Heart-Device Hacking Risks Seen

By KEITH J. WINSTEIN
March 12, 2008, Page D7

Medical devices that control the human heart may need safeguards to protect against remote-control hacking that could deliver electrical shocks to patients, researchers said.

Millions of Americans have pacemakers, which keep hearts beating regularly, or an implanted defibrillator, which can restart stopped hearts with an electric jolt. After implanting a defibrillator under a patient's skin, a doctor uses a special device, about the size of a breadbox, to tell the defibrillator what to do -- for example, to instruct it to keep the heart beating at a certain rate or deliver a test jolt.

The devices, called programmers, communicate with a defibrillator using radio waves. To prevent tampering, only physicians are allowed to buy one from the manufacturers -- Medtronic Inc., Boston Scientific Corp., and St. Jude Medical Inc.

But hackers could transmit the same radio signals -- causing a defibrillator to shock or shut down, or divulge a patient's medical information -- without needing a programmer, researchers found in a laboratory test of one model from Medtronic.
Opportunities for Fidelity-Energy Minimization in Body Area Networks: A Communications Perspective

Mark Hanson
Getting Started: RF-BANs

“The scientists of today think deeply instead of clearly. One must be sane to think clearly, but one can think deeply and be quite insane.”

~ N. Tesla

1) Image from the Library of Congress (loc.gov)
What’s Important in RF-BANs?

- Form
- Fidelity
- Energy
- Security
So where should we start?

1) Image from the Crossbow Corporation (xbow.com)

Energy Profile Using AEON  

- Sensor Board: 60%
- CPU Active: 5%
- CPU Idle: 22%
- Radio Tx: 8%
- Radio Rx: 5%

MICA2 Mote 1

MICA2 Power Model 2

<table>
<thead>
<tr>
<th>Device</th>
<th>Current</th>
<th>Device</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Active</td>
<td>7.6 mA</td>
<td>Radio (900 MHz)</td>
<td>60 μA</td>
</tr>
<tr>
<td>Idle</td>
<td>3.3 mA</td>
<td>Core</td>
<td>1.38 mA</td>
</tr>
<tr>
<td>ADC Noise</td>
<td>1.0 mA</td>
<td>Bias</td>
<td>9.6 mA</td>
</tr>
<tr>
<td>Power down</td>
<td>116 μA</td>
<td>Tx (-18 dBm)</td>
<td>8.8 mA</td>
</tr>
<tr>
<td>Power Save</td>
<td>124 μA</td>
<td>Tx (-13 dBm)</td>
<td>9.8 mA</td>
</tr>
<tr>
<td>Standby</td>
<td>237 μA</td>
<td>Tx (-10 dBm)</td>
<td>10.4 mA</td>
</tr>
<tr>
<td>Ext Standby</td>
<td>243 μA</td>
<td>Tx (-6 dBm)</td>
<td>11.3 mA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tx (-2 dBm)</td>
<td>15.6 mA</td>
</tr>
<tr>
<td>LED (each)</td>
<td>2.2 mA</td>
<td>Tx (0 dBm)</td>
<td>17.0 mA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tx (+3 dBm)</td>
<td>20.2 mA</td>
</tr>
<tr>
<td>Sensor Board</td>
<td>0.7 mA</td>
<td>Tx (+4 dBm)</td>
<td>22.5 mA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tx (+5 dBm)</td>
<td>26.9 mA</td>
</tr>
</tbody>
</table>
Radio Woes

• Observation: The radio is consuming a large proportion of the energy in sensor nodes.
• Question: What are the implications?
• Question: What can be done?

A Radio Model

Average Radio Power Consumption

\[
P_{\text{radio}} = N_{tx}[P_{tx}(T_{on-tx} + T_{st}) + P_{out}T_{on-tx}] + N_{rx}[P_{rx}(T_{on-rx} + T_{st})]
\]

Body-Area Channel Woes

- The body poses major challenges for low-power, reliable communication.
- At 2.4 GHz, there is significant attenuation due to the body.
- Sensor placement causes received signal strength to fluctuate due to variability of path loss.

More Body-Area Channel Woes

Attenuation Due to Body Movement

More Body-Area Wireless Woes

Channel Coherence Time During to Body Movement

- Observation: A moving body can cause the channel characteristics can change over time.
- Question: What are the implications?
- Question: What can be done?

Quick Detour: Information Theory

“Information is the resolution of uncertainty.”

~ C.E. Shannon

1) Image from of Bell Labs (bell-labs.com)
Source Coding Theorem

- **Motivation:**
  - Signals generated from physical sources contain redundant information
  - Efficient transmission of signals requires purposeful removal of redundancy

- **Source Coding Theorem**
  - Average code word length for a distortionless source-encoding scheme is bounded by the source entropy

Source Coding in Practice

\( \eta = \) efficiency

\( H(S) = \) entropy

\( S = \) source alphabet

\( p_k = \) probability that a symbol is emitted by the source

\( L = \) bits per symbol

\[
\eta = \frac{H(S)}{L}
\]

\[
H(S) = \sum_{k=0}^{K-1} p_k \log_2 \left( \frac{1}{p_k} \right)
\]

Popular Choices of Source Codes:
Huffman, Arithmetic LZ, RLE
Channel Coding Theorem

• Motivation:
  – Wireless channels are noisy
  – Reliable transmission in noisy environments requires purposeful injection of redundancy

• Channel-Coding Theorem
  – If the channel has a capacity $C$ and the source generates information at a rate less than $C$, then a coding technique can produce an arbitrarily low probability of symbol error

Channel Coding in Practice

- Channel Coding generally falls into two schemes:
  - Forward Error Correction (FEC)
    - No Feedback (Detect & Correct)
    - Block, Convolutional
  - Automatic Repeat Request (ARQ)
    - Feedback (Detect)

Information Capacity Theorem

\[ C = B \log_2 \left( 1 + \frac{P}{\sigma^2} \right) \text{bits/s} \]

B = Channel Bandwidth
P = Transmit Power
\( \sigma^2 \) = Variance of Channel Noise
P/ \( \sigma^2 \) = Output SNR

• Interesting observations/implications?

Information Capacity in Practice

\[ \left( \frac{E_b}{N_0} \right)_{rx} = \frac{P_{out}}{P_{loss} \bar{\alpha}} \cdot \frac{1}{WN_{th}N_{rx}} \]

- Relating Power Consumption and Fidelity
  - We can also evaluate for the expected SNR at the receiver given a general radio model
- How will the body area fading affect received SNR?
- Are there system design implications?

Rate Distortion Theory

• Motivation:
  – Alphabet of the source code is insufficient to guarantee exact source reconstruction
  – Channel (information) capacity is insufficient for the source rate

• Basic Idea:
  – Minimize information (rate) to send across a channel to approximately (distortion) reconstruct a source with a given distortion

Rate Distortion in Practice

- For a memoryless Gaussian source, $R(D)$ is a monotonically decreasing convex function.
- Pareto optimality is achieved on the rate function.
- Question: What is distortion?

$$R(D) = \begin{cases} \frac{1}{2} \log_2(\frac{\sigma_x^2}{D}), & \text{if } D \leq \sigma_x^2 \\ 0, & \text{if } D > \sigma_x^2 \end{cases}$$

1) Images from Wikimedia Commons (wikimedia.org)
Interleaving

\[ L_{\text{burst}} = R_b T_{\text{coherence}} \]

- Many channel coding schemes are designed for statistically independent, randomly distributed bit errors
- Bit errors often occur in bursts (RF-BANs)
- Interleaving scrambles the order of the channel coded source to alleviate this problem
Paper 1: Takeaway Points

Total Power Optimization for Wireless Multimedia Communication

~E. Erkip, X. Lu, Y. Wang, D. Goodman

Source of Paper 1

1) Image from Amazon (amazon.com)
Abstract Problem Formulation

- **Goal:** Minimize $P_{\text{tot}}$ subject to $D_{\text{tot}} \leq D_0$
  \[ D_{\text{tot}} = (1 - p_s)D(R) + p_s \sigma^2 \]

- **Model:** $P_{\text{tot}} = P_s + P_t$
  \[ P_{\text{tot}} = c_s f_s N + (-c_t d^\alpha R f_s N_0 \ln(2p_e)) \]

- What are the knobs?
- Is this model applicable to BANs?
- What’s missing?

---

Results of Abstract Formulation

- Figure (a) models a scenario where channel attenuation is low
- Figure (b) models a scenario where channel attenuation is high

Results of Abstract Formulation

- Figure (c) summarizes minimum total power consumption vs. distance.
- How do we interpret these results—especially in the context of rf-BANs?

H.263 Problem Formulation

- **Goal:** Model H.263
- **Differences:**
  - Use 2 State Markov channel model
  - Assume a RS(n,k) channel code with a RS power model
  - Application power profiling (H.263)
  - Introduce burst errors

Paper 1 Conclusion

- Optimum distortion-power operating points are dependent on distance
  - Large distance transmission of each bit is more costly, so more compression and more channel coding are needed
- Is this approach realizable on resource-constrained hardware?
- How will this strategy be affected by body movement?

Paper 2: Takeaway Points

Joint Source-Channel Coding and Power Allocation for Energy Efficient Wireless Video Communications

~F. Zhai, Y. Eisenberg, N. Pappas, B. Berry, A.K. Katsaggelos

Source of Paper

- The Forty-First Annual Allerton Conference on Communication, Control, and Computing
Problem Formulation 1

• Joint source-channel coding and power allocation
  – Increasing $P_{tx}$ for a fixed transmission rate can decrease BER
  – Increasing $P_{tx}$ for a fixed BER can also increase transmission rate

• Resource allocation is the primary focus
  – Minimize energy-distortion function

Minimization Problem

\[
\begin{align*}
\min_{\{\mu, \nu, \eta \in \mathbb{Q} \times \mathbb{R} \times \mathbb{P}\}} & \quad E[D] = \sum_{k=1}^{M} E[D_k(\mu, \nu, \eta)] \\
\text{s.t.} & \quad C = \sum_{k=1}^{M} B_k(\mu_k, \nu_k) P_k(\eta_k) / R_T \leq C_0 \\
& \quad T = \sum_{k=1}^{M} B_k(\mu_k, \nu_k) / R_T \leq T_0,
\end{align*}
\]

Paper 2 Conclusion

- Cross-layer minimization methodology for JSCCPA shows promise
  - Trades-off video quality and resource allocation for energy-efficient wireless video communication
  - Outperforms OERSC and JSCPA in simulations

- Is this type of minimization suitable for dynamic channel conditions?

A communication perspective is largely neglected in current BANs. Cross-layer analysis and design is necessary to meet application fidelity-energy requirements for next-gen BOTES.
Opportunities for Fidelity-Energy Minimization in Body Area Networks: A Communications Perspective

Mark Hanson