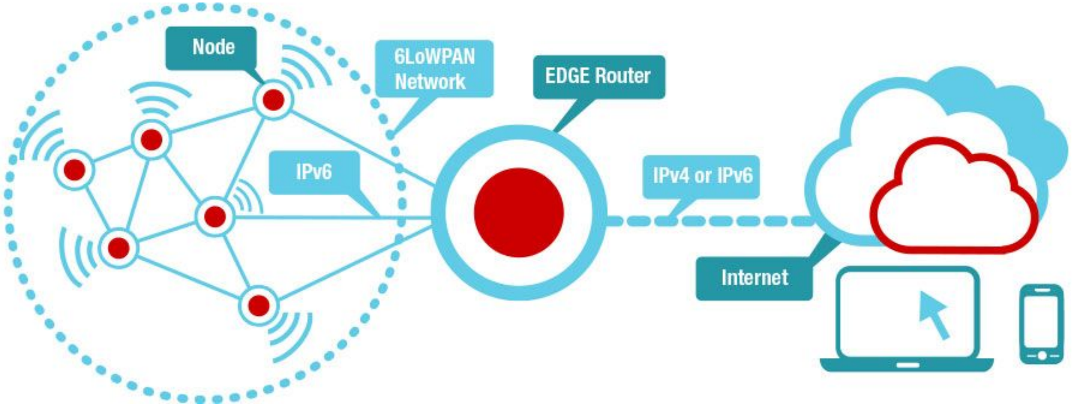
6LoWPAN Security/Attacks

By Derek Li and Danilo Torres Fleites

What is 6LoWPAN?

- Acronym for IPv**6** over **Lo**w power **W**ireless **P**ersonal **A**rea **N**etworks
- **Network standard** that allows for the efficient use of IPV6 over low-power wireless networks on the simplest of embedded devices
- Internet of Things! Smart Houses!



https://zolertia.io/6lowpan-iot-protocol/

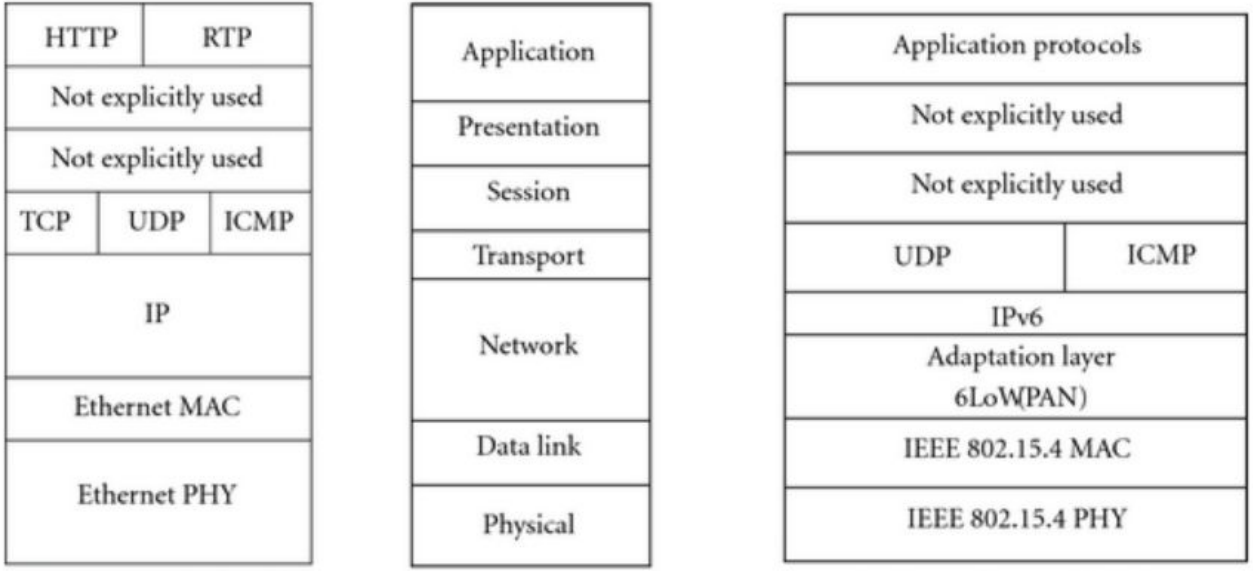
6LoWPAN Timeline

- The Internet Engineering Task Force (IETF) 6LoWPAN working group was officially started in 2005
- The first 6LoWPAN specifications were released in 2007 (RFC 4919)
- It is not very widely used in the present day as it is still a fairly new idea (it provides efficiency for very modern applications that were not needed before)
- As we aim to incorporate all of our devices in an Internet of Things, 6LoWPAN becomes more necessary

More on 6LoWPAN

- Defines encapsulation and **header compression** mechanisms that allows IPV6 packets to be transferred over IEEE 802.15.4 based networks:
- Common values are compacted.
- The version is always IPv6 so the field is not needed
- Traffic Class and Flow Label are always 0.
- Payload length defined by link header
- Src/Dst addresses can be compressed

TCP/IP Protocol Vs 6LoWPAN Protocol



HTTP | RTP

Not explicitly used

Not explicitly used

TCP | UDP | ICMP

IP

Ethernet MAC

Ethernet PHY

TCP/IP protocol stack

Application

Presentation

Session

Transport

Network

Data link

Physical

ISO/OSI layer

Application protocols

Not explicitly used

Not explicitly used

UDP | ICMP

IPv6

Adaptation layer 6LoWPAN)

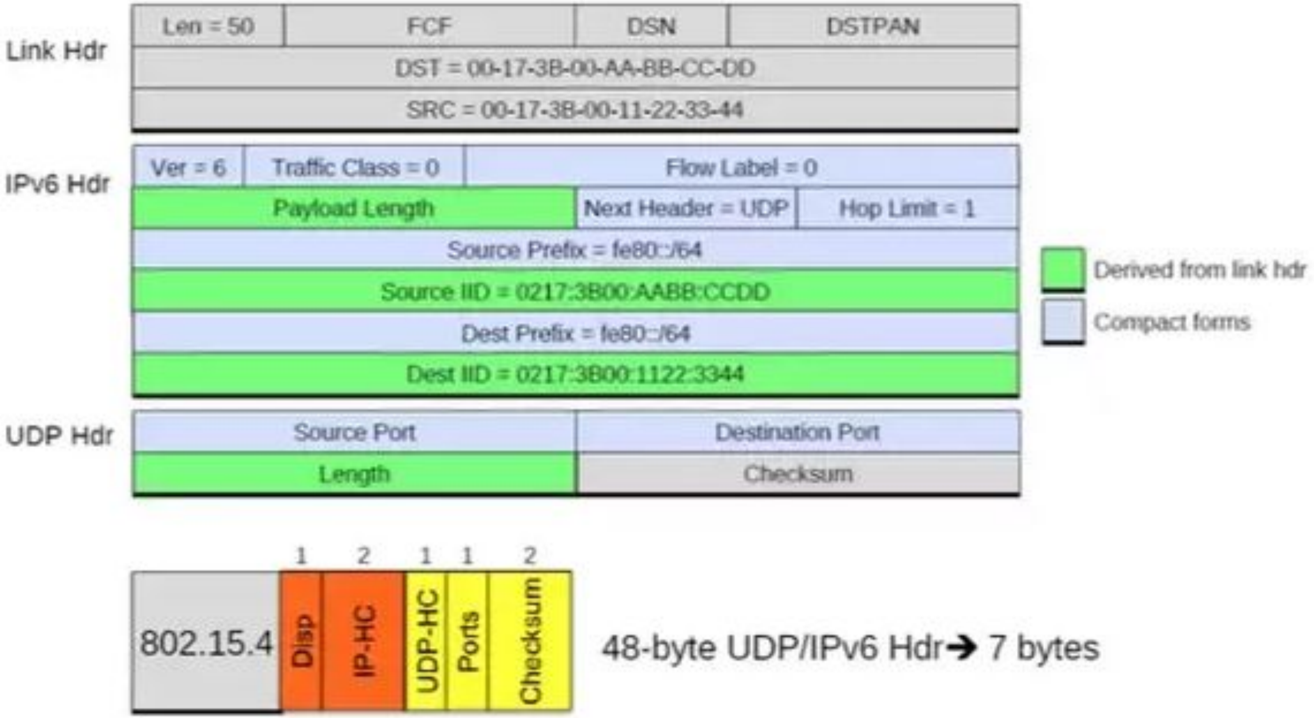
IEEE 802.15.4 MAC

IEEE 802.15.4 PHY

6LoWPAN protocol stack

https://www.hindawi.com/journals/jcnc/2012/316839/fig2/

Header Compression



Link Hdr

Len = 50 | FCF | DSN | DSTPAN

DST = 00-17-3B-00-AA-BB-CC-DD

SRC = 00-17-3B-00-11-22-33-44

IPv6 Hdr

Ver = 6 | Traffic Class = 0 | Flow Label = 0

Payload Length | Next Header = UDP | Hop Limit = 1

Source Prefix = fe80::/64

Source IID = 0217:3B00:AABB:CCDD

Dest Prefix = fe80::/64

Dest IID = 0217:3B00:1122:3344

UDP Hdr

Source Port | Destination Port

Length | Checksum

🟩 Derived from link hdr

▭ Compact forms

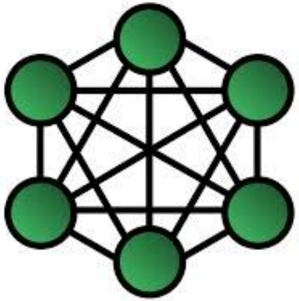
	1	2	1	1	2
802.15.4	Disp	IP-HC	UDP-HC	Ports	Checksum

48-byte UDP/IPv6 Hdr→ 7 bytes

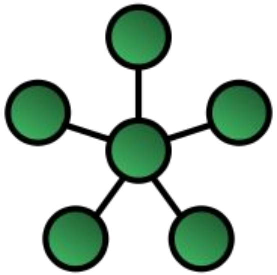
https://www.quora.com/Which-fields-are-compressed-in-a-header-compression-in-6LoWPAN

More on 6LoWPAN

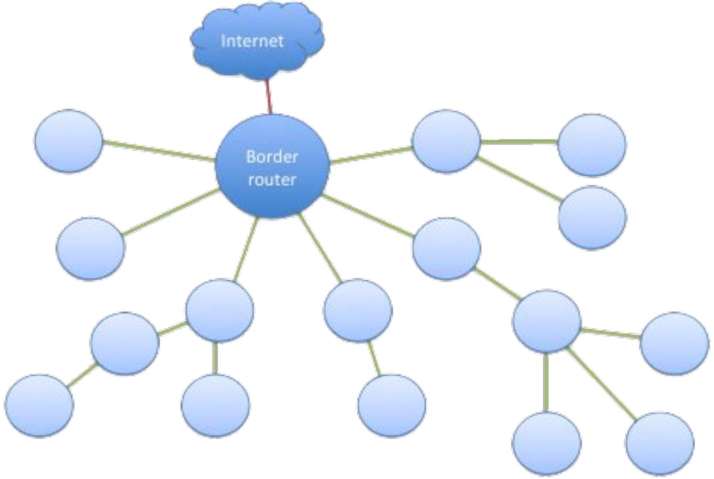
- 6LoWPAN uses either a **mesh** or **star** topology, or a combination of both
- Mesh: all nodes cooperate to distribute data amongst each other
- Star: all nodes communicate with one central point



mesh



star



https://os.mbed.com/docs/mbed-os/v5.6/tutorials/mesh.html

Characteristics of 6LoWPAN

- Small packet size (16-bit MAC addresses instead of 48)
- Offers low bandwidth, generally anywhere between 20/40/250 kbps.
- Usually battery operated
- Very affordable

Pros and Cons

Pros:

- **Massively scalable** (since it is IPv6)
- Ease of **integration** (easily communicates with other protocols)
- Efficient communication between low-powered devices

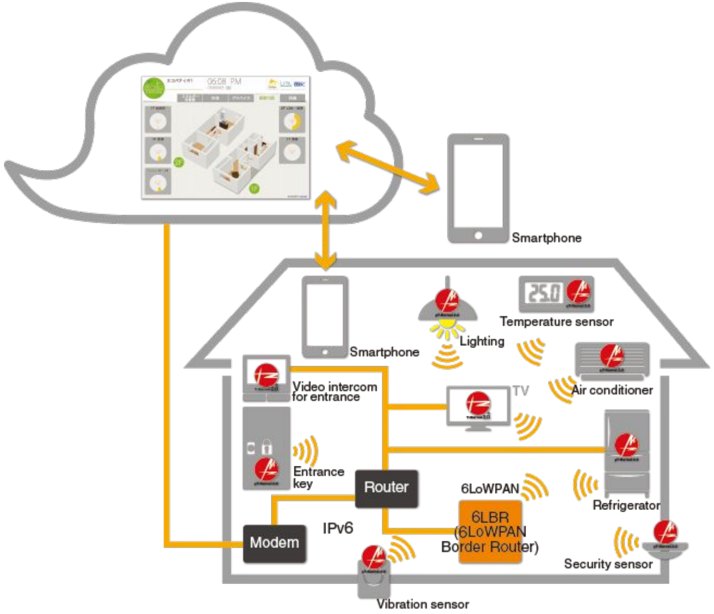
Cons:

- Unlike ZigBee (it's closest competitor), nodes cannot mostly stay in sleep mode, affecting battery life
- A lot of potential for hackers to get access into your devices and other private networks

Applications of 6LowPAN

6LowPAN can be used in the following areas:

- General automation (i.e. small connected automated devices such as sensors)
- Smart Homes
- Smart Grids (measuring and controlling energy usage)
- Industrial Monitoring - Automated factories and industrial plants



https://www.uctec.com/en/6lowpan/6lowpan-w/

Why Use it Over Bluetooth?

- You need to develop some SW to transfer data from BLE to IP and to map BLE addresses to IP
- For 6LoWPAN, the devices already have their own IP address, so you only need to bridge the MAC/Phy
- BLE is single hop, so if your devices are out of radio range of the bridge there is nothing you can do
- Whereas in 6LoWPAN you can add a router to form a mesh network

6LoWPAN

IPv6-based Low-power
Wireless Personal Area Networks

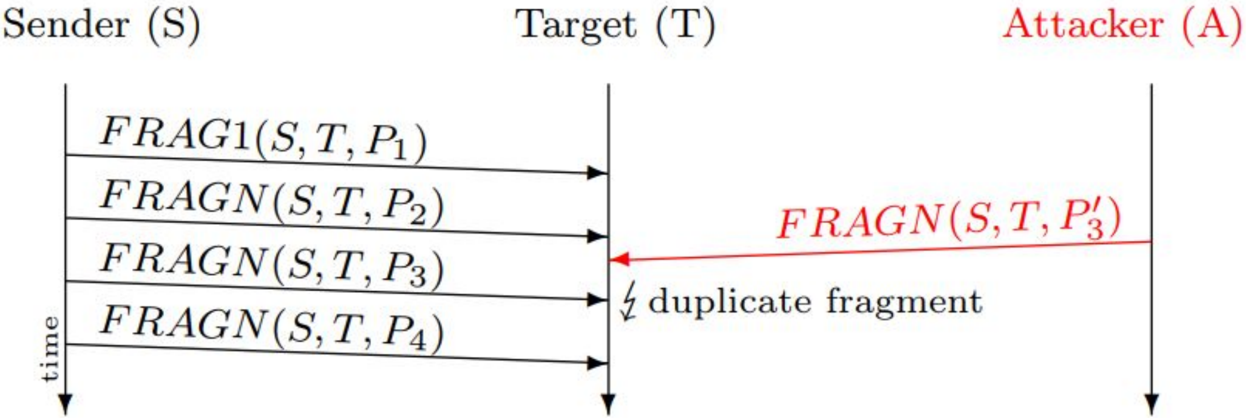
6LoWPAN Security and Attacks

6LoWPAN Vulnerabilities

- IPv6 and IPsec was not meant for low-resource devices
- No IPsec
    - No verification
    - Tampering
    - Replay Attacks
    - No encryption

Fragmentation Duplication Attack

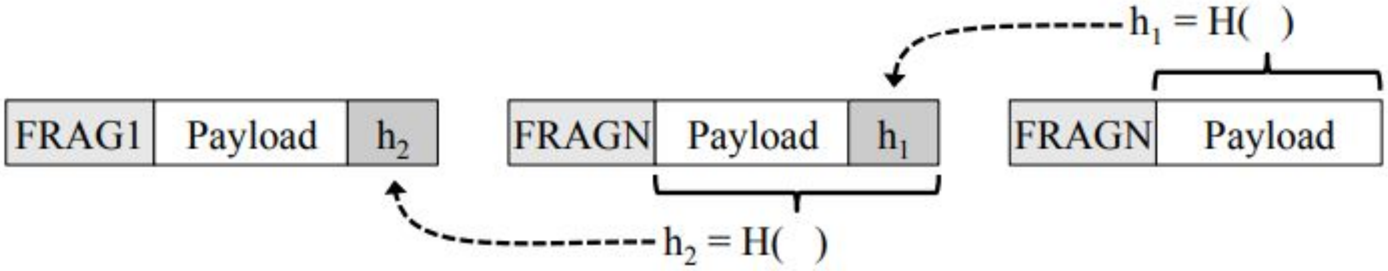
- No IPsec => devices cannot verify if a fragment is from the original sender
- The recipient cannot distinguish between legitimate or spoofed fragments
- 6LoWPAN will drop the entire packet is a corrupt fragment is received



https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-hummen-6lowpan.pdf

Content Chaining

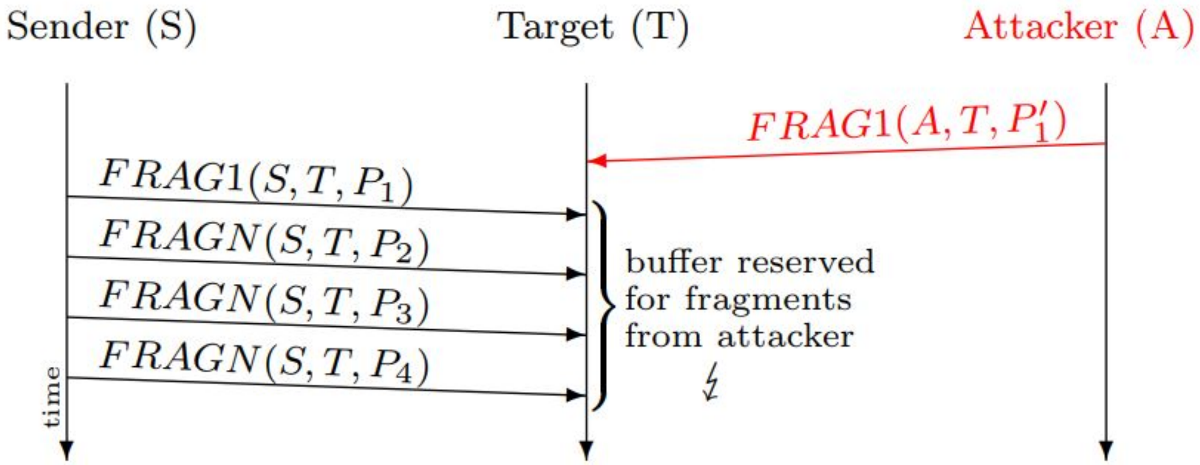
- Attach a ICV or MAC to every fragment
- Per-fragment verification



https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-hummen-6lowpan.pdf

Buffer Reservation Attack

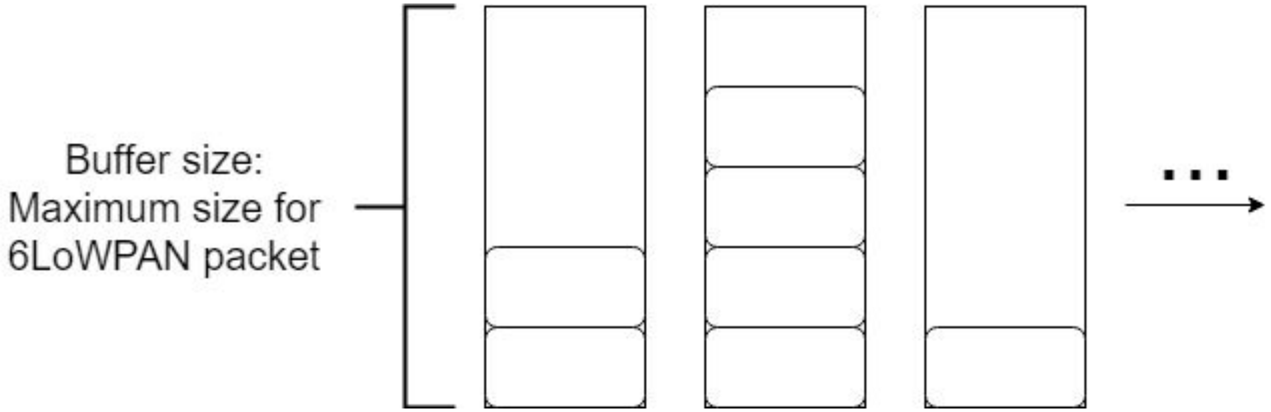
- If a fragment is received, the device optimistically reserves buffer space for the packet
- Other fragments are dropped if the buffer is reserved



https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-hummen-6lowpan.pdf

Fragment-Sized Buffer Slots

- Have multiple buffers the size of the maximum packet size
- Does not allow one packet to take up entire buffer
- Discard packets if all buffers are taken



Packet Discard Strategy

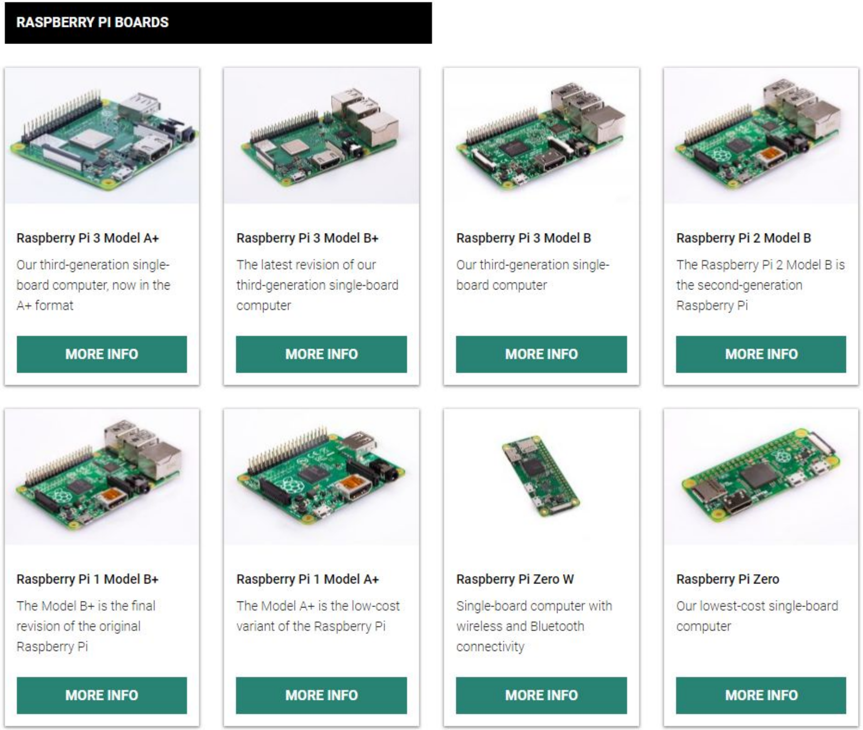
- Suspicious packets:
  - Send first fragment and skip the rest
  - Send multiple first fragments to take up as many buffers as possible
  - Send fragments very slowly
  - Rate of fragments coming in is drastically changed

Key Management System (KMS)

- 6LoWPAN devices cannot use public key infrastructure because of the energy consumption of the various processes
- Able to do private key cryptography
- Use a nearby computer to exchange public keys and create a shared secret

Other Ways to Improve Security

- Intrusion Detection Systems
- TLS on higher level protocols
- More powerful microcontrollers



RASPBERRY PI BOARDS

Raspberry Pi 3 Model A+
Our third-generation single-board computer, now in the A+ format

Raspberry Pi 3 Model B+
The latest revision of our third-generation single-board computer

Raspberry Pi 3 Model B
Our third-generation single-board computer

Raspberry Pi 2 Model B
The Raspberry Pi 2 Model B is the second-generation Raspberry Pi

Raspberry Pi 1 Model B+
The Model B+ is the final revision of the original Raspberry Pi

Raspberry Pi 1 Model A+
The Model A+ is the low-cost variant of the Raspberry Pi

Raspberry Pi Zero W
Single-board computer with wireless and Bluetooth connectivity

Raspberry Pi Zero
Our lowest-cost single-board computer

https://www.raspberrypi.org/products/

Thank y'all

- https://www.raspberrypi.org
- https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-hummen-6lowpan.pdf/
- https://www.researchgate.net/publication/261160546_Analytical_study_of_security_aspects_in_6LoWPAN_networks
- https://www.electronics-notes.com/articles/connectivity/ieee-802-15-4-wireless/6lowpan.php
- https://www.quora.com/Which-fields-are-compressed-in-a-header-compression-in-6LoWPAN