Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems

Presenter: Rob Miller

Ishtiaq Rouf, Hossen Mustafa, Miao Xu, Wenyuan Xu,
Dept. of CSE, University of South Carolina

Rob Miller, Applied Communication Sciences

Marco Gruteser, WINLAB, Rutgers University
Electric Meters

- Smart meters
  - Demand-response
  - Time of day use
- Automatic meter reading (AMR)
  - Gas, water, electricity
  - 47 million installed (2010)
AMR — Overview

• Communication protocols
  – Telephone line
  – Power line
  – Wireless communication

• Transmission methods
  – Electric meters: Bubble-up once every 30s

• Our focus
  – Wireless communication with drive-by trucks

• Meter IDs are linked with accounts
Misuse 1: Privacy

Eavesdropper monitors consumption

Empty House? Time to visit.
Misuse 2: Spoofing

Selfish

“I want to pay less…”

Bad neighbor

“I don’t like my neighbor…”

Sending spoofed packets
AMR — To Be Discovered

• **Reverse engineer** the communication protocol?
  – Messages encrypted? Authenticated?

• **How easy to spoof** AMR communication?
  – Drive-by trucks reject suspicious packets?

• **Privacy risks**?
  – How much information can be inferred?

• **How to protect** AMR communication?
Q1: Reverse-Engineering Wireless Communication

- Proprietary protocols — Patent
  - Manchester encoding
  - Multiple Channels
  - Message formats

- To be discovered
  - Modulation schemes?
  - Baud rate, channel information?
  - Message encrypted?

- Equipment
  - An electric meter
  - A gas meter
  - Universal Software Radio Peripheral (USRP)
  - Sentry 900
Q1: Reverse-Engineering Walk-Through

An AMR meter transmits at 902~928 Mhz

Determine Modulation
OOK

An AMR meter transmits at 902~928 Mhz

Scan at 902~928 Mhz for activity

Verify Message Format

Determine Baud rate 16kBd

Encoding Scheme Manchester

Determine Modulation OOK
Q1: Reverse-Engineering Results

• Observations
  – Reverse engineering possible
  – No encryption
  – Meter ID transmitted in plaintext
  – Simple frequency hopping → pre-determined channels

![Signal strength vs Channel diagram]

<table>
<thead>
<tr>
<th>Preamble</th>
<th>ID</th>
<th>Spare</th>
<th>Type</th>
<th>Data</th>
<th>Tamper</th>
<th>ID</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 bits</td>
<td>2 bits</td>
<td>3 bits</td>
<td>4 bits</td>
<td>22 bits</td>
<td>4 bits</td>
<td>24 bits</td>
<td>16 bits</td>
</tr>
</tbody>
</table>
Q2: Packet Spoofing

• How likely to spoof AMR communication?
  – Security mechanisms in receiver?
  – Override real meter transmission?

• Spoofing System
  – Developed a packet generator
    • Include a proper checksum
    • Contain arbitrary ID, usage data, etc.

• Tested on a few instruments:
  – Sentry 900 validates packet structure
  – Drive-by truck validates....

Select meter ID, tamper field and reading
Modulate (ASK) Encode (Manchester) Transmit at 916Mhz
Q2: Spoofing Validation

AMR Meter

Demonstration of Packet Spoofing Attack
Q3: Privacy Risks via Eavesdropping

- Eavesdropping System
  - Gas meters and electric meters
  - Developed a live eavesdropper

- How likely to eavesdrop?
  - How far away?
  - How many observable meters?
  - How much information?
Q2: How to link a meter ID with a house?
Eavesdropping range can be significantly boosted by a low-noise amplifier
Privacy Risks from Traditional Methods

- Privacy Risks from
  - IR flash
  - LCD display
- Which one is the worst?

Infrared LED, flash once per watt-hour usage

IR flash detection circuit

ERT (Encoder, Receiver, Transmitter) module

Digitized display

Dot on-off display
Privacy Breach Comparison

Time of day use

<table>
<thead>
<tr>
<th>Power (kW)</th>
<th>12pm</th>
<th>3pm</th>
<th>6pm</th>
<th>5pm</th>
<th>12am</th>
<th>3am</th>
<th>6am</th>
<th>5am</th>
<th>12pm</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR/Image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF (120pph)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF (25pph)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF (6pph)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# of step changes

- IR/Image: 50
- RF (120pph): 17
- RF (25pph): 15
- RF (6pph): 11

pph ➔ packets per hour
Neighborhood Watch Via Eavesdropping

- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

Days of a week

KW

3am 6am 9am 12pm 3pm 6pm 9pm 12am
Defense - Legacy meters

- **Cryptographic mechanisms**
  - Transmit on-demand
  - Reinstall new meter or upgrade firmware?

- **Spoofing**
  - Radio Fingerprint
  - Anomaly detection at data center
  - In-person visual inspect

- **Eavesdropping** → Jammer Add-on
  - A jamming signal to mask data packets
  - Work with drive-by
  - Narrowband jammer → 1 AMR meter
  - Wideband jammer → multiple AMR meters
Conclusions

- Privacy risks
  - AMR messages are transmitted in plaintext → Anyone can eavesdrop
  - Able to eavesdrop on 500 electric meters using USRP with cheap antennas
  - Eavesdropping range of about 300 meters

- Spoofing risks
  - Spoofing attacks are possible

- Raise awareness before more serious security and privacy vulnerabilities emerge

- Jamming-based protection

Thank you & Questions?

- University of South Carolina
  - Ishtiaq Rouf (Itron)
  - Hossen Mustafa
  - Miao Xu
  - Wenyuan Xu (wyxu@cse.sc.edu)

- Applied Communication Sciences
  - Rob Miller (rmiller@appcomsci.com)

- Rutgers University
  - Marco Gruteser (gruteser@winlab.rutgers.edu)