Technische
Universität
Braunschweig

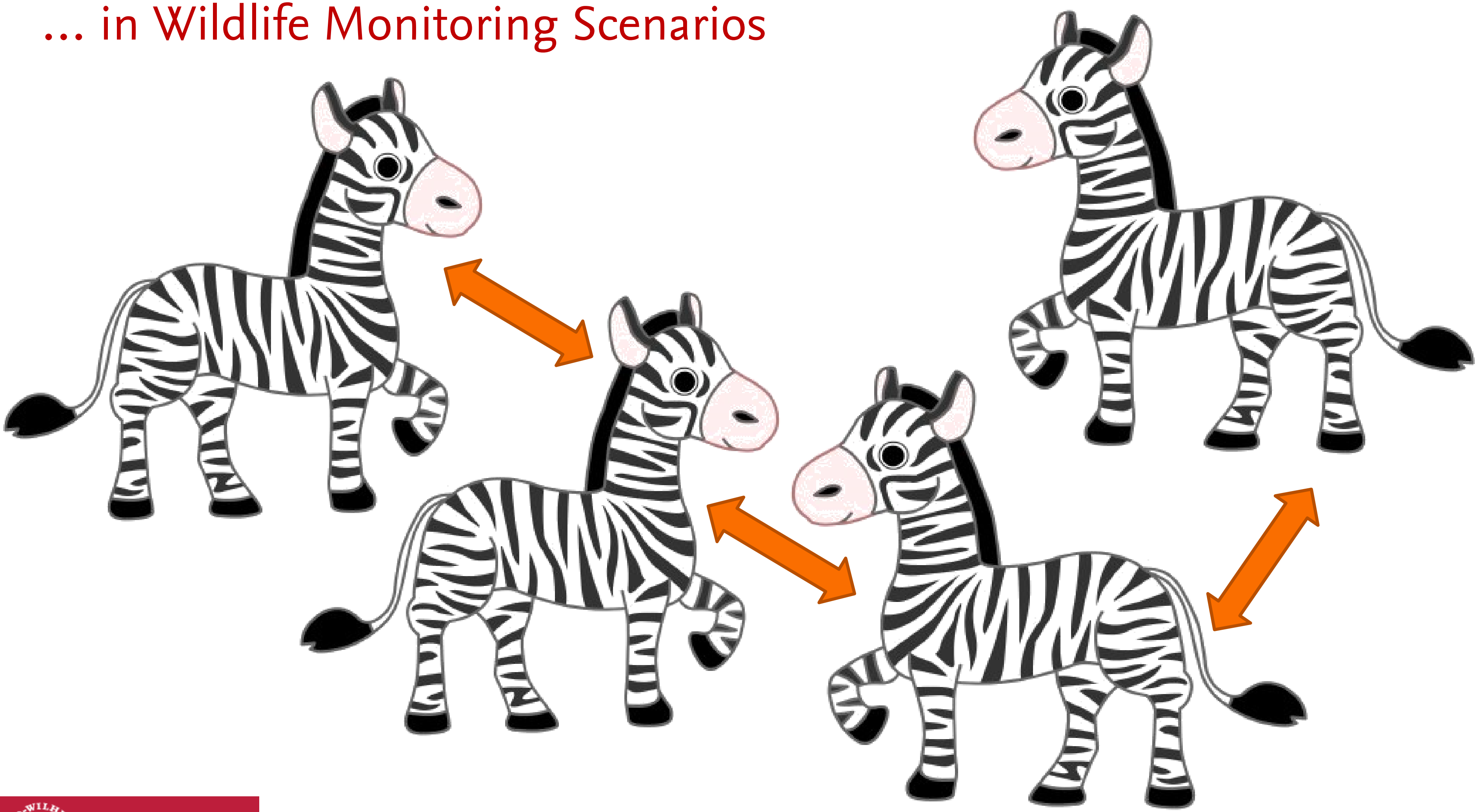
Institut für Betriebsysteme
und Rechnerverbund

RAIM: Redundant Array of Independent Motes

Dominik Schürmann, **Felix Büsching**, Sebastian Willenborg, Lars Wolf

Motivation: Store Data on WSN nodes

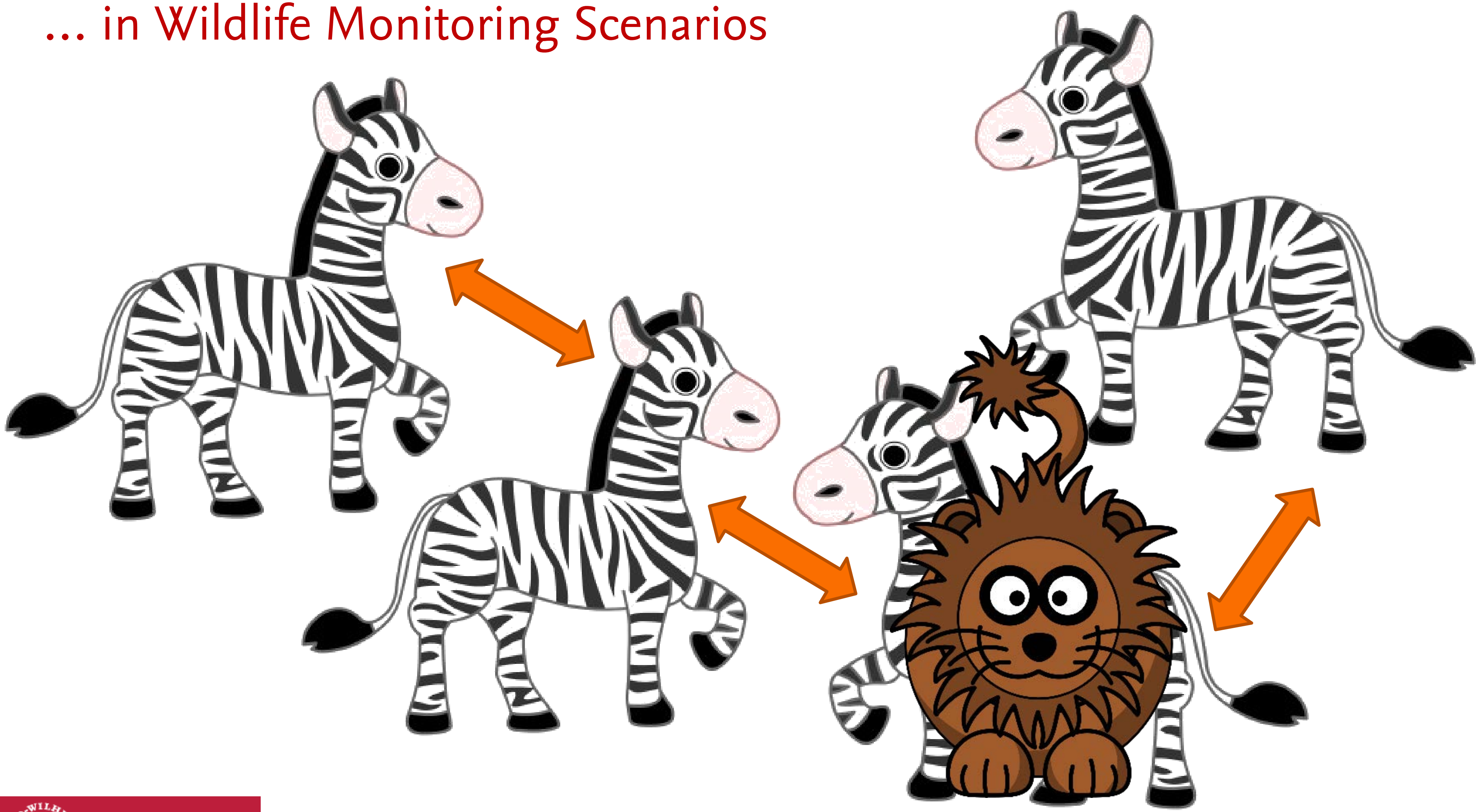
… in Wildlife Monitoring Scenarios



Wild LION appeared!

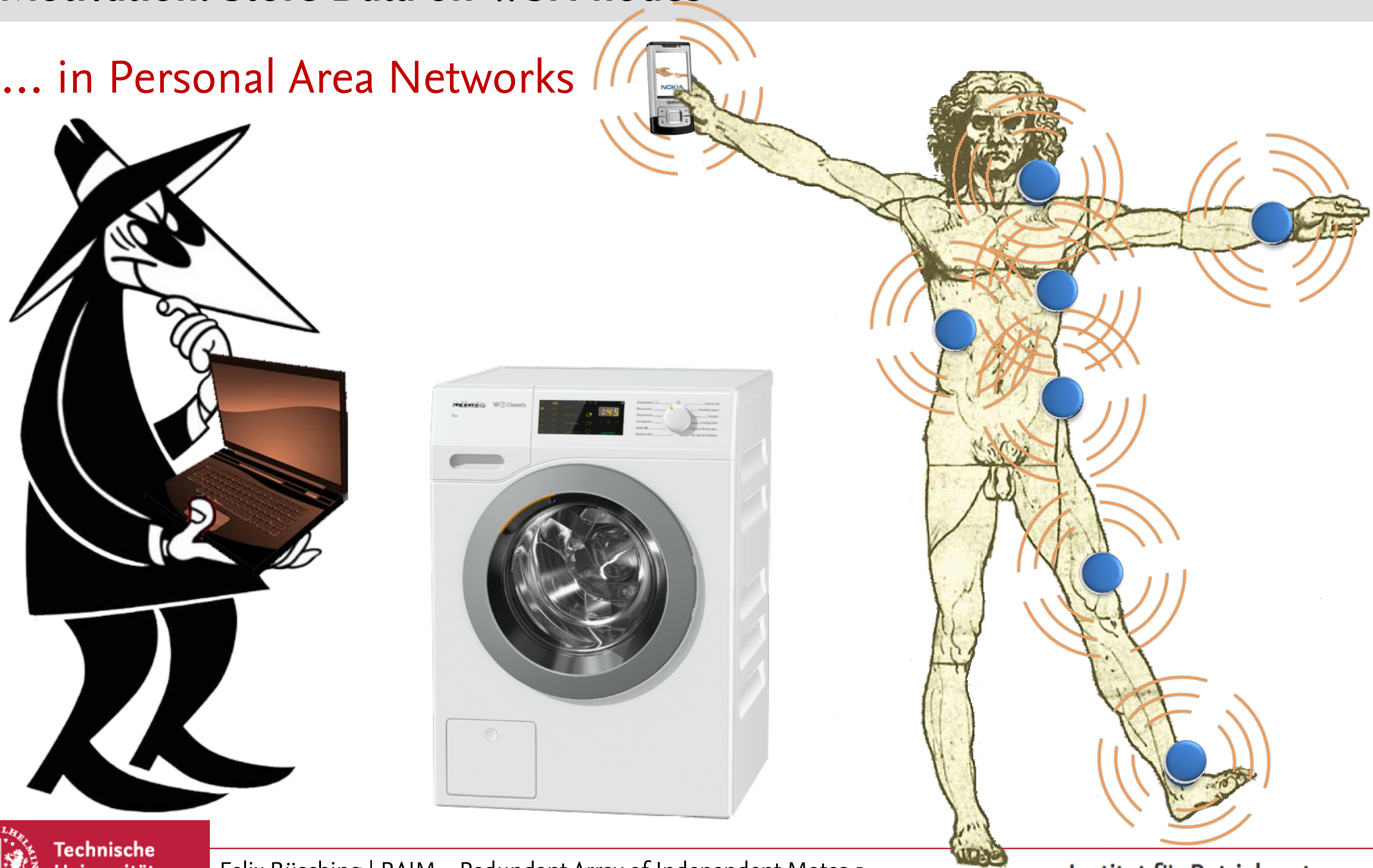
Motivation: Store Data on WSN nodes

... in Wildlife Monitoring Scenarios



Motivation: Store Data on WSN nodes

… in Personal Area Networks



WSN Challenges

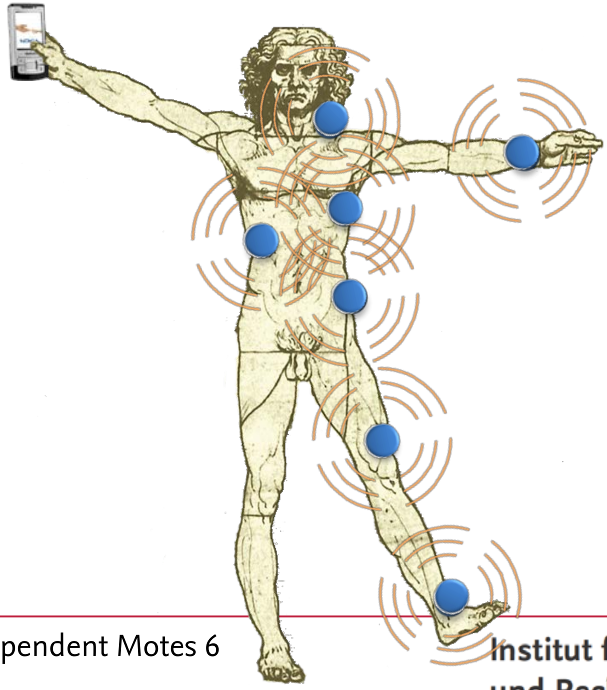
Nodes can get

- Lost
- Stolen
- Eaten
- Destroyed

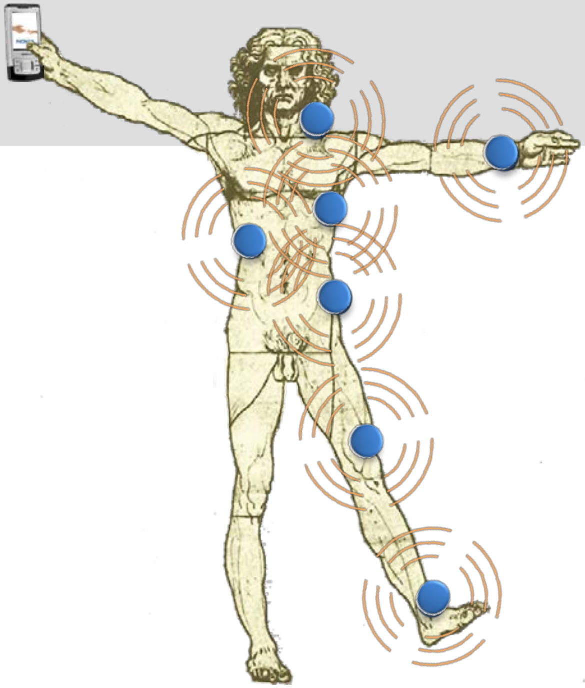
Data can be

- Private / Confidential

- Data should be preserved



So, what’s the question here?



How can we ensure

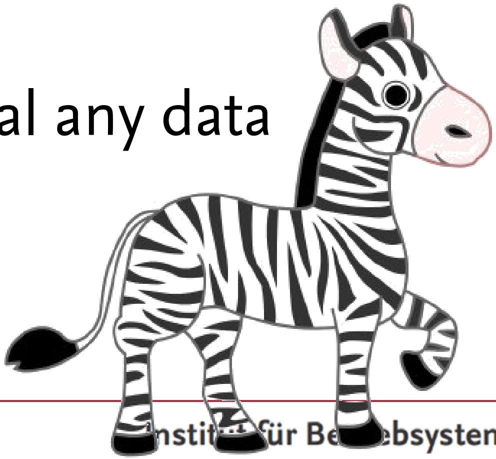
- Privacy and Confidentiality
- Data Security

… at the same time

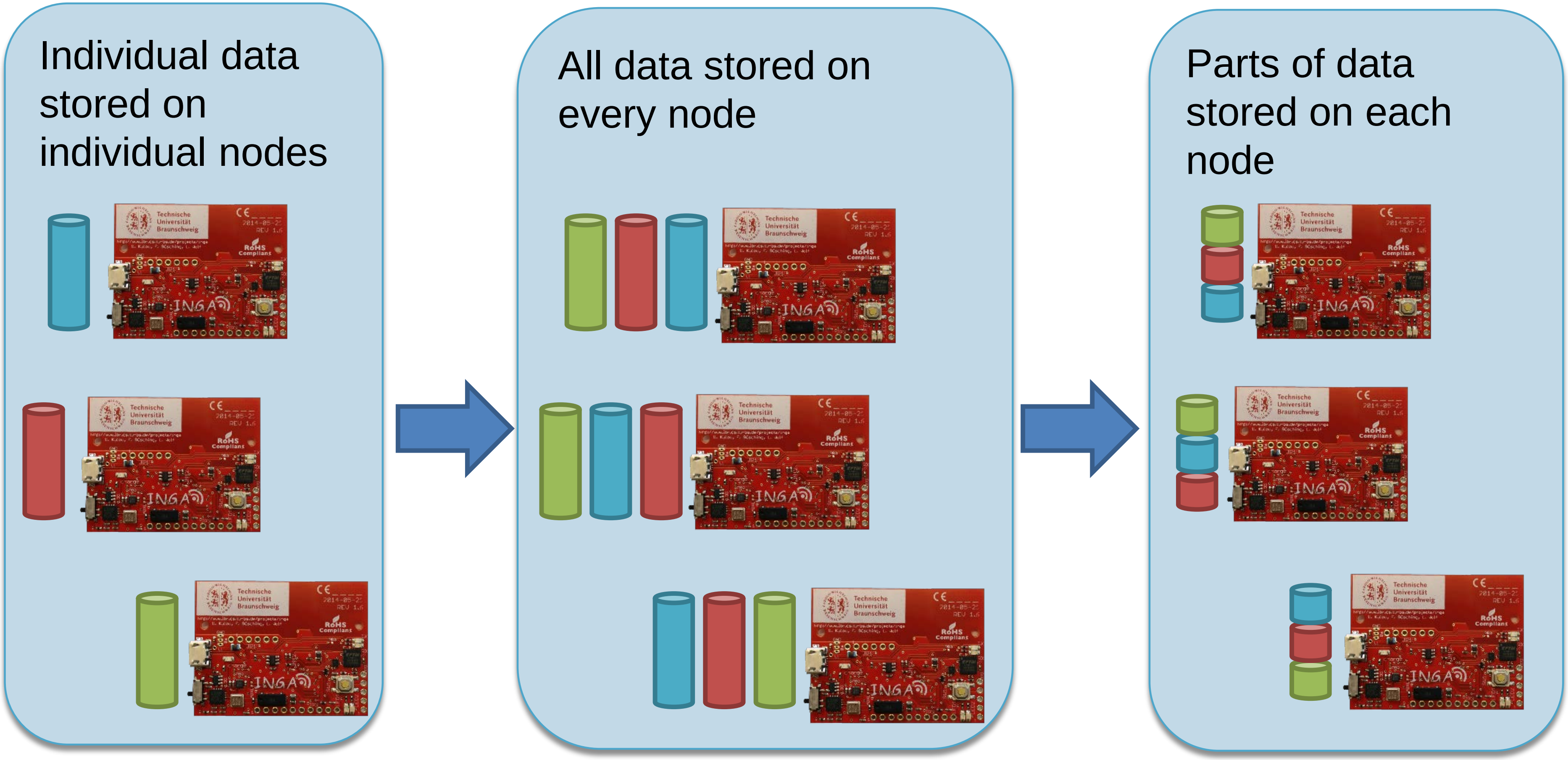
… and in different configurations?

Can we achieve different levels of Redundancy and Confidentiality?!

- A single “missing” BAN sensor should not reveal any data
- Collecting one Zebra is sufficient to get all data
- → depending on the individual scenario!



Idea



Individual data stored on individual nodes

All data stored on every node

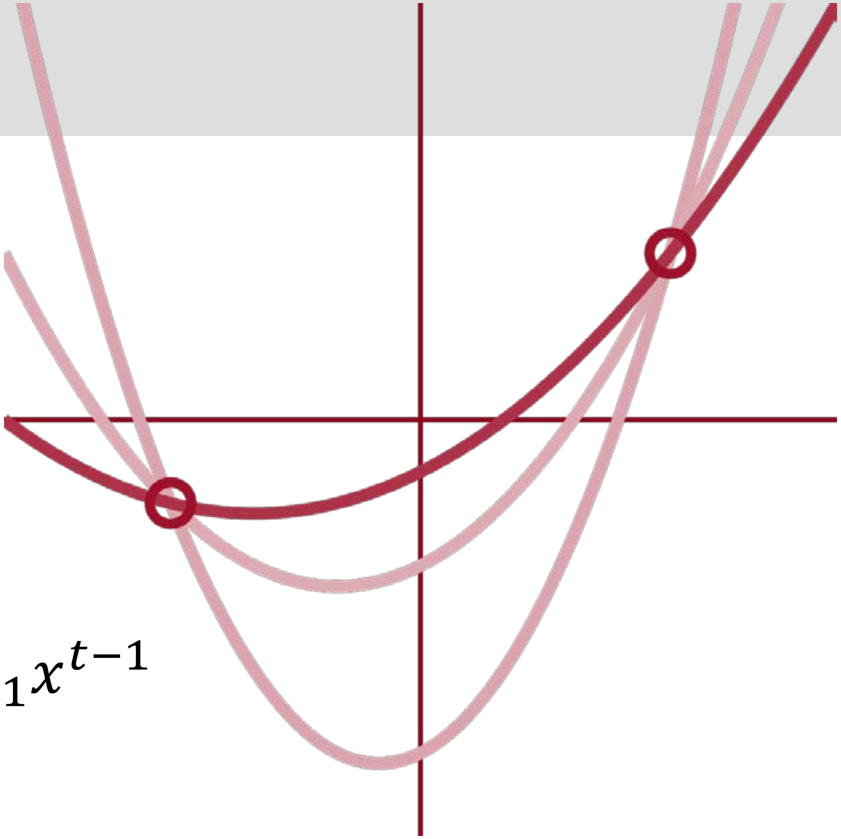
Parts of data stored on each node

No redundancy

Full redundancy

Full confidentiality

Basics: Secret Sharing



„normal“ Secret Sharing

- $s = s_1 + s_2 + \cdots + \ s_n$
- All parts of s needed

Shamir’s Secret Sharing

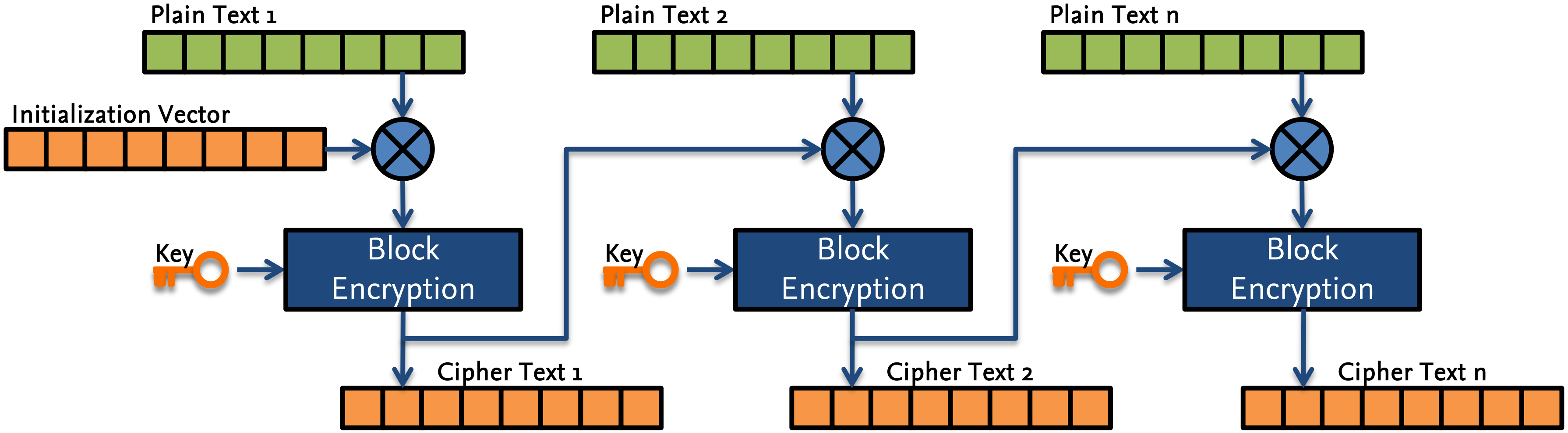
- $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$
- t pairs of values $\big(x, f(x)\big)$ needed
- $t - 1$ keys can be compromised

Optimization for µC

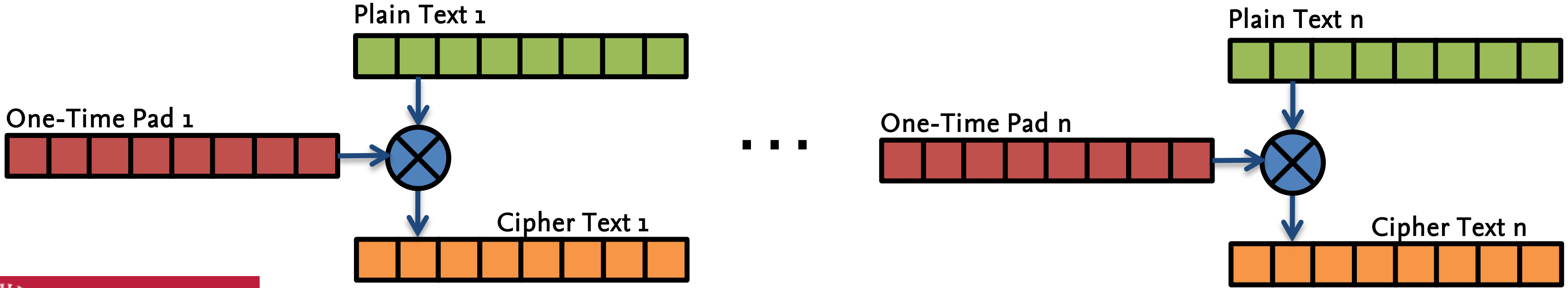
- $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}\ mod\ p$

Basics: AES and OTP

AES in CBC mode (Chiper Block Chaining)



One-Time Pads



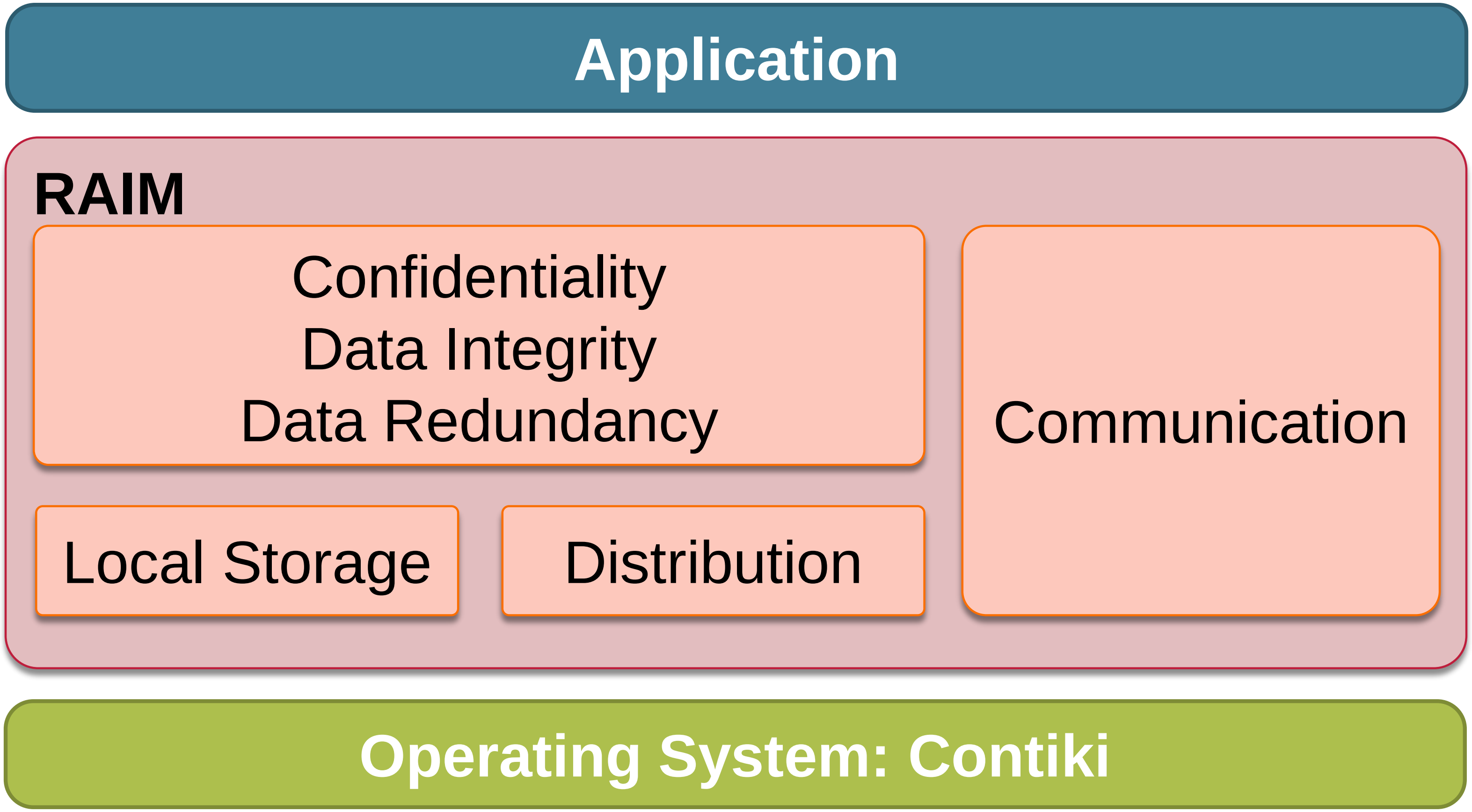
So, what did we do?

Take

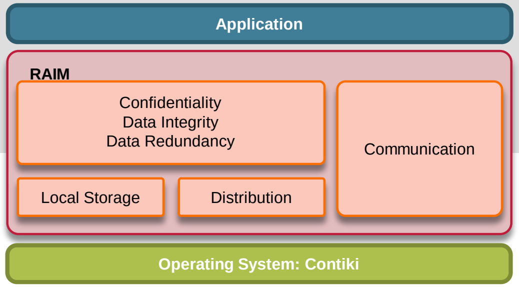
- Shamir‘s Secret Sharing
- Well known encryption methods
- Well known authentication methods

… and build it.

RAIM‘s modular architecture



Implementation – I



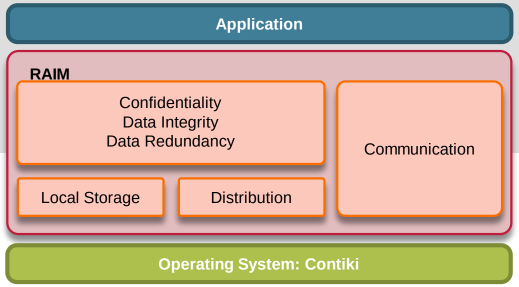
Operating System

- Contiki

Local storage

- SD-card
- FAT 32
- Special directory structure:
  - *local* – contains locally generated data
    - In OTP configuration also OTPs are stored here
  - *$mote_id* – contains data received from other nodes

Implementation – II

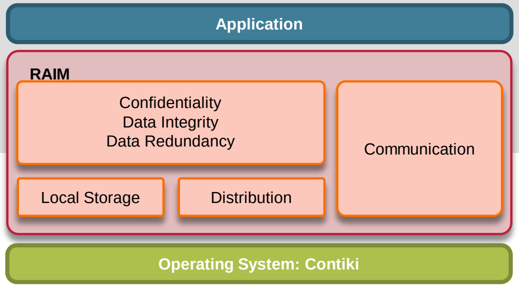


Confidentiality

- AES
  - In CBC-mode
  - Hardware AES in RF233
  - Pre-shared key
- One-Time Pads
  - In place

- OTP needs large storage
  - But not additional
- AES can be used for nodes without storage

Implementation – III

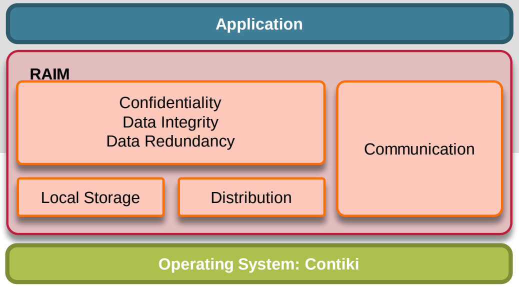


Integrity

- CBC-MAC
  - Hardware AES in RF233
  - Tag appended to transmitted data

- CRC-8 checksum
  - When no pre-shared key is available
  - Only error detection

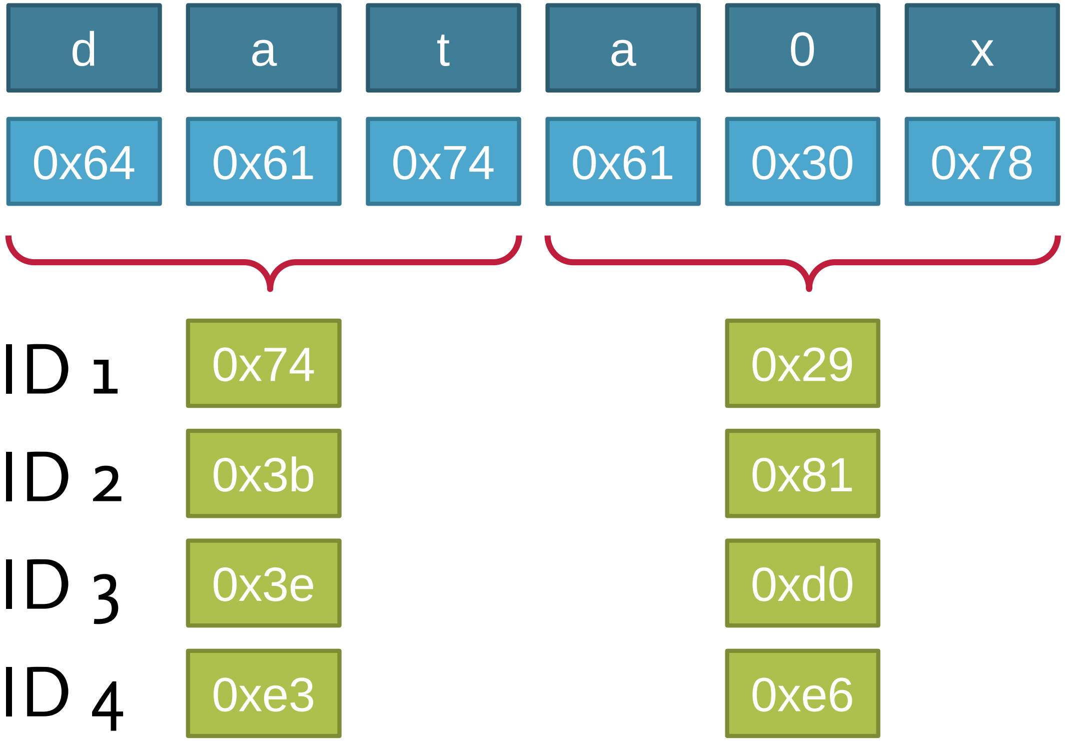
Implementation – IV



Data Redundancy and Distribution

- No redundancy
  - Data is only stored (and encrypted) locally
- Full redundancy
  - All data is spread to any other nodes
- (k;n)-threshold Sharmir’s Secret Sharing
  - Data is spread over n nodes
  - k nodes are needed for encryption

Examplary Distribution: (3;4)-threshold SSS scheme



d	a	t	a	0	x
0x64	0x61	0x74	0x61	0x30	0x78

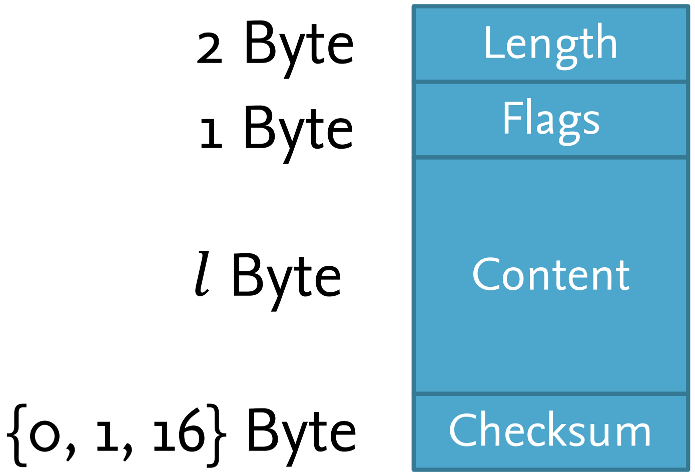
ID 1	0x74	0x29
ID 2	0x3b	0x81
ID 3	0x3e	0xd0
ID 4	0xe3	0xe6

- 6 Byte divided in
- 2 chunks a 3 Byte

- chunks distributed among 4 motes

3 out of 4 motes are required to reconstruct data

Evaluation: Storage Requirements For l Byte of Data



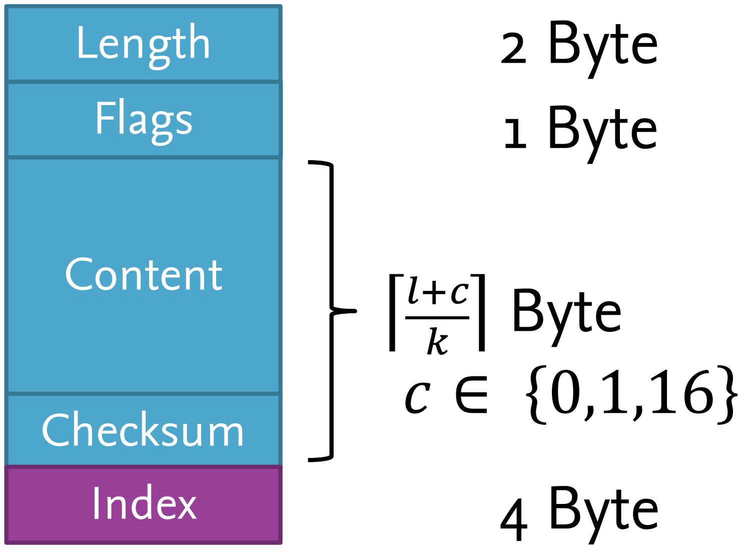
2 Byte | Length

1 Byte | Flags

l Byte | Content

{0, 1, 16} Byte | Checksum

Local storage of sensing mote



Length | 2 Byte

Flags | 1 Byte

Content, Checksum: $\left\lceil \frac{l+c}{k} \right\rceil$ Byte, $c \in \{0,1,16\}$

Index | 4 Byte

Storage of neighboring mote (remote)

Cipher Suite Configurations

Cipher Suite	Properties
CRC only	Error Detection
CBC-MAC only	Data Integrity
AES	Confidentiality
OTP	Confidentiality
OTP + CBC-MAC	Confidentiality + Data Integrity
AES + CBC-MAC	Confidentiality + Data Integrity

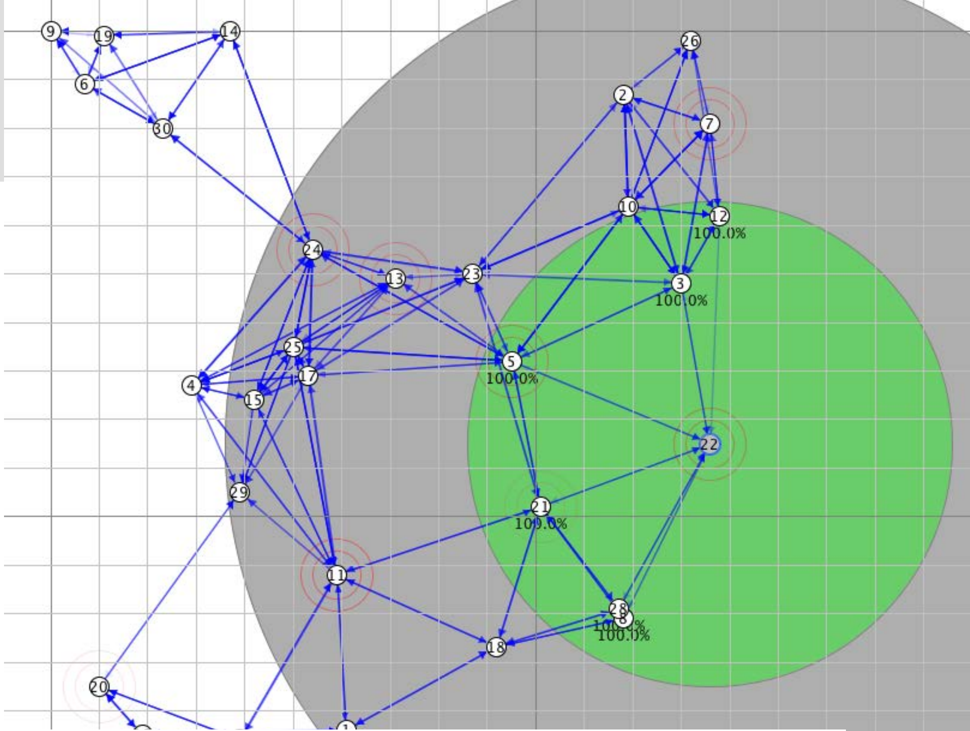
Attack Models - External Attacker

- Eavesdropping/man-in-the-middle
  - If configured for OTP/AES + CBC-MAC
  - → Data encrypted and authenticated ✓
- Insert data
  - If configured for OTP/AES
  - → Preshared key is not known ✓
- Replay attacks
  - Index included and authenticated (CBC-MAC)
  - →receiving nodes verify index not used before ✓

Attack Models – Internal Attacker

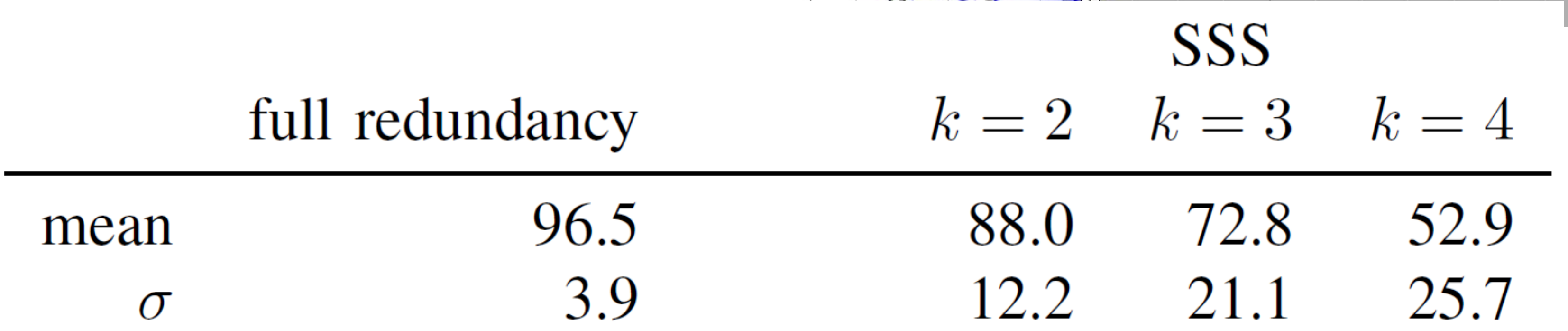
- Stolen external storage
  - Key on mote (AES) or overwritten (OTP) ✓
- Storage exhaustion
  - Files for each *$mote_id* limited ✓
- Pollution/data dropping
  - (k; n)-threshold for SSS → < n-k motes ✓
- Stolen/destroyed mote
  - redundancy layer prevents data loss ✓
- Compromised AES key
  - Decryption of future communication ⚡
  - Past data can only be recovered when k motes are stolen

Simulations in Cooja



Wildlife Monitoring

- 20 of 30 motes have storage
- Constantly, randomly moving
- Different configurations for k



	full redundancy	SSS		
		$k = 2$	$k = 3$	$k = 4$
mean	96.5	88.0	72.8	52.9
σ	3.9	12.2	21.1	25.7

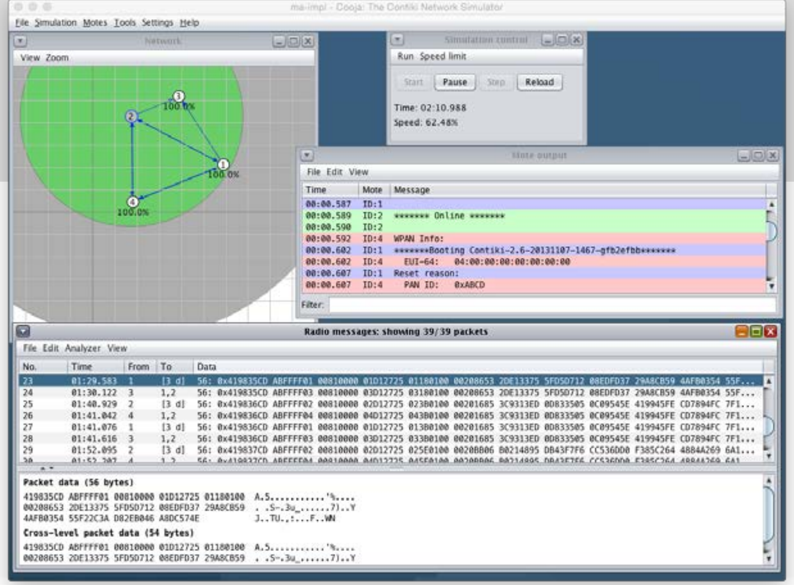
Percentage of recoverable data

- after the loss of one node at different levels of redundancy

Simulations in Cooja

Personal Health Monitoring

- 8 motes randomly generate data
- 4 motes have storage
- Other 4 just send data
- Constantly in radio range
- k = 3
- AES and CBC-MAC



Time: 02:10.988
Speed: 62.48%

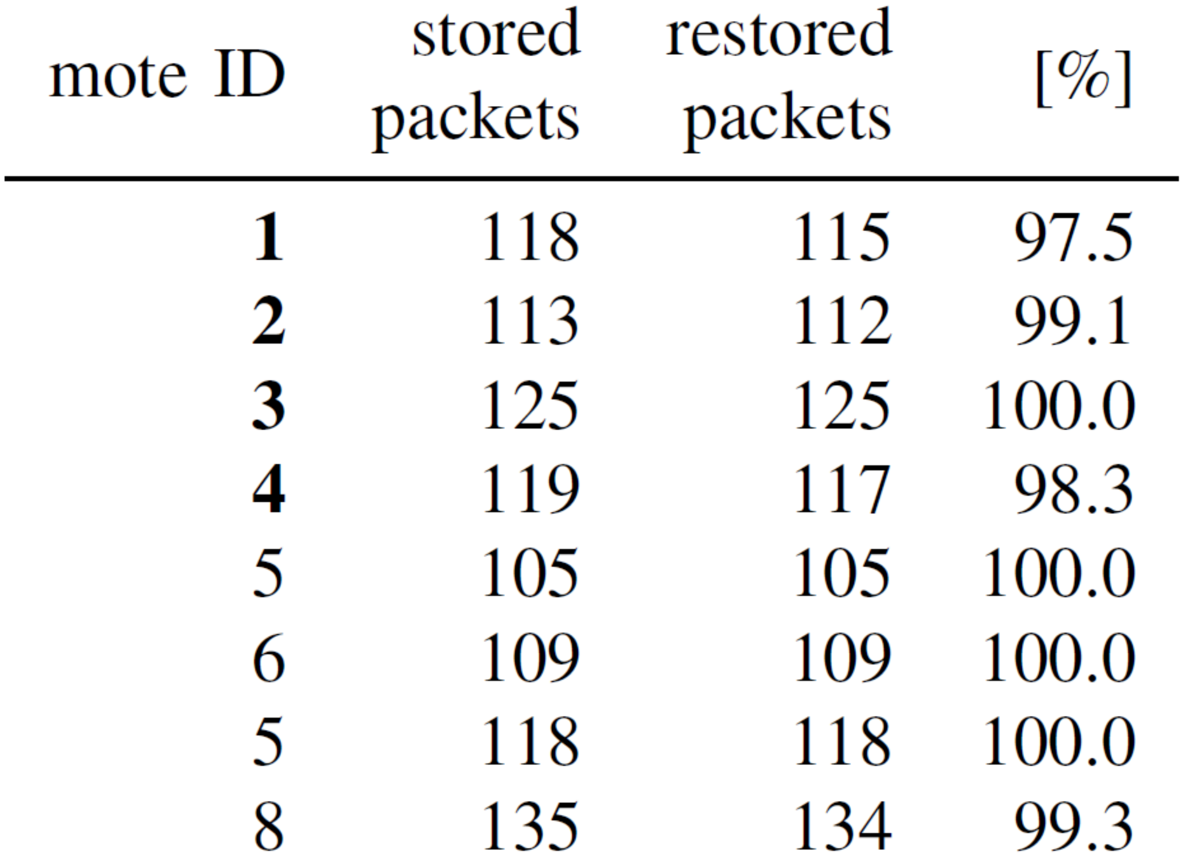
```
Time       Mote  Message
00:00.587  ID:1
00:00.589  ID:2  ******* Online *******
00:00.590  ID:2
00:00.592  ID:4  WPAN Info:
00:00.602  ID:1  *******Booting Contiki-2.6-20131107-1467-gfb2efbb*******
00:00.602  ID:4    EUI-64:   04:00:00:00:00:00:00:00
00:00.607  ID:1  Reset reason:
00:00.607  ID:4    PAN ID:   0xABCD
```

Radio messages: showing 39/39 packets

```
No.  Time       From  To     Data
23   01:29.583  1     [3 d]  56: 0x419835CD ABFFFF01 00810000 01D12725 01180100 00208653 2DE13375 5FD5D712 08EDFD37 29A8CB59 4AFB0354 55F...
24   01:30.122  3     1,2    56: 0x419835CD ABFFFF03 00810000 03D12725 03180100 00208653 2DE13375 5FD5D712 08EDFD37 29A8CB59 4AFB0354 55F...
25   01:40.929  2     [3 d]  56: 0x419836CD ABFFFF02 00810000 02D12725 023B0100 00201685 3C9313ED 0D833505 0C09545E 419945FE CD7894FC 7F1...
26   01:41.042  4     1,2    56: 0x419836CD ABFFFF04 00810000 04D12725 043B0100 00201685 3C9313ED 0D833505 0C09545E 419945FE CD7894FC 7F1...
27   01:41.076  1     [3 d]  56: 0x419836CD ABFFFF01 00810000 01D12725 013B0100 00201685 3C9313ED 0D833505 0C09545E 419945FE CD7894FC 7F1...
28   01:41.616  3     1,2    56: 0x419836CD ABFFFF03 00810000 03D12725 033B0100 00201685 3C9313ED 0D833505 0C09545E 419945FE CD7894FC 7F1...
29   01:52.095  2     [3 d]  56: 0x419837CD ABFFFF02 00810000 02D12725 025E0100 0020BB06 00214895 DB43F7F6 CC536DD0 F385C264 4884A269 6A1...
30   01:52.207  4     1,2    56: 0x419837CD ABFFFF04 00810000 04D12725 045E0100 0020BB06 00214895 DB43F7F6 CC536DD0 F385C264 4884A269 6A1
```

```
Packet data (56 bytes)
419835CD ABFFFF01 00810000 01D12725 01180100  A.5...........'%....
00208653 2DE13375 5FD5D712 08EDFD37 29A8CB59  . .S-.3u_.......7)..Y
4AFB0354 55F22C3A D82EB046 A8DC574E           J..TU.,:...F..WN
Cross-level packet data (54 bytes)
419835CD ABFFFF01 00810000 01D12725 01180100  A.5...........'%....
00208653 2DE13375 5FD5D712 08EDFD37 29A8CB59  . .S-.3u_.......7)..Y
```

Recoverable data after the loss of one node

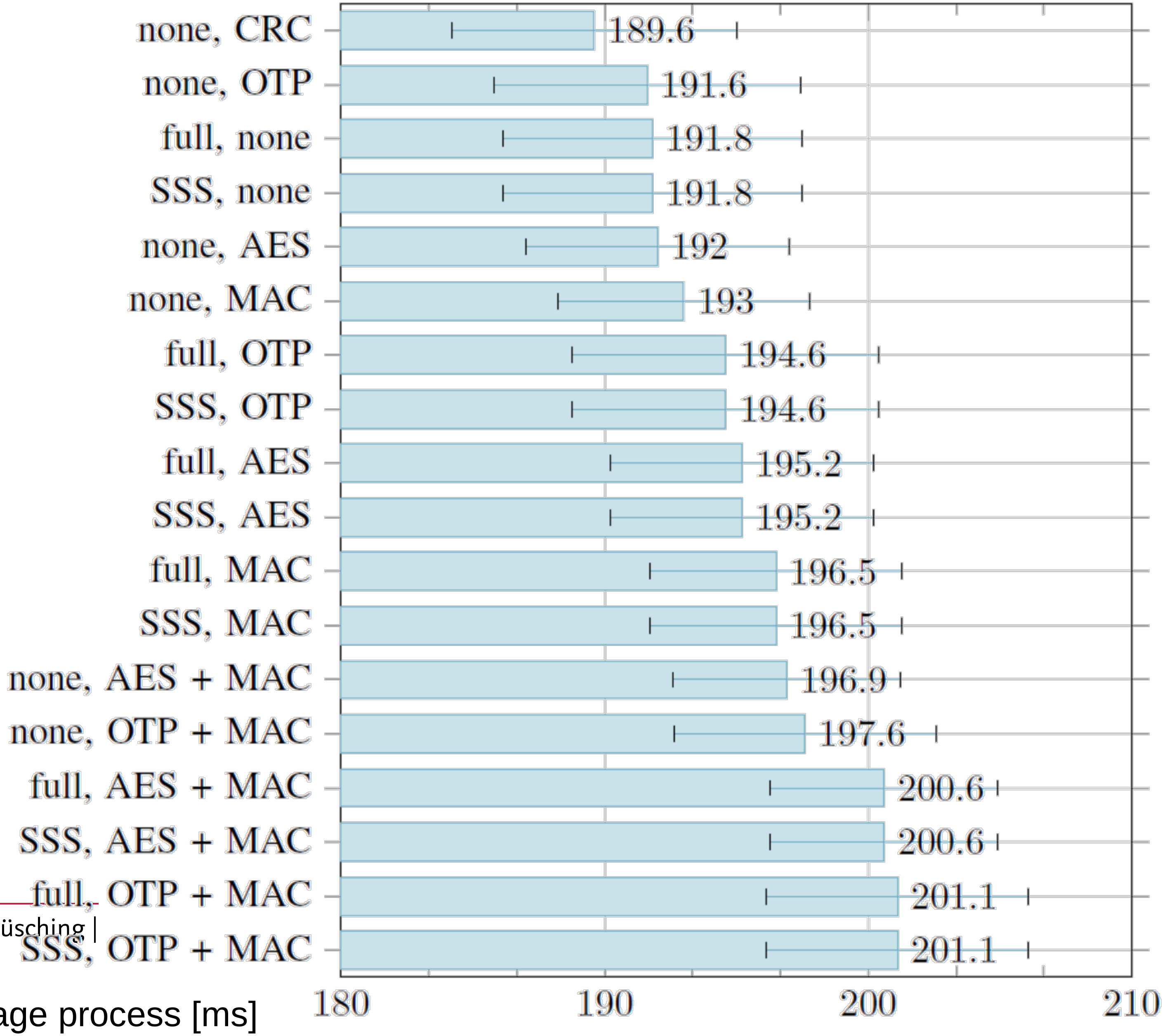


mote ID	stored packets	restored packets	[%]
1	118	115	97.5
2	113	112	99.1
3	125	125	100.0
4	119	117	98.3
5	105	105	100.0
6	109	109	100.0
5	118	118	100.0
8	135	134	99.3

} with storage

33% storage overhead

Througput (Redundancy, Chipher Suite)

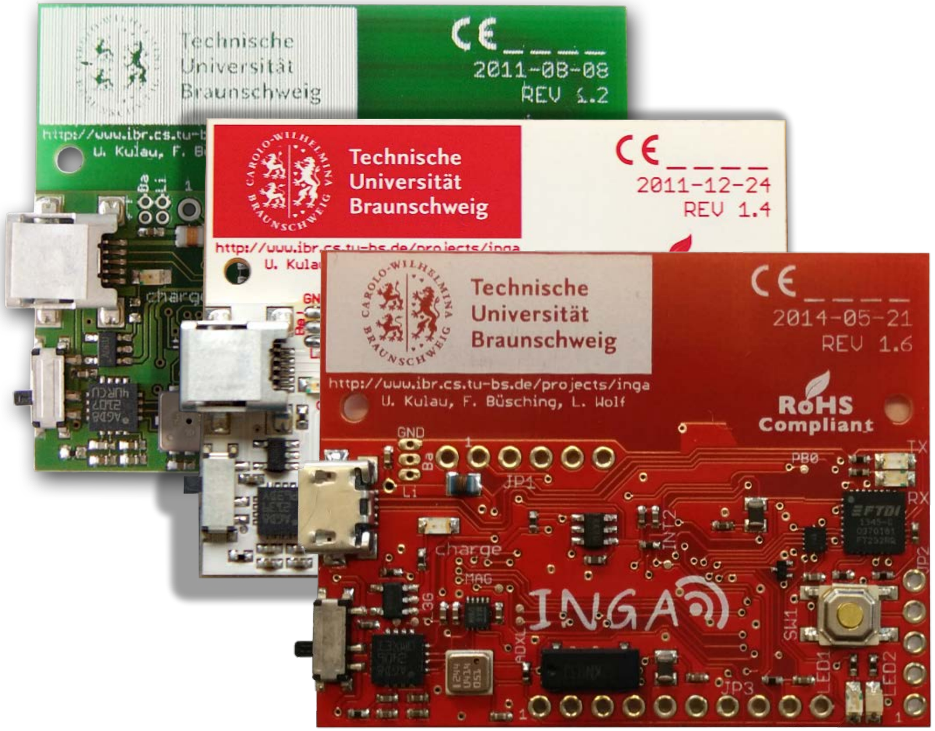


Duration of a single storage process [ms]

Measurements on physical Motes: INGA

ATmega architecture

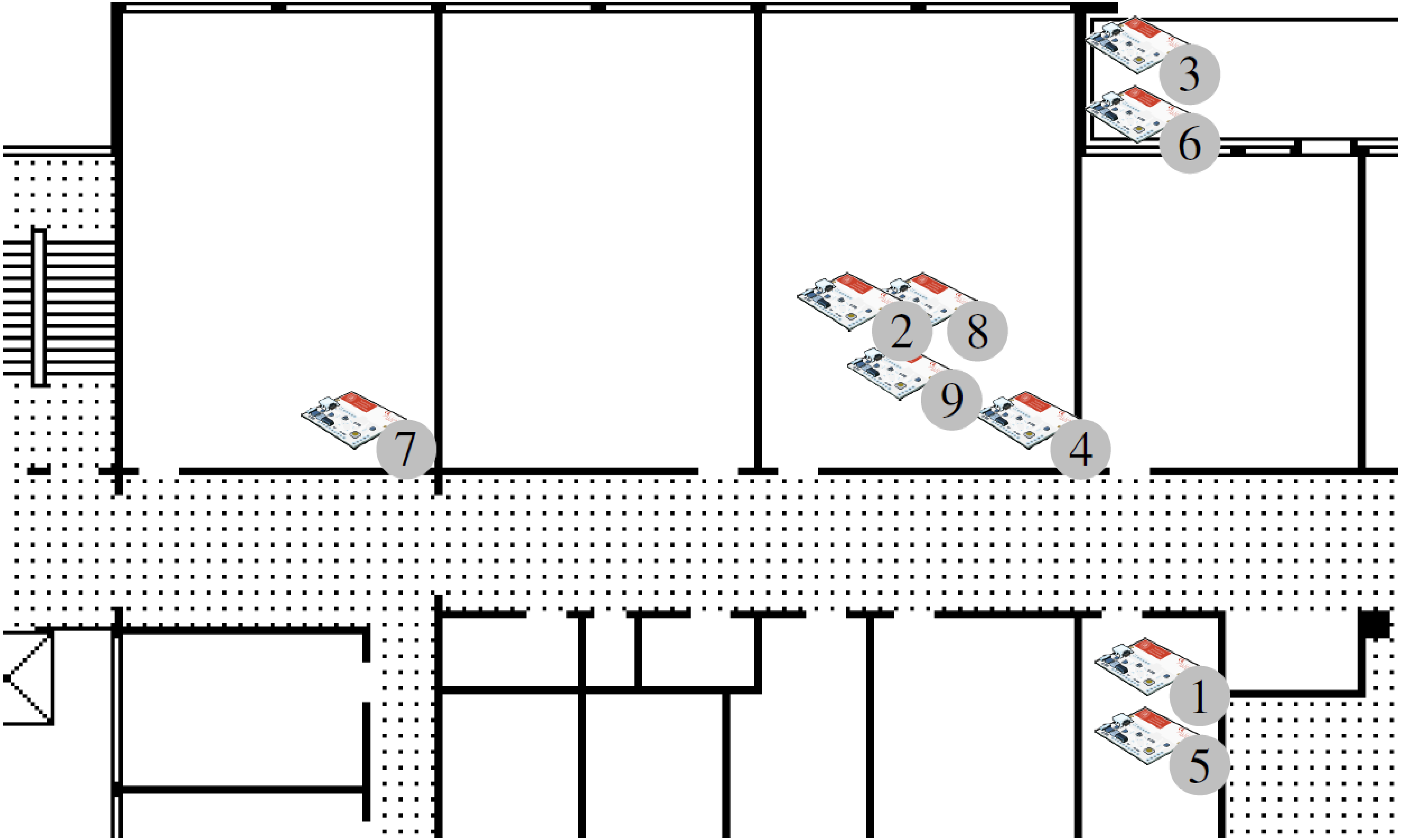
- ATmega 1284p microcontroller
  - 8 bit RISC architecture , 128 kB Flash, 16 kB SRAM, 4 kB EEPROM
- AT86RF233 Radio Transceiver


Technische Universität Braunschweig
2011-08-08
REV 1.2
Technische Universität Braunschweig
2011-12-24
REV 1.4
Technische Universität Braunschweig
2014-05-21
REV 1.6
http://www.ibr.cs.tu-bs.de/projects/inga
U. Kulau, F. Büsching, L. Wolf
RoHS Compliant
INGA

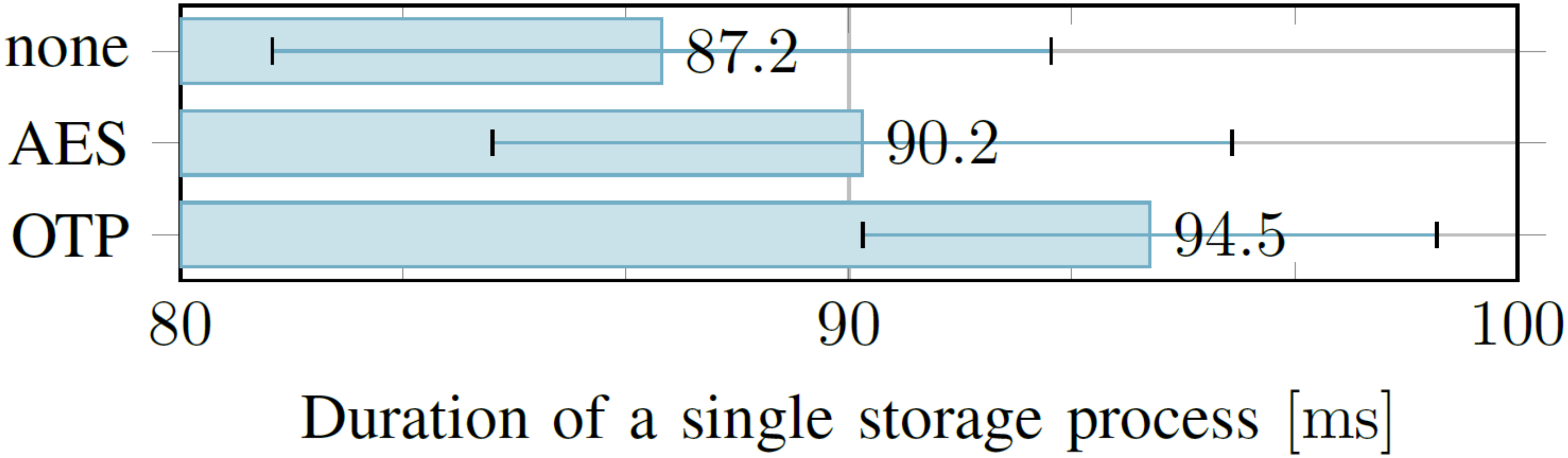
Setup

- 9 Motes measure temperature, barometric pressure every 60s

Evaluation in Testbed

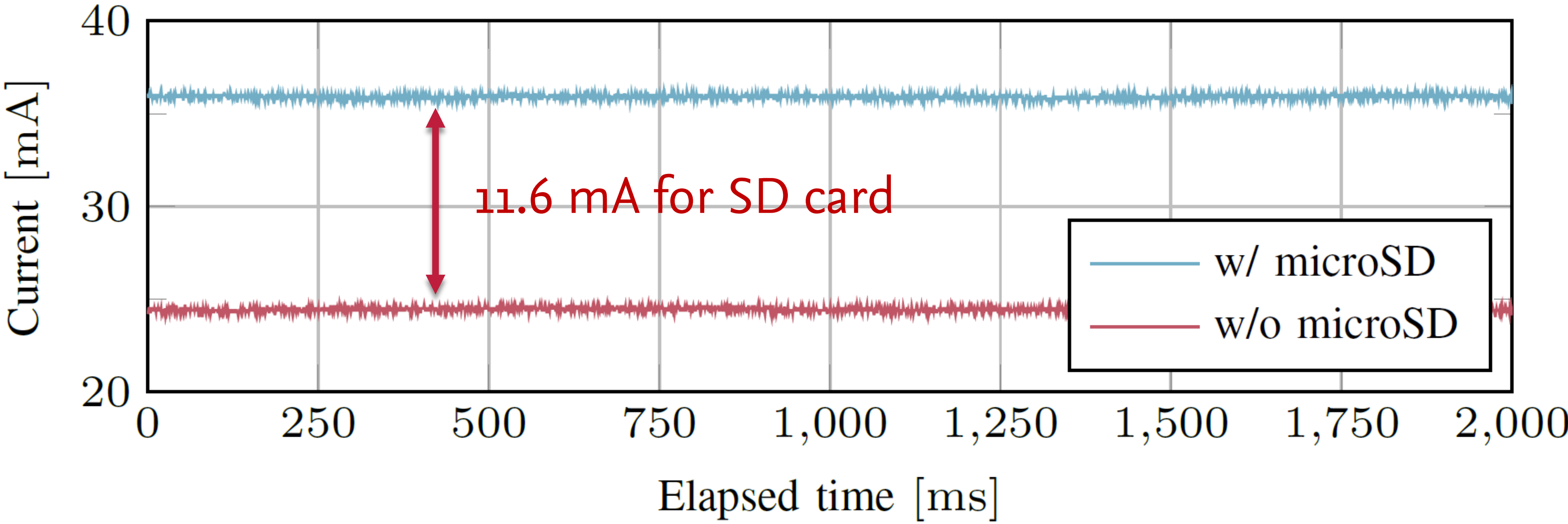


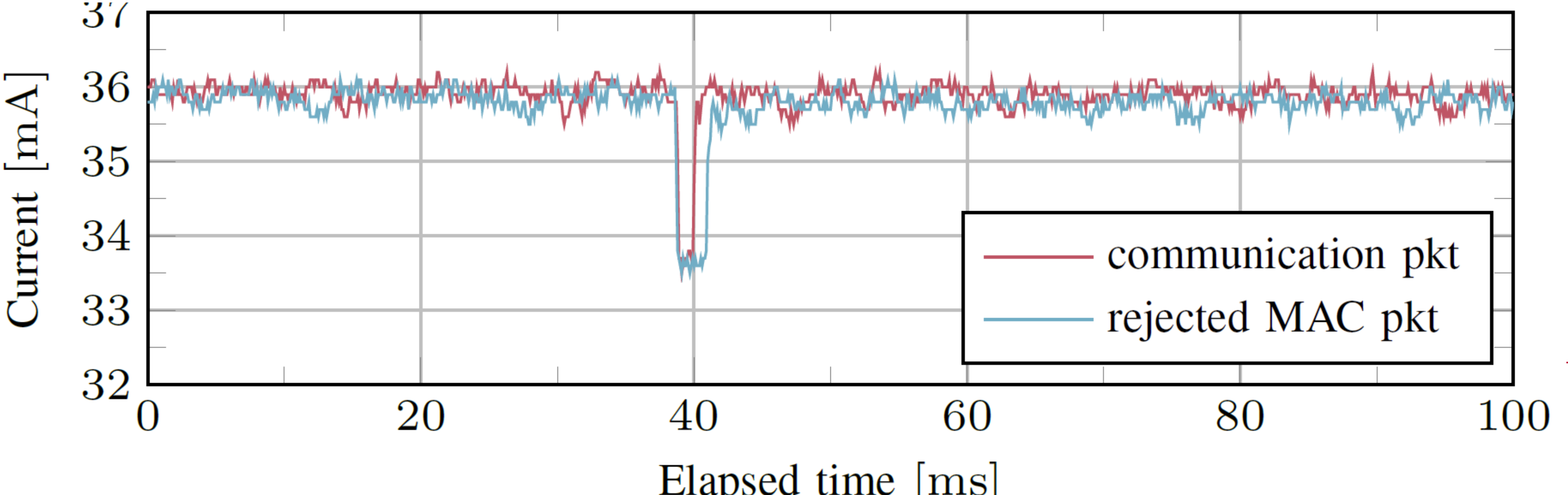
Measured throughput on physical motes



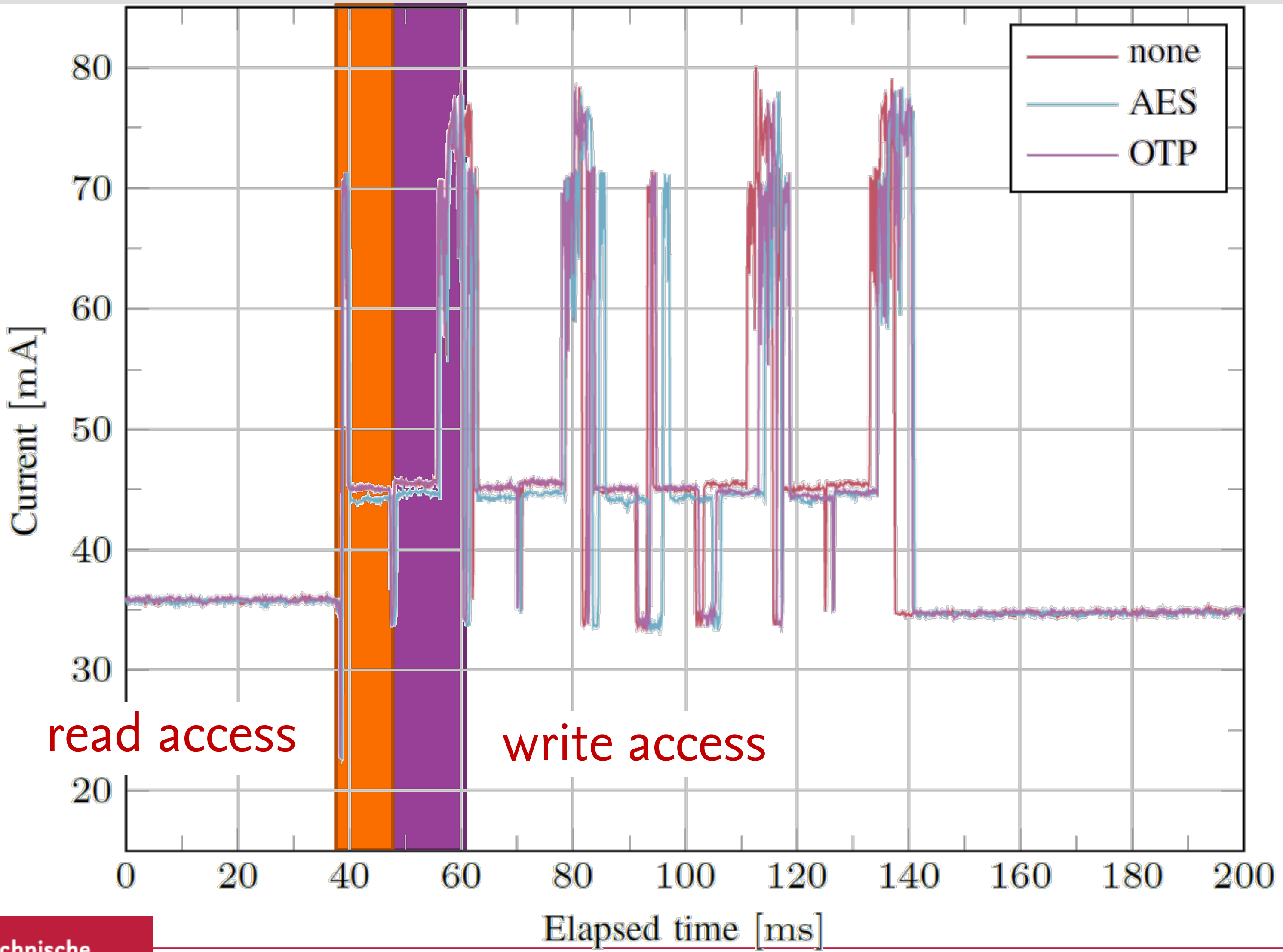
100 ms faster than simulations!

Energy Consumption





Energy Consumption



read access

write access

Summary

We combined

- Shamir’s Secret Sharing
- CBC-MAC
- AES / OTP

… to

- Distribute
- Authenticate
- Encrypt

… to ensure configurable

- Redundancy
- Privacy

Cover the whole bandwidth:

- Form full Redundancy to
- Full Confidentiality

RAIM is open soure

check it out at

https://www.ibr.cs.tu-bs.de/projects/raim

Thank you!

open source initiative