APPLICATION-DRIVEN SECURITY IN WIRELESS SENSOR NETWORKS
(SEGURIDAD ORIENTADA A APLICACIONES EN REDES DE SENSORES)

By
Rodrigo Román Castro

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR IN COMPUTER SCIENCE AT UNIVERSITY OF MALAGA

Advisor:
F. Javier López Muñoz
Profesor Titular, Universidad de Malaga
Contents

1. PRELIMINARIES - SENSOR NETWORKS
2. SECURITY PRIMITIVES & KEY MANAGEMENT SERVICES
3. SELF-AWARENESS SERVICES
4. APPLICABILITY OF SECURITY SERVICES
5. CONCLUSIONS
The need to “sense”

- Environment → full of physical events
  - We (living beings) need to perceive the physical world in order to survive
- A computer system should be able to perceive those events that are relevant to its functionality
  - Independent “Sensory System” needed
  - “Feel” the physical world = Off-the-shelf component
- Wireless Sensor Networks (WSN)
Wireless Sensor Networks

- Sensor Networks = Sensor Nodes + Base Station
  - Base Station: Interface Network ↔ Users

- Features
  - Specificity
  - Autonomy
  - Self-Configurability
  - Lifetime
  - Deployment Location
  - Mobility
Wireless Sensor Networks Applications

- **Types of Applications**
  - **“Space”**. Monitors the physical features of a certain environment.
    - Environmental and habitat monitoring, precision agriculture, indoor climate control, surveillance, treaty verification, intelligent alarms...
  - **“Things”**. Controls the status of a physical entity.
    - Structural monitoring, ecophysiology, condition-based equipment maintenance, medical diagnostics, urban terrain mapping...
  - **“Interactions”**. Monitors the interactions of things (both inanimate and animate) with each other and the encompassing space.
    - Wildlife habitats, disaster management, critical (information) infrastructure systems, emergency response, asset tracking, healthcare, manufacturing process flow...
  - **“Internet of Things”**. Objects and locations in the real world (e.g. restaurants, roads) linked to information on the web.
Wireless Sensor Networks

Security

- Sensor networks are specially vulnerable against external and internal attacks due to their peculiar characteristics

- Threats:
  - Attacks to the information flow
    - Eavesdropping, replay, injection / modification
  - Denial of Service
    - Node collaboration, jamming attack, exhaustion of power
  - Node compromise
  - Impersonation attack
    - Sybil (multiple identities), node replication (duplication)
  - Protocol-specific attacks
    - Selective forwarding, wormhole attack, sinkhole attack, spoofed routing, acknowledgement spoofing
Major Goals of the Dissertation (1)

- Sensor networks security is an important research field
  - More than 2,000 scholarly papers (probably much more)
  - Security-specific workshops (ESAS, WSNS, WISE, SASN,...), books,...

- Missing link: Sensor networks ↔ Real World
  - Sensor networks are not general purpose systems → specific functionality
  - Application: Impact on Structure, Architecture, and Protocols

- **Goal**: Consider the *influence of the applications* and their context in the protection of sensor networks and the development of the security mechanisms
  - The properties and requirements of the real world will influence over the security features that are needed in an specific sensor network deployment
Major Goals of the Dissertation (2)

- **Goal**: Specification of “complete set” of security mechanisms
  - A set of *application-aware* security mechanisms that either prevent the existence of attacks or minimize their adverse effects
  - Consider these mechanisms as part of a transversal layer

- “Complete Set”:
  - Suitability of security primitives and key management systems
  - Develop self-awareness services for allowing self-configurability
  - Integration / Interaction with the mechanisms
2. Security Primitives and Key Management Services

- **Goals:**
  - Provide an analysis of the *suitability* of the HW and SW implementations of the security primitives in constrained devices
  - Analyze whether the actual state of the art in **symmetric key-based key management systems (KMS)** can satisfy the **requirements of sensor networks applications**
  - Provide **support for public key operations** in sensor networks
Security Primitives

- Foundation of almost all secure protocols and mechanisms: Cryptographic Primitives
- Symmetric Key Cryptography (SKC)
  - Primarily protects the confidentiality of the information flow
    - Stream Ciphers: RC4
    - Block Ciphers: Skipjack, RC5, AES, Twofish
- Public Key Cryptography (PKC)
  - Useful for secure broadcasting and authentication purposes
    - Recommended: Elliptic Curve Cryptography (ECC)
    - Other: Rabin (Signature verification), NTRU, MQ-Schemes
- Hash functions
  - Creation of “digital fingerprints” - integrity
    - SHA-1
Security Primitives
Types of Sensor Nodes

<table>
<thead>
<tr>
<th>WEAK (Class I)</th>
<th>NORMAL (Class II)</th>
<th>HEAVY-DUTY (Class III)</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 4 Mhz (8 bit)</td>
<td>- 4<del>8 Mhz (8</del>16 bit)</td>
<td>- 13~180 Mhz (32 bit)</td>
</tr>
<tr>
<td>- 1 kB RAM</td>
<td>- 4~10 kB RAM</td>
<td>- 256~512 kB RAM</td>
</tr>
<tr>
<td>- 16kB ROM</td>
<td>- 48~128 kB ROM</td>
<td>- 4~32 MB ROM</td>
</tr>
</tbody>
</table>
Security Primitives
Suitability of SW Implementations

- **Conclusion:** As of 2008, sensor nodes can implement cryptographic primitives using SW implementations

<table>
<thead>
<tr>
<th></th>
<th>Class I</th>
<th>Class II</th>
<th>Class III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric Key Cryptography</td>
<td>Stream <em>(Rec)</em></td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Asymmetric Key Cryptography</td>
<td>None</td>
<td>Limited</td>
<td>All</td>
</tr>
<tr>
<td>Hash Functions</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

- **Recommendations**
  - Study the inclusion of HW cryptographic modules in Class I and Class II nodes
  - Design and develop cryptographic primitives suitable for constrained environments
    - ECRYPT Stream Cipher Project.
      - Salsa20: 1514 bytes ROM, 292 cycles/byte (ATMega8)
    - NIST Cryptographic Hash Algorithm Competition
Security Primitives
Applicability of HW Designs

**Conclusion**: The execution time of the primitives can be greatly improved using HW modules

<table>
<thead>
<tr>
<th>ECC</th>
<th>Point Multiplication</th>
<th>$\mu$Processor speed</th>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW Impl. (Seo)</td>
<td>0.99 sec</td>
<td>8 Mhz</td>
<td>GF($2^{163}$)</td>
</tr>
<tr>
<td>HW Impl. (Batina)</td>
<td>0.115 sec</td>
<td>500 kHz</td>
<td>GF($2^{131}$)</td>
</tr>
</tbody>
</table>

**Recommendations**:  
- Design interfaces between sensor nodes and cryptographic modules  
- Improve the strength of the HW implementations  
- Take advantage of existing HW support (IEEE 802.15.4, MMX)
Key Management Systems

- A sensor network needs of a Key Management System (KMS)
  - Security primitives and mechanisms require the existence of security credentials (symmetric/asymmetric keys)
  - Such credentials must be distributed securely and efficiently
- Every application and its associated context requires certain properties that a KMS should fulfil
- Contribution: Develop a methodology for selecting a KMS protocol based on the needs of the network application
  1. Help the network designer to find the KMS protocols that are more suitable for the needs of his/her application
  2. Check whether the current state of the art in KMS can offer a viable solution to existing applications
  3. Determine which are the open issues that have to be taken into account in future research
Methodology
Protocol Taxonomy

- First step: Classify and analyze the existing KMS frameworks
  - Contribution: Every framework do provide only certain properties
Methodology
Properties of KMS Protocols

- **Second step:** Relate properties with application requirements
  - **Contribution:** “Missing link” between requirements and properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory footprint ([Mem])</td>
<td>ROM and RAM used for the protocol</td>
</tr>
<tr>
<td>Communication overhead ([Comm])</td>
<td>Number of messages exchanged between peers</td>
</tr>
<tr>
<td>Processing speed ([Sp])</td>
<td>Computational cost of the protocol</td>
</tr>
<tr>
<td>Network bootstrapping ([Sec])</td>
<td>Confidentiality of the bootstrap process</td>
</tr>
<tr>
<td>Network resilience ([Res])</td>
<td>Resistance against stolen credentials</td>
</tr>
</tbody>
</table>

**Connectivity**

<table>
<thead>
<tr>
<th>Connectivity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global ((GConn))</td>
<td>Existence of a “key path” between any node</td>
</tr>
<tr>
<td>Local ((LConn))</td>
<td>Existence of a shared secret between neighbour nodes</td>
</tr>
<tr>
<td>Node ((NConn))</td>
<td>Existence of a shared secret between any nodes</td>
</tr>
<tr>
<td>Scalability ([Sca])</td>
<td>Support for big networks</td>
</tr>
<tr>
<td>Extensibility ([Ext])</td>
<td>Capability of adding new nodes</td>
</tr>
<tr>
<td>Energy ([En])</td>
<td>Optimization of the energy usage</td>
</tr>
</tbody>
</table>
Methodology
Catalogue

- **Third step:** Develop a catalogue that classifies the KMS protocols according to their properties
  - **Contribution:** Choose a certain KMS according to the required properties

<table>
<thead>
<tr>
<th>KMS Protocols</th>
<th>Ref.</th>
<th>Comm</th>
<th>GConn</th>
<th>LConn</th>
<th>NConn</th>
<th>En</th>
<th>Ext</th>
<th>Mem</th>
<th>Res</th>
<th>Sca</th>
<th>Sec</th>
<th>Sp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Infection</td>
<td>[And2004]</td>
<td>(x)</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Hybrid Designs – Generalized Quadrangle</td>
<td>[Cam2007]</td>
<td>(-)</td>
<td>(-)</td>
<td>(-)</td>
<td>x</td>
<td>(x)</td>
<td>✓</td>
<td>(-)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Probabilistic Key Predistribution</td>
<td>[Esc2002]</td>
<td>(x)</td>
<td>(x)</td>
<td>(x)</td>
<td>(x)</td>
<td>(-)</td>
<td>(x)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blom Key Predistribution</td>
<td>[Du2005]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>(-)</td>
<td>(-)</td>
<td>(-)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple Space Key Predistribution</td>
<td>[Du2005]</td>
<td>(x)</td>
<td>(x)</td>
<td>(x)</td>
<td>(x)</td>
<td>x</td>
<td>(-)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polynomial Based Key Predistribution</td>
<td>[Liu2005a]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>(-)</td>
<td>(-)</td>
<td>(-)</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>Dynamic Cluster</td>
<td>[Hua2006]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>(x)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Panja</td>
<td>[Pan2006]</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Cryptography-based KMS</td>
<td>[Liu2007]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Methodology Goals
Solutions offered by the state of the art

- Analyze which are the Key Management Systems that are more appropriate for existing applications
  - Group applications according to the mobility of the nodes and the network size

<table>
<thead>
<tr>
<th>Scenario Type</th>
<th>Examples</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-hop networks</td>
<td>Industrial machinery</td>
<td>LConn</td>
</tr>
<tr>
<td>Simple net.</td>
<td>Office monitoring</td>
<td>GConn, LConn</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>Sca, GConn, LConn</td>
</tr>
<tr>
<td></td>
<td>Large</td>
<td>Sca, GConn, LConn, NConn</td>
</tr>
<tr>
<td>w. Mobile B.S.</td>
<td>Small</td>
<td>GConn, LConn</td>
</tr>
<tr>
<td>w. Mobile Nodes</td>
<td>Small</td>
<td>NConn, GConn, LConn, Comm</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>NConn, Sca, GConn, Comm, LConn</td>
</tr>
<tr>
<td>Short-lifetime net.</td>
<td>Small</td>
<td>LConn, Comm, En, Ext</td>
</tr>
</tbody>
</table>
Methodology Goals
Solutions offered by the state of the art

- **Contribution**: Infer which protocols and frameworks could be used to protect the scenarios
  - Simple networks (small), short-life networks: Simple mathematical schemes
  - Simple networks (medium or large): Cluster-based protocols or “Key Pool”-based protocols
  - With mobile B.S.: Same as simple networks
  - With mobile nodes:
    - Small: Mathematical schemes
    - Medium: PKC-based protocols
Methodology Goals

Open issues

- **Contribution**: There exist scenarios without optimal solutions
  - Networks with mobile nodes that move at a high speed
  - Extensible networks with almost no communication overhead
  - Static networks where global connectivity is extremely important (i.e. no nodes should be disconnected from the network)

- **Contribution**: Consider certain properties in the development of new KMS protocols
  - Resilience
  - Extensibility
“Traditional” Asymmetric Cryptography

- Traditional asymmetric cryptography is possible in sensor nodes
  - Key Distribution
    - √: Security, Scalability, Connectivity, Resilience, Extensibility, Comm. Overhead
    - X: Speed, Memory
  - Signing and verifying signatures - Authenticated broadcast
  - PKC Encryption / Decryption

- Support for PKC in sensor networks:
  - Public Key Infrastructure
    - Creation and maintenance of certificates
  - Certificates
    - “This Public Key belongs to that ID”
**“Traditional” Asymmetric Cryptography**

Public Key Infrastructure (PKI)

- **Contribution**: Adapt PKIX Model to sensor networks
  - Base station - Configures all nodes, trustworthy
    - Certification Authority (CA). Generates the Digital Certificates
    - Registration Authority (RA). Initial authentication of the nodes
  - Sensor node - Decentralized devices
    - Certificate Repository. Stores certificates

- **Contribution**: Simplified Certificate Format
  - Adapted from X509v3
  - Fields
    - Validity Period: Network Deployment
    - Subject Name: ID of the sensor node
    - Subject PK Information: Public key of the sensor node
    - Certificate Signature: Signature of the CA (Base station)
Key-escrow systems
Identity-based Cryptography

- Other untraditional asymmetric cryptography primitives?
  - No need to use certificates to proof the authenticity of a public key
    - Remind: Certificate = ID + Public key + Signature CA

- Key-escrow systems: A trusted party computes the users’ secret keys
  - Identity-based cryptography: The ID is the public key
  - Self-certified cryptography: Public keys are authenticated by performing the operation (e.g. signature verification)

- These untraditional primitives may be useful in sensor networks
  - Communication Overhead (transmit information is expensive)
  - Energy Savings
Key-escrow systems
Underwater Sensor Networks

- Key-escrowed systems are useful in Underwater Sensor Networks (UWSN)
  - Sensor networks deployed under the sea
  - Use of acoustic modems
    - Slow, Energy consuming, Unreliable

<table>
<thead>
<tr>
<th></th>
<th>Mica2</th>
<th>MICAZ</th>
<th>UWM2000</th>
<th>UWM4000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working range</td>
<td>150 m</td>
<td>100 m</td>
<td>1500 m</td>
<td>4000 m</td>
</tr>
<tr>
<td>Throughput</td>
<td>19.2 kbit/s</td>
<td>250 kbit/s</td>
<td>9600 bit/s</td>
<td>4800 bit/s</td>
</tr>
<tr>
<td>Tx. consumption</td>
<td>81 mW</td>
<td>52.2 mW</td>
<td>4000 mW</td>
<td>7000 mW</td>
</tr>
<tr>
<td>Rx. consumption</td>
<td>30 mW</td>
<td>59.1 mW</td>
<td>800 mW</td>
<td>800 mW</td>
</tr>
<tr>
<td>μJ per bit (Tx)</td>
<td>4.12 μJ</td>
<td>0.204 μJ</td>
<td>416.66 μJ</td>
<td>1458.33 μJ</td>
</tr>
<tr>
<td>μJ per bit (Rx)</td>
<td>1.52 μJ</td>
<td>0.23 μJ</td>
<td>83.33 μJ</td>
<td>166.66 μJ</td>
</tr>
</tbody>
</table>
Key-escrow systems
Underwater Sensor Networks

- **Contribution (energy):** Self-certified cryptography and ID-based cryptography are better than “traditional” approaches in UWSN

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ECMQV</td>
<td>107.26</td>
<td>704.98</td>
<td>812.24</td>
<td></td>
</tr>
<tr>
<td>SOK</td>
<td>309.39</td>
<td>191.99</td>
<td>501.38</td>
<td></td>
</tr>
<tr>
<td>SC-ECMQV</td>
<td>77.25</td>
<td>352.99</td>
<td>430.24</td>
<td></td>
</tr>
</tbody>
</table>

- **Contribution (communication):** ID-based cryptography is better than other approaches in UWSN
  - Traditional cryptography: Exchanges **1410** bits
  - Self-certified cryptography: Exchanges **706** bits
  - Identity-based cryptography: Exchanges **384** bits
3. Self-Awareness Services

- **Goals:**
  - Develop situation awareness mechanisms, which can detect abnormal events that might affect the behaviour of the network
  - Develop a blueprint of a distributed Intrusion Detection System architecture for sensor networks
  - Study the applicability of trust management systems in sensor networks
Self-Configurability and Situation Awareness

- **Self-Configurability**: Sensor nodes must configure themselves in order to respond to internal/external events
  - Example: Nodes affected by malfunctioning neighbours

- **Situation Awareness**: recognize certain events that might affect its behaviour and the overall behaviour of the network
  - Existence of simple and useful mechanisms
    - “Heartbeat” messages
    - Analysis of packet information
  - Need to consider all events that may affect a sensor network
Situation Awareness Mechanisms

- In order to detect any surrounding events, it is necessary to know the nature of those events and how to detect them
  - Simile: *Sensor network as a living body*. Disease ↔ Symptoms

- In situation awareness mechanisms, the presence of certain collateral effects will be indicative of the existence of an event
  - Back pain
  - Fever
  - No packets
  - Destination does not relay
Situation Awareness Mechanisms
Identifying abnormal events

- Node malfunction
  - Node “death” (unavailability)
  - Sensory hardware providing inconsistent information

- Outsider attacks
  - Manipulation of the sensory hardware
  - Manipulation of the communication channel (e.g. DoS)
  - Node tampering

- Insider attacks
  - Impersonation attacks
  - Message creation / alteration attacks
  - Feature advertising
  - Time-related attacks
Situation Awareness Mechanisms
Identifying collateral effects

**Contribution:** Relationship abnormal events ↔ collateral effects

<table>
<thead>
<tr>
<th>Abnormal event</th>
<th>Collateral effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jamming</td>
<td>Wide data unavailability</td>
</tr>
<tr>
<td>Hw. failure (“unavailable” node)</td>
<td>Data unavailability</td>
</tr>
<tr>
<td>Node subversion</td>
<td>Node temporarily unavailable</td>
</tr>
<tr>
<td>Tampered, Malfunctioning sensor</td>
<td>Deviations, Inconsistences</td>
</tr>
<tr>
<td>Packet Replaying</td>
<td>Packet too old</td>
</tr>
<tr>
<td>Impersonation Attacks</td>
<td>New neighbours, Packets per node</td>
</tr>
<tr>
<td>Message creation</td>
<td>Changes in packet density, Inconsistent alerts</td>
</tr>
<tr>
<td>Packet alteration</td>
<td>Changes in packet (only for broadcasted)</td>
</tr>
<tr>
<td>Feature advertising</td>
<td>Inconsistent feature with neighborhood</td>
</tr>
<tr>
<td>Time-Related attacks</td>
<td>Long delays, Traffic imbalance</td>
</tr>
</tbody>
</table>
**Situation Awareness Mechanisms**

**Application influence**

- **Contribution**: The way in which collateral effects are analyzed is highly dependant on the application requirements and characteristics.

- **Examples of this kind of influence:**
  - **Network size**
    - Small networks: abnormal events do not occur or are difficult to detect
      - Base Station should have more importance in this context
  - **Node mobility**
    - Need to analyze in greater deep the collateral effects
      - Some collateral effects will only provide partial information about an event
  - **Application features**
    - Functionality influences over existing events and how to detect them
    - Need to calibrate the detection mechanisms
Intrusion Detection Systems (IDS)

- Sensor networks could also benefit from advanced detection and decision mechanisms: *Intrusion Detection Systems*

- There is no standard mechanism for developing IDS in sensor networks
  - Partial results: Agent location, detection mechanisms, interrelationships

- Properties that a IDS must fulfil:
  - Full network coverage
    - Cover all the information flow of the network
  - Simplicity
    - Use mainly simple components, statistics and mechanisms
  - Adaptability
    - Can include new or existing detection mechanisms
    - Can exclude detection mechanisms that are not relevant for the application
Applying IDS to WSN

- **Contribution**: Blueprint of a distributed IDS architecture
  - *Base Station Agent*
  - *Node ‘Local / Global’ Agent*
  - Components: Data acquisition, Detection, Collaboration, etc.

![Diagram of IDS architecture](image)

**DATA ACQUISITION**
- Sensors
- Packets
- Others

**Situation Awareness**
- Protocol-specific Analyses

**DETECTION**
- Measurements
- Collisions (Backoffs)
- Query / Alert information

**STATISTICS**
- #packets (total, per period)
- Last Sequence no. / timestamp
- Others

**COLLABORATION**
- Malicious
- Suspicious

**ALERT DB**
Applying IDS to WSN

- **Tasks of the IDS Agents**
  - **Base Station Agent:** Analyze the network from a global point of view
    - Continuous execution of detection mechanisms
  - **Node Local Agent:** Analyze the contents of packets, the features of its environment, and other local aspects
    - Execution of mechanisms whenever data is available
  - **Node Global Agent:** Snoop packets sent in the neighbourhood, analyze their headers, timing information, and others.
    - Periodic execution of detection mechanisms

- **The periodicity of the detection mechanisms depends on the network load, reaction time, acceptable energy consumption**

- **Distribution of Node Agents**
  - **Distributed Systems:** Disconnection of detection mechanisms (Redundancy)
  - **Hierarchical Systems:** Node Global Agent on Cluster Head
Trust Management Systems

- Trust?
  - “The firm belief in the reliability or truth or strength of an entity”
  - Aids the members of a distributed network (‘trustor’) to deal with uncertainty about the future actions of other participants (‘trustee’)

- Types of Trust Management Systems:
  - Credential-Based: Trust on your credentials
  - Behaviour-Based: Trust on your reputation
    - “What is generally said or believed about a person or the character or standing of a thing”

- Behaviour-Based Systems could be applicable to sensor networks
  - Is trust really important?
  - How to define Model, Metrics, Feedback?
Trust Management Systems
Trust and Sensor Networks

- Trust is important for sensor networks
  - When trust is important? Existence of uncertainty
    - “The outcome of a certain situation cannot be clearly established / assured”
  - Uncertainty = Opportunism + *Information Asymmetry*
    - Opportunism? **NO**. Nodes work towards the same goals
    - Information Asymmetry? **YES**. Partners may malfunction / be malicious

- Research on WSN Trust: Early stage
  - Can deal satisfactorily with some problems in this area
  - Need to consider sensor network-specific factors
Trust Management Systems
Network-specific features

- **Contribution**: Analysis on WSN-specific factors of Trust Management in sensor networks

- Initialization and information gathering
  - Initial Trust: In the beginning, all sensor nodes should be trusted
  - “Apoptosis”: A sensor node alerts the network about its state

- Information modelling
  - Variable impact: certain events should have more influence on reputation
  - Memory: Bad behaviour should not be forgotten easily
  - Granularity
    - Maintain separate opinions about the actions of their peers
    - Specific trust values allows taking decisions on specific situations
  - Consider ‘risk’ and ‘importance’ on calculating trust values
  - Consistence: Contradictory information should be source of mistrust
4. Applicability of Security Services

- **Goals:**
  - Apply the concepts and ideas presented in this dissertation to an ongoing middleware architecture
  - Analyze the relationship between a secure sensor network and the Internet
Middleware Architecture
SMEPP Project

- SMEPP - Secure Middleware for Embedded Peer-to-Peer systems
  - European STREP project (FP6-IST-033563) funded by the European Union under the 6th Framework Programme

- Major Goals
  - Develop a middleware for Embedded P2P Systems (EP2P)
    - Environmental monitoring: Nuclear power plants
    - Home systems: smart homes, assisted-living residents
  - Hide the complexity of the underlying heterogeneous infrastructure while providing open interfaces for application development
    - Adaptability, scalability, high availability, ubiquity...
  - Security for embedded devices: Sensor networks
    - Authentication of peers, secure communication channels, self-configurability
Middleware Architecture
Security aspects

- **Contributions**¹:
- Security as a transversal layer
  - Can be accessed by all elements in the architecture
  - Component point of view: Dynamic and adaptable
- Cryptographic services
  - Used the work in this thesis as an input (e.g. use of PKC)
- Situation awareness
  - Support for self-configurability in the routing protocol
- Application-driven security
  - Security mechanisms are designed according to the requisites of the future SMEPP applications

¹Security Mechanisms are being jointly developed by the members of the SMEPP consortium
Middleware Architecture
Levels of Security

- **Contribution**: Application developers can choose the level of security that better adapts to the requirements of their applications.
  
  - **Multiple Security Domains**:
    - One global domain (one network)
    - Various group domains (applications inside the same network)
  
  - Level of Security can be selected for every domain

1. Security Mechanisms are being jointly developed by the members of the SMEPP consortium
Integration WSN - Internet
General Perspective

• How to unleash the real potential of sensor networks?
• Publishing its services in a public network infrastructure using standard interfaces - Internet
  - The flow of information produced by the networks could be retrieved and analyzed by different applications situated in diverse geographical locations
  - An operator could control a sensor network remotely
• Challenges:
  - Discover, control, process data
  - Addressing the elements of the network
  - Balance between optimization and standard protocols
  - Availability of information
  - Etc.
• Benefits: Remote access, creation of complex services
Integration WSN - Internet

Security Challenges

- **Contribution**: Interaction between secure WSN and the Internet
- End-to-end secure channels
  - Between users and sensors, between sensors of different networks
- **Authentication**
  - Device Authentication: Standard security protocols (p. ej. SSL/TLS)
  - User Authentication: Credentials
- **Authorization**
- **Accountability**
  - Analysis and storage of interactions between users and services. Recreate security incidents and abnormal situations
- **Intrusion Detection**
- **Availability**
  - Robustness of the information flow
Integration WSN - Internet

Approaches

- Integration strategies: *Front-end proxy solution, gateway solution, TCP/IP overlay solution*

  - **Contribution:** Analysis of the challenges in these different approaches
Open Issues and Solution Proposals
Front-end Proxy

- Protection mechanisms *implemented and deployed* within the base station

- Base station will:
  - Negotiate and establish secure end-to-end channels using standard protocols
  - Authenticate itself on behalf of its sensor nodes
  - Analyze the credentials presented by the users (e.g. attribute certificates)
  - Store and analyze any interaction between the external hosts and the nodes
  - Behave as a ”cache server”, storing the sensor nodes data

- Disadvantage: the base station becomes a single point of failure
  - Solution: Use multiple base stations
    - Need to maintain the information consistency between all the base stations
Open Issues and Solution Proposals
TCP/IP

- Specific Situation: Protocols and security mechanisms used in Internet hosts should also be supported by the sensor nodes. Sensor network is no longer an independent entity

- Possible solutions:
  - Use Kerberos or public key mechanisms for user authentication and authorization
  - Create specific IDS rules and detection mechanisms for maintaining the accountability of the network
  - Device authentication: KMS protocols with “node connectivity”

- Unresolved issues:
  - Communication security and device authentication
    - Network layer solutions: IPsec vs specific security models
    - Application-layer solutions: SSL/TLS standards
  - Availability
    - Consider the low storage capacity of highly constrained nodes
Open Issues and Solution Proposals

Gateway - TCP/IP

- Include certain protection mechanisms within the base station due to its “gateway” role
  - Analyze and/or store accountability information
  - Store historic data
  - Improve network availability ("cache server", intelligent forwarder)

- Open issues:
  - Implement these mechanisms alongside end-to-end secure channels

- Note: in the TCP/IP solution, the router must translate the IPv6 packets to 6lowpan packets.
  - Translate packets within the base station, perform “gateway” roles
5. Conclusions
Goals Achieved

- “Complete set” of application-driven security mechanisms
- Review suitability of the SotA in primitives for sensor nodes
- Develop a methodology for study and analysis of KMS protocols
- Support for PKI in sensor networks, applicability of untraditional PKC
- Development of lightweight situation awareness mechanisms
- Development of a simple/adaptable/distributed IDS system
- Analysis of sensor-specific issues in trust management systems
- Application of these concepts to a middleware architecture
- Analysis of interactions between secure sensor networks and the Internet
Areas in need of further research

- Interaction between cryptographic HW modules and sensor nodes
- **Key Management Systems**
  - Scenarios without optimal KMS protocols
  - Properties that should be properly addressed
- Development of functional trust management systems for WSN
- Interactions between sensor networks and
  - ... the Internet
  - ... other pervasive systems
- Mobile sensor networks
Funding and Publications

- Funding & Dissemination:
  - I2R (Singapore), FPI (Andalusian Government), FPU (Spanish Government).
  - Projects: CRITIS (CICYT), ARES (CONSOLIDER), SMEPP (FP6).

- Publications:
  - Journals
  - Book Chapters
Funding and Publications

• Publications:
  
  - International Conferences
    
    
    
    
    
    
    
Funding and Publications

- **Publications:**

  - **Spanish Conferences**

  - **Under revision**
APPLICATION-DRIVEN SECURITY IN WIRELESS SENSOR NETWORKS

Seguridad Orientada a Aplicaciones en Redes de Sensores

Rodrigo Román Castro

June 27th, 2008
Wireless Sensor Networks - HW

- Sensing Unit
  - Temp.
  - Light
  - Vibr.
  - ...

- Microcontroller

- Power Unit

- Other Components
- External Storage

- Transceiver
Where are we heading?

- Applications
  - Requirements
  - Cost

- Smaller & Simpler
- Bigger & Better

Same, but different