

Security in Embedded Networks

Elena Reshetova, SUAI

Tutor: Michel Gillet, Nokia

Project Motivation

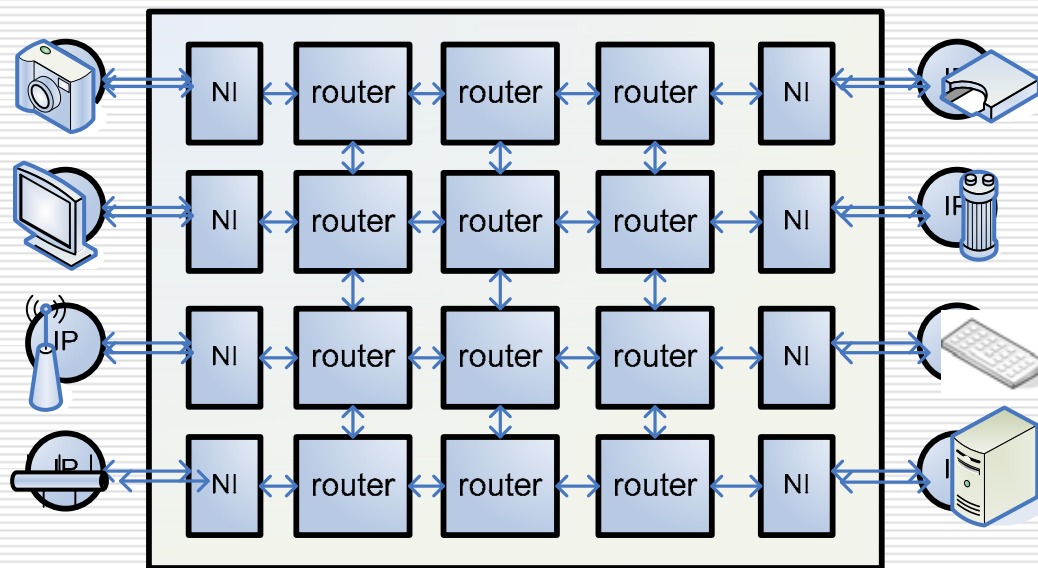
- Embedded Networks (EN) become more and more widespread
- Current standards do not address security
- Why? → two hypothesis to check:
 - There is no security problem in EN as it consists of hard-coded components
 - There is a software, which can be compromised, thus security problems should be consider
- The project examines both points of view

Project Goals



- ❑ Literature study and analysis of current security situation in EN
- ❑ Identification of EN closest network types and comparative analysis of their features
- ❑ Analysis of attacks and security solutions for these networks and the actuality for EN
- ❑ Applicability analysis of the solutions to EN
- ❑ Preparation of the project plan for research targeted in building EN security solution

Background: Embedded Networks

- EN interconnects IPs
- IPs are low-level devices provided by different vendors
- Special IP – CCM
 - Initialization
 - Reconfiguration
- Expected EN configuration
 - IPs ~ 20, Routers ~ 8
 - ~ 4 ports per routers
 - Link speed ~ 1Gb

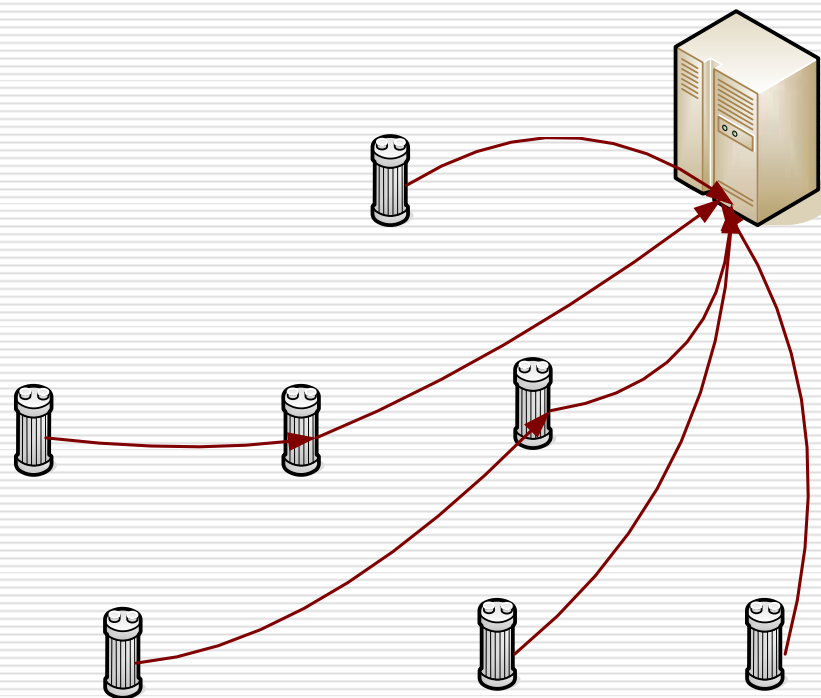


Current Situation

- No need in security at all
 - All components are hard-coded 
 - Very low or no dynamics in network structure
 - Current standards don't have security:
SpaceWire - <http://spacewire.esa.int>
MIPI alliance, UniPro – <http://www.mipi.org>
- Security might be important
 - Hard-coded components have software interfaces 
 - Components can be compromised
 - Papers:
S.Ravi, A.Raghunathan, P.Kocher, and S.Hattangady
"Security in Embedded Systems: Design Challenges"
S.Evain, J. Diguët, "From NoC Security Analysis to Design Solutions"

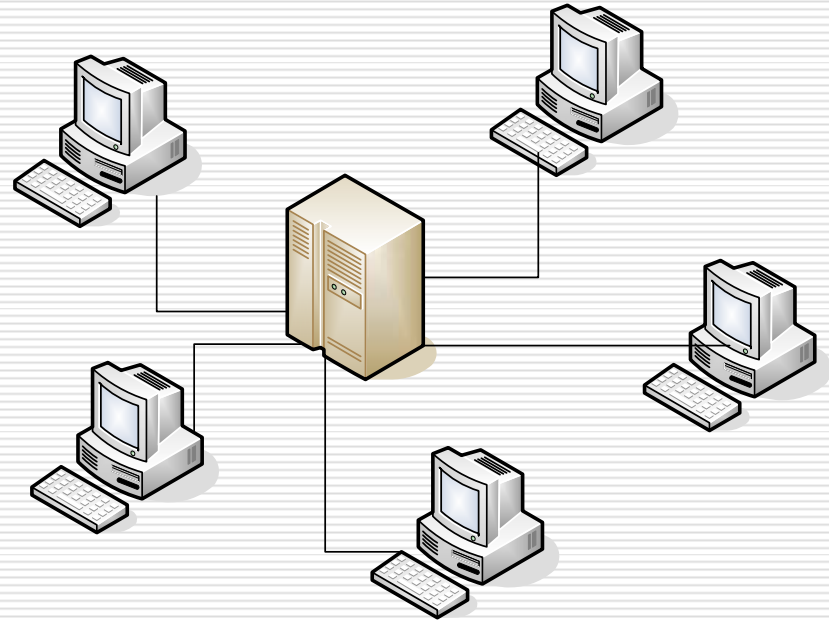
Close solutions – Sensor Networks

- Common things:
 - Power consumptions
 - Processing limitations
- Differences:
 - Network structure
 - Traffic intensity
- What are security challenges in sensor networks?
 - ~~Encryption?~~
 - Data Integrity and Authentication
 - Key management



Close solutions – LAN

- Common things:
 - Private data on each unit
 - Network structure
- Differences:
 - Big amount of processing
 - Big amount of power consumption
- What are security challenges in this network?
 - Encryption
 - Data integrity and Authentication
 - Key management
 - Security primitives



Open Question

- Has EN the same vulnerabilities?
 - No
 - Yes
- How solutions for SN and LAN can be used in EN?
- What is the cost of implementing a solution

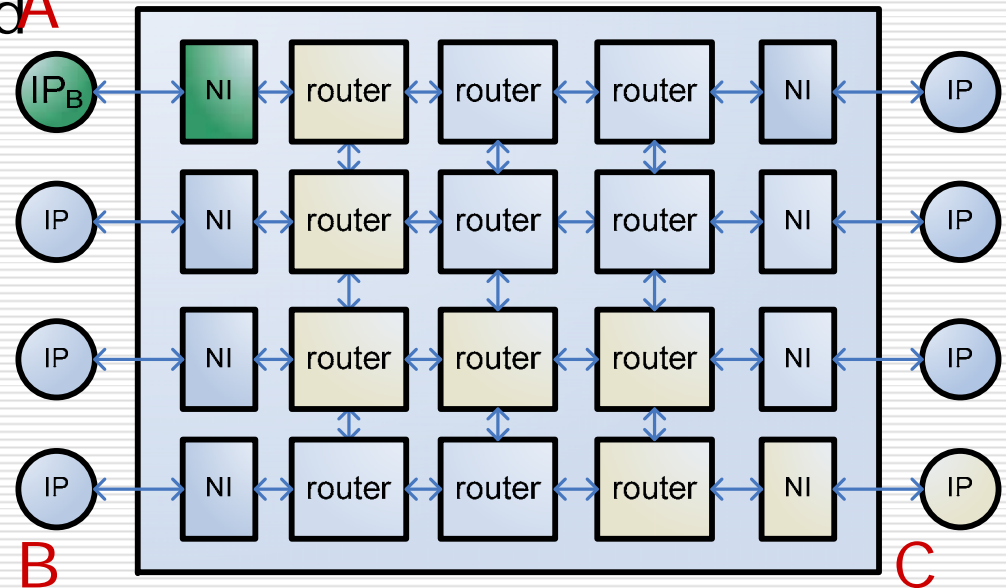
Possible attacks

□ IP or NI compromised ^A

- DoS attacks
- Masquerading

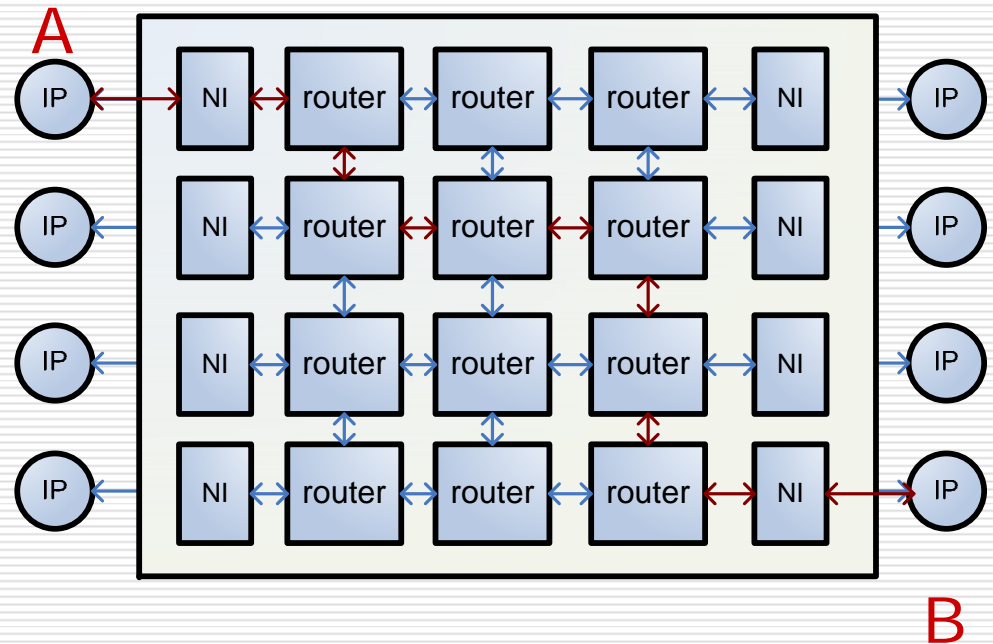
□ Router compromised

- Re-play attack
- Delete messages
- Hijacking
- Read sensitive data
- DoS attacks



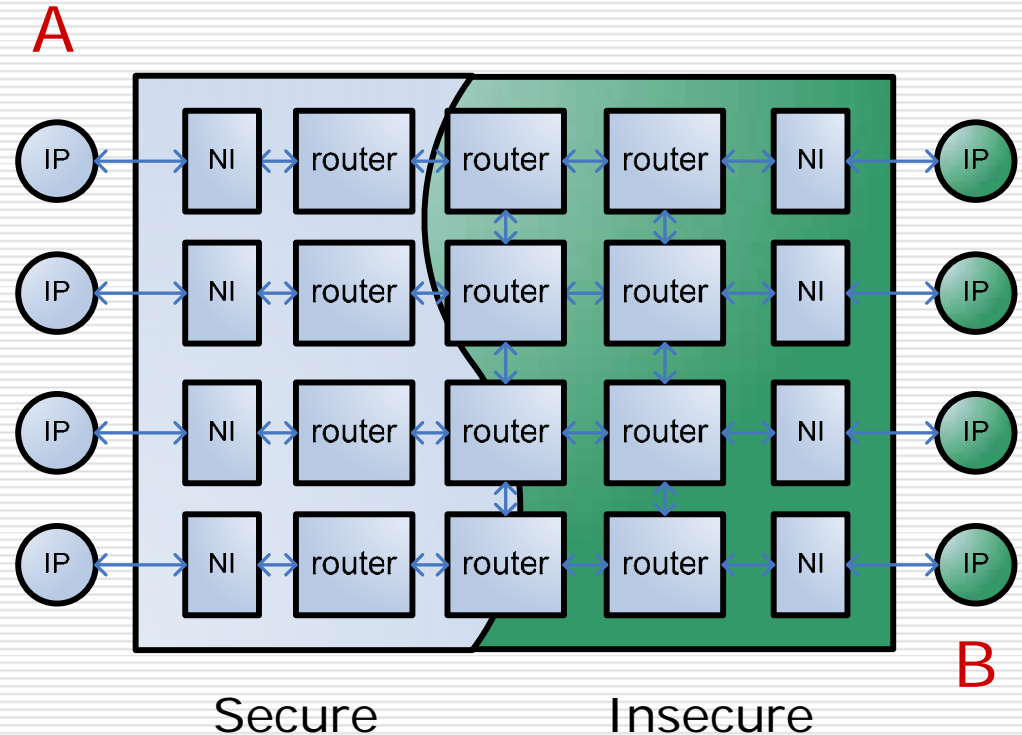
Authentication - 1

- We need authentication of data between IPs
- Self Complemented Path Coding proposed by S.Evain, J. Diguët
 - Assumption: routers can't be compromised



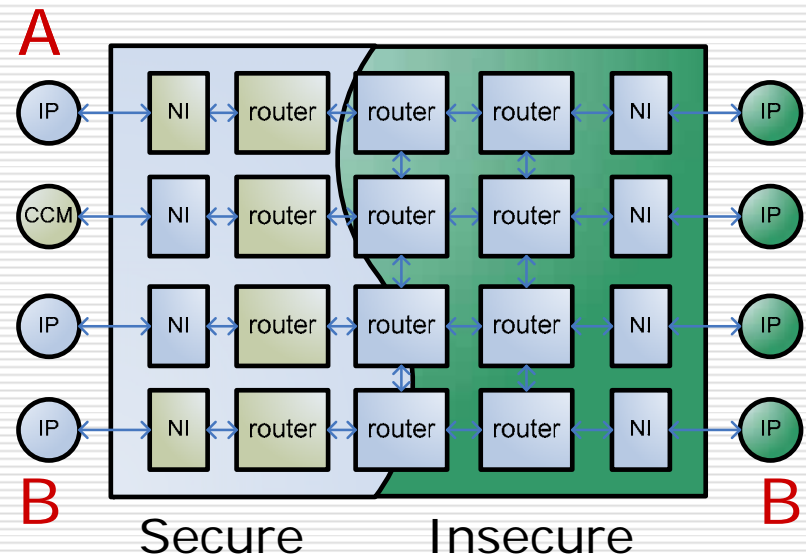
Authentication - 2

- We need a signature from CCM
- But what kind of?
 - ~~Public cryptography~~
 - Symmetric cryptography



Key management

- All nodes must have a key with CCM and between each other
- Initial key may be hard-coded during design phase
- Session keys should be used
- What should be done if the key is compromised?
 - Key between two IPs
 - CCM can send new keys to both parties
 - Key between CCM and IP
 - They can use a kind of protocol with secure IP



Conclusions

- ❑ Literature study and analysis of current security situation in EN has been done
- ❑ We identified EN closest network types and made comparative analysis of their features
- ❑ We analyzed a number of attack scenarios
- ❑ The first drafts for authentication and key management solutions were proposed

- ❑ Project is on track, but still a lot to be done

Future work

- ❑ Literature study and analysis of current security situation in EN
- ❑ Identification of EN closest network types and comparative analysis of their features
- ❑ Analysis of attacks and security solutions for these networks and the actuality for EN
- ❑ Applicability analysis of the solutions to EN
- ❑ Preparation of the project plan for research targeted in building EN security solution

Thank You & Questions

Contact information

Email: Elena.Reshetova@gmail.com

http://www.fruct.org/index.php?morus_itemid=16&morus_langsel=en