Securely accessing remote sensors in critical infrastructures.

RESEARCH PROJECT 2

PAVLOS LONTORFOS

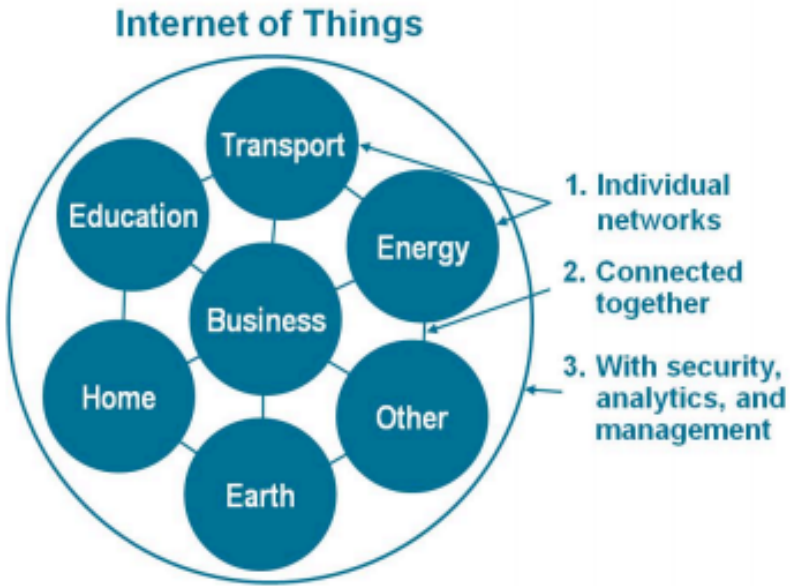
SUPERVISORS:

CEDRIC BOTH

JEROEN DO BOER

The use of sensors

- Transportation
- Power grid networks
- Health sector
- Smart home
- Infrastructure monitoring



Various sectors where sensors are used. Source: Cisco IBSG, April 2011 Image

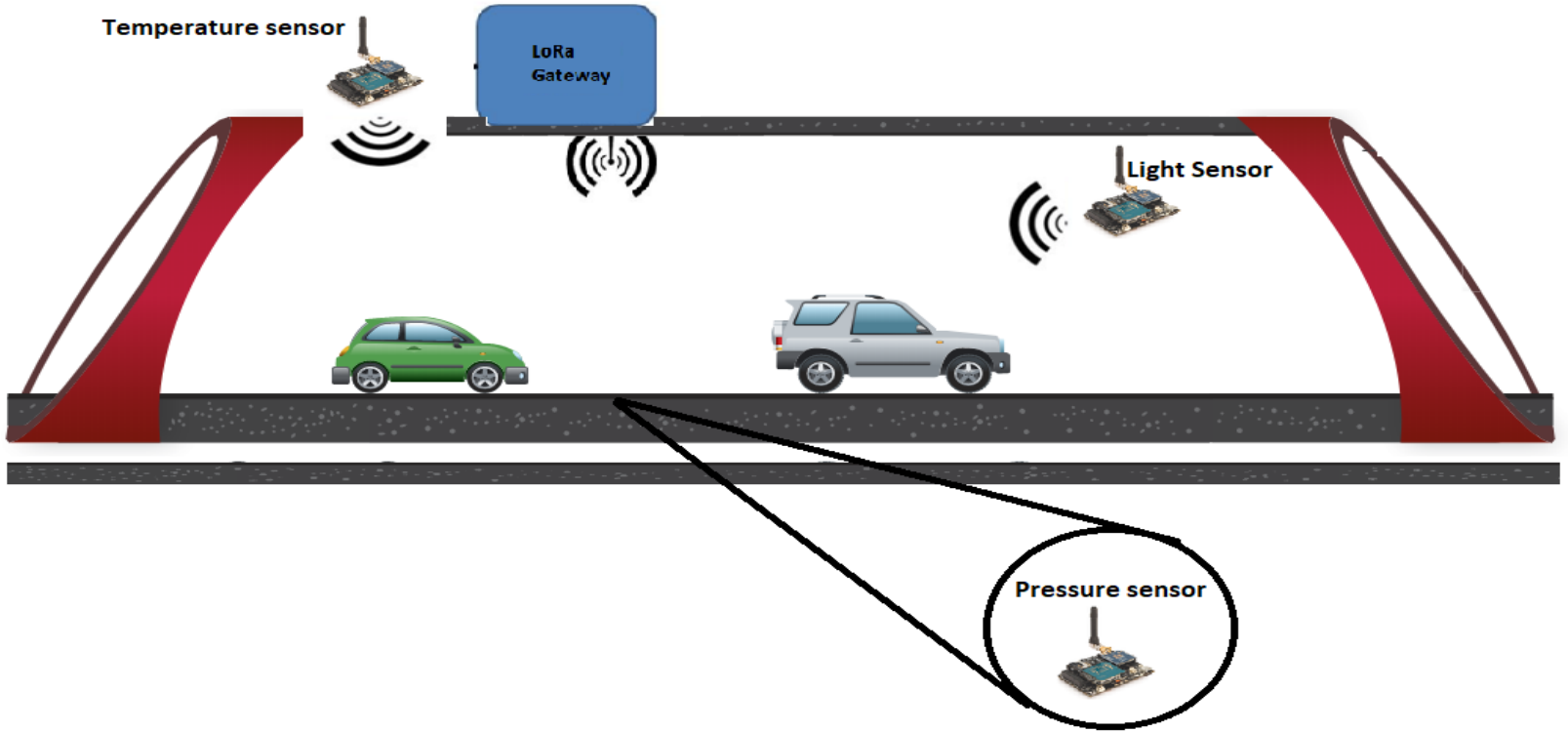
Critical Infrastructure

Monitor infrastructure environment

- Quality of Service
- Hardware failure
- Safety
- Maintenance

Challenges

- Often inaccessible
- Expensive on-site visit
- Time consuming to replace



Research question

Can Software Defined Networks (SDN) improve the redundancy and security of a sensor network in critical infrastructure?

Research question

Can Software Defined Networks (SDN) improve the redundancy and security of a sensor network in critical infrastructure?

Devided in 3 subquestions:

- How SDN affects redundancy

Research question

Can Software Defined Networks (SDN) improve the redundancy and security of a sensor network in critical infrastructure?

Devided in 3 subquestions:

- How SDN affects redundancy
- How SDN affects scalability

Research question

Can Software Defined Networking (SDN) improve the redundancy and security of a sensor network in critical infrastructure?

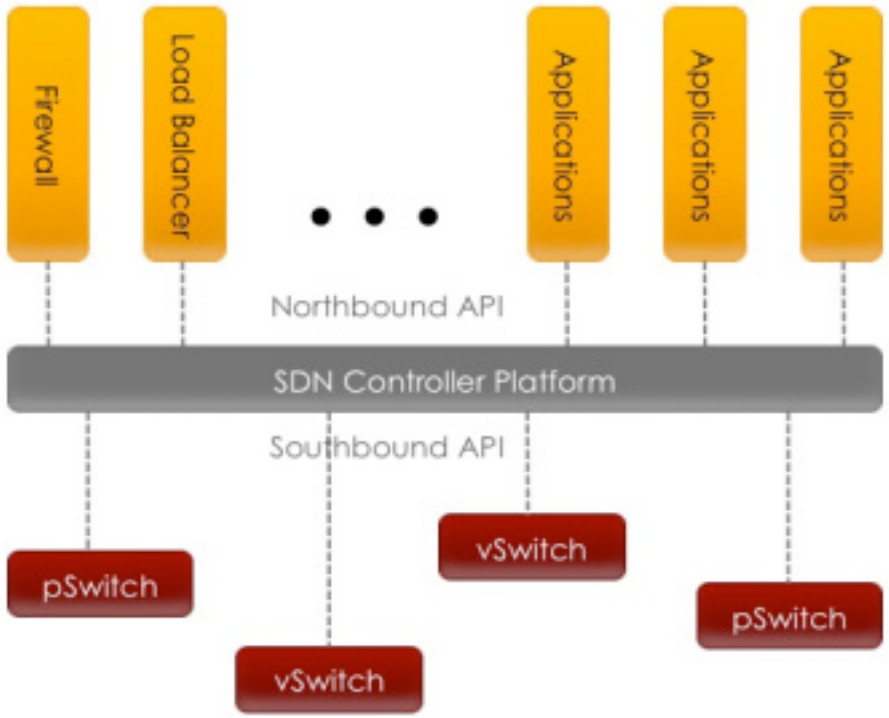
Divided in 3 sub questions:

- How SDN affects redundancy
- How SDN affects scalability
- How SDN affects security

Background

Software Defined Networks

- Separation of control and data plane
- Centralized control
- Northbound and Southbound APIs

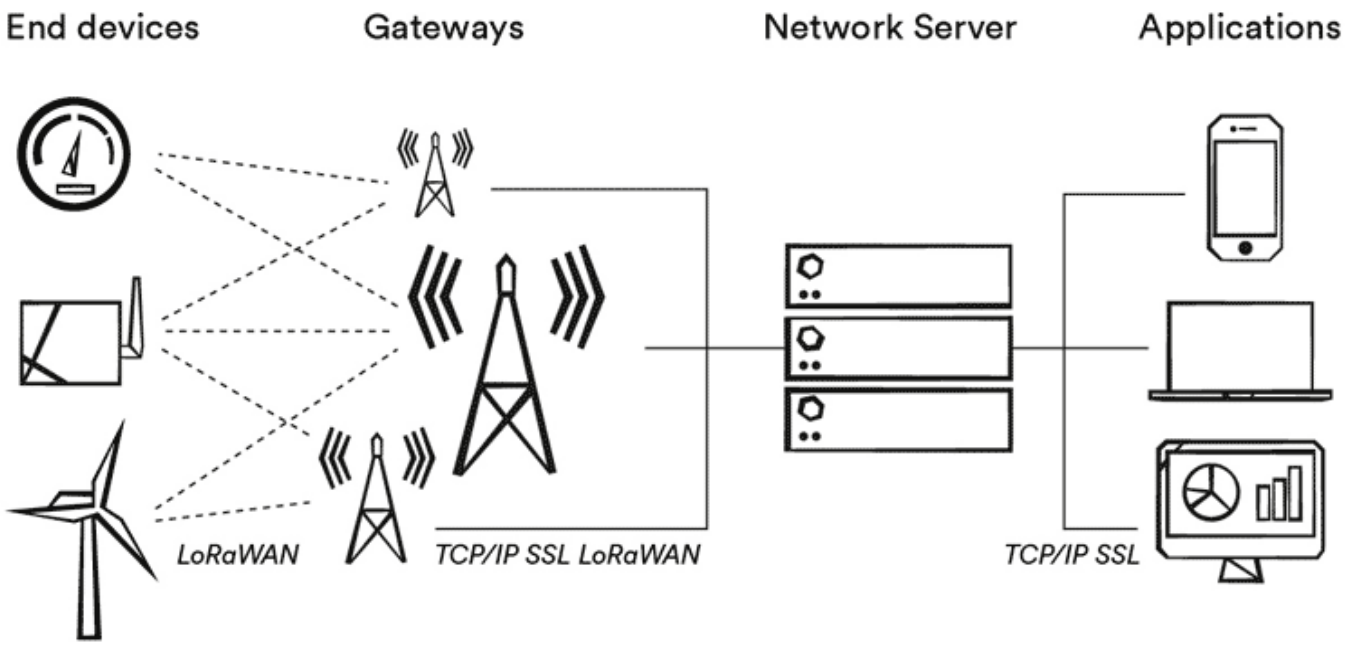


Simplified representation of SDN architecture. Source: https://www.sdxcentral.com/articles/contributed/the-sdn-gold-rush-to-the-northbound-api/2012/11/

Background cont.

LoRa

- RF modulation technology
- Physical layer
- Long Range low power
- Fixed gateways
- Network server

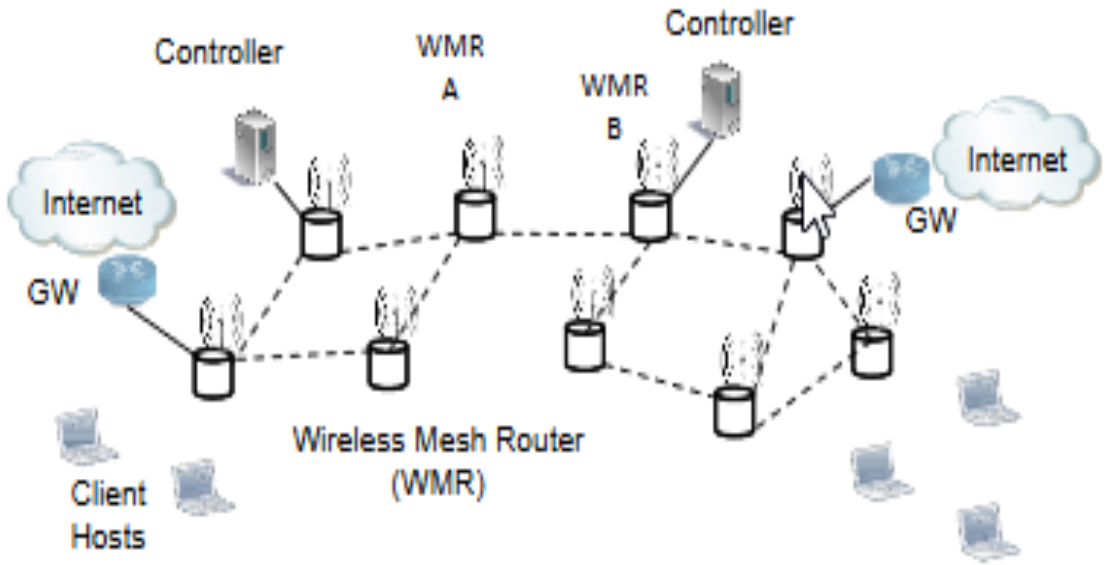


The network server connects sensors, gateways and end-user applications and ensures reliable and secure data routing all along the LoRaWAN network. Retrieved from “https://www.actility.com/lorawan-network-server/”

Related Research

In 2014, Andrea Detti et al. published research with the benefits of an SDN-based implementation of a Wireless Mesh Networks(WMN)

- Arbitrary paths for data flows
- Improved traffic engineering algorithms

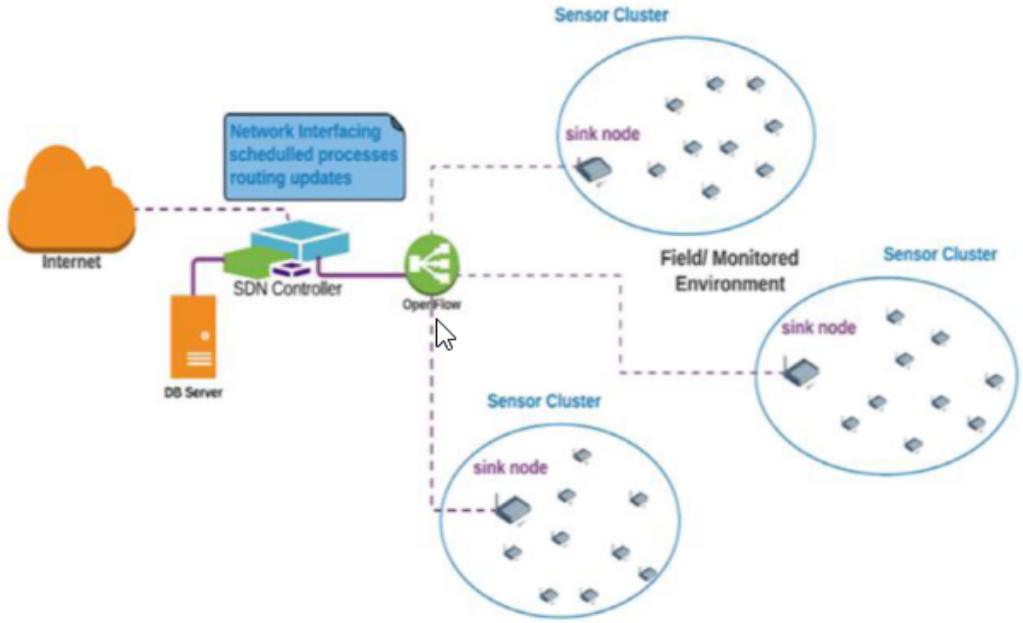


Source from research paper “Controller selection in a Wireless Mesh SDN under network partitioning and merging scenarios”

Related Research

In 2017, Zhiwei Zhang et al. proposed an Efficient Software-Defined Wireless Sensor Network architecture

- Stable and energy-efficient control plane
- Reduce the control overhead



Source from research paper " Software defined wireless sensor networks application opportunities for efficient network management: A survey"

Methodology

- Literature research
- Select the appropriate hardware
- Implement experiments in hardware
- Evaluation of results

Network control experiment

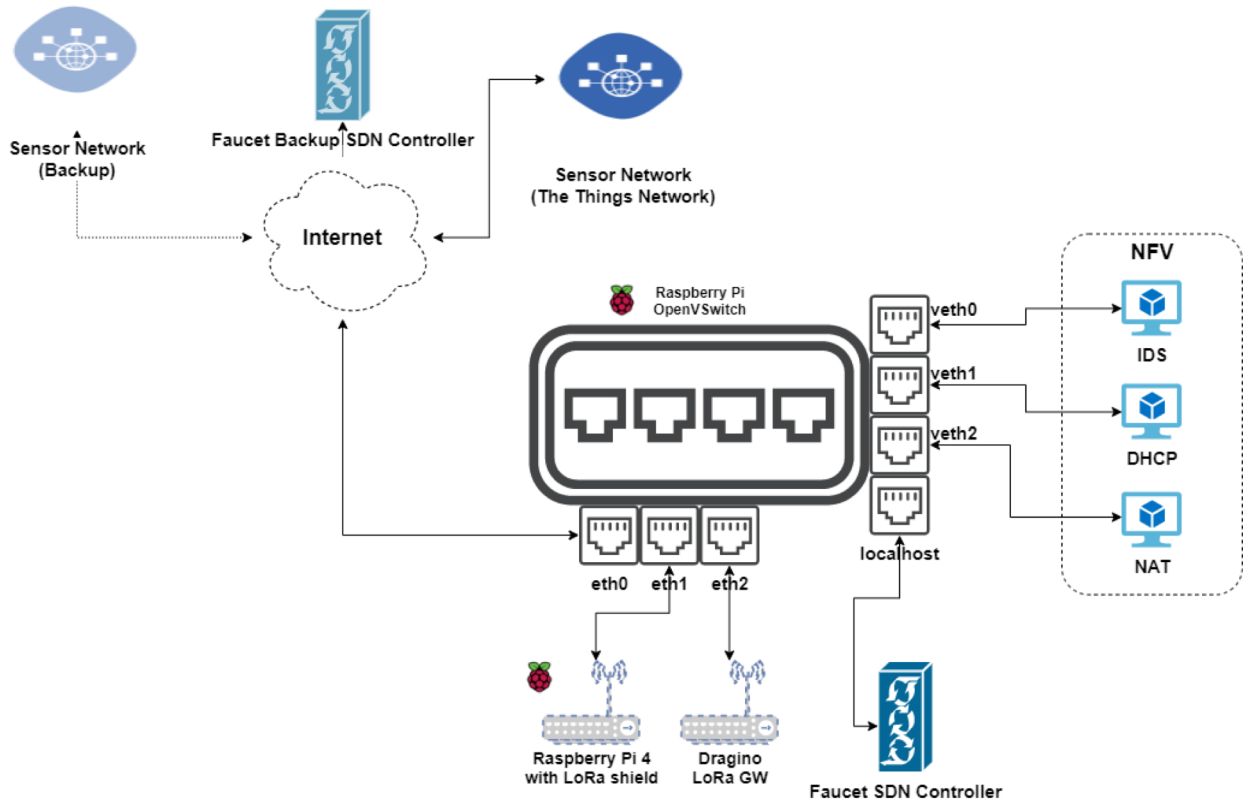
Network Function Virtualization
- DHCP
- NAT
- IDS

OpenVSwitch (OVS)

SDN Controller
- Faucet controller

LoRa Gateways
- Dragino Gateway
- Raspberry Pi with LoRa shield

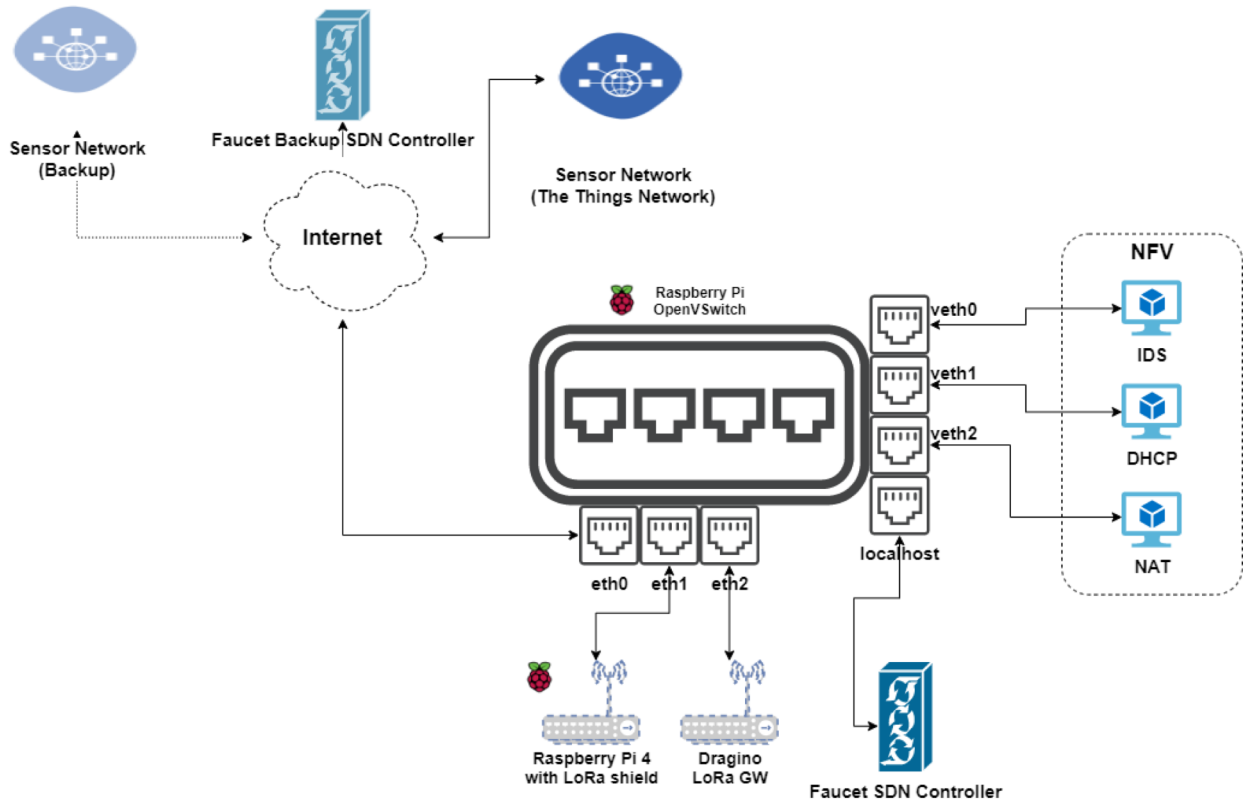
The Things Network



Network control experiment

Centralized control, ACLs and QoS

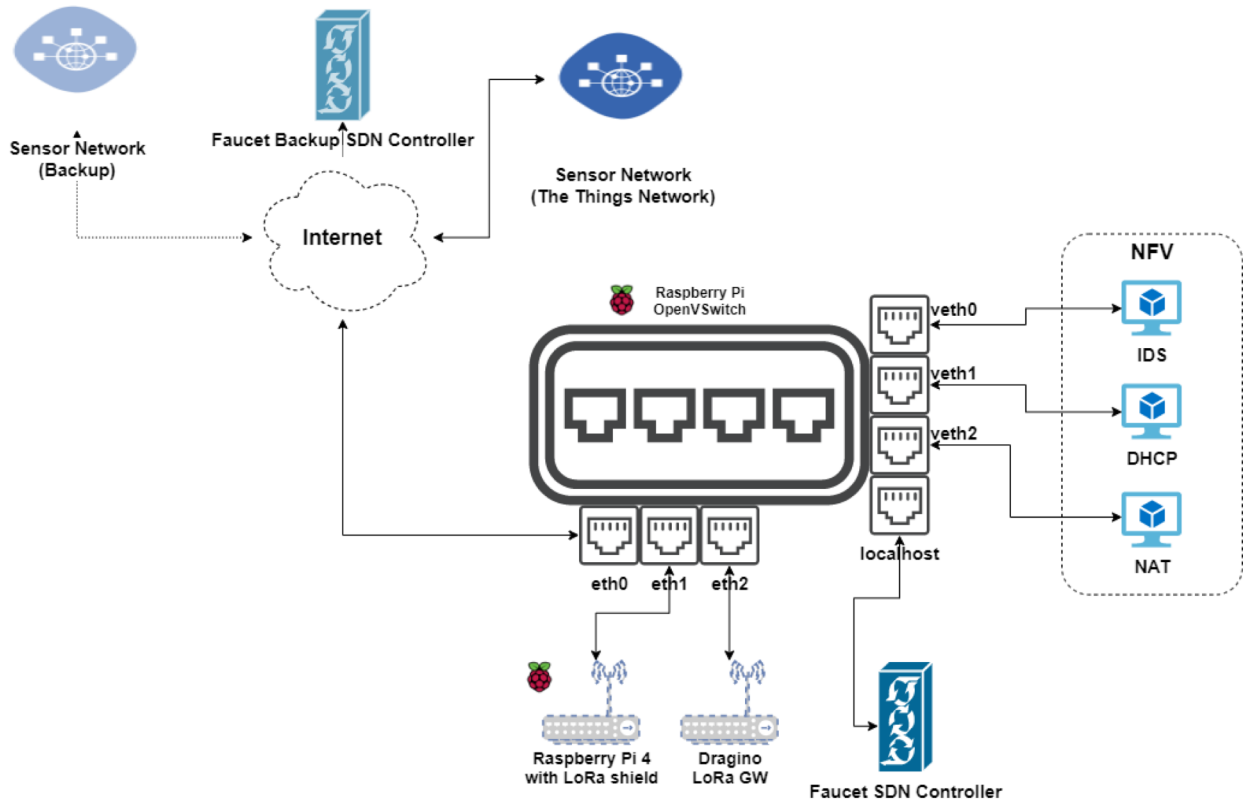
- Fine-grained control of the sensor network
- Load balance flows
- Prioritize critical flows



Network control experiment

Controller failure

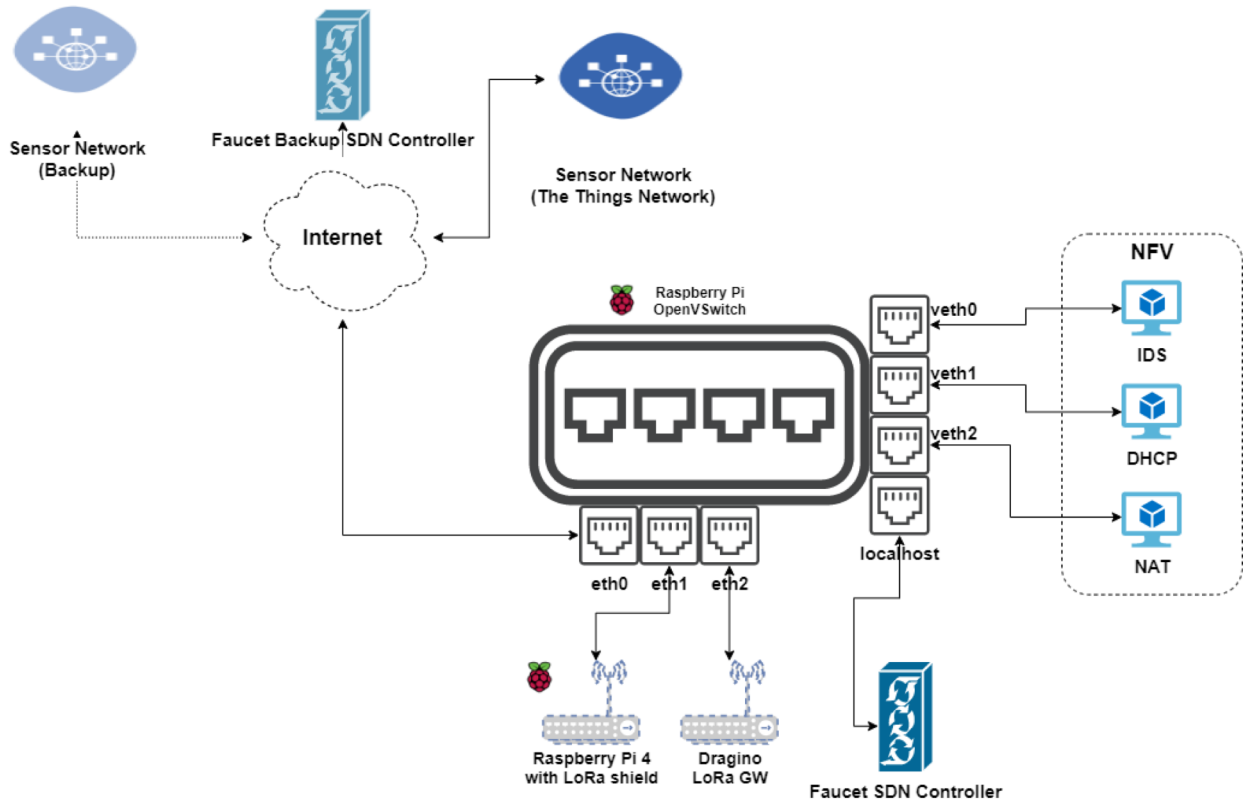
- Secondary takes over
- If both fail, work as regular switch
- Never lost connectivity to sensor network server



Network control experiment

Redundant sensor network server

- Load balance between sensor servers
- Automate behavior using northbound APIs



Network control experiment cont.

Individual Sensor Handling

- No control of individual sensors
- Deep packet inspection firewall

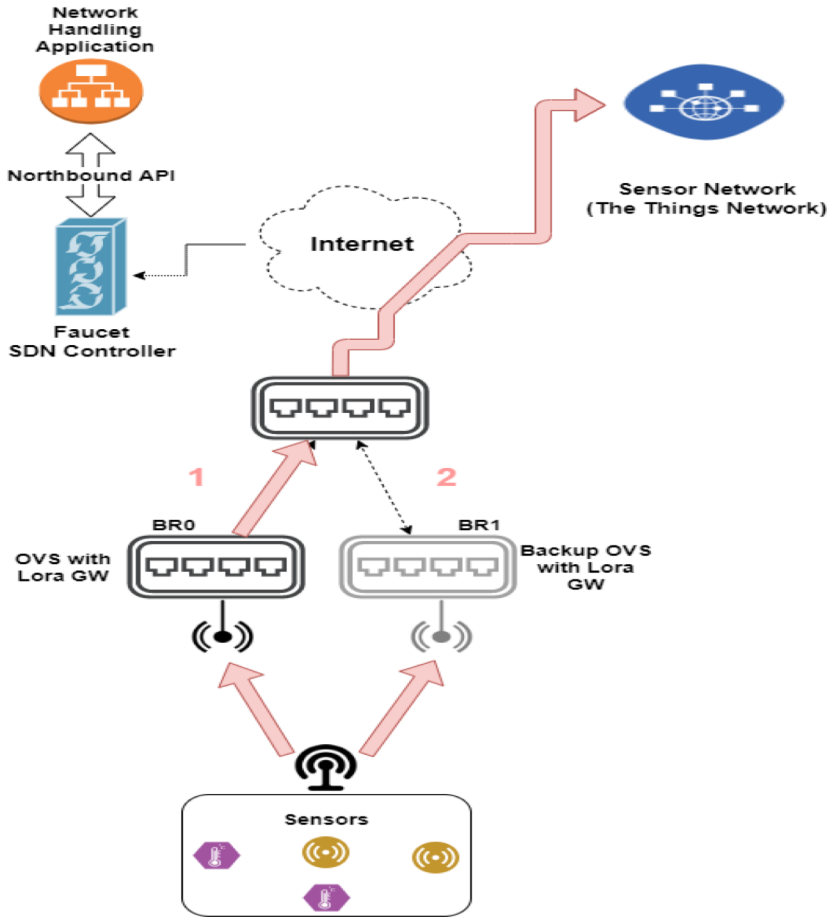
```
▸ Frame 31: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits)
▾ Linux cooked capture
    Packet type: Sent by us (4)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: DraginoT_1d:a8:9a (a8:40:41:1d:a8:9a)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 192.168.178.55, Dst: 52.169.76.203
▸ User Datagram Protocol, Src Port: 54770, Dst Port: 1700
▸ Data (242 bytes)
```


```
{"rxpk":[{
"tmst":614126211,
"time":"2020-06-18T17:19:15.964458Z",
"chan":2,
"rfch":1,
"freq":868.500000,
"stat":1,"modu":"LORA",
"datr":"SF7BW125",
"codr":"4/5",
"lsnr":6.8,
"rssi":-41,"size":23,
"data":"ADIZgqFaQUCoMhmCUZ9BQKhWcC+ENbk="}]}
```

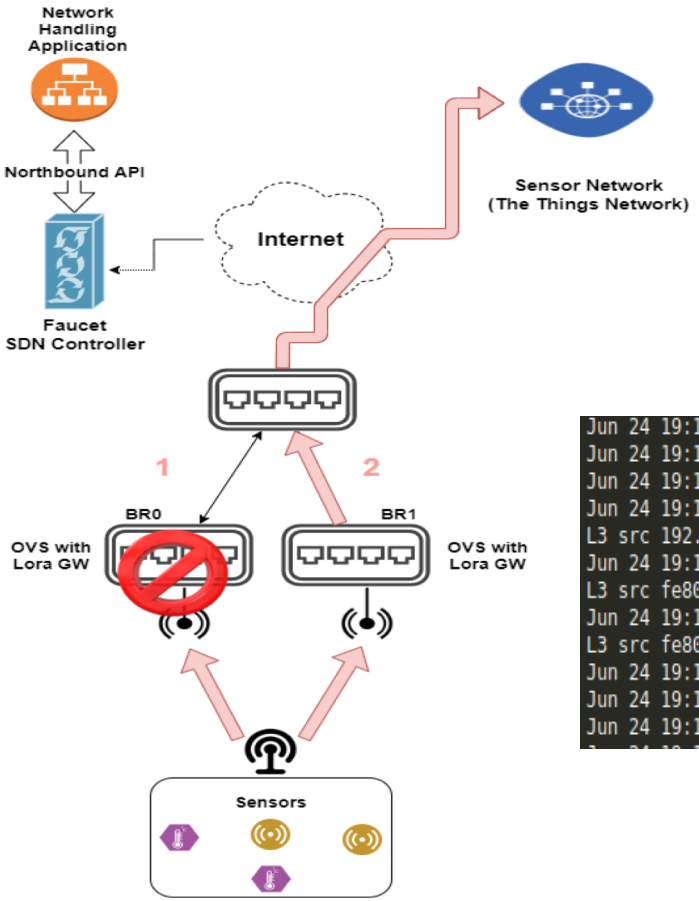
Switch failure experiment

Gateway or switch failure

- Deploy backup LoRa gateways
- Disable duplicate flows
- Enable if failure happens



Switch failure experiment




```
Jun 24 19:12:31 faucet.valve WARNING  DPID 1 (0x1) br0 datapath down
Jun 24 19:12:31 faucet.valve INFO     DPID 1 (0x1) br0 Port 1 (br0 stack link to br2) down
Jun 24 19:12:31 faucet.valve INFO     DPID 1 (0x1) br0 Port 2 (br0 stack link to br3) down
Jun 24 19:12:32 faucet.valve INFO     DPID 4 (0x4) br3 L2 learned on Port 8 e2:d0:5f:82:79:a9 (L2 type 0x0800, L2 dst fa:5c:33:de:6b:bd,
L3 src 192.168.2.18, L3 dst 192.168.2.2) Port 8 VLAN 200 (1 hosts total)
Jun 24 19:12:39 faucet.valve INFO     DPID 4 (0x4) br3 L2 learned on Port 7 de:57:a3:84:34:b4 (L2 type 0x86dd, L2 dst 33:33:00:00:00:02,
L3 src fe80::dc57:a3ff:fe84:34b4, L3 dst ff02::2) Port 7 VLAN 200 (2 hosts total)
Jun 24 19:12:39 faucet.valve INFO     DPID 4 (0x4) br3 L2 learned on Port 10 3a:92:da:38:50:88 (L2 type 0x86dd, L2 dst 33:33:00:00:00:02,
L3 src fe80::3892:daff:fe38:5088, L3 dst ff02::2) Port 10 VLAN 300 (4 hosts total)
Jun 24 19:12:40 faucet.valve INFO     DPID 1 (0x1) br0 LLDP for Port 1 inactive after 15s
Jun 24 19:12:40 faucet.valve INFO     DPID 1 (0x1) br0 LLDP for Port 2 inactive after 15s
Jun 24 19:12:40 faucet.valve ERROR    DPID 1 (0x1) br0 Stack Port 1 GONE, too many (3) packets lost, last received 15s ago
```

Summary

Redundancy

- Better control over the network
- Automated countermeasures using APIs
- Cost efficient hardware can lead to redundant topologies
- Prioritize critical flows

Scalability

- Network Function Virtualization
- Automated control though APIs
- Cost efficient hardware

Summary

Security

- Improved monitoring centralized alerts for events
- Access lists (ACLs)
- Easier configuration – less errors

Conclusion

Can SDN improve redundancy

Yes, due to better control and automated countermeasures

Can SDN improve scalability

Yes, using virtualized network functions and northbound API

Can SDN improve security

Probably yes, due to easier monitoring of the network

Can Software Defined Networks (SDN) improve the redundancy and security of a sensor network in critical infrastructure?

Yes

Future Research

Virtualized Network Functions

- Develop virtual functions aimed to sensor networks

Individual sensor handling for LoRa sensors

- Ways to control individual sensors on network level

Thank you for your attention!