Security for distributed wireless sensor nodes

Ingrid Verbauwhede
Department of Electrical Engineering
University of California Los Angeles
ingrid@ee.ucla.edu

Outline

- Motivation
- Security attacks
- What is different, special to sensor networks
- Links to other security problems
- Topics of research
Motivation

- security problems & cryptographic techniques to protect them.

- **Privacy** for individual sensors: *depends*
  - tank passes in a battlefield: not really needed
  - individual heart beats of patients: not much information
  - at home: sensor tells me that the jacuzzi is ready: not much information

- **Authentication** for individual sensors: *for sure*
  - don’t want the enemy to inject false alarms on tank locations
  - don’t want to adjust the insulin level of the wrong patient
  - don’t need to know that my neighbor’s jacuzzi is ready

Sensor specific attacks?

<table>
<thead>
<tr>
<th>Attack</th>
<th>solution</th>
<th>Sensor specific</th>
</tr>
</thead>
<tbody>
<tr>
<td>False messages</td>
<td>authentication</td>
<td>no</td>
</tr>
<tr>
<td>Replay messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Denial of service</td>
<td>Security checks in nodes (challenge response)</td>
<td>no</td>
</tr>
<tr>
<td>Jamming/interference</td>
<td>Spread Spectrum Radio (with non-linear codes)</td>
<td>no</td>
</tr>
<tr>
<td>Signal hiding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pattern or traffic analysis</td>
<td>Random activity, noise sources</td>
<td>no</td>
</tr>
</tbody>
</table>

Almost every attack to a sensor node has an equivalent in a regular network, or in radio communication. Main difference = energy drainage instead of performance drop.
Research approach

- Adapt security level to information content!
- Combine with distributed computing
- Assume a hierarchical structure

Hierarchy of nodes

Super node

Intermediate nodes

Leaf nodes: > 10K, 100K

Hierarchy established dynamically, depending application or circumstances
Assumptions

- Distributed network of heterogeneous nodes (different types of sensors, different levels of processing capabilities)
- Nodes establish ad hoc connections
- Assume the existence of a hierarchy of nodes, with
  - hierarchy is dynamically established
  - hierarchy might change depending on application, power budget
- The higher up in the hierarchy, the more energy is available and the higher the security level
- If an intermediate node is compromised, the tree below it will be.

Hierarchy of security

<table>
<thead>
<tr>
<th>Information content:</th>
<th>Energy availability</th>
<th>Security requirement</th>
<th>Trust Level:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>unlimited</td>
<td>highest</td>
<td>Top</td>
</tr>
<tr>
<td>Distributed</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>optimization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low processing:</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>• feature extraction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• motion detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extremely low</td>
<td>Extremely low</td>
<td>None to low</td>
<td>Assume zero, Build up</td>
</tr>
<tr>
<td>• Short messages</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Small set of possibilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Yes/no or Red/green/blue</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cryptographic techniques

Between Levels:
- Challenge response system (i.e. communication initiated by the higher level)
  - to avoid denial-of-service (energy drainage)
- Communication versus computation!

A: challenge (includes time factor, randomness)
B: response
C: verify response

- Response could contain requested information since possible answers are from limited set.
- Requires one-way hash function or encryption in leaf nodes.
- Requires two radio transmissions per leaf node!

At intermediate levels:
- Set up "conference key",
- Combine with distributed computations & optimizations

\[
\min( E_C + E_R + E_S )
\]

Example: Burmester-Desmedt conference key protocol:
- exponentiation \( z_i \)
- broadcast \( z_i \)
- exponentiation, \( X_i = f( z_{i-1}, z_{i+1} ) \)
- broadcast \( X_i \)
- exponentiation, compute \( K = f(z_i, X_i) \)
Inference Control in database

Sensor data (similar to a “mystery box”)
- It is yellow
- It does not make noise
- It turns its head towards the sun

- Individual sensors: not much information content
- Data fusion: information extraction
- If the good guys can, so can the “bad” guys.

Inference control in data bases (1980’s):
- allow statistical data extraction
- protect privacy of individuals
  e.g. medical or employee data bases
- add noise or restrict access

Conclusions:

- Individual tasks similar/related to existing problems
- Combination of these tasks unique to sensor networks
- Current activities:
  - Power security trade-off
  - Measure of security for energy budget
  - co-processors for low power encryption
- Cryptographic techniques with minimal communication overhead