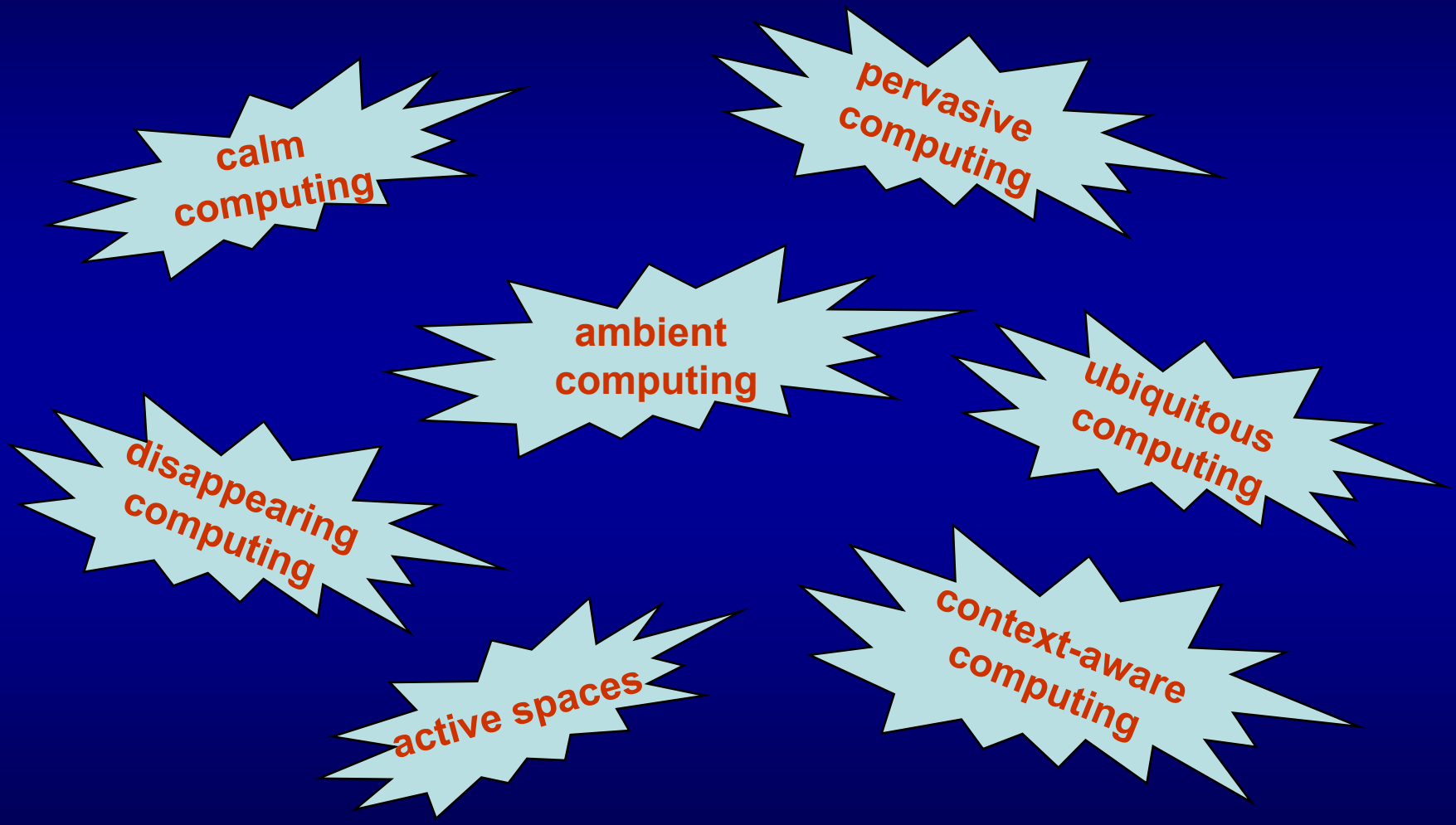
WSN
for
Critical Infrastructure Protection

Javier Lopez
Computer Science Department
University of Malaga
Spain

jlm@lcc.uma.es

Understanding the scenario

Confusing terminology



Mobile Computing

- Mobile computing is about increasing our capability to physically move computing services with us.
- An important limitation is that the computing model does not considerably change while we move.
  - Because the computing device cannot flexibly obtain information about the context and adjust it accordingly.
  - The only way to accommodate the needs and possibilities of changing environments is to have users manually control and configure the applications while they move.

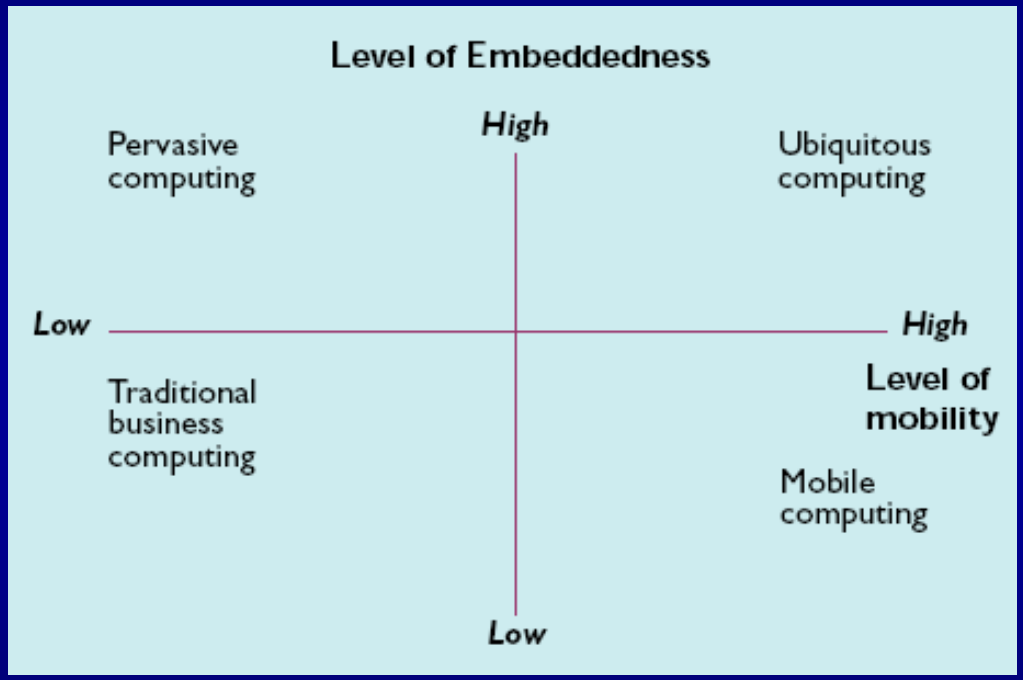



Pervasive Computing

- The computer has the capability to obtain the information from the environment in which it is embedded.
- The process is reciprocal:
  - The environment can and should also become "intelligent" in that it also has a capability to detect other computing devices entering it.
- This mutual dependency and interaction results in a new capacity of computers to act "intelligently" upon and within the environments in which we move.

Ubiquitous Computing

- Ubiquitous computing realm will integrate large-scale mobility with pervasive computing functionality.
- Computers will be embedded in our natural movements and interactions with our environments.



Ubiquitous Computing

- The shift towards ubiquitous computing poses multiple novel technical, social, and organizational challenges.
- At the technological software level:
  - Design and development of ubiquitous services
  - Design and implementation of computing architectures that enable, for instance, the dynamic configuration of ubiquitous services on a large scale
  - Security
  - Etc.
- Different HW technologies used and under development:
  - Wireless Sensor Networks is one of the key technologies of the ubiquitous computing visions.

WSN Basics

Real World

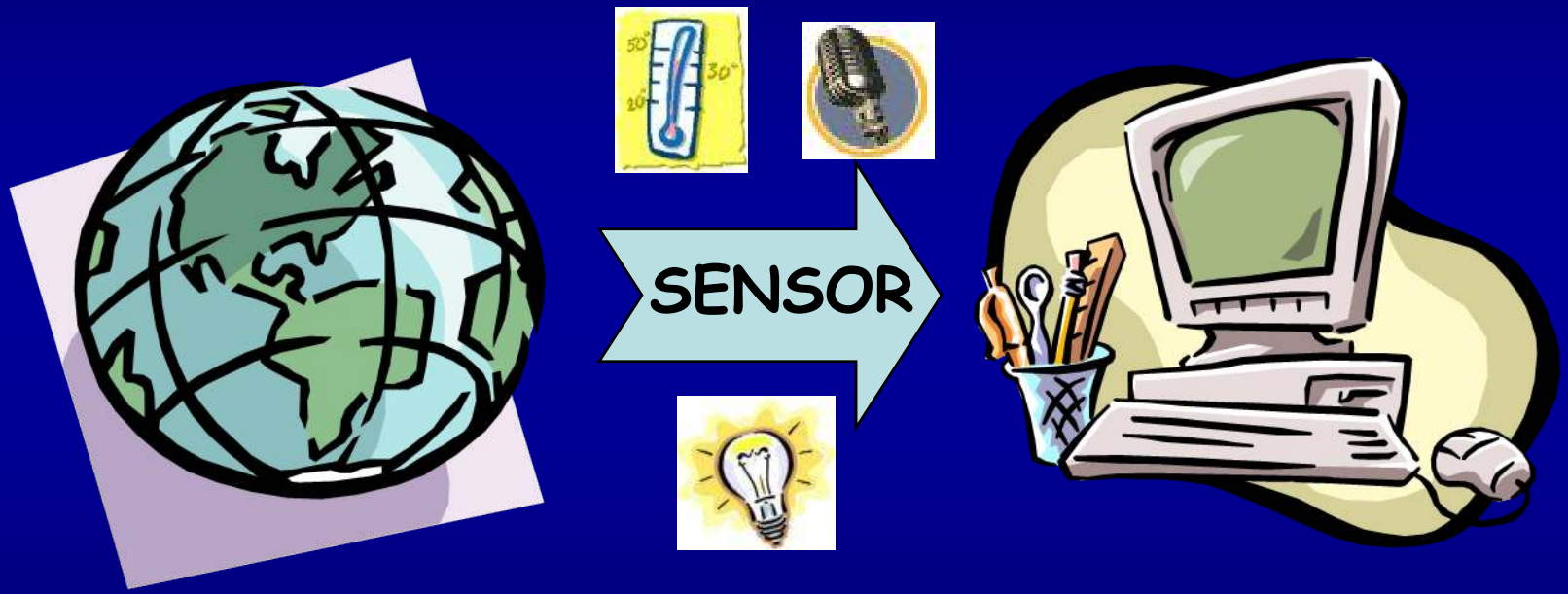
Real World

Temperature

Sound

Light

Real World → Computer

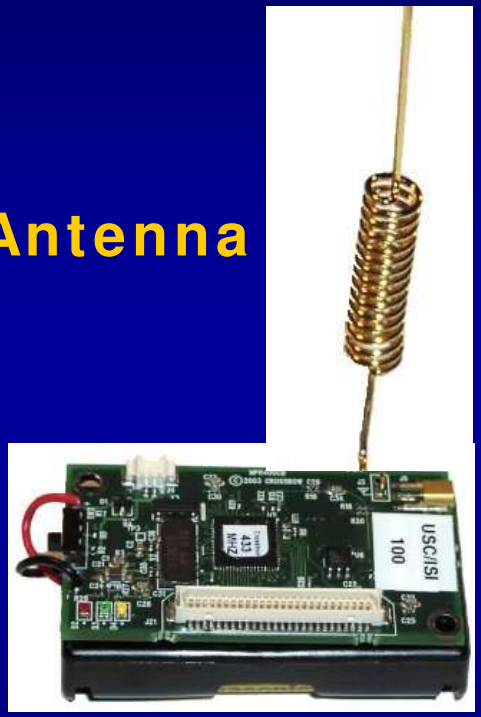


Real World

Computer World

From sensors to sensor nodes

Antenna



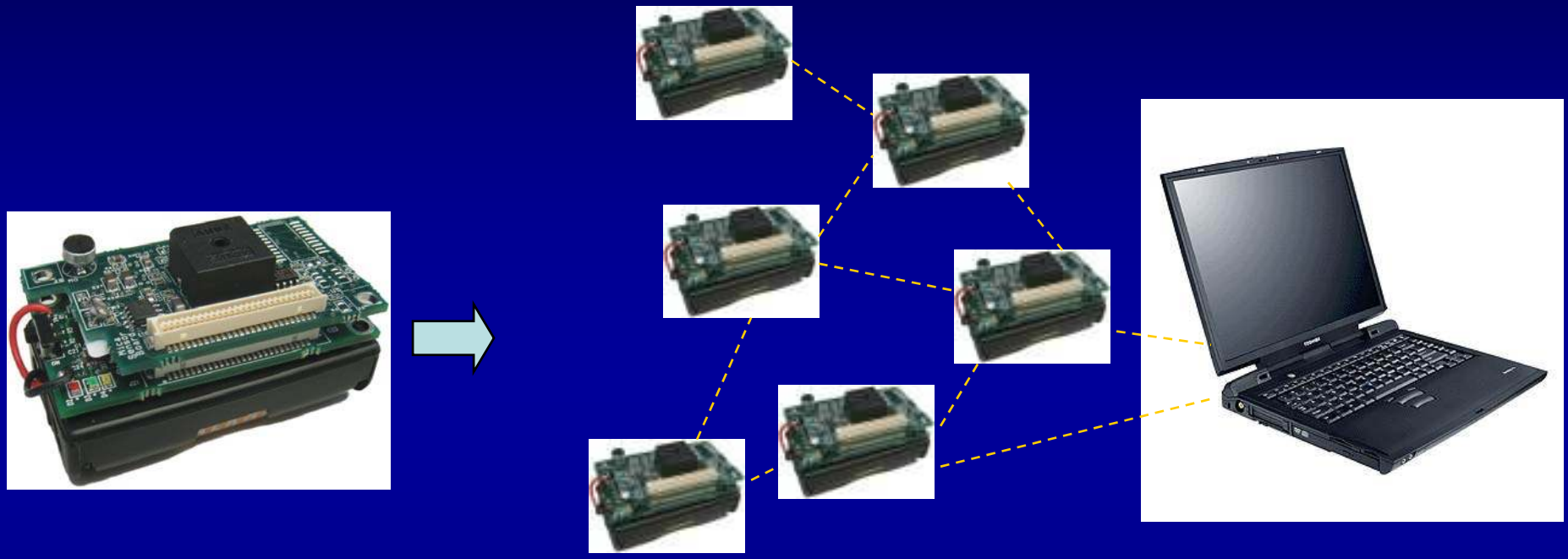
Autonomous Computer

+

=

SENSOR NODE

From sensor nodes to sensor networks

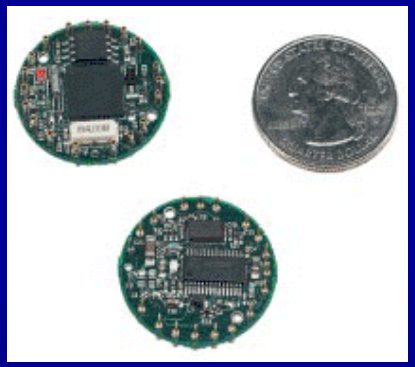


(Collaboration, Event-driven processing, ...) =

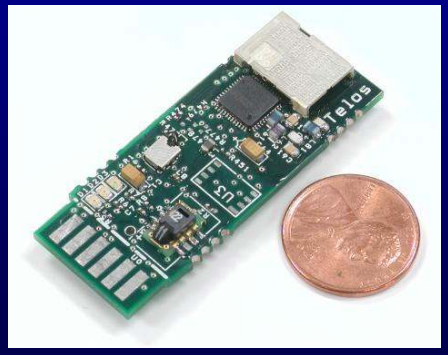
Distributed Applications

WSN Products

- The market already offers a number of sensor network hardware products
  - not only for research purposes,
  - but for the integration and deployment in real-world ubiquitous applications:
    - EMS nodes by *Sensicast Systems*,
    - EM chips by *Ember Corporation*,
    - Mesh485 by *Millenial Net*,
    - Mote kits by *Crossbow Technology*,
    - SmartMesh-XR by *Dust Networks*,
    - Tmote Invent System by *Moteiv*.
    - etc.



MICADOT motes



Telos mote

Sensors limitations

- For the case of *Mica* family (*Mica2*, *Mica2dot*, *MicaZ)*, and *Telos* nodes:
  - Processor:
    - 8-bit Atmel ATmega processor
    - Telos: 16-bit TI MSP430 processor
  - Memory:
    - 128 KB ROM and 4 KB RAM
    - Telos: 48 KB ROM and 10 KB RAM
  - Speed:
    - Mica2dot: 4 MHz
    - Mica2 and MicaZ: 7.37 MHz
    - Telos: 8MHz

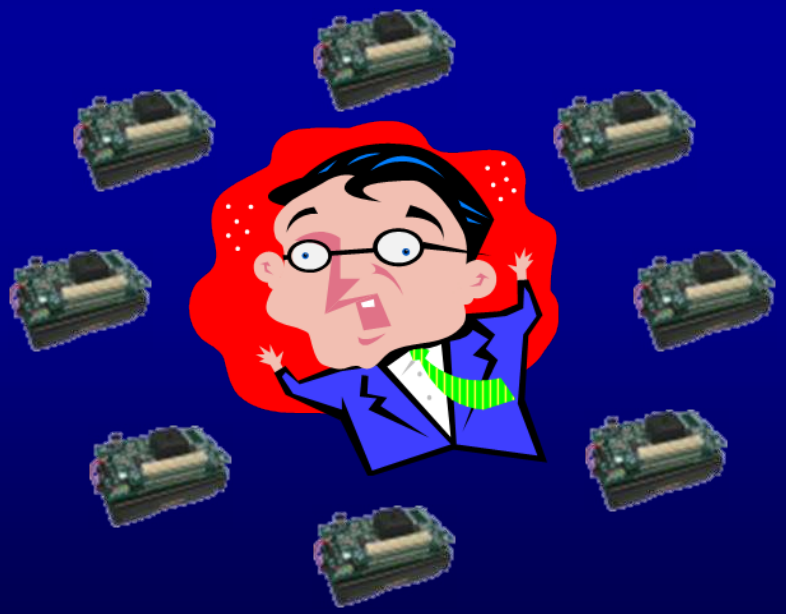
Sensors limitations

- Communications:
  - Mica2dot and Mica2 deliver up to 20 kbps on a single shared channel, with a range of up to around a hundred meters
  - MicaZ and Telos deliver up to 250 kbps.
- Software:
  - *TinyOS* operating system
    - Highly optimized (small, fast,…)
    - Support real-time tasks (multi-threaded, events-oriented)
  - C variant called *nesC* for programming purposes
    - featuring an event-driven concurrency model

Sensors limitations

- The current generation of wireless sensor nodes is still relying on batteries as its source of power.
  - The limited lifetime of batteries, however, significantly impedes the usefulness of such devices since maintenance accesses would become necessary whenever the battery is depleted.

- Furthermore, the intention of having large amounts of tiny nodes scattered over a large area would render maintenance impractical.



Sensors limitations

- Next generation sensor nodes will combine ultra-low power circuitry with power scavengers, which allow for maintenance-free operation of the nodes.
  - This opens up a whole new range of applications where the nodes can be placed in inaccessible location.
- Power scavengers are devices able to harvest small amounts of energy from ambient sources such as light, heat or vibration.
  - This energy is stored in a capacitor and can be used to power the sensor node either continuously, for small amounts of power, or in intervals if the demand is higher.

Sensors limitations

	Btnode 3	mica2	mica2dot	micaz	telos A	tmote sky	EYES
Manufacturer	Art of Technology	Crossbow			Imote iv		Univ. of Twente
Microcontroller	Atmel Atmega 128L				Texas Instruments MSP430		
Clock frequency	7.37 Mhz		4 MHz	7.37 MHz	8 MHz		5 MHz
RAM (KB)	64 + 180	4	4	4	2	10	2
ROM (KB)	128	128	128	128	60	48	60
Storage (KB)	4	512	512	512	256	1024	4
Radio	Chipcon CC1000 315/433/868/916 MHz 38.4 Kbauds			Chipcon CC2420 2.4 GHz 250Kbps IEEE 802.15.4			RFM TR1001868 MHz 57.6 Kbps
Max Range (m)	150-300			75-100			
Power	2 AA batteries		Coin cell	2 AA Batteries			
PC connector	Through PC-connected programming board				USB		Serial Port
OS	Nut/OS	TinyOS					PEEROS
Transducers	On acquisition board				On board		On acquisition board
Extras	+ Bluetooth radio						

Challenges

- Despite the resource limitations of the nodes, their tiny size makes them feasible for ubiquitous and real-time embedded applications.
- It is precisely this combination (of certainly contradictory characteristics) what gives rise to new research challenges:
  - design of different types of protocols,
  - development and deployment of applications and,
  - specification and design of new security models and solutions.

WSN Architecture and Applications

WSN Architecture

- Sensors operate and cooperate in an ad hoc manner using radio interfaces, resulting in a mesh architecture where nodes:
  - communicate directly only with nodes nearby
    due to limited power
    - some nodes communicate with a base station
  - support multiple communication paths
  - provide routing capabilities

what turns out to be an advantage in comparison with 802.11 and Bluetooth.

WSN Architecture

Admin

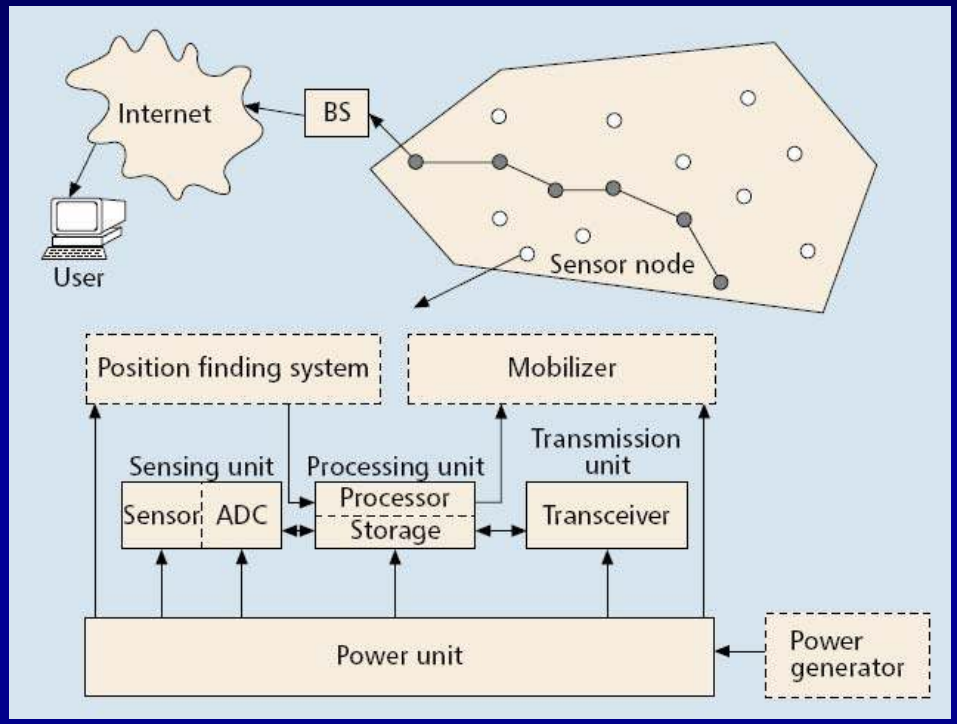
Users

Data Acquisition Network

Data Dissemination Network

WSN Architecture

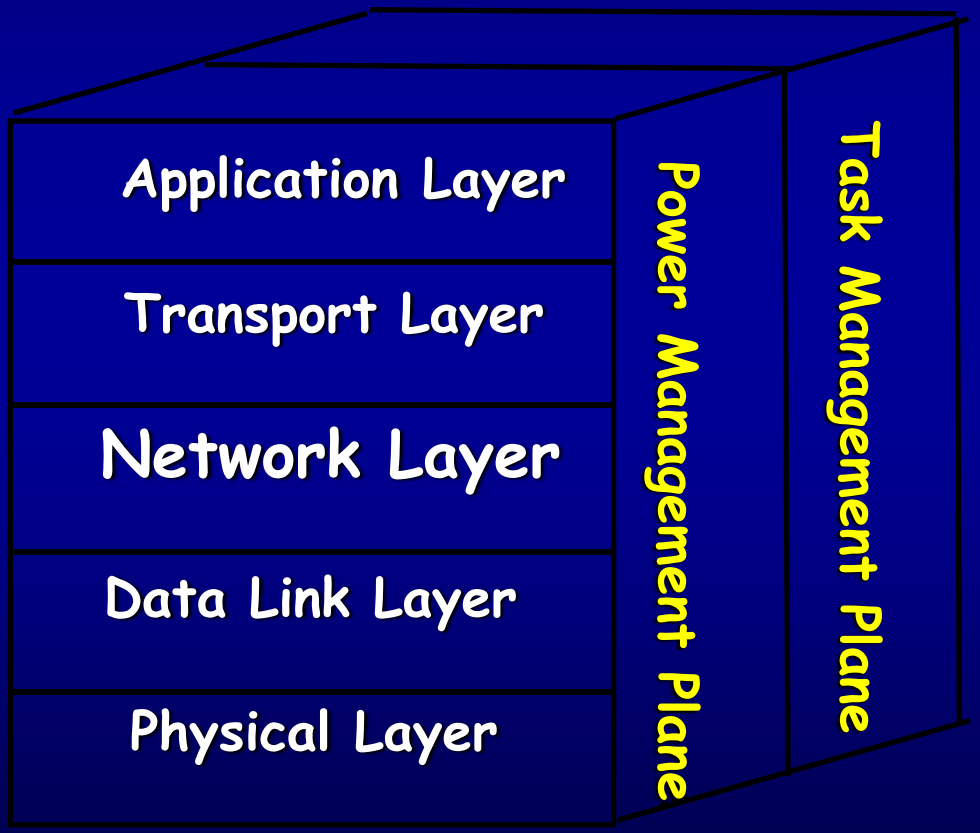
- The base station collects the data from the sensors, aggregate and send it to the outside world:
  - A central computing system where the information is stored for different purposes (analysis, control decision making, etc.)



- Contrarily to the case of the sensors, it is supposed that the base station has no limited resources
  - not only for all necessary computations but for all internal and external communications to the WSN.

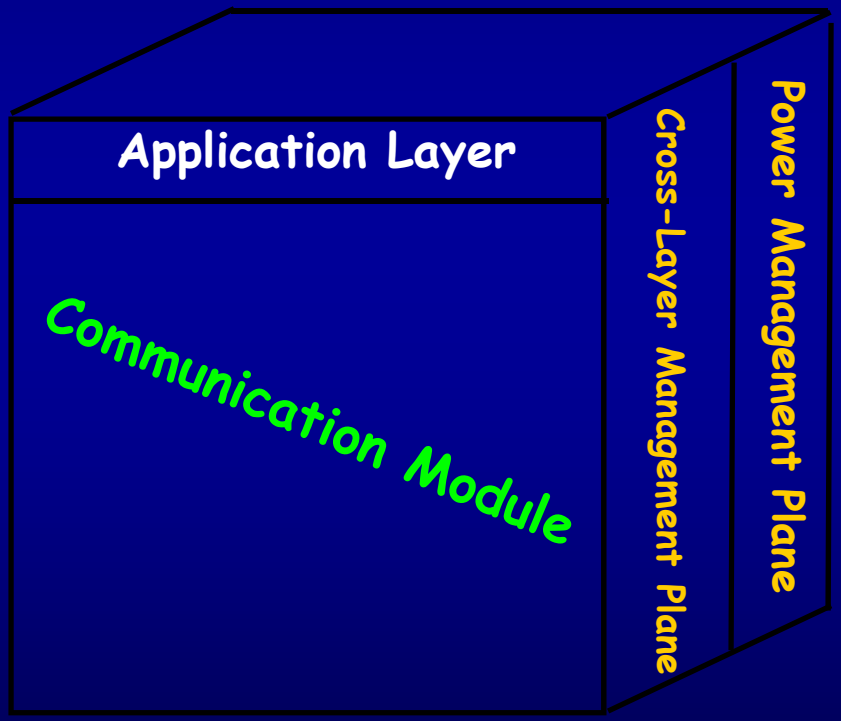
WSN Communication Architecture

- The communication architecture may be initially considered in the following way



WSN Communication Architecture

- Due to cross-layer melting, it is evolving to the following



WSN Applications

- Generally speaking, WSNs can be used in applications where sensors are unobtrusively embedded into systems, consequently involving operations like:
  - monitoring
  - tracking
  - detecting
  - collecting
  - reporting

WSN Applications

- By sectors, WSNs can be used in:
  - agricultural
  - business
  - critical infrastructure protection
  - environment
  - health care
  - homeland security
  - industrial
  - military applications
  - etc.

WSN Applications

- Specific applications:
  - farmland monitoring
  - animal identification and tracking
  - cultivation conditions (temperature, humidity, etc.)
  - inventory control
  - goods tracking and delivery
  - smart office
  - supply of water and electricity
  - freeway traffic monitoring and control
  - detection of structural integrity problems in buildings
  - wildlife habitat monitoring
  - microclimate control
  - detection of out-of-tolerance environmental conditions
  - recording wild animal habits
  - emergency medical care
  - remote medical monitoring
  - medicines tracking
  - frontiers surveillance
  - detection of illegal materials in custom controls
  - monitoring factory instrumentation
  - remote control of manufacturing systems
  - collecting pollution levels
  - detection of structures vibrations
  - target tracking
  - detection of biological or chemical weapons
  - location of vehicles and arms
  - wearable smart uniforms
  - etc.

WSN Applications … for Internet

- Still a wide range of applications to come when sensors can globally exchange information with entities on the Internet:
  - reaching, for instance, home environments.
  - creating what already has been called:
    - “network of things” or “Internet of things”
    - “tangible Internet”
    - “Blogjects in the world of interconnected things”.

The special case of CIP

The Landscape

- The growing dependence on interconnected infrastructures (transport, energy, information, …) increases the vulnerability of modern societies.
  - Conflicts in remote regions can destabilize the international order and directly affect any country's security and interests.
- Therefore, security risks and vulnerabilities are more diverse and less visible …
  - … because, once emerged, they ignore state borders and target interests outside and inside a country territory.

The Landscape

- Because security is compromised, directly or indirectly, by global challenges:
  - in Europe and elsewhere, the evolving global situation and some shocking events have profoundly changed the understanding of the term 'Security'.

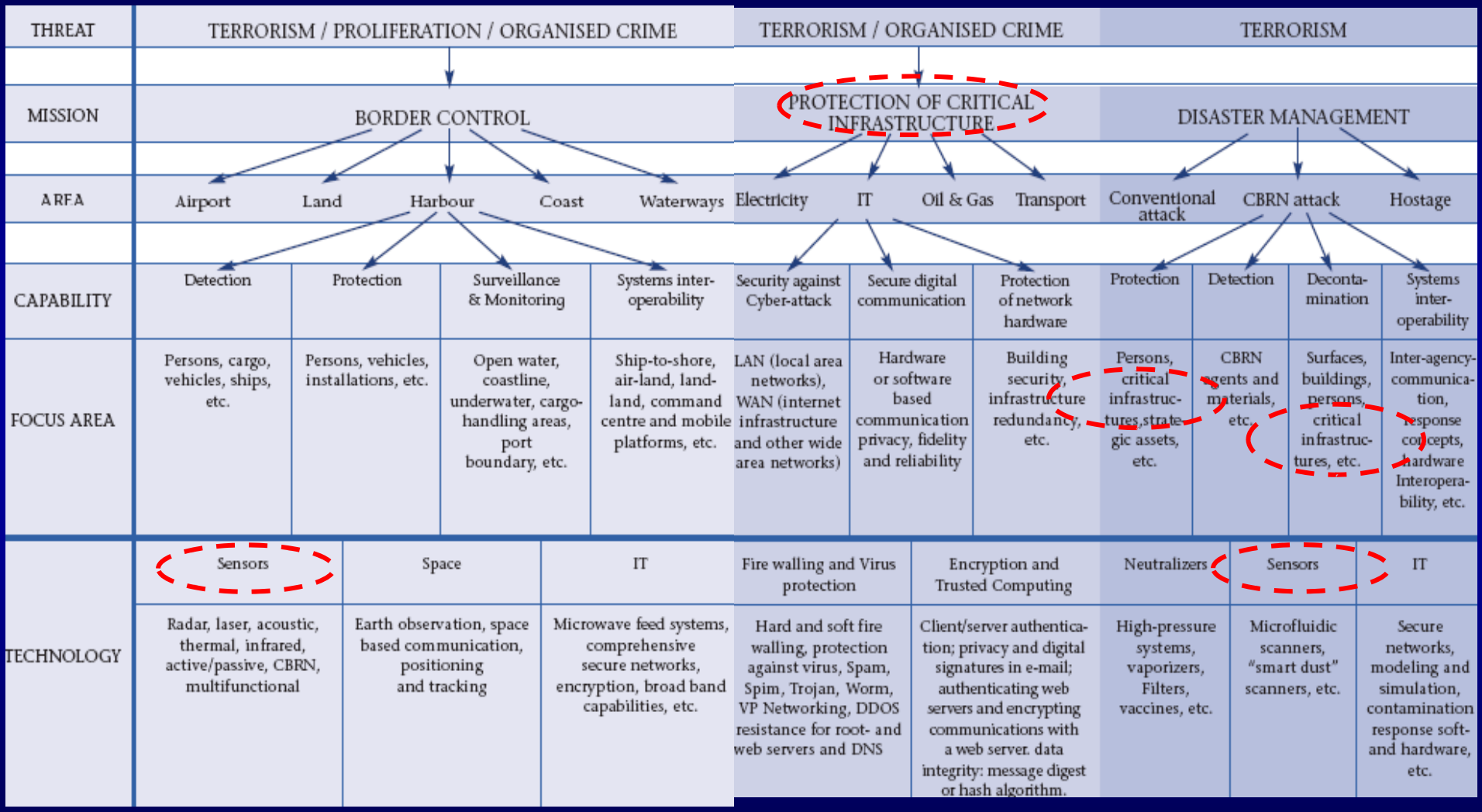
- In 2004, the European Community published the document: *Research for a Secure Europe*, that stated:

  "*The stakes are too high to trivialize threats, hoping that catastrophic events would spare EU territory*"

The Landscape

- It is not only that a new notion of security concept has been adopted. Also, we observe:
  - existence of record-breaking investments in defense and security.
  - establishment of Departments of Homeland Security to prevent terrorist attacks.
  - development of policies to:
    - reduce vulnerabilities to terrorism
    - minimize the damage from potential attacks and … natural disasters!!

EU vision


THREAT
TERRORISM / PROLIFERATION / ORGANISED CRIME
TERRORISM / ORGANISED CRIME
TERRORISM
MISSION
BORDER CONTROL
PROTECTION OF CRITICAL INFRASTRUCTURE
DISASTER MANAGEMENT
AREA
Airport
Land
Harbour
Coast
Waterways
Electricity
IT
Oil & Gas
Transport
Conventional attack
CBRN attack
Hostage
CAPABILITY
Detection
Protection
Surveillance & Monitoring
Systems inter-operability
Security against Cyber-attack
Secure digital communication
Protection of network hardware
Protection
Detection
Deconta-mination
Systems inter-operability
FOCUS AREA
Persons, cargo, vehicles, ships, etc.
Persons, vehicles, installations, etc.
Open water, coastline, underwater, cargo-handling areas, port boundary, etc.
Ship-to-shore, air-land, land-land, command centre and mobile platforms, etc.
LAN (local area networks), WAN (internet infrastructure and other wide area networks)
Hardware or software based communication privacy, fidelity and reliability
Building security, infrastructure redundancy, etc.
Persons, critical infrastruc-tures,strate-gic assets, etc.
CBRN agents and materials, etc.
Surfaces, buildings, persons, critical infrastruc-tures, etc.
Inter-agency-communica-tion, response concepts, hardware Interopera-bility, etc.
TECHNOLOGY
Sensors
Space
IT
Fire walling and Virus protection
Encryption and Trusted Computing
Neutralizers
Sensors
IT
Radar, laser, acoustic, thermal, infrared, active/passive, CBRN, multifunctional
Earth observation, space based communication, positioning and tracking
Microwave feed systems, comprehensive secure networks, encryption, broad band capabilities, etc.
Hard and soft fire walling, protection against virus, Spam, Spim, Trojan, Worm, VP Networking, DDOS resistance for root- and web servers and DNS
Client/server authentica-tion; privacy and digital signatures in e-mail; authenticating web servers and encrypting communications with a web server. data integrity: message digest or hash algorithm.
High-pressure systems, vaporizers, Filters, vaccines, etc.
Microfluidic scanners, "smart dust" scanners, etc.
Secure networks, modeling and simulation, contamination response soft- and hardware, etc.

Critical Infrastructure Protection

- Infrastructure:
  - *The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.*
- Critical Infrastructures (CI):
  - *Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.*
- Critical Infrastructures Protection (CIP):
  - *The programs, activities and interactions used by owners and operators to protect their critical infrastructure.*

CIP Sectors

- CI extend across many sectors of the economy as well as key government services, including:
  - Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system).
  - Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)
  - Finance (e.g. banking, securities and investment)
  - Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)

CIP Sectors

- Food (e.g. safety, production means, wholesale distribution and food industry)
- Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)
- Water (e.g. dams, storage, treatment and networks)

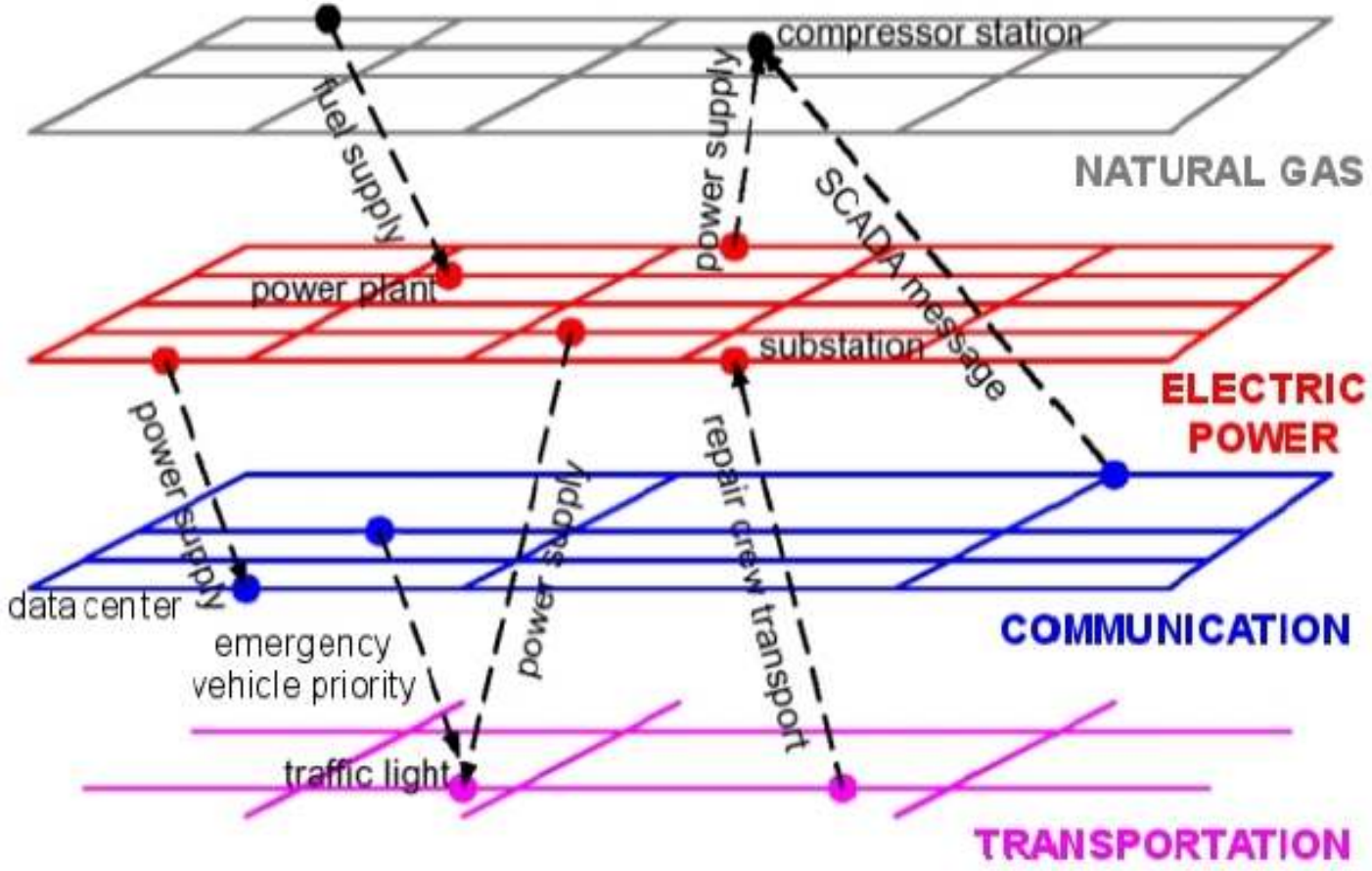
- Some critical elements in these sectors are not strictly speaking 'infrastructure‘
  - but are in fact, networks or supply chains that support the delivery of an essential product or service.

Public vs. Private

- These infrastructures are owned or operated by both the public and the private sector.
- However, the European Commission has declared that:
  - "The reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State".

Consequences in CIP Sectors

- The consequences of an attack could vary widely:
  - A successful cyber attack would cause few, if any, casualties, but might result in loss of vital infrastructure service (e.g. cyber-attack on the public telephone switching network)
  - However, an attack on a chemical or liquid natural gas facility's control systems might lead to more widespread loss of lives as well as significant physical damage.
  - Another type of failure might be when one part of the infrastructure leads to the failure of other parts, causing widespread cascade effect.
    - Europe's CI are highly connected and highly interdependent because of: corporate consolidation, industry rationalization, efficient business practices, population concentration in urban areas, etc.


compressor station
fuel supply
power supply
SCADA message
NATURAL GAS
power plant
substation
ELECTRIC POWER
power supply
power supply
repair crew transport
data center
emergency vehicle priority
COMMUNICATION
traffic light
TRANSPORTATION

Critical Information Infrastructures

- As an example, Europe's CI have become more dependent on information technologies, including the Internet:
  - Problems can cascade through the interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services.
  - Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction.
- The information infrastructure underpins many elements of the CI, and is hence called Critical Information Infrastructures (CII).

European Initiatives

- With all this in mind, the Commission constitutes the European Programme for Critical Infrastructure Protection (EPCIP)
  - to provide an dynamic partnership among EU institutions, CI owners/operators and EU Member States
    - in order to assure the continued functioning of Europe's CI
  - through:
    - adequate and equal levels of protective security on critical infrastructure,
    - minimal points of failure, and
    - rapid recovery arrangements throughout the Union.
- CIWIN (Crit. Infrast. Warning Information Network)

European Initiatives (PASR)

- PASR (Preparatory Action on Security Research). Five Project Areas:
  - Improving situation awareness
    - Aim: To identify the main threats that could affect Europe, particularly land and sea borders and assets of global interest, by appropriate information gathering, interpretation, integration and dissemination leading to the sharing of intelligence. Concepts and technologies for improved situation awareness at the appropriate levels could be developed and demonstrated.
  - Optimising security and protection of networked systems
    - Aim: To analyse established and future networked systems, such as communications systems, utility systems, transportation facilities, or networks for (cyber) commerce and business, with regard to the security of use, vulnerabilities, and identification of interdependencies to show how to implement protective security measures against both electronic and physical threats.

European Initiatives (PASR)

- Protecting against terrorism (including bio-terrorism and incidents with biological, chemical and other substances)
  - Aim: To identify and prioritise the material and information requirements of governments, agencies and public authorities in combating and protecting against terrorism and to deliver technology solutions for threat detection, identification, protection and neutralisation as well as containment and disposal of threatening substances including biological, chemical and nuclear ones and weapons of mass destruction.
- Enhancing Crisis Management (including evacuation, search and rescue operations, active agents control and remediation)
  - Aim: to address the operational and technological issues that need to be considered from three perspectives: crisis prevention, operational preparedness and management of declared crisis.

European Initiatives (PASR)

- Achieving interoperability and integrated systems for information and communication
  - Aim: to develop and demonstrate interoperability concepts for (legacy) information systems in the domain of security, enabling the linking of existing and new assets in clusters to offer improved performance and enhanced adaptive functionality. To support interoperability, system providers need to involve end-users and standardisation.

European Initiatives (FP7)

- Focus of the ICT Theme
  - Technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures so that they survive malicious attacks or accidental failures, guarantee integrity of data and continuous provision of responsive and trustworthy services, and support dynamically varying trust requirements.
- Focus of the Security Theme
  - Technology building blocks for creating, monitoring and managing secure, resilient and always available transport and energy infrastructures that survive malicious attacks or accidental failures and guaranteeing continuous provision of services.
    - Risk assessment and contingency planning for interconnected transport or energy networks
    - Modeling and simulation for training
    - Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures
    - ICT support for first responders in crises occurring in critical infrastructures

Underlying Technology

- An essential step in the research of CII is a comprehensive assessment to determine which underlying communications technologies and security options are appropriate for utility operations.

- CII are characterized by unique requirements for communications performance
  - including timing, redundancy, centers control and protection, and equipment control and diagnostics.

Underlying Technology

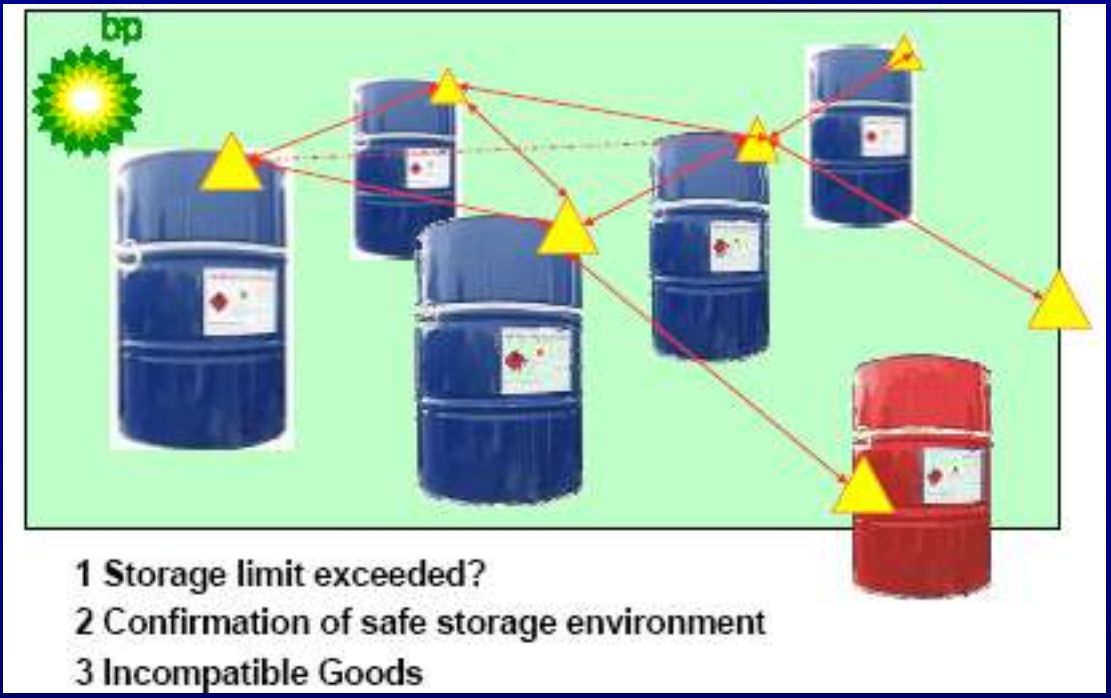
- Although strong centralized control is essential to reliable operations, CII requires:
  - multiple high-data-rate communication links,
  - a powerful central computing facility,
  - and an elaborate operations control center.
- For deeper protection, intelligent distributed control is strongly required to keep parts of the network operational.
- It is commonly agreed by network experts that Wireless Sensor Networks is the technology that better fulfills features like the ones required by CII.

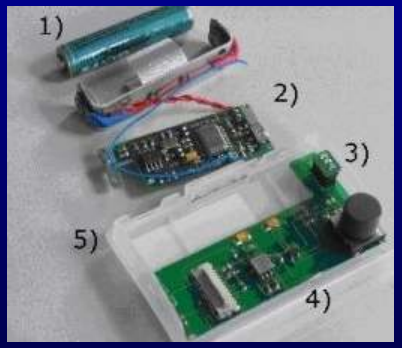
CoBIS

- Goal: embed business logic in the physical entities (business logic on-the-item), thereby creating Collaborative Business Items (CoBIs).
  - closing the gap between networked embedded systems technologies and their application in large-scale business and enterprise software systems.
- Items like materials, chemistry, machine parts, modules, etc. will have unique digital identities, embodied sensors to monitor their state and environmental conditions.

CoBIS

- Scenario: Support for safety-critical processes such as alerting against inappropriate materials being stored together or outside of approved storage facilities



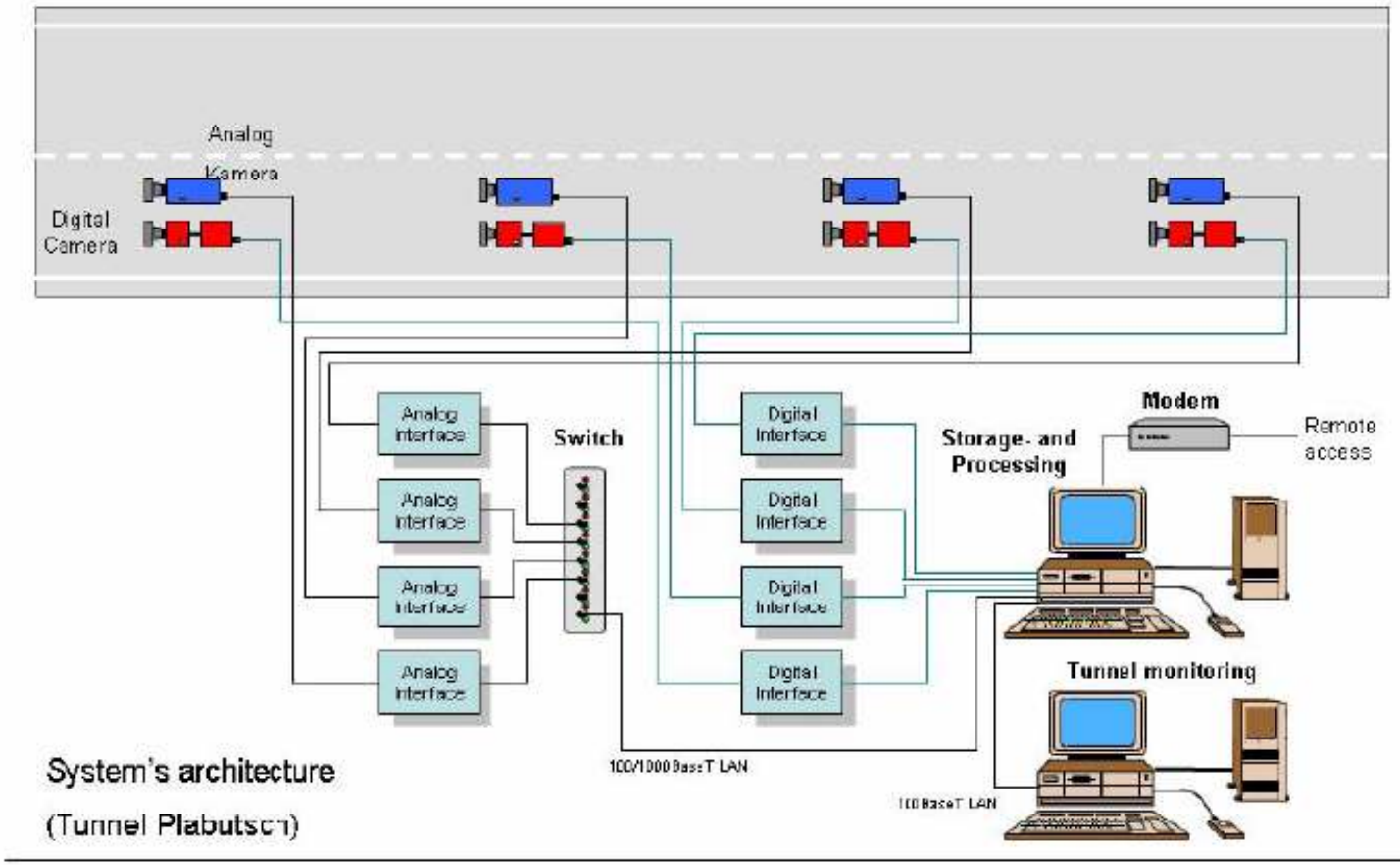


VITUS

- VITUS (**V**ideo **I**mage analysis for **TU**nnel **S**afety)
  - The main aim of this project is to build and implement a prototype for an automatic video image analysis system in order to increase safety in tunnel roads.

VITUS

Pilot system - Tunnel Surveillance



System's architecture

(Tunnel Plabutsch)

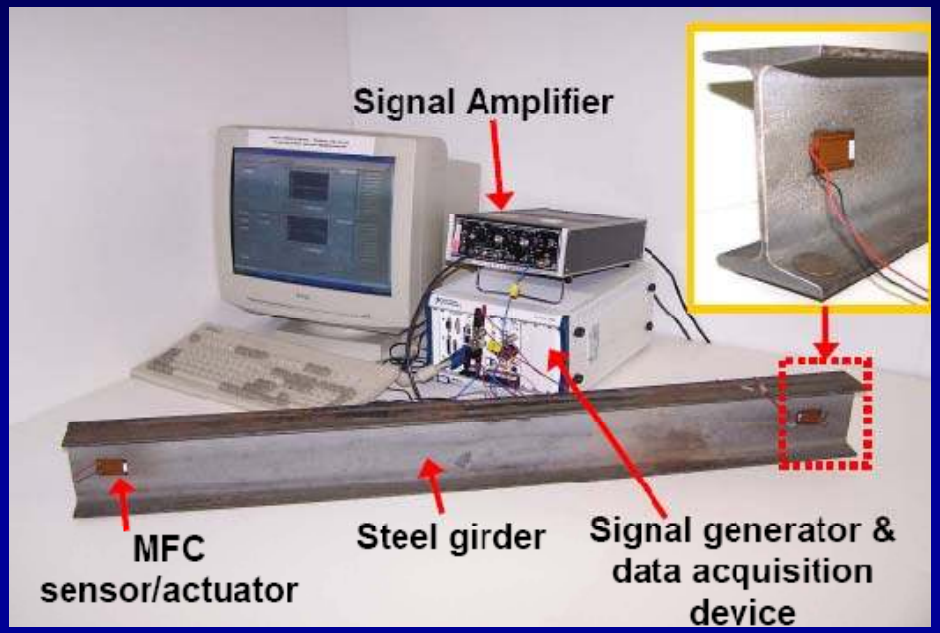
CenSCIR

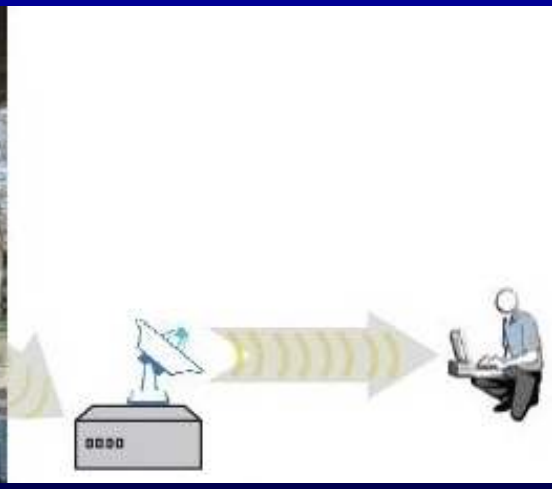
- The Center for Sensed Critical Infrastructure Research aims at delivering cost-effective, sensor-based monitoring systems for a broad range of critical infrastructure applications.
- These monitoring systems could be used for:
  - decaying bridges,
  - oil and gas pipelines,
  - unstable electric power grids,
  - leaking water distribution systems.

CenSCIR

Subject	2001 Grade	2005 Grade
Bridges	*C*	*C*
Dams	D	D
Drinking Water	*D*	D-
National Power Grid	*D+*	D
Navigable Waterways	*D+*	D-
Roads	*D+*	*D*
Solid Waste	*C+*	C+
Transit	*C-*	*D+*
Wastewater	*D*	D-
Total Investment Needs = $1.6 Trillion		

CenSCIR (and Sustainable Bridges)





(Non)-sustainable Bridge: The case of Minneapolis

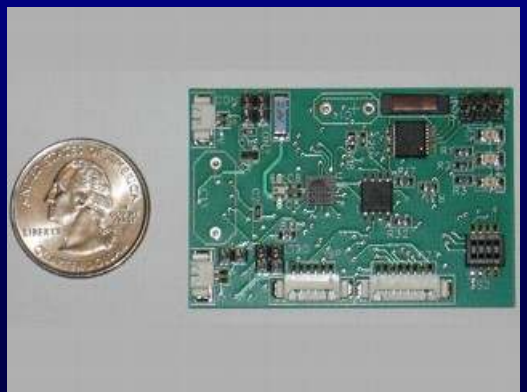
- ABC News:

Could Tiny Sensors Detect Bridge Crises?

Researchers Hope Tiny Sensors Placed on Bridges Can Offer Warning Before Disaster

This undated photo provided by Los Alamos National Laboratory, shows an experimental electronic sensor that could possibly be used to detect electrical charges emitted by stress on material, such as steel-reinforced concrete. LANL scientists are working on the technology that could provide early warnings of potential failures in highway bridges, according to officials.

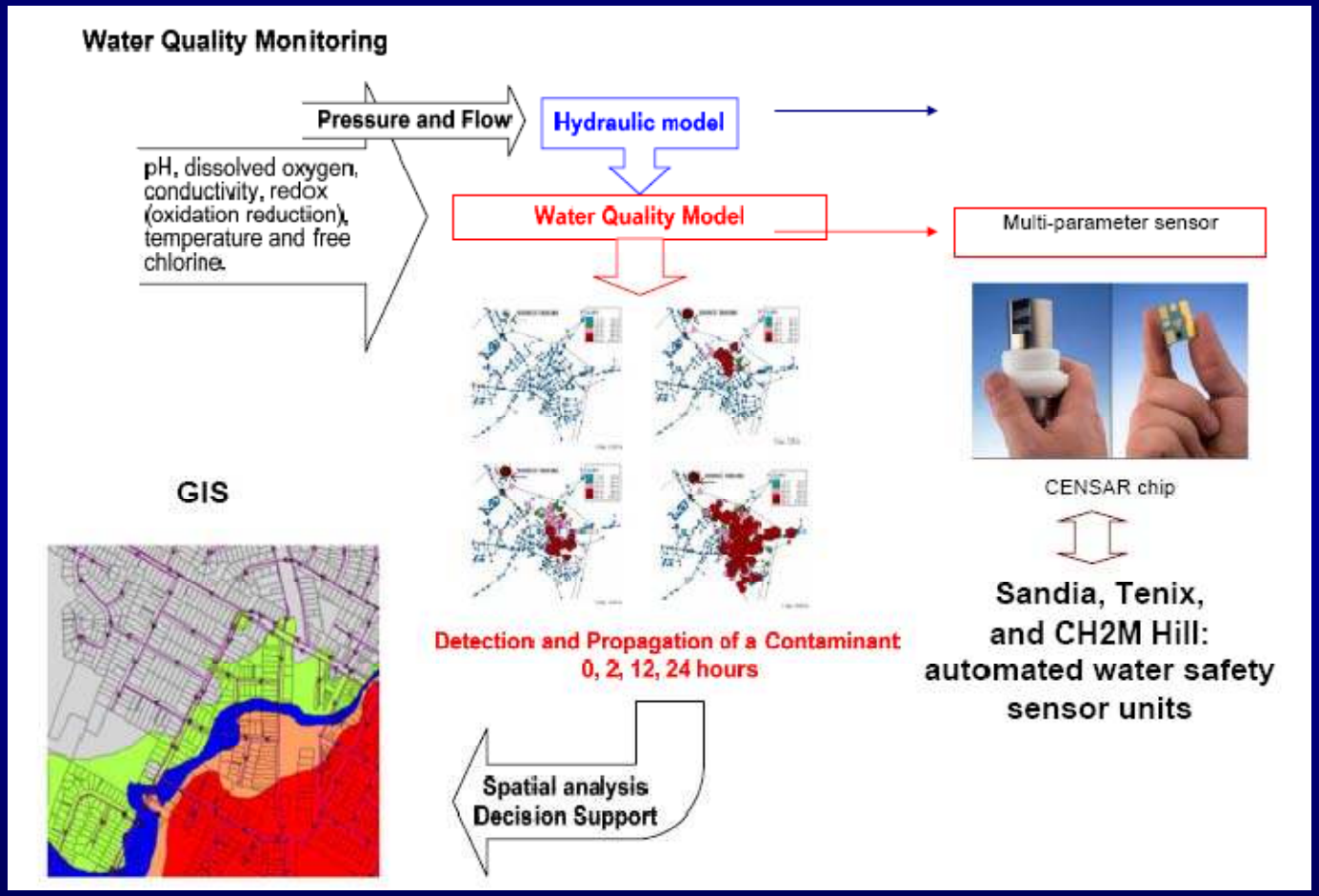
Researchers here are hoping small sensors put on bridges about the size of a credit card and costing only $1 apiece could provide an early warning to potential failures like the one in Minneapolis.



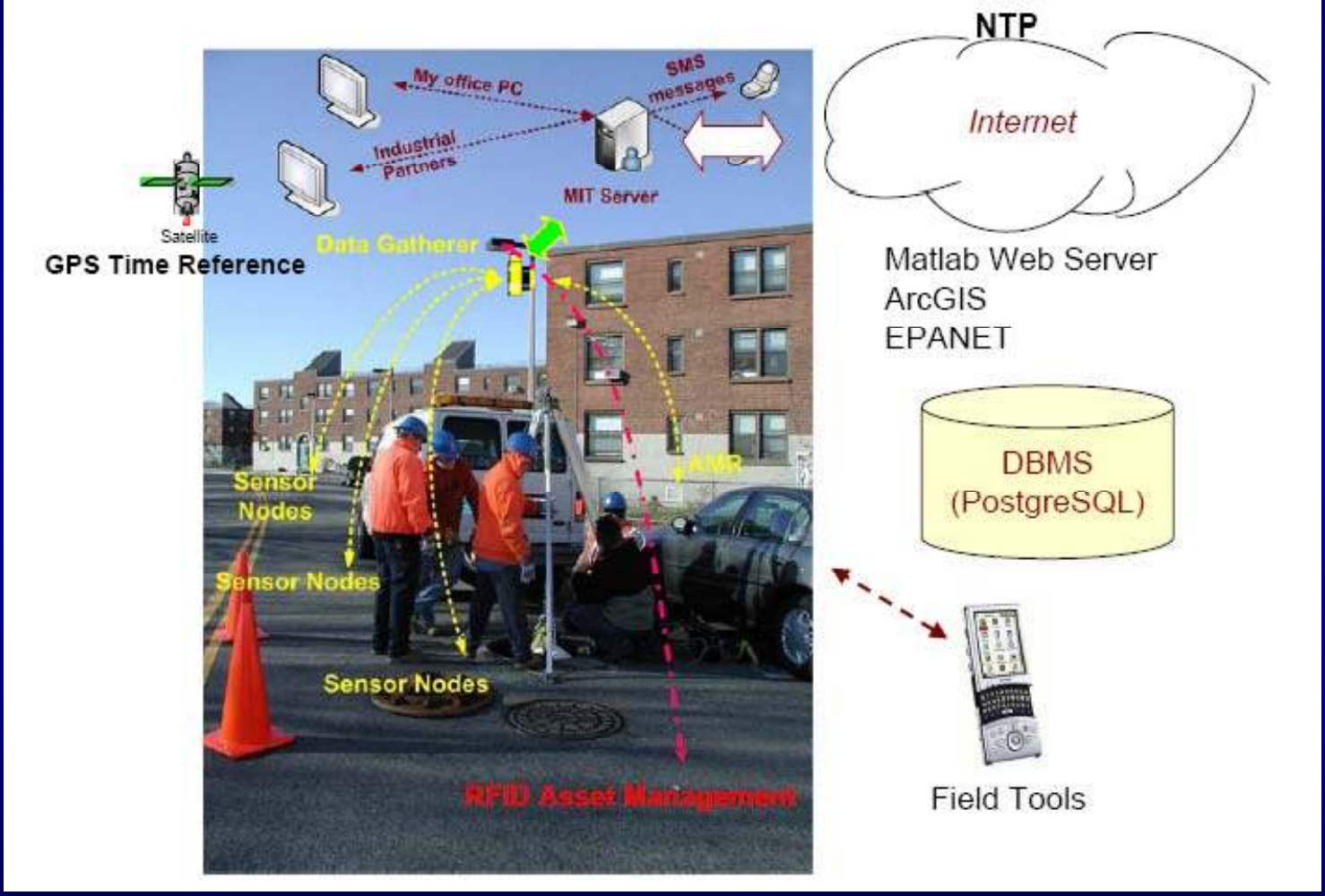
WINES II

- Goal: Use of Wireless Sensor Networks for Ageing Engineering Infrastructures (water supply, tunnels, bridges, etc.)

WINES II


Water Quality Monitoring
Pressure and Flow
Hydraulic model
pH, dissolved oxygen, conductivity, redox (oxidation reduction), temperature and free chlorine.
Water Quality Model
Multi-parameter sensor
CENSAR chip
GIS
Detection and Propagation of a Contaminant
0, 2, 12, 24 hours
Sandia, Tenix, and CH2M Hill: automated water safety sensor units
Spatial analysis
Decision Support

Boston Water Project



CONS:
Security concerns, requirements and attacks

Security concerns

- The reasons why security becomes an essential issue in WSN are:
  - sensitive nature of many of those applications (specially CIP)
  - untrusted environment where the sensors are deployed
  - share the drawbacks of any wireless network:
    - natural physical insecurity of wired communications is present.

Security concerns

- It is difficult to protect WSN because every node becomes a potential point of logical and physical abuse
  - Logical:
    - monitor transmissions,
    - intercept and modify data, and
    - impersonate nodes injecting false information to others.
  - Physical:
    - gain access to one or more of them and reprogram their operation
    - introduce his own fake nodes.

Security concerns

- Could tamper-resistant sensors help in hardening some of those attacks?
  - It would increase the cost, and their use would not result so attractive
  - Actual prices:
    - Set 8 MICAZ nodes + programming board: 3000$
    - Set 10 Telos nodes + programming board: 1200$

Security Requirements

- After the overview of the security concerns it is possible to argue about the security requirements for WSN
- Data Confidentiality
  - A sensor network should not leak sensor readings to its neighbors (especially in a military application, the data stored in the sensor node may be highly sensitive).
  - Key distribution is extremely important to build a secure channel.
  - Sensor identities and public keys should also be encrypted
- Authentication
  - The receiver needs to ensure that the data used in any decision-making process originates from the correct source
  - Also necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle).

Security Requirements

- Data Integrity
  - With confidentiality, an adversary may be unable to steal information. However, it can change the data, so as to send the sensor network into disarray.
  - For example, a malicious node may add some fragments or manipulate the data within a packet, that is later sent to the original receiver.
- Data Freshness
  - It is necessary to ensure that the data is recent and that no old messages have been replayed.
  - especially important when there are shared-key strategies employed in the design.

Security Requirements

- Availability
  - Adjusting the traditional encryption algorithms to fit within the WSN is not free, and will introduce some extra costs.
    - Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
    - Additional communication also consumes more energy.
  - A single point failure will be introduced if using the central point scheme, what greatly threatens the availability of the network.
- Self-Organization
  - WSN must self-organize to support multihop routing, and also to conduct key management and building trust relations.
  - If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

Security Requirements

- Time Synchronization
  - In order to conserve power, an individual sensor's radio may be turned off for periods of time.
  - Furthermore, sensors may wish to compute the end-to end delay of a packet as it travels between two pairwise sensors.
  - A more collaborative sensor network may require group synchronization for tracking applications, etc.
- Secure Localization
  - Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network.
  - For instance, a sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault.

Security Requirements

- Non-repudiation
  - A node can not deny sending a message previously sent
- Forward secrecy
  - A sensor should not be able to read any future message after it leaves the network
- Backward secrecy
  - A joining sensor network should not be able to read any previously transmitted message

Security Requirements

- BUT, there are important issues that directly affect requirements.
- It is questionable if primitives traditionally used in other networking scenarios are suitable for sensor networks
  - because small amount of RAM memory.
  - and very modest computational power.
- Thus, cryptographic operations must be designed to minimize the use of memory.
- Also, design of secure protocols should consider that
  - Each bit transmitted consumes as much power as executing hundreds of instructions.

Attacks

- Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, etc.
- Denial of service:
  - Can range from simply jamming the sensor's communication channel to more sophisticated attacks
    - more alarming is the projected use of sensor networks in highly critical and sensitive applications
  - Simple jamming is the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network
  - Retransmission of packets deplete a sensor node's power supply by forcing too many retransmissions

Attacks

- Sybil attack:
  - A malicious device illegitimately taking on multiple identities.
  - It is effective against routing algorithms, data aggregation, etc.
    - Regardless of the target, it functions similarly.
  - For instance, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, thus routing multiple paths through one malicious node.

Attacks

- Traffic Analysis:
  - For an adversary to effectively render the network useless, the attacker can simply disable the base station.
    - The base station can be identified (with high probability) without even understanding the contents of the packets (if the packets are themselves encrypted)
  - Idea: nodes closest to the base station tend to forward more packets. An attacker need only monitor to whom a node sends its packets.

Attacks

- Node replication:
  - An attacker seeks to add a node to an existing sensor network by copying (replicating) the ID of an existing node.
    - Packets can be corrupted or even misrouted.
  - An attacker can copy cryptographic keys to the replicated sensor and can also insert the replicated node into strategic points in the network
    - could easily manipulate a specific segment of the network

Attacks

- Attack against privacy:
  - Sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access.
  - Adversaries need not be physically present to maintain surveillance.
    - They can gather information in a low-risk, anonymous manner.
    - Remote access also allows a single adversary to monitor multiple sites simultaneously.

Attacks

- Physical attacks:
  - Sensor networks typically operate in hostile outdoor environments.
    - The small form factor of the sensors, and the unattended and distributed nature of their deployment, become a problem.
  - Physical attacks destroy sensors permanently, so the losses are irreversible.
  - Attackers can:
    - extract cryptographic secrets,
    - tamper with the associated circuitry,
    - modify programming in the sensors,
    - replace them with malicious sensors under the control of the attacker,
    - etc.

PROS:
Defensive measures, symmetric crypto-primitives and key infrastructures

Defensive measures

- Defending against DoS attacks
  - Identify the jammed part of the WSN and route around.
- Secure broadcasting and multicasting
  - Based on encryption techniques and key management techniques.
- Defending against attacks on Routing Protocols
  - For instance, employing redundancy. Multiple identical messages are routed between the source and the destination (supported by an authentication scheme).
- Defending against the Sybil attack
  - For instance, by using a trusted node that validates identity of the other nodes.

Defensive measures

- Detecting node replication
  - Randomized multicast and line-selected multicast
- Defending against attacks on sensor privacy
  - Anonymity mechanisms to protect location information
- ….
- Key Establishment and cryptographic operations!!

Crypto primitives

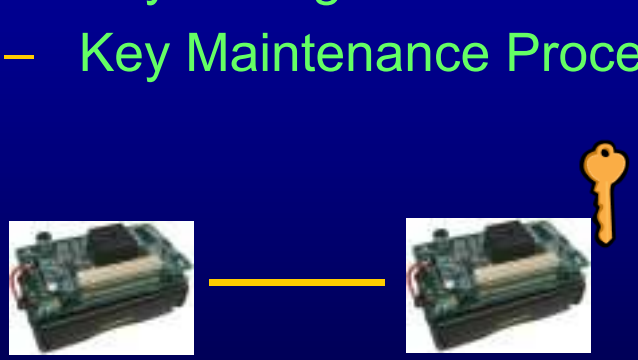
- It is crucial to provide basic security primitives to the nodes in order to:
  - Provide a minimal protection to the information flow
  - Provide a foundation to create secure protocols
- HW is expensive; so SW is, in most cases, the way to go.
- Global challenge:
  - To design strong and secure primitives using less energy, computational time and memory space

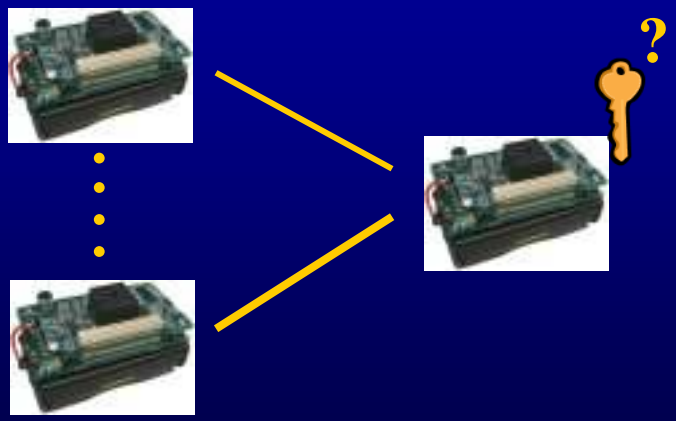
Crypto primitives

- Strong cryptography is a problem because of the mentioned limited sensor hardware
- Symmetric key techniques are attractive due to their energy efficiency
  - A simple security model for a sensor network employees a single secret key that is known by all nodes in the sensor network
    - There are other stronger models

Key Infrastructure

- The communication channel between any pair of devices must be protected
- The protection is provided by the security primitives; however, primitives make use of keys
  - Thus, a key infrastructure is needed
- Basic factors:
  - Key Distribution Protocols
  - Key Storage Policies
  - Key Maintenance Procedures



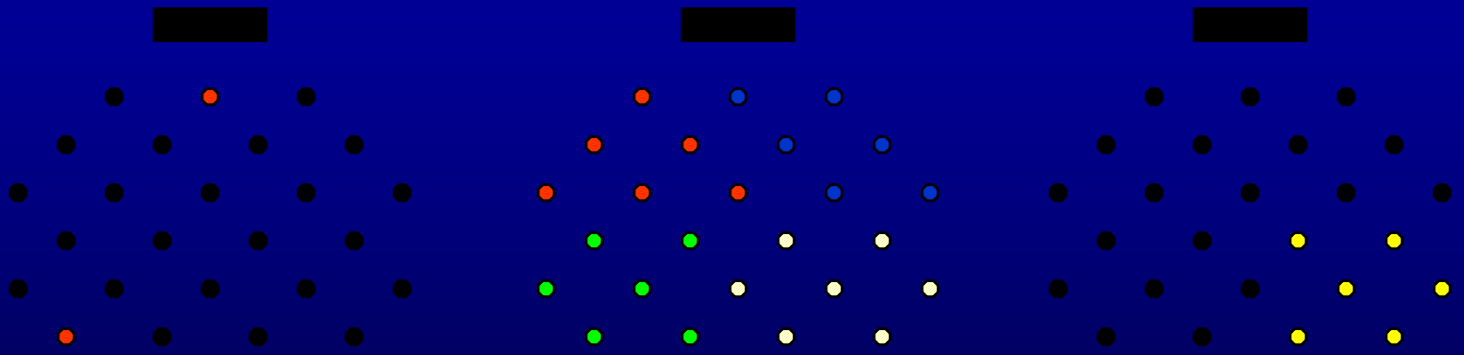


Key Infrastructure

- Key Distribution Protocols
  - How keys are issued to sensor nodes
    - Before Deployment
      - Keys cannot be captured during distribution
      - (In most cases) Network topology should be known!
    - After Deployment
      - Prone to be attacked
- Key Storage Policies
  - Number of keys inside a node in order to securely reach all other network nodes
  - Influence:
    - Network resilience (% of network under control of the adversary)
    - Node free memory
- Key Maintenance Procedures
  - How keys are refreshed
  - How nodes can be included/excluded from the network

Key Infrastructure

- Three different types of Key Infrastructure scenarios:
  - Global/Flat – Node reaching “any” other nodes in the network
  - Clustered – Secure Groups of nodes
  - Local – Dynamically generated autonomous secure groups



Key Infrastructure – CRISIS Project

- Classify Key Management Systems based on their properties:
  - Memory Footprint. Keys waste (limited) memory space.
  - Security. Confidentiality on bootstrapping Keys
  - Network Resilience. Node reveals Keys. % of network in danger?
  - Connectivity. Chance of two nodes sharing Keys.
  - Scalability. 10 – 100 – 1000 …
  - Communication overhead. Nodes negotiate parameters, expensive!
  - Energy. “Any mJ spent is one step towards oblivion…”

Key Infrastructure – CRISIS Project

(1)	(2)	(3)
Network Resilience	*AT-13* - Blom Key Predistribution [15]	✓: Res., Mem., Conn., Comm., Sca.
		× : Ext., *DES*{Mem., Res.}
	AT-14 - Multiple Space Key Predistribution [15]	✓: Res., Sca.
		× : *DES*{Conn., Mem., Comm.}, En.
	AT-07 - Q-Composite [17]	✓: Res.
		× : En., Sca., *DES*{Mem., Res., Conn.}
	AT-21 - Deterministic Multiple Space Blom DMBS [18]	✓: Res., Ext., Comm., Sca.
		× : Mem., Conn.
	AT-25 - Polynomial Based Key Predistribution [19]	✓: Res., Comm., Sca.
		× : Mem., En.
	AT-24 - Grid Based Key Predistribution [19]	✓: Res., Conn., Comm., Sca.
		× : Ext., Mem., En., *DES*{*LOC*}
	AT-01 - Key Infection [20]	✓: Res., Conn., Sca., Mem.
		× : Comm., Sec.

- *(1)* Essential (main) property (MUST)
- *(2)* Name and reference of the KMS
- *(3)* Advantages (√) and Disadvantages (×)

Additional PRO: public-key crypto?

Symmetric vs. Asymmetric Crypto

- Open discussion regarding scalability issue, key distribution, key management, communication with external parties, etc.
- The use of public key cryptography would eliminate the need for complicated protocols.
- The challenge is to overcome the considerable computational complexity of standard public key encryption algorithms and make public key encryption possible in self powered sensor nodes.
- Any solutions?

Statements regarding PKC in WSN

"Many current sensor devices have limited computational power, making public-key cryptographic primitives too expensive in terms of system overhead"

Communications of the ACM, June 2004

"Public key cryptography is prohibitively expensive for sensor networks in terms of computation and energy consumption"

ACM Conference on Embedded Networked Systems, Nov. 2004

"Traditional public key cryptography is not going to work in this environment"

ISC'05 Keynote: *Security in Sensor Webs*, Sept. 2005

Emulation of asymmetric crypto primitives

- Protocols like SNEP and μTESLA provide secure authentication using only symmetric key techniques
- In order to provide authentication to insecure nodes μTESLA has to emulate asymmetry through a delayed disclosure of symmetric keys
- The emulation of an asymmetric cryptographic primitive requires that is each node:
  - is time synchronized with the base station
  - has key management functions
  - has ample storage

Emulation of asymmetric crypto primitives

- Keys shared among all nodes need to be updated in regular intervals
  - Requiring broadcasts from the base station to all nodes
  - As in many settings the base station can not directly communicate with all nodes, these keys need to be forwarded from node to node
  - There is a protocol overhead (increased energy consumption of the nodes) as keys and key management messages need to be transmitted frequently
- Complex key management and high storage requirements for multiple keys and messages put a considerable burden on the power consumption of the nodes.

Optimization: hardware/architecture

- There are some experiences where cell phones, PDAs, etc. use efficient elliptic curve based algorithms which execute faster than traditional schemes
  - like RSA or ElGamal
  - while preserving the same level of security
- Gaubatz et al. consider that this comes at the price of much more complex arithmetic primitives
  - The heterogeneous structure and larger storage requirements of ECC makes it less scalable
  - And less attractive for energy efficient low-power implementations

Optimization: hardware/architecture

- Therefore, they propose a custom hardware assisted approach using:
  - Right selection of algorithms
    - Rabin's scheme
    - NTRUEncrypt
  - Right selection of associated parameter
    - Depending on the application it is possible to fix the public key to a constant value
  - Careful optimization
  - Low-power design techniques

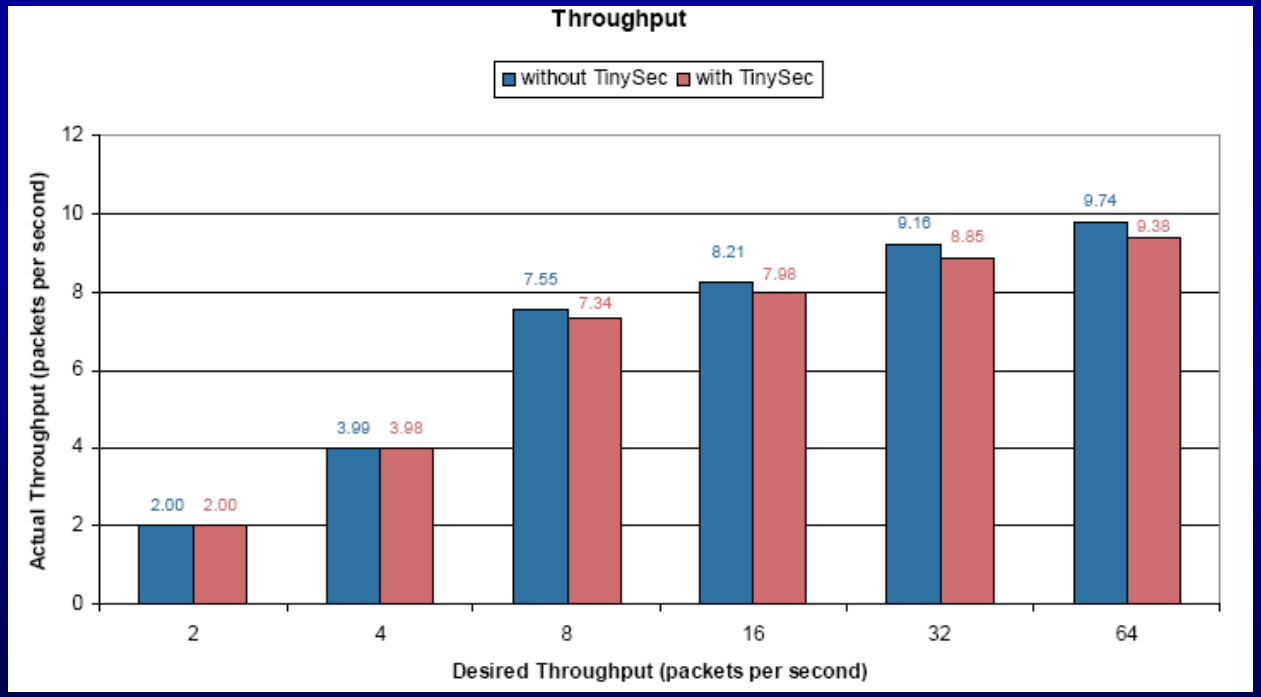
Optimization: hardware/architecture

- Two architectures, each implementing one of previous algorithms

	Rabin	Ntru
Equivalent security	60 bits	57 bits
Area (equ. gates)	16725	2850
Delay (avg. #cycles)	1440	29225
Avg. power @500kHz	148.18 µW	19.13 µW
Throughput (encrypted)	177.8 kbits/s	4.52 kbits/s

Optimization: Algorithms

- TinyOS offers MICA2 security capabilities through TinySEC (link layer security mechanism based on Skipjack)
- Impact on TinySec on MICA2's performance is reasonable



Optimization: Algorithms

- However, key distribution for applications based on MICA2 is still a problem.
- Thus, Malan et al. provided the first implementation of ECC for sensor networks, based on MICA2 mote.
  - Proved that D-H performance was slow.
  - Tried with two different ECC implementations.
    - Main result: public keys generated within 34 seconds.

Optimization: Algorithms

- However, Blaβ et al. have recently performed another implementation of asymmetric encryption and signature generation schemes for the MICA2 platform.
- The implementation is also based on elliptic curve cryptography.
  - Algorithms like Diffie-Hellman, El-Gamal and DSA based on ECC, offering the same security but less memory and computing power.

Optimization: Algorithms

- Optimization key points:
  - Saving memory by moving unchangeable data from RAM to flash-ROM or EEPROM (supported by MICA2 platform)
    - Offline precomputation and pre-deployment distribution of the constant multiplication matrix of ECC (saves 22% of RAM)
    - The same for field inversion operation (saves additional 28% of RAM)
  - Handcrafting the source code for the target platform
    - Avoiding loop checks
    - Moving outside the loops computations that do not change
    - Etc.
- Result: A total of 73KBytes of flash-ROM is permanently used for ECC operations (approx. 57%)
  - 55KByte for normal sensor code

Optimization: Algorithms

Operation	Time [s]	Malan et al. [est. s.]
Point multiplication (fixed)	6.74	~34
Point multiplication (random)	17.28	~34
Key generation	6.74	~34
Complete D-H key exchange	17.28	~68
El-Gamal encryption	24.07	~68
El-Gamal decryption	17.87	~34
ECDSA signature	6.88	~34
ECDSA verification	24.17	~68

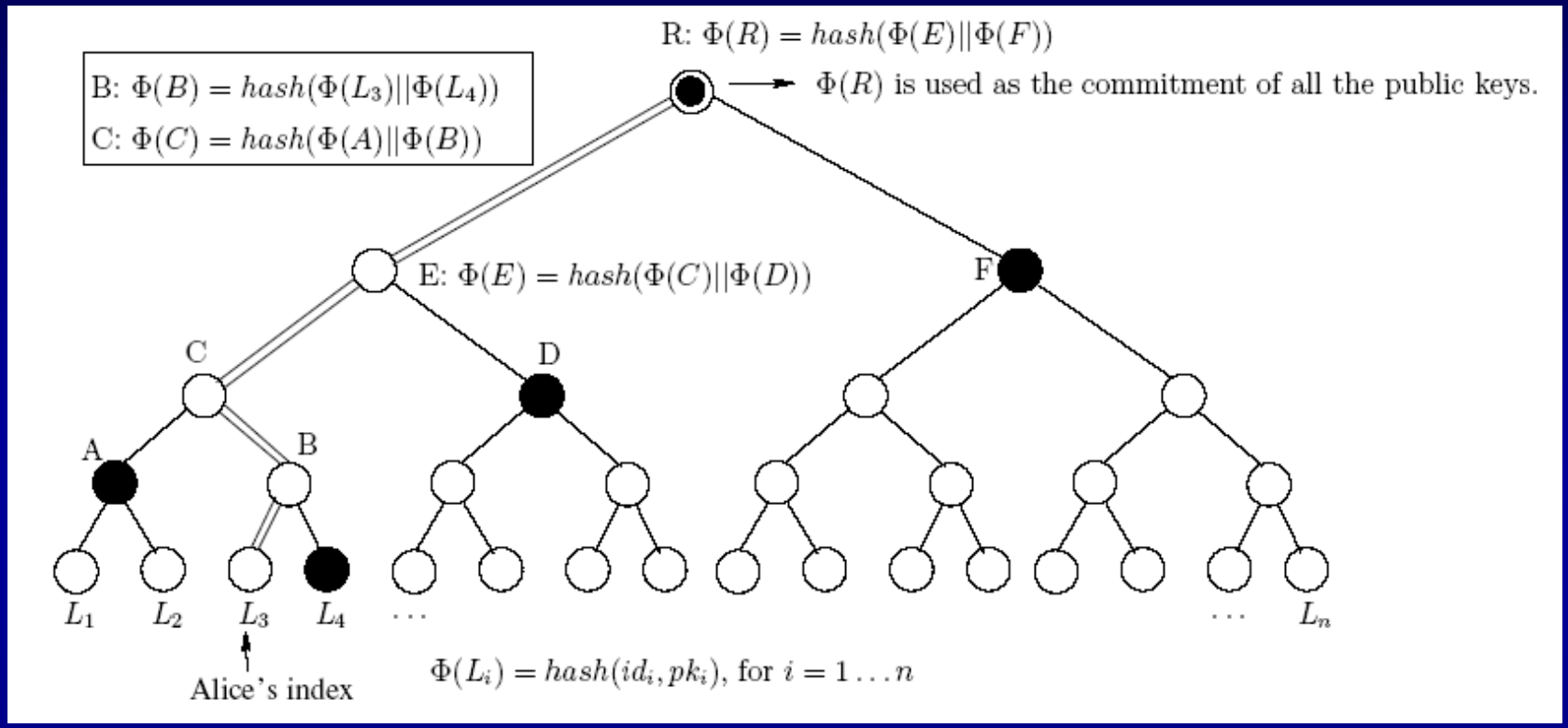
Optimization: network properties

- Du et al claim that previous results show that PKC is close to being practical in sensor nodes, but still expensive in terms of energy consumption
  - Underlying point: it is necessary to maximize the lifetime of sensors.
- Main idea:
  - Certificates are meant for user with no pre-established trust relation, but if users meet, they can interchange public keys personally.
  - Sensor nodes meet each other during the deployment phase because they usually belong to the same administrative entity, thus, they can exchange public keys securely.

Optimization: network properties

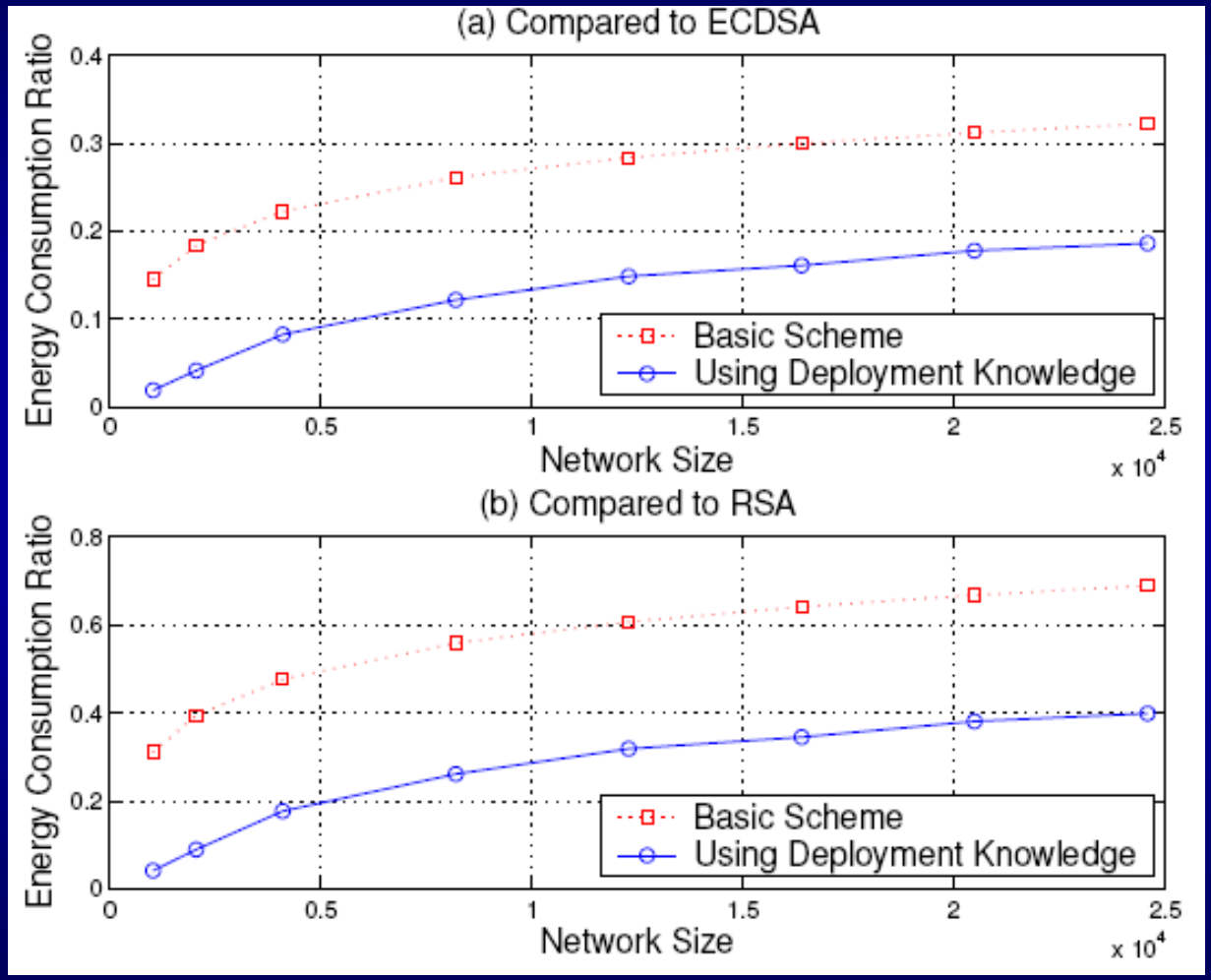
- Naive solution: Each node stores all other nodes' public keys.
  - Problem: Not enough memory on the sensor.
- Improved naive solution: Each node stores one-way hash values of all other nodes' public keys
  - Later, when A sends to B her public key, B checks that the hash value is the same one that he stores.
  - This means to replace public key authentication with symmetric key operations (using one-way hash functions).
  - Problem: Still not enough memory for large networks
- Memory-efficiency solution: Use Merkle tree technique for memory usage problem.

Optimization: network properties



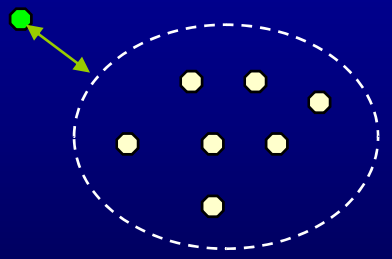
- Each leaf corresponds to a sensor node and contains the bindings between its identity and public key
- In comparison with the naive solutions, the communication overhead is increased (L x log N)

Optimization: network properties



PKI-like

- Watro et al.[6] propose TinyPK for authentication and key exchange between an external party and a sensor network.
- In order to make TinyPK practical, protocols require only public key operations on the sensor.
  - TinyPK is based on RSA cryptosystem, using e=3 as the public exponent.
    - The basic public operation is to cube a 1024-bit number and to take its residue modulo a large prime.

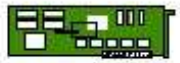


PKI-like

- TinyPK requires a Certification Authority.
- Every node is pre-installed the CA's public key.
- Any external party that wishes to interact with the nodes also requires its own public/private key pair
  - And must have its public key signed by the CA's private key, thus establishing its identity.
- The scheme does not make use of certificates because nodes are assumed to not have enough processing power to make use of certificates
  - No real-time access to the CA infrastructure.
  - No revocation issues
- Protocol based on challenge-response

PKI-like

External Party (EP)



PK Mote

{EPuK} CA Pvt Key → Cyphertext1*

{ nonce, checksum of EPuK}EP Pvt Key → Cyphertext2

Send Cyphertext1 + Cyphertext2 ⇒ Collect messages

Missing msg

{Cyphertext1} CA Pub Key → EPuK

{Cyphertext2}EPuK → nonce, checksum

Calculate checksum of EPuK

Verify checksums equal — Bad signature

Verify nonce > old nonce — Wrong nonce, replay attack

{nonce, TinySec key} EPuK → Cyphertext3

Send Cyphertext3

Collect messages

Missing msg

{Cyphertext3}EP pvt Key → nonce, TinySec key

Verify correct nonce

Write TinySec key to ~/.keyfile

Load TinySec to attached Mote

Legend

{A }B → C:

A transform to C using B.

EPuK: External Party Public Key

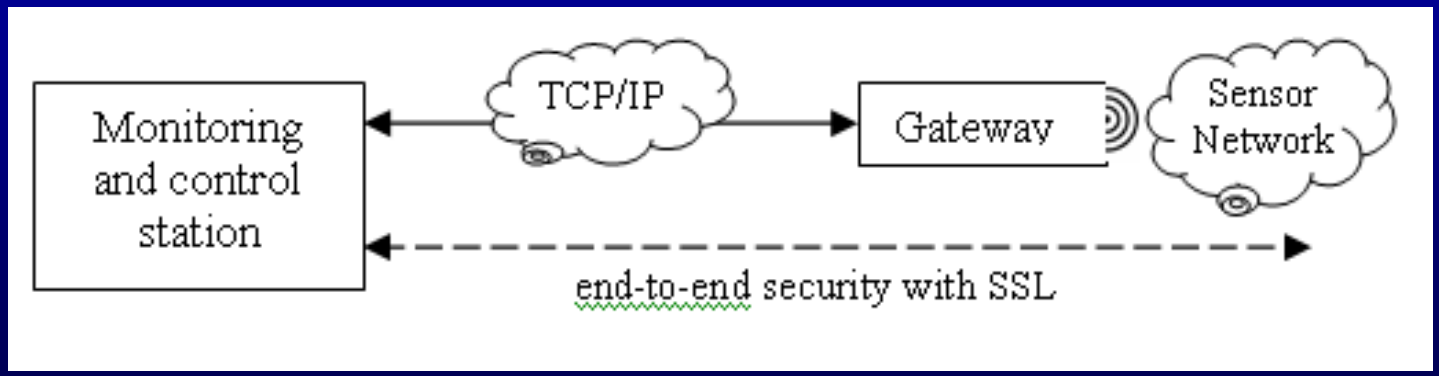
*: Cyphertext1 will be pre-loaded on real deployment

Approach: End-to-End Security

- Gupta et al. have recently developed Sizzle ("Slim SSL"):
  - A secure web server stack that runs on the Mica2dot mote.
- Goal: embed a secure web server in an array of tiny devices while using a web browser as the monitoring/controlling application.
- Scenarios proposed range from home appliances to personal medical devices, where monitorization is done via Internet.

Approach: End-to-End Security

- Devices in the WSN are connected via a gateway.
- The secure web server within each device of the WSN is mapped to different TCP ports at such gateway
  - from where access to the sensor nodes is controlled.
- The connection from the gateway to the nodes uses a special purpose simple and reliable protocol



Approach: End-to-End Security

- Based on highly optimized, assembly language implementations of PKC
  - and integrates ECDH and ECDSA in SSL.
- Uses a persistent HTTP connection
  - keeps the TCP connection open for a configurable duration so that other arriving requests are serviced in the same connection.
    - saves CPU time and memory,
    - reduces network congestion,
    - improves response time
- Makes use of an abbreviated SSL handshake.

More Security Issues

Routing

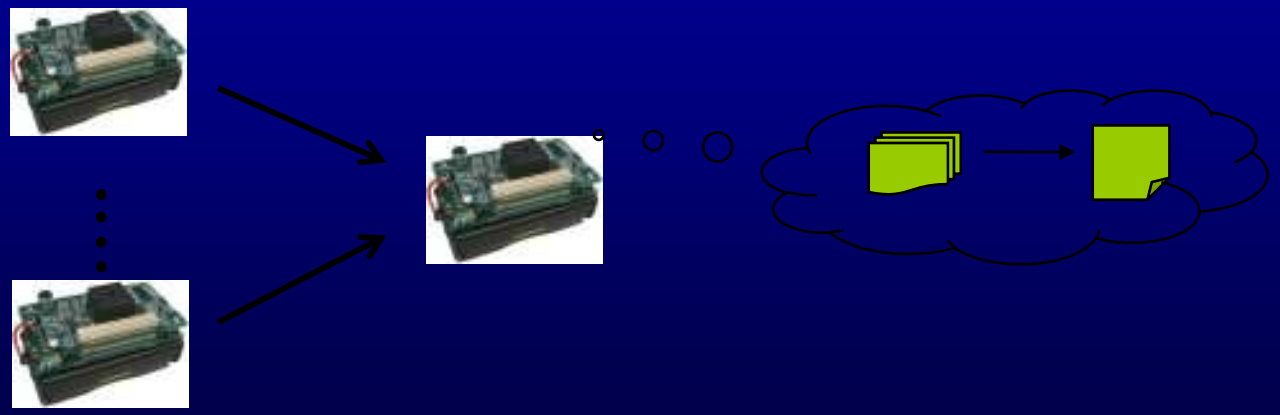
- Maximum transmission distance of current generation of sensor nodes ranges between 100 and 300 mts
  - Thus, messages can not be transmitted directly between any two nodes
  - A routing infrastructure is needed
- Algorithms should work:
  - Even when nodes start to fail due to energy issues
  - With any network size and node density
  - Providing a certain quality of service
  - Minimizing the memory usage, speed and energy consumption
- And Security must be considered!!!

Secure Routing

- Key infrastructure may help in the defense by authenticating nodes and protecting the routing infrastructure, but this is not enough:
  - Malicious nodes and denial of service still possible
- It is essential to make the routing algorithm robust against attacks
- Some work that focus on protection of existing routing protocols
- Others focus on designing new protection techniques
- Challenge: (almost) no protocols with security in mind from scratch!

Secure Aggregation

- Main purpose of Sensor networks: Send data to users
  - Large amounts of raw data
  - Dense networks => Redundant data
- Costly! (energy, time,…). Solution: Aggregate (summarize) data
  - (Data, Data, … , Data) → Report
- Who? Aggregators (Cluster heads, Special nodes,…)



Secure Aggregation

- Aggregation is prone to be attacked
  - Normal
    - Data injection, Data integrity
  - Internal adversaries
    - False Data (Nodes)
    - False Reports (Aggregator)
    - Data on Transit (Routing)

Auditing

- User/Admin can only access to Base Station (directly or not)
  - Base station only collects data from nodes
  - Impossible to know, for instance, state of the nodes (energy!)
- Solution: Audit subsystem
  - Able to inform about the internal state of a node/group
- Based on audit information: Intrusion Detection Systems
  - IDS: Monitor network, detects problematic situations, alerts users
  - Tools: Anomaly detection, Misuse detection
- Challenge: Provide IDS solutions

Privacy

- Two types of privacy
  - Network Privacy
    - Privacy of the network itself (nodes, information)
    - Sometimes important (battlefield), sometimes not (earthquake)
  - Social Privacy
    - Privacy of the subjects under surveillance

Privacy

- Threats to network privacy
  - Content Privacy
    - Meaning of a communication exchange? Messages, Context
  - Identity Privacy
    - Deduce identities of nodes in a communication
  - Location Privacy
    - Infer (or approximate) physical position of node
- Nodes will get smaller, cheaper…
  - Easy to create “surveillance” network
  - Get data about subjects at a “safe” distance
  - Automatic data collection, analysis and event correlation!

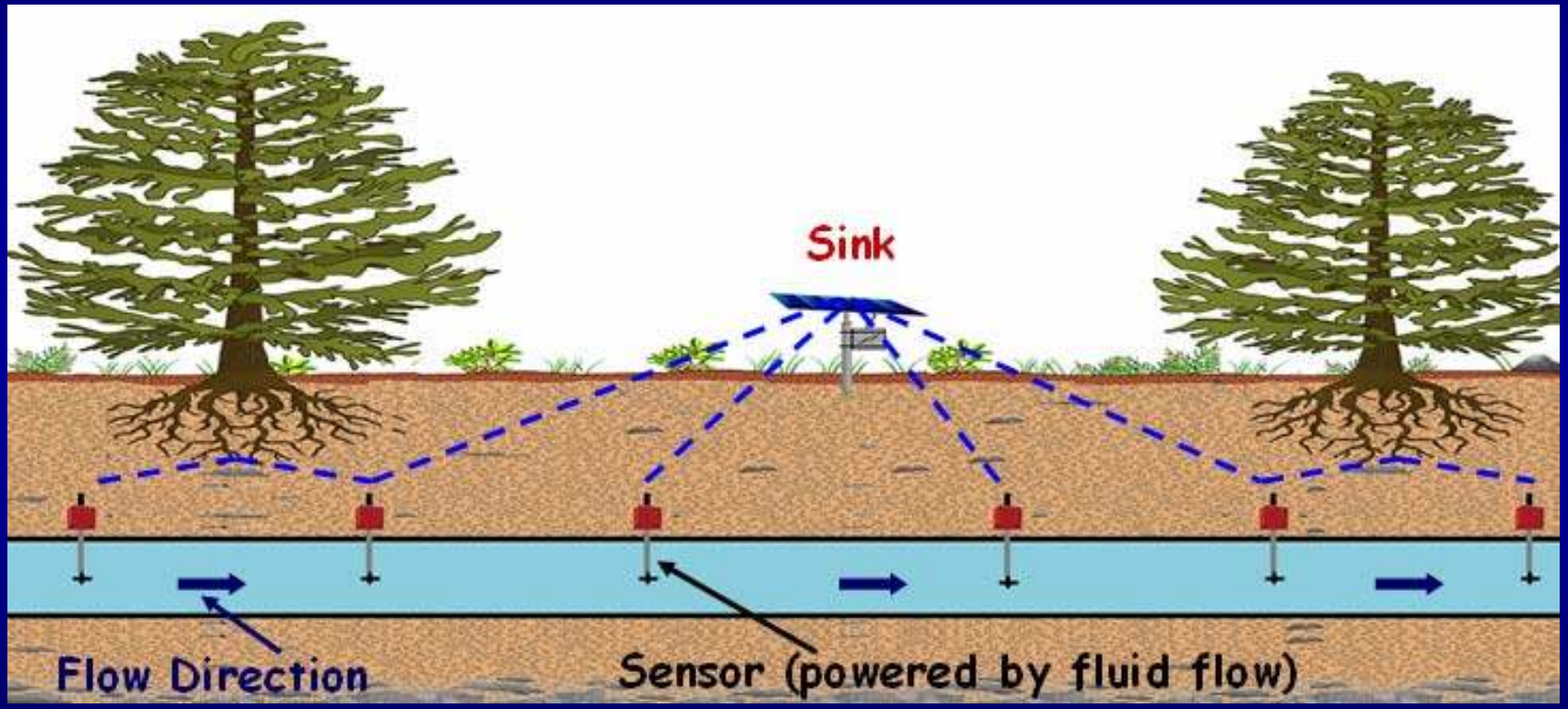
Other Issues

- Mobile Agents
  - Could be useful on a Sensor Network context
  - Constrained environment, no protection
- Delegation between the Base Station and the Sensor Nodes
  - All previous cases: static environments
- Automatic reaction against external/internal problems
  - Denial of Services attacks
- Challenges: All above

Further scenarios

Underground sensor networks

Underground sensor networks



Underwater sensor networks

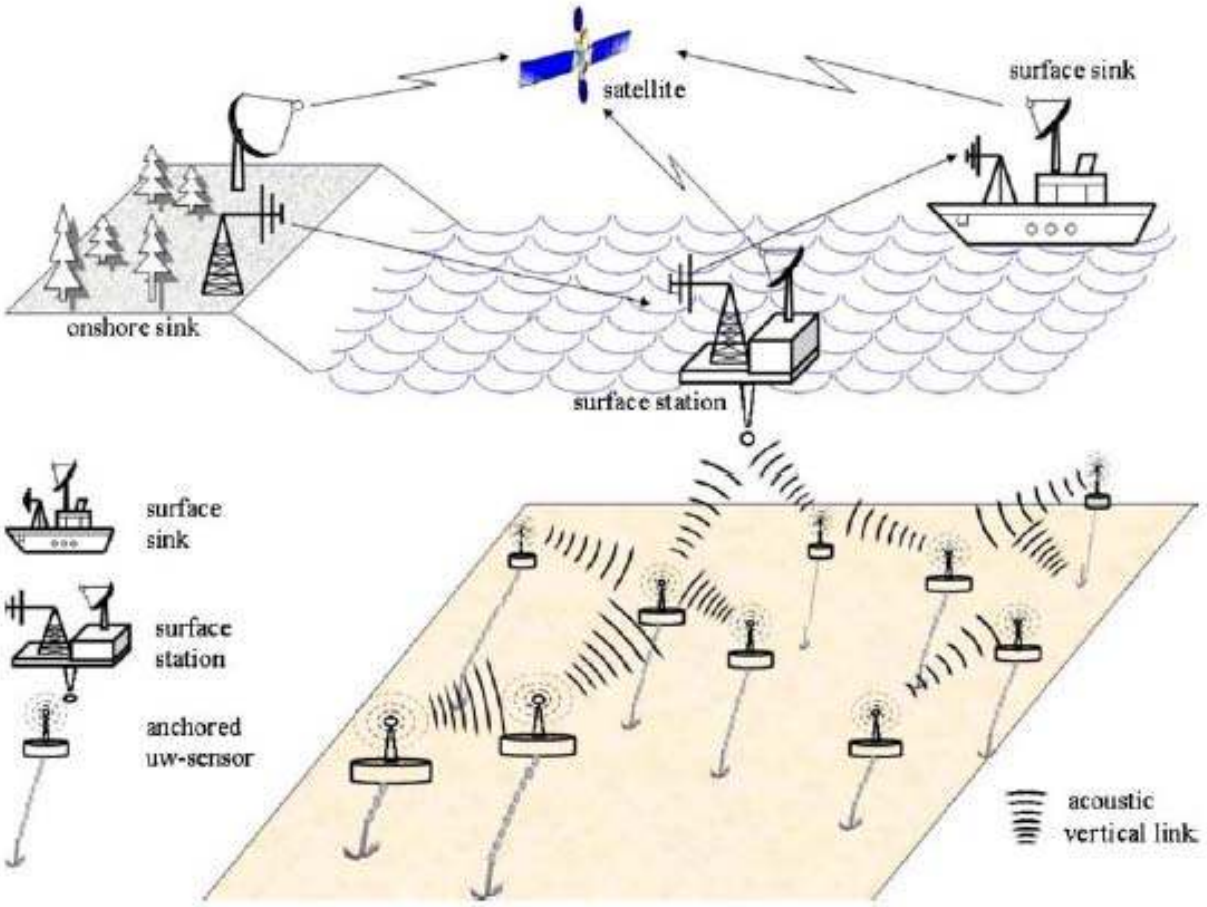
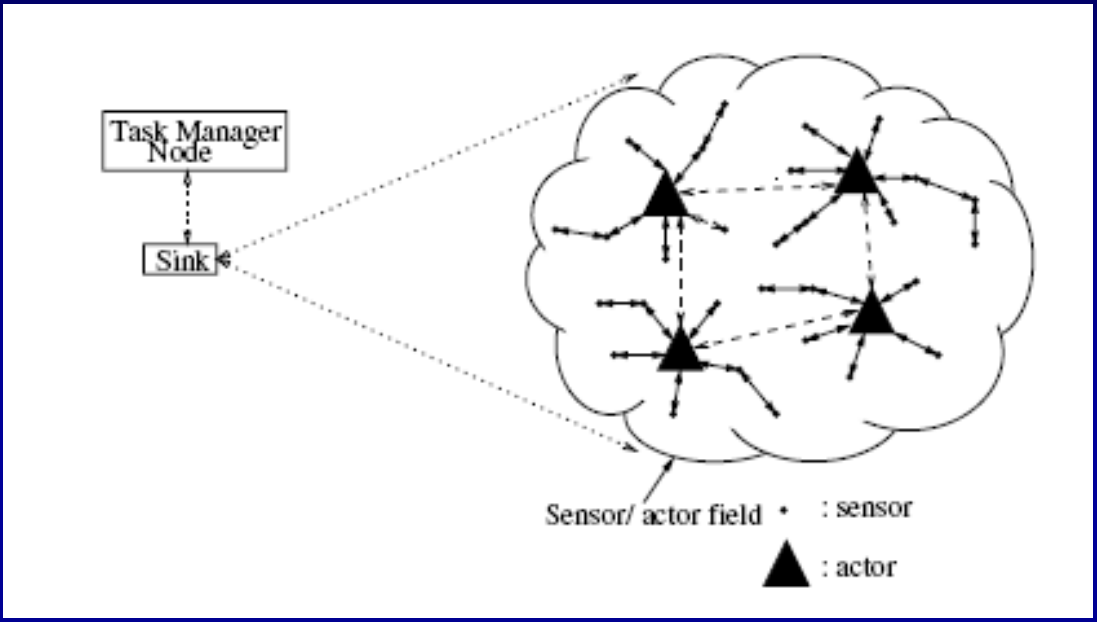


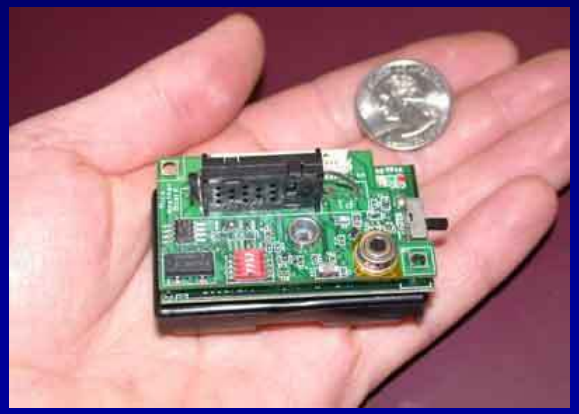
Fig. 2. Architecture for 3D underwater sensor networks.

Wireless Sensor and Actuator Networks

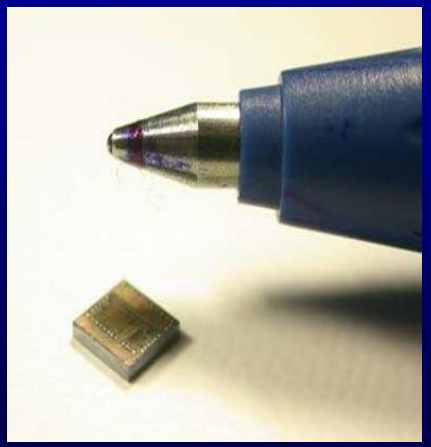


Final remark

Final remark




MEGA128L




IN GOD WE TRUST
LIBERTY
2001
D


CENT

Thanks for your attention!

Javier Lopez
Computer Science Department
University of Malaga
Spain

jlm@lcc.uma.es