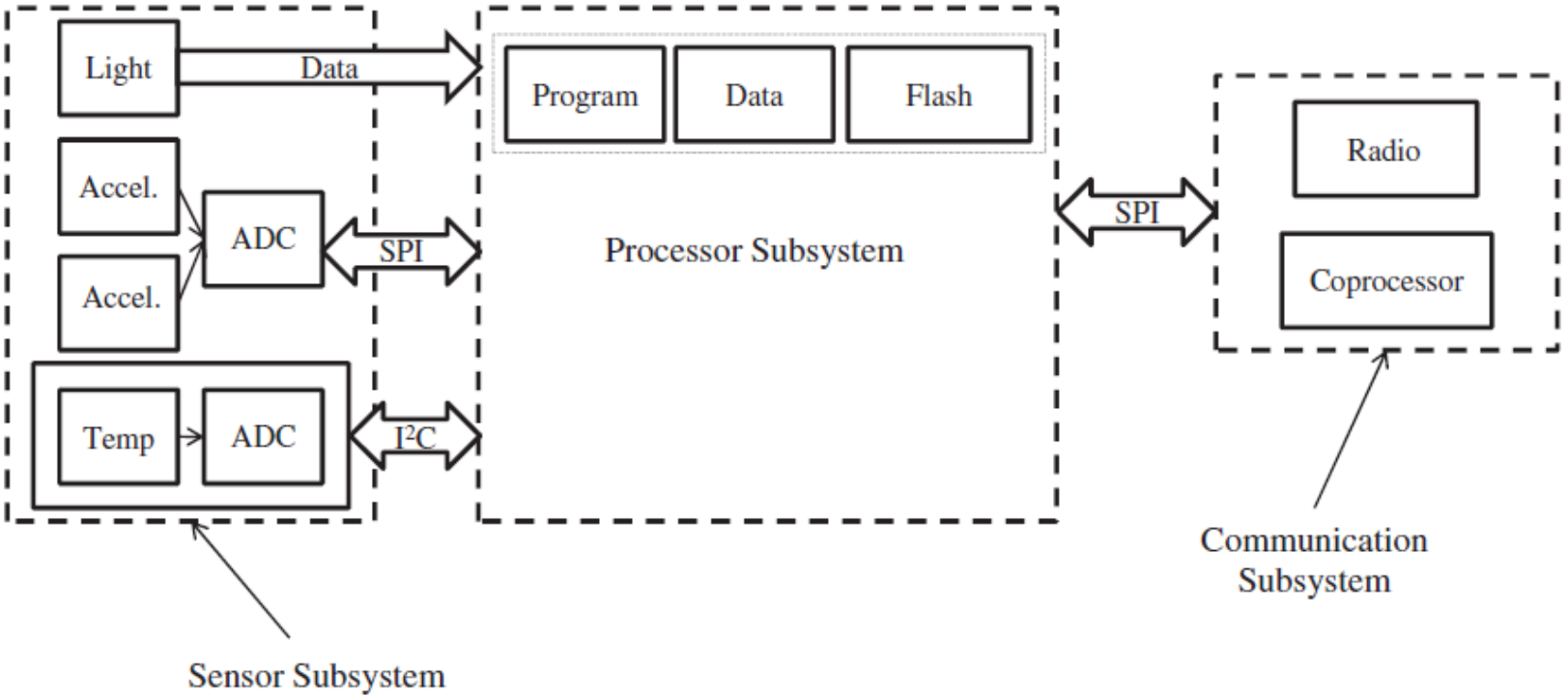
2.) Alkalmazási példák

- Okos környezet (Smart Environment):

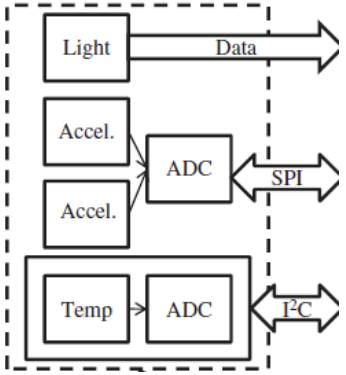


3.) Csomópont architektúra

- **Csomópont által megvalósított funkciók**:
  - Érzékelés
  - Feldolgozás (mikrokontroller, DSP, ASIC, FPGA)
  - Kommunikáció (belül SPI, kívül WiFi, ZigBee, NFC, …)
  - Energia menedzsment (DC)
  - Belső kapcsolat (SPI – Serial Peripheral Interface busz)



3.) Csomópont architektúra



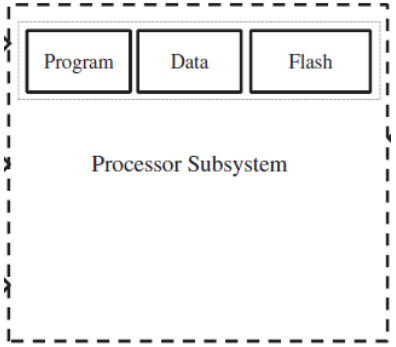
- **Csomópont érzékelő alrendszere**:
  - Egy vagy több szenzor integrálása
  - ADC átalakítók: időben és értékben diszkrét,
    - kvantálási felbontás (Q)

$$Q = \frac{E_{\mathrm{pp}}}{2^M}$$

    - mintavételezési ráta (f_s): zaj miatt $f_s > f_{Nyquist}$

  - Pl.: [-20 ˚C, +80 ˚C] tartományban hőmérséklet mérése
    - 0,5 ˚C pontossággal: M = 8 ($100/2^8$ =0,39)
    - 0,1 ˚C pontossággal: M = 10 ($100/2^{10}$ =0,09)
  - Fontos: legtöbb ADC mérési pontossága érték-függő
    - MSB: 1,5·Q szerint
    - (MSB…LSB): 1,0·Q szerint
    - LSB: 0,5·Q szerint

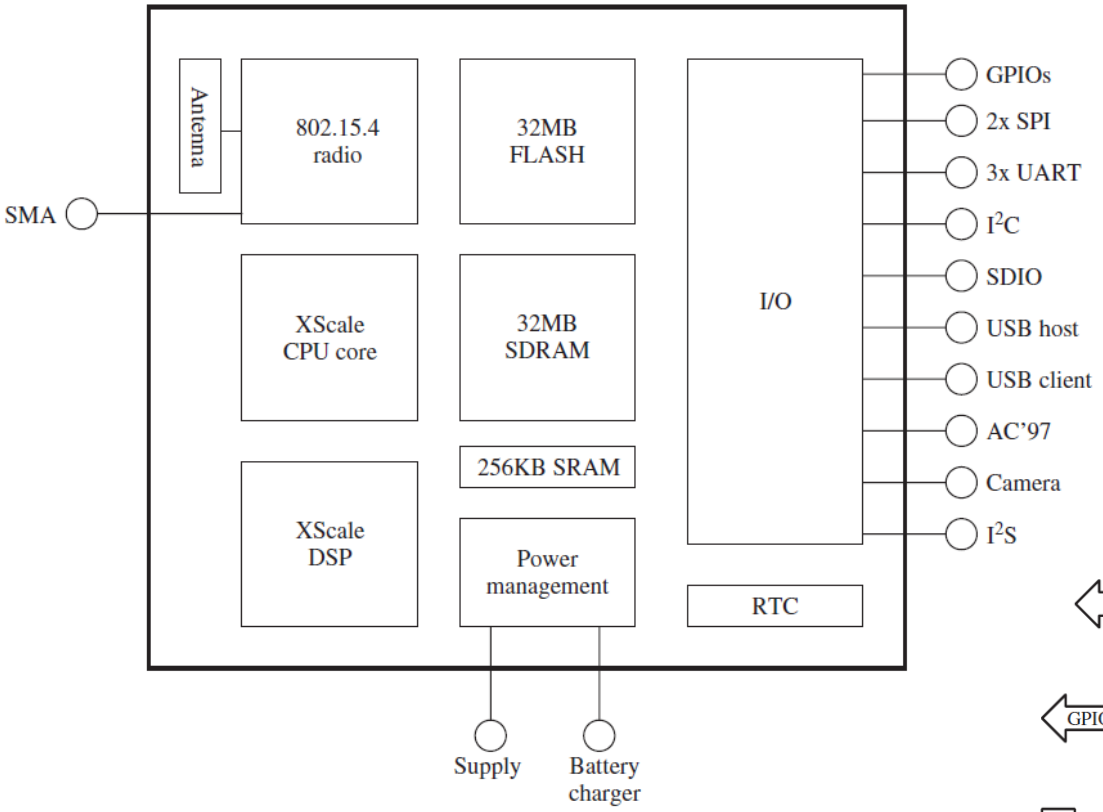
3.) Csomópont architektúra



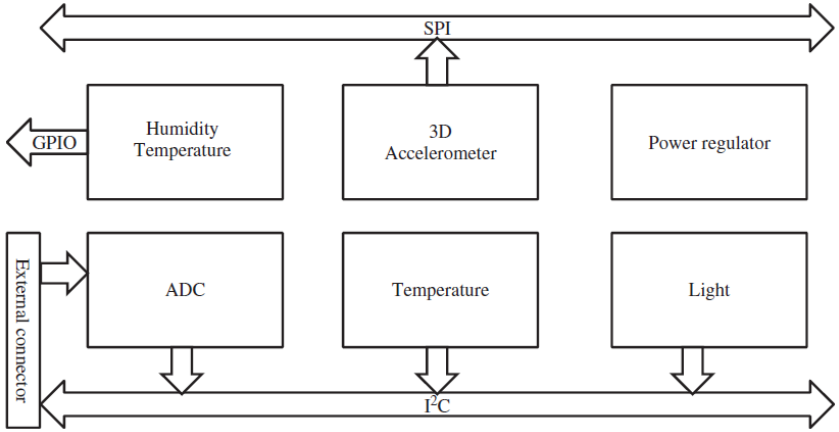
- **Csomópont feldolgozó alrendszere**:
  - Összehangolja az érzékelést, kommunikációt és önszervezést
  - Elemek: P, Flash, RAM, Clock
  1) P (Processzor):
     - Általános mérési folyamatnál alkalmazzák
     - Szempontok: költség, rugalmasság, számolási teljesítmény, energiafogyasztás
     - Előny: bő választék létezik a piacon
     - Hátrány: energiahasználat viszonylag magas
  2) P (DSP, ASIC, FPGA):
     - Rögzített mérési folyamatnál alkalmazzák
     - Előny: energiafogyasztásúk hatékony
     - Hátrány: tervezés és kivitelezés költséges
  3) P (mikrokontroller):
     - legelőnyösebb ötvözött megoldás

3.) Csomópont architektúra

- Csomópont példa 1.: **Imote (Imote2) Node** (Crosbow Tech. Inc.)
  - többcélú architektúra

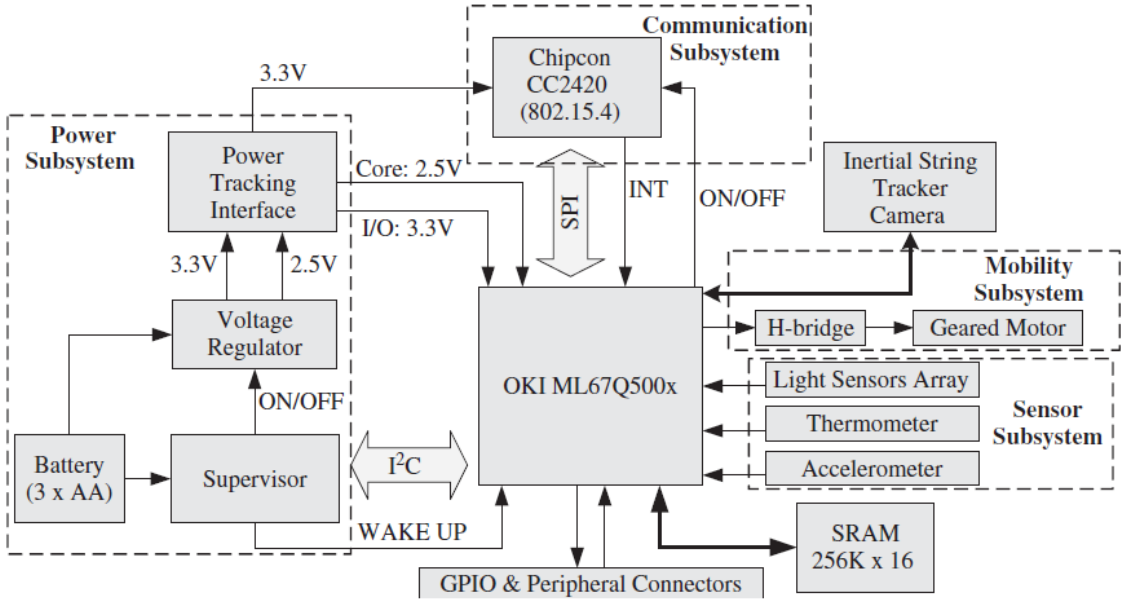


Érzékelő alrendszer



3.) Csomópont architektúra

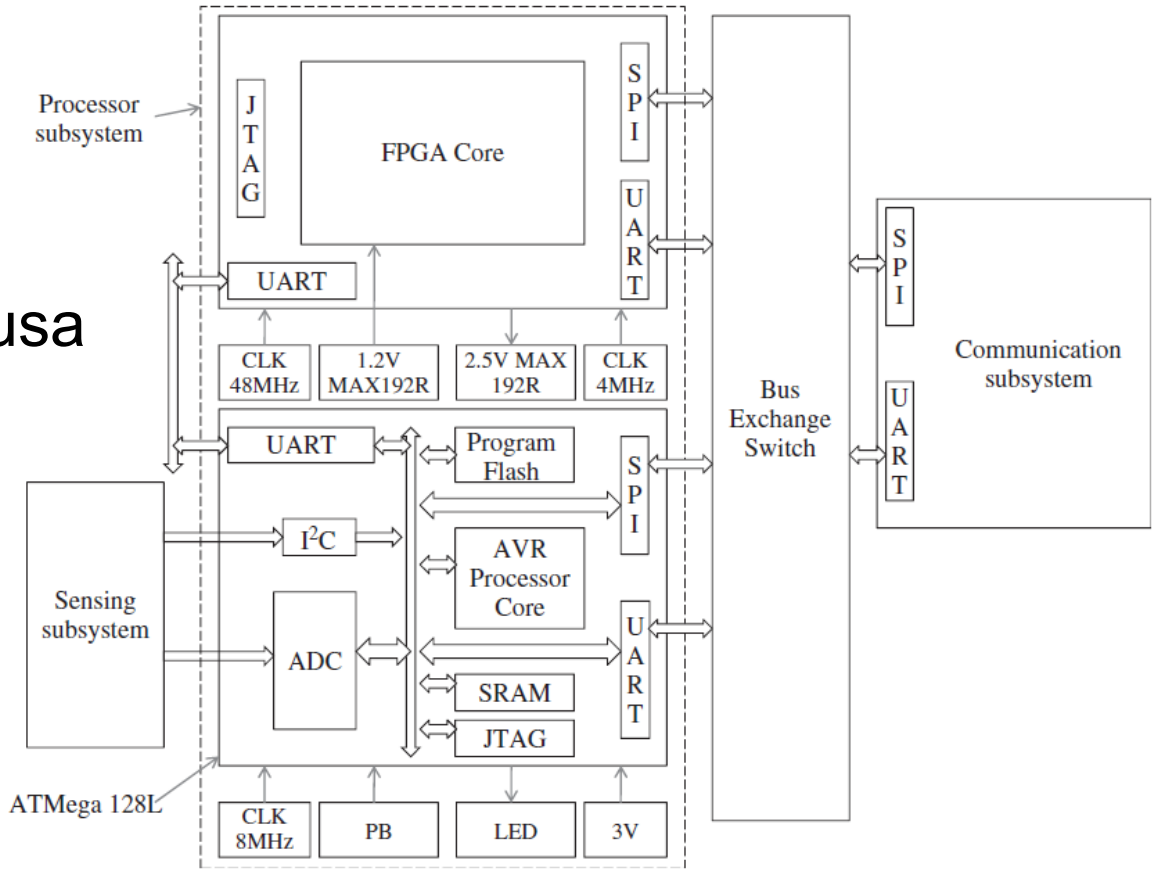
- Csomópont példa 2.: **XYZ Node** (Yale University, open source)
  - mikrokontroller alapú
  - Négy 10-bites ADC bemenet
  - Kommunikáció: RS232, SPI, I²C, SIO, GPIO, IEEE 802.15.4



3.) Csomópont architektúra

- Csomópont példa 3.: **Hogthrob Node** (Hogtrob Project, 2004)
  - P (2 db): rendszer
  - Mikrokontroller (1 db): kommunikáció vezérlése
  - FPGA (1 db): monitorozás
  - SPI, I^2C: adat
  - JTAG: program

  - Állatok életritmusa



4.) Operációs rendszer és referencia modell

- WSN csomópont **OS funkciók**:
  - Memória menedzsment
  - Energia menedzsment
  - Fájl menedzsment
  - Hálózat kezelés
  - Programozási környezet és eszközök
  - Érzékelő erőforrások hozzáférése írásra
- OS-ek osztályozása:

Task \ User	Single-user	Multi-user
Single-task	STSU	STMU
Multitask	MTSU	MTMU

  - MT: előnyös lenne, de erőforrás igényes
  - ST: a task-ok csak rövidek lehetnek
  - SU/MU: egy/több felhasználó használja egyszerre a közös erőforrásokat

4.) Operációs rendszer és referencia modell

- **WSN OS kiválasztásának megfontolásai**:
    1.) Adat típus:
        - Komplex adat: sok információ és sok erőforrás
        - Egyszerű adat: kevés információ olcsón
    2.) Task ütemezés:
        - Queuing alapú: várakozás és sorrendi szabály
            - FIFO: beérkezési sorrendben, de hosszú task blokkolhat rövid task-ot
            - Rendezett Queue: szabály alapján (pl. végrehajtási idő: SJF), de folyamatos sorba rendezés szükséges.
        - Round-Robin alapú: ki nem használt időszelet következő aktív task-hoz rendelése
        - Preemptív/Nempreemptív típusú: interrupt kezelés szükséges kezdeményező esetén

4.) Operációs rendszer és referencia modell

- **WSN OS kiválasztásának megfontolásai (folyt.)**:
  - 3.) Vermek:
    - LIFO szabály szerinti adat hozzáférés
    - Többszálas OS túlságosan költséges WSN-nek
  - 4.) Rendszer hívások:
    - Szenzor, watch-dog időzítő, rádiós interfész elérése ezeken keresztül
  - 5.) Megszakítás kezelés:
    - Interrupt jel: hardver (szenzor, watch-dog, rádiós interfész) által generált aszinkron jel
    - Interrupt kezelő (handler): megszakítástól függő tevékenységek (prioritások)
  - 6.) Többszálas futtatás:
    - párhuzamos szálak futása I/O alrendszernél
    - különböző futásidejű szálak egyszerre futhatnak

4.) Operációs rendszer és referencia modell

- **WSN OS kiválasztásának megfontolásai (folyt.)**:
  - 7.) Szál vagy esemény alapú programozás:
    - Szál alapú:
      - WSN erőforr. nem blokkolh. többszálnál
      - WSN adat védelme szüks. szemaforokkal
      - Program végreh. szinkronizált módon
    - Esemény alapú:
      - Események és eseménykezelők haszn.
  - 8.) Memória kezelés:
    - Fizikai korlátok miatt rövid kód szükséges
    - Időkorlátok miatt hatékony kód szükséges
    - Dinamikus: rugalmas, de menedzsment többlet
    - Statikus: fix helyen, de futáskor nem adaptálható
    - Kapacitás növelés: EEPROM/Flash, de energiát igényel az írás/olvasás

4.) Operációs rendszer és referencia modell

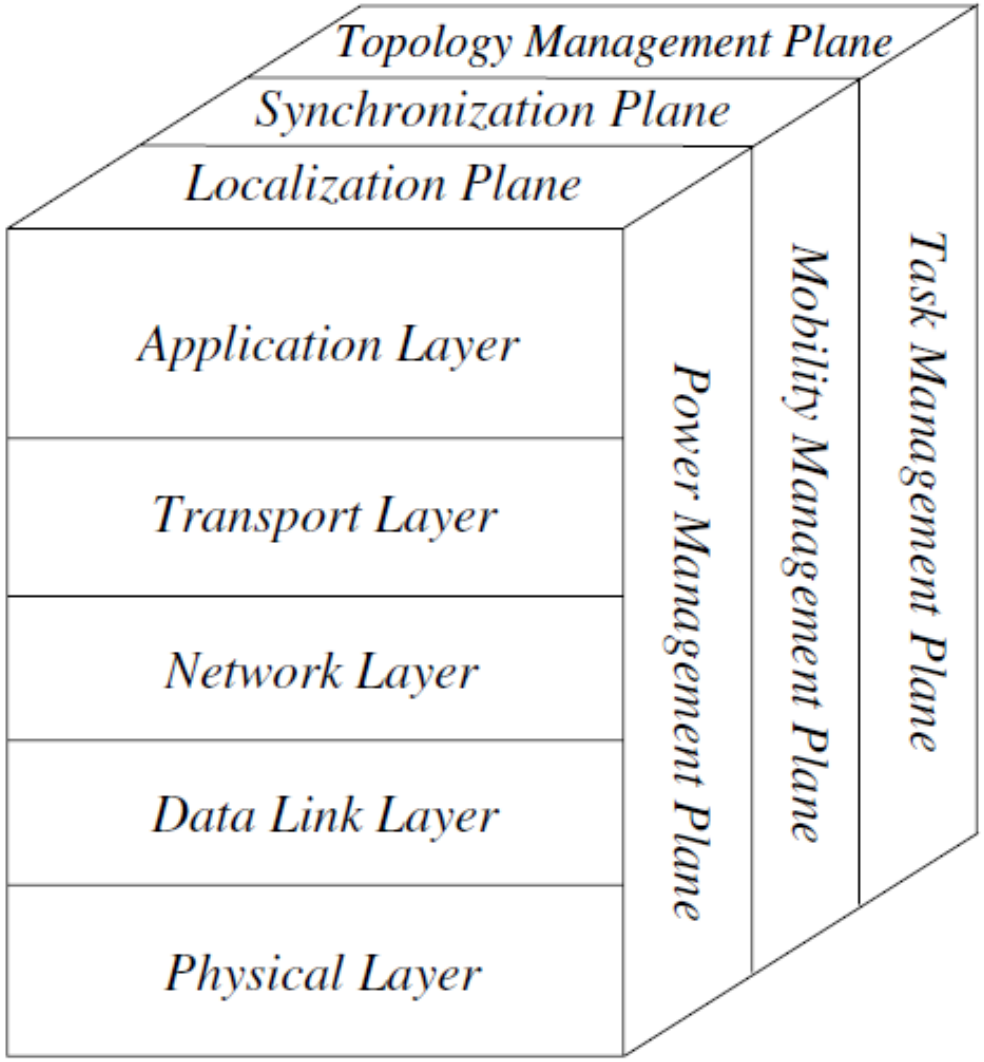
- **WSN OS-ek összehasonlítása:**

OS	Programming paradigm	Building blocks	Scheduling	Memory allocation	System calls
TinyOS	Event-based (split-phase operation, active messages)	Components, interfaces, and tasks	FIFO	Static	Not available
SOS	Event-based (active messages)	Modules and messages	FIFO	Dynamic	Not available
Contiki	Predominantly event-based, but it provides optional multithreading support	Services, service interface stubs, and service layer	FIFO, poll handlers with priority scheduling	Dynamic	Runtime libraries
LiteOS	Thread-based (based on thread pool)	Applications are independent entities	Priority-based scheduling with optional round-robin support	Dynamic	A host of system calls available to the user (file, process, environment, debugging, and device commands)

4.) Operációs rendszer és referencia modell

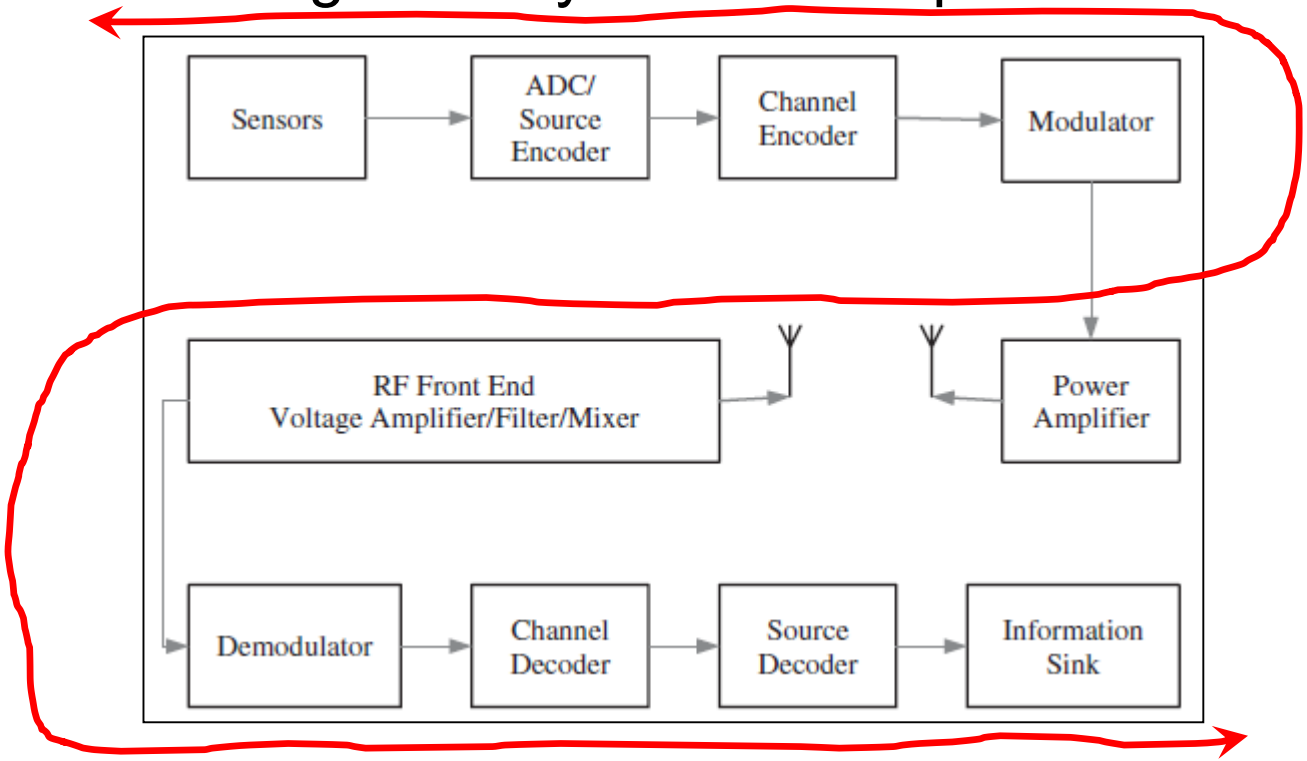
- **WSN protokoll stack:**

  - Rétegek
  - Síkok

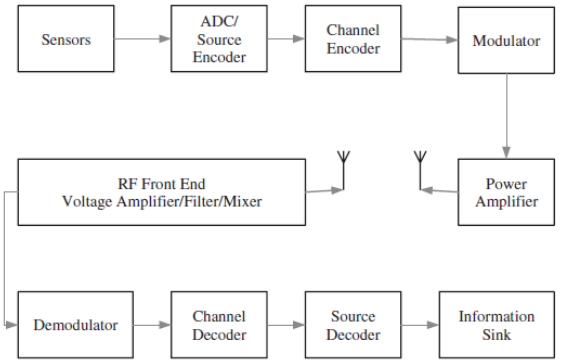


5.) Fizikai réteg

- **WSN kommunikációs kihívások**:
  - korlátos sávszélesség
  - korlátos hatótávolság
  - gyenge minőségű kézbesítési teljesítmény
    (interferencia, csillapítás, többutas szórás)
- WSN: kis távolságra elhelyezett csomópontok



5.) Fizikai réteg



- **Forrás kódolás:**
  - **ADC átalakítás**
    - Mintavételezés: s(t)
    - Kvantálás: S = (s[1], …, s[n])
    - Kódolás: s[j] < --- > szimbólum
      - szimbólum méret: r [bit]
      - kódkönyv: C (r változik szimbólumonként)
        - C(C(1), C(2), …(C(u))
        - gyakori mintának rövid szimbólum
        - ritka mintának hosszú szimbólum
      - tömbkód: C (r konstans szimbólumonként)
  - Egyértelműen dekódolható kódkönyv feltétele:

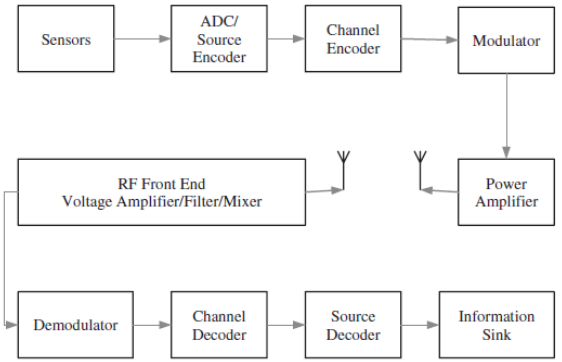
$$\sum_{i=1}^{u} \left(\frac{1}{r}\right)^{l_i} \leq 1$$

    - u[]: a kódkönyv hosszúsága
    - l_i [bit]: a C(i) kódszó hosszúsága

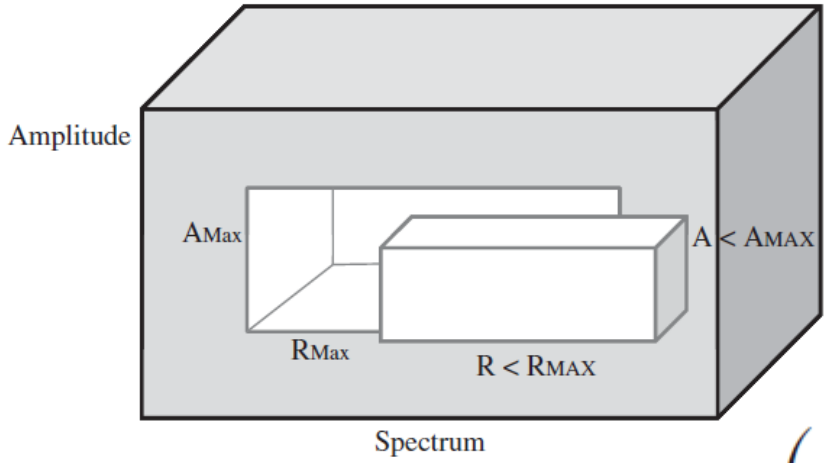
- **Forrás kódolás (folyt.):**
  - Azonnal dekódolható kódkönyv: ha minden szimbólum önállóan dekódolható, függetlenül az előzőektől
  - Példa kódok: C^1, C^2, …, C^6
    - s1, …, s4: r = 2
    - $\Sigma^1 = (1/2)^1+(1/2)^2+(1/2)^2+(1/2)^2 = 5/4 > 1$
    - $\Sigma^4 = (1/2)^1+(1/2)^2+(1/2)^3+(1/2)^4 = 15/16 < 1$

	C^1	C^2	C^3	C^4	C^5	C^6
s_1	0	00	0	0	0	0
s_2	10	01	100	10	01	10
s_3	00	10	110	110	011	110
s_4	01	11	11	1110	111	111
Block code	No	Yes	No	No	No	No
Uniquely decoded	No	Yes	No	Yes	Yes	Yes
$\sum_{i=1}^{n} \left(\frac{1}{2}\right)^{l_i}$	$1\frac{1}{4}$	1	1	$\frac{15}{16} < 1$	1	1
Instantly decoded	No	Yes (block code)	No	Yes (comma code)	No	Yes

5.) Fizikai réteg

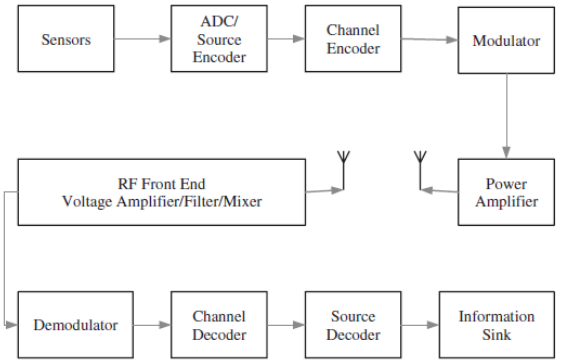


- **Csatorna kódolás**:
  - Cél: zajra ellenálló, hibadetektáló és FEC képesség
  - Egyszerű transceiver: csak hibadet.
  - Csatorna sztochasztikus modellje:



  - Shannon – Hartley tétel: $C = B \cdot \log_2\left(1 + \frac{S}{N}\right)$
    - C [b/s]: csatorna hiba nélküli kapacitása
    - B [Hz]: sávszélesség
    - S [W]: jel átlagos teljesítmény a teljes sávszél.
    - N [W]: zaj átlagos teljesítmény a teljes sávszél.

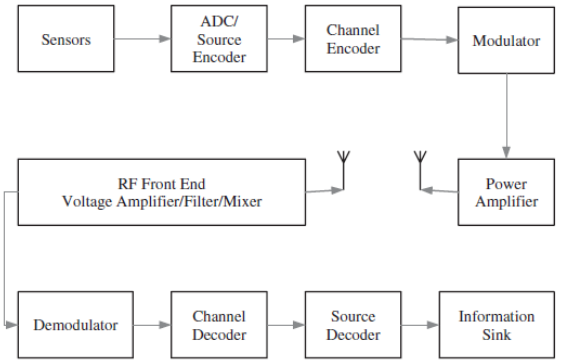
5.) Fizikai réteg



- **Moduláció:**
  - Vivő jel jellemzőinek (amplitúdó, frekvencia, fázis) módosítása időben az alapsávi üzenet függvényében
  - Előnyök:
    - üzenet jel rugalmas lesz a zajra
    - csatorna spektruma hatékonyan használható
    - jel detektálás egyszerű lesz
  - Típusok:
    - AM (Amplitude Modulation)
    - FM (Frequency Modulation)
    - PM (Phase Modulation)
    - ASK (Amplitude Shift Keying)
    - FSK (Frequency Shift Keying)
    - PSK (Phase Shift Keying)
    - QAM (Qudratic Amplitude Modulation), …

5.) Fizikai réteg

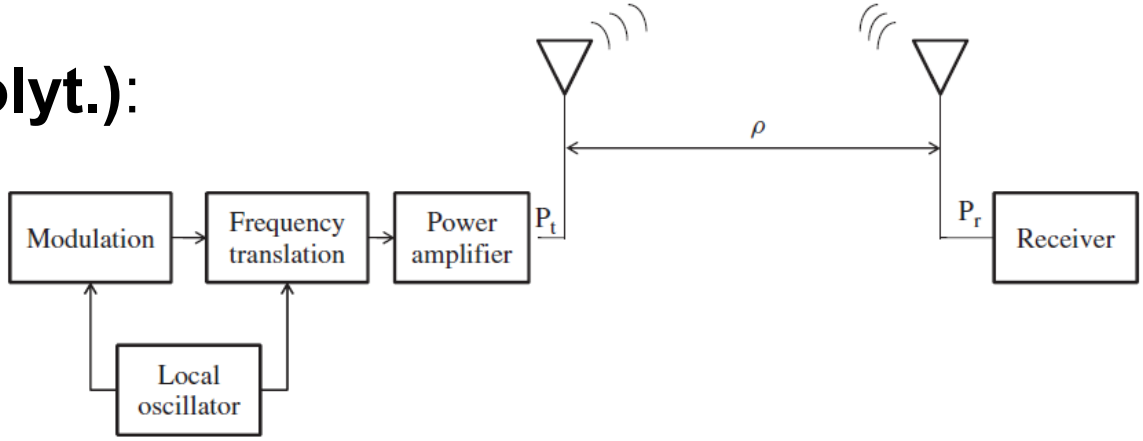
- **Jel terjedése**:
  - WSN spektrum: ISM (Industrial Science and Medical)
  - Zaj: Additive White Gaussian Noise



Spectrum	Center frequency	Availability
6.765–6.795 MHz	6.780 MHz	Subject to local regulations
13.553–13.567 MHz	13.560 MHz	
26.957–27.283 MHz	27.120 MHz	
40.66–40.70 MHz	40.68 MHz	
433.05–434.79 MHz	433.92 MHz	Europe, Africa, the Middle East west of the Persian Gulf including Iraq, the former Soviet Union and Mongolia
902–928 MHz	915 MHz	The Americas, Greenland and some of the eastern Pacific Islands
2.400–2.500 GHz	2.450 GHz	
5.725–5.875 GHz	5.800 GHz	
24–24.25 GHz	24.125 GHz	
61–61.5 GHz	61.25 GHz	Subject to local regulations
122–123 GHz	122.5 GHz	Subject to local regulations
244–246 GHz	245 GHz	Subject to local regulations

5.) Fizikai réteg

- **Jel terjedése (folyt.)**:



- P_t [W]: küldött teljesítmény
- ρ [m]: távolság
- A_t [m2]: küldő antenna effektív területe: $A_t = g_t \frac{\lambda^2}{4\pi}$
- λ [m]: vivő jel hullámhossza
- g_t []: küldő antenna nyeresége
- P_r [W]: fogadott teljesítmény

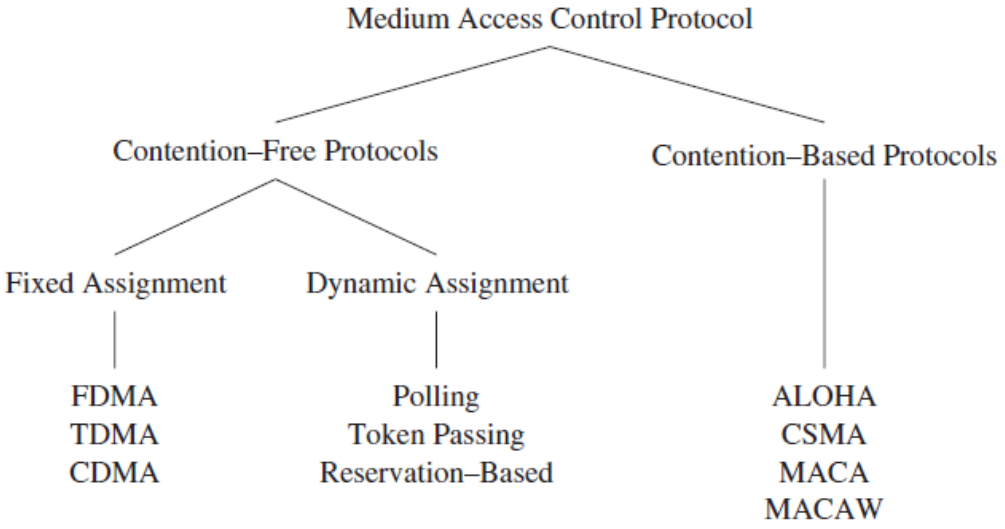
$$P_r = \frac{P_t}{4\pi\rho^2} g_t \times A_r \qquad P_r = \frac{P_t}{4\pi\rho^\gamma} g_t \times g_r \frac{\lambda^2}{4\pi}$$

- a(t) []: terjedési veszteség

$$a(t) = \frac{P_t}{P_r} = \left(\frac{4\pi\rho}{\lambda}\right)^2 \times \frac{1}{g_r g_t} \qquad a(t)/\mathrm{dB} = 20\log\left(\frac{4\pi\rho}{\lambda}\right) - 10\log\left(g_r g_t\right)$$

6.) Közeghozzáférés vezérlési réteg

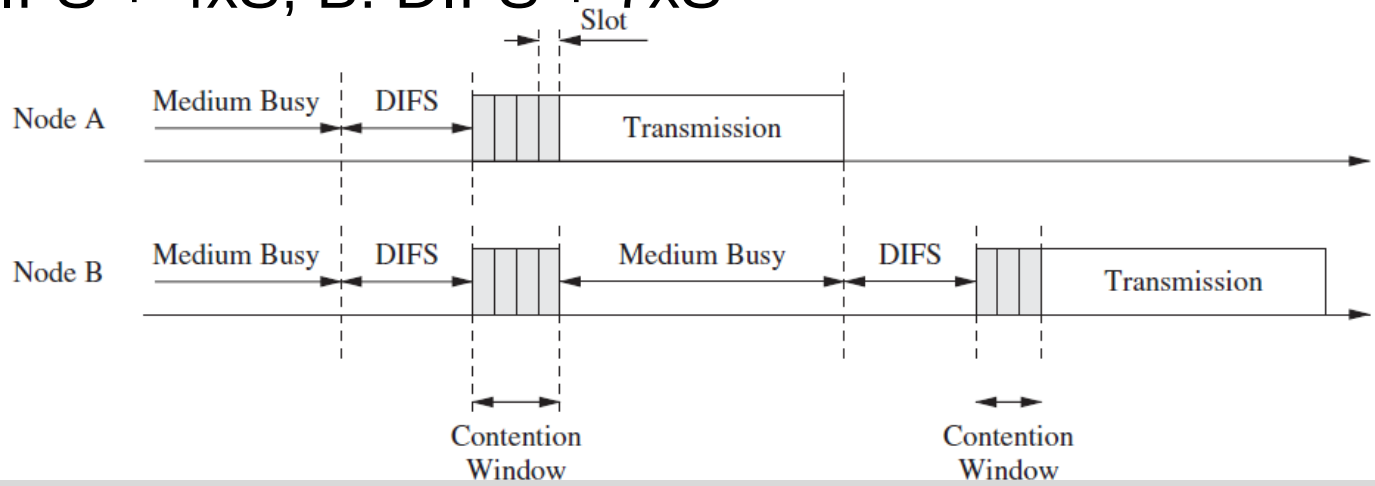
- **MAC (Medium Access Control):**
  - Csatorna: ISM sávban, közös közeg, zajjal és interferenciával szennyezve
  - Közeghozzáférés: több csomópont, aszimmetrikus kapcsolatok
  - Energiafelhasználás célja: küldés, fogadás, figyelés
  - Energiahatékonyságra való törekvési módszerek
    - Lappangási (latency) idő növelése
    - Átviteli ráta csökkentése
  - MAC kategóriák:



6.) Közeghozzáférés vezérlési réteg

- **CSMA/CA (CSMA with Collision Avoidance):**
  - CSMA egy változata, amely megelőzi az ütközést
  - Figyeli a közeget, de üres állapotban nem azonnal foglalja el, hanem várakozik:
    - Várakozás = DIFS + Rand(Backoff time)
    - DIFS: DCF Interframe Space (időtartam)
    - DCF: Distributed Coordination Function
    - Rand(Backoff time) = Rand() · Slot_time
  - Egyidőben figyelők közül a kisebb várakozási idejű küld
  - Pl.: A: DIFS + 4xS, B: DIFS + 7xS

A: 4xS
B: 4xS
A: küld
B: 3xS
B: küld



6.) Közeghozzáférés vezérlési réteg

- **MACA (Multiple Access with Collision Avoidance):**
  - Dinamikus foglalási mechanizmus
  - Vezérlő csomagok (handshake):
    - RTS (Ready-To-Send): küldésre kész (küldő)
    - CTS (Clear-To-Send): küldés lehetséges (nyelő)
    - RTS/CTS zaj nélküli eset: sikeres foglalás
    - RTS/CTS zajos eset: Retry

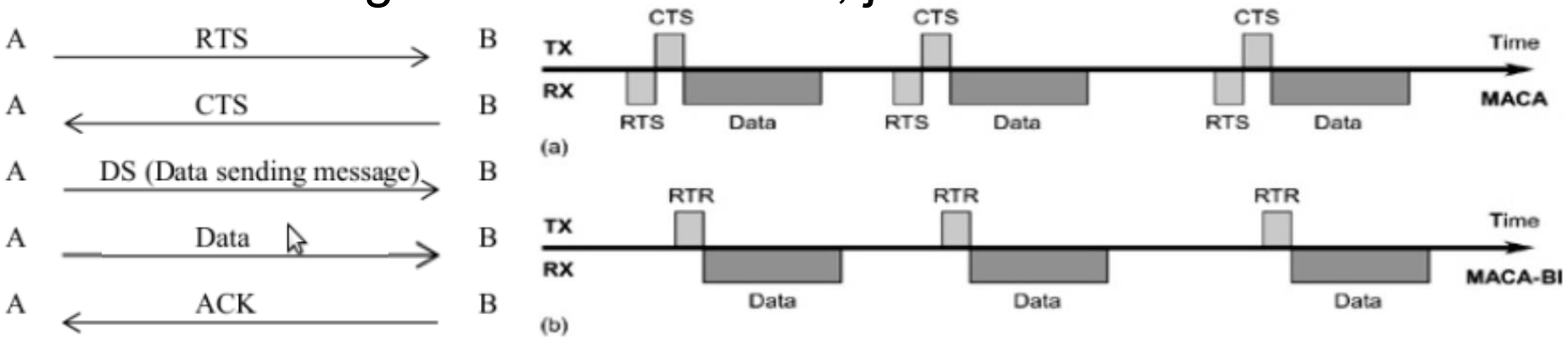
(a) A Sending RTS to B

(b) B sending CTS to A

(c) Data Transmission between A and B

6.) Közeghozzáférés vezérlési réteg

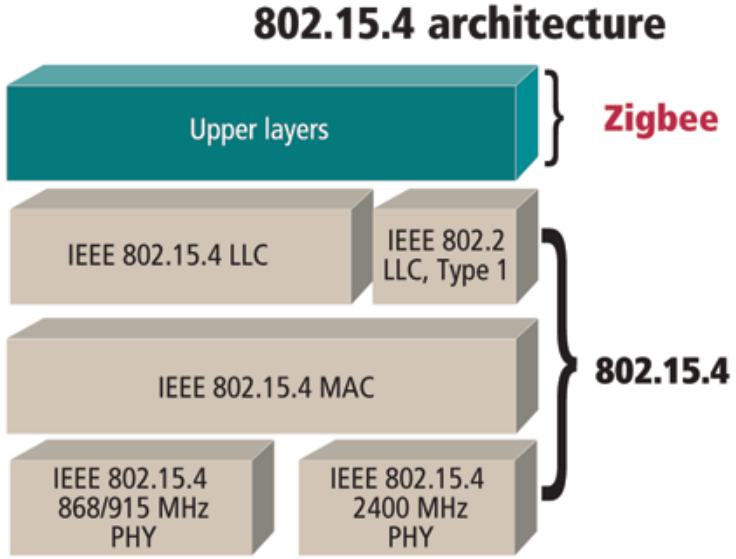
- **MACAW (MACA for Wireless LANs):**
  - Nyelő ACK-t küld, adatcsomag sikeres fogadása után és ezzel felszabadítja a lefoglalt csatornát.
  - Küldő DS-t (Data Sending) küld CTS fogadása után, de még adat küldése előtt, jelezve a biztos küldést.

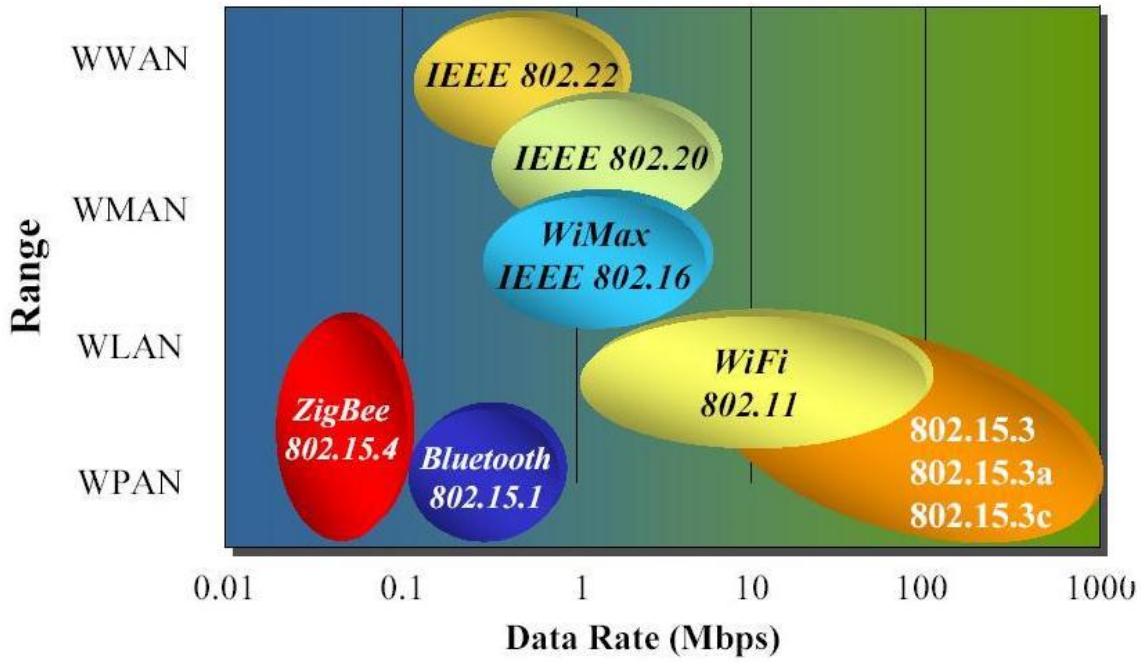


- **MACA-BI (MACA By Invitation):**
  - RTR (Ready-To-Receive): nyelő küldi fogadás előtt
  - Kisebb overhead, de a célnak tudnia kell a vételezés pillanatát (korlátos alkalmazhatóság)
  - Küldő opcionálisan jelezheti adat csomagban Nyelőnek a várakozó csomagok számát

6.) Közeghozzáférés vezérlési réteg

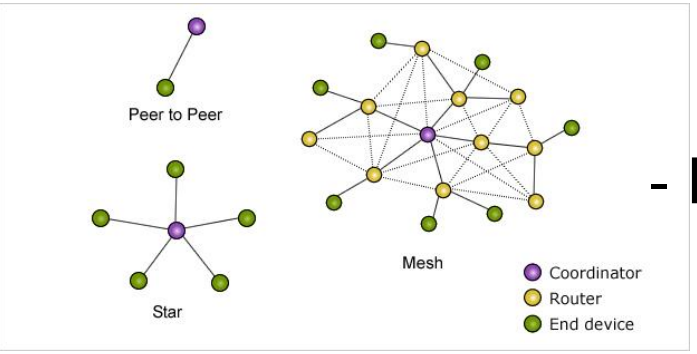
- **IEEE 802.15.4:**
  - ZigBee Alliance és IEEE összefogása, CSMA/CA
  - Frekvencia sávok: 868 MHz; 915 MHz; 2,45 GHz
  - Átviteli ráta: 20 kb/s, 40 kb/s, 250 kb/s





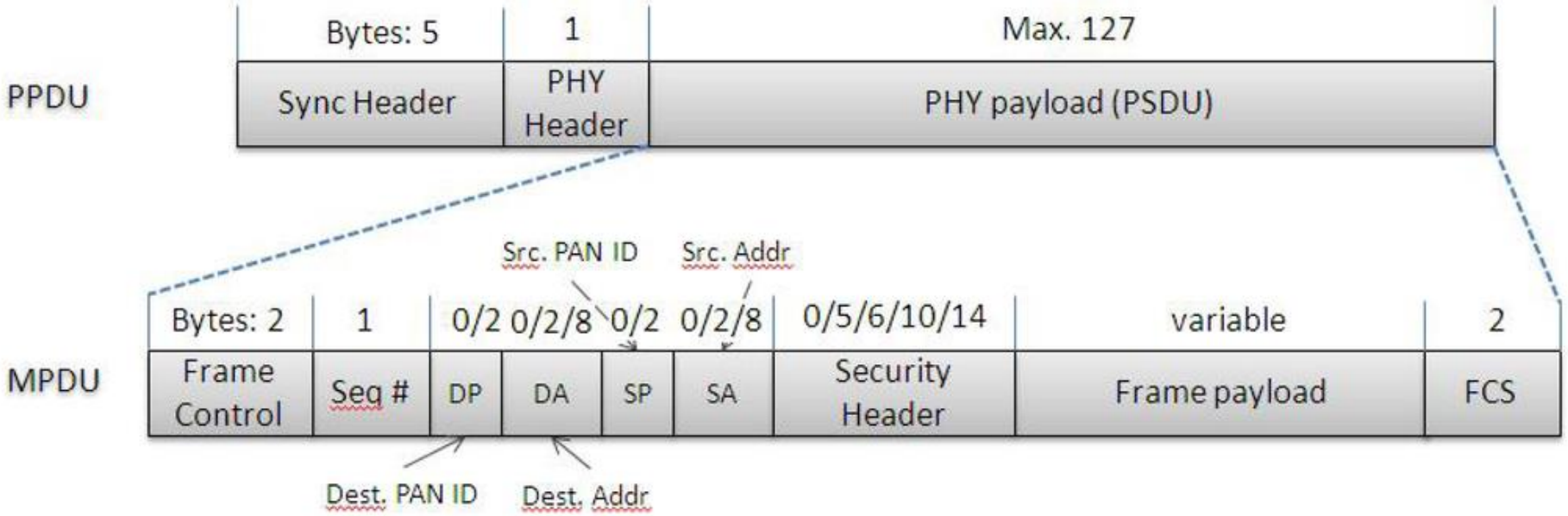
6.) Közeghozzáférés vezérlési réteg

- **IEEE 802.15.4 (folyt.):**
  - Két különböző topológia üzemmód:
    - Csillag üzemmód: PAN koordinátoron keresztül
      - Szinkronizált (beacon-szabályozott) mód:
        - Random Backoff érzékelés előtt,
        - Réselt csatorna hozzáférés.
      - Nem szinkronizált mód:
        - Random Backoff érzékelés előtt,
        - Azonnali csatorna hozzáférés.
      - Kliens előre kérvényezi a küldését
      - PAN koordinátor csak a kliens kérésére küld adatot a klienshez
    - Peer-to-Peer üzemmód: ad-hoc jelleggel
      - Nincs pontosan specifikálva ez az üzemmód a szabványban



6.) Közeghozzáférés vezérlési réteg

- **IEEE 802.15.4 (folyt.):**
  - PPDU (Physical PDU)
  - MPDU (MAC PDU)



6.) Közeghozzáférés vezérlési réteg

- IEEE 802.15.4 (folyt.):

Short 802.15.4 packet (3 - 56 bytes)

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	...	Byte len+5	Byte len+6
00	Timestamp (2 ^ -16 seconds)		Timestamp (seconds)		Data Len	802.15.4 packet (no FCS)		RSSI	FCS OK / LQI

Medium 802.15.4 packet (57 - 119 bytes) – observed

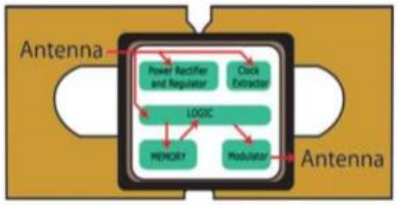
	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	...	Byte 62	Byte 63
First USB chunk	00	Timestamp (2 ^ -16 seconds)		Timestamp (seconds)		Data Len	802.15.4 packet part 1			
Second USB chunk	00	802.15.4 packet part 2 (no FCS)						RSSI	FCS OK / LQI	

Long 802.15.4 packet (120 - 125 bytes) -– like Higgs particle: predicted but never observed!

	Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	...	Byte 62	Byte 63
First USB chunk	00	Timestamp (2 ^ -16 seconds)		Timestamp (seconds)		Data Len	802.15.4 packet part 1				
Second USB chunk	00	802.15.4 packet part 2									
Third USB chunk	00	802.15.4 packet part 3 (no FCS)					RSSI	FCS OK / LQI			

6.) Közeghozzáférés vezérlési réteg

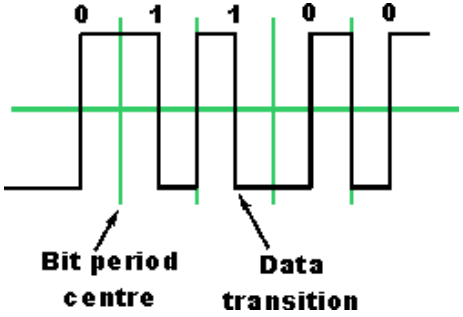
- **NFC (Near Field Communication):**
  - Rövid hatótávolságú (max. 0,1 m) vezetéknélküli
  - Mobil és kézi készülékek számára
  - Kommunikációs lehetőségek:
    - Két aktív (saját energiaforrás) eszköz között
    - Aktív és passzív eszköz között
  - RFID (Radio Frequency Identification) kiterjesztése
  - Frekvencia: 13,56 MHz
  - Sávszélesség: 14 kHz
  - Adatátviteli ráta: 106,22 kb/s, 424 kb/s
  - Kommunikáció feltételei:
    - Egyik eszköz NFC Reader/Writer
    - Másik eszköz NFC tag
    - Initiator: Request
    - Target: Reply



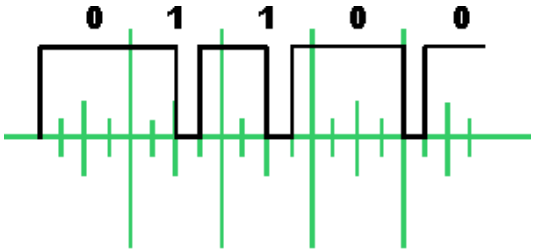
An NFC Reader (A Smartphone)

6.) Közeghozzáférés vezérlési réteg

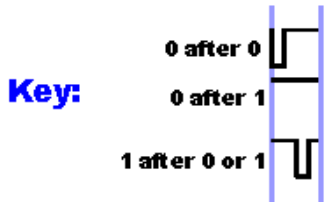
- **NFC (folyt.):**
  - Kommunikáció:
    - Initiator: Request
    - Target: Reply
    - Adat kódolás:



- 106,22 kb/s: Modified Miller Coding és 100% moduláció
  - „0”: H -> L
  - „1”: L -> H



- 424 kb/s: Manchester Coding és 10% moduláció
  - „0”: függ az előző bittől
  - „1”: bijektív leképezés



6.) Közeghozzáférés vezérlési réteg

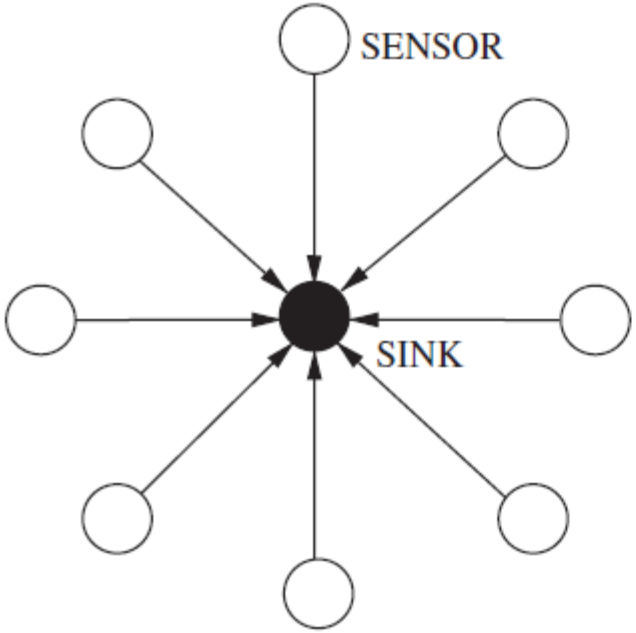
- **Összehasonlítás (NFC, RFID, IrDa, Bluetooth):**

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

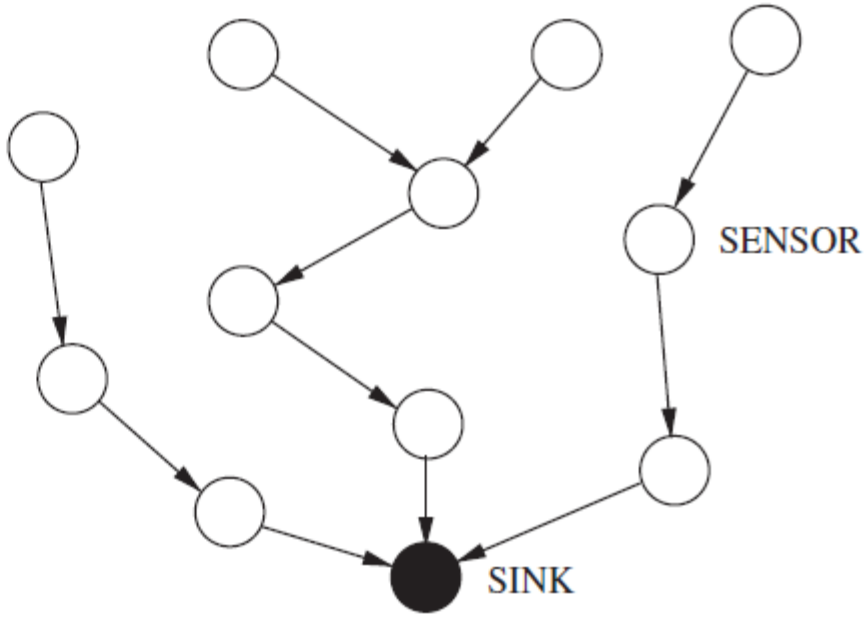
7.) Hálózati réteg

- **Csomag továbbítás funkció**:

Single-hop útválasztás



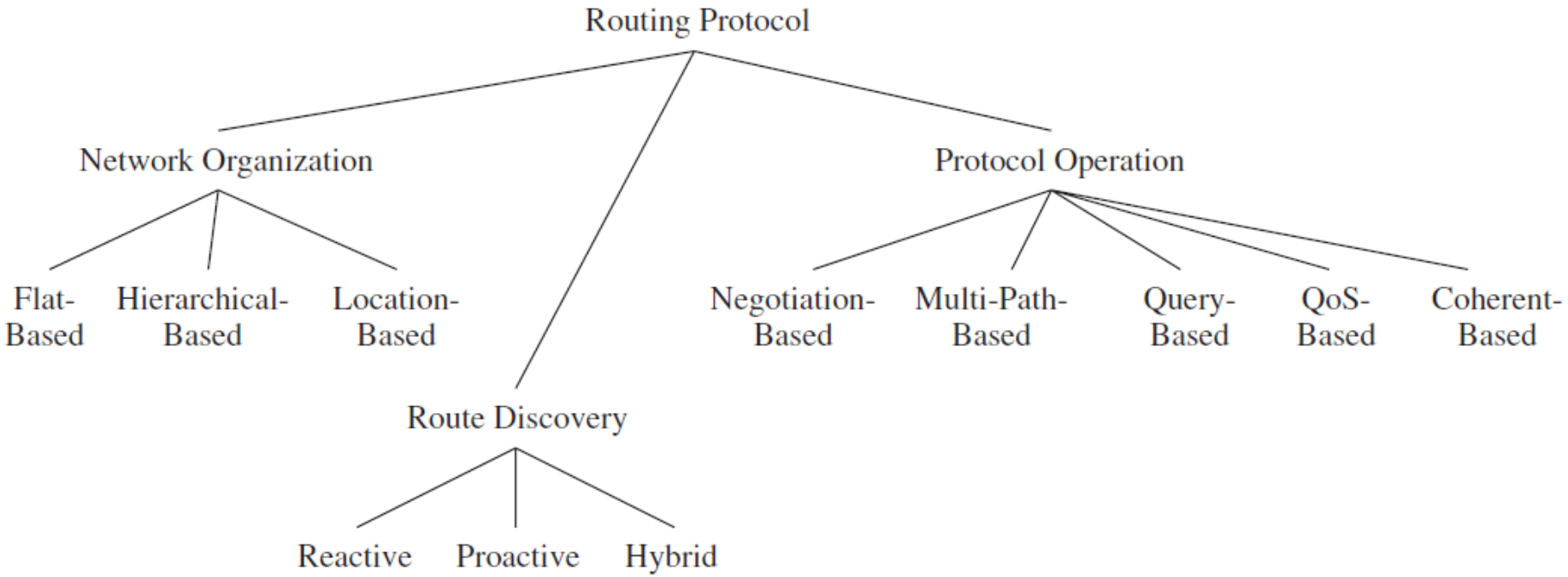
Multi-hop útválasztás



- Útvonal típusok:
  - Előre meghatározott topológia (statikus routing)
  - Véletlenszerű topológia (dinamikus routing)
    - Szomszédok azonosítása
    - Útvonal felfedezése a gateway/sink-ig

7.) Hálózati réteg

- **Routing protokoll osztályozási szempontok**:



- Hálózat szervezése szerint: útvonal megh. fizikai helye
- Útvonal felfedezése szerint: útvonal megh. ideje és ára
- Protokoll működése szerint: útvonal megh. módja

7.) Hálózati réteg

- **WSN routing protokoll metrikák:**
  - Adatok begyűjtése WSN-ben:
    - Időfüggő vezérlés (pl. hőmérséklet lekérdezés)
    - Eseményfüggő vezérlés (pl. futótűz detektálás)
    - Igényfüggő vezérlés (sink igénye szerint)
  - Routing-ot meghatározó kényszerek:
    - Rendelkezésre álló hálózati erőforrások
    - Alkalmazások igénye
  - Leggyakoribb metrikák:
    - Legkevesebb ugrás (hop) száma (legrövidebb út hossza, késleltetés)
    - Energia (csomagonkénti igény, partícionálás ideje, csomópontonkénti igény, legtöbb energiájú csomópontok, leghosszabb élet)
    - QoS (késleltetés, dzsitter, csomagvesztés)
    - Erőteljesség: link minőség, link stabilitás

- **WSN routing protokollok áttekintése:**

Protocol	Characteristics
SPIN	Flat topology, data-centric, query-based, negotiation-based
Directed diffusion	Flat topology, data-centric, query-based, negotiation-based
Rumor routing	Flat topology, data-centric, query-based
GBR	Flat topology, data-centric, query-based
DSDV	Flat topology with proactive route discovery
OLSR	Flat topology with proactive route discovery
AODV	Flat topology with reactive route discovery
DSR	Flat topology with reactive route discovery
LANMAR	Hierarchical with proactive route discovery
LEACH	Hierarchical, support of MAC layer
PEGASIS	Hierarchical
Safari	Hierarchical, hybrid route discovery (reactive near, proactive remote)
GPSR	Location-based, unicast
GAF	Location-based, unicast
SPBM	Location-based, multicast
GEAR	Location-based, geocast
GFPG	Location-based, geocast
SAR	Flat topology with QoS (real-time, reliability), multipath
SPEED	Location-based with QoS (real-time)
MMSPEED	Location-based with QoS (real-time, reliability)

7.) Hálózati réteg

- QoS alapú Routing: SPEED

- Adatok begyűjtése határidő alatt (pl. felügyeleti rendsz.)
- Valós idejű: unicast, area-multicast, area-anycast
- Node a szomszédjaitól pozíció információt kap és nem routing információt: HELLO[Src,Position,Rx_Delay]
- Node saját szomszédsági tábláját aktualizálja
  [$Node_{\#}$,Position,ExpireTime,Rx_Delay,Tx_Delay]
- Routing algoritmus: Stateless Nondeterministic Geographic Forwarding (SNGF)
- FS_i^{Dst} : Forwarding node-ok halmaza S_i-ből Dst-ba
  $FS_i^{DST} = \{ j \mid L_i - L_j \geq K\}$, ahol L_i a távolság S_i-ből Dst-ba. Ha ez üres halmaz, akkor csomag eldob.
- S_i-ből Dst felé csak FS_i^{Dst} halmazhoz van küldés
- FS_i^{Dst} felosztása két diszjunkt részhalmazra (D := $Hop_{\#}$)
  $S_{i,1} = \{ j \mid Tx\_Delay_j < D\}$, $S_{i,2} = \{ j \mid Tx\_Delay_j \geq D\}$

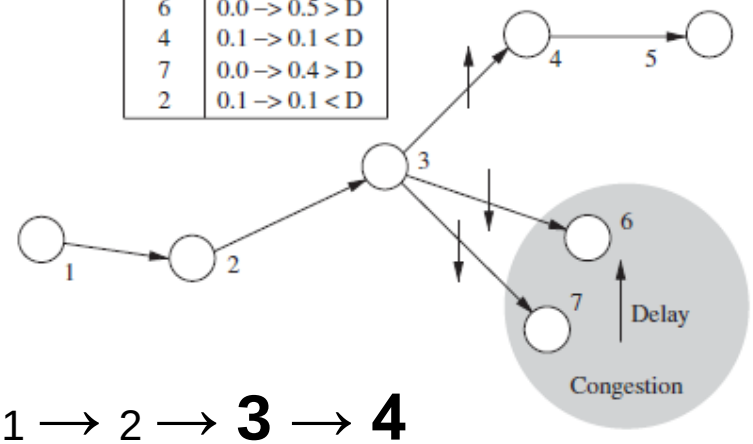
- **QoS alapú Routing: SPEED (folyt.)**
  - FS_i^{Dst} felosztása két diszjunkt részhalmazra ($D := Hop_{\#}$)

    $S_{i,1} = \{ j \mid Tx\_Delay_j < D\}$, $S_{i,2} = \{ j \mid Tx\_Delay_j \geq D\}$
  - Továbbító node: $S_{i,1}$ -ből választva az, amelynek a RelaySpeed értéke maximális

    $RelaySpeed_{i,j} = | L_i - L_j | / Tx\_Delay_j$, $j \in S_{i,1}$
  - Back-Pressure Rerouting: problémák megoldása
    - következő node nem létezésének esete
    - ütközések minimalizálása

3's Neighbor Table

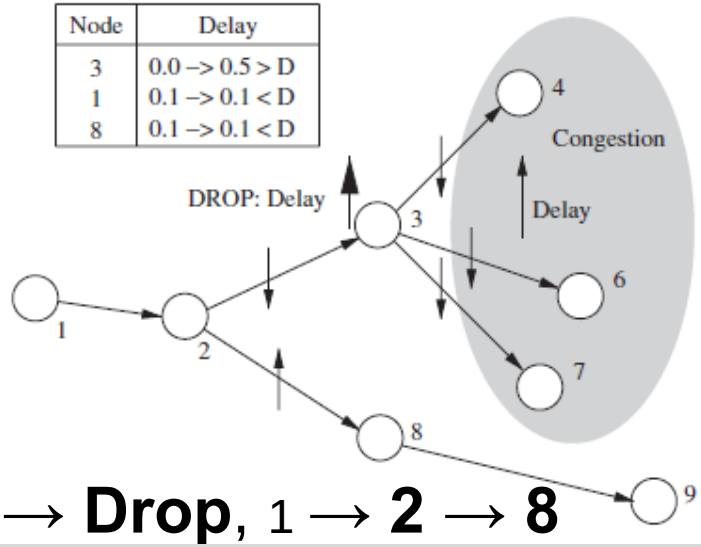
Node	Delay
6	0.0 –> 0.5 > D
4	0.1 –> 0.1 < D
7	0.0 –> 0.4 > D
2	0.1 –> 0.1 < D



1 → 2 → **3 → 4**

2's Neighbor Table

Node	Delay
3	0.0 –> 0.5 > D
1	0.1 –> 0.1 < D
8	0.1 –> 0.1 < D



3 → Drop, 1 → **2 → 8**

8.) Energia menedzsment

- **WSN energia problémák:**
  1) Kis fizikai méret, sok feladat (érzékelés, feldolgozás, önmenedzselés, kommunikáció), kis akkumulátor
  2) WSN: nagyszámú node, akkumulátor csere lehetetlen
  3) Kis fizikai méret az újratöltést nem teszi lehetővé
  4) Néhány node kiesése a hálózatot gyorsan darabolja
- **Energia problémák megoldásai**:
  1) Energiahatékony kommunikációs protokollok
  2) Fölösleges feladatok megszűntetése (node-on belül, illetve a hálózatban)
     - Több ideig forgalmazás, mint a terv szerinti idő
     - Nem létező node-okhoz való gyakori kapcsolódási próba
     - Nem optimális konfigurációk a hardverben, illetve a szoftverben
  3) Dynamic Power Management (DPM): helyi és globális

8.) Energia menedzsment

- **Dinamikus energia menedzsment (DPM):**
  - DPM stratégiák:
    1) Dinamikus működési módok
    2) Dinamikus skálázás
    3) Energia megtakarítás

1) **DPM dinamikus működési módok:**
  - Idő függvényében üzemmód váltás
  - Üzemmódok száma: n
  - Hardver komponensek száma: x
  - Energia üzemmódok száma: $P_n = x \cdot n$
  - Energia konfiguráció kiválasztási kihívások:
    a) Üzemmód váltás többlet energiát fogyaszt
    b) Váltás késleltetést okoz, ami a megfigyelt folyamat fontos eseményének nem észlelését okozhatja.

8.) Energia menedzsment

- **Dinamikus energia menedzsment (DPM) (folyt.):**

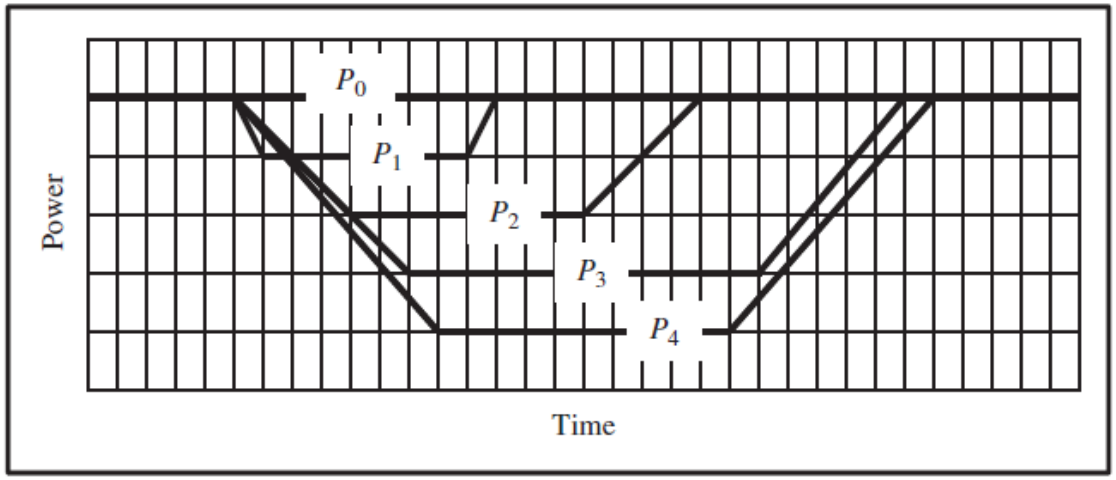
1) DPM dinamikus működési módok (folyt.):

- Pl.: Energia megtakarítási konfigurációk

Configuration	Processor	Memory	Sensing subsystem	Communication subsystem
P_0	Active	Active	On	Transmitting/receiving
P_1	Active	On	On	On (transmitting)
P_2	Idle	On	On	Receiving
P_3	Sleep	On	On	Receiving
P_4	Sleep	Off	On	Off
P_5	Sleep	Off	Off	Off

Üzemmód váltás

A következő feladat ismerete befolyásolja az optimális üzemmódba kapcsolást, vagyis a fogyasztás mértékét.

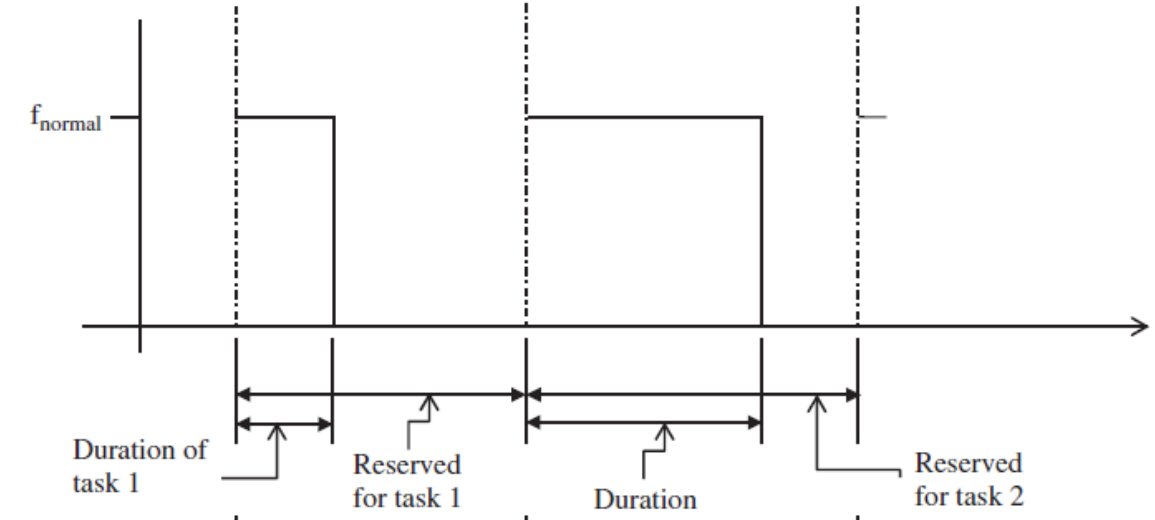


8.) Energia menedzsment

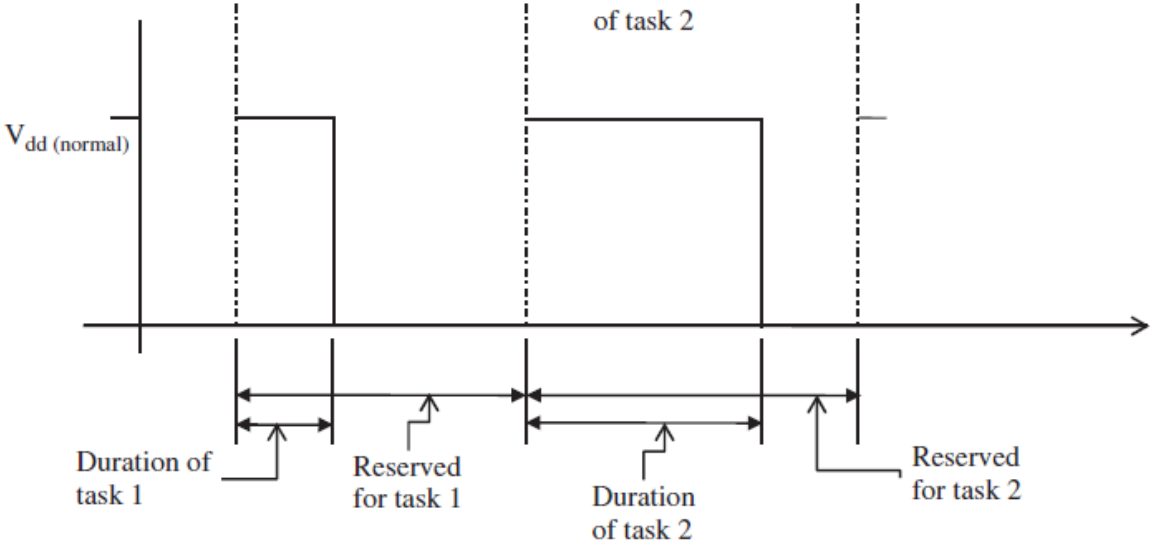
- **Dinamikus energia menedzsment (DPM) (folyt.):**

2) DPM dinamikus skálázás: pazarló eset

- **DFS**
Dynamic
Frequency
Scaling



- **DVS**
Dynamic
Voltage
Scaling

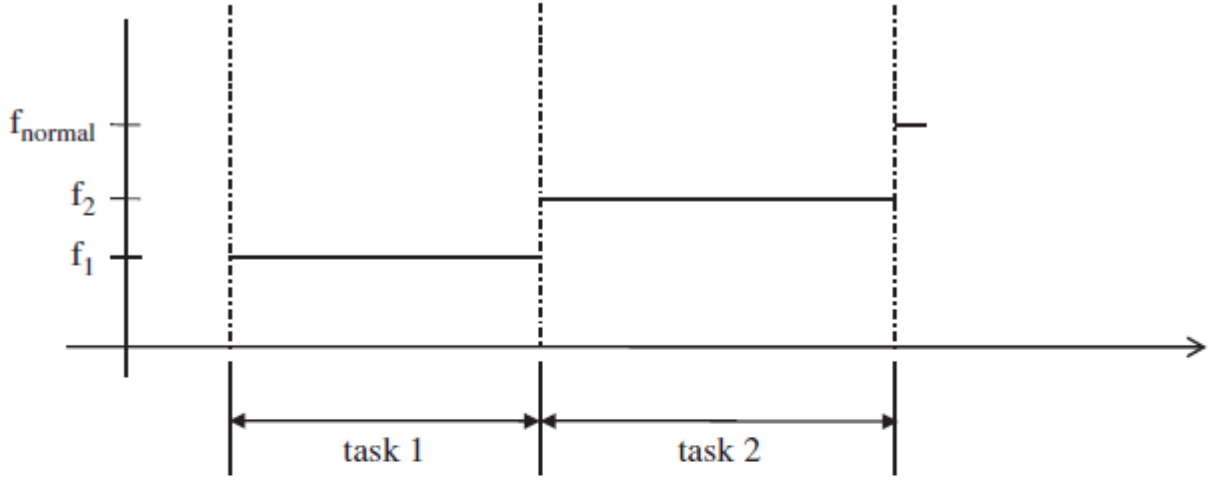


8.) Energia menedzsment

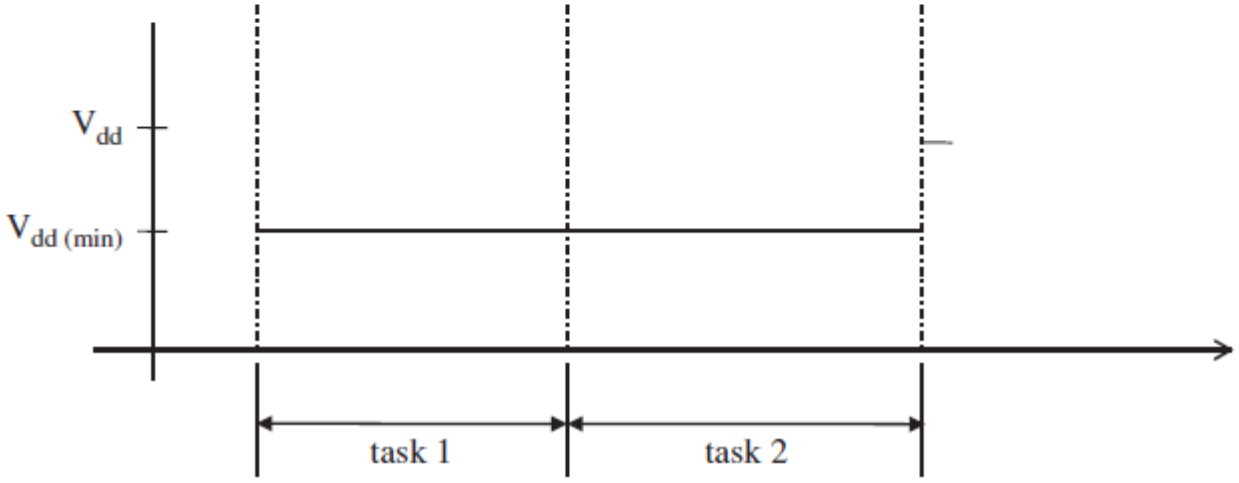
- **Dinamikus energia menedzsment (DPM) (folyt.):**

2) DPM dinamikus skálázás: takarékos eset

- **DFS**
Dynamic
Frequency
Scaling



- **DVS**
Dynamic
Voltage
Scaling



8.) Energia menedzsment

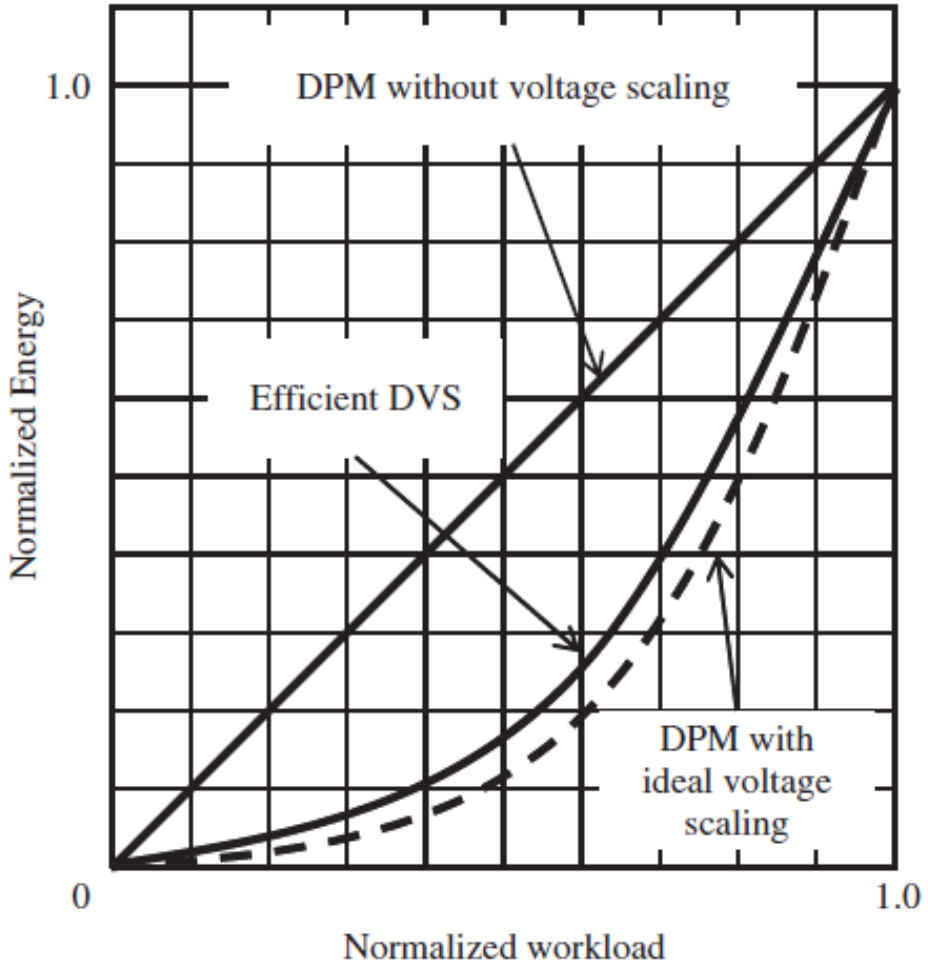
- **Dinamikus energia menedzsment (DPM) (folyt.):**

3) DPM energia megtakarítás:

- Tranzisztorok (logikai kapuk) energia igénye:

- Működési frekvenciával egyenesen arányos

- Tápfeszültséggel négyzetesen arányos



8.) Energia menedzsment

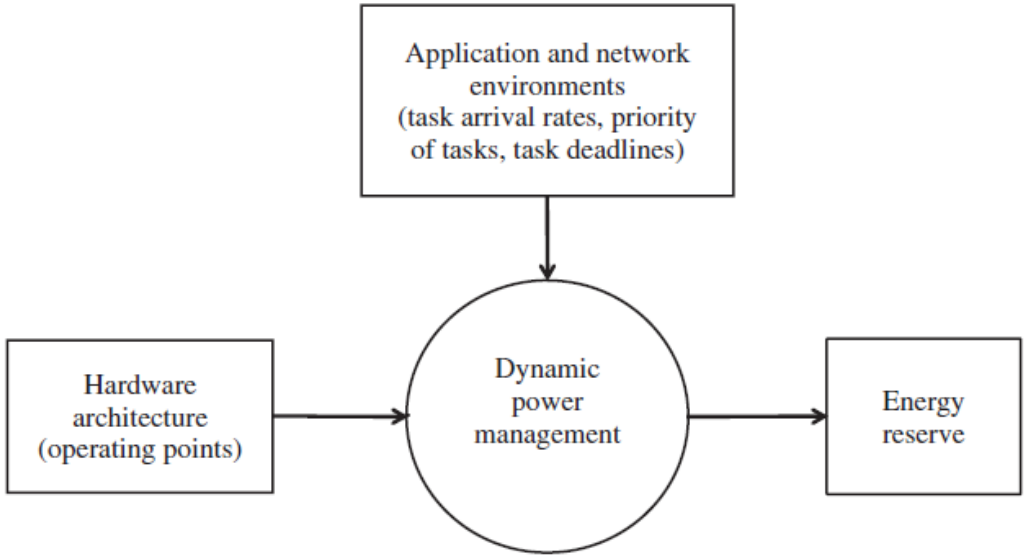
- Dinamikus energia menedzsment (DPM) (folyt.):

- Koncepcionális megfontolások:

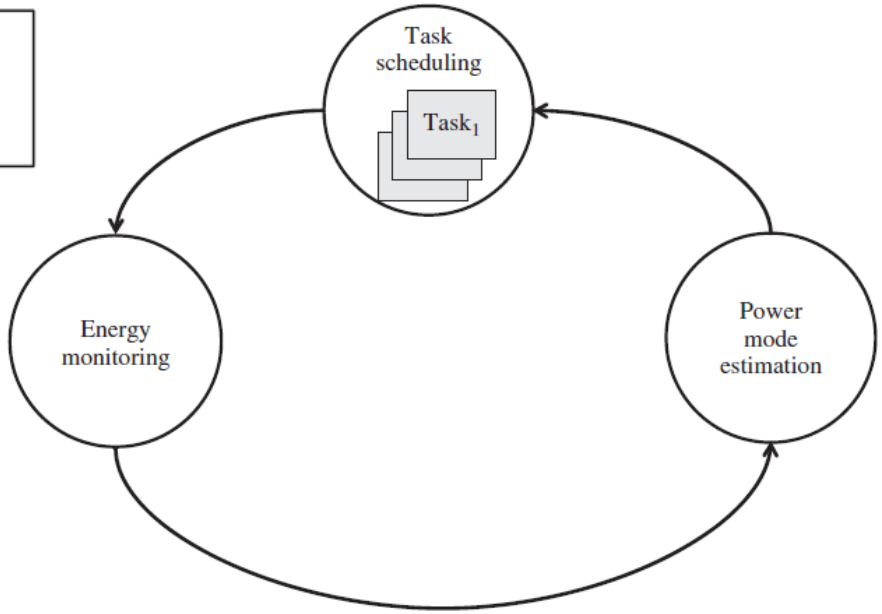
- DPM stratégia energiatöbblet mértéke
  - Hardver modulok fogyasztása összesen
  - Alkalmazások minőségi és teljesítmény igényei
  - Maga a DPM többlet fogyasztása
- DPM stratégia típusa:
  - Centralizált eset: fogyasztás könnyebb áttekintése és hatékony adaptáció
  - Elosztott eset: több energia, de jobb skálázhatóság. Lokális stratégiák ellent mondhatnak a globális céloknak.
- Centralizált DPM esetén a DPM task futtatásának helye:
  - Processzor alrendszer eset: mindent lát, előnyös
  - Energia alrendszer eset: extra intelligencia kellene, ami költségesebbé tenné

8.) Energia menedzsment

- Dinamikus energia menedzsment (DPM) (folyt.):



DPM stratégiát befolyásoló tényezők

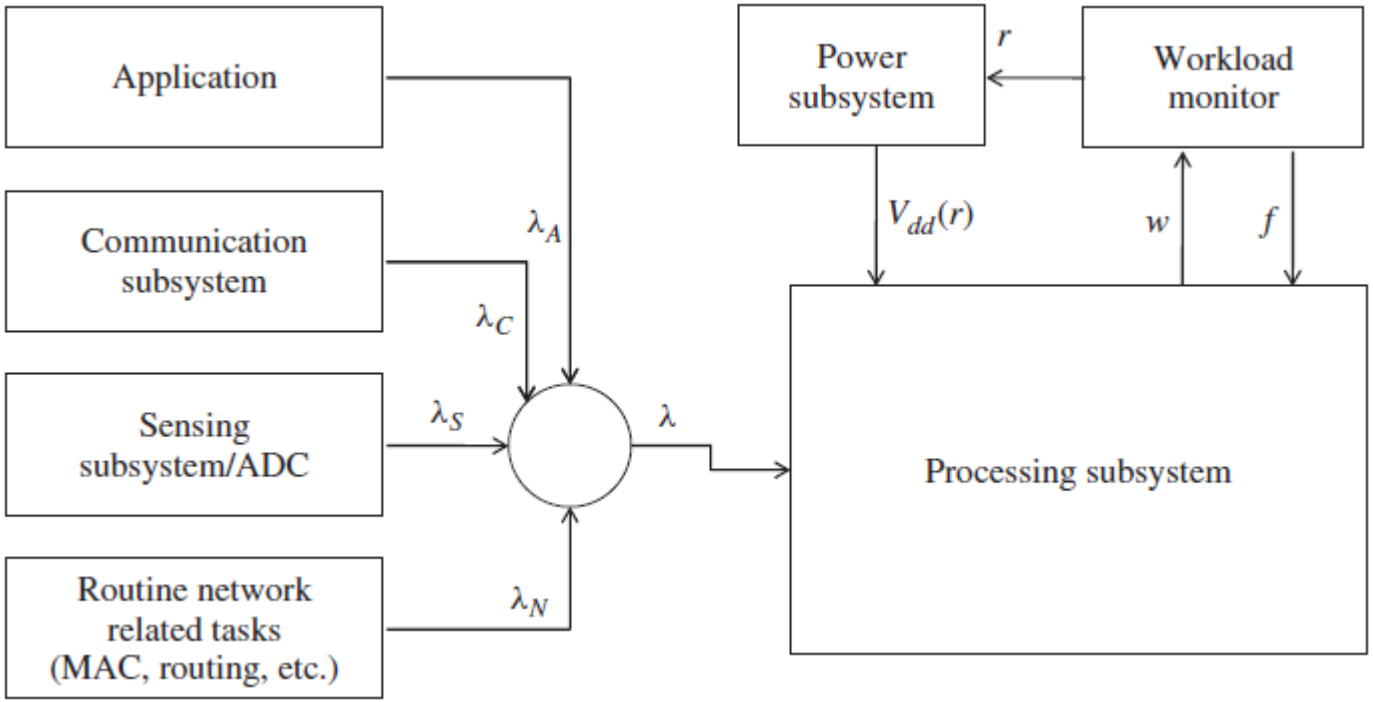


DPM stratégia végrehajtása

8.) Energia menedzsment

- Dinamikus energia menedzsment (DPM) (folyt.):

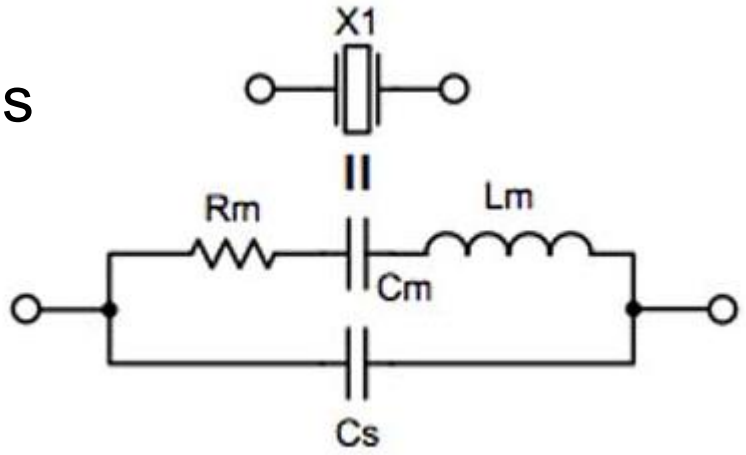
- DPM koncepcionális architektúra

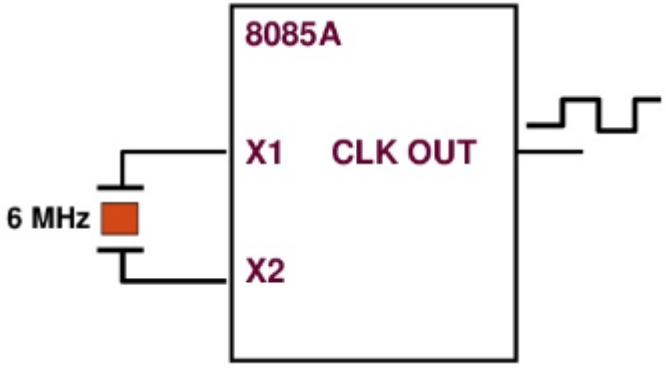


- Task beérkezési intenzitás: $\lambda = \Sigma \lambda_i$
- Workload monitor: érzékeli τ ideig a w igényeket és előre jelzi β ideig az r intenzitást és f órajelet
- Energia alrendszer: $V_{dd} = V_{dd}(r)$

9.) Idő szinkronizálás

- **Elosztott rendszer időzítési problémája**:
  - Sok csomópont hálózatban, egymástól függetlenül
  - Idő függvényében történő tevékenységek
  - Kommunikáció szükségessége: saját és tranzit adatok
  - Saját órák eltérése:
    - Órajel frekvencia eltérés
    - Időpont eltérés
- Szükséges funkciók:
  - Önkonfiguráció
  - Megbízhatóság
  - Energia konzerválás
- **Számítógép óra összetétele**:
  - Kvarc oszcillátor
  - Ciklikus hardver számláló





9.) Idő szinkronizálás

- **Óra működése**:
    - Ciklikus hardver számláló „0” állapotban: interrupt
    - Két interrupt közötti időtartam: Clock Tick
    - Szoftver óra (számláló)
        - Időegysége, felbontása: Clock Tick
        - Hozzáférés: API-n keresztül
        - Értéke: helyi idő (local time): C(t)
        - Clock rate: $f = 1/C(t)$
- Két szenzor (1, 2) órája közötti különbségek:
    - Clock Offset = $C(t_1) - C(t_2)$
    - Clock Skew (eltérés) = $f_1 – f_2$
- Tökéletes óra esetén: $dC/dt = 1$, folyamatosan
- Óra frekvenciáját befolyásoló tényezők:
    - Környezeti hőmérséklet, nedvesség, légnyomás
    - Kvarc tápfeszültsége és életkora

9.) Idő szinkronizálás

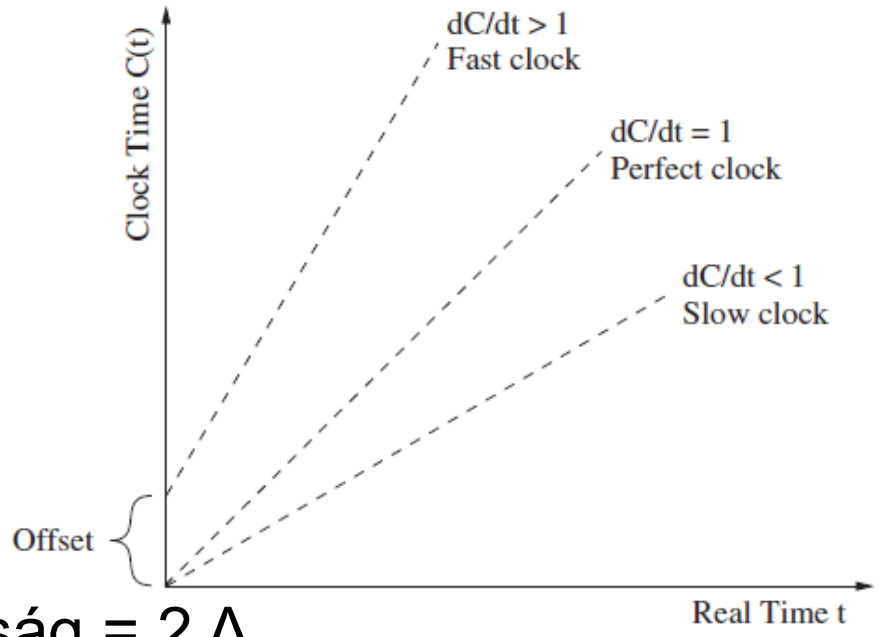
- Drift ráta: $D_i = dC/dt - 1$
  - Drift ráta maximuma: ρ [ppm], ppm = 10^{-6} (parts/million)
  - Tipikus óra drift rátája: 1 ppm < ρ < 100 ppm
  - Drift rátát a gyártó specifikálja: (1 ppm ~ 1s/12 nap)

$$1 - \rho \leq dC/dt \leq 1 + \rho$$

- Szenzoroknál periodikus szinkronizálás szükséges:
  - Két óra drift különbsége: $2\rho_{max}$
  - Két óra relatív offsetje: δ
  - Szinkronizálási periódus:

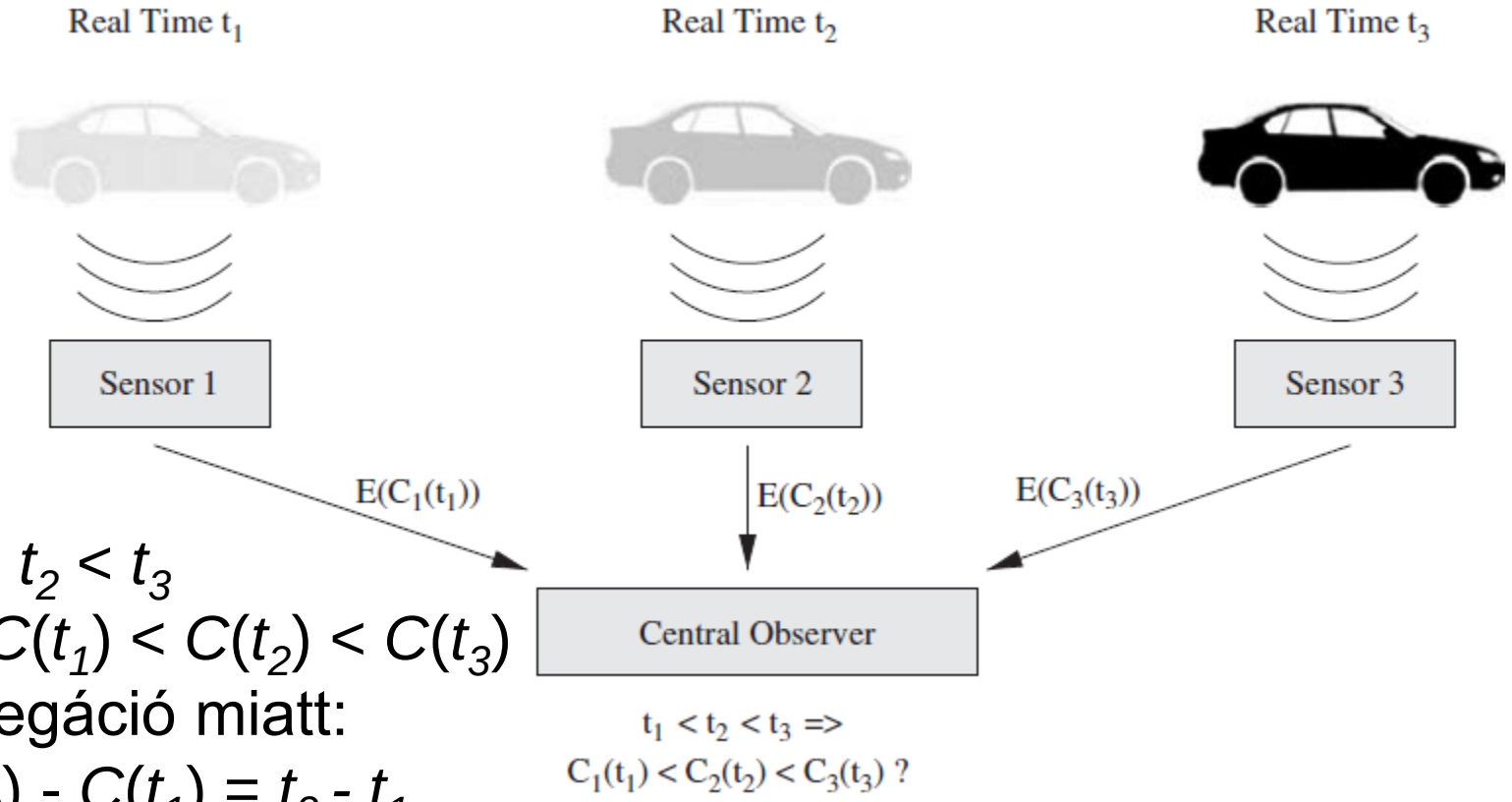
$$\tau \leq \delta/(2\rho_{max})$$

- Szinkronizálás típusok:
  - Külső: referencia órához
    offset neve: <u>hitelesség</u>
  - Belső: egymás között
    offset neve: <u>pontosság</u>
- Ha hitelesség = Δ, akkor pontosság = 2 Δ



9.) Idő szinkronizálás

- **Idő szinkronizálás WSN-ben**:
  - NTP (Network Time Protocol): robosztus, skálázható, önkonfigurálható, de WSN-hez nem alkalmazható
  - GPS (Global Positioning System): hitelesség $n \cdot \mu s$
  - Szinkronizálás szükségessége: Pl. autók érzékelése



Valós: $t_1 < t_2 < t_3$

Szenzor: $C(t_1) < C(t_2) < C(t_3)$

Adat aggregáció miatt:

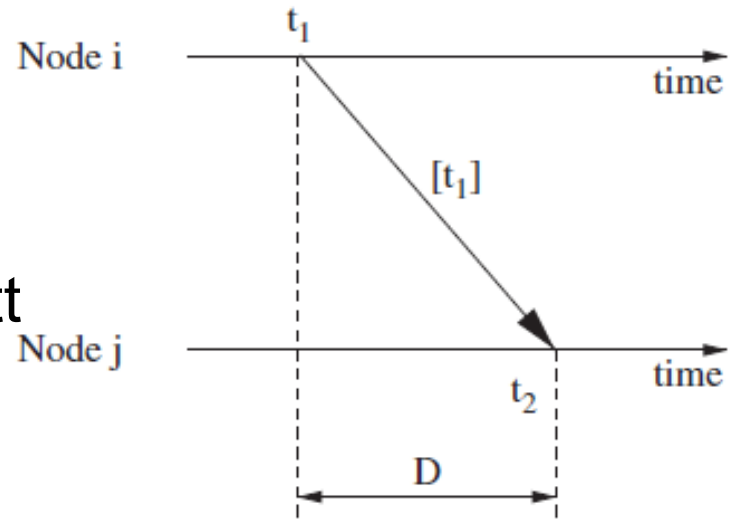
$\Delta = C(t_2) - C(t_1) = t_2 - t_1$

9.) Idő szinkronizálás

- **Idő szinkronizálás WSN-ben (folyt.)**:
    - Oszcillátor driftje
        - Ellenőrzött környezetben: ρ = 3 ppm (1 s / 4 nap)
        - Klasszikus környezetben: ρ > 6 ppm
    - WSN kommunikációs közeg tulajdonságait befolyásoló tényezők:
        - Eső
        - Köd
        - Szél
        - Hőmérséklet
        - Aszimmetrikus kommunikációs késleltetések
    - Pontossági igények a gyakorlatban:
        - Megfigyelő rendszereknél: $n \cdot \mu s$
        - Gyalogos megfigyelésnél: 1 s

9.) Idő szinkronizálás

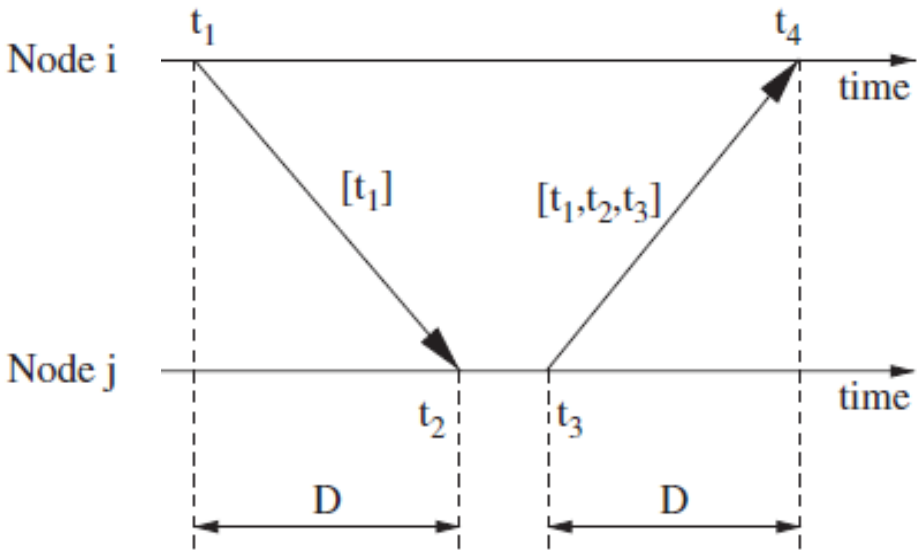
- **Szinkronizálás üzenetei**:
  - **Pár szintű szinkronizálás**: két óra szinkronizálása legalább egy üzenet segítségével
  - **Hálózat szintű szinkronizálás**: pár szintű szinkroniz. ismétlése több pár között mindaddig, amíg mindegyik node beállítja a saját óráját.
- **Egyutas üzenet küldés**:
  - $Node_i$-től $Node_j$-hez,
    t_1 időbélyeg küldése
    $$t_2 - t_1 = D + \delta$$
    D: ismeretlen terjedési idő
    δ: offset $Node_i$ és $Node_j$ között
  - WSN-nél D elhanyagolható,
    így $Node_2$ számára az
    offset meghatározható



$t_2 = t_1 + D + \delta$

9.) Idő szinkronizálás

- **Kétutas üzenet küldés**:
  1) Node$_i$-től Node$_j$-hez,
     t_1 időbélyeg küldése
  2) Node$_j$-től Node$_i$-hez
     t_1, t_2, t_3 időbélyegek küldése. Terjedési idő mindkét irányba azonos: D
  3) Idők meghatározása Node$_i$-nél
     $D = (t_2\text{-}t_1) + (t_4\text{-}t_3) / 2$
     $\delta = (t_2\text{-}t_1) - (t_4\text{-}t_3) / 2$
  4) Node$_i$ visszaküldi D és δ értékét Node$_j$-nek

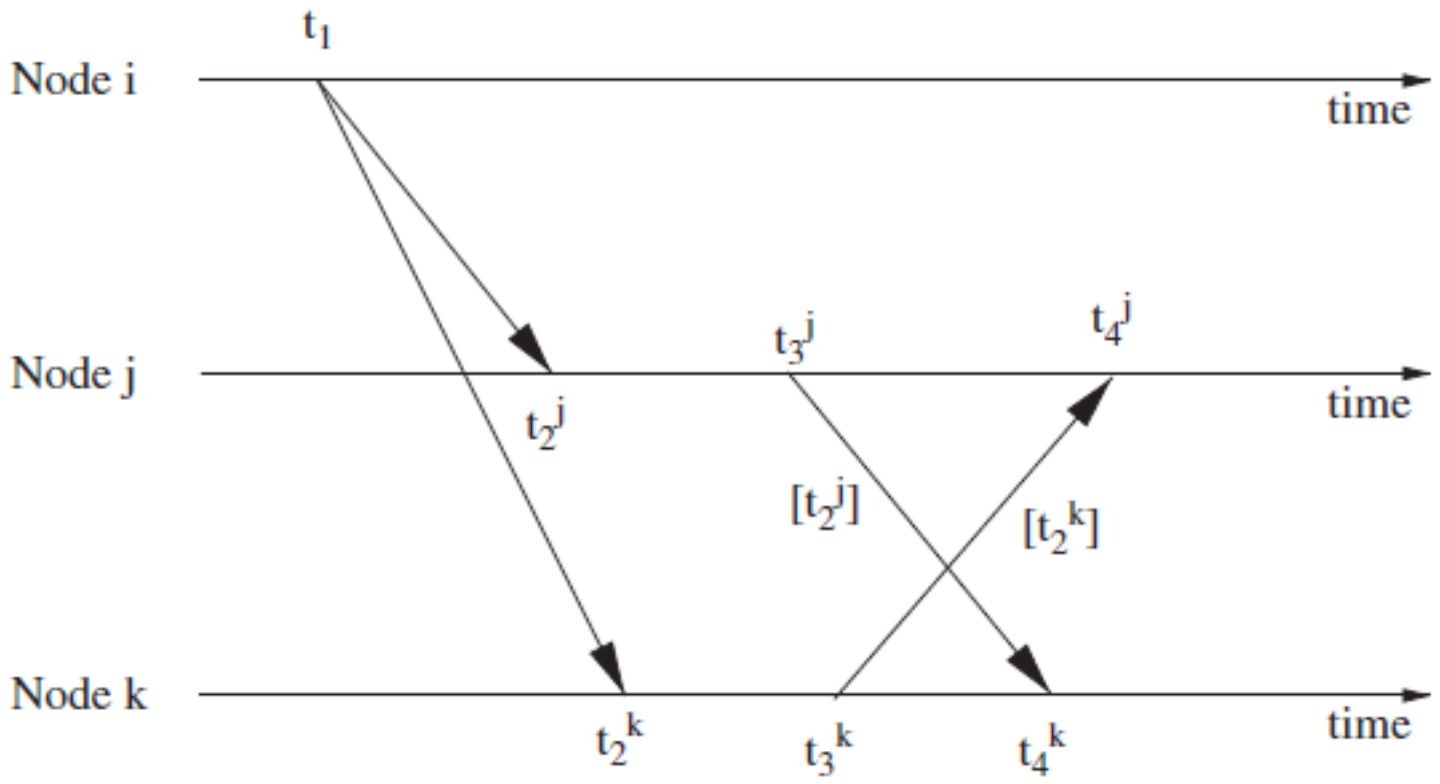


$t_2 = t_1 + D + \delta$

$t_4 = t_3 + D - \delta$

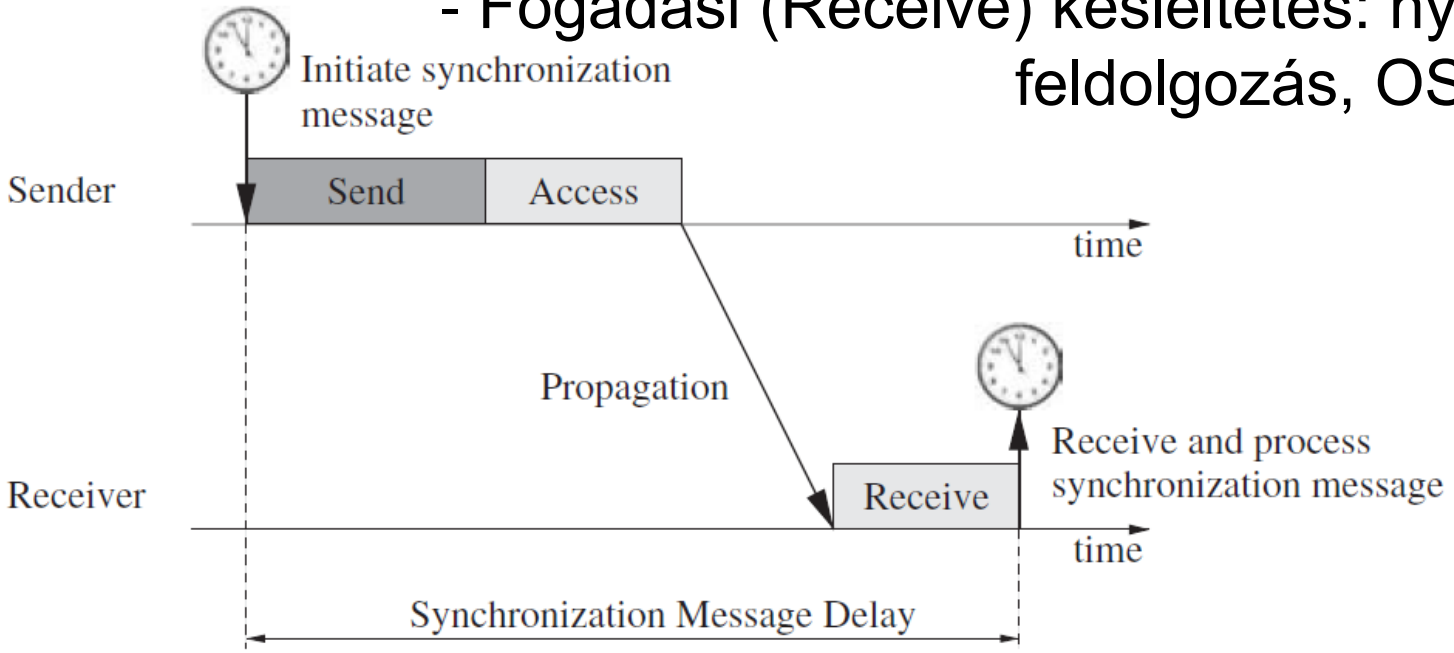
9.) Idő szinkronizálás

- **Fogadó-fogadó szinkronizálás**:
  1) $Node_i$ időbélyeg nélküli órajelet küld üzenetszórással, amit a többi node kb. azonos időpillanatban vesz.
  2) $Node_j$, $Node_k$ kétutas üzenetküldéssel szinkronizál.



9.) Idő szinkronizálás

- **Kommunikációs késleltetés ingadozása**:
  - Befolyásolja a pontosságot
  - Több összetevő közös hatása:
    - Küldési (Send) késleltetés: OS, hálózati protokoll stack, hálózati meghajtó firmware
    - Hozzáférési (Access) késleltetés: MAC
    - Továbbítási (Propagation) késleltetés:
    - Fogadási (Receive) késleltetés: nyelés, feldolgozás, OS értesítése



9.) Idő szinkronizálás

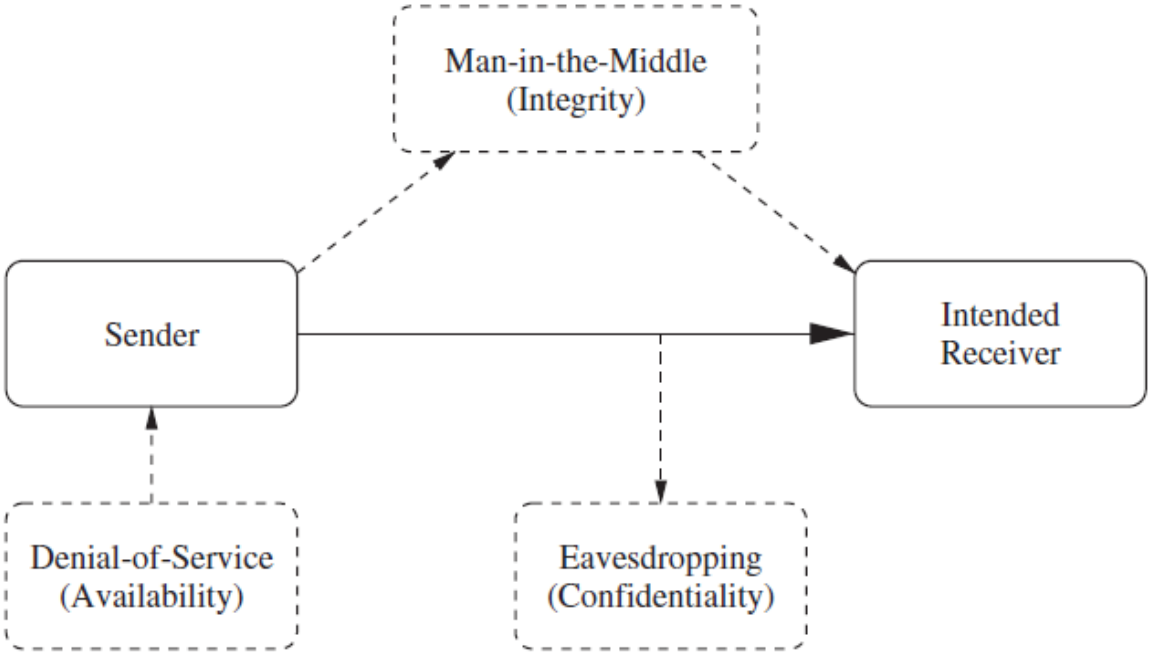
- **Idő szinkronizáló protokollok**:
    1) Reference Broadcast Using Global Sources of Time
    2) Lightweight Tree-Based Synchronization (LTS)
    3) Timing-sync Protocol for Sensor Networks (TPSN)
    4) Flooding Time Synchronization Protocol (FTSP)
    5) Reference-Broadcast Synchronization (RBS)
    6) Time-Diffusion Synchronization Protocol (TDP)
    7) Mini-Sync
    8) Tiny-Sync protokollok

10.) Biztonság

- **WSN biztonság témakör motivációja:**
  - Terep („csatatér”) megfigyelése és értékelése
  - Célpont követése
  - Civil infrastruktúra (híd, alagút) monitorozása
  - Katasztrófa terület értékelése beavatkozáshoz
- Meghibásodás vagy illetéktelen beavatkozás közötti különbségtétel nagyon nehézkes, mivel az erőforrások szűkösek
- **CIA biztonsági modell**:
  - **C**onfidentiality (bizalmasság): csak az illetékes címzett érti az üzenetet
  - **I**ntegrity (sértetlenség): küldés közben nem módosul az üzenet
  - **A**vailability (érvényesség): az alkalmazások bármikor hozzáférhetnek az üzenethez

10.) Biztonság

Pl. Támadás a CIA modellben:



- Eavesdropping (hallgatózás)
- Man-in-the-Middle (tégla)
- Denial-of-Service (szolgáltatásmegtagadás)

- Authentication (hitelesítés)
- Nonrepudiation (el nem utasítás)
- Digital signature (digitális aláírás)

10.) Biztonság

- **Biztonsági kihívások WSN-ben:**
  - 1) Erőforrás korlátok (RAM, CPU, energia):
    - Hagyományos biztonsági mechanizmusok nem alkalmazhatók
  - 2) Nincs központi ellenőrzés:
    - Nagy skála, erőforrás korlát, hálózat dinamika
  - 3) Távoli helyszín:
    - Megközelíthetetlen helyek ellenőrzéshez, magas költségű a helyszíni ellenőrzés
  - 4) Hiba-hajlamú kommunikáció:
    - Csomagok elvesztése gyakori (csatorna hiba, routing hiba, ütközés), ami megnehezíti a támadás, illetve egyéb hiba közötti különbség tételt
  - Önmenedzselő és önjavító képesség tovább működteti a megtámadott WSN rendszert is.

10.) Biztonság

- **Biztonsági kihívások WSN-ben (folyt.):**
  - Szenzorok által mért érzékeny adatok védelme titkosítást tesz szükségessé.
  - Adatok frissessége: nem a régi adatok újraküldése
  - Szenzor node lokalizációja jó helyen történő méréshez
  - Idő nem szinkronizálása adat-aggregáció hibát okoz
  - Hamis időbélyeg hibás szinkronizációt okoz

- **Támadások:**
  1) **Fizikai réteg DoS (Denial-of-Service)**:
     - Jamming: szándékos interferencia
     - Tampering: node fizikai babrálása
  2) **Adatkapcsolati réteg DoS**:
     - Collision: szándékos ütközés
     - Exhaustion: elemek lemerítése

10.) Biztonság

- **Támadások (folyt.):**
  - 3) **Routing réteg**:
    - Blackhole: fekete lyuk szerepkör
    - Selective forwarding: csak bizonyos csomagok
    - Rushing (hajsza): minden irányba elküldi az érkező választ, így magához szívja a forgalmat
    - Sinkhole: Sink node funkció átvétele
    - Sybil: több azonosság egyidőben, forgalom elszívása
    - Wormhole: két támadó összejátszik a forgalom elterelése céljából, majd blackhole/sinkhole
  - 4) **Szállítási réteg:**
    - Flooding: intenzív kapcsolat-felépítés, erőforrás elfogyasztás TCP-nél
    - Desynchronization: hamis csomag beküldése, szekvencia újraküldése TCP-nél

10.) Biztonság

- **Támadások (folyt.):**
    5) **Adat aggregálási réteg**:
        - **Átlag függvény:** egy elem megváltoztatása hibás aggregált értéket ad
        - **Összeg/Min/Max függvény**: egy elem megváltoztatása hibás aggregált értéket ad
    6) **Titok felfedése**:
        - **Lehallgatás**: illetéktelen hozzáférés adatokhoz
        - **Forgalomelemzés**: fontos node-ok azonosítása

- **Biztonsági protokollok és mechanizmusok:**
    1) **Szimmetrikus és publikus kulcsú kriptográfia:**
        - Szimmetrikus kulcsú kriptográfia, olcsóbb
        - RSA (Rivest-Shamir-Adleman) publikus kulcsú kriptográfia, drágább
        - ECC (Elliptic Curve Cryptography), drágább

10.) Biztonság

- Biztonsági protokollok és mechanizmusok (folyt.):

2) **Kulcs menedzsment:**

- Peer Intermediaries for Key Establishment (PIKE)

3) **DoS kivédése:**

- Jamming: zóna kikerülése
- Collision/Exhaustion: ECC kód használata
- Spoofing/Alteration: üzenet azonosítás kód hasz.
- Path DoS: hash lánc használata

4) **Aggregáció védelem**:

- Késleltetett aggregáció
- Késleltetett hitelesítés

5) **Routing védelem**:

- Sybil: node ID ellenőrzése
- Sinkhole/Wormhole: geográfiai routing
- Rushing: szomszéd biztonságos azonosítása

10.) Biztonság

- Biztonsági protokollok és mechanizmusok (folyt.):

6) **Secure Network Encryption Protocol (SNEP):**

- Titkosítás, hitelesítés és véletlenszám generálás

7) **TinySec**:

- Hitelesítés titkosítás opció
- Csak hitelesítés opció

8) **Localized Encryption and Authentication Protocol**

- LEAP négy kulcs mechanizmussal (egyéni, csoport, klaszter, pár szintű)

9) **IEEE 802.15.4 és ZigBee biztonság**:

- Négy biztonsági modell egyidőben:
  - Access Control
  - Message Integrity
  - Message Confidentiality
  - Replay Protection

Ajánlott irodalom

1) Waltenegus Dargie, Chritian Poellabauer, **Fundamentals of Wireless Sensor Networks – Theory and Practice**, Wiley Series on Wireless Communications and Mobile Coputing, Wiley, 2010.
2) Ian F. Akyildiz, Mehmet Can Vuran, **Wireless Sensor Networks**, Ian F. Akyildiz Series in Communications and Networking, Wiley, 2010.
3) Ananthram Swami, Qing Zhao, Yao-Win Hong, Lang Tong, **Wireless Sensor Networks – Signal Processing and Communications Perspectives**, Wiley, 2007.
4) Kaveh Pahlavan, Allen H. Levesque, **Wireless Information Networks**, Second Edition, Wiley-Interscience, 2005.


Köszönöm a figyelmet!
zgal@unideb.hu