Security is crucial in IoT environment, but connected devices have:

- heterogeneous constraints
- dynamic behaviors
- heterogenous security

How to guarantee secure communication and access to the connected devices?

- manage heterogeneity of the devices, their protocols and their security.
- manage dynamism, to handle smooth arrival and departure of devices.
- handle security for all devices, from high end to low cost.
- provide convenient interfaces, to ease pervasive application development.

Device security

How security is managed in current IoT protocols?

- WiFi: Simple, mutual authentication, shared secret, confidentiality and integrity.
- 802.11a/b/g/n: Simple, mutual authentication, shared secret, configuration-dependent security.
- None, simple, mutual authentication, shared secret, yes.
- None, simple, mutual authentication, user validation, configuration-dependent security.

Security is present but heterogeneous

Strong reliance on secrets

How secrets are stored on the devices? [2]

- None: low security, low cost, low adoption.
- High: high security, high cost, domain-specific.
- Moderate: moderate security, moderate cost, low adoption.

Lack of affordable yet secure solution for low cost devices

Can PUF be a complementary solution?

Fog middleware

Objective:

- facilitate the secure communication and access with connected devices while supporting their heterogeneity and dynamism.

Main characteristics:

- secure by design with secret management, authentication and secure protocols to provide end-to-end security from applications to devices.
- security for every device, with support of solutions adapted to various constraints and security requirements.
- Service-Oriented Approach (SOA) to abstract the complexity of the devices and their security, simplifying access for applications.
- module-based architecture to ease the dynamic integration of new protocols, improving heterogeneity and dynamism support.

Implementation and Validation

Featured technologies:

- modules implemented as micro-services with a reactive Java framework.
- secure REST interfaces provided by modules using HTTPS with authentication mechanisms.
- publish/subscribe secure communication used between devices and the middleware.

References