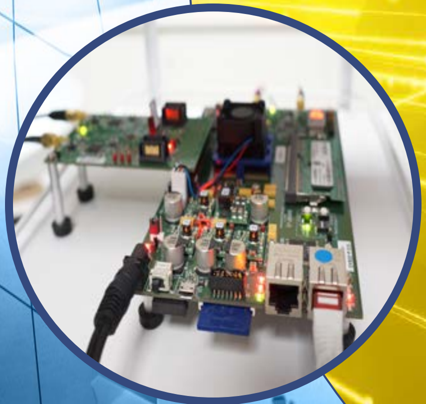
Institut d'Électronique et de Télécommunications de Rennes

IETR
INSTITUT D'ÉLECTRONIQUE ET DE TÉLÉCOMMUNICATIONS DE RENNES

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

الجامعة اللبنانية
UNIVERSITE LIBANAISE



Mobility & LPWANs

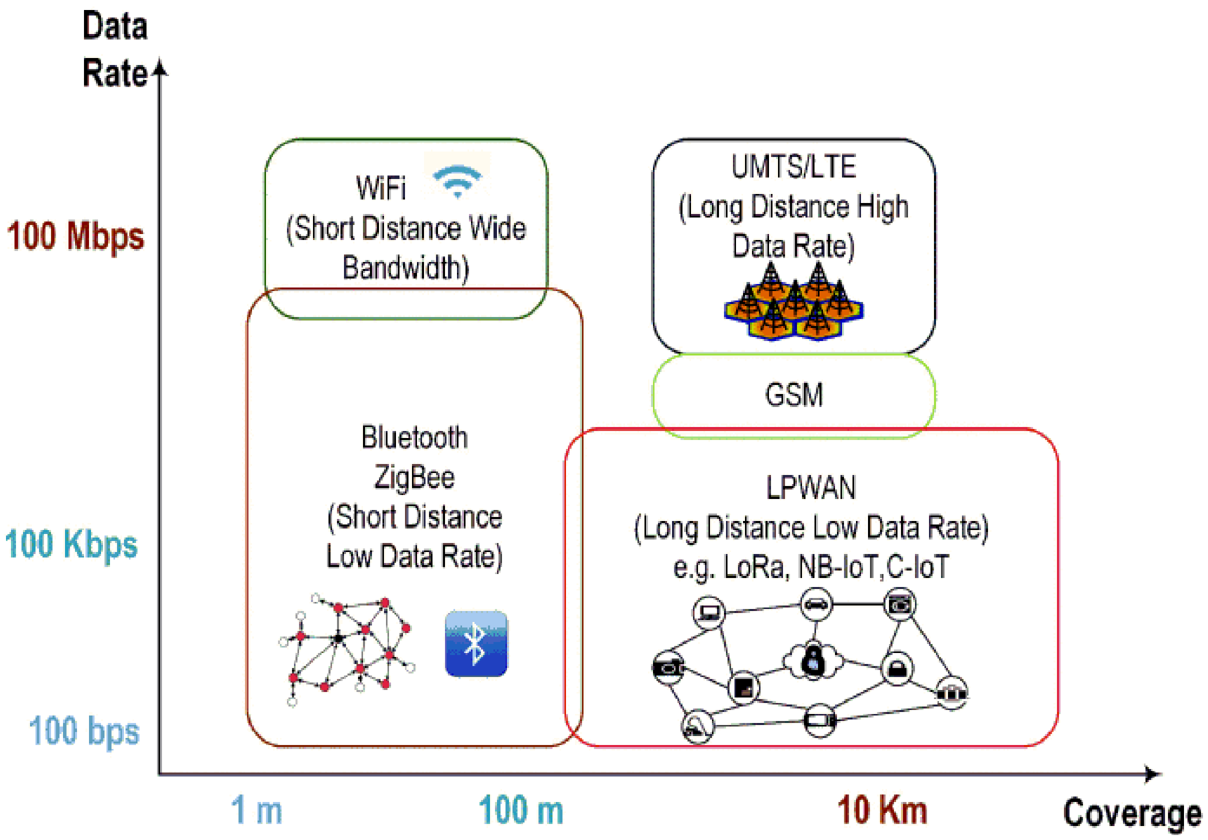
Ivan MARTINEZ, Wael AYOUB, Fabienne NOUVEL, Philippe Tanguy, A.SAMHAT, M. MROUE, J.C. PREVOTET

1/04/2019

Introduction

INSTITUT D'ÉLECTRONIQUE ET DE TÉLÉCOMMUNICATIONS DE RENNES

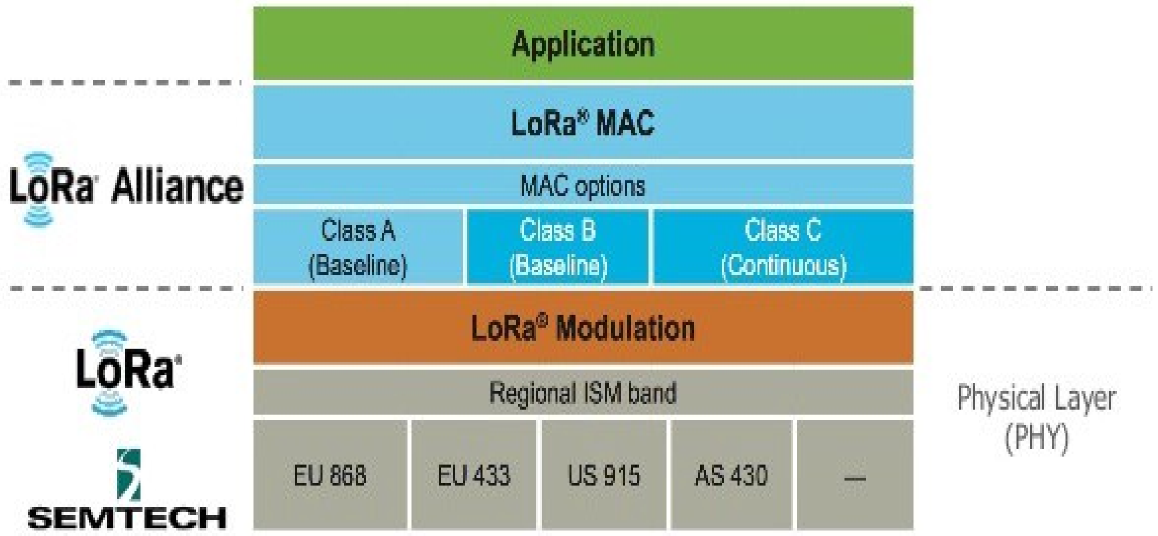
- We work on IoT mobility and on IoT Cybersecurity.
- Focus on LPWAN Networks : LoRaWAN, DASH7 and NbIoT.
- LPWAN are characterized by long-range communication and low power consumption.
- Mobility earns a considerable percentage in IoT applications and research in: smart cities, health-care, smart.
  - 2 Mobility's schemes :
    - *in one LPWAN : intra-mobility*
    - *between LPWANs : inter-mobility*
- Cybersecurity represents a big issue in most IoT use-cases.
  - Jamming attacks at PHY Level



INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

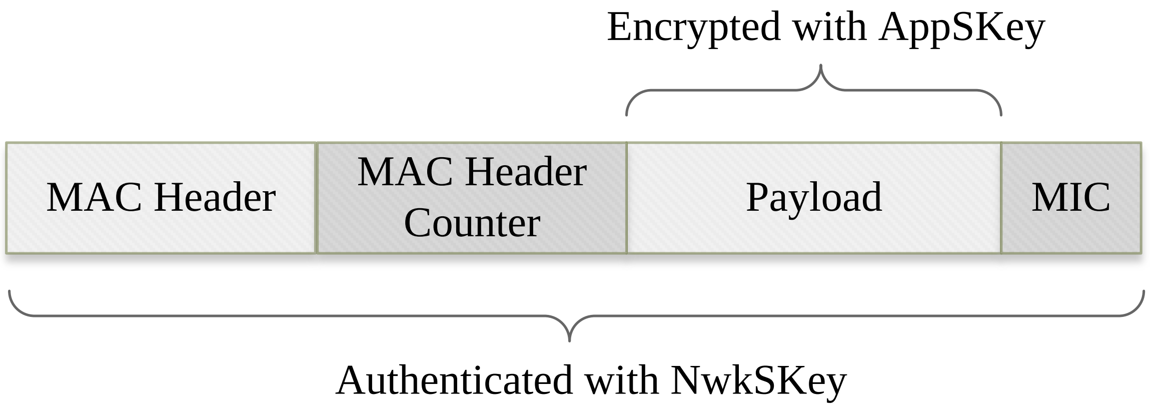
الجامعة اللبنانية
UNIVERSITE LIBANAISE

Introduction LoRaWan

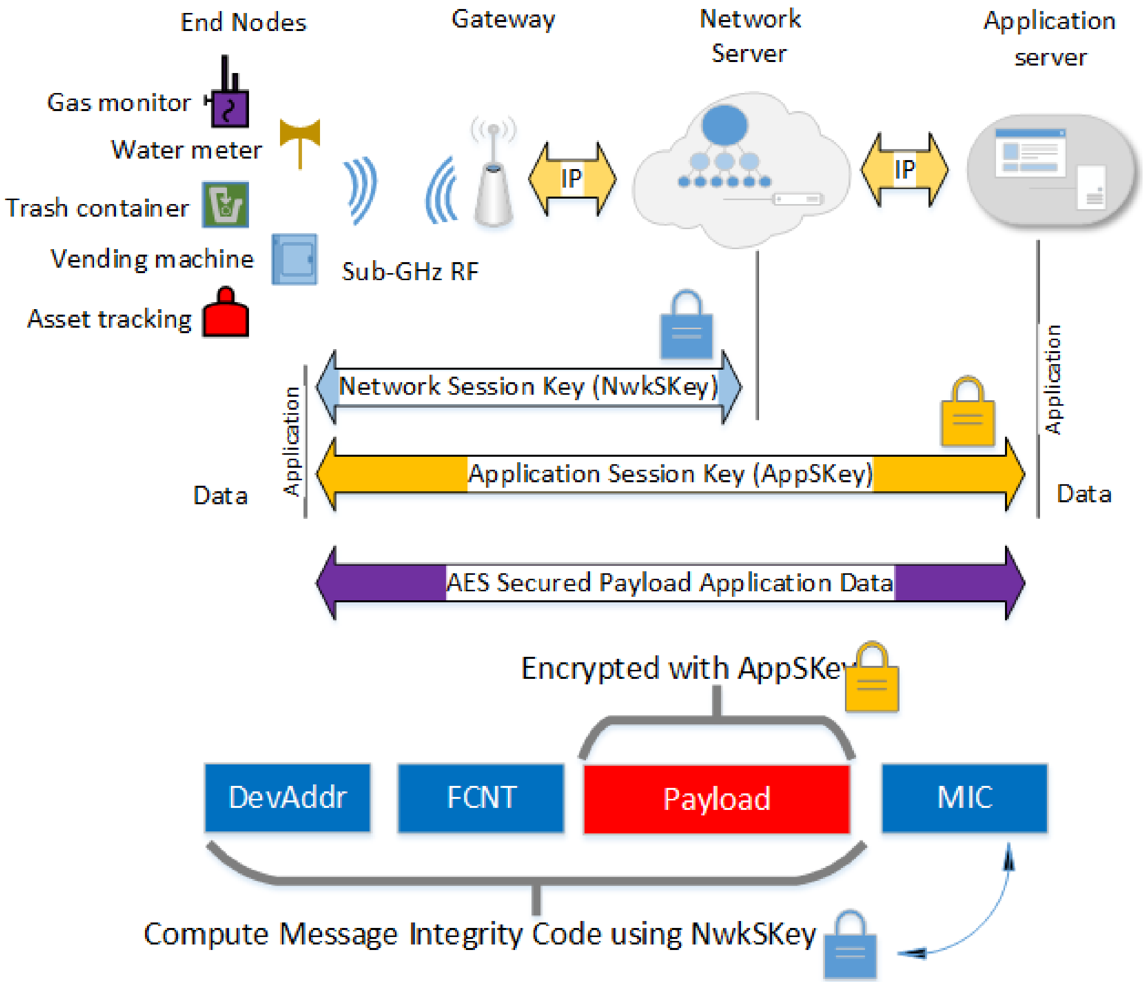


- **Class A (baseline)**
  - The end device decides whether it sends data or not based on its own schedule
  - Each uplink transmission is followed by two receive windows
  - Downlink data is only allowed after an uplink event has been made
- **Class B (Beacon Enabled)**
  - Allows more downlink receive windows at scheduled times
  - The gateway sends a beacon frame allowing synchronization
- **Class C (Always listening)**
  - The end-device can receive windows without waiting for a beacon signal

Introduction LoRaWan : MAC Security

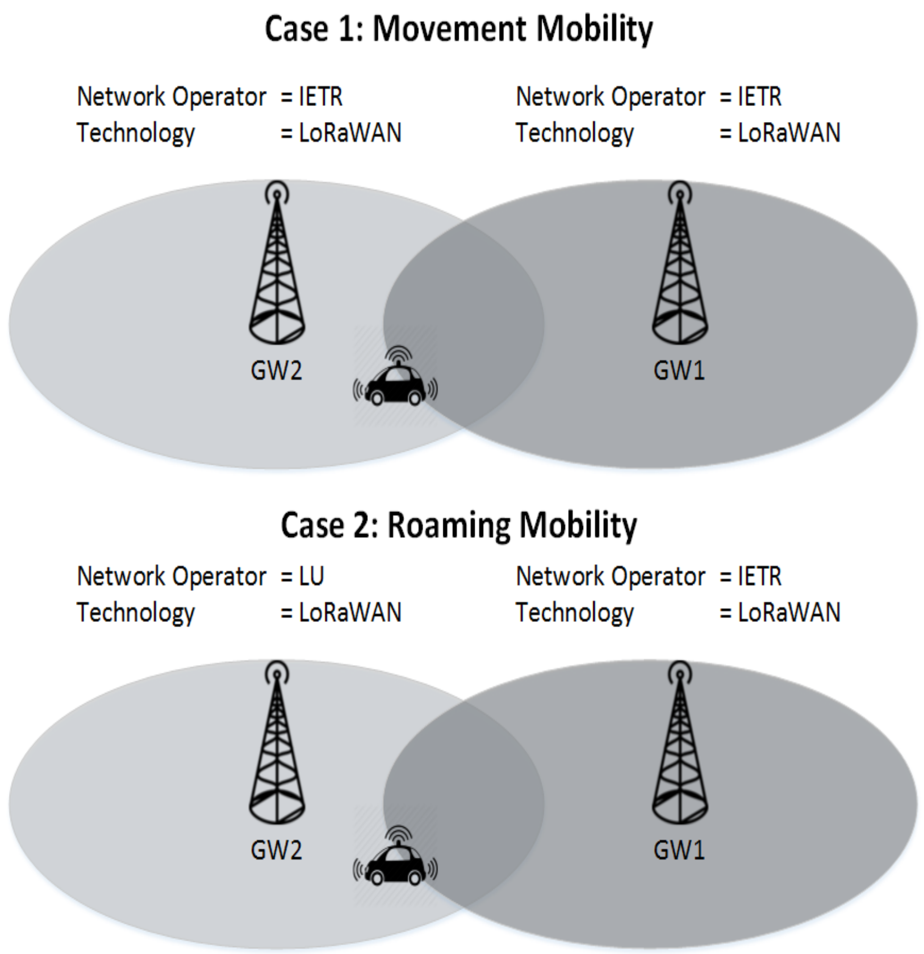


- End to end Encryption of the payload
- End-device to network Integrity



Mobility

- Mobility in IoT refers to ensuring the delivery of information on demand to Application during mobility/moving of the Device.
- Mobility between two operators has not been addressed yet in IoT. Until now, device is assigned to a one operator and cannot be assigned to another.
- We focus on the Roaming mobility while keeping session with Application.
- One of the solutions for heterogeneity, mobility, etc. is a level that can be common and hides all these differences.
- We found that IPv6 can be a solution. But IPv6 cannot be ran over constrained nodes. A compress mechanism needed to achieve short messages



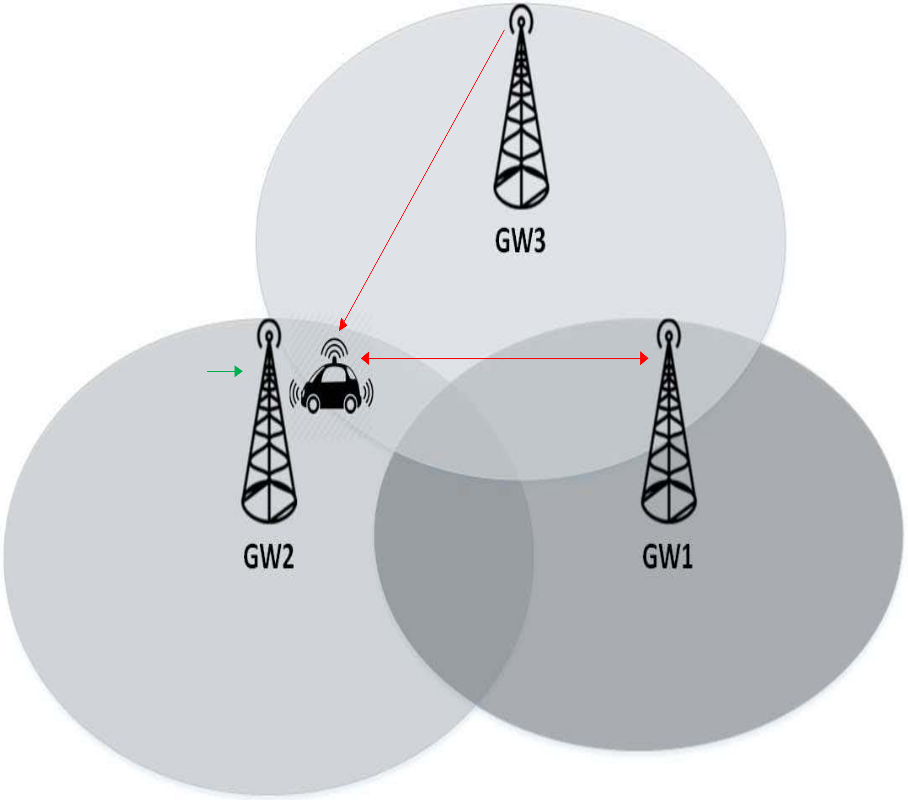
Mobility : scenario

Step 1:
At startup, a broadcast message will be transmitted. Only GW1 will ACK.

Step 2:
As ACK received for each transmit, car will stay associate with GW1.

Step 3:
1- No ACK received for the transmit.
2- Message repeated in broadcast.
3- GW3 and GW2 will ACK.
4- Car selects GW2.
RSSI(GW2)>RSSI(GW3).

Step 4:
As ACK received for each transmit, car will stay associate with GW2.



IPv6 and compression/mobility

- IPv6 offers several features and arguments in the future of IoT.
- Main features of IPv6:
  - Scalability
  - Overcomes the NAT barriers in IPv4
  - Multiple IP addresses per device according the scenario
  - Group operation and Multicast
  - Mobility, session continuity and interoperability
  - Stateless Address Auto-configuration (SLAAC)

IPv6 and compression/mobility

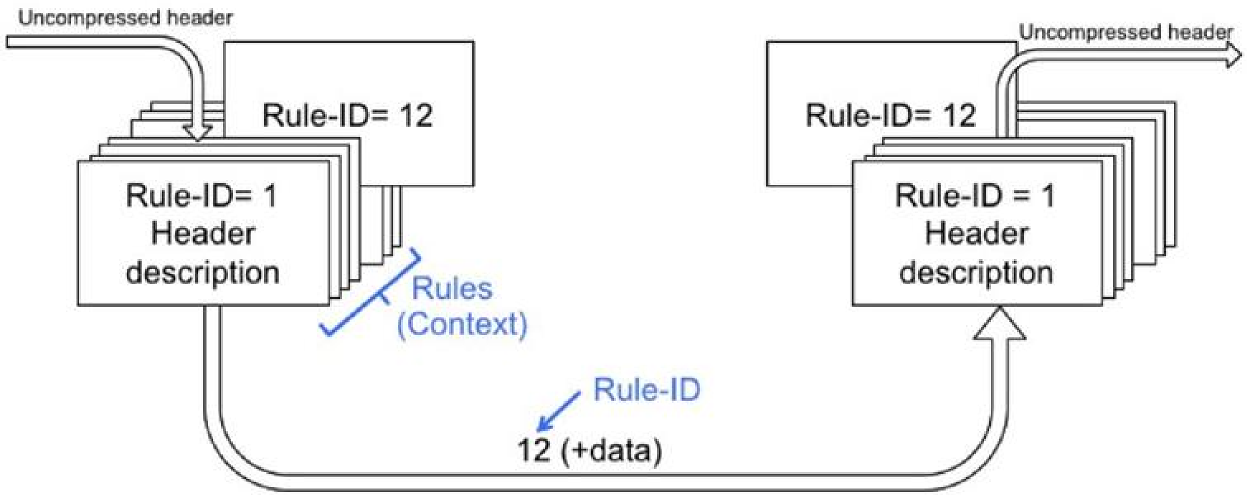
- IPv6 drawbacks in the future of IoT :
  - Length of IP header
  - IP addresses defined in or our of the local network
  - Solutions for mobility but with no restrictions for length

- Available set of complementary standards for IoT needs :
- 6LoWPAN, 6Lo, 6TiSCH, ROHC, IPHC and NHC, ROLL and RPL, SCHC.

Among these solutions 6LoWPAN and SCHC most applicable with LPWAN.

SCHC compression

- Static Context Header Compression (SCHC) is a header compression scheme that supports fragmentation level.
- Executed between l2 and l3 layer to compress the IPv6/UDP/CoAP headers into Rule ID
  - => (size of 1-2 bytes)
- Forward the data to lower layers.
- If data does not fit in one N2 frame
  - => fragmentation mechanism is applied

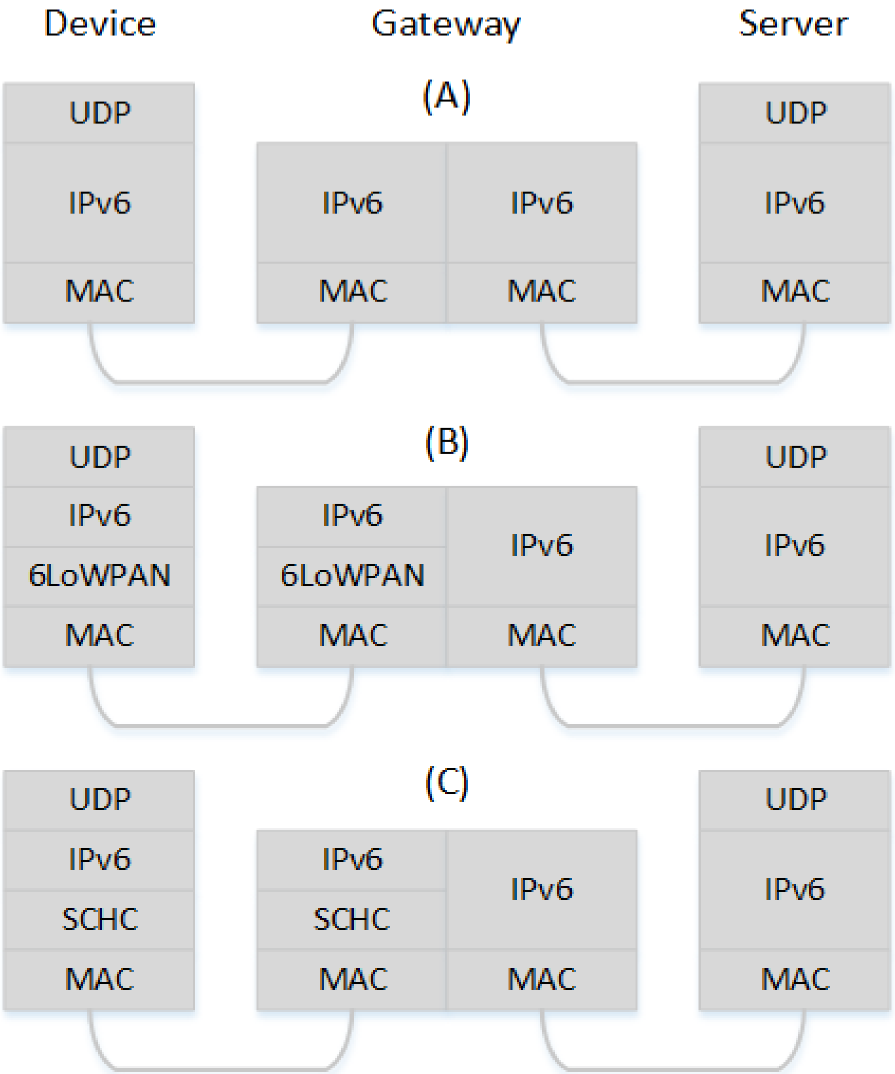


6LoWPAN/SCHC Comparison

- To evaluate the performance of the SCHC protocol, we performed three simulation scenarios:
  - In scenario A, packets transmitted without compression.
  - In scenario B, packet headers are compressed using 6LoWPAN compression.
  - In scenario C, the headers are compressed using the SCHC compression.
- In the three scenarios,

a ping from the device to server passing by the gateway.

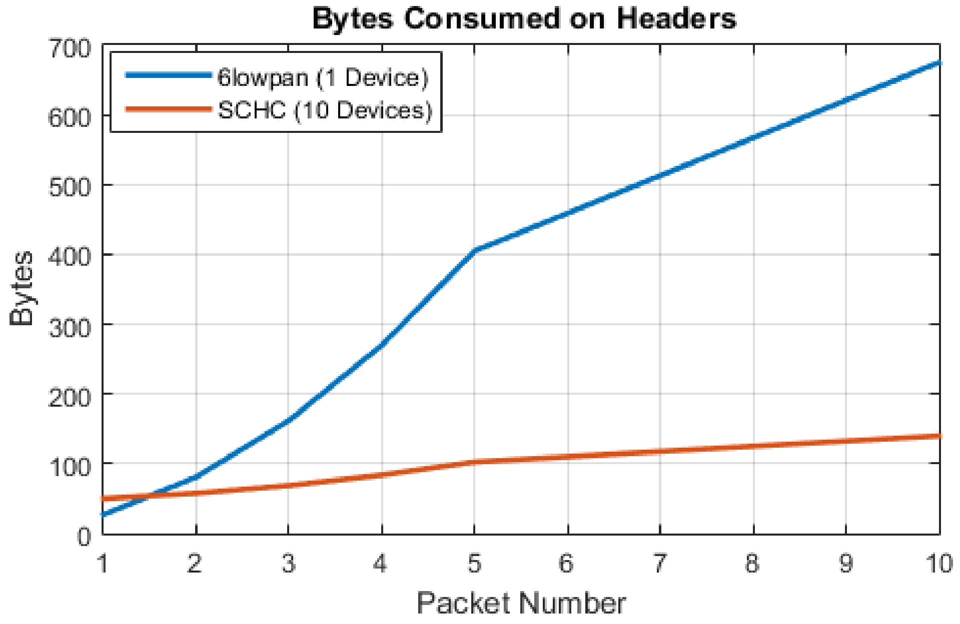
We consider the ruleID (3 bits) & the compression headers space (n bits) together as a header.



Comparison Results

- Even with the use of header compression, the size of headers is considerable. To show the amount of these bytes, we set at the gateway a byte counter to count the headers size generated by each standard after the transmission of 10 packets. We compare one 6LoWPAN device with ten SCHC devices. The results show that more than 600 bytes are consumed as headers to transmit ten packets. While ten devices using SCHC standard consume less than 150 bytes.

Scenario	A:IPv6	B:6LoWPAN	C:SCHC
Data rate	high	medium	low
Memory Usage	low	low	High
Mobility support	Yes	Yes	No
Interoperability	Yes	Yes	Specific technologies
Scalability	Yes	Yes	No
Network topology	Mesh	Mesh/star	Star
Header compression	no compression	>6 bytes <37 bytes	>1 bit <6 bytes
48 bytes header compression	48 bytes	27 bytes	5 bytes then 3 bits
Compression gain	0%	43%	90%

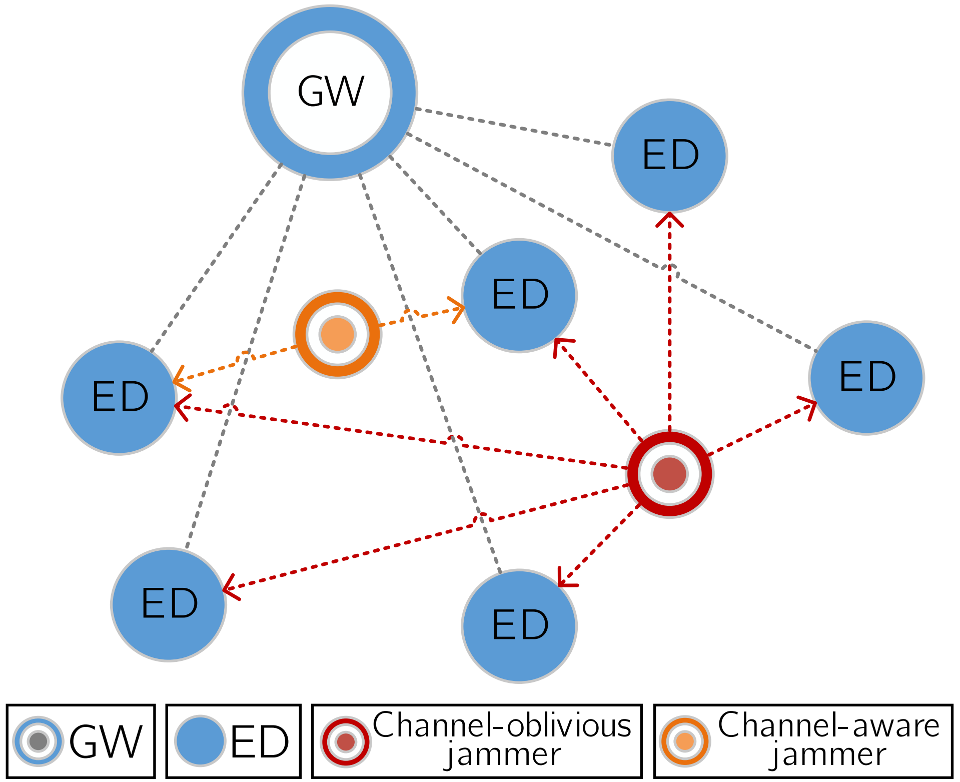


Cybersecurity

- Cybersecurity in IoT refers to the protection of internet-connected things, it can be addressed at different levels: application, information, **network**, end-user.
- We focus on Network Security and more specifically on security issues on PHY level.
- Our motivation is to propose a security framework dedicated to LoRaWAN networks to help designers to integrate cybersecurity threats at low level at an early development stage
  - Fisrt step: Performance evaluation of **LoRaWAN Networks under jamming attacks**.

Jamming Attacks

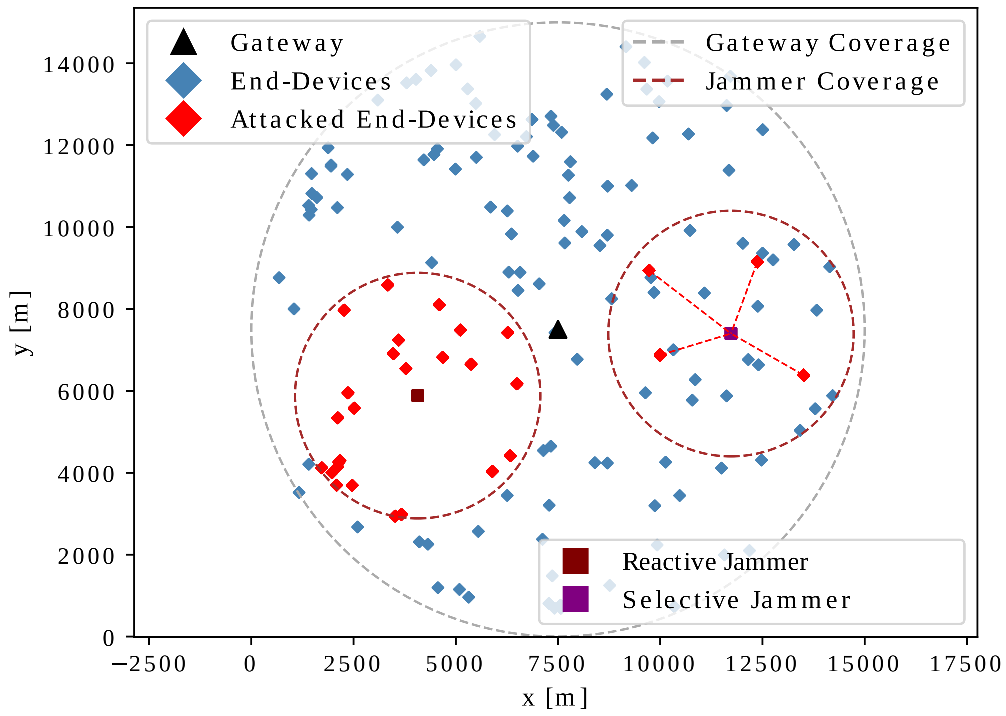
- We consider two categories of Jammers:
  - Channel-aware : Is able to sense the network and perform reactive attacks.
  - Channel-oblivious : It sends unauthenticated packets on the network in order to disrupt the communication of EDs and GWs on a regular basis.



Performance Evaluation

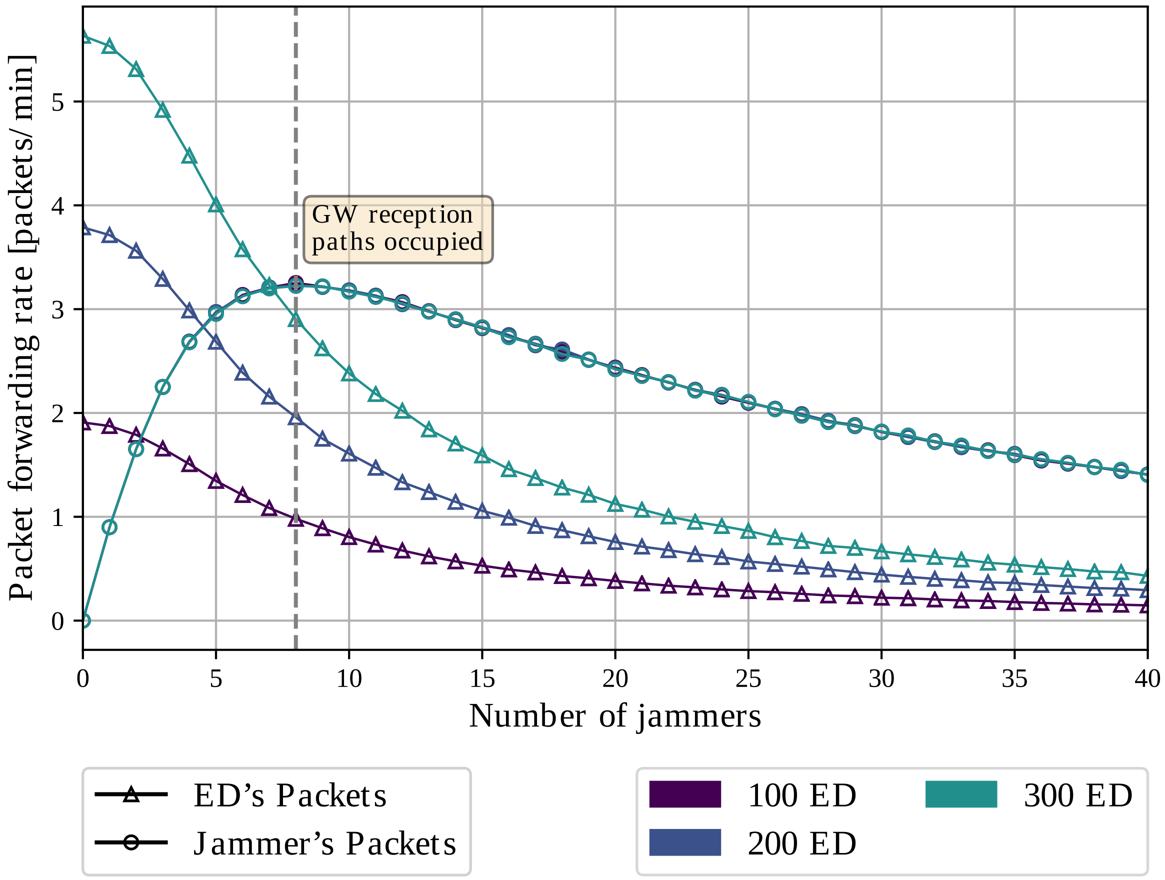
- We evaluate the performance impact of a LoRaWAN Network in the presence of Jamming Attacks.
- We follow a simulation approach:
  - Event oriented simulations – NS-3
  - Evaluation of GW and ED side metrics

Simulation Scenario



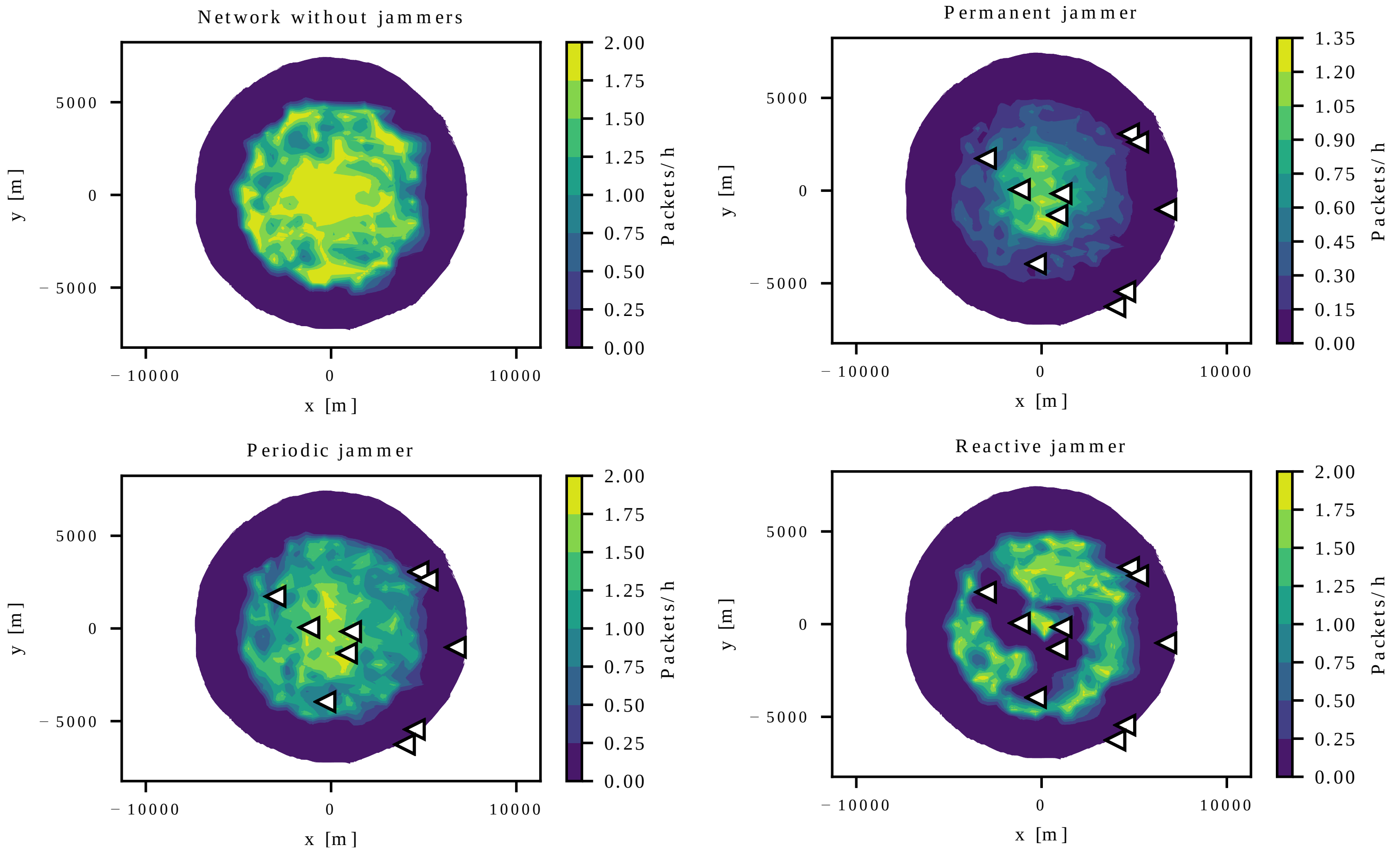
Performance impact – GW side

- We evaluate the impact of permanent jammers on the GW performance.
  - A LoRaWAN cell with 1 GW and we vary the number of EDs from 100 to 300 was simulated.
  - The number of permanent jammers vary from 1 to 40.
- Here, we show the amount of packets processed by the GW comming from EDs and Jammers



Performance impact – ED side

- We evaluate the impact of channel-aware and channel oblivious jammers on ED throughput.
  - A LoRaWAN cell with 1 GW and 1000 ED.
  - 10 jammers of each type.
- Here, we show the throughput from a geographical point of view



References

[1] P. Patel, M. I. Ali, and A. Sheth, “On using the intelligent edge for iot analytics,” IEEE Intelligent Systems, vol. 32, pp. 64–69, September 2017.

[2] R. Morello, S. C. Mukhopadhyay, Z. Liu, D. Slomovitz, and S. R. Samantaray, “Advances on sensing technologies for smart cities and power grids: A review,” IEEE Sensors Journal, vol. 17, pp. 7596–7610, Dec 2017.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of things for smart cities,” IEEE Internet of Things Journal, vol. 1, pp. 22–32, Feb 2014.

[4] G. Z. Papadopoulos, V. Kotsiou, A. Gallais, G. Oikonomou, P. Chatzimisios, T. Tryfonas, and T. Noel, “A mobility-supporting mac scheme for bursty traffic in iot and wsns,” in 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6, Dec 2016.

[5] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.

[6] P. Hank, S. Mller, O. Vermesan, and J. V. D. Keybus, “Automotive ethernet: In-vehicle networking and smart mobility,” in 2013 Design, Automation Test in Europe Conference Exhibition (DATE), pp. 1735– 1739, March 2013.

[7] Y. Shibata and G. Sato, “Iot based mobility information infrastructure in challenged network environment toward aging society,” in 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 645–648, March 2017.

[8] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, “Lightweight mobile ipv6: A mobility protocol for enabling transparent ipv6 mobility in the internet of things,” in 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2791–2797, Dec 2013.

[9] M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara, “A network mobility solution based on 6lowpan hospital wireless sensor network (nemo-hwsn),” in 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 433–438, July 2013.

[10] N. A. Surobhi and A. Jamalipour, “An iot-based middleware for mobility management in post-emergency networks,” in 2014 21st International Conference on Telecommunications (ICT), pp. 283–287, May 2014.