universitätbonn

Selective and Secure Over-The-Air Programming for Wireless Sensor Networks

Nils Aschenbruck, Jan Bauer, Jakob Bieling, Alexander Bothe,

and Matthias Schwamborn

Univ. of Bonn and Univ. of Osnabrück, Germany

The 6th International Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN2012)

Munich, Germany

July 30, 2012

Outline

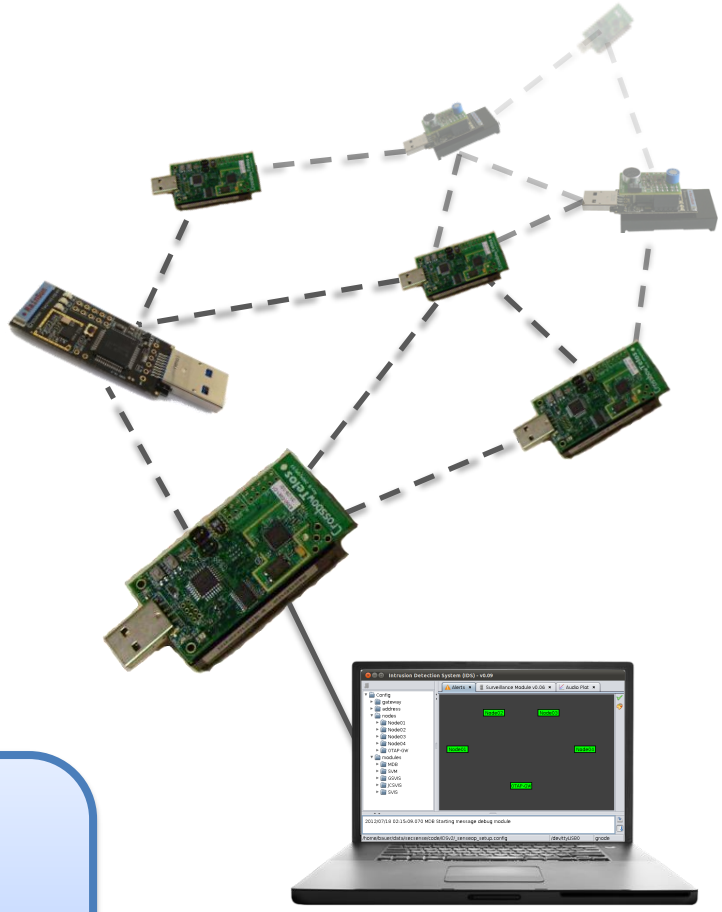
- Introduction
- Security Threats
- Concept of SenSeOP
- Performance Evaluation
- Conclusion

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de

Wireless Sensor Networks (WSNs):

- **plurality of small, cost-effective sensor notes**
- **wireless communication**
- **distributed manner**
- **self-organizing**
- **convergecast traffic to base station**



Challenges:

- **heterogeneous devices**
- **resource constrained**
  (processing power, memory, battery power, network capacity)

Applications:

- **military, industrial, civilian**

Reprogramming WSNs:

- **maintenance, re-tasking, updates, bug fixes**
- **long-life applications, dynamic environments, node failures**

→ Over-The-Air-Programming (OTAP):

- **wireless reprogramming**
- flexible, in-situ **remote maintenance**
- crucial if nodes are **inaccessible** after deployment
- two steps: **transfer** and **booting** of program code

Requirements:

- **reliability**
- **time-efficiency**
- **energy-efficiency**
- **light-weight**
- **selectivity**
- **security**
- **…**

Selective OTAP:

- **group-wise reprogramming** of a specific **subset** of nodes
- essential due to:
  - **heterogeneity of hardware, sensing-, and communication tasks**
  - **spatial dependencies** of sensor nodes

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de

Without security the WSN is lost!

Type of attacks:

- **Reprogram node attack:**
  - **inside attacker manipulates program code** during transmission
  - **inside attacker injects malicious code** and forces nodes to run that code

  → **capturing of individual nodes / entire WNS**

  → disruption of WSN's functionality

- **Replay attack**
  - **inside attacker uses eavesdropped program code to reprogram arbitrary nodes** with (obsolete) code

- **DoS attacks**
  - against **OTAP service**
  - against **WSN service**

Computer Science 4 – TacNet@cs.uni-bonn.de

Deluge:

- default **TinyOS** network programming protocol
- **efficient self-organized, network-wide dissemination**
- **NO selectivity**
- **NO security**

"Security Extensions" of Deluge:

- Dutta et al., Sluice, Seluge, Secure Rateless Deluge
- based on **asymmetric cryptography**
- **authenticity/integrity via digital signatures**

There exists no selective and secure OTAP protocol.

Selective ‘n’ Secure Over-the-air-Programming (SenSeOP):

- based on the threat model
- adopted from **NWProg** (part of BLIP):
  - **message format, image creation/processing routines**
- adopted from **Deluge,** e.g.**:**
  - image **fragmentation scheme, flash memory layout** (multiple slots)
- **simple propagation** instead of complex dissemination of Deluge

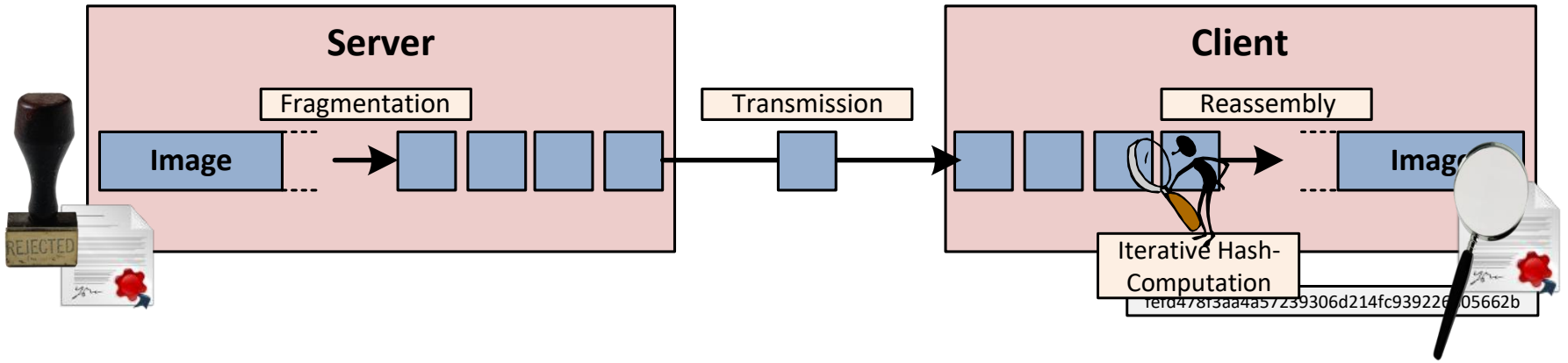
Selectivity:

- **via uni-, multi-cast transmissions** (broadcast available as well)
- **no multicast in IEEE 802.15.4 → explicit multicast (Xcast)**

Intrusion Detection System (IDS): optional IDS integration

Security mechanism:

- **digital signatures (ECC):**
  - nodes can check **integrity** and **authenticity**



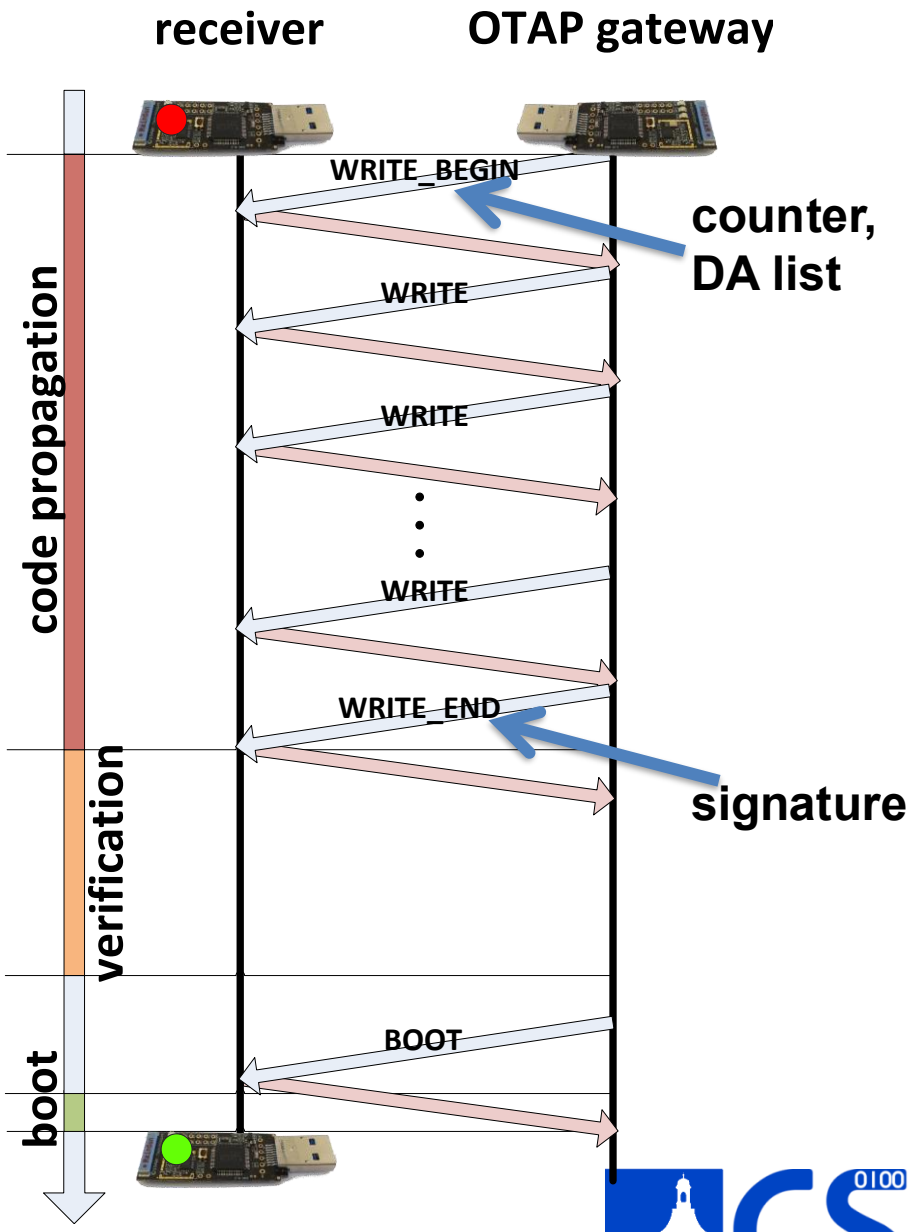
- **invalid signature:**
  - deleting image
  - **locking OTAP module** (primary app not disrupted)
  - **IDS report**
- **asymmetric cryptography**
- **version counter** and **destination address** included in signature

Security features:

- **Reprogram node attack resilience**
- **mitigation of DoS attacks**
- **compromise-tolerant**
- **Replay attack resilience**

OTAP operation phases:

1. **image preparation**
   - signature
   - version counter
   - fragmentation
2. **image propagation**
   - primary app not interrupted
   - timeout triggers IDS alert
3. **image verification**
   - **disruption of primary app**
   - duration: 9-14 sec
   - failure triggers IDS alert
4. **image booting**
   - confirmation with IDS notification



Computer Science 4 – TacNet@cs.uni-bonn.de

Performance Evaluation:

- **SenSeOP** implemented in **TinyOS**
  - **TOSBoot**
  - **TinyECC** (192 bit keys, SHA-1 hash)
- performance of **uni-, multi-, broadcast**

Platforms:

- frequency:
- data rate:
- max. payload size:

→ **# packets for OTAP**

TelosB

- 2.4 GHz
- 250 kbps
- 114 byte

→ **487 packets**

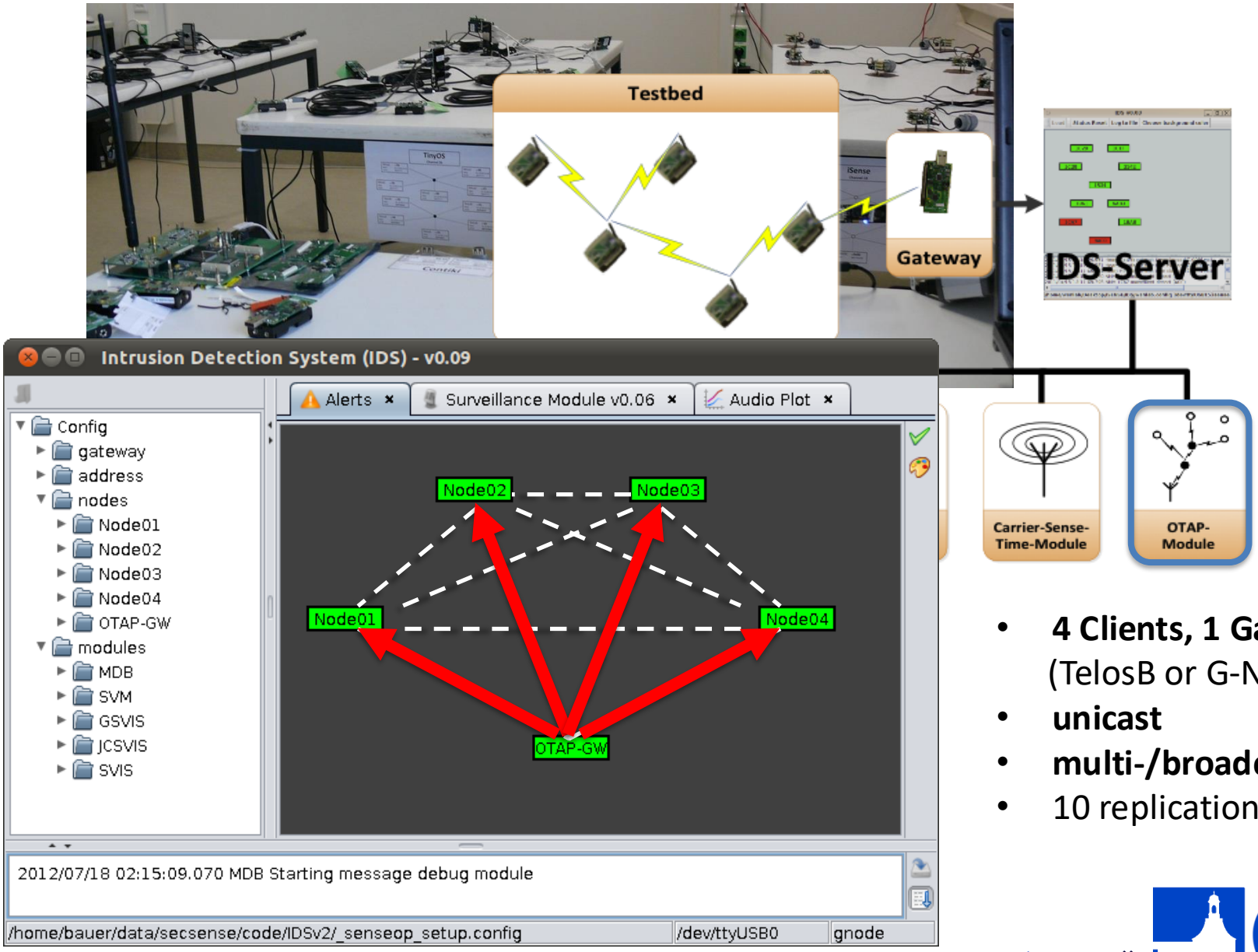
G-Node

- 868 MHz
- 38.4 kbps
- 52 byte

→ **928 packets**

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de



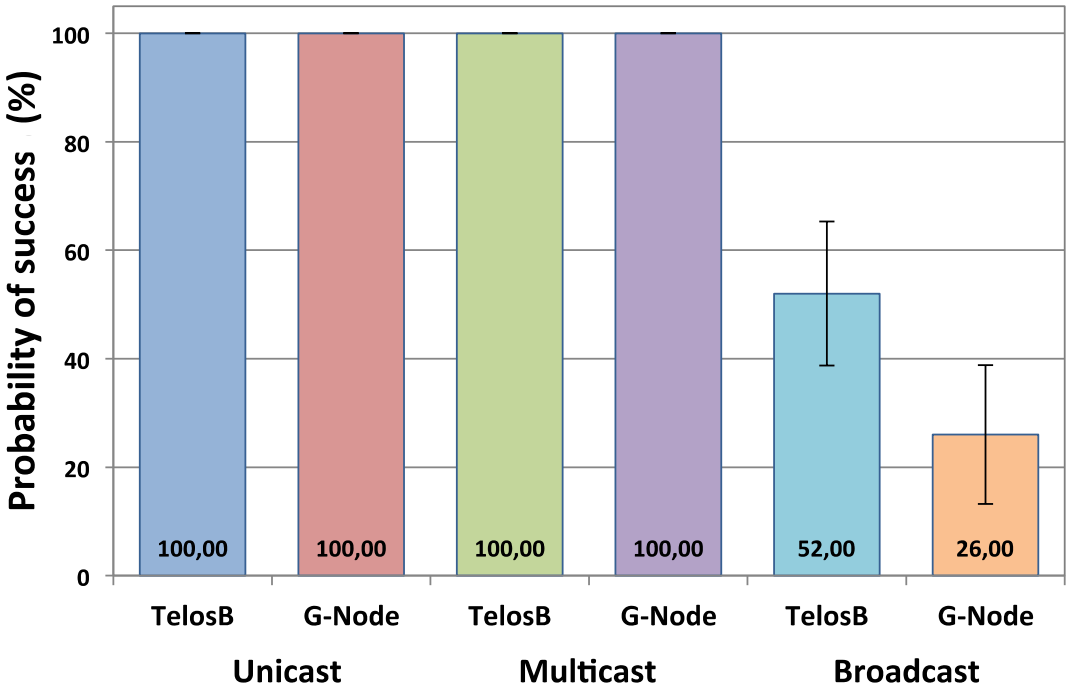
- **4 Clients, 1 Gateway** (TelosB or G-Node)
- **unicast**
- **multi-/broadcast**
- 10 replications

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de

Reliability:

- **success of OTAP transfer**



- **uni- and multicast mode:**
  - **100% reliable** (ACKs)
- **broadcast mode:**
  - unknown # receivers → unknown # ACKs
  - **retransmission only if NO ACK received**

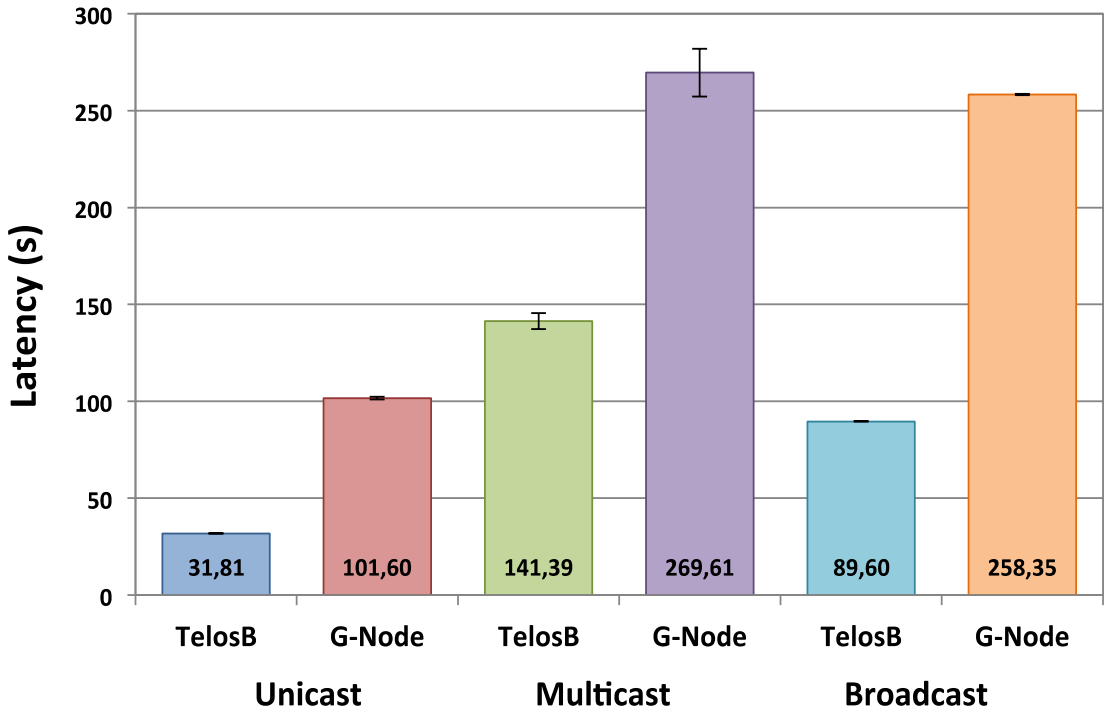
→ **not applicable**

Computer Science 4 – TacNet@cs.uni-bonn.de

Latency:

- **duration of OTAP transfer**

(w/o verification of signature)

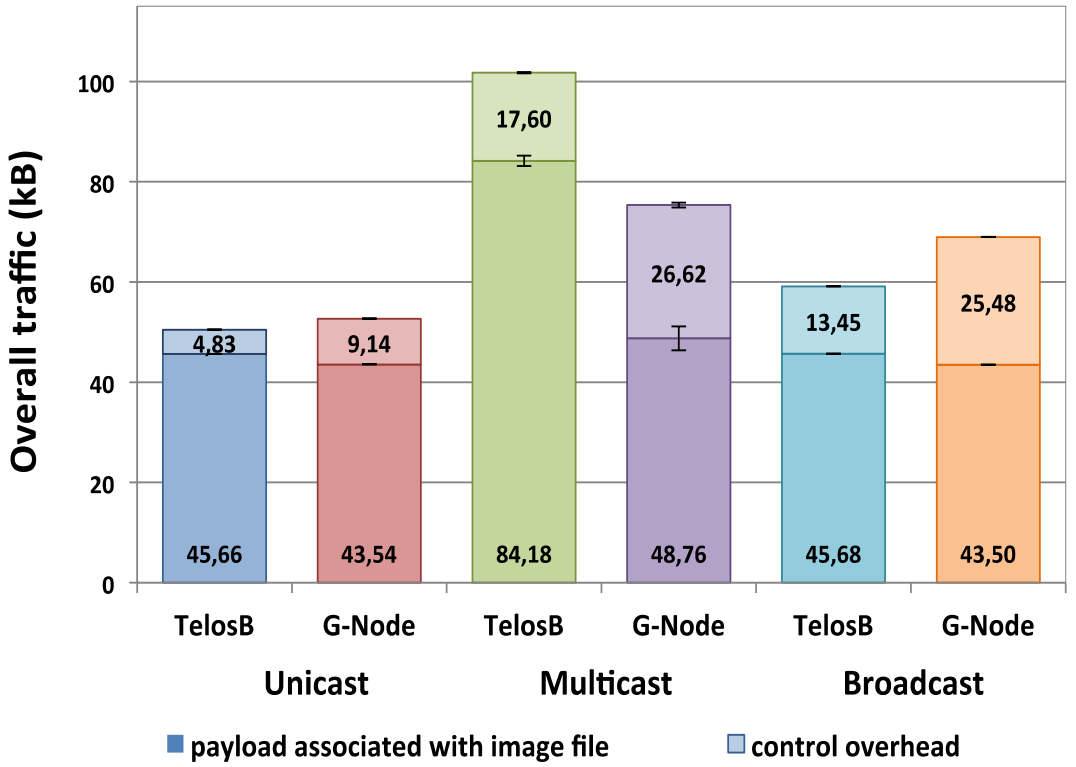


- **multicast mode:**
  - **higher inter-packet buffer required**
    to avoid collisions of multiple replies

→ **no substantial benefit**

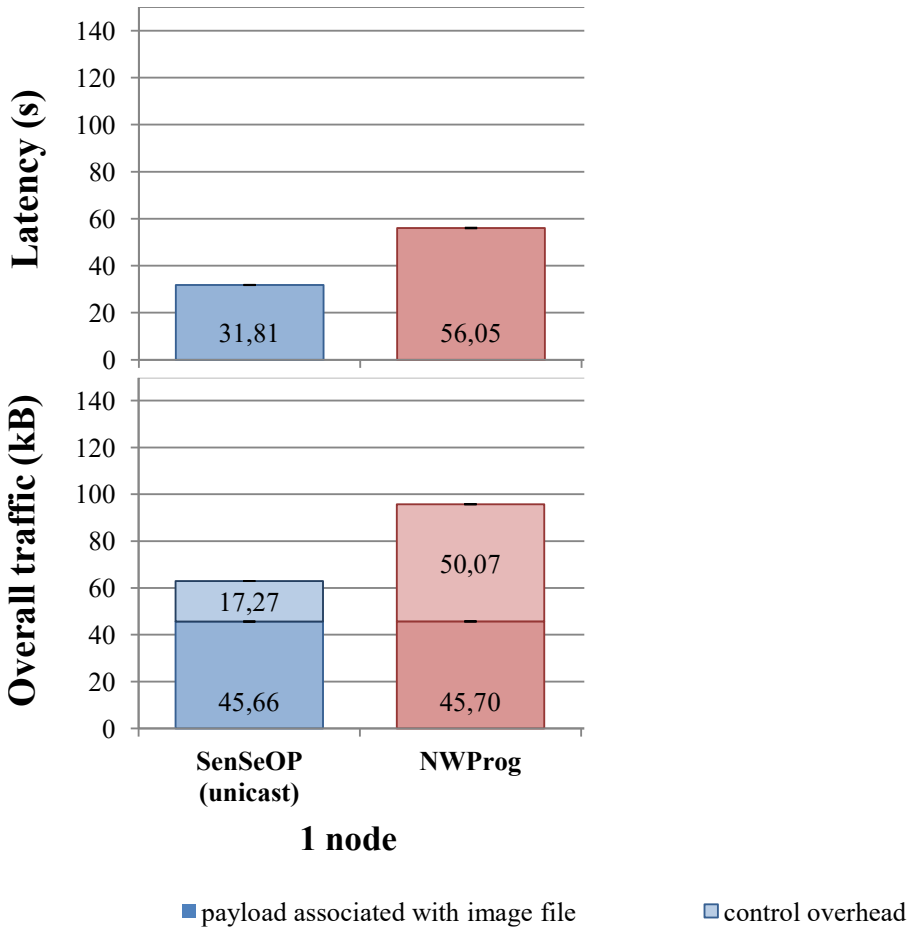
Traffic load:

- including:
  - **control overhead**
  - **data packets** and **retransmits**
- representing **energy usage**



- **multicast mode:**
  - **reduction of network load and energy consumption**

→ **significant benefit**



Future Work:

- **multi-hop support**
- **code size reduction techniques**

- **NWProg: link layer ACKs → less performance** (in this scenario)
- **Deluge:**
  - **higher performance**
  - **less overhead** due to **selective ACKs**

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de

Conclusion:

- **SenSeOP (selective'n'secure Over-the-air-Programming):**
  - **selectivity** (explicit multicast)
  - **security** (asymmetric cryptography, IDS integration)
  - **light-weight** (simple propagation)

- **Performance Evaluation**
  - **significant benefit of multicast-mode**
    - **energy-efficiency**
    - **reduction of network load**

universitätbonn CS 0100

Computer Science 4 – TacNet@cs.uni-bonn.de

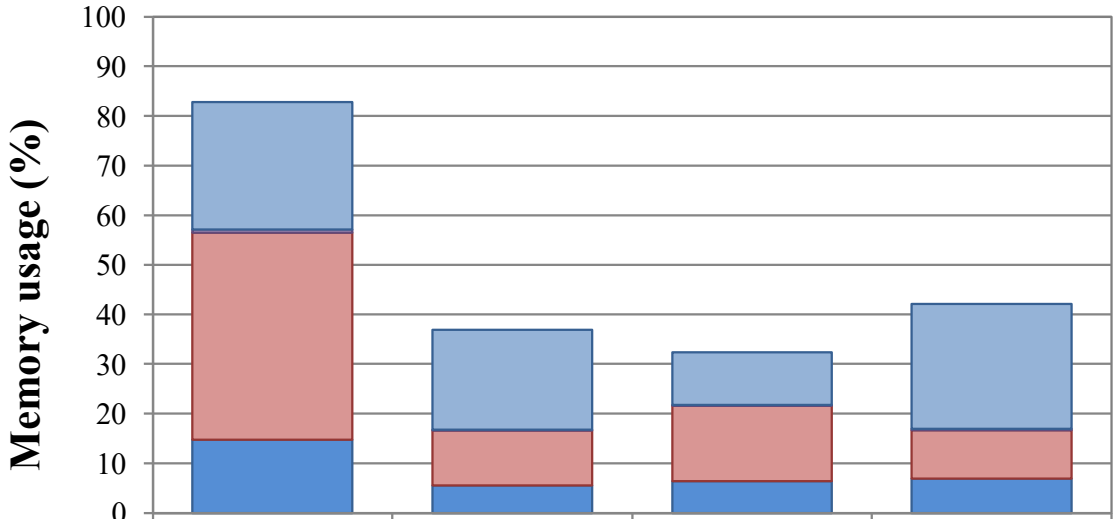
Rheinische Friedrich-Wilhelms-Universität Bonn

Institute of Computer Science 4
Communication and Distributed Systems

Dipl.-Inform. Jan Bauer

Friedrich-Ebert-Allee 144
D-53113 Bonn, Germany
Phone: +49 228 73-54204
Fax: +49 228 73-4571
bauer@cs.uni-bonn.de
http://net.cs.uni-bonn.de/jb

Picture by Nils Aschenbruck



	TelosB ROM	TelosB RAM	G-Node ROM	G-Node RAM
security ext.	25,72	20,06	10,57	25,12
multicast ext.	0,65	0,23	0,24	0,27
OTAP	41,75	11,04	15,22	9,74
core system	14,67	5,53	6,33	6,96

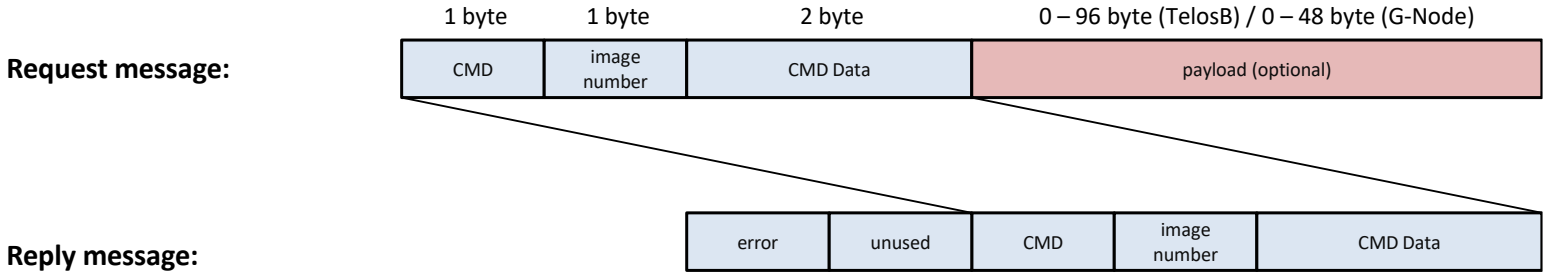
TelosB:
48 kB ROM
10 kB RAM

G-Node:
116 kB ROM
8 kB RAM

- **inherent memory demand:**
  - **OTAP module** (TOSBoot)
  - **Security extension** (TinyECC)
- **however:**
  - many components can be **reused** by primary app
    → **little additional code size**

universitätbonn CS 0100
Computer Science 4 – TacNet@cs.uni-bonn.de

Message format (adopted from NWProg):



Reliability:

- **ARQ mechanism**
  (ACKs, Timeouts)

Security:

- **additional packets**
- additional **IDS alert messages**

CMD	Image-Slot	CMD Data	Payload
erase	{0,1}	--	DA list
boot	{0,1}	time	DA list
reboot	--	time	DA list
write	{0,1}	position	**data**
write_begin	{0,1}	**counter**	**DA list**
write_end	{0,1}	--	**signature**