GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications

Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen, University of Waterloo
Xiaodong Lin, University of Ontario Institute of Technology
Key points

• High level overview
• Machine-to-Machine challenges
  • Energy Efficiency (Green)
  • Reliability
  • Security
• Approaches to GRS requirements
• Conclusions
Machine-to-Machine Communications

“a large number of intelligent machines sharing information and making collaborative decisions without direct human intervention”

<table>
<thead>
<tr>
<th>Typical applications</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-healthcare</td>
<td>Remote patient monitoring for better healthcare</td>
</tr>
<tr>
<td>Smart home</td>
<td>Real-time remote security and surveillance</td>
</tr>
<tr>
<td>Environmental monitoring</td>
<td>Effective monitoring at low cost</td>
</tr>
<tr>
<td>Industrial automation</td>
<td>Remote equipment management for cost savings</td>
</tr>
</tbody>
</table>

Table 1. Typical applications and benefits of M2M communications.
M2M Evolution

- Started as one-way propagation of data
- More nodes are added
- Group communications
- Logic
- Environment-aware nodes
- Increased potential
- Increased complexity
Future and challenges

“the flourishing of M2M communications still hinges on fully understanding and managing the existing challenges”

• Deployment architecture
• Software architecture
• Energy efficiency (green)
• Reliability
• Security
M2M architecture and requirements

Figure 2. M2M communications: a) architecture; b) GRS requirements.
M2M Architecture

- M2M domain
  - Smart devices/Gateways
- Network domain
  - Wired/wireless communication channels
- Application domain
  - Back-end server
• Challenging issue
• Vital to the establishment of M2M
• Communication dominates energy consumption
  • Transmission power
  • Communication protocols
  • Activity scheduling
- Time slot based
- Round based
- Random timeout
- Autonomous decisions
- Local communication
- Few control messages

- Energy efficient

Figure 4. An example that node $N_0$ may switch to sleep mode because its sensing range is fully covered by the connected neighbors $N_1$, $N_2$, $N_3$, and $N_4$. 
• Conflicting with energy efficiency
• “How to balance greenness and reliability in M2M communications needs further exploration.”
• Multiple points of interest
  • Sensing and processing
  • Transmission
  • Back-end server
Sensing and processing

- Majority vote is desirable
- Local Vote Decision Fusion (LVDF)
- Corrected decision strategy
- Uses additional information and introduces temporal redundancy
Transmission

• For efficiency, data can be aggregated
• This may result in unreliable transmission
• Spatial redundancy is employed

• Redundant transmissions
• Higher reliability
Back-end server

- Single server for energy efficiency
- Multiple servers to ensure QoS
- Dynamically activated based on load

Figure 5. The deployment of primary and second servers to achieve reliability.
Attacks can be classified as:

- **Passive**
  - Harder to detect
  - Cause less damage

- **Active**
  - External
  - **Internal**
Security Requirements:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation
- Access control
- Availability
- Privacy
• External attacks can be prevented by cryptographic techniques
• Internal attacks require more sophisticated security mechanisms
• Stages of a node compromise attack
  • Capture and compromise
  • Re-deployment
  • Internal attack
Early detecting node compromise

- First line of defense
- Nodes form couples to monitor each-other
- Detects compromise during the first stages

Figure 6. Early detecting node compromise with couple.
BW efficient cooperative authentication

- Second line of defense
- False data filtering
- Authenticates the sensory data cooperatively
- Prevents contamination from compromised nodes
BW efficient cooperative authentication

Figure 7. Bandwidth-efficient cooperative authentication to filter false data.
BW efficient cooperative authentication

Figure 8. Simulation results (EFP, FR) of BECAN for the neighboring parameter $k = 4$, and the transmission radius $TR = 15, 20m$. 
Conclusions

- Studied the issues to achieve energy efficiency
- Offered several approaches to address the reliability and security issues
- Did they?
- Further efforts are needed to identify the GRS issues in specific contexts
Criticism

• Too focused on just a few of the issues raised
• No metrics to support why the proposed activity scheduling scheme is better than others
• No explanation of node compromise
• The simulation doesn’t prove anything
Thank you