CAN IMPLANTS LEARN TO RESIST ATTACKS?

PARF: Profiling-based Adaptive Resilience Framework for Medical Devices

Foroozan Ghosairi Darbandeh, Muhammad Rizwan Asghar, Liqun Chen

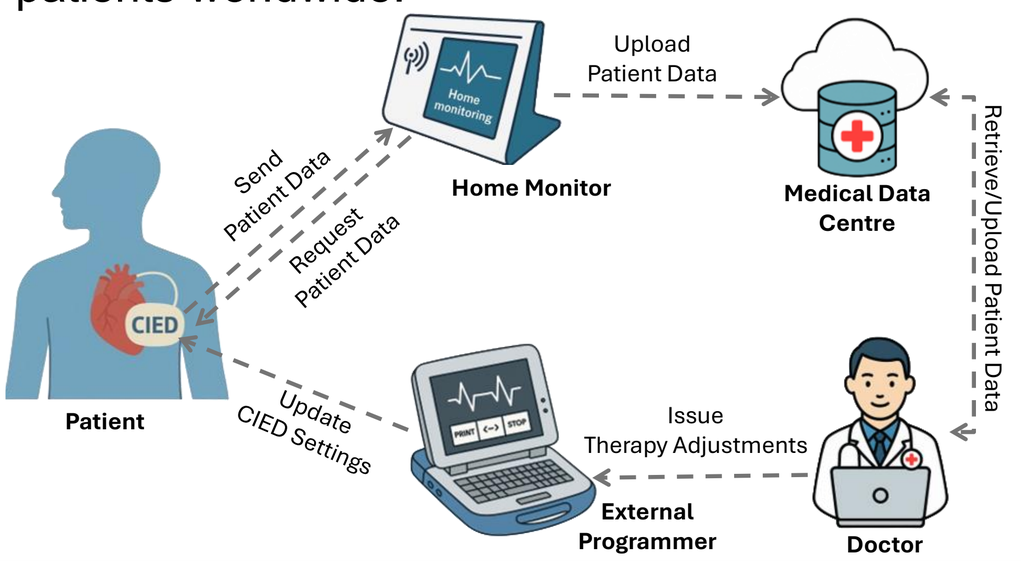
UNIVERSITY OF SURREY

HealthCare Beyond Hospital Walls

- The ***Internet of Medical Things*** (**IoMT**) connects medical devices to monitor patients and provide better care.
- NHS reports indicate that nearly **three million devices** are currently in use across the UK.

What is the CIED?

- A ***Cardiac Implantable Electronic Device*** (**CIED**) system monitors heart activity, delivers therapy when needed, and transmits data for remote patient care.
- CIEDs are one of the fastest-growing categories of IoMT devices, supporting millions of cardiac patients worldwide.

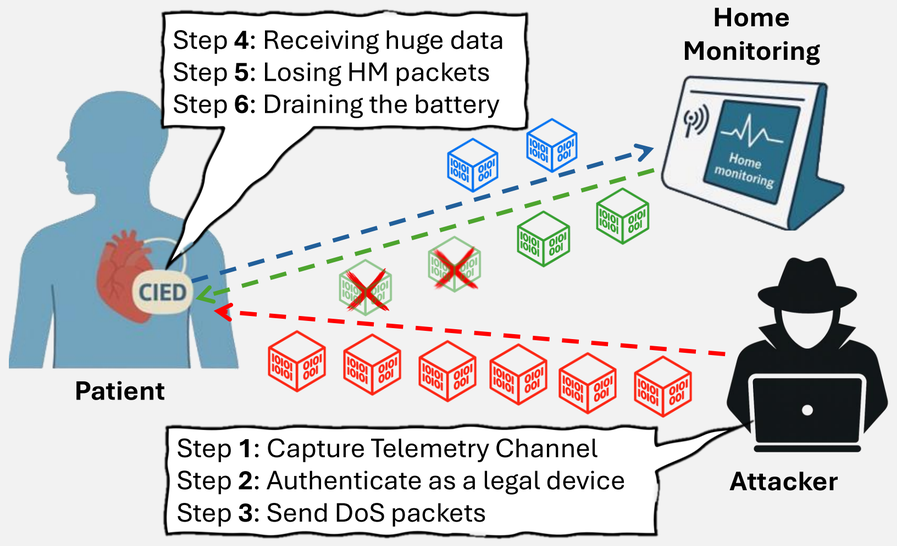


Hazards and Risks

- Severe energy constraints limit advanced security mechanisms in implantable medical devices.
- Known cybersecurity vulnerabilities increase their exposure to attacks.
- Energy limitations in battery-powered implantable medical devices make availability fragile, placing DoS among the most critical threats.

How Do *Denial-of-Service* (DoS) Attacks Affect CIED?

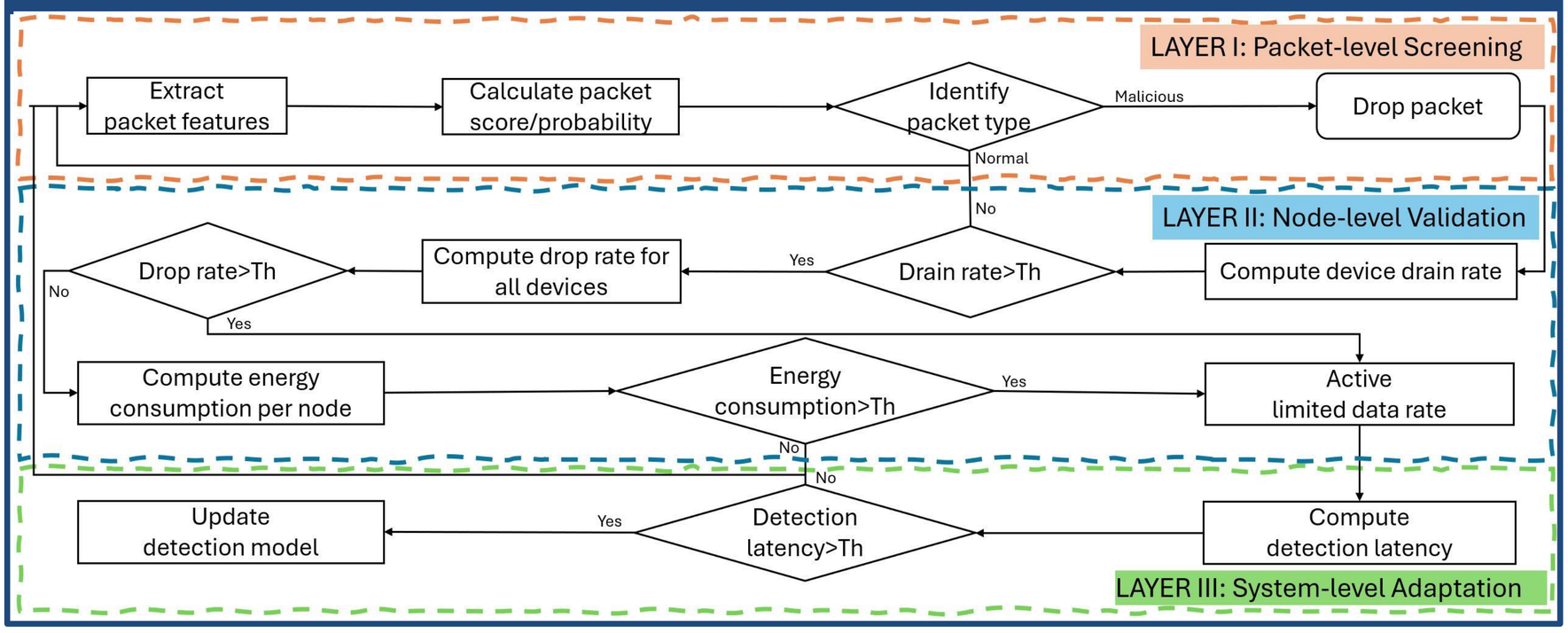
- By interrupting treatment signals and rapidly draining device batteries, DoS attacks can turn a cyber incident into a real threat to patient survival.
- Overwhelmed with malicious traffic, exhausting its limited computing resources and failing to receive or deliver essential therapy signals.
- Battery exhaustion caused by DoS attacks may leave CIED patients facing unnecessary and risky surgical intervention.
- DoS attacks can be executed through large packets (Low-Rate), massive bursts of traffic (Flooding), or replaying previously trusted packets (Replay).



PARF Methodology

- ***LAYER I:*** PARF detects and immediately drops abnormal packets to mitigate DoS impact.
- ***LAYER II:*** Analyses device-level behaviour to identify malicious nodes and enforce data rate limiting to recover system stability.
- ***LAYER III:*** The detection model is updated when necessary to adapt to emerging attacker behaviours.

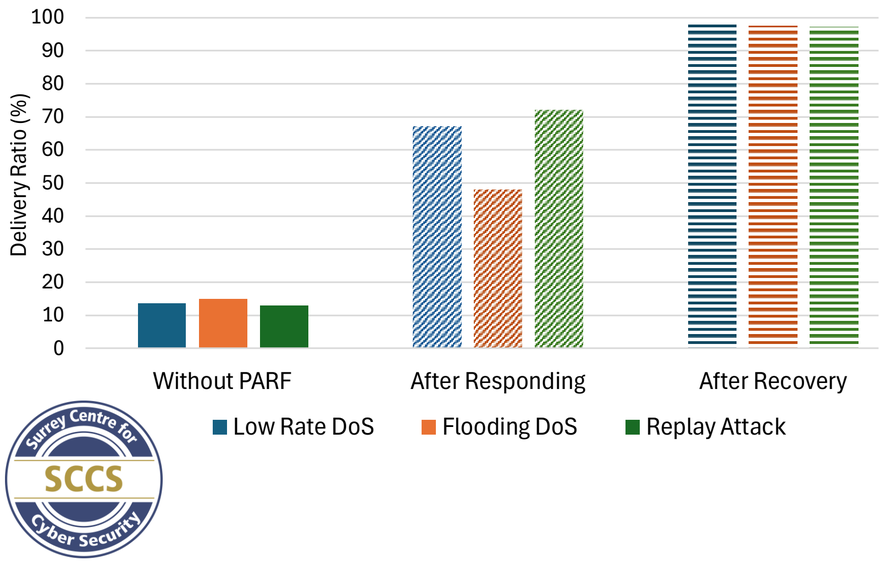
Profiling-based Adaptive Resilience Framework



Results

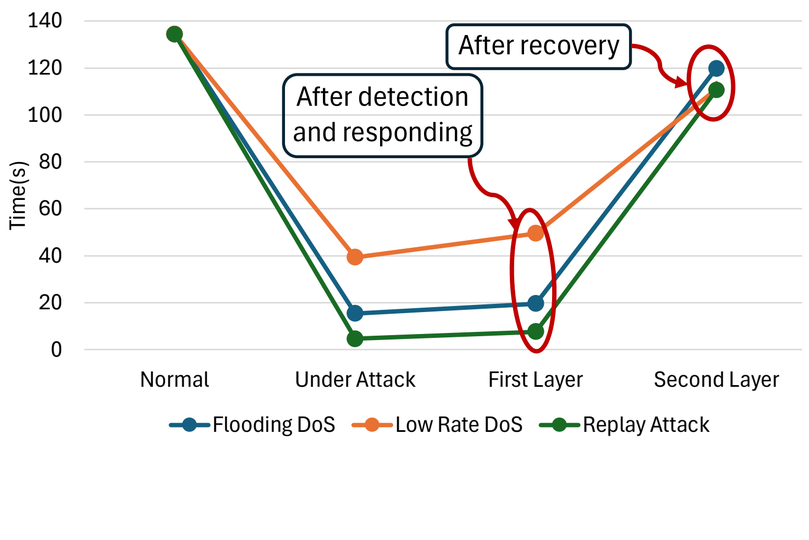
Packet Delivery Ratio

- Therapeutic packet delivery surged from 15% to 79%, restoring reliable care even under attack.



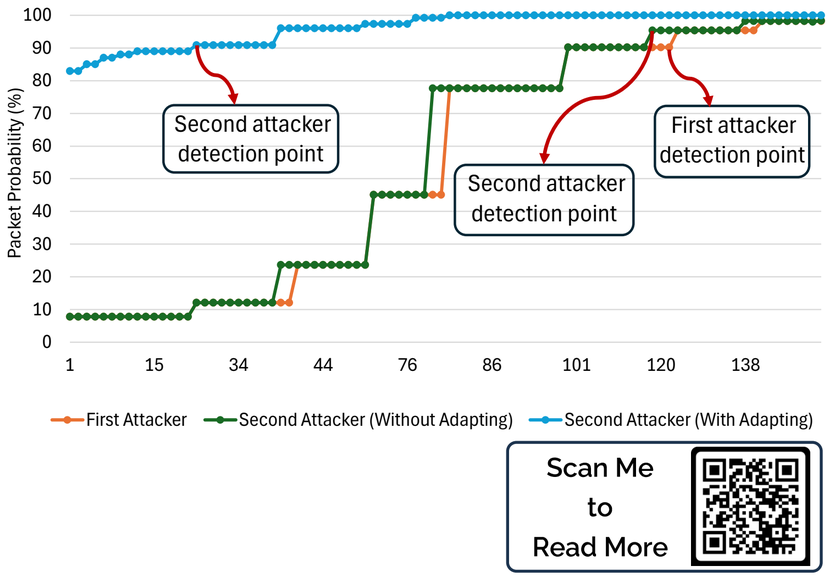
Energy Drain Rate

- Eliminating malicious processing reduced energy consumption by 52.3%. System halt time improved from 4s to over 110s.



Adaptability

- Learning from emerging threats, the updated model detected new attackers almost twice as quickly.



Surrey Centre for SCCS Cyber Security

Scan Me to Read More