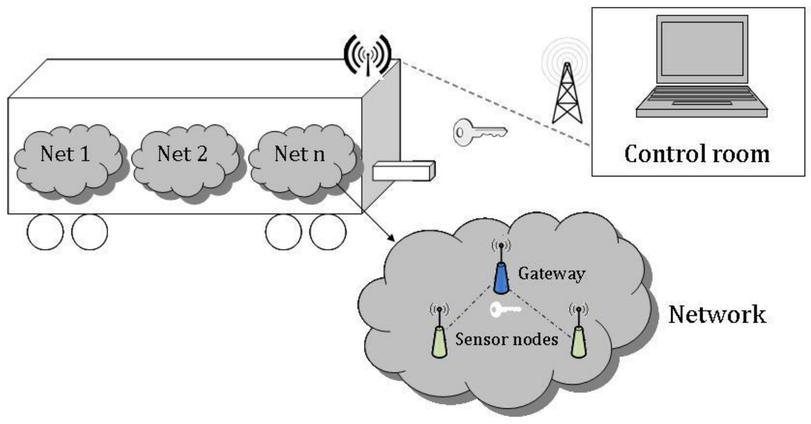
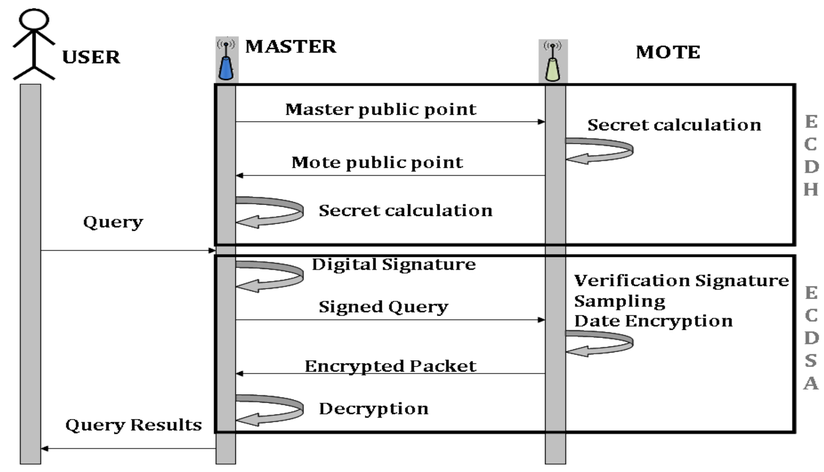
Description of the monitoring system experimentation on the freight car

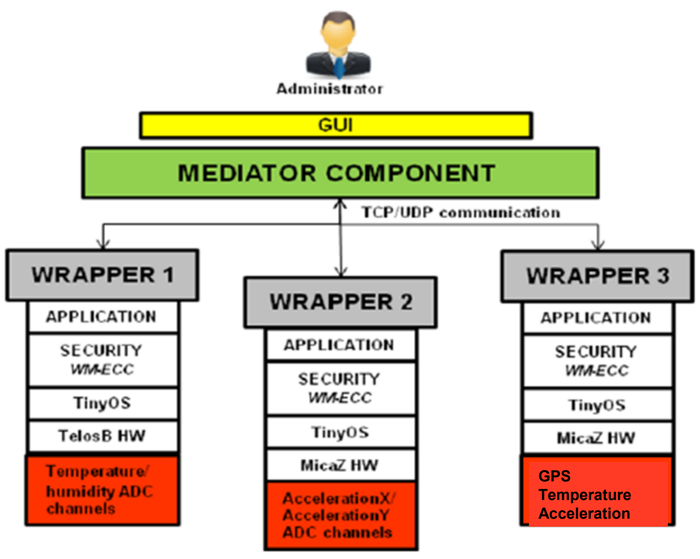
pSHIELD Demonstrator



The monitoring system features Wireless Sensor Networks (WSN) installed on the freight car and a control room in which a security management application remotely collects different data measured by the smart-sensors. Several heterogeneous networks are installed on the car, measuring different parameters (e.g. temperature, humidity, accelerations, GPS coordinates). Each network has a gateway (master node) that is responsible to send the query to the nodes (motes) through an encrypted connection, to collect the response and forward it to the control room by a secure connection.



In such a scenario, several problems and challenges need to be tackled. In particular, the issues related to **information Availability, Integrity and Privacy** need to be addressed. In order to achieve those requirements, a mechanism for key exchanging (between the master and the motes) based on the **ECDH** protocol has been implemented. It allows to establish a shared secret key for channel encryption and a mechanism to achieve broadcast authentication of query messages sent by the master to the motes through the **ECDSA** protocol. The cryptosystem is based on the WM-ECC library, a publicly available open source implementation of a 160-bit ECC (Elliptic curve cryptography) cryptosystem.



The monitoring architecture allows to manage heterogeneous networks by means of a unified interface. We adopted such a platform to design a sensor network infrastructure where heterogeneity lies both in technological aspects and security requirements.

In particular, regarding the pSHIELD experimentation, three different networks have been installed on the car: the first measures temperature, the second measures acceleration and the third measures GPS coordinates, temperature and accelerations

.

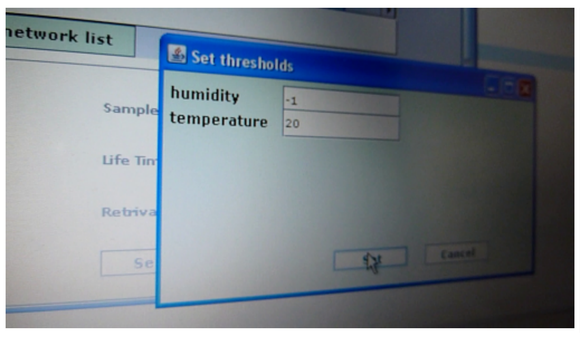
Testbed Architecture

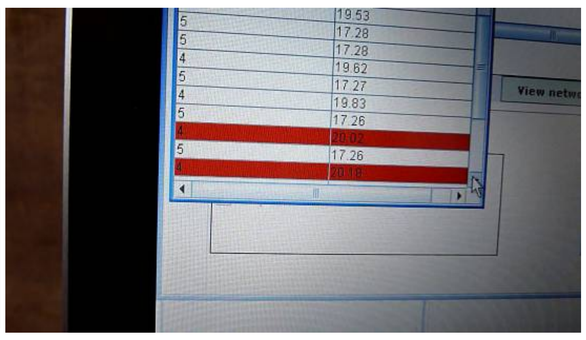
For the on-the-field experimentation, the monitoring system has been installed and tested on a real freight car by taking advantage of a trial-site made available by the Italian Railway Authority (RFI/Trenitalia) at the Roma Smistamento station.

The WSN have been installed both inside and outside the car. The network measuring the temperature, installed inside the car, is based on TelosB motes. The other two networks, installed outside the car, are based on MicaZ sensors measuring temperature, acceleration and GPS coordinates.

Functional Requirements

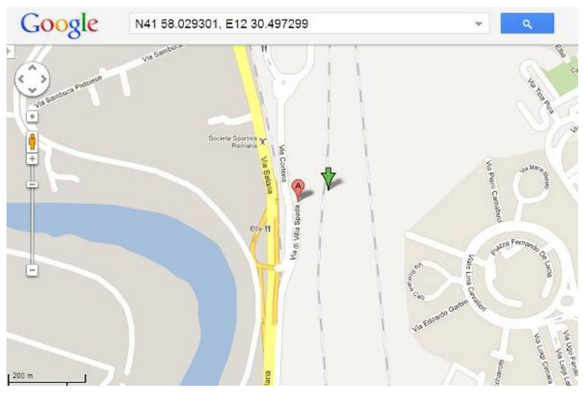
Through a specifically developed application and appropriate queries, the monitoring platform continuosly collects the parameters of interest: temperature, humidity, acceleration and GPS coordinates.
Values exceeding the user preset thresholds are highlighted in red.





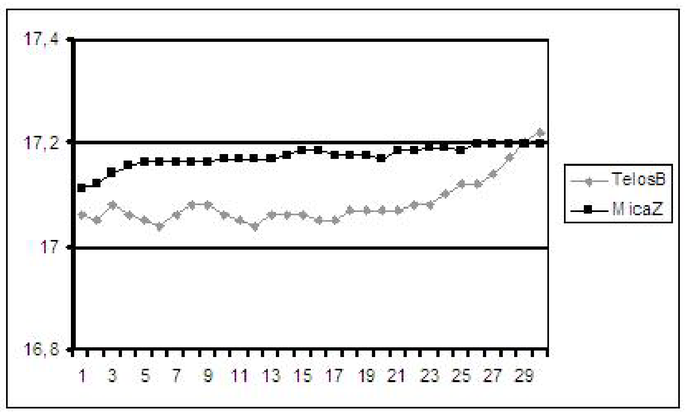

```
[2011/12/06 15:58:58] MTS420 [sensor data converted to engineering units]:
   Fix taken at 14:58:45.000000 UTC
   Latitude 41 deg 58.033401
   Longitude 12 deg 30.496000

[2011/12/06 15:59:02] MTS420 [sensor data converted to engineering units]:
   Fix taken at 14:58:49.000000 UTC
   Latitude 41 deg 58.029301
   Longitude 12 deg 30.497299
```



SPD Functionalities

A security attack has been simulated in which an intruder node tries to intercept the ECDH protocol in order to pick up private information. Since the master node knows the nodes participating in the protocol and by their ID Number (established at system deployment), it becomes aware of an intrusion, then it immediately toggles a red led and stops the communication.



Furthermore, in order to achieve fault-tolerance through data redundancy and diversity, the third network measures the same parameters of the other two by using different hardware (TelosB vs MicaZ sensors).

The graph above shows that – within a reasonable deviation – the values measured during the on-the-field experimentation are the same. A real-time comparison of those values allows to detect and discard faulty measures.