CommLab

Recent Advances in Wireless Body Sensor Networks for Physiological Monitoring

Engineering in Medicine and Biology Society - Syracuse Chapter
The EMBS HealthTech Symposium
Spring 2010

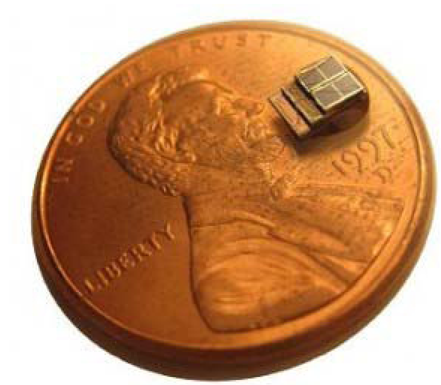
Dr. Gill R. Tsouri

Communication Laboratory (CommLab)
Department of Electrical & Microelectronic Engineering
Kate Gleason College of Engineering
Rochester Institute of Technology (RIT)

Body Sensor Networks

Background

- Intercommunicating **wireless body mounted biomedical sensors**.
- Used to **collect medical data** and relay to remote caregiver.
- Future applications would include **automatic drug delivery**.
- Sensors and power sources are small and efficient.
- **The main power consumer is the wireless transceiver**.
- Major concerns: patient **privacy**, **safety** and **reliability**, prolonging sensor lifetime.



["Tiny Sensor Could Run for Years Harnessing Energy from Environment", Singularity Hub, February 24th, 2010]

[Michigan Tech. Enterprise Program]

[Y. M. Chi, S. R. Deiss and G. Cauwenberghs, "Non-contact Low Power EEG/ECG Electrode for High Density Wearable Biopotential Sensor Network", 6th International Workshop on Wearable and Implantable Body Sensor Networks, 2009]

Body Sensor Networks

Personal Status Monitoring (PSM)

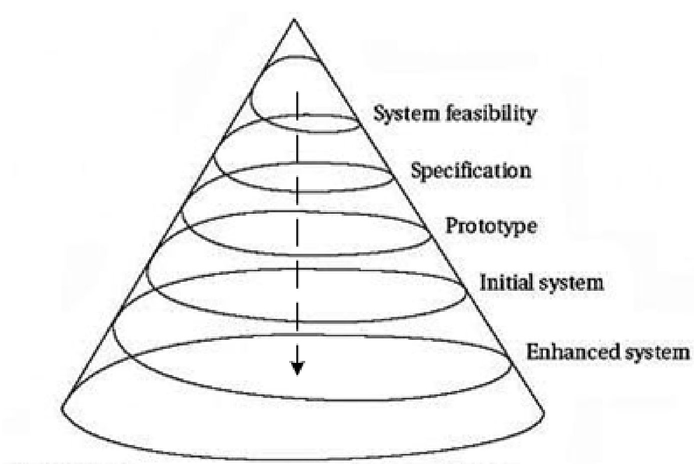
- Shirt with easily embedded wireless enabled sensors.
- Collect sensor data to PSM which displays data and acts as a gateway to a remote caregiver.
- Potential applications:
  - Automated home monitoring.
  - Smart soldier outfit.
  - Patient monitoring in hospitals.
- A 9 months project in *CommLab* to design a body sensor network platform, sponsored by:

BLUE HIGHWAY
-DESTINATION: INNOVATION-

A WelchAllyn COMPANY

(with MSc student Adrian Sapio)

- A 3 year prototyping project is underway.



[W. Wolf, *Computers As Components*, 2nd Edition, Elsevier, 2008]

Project Description

CommLab

Design a reliable and secure wireless communication platform for Body Sensor Networks (BSNs) with ultra low-power consumption

- Data gathered from sensors to a PSM (up to range of 2m).
- PSM acts as gateway to remote caregiver.
- Sensors are non-redundant, simple and low-cost.
- Complexity resides in PSM.
- Mitigate interference from other devices and multiple BSNs.
- Support mobility.

<u>Design novelties:</u>

- Use ***relaying of creeping-waves*** to reduce power consumption.
- Apply ***wireless physical layer security*** to secure communication.

Outline

- System Requirements.
- System Design.
- **Relaying of Creeping Waves.**
- **Wireless Physical Layer Security.**
- Conclusion.

System Requirements

- Use 2.4-2.4835 GHz unlicensed ISM band
  - No licensing fee - worldwide.
  - Small antennas.
  - Off-the shelf components.

- Meet FCC requirements
  - Spread Spectrum modulation.
  - Power emissions.

- Use centralized architecture
  - PSM is master, sensors are slaves.

- Provide data rates greater than 500kbps with bit error rates less than 10^{-6}.

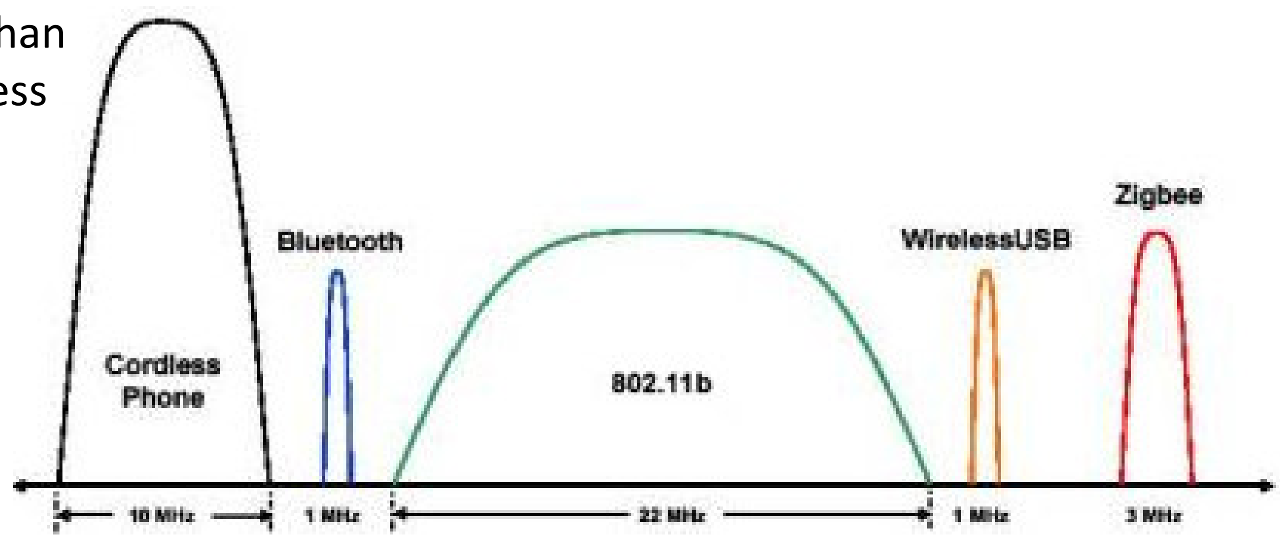
- Support multiple BSNs in close proximity.

- **Maximize battery life**

- **Secure links**

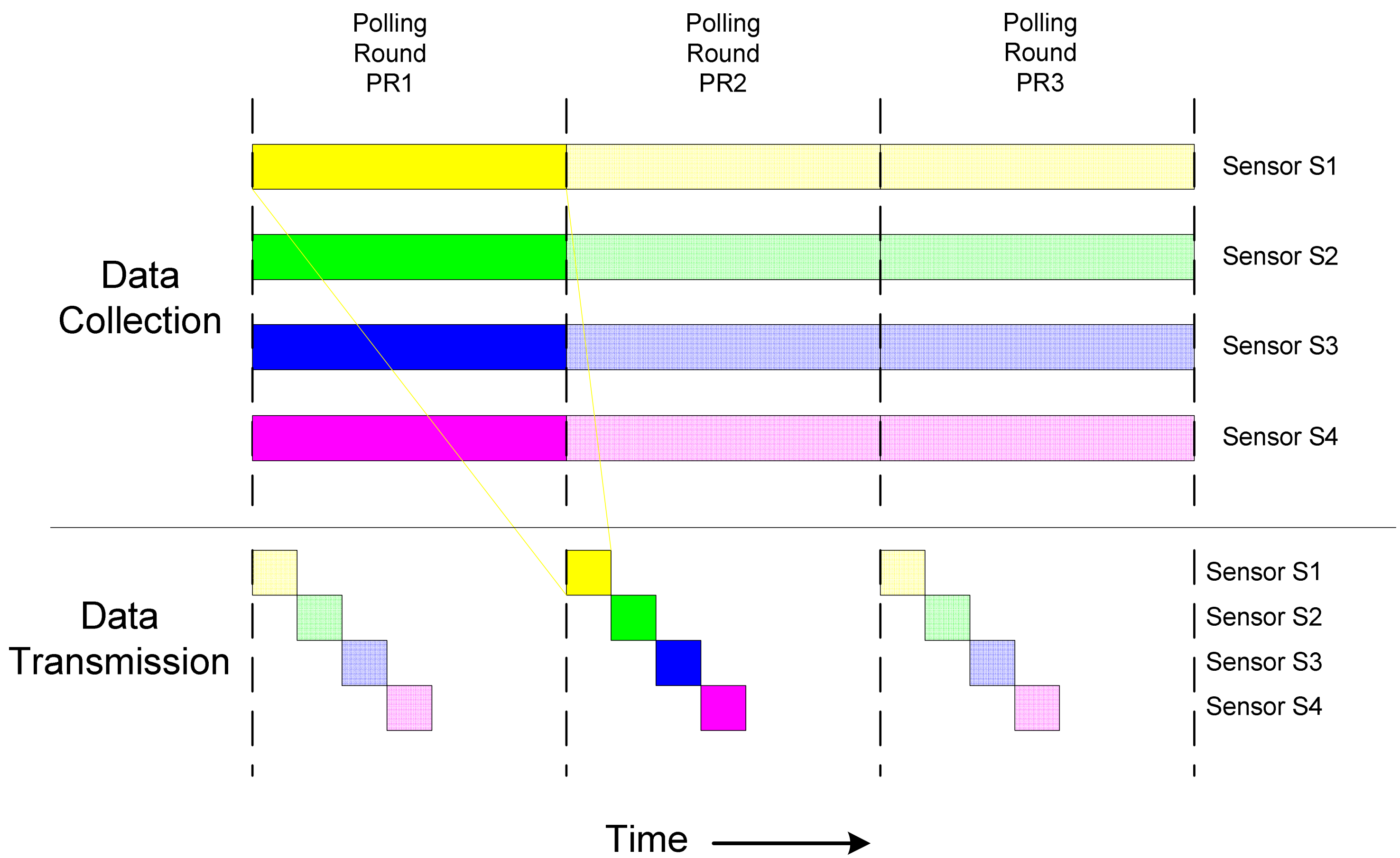
- **Support mobility**

- **Mitigate Interference**
(Wireless USB, Bluetooth, Wireless LANs, ZigBee, cordless phones, CCTV cameras, Proprietary technologies…)



System Design

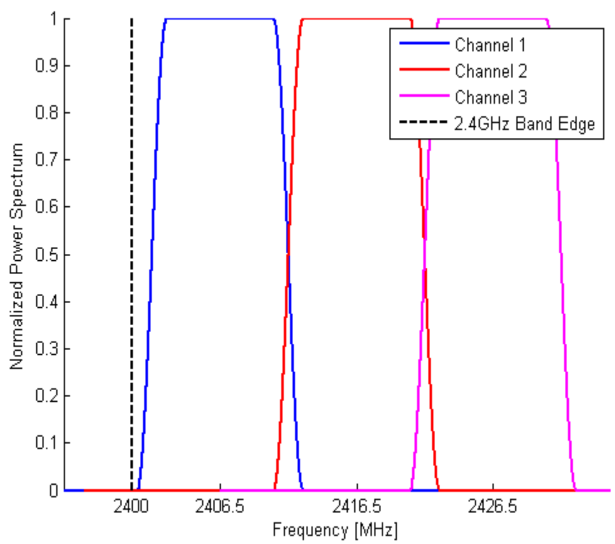
Data Collection & Transmission



System Design

Channelization & Data Rates

Channel	Center Frequency (MHz)	Frequency Range (MHz)
1	2406.5	2401.5 - 2411.5
2	2416.5	2411.5 - 2421.5
3	2426.5	2421.5 - 2431.5
4	2436.5	2431.5 - 2441.5
5	2446.5	2441.5 - 2451.5
6	2456.5	2451.5 - 2461.5
7	2466.5	2461.5 - 2471.5
8	2476.5	2471.5 - 2481.5



Chip Rate	10	Mcps
Symbol Rate	322.5	Ksps
Bit Rate	645.1	Kbps

Channels

- 8 channels each 10MHz wide.
- Raised Cosine pulse with roll off factor 0.22.

Spread Spectrum processing gain: 31

- ~31 orthogonal PANs.
- Interference energy reduction factor of 1/31.

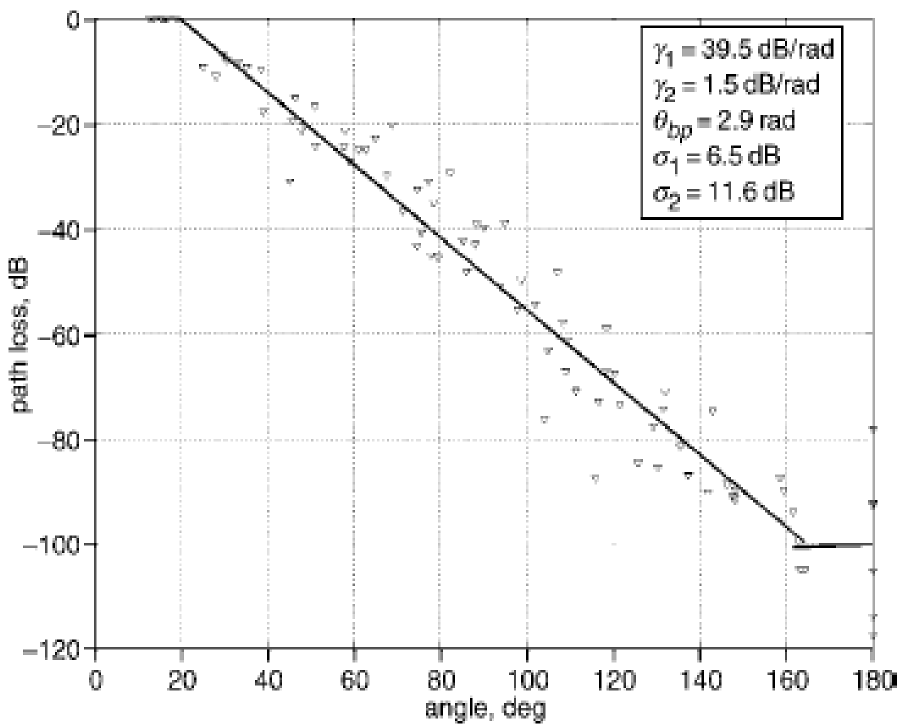
Outline

- System Requirements.
- System Design.
- ***Relaying of Creeping Waves.***
- Wireless Physical Layer Security.
- Conclusion.

Creeping Waves

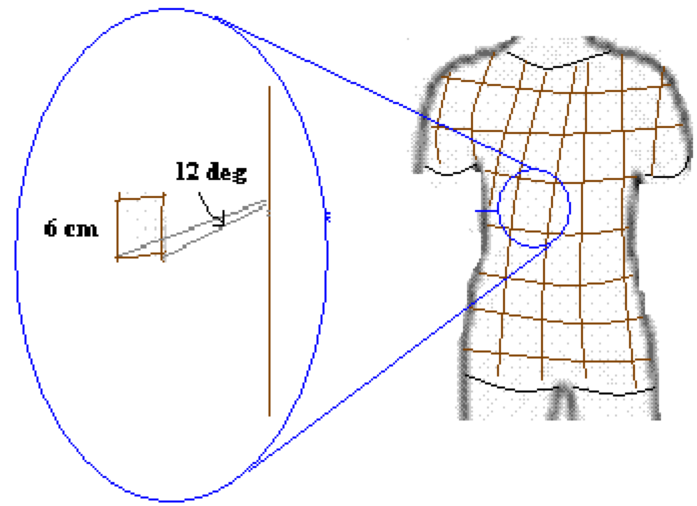
Path Loss Model

Path loss measurements for a frequency of 2.4GHz



[J. Ryckaert, P. D. Doncker, R. Meys, A. de Le Hoye, and S. Donnay, “Channel model for wireless communication around human body”, Electronic Letters, vol. 40, no. 9, pp. 543-544, Apr. 2004]

$$\overline{PL}(\theta) = \begin{cases} 39.5\theta - 13\ [dB] & ; \quad 0.11\pi[rad] < \theta < 0.88\pi[rad] \\ 1.5\theta + 96\ [dB] & ; \quad 0.88\pi[rad] < \theta < \pi[rad] \end{cases}$$



- Nice fit of model to sensor-embedded shirt.
- Variance of path-loss due to height is low.
- No past work on BSN design based on creeping waves.
- Single variable (phase).

Creeping Waves

Generic Link Budget

$$\overline{PL}(\theta) = \begin{cases} 39.5\theta - 13\ [dB] & ; \quad 0.11\pi[rad] < \theta < 0.88\pi[rad] \\ 1.5\theta + 96\ [dB] & ; \quad 0.88\pi[rad] < \theta < \pi[rad] \end{cases}$$

$26\ dB$ (4 standard deviations protection margin for height variance and interference range)

$$L_{CW}(\theta) = 39.5\theta + 13\ [dB] \quad ; \quad 0 < \theta < \pi[rad]$$

$$\boxed{P_{tx}(\theta) = G_T + L_{cw}(\theta)}$$

$$G_T = P_{rx} - G_{tx} - G_{rx} + L_{fm}$$

$P_{tx}(\theta)$	= Transmitter power as function of the creeping angle.
P_{rx}	= Receiver sensitivity.
G_{tx}	= Transmitter antenna gain.
G_{rx}	= Receiver antenna gain.
$L_{cw}(\theta)$	= Creeping wave path loss as function of the creeping angle.
L_{fm}	= Channel fade margin.

Creeping Waves

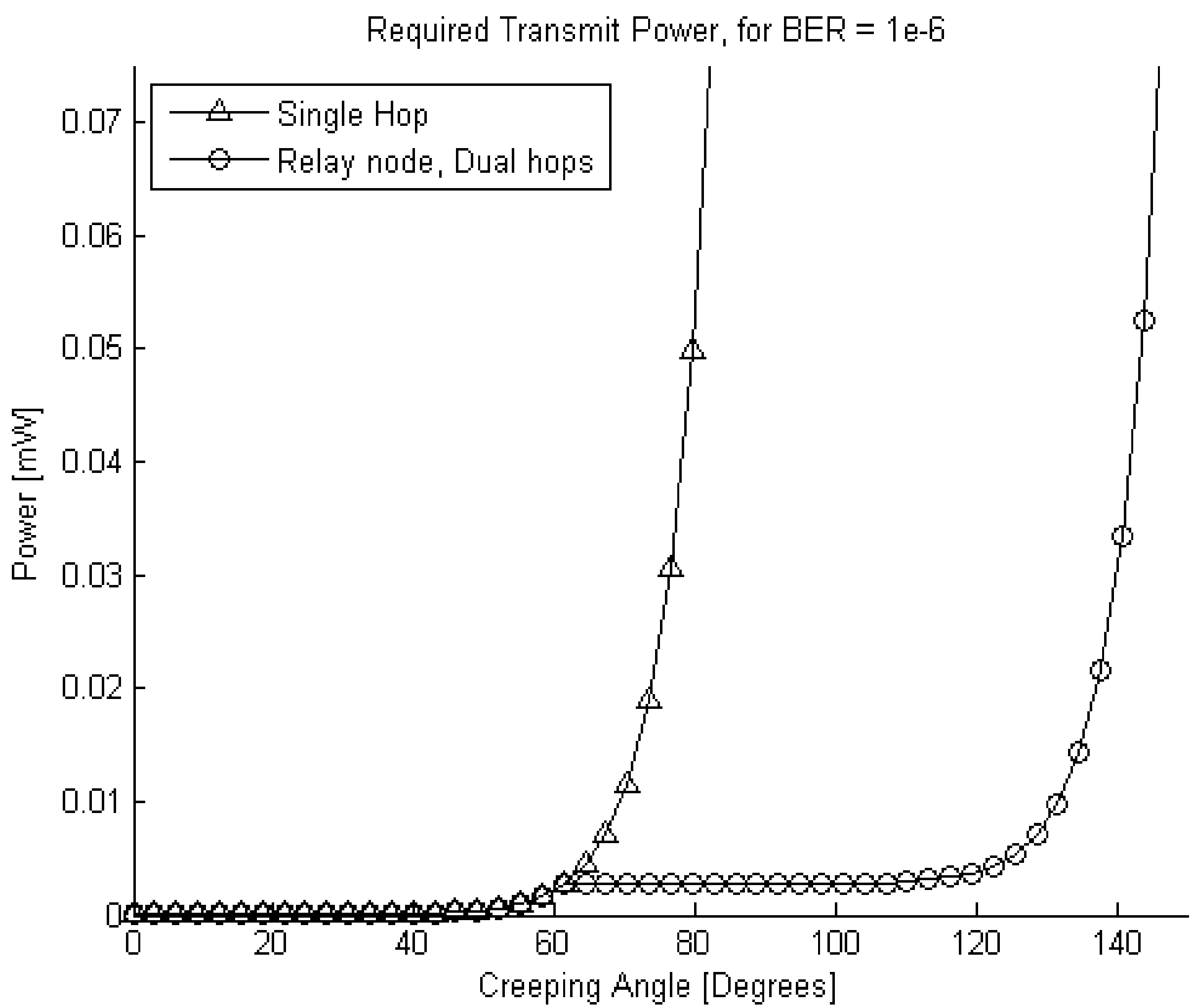
Specific Link Budget

- Worst-case **temperature of 370^{O} K**.
- Spread Spectrum **processing gain of 31**.
- Off the shelf 2.4GHz components with **Noise Figure of 7 dB**.
- Achieve **Bit Error Rate of 10^{-6}** .
- Use Differential Quadrature Phase Shift Keying (**DQPSK**) modulation.
- Use **simple omni-directional dipole antennas with 0 dB gains**.
- Make sure that **99% of multipath fading instances** are below median signal level.

$$G_T = -67.89[dB]$$

Creeping Waves

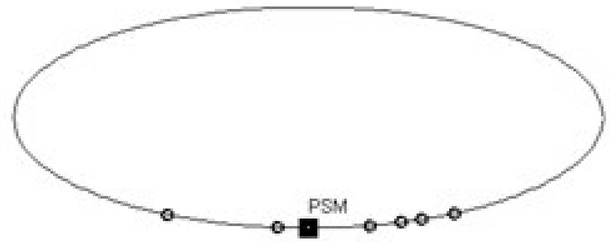
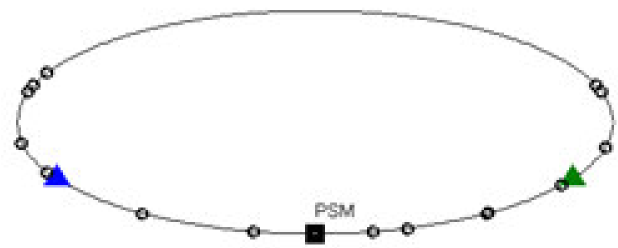
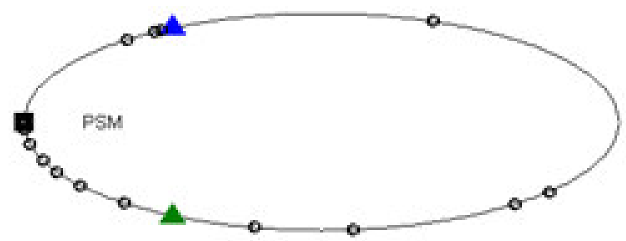
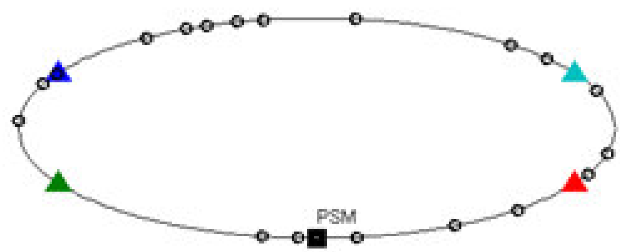
Relaying of Creeping Waves Around Body



- Break point for specific link budget is around 60°.
- Relaying before the breakpoint is justified despite the need for retransmission.

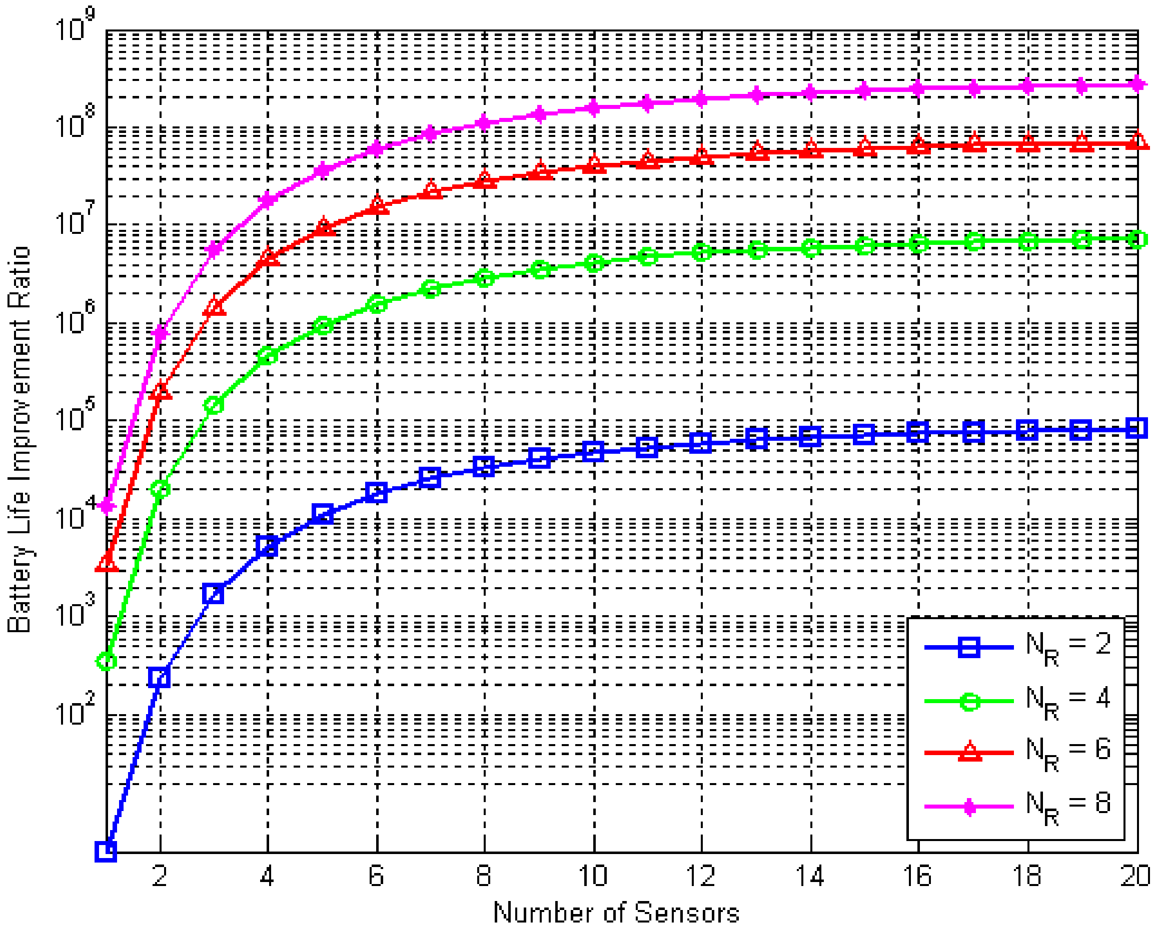
$$G_T = -67.89[dB]$$

Network Topologies

Type 1 Topology (Narrow Front Coverage)	
Type 2 Topology (Wide Front Coverage)	
Type 2 Topology (Wide Flank Coverage)	
Type 3 Topology (Full Coverage)	

Performance Analysis

Gain in Network Lifetime



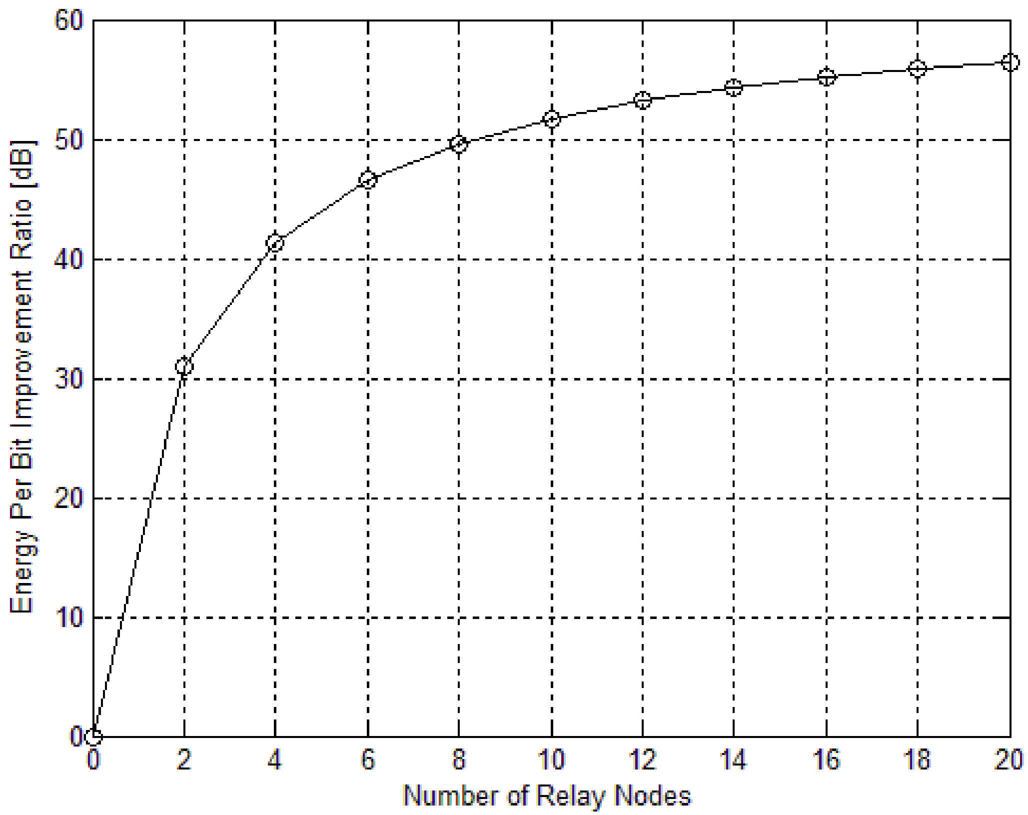
- **Network Lifetime** is defined as the time it takes a single network component to empty its power source.
- Dramatic improvement despite retransmissions.
- Gain increases as number of sensors increases.
- Gain has asymptotic behavior.
- For a full coverage topology (4 relay nodes) gain is **10^7** fold increase .
- Analytical results.

$$R_{NL} = P_{tx}\left(\pi \frac{N_S}{N_S+1}\right) - \left\{P_{tx}\left(\frac{2\pi}{N_R+2}\right) + 10\ log_{10}\left[\frac{N_S}{2}\left(1 - \frac{2}{N_R+2}\right)\right]\right\}\ [dB]$$

$$P_{tx}(\theta) = G_T + 39.5\theta\ [\text{dB}],\quad 0 < \theta < \pi$$

Performance Analysis

Gain in Average Energy per Bit



$$R_{EPB} = \frac{\left(N_R/2 + 1\right)\left(10^{P_{tx}\left(\frac{\pi}{2}\right)/10} t_B\right)}{\sum_{i=0}^{N_R/2} \left\{ 10^{\left(P_{tx}\left(\frac{\theta_R}{2}\right)/10\right)} + i \cdot 10^{\left(P_{tx}(\theta_R)/10\right)} \right\}}$$

- **Average Energy per Bit** is defined as the average energy that is required to reliably send and receive a single information bit.
- Dramatic improvement despite retransmissions.
- Gain increases as number of relay nodes increase.
- Gain has asymptotic behavior.
- For a full coverage topology (4 relay nodes) gain is ~40dB ⇔ **10^4** fold decrease .
- Analytical results.

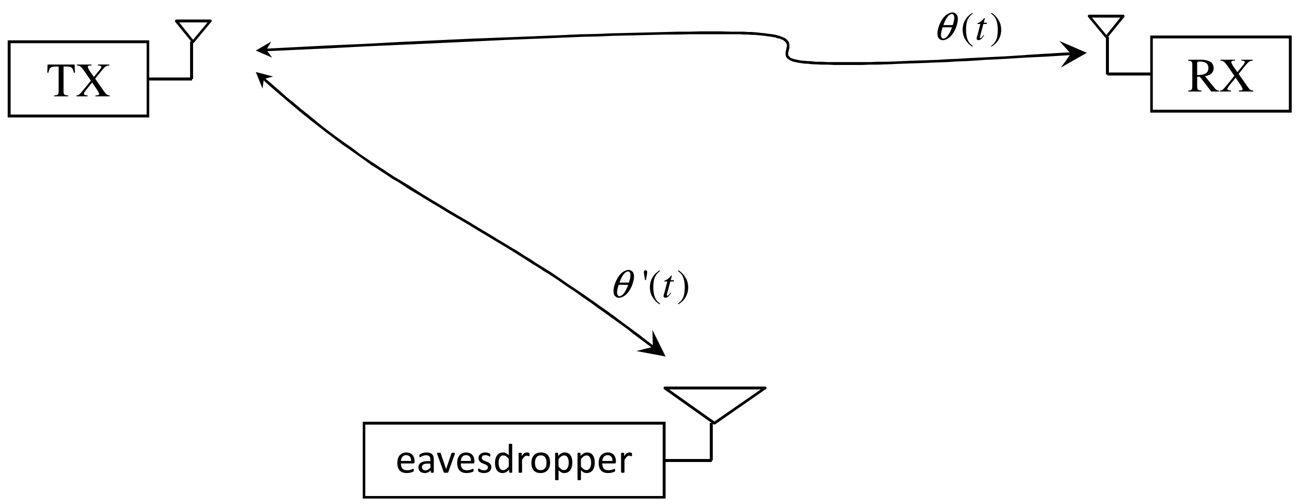
Outline

- System Requirements.
- System Design.
- Relaying of Creeping Waves.
- ***Wireless Physical Layer Security.***
- Conclusion.

Wireless Physical Layer Security

Principle

- Existing security algorithms (DES, AES, Diffie-Hellman, etc.) offer sufficient security strength but require excessive system resources.
- Make use of three properties of the wireless channel:
    - Channel de-correlates in time.
    - Channel de-correlates in space.
    - Channel is reciprocal.
- Short term estimation of channel parameters is a **common secret**.
- Concept was not applied to BSNs before.

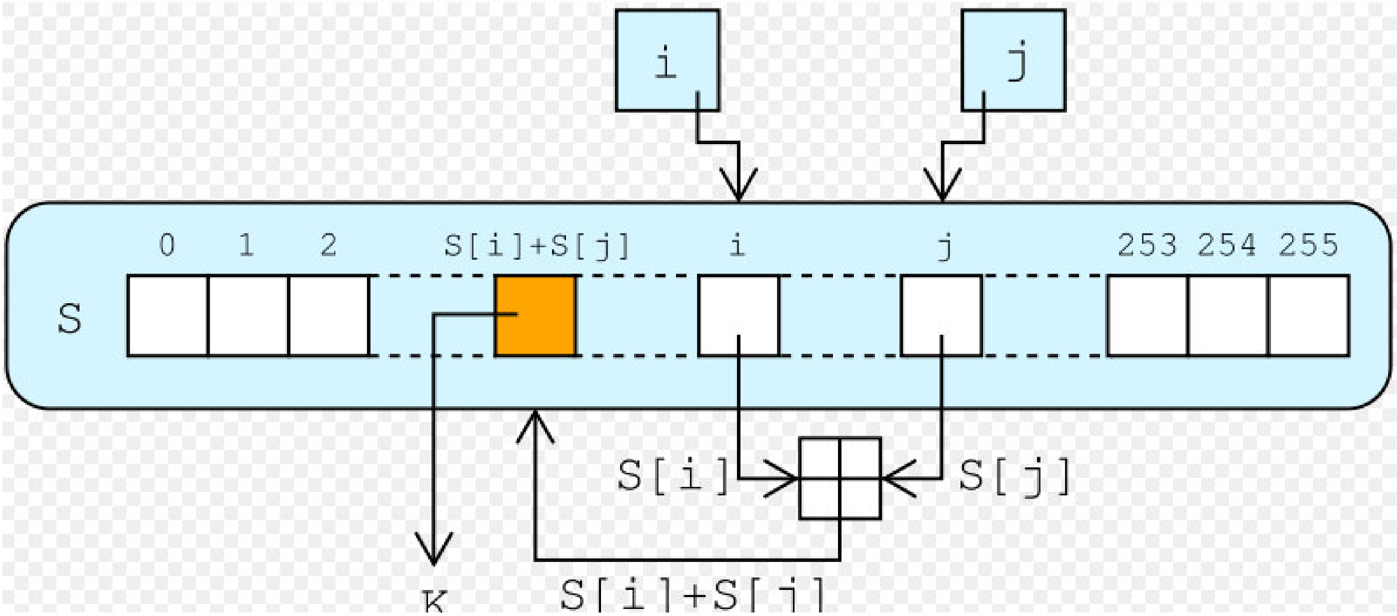


Wireless Physical Layer Security

Principle

• Quantize phase estimates to periodically refresh a symmetric key to be used with a simple stream cipher, while introducing negligible system overheads.

• Low cost ***key refreshing*** and simple ***stream cipher*** encryption replace "heavy" cryptography relying on complex algorithms and large pre-deployed key (e.g., **DES** with 128 bit key, **Diffie-Hellman** key distribution, **RSA** etc…).



Security

Key Refreshing Algorithm

Algorithm is embedded in the polling protocol and requires no overhead.

Baseband model for received symbol at correlator output:

$$r_i = A|h|e^{j\varphi_i}e^{j\alpha} + n_i$$

1. Sensor checks *polling* packet for Cyclic Redundancy Check (CRC) and proceeds when no error is present (this is almost always the case due to link budget).
2. Sensor removes information using decision feedback:

$$p_i = r_i e^{-j\varphi_i} = A|h|e^{j\alpha} + n_i e^{-j\varphi_i}$$

3. Sensor estimates phase using all symbols in packet (best possible estimator):

$$A|h|e^{j\alpha} \approx \frac{1}{N}\sum_{i=1}^{N} r_i \quad \Leftrightarrow \quad \hat{\alpha} = \arctan\left(\frac{Im\{\sum_{i=1}^{N} r_i\}}{Re\{\sum_{i=1}^{N} r_i\}}\right)$$

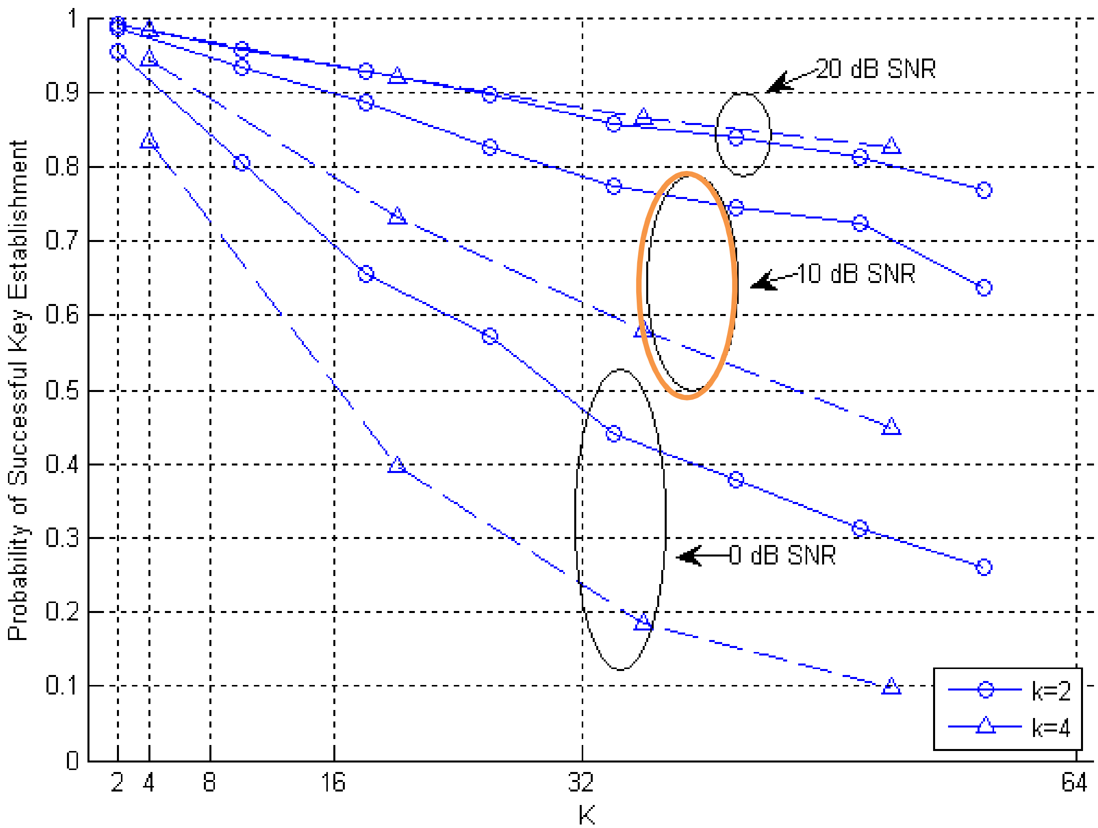
4. Sensor quantizes channel phase estimate to generate k key bits.

$$\mathbf{k} = \left\lfloor \hat{\alpha}\,\frac{2^k}{2\pi} \right\rfloor$$

5. PSM goes through 1-4 using the *response* packet it receives from the sensor.
6. Process is repeated $\left\lceil \frac{K}{k} \right\rceil$ times to generate a complete K bits key.
7. PSM and sensor authenticate new key by concatenated encryption of next polling.

Performance Analysis

Successful Key Establishment



$$P_{key} = [P_r(\mathbf{k}_1 = \mathbf{k}_2)]^{\lceil \frac{K}{k} \rceil},$$

- Failure is due to different quantization of phase at PSM and sensor.
- For short packets of 320 symbols.
- Recall that no overhead is required for key establishment.
- Key establishment failure only means we have to retry.
- Probability of a single successful attempt out of many is close to 1.
- Numerical computation results.

Conclusion

- **Relaying of creeping waves** results in substantial gains when designing a reliable body sensor networks.

- **Wireless Physical Layer Security coupled with stream ciphering** is an attractive solution for securing a BSN with low overheads.

Conclusion

Publications

- G. R. Tsouri and A. Sapio, "Method of Securing Resource-Constrained Wireless Enabled Devices via Channel Randomness", *IEEE 28th International Conference on Consumer Electronics (ICCE)*, Jan. 2010.

- A. Sapio and G. R. Tsouri, “Ultra-Low Power Body Sensor Network for Wireless ECG”, *International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Jun. 2010.

- A. Sapio and G. R. Tsouri, “Robust and Efficient Networking of Body Sensors using Relaying of Creeping Waves in the Unlicensed 2.4GHz Band”, submitted to *ACM/Springer Trans. on Mobile Networks & Applications – Special Issue on Ubiquitous Body Sensor Networks*.

Prototyping to begin soon in *CommLab*