Security in Distributed Wireless Sensor Networks

Hon. Prof. Dr. Peter Langendörfer & Prof. Dr. Ing. Rolf Kraemer
Outline

• Wireless Sensor Networks and Security

• Security Engineering

• Secure Sensor Node Architecture

• Conclusion
Wireless Sensor Networks

Multihop Network

Clustered Network

WPAN/WSN cluster

mesh router

mesh client

end node

BAN or PAN Network
Security Fundamentals

• **Confidentiality**
  
  Information should only be revealed to authorized entities; any other entity should not be able to discover the information from eavesdropping or from read in memory.

• **Data Integrity**
  
  The receiver of information wants to be sure that data is not modified in transit, either intentionally or by accident.

• **Accountability**
  
  The entity requesting a service, triggering an action, or sending a packet must be uniquely identifiable.

• **Availability**
  
  Legitimate entities should be able to access a certain service/information and to enjoy proper operation.

• **Controlled Access**
  
  A service or information access should only be granted to authorized entities.
Security features

• Authentication (data and source authentication (data integrity))/non repudiation
  Does not help against insider attacks
  Intrusion detection (identification of compromised nodes)

• Secrecy
  Use of appropriate cipher means

• Service Integrity
  Plausibility check of sensor readings

• Availability
  Denial of service may cause serious harm
  Graceful degradation needed
Basic Threads

• Eavesdropping
  Listening to a communication to get unauthorized information
• Masquerading
  Pretending to have another entity identifier
• Authorization Violation
  Using services without being allowed to use them
• Provoking loss or modification of information
• Forgery
  Creating new or false information
• Repudiation
  Denial that one participated in or was the origin of communication
• Sabotage
Classification of Threats

- **Outsider attacks**
  - Eavesdropping
  - Jamming
  - Alter packets
  - Destroying nodes

- **Insider attacks (Compromised sensor nodes; laptops)**
  - Authorized participant
  - Steal secrets or disrupt normal functioning

- **Base station/cluster head as point of trust?**
  - Powerful device;
  - Tamperproof HW;
  - Scalability may become a serious problem
  - Battery power of nodes around the base station
Security Threat Analysis for sensor nodes

Dolev-Yao (known) :

Extended Dolev-Yao:
(WSN relevant)

Paradox
State of the art:

Options for security improvement:
	Tamper-resistant nodes ( ⇒ too expensive)
	“Probabilistic” security ( ⇒ attacker receives only limited gain)

Threat-Model with up to 5 years delay

Dolev-Yao
Extended Dolev-Yao

intercept
overhear
physically read out
Physical Attacks & Security

- **Device classes** (FIPS 140-2 level1-level4)
  - unprotected (L1 u. L2)
  - partly protected (L3)
  - tamper resistant (L4)

- **Attacker**
  - clever outsider (<5000 EUR)
    - “insufficient knowledge of the system”
  - knowledgeable insider (>5000 EUR)
    - “substantial technical education/experience”
  - funded organisation (several 100 KEUR)
    - “teams of specialists”
Real Life Connectivity

- Figures show WSN deployed on a flat parking lot

- Expected: simple, circular shape of “region of communication” – not realistic

- Instead:
  
  Correlation between distance and loss rate is weak; iso-loss-lines are not circular but irregular
  
  Asymmetric links are relatively frequent (up to 15%)
  
  Significant short-term PER variations even for stationary nodes
Three regions of communication

- **Effective region:** PER consistently < 10%

- **Transitional region:** anything in between, with large variation for nodes at same distance

- **Poor region:** PER well beyond 90%
Open issues: Detection of compromised nodes

- Secure routing protocols
- Secure & efficient time synchronisation
- Secure localization
- Efficient cipher means
- Secure misbehaviour detection
- Means for non security experts to design secure WSNs
Security Engineering
Security Engineering in WSN

- Limitations:
  - Processing power: 8 or 16 bit µC
  - Memory: 16 to 256 kByte
  - Energy resources: typical small batteries 1000-5000 mAh
    - energy harvesting
  - Active Time: 1-15 years
  - Cost: 1-100 $
  - Security: open to security critical
How to distribute secret keys in networks

- Secure channel
  Pre-deployment
- Third party
  security authority
  Transitivity of trust (If node A and B trust C, C can generate key for A and B)
- Public key based key establishment
  Computation of session key based on a unique public/private key pair
- Key agreement based on one way functions
  Diffie-Hellman
Diffie-Hellman Key Establishment

• If we have a one-way-function:
  \[ y = a \cdot x \text{, it is infeasible to compute } a \text{ for given } x \text{ and } y \]
  \[ a \cdot b \cdot x = b \cdot a \cdot x \text{ (commutative)} \]

Alice
random a and x
compute \( a' = a \cdot x \)
compute shared key
\( k = a \cdot b' = a \cdot b \cdot x \)

Bob
generate random b
compute \( b' = b \cdot x \)
compute shared key
\( k = b \cdot a' = a \cdot b \cdot x \)

• Advantages:
  Simple protocol
  Key agreement of peers without prior knowledge

• Problems:
  One-way-function (Elliptic curve cryptography, discrete logarithm) is computationally expensive
  Authentication between Alice and Bob is not supported
Authentication: How to prove that Alice is Alice

• By Third Party
  Security Authority
  Transitivity of trust
• By Secret keys
  Alice and Bob share a secret key
• By Inverted hash key chains (e.g. TESLA)
  If $H(x)$ is a not-invertible hash function
  Authentication with tuple $(x_n, H(x_{n+1}))$; trust anchor $H(X_n)$
  $x_n$ authenticates the one who sent $H(x_n)$ earlier
  Problem:
    - lot of storage (for each communication previous hash keys)
    - initial trust (how can I authenticate the first message)
• Signed certificates
  → needs public key cryptography
  → Offline certification
  Problem:
    computational expensive
Combining Security & Embedded Systems Design

Application Requirements

Sensor node description

ConfigKIT
1. Req. vs. features of modules
2. Interoperability of modules
3. Security of combination

Application
- Sec. robust data storage
- Resilient data aggregation alg_1
- CDA_alg2
- Sec. rout_1
- Secure local
- ECC
- AES
- OS

Sensor node HW

Tailor made security architecture
Setup of Hardware Repository

- Structural view/selection of sub-components
- Parametrisation
- Re-usable XML, part of hardware repository
Setup of Software Repository

- structural view
- dependency graph
- selection of sub-components

Setting of parameters, dependencies, requirements

Re-usable XML, part of software repository
configKIT-approach

User Interface, Application designer

Hardware selection

Application description

Module Selection

- Resolve Dependencies
- Semantic Evaluation
- Estimation of
  - Code size
  - Security properties
  - Energy assessment

List of potential solutions satisfying requirements

Blueprint for system integration

Module Designer Interface

Update repository

Hardware Repository (XML)

Software Repository (XML)
configKIT for Application Designers

- Selection of hardware
- Selection of required functions
- Definition of security properties

- Each change of inputs immediately updates the result → Fast and easy refinement process

- Proposed software configuration
  - Including prediction of footprint
Secure Sensor Node Architecture
Secure Sensor Node

- Secure Sensor Node Diagram

- I-Cache (16 kB)
- CardBus (Master)
- CardBus (16 kB)
- MIPS Processor Core
- EJTAG (Debug)
- Bridge (Master)
- AMBA AHB Bus
- Data I/O Control (Master)
- Packet Filter / Checksum
- Memory Controller (AHB Slave)
- UART
- GPIO
- D-SPRAM (8 kB)
- Memory Controller (AHB Slave)
- EPP
- UART
- Data I/O
- Internal SRAM (32 kB)
- AES / MD5
- Internal SRAM (32 kB)
- ECC
- Check Sum
- Registers & Control

IHP Im Technologiepark 25 15236 Frankfurt (Oder) Germany

© 2008 - All rights reserved
ECC Processor B233: Optimized Version

Area consumption: optimized vs. original ECC Processor Version

<table>
<thead>
<tr>
<th>Partial Multiplier</th>
<th>Length of Operand [bits]</th>
<th>Poly. Mult. Area [mm²]</th>
<th>Poly. Mult. area [mm²]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Optimized</td>
<td>Original Version</td>
</tr>
<tr>
<td>2 segments</td>
<td>128</td>
<td>1.17</td>
<td>2.18</td>
</tr>
<tr>
<td>4 segments</td>
<td>64</td>
<td>0.62</td>
<td>1.51</td>
</tr>
<tr>
<td>8 segments</td>
<td>32</td>
<td>0.44</td>
<td>1.67</td>
</tr>
</tbody>
</table>

Design:
- Modular Architecture
- Reduction done on partial results
- Regular Structure
Competitive Position: ECC

<table>
<thead>
<tr>
<th>Company</th>
<th>Size KGates</th>
<th>Energy mJ</th>
<th>Time/Op ms</th>
<th>Technology used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliptic Semi: B-233</td>
<td>71</td>
<td>0.14</td>
<td>6.68</td>
<td>0.13μm</td>
</tr>
<tr>
<td>IHP B-233</td>
<td>72-42</td>
<td>0.02-0.04</td>
<td>0.08-0.35</td>
<td>0.25μm</td>
</tr>
<tr>
<td>IBM B-163+GF(p)</td>
<td>117</td>
<td>-</td>
<td>0.19</td>
<td>0.13μm</td>
</tr>
<tr>
<td>IHP B-163</td>
<td>47</td>
<td>0.01</td>
<td>0.06</td>
<td>0.25μm</td>
</tr>
</tbody>
</table>

Advantages of IHP:
- Minimal area consumption
- Iterative Karatsuba approach (patent filed)
- Flexible ECC Designs (patent filed)
AES

1. **Add key operation**: the incoming/outgoing data is “XORed” with the current round key.

2. **SBOX**: The S-Box maps an 8-bit-input into an 8-bit-output. (result depends on the direction)

3. **Shift Row**: The shift row operation is performing a cyclic shift within a single row.

4. **Mix Column**: In the mix column operation each column is multiplied with a given polynomial.
### Competitive Position: AES

<table>
<thead>
<tr>
<th>Company</th>
<th>Size Gates</th>
<th>Clock cycles per 128 Bit</th>
<th>Clock frequency</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elliptic Semi: AES</td>
<td>8.000</td>
<td>379</td>
<td>100 MHz</td>
<td>33.7 Mbit/s</td>
</tr>
<tr>
<td></td>
<td>+1.400 bit Memory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IHP AES</td>
<td>8.450</td>
<td>70</td>
<td>66 MHz</td>
<td>108 MBit/s</td>
</tr>
<tr>
<td>IAIK Graz</td>
<td>8.930</td>
<td>64</td>
<td>64 MHz</td>
<td>128 MBit/s</td>
</tr>
</tbody>
</table>

**Advantages of IHP:**
- Integration with ECC
- Integration with protocols such as TCP
- Results equivalent to those of the Inventor of AES (Rijmen TU Graz)
Conclusions
Conclusions

• Security in distributed systems is still a hot issue to solve
• Several approaches have been followed and have successfully been applied to several problem areas
• Distributed wireless sensor-networks are a special class of distributed systems that do not allow rigorous means to achieve security
• We have used a combined HW/SW approach to be able to make use of high grade encryption mechanisms like AES or ECC
• We have developed a security design environment that allows to engineer security in sensor-networks as required and achievable
• The results have been demonstrated and have been patented
TANDEM: Power Switches

Power Switch

Power Mgmt.

Power Supply

µC

IPMS430

Memory

Hardware-Accelerator e.g. ECC

I/O

Bass Band

Analog Frontend

µC