Security and Privacy issues in Structural Health Monitoring Systems

Roberto Di Pietro
Assistant Professor at Maths Dept. UniRoma3
Chair of Excellence Carlos III Madrid
dipietro@mat.uniroma3.it
Outline

• Motivations for SHMS

• Modelling SHMS
  - Adversarial model
  - Network model
  - Communication model

• SHMS Features

• S&P: What to focus on

• Conclusions
**Motivation for SHMS**

• Local damage detection methods (aka Non-Destructive Evaluation (NDE)), are old fashioned, well developed, highly efficient and used methods.

But...

• These methods have difficulties when large surface areas need to be inspected and when the damage lies below the surface.

• Need for global and automated damage detection methods.
Motivation for SHMS

- Economic and life-safety advantage

- New business models: Manufacturers of large capital investment HW can charge by the amount of life used (instead of a time-based lease).
Adversary model

• Capabilities?
  - Low end of the IT spectrum (hammer)
  - High end of the IT spectrum (Flamer)

• Motivations?
  - Industrial espionage?
    • Of the nodes
    • Of the readings/activation
  - Data preview?
  - Service Disruption (even better: poisoning)?
  - ...
Network model

- Singleton(s)?
- P2M?
- Mesh?
- P2P?
Node-to-Sink Communication Model

To the extreme:

- Real Time/QRT off-loading?
- Unattended?
Features

• Unattended nature

• Cooperating capabilities (in some scenarios)

• Static (yes, but...)

• Not tamper proof
  (but sometimes not easily reachable)

• Well defined domain of application
What's worth investigating/addressing

- Code attestation;
- Data poisoning;
- Node capture/replacement;
- Privacy (for some specific applications).

(you got it, it’s a guess---an educated one 😊 ?)
Conclusions

• Unique features of SHMS
  (individually, none of them is, but their combination is)

• S&P: years of contributions in the literature for WSNs
  (reinventing the weel?)

• Where to spend effort/time (i.e. €)?
  (risk assessment driven)
• Thank you!
• Questions?