

Privacy in IoT

A (pure?) Technical Perspective

Prof. Dr. Thomas Engel
Vice-Director Snt, Head of SECAN-Lab
University of Luxembourg

Further contacts within the team:
Dr. Maria Rita Palattella
Dr. Foued Melakessou
Latif Ladid, president IPv6Forum



Interdisciplinary Centre for Security, Reliability and Trust



Overview

- IoT Projects and Activities of SECAN-Lab
 - IoT6
 - Butler
 - IETF 6TSCH
- How to fill the privacy „gap“
- Conclusions

IoT6: “Universal Integration of the Internet of Things through an IPv6-based Service Oriented Architecture enabling heterogeneous components interoperability”

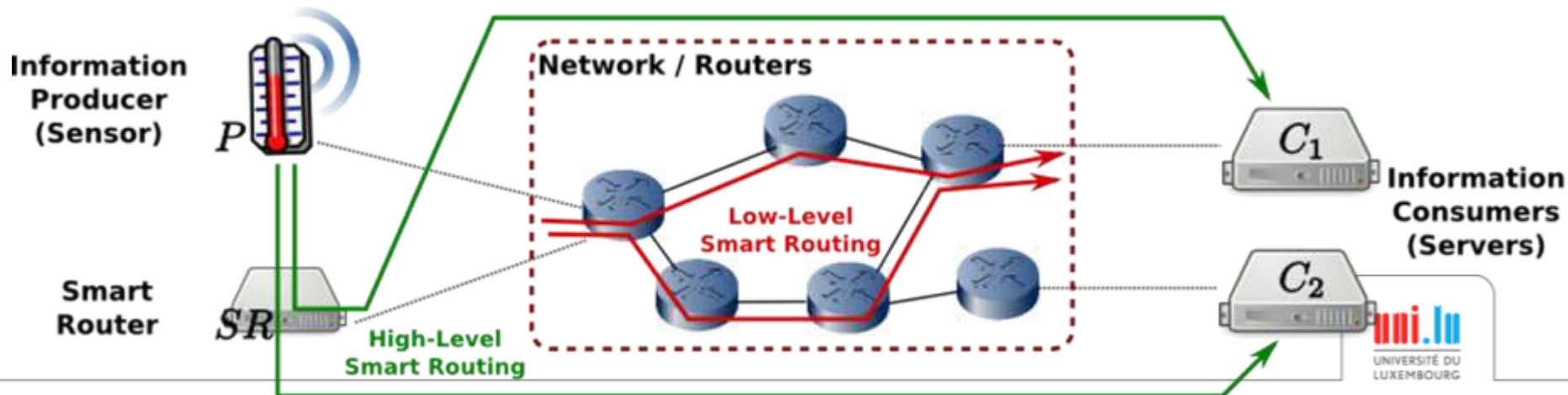
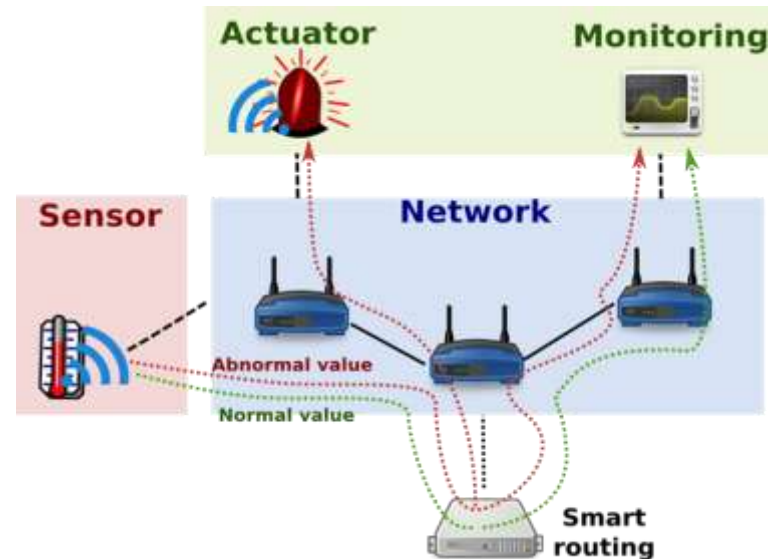
3 years FP7 European research project (October 2011- September 2014)

Aims and objectives

- ☐ Research the potential of IPv6 and related standards to support the future Internet of Things and to overcome its current fragmentation.
- ☐ Develop a highly scalable IPv6-based Service-Oriented Architecture to achieve interoperability, mobility, cloud computing integration and intelligence distribution among heterogeneous smart things components, applications and services.
- ☐ Explore innovative forms of interactions with:
 - a) Multi-protocol integration & interoperability with heterogeneous devices.
 - b) Mobile & cellular networks.
 - c) Cloud computing services (SaaS).
 - d) RFID tags and related systems, such as EPCIS.
 - e) Information and intelligence distribution.

Smart routing, based on:

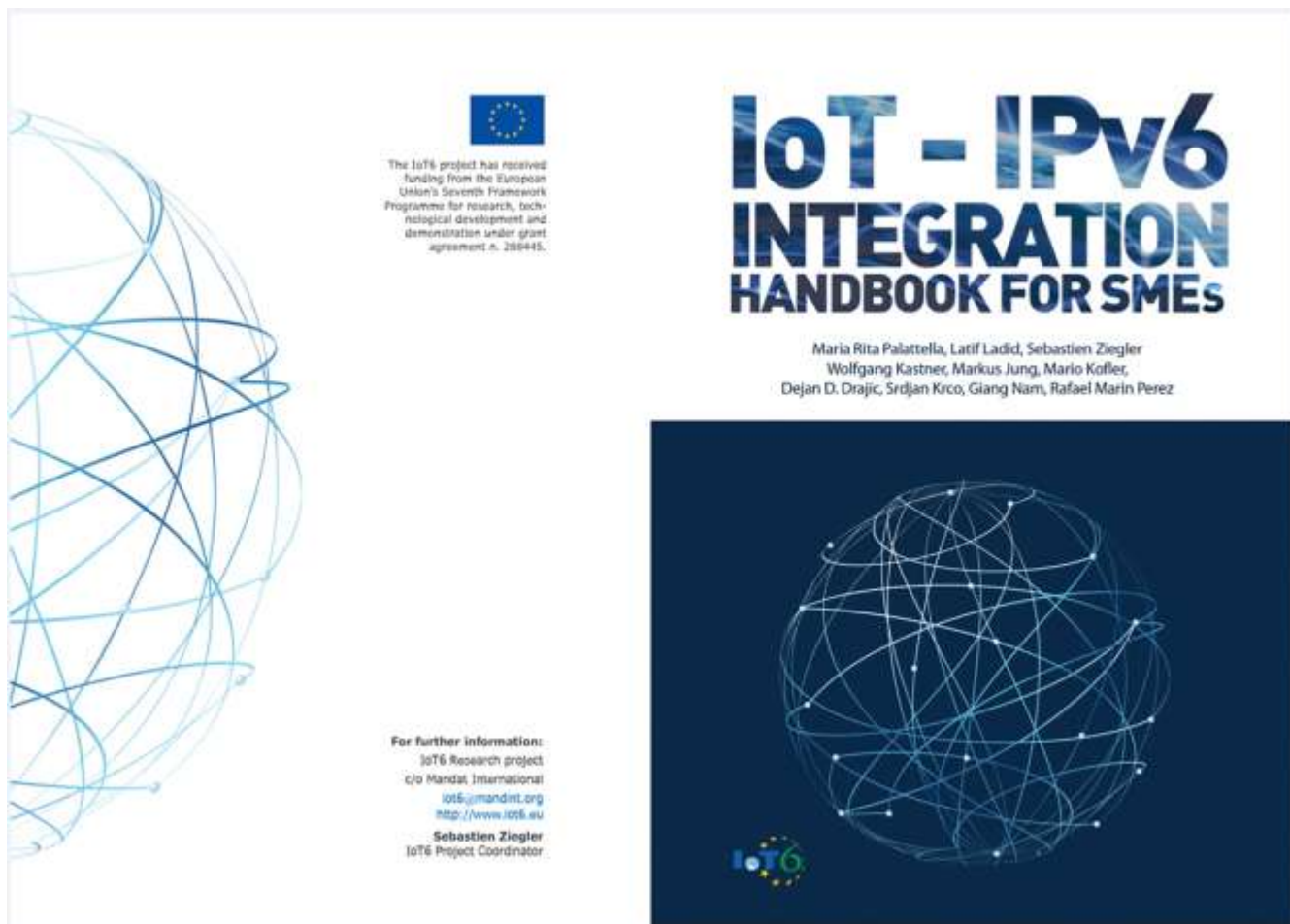
- Traffic analysis / packet filtering
- CCN
- SDN (per-flow)





IoT6.eu

Researching IPv6 potential for the Internet of Things



The IoT6 project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n. 289445.

IoT - IPv6 INTEGRATION HANDBOOK FOR SMEs

Maria Rita Palattella, Latif Ladid, Sebastian Ziegler
Wolfgang Kastner, Markus Jung, Mario Kofler,
Dejan D. Drajić, Srdjan Kirco, Giang Nam, Rafael Marin Perez

For further information:

IoT6 Research project
c/o Mandat International
iot6@mandint.org
<http://www.iot6.eu>

Sebastian Ziegler
IoT6 Project Coordinator



UNIVERSITÉ DU
LUXEMBOURG



Content

Preface	7
1 Application and Benefits of IPv6 for the IoT	11
1.1 Introduction to IPv6	11
1.2 Main benefits of IPv6 for the IoT	12
1.3 Integration with the Cloud	16
1.4 Integration with the mobile world	17
1.5 Integration with tags, RFID and NFC	18
1.6 Integration with building automation	19
1.7 IoT Emerging standards and trends	21
2 Application and benefits of IPv6 for SMEs	23
2.1 Main benefits of IPv6 to a SME	23
2.2 IPv6-based IoT Applications: IoT6 use cases	24
2.2.1 Use Case 1: Smart Office and legacy devices Integration	24
2.2.2 Use Case 2: Safety alert and dynamic routing	25
2.2.3 Use Case 3: Building maintenance	27
2.3 IPv6 Business Case: Mobile phone as a sensing tool	28
3 Practical steps: How to deploy IPv6 in an SME	33
3.1 How to set up IPv6?	33
3.2 Enabling low-power IPv6-IoT networks with 6LoWPAN	36
3.3 Enabling DNS with IPv6	37
3.3.1 DNS Considerations about Special IPv6 Addresses	38
3.3.2 Recommendations for Service Provisioning Using DNS	38

3.4 Enabling a Mail Server with IPv6	40
3.5 Tunneling for providing IPv6 connectivity	41
3.6 Enabling a web server with IPv6	43
3.7 Enabling Security with IPv6	45
3.7.1 Neighbor discovery threats	46
3.7.2 DHCP related threats	47
3.8 Integrating legacy devices	48
4 Conclusion	53
5 Glossary	55
6 References	59
6.1 Useful web sites and tools	63
Acknowledgements	64



IoT-PRIVACY CHALLENGES AND THREATS, A TECHNICAL PERSPECTIVE

Contact at the University of Luxembourg:
Dr. Foued Melakessou, SnT



BUTLER Project



- FP7 call: FP7-ICT-2011-7, Integrated Project, 15 M€
- October 2011 → September 2014, 1234 man-months



Project Objective



- Design and demonstrate prototype of a **comprehensive, pervasive** and **effective Context-Aware** information system, which will operate transparently and seamlessly across various scenarios towards a unified **Smart Life** environment (Home, Health, Transport, City and Shopping)
- Internet-of-Things (IoT): Large number of constrained and low cost embedded devices (low power consumption, limited ROM/RAM, wireless communication range, etc.)
- Smart Object & Smart Server & Smart Mobile



Integrated IoT Enabling Technologies

- The Butler security framework enables end-to-end security between a data provider and a data consumer
- The security protocols insure confidentiality, integrity of the messages and authentication of the peers
- Data can only be received by allowed entities
 - All technical components (gateways, proxies) used to transport data shall not have access to the data
 - The data cannot be retrieved and used by entities without user controls



BUTLER Security Framework 1/2

- “Things” are able to communicate
- In legacy M2M architecture, devices regularly sends data to Service Platform and Applications retrieve such data from the Service Platform.
- The two links can be secure point-to-point but there is no end-to-end security between the consuming application and the device
 - Privacy issue: the data is kept in clear at Service Platform and may be used in fraudulent way or without control of user
 - the Service Platform must follow data storage and protection regulation rules which may higher the operational cost of the Service Platform
 - In BUTLER, an IoT Security Framework have been prototyped supporting authorization paradigm and end-to-end security between devices and applications

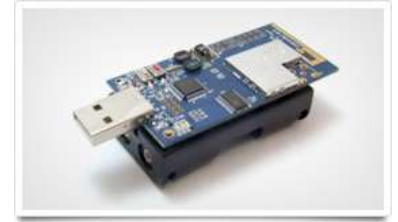


BUTLER Security Framework 2/2

- The BUTLER Security Framework provides a simple security and privacy paradigm that can be implemented in low cost device
- Using the Trust Manager, the user specifies its resources and manages the access permissions to his resources
- The Trust Manager is not involved during the transfer of data between the resources and the applications and in consequence, business data management is the responsibility of the applications
- The applications may use Service Platform to perform access to resources
- The Security framework gives a way for applications to access resource using a Service Platform
 - the Service Platform does not have access to clear data and cannot valuate clear business data
 - the Service Platform shall act as application and be allowed to use data on behalf of the user



Security solutions in 6LoWPAN networks



- Coap Tesbed (TelosB/Sky platforms)
 - real-time monitoring of temperature and humidity in an office environment
- Several security schemes had been tested for IoT devices running on TinyOS (e.g. TinySec, AES Encryption of CC2420, MiniSec, Relic and TinyECC) or Contiki (e.g. ContikiSec, Contiki-TLS-DTLS, Contiki IPsec, CoAPs: COAP over DTLS/TLS)
- Low level security can be ensured at the link layer in respect with the Advanced Encryption Standard (AES) scheme (Pre-shared keys)



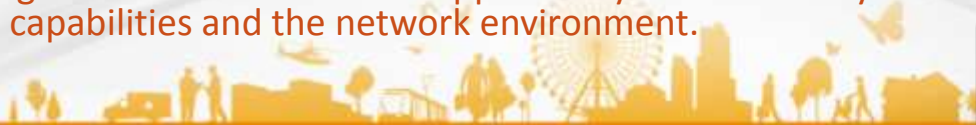
Summary of Security Issues

- Low Level
 - In constrained environments, the addition of a lightweight cryptography often became impossible due to the lack of memory space
 - Bootstrapping of the security (LAN)
 - Securing data between an object and a gateway/proxy/modem linked to the WAN
 - Crediting the components of the LAN with a shared “local” session key
- Application Level
 - Bootstrapping of the security:
 - Secure addition of a new object to the IoT network thanks to trust operations including authorization and authentication
 - Attacks must be prevented thanks to the threat analysis of the whole network
 - The device identity and the secret keys used during the running cycle are provided during the bootstrapping phase. Once deployed, the device is under the control of its owner.
 - The distribution of the access rights is done according to access-token and cryptographic keys to the components of the WAN, in order to exchange information or to access to resources.
 - The Session establishment addresses the problem of ephemeral session credentials distribution from the object to the user in order to implement “hop-by-hop” or “end-to-end” security.
 - Privacy: the current IoT solutions are vertical solutions where the data are stored in clear at Service Platform and can be retrieved later by applications. There is a security link from resource to Service Platform and another security link between application and Service Platform, in consequence there is no end-to-end security between the application and the resource, the Service Platform may perform data analysis but without user consent and therefore this poses a problem of privacy.
 - authorization allows the user to grant access permission to applications



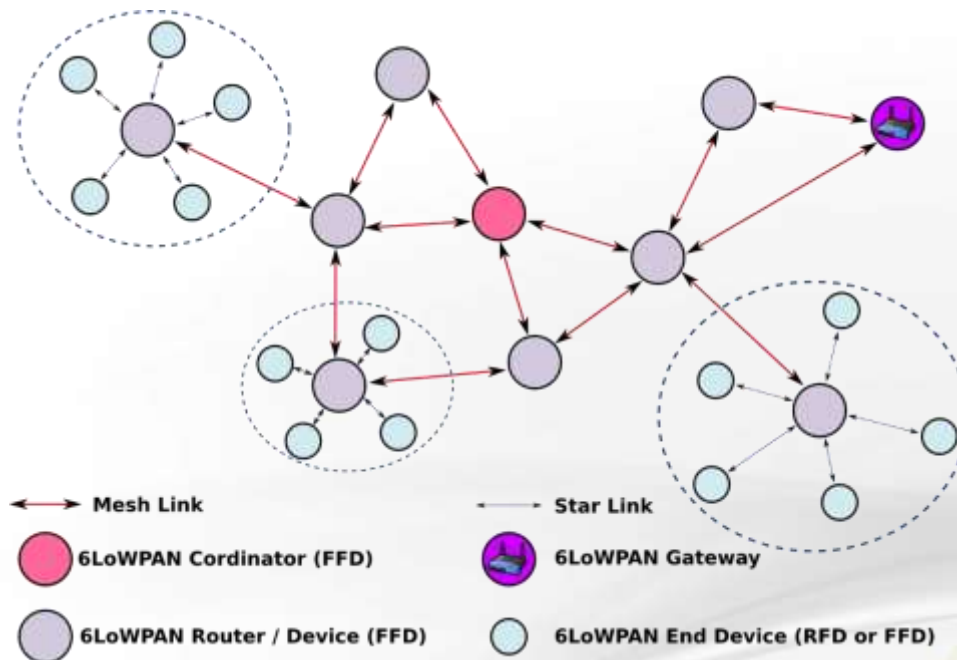
Challenges

- Final users requires low cost and user friendly solutions that automatically support security and privacy.
- Solution providers need also low cost implementation
 - the privacy requirement is not the “most important” requirement,
 - they want to use data, perform data analytics to enhance the data value.
- Technically, the challenges concern:
 - the security of the Local Area Network (LAN) which can be deployed everywhere,
 - the security of the devices which are the data provider (and/or actuator),
 - the security of the Wide Area Network(WAN) which transports data between peers,
 - the security of the applications.
 - Applications may use intermediate technical entities (server , gateways etc...) to communicate with devices. Such intermediate entities could be a wake point where data can be retrieved and used without user consent
- BUTLER addressed the security and privacy at design level and focused on architecture and communication
 - BUTLER marginally addressed the security of the server and device implementations,
 - At application level, the challenges concern the initialization of the security credentials allowing security bootstrapping in heterogeneous horizontal environment,
 - At LAN level, the challenges concern the concrete applicability of the security technics according to the device capabilities and the network environment.



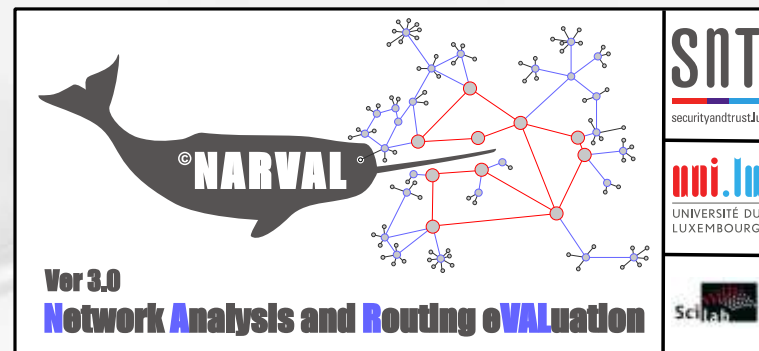
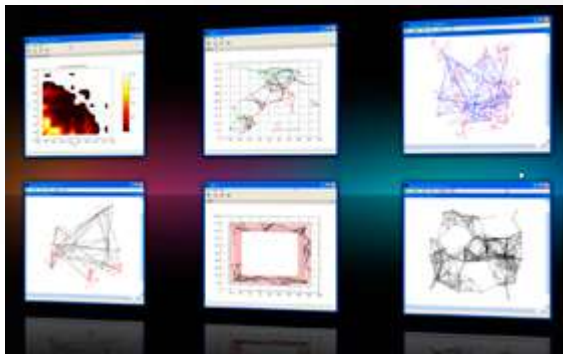
Technical Challenges Solved

- Deployment of **constrained devices** (6LowPAN)
- Security at “Lower-Layers” and “Upper-Layers” (**6LowPAN**)
- **Simulation** of 6LowPAN networks



Simulation Environment

- NARVAL (**N**etwork **A**nalysis and **R**outing **e**VALuation)
 - Complete software environment enabling the understanding of available communication algorithms, but also the design of new schemes
 - Analysis of network protocols: Graph Optimization, Topology, Internet Traffic, Routing, Transmission Protocol, Route Diversity, Mobility, Database, Security, Anonymity, Path Planning, Wireless Sensor Network, IoT, Geostatistical Mapping, etc.
 - Target audience: academics, students, engineers and scientists
 - <http://atoms.scilab.org/toolboxes/NARVAL>



6TiSCH status

- UL is **one of the leading member** of the newly defined [IETF 6TiSCH Working Group](#): “IPv6 over the TSCH mode of IEEE 802.15.4e”
- Discussions started in December 2012
- Very traditional IETF procedure
 - IETF mailing list created 24/01/2013
 - 147 members (mix between academic and non academics)
 - First face-to-face meetings at IETF 86 in Orlando (March 2013)
 - Towards formal IETF working group status in Berlin (July 2013)

... in practice

Mailing list

6tisch@ietf.org

<https://www.ietf.org/mailman/listinfo/6tisch>

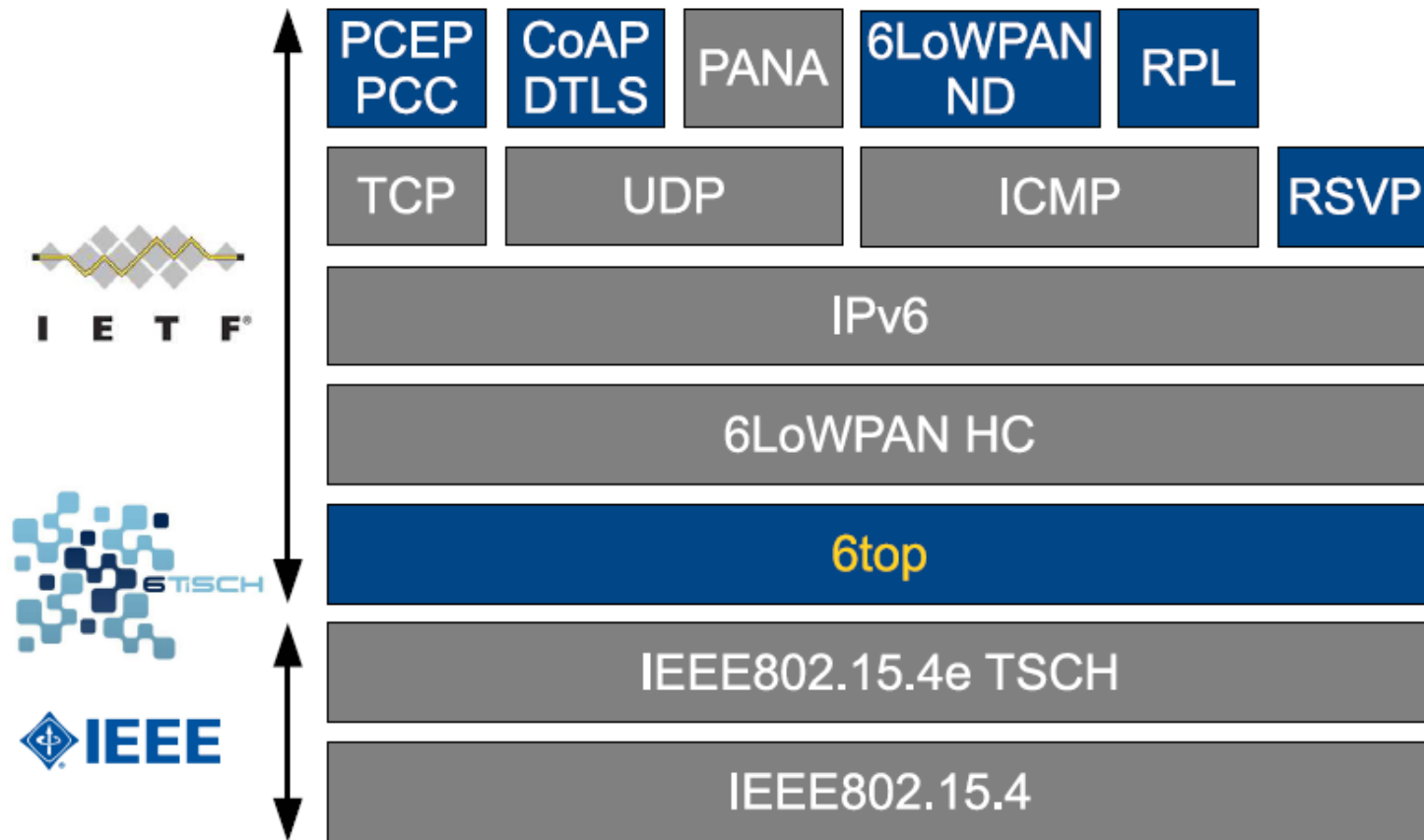
bi-Weekly Webex calls

Homepage

<https://bitbucket.org/6tisch/>

6TiSCH Protocol Stack

Gluing together existing upper IETF and lower IEEE stack

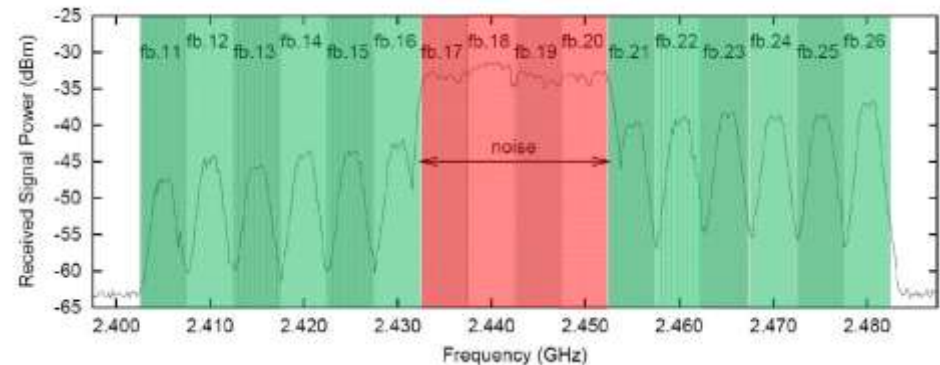
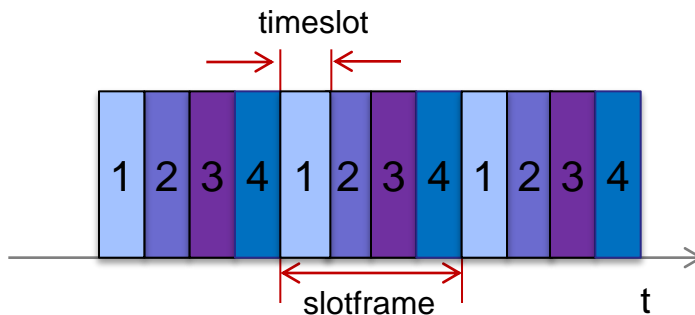


MAC layer: IEEE 802.15.4e TSCH

Application	CoAP
Transport	UDP
routing	IETF RPL
Network	IPv6
adaptation	IETF 6LoWPAN
MAC	IEEE 802.15.4e
PHY	IEEE 802.15.4-2006

- **TSCH: TimeSlotted**

- Time is divided in slots
- All motes are synchronized to a given slotframe
- *Slotframe*: group of slots which repeats over time
- Number of slots in a slotframe is tunable

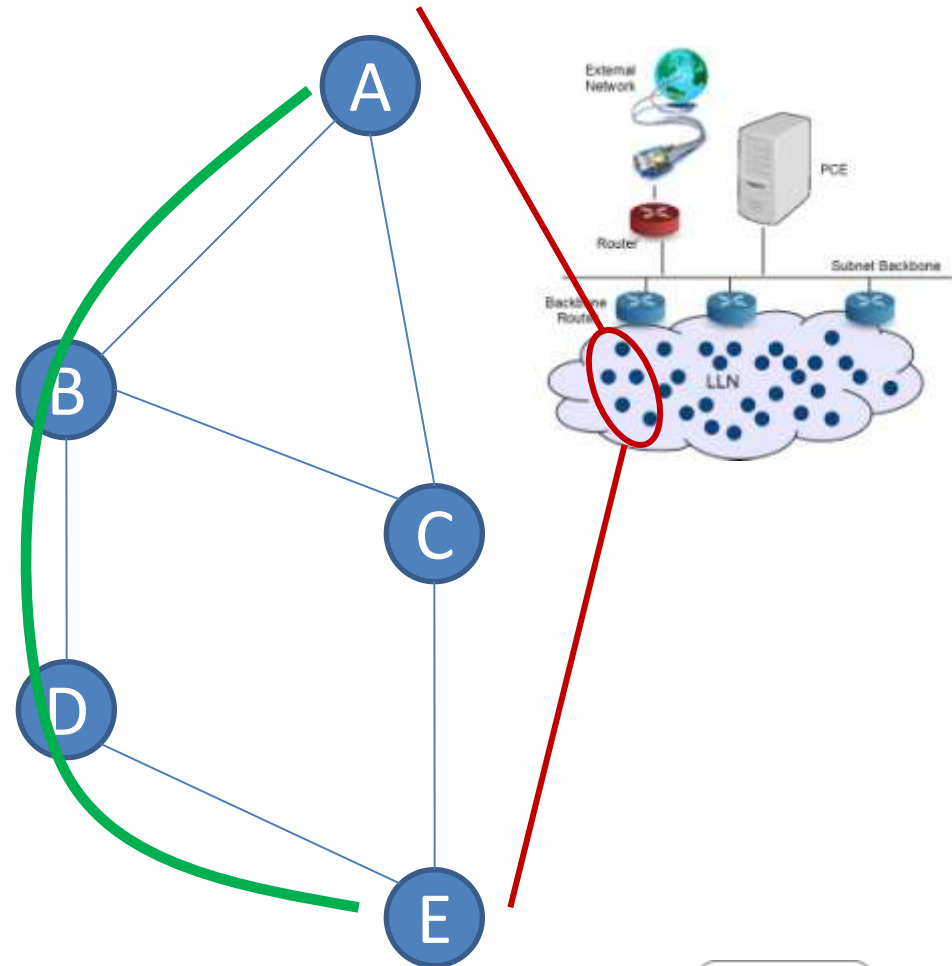


- **TSCH: Channel Hopping**

- 16 channels are available in the 2.4GHz frequency band (optional *blacklist*)
- A single time slot can be used by multiple pairs of nodes -> **Network capacity is increased**
- The channel offset is translated into a frequency (i.e., a real channel)
- A given mote sends subsequent packets on different channels -> **Interference and multipath fading are mitigated**

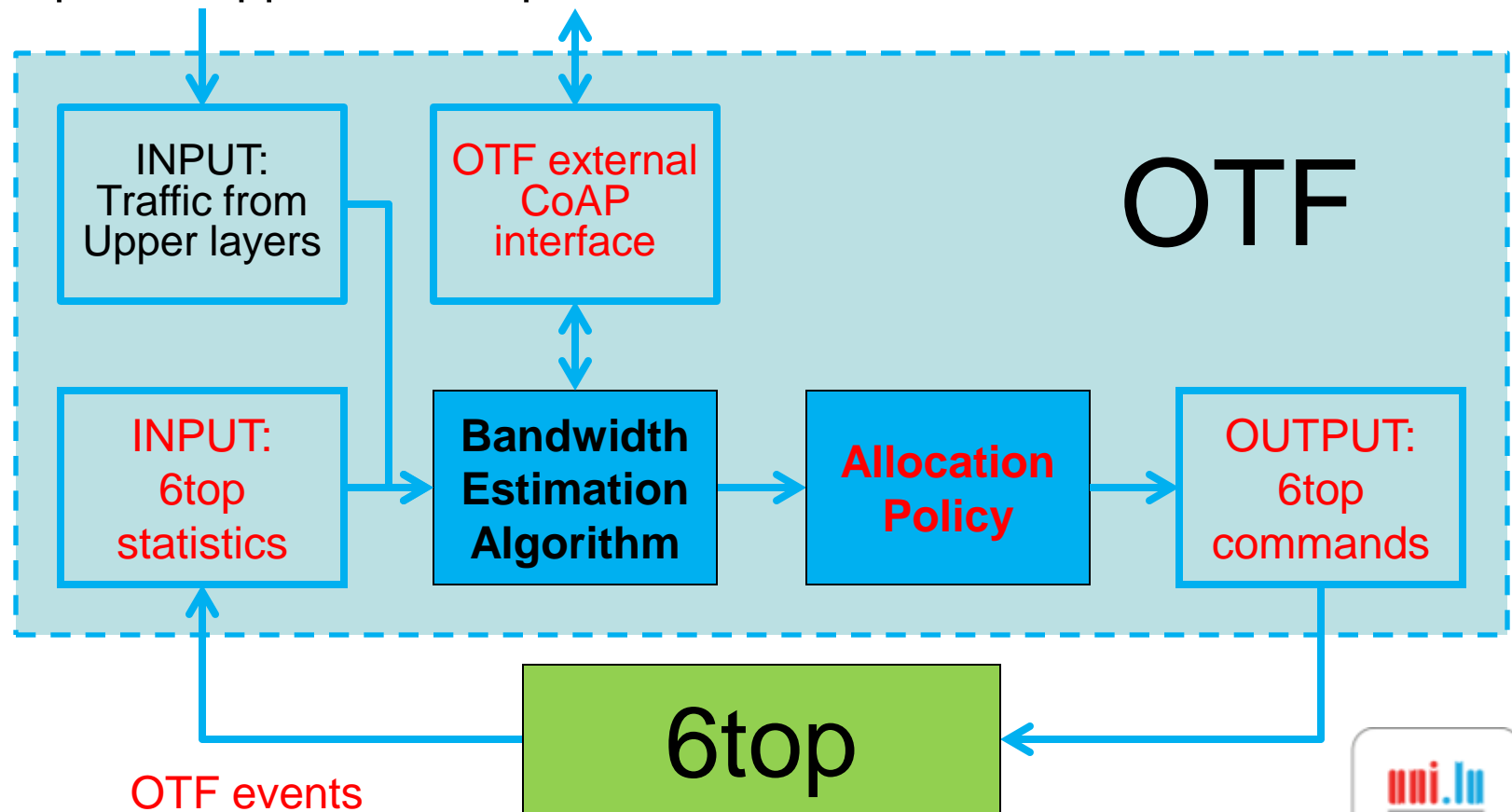
6TiSCH – Distributed Scheduling

- A installs a “pipe” of data to E
 - A sends a packet along the $A \rightarrow B \rightarrow D \rightarrow E$ multi-hop path
 - At each hop, neighbor nodes negotiate with one another to add cells into their TSCH schedule
 - Monitoring process recovers from topological changes and collisions
- ❑ Candidate solutions:
- ❖ RSVP/MPLS
 - ❖ NSIS



6TiSCH – On-The-Fly-Scheduling (OTF)

Layer-3 mechanism to dynamically adapt the aggregate bandwidth, i.e., the number of reserved soft cells between neighbor nodes, based on the specific application requirements.



The remaining „Privacy issue“ in IoT

- Is it expensive? Do we really need it?
- Privacy or (Quality of) service: Is this a choice between black and white?
- Quality of Service in a distributed („cloud“) scenario: reliability and redundancy
- Privacy by distribution: Shannon's entropy helps here
- Authentication on data plane needed (instead of proprietary application layer solutions)
- (Distributed) Policy Enforcement to detect and stop violations, send alarms. This is easier in a centralized architecture, but unsolved in a real IoT cloud

Conclusion

- IoT interoperability and integration
- Change of paradigm: Privacy **by** distribution
- Authentication of data/packets/flows/pipes rather than users/devices, still lacking behind
- Better do practical steps than (just) talk about „global visions“
- We offer R&D support

Prof. Dr. Thomas Engel
thomas.engel@uni.lu
Tel. (+352) 46 66 44 – 5486