Design Challenges and Practical Solutions for Securing Wireless Body Area Networks

Dr. Ming Li
10/16/2013

Assistant Professor,
Dept. of Computer Science,
Utah State University
Outline

- Background on Body Area Networks (BAN)
- Main Design Challenges
- BANA: Body Area Network Authentication Exploiting Channel Characteristics
- ASK-BAN: Authenticated Secret Key Extraction for BANs
- Conclusion and Future Work
Background

- Wireless Body Area Network (BAN)

[Source: http://inertia.ece.virginia.edu/_/rsrc/1252884016768/engineering-research/body-area-sensor-networks/]
Security Issues in BAN

- Medical devices can also have *actuators*

**Board Urges Feds to Prevent Medical Device Hacking**

By *Kim Zetter*  
April 10, 2012 | 3:47 pm | Categories: Cybersecurity

In the wake of increasing concern about the security of wireless medical devices, a privacy and security advisory board is calling on the government to grant the FDA or other federal entity the authority to assess the security of devices before they’re released for sale to the market.

The group also wants the government to establish a clear channel through the United States Computer Emergency Readiness Team for reporting security problems with medical devices — including pacemakers, defibrillators, and insulin pumps — so vulnerabilities can be easily tracked and addressed.

“Who has to die before Security is Increased in Wireless Enabled Medical Devices?”
Security Issues in BAN (cont’d)

- System and device-level security (authentication & integrity)
  - Data must come from legitimate devices, and should not be modified.
  - Affect safety!
- Invasion of privacy (data confidentiality)
  - Why should we care?
- Availability (robustness)
  - Against inadvertent or malicious Denial-of-Service

Wearable ECG monitors, Pulse Oximeter, Glucose Monitors, Cardiac Defibrillators
Secure Trust Initialization

- Bootstrap secure communication within a BAN
  - Establish authenticated secret keys to protect BAN from attacks
  - Securing both one-to-one and group communication

- Attack model
  - Can eavesdrop, modify, insert, delete information from the wireless channel
  - May compromise devices afterwards

- General assumption
  - Devices share no secret information a priori
BAN Security Challenges

- **Resource-constraint**
  - Battery power;
  - Hardware (memory, speed, interfaces) etc. - *lightweight*

- **Security & safety dilemma**
  - Strict security is needed in normal cases
  - But how about in an emergency? - *fail safe*

- **Usability requirement**
  - Your grandma should be able to use it! - *intuitive*
Existing Approaches

- **Key pre-distribution**
  - Requires *physical contact* or *extra hardware*
  - Not easy to update keys
    
    E.g.: Resurrecting duckling [Andersen, 1999]; (wire, USB)
    Message-in-a-bottle, [SenSys’07], KALwEN (faraday cage).

- **Biometrical measurements**
  - Extract keys from shared biometric signs; plug-and-play
  - Require specialized sensing hardware
    
    E.g.: [Poon et al., IEEE Communication Magazine 2006; Venkatasubramanian et al., IEEE Transaction 2010; Venkatasubramanian et al., TOSN 2010; Xu et al., INFOCOM 2011]
Physical-layer Security Approaches

Basic idea

- Non-cryptographic, use the characteristics of wireless channel
- Advantage: against key compromise, etc.

Related work

- Secret key extraction from wireless channel
  - Vulnerable to Man-in-the-Middle (MitM) attack!
- Physical-layer authentication/proximity-based access control
  - [Cai et al., NDSS 2011; Mathur et al., MobiSys 2011; Patwari et al., MobiCom 2007; Rasmussen et al., CCS 2009; Zeng et al., Wireless Commun. 2010]
  - Need advanced hardware: not compatible
Outline

- Background on Body Area Networks (BAN)
- Main Design Challenges
- BANA: Body Area Network Authentication Exploiting Channel Characteristics
- ASK-BAN: Authenticated Secret Key Extraction for BANs
- Conclusion and Future Work
Problem Statement

Can we achieve BAN device authentication \textit{without out-of-band channels and human interaction}? (merely using wireless)

Lu Shi*, Ming Li#, Shucheng Yu*, Jiawei Yuan,*ACM WiSec, Tucson, AZ, 2012.
Goal:
- CU differentiates on-body sensors from off-body sensors
- On-body sensors authenticate CU.

Assumption
- Honest sensor nodes are on-body
- CU is on-body or near-body, relatively static to the body whether static or in motion during authentication.
Models and Assumptions (cont’d)

- **System Model**
  - Multiple COTS sensors and one CU.
  - CU is not compromised.
  - No additional hardware or out-of-band channel.

- **Attack Model**
  - One or more attackers, physically away from body.
  - Eavesdropping, message injection, changing transmission power.
  - Jamming or DoS attacks are not considered.
Exploit Unique Channel Characteristics

Observation 1:

- **RSSI variations** for on-body channels are greatly different from RSSI variations between off-body channels, under artificially introduced motions or channel disturbance.

- RSSI variations can be used as an indicator of channel stability.
Experiment Evidence

RSSI variations under two classes of scenarios:
(1) Body motion: A-D
(2) Channel disturbance: E
Theoretical Explanation

- **On-body Channel**: effect of human body is negligible for on-body devices which are very close and relative static to each other; direct path effect is the dominant factor.

- **Off-body Channel**: motions introduce Doppler shift; multi-path effect is the dominant factor.
BANA Protocol

- The metric to differentiate between on-body sensors and off-body sensors?
  - Average RSSI variations (ARV)
    \[
    ARV_i = \frac{\text{Sum}_i}{NT}, \text{ while } \text{Sum}_i = \sum |RSSI_k - RSSI_{k-1}|
    \]

- How to deal with ARVs for final decision?
  - Classification: [ accept ], [ reject ]
Calculate $ARV_1, ARV_2, ..., ARV_i, ..., ARV_{n-1}, ARV_n$ by
$ARV = \text{Sum of } |RSS_k - RSS_{k+1}|$

Classify $ARV_1, ARV_2, ..., ARV_i, ..., ARV_{n-1}, ARV_n$ into two groups.

Accept if $ARV$ belongs to small value group; reject otherwise.
Experiment Setup

Sensor deployment:
- 7 on-body: chest, arm, waist, thigh.
- 6 off-body.

Experiment locations: (WxLxH, m)
- Small room: 2.8x3.3x2.7
- Medium room: 4.5x5.5x2.7
- Corridor: 4.5x40x2.7
Experiment Testing Plans

<table>
<thead>
<tr>
<th>Test Plan</th>
<th>Location</th>
<th>Movement</th>
<th>Patient</th>
<th>Attacker Placement</th>
</tr>
</thead>
</table>
| 1         | Small room| sitting-and-rotating     | person 1  | Attacker #1,2: inside of the room.  
Attacker #3,4: next door (separated by a wooden wall)  
Attacker #5,6: more than 5 meters away |
| 2         | Small room| walking                   | person 1  | Attacker #1,2: inside of the room.  
Attacker #3,4: next door (separated by a wooden wall)  
Attacker #5,6: more than 5 meters away |
| 3         | Medium room| sitting-and-rotating     | person 3  | Attacker #1,2: inside of the room.  
Attacker #3,4: next door (separated by a wooden wall)  
Attacker #5,6: more than 5 meters away |
| 4         | Corridor  | sitting-and-rolling      | person 1  | Attacker #1: following the patient.  
Attacker #2-6: static, at different distances |
| 5         | Corridor  | sitting-and-rolling      | person 2  | Attacker #1: following the patient.  
Attacker #2-6: static, at different distances |
ARV measurements in 5 Test Plans

<table>
<thead>
<tr>
<th></th>
<th>Plan 1</th>
<th>Plan 2</th>
<th>Plan 3</th>
<th>Plan 4</th>
<th>Plan 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBS1</td>
<td>1.605</td>
<td>0.482</td>
<td>2.012</td>
<td>1.899</td>
<td>1.814</td>
</tr>
<tr>
<td>OBS2</td>
<td>2.699</td>
<td>0.932</td>
<td>1.734</td>
<td>2.286</td>
<td>4.870</td>
</tr>
<tr>
<td>OBS3</td>
<td>2.463</td>
<td>0.991</td>
<td>1.626</td>
<td>1.923</td>
<td>2.890</td>
</tr>
<tr>
<td>OBS4</td>
<td>3.104</td>
<td>1.149</td>
<td>2.142</td>
<td>2.264</td>
<td>2.104</td>
</tr>
<tr>
<td>OBS5</td>
<td>3.544</td>
<td>1.181</td>
<td>1.947</td>
<td>2.115</td>
<td>2.395</td>
</tr>
<tr>
<td>OBS6</td>
<td>2.133</td>
<td>1.010</td>
<td>1.844</td>
<td>1.910</td>
<td>1.677</td>
</tr>
<tr>
<td>OBS7</td>
<td>1.922</td>
<td>0.836</td>
<td>1.709</td>
<td>2.122</td>
<td>2.359</td>
</tr>
<tr>
<td>ATK1</td>
<td>5.667</td>
<td>6.182</td>
<td>6.319</td>
<td>4.536</td>
<td>4.447</td>
</tr>
<tr>
<td>ATK2</td>
<td>6.346</td>
<td>6.342</td>
<td>5.301</td>
<td>5.971</td>
<td>5.860</td>
</tr>
<tr>
<td>ATK3</td>
<td>5.754</td>
<td>7.003</td>
<td>6.005</td>
<td>5.097</td>
<td>4.964</td>
</tr>
<tr>
<td>ATK4</td>
<td>5.259</td>
<td>5.936</td>
<td>6.211</td>
<td>5.365</td>
<td>5.359</td>
</tr>
<tr>
<td>ATK5</td>
<td>5.835</td>
<td>6.670</td>
<td>5.255</td>
<td>5.173</td>
<td>5.778</td>
</tr>
<tr>
<td>ATK6</td>
<td>5.152</td>
<td>4.721</td>
<td>5.438</td>
<td>5.527</td>
<td>5.753</td>
</tr>
</tbody>
</table>

- ARVs of 34/35 on-body sensors are less than 4dB.
- ARVs of on-body sensors are relatively small.
- Utilize **K-means clustering** to partition ARVs into two groups.
Effectiveness

- False positive rates and false negative rates are calculated based on 15 sets of data under different settings.

<table>
<thead>
<tr>
<th></th>
<th>False Positive</th>
<th>False Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>small</td>
<td>3.7%</td>
<td>0</td>
</tr>
<tr>
<td>medium</td>
<td>2.9%</td>
<td>0</td>
</tr>
<tr>
<td>corridor</td>
<td>3.3%</td>
<td>0</td>
</tr>
<tr>
<td>sitting-and-rotating</td>
<td>2.2%</td>
<td>0</td>
</tr>
<tr>
<td>sitting-and-rolling</td>
<td>3.7%</td>
<td>0</td>
</tr>
<tr>
<td>walking</td>
<td>4.8%</td>
<td>0</td>
</tr>
<tr>
<td>person 1</td>
<td>2.0%</td>
<td>0</td>
</tr>
<tr>
<td>person 2</td>
<td>4.8%</td>
<td>0</td>
</tr>
<tr>
<td>person 3</td>
<td>2.8%</td>
<td>0</td>
</tr>
<tr>
<td>overall</td>
<td>3.3%</td>
<td>0</td>
</tr>
</tbody>
</table>
Security Against Strategic Attackers

- **Attacker strategy 1**: deploy a large number of attacker nodes to deviate classification result.
  - expensive & easily detected.
Security Against Strategic Attackers

- **Attacker strategy 2:** statistically predict the communication channel between on-body sensors and CU.
  - Predict the channel and change transmission power or refer to historical measurements
    - Channel is dynamic with short coherence time
    - Both CU and on-body sensors are more than half wavelength away from off-body attackers.

- **Beam-Forming Attacks**
  - Raise suspicion due to large size.
  - Difficult to perform in NLOS scenarios.
**Efficiency**

- **Authentication time** is up to 12 seconds.

![Sitting-and-rotating (Medium Room)](image1)

- **Computation and communication cost** is negligible for sensor nodes.

![Sitting-and-rolling (Corridor)](image2)
Summary

- Discovered a new type of channel characteristics in BAN environment.

- Proposed BANA: lightweight, commercial off-the-shelf, non-cryptographic without prior-trust, fail-safe.

- Experiments show effectiveness and efficiency of BANA.
Outline

- Background on Body Area Networks (BAN)
- Main Design Challenges
- BANA: Body Area Network Authentication Exploiting Channel Characteristics
- ASK-BAN: Authenticated Secret Key Extraction for BANs
- Conclusion and Future Work
Problem Statement

Can we achieve authenticated secret key extraction in BAN using merely wireless communication?

Lu Shi*, Jiawei Yuan*, Shucheng Yu*, Ming Li#, ACM WiSec, Budapest, Hungary, April 2013.
The Challenge: A Dilemma

- Rate is the critical issue for key generation
  - Higher key generation rate requires **dynamic** channel.

- Device authentication via BANA requires the opposite
  - Utilizes **stability** of on-body channel

- How to solve this tension?
Observation II:

- **On-Body channels** exhibit obviously different **RSSI** variations

- Channels between **Line-of-sight on-body** devices tend to be much more **stable** than devices in **Non-line-of-sight** locations (e.g. front-to-back).

- Can deploy auxiliary sensor to create both channels
Experimental Evidence

Front View  Back View

On-body Sensors

Channels between CU and S1 to S5

Channels between S4 and S1, S2, S3, S5

RSS (dBm)

Samples (per 200 ms)
Theoretical Explanation

- **Line-of-sight channels**: the direct path effect is the dominant factor between closely placed devices.
  - → **Stable fading** if relatively static.

- **Non-line-of-sight channels**: affected by the device placement, body movements, human tissue and body surface.
  - → **Unpredictable fading**.
Basic Idea

- Use stable channels for authentication
  - How to authenticate on-body devices with unstable NLOS channels?
  - Exploit multi-hop authentication and transitive trust!

- Use dynamic channels for key generation
  - How to achieve high key generation rate for LOS devices?
  - Exploit node cooperation (multi-hop relay) → modeled as a max-flow problem!

- Needs to achieve key authenticity and secrecy simultaneously
ASK-BAN Protocol

1. Pairwise Key Generation

For each node $S_i$ and CU:

Adopt Adaptive Secret Bit Generation (ASBG) to build initial shared secret key from RSS measurements.

Generate $(n + 1)^2$ pairwise keys among $n + 1$ nodes including CU.
2. Initial Authentication

CU broadcasts an initiating message:

\[ M = (x, t_0, t) \]

- \( x \): a random number
- \( t_0 \): total response time
- \( t \): time interval of each response message

All the nodes, including CU, measure channels.

\[ t_{r1} < t_{r2} < \ldots < t_{r5} \]

After

\[ x + t_{r1}/1000 \text{ sec} \]

After

\[ x + t_{r2}/1000 \text{ sec} \]

After

\[ x + t_{r3}/1000 \text{ sec} \]

After

\[ x + t_{r4}/1000 \text{ sec} \]

After

\[ x + t_{r5}/1000 \text{ sec} \]

Response message broadcasting repeats every \( t \) ms, lasts for \( t_0 \) sec.
ASK-BAN Protocol

2. Initial Authentication

For each node $S_i$ and CU:

Calculates ARV by 
$ARV = \text{Sum of } [RSS_k - RSS_{k+1}]$

Classifies ARV values into two groups.

Accepts nodes whose ARV belongs to the small value group, records as $(S_j, T)$. Otherwise, rejects and records as $(S_j, F)$.

Constructs a trust table.
3. Authenticated Secret Capacity Broadcast

For each node $S_i$ and CU:

- Broadcasts a secret capacity message:
  \[ M_{ij} = (ID_i, ID_j, T/F, C_{ij}) \]

- Computes ARVs and performs classification on ARVs. Adds valid $S_j$ and trusted neighbors of $S_j$ into Trust Group.

- Constructs a security capacity topology.
4. Deciding Maximum Entropy

For $S_i$:

Based on the capacity topology, runs the max-flow algorithm to find the path(s) to CU that can transmit maximized entropy of key information.
5. Key Aggregation Broadcast

Between $S_i$ and CU:

Each $S_j$ on the max-flow path broadcasts the XORed value of keys between it and its two neighbors respectively.

$S_i$ and CU obtain each other’s pairwise key shared with neighbor along the max-flow path, pick one as the final key between $S_i$ and CU.

Multiple max-flow paths: Concatenation of the keys from individual max-flow paths.
5. Key Aggregation Broadcast

Max-flow multi-path merging/splitting:
- No overlapped bits are used in the XORed value sent from the same node.
- The broadcast message includes the bit segment starting position of each key used by the XOR operation.

(a) 

(b)
Security Analysis

- **Node Authentication**
  - Legitimate nodes: successful authentication probability increases
  - Attacker: does not get more chances to be authenticated
  - Man-In-The-Middle attacks are prevented

- **Secrecy of the Extracted Key**
  - Attacker channels are uncorrelated to on-body channels.
  - Attackers cannot derive secret key bits generated by on-body nodes.
Experiment Setup

- Sensor deployment
  - 8 on-body: chest, arm, waist, thigh, back.
  - 1 CU.
  - 1 off-body.
- Room locations unchanged
- Subjects:
  - 2 males, 1 female.
- Body movements:
  - Sitting-and-rotating
  - Sitting-and-rolling
  - Walking
- Test plans:
  - Different combinations of sensor deployment, location, subject, and body movement.
Effectiveness: Authentication

- **False negative rate** under different on-body to off-body node ratios remains 0.
- **False positive rate** comparison

<table>
<thead>
<tr>
<th>Location</th>
<th>ASK-BAN</th>
<th>BANA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>2.38%</td>
<td>38.10%</td>
</tr>
<tr>
<td>Medium</td>
<td>2.70%</td>
<td>37.84%</td>
</tr>
<tr>
<td>Corridor</td>
<td>0.00%</td>
<td>37.14%</td>
</tr>
<tr>
<td>Sitting-and-rotating</td>
<td>0.00%</td>
<td>34.29%</td>
</tr>
<tr>
<td>Sitting-and-rolling</td>
<td>0.00%</td>
<td>37.14%</td>
</tr>
<tr>
<td>Walking</td>
<td>4.55%</td>
<td>40.91%</td>
</tr>
<tr>
<td>Subject 1</td>
<td>3.13%</td>
<td>31.25%</td>
</tr>
<tr>
<td>Subject 2</td>
<td>2.27%</td>
<td>40.91%</td>
</tr>
<tr>
<td>Subject 3</td>
<td>0.00%</td>
<td>39.47%</td>
</tr>
<tr>
<td>Overall</td>
<td>1.75%</td>
<td>37.72%</td>
</tr>
</tbody>
</table>
Efficiency: Key Generation Rate

- **Direct Generation**
- **One-hop Relay**
- **ASK-BAN**

---

**t = 6 ms, Small Room**

**t = 6 ms, Corridor**

**t = 5 ms, Small Room**
Conclusions and Future Work

- Body area network introduce big challenges in security & privacy research
- We proposed two trust initialization schemes exploiting channel characteristics that are low-cost, usable, and fail-safe

Ongoing and future work
- Authenticated key extraction.
- Against other attacks.
- Robustness against interference and jamming.
- More…
Related Publications

- Lu Shi, Ming Li, Shucheng Yu and Jiawei Yuan, "BANA: Body Area Network Authentication Exploiting Channel Characteristics", *IEEE Journal of Selected Areas on Communications (JSAC)*, Sept. 2013.
- Lu Shi, Jiawei Yuan, Shucheng Yu, and Ming Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks", *ACM WiSec*, Budapest, Hungary, April 17-19, 2013.
Thanks for your attention!

Q & A