Autonomous Networking

Gaia Maselli
Dept. of Computer Science

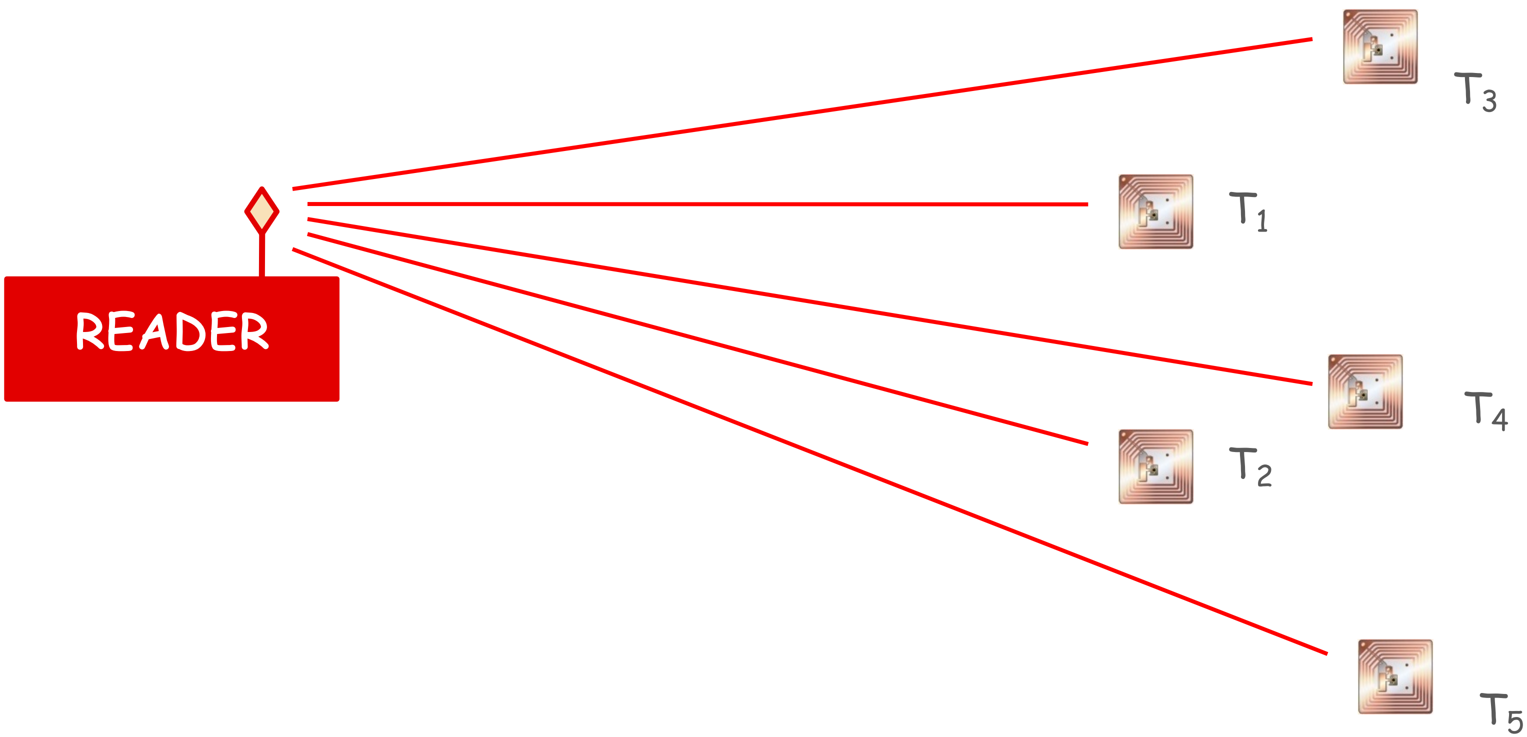
Some slides in this course are readapted from lecture slides from ***Prof. Tommaso Melodia*** *(Northeastern University, Boston)*

Today’s plan

- Wireless Sensor Networks (WSN)
- Applications of Wireless Sensor Networks
- A MAC protocol for wireless networks (CSMA/CA)

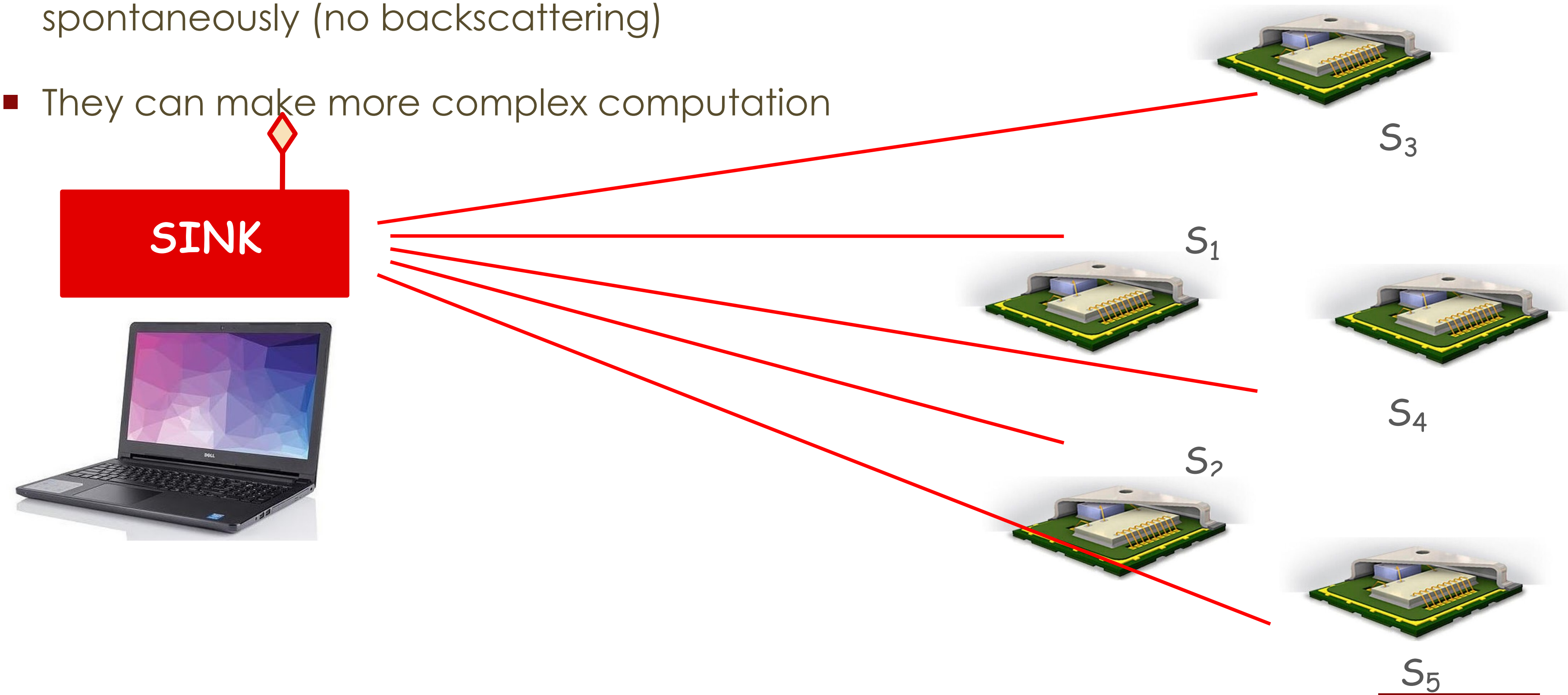
RFID network

- RFID tags transmit their unique ID (typically 96 bits, maximum 256 bits)
- Star topology

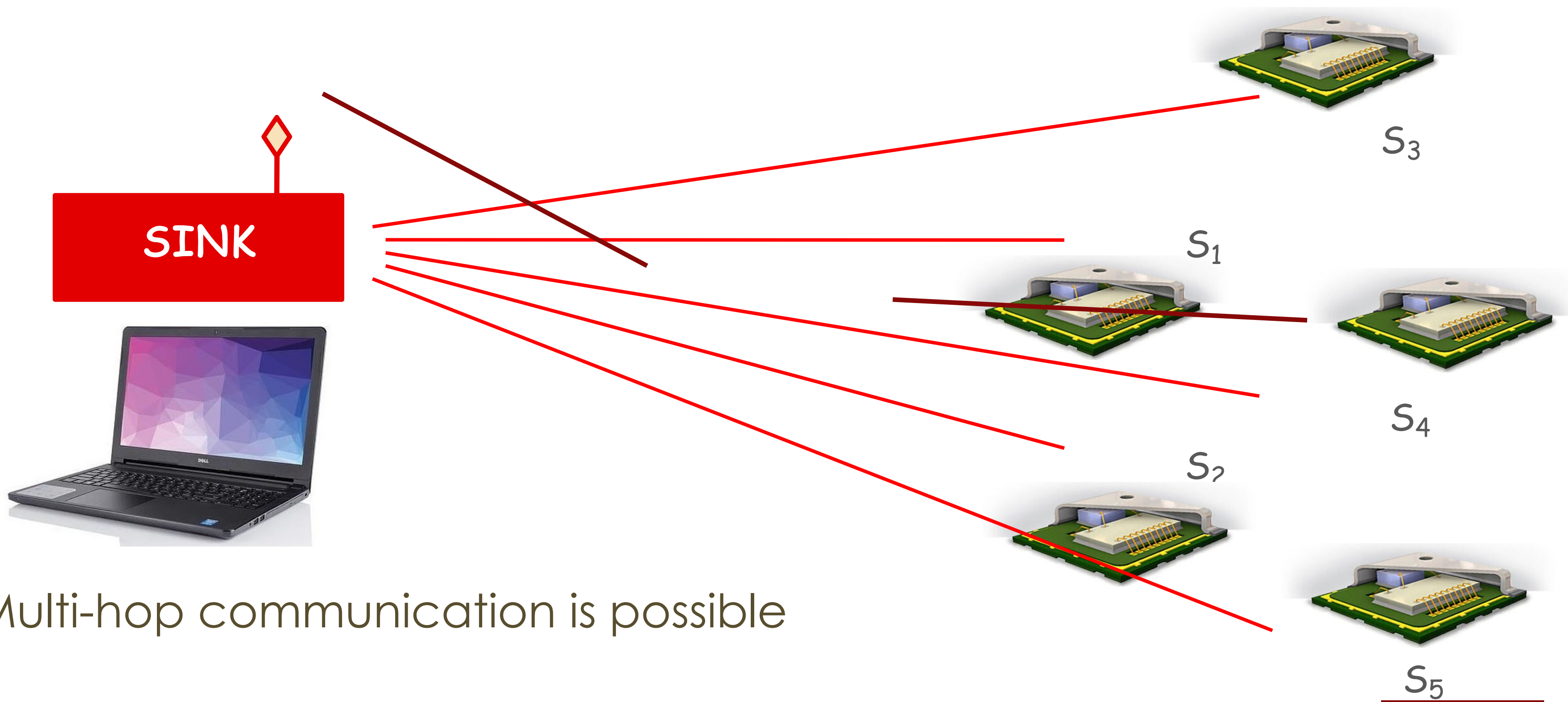


Sensor network

- Sensors have batteries onboard
- Continuosly sense the environment
- They can listen to the channel (carrier sense) and trasmit spontaneously (no backscattering)
- They can make more complex computation



Sensor network

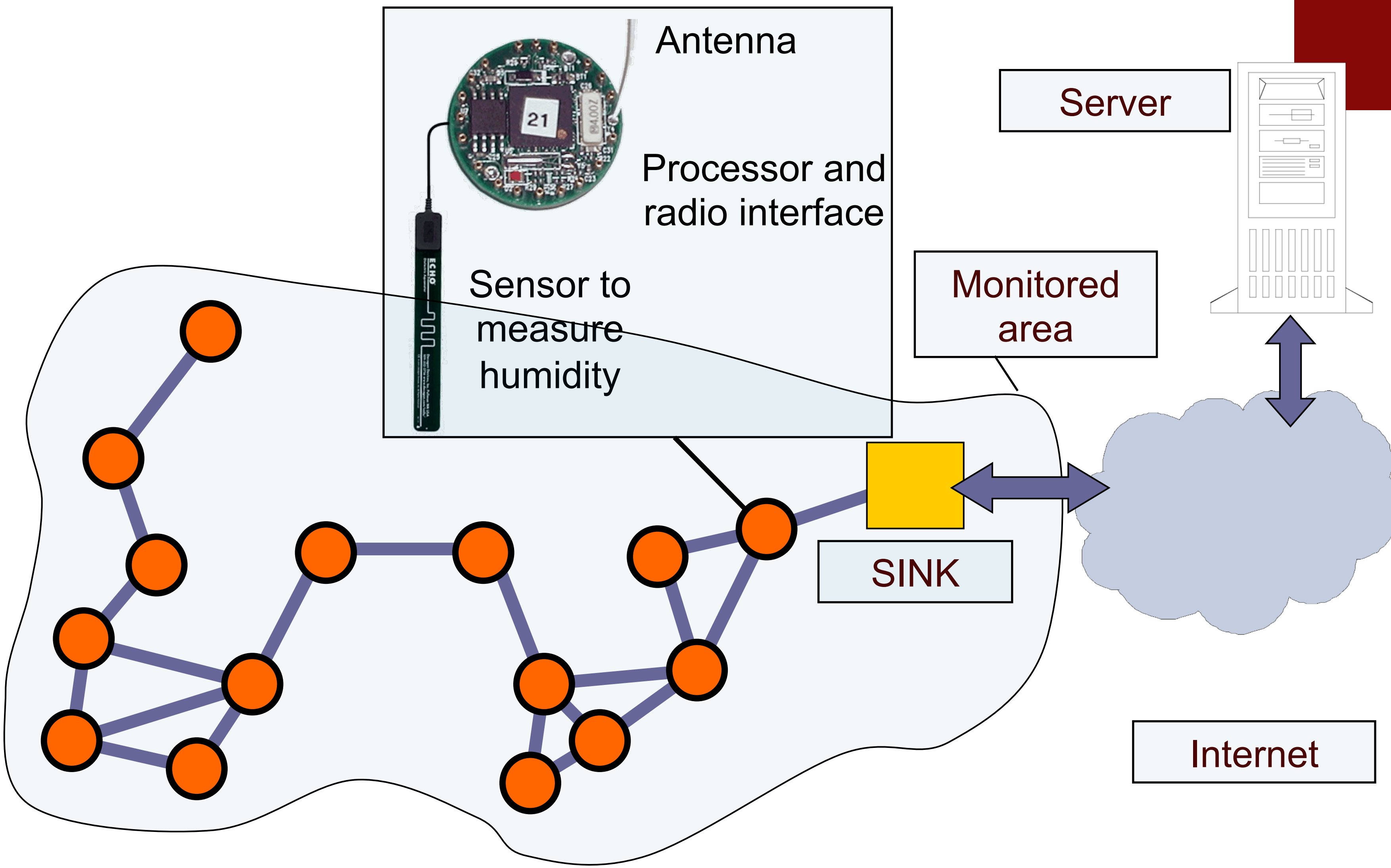


- Multi-hop communication is possible

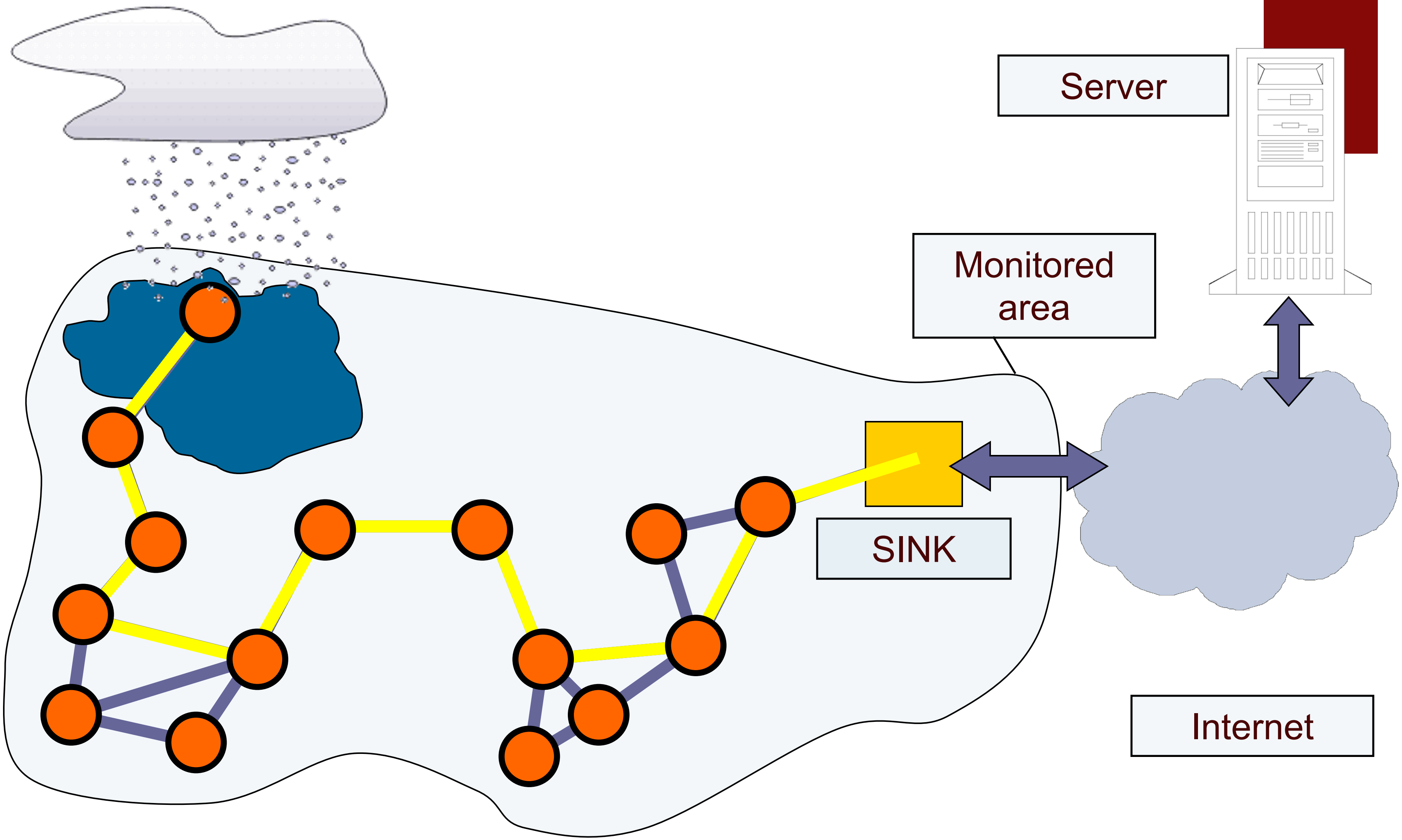
WSN definition

- Sensor networks are composed of distributed devices that monitor and record environmental conditions, sending the data to a central node for processing and analysis

Wireless Sensor Network: architecture



Wireless Sensor Networks: data gathering



Benefits of Sensor Networks

- **Large-Scale Coverage**: Collects data across vast geographic areas, even in remote or inaccessible locations.
- **Autonomous Operation**: Sensors operate independently, reducing the need for human intervention.
- **Real-Time Data**: Immediate access to critical data enables rapid response to environmental changes.

WSN: applications

Application Areas: **Everywhere** there is a need for monitoring a physical space OR using sensors for controlling a procedure.

- Industrial Control: Networked Control Systems – closing the industrial loop over WSN
- Environmental Monitoring & Agriculture: Wild Life Monitoring, Vineyards, Forest Fire Detection
- Structural Health Monitoring
- Marine monitoring: Ocean life & ecosystem
- Health Care: rehabilitation, prosthetics, chronic conditions management, emergency response
- Smart Homes – Smart Buildings – Smart Cities: Energy consumption monitoring and optimization, transportations & traffic management, etc

Environmental monitoring

- **Real-Time Sensing of Environmental Phenomena:** Distributed, autonomous, and self-managing sensor networks provide access to real-time environmental data over large areas.

- Key parameters monitored include:
  - **Temperature**, **Humidity**, **Light**
  - **Wind Speed** and **Rainfall**
  - **River and Water Body Levels** (e.g., flood prediction)
  - **Ground Vibrations** (for seismic activity)
- **Applications of Environmental Monitoring**
  - **Monitoring of Critical and Remote Areas**: Volcanic regions, earthquake-prone areas, and other remote, high-risk zones can be monitored in real-time to provide early warnings.
  - **Fire Detection Alarms**: Continuous monitoring of fire-prone regions helps detect wildfires early, triggering alarms to prevent major damage.
  - **Agriculture Monitoring**: Sensors track key agricultural factors such as soil moisture, temperature, and crop health, optimizing irrigation and crop management.

Structural health monitoring (SHM)

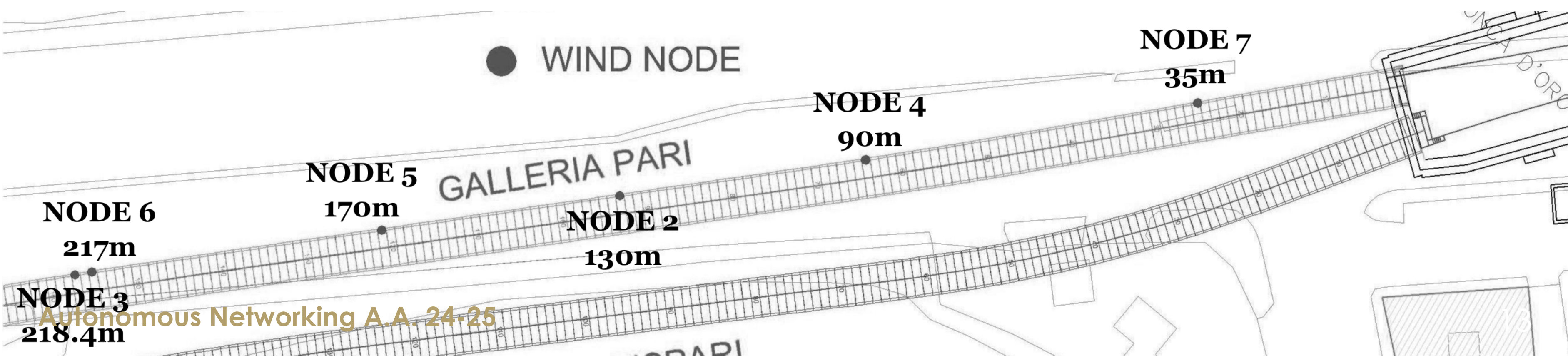
- SHM allows to detect deteriorations and potential damages of a structural system by observing the changes of its material and geometric properties over long periods of time.

- Usually there are 3 main risks in a lifetime of a structure:

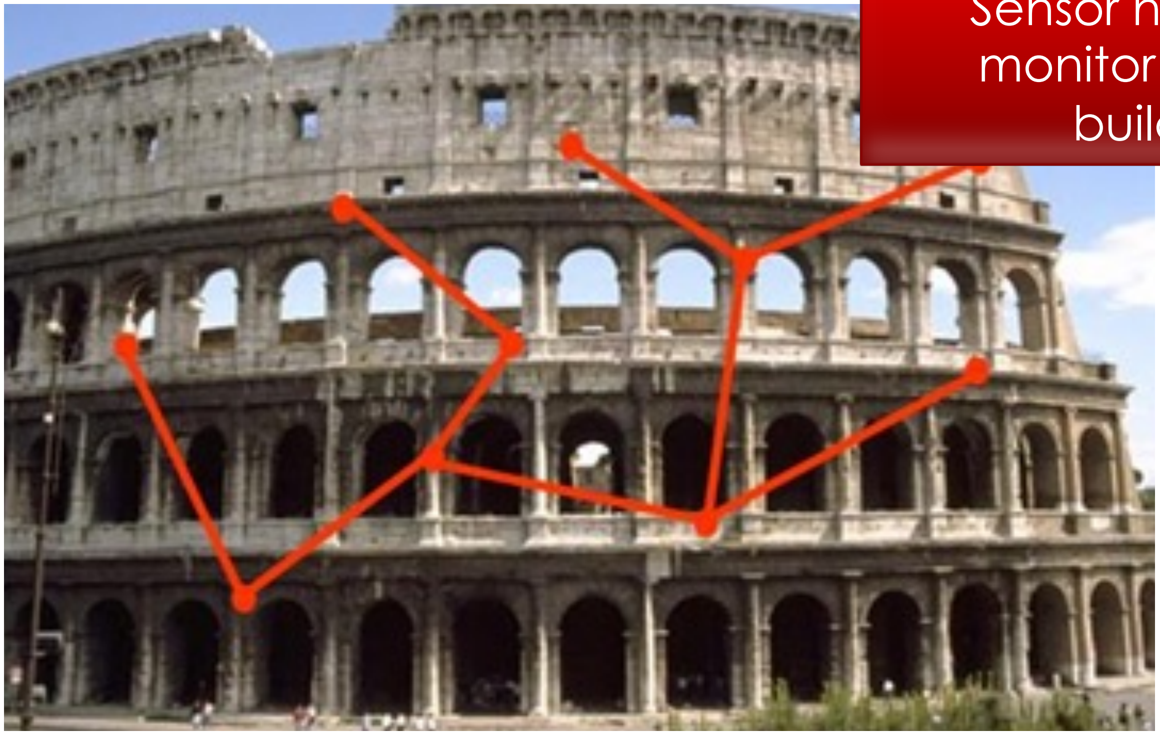
1. **During or directly after the construction** or reconstruction (design failures, quality problems, uncertain or unknown outer parameters, e.g. geology)
2. **Due to or after an outer impact** (possibly repeated)
3. When the **structure gets old** and maintenance is inadequate

Structural health monitoring

- SHM is a vital tool to help engineers improving the safety of critical structures, avoiding the risks of catastrophic failures.
- Wireless sensor networks can provide a quality of monitoring similar to conventional (wired) SHM systems with lower cost.
- WSNs are both non-intrusive and non-disruptive and can be employed from the very **early stages of construction**.



Structural health monitoring



Sensor network to monitor historical buildings

Structural health monitoring

The **Golden Gate Bridge Case Study** (Stanford Univ. - 2005) Objectives:

- determine the response of the structure to both ambient and extreme conditions
- **compare actual performance to design predictions**
- measure ambient structural accelerations from wind load
- measure strong shaking from a potential earthquake
- **the installation and the monitoring was conducted without the disruption of the bridge's operation**

http://sukunkim.com/research/ggb/

WSN

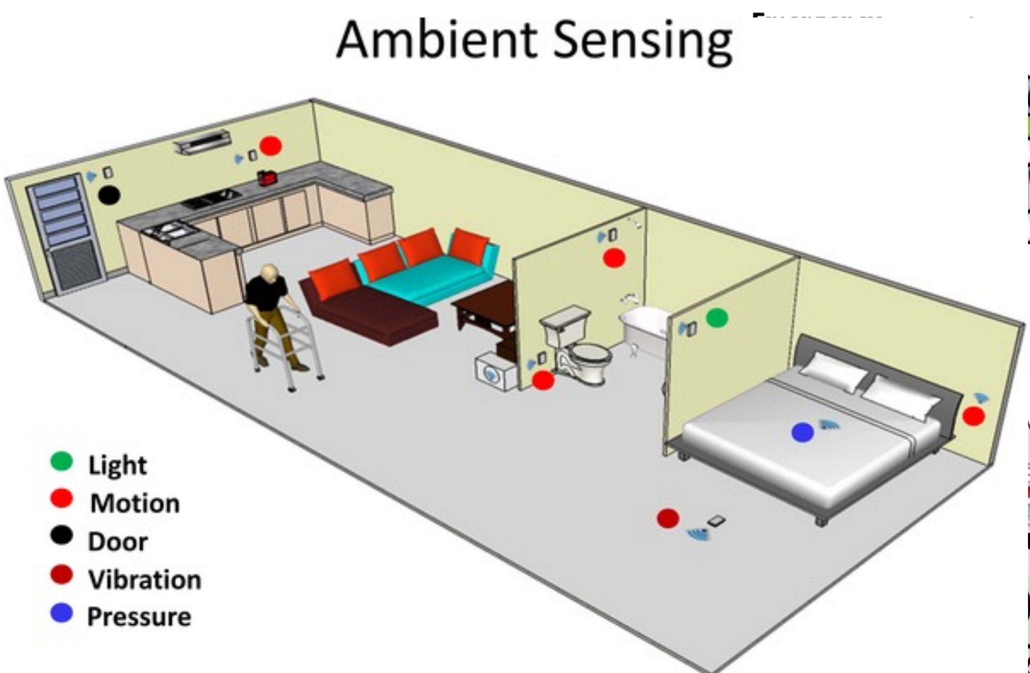
- 64 wireless sensor nodes
- Synchronous monitoring of ambient vibrations
- 46-hop network

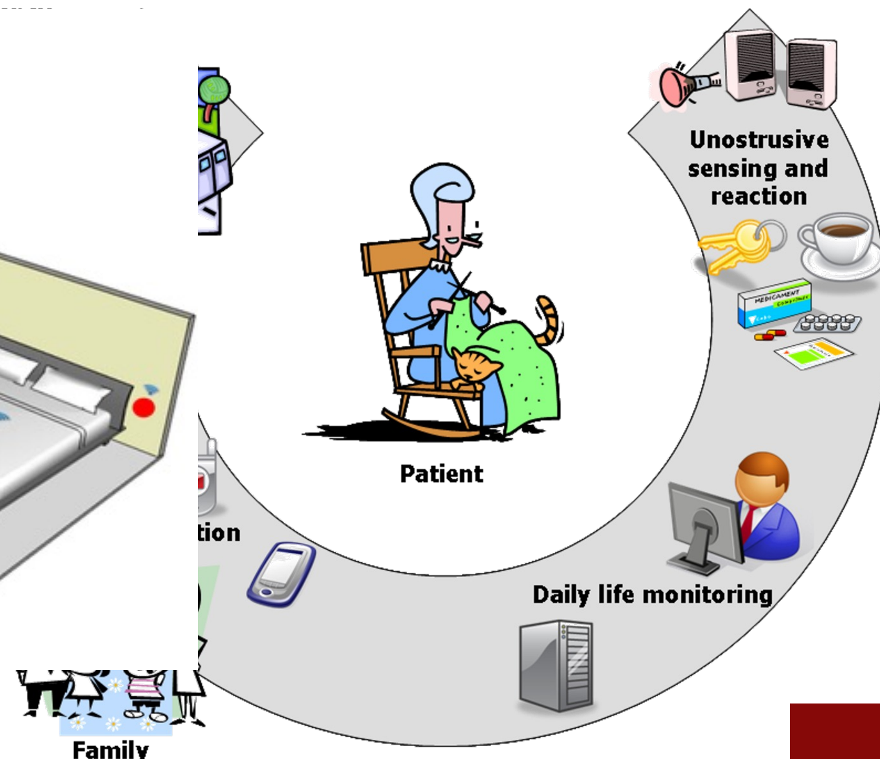
Health-care

- **In hospital** – patients carry **medical sensors** to monitor parameters such as **body temperature, blood pressure, breathing activity** but also **location** and **activity** sensors to monitor patient activities

Health-care

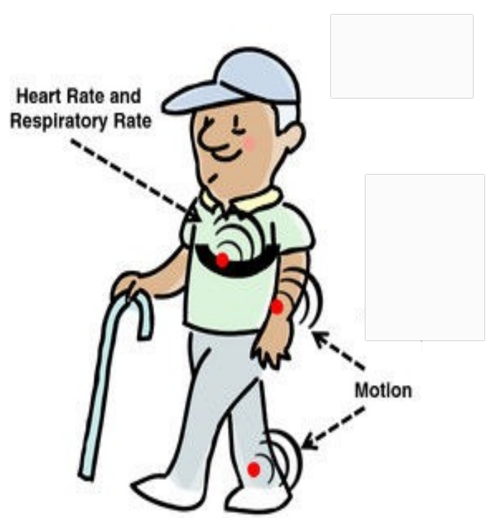
- **At home** – besides body sensors, wearable (accelerometers, gyroscopes) or fixed (proximity) **sensors can be used to infer user's activities and state in his/her living environment**. This is particularly useful for the **elderly** who live alone (detection of falls or illness)

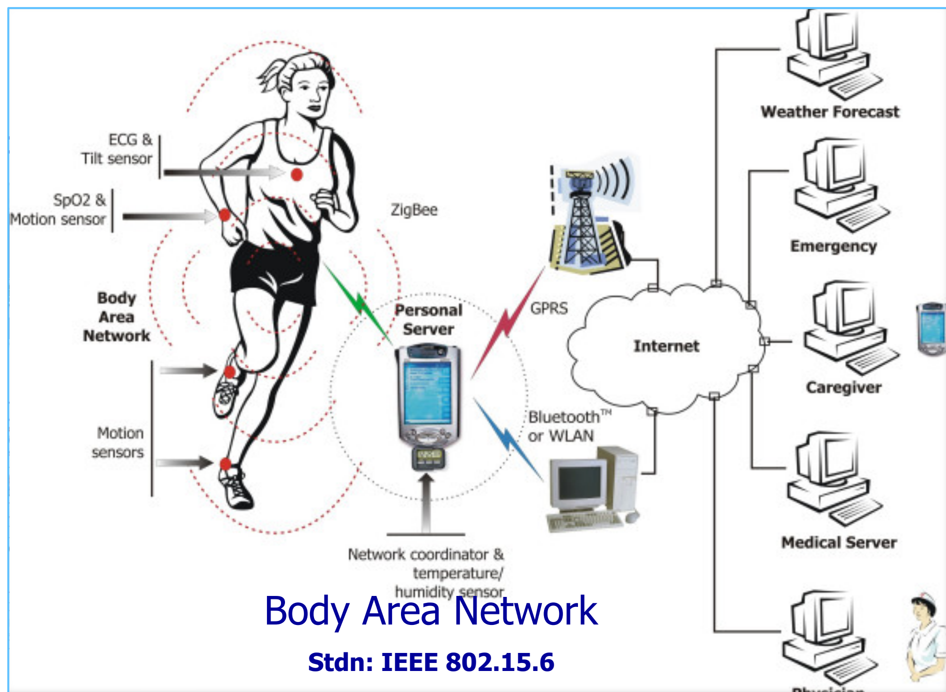




Health-care: well being

- Personalized health-care and well-being solutions
- The use of wearable sensors, together with suitable applications running on personal computing devices enables people to **track their daily activities (step walked, calories burned, exercises performed**, etc.) providing suggestions for enhancing their lifestyle and prevent the onset of health problems



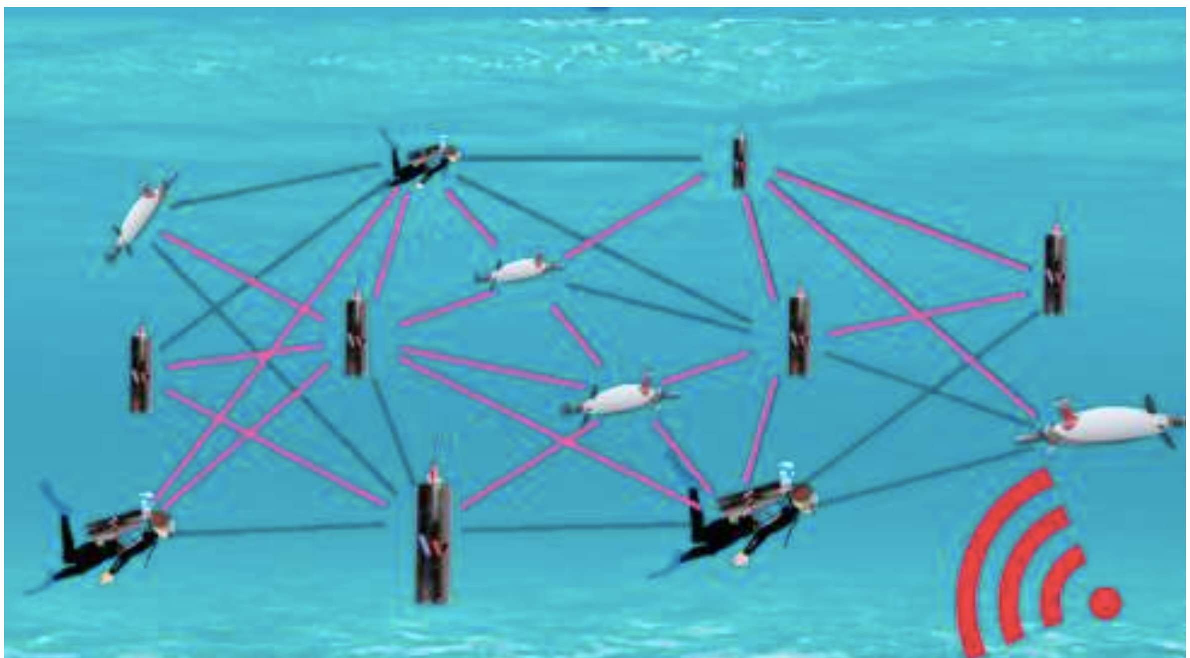


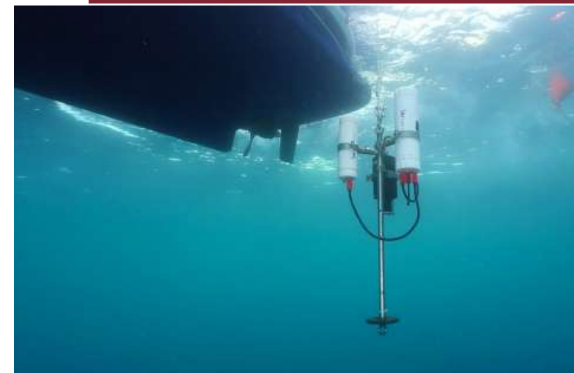
Security and surveillance

- Sensor networks can significantly improve surveillance in a wide range of public and private spaces, including Enterprise Buildings, Shopping Malls, Factory Floors, Car Parks, Airports, Stadiums, and Other Public Venues
- **Ambient Monitoring** for Hazardous Substances
  - Environmental Sensors: Sensors can detect the presence of dangerous chemicals or hazardous materials, ensuring quick response to potential health threats.
- **Behavioral Monitoring** for Suspicious Activity
  - Human Behavior Sensors: Advanced sensors and machine learning algorithms can analyze patterns in human behavior to identify potential security threats or suspicious activities, helping to prevent incidents before they occur.
- Building Efficient Early Warning Systems
  - Proactive Surveillance: Early warning systems based on sensor networks can provide real-time alerts to authorities, allowing for faster intervention and improving public safety.

Underwater WSN

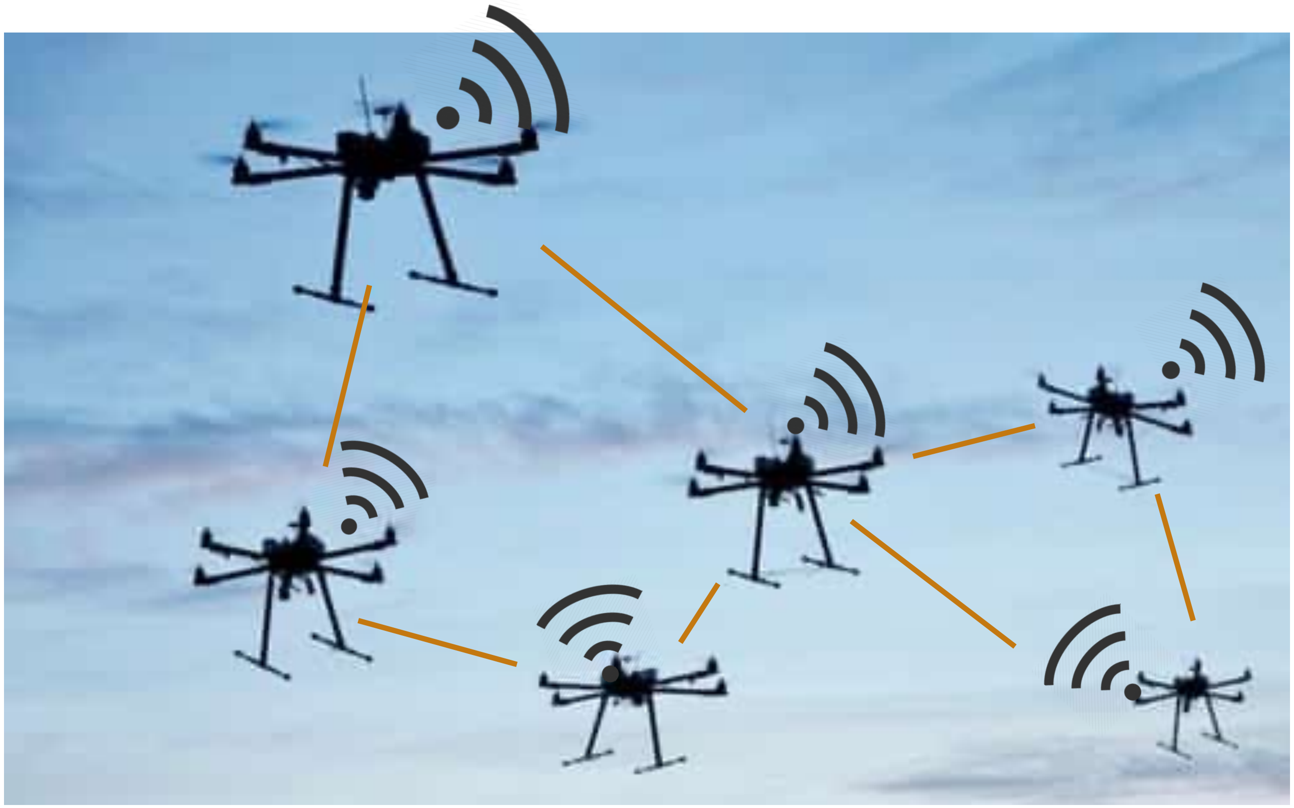
- Allows to interconnect underwater sensors, underwater robotics technologies, enabling **real-time data, reliable, secure information exchange**, providing an unprecedented opportunity to map, know, understand, sustainably exploit the marine environments





Aerial WSN: dronet

- Drones can be equipped with different types of sensors to monitor an environment and report information on large areas



Roles of participants in WSN

Sources of data: measure data, report them “somewhere”

Sinks of data: interested in receiving data from WSN

Actors/actuators: control some devices based on data

Deployment Options

SAPIENZA UNIVERSITÀ DI ROMA

Random deployment	• Dropped from aircraft • Usually uniform random distribution for nodes over finite area is assumed
Regular deployment	• Well planned, fixed • Not necessarily geometric structure, but that is often a convenient assumption
Mobile sensor nodes	• Can move to compensate for deployment shortcomings • Can be passively moved around by some external force (wind, water) • Can actively seek out “interesting” areas

Characteristics of WSN

SAPIENZA
UNIVERSITÀ DI ROMA

Scalability

- Support **large number of nodes**
- Performance should not degrade with increasing number of nodes

Wide range of densities

- Vast or small number of nodes per unit area, very application-dependent

Limited resources for each device

- Low amount of energy
- Low cost, size, and weight per node
- Nodes may not have a global ID such as an IP address

Mostly static topology

- Recently new sensor network paradigm introduce continuously changing topology

Characteristics of WSN

Service in WSN

- Not simply moving bits like traditional networks
- In-network processing
  - Provide answers (not just numbers)
- **Communication is triggered by queries or events**
- **Asymmetric flow of information** (sensors to sink)

Quality of service

- Traditional QoS metrics do not apply

Fault tolerance

- Be robust against node failure
  - Running out of energy, physical destruct

Characteristics of WSN

SAPIENZA UNIVERSITÀ DI ROMA

Lifetime

- The network should fulfill its task **as long as possible** – definition depends on application
- Lifetime of individual nodes relatively unimportant
- But often treated equivalently

Programmability

- **Re-programming** of nodes in the field might be necessary, improve flexibility

Maintainability

- WSN has to **adapt** to changes, self-monitoring, adapt operation
- Incorporate possible additional resources, e.g., **newly deployed nodes**

Typical Adopted Mechanisms

- **Multi-hop wireless communication**
- **Energy-efficient operation** — Both for communication and computation, sensing, actuating
- **Self-configuration**
- **Collaboration & in-network processing** — Nodes in the network collaborate towards a joint goal. Pre-processing data in network (as opposed to at the edge) can greatly improve efficiency

Mechanisms to Meet Requirements

Data centric networking	**Focusing network design on data**, not on node identifiers (id-centric networking)
Locality	**Do things locally** (on node or among nearby neighbors) as far as possible
Exploit tradeoffs	For example between invested **energy and accuracy**

WSN: reasoning of existence

Collect	Collect information from the physical environment – regardless of how easily accessible that is;
Couple	Couple the end-users directly to the sensor measurements (cyber to physical space);
Provide	Provide information that is precisely localized (in spatio-temporal terms) according to the application demands;
Establish	Establish a bi-directional link with the physical space (remote & adaptable actuation based on the sensing stimulus)

WSN: devices

Wireless Sensor Networks combine

Sensing

Processing

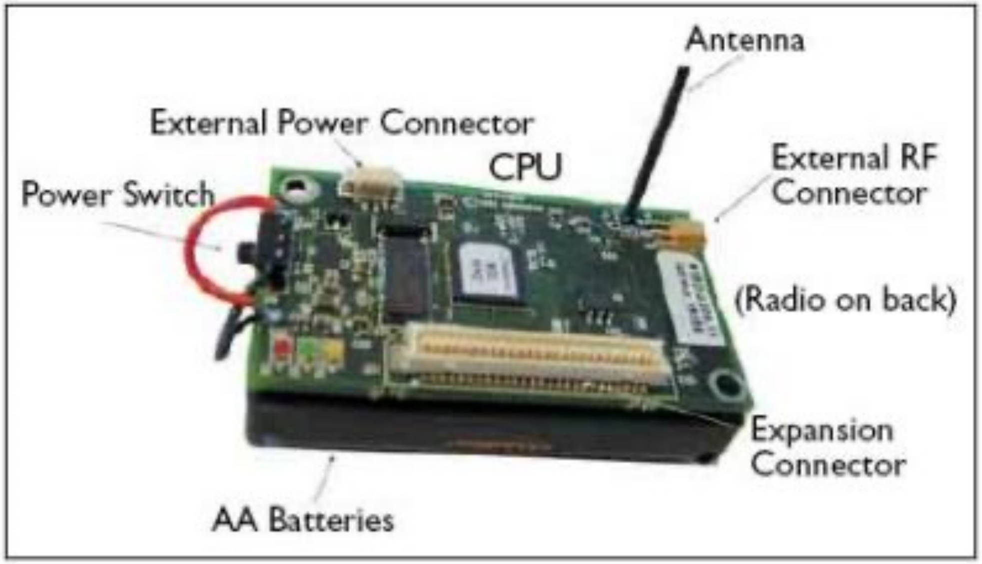
Networking

over miniaturized embedded devices

→ sensor nodes

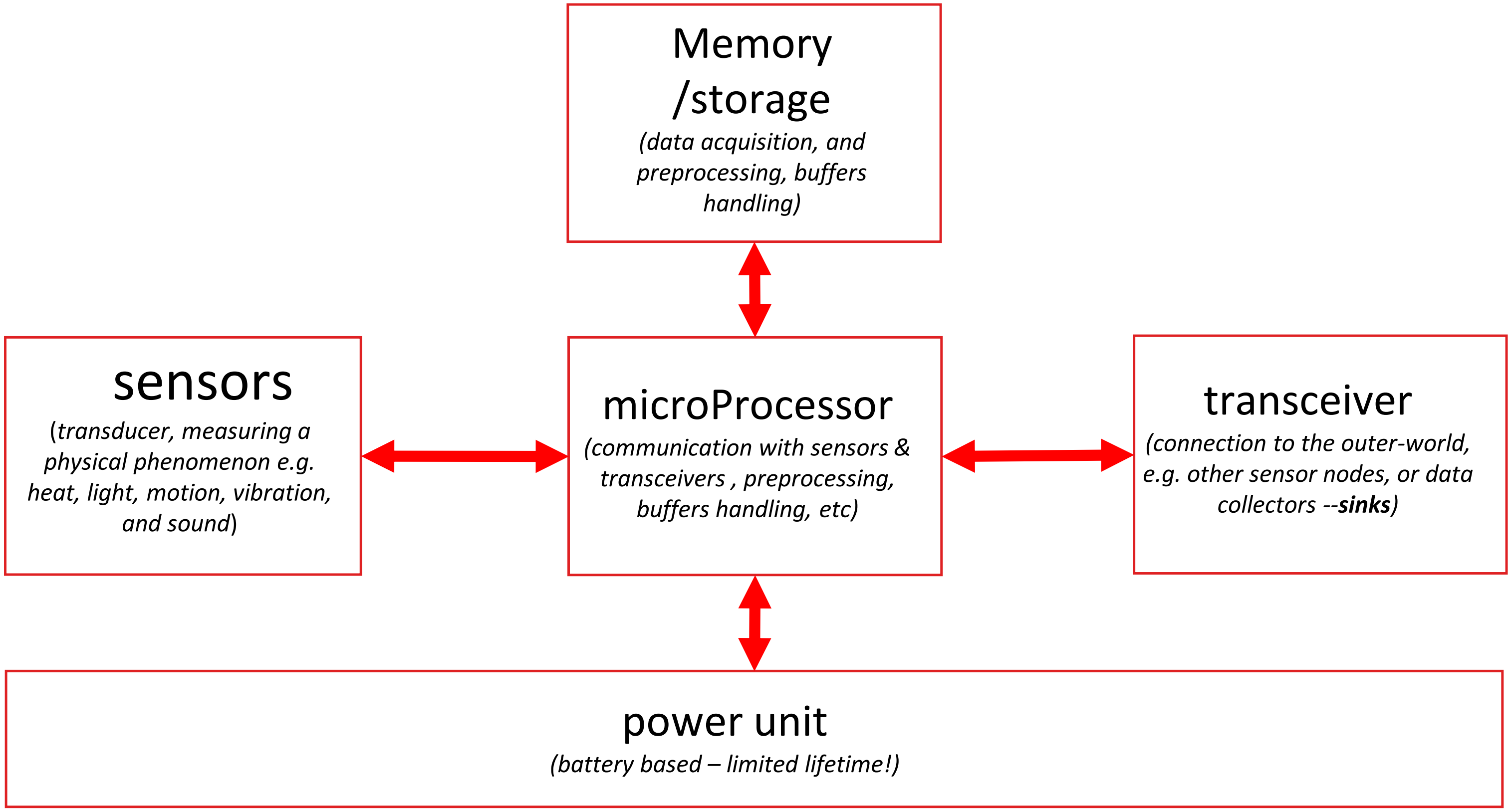
Main sensor node components

- an antenna and a radio frequency (RF) transceiver to allow communication with other nodes,
- a memory unit
- a CPU
- the sensor unit (i.e. thermostat)
- the power source which is usually provided by batteries or a power bank.



- The operating system running on sensor nodes is called TinyOS and was initially developed at the University of California, Berkeley. TinyOS is designed to run on platforms with limited computational power and memory space. The programming language of TinyOS is stylized C and uses a custom compiler called NesC.

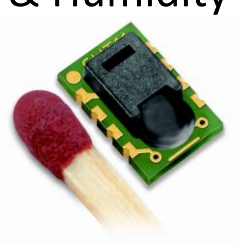
Sensor node


Memory
/storage
(data acquisition, and preprocessing, buffers handling)
sensors
(transducer, measuring a physical phenomenon e.g. heat, light, motion, vibration, and sound)
microProcessor
(communication with sensors & transceivers , preprocessing, buffers handling, etc)
transceiver
(connection to the outer-world, e.g. other sensor nodes, or data collectors --sinks)
power unit
(battery based – limited lifetime!)

Sensing elements

- Sensors: capture a signal corresponding to a physical phenomenon (process, system, plant)
- Signal conditioning prepare captured signals for further use (amplification, attenuation, filtering of unwanted frequencies, etc.)
- Analog-to-digital conversion (ADC) translates analog signal into digital signal
- **Model to translate raw value to measurable unit**

Temperature & Humidity



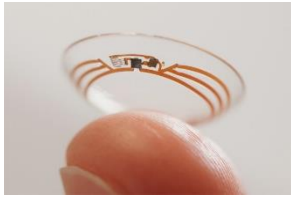
Image

Sound

Pressure

Vibration, Motion

Glucose (&biometrics)



WSN vs. conventional networks

Conventional Networks	WSN
General purpose design (many applications)	Serving a single application or a bouquet of applications
Network Performance and Latency	Energy is the primary challenge
Devices and networks operate in controlled / mild environments (or over an appropriate infrastructure)	Unattended, harsh conditions & hostile environments
Easily accessible	Physical access is difficult / undesirable
Global knowledge is feasible and centralized management is possible	Localized decisions – no support by central entity

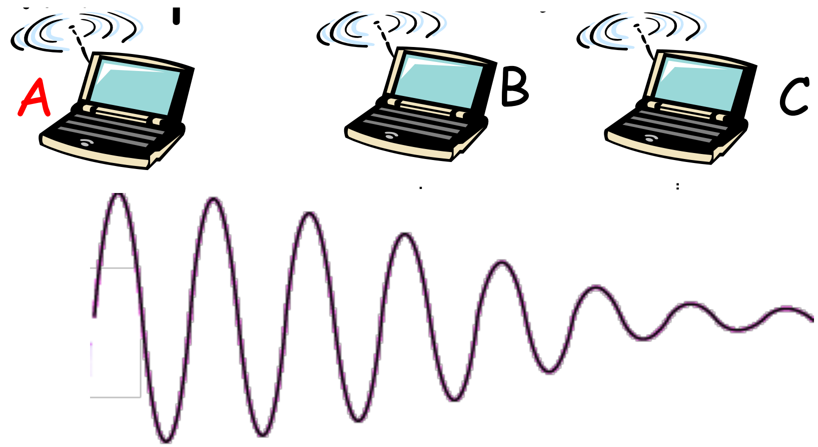
WSN: characteristics

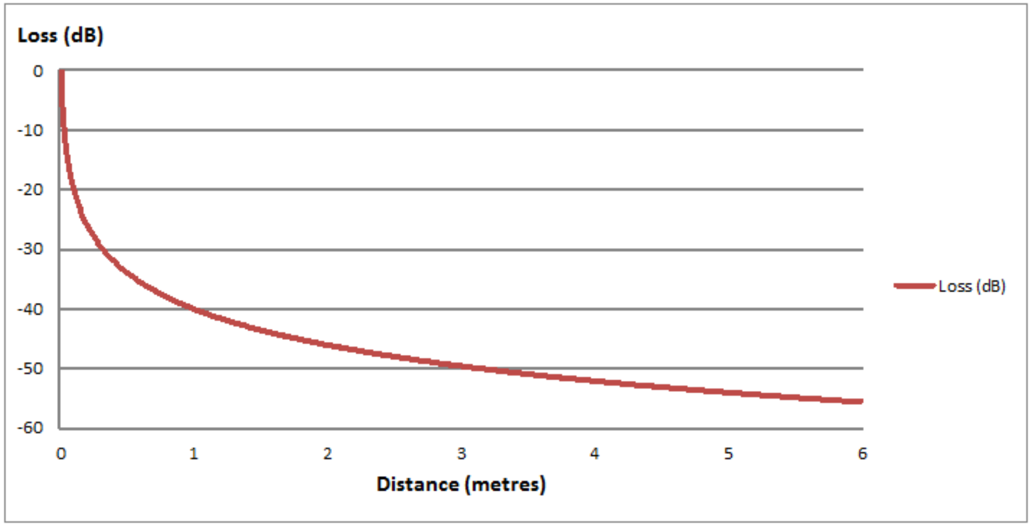
WIRELESS SIGNAL

BATTERY POWERED

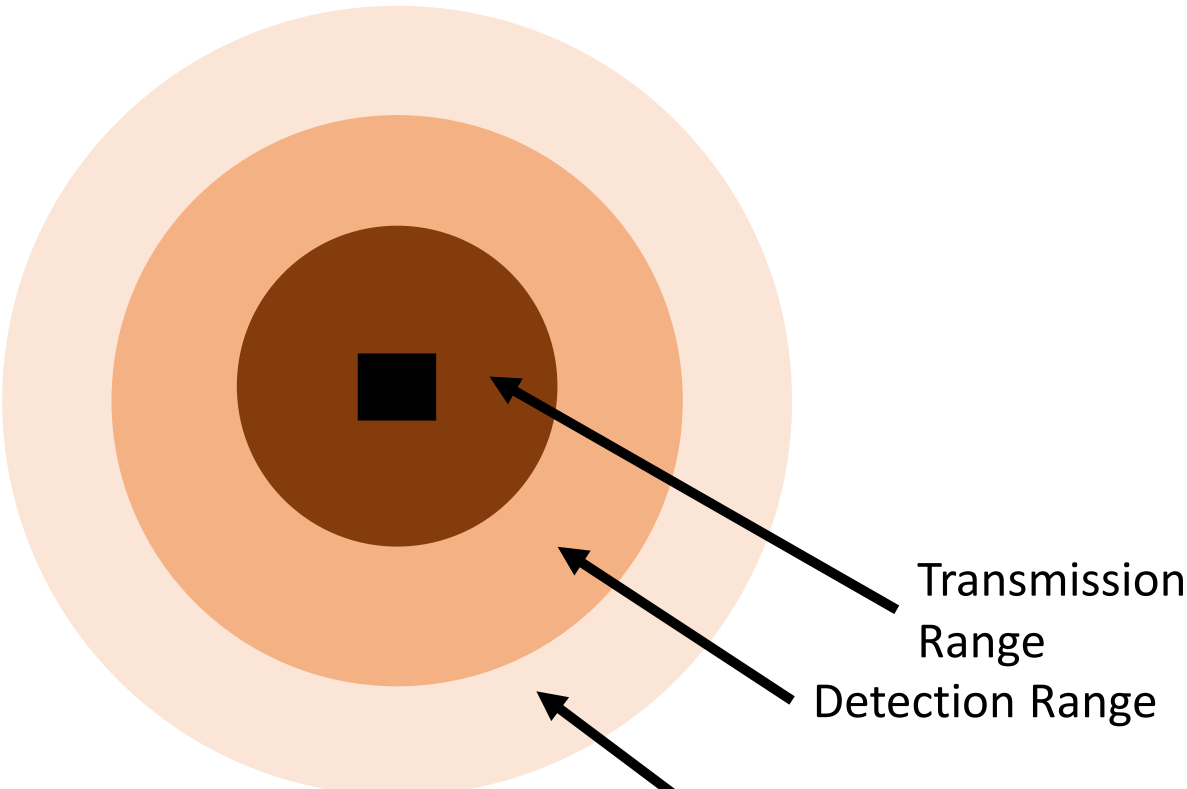
Wireless signal

- Attenuation
  - The strength of the electromagnetic signals decreases rapidly as the distance from the transmitter increases (the signal is dispersed in all directions)





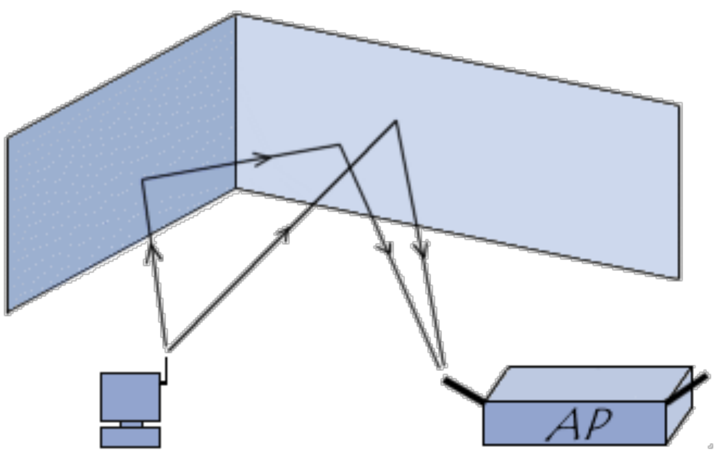
Wireless signal



In theory

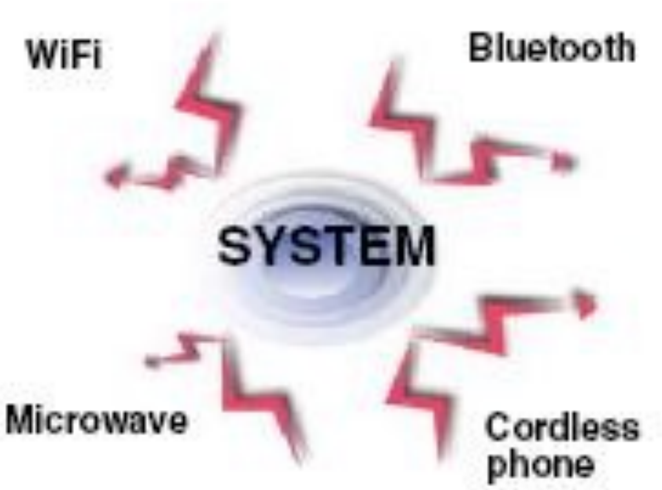
Wireless signal

- Multi-path propagation
  - When a radio wave encounters an obstacle, all or part of the wave is reflected, with a loss of power
  - A source signal can arrive, through successive reflections (on walls, ground, objects), to reach a station or an access point through multiple paths



Wireless signal

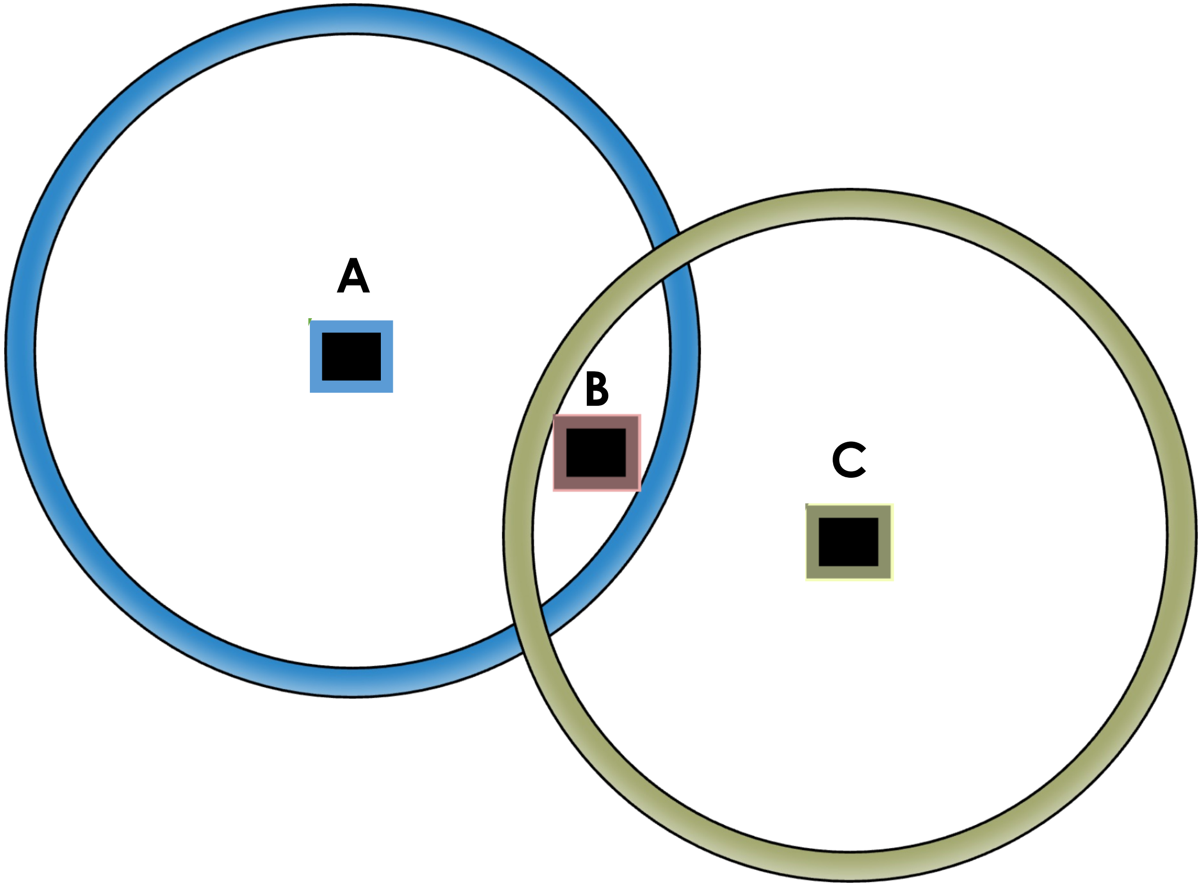
- Interference
  - **From the same source**: A recipient can receive multiple signals from the desired sender due to multipath
  - **From multiple sources**: other transmitters are using the same frequency band to communicate with other recipients



Errors

- The characteristics of wireless links cause errors
- **Signal to Noise Ratio (SNR)** measures the ratio of good to bad signal (signal to noise)
  - High: the signal is stronger than the noise, so it can be converted to real data
  - Low: the signal has been damaged by noise and the data cannot be recovered

Hidden terminal problem



Medium Access Control (MAC) protocols

Objectives of MAC

- Controls how the shared medium (transmission channel) is used by different devices
- Controls when to **send a packet**, and when to **listen for a packet**
- Perhaps the two most important operations in a wireless network
  - Especially, idle waiting wastes huge amounts of energy
- We need schemes for medium access control that are
  - Suitable to mobile and wireless networks
  - Emphasize energy-efficient operation

Objectives of MAC

- Collision Avoidance
  - Reduce Retransmissions
- Energy Efficiency
  - Avoid Idle Listening
- Scalability
- Latency
- Fairness
- Throughput
- Bandwidth Utilization

Energy efficiency

- Wireless sensor networks use battery-operated computing and sensing devices. A network of these devices will collaborate for a common application such as environmental monitoring.
- Sensor nodes are typically battery powered
- **Batteries** have **finite power**
- Battery replacement is a costly process to be avoided as much as possible, especially for large-scale deployments and it is often very difficult to change or recharge batteries for these nodes.
- Low power communication is required
- Sensor networks are typically deployed in an ad hoc fashion, with individual nodes *remaining largely inactive for long periods of time*, but then becoming suddenly active when something is detected.
- **Prolonging network lifetime** is a critical issue.

Reasons of energy waste

- ***Collision***: When a node receives more than one packet at the same time, these packets are termed **collided**, even when they coincide only partially. All packets that cause the *collision* have to be discarded and retransmissions of these packets are required, which increase the energy consumption.

- ***Overhearing***: meaning that a node receives packets that are destined to other nodes.

- ***Control-packet overhead***: A minimal number of control packets should be used to make a data transmission.

- ***Idle listening***: listening to an idle channel in order to receive possible traffic.

- ***Overemitting***: caused by the transmission of a message when the destination node is not ready.

Communication patterns

1. Broadcast or Interest Dissemination (1 to All)

- **Definition**: A communication pattern where a base station (sink) transmits information to all sensor nodes in the network.
- **Receivers**: All nodes in the network are intended to receive the broadcasted information.
- **Use Cases**:
  - Dissemination of queries to gather data.
  - Program updates for sensor nodes.
  - Control packets to manage the entire system.

2. Convergecast or Data Gathering (All/Many to 1)

- **Definition**: In this pattern, all or a subset of sensor nodes send data to a single sink node.
- **Receivers**: The base station (sink) is the sole recipient of data from many sensors.
- **Use Cases**:
  - Collection of sensed data from the environment.
  - Sensor network management and monitoring.

Properties of a well-defined mac protocol

- To design a good MAC protocol for wireless sensor networks, the following attributes must be considered
- **Energy efficiency:** energy-efficient protocols in order to prolong the network lifetime must be defined
- **Scalability** and **adaptability to changes**: changes in network size, node density, and topology should be handled rapidly and effectively for successful adaptation
- Latency, throughput, and bandwidth utilization may be secondary in sensor networks, but desirable

Techniques for WSN MAC

SAPIENZA
UNIVERSITÀ DI ROMA

Contention based	Scheduled based: Fixed assignment or on demand
• On-demand allocation for those that have frames for transmission • Sensing the carrier before attempting a transmission • **Scalable / no need for central authority** • **Idle listening / Interference / Collisions / Traffic fluctuations -> Energy consumption** • **Multi-hop topologies (hidden / exposed terminal problem)**	• Schedule that specifies when, and for how long, each node may transmit over the shared medium • **Energy efficient** • **Interference, collisions are not a problem** • **Synchronization** • **Central authority**

Contention-based MAC Protocols

- There is a contention to access channel (it is not assigned)
- Channel access through **carrier sense** mechanism
- Provide robustness and scalability to the network
- Collision probability increases with increasing node density

Contention-Based MAC Protocols: CSMA/CA (IEEE 802.11)

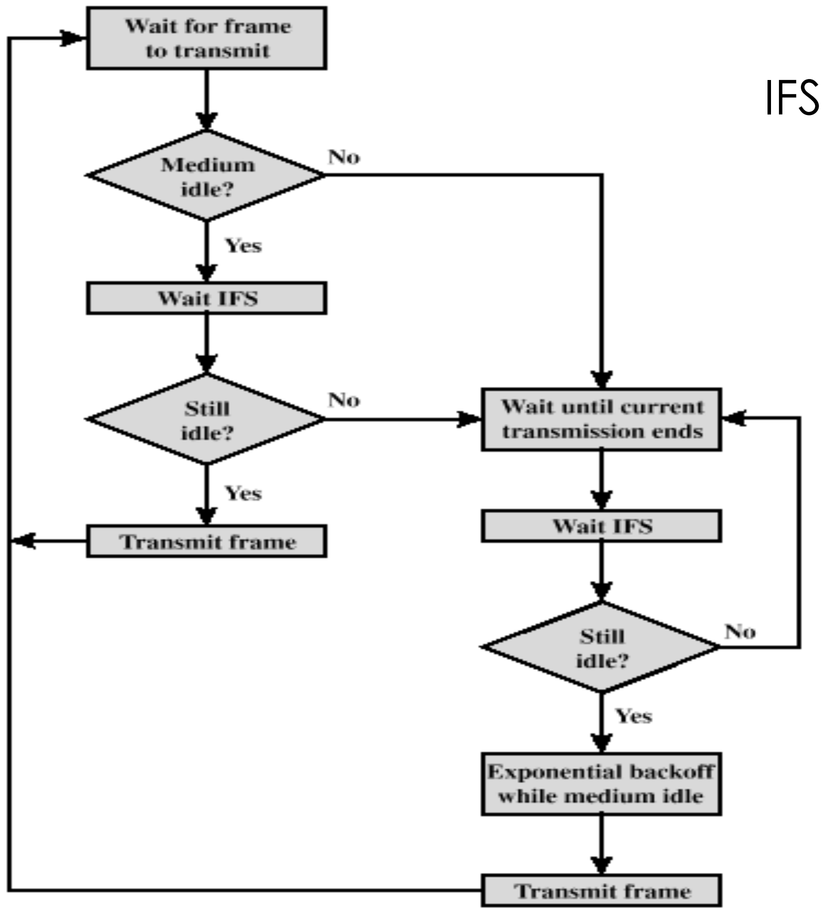
CSMA/CA

- Carrier Sense Multiple Access with Collision Avoidance
- In wireless networks it is not possible to detect collisions (interrupt a transmission)
- CSMA/~~CD~~
- Goal: if you cannot detect collision then you must try to **avoid** them as much as possible!
- Distributed protocol (no central entity!)

CSMA/CA

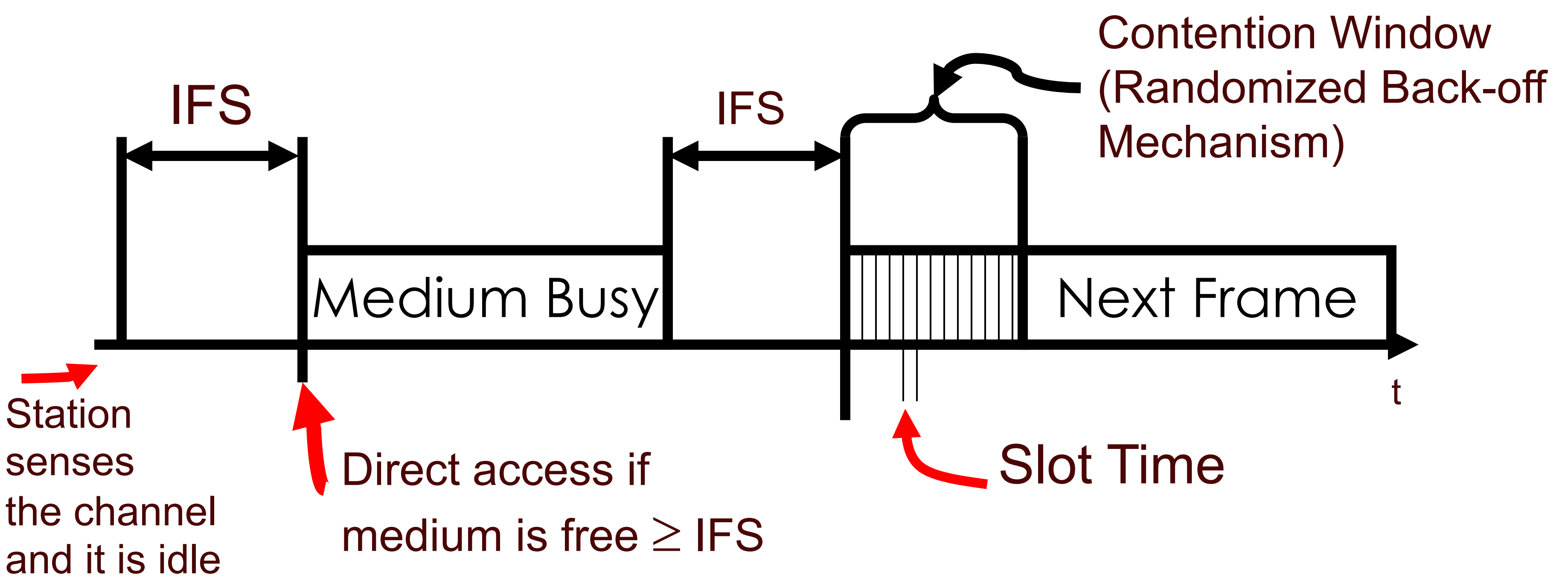
IEEE 802.11 Distributed Coordination Function

IFS: interframe space



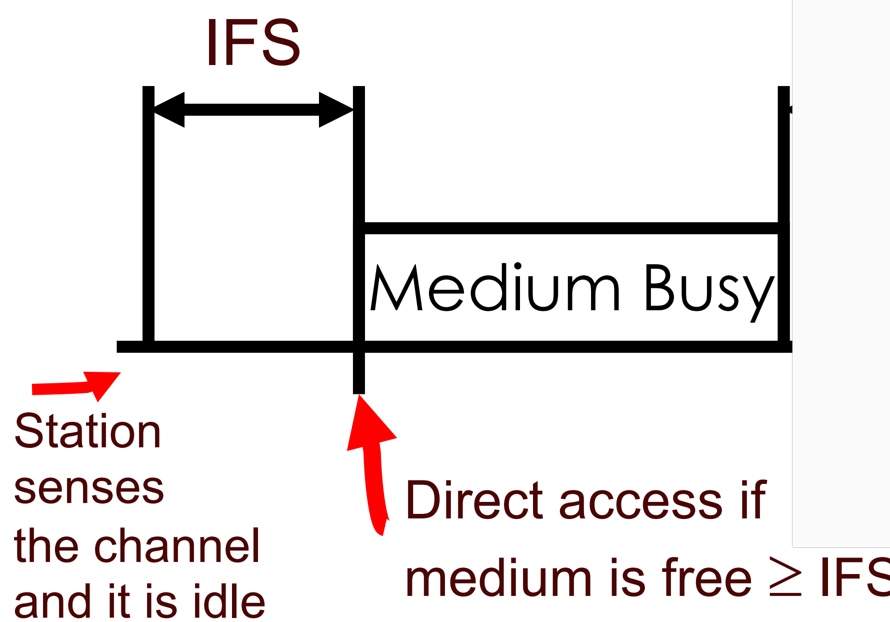
IEEE 802.11, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," 1999

Basic CSMA/CA



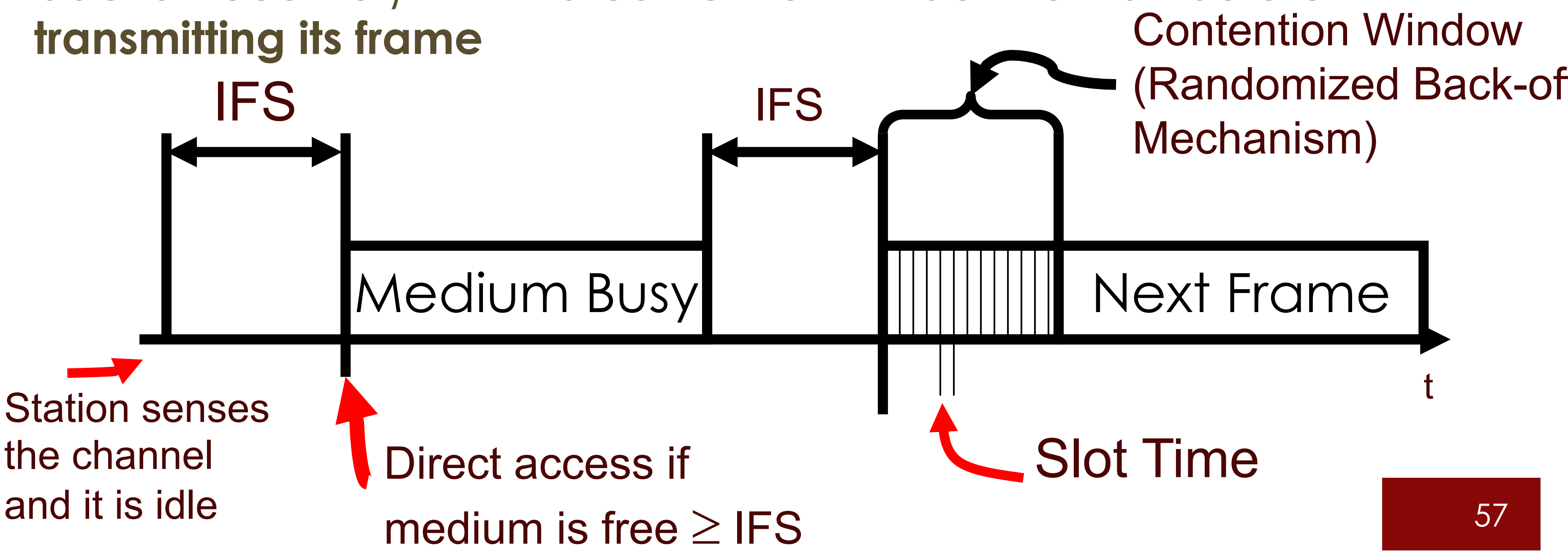
Basic CSMA/CA

- A station with a frame to transmit senses the medium (channel)
- IF IDLE -> waits to see if the channel remains idle for a time equal to IFS (inter-frame spacing). If so, the station may transmit immediately
- IF BUSY -> (either because the station initially finds the channel busy or because the channel becomes busy during the IFS idle time), the station defers transmission and continues to monitor the channel until the current transmission is over



Basic CSMA/CA

- Once the current transmission is over, the station **delays another IFS**
- If the medium remains idle for this period, the station **backs off** using a **binary exponential backoff** scheme and again keeps sensing the medium
- **The station picks up a random number of slots** (the initial value of backoff counter) **within a contention window to wait before transmitting its frame**



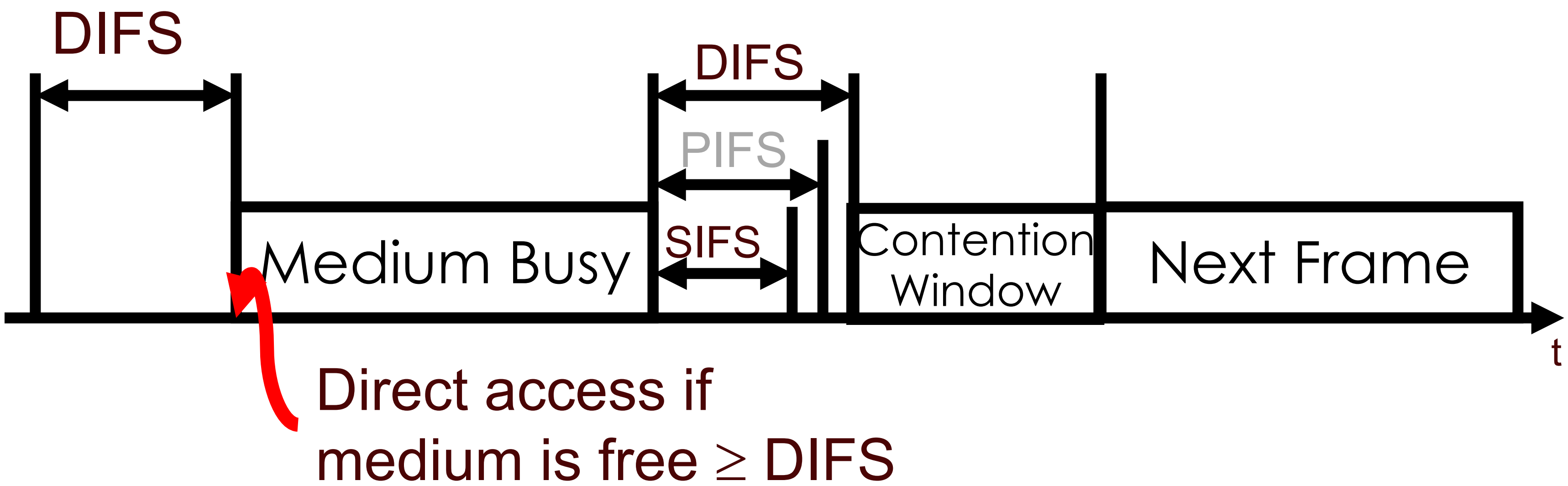
Backoff implementation

- MAC runs a **random number** generator to set a BACKOFF CLOCK for every contending station
- The backoff clock is randomly chosen between [0, CW-1], where CW represents a CONTENTION WINDOW
- During contention, all stations having packets for transmission run down their BACKOFF clocks
- The first station whose clock expires starts transmission
- Other terminals sense the new transmission and freeze their clocks to be restarted after the completion of the current transmission in the next contention period

CSMA/CA Algorithm

- If Collisions (Control or Data)
- Binary exponential increase (doubling) of CW
- Length of backoff time is exponentially increased as the station goes through successive retransmissions

Different Inter-frame Spaces (IFS)for different priorities



Inter-frame Spaces (IFS)

- Priorities are defined through different inter frame spaces

- SIFS (Short Inter Frame Spacing)
  - Highest priority packets such as ACK, CTS, polling response
  - **Used for immediate response actions**

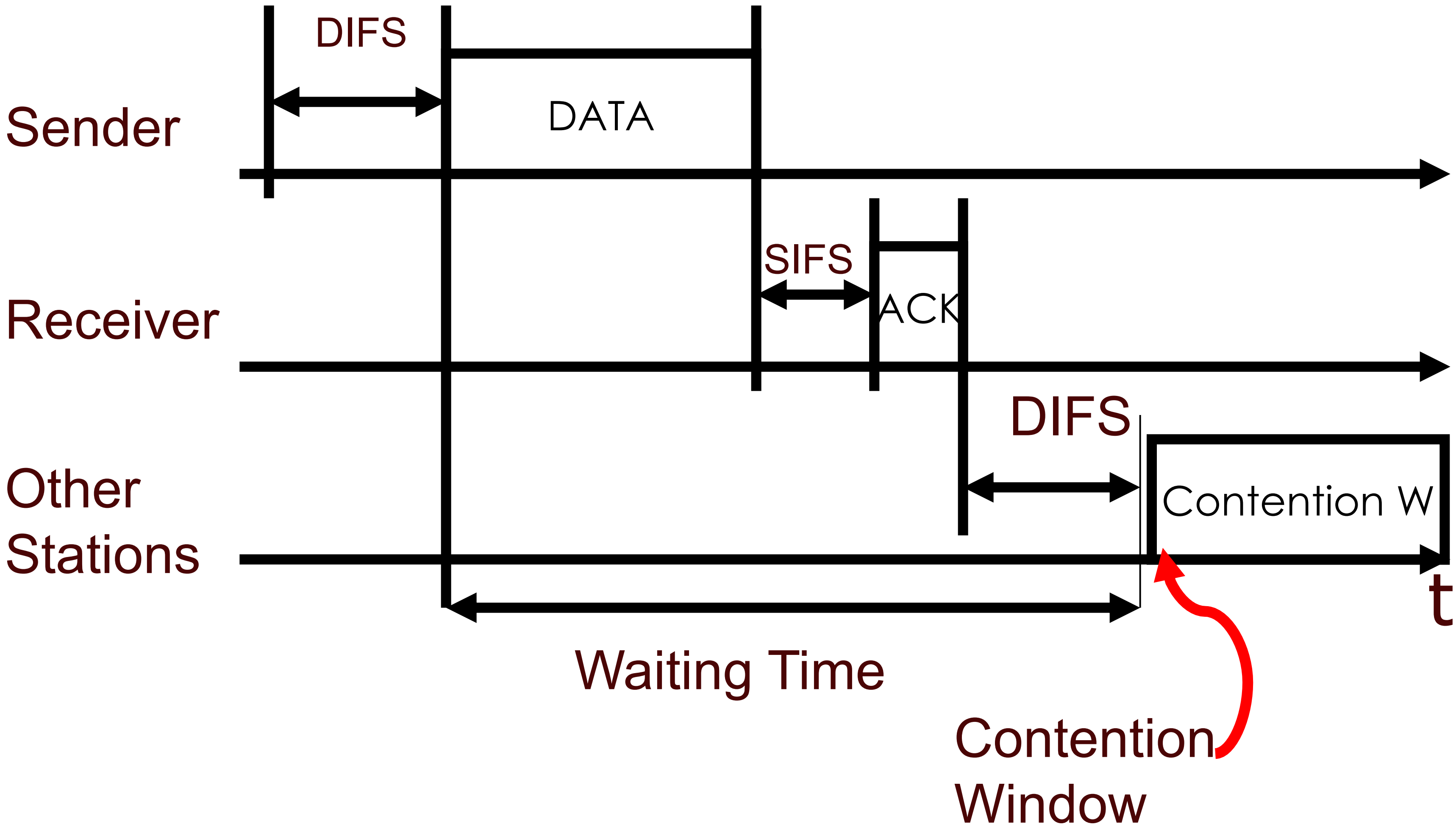
- PIFS (PCF IFS, Point Coordination Function Inter Frame Spacing)
  - Medium priority, for real time service using PCF
  - SIFS + One slot time
  - Used by centralized controller in PCF scheme when using polls

- DIFS (DCF, Distributed Coordination Function IFS)
  - Lowest priority, for asynchronous data service
  - SIFS + Two slot times
  - **Used as minimum delay of asynchronous frames contending for access**

DCF CSMA/CA with ACK

- Station has to wait for DIFS before sending data
- Receiver ACKs immediately (after waiting for SIFS < DIFS) if the packet was received correctly (CRC))
- Receiver transmits ACK without sensing the medium
- If ACK is lost, retransmission done
- Automatic retransmission of data packets in case of transmission errors

DCF CSMA/CA with ACK

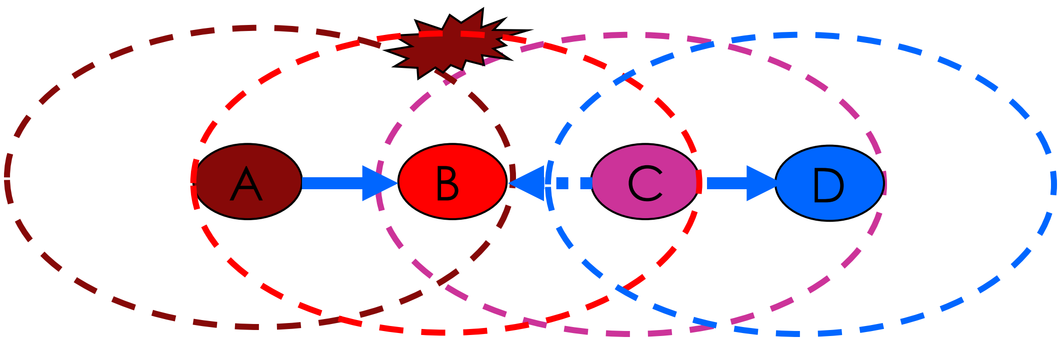


CSMA/CA

Dealing with

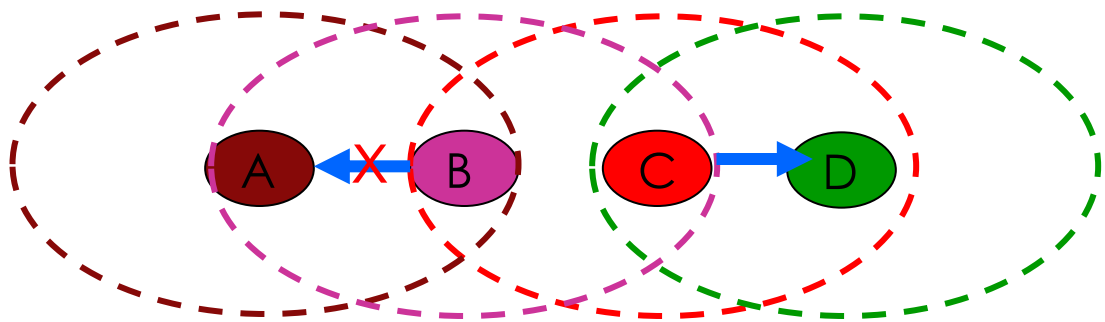
- Hiddent terminal
- Exposed terminal

Hidden Terminal Problem



- Node B can communicate with A and C
- A and C cannot hear each other
- When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
- If C transmits to D, collision will occur at B

Exposed Terminal Problem



- Node C can communicate with B and D
- Node B can communicate with A and C
- Node A cannot hear C
- Node D can not hear B
- When C transmits to D, B detects the transmission using the carrier sense mechanism and postpones transmission to A, even though such transmission would not cause collision

RTS/CTS

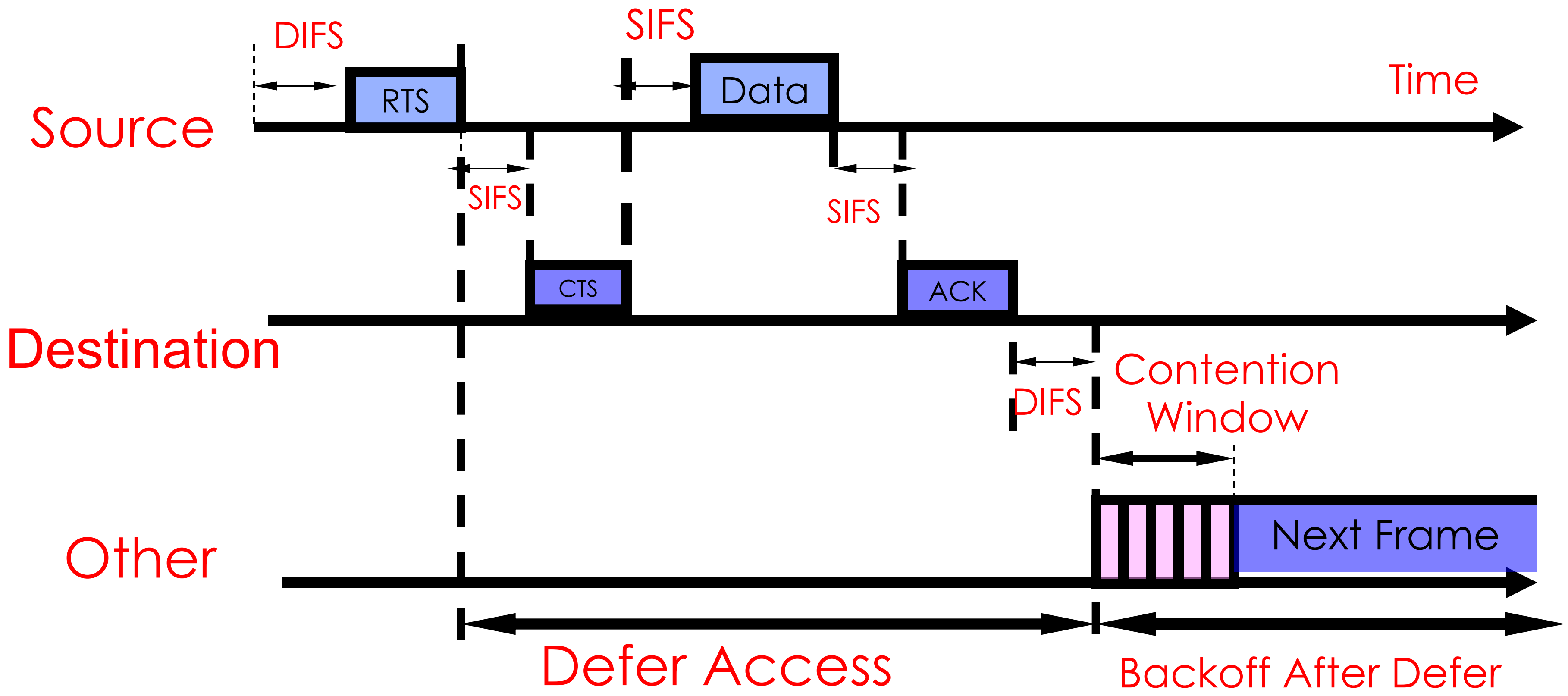
- Transmitter sends an RTS (Request To Send) after medium has been idle for time interval more than DIFS

- Receiver responds with CTS (Clear To Send) after medium has been idle for SIFS

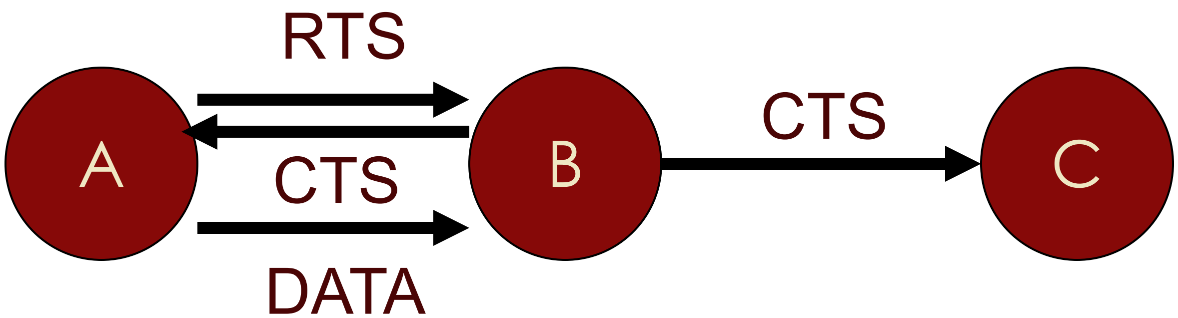
- Data is transmitted

- RTS/CTS is used for **reserving channel** for data transmission so that the collision can only occur in control message

DCF CSMA/CA with RTS/CTS

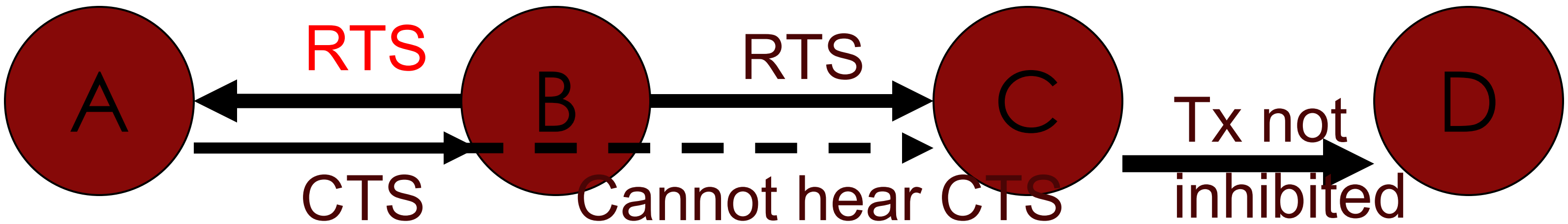


Hidden Terminal Problem Solved



- A sends RTS
- B sends CTS
- C overhears CTS
- C inhibits its own transmitter
- A successfully sends DATA to B

Exposed Terminal Problem Solved



- B sends RTS to A (overheard by C)
- A sends CTS to B
- C cannot hear A's CTS
- C assumes A is either down or out of range
- C does not inhibit its transmissions to D

Collisions

- Still possible – RTS packets can collide!

- Binary exponential backoff performed by stations that experience RTS collisions

- RTS collisions not as bad as data collisions in CSMA (since RTS packets are typically much smaller than DATA packets)

Network Allocation Vector (NAV)

- Both Physical Carrier Sensing and Virtual Carrier Sensing used in 802.11

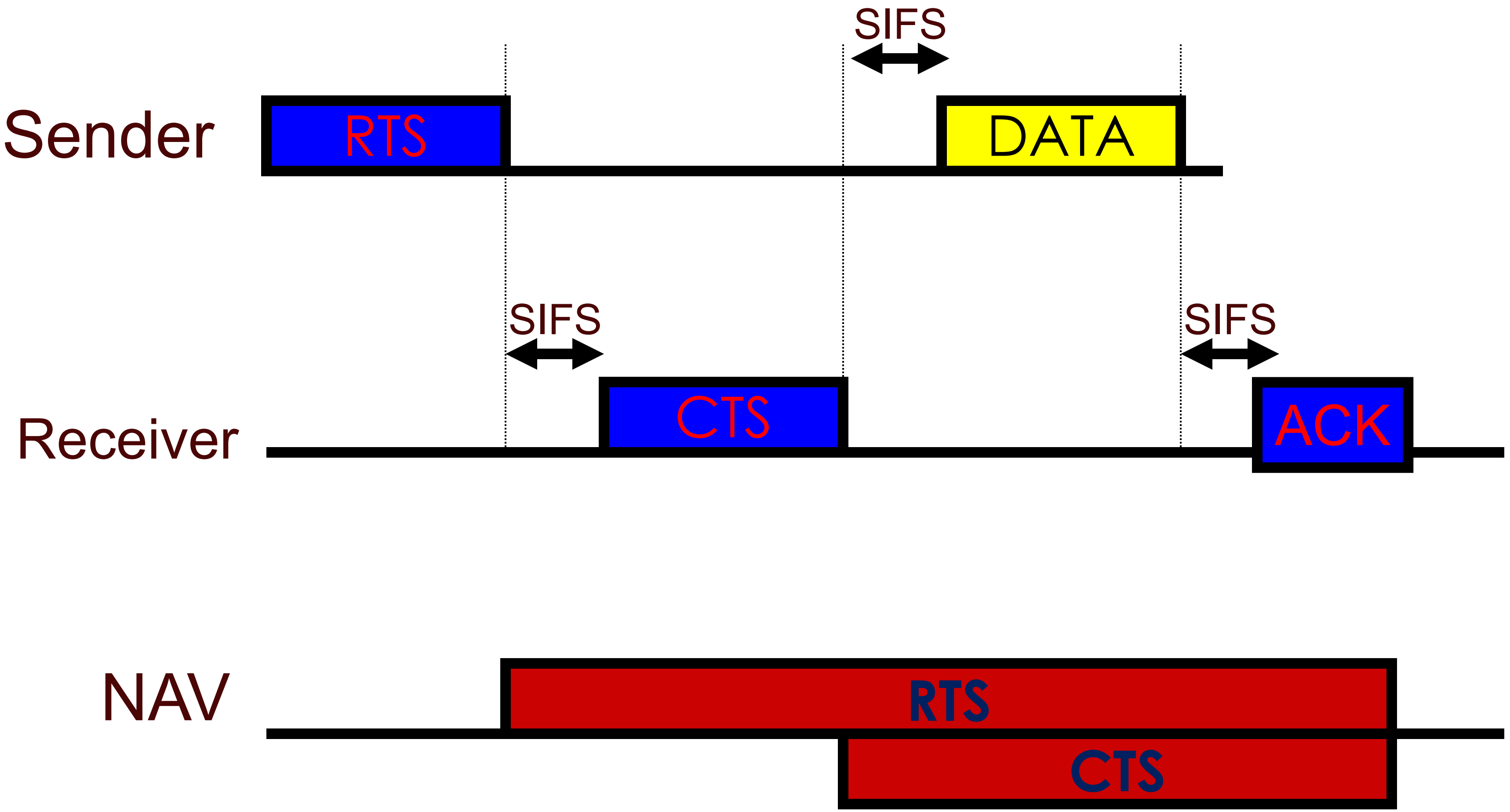
- If either function indicates that the medium is busy, 802.11 treats the channel to be busy

- Virtual Carrier Sensing is provided by the NAV (Network Allocation Vector)

Network Allocation Vector (NAV)

- Most 802.11 frames carry a duration field which is used to **reserve the medium for a fixed time period**
- Tx sets the NAV to the time for which it expects to use the medium
- Other stations start counting down from NAV to 0
- As long as NAV > 0, the medium is busy
- CHANNEL VIRTUALLY BUSY -> a NAV SIGNAL is turned on!
- Transmission will be delayed until the NAV signal has disappeared
- When the channel is virtually available, then MAC checks for PHY condition of the channel

Illustration



CSMA/CA with RTS/CTS (NAV)

- If receiver receives RTS, it sends CTS (Clear to Send) after SIFS

- CTS again contains duration field and all stations receiving this packet need to adjust their NAV

- Sender can now send data after SIFS, acknowledgement via ACK by receiver after SIFS

CSMA/CA with RTS/CTS (NAV)

- Every station receiving the RTS that is not addressed to it, will go to the Virtual Carrier Sensing Mode for the entire period identified in the RTC/CTS communication, by setting their NAV signal on
- Network Allocation Vector (NAV) is set in accordance with the duration of the field
- NAV specifies the earliest point at which the station can try to access the medium
- Thus, the source station sends its packet without contention
- After completion of the transmission, the destination terminal sends an ACK and NAV signal is terminated, opening the contention for other users