Networking the IoT with RIOT

Thomas C. Schmidt, Internet Technologies

t.schmidt@haw-hamburg.de

HAW Hamburg, Dept. Informatik

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Outline

- The Internet of Things
- The RIOT Operating System
- The RIOT Networking Subsystem
- Federated Authentication for the IoT
- The Case for Information-centric Networking?
- Conclusions & Outlook

The Internet of Things

"A system in which objects in the physical world can be connected to the Internet by sensors and actuators"

(coined 1999 by Kevin Ashton)

50 billion IoT devices expected by 2020!

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

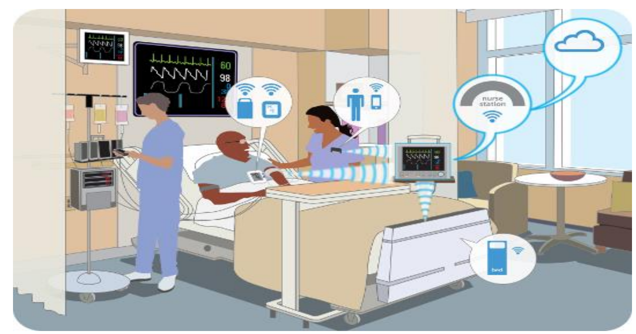
IoT Networking: Connecting the Physical World to the Internet

Micro- & Nano Satellites

Industrial Automation

Connected Vehicles

Smart Homes



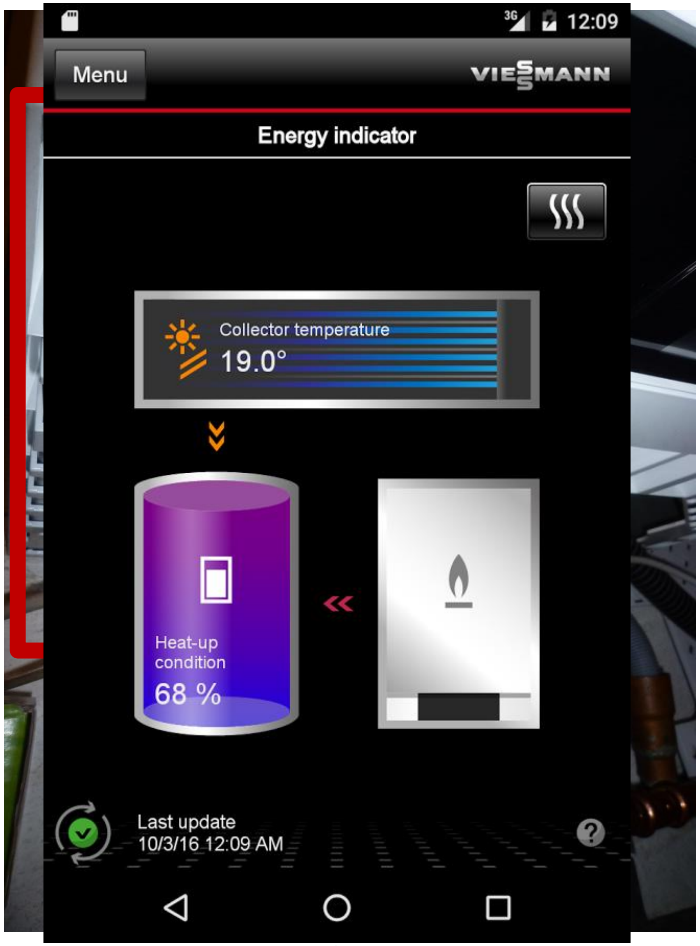
eHealth

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Use Case: Security in Harsh Industrial Environments

Smart DOM Hamburg

‚Smart‘ Heating



Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Evolution Towards an IoT

Distributed local intelligence		Wireless sensor network		Internet of Things ?
Embedded Controllers	+	**Wireless Networking**	+	**IPv4 Uplink to the Cloud**

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

This is not yet an Internet of Things!

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

No Internet without Open Speech and Open Standards

Layer	Standards
Application	XDI, CBOR, RDF, XHTML, JSON, Telnet, CoAP, HTTP, XMPP
Transport	UDP, TCP, TLS/SSL
Network	OSPF, RPL, DHCP, BGP, OLSR, IPv6, SLAAC, IPv4
Link	IEEE802.15.4, LoRa, BLE, Ethernet

Evolution towards an *Internet* oT

Distributed local intelligence		Wireless sensor network		Hype-Internet of Things
Embedded Controllers	+	**Wireless Networking**	+	**IPv4 Uplink to the Cloud**
+		+		+
Interoperable Information	+	**Distributed Security**	+	**Things loosely joined by IPv6**

The Real Internet of Things (C. Bormann)

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

The many faces of IoT

High-end IoT

Linux

android

Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

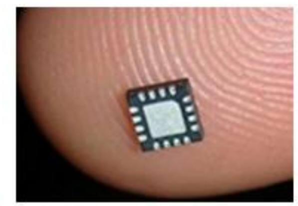
The many faces of IoT

High-end IoT

Linux ANDROID

Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Low-end (or constrained) IoT



RIOT

Processor: MHz, 8/16/32 Bit
Memory: kbytes
Energy: MWatt
Network access: 802.15.4, BLE

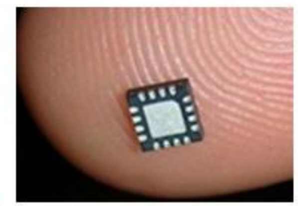
The many faces of IoT

High-end IoT

Linux

android

Low-end (or constrained) IoT

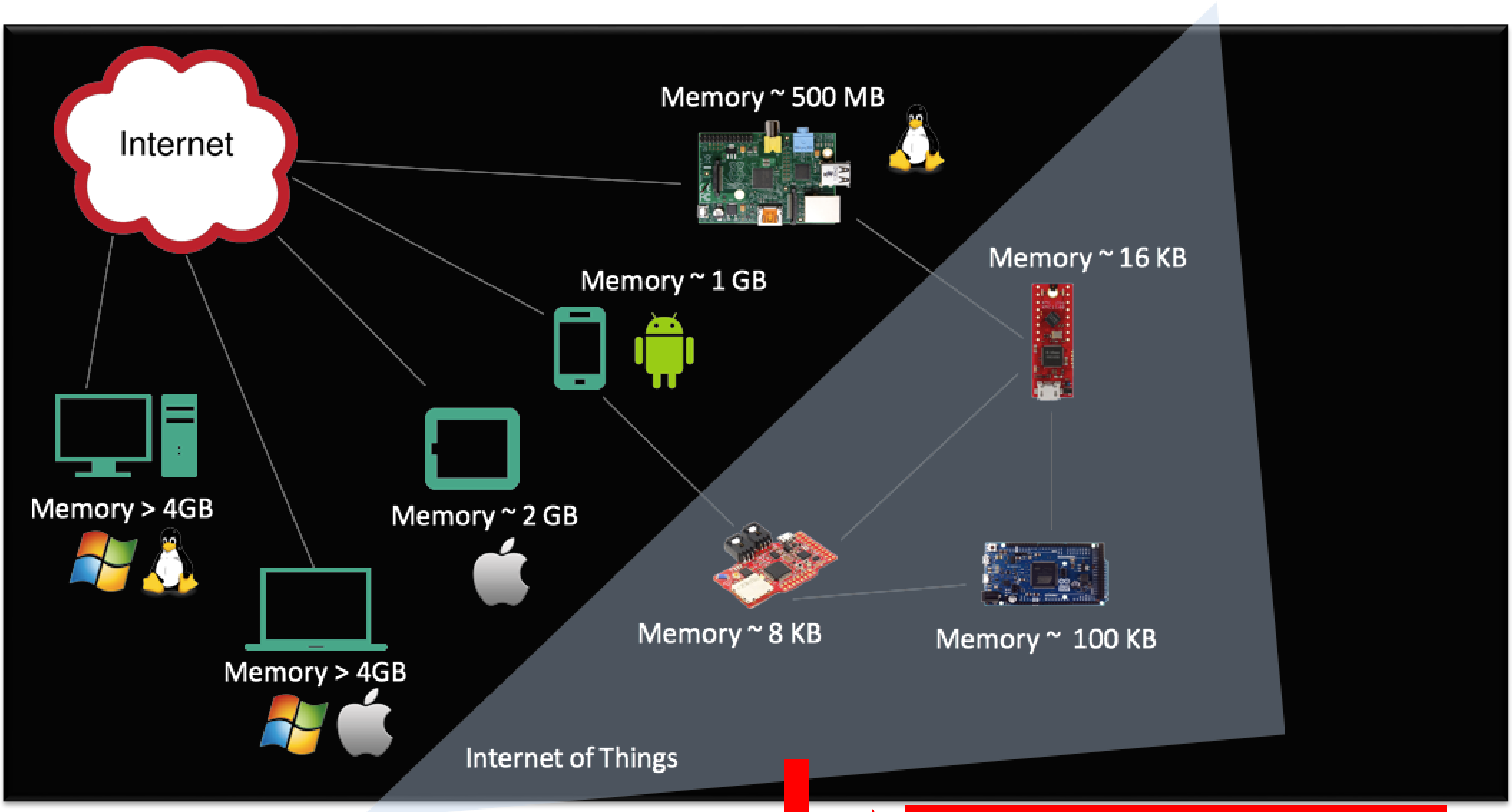


RIOT

Processor: GHz, 32/64 Bit
Memory: M/Gbytes
Energy: Watt
Network access: 5G, WLAN

Processor: MHz, 8/16/32 Bit
Memory: kbytes
Energy: MWatt
Network access: 802.15.4, BLE

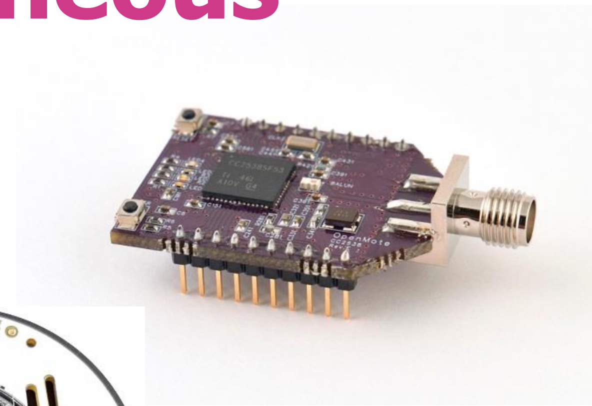
The Constrained Internet of Things (IoT)



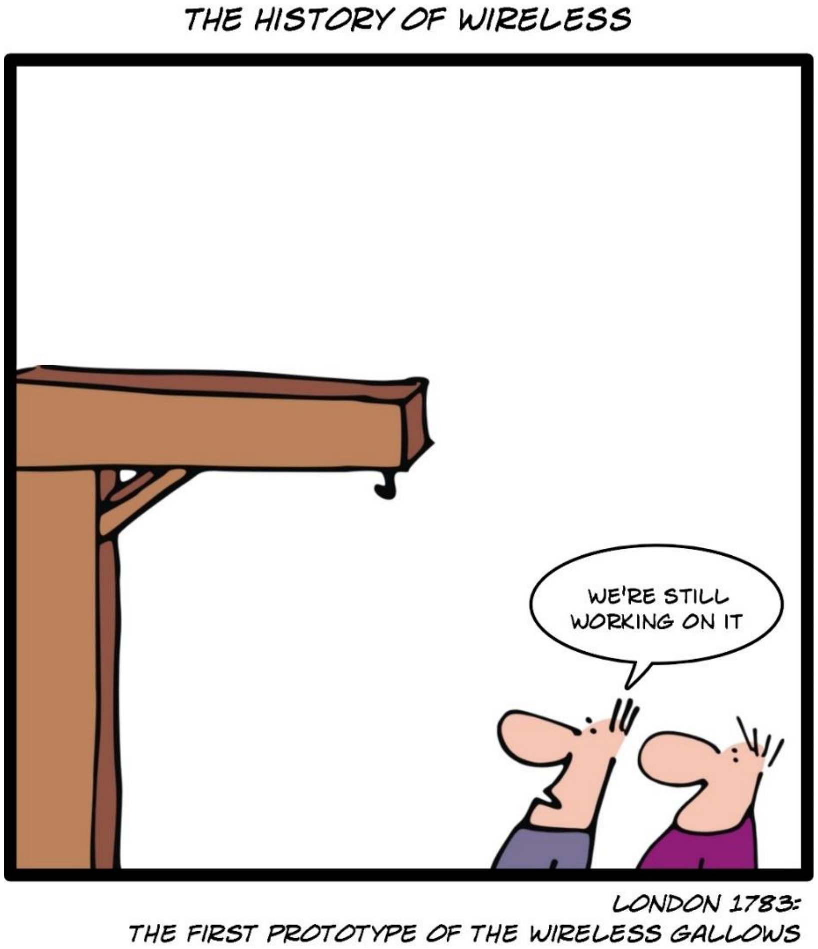
Constrained + Wireless!

The IoT is Very Heterogeneous

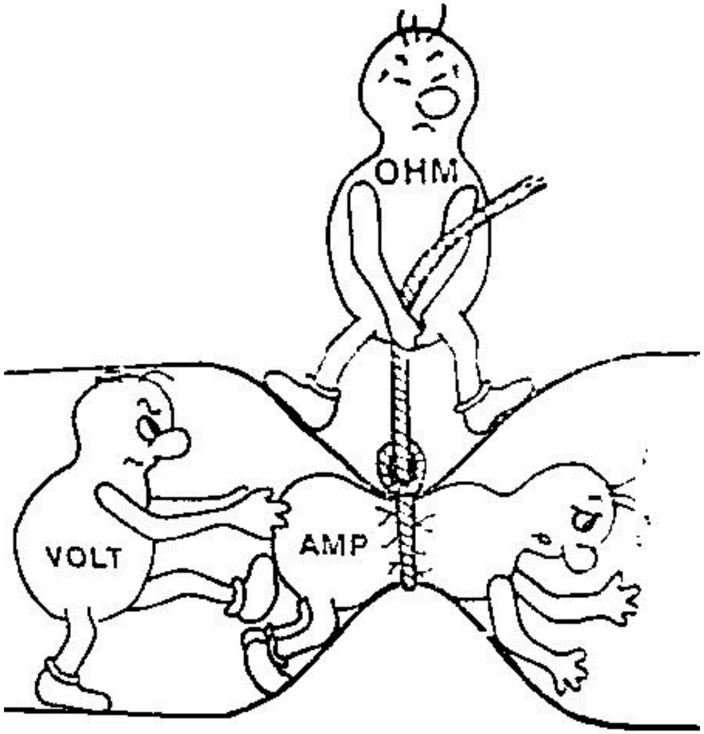
- o Various boards
- o A zoo of components
- o Broad range of radios
- o Different Link-layers
- o Competing network layers
- o Diverging interests and technologies
- o A lot of experimentation …



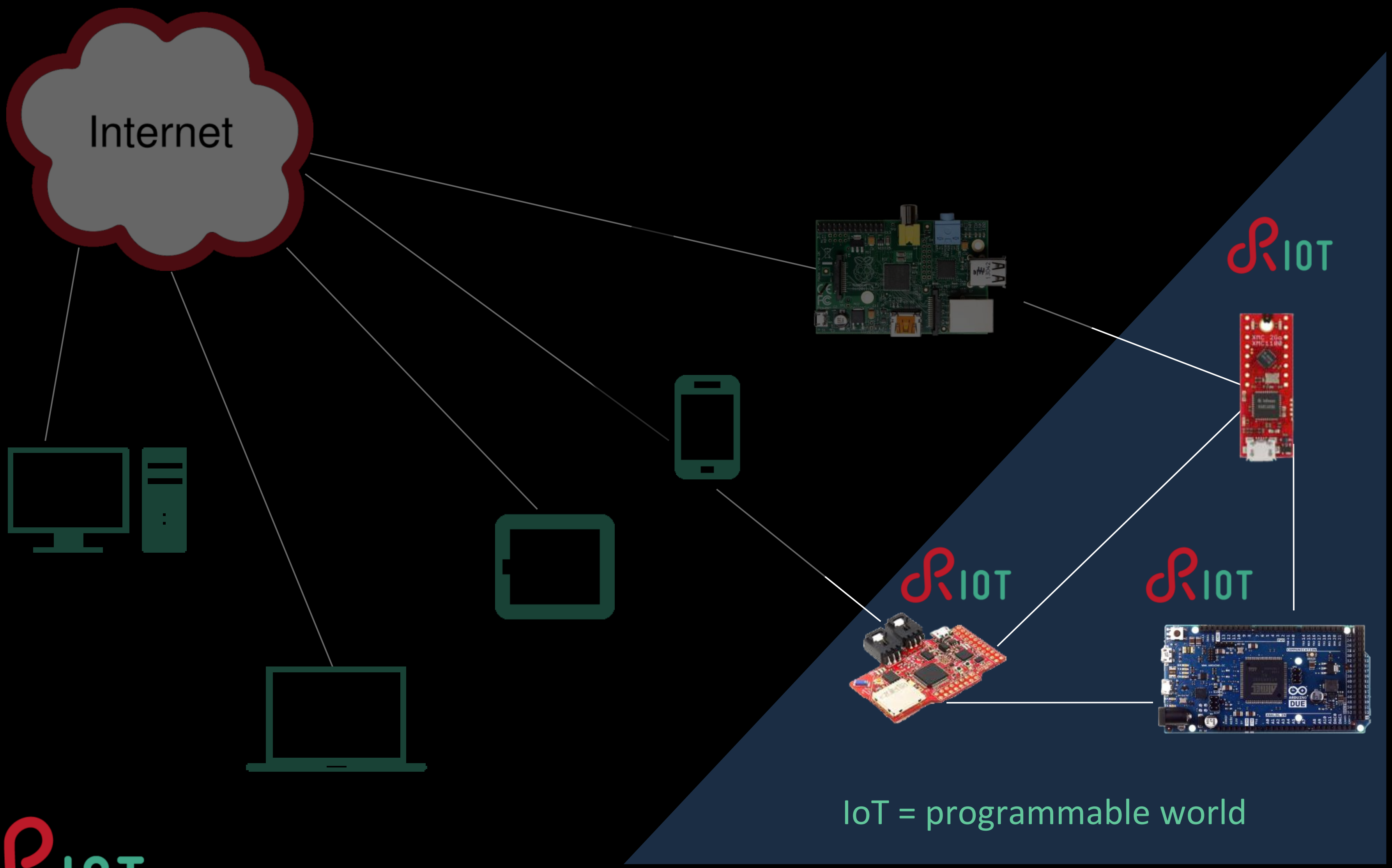
Low power lossy wireless



Key problem: Energy



RIOT: The Friendly OS for the IoT



If your IoT device cannot run Linux, then run

RIOT: Facts sheet

- Microkernel architecture (for robustness)
  - The kernel itself uses ~1.5K RAM @ 32-bit
- Efficient hardware abstraction
- Tickless scheduler (for energy efficiency)
- Deterministic O(1) scheduling (for real-time)
- Low latency interrupt handling (for reactivity)
- Modular structure (for adaptivity)
- Preemptive multi-threading & powerful IPC
- Appealing API

RIOT Origins

History

- 2008 – Project roots:
  The kernel was started
  as part of the FireWhere project
- 2010 – Towards the IoT:
  Implementation of 6LoWPAN
  and RPL was initiated (GLAB)
- 2013 – RIOT goes public:
  Branding of RIOT as part of the
  SAFEST project, source code
  moved to GitHub

Founding institutions

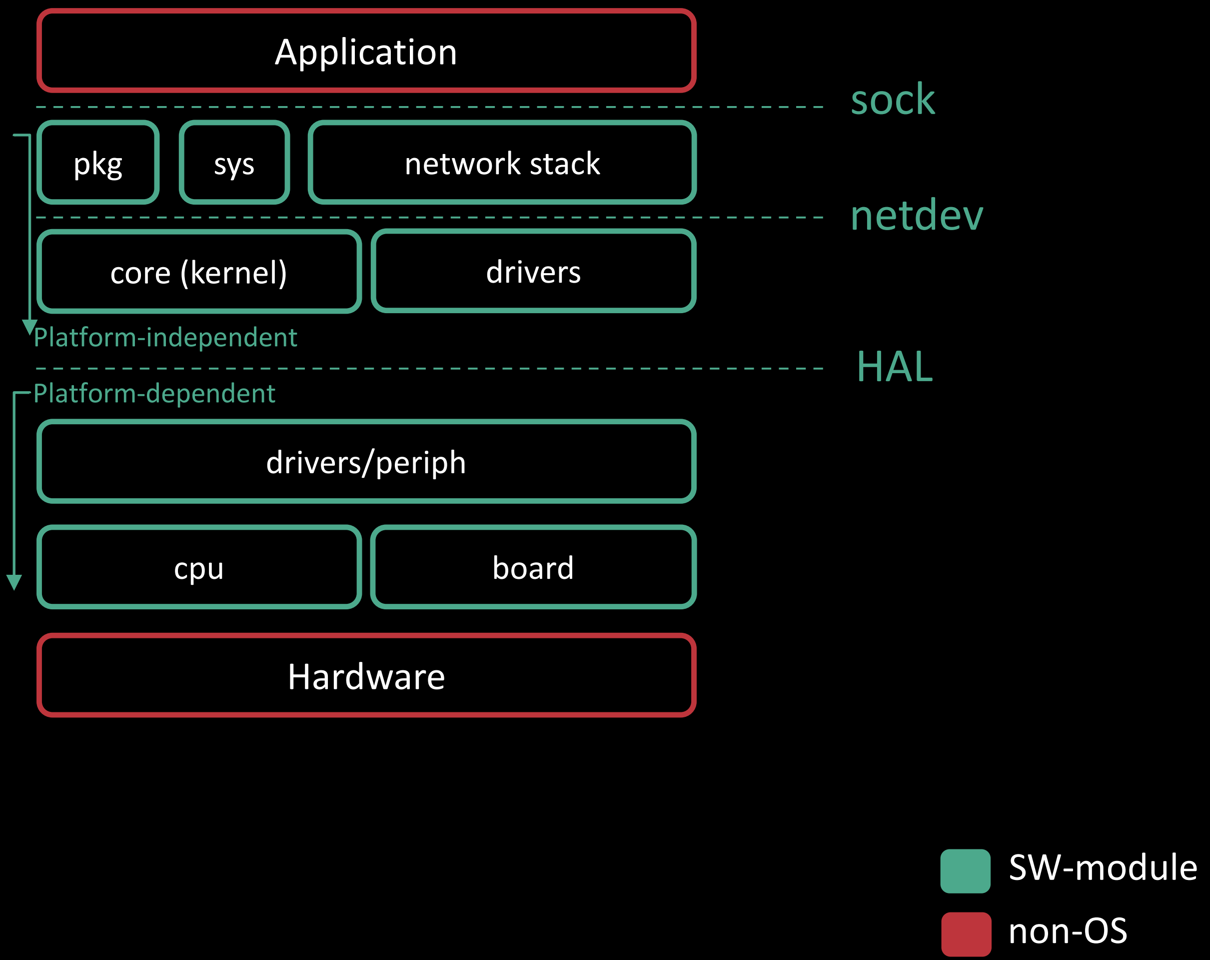
Freie Universität Berlin

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

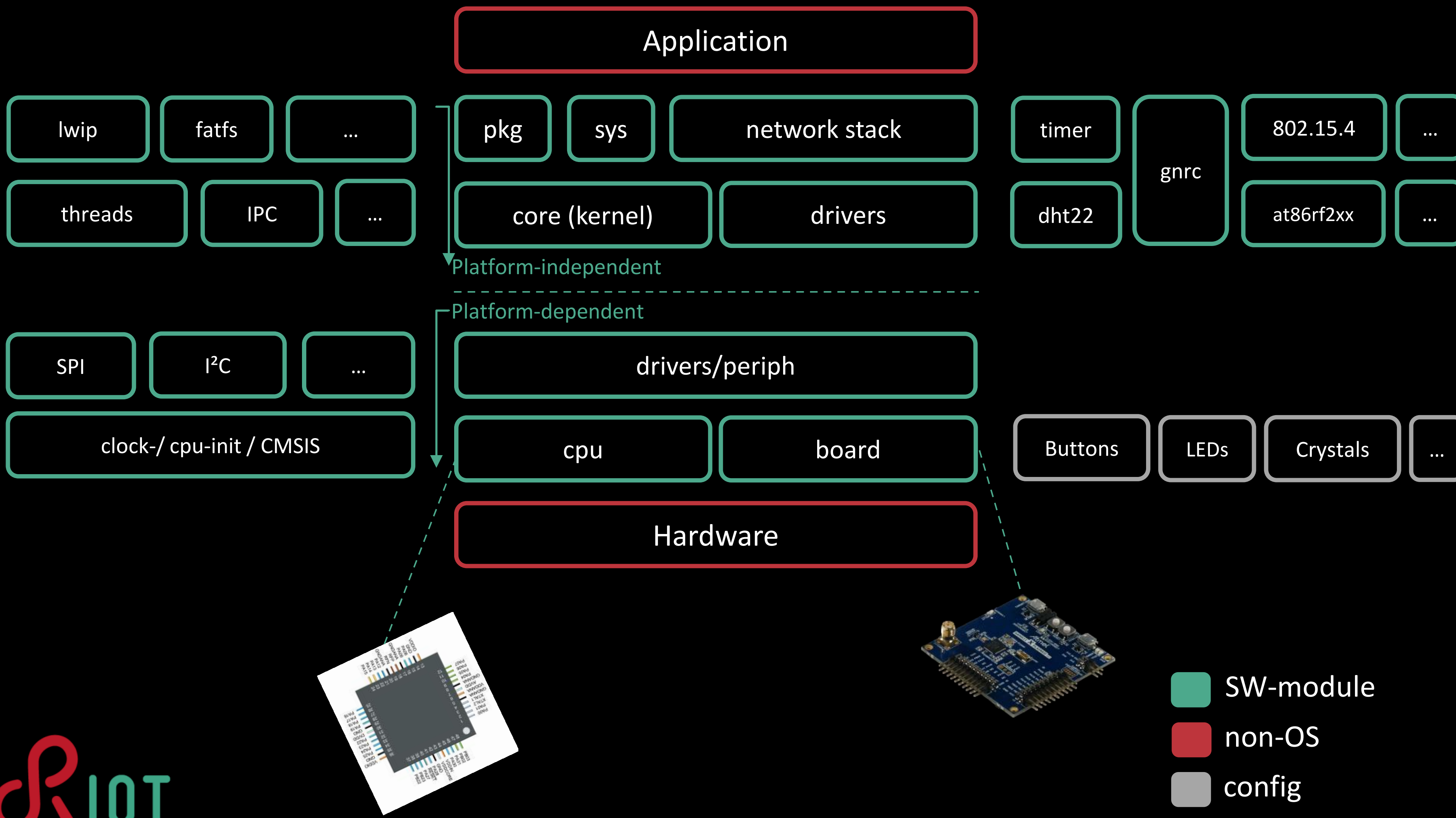
Inria
INVENTORS FOR THE DIGITAL WORLD

RIOT

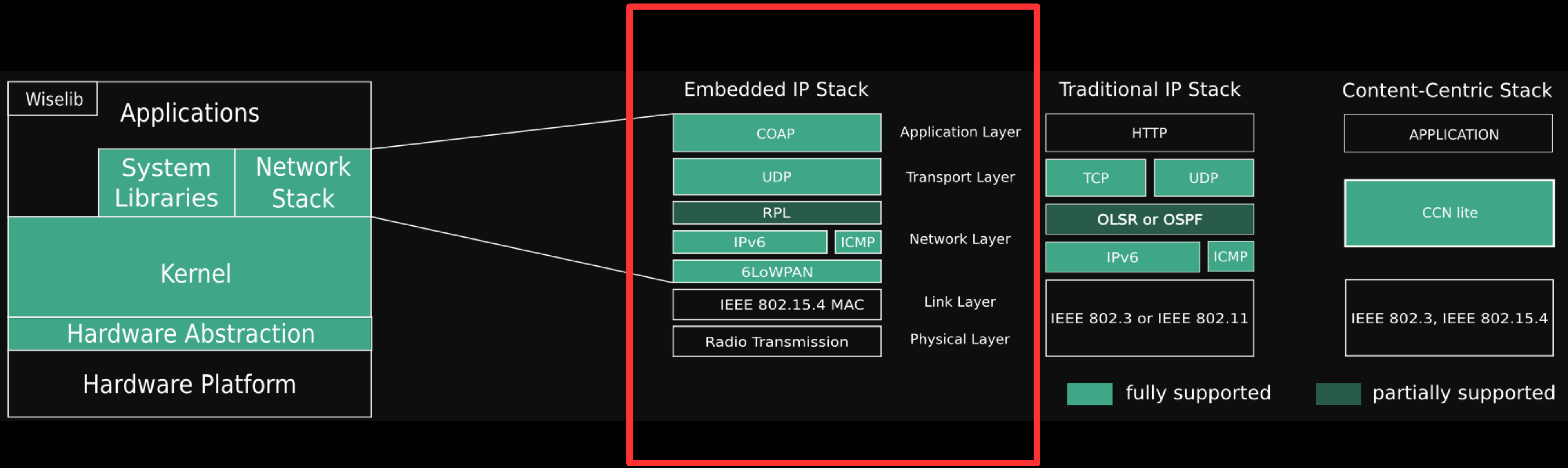
RIOT Software Components



RIOT Software Components (2)



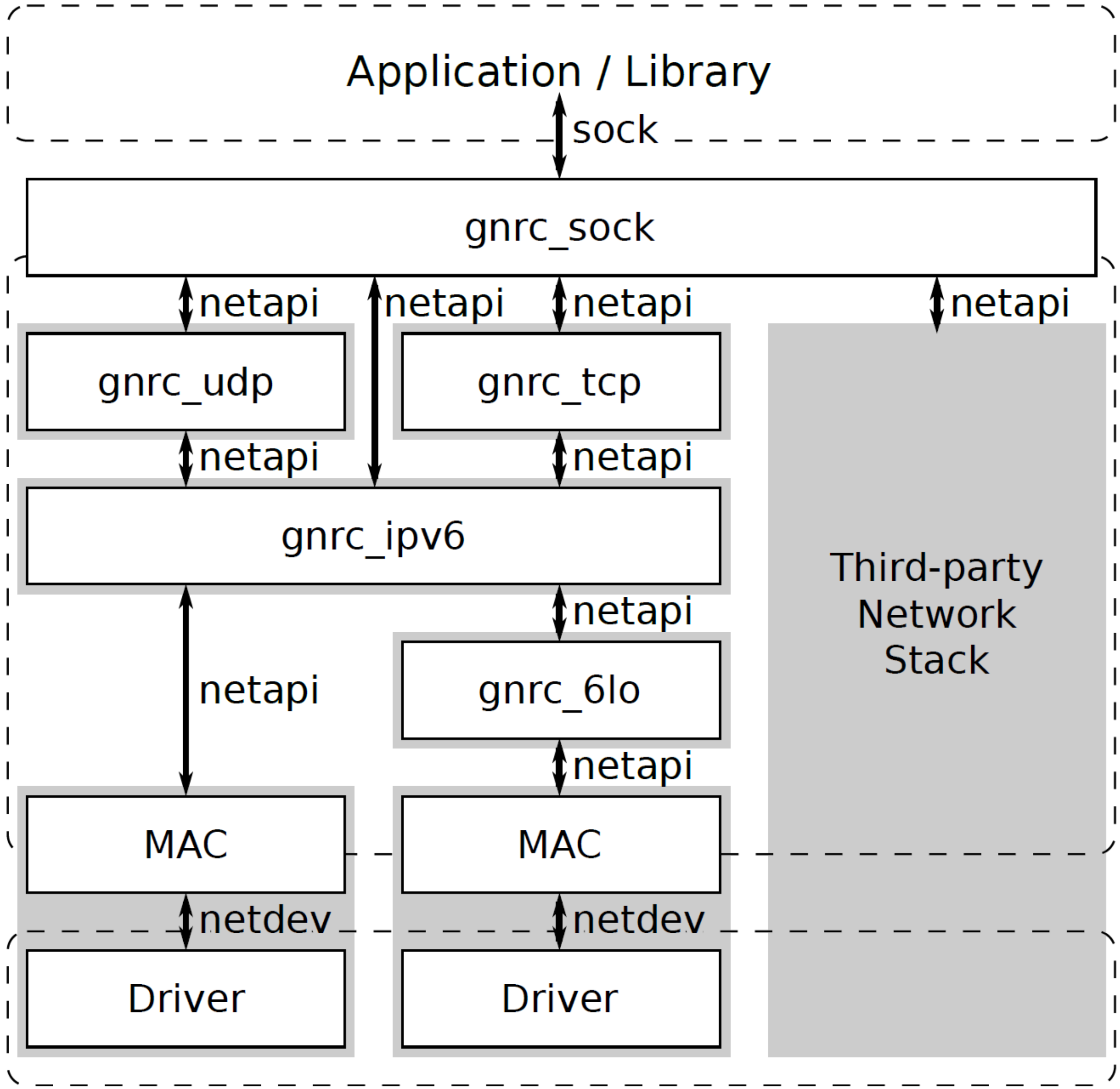
RIOT: Built to connect



- Open-access protocols
  - e.g. 6LoWPAN, IPv6, CoAP, ...
- RIOT supports several network stacks
- On many wireless technologies and NICs

RIOT Network Architec-ture:

A Closer Look



API Design (netdev, netapi)

- o Transmission
  - Asynchronous **`send/recv`**
- o Configuration and Initialization
  - Functions **`get/set`** for options defined in a global key-value store: **`netopt`**
- o Event Handling
  - Signaling related to the categories RX, TX, link, or system
  - Provides external event callback to break out of ISR

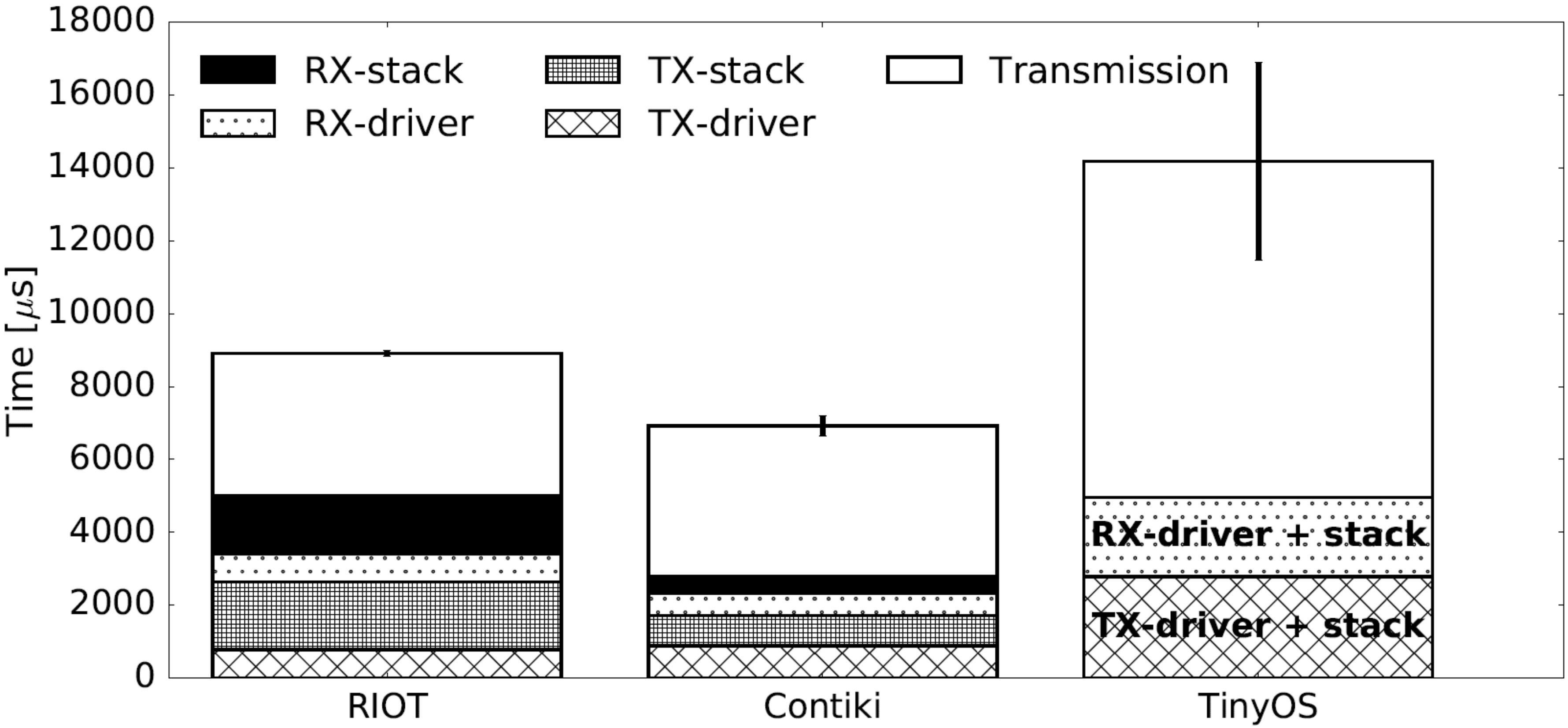
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Supported Components

- Full Stacks
  - GNRC
  - LwIP
  - emb6
  - OpenWSN
  - CCN-Lite
  - NDN-RIOT
  - LoRA-WAN
  - (Nimbel BLE)
- Network Access
  - 802.15.4 (various radios)
  - 802.15.4 CSMA
  - 802.15.4 TSCH
  - 802.3 Ethernet
  - LoRA
  - (BLE)

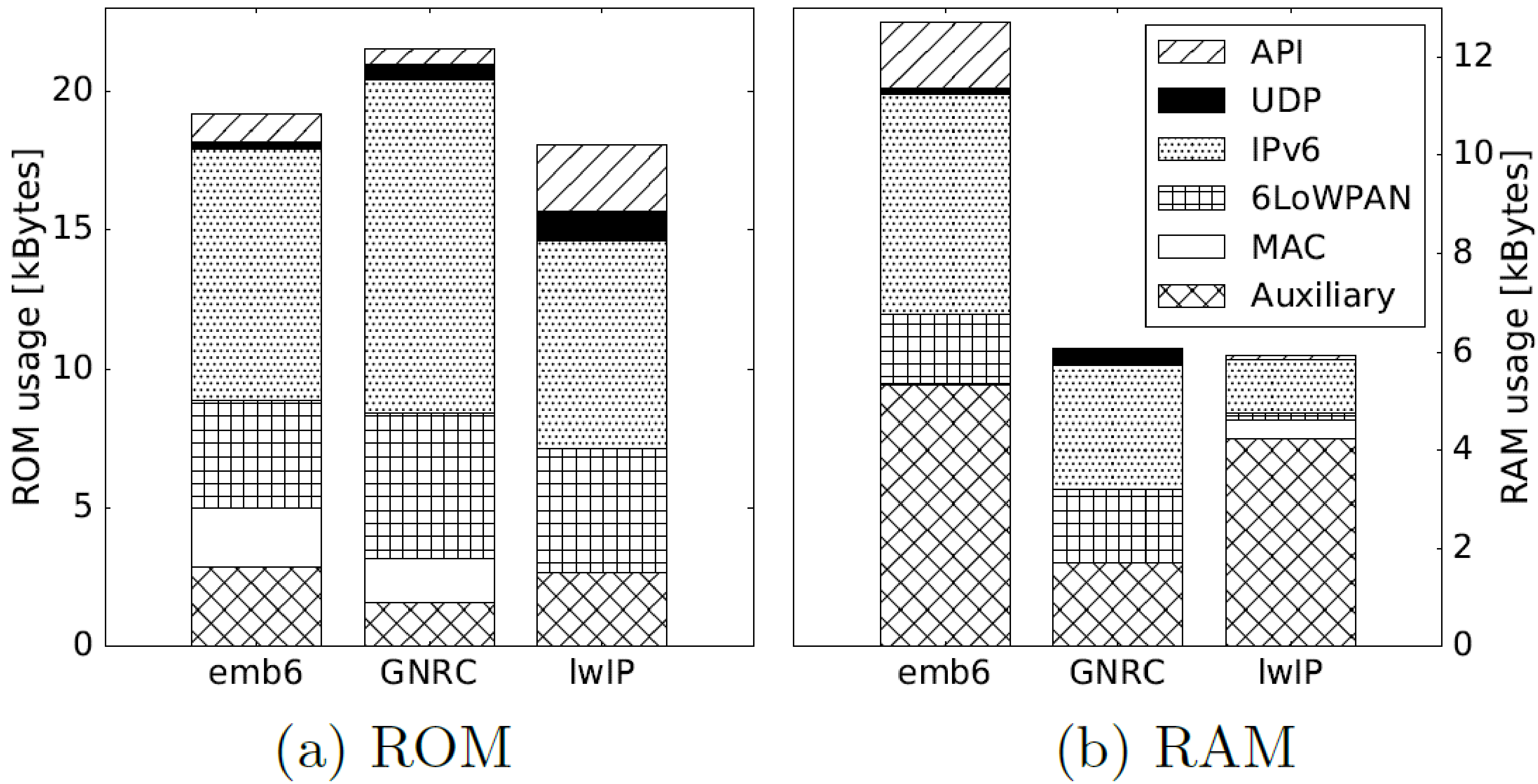
Performance of a Fully Layered Stack?

Transmitting a UDP Packet



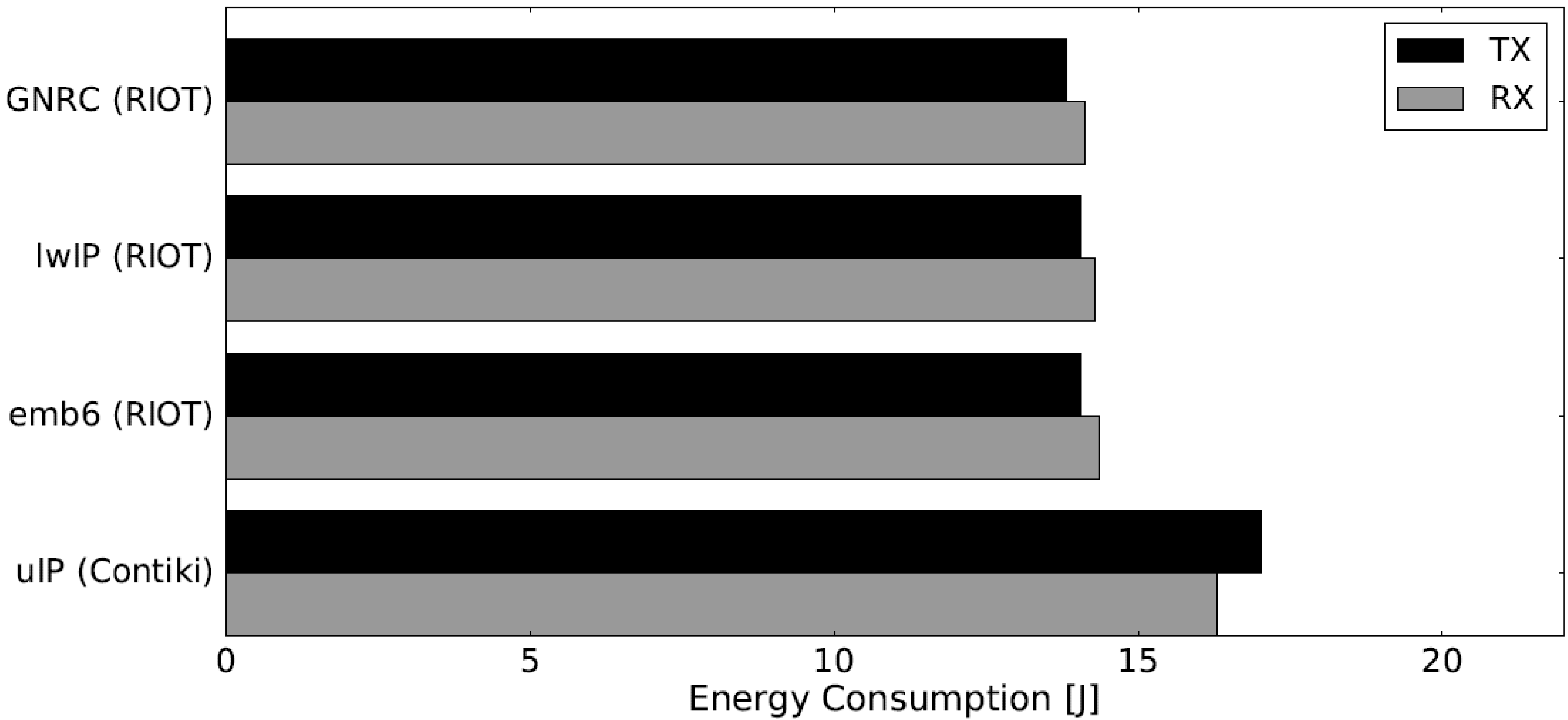
msp430 16-bit MCU, 16 MHz, 92 KB Flash, 8 KB RAM, on-board 2,4 GHz 802.15.4 radio

Memory

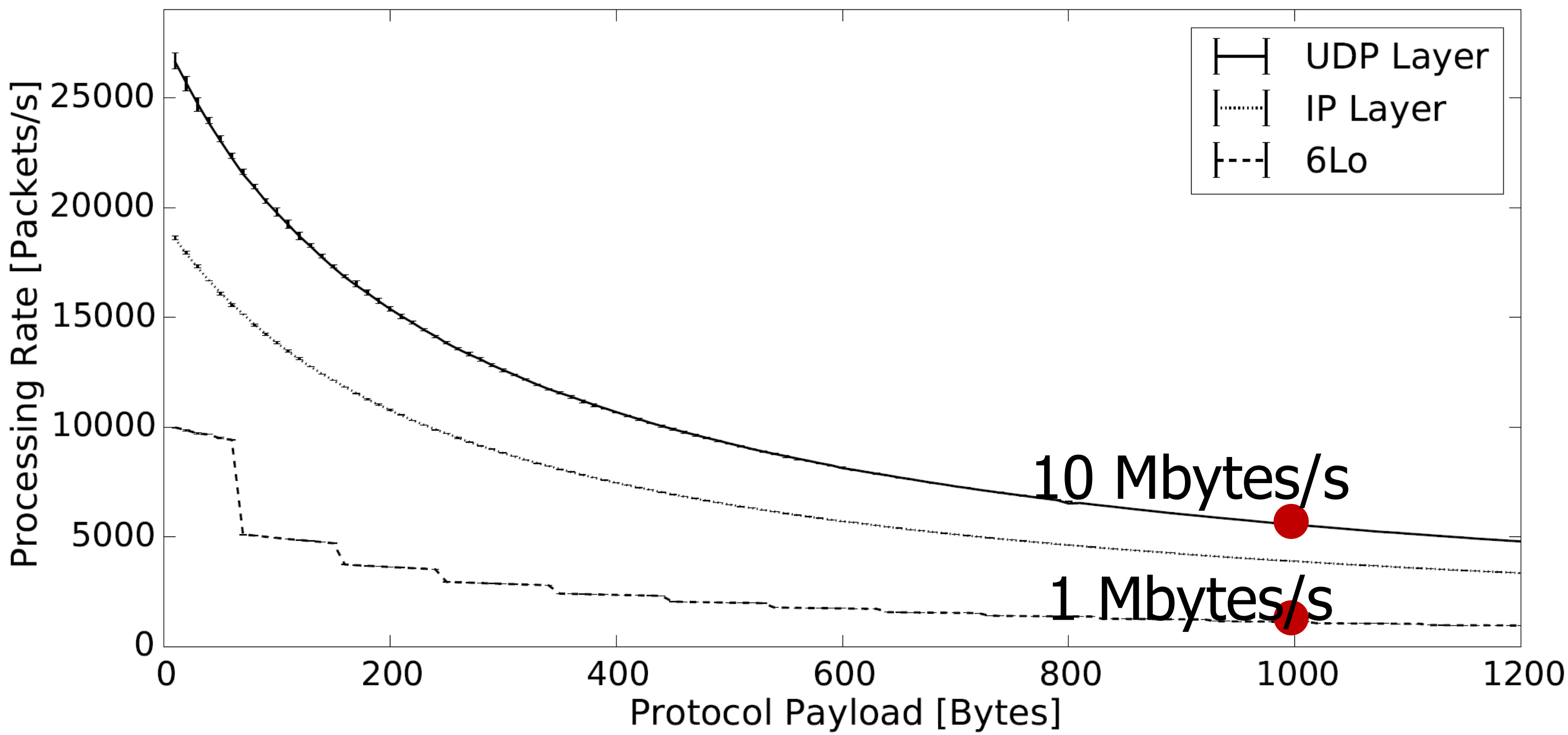


ROM usage [kBytes]
0
5
10
15
20
emb6
GNRC
lwIP
(a) ROM
API
UDP
IPv6
6LoWPAN
MAC
Auxiliary
RAM usage [kBytes]
0
2
4
6
8
10
12
emb6
GNRC
lwIP
(b) RAM

Energy

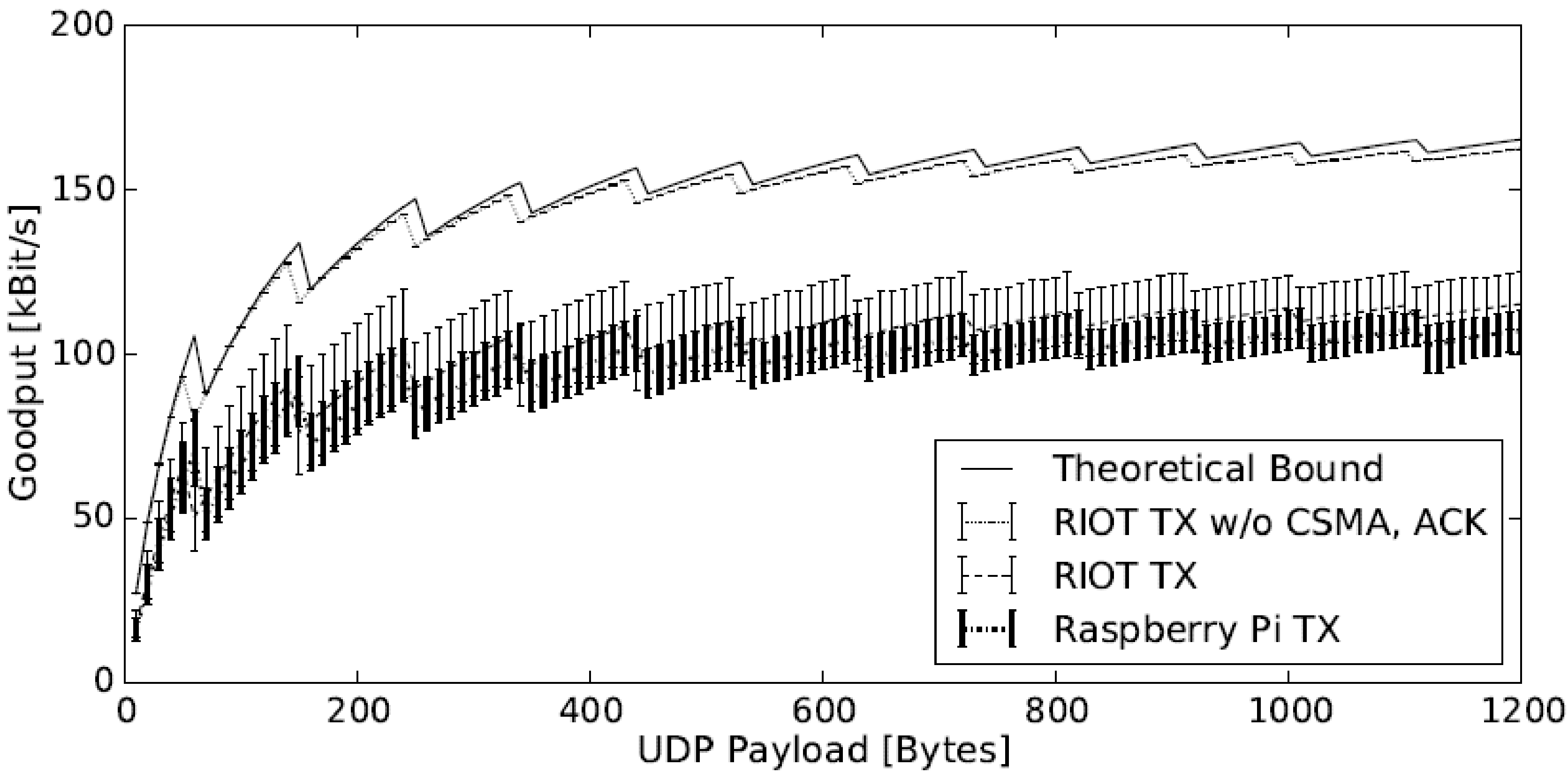

GNRC (RIOT)
lwIP (RIOT)
emb6 (RIOT)
uIP (Contiki)
TX
RX
0
5
10
15
20
Energy Consumption [J]

RIOT Network Stack: Packet Processing Rates

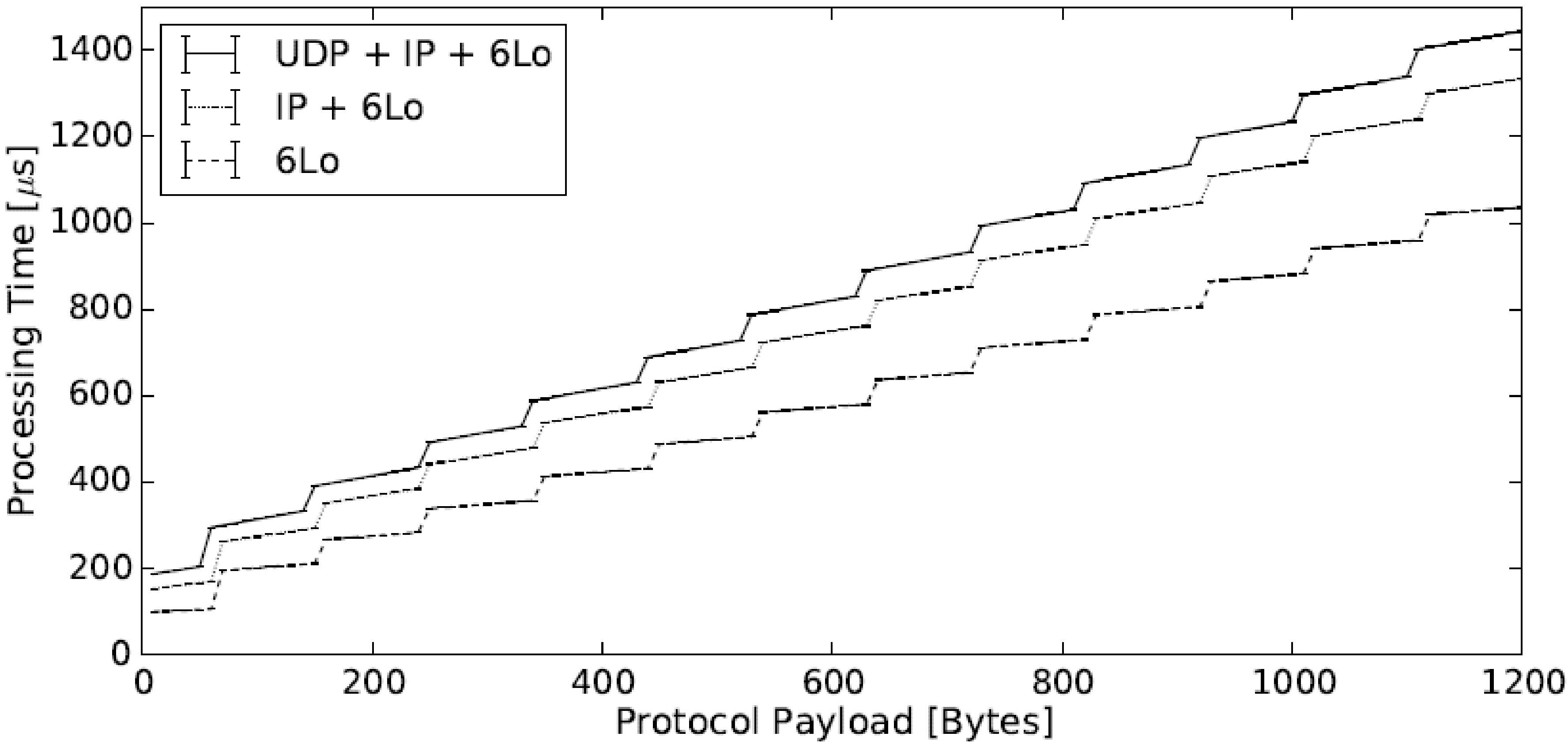


Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

IoT Stacks in the Wild: RIOT versus RasPi



Processing Time per Layer



Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Outline

- The Internet of Things
- The RIOT Operating System
- The RIOT Networking Subsystem
- Federated Authentication for the IoT
- The Case for Information-centric Networking?
- Conclusions & Outlook

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

The IoT Authentication Problem

- IoT systems may rely on peerwise verifiable identities
- Current standards (DTLS) leave authentication open
- Huge numbers and heterogeneous deployment hinder central trust hierarchy – TLS analogy is traditional PKI
- Autonomous local configuration and federated trust management preferred
- Constrained environments urge for minimal overhead
- Trust anchors may (should) be outside the loop

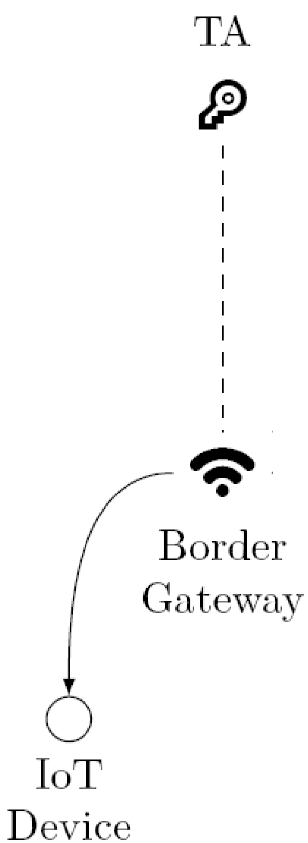
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

IoT End-to-End Authentication

Infrastructure-centric approach for DTLS:

- o Identity-based crypto IPs authenticate IoT nodes without individual public keys
- o Twisted Edwards ECC enables IBC on constrained nodes
- o Federation between subnets - bound to local trust

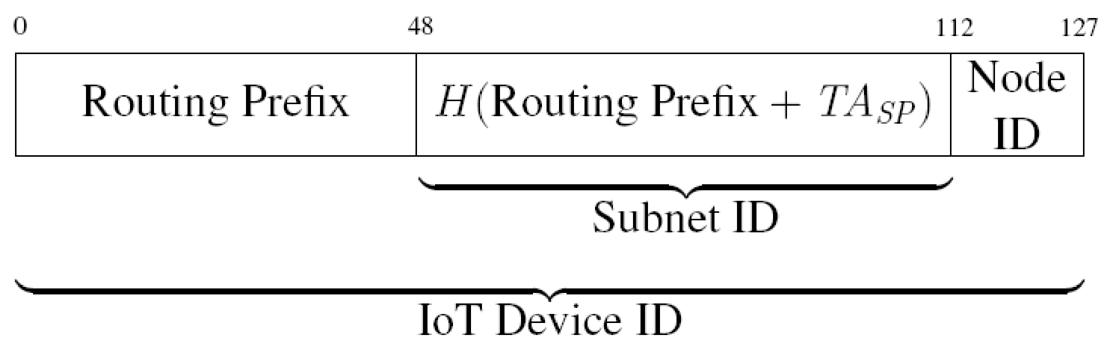
Local Approach



- o Bootstrap: either offline or
  1. TA pre-initializes Gateway with Identity credentials – then can go offline
     Alternative: TA locally protected configurator
  2. Gateway (or TA) performs host configuration by authenticated encryption using symmetric cypher (AEAD)
  3. Gateway distributes TA*PK*
- o Authentication Process:
  - Peerwise end-to-end using IBC signatures

Federated Approach

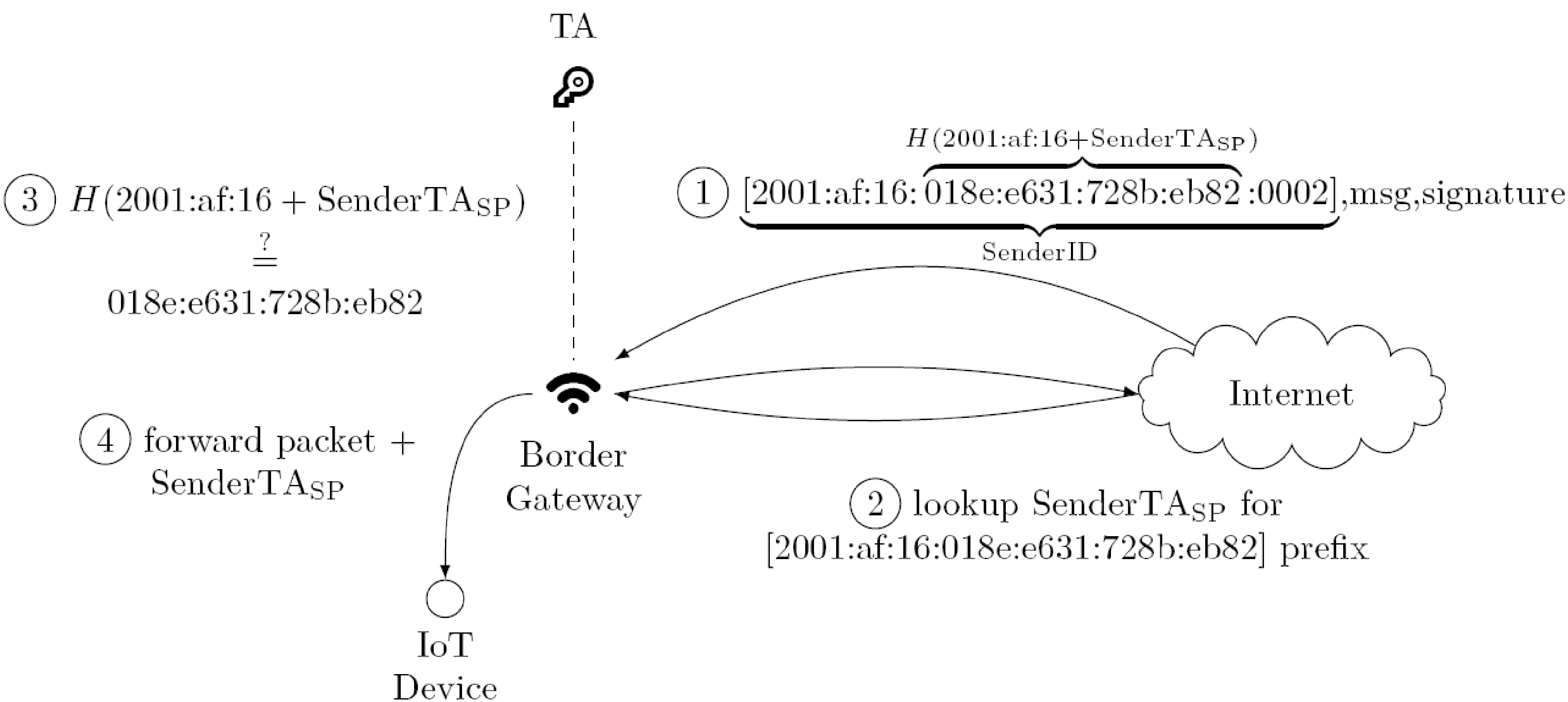
- Problem: Requires local trust anchor
- Solution: Subnet-local Trusted Authorities (TAs) with Cryptographic Subnet IDs



- Federated Public Key Exchange
- Gateway-assisted End-to-end Authentication
- Key Revocation by renumbering

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

GW-assisted Authentication Process

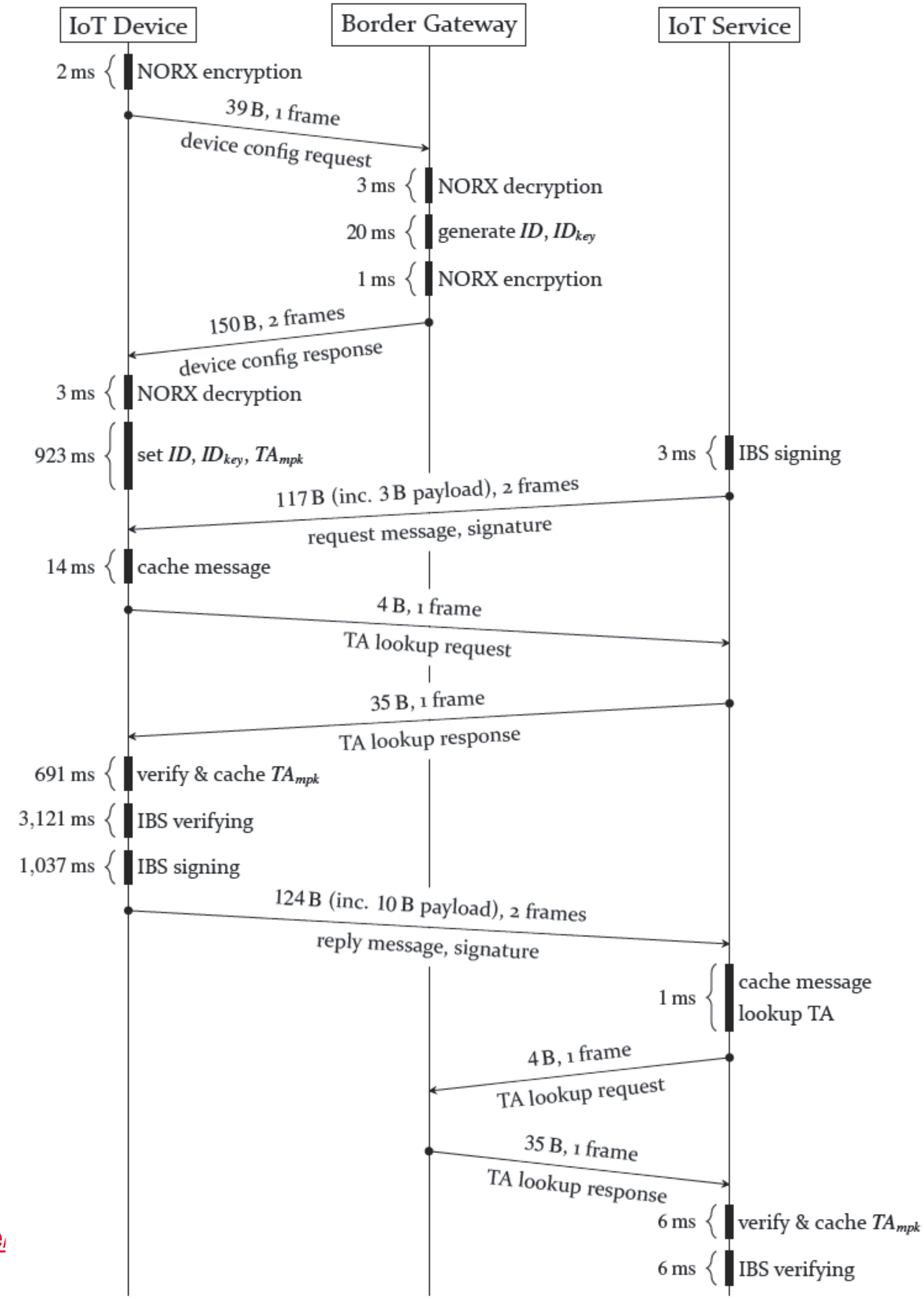


Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Protocol Evaluation

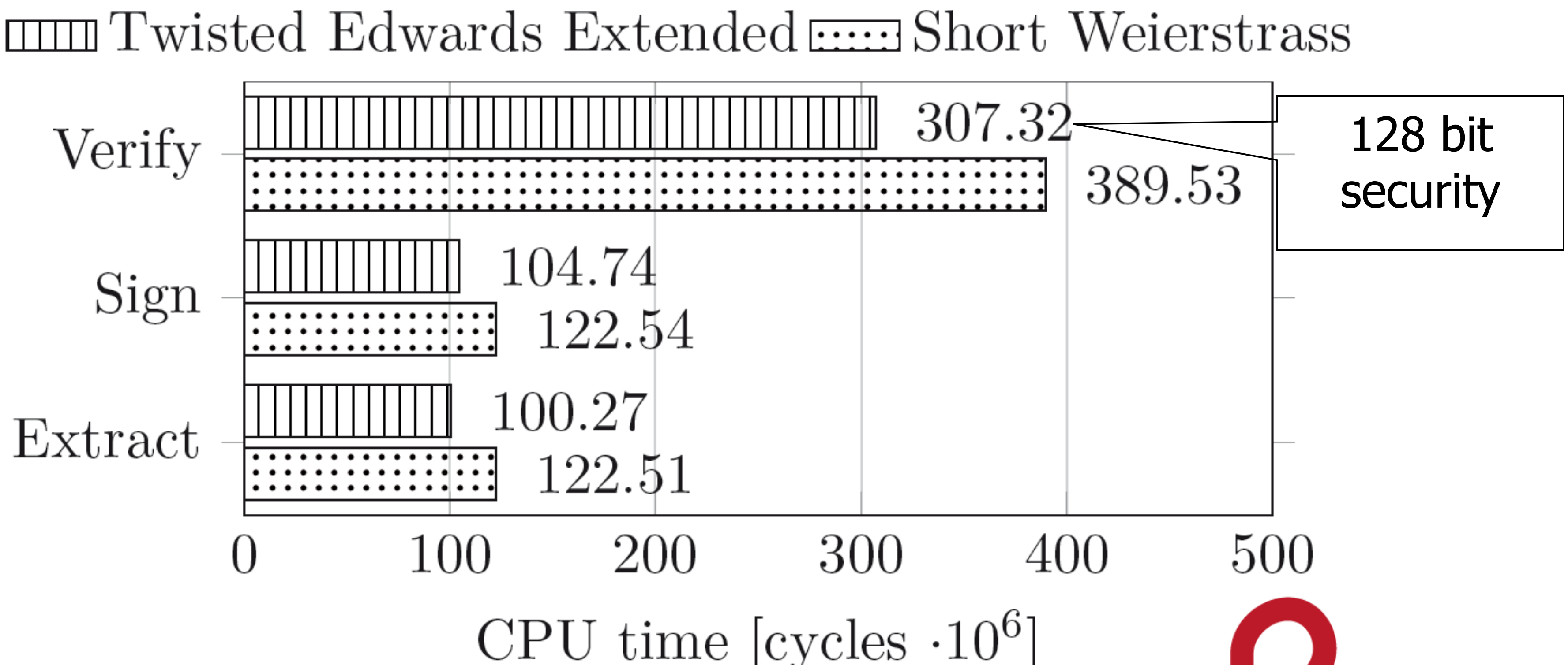
Scenario:

- o IoT node: SAM R21 from FIT IoT Lab running RIOT
- o Gateway: Rasberry PI



Evaluation: Crypto Load

- Load reduction by Edwards Curve25519



- Contribution to the Relic Library on

Outline

- The Internet of Things
- The RIOT Operating System
- The RIOT Networking Subsystem
- Federated Authentication for the IoT
- The Case for Information-centric Networking?
- Conclusions & Outlook

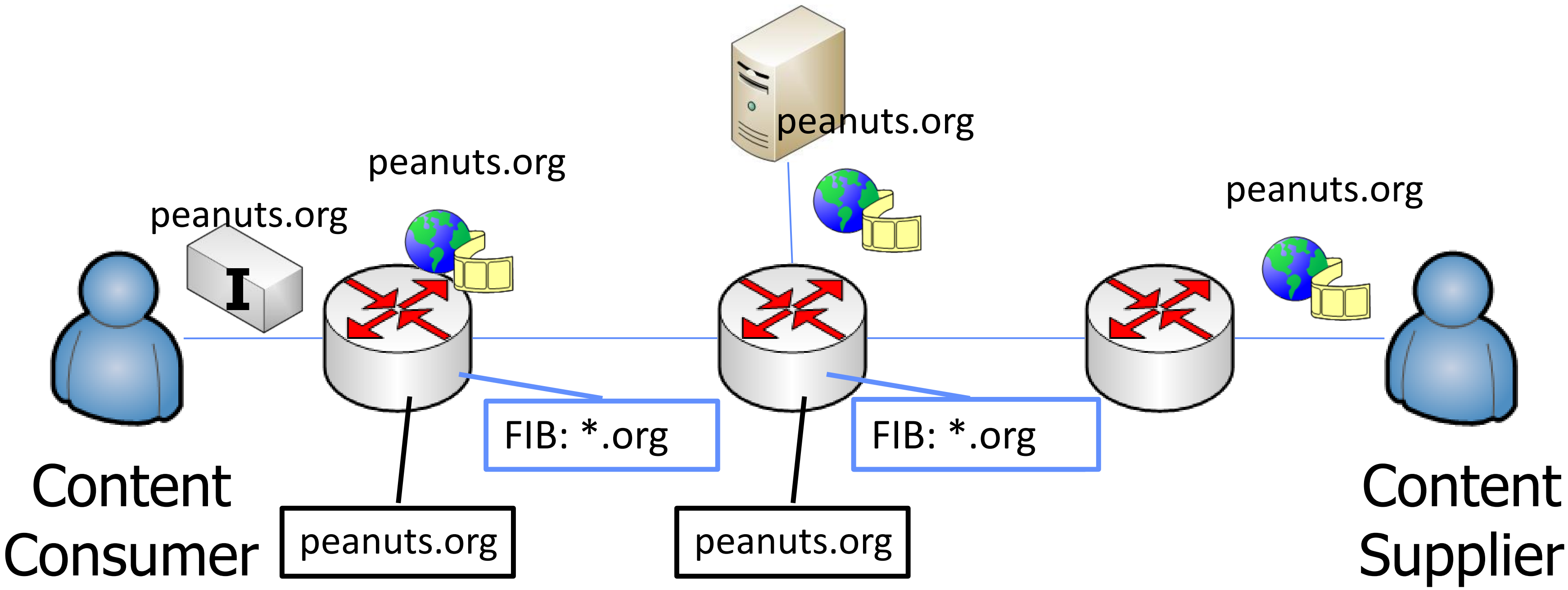
Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Information-centric Networking

Idea:

- o Access content – not nodes – in a request/response paradigm
  - Address content directly by name
  - Augment content with (self-)authentication
  - Ubiquitous in-network storage (caching)
- o Various approaches
  - Seminal: TRIAD (Gritter & Cheriton 2001)
  - Most popular: NDN (Van Jacobson et al. 2009)

Basics: Content Centric Routing

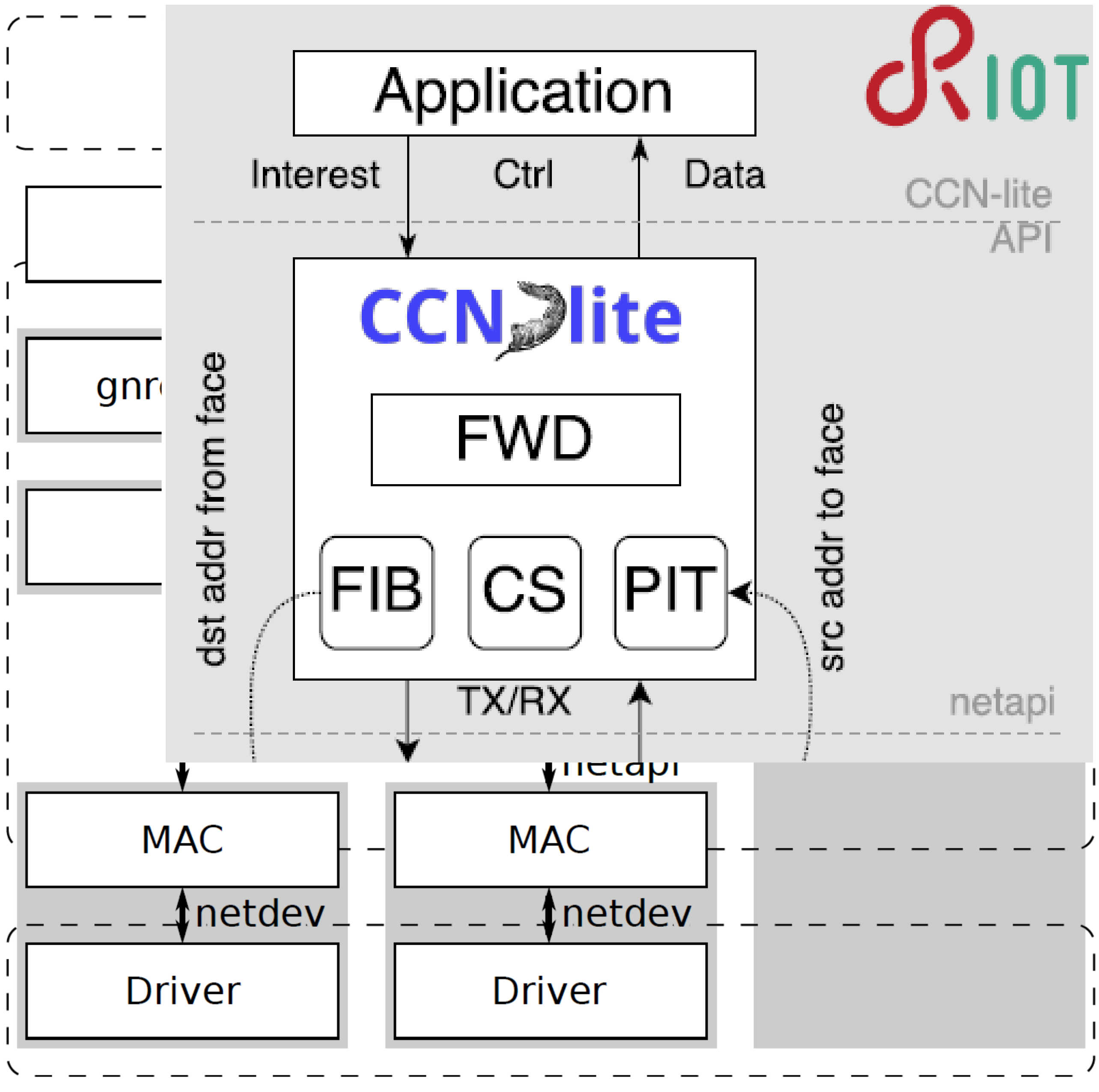


- Observation 1: In-network states driven by data
- Observation 2: End-users affect backbone states

Opportunities with ICN for IoT

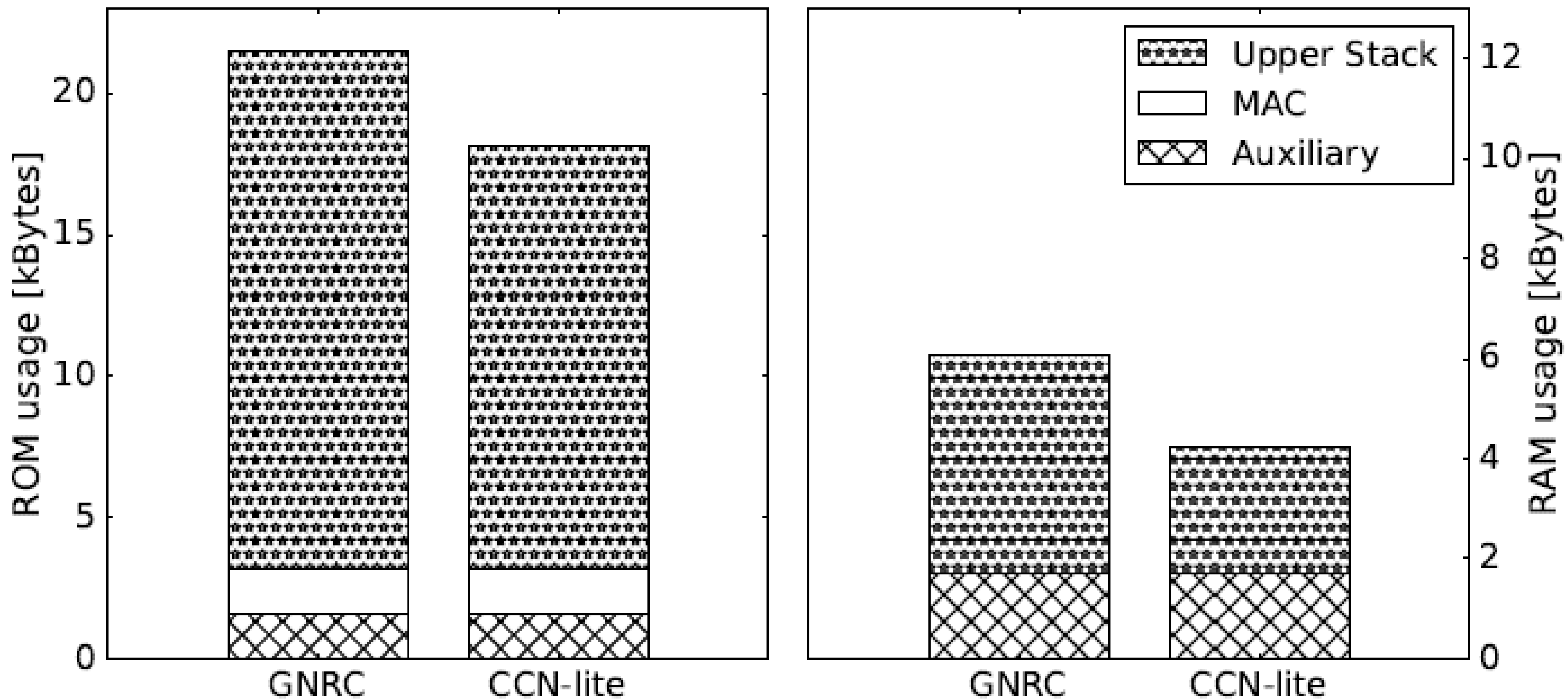
- Resilience
  - Hop-by-hop traversal with in-network caching
- Mobility
  - Seamless support for mobile consumers
- Security
  - DoS difficult: No unwanted data
- Network management
  - Easy deployment and auto-configuration
- Network caches
  - May reduce latency for multiple services
  - Fixed deputies may preserve energy

ICN in RIOT



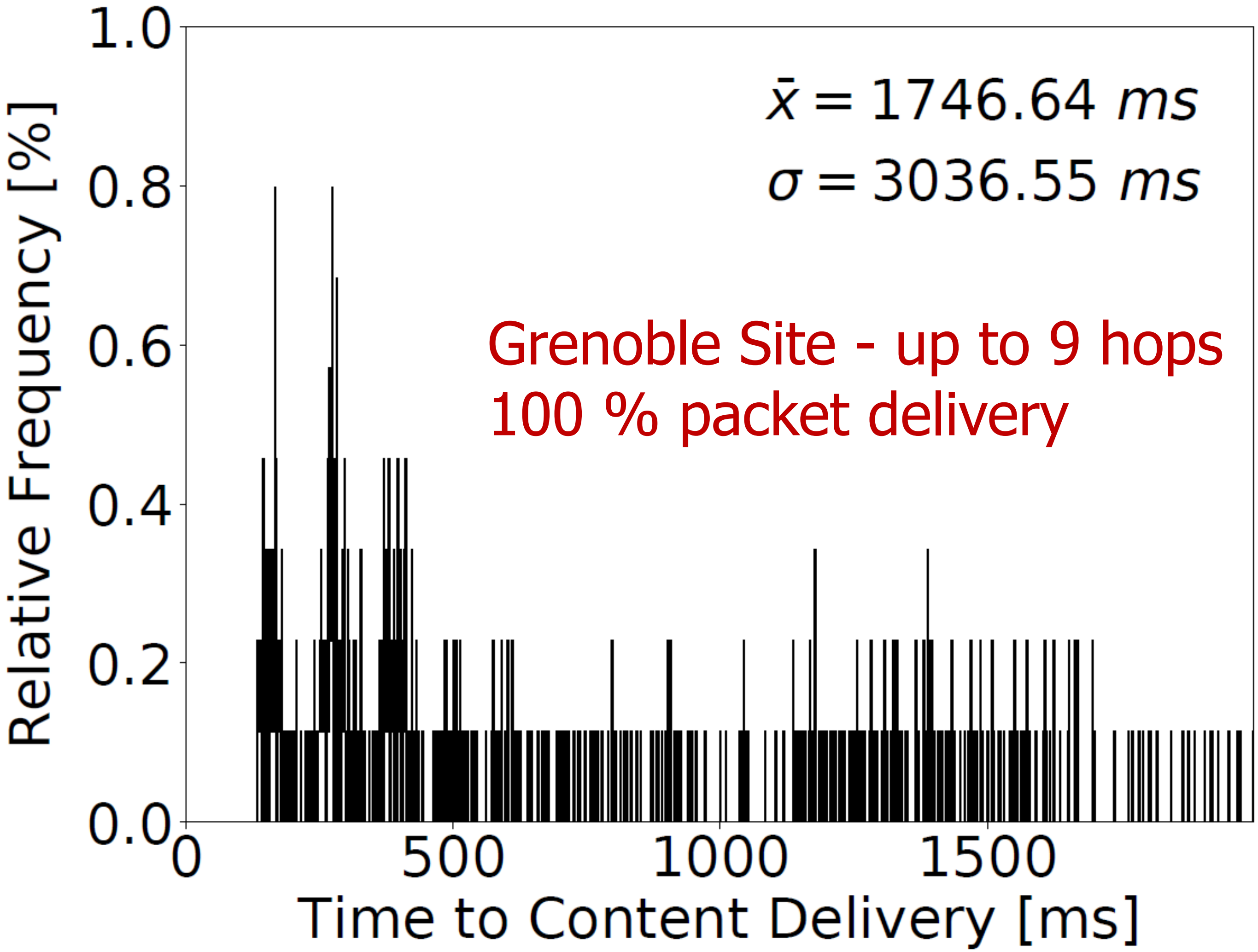
Application
Interest
Ctrl
Data
RIOT
CCN-lite API
CCN lite
FWD
FIB
CS
PIT
dst addr from face
src addr to face
TX/RX
netapi
gnr
netapi
MAC
MAC
netdev
netdev
Driver
Driver

GNRC versus CCN-Lite



(a) ROM (b) RAM

NDN Network Performance



Conclusions & Outlook

- There is demand for a flexible software support with versatile experimentation options
- The RIOT networking architecture satisfies these demands by
  - High-level hardware abstraction with clean interfaces
  - Powerful, recursive layering

  at very low performance penalty
- Federated trust - bootstrapped by crypto-based identifiers
- ICN a promising candidate for IoT deployment

References

- Emmanuel Baccelli, Oliver Hahm, Mesut Günes, Matthias Wählisch, T. C. Schmidt, *RIOT OS: Towards an OS for the Internet of Things,* In**:** *Proc. of the 32nd IEEE INFOCOM. Poster,* IEEE Press : Piscataway, NJ, USA, 2013.
- *RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT, The IEEE Internet of Things Journal,* IEEE, 2018. (in press)
- Martine Lenders, et al., *Connecting the World of Embedded Mobiles: The RIOT Approach to Ubiquitous Networking for the Internet of Things,* Technical Report, No. arXiv:1801.02833, January 2018.
- Tobias Markmann, T. C. Schmidt, Matthias Wählisch: *Federated End-to-End Authentication for the Constrained Internet of Things using IBC and ECC,* In: *SIGCOMM Comput. Commun. Rev.,* Vol. 45, No. 5, p. 603–604, ACM, 2015.
- E. Baccelli, C. Mehlis, O. Hahm, T. C. Schmidt, M. Wählisch, *Information Centric Networking in the IoT: Experiments with NDN in the Wild,* In: *Proc. of 1st ACM Conf. on Information-Centric Networking (ICN-2014),* p. 77–86, ACM, 2014.

Thanks & Questions ?

Group: http://inet.haw-hamburg.de/

RIOT: http://www.riot-os.org/

RIOT Summit

September 13 – 14, 2018

Meet in Amsterdam!

http://summit.riot-os.org