Critical Infrastructures Protection

Javier Lopez

Computer Science Department

University of Malaga, Spain

Outline (1st part)

- The Landscape
- New vision of Security
- European Perspective
- Applications and Technology
- Critical Infrastructures Protection (CIP)
- CIP Sectors
- Critical Information Infrastructures (CII)
- European Initiatives
- Underlying Technology
- Projects

The Landscape

- Globalization is multiplying and strengthening links among countries, and fostering the integration into an emerging global society.
- Political, social, economic and technological developments have created a fluid environment and new opportunities
  - However, 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

- More precisely, conflicts in remote regions can destabilize the international order and directly affect any country's security and interests.
  - The growing dependence on interconnected infrastructures in
    - Transport,
    - Energy,
    - Information,
    - etc.

    increases the vulnerability of modern societies.

The Landscape: New vision of 'Security'

- At the same time, the natural diffusion of technological know-how resulting from scientific and industrial development facilitates that technological advancements are used malevolently.
- Security is compromised, directly or indirectly, by global challenges, thus:
  - in Europe and elsewhere, the evolving global situation and some shocking events have profoundly changed the understanding of the term 'Security'.

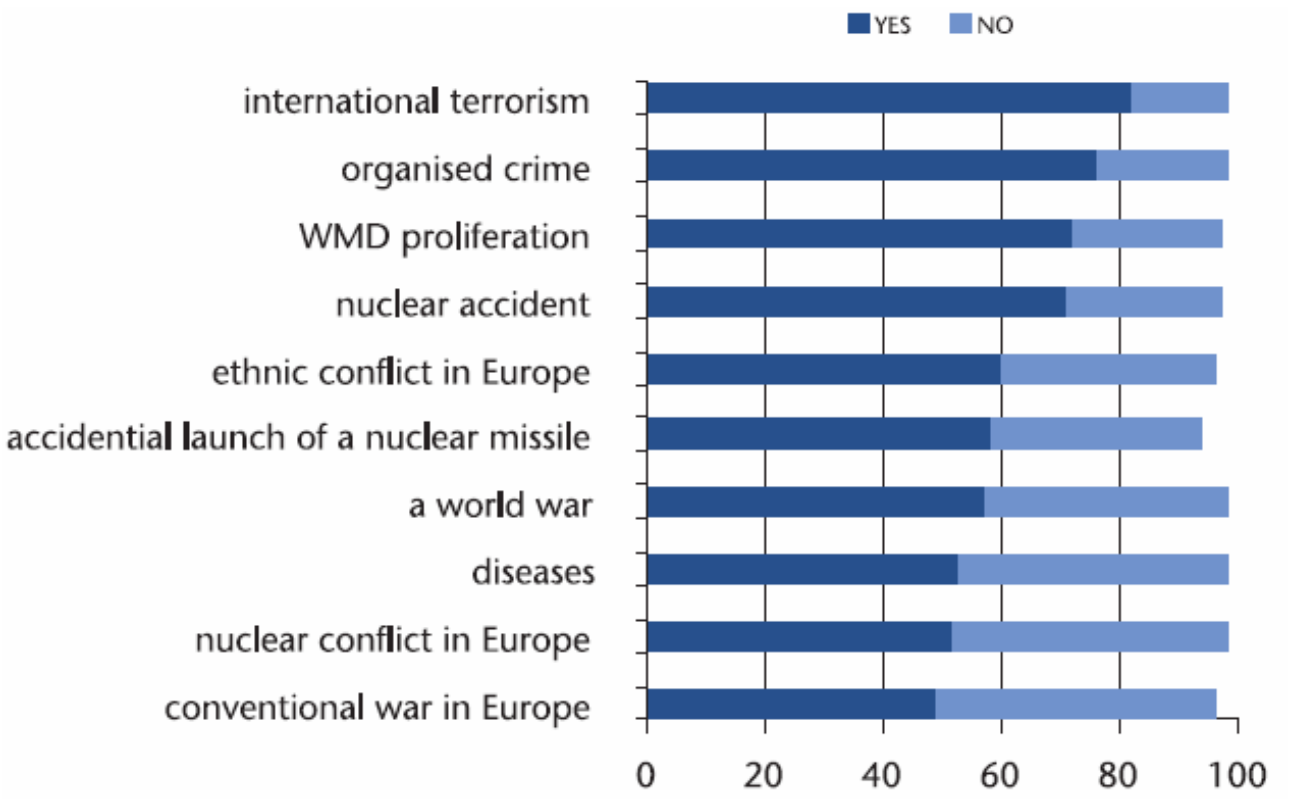
The Landscape: New vision of 'Security'

- 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: New vision of 'Security'

- What do European citizens fear?



Security and its Implications

- Terrorist attacks have brought about a new sense of vulnerability.
- 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!!

European perspective

- There is a major challenge for the formation of Security policies and a need for common European answers.
- As mentioned, current threats ignore national borders and can damage European interests at home and abroad:
  - the distinction between "external security" and "internal security" becomes increasingly indistinct.
  - thus, there is a need for the EU to develop a comprehensive approach that links the external and internal dimensions of security.

Role of Technology

- Technology is a key 'force enabler' for a more secure Europe
  - technology itself cannot guarantee security, but security without the support of technology is impossible.
- Moreover, the technology base for defense, security, and civil applications increasingly forms a continuum,
  - across this continuum, applications in one area can often be transformed into applications in another area,
  - and it is possible to combine the use of civil and military means.
- However, all this makes the provision of security an extremely complex management task.

Threats, missions, capability

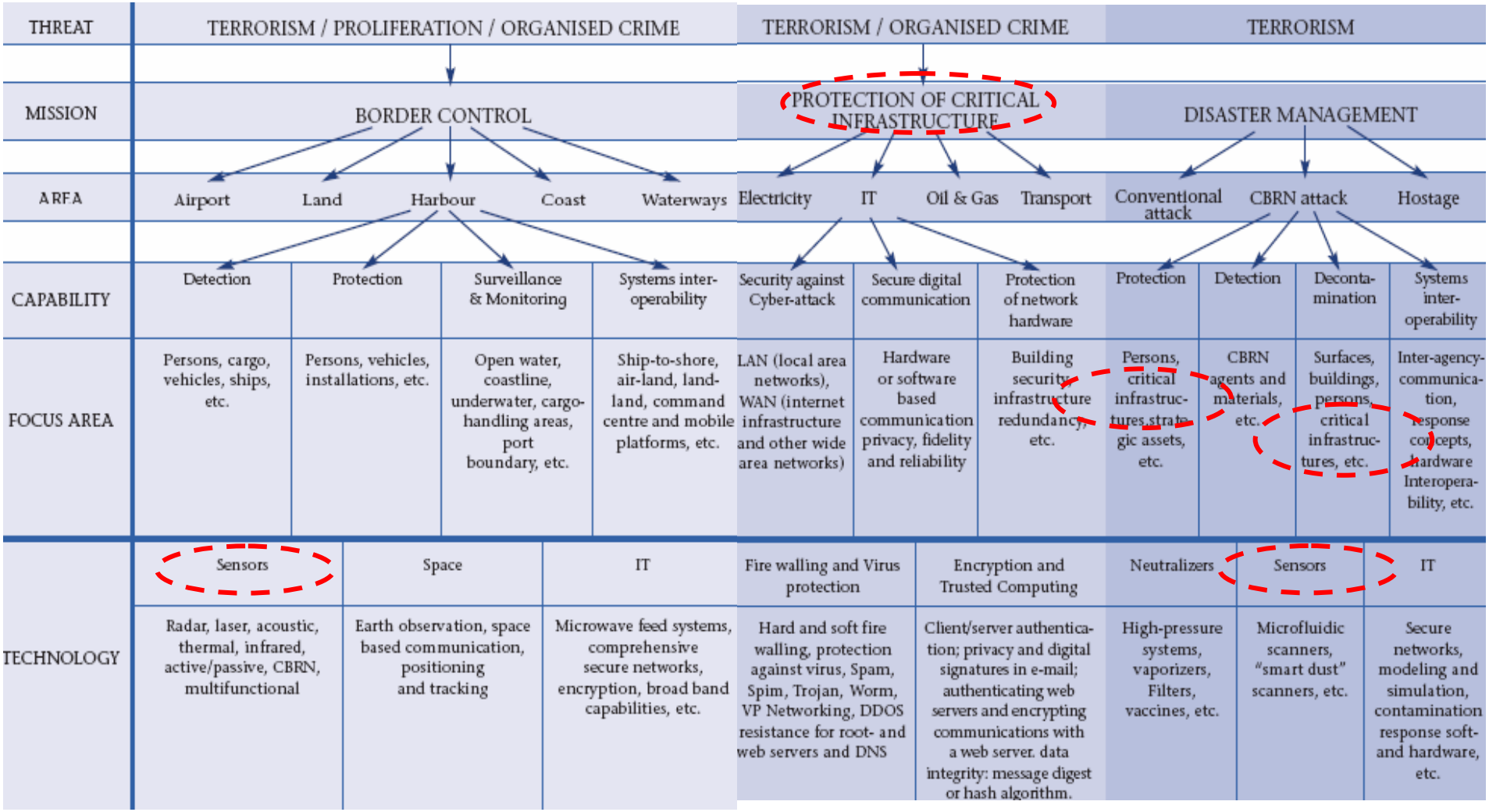
- Some examples of the link between threats, missions and capability needs are enough to show that:
  - Although each threat may have its specificities, an effective defense against them will often require the same missions.
  - It is also clear that many capabilities serve internal and external as well as military and non-military purposes.

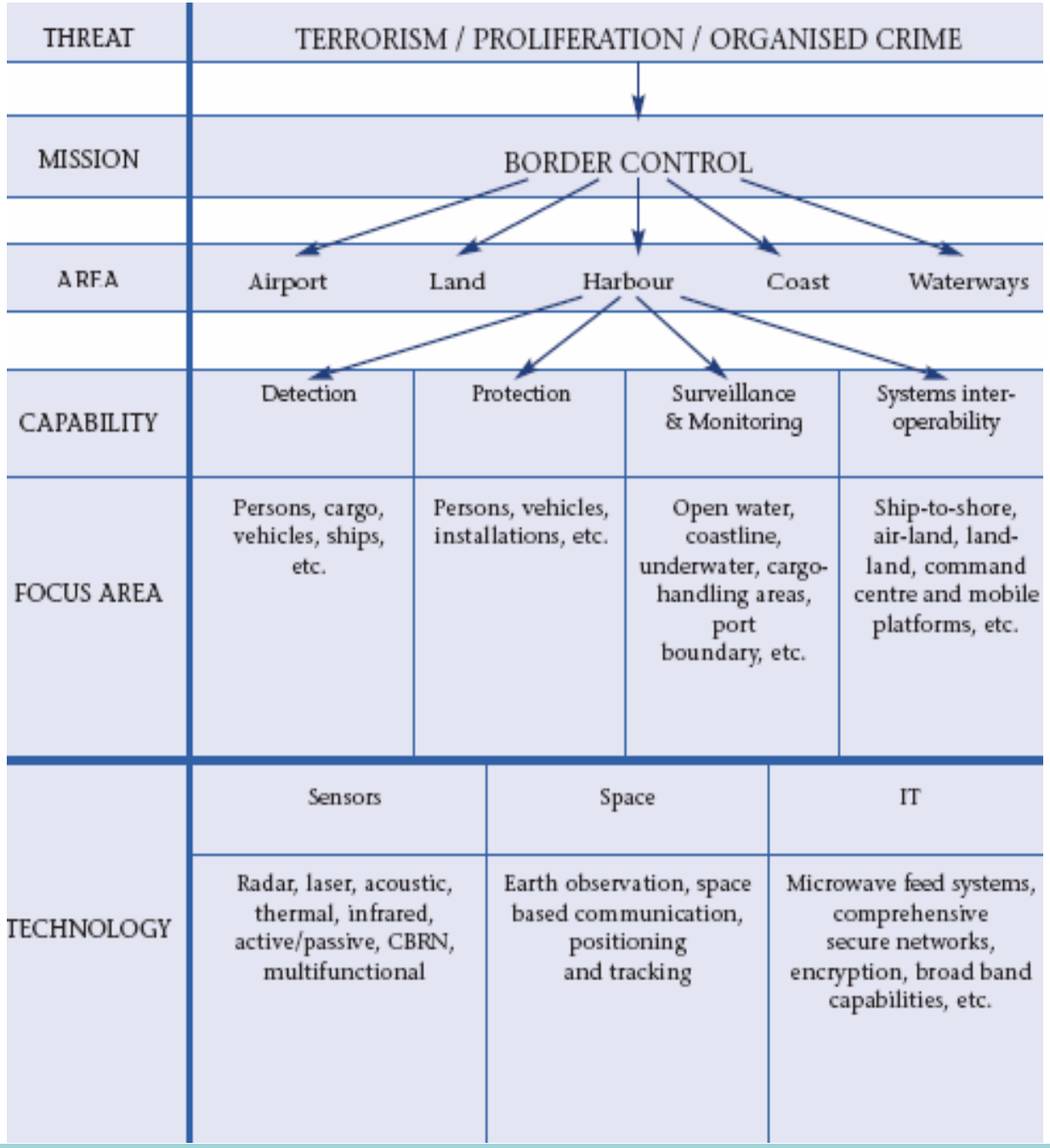
		International Terrorism	Organized Crime	Proliferation of WMD
Missions	Protection of Critical Infrastructure	X	X	
	Border Control	X	X	X
	Civil Defence/Protection	X		
	Disaster Management	X		
	Law enforcement (Arrests / Neutralization)	X	X	X
	Law enforcement against trafficking	X	X	X
	Law enforcement against financial crimes	X	X	
	Treaty verification			X
	Export control			X
Capabilities	Intelligence	X	X	X
	Assessment and Analysis	X	X	X
	Surveillance (of borders and critical sites)	X	X	X
	Monitoring (of trade and financial flows)	X	X	X
	Secured Communications	X	X	X
	Identification (IDs, access control)	X	X	
	Detection (persons, CBRN, explosives)	X	X	X
	Disposal (explosives, CBRN)	X		X
	Decontamination	X		
	Modeling/Simulation	X	X	

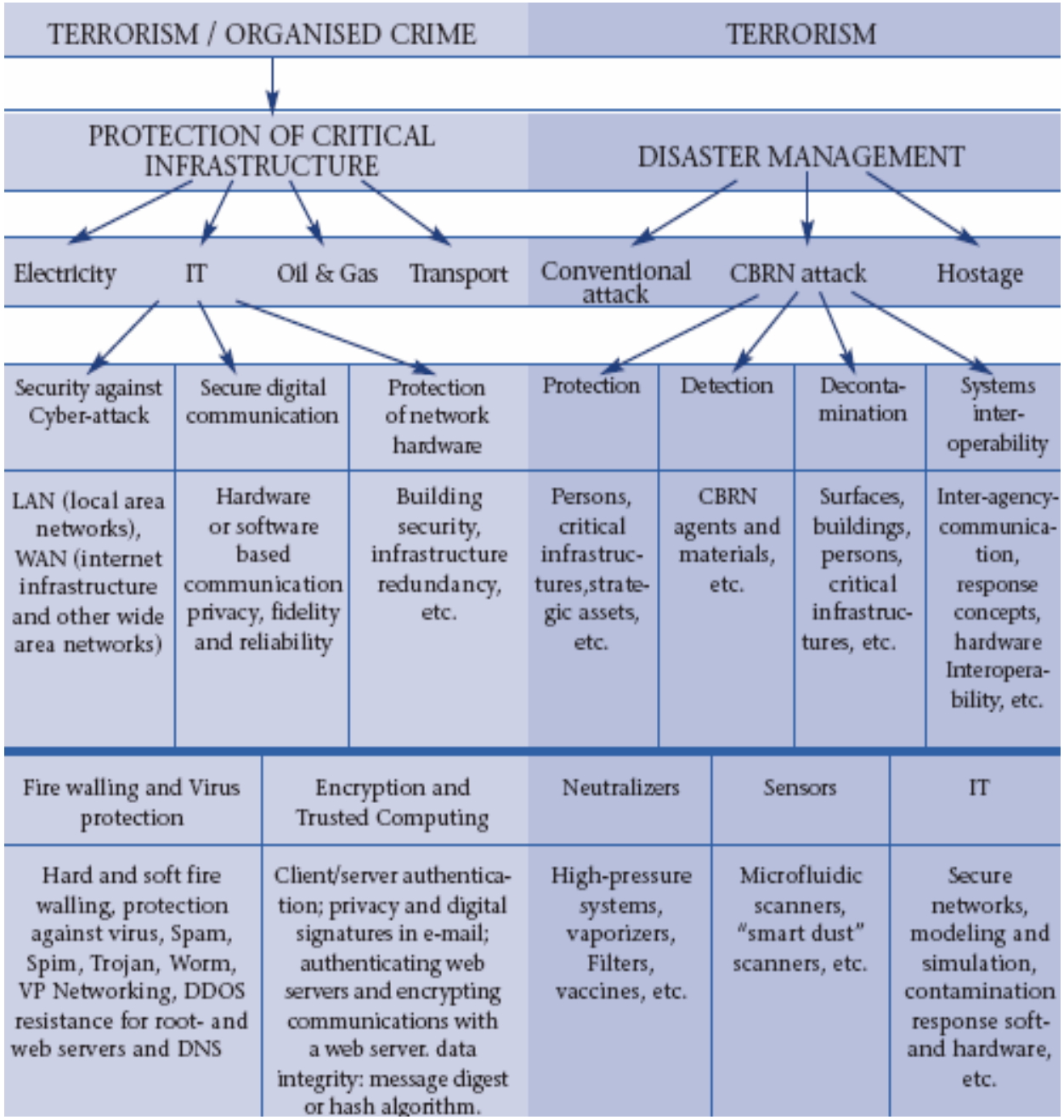
Capability, Technology and Applications

- The following figure goes one step further and gives some examples of how a capability-related approach can help to identify more specific applications and technologies.

Capability, Applications and Technology




THREAT
TERRORISM / PROLIFERATION / ORGANISED CRIME
MISSION
BORDER CONTROL
AREA
Airport
Land
Harbour
Coast
Waterways
CAPABILITY
Detection
Protection
Surveillance & Monitoring
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.
TECHNOLOGY
Sensors
Space
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.


TERRORISM / ORGANISED CRIME
TERRORISM
PROTECTION OF CRITICAL INFRASTRUCTURE
DISASTER MANAGEMENT
Electricity
IT
Oil & Gas
Transport
Conventional attack
CBRN attack
Hostage
Security against Cyber-attack
Secure digital communication
Protection of network hardware
Protection
Detection
Deconta-mination
Systems inter-operability
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.
Fire walling and Virus protection
Encryption and Trusted Computing
Neutralizers
Sensors
IT
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)

CIP Sectors

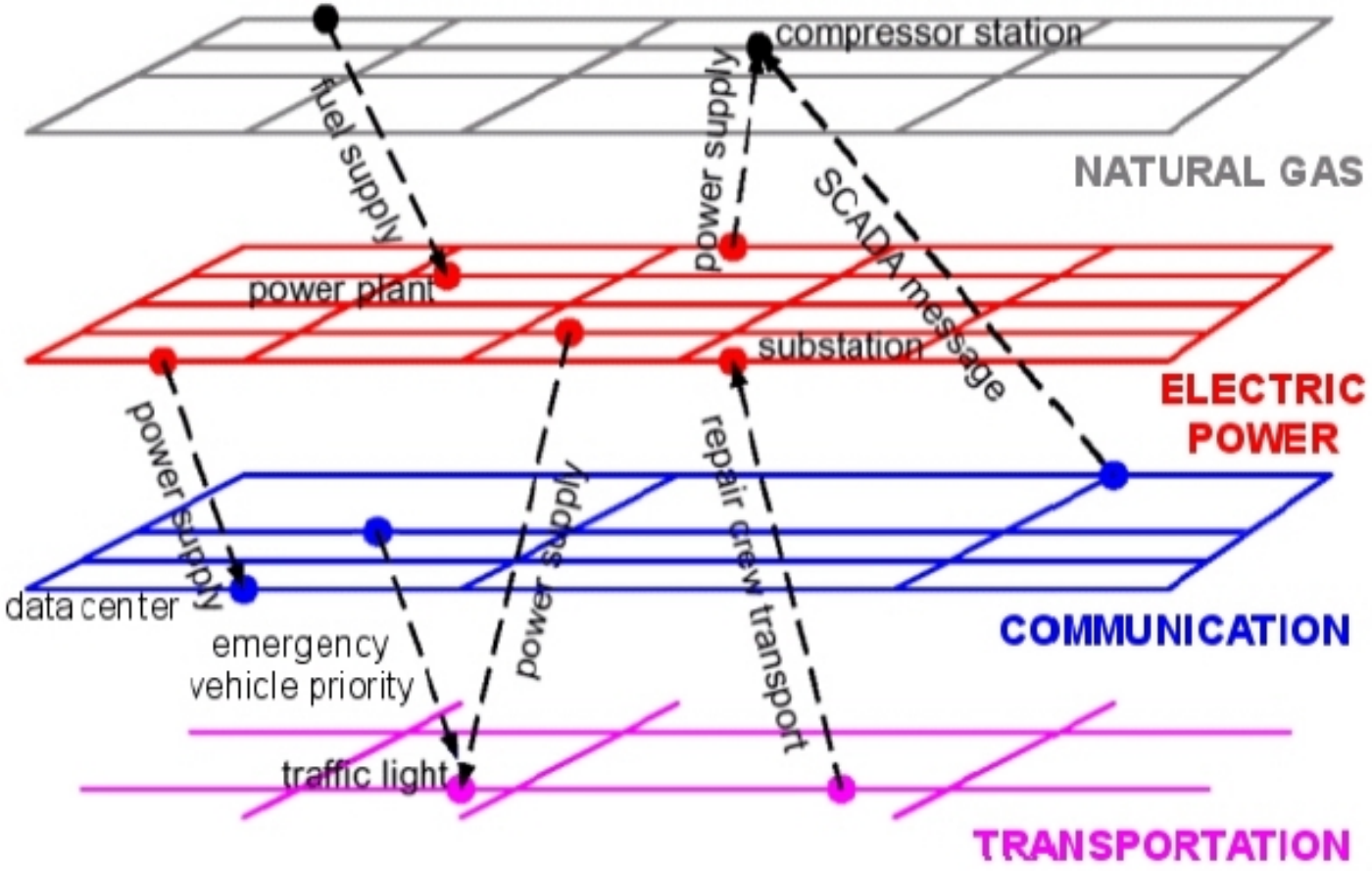
- Some critical elements in these sectors are not strictly speaking 'infrastructure'
  - but are in fact, networks or supply chains that support the delivery of an essential product or service.
- These infrastructures are owned or operated by both the public and the private sector.
- However, the Commission 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 on the industrial control systems of critical infrastructure could vary widely.
- It is commonly assumed that a successful cyber attack would cause few, if any, casualties, but might result in loss of vital infrastructure service.
  - For example, a successful cyber-attack on the public telephone switching network might deprive customers of telephone service while technicians reset and repaired the 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.

Consequences in CIP Sectors

- Europe's CI are highly connected and highly interdependent because of:
  - corporate consolidation,
  - industry rationalization,
  - efficient business practices
  - population concentration in urban areas, etc.
- Therefore, another type of failure might be when one part of the infrastructure leads to the failure of other parts, causing widespread cascade effect.


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 (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

- 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

- 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.

Underlying Technology

- In CII, all organizations must attempt to protect their business systems and control centers from cyberattacks
  - but plant control systems, substations, distribution centers, etc. might not be adequately protected,
    - thus allowing the penetration of mission-critical operational systems via unsecured access points.
- 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.

Underlying Technology

- CII are characterized by unique requirements for communications performance
  - including timing, redundancy, centers control and protection, and equipment control and diagnostics.
- Although strong centralized control is essential to reliable operations, CII require:
  - multiple high-data-rate communication links,
  - a powerful central computing facility,
  - and an elaborate operations control center.
- All of them are especially vulnerable when they are needed most —during serious system stresses or disruptions.

Underlying Technology

- 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 (WSN) is the technology that better fulfills features like the ones required by CII.

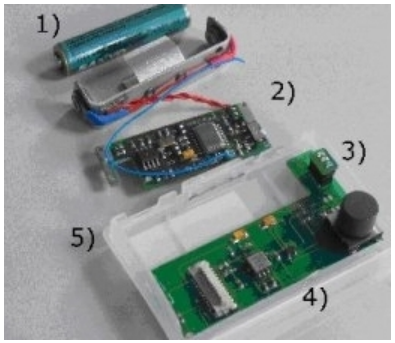
CIBIS

- 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.

CIBIS

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

1 Storage limit exceeded?
2 Confirmation of safe storage environment
3 Incompatible Goods

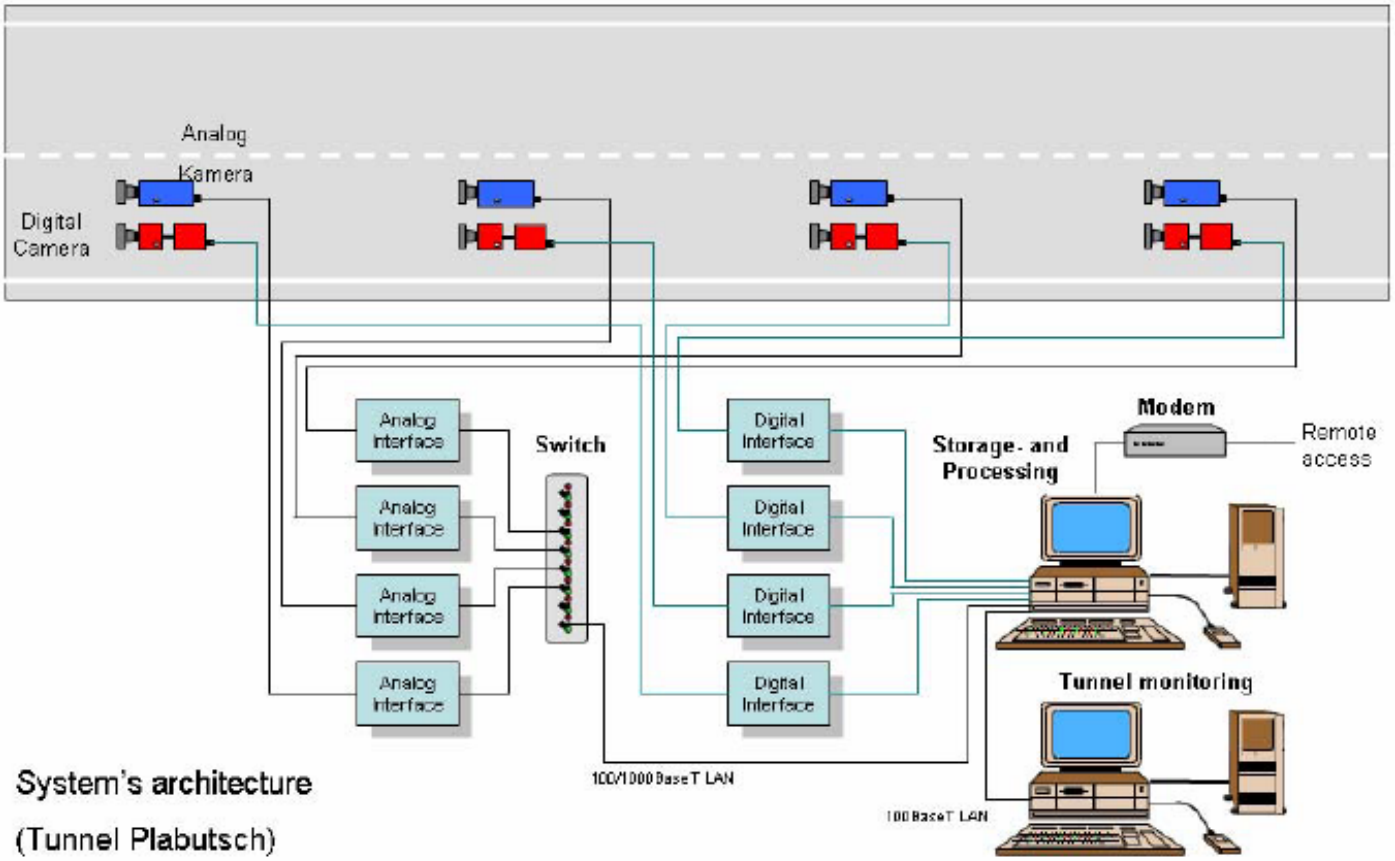


VITUS

- 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

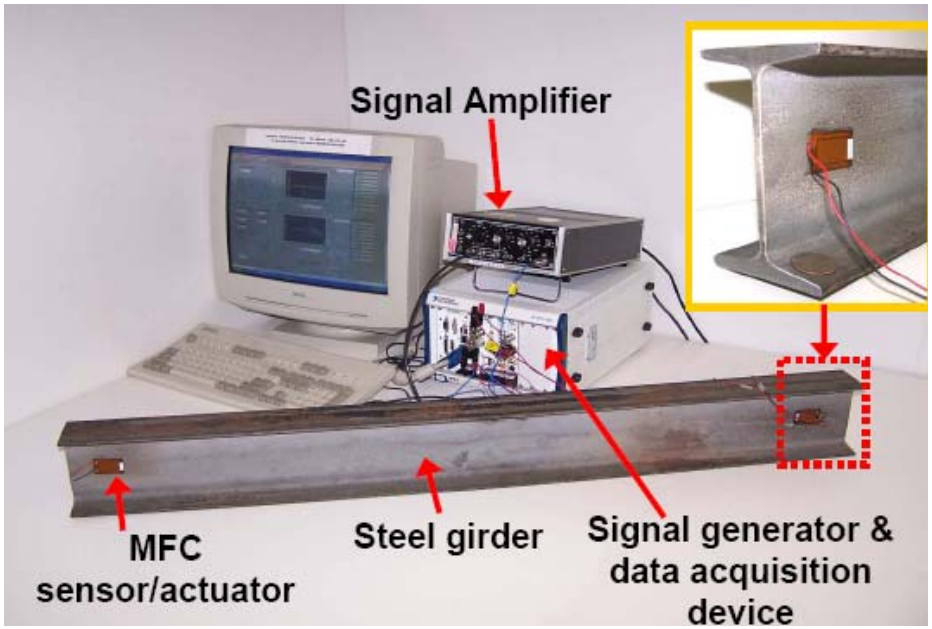
- The Center for Sensed Critical Infrastructure Research aims at delivering cost-effective, sensor-based monitoring systems for a broad range of critical infrastructure applications.
- These monitoring systems could be used for:
  - decaying bridges,
  - oil and gas pipelines,
  - unstable electric power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

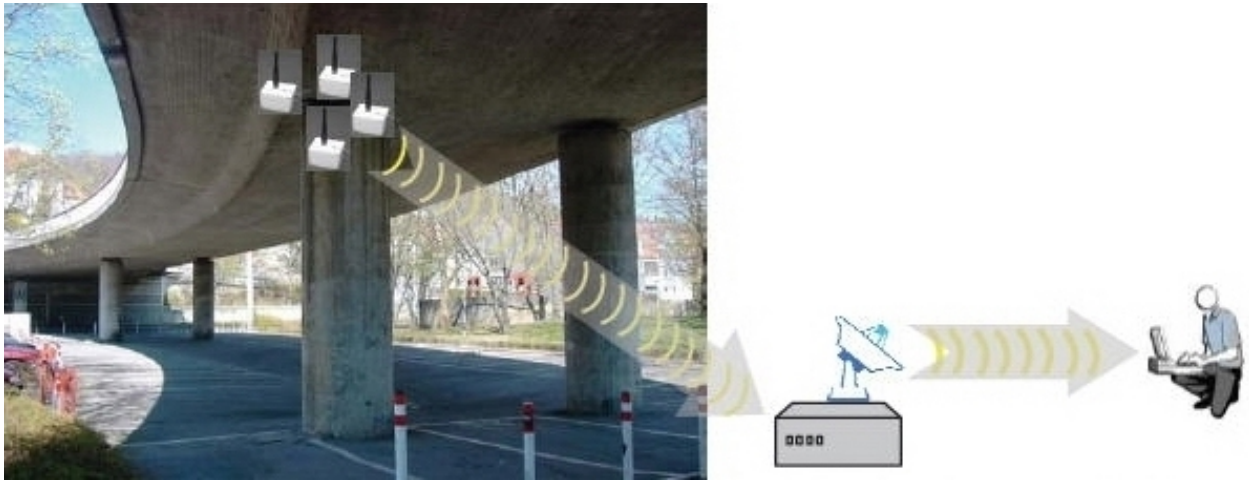
CenSCIR

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

CenSCIR (and Sustainable Bridges)

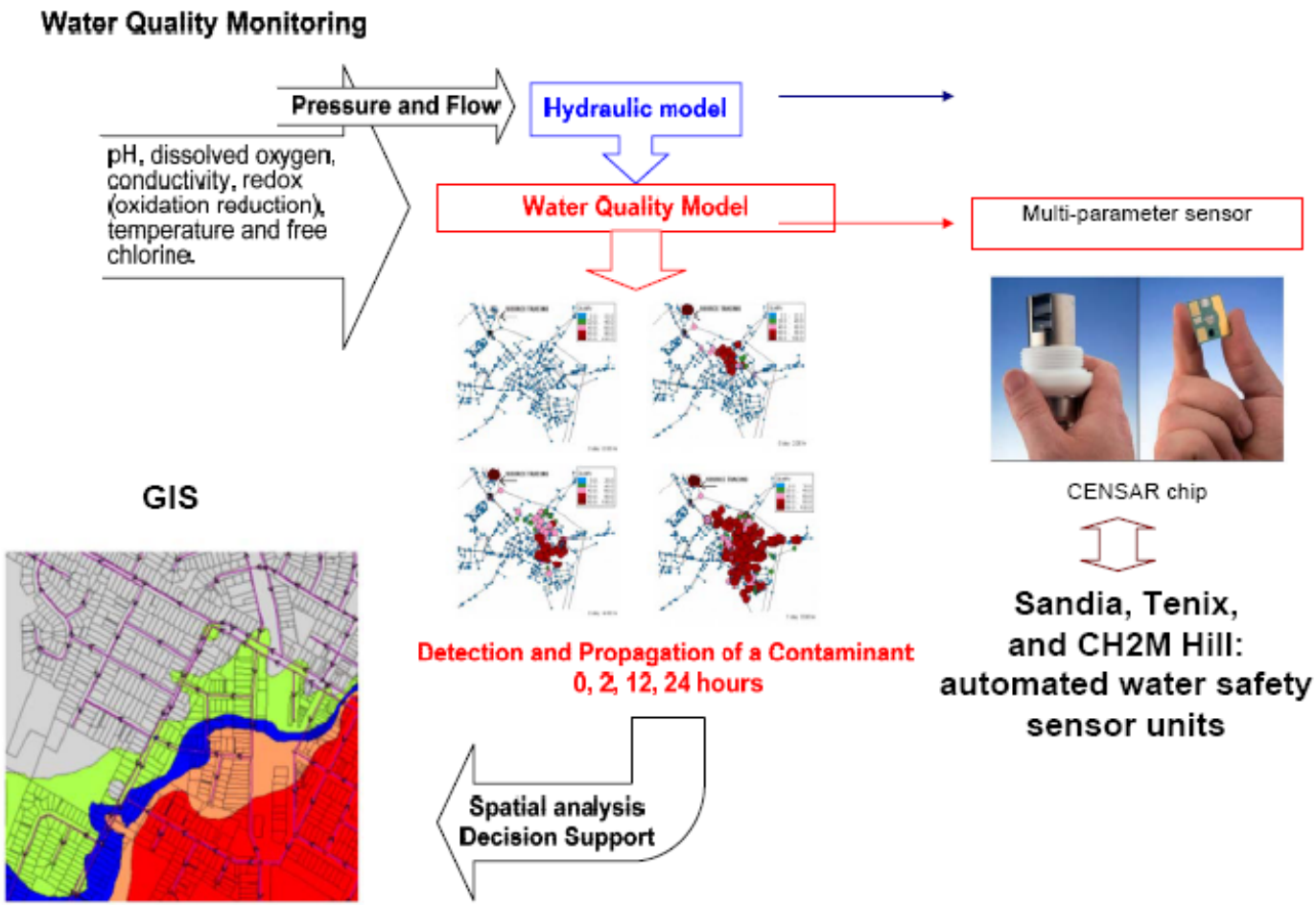




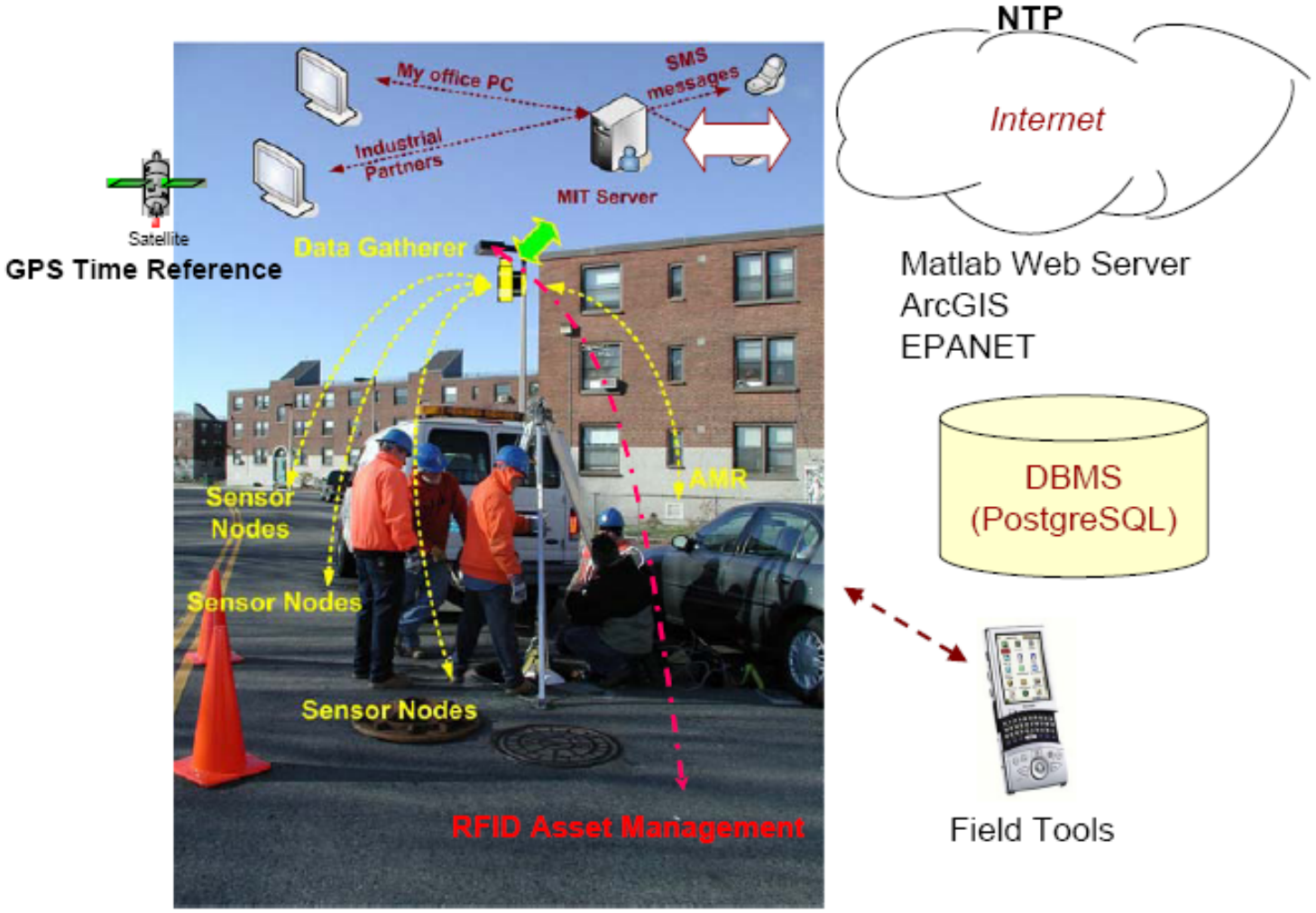
WINES II

- 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

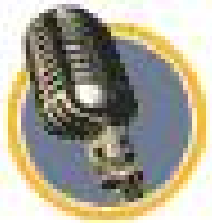


Outline (2nd part)

- Introduction to WSN
- WSN Applications
- WSN Architecture
- HW, SW and Communications Features
- General Security Issues
- Primitives
- Key Infrastructure
- Routing
- Aggregation
- Privacy

Introduction to WSN

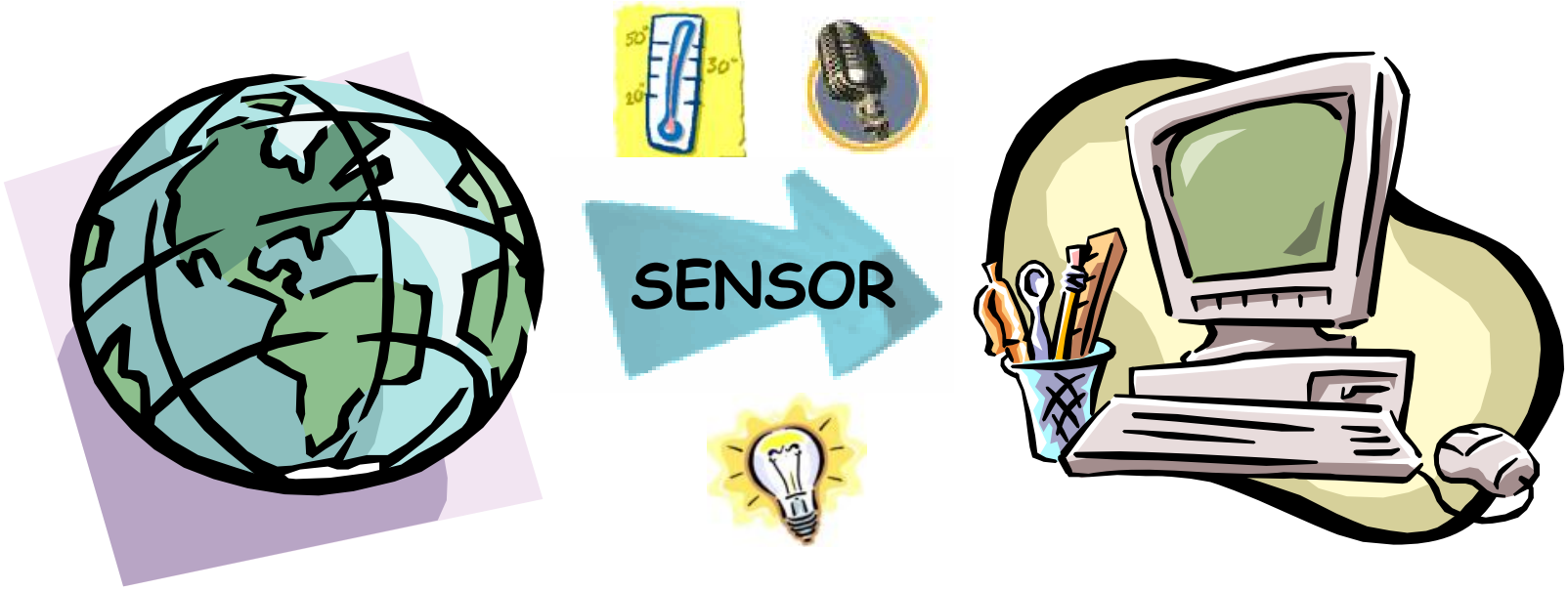
Temperature



Sound

Light

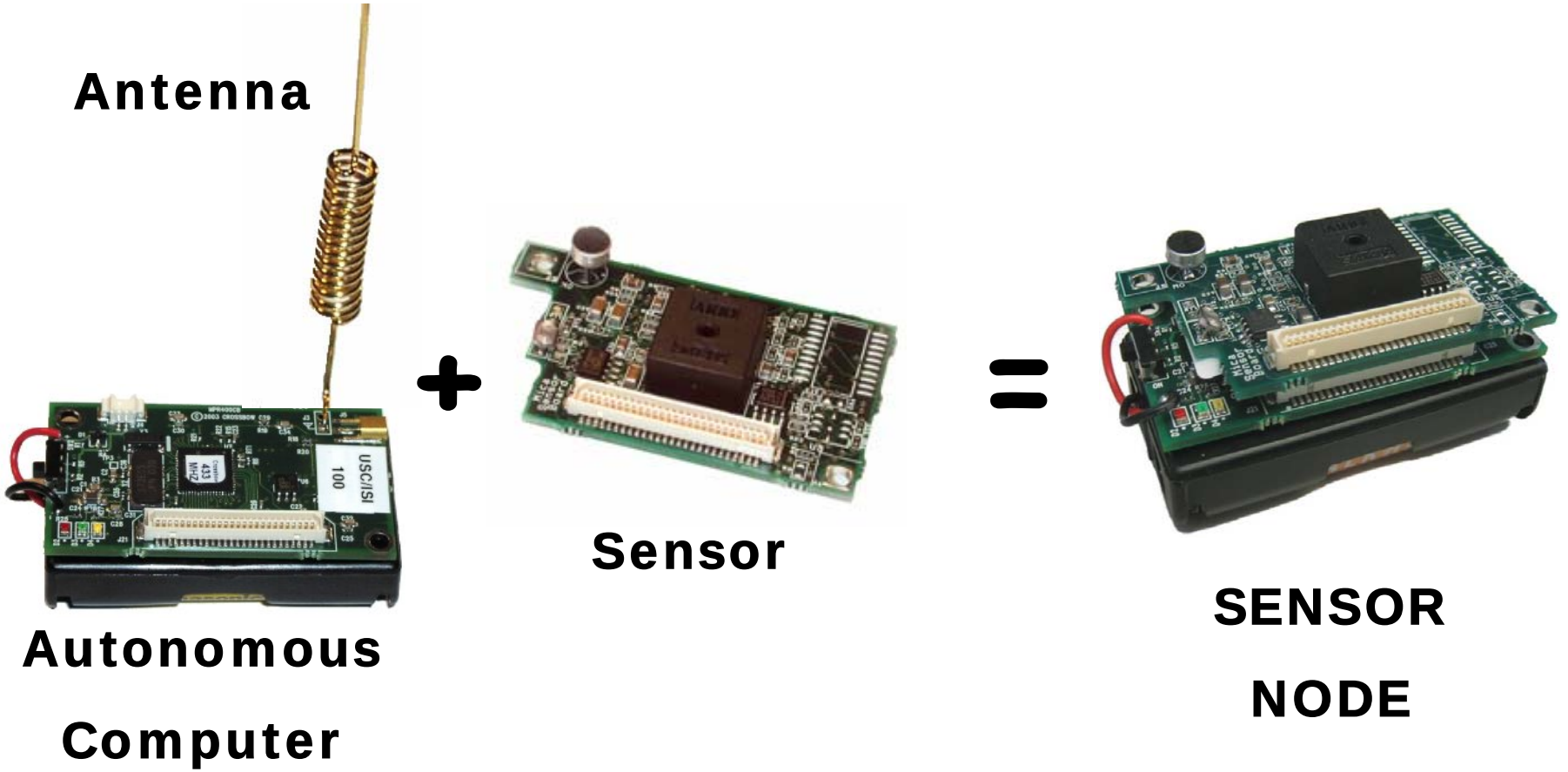
Introduction to WSN



Real World

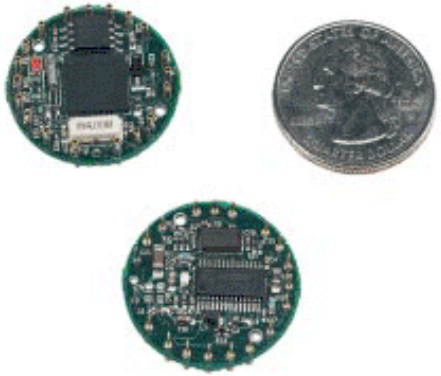
Computer World

Introduction to WSN



Introduction to WSN

MICA mote



MICADOT motes

Telos mote

Introduction to WSN

- Low cost
  - Node prices: 100$ - 250$ (not mass produced nowadays).
  - No cost for wired infrastructures.
- Easy to Deploy
  - Easy to maintain?
- Access and Measure unreachable events

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,
  - environment,
  - health care,
  - homeland security,
  - industrial,
  - military applications,
  - etc.

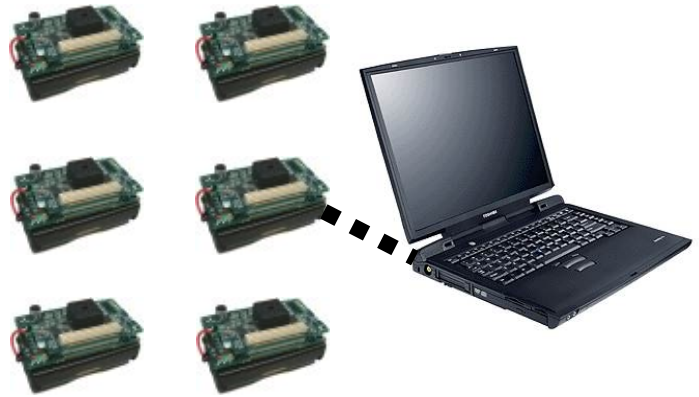
WSN Applications

- 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 Architecture

- In a WSN, hundred of sensors operate and cooperate in an ad hoc manner, establishing communication paths with other nodes in a close distance.
- This results in a mesh architecture where every node:
  - supports multiple communication paths, and
  - provides routing capabilities

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



WSN Architecture

- Sensors also communicate with one or more base stations that:
  - collect information 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, the base station is supposed to have enough resources
  - not only for all necessary computations but for all internal and external communications to the WSN.

WSN Architecture

WSN Architecture

- Sensor Nodes "roles":
  - Harvester: Collect information of their surroundings.
  - Router: Send information to its destination (another node or a base station).
  - Distributed platform: Process its own information, information from other Sensor Nodes, or control information from the base station.

HW, SW and Communications features

- 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: the processor is clocked to 4 MHz,
    - to 7.37 MHz in the case of Mica2 and MicaZ,
    - and to 8MHz in the case of Telos.

HW, SW and Communications features

- 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

Batteries

- The current generation of wireless sensor nodes is still relying on batteries as its source of power.
- The limited lifetime of batteries 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.

Batteries

- Next generation sensor nodes will therefore combine ultra-low power circuitry with so-called power scavengers
  - which allow 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.

General Security Issues

- Due to extreme constraints of the network infrastructure, a sensor network is highly vulnerable to any external or internal attack.
  - Thus, the infrastructure and protocols must be prepared to face these situations.
- Generally speaking:
  - Physical attacks: against the physical structure of the node/network.
  - Logical attacks: against the information/protocols.

General Security Issues

- A sensor is physically vulnerable:
  - Destroyed, stolen nodes – no network/inaccessible!
  - Subverted nodes – disclose info, become malicious
  - Public wireless channel: jamming
  - Measurement vulnerabilities
  - Battery exhaustion attacks (sleep deprivation torture)

General Security Issues

- A sensor is logically vulnerable:
  - Public wireless channel: eavesdropping, injection
  - Attacks to protocols: external, internal nodes
    - Change network behaviour, unusable network
    - Even non-malicious nodes can harm!
  - Identity and Instruction Integrity – Easy to bypass

General Security Issues

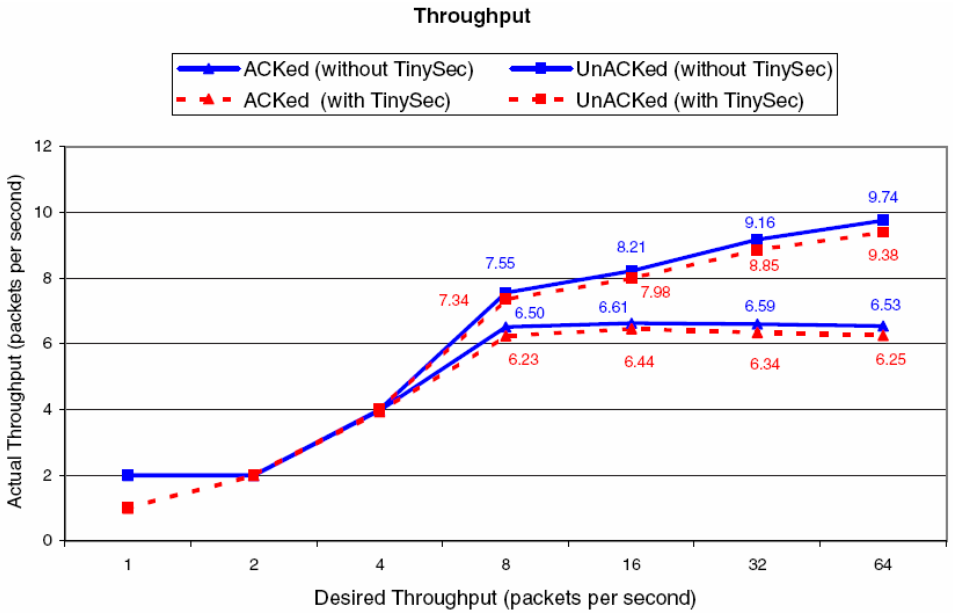
- What do we need (in a broad sense)?
  - Protect communication channels
    - Create secure primitives and secure communication protocols
    - Distribute keys securely over the network
  - "Bullet-proof" information management protocols
    - E.g.: Routing, Data Aggregation
  - Audit events in the WSN
  - Other issues
    - Tamper protection
    - Protect (network and social) privacy
    - …

Security 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
- We can consider: Symmetric Key Encryption (SKE), Message Authentication Codes (MAC), Public Key Cryptography (PKC)
- HW is expensive; so SW is, in most cases, the way to go.
- Global challenge: Design strong and secure primitives using less energy, computational time and memory space

Security Primitives

- Example of SW SKE on Sensor Nodes: TinySEC protocol
  - Block Ciphers (Skipjack, RC5,… AES)
  - Non-standard CBC (IV uses counter – replay protection)
  - Low RAM (256B Data, 8KB Instruction)
  - Low Computational/Latency Overhead
  - Low Energy Usage



Security Primitives

- MAC (usually) reuses algorithms used in SKE
  - Most common: CBC-MAC
    - Creates a MAC using a block cipher
  - Why reuse?
    - Efficient and Fast
    - Less memory footprint for calculating MAC

Security Primitives

- PKC was initially rejected as "non-possible" in a sensor node
  - Decrypt 64 bits (1024 bit key) in 14.5 sec.
- Afterwards, ECC starts looking promising
  - Fundamental operation underlying ECC: point multiplication
  - Less memory/energy usage than RSA

Security Primitives

- First usable PKC over TinyOS
  - Deeply optimized!
  - Using Elliptic curves (ECC) with keys of 163 bits
  - Low RAM
  - Acceptable Computational times
    - Generation of Keys / Shared Secret = 34 sec each
  - Acceptable Energy Usage
    - ±54.000 PKC operations in its lifetime
- Challenge: Accommodate advantages (tools and services) of PKC technology to sensor networks

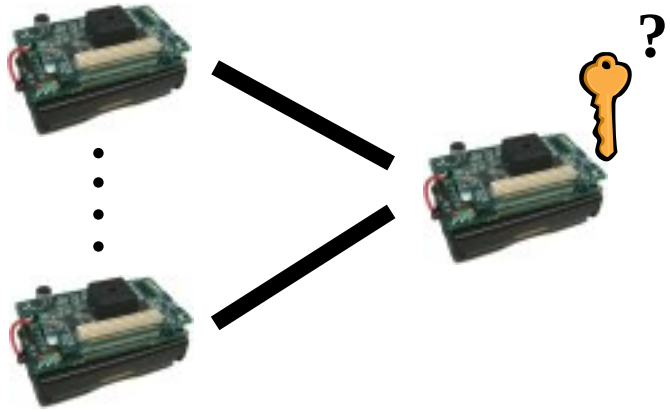
Security Primitives

- New results

Operation	*Key generation*	*ECDSA signature*	*ECDSA verification*	*D-H key exchange*	*El-Gamal encryption*	*El-Gamal decryption*
Time (seconds)	6,74 s.	6,88 s.	24,17 s.	17,28 s.	24,07 s.	17,87 s.

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 Management Procedures

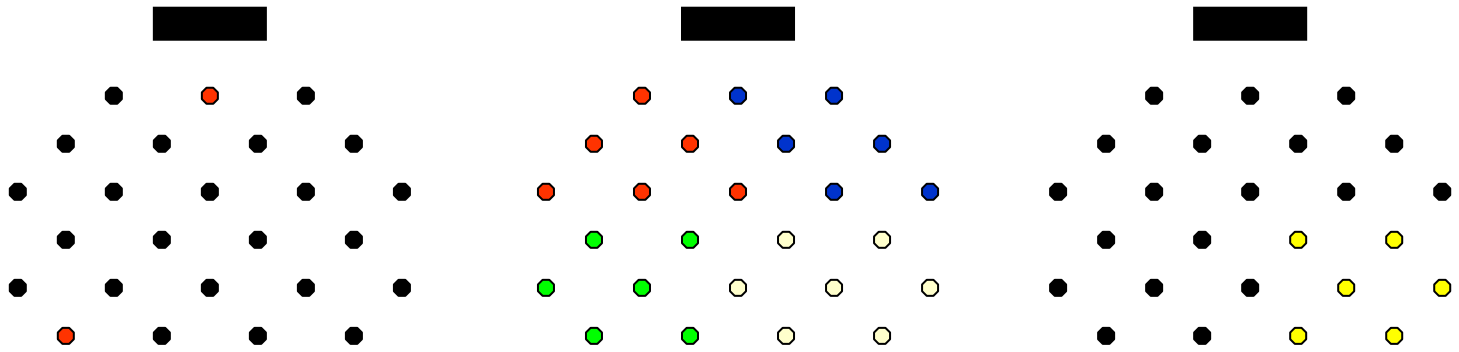


Key Infrastructure

- Key Distribution Protocols
  - How keys are issued to sensor nodes
- 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



Global (GKI) Clustered (CKI) Local (LKI)

Key Infrastructure

- Key Distribution
  - Before Deployment
    - Keys cannot be captured during distribution
    - (In most cases) Network topology should be known!
  - After Deployment
    - Prone to be attacked
  - Challenge: PKC – still in development

Key Infrastructure

- Key Distribution
  - Two types of keys:
    - Local communications
    - Communications between clusters
  - Two situations:
    - Static clusters (fixed network topology)
    - Dynamic clusters (self-configuration)
- General Solutions? "Rich uncle" cluster head (manages key distribution, storage and maintenance)
- Challenge: Any node in the cluster should be able to become the cluster head and provide that functionality

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 (×)

Key Infrastructure – CRISIS Project

- 1) Find properties of the KMS in the scenario
  - MUST – Main Properties
  - SHOULD – Secondary Properties
- 2) Select protocols whose first column equals a main property
- 3) Select Protocols that satisfy the following:
  Main Properties $\in$ Advantages ($\surd$).
  [Optional] Secondary Properties $\in$ Advantages ($\surd$).
  Main Properties, Secondary Properties $\notin$ Disadvantages ($\times$)
- 4) Review protocols and choose most suitable
- Other details / Exceptions:
  - LOC: The designer must know the final location of the nodes
  - DES{α}: The property α is affected by the protocol design params.

Key Infrastructure – CRISIS Project

- Example: Monitoring of Ageing Infrastructures
  - Main properties:
    - Connectivity (Sensors working on "hostile" environment)
  - Secondary Properties:
    - Resilience (Data Reliability – Important Infrastructure)
    - Security (Deployment area is "public")
- Protocol?
  - Location of the nodes is known: AT-24

necti	*AT-24* - Grid Based Key Predistribution [19]	✓: Conn., Res., Comm., Sca. × : Ext., Mem., En., $DES\{LOC\}$

  - Otherwise: AT-04

	AT-04 - Hybrid Designs - Generalized Quadrangle [22]	✓: Conn., Sca., Mem., Res. × : $DES\{$Conn., Sca.$\}$

Routing

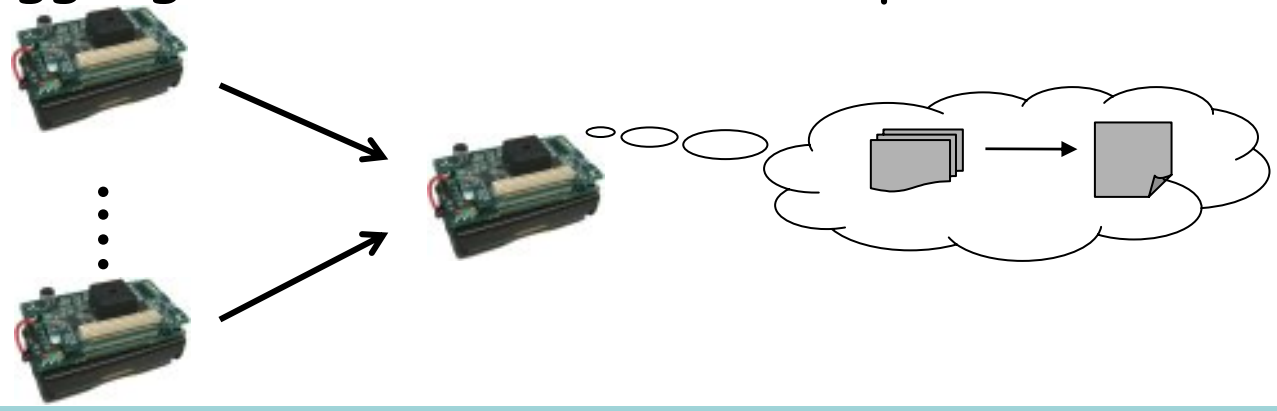
- Maximum transmission distance of current generation of sensor nodes ranges between 100 and 300 mts
  - Thus, messages can not be transmitted directly between any two nodes
  - A routing infrastructure is needed
- Algorithms should work:
  - Even when nodes start to fail due to energy issues
  - With 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!!!

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!

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,…)



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

Thanks for your Attention!