NOKIA Bell Labs

IoT Network Control and Management

LINCS seminar

- Ludovic Noirie with many colleagues from Nokia Bell Labs (IoT-Control department), Nesrine Ammar (ex-PhD student) and Sébastien Tixeuil (Sorbonne Université)
- 03/06/2020

1

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

   NOKIA Bell Labs

2

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

Context of IoT private Network
What is the Internet of Things (IoT)?

In **red**: what we consider in this presentation

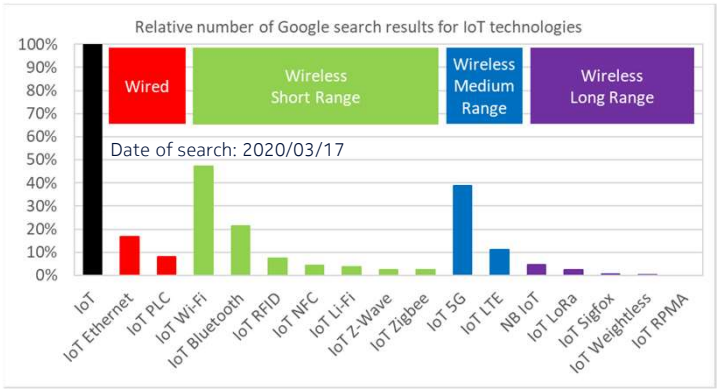
IoT = Internet of Things

- "Things" = anything = **any connected end-device in the network**
  - Things = devices interacting with the environment and/or humans, usually with limited capacities…
  - But "before-IoT-era" machines (such as PCs, laptops, smartphones…) are also part of the IoT!
  - Network Elements (NEs, such as Ethernet switches, routers, access points, …) may not be considered as "things" as they are not "end-devices"
    - User's access to NEs is mainly/only for their configuration
- "Internet" = **interconnection of networks (IoT: with their devices!)**
  - Many communication/network technologies for IoT: **IP/Eth/Wi-Fi**, Bluetooth, ZigBee, Z-Wave, LoRA, NB-IoT, …
  - IP (v4 & v6) is the network protocol for the Internet, **SDN/NFV** may be used for network control and management…
- L1 to L7 layers are concerned by IoT
  - (Multi-)Point-to-(Multi-)Point communication protocols between devices (L1-L2)
  - Network protocol (L3, mainly IP) with **network control** (e.g., SDN) and **network management** (e.g., NFV)
  - **IoT Services/Applications** (L7+): Apps on devices, on smartphones connected to IoT devices, in the Cloud…

Context of IoT private Network
Relevant (layers 1-2) network technologies for IoT

Source: https://en.wikipedia.org/wiki/Internet_of_things#Enabling_technologies_for_IoT

- **Wired**: Ethernet, PLC (Power Line Communication)
- **Short-range wireless**: Wi-Fi, Bluetooth, RFID, NFC, Li-Fi, Z-Wave, Zigbee
- **Medium-range wireless**: 5G, LTE
- **Long-range wireless**: NB IoT, LoRa, Sigfox, Weightless, RPMA (Ingenu)



Popularity of each network technology

- Google search with IoT + <techno>
  - Relatively to IoT alone
- Top 5 (>10% vs. IoT alone): Wi-Fi, 5G, Bluetooth, Ethernet, LTE

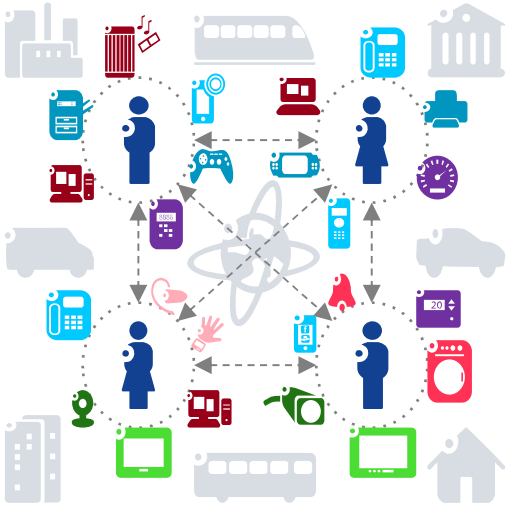
Private networks ⇒ Focus on Eth & Wi-Fi

5

Context of IoT private Network
Towards interconnection of smart environments?

Smart environments

- Smart Home
- Smart Building
- Smart Office
- Smart City
- Etc.



Interconnection of home/enterprise networks?

- Bring Your Own Device
- Telecommuting

⇒ How to isolate devices (security/privacy)?

⇒ How to easily control and manage them?

6

Context of IoT private Network

Control and management of IoT networks and their devices

Network

- Flexible/programmable control
- Autonomous management
- Taking into account the devices: fine grain control & management

Devices

- Management of the devices in the network
- Privacy / security aspects
- Monitoring

7

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

8

SDN/cloud-based platform for IoT private networks: Future Spaces
Softwarization / Programmability of Networks and Everything

Virtualization

- *SDN definition:* abstraction of hardware resources / network elements (for HW control by SW ⇒ programmable networks).
- *Computing/NFV definition:* separation of functionality from infrastructure (function implementation in commodity HW).
  - Note: these virtualized functions are naturally abstracted and controllable in a SDN way… But the reverse may not be true, e.g., optical elements, HW routers (SW routers can be virtualized in a NFV way)…

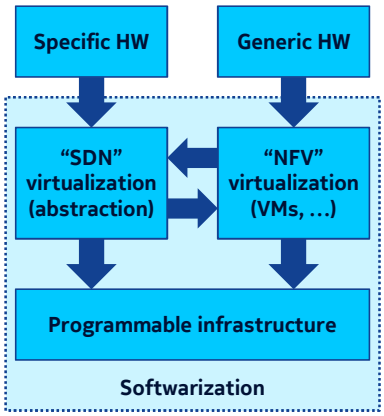
Programmability

- Make some elements/functions SW-controllable by the "user"
  - According to the context, "user" = infrastructure operator, network operator, potentially end-users in some context…

Softwarization

- Software-based control and management of elements/functions

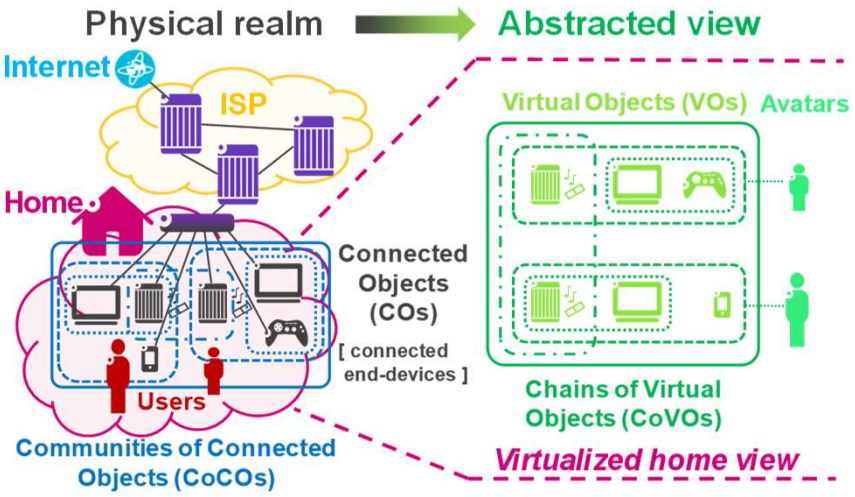
SDN: Software-Defined Network(ing)
NFV: Network Function Virtualization



[CNSM2014, ICT2015]

SDN/cloud-based platform for IoT private networks: Future Spaces
Majord'Home

- **Connected Object (CO):** an entity that can generate, receive and/or impact data flows that are carried through the network of a smart environment.
- **Community of Connected Objects (CoCO):** a group of connected objects (COs) which have something in common, with something being anything.



[CNSM2014, ICT2015]

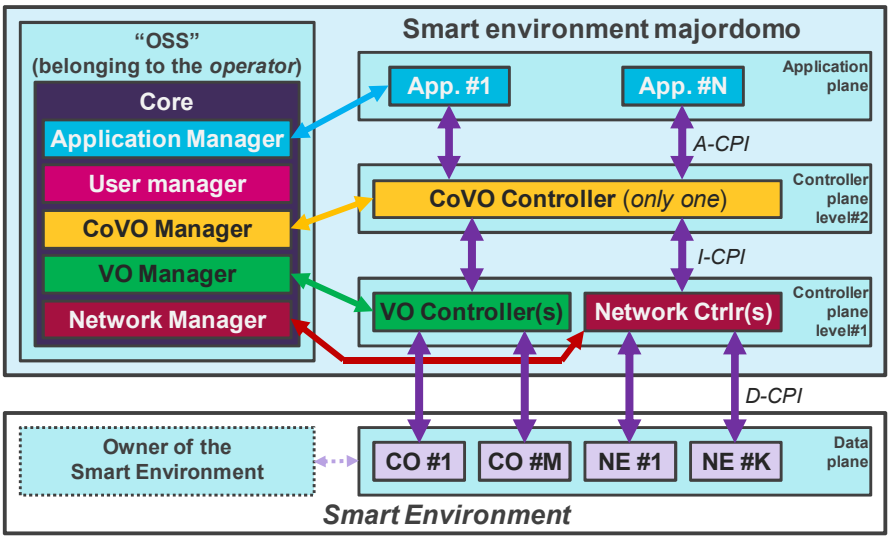
SDN/cloud-based platform for IoT private networks: Future Spaces
Majord'Home

SDN-like approach

- Compatible with SDN architecture

NFV-like approach

- Softwarization: some functions can be implemented in the cloud…



[Soft2016]

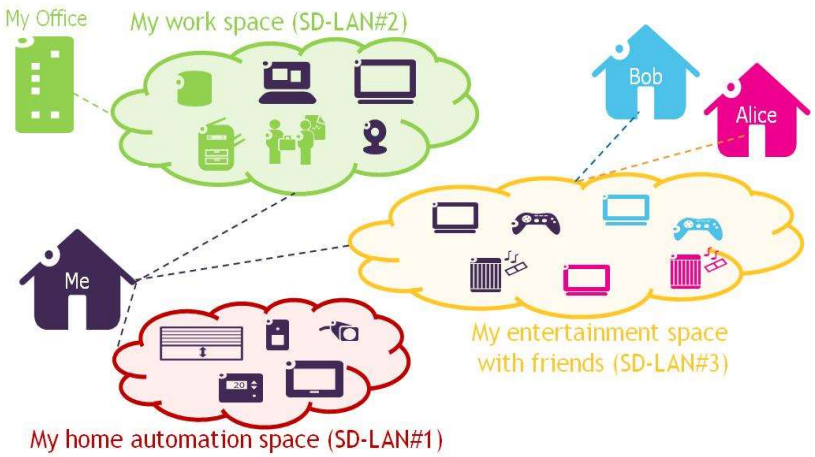
SDN/cloud-based platform for IoT private networks: Future Spaces
Software-Defined LANs (SD-LANS)

Sharing of devices between different smart spaces

- Home / Office
- Multi-Home

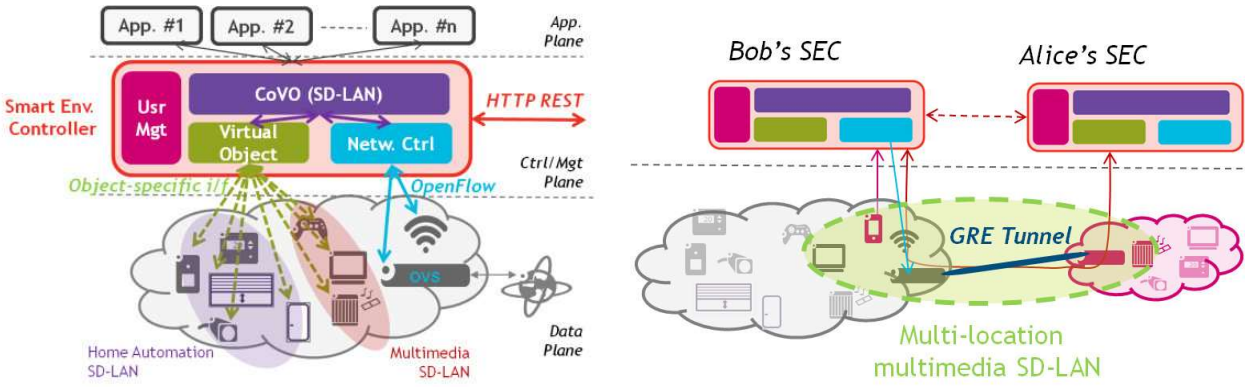
SD-LAN

- Isolation of devices in SD-LAN
- Implementation: SDN micro-slices, implemented in Open vSwitch routing tables (rules)



[Soft2016]

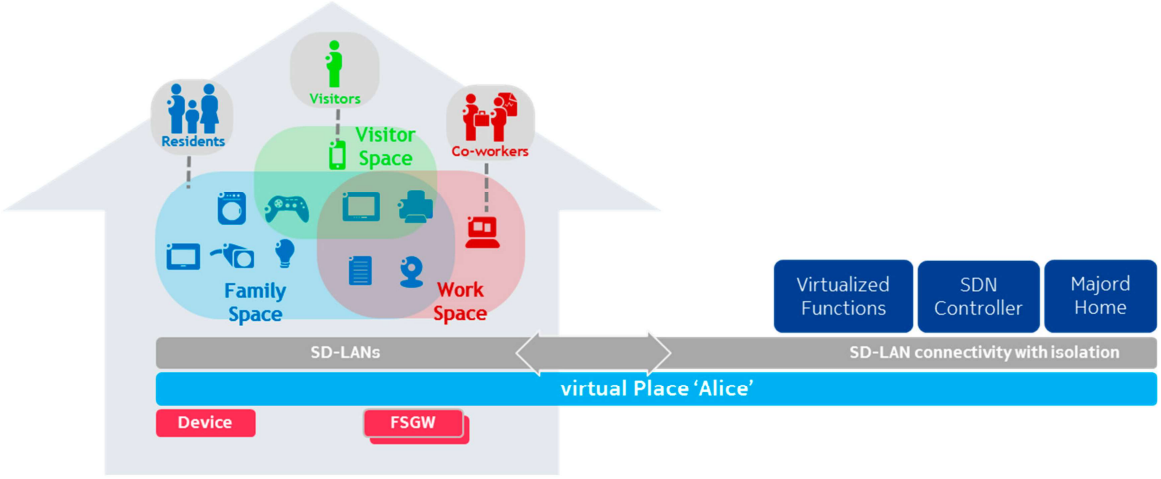
SDN/cloud-based platform for IoT private networks: Future Spaces
Software-Defined LANs (SD-LANS)



13

[Sens2018]

SDN/cloud-based platform for IoT private networks: Future Spaces
From SD-LAN to Future Spaces (Future-X Networks)

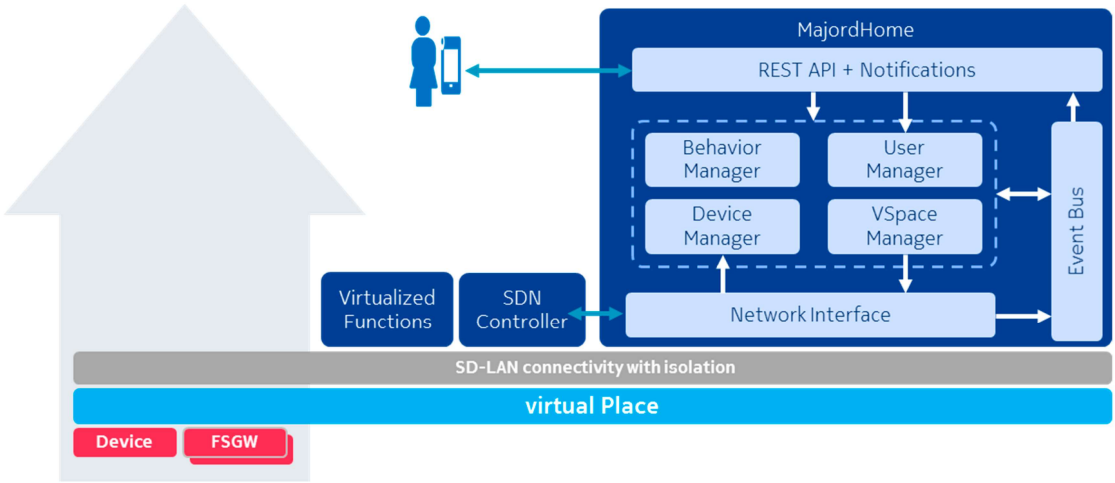


14

[Sens2018]

SDN/cloud-based platform for IoT private networks: Future Spaces

Majord'Home to set-up SD-LANs in Future Spaces

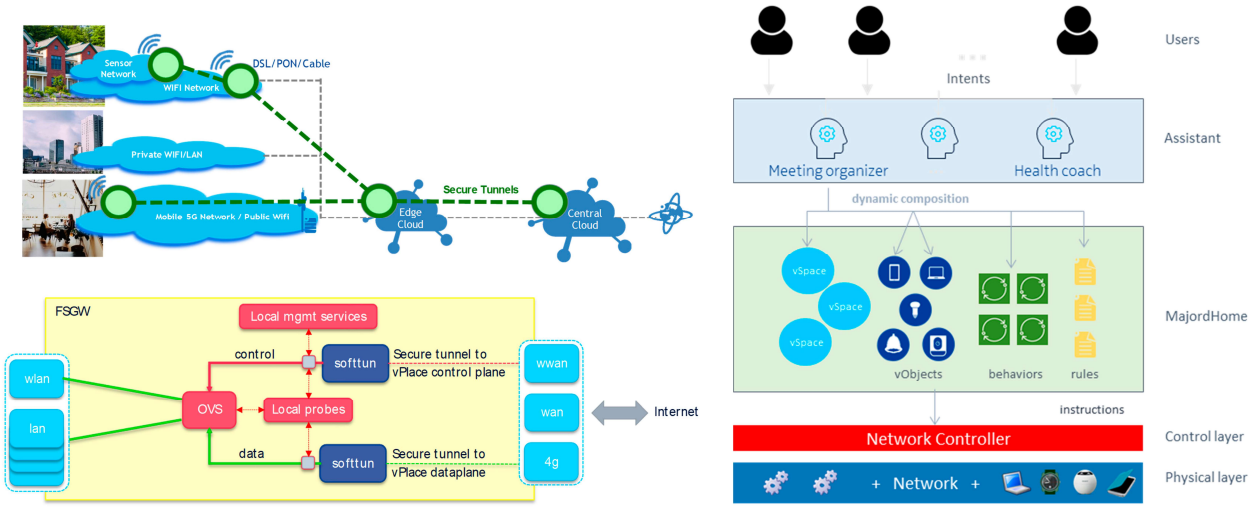


15

[Sens2018]

SDN/cloud-based platform for IoT private networks: Future Spaces

Future Spaces: distributed system (cloud + gateways)



16

Outline

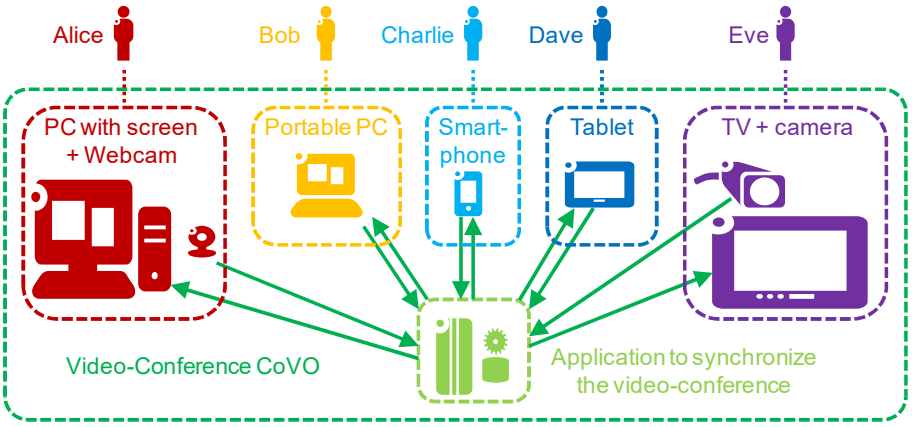
1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

17

SDN/cloud-based platform for IoT private networks: Future Spaces
SD-LAN for a specific "IoT service"

IoT service = on demand SD-LAN for a specific usage

- Example of videoconference



18

[IoT2016]
[ICIN2017]

SDN/cloud-based platform for IoT private networks: Future Spaces
Universal characterization of IoT services & automated recommendation

Algorithm for IoT service characterization

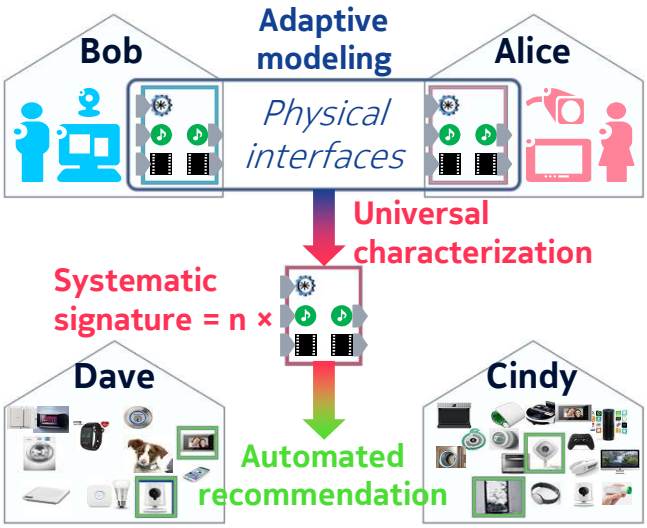
- Focus on the **physical interfaces** of the connected objects and their location in spaces
- Identify the profile of each space

  Profile = set of the physical interface types that are in the given space.
- For each profile, count how many spaces have the same profile

⇒ "Signature" of the service

Use for IoT service recommendation

- Service catalog with classes
- Signature matching of user's request



19

[ICIN2018]

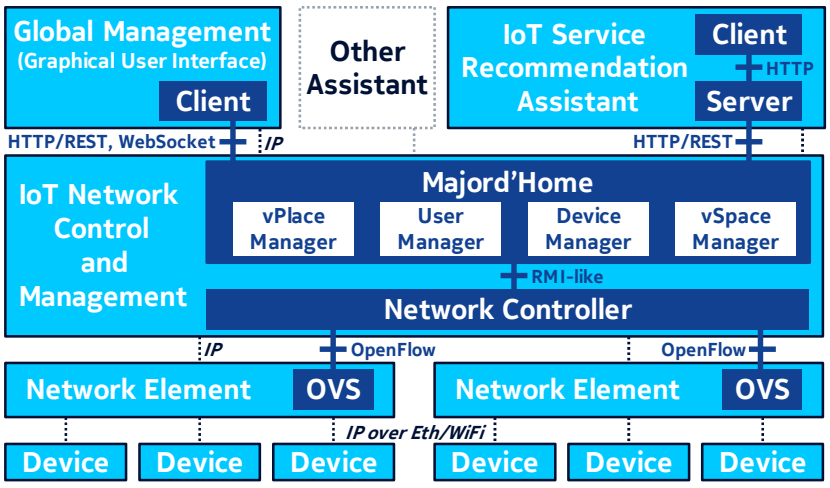
SDN/cloud-based platform for IoT private networks: Future Spaces
IoT service recommendation assistant

Implementation

- Use of the Future Space platform
- IoT service recommendation implemented as an assistant on top

Demo

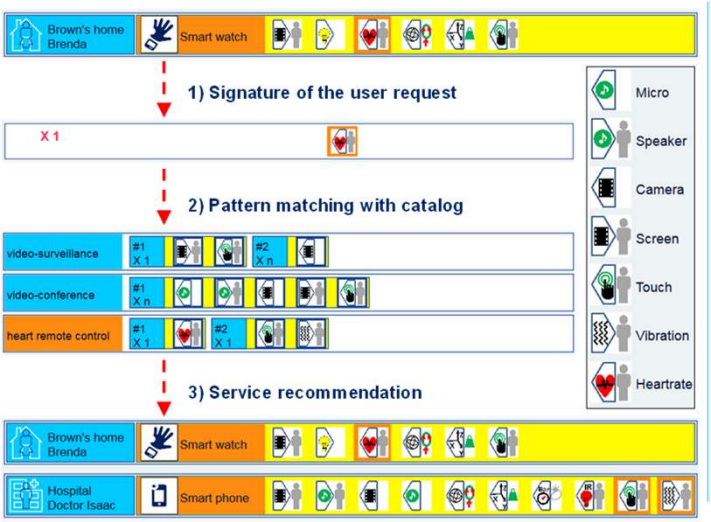
- The user select an IoT service
- The assistant propose devices in rooms
- The assistant establish an SD-LAN between the device that can then communicate



20

[ICIN2017]

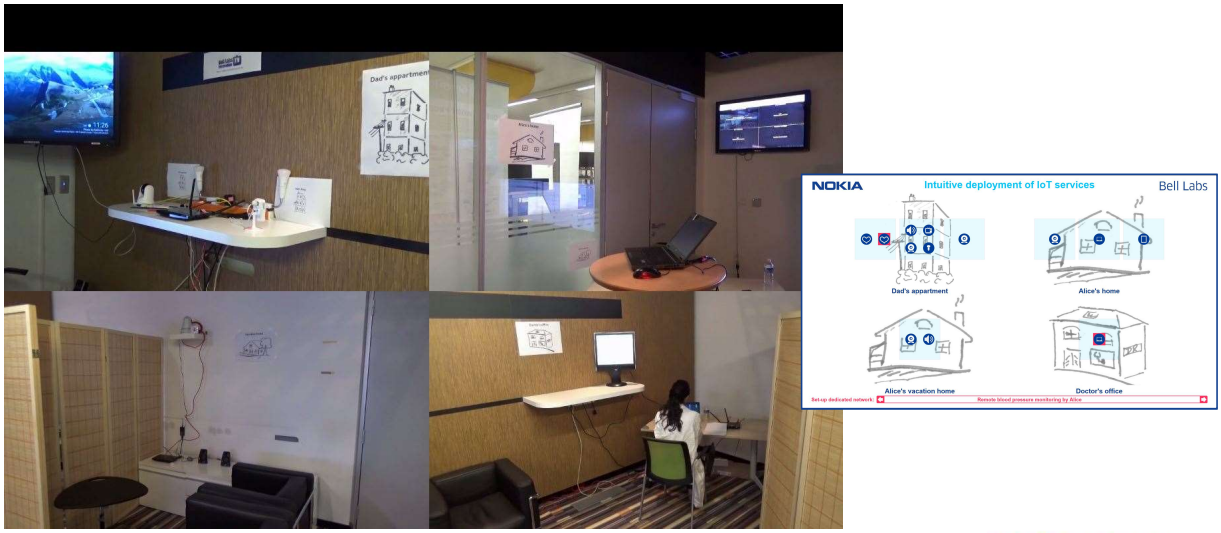
SDN/cloud-based platform for IoT private networks: Future Spaces
Demo @ ICIN 2017 (emulation on PC): IoT service recommendation (algo)



21

[ICIN2017]

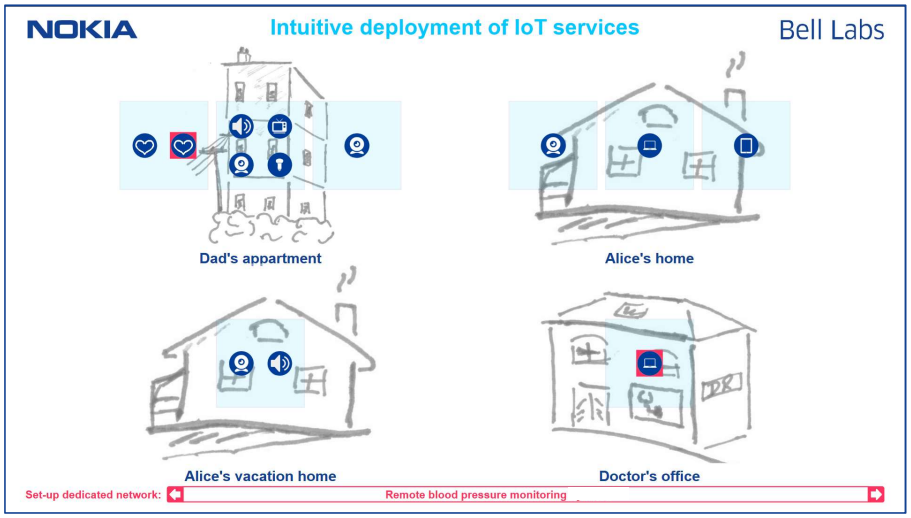
SDN/cloud-based platform for IoT private networks: Future Spaces
Demo @ ICIN 2018 (and Nokia Paris Saclay "Open Days") using real devices



22

[ICIN2017]

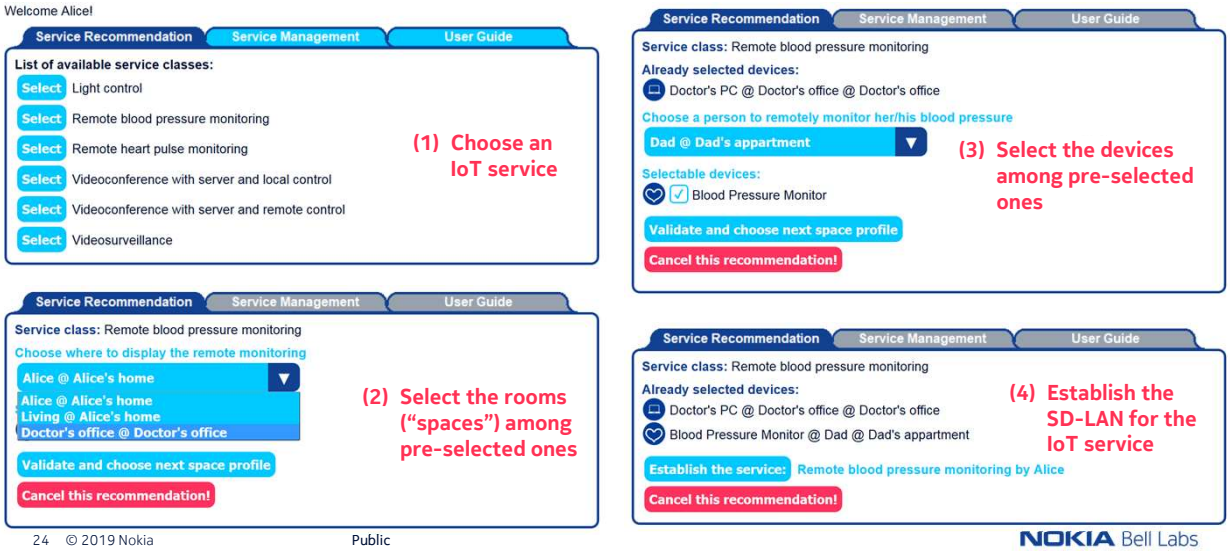
SDN/cloud-based platform for IoT private networks: Future Spaces
Demo @ ICIN 2018 using real devices 1/3



23

[ICIN2017]

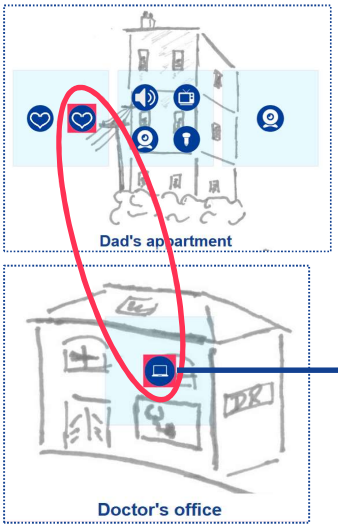
SDN/cloud-based platform for IoT private networks: Future Spaces
Demo @ ICIN 2018 using real devices 2/3



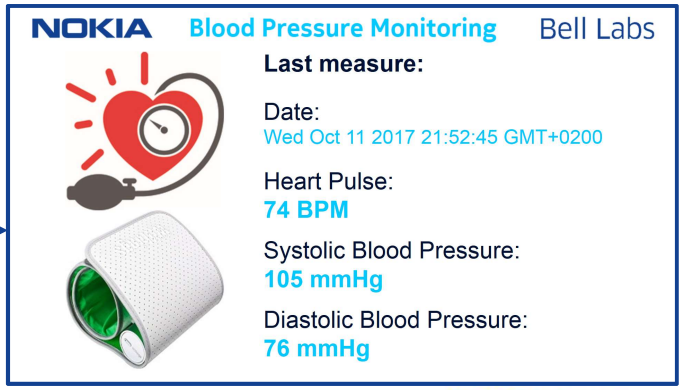
24

[ICIN2017]

SDN/cloud-based platform for IoT private networks: Future Spaces
Demo @ ICIN 2018 using real devices 3/3



The IoT service is enabled: the devices can communicate through the SD-LAN



25

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

26

Use-case: IoT-device-type identification
Context

IoT complexity for end-users

- Many devices / Heterogeneity
- Many applications / Silos
- Lack of know-how
- Lack of knowledge

⇒ Need for digital assistance

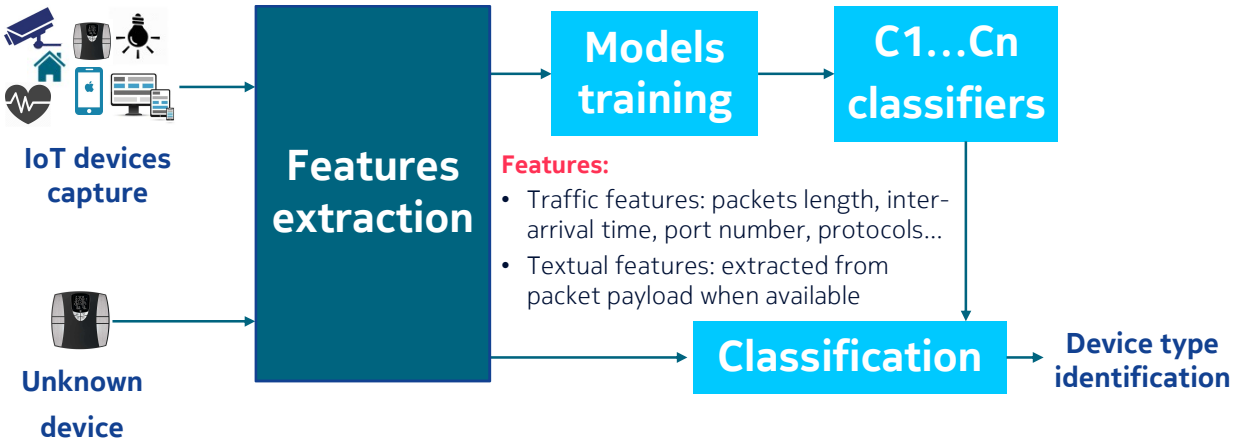
⇒ Need to know the capabilities of the connected devices

⇒ Need to identify the nature of the connected devices

27

[ICC2020]

IoT device type identification methodology
Methodology using supervised Machine Learning techniques



28

[ICC2020]

IoT device type identification methodology

Machine Learning techniques used

We tested the following ML techniques:

- Random Forest
- Decision Tree
- K-nearest Neighbors
- Support Vector Machine
- Naïve Bayes

Algorithm	Accuracy	Recall	Precision
Random Forest	0.95	0.96	0.96
Decision Tree	0.98	0.97	0.97
K-nearest Neighbors	0.97	0.97	0.95
Support Vector Machine	0.89	0.92	0.94
Naive Bayes	0.96	0.99	0.95

Best = Decision Tree

- Best on Precision and Accuracy
- Possibility to "understand" what Decision Tree is doing by inspection (interpretability)

Notes:

- We did not test Artificial Neural Network (no need…)

29

[ICC2020]

IoT device type identification performance evaluation

Dataset with 28 devices

Dataset

- 22 Wi-Fi/Eth devices from Miettinen et al. 2017
- 6 additional devices from our lab

Good diversity

- **Cameras**: D-Link (5020L, 930L, 935L), Panasonic, Edimax
- **Plugs**: Edimax (1101W, 2101W), TP-Link (HS100, HS110)
- **Switches**: D-Link, Wemo
- **Smartphones**: Nokia, iPhone
- **Scales**: Aria, Withings

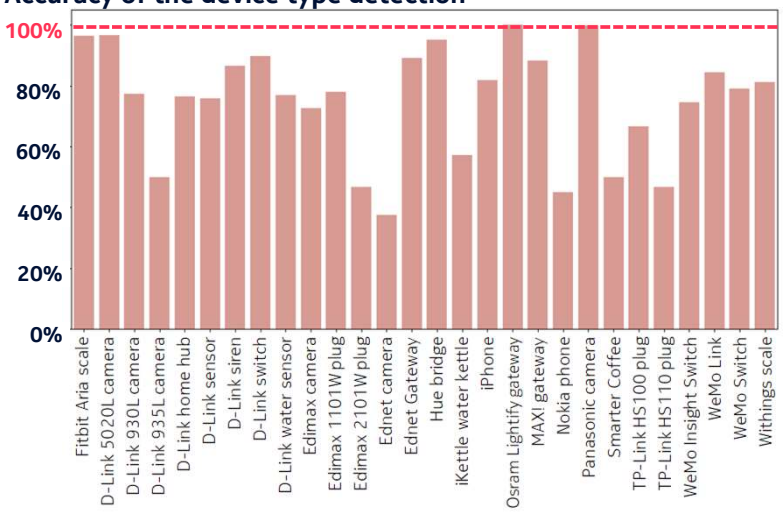
30

[ICC2020]

IoT device type identification performance evaluation

Evaluation on 28 devices using Decision Tree, statistical traffic feature only

Accuracy of the device type detection



Poor accuracy using only statistical characteristics of the traffic emitted by the devices when they connect to the network

Note: Only 94% using only textual information of the traffic emitted by the devices when they connect to the network [FMEC2019]

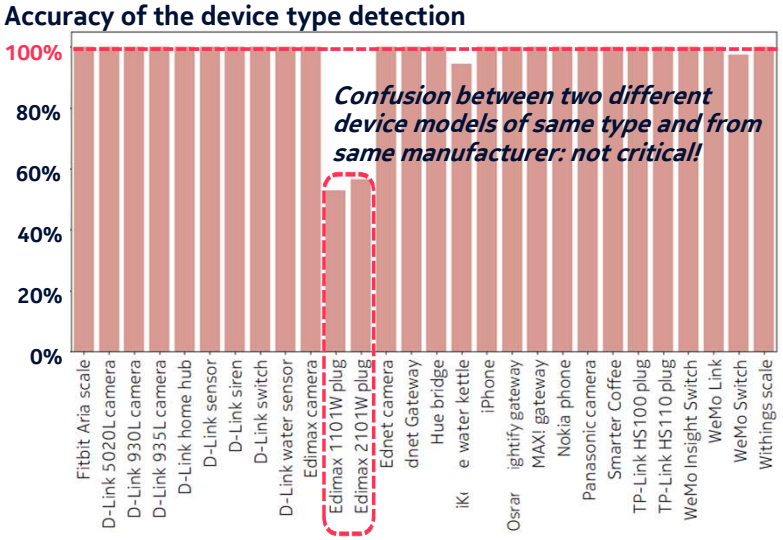
NOKIA Bell Labs

[ICC2020]

IoT device type identification performance evaluation

Evaluation on 28 devices using Decision Tree, textual + statistical traffic features

Accuracy of the device type detection

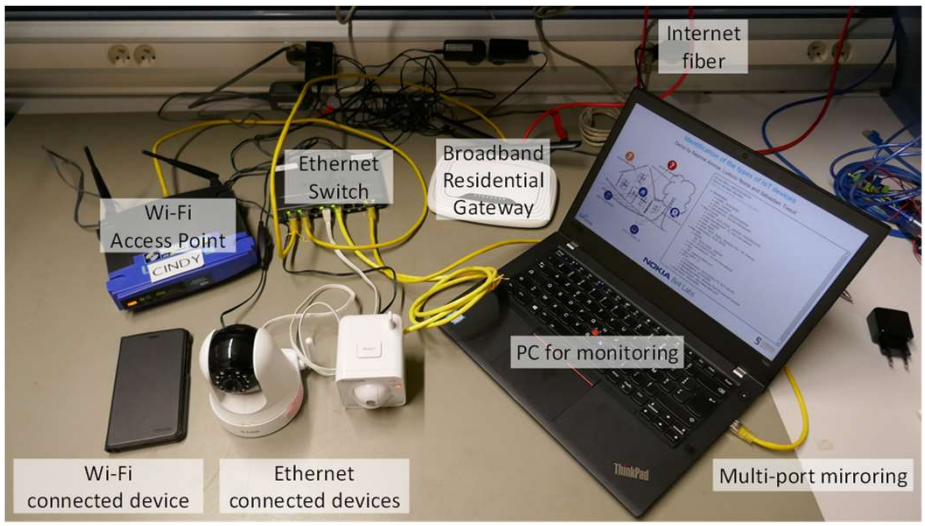


Using both textual information and statistical characteristics of the traffic emitted by the devices when they connect to the network, our machine-learning-based solution autonomously detects their types with a very high accuracy:
97% [*>99%*] accuracy *on average* with the 28 devices of our dataset

NOKIA Bell Labs

[TMA2019]

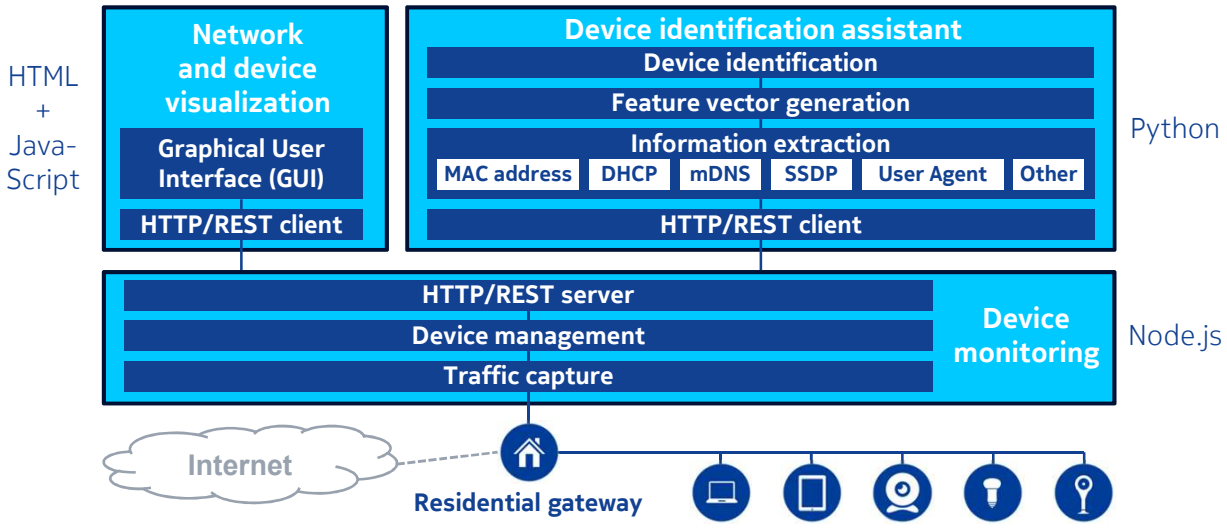
IoT device type identification demo
Experimental set-up



33

[TMA2019]

IoT device type identification demo
Prototype architecture : Software implementation

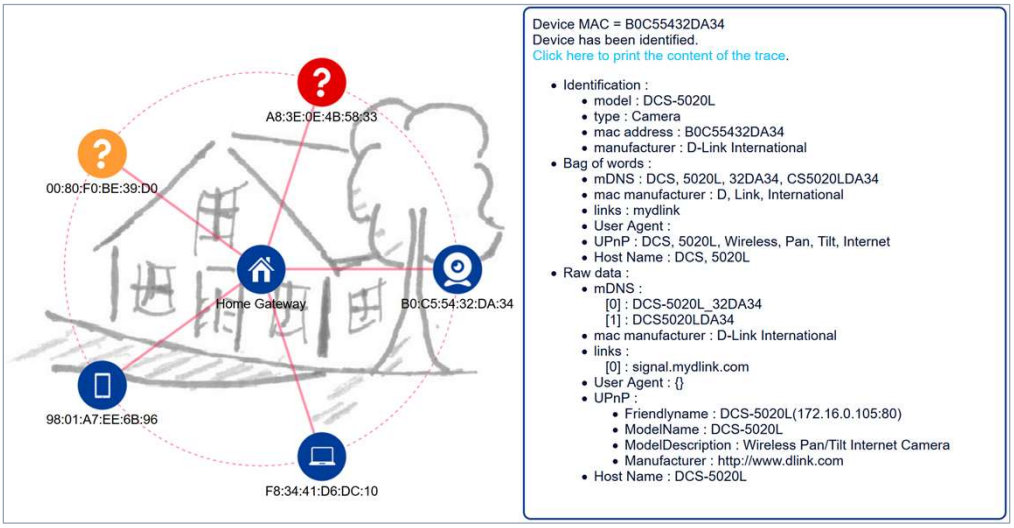


34

[TMA2019]

IoT device type identification demo

Demo GUI, with examples of textual data



Best demo award @ TMA 2019

35

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

36

Need for IoT network monitoring
Need for a generic IoT Network Monitoring architecture

Some use-cases

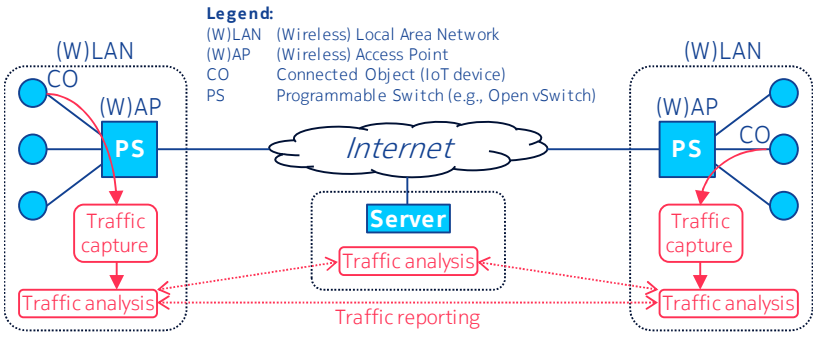
- IoT device management: “fingerprinting” of IoT devices
  - Identification of IoT device types using ML techniques on traffic generated by IoT devices
- IoT device management : anomaly detection
  - Detection of deviant traffic patterns, for faulty or malicious behavior detection
- IoT application & service management: network-protocol-based fingerprinting
  - Correlation of traffic patterns between IoT devices to identify which services/applications are used
- IoT knowledge sharing: multi-tenant aspects of distributed traffic analysis
  - Trade-off between data richness for better efficiency and privacy/security constraints
- Many other…

⇒ **Need for a generic traffic monitoring architecture for IoT network infrastructures**

Need for IoT network monitoring
Commonalities for IoT Network Monitoring

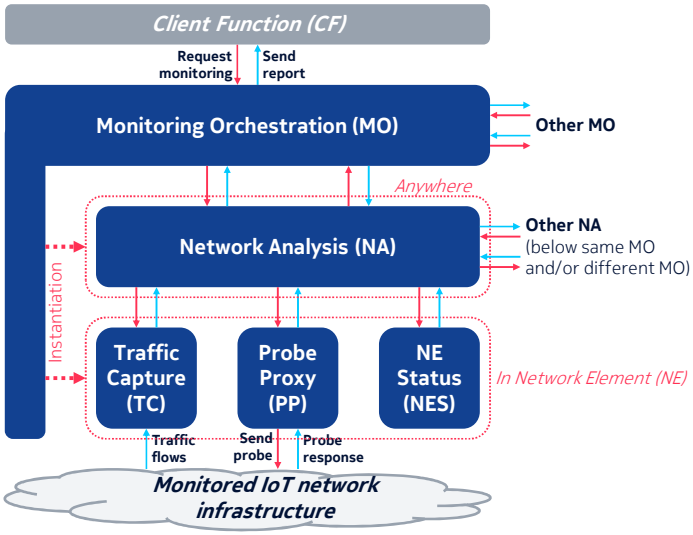
Splitting in generic functions:

- Traffic capture & Network Probe
  - Common to all use cases: each use case processes the relevant data in the traffic captures
- Traffic analysis
  - Specific to each use-case: processed data and ways to process those data
- Traffic reporting
  - Some aspects common to all use cases: privacy, security…
  - Some aspects specific to each use case: reported data
    - This will be driven by the different traffic analyses



Need for IoT network monitoring

High-level functional view of IoT Network Monitoring Architecture

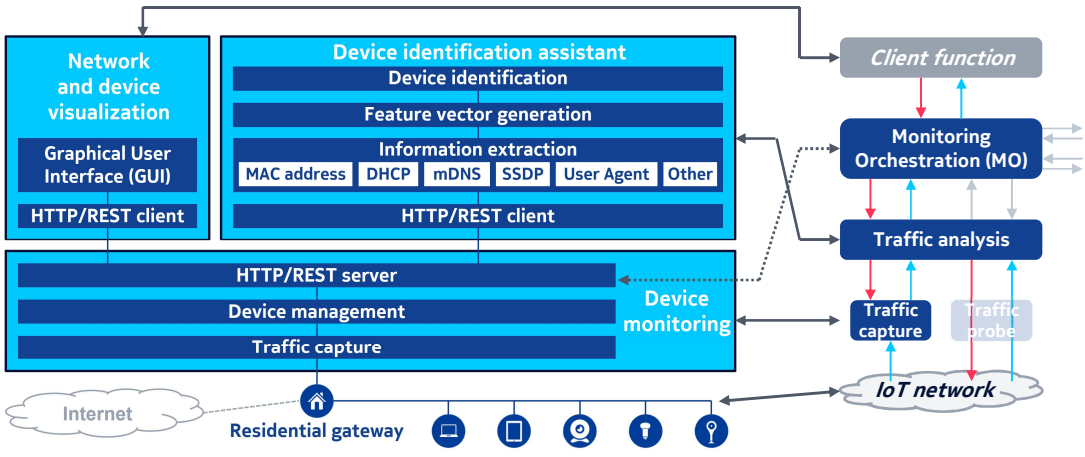


39

Need for IoT network monitoring

Autonomous IoT Device Identification Prototype – SW implementation

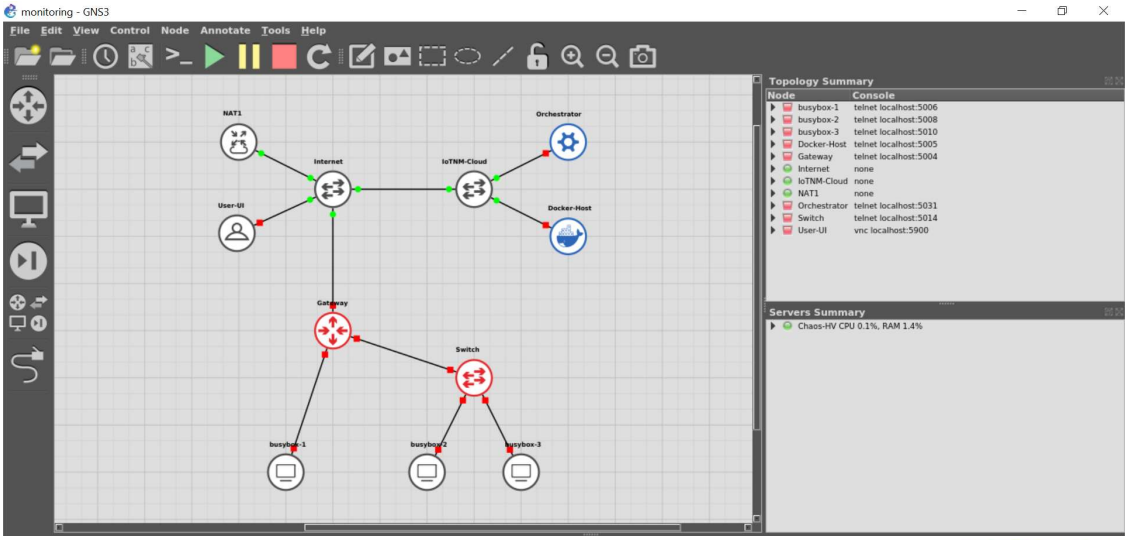
Demo implementation architecture vs. generic IoT Monitoring architecture



40

Need for IoT network monitoring

Implementation on GNS3 emulation platform (ongoing work)



41

Outline

1. Context of IoT private Network
2. SDN/cloud-based platform for IoT private networks: Future Spaces
3. IoT service recommendation
4. IoT-device-type identification
5. Need for IoT network monitoring
6. Conclusion

42

Conclusion
Control and management of IoT networks and their devices

SDN/cloud-based platform for IoT networks:

- Ease the usage of IoT devices by people: Majord'Home
- Isolation of devices: SD-LANs (micro-slicing) ⇒ security/privacy
- Collaborations of devices in multiple smart environments: Future spaces
- Security application (not shown in this presentation):
  use of Future Spaces platform with blockchains for IoT device security [WINF2019]
- Use of this platform to recommend IoT services to end-users

A specific management function: IoT network monitoring

- Required for security/privacy of IoT device usage
- Leverage on SDN/NFV/cloud for flexibility/programmability
- Example of IoT device type identification

Conclusion
Some references

SDN/NFV-based platform for IoT networks (Majord'Home / SD-LANs / Future Spaces)

[CNSM2014] M. Boussard et al., *The Majord'Home: a SDN Approach to Let ISPs Manage and Extend Their Customers' Home Networks*, CNSM/ManSDNNFV 2014, https://dx.doi.org/10.1109/CNSM.2014.7014207

[ITC2015] M. Boussard et al., *Software-Defined LANs for Interconnected Smart Environment*, ITC 27 (2015), https://dx.doi.org/10.1109/ITC.2015.33

[Soft2016] N. Le Sauze et al., *SDN in LANs: Programming the Network to Secure IoT Traffic*, Webminar IEEE Softwarization May 2016, https://sdn.ieee.org/newsletter/may-2016/sdn-in-lans-programming-the-network-to-secure-iot-traffic

[Sens2018] N. Le Sauze et al., *Future Spaces: Reinventing the Home Network for Better Security and Automation in the IoT Era*, Sensors 2018, https://doi.org/10.3390/s18092986

[WINF2019] M. Boussard et al., *STewARD:SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices*, Workshops @ INFOCOM 2019, https://doi.org/10.1109/INFCOMW.2019.8845126

IoT services management (IoT service recommendation & deployment)

[IoT2016] M. Le Pallec et al., *Physical-Interface-Based IoT Service Characterization*, IoT 2016, https://dx.doi.org/10.1145/2991561.2991567

[ICIN2017] L. Noirie et al., *Towards automated IoT service recommendation*, demo ICIN 2017, https://dx.doi.org/10.1109/ICIN.2017.7899397

[Algotel2017] N. Ammar et al., *Algorithme de Caractérisation des Services IoT: Évaluation des Performances*, ALGOTEL 2017, https://hal.archives-ouvertes.fr/hal-01515597

[ICIN2018] M. Le Pallec et al., *Digital assistance for the automated discovery and deployment of IoT services*, demo ICIN 2018, https://dx.doi.org/10.1109/ICIN.2018.8401599

[ICSE2019] A. Krishna et al., *IoT Composer: Composition and Deployment of IoT Applications*, demo ICSE 2019, https://dx.doi.org/10.1109/ICSE-Companion.2019.00028

[FMSE2019] A. Krishna et al., *Rigorous Design and Deployment of IoT Applications*, FormaliSE 2019, https://dx.doi.org/10.1109/FormaliSE.2019.00011

IoT device management (Identification of IoT device types)

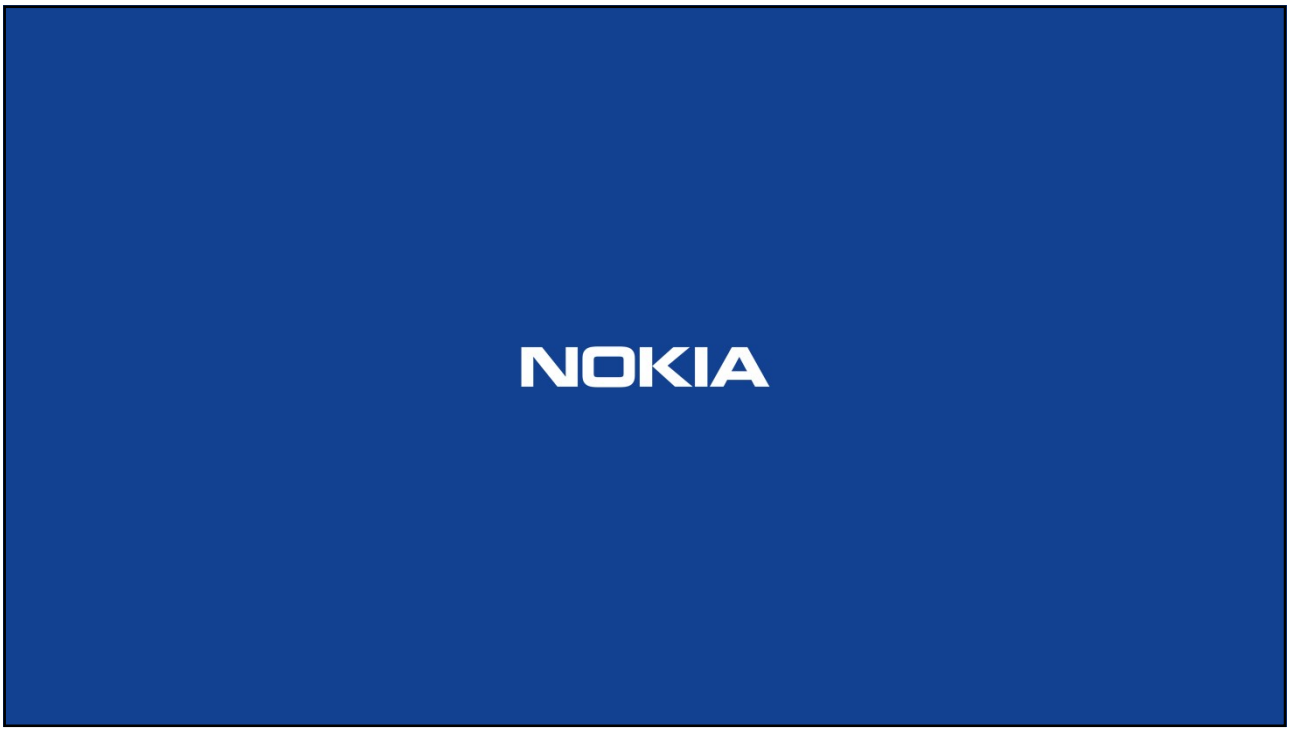
[CORES2018] N. Ammar et al., Identification du type des objets connectés par les informations des protocoles réseaux, CORES 2018, https://hal.archives-ouvertes.fr/hal-01785952

[CORES2019] N. Ammar et al., Amélioration de l'identification du type des objets connectés par classification supervisée, CORES 2019, https://hal.archives-ouvertes.fr/hal-02126555

[FMEC2019] N. Ammar et al., *Network-Protocol-Based IoT Device Identification*, FMEC/IoTNAT 2019, http://dx.doi.org/10.1109/FMEC.2019.8795318

[TMA2019] N. Ammar et al., *Autonomous IoT Device Identification Prototype*, best demo award TMA 2019, https://doi.org/10.23919/TMA.2019.8784517

[ICC2020] N. Ammar et al., *Autonomous identification of IoT device types based on a supervised classification*, ICC 2020, to be presented next week…



45