Human and Critical Infrastructures Surveillance: Security and Investigation Issues

Presented By:

Nourhene Ellouze

ISLAIB

Higher Institute of Languages and Computer Science of Beja
University of Jendouba, Tunisia

Human and Critical Infrastructures Surveillance Applications

- Are developed using Wireless Sensor Networks (WSNs)
- Monitor and control critical assets (e.g., waterways)
- Detect suspicious events
- Characteristics of these applications:
  - Critical nature of the provided services
  - Time constraints on the responses' delivery
  - Harshness of the environments where they are deployed
  - Subject to threats on availability and accuracy

Examples of Surveillance Applications

Critical Infrastructure Surveillance

❑ Application

- Water monitoring system

❑ Critical function

- The identification and the localization of water contamination through waterways
  - Waterways exhibit irregularities and presence of obstacles

❑ Harm induced by failure

- Environmental safety

Human Surveillance

❑ Application

- Cardiac Implantable Medical Devices (cardiac IMDs)

❑ Critical functions

- The surveillance of the physiological parameters of human's body
- The delivery of life-sustaining functions, when required

❑ Harm induced by failure

- Patients' health safety

Main research Issues

- ❑ Cost minimization in the implementation of a surveillance application
- ❑ Energy preservation in the design of a surveillance application
- ❑ Accurate localization of the detected suspicious events
- ❑ Protection and resilience to security attacks
- ❑ Accurate investigation of security attacks on a surveillance application

Contributions

- Design of a RFID-based water monitoring system for the accurate localization of polluted areas
  - Design of RFID tags deployment scheme inside monitoring areas
  - Development of techniques and algorithms to minimize energy consumption
- Development of energy-aware security mechanisms to protect cardiac IMDs against security threats
  - Implementation of a radio frequency energy harvesting solution
  - Development of powerless mutual authentication protocol which prevents battery depletion attacks
- Design of techniques and methodologies for the investigation of attacks on cardiac IMDs
  - Design of a postmortem investigation system which aggregates the professional experts' efforts and the technical investigators' efforts
  - Development of an inference system and a model checking based algorithm

Outline

1. Design of a water monitoring system
2. Securing cardiac IMDs
3. Digital investigation of attacks on cardiac IMDs

Outline

1. Design of a water monitoring system
2. Securing cardiac IMDs
3. Digital investigation of attacks on cardiac IMDs

Towards the need of a Water quality surveillance application

Former and classical techniques

- ❑Rely on the use of a team of water samplers
- ❑Inability to access to obtain samples from all locations
- ❑Inaccurate localization of water contamination
- ❑laborious and expensive tasks

Design of a Water quality surveillance application

Design issues

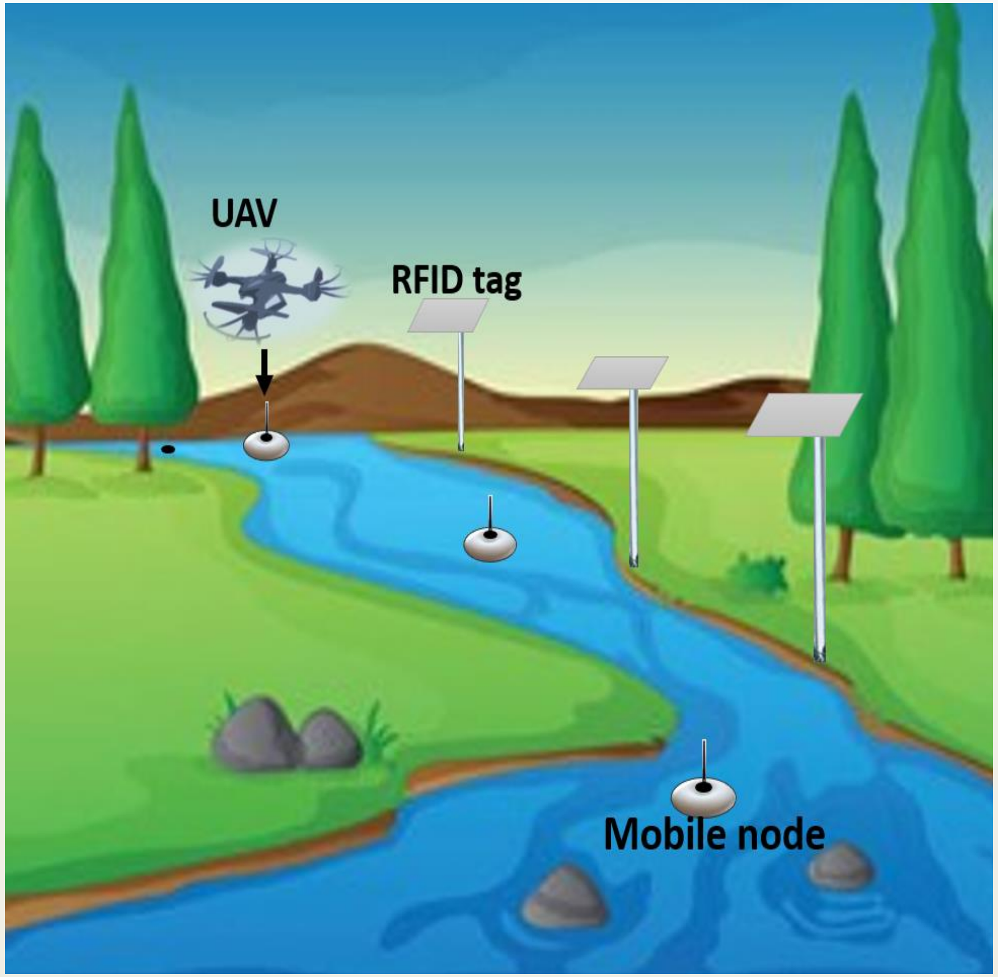
- ❑Need to cope with the irregularities and obstacles within waterways
- ❑Need to reduce energy consumption
- ❑Provision of accurate pollution detection
- ❑Assurance of system availability and scalability

Proposal

- Design of a water quality monitoring system
- Proposal of an accurate and low-energy positioning system
- Development of techniques to trace sensors activity and identify locations of blocked sensors
- Design of energy saving algorithm to minimize the energy consumption of sensor nodes

System Architecture

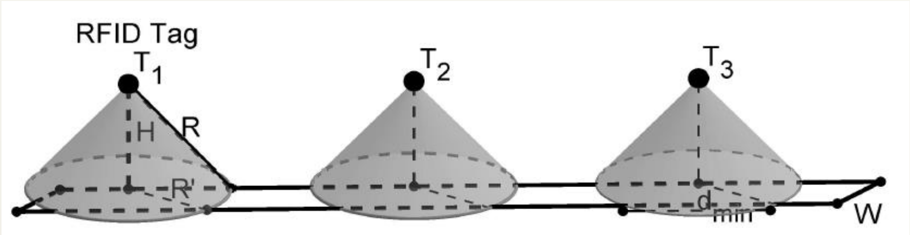
- Mobile Sensor Nodes
  - Integrate RFID readers
  - Are transported by the water flow
- RFID Tags
  - Deployed next to the waterway
  - Integrate rewritable memory
  - Provide location information to sensor nodes
  - Act as fixed sensor nodes



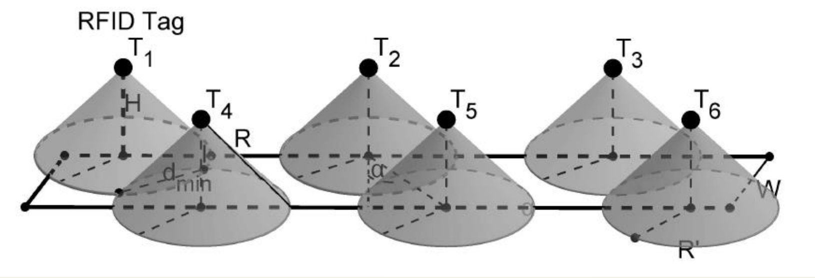
RFID tags: deployment scheme

- Tags are deployed:
  - In one or two banks based on the waterways' width
  - At a fixed height H with respect to the surface of the water
  - Their elliptical horn antennas are oriented downward
    - Emitted radio waves take a cone formation

Tags deployment in one bank



Tags deployment in two banks



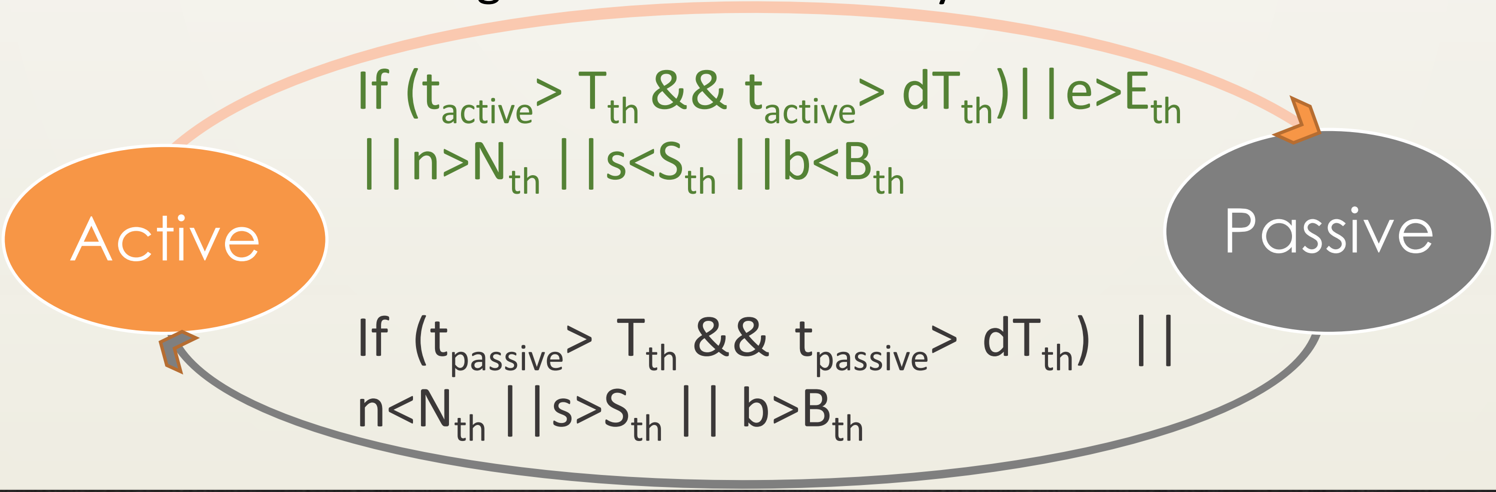
- Periodic communication between sensors and tags
  - The minimum distance of a tag coverage should allow a crossing node to at least write data and read it three times: $d_{\min} = Speed_{Max}.(T_{Writing} + 3.T_{Reading})$

Mobile nodes activities and states

- Scarcity of energy resources of mobile nodes
  - Two states (active and passive) are defined
- An **active node** should:
  - Sense pollution
  - Identify its position and compute its speed
  - Update the tag contents by recording:
    - Its identity to be located when blocked
    - Sensitive events to be forwarded to subsequent nodes
    - Its state to allow subsequent nodes determining active nodes
  - Read and transport data from the encountered tags
- A **passive node** should:
  - Neither sense pollutions nor write to the encountered tags

Energy saving algorithm

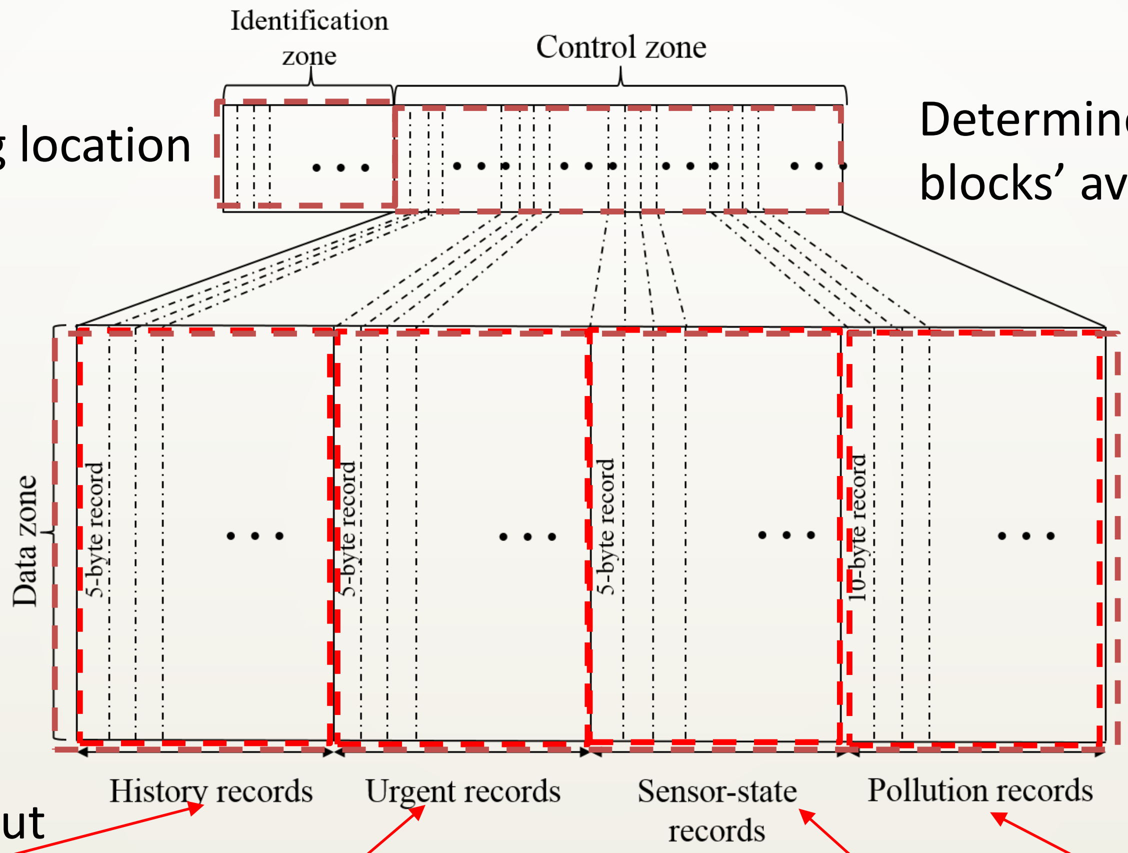
- A set of thresholds:
  - Maximum energy consumption (E_{th})
    - To reduce energy consumption
  - Minimum number of active nodes at a given area (N_{th})
    - To guarantee the required detection accuracy
  - Maximum and minimum period elapsed during a state (T_{th} , dT_{th})
    - To ensure a faire schedule between states
  - Minimum speed and energy level in battery (S_{th}, B_{th})
    - To cope with the harshness and irregularities of waterways



RFID tags: data structures

Identifies the tag location

Determines the data blocks' availability



Information about mobile sensors

distress messages of sensor nodes (low power, low speed or blocking)

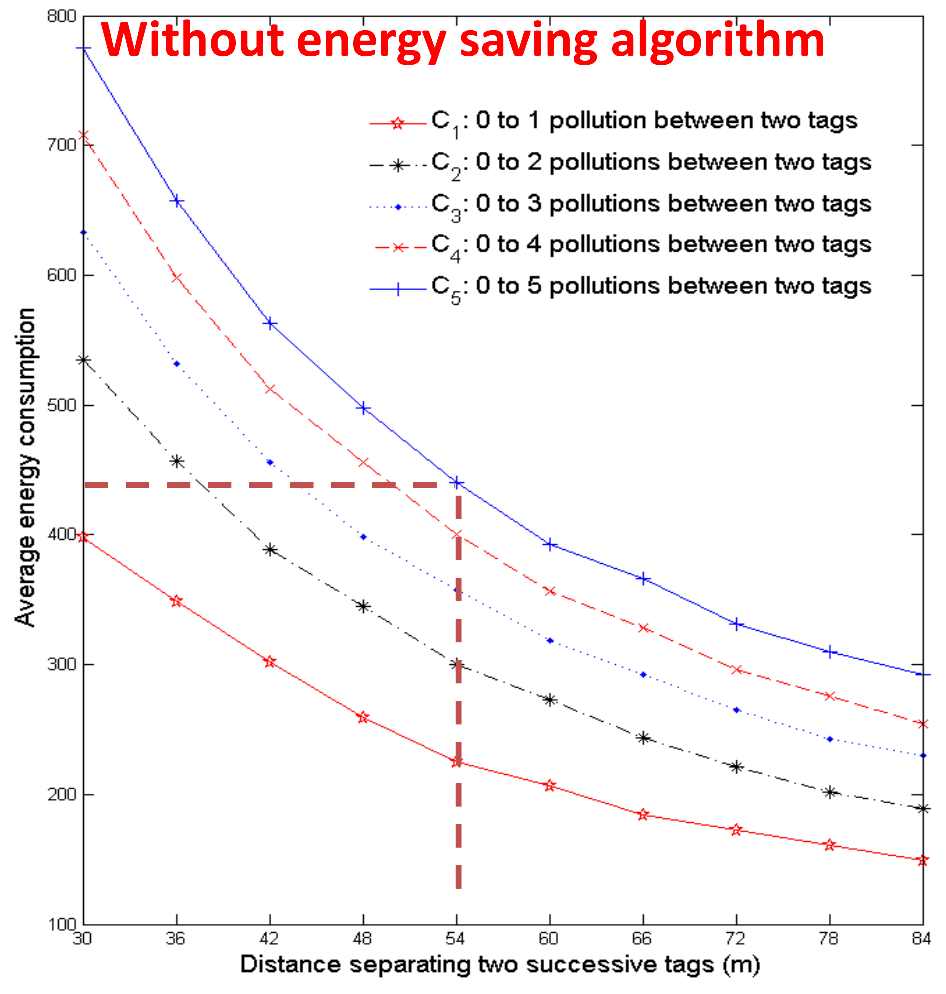
Information about Nodes' states

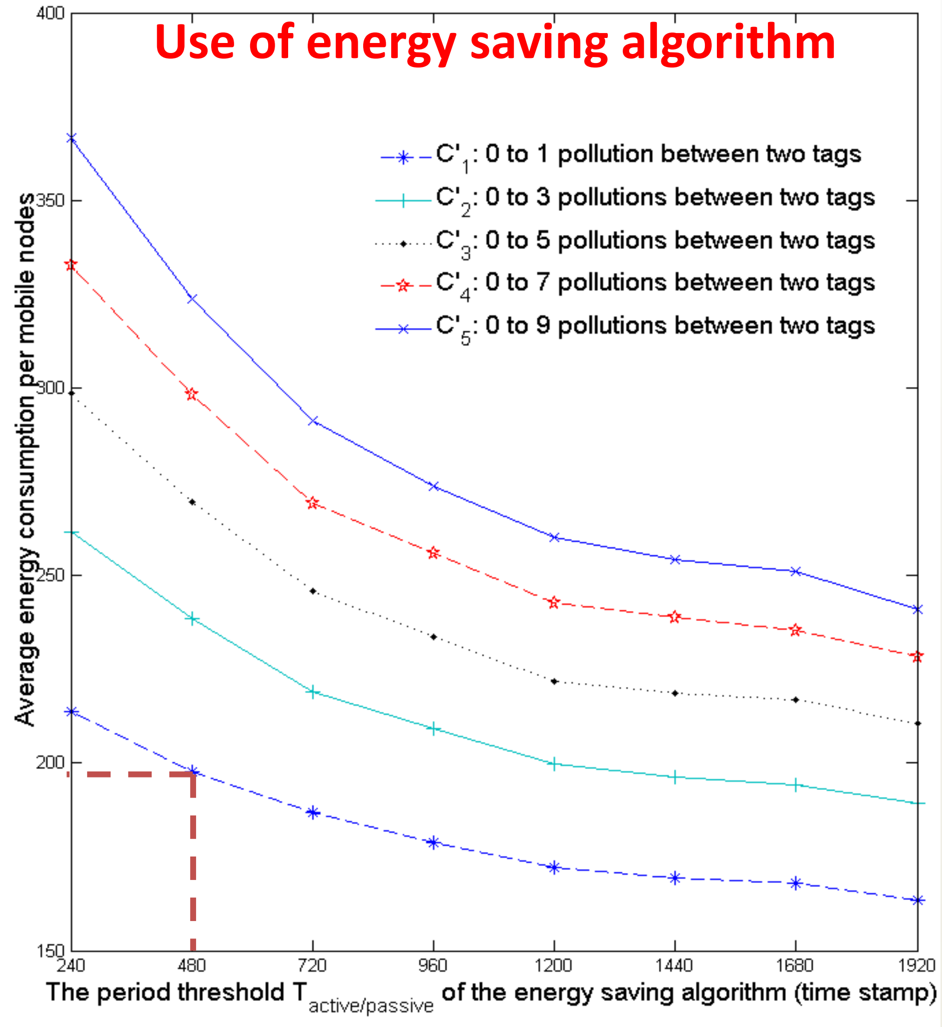
Information about detected pollution

Simulation model

- Regular waterway:
  - Dimension: 8 m x 2500 m
  - 54m spaced 47 tags
  - No obstacles, constant water velocity (1.5m/s)
- 15 Sensor nodes injected, every 100 second
  - Each time slot (0.5 s), the node moves with a fixed distance (0.675m) and a random direction (varies from -60° to 60°)
- Polluted areas are simulated as circles
  - One pollution per slot
    - Area separating two tags is divided into a set of slots
  - Mobile pollutions (speed from 0 to 50% of water velocity)

Energy consumption





- An energy saving of approximately 39% for $T_{active/passive}$ = 480 timestamp

Outline

1 Design of a water monitoring system

2 Securing cardiac IMDs

3 Digital investigation of attacks on cardiac IMDs

Need to secure Implantable Medical Devices (IMDs)

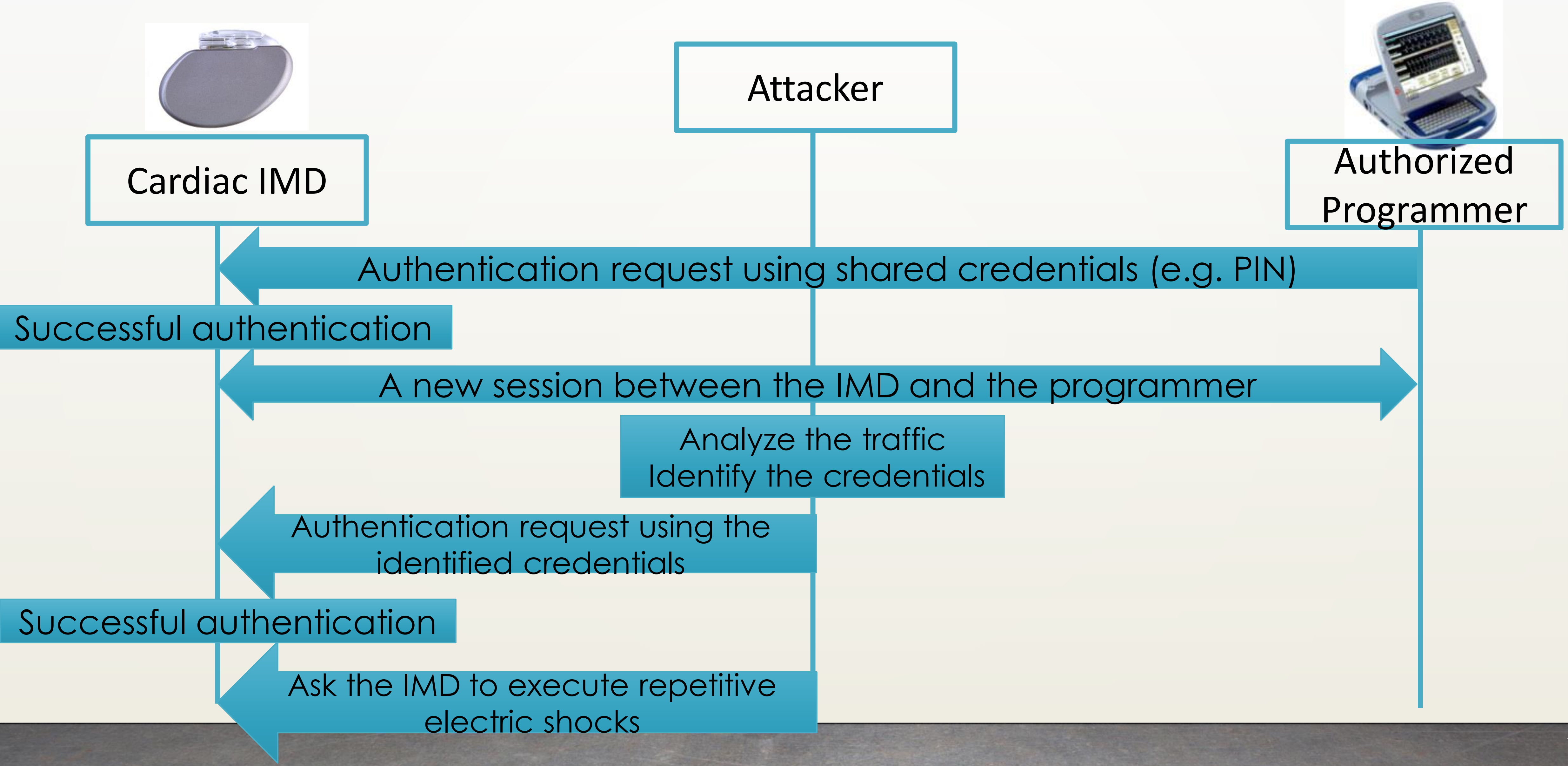
Implantable Medical Device

- Surgically implanted into a patient's body
- Perform therapeutic functions in response to abnormal physiological events
- Wirelessly configured through a programmer using dedicated communication protocols

Security Vulnerabilities

- Unencrypted traffic between IMDs and programmers
- Use of weak authentication techniques
- Inefficient protection against denial of service attacks and resources depletion attacks

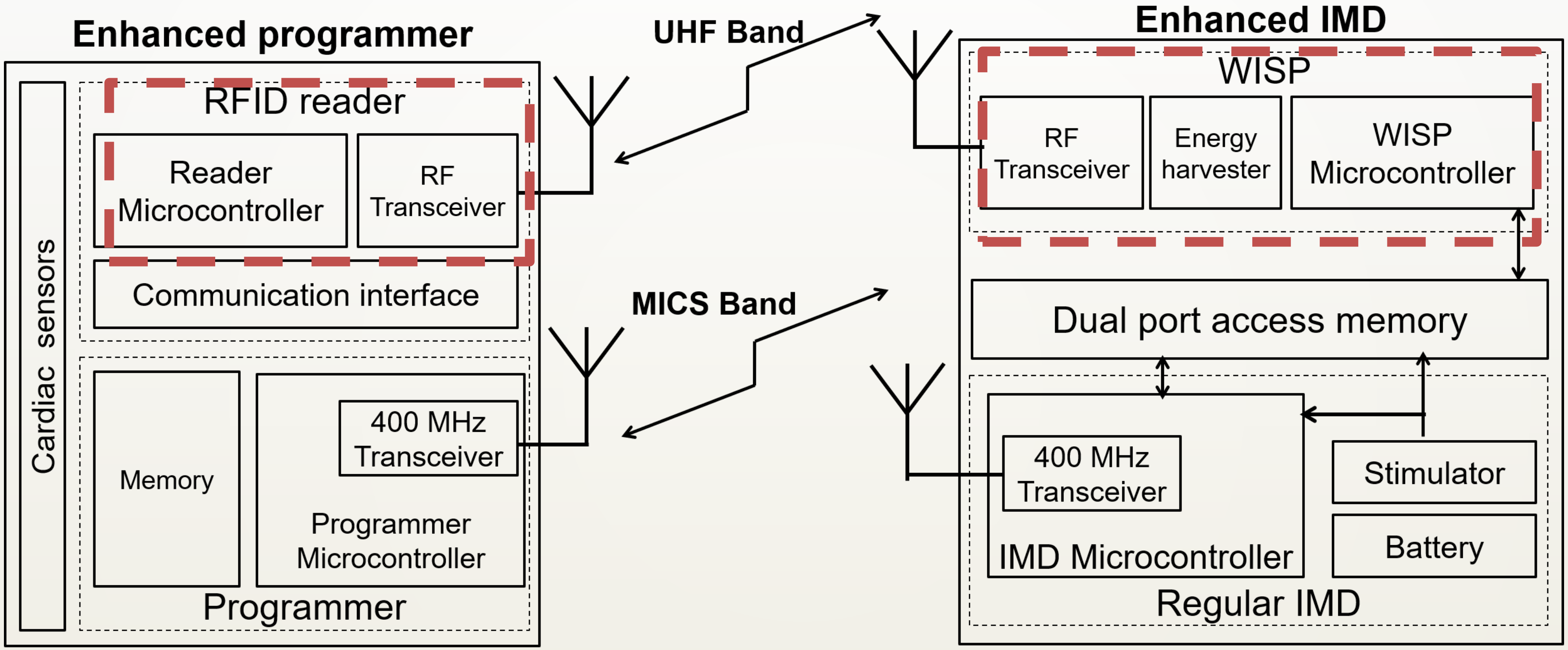
Example of a lethal attack on a cardiac IMD



Proposal

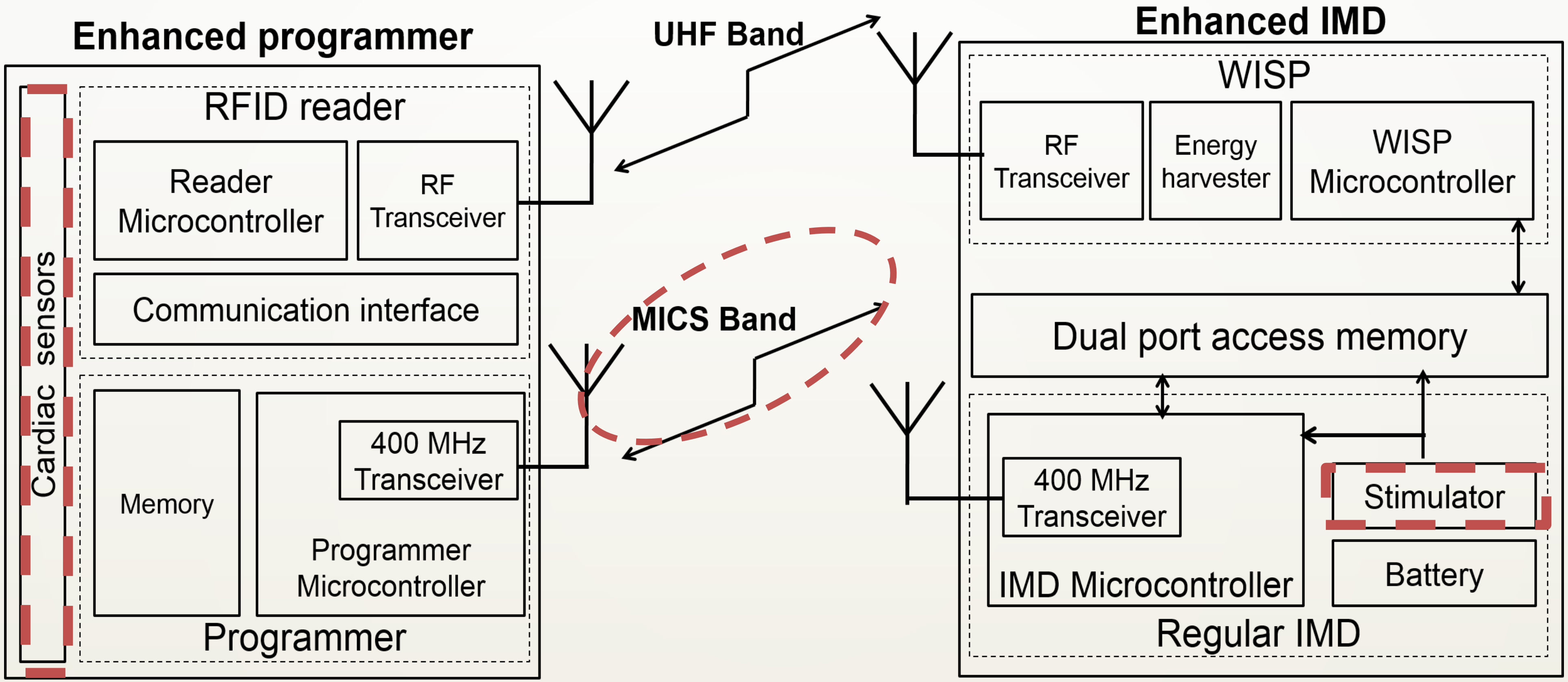
- Extension of the IMD architecture with an enhanced Wireless Identification and Sensing Platform (WISP)
  - Use of Radio Frequency energy harvesting solution
  - Powerless execution of the implemented security functions
- Design of powerless mutual authentication protocol between the IMD and the programmer
  - Prevention of battery depletion attack
- Implementation of an ECG based key distribution technique
  - Secure access to IMDs in regular and emergency situations

Hardware architecture of a cardiac IMD



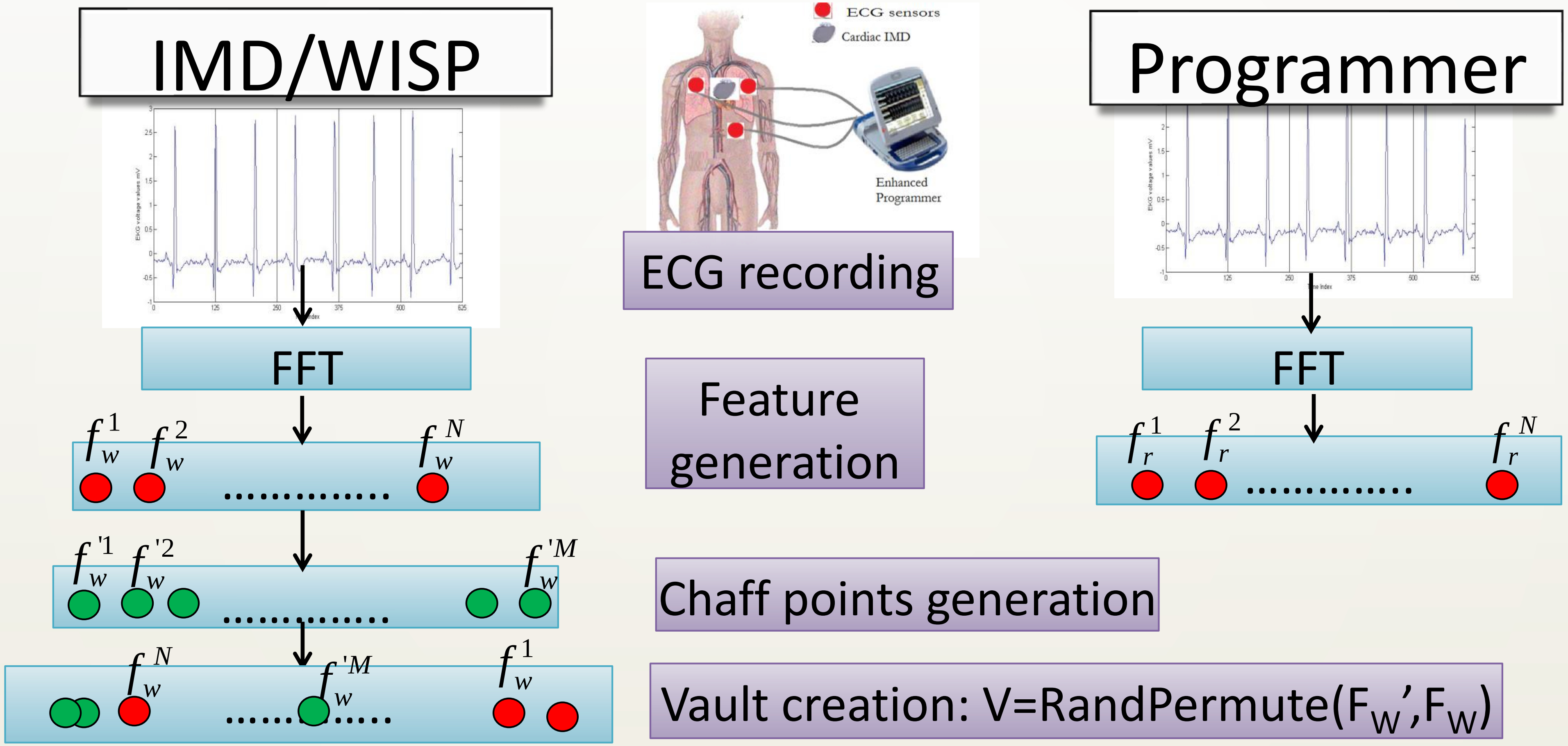
- Integration of RFID system to implement an energy harvesting solution
- Authentication protocol executed through the UHF band

Hardware architecture of cardiac IMDs



- Allow the collection of the ECG signal to enable the generation of biometric keys
- Use of MICS band after successful authentication

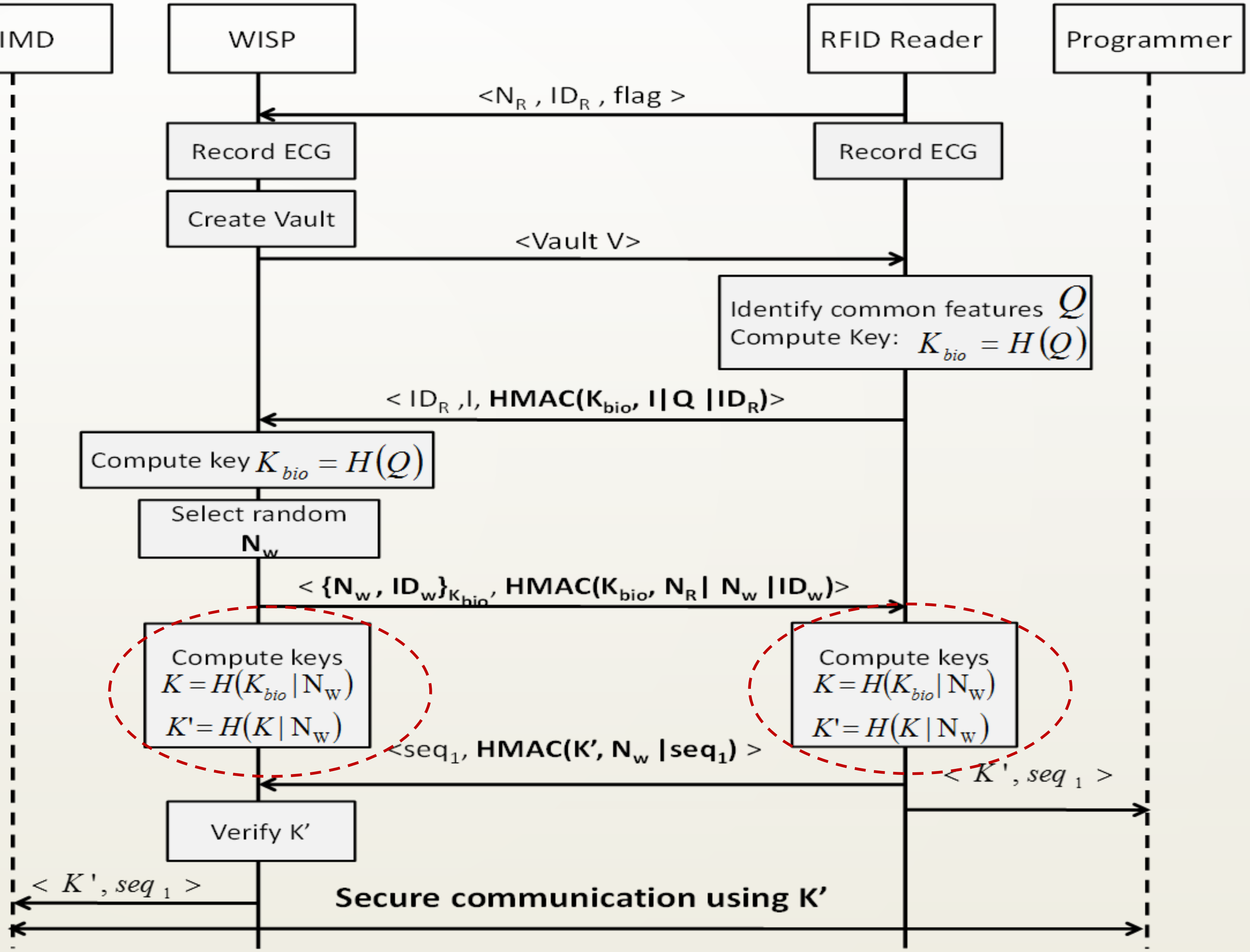
Biometric keys generation scheme



To be authenticated to the IMD, the programmer should identify the vector I of common features positions during generation

Mutual Authentication Protocol in emergency mode

- A synchronization request to initiate the biometric key generation scheme
- Identification of the common features Q and the vector I of features positions to compute the biometric key
- After agreeing on the biometric key, master and session keys will be generated

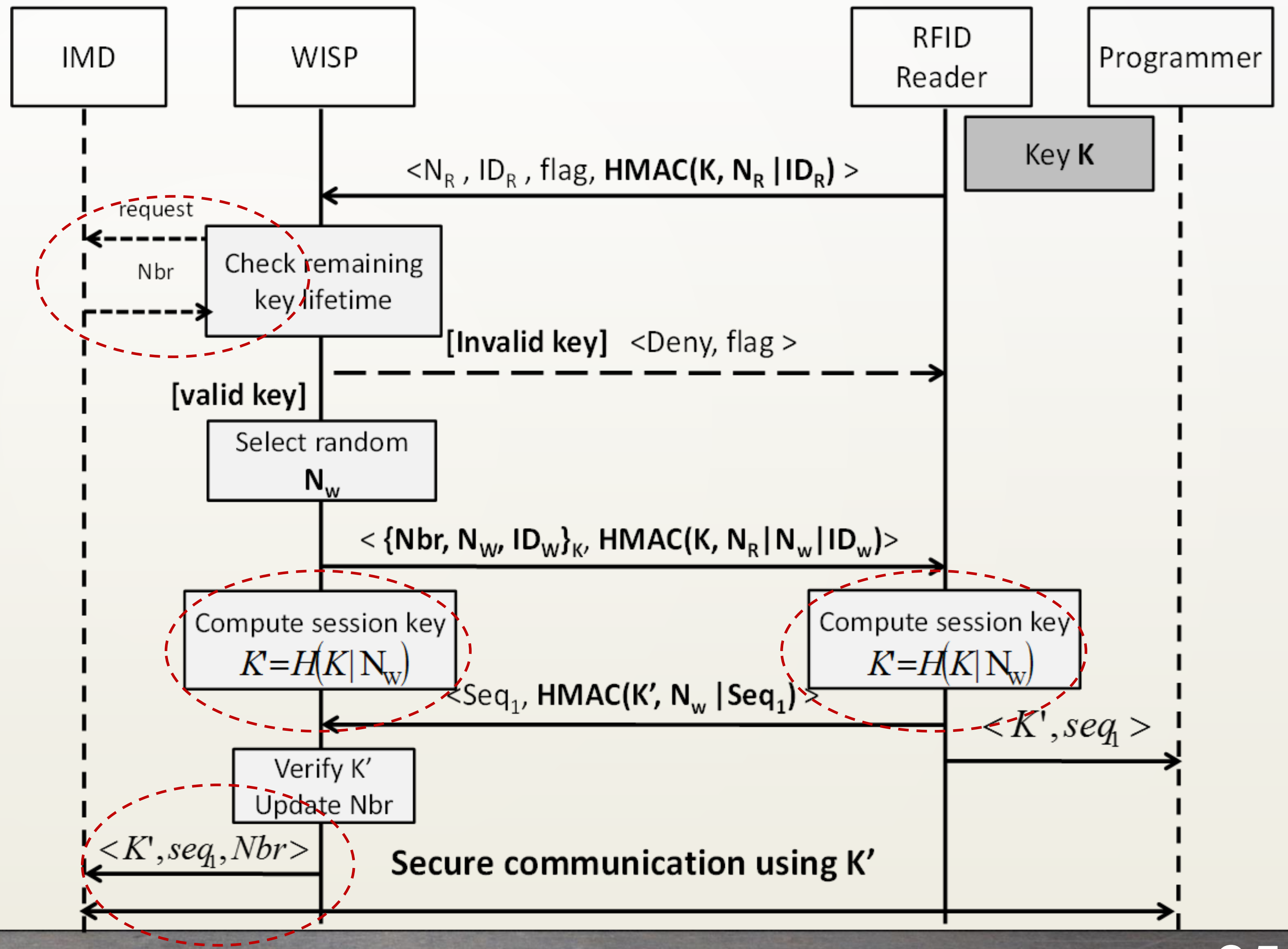


Mutual Authentication Protocol in regular mode

WISP checks the key validity

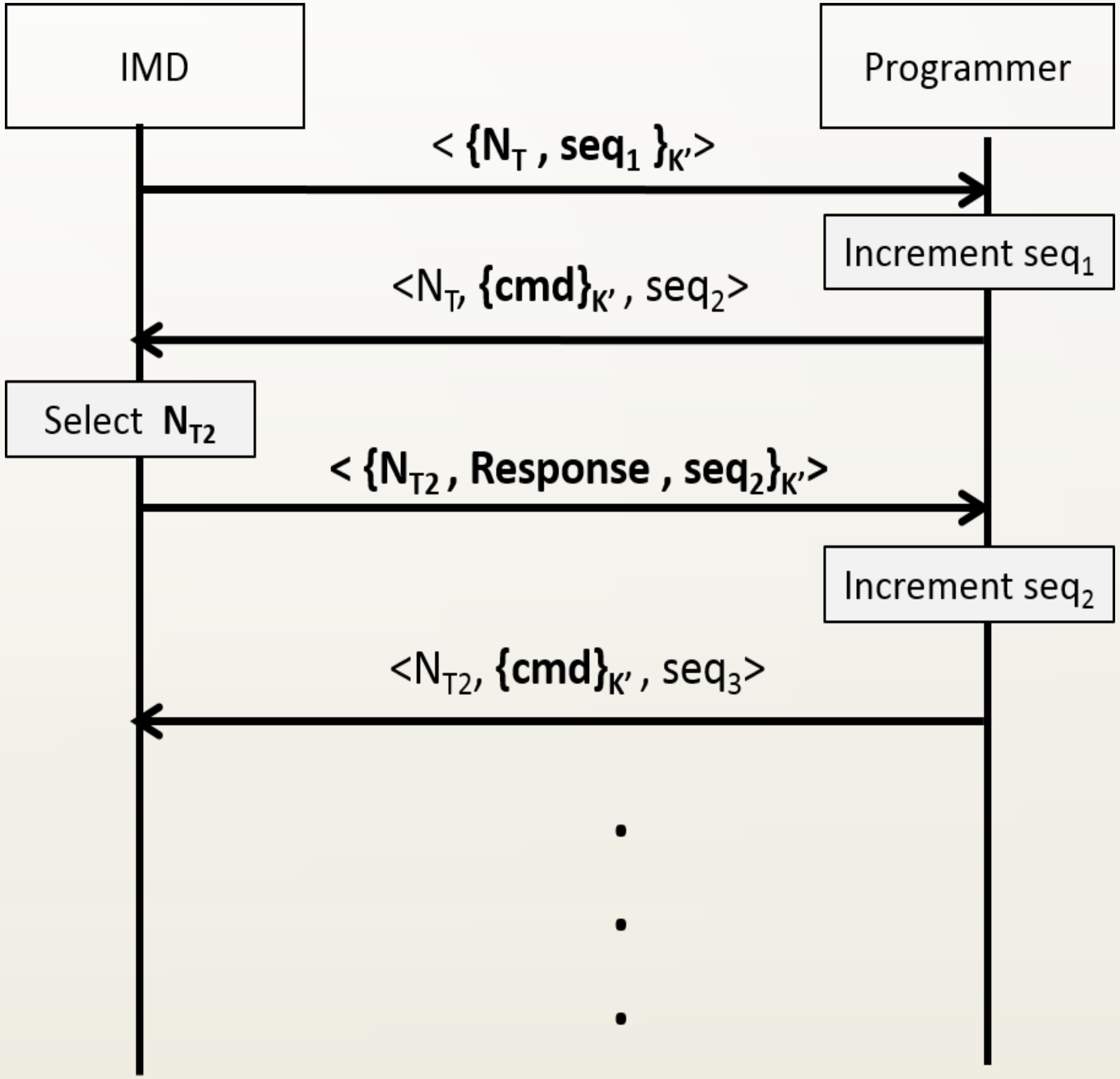
Both of them compute session key

WISP updates the Nbr value identifying the number of session keys derived



Secure Communication Protocol

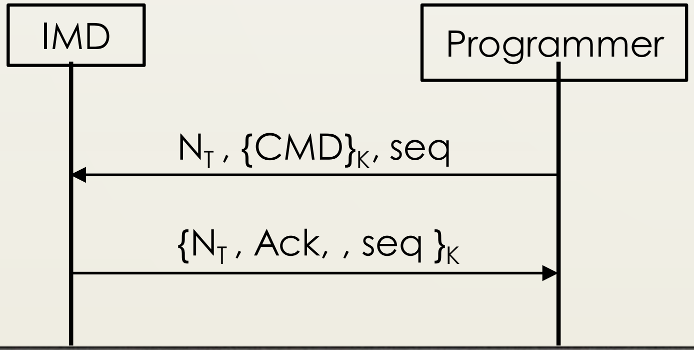
- Resilience to DoS attacks
  - IMD checks the anti-clogging cookies before messages' decryption
  - IMD does not resend the same message more than a predefined threshold



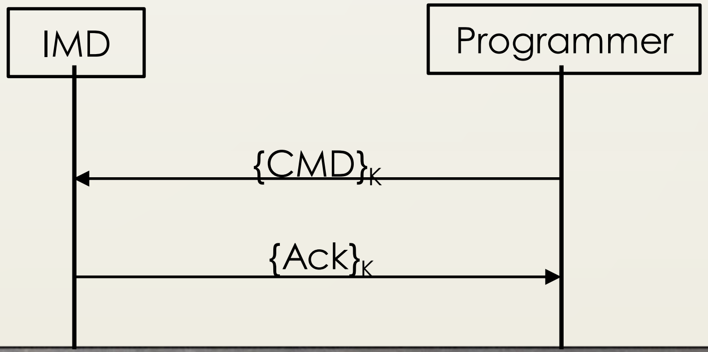
Simulation Model

- Periods separating two consultations are randomly selected
  - Poisson process with arrival rate λ during one year (365 days)
- The consultation duration is randomly selected between 15mn and 20mn
  - Three types of requests: real time EMG analysis, one time (Re)- configuration, examination of history records
- A battery depletion attack can be only executed during a consultation

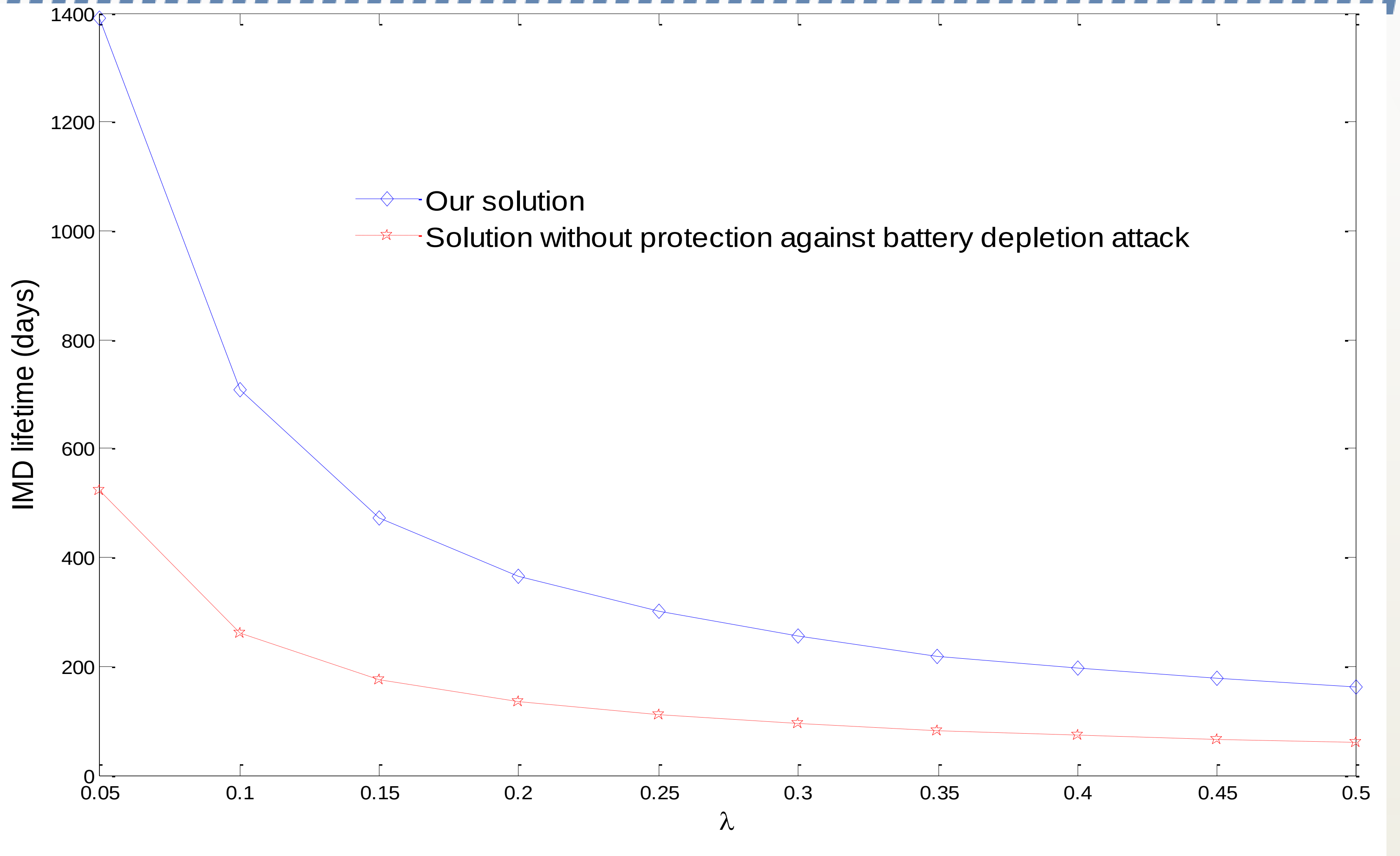
Our solution



Solution without protection against battery depletion



IMD lifetime W.R.T Consultation frequency



- Our solution offers a lifetime higher than the one offered by the other solution

Outline

1 Design of a water monitoring system

2 Securing cardiac IMDs

3 Digital investigation of attacks on cardiac IMDs

Issues of digital investigation of lethal attacks on cardiac IMDs

- Cardiac IMDs provide a set of digital traces (e.g., EMG history) that are not yet used for the purpose of investigation

  ➡ **Can we use them to identify the primary cause of death?**

- Absence of security mechanism protecting these traces

- These traces are insufficient to conduct postmortem investigation of attacks on IMDs

Proposal

- Identification of lethal attacks targeting cardiac IMDs
- Reconciliation of technical and medical scenarios
  - To check the existence of an attack scenario that arguments a patient death
- Design of an inference system including a library of medical rules
  - Identifies medical scenarios source of victim death
- Proposition of a Model Checking based algorithm
  - Reconstructs attack scenarios that may have targeted IMDs

Data structure in IMD logs

- Extension of data structure stored in IMD logs (e.g., access data, configuration update, therapy update)
  - Enable an accurate postmortem investigation
  - Show an overview of the executed actions
- Implementation of an in-depth security solution to protect and secure access to IMD logs
  - Guarantee of the integrity and the trustworthy of evidential traces
- Use of the WISP to collect evidential traces
  - Deal with energy constraints (e.g., exhausted battery)

Three-step investigation methodology

- Medical scenarios reconstruction in backward chaining
  - Use of inference system
  - Provide an explanation about the death
- Technical scenarios reconstruction in forward chaining
  - Use of a library of actions
  - Could not prove whether a technical scenario has an impact on the patient health status
- Correlation of the two types of generated scenarios
  - Prove whether medical scenarios are the consequence of technical scenarios

Medical Inference System

- Inference rules are executed in backward chaining, starting from an observed Heart Death in the medical evidence, based on
  - The collected medical evidence $\mathcal{E}_{Med}$ = <E_1, …, E_n> :
    - E_i= (ev_i, $resp_i$, tm_i)
      - ev_i : the i^{th} event read from the EMG history
      - $resp_i$: the IMD response
      - tm_i : the timestamp of ev_i
  - Use of a library of inference medical rules
    - Describe the causal relations between events
- Reconstruction process stops when:
  - None of the inference rules can be executed
  - Events in the reconstructed graph start to be old
  - Recent events in the medical evidence were included in the graph
- A graph of medical scenarios is generated

Technical scenarios reconstruction

- A Model Checking based algorithm is executed in forward chaining based on:
  - The IMD's initial system state
  - A library of actions (malicious and legitimate)
- The algorithm proceeds as follows:
  - S=$\langle s_0, A_1, s_1, \ldots, A_i, s_i \rangle$ is a scenario under construction
  - $obs(S) \sqsubseteq E$, Where E is the technical evidence
  - If there is an action A in the investigation library such that $A(s_i)$=$S_{(i+1)}$, then verifies if $obs(S|\langle A, s_{(i+1)} \rangle) \sqsubseteq E$
  - If verified, then S=$S|\langle A, s_{(i+1)} \rangle$
- A graph of technical scenarios satisfying the provided evidence is generated

Correlating potential scenarios

- Analysis of medical evidence and scenarios to:
  - Check the existence of suspicious IMD responses
  - Identify the parameters related to that responses
- In-depth analysis technical evidence and scenarios to:
  - Determine malicious actions threatening IMD security
  - Identify modifications brought by these malicious actions
- Verification whether the suspicious IMD responses are caused by the identified malicious actions
  - The patient death is a consequence of a criminal attack

Case study: Scenario description

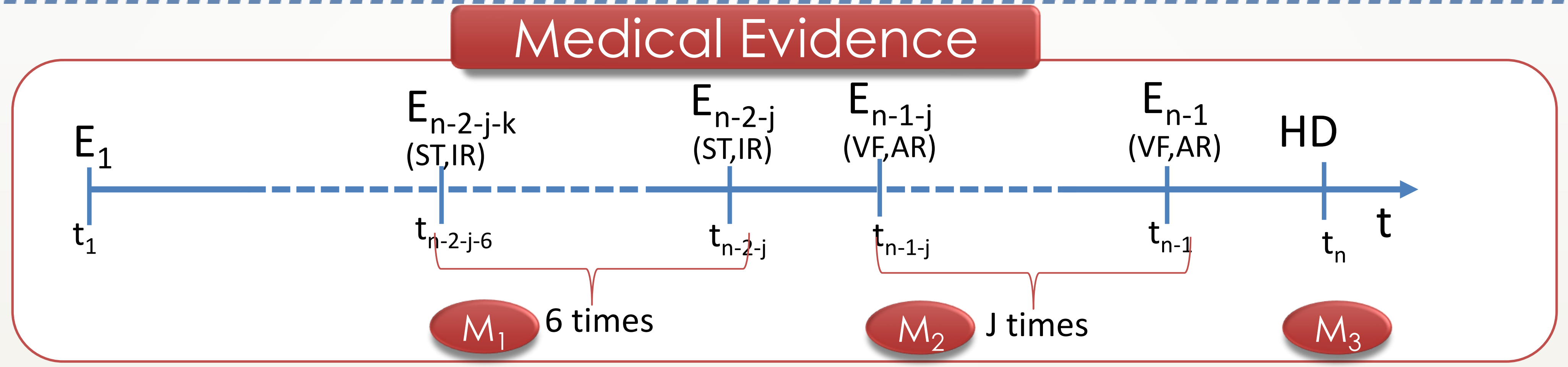
❑ Criminal attack scenario

- Acquiring credentials and gaining access to the IMD
- Modification of therapy settings affecting the detection of ***Ventricular Fibrillation (VF)***
- Disconnection of the attacker

❑ Medical incident: (Misconfigured IMD)

- ***Sinus-Tachycardia (ST)*** episodes are detected by the IMD as ***VF*** episodes
  - The IMD reacts by delivering 6 electric shocks
- Occurrence of real ***VF*** and absence of IMD reactions
  - The maximum number of shocks was already delivered
- **Death of the patient**

Case study: Medical Scenarios



M_3 Death of the patient

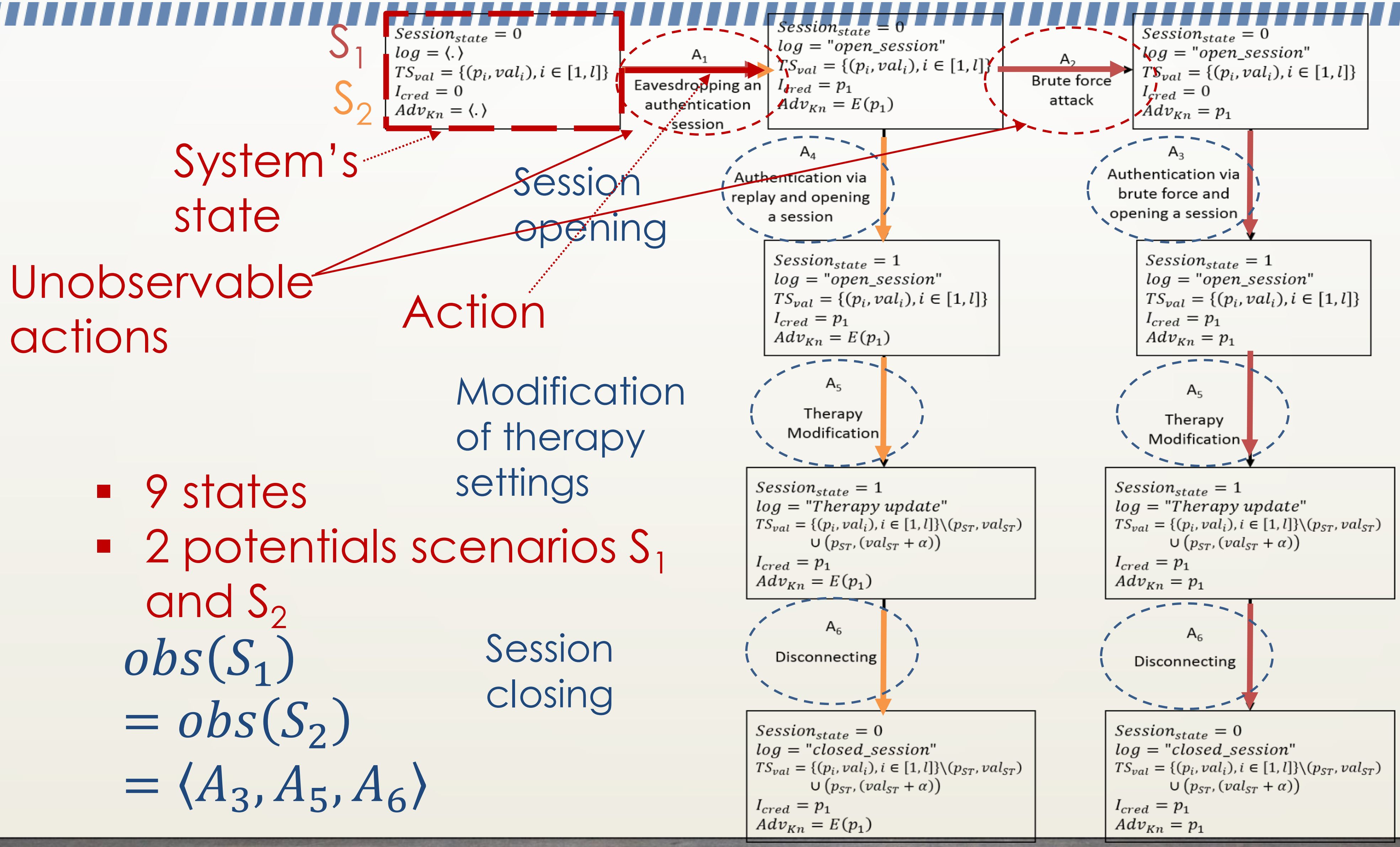
M_2 Several episodes of VF and absence of IMD reactions (AR)

The absence of IMD reactions to the occurred VF induced the heart death (HD) of the patient

M_1 6 ST episodes followed by a delivery of a therapy (IR) suitable for VF

The inappropriate IMD reactions to the occurred ST caused the occurred VF episodes

Case study: Technical Scenarios



- 9 states
- 2 potentials scenarios S_1 and S_2

$$obs(S_1) = obs(S_2) = \langle A_3, A_5, A_6 \rangle$$

Case study: Correlation of scenarios

- Therapy modification (Action A_5) in the technical scenario **caused** the inappropriate IMD response to the occurred ST in the medical scenario
- Action A_5 also **caused** the absence of IMD response to the occurred VF in the medical scenario

➡ The settings modified by A_5 make the IMD unable to respond appropriately

➡ The patient death could be considered as a consequence of a lethal attack on the IMD

Conclusion

- Architecture and techniques proposed for the water quality surveillance system could be used for the surveillance of other critical infrastructures
  - E.g., Dams, water distribution systems
- Security mechanisms proposed to secure cardiac IMDs could be generalized and applied to other human surveillance applications
  - Medical Wireless Body Area Networks (WBAN), Medical Cyber physical Systems (MCPS)
- Energy-aware solution is suitable to any inaccessible device or equipment
- Investigation methodology which aggregates the professional's experts in the field efforts and the security investigators' efforts could be applied to diverse applications
  - Digital investigation of power grid need to be based on the efforts of electricity experts together with security experts

Thank you