Motivation:

- Embedded systems with a shared network
  - Mixture of critical & non-critical nodes
  - Typical design assumption: “Trust any message from a critical node”
- System defects (software, hardware) can lead to masquerading
  - Masquerading of critical nodes may compromise critical systems

Previous Solutions:

- Network-provided or Application-level CRCs
  - Effective against random bit errors (noise) & some networking defects
  - Inexpensive (bandwidth, processing, memory, etc.)
  - Vulnerable to masquerading due to design defects & malicious attacks
- Symmetric & Asymmetric Digital Signatures
  - Effective against design defects and malicious attacks
  - Expensive (bandwidth, processing, memory, etc.)

Our Technique:

Application-Level CRC with Secret Polynomial/Seed

- Protects against non-malicious masquerading by non-critical sources
- Same cost as application-level CRC
- Still vulnerable to non-malicious masquerading by critical sources
- Still vulnerable to malicious attacks

Asymmetric Application-Level CRCs

- Protects against non-malicious masquerading by critical sources
- Cost of application-level CRC plus cost of signature X
- Still vulnerable to malicious attacks

Ongoing Research:

- Analysis of commercial safety-critical networks
- Masquerading in event-triggered and time-triggered domains
- FlexRay, TTP/C, TTCAN, TCN, Embedded IP
- Application of techniques from train to automotive