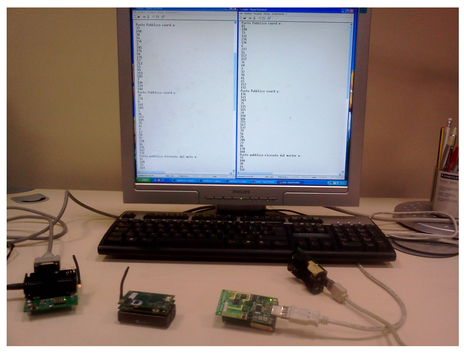
Description of the architecture and SPD-functionalities of the rail car monitoring system

Objective

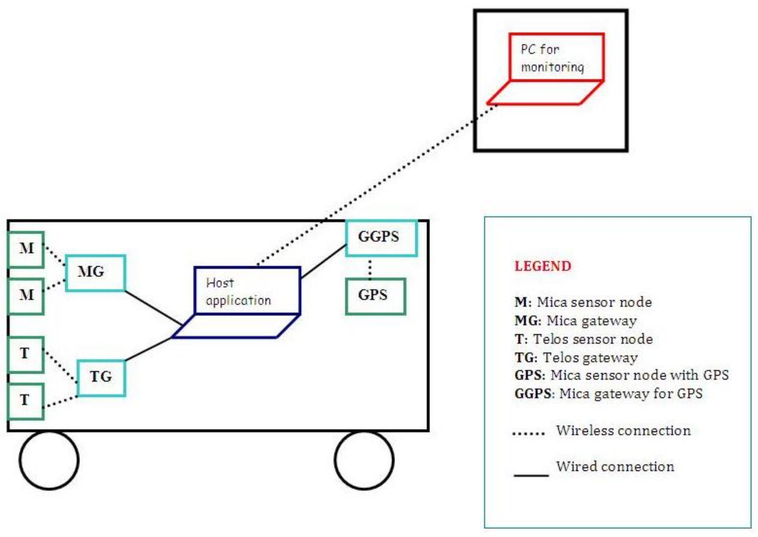
To ensure secure and dependable monitoring of rail cars transporting hazardous materials, providing resiliency against both random and malicious threats

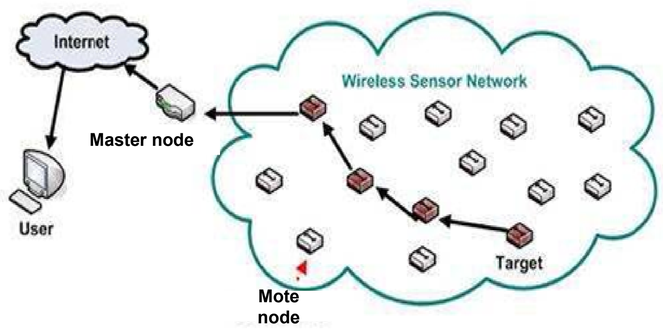


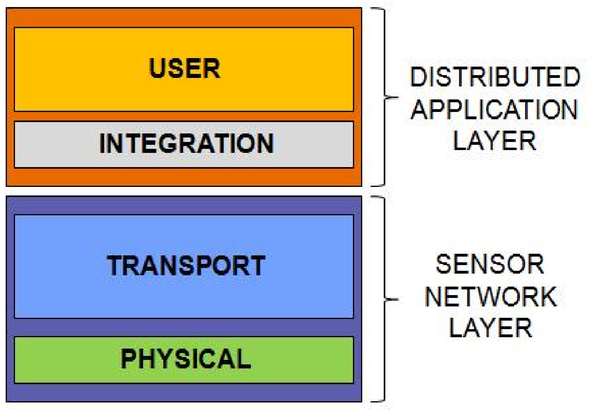
Phases of the experimentation:

- 1 – Provide SPD functionalities to off-the-shelf smart-sensors (i.e. WSN motes) measuring environmental parameters like temperature, vibrations, etc. and test them in the laboratory
- 2 – Develop a monitoring application detecting abnormal operating conditions and test the overall system in a real-environment for SPD functionalities like node authentication, checksum, cryptography, etc. also by simulating SPD threats

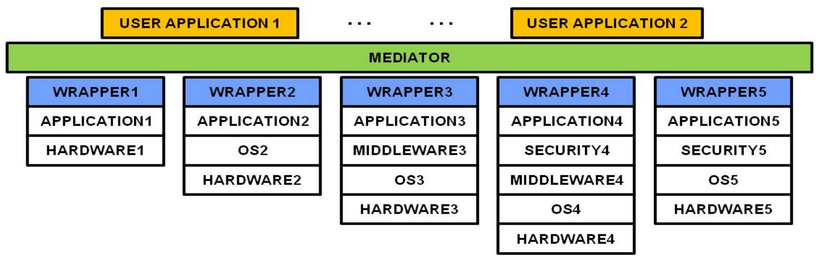
Architecture of the Testbed







A monitoring system can be structured into 2 main layers:
sensor network layer
Physical level: is responsible of the processing of the locally generated data at the node level
Transport level: controls the communication between the nodes of the network
application layer
Integration level: is responsible of the integration of data belonging to different sensor networks
User level: executes the user distributed applications



The monitoring architecture allows to manage heterogeneous networks by means of a unified interface. We adopted it to design an heterogeneous sensor network infrastructure where the heterogeneity is not only in the technology aspects but also in the different security requirements. The proposed architecture allows to cope with new security features by means of ad-hoc wrappers matching the underlying security mechanisms and protocols.

SPD Functionalities

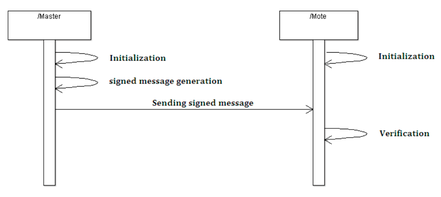
The proposed cryptosystem

In order to enforce security requirements at the transport level of our reference sensor network, we exploited the WM-ECC library (*) to:
- implement a mechanism for *key exchanging* between the master and the motes based on the ECDH protocol in order to establish a shared secret key for channel encryption
- achieve *broadcast* authentication of query messages sent by the master to the motes
- achieve *end-to-end encryption*, integrity and freshness of query response messages sent by motes to the base station by exploiting the Skipjack cipher

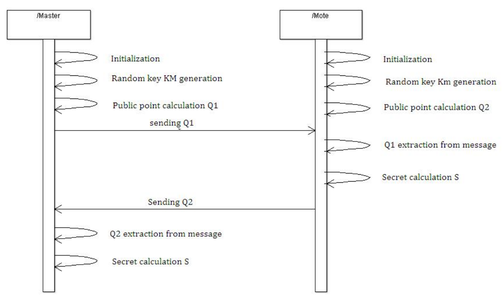
(*) H.Wang, B. Sheng, C.C. Tan and Qun Li, *WM-ECC: an Elliptic Curve Cryptography Suite on Sensor Motes*, Technical report, Oct. 30, 2007

Enhancement of the WM-ECC Library with the implementation of the ECDH protocol (*)

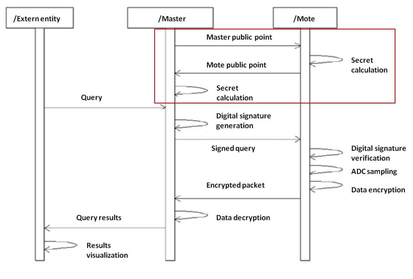
key_agree function



Message signature: ECDSA

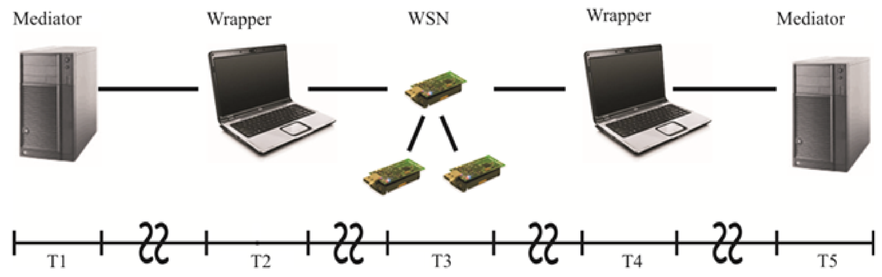


Key agreement among nodes: ECDH

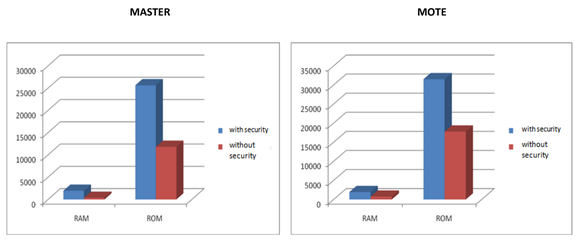


An example scenario: secure query and response

Performance Analysis



We did not consider the delays related to communications over the TCP/IP network as they depend on how the application is distributed to monitor a particular environment



Time overhead

The cryptographic operations performed at the master and mote sides for encrypting/decrypting and digitally signing packets, produce a fixed latency (about 4 seconds) in returning the first results to the wrapper for each executed query this can certainly be acceptable in all monitoring applications where real-time requirements are not very strict.