Mobile Computing & Sensing

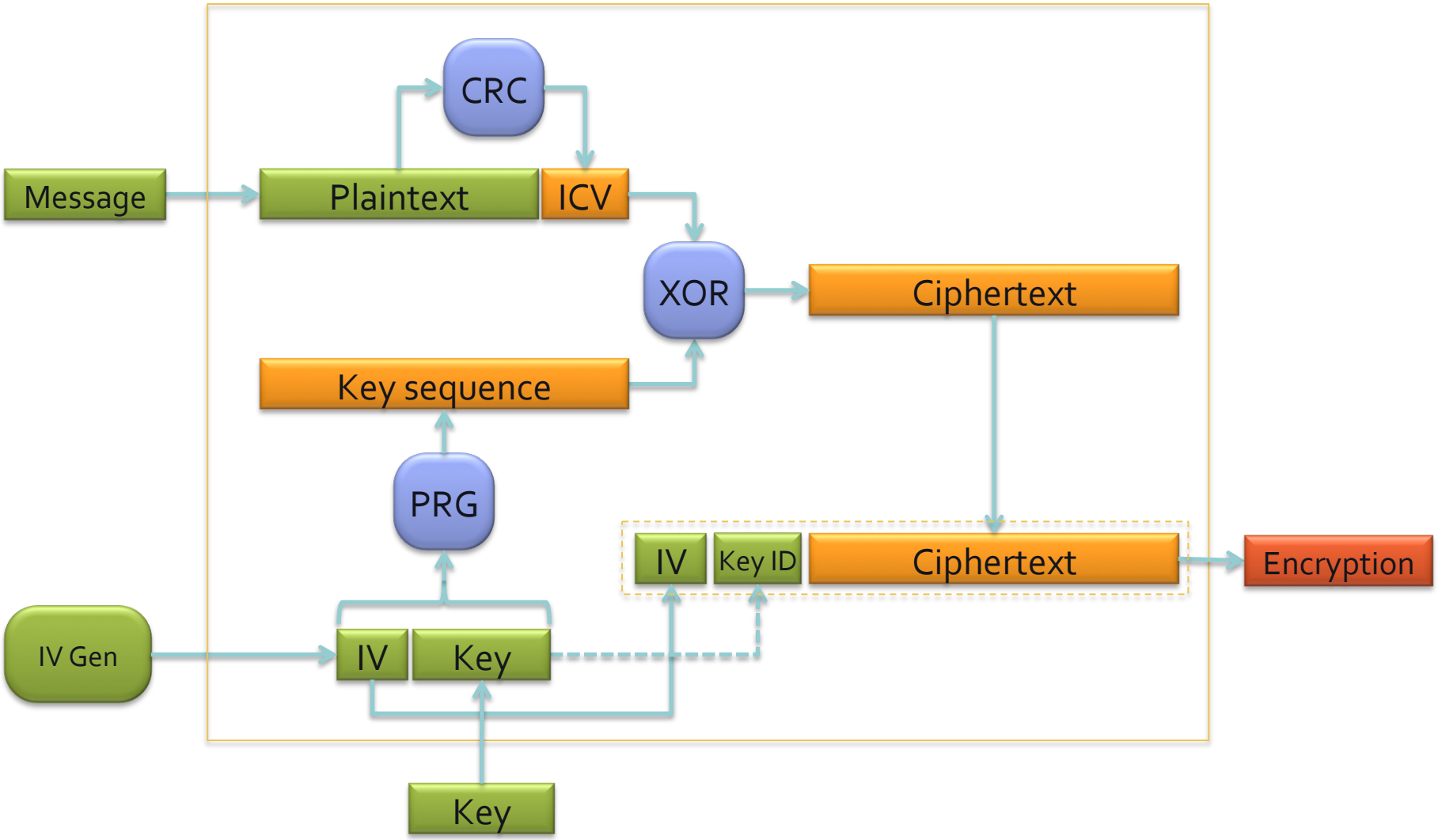
Mobile Computing

Minho Shin

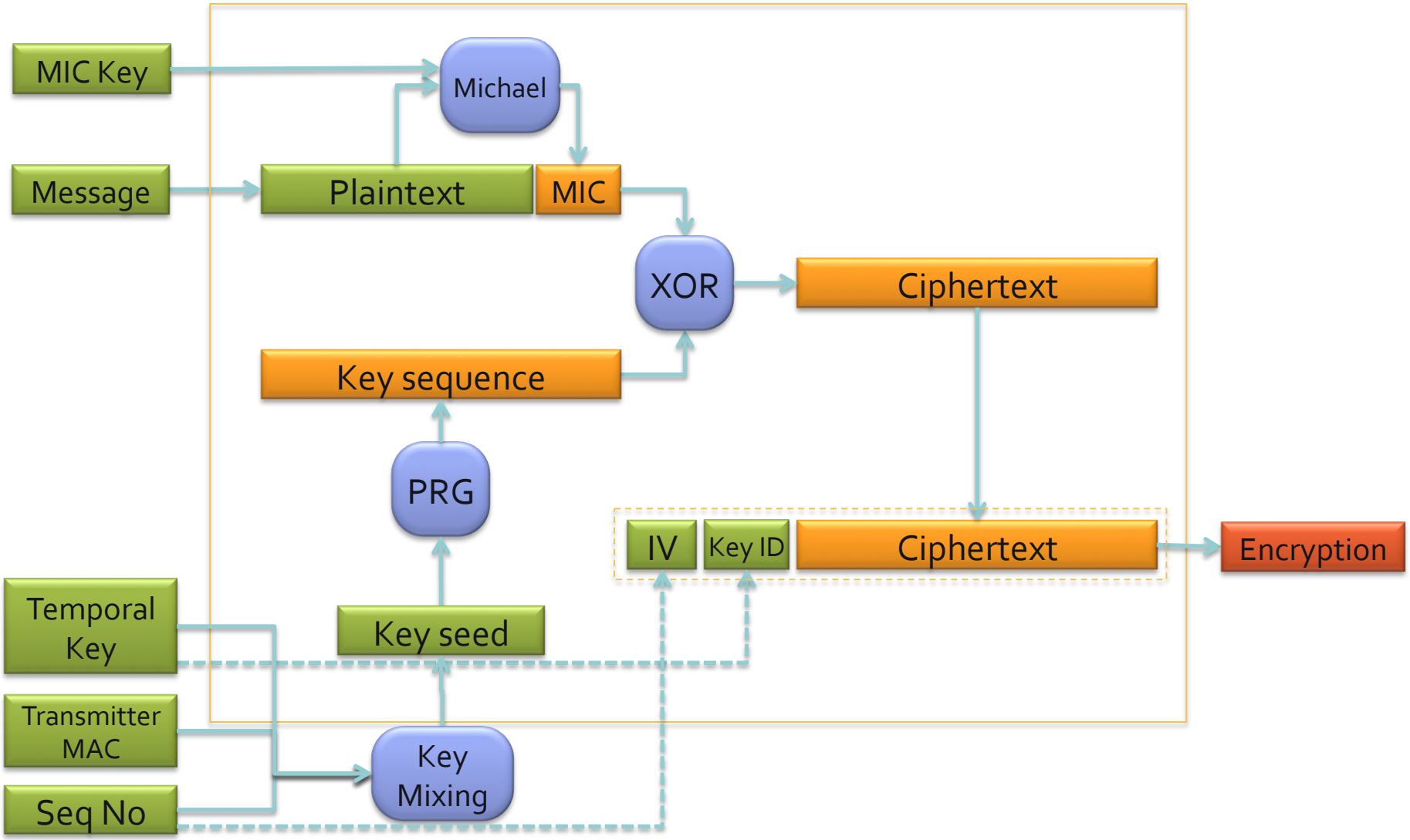
2012. 9

REVIEW: WLAN SECURITY

WEP: RC4


CRC
Message
Plaintext
ICV
XOR
Ciphertext
Key sequence
PRG
IV
Key ID
Ciphertext
Encryption
IV Gen
IV
Key
Key

Enc/Dec of TKIP



Why WEP is not secure?

- Authentication
  - Non-mutual autentication
  - Key streams are revealed with corresponding IVs
- Integrity
  - Flipping & CRC analysis allows modification
- Confidentiality
  - Frequent IV reuse reveals plaintext
  - Direct key attack possible

Quiz

- Explain how the RC4 algorithm in WEP encrypts and decrypts a frame

Quiz

- Why WEP is considered insecure in three aspects of security?

process

OUTPUT

Goals of Mobile Sensing

- Personal sensing
  - Provide services that are best for given personal context
- Large-scale sensing
  - Provide aggregate information based on a large number of user contexts

What to sense?

- About Environment
  - Air pollution
  - Noise Level
  - Brightness
  - Weather
  - Traffic
  - Near-by stores
- About the user
  - Location, Place
  - Activity
  - Social surroundings
  - Intention
  - Transportation
  - Emotion
  - Health

What is a sensor?

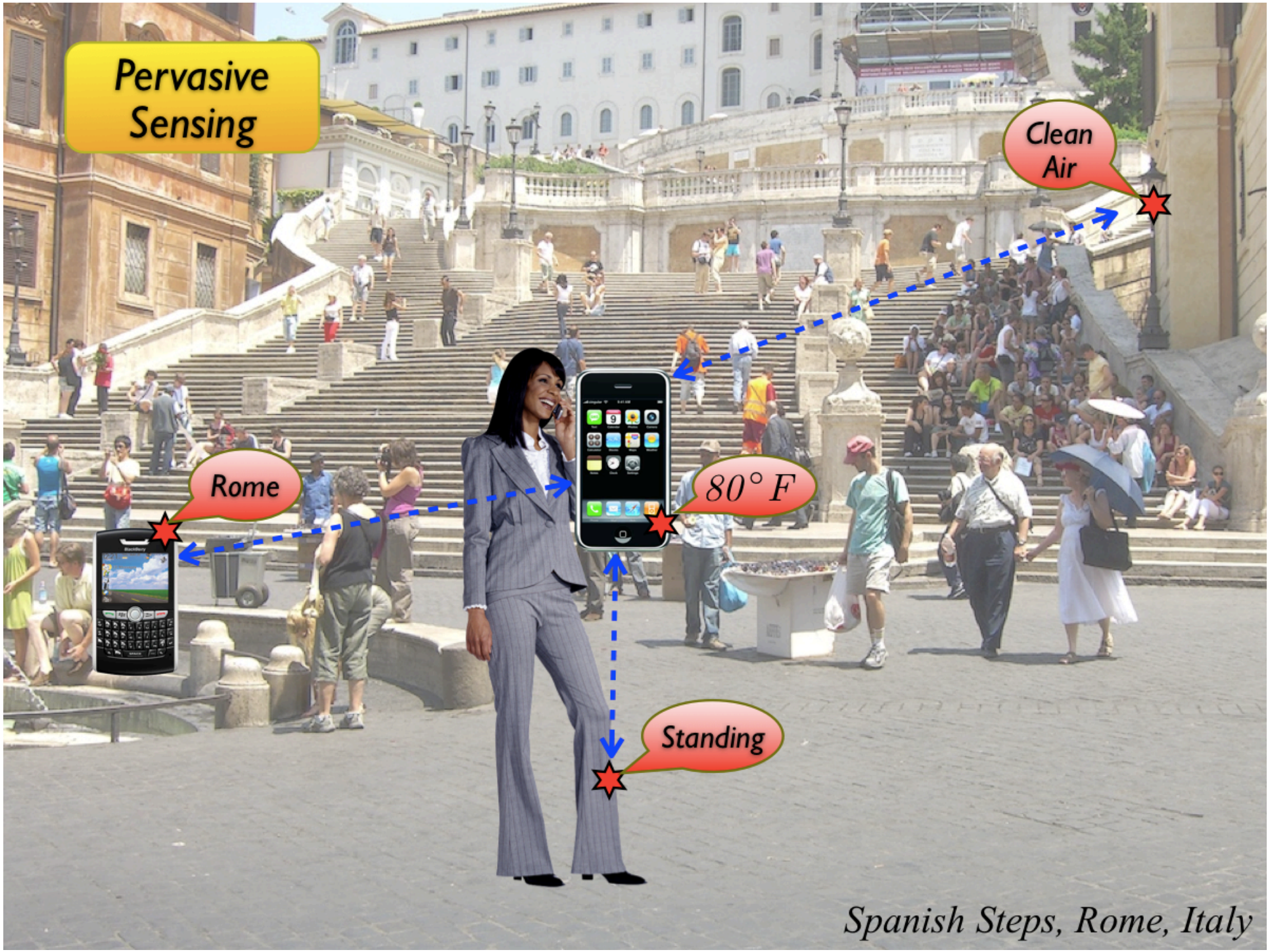
- A sensor is a (physical) device for detecting and signaling a changing condition
- Changing condition:
  - Discrete sensing: the presence or absence of an object or material
  - Analog sensing: It can also be a measurable quantity like a change in distance, size or color

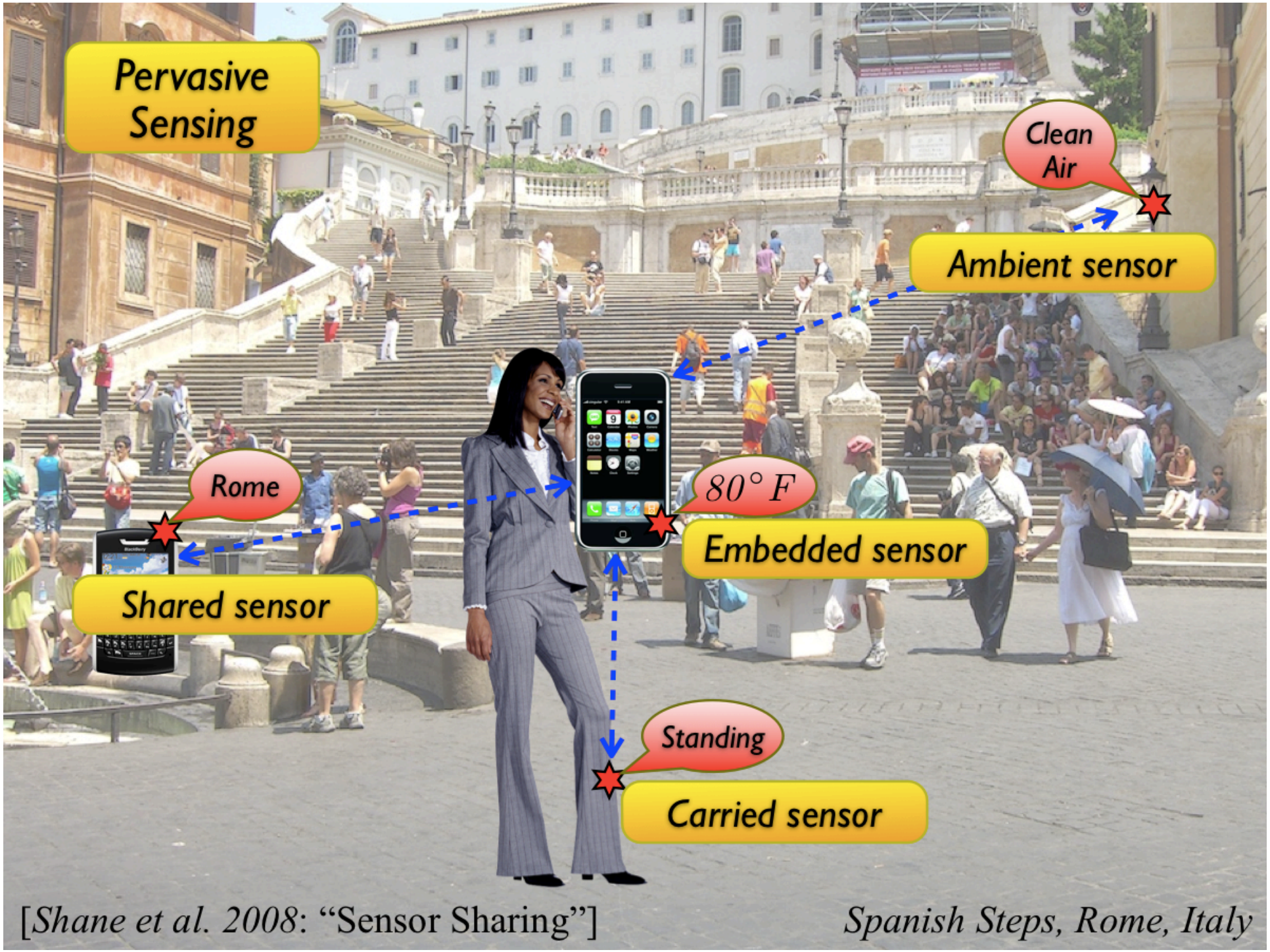

Pervasive Sensing
Spanish Steps, Rome, Italy


Pervasive Sensing
80° F
Spanish Steps, Rome, Italy


Pervasive Sensing
80° F
Standing
Spanish Steps, Rome, Italy


Pervasive Sensing
Rome
80° F
Standing
Spanish Steps, Rome, Italy


Pervasive Sensing
Clean Air
Rome
80° F
Standing
Spanish Steps, Rome, Italy


Pervasive Sensing
Clean Air
Ambient sensor
Rome
80° F
Embedded sensor
Shared sensor
Standing
Carried sensor
[Shane et al. 2008: "Sensor Sharing"]
Spanish Steps, Rome, Italy

Types of Sensors: by Location

- Embedded Sensor
  - Enclosed within the mobile device
- Carried Sensor
  - Attached to the body
- Shared Sensor
  - Shared by a near-by user (embedded or carried)
- Ambient Sensor
  - Installed on infrastructure

Virtual Sensor

- A virtual sensor is a software component for detecting and signaling a changing condition
  - from Information server
  - from PIMS (Personal Info. Management System)
  - Semantic Information

Sensor Modality

- Types of changing condition being sensed
- Smartphone embedded sensors
  - GPS
  - Accelerometer
  - Gyroscope
  - Light sensor
  - Proximity
  - Microphone
  - Camera
  - WiFi interface
  - Bluetooth interface

Sensor Modality

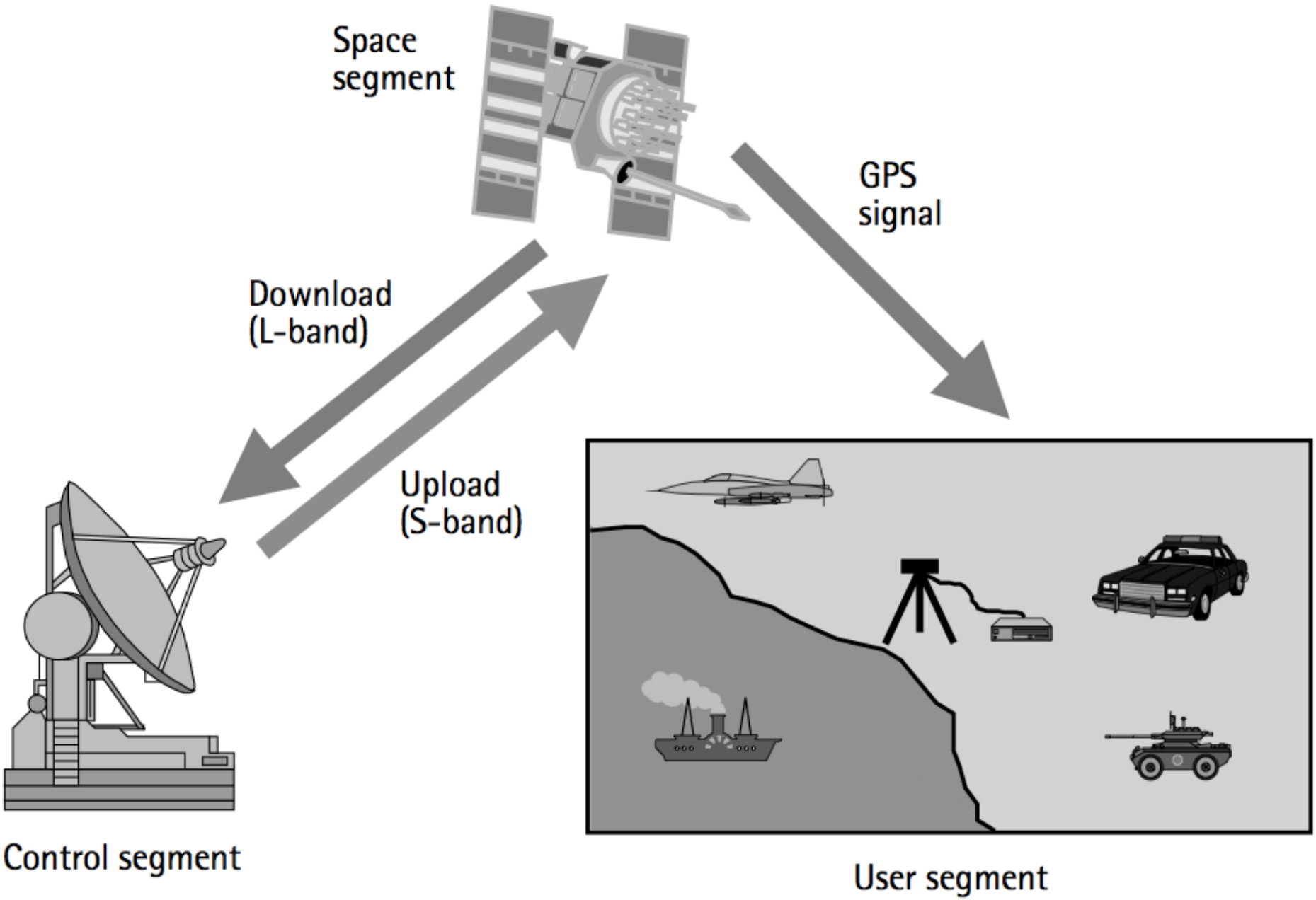
- Attached/ Installed sensors
- Environment
  - Temperature
  - Humid
  - Air pressure
  - Air pollution
- Medical
  - ECG (Electrocardiography)
  - EEG (Electroencephalograph)
  - Heart rate
  - GSR (Galvanic Skin Response)

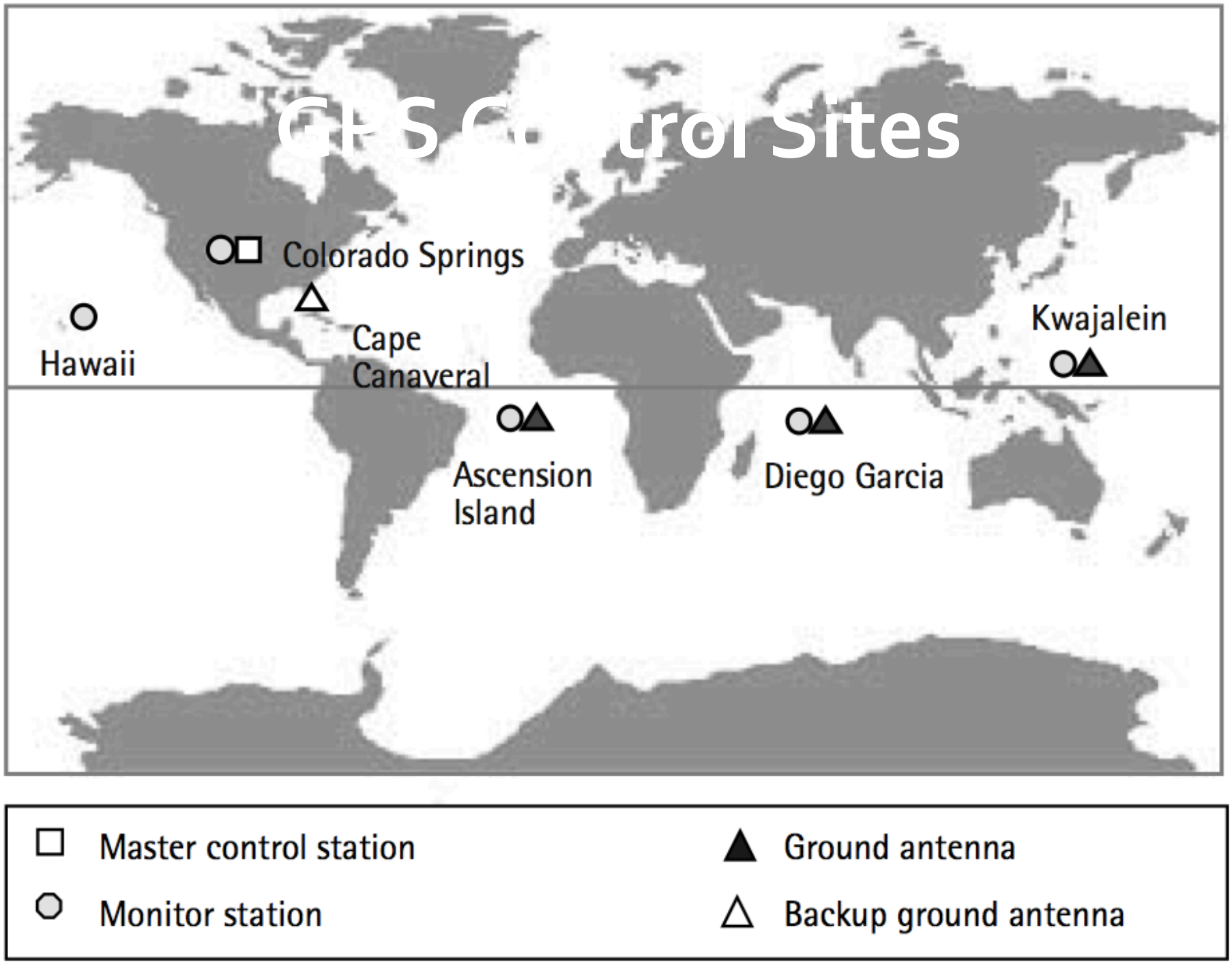
GPS: History

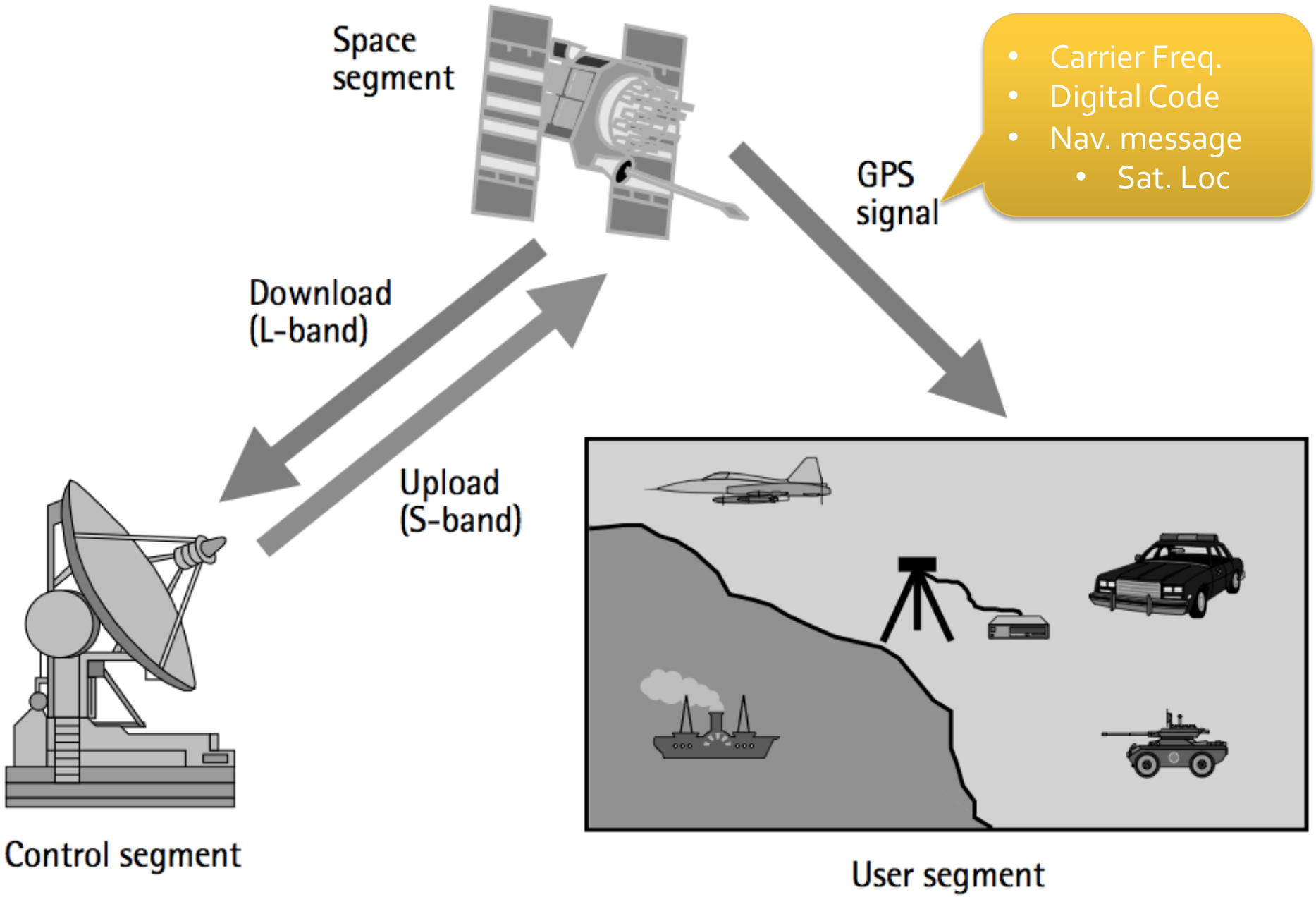
- NAVSTAR (Navigation Satellite Timing and Ranging) Global Positioning System (GPS) is a satellite-based navigation system
- Developed by the U.S. Department of Defense (DoD) in the early 1970s as a military system
- Later made available to civilians
- Now a dual-use system that can be accessed by both military and civilian users

GPS overview

- Services:
  - Location (X,Y,Z) & Time
  - Velocity
- Any- where in the world under any weather conditions.
- Serves an unlimited number of users
- Accuracy
  - 22m (95%) for single receiver
  - a few meters with two receivers (differential method)

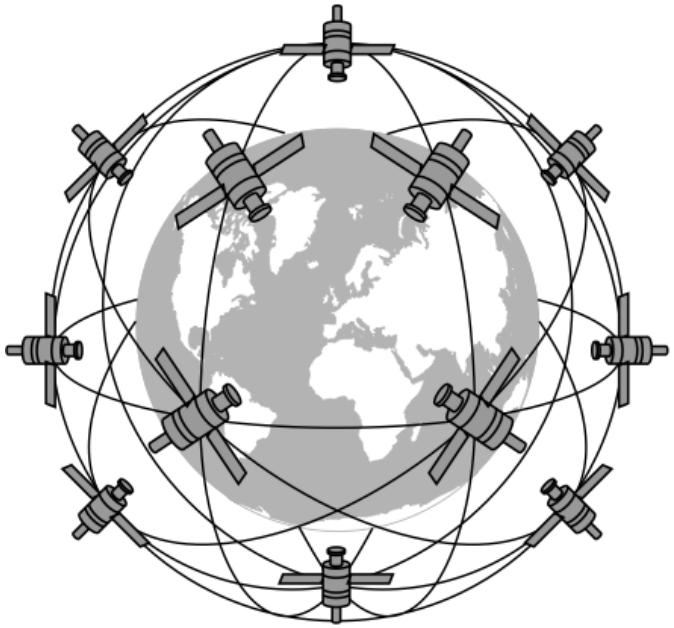

Space segment
GPS signal
Download (L-band)
Upload (S-band)
Control segment
User segment


GPS Control Sites
Colorado Springs
Hawaii
Cape
Canaveral
Kwajalein
Ascension
Island
Diego Garcia
Master control station
Monitor station
Ground antenna
Backup ground antenna


Space segment
GPS signal
Carrier Freq.
Digital Code
Nav. message
Sat. Loc
Download (L-band)
Upload (S-band)
Control segment
User segment

GPS satellites (1)

- GPS consists of 24 satellites (29 currently), orbiting 12,000 miles above at 7,000 miles/h, taking 12 hrs to circle the earth
- 4-10 satellites are visible anywhere in the world



GPS satellites (2)

- Computer: controls its flight and other functions.
- Atomic clock: accurate time within three nanoseconds
- Radio transmitter: sends signals to Earth
- NUDET Sensor (NUclear DETonation):
  - detect nuclear-weapon explosions, assess the threat of nuclear attack, and help evaluate nuclear strike damage.
- Solar-powered, lasting for around 10 years

Types of GPS signal

C/A-code

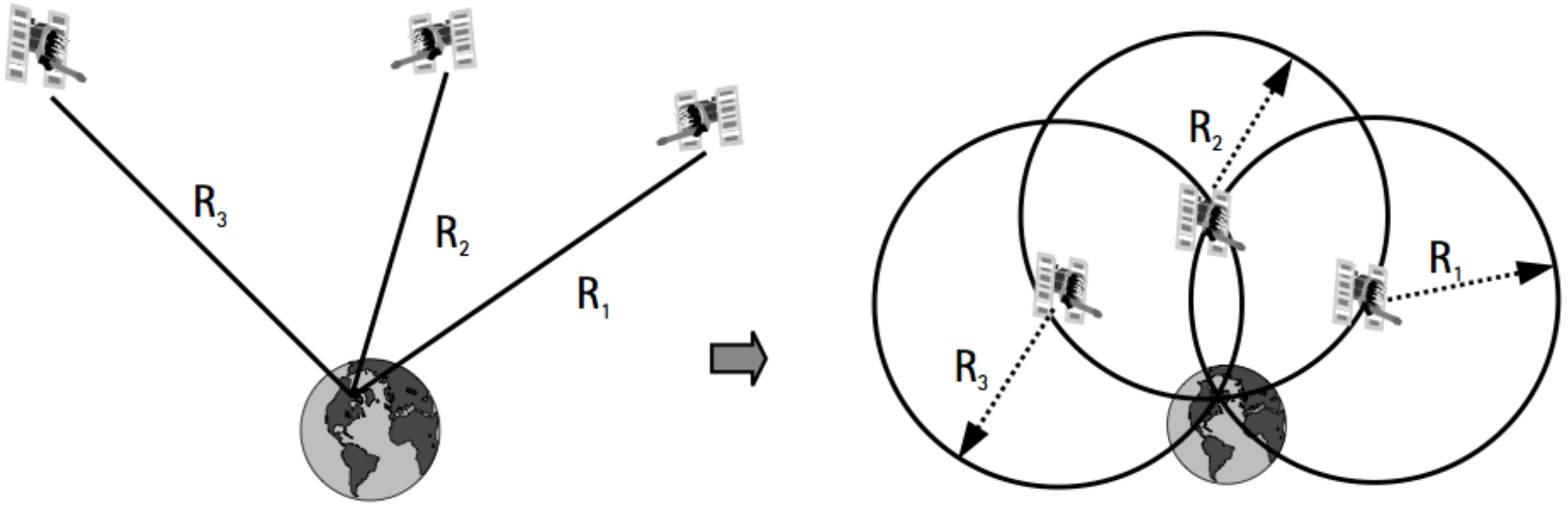
- Coarse Acquisition code
- SPS (Standard Positioning Service) at 1575.42MHz
- Less accurate
- Easier to jam and spoof
- Quick to acquire position
- Consumer GPS units
- 100m (now 22m)

P-code

- Precision code
- PPS (Precise Positioning Service) at 1227.6 MHz.
- Highly precise
- Difficult to jam and spoof.
- Encrypted
- The U.S. military only
- 16m

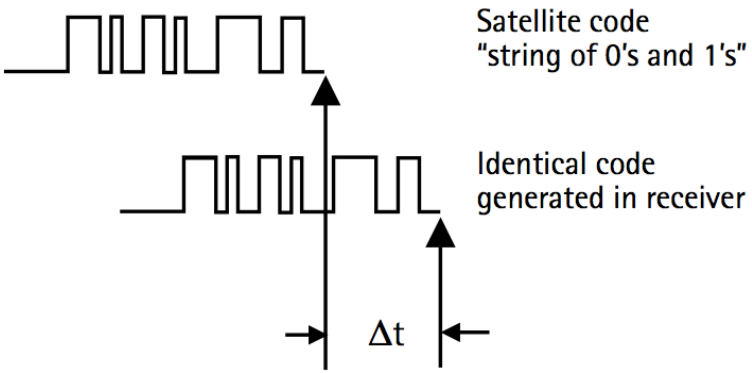
How GPS works?

- Given distances of three (or more) satellites and their locations, calculate my position
  - Location: from the Navigation Message

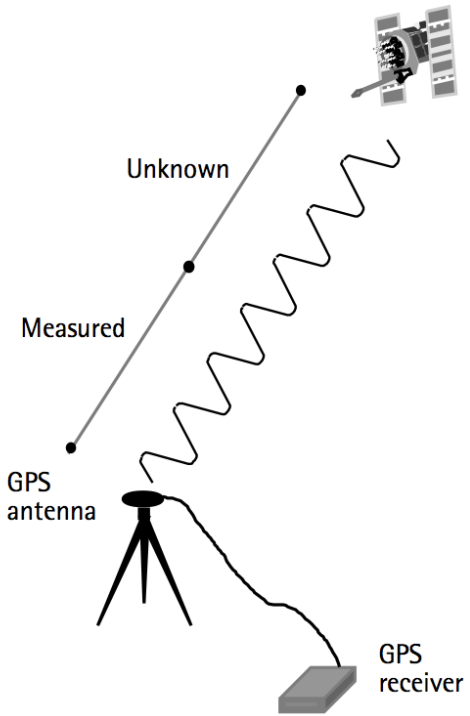


Distance Measurement

- Pseudorange measurement



- Carrier-phase measurement



GPS data

- Time: time information from atomic clocks
- Location:
  - Latitude (x coordinate)
  - Longitude (y coordinate)
  - Elevation
- Speed: your moving speed.
- Direction of travel: direction of travel if you're moving.

Application of GPS data

- Raw
  - Position: LBS (Location-based Services)
  - Speed: Traffic monitoring
  - Time
- Processed
  - Mobility trace
  - Significant places analysis

GPS: Pros & Cons

- Pros:
  - Free of service
  - Fairly accurate
- Cons
  - Energy starving
  - Outdoor only
  - No semantics