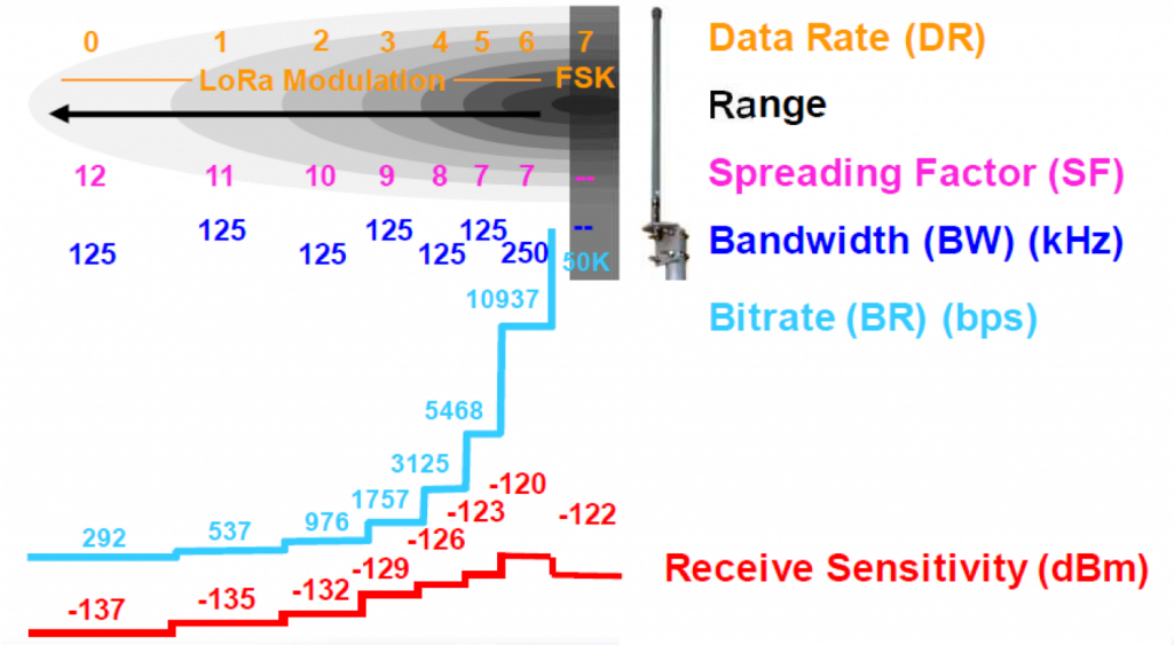


Figure 1: LoraWan Parameters.

LoRa has three configurable parameters:

- Bandwidth (BW)
- Carrier Frequency (CF)
- Coding Rate (CR)
- Spreading Factor (SF)

SF	Sensitivity[dBm]	Data Rate[kb/s]		
6	-118	9.38		
7	-123			
8	-126			
9	-129			
10	-132			
11	-133			
12	-136			

Table 1

SF/BW	**125kHz**		**250kHz**		**500kHz**		
-	Sensitivity	Data Rate	Sensitivity	Data Rate	Sensitivity	Data Rate	
6	-118		-115		-111		
7	-123		-120		-116		
8	-126		-123		-119		
9	-129		-125		-122		
10	-132		-128		-125		
11	-133		-130		-128		
12	-136		-133		-130		

Table 2: Receiver sensitivity [dBm]

[1] Nous avons vu en effet plus haut quil a été démontré que la méthode CSMA est plus efficace pour le traitement des faibles trafics, tandis que TDMA est nettement plus appropriée pour supporter les trafics intenses.

Smart systems in smart cities [2]

- Smart Mobility
- Smart semaphores controle
- Smart Red Swarm

- Smart panels
- Smart bus scheduling
- Smart EV management
- Smart surface parking
- Smart signs
- Smart energy systems
- Smart lighting
- Smart water jet systems
- Smart residuals gathering
- Smart building construction
- Smart tourism
- Smart QRinfo
- Smart monitoring
- Smart hawkeye

Routing protocol	Control Cost	Link Cost	Node Cost
OSPF/IS-IS	✗	✓	✗
OLSRv2	?	✓	✓
RIP	✓	?	✗
DSR	✓	✗	✗
RPL	✓	✓	✓

Table 3: Routing protocols comparison [_**rpl2**_]

Application protocol	Rest-Full	Trans-port	Publish/Sub-scribe	Request/Re-sponse	Security	QoS	Header size (Byte)
COAP	✓	UDP	✓	✓	DTLS	✓	4
MQTT	✗	TCP	✓	✗	SSL	✓	2
MQTT-SN	✗	TCP	✓	✗	SSL	✓	2
XMPP	✗	TCP	✓	✓	SSL	✗	-
AMQP	✗	TCP	✓	✗	SSL	✓	8
DDS	✗	UDP TCP	✓	✗	SSL DTLS	✓	-
HTTP	✓	TCP	✗	✓	SSL	✗	-

Table 4: Application protocols comparison

0.1 Lora modules

Ref	Module	Frequency MHz	Tx power	Rx power	Sensitivity	Channels	Distance
[3]	**Semtech SX1272**	863-870 (EU) 902-928 (US)	14 dBm	dBm	-134 dBm	8 13	22+ km
[3]	**rn2483**						
[3]	**rn2903**						
[3]	**rak811**						
[3]	**Semtech sx1276**						
[3]	**rfm95**						
[3]	**CMWX1ZZABZ-078**						
[3]	**LoPy4**						
[3]	**mDot**						
[3]	**xDot**						
[3]	**Laird RM192**						
[3]	**Laird RM186**						
[3]	**CMWX1ZZABZ-078**						
[3]	**Also Laird RM1xx**						
[3]	**iMST iM88x/iM98x**						
[3]	**Mic SAM RN34/35**						
[3]	**Semtech SX1278**						

Table 5

New York (NY)

Callenges-Applications	Gids	EHealth	Transportations	Cities	**Building**
Ressources cinstraints	+	+++	-	++	+
Mobility	+	++	+++	+++	-
Heterogeneity	++	++	++	+++	+
Scalability	+++	++	+++	+++	++
QoS cinstraints	++	++	+++	+++	+++
Data management	++	+	+++	+++	++
Lack of standardization	++	++	++	++	+++
Amount of attacks	+	+	+++	+++	+++
Safety	++	++	+++	++	+++

Table 6: Main IoT challenges[4]

Plan de controle	**Plan de gestion**	**Plan de doonées**
Controle d'admission	Controle et supervision de QoS	Controle du trafic
Réservation de ressources	Gestion de contrats	Façonnage du trafic
Routage	QoS mapping	Controle de congestion
Signalisation	Politique de QoS	Classification de paquets
		Marquage de paquets
		Ordonnancements des paquets
		Gestion de files d'attente

Table 7: An example table.

(a) Sensors diversity.

(b) Data diversity.

Figure 2: Sensors & data diversity.

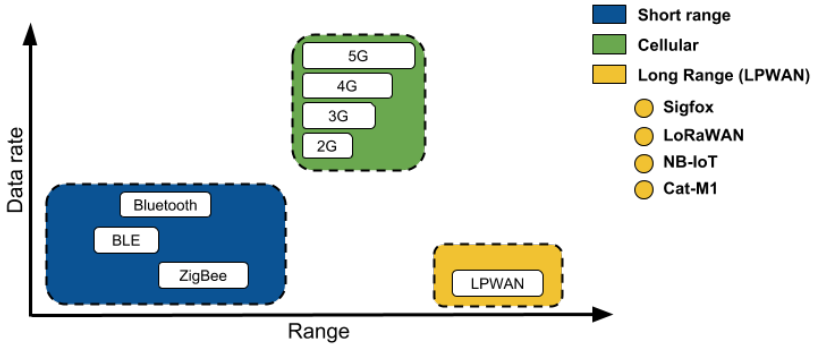


Figure 3: Communication diversity.

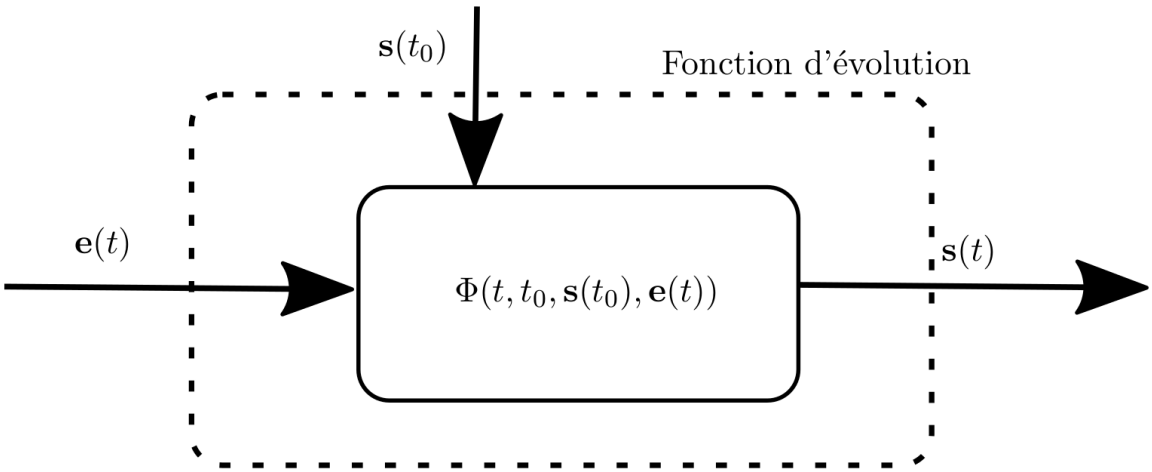
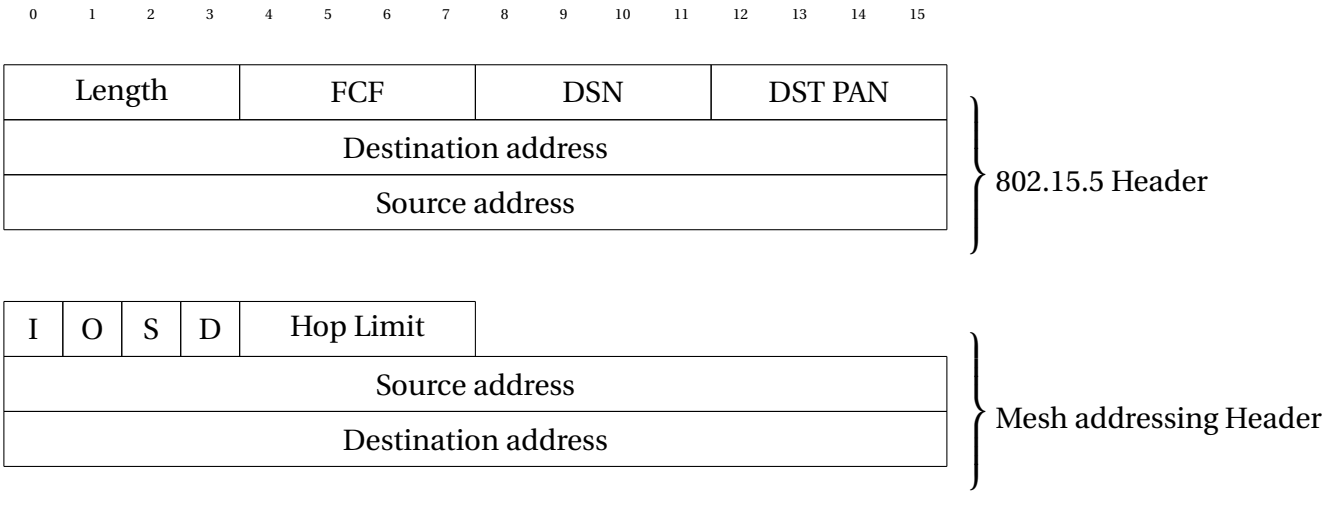


Figure 4: Filtres [5].



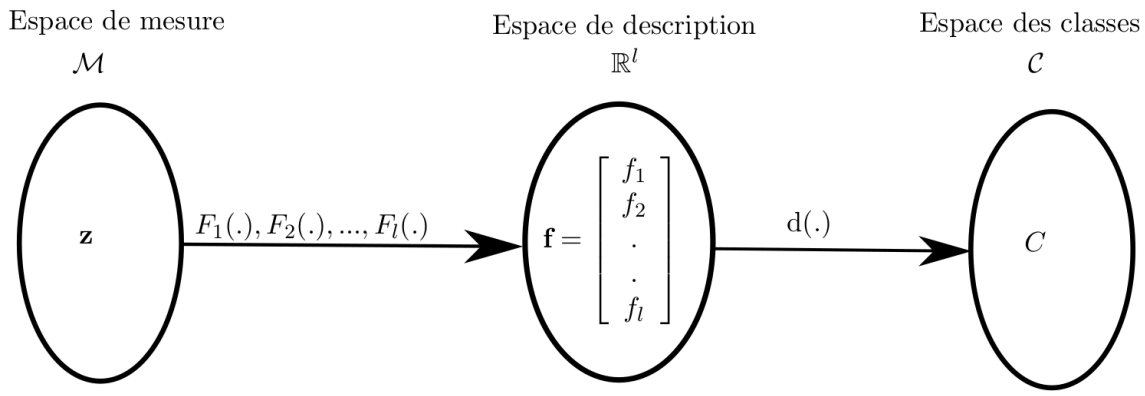


Figure 5: classification [5].

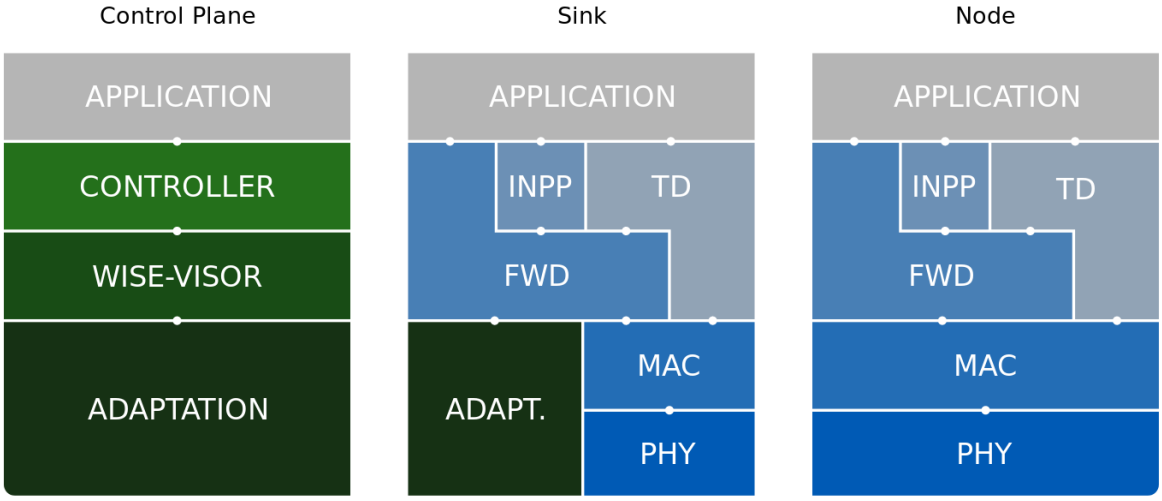


Figure 6: LPWAN connectivity.

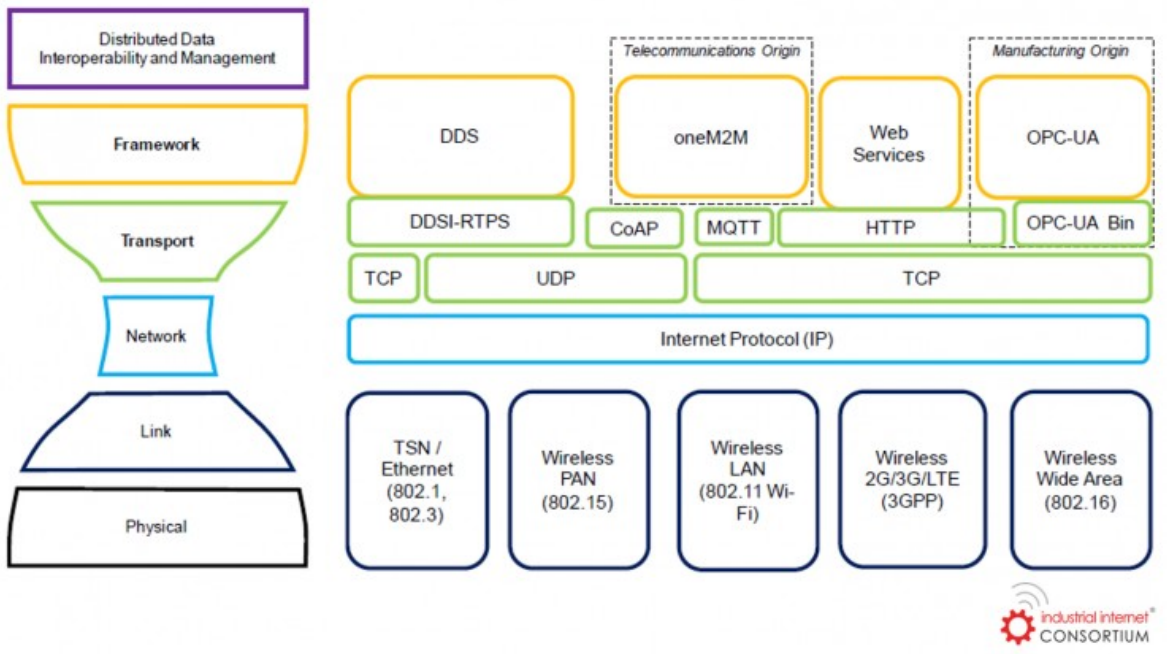


Figure 7: Interoperability.

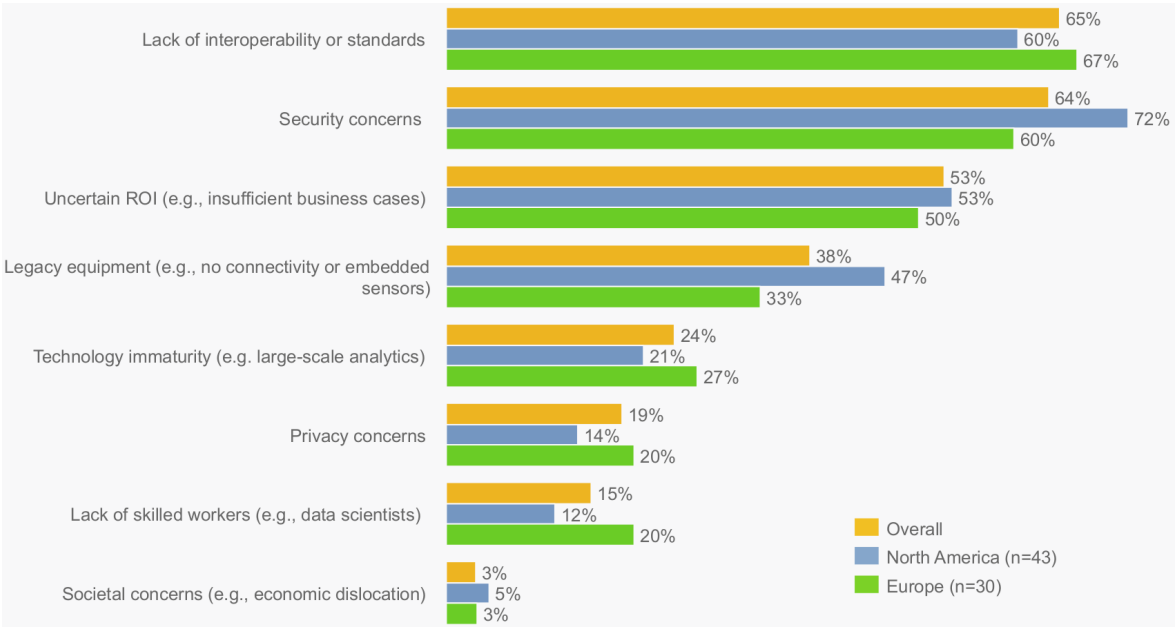


Figure 8: Key barriers in adopting the Industrial Internet[1].

Figure 9: wsn-IoT.

Application	CoAP, MQTT			
Transport	UDP/TCP			
Network	IPv6 RPL	IPv4/IPv6		
	6LowPan	RFC 2464		RFC 5072
MAC	IEEE 802.15.4	IEEE 802.11 (Wi-Fi)	IEEE 802.3 (Ethernet)	2G, 3G, LTE
	2.4GHz, 915, 868MHz	2.4, 5GHz		
	DSS, FSK, OFDM	CSMA/CA	UTP, FO	

Table 8: An example table.

- Network selection
  - MADM
    - Ranking methods
    - Ranking & weighted methods
  - Game theory
    - Users vs users

        * Users vs networks
        * Networks vs network
    - Fuzzy logic
        * as a score method
        * another theory
    - Utility function
        * 1
        * 2

Naïve modes	Instantaneous Hist. average Clustering
Parametric models	Rarely used Traffic Models Time Series Linear regression ARIMA Kalman filtering ATHENA SETAR Gaussian Maximum Likelihood
Non-Parametric models	k-Nearest Neighbor Locally Weighted Regression Fuzzy Logic Bayes Network Neural Network Include temporal/spatial patterns

Table 9: Taxonomy of prediction models [7]

Parameters	**Parameters**	**Type**	**Expected as**
Network conditions	network load	Dynamic	Minimized
	network coverage	Static	Fixed
	network connection time	Dynamic	Minimized
	available bandwidth	Dynamic	Minimized
Application requirements	throughput	Dynamic	Minimized
	delay	Dynamic	Minimized
	jitter	Dynamic	Minimized
	PLR	Dynamic	Minimized
	energy consumption	Dynamic	Minimized
User preferences	budget	Static	Fixed
	cost	Static	Fixed
	design		
Mobile equipment	energy	Dynamic	Fixed
	mobility	Dynamic	Fixed

Table 10: Network selection inputs and classification of parameters [8]

QoS parameters [9] [10]

- Application layer
    - Service time
    - Service availability
    - Service cost
    - Service reliability
- Network layers
    - Bandwidth
    - Packet loss
    - Jitter
    - Delay
- Sensing layer
    - Data accuracy
    - Data collection delay

  - Sampling rate
  - WSN lifetime
  - WSN coverage
- Sensing layer
  - Information accuracy
    - Data accuracy
    - Sensing time accuracy
    - Spatial accuracy
    - Reduce data redundancy
    - Data packaging
  - Energy compsumption
    - Sleep management
    - Life time management
  - Coverage
    - Sensing area

	802.15.4	**802.15.4e**	**802.15.4g**	**802.15.4f**
Frequency	2.4Ghz (DSSS + oQPSK) 868Mhz (DSSS + BPSK) 915Mhz (DSSS + BPSK)	2.4Ghz (DSSS + oQPSK, CSS+DQPSK) 868Mhz (DSSS + BPSK) 915Mhz (DSSS + BPSK)	2.4Ghz (DSSS + oQPSK, CSS+DQPSK) 868Mhz (DSSS + BPSK) 915Mhz (DSSS + BPSK)	2.4Ghz (DSSS + oQPSK,CSS+DQPSK) 868Mhz (DSSS + BPSK) 915Mhz (DSSS + BPSK) 3~10Ghz (BPM+BPSK)
Data rate	Upto 250kbps	Upto 800kbps	Up to 800kbps	
Differences	-	Time sync and channel hopping	Phy Enhancements	Mac and Phy Enhancements
Frame Size	127 bytes	N/A	Up to 2047 bytes	N/A
Range	1 75+ m	1 75+ m	Upto 1km	N/A
Goals	General Low-power Sensing/Actuating	Industrial segments	Smart utilities	Active RFID
Products	Many	Few	Connode (6LoWPAN)	LeanTegra PowerMote

Table 11: IEEE 802.15.4 standards [**sarwar_iot**_]

Phy protocol	**IEEE 802.15.4**	**BLE**	**EPCglobal**	**Z-Wave**	**LTE-M**	**ZigBee**
Standard Body		IEEE 802.15.1				IEEE 802.15.4, ZigBee Alliance
Radio band (MHz)	868/915/2400	2400	860-960	868/908/2400	700-900	
MAC address	TDMA, CSMA/CA	TDMA	ALOHA	CSMA/CA	OFDMA	
Data rate (bps)	20/40/250 K	1024K	varies 5-640K	40K	1G (up), 500M (down)	
Throughput				9.6, 40, 200kbps		
Scalability ???	65K nodes	5917 slaves	-	232 nodes	-	
Range	10-20m	10-100m				
Addressing	8|16bit	16bit				

Table 12: IoT cloud platforms and their characteristics [11]

[13] Many studies have identified SDN as a potential solution to the WSN challenges, as well as a model for heterogeneous integration.

[13] This shortfall can be resolved by using the SDN approach.

[14] SDN also enhances better control of heterogeneous network infrastructures.

[14] Anadiotis et al. define a SDN operating system for IoT that integrates SDN based WSN **(SDN-WISE)**. This experiment shows how heterogeneity between different kinds of SDN networks can be achieved.

[14] In cellular networks, OpenRoads presents an approach of introducing SDN based heterogeneity in wireless networks for operators.

Characteristics	6LoWPAN	LoRaWAN	SigFox	Narrow-band
Standar body		LoRa Alliance		3GPP
TX Active Power @ 3V				
Frequency band (MHz)	902-929 868-868.6	902-928 863-870 and 434	902 868	
Number of channels (channels for MHz)	0016 for 2400 0010 for 915 0001 for 868.3	80 for 915 10 for 868 and 780	25	
Channel bandwidth (MHz)	0005 for 2400 0002 for 915 0600 for 868.3	0.125 and 0.50 for 915 0.125 and 0.25 for 868 and 780	0.0001-0.0012	
Maximum data rate (kbps for MHz)	0250 for 2400 0040 for 915 0020 for 868.3	0.00098-0.0219 for 915 0.250-0.05 for 868 and 780	0.1-0.6	
Channel modulation	QPSK for 2400 BPSK for 915 BPSK for 868.3	LoRa for 915 LoRa and GFSK for 868 and 780	BPSK and GFSK	
Channel coding (dBm for MHz)	-085 for 2400 -092 for 915 -092 for 868.3	-137	-137	
Protocol data unit (bytes)	6+127	x + (19 to 250)	12+ (0 to 12)	
Channel coding	Direct	CSS	Ultra	
Transmission range	10-100 m	5-15 km	10-50 km	
Battery lifetime	1-2 years	<10 years	<10 years	
Standard Body	IETF			
Security	Access Control List (ACL)			
Uplink			100bps, 12 bytes/msg, max 140 msg/day	
Downlink			8 bytes/msg, max 4 msg/day	
Scalability				
Proprietary			✓	
Cost		High		

Table 13: LPWan Characteristics [12]

Feature	Wi-Fi	802.11p	UMTS	LTE	LTE-A
Channel width MHz	20	10	5	1.4, 3, 5, 10, 15, 20	<100
Frequency band(s) GHz	2.4 , 5.2	5.86-5.92	0.7-2.6	0.7-2.69	0.45-4.99
Bit rate Mb/s	6-54	327	2	<300	<1000
Range km	<0.1	<1	<10	<30	<30
Capacity	Medium	Medium	✗	✓	✓
Coverage	Intermittent	Intermittent	Ubiquitous	Ubiquitous	Ubiquitous
Mobility support km/h	✗	Medium	✓	<350	<350
QoS support	EDCA Enhanced Distributed Channel Access	EDCA Enhanced Distributed Channel Access	QoS classes and bearer selection	QCI and bearer selection	QCI and bearer selection
Broadcast/multicast support	Native broadcast	Native broadcast	Through MBMS	Through eMBMS	Through eMBMS
V2I support	✓	✓	✓	✓	✓
V2V support	Native (ad hoc)	Native (ad hoc)	✗	✗	Through D2D
Market penetration	✓	✗	✓	✓	✓
Data rate	<640 kbps	250 kbps	106424 kbps	✓	✓

Table 14: An example table.

[15] There has been a plethora of (industrial) studies synergising SDN in IoT. The major characteristics of IoT are low latency,wireless access, mobility and heterogeneity.

[15] Thus a bottom-up approach application of SDN to the realisation of heterogeneous

IoT is suggested.

[15] Perhaps a more complete IoT architecture is proposed, where the authors apply SDN principles in IoT heterogeneous networks.

[16] it provides the SDWSN with a proper model of network management, especially considering the potential of heterogeneity in SDWSN.

[16] We conjecture that the SDN paradigm is a good candidate to solve the heterogeneity in IoT.

Management architecture	Management feature	Controller configuration	Traffic Control	Configuration and monitoring	Scapability and localization	Communication management
[17] Sensor Open Flow	SDN support protocol	Distributed	in/out-band	✓	✓	✓
[18] SDWN	Duty sycling, aggregation, routing	Centralized	in-band	✓		
[19] SDN-WISE	Programming simplicity and aggregation	Distributed	in-band		✓	
[degante_smart_2014] Smart	Efficiency in resource allocation	Distributed	in-band		✓	
SDCSN	Network reliability and QoS	Distributed	in-band		✓	
TinySDN	In-band-traffic control	Distributed	in-band		✓	
Virtual Overlay	Network flexibility	Distributed	in-band		✓	
Context based	Network scalability and performance	Distributed	in-band		✓	
CRLB	Node localization	Centralized	in-band			
Multi-hope	Traffic and energy control	Centralized	in-band			✓
Tiny-SDN	Network task measurement	-	in-band			

Table 15: SDN-based network and topology management architectures. [15]

- Routing over low-power and lossy links (ROLL)
- Support minimal routing requirements.
  - like multipoint-to-point, point-to-multipoint and point-to-point.
- A Destination Oriented Directed Acyclic Graph (DODAG)
  - Directed acyclic graph with a single root.
  - Each node is aware of ts parents
  - but not about related children
- RPL uses four types of control messages
  - DODAG Information Object (DIO)
  - Destination Advertisement Object (DAO)
  - DODAG Information Solicitation (DIS)
  - DAO Acknowledgment (DAO-ACK)
- Standard topologies defined in IEEE 802.15.4e networks are

Star contains at least one FFD and some RFDs

Mesh contains a PAN coordinator and other nodes communicate with each other

Cluster consists of a PAN coordinator, a cluster head and normal nodes.

- The IEEE 802.15.4e standard supports 2 types of network nodes

Application protocol	DDS	CoAP	AMQP	MQTT	MQTT-SN	XMPP	HTTP
Service discovery		mDNS			DNS-SD		
Network layer				RPL			
Link layer				IEEE 802.15.4			
Physical layer		EPCglobal		IEEE 802.15.4		Z-Wave	

Table 16: Standardization efforts that support the IoT

	LiteOS	**Nano-RK**	**MANTIS**	**Contiki**
Architecture	Monolithic	Layered	Modular	Modular
Scheduling Memory	Round Robin	Monotonic harmonized	Priority classes	Interrupts execute w.r.t.
Network	File	Socket abstraction	At Kernel COMM layer	uIP, Rime
Virtualization and Completion	Synchronization primitives	Serialized access semaphores	Semaphores	Serialized, Access
Multi threading	✓	✓	✗	✓
Dynamic protection	✓	✗	✓	✓
Memory Stack	✓	✗	✗	✗

Table 17: Common operating systems used in IoT environment [11]

Paper	Architec-ture	Avail-ability	Relia-bility	Mo-bility	Perfor-mance	Manage-ment	Scala-bility	Interoper-ability	Secu-rity
IoT-A									
IoT@Work									
EBBITS									
BETaas									
CALIPSO									
VITAL									
SENSAI									
RERUM									
RELEYonIT									
IoT6									
OpenIoT									
Apec IoV									
Smart Santander									
OMA Device									
OMA-DM									
LWM2M									
NETCONF Light									
Kura									
MASH									
IoT-iCore									
PROBE-IT									
OpenIoT									
LinkSmart									
IETF SOLACE									
BUTLER									
Codo									
SVELETE									

Table 18: An example table.

Platform	**COAP**	**XMPP**	**MQTT**
Arkessa			✓
Axeda			
Etherios			
LittleBits			
NanoService	✓		
Nimbits		✓	
Ninja blocks			
OnePlateformv	✓	✓	
RealTime.io			
SensorCloud			
SmartThings			
TempoDB			
ThingWorx			✓
Xively			✓
Ubidots			✓

Table 19: IoT cloud platforms and their characteristics

FFD Full function device: serve as a coordinator
- It is responsible for creation, control and maintenance of the net
- It store a routing table in their memory and implement a full MAC

RFD Reduced function devices: simple nodes with restricted resources
- They can only communicate with a coordinator
- They are limited to a star topology

Preamble	PHDR	PHDR_CRC	MHDR	FHDR	FPort	Payload	MIC	CRC

Use cases			
Health Monitoring			
Water Distribution			
Electricity Distribution			
Smart Buildings			
Intelligent Transportation			
Surveillance			
Environmental Monitoring			

Table 20: Use cases [20]

Routing protocol	**Control Cost**	**Link Cost**	**Node Cost**
OSPF/IS-IS	✗	✓	✗
OLSRv2	?	✓	✓
RIP	✓	?	✗
DSR	✓	✗	✗
RPL	✓	✓	✓

Table 21: Routing protocols comparison [_**rpl2**_]

Application protocol	Rest-Full	Trans-port	Publish/Sub-scribe	Request/Re-sponse	Security	QoS	Header size (Byte)
COAP	✓	UDP	✓	✓	DTLS	✓	4
MQTT	✗	TCP	✓	✗	SSL	✓	2
MQTT-SN	✗	TCP	✓	✗	SSL	✓	2
XMPP	✗	TCP	✓	✓	SSL	✗	-
AMQP	✗	TCP	✓	✗	SSL	✓	8
DDS	✗	UDP TCP	✓	✗	SSL DTLS	✓	-
HTTP	✓	TCP	✗	✓	SSL	✗	-

Table 22: Application protocols comparison

1 | Introduction

1.1 Introduction

1.1.1 Context & motivation

The exponential growth of 5G networks and the development of IoT that will greatly come with it, would considerably raise the number of Smart Cities applications. The aim of such technology is mainly to improve the comfort and the safety of users through wireless IoT networks. Wireless Sensor Networks (WSNs) are the source of sensed data of cities things, i.e. roads, cars, pedestrians, houses, parking, etc. The cloud is the entity that collects the sensed data and allows users and machines to do data analysis and improve services. For Smart Cities, one objective is improving the welfare of citizens as well as its safety getting real-time information about the city infrastructure. One application would be the transportation systems, and traffic lights control having as an objective avoids congestion and dangerous situations. A static cycle of traffic lights has a direct impact on traffic jams. The long period at red or green light could impact the fluidity of the city traffic. The Internet of Things (IoT) would give an answer to the required interoperability between heterogeneous wireless networks. Our objective is to model, prototype and evaluate a traffic control system. Indeed, different infrastructures have different purposes and technologies, this means that it is not possible to state communication between two infrastructures following a Device-to-Device approach. However, thinking of an indirect or Device-to-Cloud communication between infrastructures seems useful when every connected system has its own technologies, e.g. Zigbee, LoRa, SigFox, ITS-G5. Consequently, IP stack would be the suitable mediator for interconnecting these networks. It removes the barriers of rigid standard specifications of the hardware despite the overhead of the extra network configuration. Furthermore, we want to have a scalable solution not limited only on the traffic light management system. We can deploy sensors and actuators to measure noise or air pollution via panels or roads and offer new services, e.g. where and when jogging is better. To implement our Urban Traffic Light Control based on an IoT network architecture (IoT-UTLC), we setting a real IEEE 802.15.4 WSN devices that would act as actuators and sensors. All these small traffic light devices are driven by a Border Router (BR) which is a gateway to the Internet. This BR

1.1.2 Methodology and contributions

1.1.3 Organization of the thesis

2 | State of the art [21]

2.1 Introduction

jjh

2.2 IoT Hardware and software platforms

2.2.1 Software platform: Operating systems

The operating system is the foundation of the IoT technology as it provides the functions for the connectivity between the nodes. However, different types of nodes need different levels of OS complexity; a passive node generally only needs the communication stack and is not in need of any threading capabilities, as the program can handle all logic in one function. Active nodes and border routers need to have a much more complex OS, as they need to be able to handle several running threads or processes, e.g. routing, data collection and interrupts. To qualify as an OS suitable for the IoT, it needs to meet the basic requirements: Low Random-access memory (RAM) footprint Low Read-only memory (ROM) footprint Multi-tasking Power management (PM) Soft real-time These requirements are directly bound to the type of hardware designed for the IoT. As this type of hardware in general needs to have a small form factor and a long battery life, the on-board memory is usually limited to keep down size and energy consumption. Also, because of the limited amount of memory, the implementation of threads is usually a challenging task, as context switching needs to store thread or process variables to memory. The size of the memory also directly affects the energy consumption, as memory in general is very power hungry during accesses. To be able reduce the energy consumption, the OS needs some kind of power management. The power management does not only let the OS turn on and off peripherals such as flash memory, I/O, and sensors, but also puts the MCU itself in different power modes. As the nodes can be used to control and monitor consumer devices, either a hard or soft real-time OS is required. Otherwise, actions requiring a close to instantaneous reaction might be indefinitely delayed. Hard real-time means that the OS scheduler can guarantee latency and execution time, whereas Soft real-time means that latency and execution time is seen as real-time but can not be guaranteed by the scheduler. Operating systems that meet the above requirements are compared in table 2.1 and 2.2.

Contiki

Contiki is a embedded operating system developed for IoT written in C [12]. It supports a broad range of MCUs and has drivers for various transceivers. The OS does not only support TCP/IPv4 and IPv6 with the uIP stack [9], but also has support for the 6LoWPAN

OS	Architecture	Multi threading	Scheduling	Dynamic Memory	Memory protection	Network Stack	Virtualization and Completion
Contiki/Contiki-ng	Modular	✓	Interrupts execute w.r.t.	✓	✗	uIP Rime	Serialized Access
MANTIS	Modular	✗	Priority classes	✓	✗	At Kernel COMM layer	Semaphores.
Nano-RK	Layered	✓	Monotonic harmonized	✗	✗	Socket abstraction	Serialized access semaphores
LiteOS	Monolithic	✓	Round Robin	✓	✓	File	Synchronization primitives

Table 2.1: Common operating systems used in IoT environment [11]

stack and its own stack called RIME. It supports threading with a thread system called Photothreads [13]. The threads are stack-less and thus use only two bytes of memory per thread; however, each thread is bound to one function and it only has permission to control its own execution. Included in Contiki, there is a range of applications such as a HTTP, Constrained Application Protocol (CoAP), FTP, and DHCP servers, as well as other useful programs and tools. These applications can be included in a project and can run simultaneously with the help of Photothreads. The limitations to what applications can be run is the amount of RAM and ROM the target MCU provides. A standard system with IPv6 networking needs about 10 kB RAM and 30 kB ROM but as applications are added the requirements tend to grow.

RIOT

RIOT is a open source embedded operating system supported by Freie Universität Berlin, INIRA, and Hamburg University of Applied Sciences [14]. The kernel is written in C but the upper layers support C++ as well. As the project originates from a project with real-time and reliability requirements, the kernel supports hard real-time multi-tasking scheduling. One of the goals of the project is to make the OS completely POSIX compliant. Overhead for multi-threading is minimal with less than 25 bytes per thread. Both IPv6 and 6LoWPAN is supported together with UDP, TCP, and IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL); and CoAP and Concise Binary Object Representation (CBOR) are available as application level communication protocols.

TinyOS

TinyOS is written in Network Embedded Systems C (nesC) which is a variant of C [15]. nesC does not have any dynamic memory allocation and all program paths are available at compile-time. This is manageable thanks to the structure of the language; it uses modules and interfaces instead of functions [16]. The modules use and provide interfaces and are interconnected with configurations; this procedure makes up the structure of the program. Multitasking is implemented in two ways: trough tasks and events. Tasks, which focus on computation, are non-preemptive, and run until completion. In contrast, events which focus on external events i.e. interrupts, are preemptive, and have separate start and stop functions. The OS has full support for both 6LoWPAN and RPL, and also have libraries for CoAP.

freeRTOS

One of the more popular and widely known operating systems is freeRTOS [17]. Written in C with only a few source files, it is a simple but powerful OS, easy to overview and

extend. It features two modes of scheduling, pre-emptive and co-operative, which may be selected according to the requirements of the application. Two types of multitasking are featured: one is a lightweight Co-routine type, which has a shared stack for lower RAM usage and is thus aimed to be used on very small devices; the other is simply called Task, has its own stack and can therefore be fully pre-empted. Tasks also support priorities which are used together with the pre-emptive scheduler. The communication methods supported out-of-the-box are TCP and UDP.

2.2.2 Hardware platform

Even though the hardware is in one sense the tool that the OS uses to make IoT possible, it is still very important to select a platform that is future-proof and extensible. To be regarded as an extensible platform, the hardware needs to have I/O connections that can be used by external peripherals. Amongst the candidate interfaces are Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I 2 C), and Controller Area Network (CAN). These interfaces allow developers to attach custom-made PCBs with sensors for monitoring or actuators for controlling the environment. The best practice is to implement an extension socket with a well-known form factor. A future-proof device is specified as a device that will be as attractive in the future as it is today. For hardware, this is very hard to achieve as there is constant development that follows Moores Law [4]; however, the most important aspects are: the age of the chip, its expected remaining lifetime, and number of current implementations i.e. its popularity. If a device is widely used by consumers, the lifetime of the product is likely to be extended. One last thing to take into consideration is the product family; if the chip belongs to a family with several members the transition to a newer chip is usually easier.

OpenMote

OpenMote is based on the Ti CC2538 System on Chip (SoC), which combines an ARM Cortex-M3 with a IEEE 802.15.4 transceiver in one chip [18, 19]. The board follows the XBee form factor for easier extensibility, which is used to connect the core board to either the OpenBattery or OpenBase extension boards [20, 21]. It originates from the CC2538DK which was used by Thingsquare to demo their Mist IoT solution [22]. Hence, the board has full support for Contiki, which is the foundation of Thingsquare. It can run both as a battery-powered sensor board and as a border router, depending on what extension board it is attached to, e.g OpenBattery or OpenBase. Furthermore, the board has limited support but ongoing development for RIOT and also full support for freeRTOS.

MSB430-H

The Modular Sensor Board 430-H from Freie Universität Berlin was designed for their ScatterWeb project [23]. As the university also hosts the RIOT project, the decision to support RIOT was natural. The main board has a Ti MSP430F1612 MCU [24], a **Ti CC1100 transceiver**, and a battery slot for dual AA batteries; it also includes a SHT11 temperature and humidity sensor and a MMA7260Q accelerometer to speed up early development. All GPIO pins and buses are connected to external pins for extensibility. Other modules with new peripherals can then be added by making a PCB that matches the external pin layout.

Zolertia

As many other Wireless Sensor Network (WSN) products, the Zolertia Z1 builds upon the MSP430 MCU [25, 26]. The communication is managed by the Ti CC2420 which operates in the 2.4 GHz band. The platform includes two sensors: the SHT11 temperature and humidity sensor and the MMA7600Q accelerometer. Extensibility is ensured with: two connections designed especially for external sensors, an external connector with USB, Universal asynchronous **receiver/transmitter (UART)**, SPI, and I 2 C.

2.2.3 Communication protocol

Several different wireless communication protocols, such as Wireless LAN (WLAN), BLE, 6LoWPAN, and ZigBee may be suitable for IoT applications. They all operate in the 2.4GHz frequency band and this, together with the limited output power in this band, means that they all have a similar range. The main differences are located in the MAC, PHY, and network layer. WLAN is much too power hungry as seen in table 2.6 and is only listed as a reference for the comparisons.

IEEE 802.15.4

The IEEE 802.15.4 standard defines the PHY and MAC layers for wireless communication [6]. It is designed to use as little transmission time as possible but still have a decent payload, while consuming as little power as possible. Each frame starts with a preamble and a start frame delimiter; it then continues with the MAC frame length and the MAC frame itself as seen in figure 2.2. The overhead for each PHY packet is only 4+1+1 133 tild 4.5%; when using the maximum transmission speed of 250kbit/s, each frame can be sent 133byte in 250kbit/s = 4.265ms. Furthermore, it can also operate in the 868MHz and 915MHz bands, maintaining the 250kbit/s transmission rate by using Offset quadrature phase-shift keying (O-QPSK).

Several network layer protocols are implemented on top of IEEE 802.15.4. The two that will be examined are 6LoWPAN and ZigBEE.

6LoWPAN is a relatively new protocol that is maintained by the Internet Engineering Task Force (IETF) [7, 6]. The purpose of the protocol is to enable IPv6 traffic over a IEEE 802.15.4 network with as low overhead as possible; this is achieved by compressing the IPv6 and UDP header. A full size IPv6 + UDP header is 40+8 bytes which is tild 38% of a IEEE 802.15.4 frame, but with the header compression this overhead can be reduced to 7 bytes, thus reducing the overhead to tild 5%, as seen in figures 2.3 and 2.4.

ZigBee is a communication standard initially developed for home automation networks; it has several different protocols designed for specific areas such as lighting, remote control, or health care [27, 6]. Each of these protocols uses their own addressing with different overhead; however, there is also the possibility of direct IPv6 addressing. Then, the overhead is the same as for uncompressed 6LoWPAN, as seen in figure 2.5.

A new standard called ZigBee 3.0 aims to bring all these standards together under one roof to simplify the integration into IoT. The release date of this standard is set to Q4 2015.

Bluetooth LE

BLE is developed to be backwards compatible with Bluetooth, but with lower data rate and power consumption [28]. Featuring a data rate of 1Mbit/s with a peak current consumption less than 15mA, it is a very efficient protocol for small amounts of data. Each frame can be transmitted 47bytes in 1Mbit/s = 376Mus; thanks to the short transmission time, the transceivers consumes less power as the transceiver can be in receive mode or completely off most of the time. BLE uses its own addressing methods and as the MAC frame size (figure 2.6) is only 39bytes, thus IPv6 addressing is not possible.

Starting from Bluetooth version 4.2, there is support for IPv6 addressing with the Internet Protocol Support Profile; the new version allows the BLE frame to be variable between 2 257 bytes. The network set-up is controlled by the standard Bluetooth methods, whereas IPv6 addressing is handled by 6LoWPAN as specified in IPv6 over Bluetooth Low Energy [29].

LoaraWAN

SEMTECH

ALIANCE

Class-A

Uplink LoRa Server supports Class-A devices. In Class-A a device is always in sleep mode, unless it has something to transmit. Only after an uplink transmission by the device, LoRa Server is able to schedule a downlink transmission. Received frames are deduplicated (in case it has been received by multiple gateways), after which the mac-layer is handled by LoRa Server and the encrypted application-playload is forwarded to the application server.

Downlink LoRa Server persists a downlink device-queue for to which the application-server can enqueue downlink payloads. Once a receive window occurs, LoRa Server will transmit the first downlink payload to the device.

Confirmed data LoRa Server sends an acknowledgement to the application-server as soon one is received from the device. When the next uplink transmission does not contain an acknowledgement, a nACK is sent to the application-server.

Note: After a device (re)activation the device-queue is flushed.

Class-B LoRa Server supports Class-B devices. A Class-B device synchronizes its internal clock using Class-B beacons emitted by the gateway, this process is also called a beacon lock. Once in the state of a beacon lock, the device negotioates its ping-interval. LoRa Server is then able to schedule downlink transmissions on each occuring ping-interval.

Downlink LoRa Server persists all downlink payloads in its device-queue. When the device has acquired a beacon lock, it will schedule the payload for the next free ping-slot in the queue. When adding payloads to the queue when a beacon lock has not yet been acquired, LoRa Server will update all device-queue to be scheduled on the next free ping-slot once the device has acquired the beacon lock.

Confirmed data LoRa Server sends an acknowledgement to the application-server as soon one is received from the device. Until the frame has timed out, LoRa Server will wait with the transmission of the next downlink Class-B payload.

Note: The timeout of a confirmed Class-B downlink can be configured through the device-profile. This should be set to a value less than the interval between two ping-slots.

Requirements

Device The device must be able to operate in Class-B mode. This feature has been tested against the develop branch of the Semtech LoRaMac-node source.

Gateway The gateway must have a GNSS based time-source and must use at least the Semtech packet-forwarder version 4.0.1 or higher. It also requires LoRa Gateway Bridge 2.2.0 or higher.

Class-C

Downlink LoRa Server supports Class-C devices and uses the same Class-A downlink device-queue for Class-C downlink transmissions. The application-server can enqueue one or multiple downlink payloads and LoRa Server will transmit these (semi) immediately to the device, making sure no overlap exists in case of multiple Class-C transmissions.

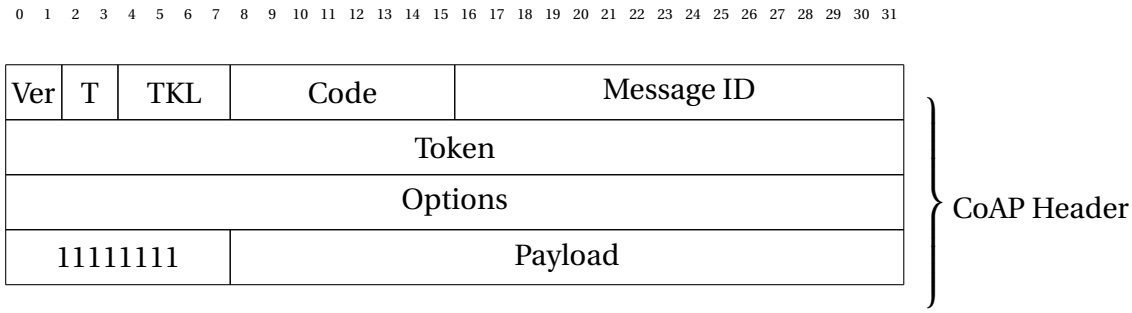
Confirmed data LoRa Server sends an acknowledgement to the application-server as soon one is received from the device. Until the frame has timed out, LoRa Server will wait with the transmission of the next downlink Class-C payload.

Note: The timeout of a confirmed Class-C downlink can be configured through the device-profile.

2.2.4 Application protocol

CoAP

- Constrained Application Protocol
- The IETF Constrained RESTful Environments
- CoAP is bound to UDP
- CoAP can be divided into two sub-layers
  - messaging sub-layer
  - request/response sub-layer
    a) Confirmable.
    b) Non-confirmable.
    c) Piggybacked responses.
    d) Separate response
- CoAP, as in HTTP, uses methods such as:
  - GET, PUT, POST and DELETE to
  - Achieve, Create, Retrieve, Update and Delete
  - Ex: the GET method can be used by a server to inquire the clients temperature

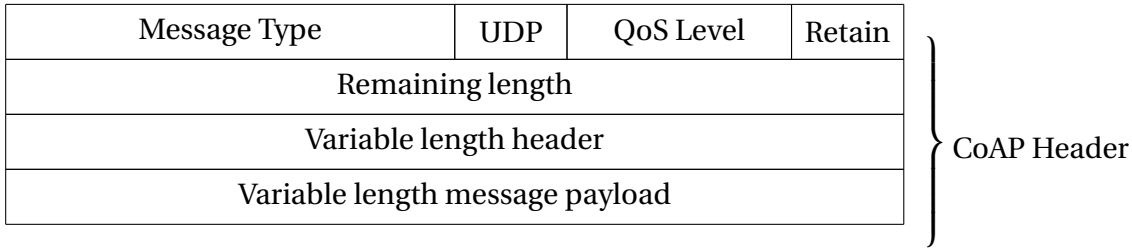


Ver: is the version of CoAP
T: is the type of Transaction
TKL: Token length
Code: represents the request method (1-10) or response code (40-255).
- Ex: the code for GET, POST, PUT, and DELETE is 1, 2, 3, and 4, respectively.

Message ID: is a unique identifier for matching the response.
Token: Optional response matching token.

MQTT

- Message Queue Telemetry Transport
- Andy Stanford-Clark of IBM and Arlen Nipper of Arcom
  - Standardized in 2013 at OASIS
- MQTT uses the publish/subscribe pattern to provide transition flexibility and simplicity of implementation
- MQTT is built on top of the TCP protocol
- MQTT delivers messages through three levels of QoS
- Specifications
  - MQTT v3.1 and MQTT-SN (MQTT-S or V1.2)
  - MQTT v3.1 adds broker support for indexing topic names
- The publisher acts as a generator of interesting data.



Message type: CONNECT (1), CONNACK (2), PUBLISH (3), SUBSCRIBE (8) and so on
DUP flag: indicates that the massage is duplicated
QoS Level: identify the three levels of QoS for delivery assurance of Publish messages
Retain field: retain the last received Publish message and submit it to new subscribers as a first message

XMPP

- Extensible Messaging and Presence Protocol
- Developed by the Jabber open source community
- An IETF instant messaging standard used for:
  - multi-party chatting, voice and telepresence

- Connects a client to a server using a XML stanzas
- An XML stanza is divided into 3 components:
  - message: fills the subject and body fields
  - presence: notifies customers of status updates
  - iq (info/query): pairs message senders and receivers
- Message stanzas identify:
  - the source (from) and destination (to) addresses
  - types, and IDs of XMPP entities

AMQP

- Advanced Message Queuing Protocol
- Communications are handled by two main components
  - exchanges: route the messages to appropriate queues.
  - message queues: Messages can be stored in message queues and then be sent to receivers
- It also supports the publish/subscribe communications.
- It defines a layer of messaging on top of its transport layer.
- AMQP defines two types of messages
  - bare massages: supplied by the sender
  - annotated messages: seen at the receiver
- The header in this format conveys the delivery parameters:
  - durability, priority, time to live, first acquirer & delivery count.
- AMQP frame format

  Size the frame size.

  DOFF the position of the body inside the frame.

  Type the format and purpose of the frame.
    - Ex: 0x00 show that the frame is an AMQP frame
    - Ex: 0x01 represents a SASL frame.

DDS

- Data Distribution Service
- Developed by Object Management Group (OMG)
- Supports 23 QoS policies:
  - like security, urgency, priority, durability, reliability, etc
- Relies on a broker-less architecture
  - uses multicasting to bring excellent Quality of Service
  - real-time constraints
- DDS architecture defines two layers:

  DLRL Data-Local Reconstruction Layer
    - serves as the interface to the DCPS functionalities

  DCPS Data-Centric Publish/Subscribe
    - delivering the information to the subscribers
- 5 entities are involved with the data flow in the DCPS layer:
  - Publisher:disseminates data
  - DataWriter: used by app to interact with the publisher
  - Subscriber: receives published data and delivers them to app
  - DataReader: employed by Subscriber to access received data
  - Topic: relate DataWriters to DataReaders

- No need for manual reconfiguration or extra administration
- It is able to run without infrastructure
- It is able to continue working if failure happens.
- It inquires names by sending an IP multicast message to all the nodes in the local domain
  - Clients asks devices that have the given name to reply back
  - the target machine receives its name and multicasts its IP @
  - Devices update their cache with the given name and IP @

mDNS

- Requires zero configuration aids to connect machine
- It uses mDNS to send DNS packets to specific multicast addresses through UDP
- There are two main steps to process Service Discovery:
  - finding host names of required services such as printers
  - pairing IP addresses with their host names using mDNS
- Advantages
  - IoT needs an architecture without dependency on a configuration mechanism
  - smart devices can join the platform or leave it without affecting the behavior of the whole system
- Drawbacks
  - Need for caching DNS entries

2.2.5 Summary and discussion

2.3 IoT applications

2.3.1 Transportation and logistics

2.3.2 Healthcare

2.3.3 Smart environnement

2.3.4 personal and social

2.3.5 Futuristic

2.3.6 Summary and discussion

2.3.7 Summary and discussion

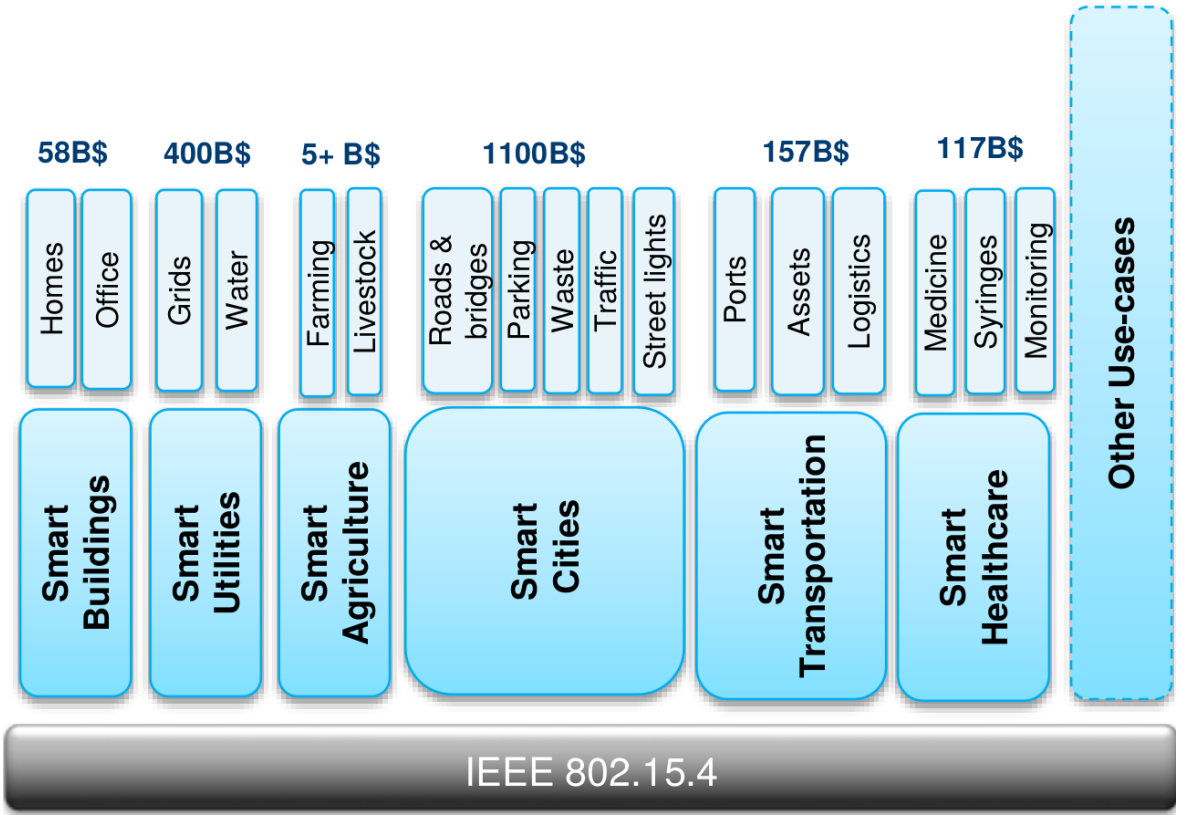


Figure 1: 802.15.4 use cases [**sarwar_iot_**].

2.4 IoT security

2.4.1 Summary and discussion

2.5 Conclusion

3 | Aghiles [21]

3.1 Introduction & problem statement

3.1.1 Background

Internet of Things (IoT) is a concept aiming at connecting all things to the Internet [1]. The different kinds of devices range from simple sensor devices to complex machines such as industry robots. Home automation has been available for a few years in the forms of timers and remotely controlled devices, such as lights, garage door, and climate control equipment. Also in the industry and workplace, there are current systems that have some of the functionality of IoT, e.g, sensors in robots and machines which keep track of the system status so that maintenance can be scheduled at the right time. However, these systems or sensors rarely communicate with each other or make decisions based on other sensor values; instead they depend on input from a user. In the same way cellphones connected people and made them constantly connected to the Internet, IoT will connect devices and make them constantly connected to the Internet [2]. In theory, this could lead to a future with autonomous technology all around us. The benefits could be huge as it would save time and energy for both the individual at home and for the industry [3]. IoT could be used in industry to automate power-heavy tasks to run when the electricity price is low. This principle can also be applied for the home user with laundry machines and charging of e.g. electric cars. This practice would lead to reduced energy consumption and thus a reduced environmental footprint. i3tex AB wants to investigate potential fields of applicability of this upcoming technology. i3tex AB has customers in the automotive, communication, and pulp industries; those customers have made inquiries on how to integrate IoT and sensor networks into production. As technology evolves, size and energy consumption of the IoT devices will decrease and computation power will increase [4]. This reduction in size and energy consumption, together with the increased computing power, will open up new fields for IoT. Thus, i3tex AB want to have an IoT platform to present to their current and potential customers. The interest in IoT is rapidly increasing, and thus, in the near future, the number of devices connected to the Internet is expected to increase rapidly. To support this huge increase in both number of connected devices and the sheer amount of data that will be sent over both wired and wireless networks, the communication technology must be ready [5].

3.1.2 Purpose (Goal)

The purpose of this project is to find and examine a communication method for devices that are made to be a part of IoT. This will be done by examining the available technologies and then developing a prototype based on the findings, which will be used for examining the communication method. This project will examine the physical, link, and network

layers [6, 7] of the Open Systems Interconnection model (OSI model) [8], in order to find suitable technologies on the market. As IoT is still only defined as a concept, there are several technologies to take into consideration and examine in further detail. The prototype will be delivered to i3tex AB together with appropriate documentation, e.g. technical specification, hardware manual, software manual, and API specification.

3.1.3 Limitations

To be able to achieve the project goal within the available time, limitations need to be defined in the three main areas of: Operating System (OS), hardware, and communication method. The OS will not be custom-made, but rather selected amongst those already on the market. Thus, to simplify the hardware selection, only those OSs which already have hardware support that meets the requirements will be taken into consideration. Furthermore, support for either 6LoWPAN, ZigBee, or Bluetooth Low Energy (BLE) as communication method is required, since development to make those standards available is outside the scope of the project. On the hardware side, the limitations will be to only use existing devices and parts as there will be no time for developing hardware or Printed Circuit Boards (PCBs). However, the hardware does not need to have an integrated radio transceiver, but needs to support at least one transceiver supporting IEEE802.15.4 [6]. Thus, communication methods will be primarily selected from specifications building on the IEEE 802.15.4.

3.1.4 Method

To ensure that the right technologies were selected and investigated, the first phase of the project was a literature study. The study served as a foundation when developing and performing the evaluation of the communication methods. At the end of the phase, a requirements specification was formulated to serve as a platform for the next phase. After the literature study, a selection process was performed, where the most promising technologies that met the requirements were examined in further detail and brought into the development phase. This process included the selection of development tools and other decisions bound to the product development. In the development phase, the chosen set-up was configured and assembled to prepare for testing; it was then tested according to throughput, range, latency, and energy consumption. Throughput was measured in kilobyte per second (KB/s) and tested by transferring data of different sizes in both congested and uncongested network set-ups to simulate real world and lab environments. The same set-up was used to measure the latency of a transmission, which was measured in microseconds (ms). Range was calculated instead of measured, with meters (m) as the unit. The power consumption was measured in watts (W). Each week a meeting with the company supervisors was performed, to keep the work on the right track. Here, feedback was be given and other issues and questions handled.

3.2 Background

The goal of the implementation phase is to have a working prototype for future assessment. To make the process of implementing the prototype possible, the first part of the implementation process will be to create a set of requirements. When these are set, the process will continue by comparing the data from chapter 2 to find the candidates that fulfil the requirements. After the technologies are selected, the process will continue with

setting up the workspace, which includes the platform for development and the required tools to build, debug and test the prototype. Finally, when these three steps have been performed, the next step will be to start with the actual prototype development.

3.2.1 Requirements

As the time dedicated for development is limited, the requirements have to make sure that the development process does not run into any major obstacles. All parts of the total prototype need to fit together seamlessly. However, the hardware platform and the operating system are tied most closely together. Therefore, they need requirements that complement each other, so that they can act as a platform for software development. Naturally, both the hardware and the operating system requirements might have to be altered slightly to enable the best match.

Hardware

Transceiver with IEEE 802.15.4 or IEEE 802.15.1 Integrated sensor/sensors MCU with low power mode under 5MicroA Wakeup from low power mode with timer Border router ability Joint Test Action Group (JTAG) support

Operating system

Support for the SoC/MCU and transceiver 6LoWPAN, ZigBee or BLE stack Soft real-time RAM and ROM footprint matching the hardware

Communication protocol

IPv6 addressing support Existing OS support Network type is mesh UDP

3.2.2 Hardware

Each platform examined in chapter 2 has different strengths and weaknesses. When looking at the MCU, OpenMote has a ARM Cortex-M3 which is more powerful compared to the other two alternatives: it features a 32bit 32MHz core with 32KB RAM and 512KB flash memory compared to the MSP430 16bit 25MHz core with 10KB/100KB memory configuration. In terms of peripherals all three platforms are comparable, with similar amount of DAC, GPIO pins, and external busses. All of the platforms have a temperature sensor and an accelerometer, but OpenMote also features an light/uv-light sensor and a voltage sensor built into the MCUs ADC. The MSB430 platform has a somewhat lower power consumption in active RF mode thanks to the less power-hungry sub-GHz transceiver. On the other hand, the less powerful MSP430 MCU has a better deep sleep power consumption, but as the radio is not integrated in the chip as it is in the CC2538 SoC, that advantage is offset by the external transceiver. Comparing the transceivers, there are two 2.4GHz models and one subGHz model; the sub-GHz CC1100 has a higher transmit power of 10dBm compared to 0dBm for CC2420 and 7dBm for CC2538. Also the sensitivity is similar for all the alternatives but gives a slight advantage to CC2538 with -97dBm compared to -95dBm and -93dBm for CC2420 and CC1100. Using these numbers and Friis range equation (equation 4.1) the range of each transceiver with a Fade margin (FM) of 20dB can be seen in figure 3.1. The benefits of working with lower frequencies can clearly be seen as the theoretical range of CC1100 is almost 3 times longer than the 2.4GHz transceivers.

Adding all this information together, the choice of platform will land on OpenMote with the CC2538SoC. It both has a MCU with more memory and better performance, and a transceiver with really good characteristics both in terms of energy consumption and range. Also OpenMote is the only option that can act as a border router using OpenBase; it lets the SoC interface with USB, UART, JTAG, and Ethernet, which enables the standalone border router mode without the need to be connected to a computer or other hardware. The OpenBattery extension lets the SoC operate as a node in a mesh network and provides a dual AAA battery slot connected to the PCB.

3.2.3 Operating system

As a modern operating system can be compiled to match almost any hardware, the most important thing to have in mind is the out-of-the-box hardware support. Only RIOT and Contiki have full support for the ARM Cortex-M3 of the considered operating systems and thus both TinyOS and freeRTOS are directly eliminated as developing the support would take too much time. Compared to RIOT, Contiki also has full driver support for the sensors and transceiver, which should decrease the implementation time significantly. When compiled into binary form, RIOT uses less RAM and ROM and thus probably is a bit faster compared to Contiki, which could be important if the application consumes much resources. The lower memory usage might also give RIOT an advantage in being future-proof. Contiki also has support for soft real-time scheduling compared to the hard real-time scheduling of RIOT; this is however not crucial, as the software that will be running on the OS does not have any hard real-time constraints. Both RIOT and Contiki have support for 6LoWPAN but no support for either ZigBee or BLE; this is due to the fact that these are proprietary stacks. Support could be added but would take some time to customize for the given OS. What gives Contiki the largest advantage is that it also have border router software ready for deployment, which in the RIOT case would have to be developed. All in all, as the project has such a limited time frame, Contiki will be selected as the OS; this, mainly because Contiki comes with most advantages time-wise; this choice means that the focus of the software development will be the creation of a test and evaluation system.

3.2.4 Communication protocol

The OpenMote platform has a IEEE 802.15.4 transceiver and thus supports both ZigBee and 6LoWPAN; this means that BLE is not an option. As ZigBee does not have full IPv6 support yet and is not integrated into Contiki, the natural choice is 6LoWPAN. This choice will not only save some development time but also enables evaluation of the header compression. As seen in figure 3.2, the 6LoWPAN stack in Contiki will replace the IP stack while maintaining the same functionality. As the functionality is the same, TCP and HTTP will work with 6LoWPAN, but including them in the source increases the OS build size considerably. On top of the UDP layer, Contiki also has a working implementation of CoAP that can be used for retrieving data from the nodes in a power efficient manner. CoAP is a stateless protocol that uses the HTTP response headers to achieve a very low overhead in transmissions while using application level reliability methods to ensure packet delivery.

3.2.5 Workspace and tools

The ARM Cortex-M3 chip that OpenMote and CC2538 is built upon requires the GCC ARM Embedded compiler. This tool-chain is free and runs on both Linux, OSX, and Windows;

however, there is no bundled development application so a secondary application for programming is needed. In Windows, there are several Integrated Development Environments (IDEs) such as IAR Workbench ARM [30], Code Composer Studio [31] and the Eclipse plug-in ARM DS-5 [32, 33]; these IDEs use various proprietary toolchains and have a price tag ranging from free to several thousand SEK. Most of the IDEs also have a code size restriction for the free versions. To minimize the costs, the development machine development machine used in this project will run Ubuntu 14.04 LTS, the used tool-chain is GCC ARM Embedded, and Geany is used as the code development application. To analyse the network traffic in real-time, the open source tool Wireshark is used together with a IEEE 802.15.4 packet sniffer. Together with a laptop, the packet sniffer will grant the ability to traverse the mesh network and analyse the network in real-time as it is seen by the nodes.

3.3 Prototype

The goal of the development process is to have a functional border router and at least two nodes to be able to test how response time and throughput differs with each hop in a mesh network. To be able to measure response time and throughput, each node needs to have a CoAP server which can respond to ping and also receive an arbitrary amount of data for throughput measurement. It is desirable for each node to be able to send information about each sensor so the project can be used as a tech-demo. The first part of the development was to set-up of the workspace and tools mentioned in section 3.1.5. Ubuntu OS was installed in a VirtualBox Virtual Machine to make it easier to duplicate and backup; this procedure gave a noticeable decrease in performance and it is recommended to have a dedicated native Ubuntu machine for this type of development. Even though Ubuntu uses an easy-to-use package system, there were some problems in finding a version of GCC ARM Embedded tool-chain that was compatible with Contikis built-in simulator Cooja [34, 35]; eventually, version 4.82 was used to successfully build Contiki. Cooja is a useful tool for testing and debugging network configurations but does not have support for the CC2538 MCU; instead, nodes called Cooja Motes are simulated with generic hardware. As Cooja is written in Java and runs in a JVM, Oracle Java 1.8 was also installed.

3.3.1 Drivers and firmware

Figure 3.3 shows an overview of the full system. The foundation is the SoC with the MCU, transceiver, and sensors. The Contiki operating system implements the soft real-time kernel together with the firmware for the SoC/MCU and the drivers for the peripherals and sensors. The last part is the communication stack, which provides TCP and UDP connectivity over 6LoWPAN. On top of the TCP and UDP protocols, HTTP and/or CoAP can be implemented. The firmware required for the OS to work properly on the hardware platform was already implemented. However, the drivers for the I 2 C bus and the sensors were not implemented. The I 2 C driver is required for the sensor drivers which in turn enables the MCU to communicate with the sensors on the OpenBattery platform.

3.3.2 CoAP server

In order to make each nodes sensor data accessible, a CoAP sever was implemented as an application running on top of Contiki. A CoAP server in general can handle any number of

resources; in this implementation, one resource was made for each sensor value i.e. temperature, light, humidity, and core voltage. The temperature, light, and humidity sensors all work in a similar fashion. When their value is requested, the I 2 C bus is initialized and then a request is sent over the bus. When the response with the value arrives, that data is put into either a plain-text or JavaScript Object Notation (JSON) formatted message depending on the request and then sent back to the requester. As the core voltage sensor is part of the MCUs ADC, that value is retrieved by simply getting data from a register (a somewhat faster operation). As a buffer for testing throughput speed was also needed, a resource with a circular buffer was implemented. This resource is configured with CoAPs block-wise transfer functionality for arbitrary data size; however, the buffer in itself is only 1024Kb to allow the program variables to fit into the ultra low leakage SRAM. For testing purposes, the data could have been discarded instead of actually saved into the buffer, but then the transfer can not be verified. Resources are defined by paths as CoAP works in a very similar way as HTTP.

Each resource is registered in the server with its path, media type, and content type. When a package arrives on the CoAP port, the server starts to break down the package to be able to direct it to the right resource. It starts with verifying that the package is actually a CoAP package, and then it checks the path and sends it to the correct resource. The resource then inspects the method field in the package header to direct the incoming data to the right function. CoAP package method can be either GET, PUT, POST or DELETE. This function then inspects the request media type and answer content type so that the function can parse the request and send a correctly formatted answer. If the resource does not implement the received method, the server responds with 405 Method not allowed and if the content/media type is not supported the answer is 415 Unsupported Media Type. The content/media types are text/plain, application/json, application/exi, and application/xml.

Testing

Contiki is shipped with a simulation tool called Cooja which is written in Java; it can simulate an arbitrary number of nodes with different roles and configurations. All simulation data, such as radio packages and node serial output may be viewed through different windows and exported to various formats. Unfortunately Cooja did not have support for ARM Cortex-M3, but the general set-up was still tested by using Cooja Motes, which are nodes without specified hardware, and MSP430 nodes such as Wismote or Skymotes. With this simulator the basic understanding of the communication between nodes was gained; also, before the hardware arrived, early testing was performed to test the OS and application software.

Final prototype

The final prototype consists of four OpenBattery nodes and one OpenBase border router. Both the nodes and the border router are deployed with Contiki. Each node runs a CoAP server, described in section 3.2.2, on top of the OS in its own thread. The border router runs a router software called 6lbr that acts a as translator between Ethernet and IEEE 802.15.4 [36]. Both types of hardware are configured with a 8Hz Radio Duty Cycle (RDC) driver to keep the power consumption to a minimum. RDC is a OS driver that cycles the listening mode of the transceiver to reduce power consumption. As Contiki puts the MCU into Low Power Mode (LPM) when no function is running and the transceiver is off, the RDC driver indirectly controls when the MCU is in LPM. When using the RDC

protocol, the nodes repeatedly send messages until the target node wakes up and sends an Acknowledge packet (ACK); this makes communication seamless, even though most of the time the nodes transceivers are not active. Also, an always-on RDC driver, where the transceiver is constantly listening, will be used to be able to look at the performance impact of the 8Hz RDC.

3.4 Evaluation

In this chapter the results from each type of assessment are presented. The first assessment is range, followed by response time, after that connection speed, and finally the power consumption. The only assessment that is not performed on the prototype is the range assessment.

3.4.1 Range

Range is very hard to measure without advanced equipment and isolated rooms but can be roughly estimated with equation 4.1 called Friis range equation [37]. P t is the sender transmit power, P r the receiver sensitivity, d is the distance between the antennas in meters, f is the signal frequency in hertz, and is the wavelength. G t and G r is the antenna gain for the trans- mitter and the receiver. The last term in equation 4.1, when inverted, is the Free-space path loss (FSPL) and can be expanded as shown in equation 4.3. P r (dB) = P t + G t + G r + 20 log 10 ( ) 4d c f FSPL(dB) = 20 log 10 (d) + 20 log 10 (f) 147.56 = (4.1) (4.2) (4.3) Unlike Friis range equation, the Link budget equation 4.4 also takes external loss like FM into account [38]. This is needed to make a correct estimation of the actual range as there are several things in the environment that obstructs and distorts the signal. P r = P t + G t + G r FM FSPL (4.4) Combining equation 4.1, 4.3 and 4.4 gives us the equation for the estimated distance as seen in equation 4.5. d = 10 x P t + G t + G r P r F M + 147.56 20 log 10 (f)

With this equation an estimation of the transceiver range can be made for different FMs and transmit powers. When deployed, the transceiver is configured to only accept packages with a signal strength of -70dBm and above to minimize packet loss and corruption. The antenna gain for OpenMote is 0dBi and can thus be omitted. Figure 4.1 shows a comparison between three different levels of FM: 0dB, 10dB, and 20dB. A FM of 0dB means that there is no signal loss except the FSPL and this is very hard to achieve outside of a lab environment. When increasing the FM to 10dB, which corresponds to a normal home environment, the maximum range drops to 22m. However, in these kind of environments the desired range is usually around 10m which would let the device reduce the transmit power to around 0dBm. Finally, the FM is increased to 20dB which is roughly what it would be in a office or industrial environment. The maximum range in this environment is now reduced to only 7m when transmitting at maximum power.

Response time Before measuring the response time, some theoretical estimations are needed to be able to evaluate the real values. The theoretical values are based upon the radio duty cycle (RDC) and the average response time to reach a node can thus be derived from equation 4.6, 4.8, 4.9 and 4.10. As each node only

3.4.2 Response time

Before measuring the response time, some theoretical estimations are needed to be able to evaluate the real values. The theoretical values are based upon the radio duty cycle

(RDC) and the average response time to reach a node can thus be derived from equation 4.6, 4.8, 4.9 and 4.10. As each node only checks the radio every 125ms, this duration combined with the data packet send time of 4ms (equation 4.7.) and ACK send time corresponds to the worst case delivery, as the node needs to wait a whole cycle before being able to send the package the desired node. When the target node is already listening, the best case delivery time is 5ms. Thus, the average theoretical delivery time to reach any adjacent node is 67.5ms. Radio duty cycle: Transfer time: 1s = 0.125s = 125ms 8 (4.6) 133B + 4B 4ms 31.25KB/s (4.7) Worst case delivery: 125ms + 4ms + 1ms (4.8) Best case delivery: 4ms + 1ms (4.9) 130ms + 5ms = 67.5ms (4.10) 2 The delivery time is only calculating the time to send a packet over a link, but when calculating the response time, the acknowledge (ACK) response has to be included in the calculation. Each ACK also needs to wait for the target node to be awake, adding one more instance of average delivery time, resulting in 125ms in average response time. This time will multiply with each hop, resulting in equation 4.11, 4.12 and 4.13. Avg. delivery: Avg. response time: (2 ů 67.5ms) ů hops (4.11) Best case response time: (2 ů 5ms) ů hops (4.12) Worst case response time: (2 ů 130ms) ů hops (4.13) After doing a test with real nodes set-up with a 8Hz RDC with three hops, as seen in figure 4.2, the values in table 4.1 were obtained. Each node was pinged 200 times at a one minute interval to simulate some traffic on the network. What can clearly be seen in the average field of the table is that the average of 765ms is much higher than the expected average of 135ms; the difference is mainly due to the worst-case pings that in some cases had response times up to 30 seconds. However, when looking at the geometrical mean which is better at smoothing out big spikes seen in figure 4.3, the observed response time is still 265ms which is a bit longer than the expected worst case response time for one hop. Also, for two and three hops the observed average is high, but the geometrical mean shows that this is due to the spikes. The estimated response time for two hops is 270ms which as seen in the geometrical mean table 4.1 is way off by 500ms. The same observation goes for three hops where the observed geometrical mean response time is 1181ms which compared to the estimated response time of 405ms is significantly higher.

With these observations in mind, the estimation could be described much better with equation 4.14. which would result in an average response time of 266, 532 and 1064 ms for one, two and tree hops. However, this would mean that the response time is doubled for one hop and then doubled for each consequent hop making the response time exponential which should not be the case.

With the RDC disabled, i.e. the transceiver is always listening and the MCU does not go into sleep mode, the response time is completely different. As seen in table 4.2 the average response time is around 12ms per hop and the spikes seen in the response time for 8Hz RDC is gone. Furthermore, the estimated best case response time of 10ms is very close to the observed average response time. The response time also scales to the number of hops as expected and is roughly 12ms per hop. It appears there might be a problem in

3.4.3 Connection speed

Connection speeds can be measured in several ways each with their own different pros and cons. One of the most popular ways is throughput, i.e. the amount of data over the link is divided by the time it took to reach the target. However, this gives a false picture of how fast the connection actually is from the developers point of view, as the measured data does not only contain application data but also headers and checksums. IEEE 802.15.4 has a theoretical data rate of 250kb/s as seen in equation 4.15. but this is only

a measure of how many bits per second the transceiver is able to output. The application data part, when using no header compression, is only 41% of the total transfer. Thus, resulting in a theoretical application data rate, also called goodput, of only 12.81KB/s. Data rate: 250kb/s = 31.25KB/s 133B 54B = 0.59 133B Theoretical goodput: 31.25KB/s ů (1 0.59) = 12.81KB/s Overhead: (4.15) (4.16) (4.17) When using CoAP as the application level protocol, each package can carry either 32 or 64 bytes of application data. In practice, the 64B mode is only applicable when sending packages between nodes on the same mesh network, as the addressing fields then can be fully compressed. When using applications outside the mesh network, each package can only carry 32B of data, resulting in a packet size of 111B as shown in equation 4.18; this does not affect the theoretical data rate but has a noticeable impact on the goodput due to the large overhead of 71as shown in equation4.19. To be able to use the full data rate, the application needs to use a protocol without handshakes, i.e. UDP, as the transceiver then can send the packets as fast as physically possible. CoAP is implemented on top of UDP and thus has a low transport layer overhead, but uses its own mechanism for handshaking, delivery and ordering. The theoretical CoAP application throughput can be estimated by looking at the average response time of the node and then add that time to the the data delivery time. Each package needs to be acknowledged before the next package is sent, and thus the node response time needs to be taken into consideration. When doing so, the throughput as calculated in equation 4.20. is only 1.64KB/s and thus the theoretical goodput is reduced from 12.81KB/s down to 0.48KB/s as shown in equation 4.21. Packet size: 133B 54B + 32B = 111B Actual overhead: 79B = 0.71 111B (4.18) (4.19)

Using the packet size of 111B together with the theoretical response time from equation 4.11 would give the results shown in figure 4.4. To verify these calculations, the same test set-up as shown in figure 4.2, which also was used in section 4.2, was used to test throughput and goodput at different number of hops. Each node was sent 1KB data each minute for 200 minutes; the time from the first package sent to the final acknowledge packet received was measured for each 1KB transmission. The first test was performed with an RDC of 8Hz and resulted in the values shown in figure 4.5. As the chart shows, the theoretical throughput and goodput is much higher than the observed values, but this is due to the fact that the actual average response time is higher than the theoretical one. With some calculations made the observed throughput and goodput are within range of what is expected, given the observed response times in table 4.1. Equation 4.22 uses the observed values to calculate the average response time, given the values in figure 4.5.

3.4.4 Power consumption

To measure power on devices that use very low power and also changes the power consumption very rapidly and frequently is not an easy task. According to the currency specification from the CC2538, the different power modes have the consumption seen in table 4.3 using the built in voltage regulator TSP6750 that switches the input voltage down from the 3V to 2.2V. The components on the OpenBattery supplied directly by the 3V batteries have the current and power consumption specifications as seen in table 4.4.

Given these power profiles, combined with the time it takes to receive and transmit packages, and retrieve a measurement, the theoretical power for one RDC cycle results in the chart seen in figure 4.7. The node starts in sleep mode using 112.81W and after 109ms wakes up and goes into RX mode where a request for a sensor value is received. The node then switches off the radio and fetches the sensor value. After the value is retrieved from the sensor, the radio is once again put in to RX mode for a Channel Clear Assessment

(CCA) before entering TX mode and sending the payload. The transmission is successful and the node goes into RX mode to listen for the ACK, when it is received the node enters sleep mode again. For this cycle the average power consumption is 4.8mW which would drain the 2250mWh batteries in 19 days.

However, as the nodes have a RDC running at 8Mz, most of the time there will be no package for the node to receive and thus no measuring and transmitting, as seen in figure 4.8. This cycling reduces the average power consumption to 0.47mW, which would make the batteries last for ca 200 days. The goal is to have a node that can run for one year without having to change the batteries and to be able to do this on 2xAAA batteries with 750mAh the average consumption has to be under 257W as calculated in

To verify these assumptions, we used a Keithley 2280S power supply [39] to measure the total current draw of the prototype. The node was connected to the power supply, which was set up to make 277 measures each second with a supply voltage of 3V. Several measurements were performed. One of the most interesting ones can be seen in figure 4.9. In this picture, we can clearly see the different operating modes, as the node performs 3 transmissions during the interval. In the first transmission at the 1.6s mark, the strobing feature of the RDC protocol is seen as the package is sent 5 times before the receiving node is awake and can receive the package. In the two following transmissions, the package is delivered on the first try. As our measurement is limited to 277Hz, the current peaks when only waking up to listen for traffic are sometimes missed, and the peak value is hard to extract; but the 8Hz RDC cycle is still visible. The average power consumption for these cycles is 8mW, which would make the batteries only last for 11 days. However, when taking the average of a measuring series without any transmissions, the average goes down to 4mW, which increases the battery time to 23 days. The theoretical sleep power of 0.11mW compared to the measured of 3mW is what makes the average power consumption that high.

Reducing this power consumption by a tenfold would result in an average consumption of 0.39mW, which is closer to the theoretical average power consumption. A discovery made when measuring the power was that the nodes consumed less power when supplied with a lower input voltage. Simply by reducing the voltage from 3V to 2.6V reduced the power consumption in LPM by 15%. However, this reduction could affect the range of the nodes.

3.5 Discussion

Internet of Things can be realised in several ways as there are still many viable options on the market, mainly in terms of hardware, operating systems, and communication standards. Given the recent development in the field, Thingsquare recently released a technology demo using the same practices as used in this thesis; the choices taken are on track with the latest development [40]. Also, both Google and Microsoft have announced that they are developing IoT OSs. When these products are released, it would be very interesting to compare them with Contiki. It would be exciting to see if an open-source project can surpass the commercial offerings in terms of speed, RAM and ROM footprint, and device support. Furthermore, an in-depth comparison between RIOT and Contiki would give much insight into the kind of OS practices that benefit IoT development the most. Google have also started to develop a substitute for 6LoWPAN and UDP that they have named Thread [41]. As 6LoWPAN and ZigBee, it runs on top of IEEE 802.15.4 and thus might be able to out-compete the existing implementations. Google promises lower latencies and power consumption compared to the existing technologies.

3.5.1 The prototype

The prototype development took more time than initially planned; mostly because of the complexity of the OS, but also due to bugs in the untested drivers. The prototype combines the technology from each field, i.e. hardware, OS, and communication protocol, and fulfils the requirements set in section 3.1.1. Even though the OS is relatively simple, compared to Linux, Windows, and OS X, understanding the mechanics of the RDC driver and the LPM driver was difficult, but necessary to be able to interpret the test results. The prototype worked very well during most of the testing, with only a few unforeseen deviations. One occurred during the power measurement, where the power consumption in low power mode tripled in one of the test series; this behaviour could not be reproduced and is therefore not included in the results. Also, in the early stages when working with the 8Hz RDC driver, packet losses over 50% were recorded for packets with more than one hop; this problem was solved, when a new version of radio driver was released by the OS development team. Selecting OpenMote to be the hardware platform together with Contiki as the OS, was a very good choice as companies are starting to build their IoT solutions around Contiki and similar hardware platforms [42, 43]. Already in the beginning of the development, several benefits were noticed; new drivers and bug-fixes were released increasing the stability and functionality of the OS. The active community around the combination of OpenMote and Contiki was really helpful when developing the drivers for the I 2 C and sensor drivers. Example projects for other platforms could be used as references, giving much insight to how the programming for this type of OS worked. It would have been interesting to examine the differences between two operating systems; not only to test which one has the better performance, but also to compare which one that has the more favourable code structure and development procedure.

Results

Collecting the data went well and were reasonably straight forward; it was easy to transition between the two different test set-ups and thus making several test scenarios. Assessments were made in the areas of range, response time, connection speed, and power consumption. In each area, the theoretical values were first calculated and then compared to the retrieved measurements; except in the range case, as the required equipment for measuring was not economically justifiable to purchase.

Range The theoretical range for OpenMote when transmitting at full power in an office environment is only 7m. As measuring the range was not a viable option due to the cost of measuring equipment, only distance estimations from the placement of the nodes when maintaining a stable connection can be used as a reference. Using a map of the office and the position of the nodes the range seems to be around 10m, which would mean that the effective FM of the office is around 16dB using the always-on RDC. The FM changed a bit when using the 8Hz RDC as more packages congested the air and the range dropped to somewhere around 5m; resulting in an effective FM of 23dB. To increase the range of the transceiver, a switch to the 860MHz frequency band would be the most effective solution; with a FM of 23dB, the theoretical range would increase to 14m with the same transceiver properties, and with a FM of 16dB the range would be 31m. Usually, transceivers with a lower frequency output also have a lower power consumption while transmitting. Working in sub-GHz also gives the benefit of less interference as fewer other devices uses those frequencies. Changing to a sub-GHz band would thus decrease the power consumption and increase the range, without changing the functionality of the nodes.

Response time Initially when measuring the response time the always-on RDC was used and the measured response time was very close to the theoretical value. However, when using the 8Hz RDC protocol the values started to drastically differ from the theory. This behaviour is likely to originate from the way the RDC driver predicts the next time when the target node should be awake. The procedure is called phase optimization; when enabled, the node saves the time when the node was last seen, it then uses this value to predict the next time the node should be awake based on the RDC cycle. However, this prediction is based on the nodes internal clock. As the clock can differ from those of the other nodes, misalignments seem to occur, resulting in misses when trying to reach the target node. Each misalignment increases the time it takes to reach the target node as the node then needs to strobe the package until the target nodes wakes up again. In theory, when sending strobes the target node should wake up and receive the package within one cycle (125ms); however, this is not guaranteed as other transmissions might occupy the air, further increasing the response time. If the phase optimization could be improved to guarantee the alignment between the nodes, the response time should get much closer to the theoretical value; as the time to reach the node would be maximum one cycle and the air would not be as congested by nodes sending strobes.

Connection speed The connection speed, when using CoAP or any other protocol with perpacket ACK, is directly bound to the response time. IEEE 802.15.4 has a relatively low data-rate, only 250kbps, compared to other solutions, e.g. BLE (1Mbps) and WLAN (>54Mbps). As throughput is based on datarate over a longer period of time, both the overhead and the response time is needed to make a good estimation. CoAP has a very low header size compared to many other communication protocols, but due to the very small frame size, the overhead is still relatively high. As of now, the results clearly show that when a reliable transfer is desired the connection speed of IEEE 802.15.4 and CoAP is only sufficient for data exchanges around 32 bytes. When the nodes use the always-on RDC, the goodput is less than 3KB/s for one hop and is halved for every hop; however, when the 8Hz RDC is enabled, the goodput is reduced to under 0.1KB/s. Using messages without per-packet ACK, thus removing the response time from the equation, would let the nodes transfer real-time audio and maybe even highly compressed video. However, using messages without the per-packet ACK disables the reliable transmission guarantee, and thus it can only be used with data streams where packet loss is acceptable.

Power consumption Making a rough estimation of the power consumption of the platform was straight forward task and so was measuring the actual consumption. When comparing, the two the values differed by a factor of 30, which was not expected. The reason probably originates from the clock interrupt which is triggered every 8ms. Initially, this interrupt was assumed to be disabled when the system entered the lower power modes, but this was not the case. As the interrupt fires at 125Hz and the time to wake up and go back to LPM is only 272s, the power spikes from these interrupts were not seen on the measuring instruments. As seen in figure 4.9, even the peaks from the listening cycles were hard to record and those lasted for at least 4ms; instead, the power consumption from the clock timer looks like an increased LPM power consumption. At the time this was discovered there was no time to fix it, but doing so should decrease the average power consumption to within the limits, granting the nodes the ability to run on battery power for a year. As no delays from calculation could be observed, the clock speed on MCU could, in all probability, have been reduced to save power on the nodes. However, this reduction would only have affected the consumption when the node was in active mode,

which is only a few percent of the total cycle time. The OpenMote chip has a step-down DC-DC converter for this purpose which is switched off in LPM mode to reduce quiescent currents; however, as most of the time is spent in LPM, reducing the input voltage to 2.1V by changing battery type and removing the step-down converter would be preferable as it would reduce the power consumption. These changes could affect the range of the device, but this has to be assessed.

3.5.2 Project execution

Looking at the time plan and the milestones, as seen in Appendix A and B, each milestone matches a task or transition in the time plan. The planning report was not submitted to the examiner until the 6/2-15, which is two weeks behind schedule, exceeding the time planned for milestone M1. The first draft was submitted before deadline, but several revisions were necessary. In retrospect, the litterature study should probably have been planned in parallel with the planning report, as the information from the study helped with the report. Milestone M2 marks the switch from the literature study and selection of technology to the development phase. This milestone was met and development could begin in the following week. As seen in Appendix C, the development phase have several risks to consider. The only risk encountered in this phase was R4, as one of the hardware platforms was delivered with a broken sensor. However, this malfunction did not affect the time plan as the development could continue regardless of the malfunction. The end of the development phase was defined by milestone M3, approval of prototype, which was completed ahead of schedule granting an early transition into the assessment phase. In the assessment phase, it could be argued that risk R9 was encountered when measuring the power consumption, as the results from those measurements did not properly show the wake-ups from the clock timer. This phase contained milestone M4 and M5, of which of only M5 was done in time. The Half-time presentation, milestone M4, was performed on the 8/4-15 in the form of a meeting, where the progress, results and continuation plan were discussed. Also, a half-time version of the report was sent the 17/4-15 and approved by the examiner. Milestone M6, deliver the final prototype, was completed a few days before the set deadline which eliminated risk R11 and gave more time to work on the writing and the presentation. Both of the oral presentations were attended on the 1/6-15 to grant some experience in how the presentation and opposition are carried out, thus now following the time plan. However, there were not many presentations to watch during the planned weeks, as the presentation schedule follow the academic semesters. The presentation for this thesis was not performed until the 3/6-15, thus being two weeks behind schedule. However, it was scheduled on the first available date suggested by the institution. The final version of the report will be submitted to the examiner before the 19/6-15, thus successfully completing milestone M7.

3.6 Conclusion

The purpose of the project was to find and examine a communication protocol that could be suitable for IoT applications, by investigating the current hardware, OS, and communication protocols and building a prototype from the selected choices. What can be said about the investigation is that it is difficult to examine all candidates in detail; this means that a rough selection has to be made based on initial knowledge potentially discarding good options. The general feeling is, however, that all of the examined candidates in this project were relevant and added valuable insights to the current technology status.

The assessment gave relevant and interesting results that improved the understanding in what IoT can be used for, and what further areas of investigation could be. One of the most interesting areas of further investigation would be the RDC driver, as it directly affects the response time and thus also the connection speed. Even though the power consumption was not in line with the expectations, the reason has been found and can be resolved. Another conclusion is that IoT is not ready for real-time applications as the latency is much higher than expected, for the technologies assessed in this thesis, and also has a high spread. As the latency increases for each subsequent network hop and the minimum observed latency per hop is 11ms, when using the always-on RDC, this type of communication will probably only be used for applications where response time can vary greatly, without affecting the functionality. CoAP as a communication protocol shows a lot of promise when combined with 6LoWPAN and IEEE 802.15.4. It performs well given its simplicity but has one disadvantage: the large overhead which comes from the MAC addressing fields in the IEEE 802.15.4 frame. If this overhead could be reduced from the current 71% to only 30the goodput would double. A solution would be to use a similar mechanism as BLE where the packet size varies depending on application. Each node also has computing time left as the MCU is more powerful than needed for the given application; an improvement would be to use a less powerful MCU, like the ARM Cortex-M0+, to reduce the clock speed as suggested in the discussion. When looking at the future-proof aspect the later suggestion is probably the better, as the clock then could be increased if more computing power is needed. In the future, batteries will hopefully be able to store more energy, thus increasing the time between battery changes or reducing the battery size.

4 | SDN: Sentilo [22]

4.1 Introduction & problem statement

From the start of the computer networks, to the mobile applications nowadays, the amount of information shared has been constantly increasing. We have all kind of devices, from the big servers in datacenters, the TVs at home, mobile phones, car sensors, ... The Internet Of Things (IOT) refers to the idea of connecting all the thingsto the Internet. By things, it refers to any ordinary object that can be useful getting information. These things should be connected by an embedded device, capable to connect to the Internet in one side, and get information from the thing on the other.

4.1.1 Background

4.1.2 Purpose (Goal)

The first objective of this thesis is to document the capabilities of the Z1 motes and the Contiki OS for the IOT, by building applications to gather data from sensors and the network capabilities both from the motes and the OS. Secondly, to build an application using the Z1 motes, and the Contiki OS, using COAP(Constrained Application Protocol) and 6LoWPan(IPv6 over Low power Wireless Personal Area Networks) to retrieve information from the motes, and connect them to Sentilo, an open source sensor and actuator platform.

4.1.3 Limitations

There has been an increased research and development for the Smart Cities. The smart cities objective is to gather information from the city, to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. This project is intended to approach two goals, to be used as a starting point for anyone who wants to use the Contiki OS with the Z1 motes, and to build a simple application for the Smart Cities, to collect data from sensors, and sending it to an information center.

4.1.4 Method

This document is divided in two parts. First, the description of the main tools used to create the experimental environments. A description of the Contiki OS, the Z1 motes, and the protocols used to communicate, IEEE 802.14.5, 6LowPAN and CoAP. The a brief description of the sensor data collector Sentilo Secondly, a description of the environment setup, and an explanation of how it works. Finally, conclusions and future work is presented.

4.2 Background

4.2.1 Requirements

4.2.2 Hardware: Zolertia Z1 Motes

The Z1 is a low power wireless module compliant with IEEE 802.15.4 and Zigbee protocols intended to be used for Wireless Sensor Networks. This mote has support for Tiny OS, Contiki OS, OpenWSN and RIOT. The MCU architecture is based upon the MSP430 and the radio transceiver on CC2420 architecture, both from Texas Instruments.

Peripherals ports

North Port

East Port

South Port

West Port A Z1 mote has 2 internal sensors, and using the external ports, can be connected to a variety of external sensors. The main issue about collecting data with Contiki is the lack of support for floating point numbers in the stdio library, because of the large amount of code it requires. It has floating point numbers, but those are only usefull for internal operations. If a program needs to send the decimal data to an external source, has to use integers in the stdio functions, to write into the buffers.

Internal sensors

Temperature Sensor The internal temperature sensor in the Z1 mote is the tmp102 sensor from Texas Instruments. This sensor is integrated with the z1 motes using the I2C interface. It can read the temperature range of -40oC to +125oC. The Contiki OS has his own library of functions that can read the sensor data, located in "platform/z1/dev/tmp102.h". To use it in a program, it has to include the library dev/tmp102.h

Accelerometer The internal accelerometer in the Z1 motes is the adxl345 from Analog Devices Inc. This sensor is integrated with the z1 motes using the I2C interface. The Contiki OS has his own library of functions that can read the sensor data, located in "platform/z1/dev/adxl345.h". To use it in a program, it has to include the library dev/adxl345.h The sensor has 8 different interrupts to enable and 2 pins for mapping the interrupts.

External Sensors

The Z1 motes have several ways to connect sensors. In the next chapters, there are some examples of sensors, and how to read the data.

Analog sensors To read the analog sensors, there is a Contiki library in platform/z1/dev/z1phidgets.h This library reads the values of 4 of the pins of the north ports, and returns a 16 bit register, representing the value. It uses a 12bits A/D converter, so the min value is 0 and the max in 4095.

Precision Light Sensor The precision light sensor used as an example is the Phidget P/N 1127 sensor. This sensor is an analog sensor that measures light intensities of up to 1000 lux. It is a non-radiometric sensor. The output value does not depend on the input voltage, but the input voltage will limit the maximum measurement value. The sensor can be connected to the north port of the Z1 motes, into the 3V port or the 5V port.

In Fig.60, to read the value of the sensor, the phidgets library from Contiki is used. After a raw read, the value is transformed to lux, knowing the maximum value of the A/D converter is 4095, and the maximum value the sensor can give is 1000 lux. (In this case is connected to 5V)

Force Sensor The force sensor used used as an example is the Phidget P/N 1106 sensor. This force sensor can be used as a button for human input or to sense the presence of a small object. It is a radiometric sensor. The output value depends on the input voltage. It measures the same force value with 3V or 5V.

In Fig. 64, to read the value of the sensor, the phidgets library from Contiki is used. Once the raw value is read, it is transformed it to Newtons, knowing the maximum value of the A/D converter is 4095, and the maximum value the sensor can give is 39.2 Newtons.

Relay actuator

The relay used as an example is the Electronic brick 5V Relay form seeedstudio.

This actuator, works as a switch, when a signal is sent through the signal pin. It has a library for the Z1 motes in platform/z1/dev/relay-phidget.h".

This library conflicts with the phidgets library, because it turns the selected pin from the north port as an output, and the phidgets functions as an input. In this configuration, the switch is powered with 5V supplied by the Z1 in the ON port, and with ground in the OFF port. It toggles the led on and off, each time the signal is triggered.

In Fig.68 example, the main loop waits for a specified time, and then toggles the relay.

Distance sensor

The distance sensor used as an example is the SEN-12784 from SparkFun. It has an VL6180 digital sensor integrated, that can read light and distance. It uses the an I2C interface to extract the values from the sensor registers.

Contiki has a I2C interface library adapter for the Z1 motes in platform/z1/dev/i2cmater.h To use it in a program, it has to include the library dev/i2cmaster.h

The function in Fig.71, shows how to read the distance from the device. It calculates the distance by sending a pulse of light, and retrieving it back, the doing an internal calculation with the difference between the power of the signal sent and the received. Between the activation and the collection of the value, there is some time waiting for the light to travel. The functions in Fig.71 and Fig.73, show how to set and get a register from the sensor, using the I2C interface.

4.2.3 Operating systems

Contiki is an open source operating system for the Internet of Things. Contiki connects tiny low-cost, low-power micro-controllers to the Internet.

Main aspects

2k RAM, 60k ROM; 10k RAM, 48K ROM Portable to tiny low-power micro-controllers I386 based, ARM, AVR, MSP430, ... Implements uIP stack IPv6 protocol for Wireless Sensor Networks (WSN) Uses the protothreads abstraction to run multiple process in an event based kernel. Emulates concurrency Contiki has an event based kernel (1 stack) Calls a process when an event happens

Contiki size

One of the main aspect of the system, is the modularity of the code. Besides the system core, each program builds only the necessary modules to be able to run, not the entire system image. This way, the memory used from the system, can be reduced to the strictly necessary. This methodology makes more practical any change in any module, if it is needed. The code size of Contiki is larger than that of TinyOS, but smaller than that of the Mantis system. Contiki's event kernel is significantly larger than that of TinyOS because of the different services provided. While the TinyOS event kernel only provides a FIFO event queue scheduler , the Contiki kernel supports both FIFO events and poll handlers with priorities. Furthermore, the flexibility in Contiki requires more run-time code than for a system like TinyOS, where compile time optimization can be done to a larger extent.

The documentation in the doc folder can be compiled, in order to get the html wiki of all the code. It needs doxygen installed, and to run the command make html. This will create a new folder, doc/hmtl, and in the index.html file, the wiki can be opened.

Contiki Hardware

Contiki can be run in a number of platforms, each one with a different CPU. Tab.7 shows the hardware platforms currently defined in the Contiki code tree. All these platforms are in the platform folder of the code.

Kernel structure

4.2.4 Communication protocol

Wireless sensor networks combines 3 concepts together: sensor + CPU + radio. However, combining sensors, radio and CPU's together requires an extensive understanding of the hardware components as well as modern networking technologies to connect the devices. Each node needs to have the necessary tools to send data over the radio channel, while meeting the requirements of size, cost and power consumption. The research and development of this kind of devices, has been increased over the last years. There are a number of operating systems focused on providing communications stacks and at the same time focused on saving power. On the other hand, the devices integrating a CPU and a radio transceiver have become more available and efficient.

Composition

There are four main types of nodes in a WSN structure. Sensor nodes: These nodes are in charge of collecting data, and sending it to the network. These nodes have 2 parts, the sensors board and the mote. The sensor board, contains the sensor to acquire data (light, temperature, humidity,...) The mote integrates the CPU and the radio transceiver. Route nodes: Nodes with the only purpose of making possible the link between the sensor nodes

and the rest of the network. They work as a repeater of the radio signal, and implement routing tasks. Server station: It is the concentrator of the data sent over the network. It is a node itself, or a node attached to a more powerful machine, able to manage lots of data. Gateway: Connects the WSN to an external network, if needed.

The transmission of sensor's data is done by all the nodes of the network. Each data packet, is sent to the server station hop by hop. Reducing the transmission power in the nodes, may reduce the power consumption on it, but it may require a larger number of hops to arrive to the server station

Physical and MAC Layer (IEEE 802.15.4)

At present days, there are several technology standards. Each one is designed for a specific need in the market. For the Wireless Sensor Networks, the aim is to transmit little information, in a small range, with a small power consumption and low cost. The IEEE 802.15.4 standard offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs)

Physical Layer The standard operates in 3 different frequency bands: - 16 channels in the 2.4GHz ISM band - 10 channels in the 915MHz ISM band - 1 channel in the European 868MHz band

Definitions Coordinator: A device that provides synchronization services through the transmission of beacons. PAN Coordinator: The central coordinator of the PAN. This device identifies its own network as well as its configurations. There is only one PAN Coordinator for each network. Full Function Device (FFD): A device that implements the complete protocol set, PAN coordinator capable , talks to any other device. This type of device is suitable for any topology. Reduced Function Device (RFD): A device with a reduced implementation of the protocol, cannot become a PAN Coordinator. This device is limited to leafs in some topologies.

Topologies Star topology: All nodes communicate via the central PAN coordinator , the leafs may be any combination of FFD and RFD devices. The PAN coordinator usually uses main power.

Peer to peer topology: Nodes can communicate via the central PAN coordinator and via additional point-to-point links . All devices are FFD to be able to communicate with each other.

Combined Topology: Star topology combined with peer-to-peer topology. Leafs connect to a network via coordinators (FFDs) . One of the coordinators serves as the PAN coordinator .

RIME

RIME is a communication stack designed for Contiki. It provides a hierarchical set of wireless network protocols. This protocol stack can send data over the standard IEEE 802.14.5 with very few transmissions and less overhead than an IP based protocol, saving energy in the devices involved in the connection. Implementing a complex protocol (say the multi-hop mesh routing) is split into several parts, where the more complex modules make use of the simpler ones.

These are some of the different modules of Rime:

abc: the anonymous broadcast, it just sends a packet via the radio driver, receives all packets from the radio driver and passes them to the upper layer; **broadcast:** the identified broadcast, it adds the sender address to the outgoing packet and passes it to the abc module;

unicast: this module adds a destination address to the passed packets to the broadcast block. On the receiver side, if the packet's destination address doesn't match the node's address, the packet is discarded;

stunicast: the stubborn unicast, when asked to send a packet to a node, it sends it repeatedly with a given time period until asked to stop. This module is usually not used as is, but is used by the next one.

runicast: the reliable unicast, it sends a packet using the stunicast module waiting for an acknowledgement packet. When it is received it stops the continuous transmission of the packet. A maximum retransmission number must be specified, in order to avoid infinite sending.

polite and ipolite: these two modules are almost identical, when a packet has to be sent in a given time frame, the module waits for half of the time, checking if it has received the same packet it is about to send. If it has, the packet is not sent, otherwise it sends the packet. This is useful for flooding techniques to avoid unnecessary retransmissions.

multihop: this module requires a route table function, and when it is about to send a packet it asks the route table for the next hop and sends the packet to it using unicast. When it receives a packet, if the node is the destination then the packet is passed to the upper layer, otherwise it asks again the route table for the next hop and relays the packet to it.

6LowPAN

6LoWPAN is a networking technology or adaptation layer that allows IPv6 packets to be carried efficiently within a small link layer frame, over IEEE 802.15.4 based networks. As the full name implies, IPv6 over Low-Power Wireless Personal Area Networks, it is a protocol for connecting wireless low power networks using IPv6.

As the full name implies, IPv6 over Low-Power Wireless Personal Area Networks, it is a protocol for connecting wireless low power networks using IPv6.

Characteristics

- Compression of IPv6 and UDP/ICMP headers
- Fragmentation / reassembly of IPv6 packets
- Mesh addressing
- Stateless auto configuration
-

Encapsulation Header format All LowPAN encapsulated datagrams are prefixed by an encapsulation header stack. Each header in the stack starts with a header type field followed by zero or more header fields.

Fragment Header The fragment header is used when the payload is too large to fit in a single IEEE 802.15.4 frame. The Fragment header is analogous to the IEEE 1394 Fragment header and includes three fields: Datagram Size, Datagram Tag, and Datagram Offset. Datagram Size identifies the total size of the unfragmented payload and is included with

every fragment to simplify buffer allocation at the receiver when fragments arrive outoforder. Datagram Tag identifies the set of fragments that correspond to a given payload and is used to match up fragments of the same payload. Datagram Offset identifies the fragments offset within the unfragmented payload and is in units of 8-byte chunks.

Mesh addressing header The Mesh Addressing header is used to forward 6LoWPAN payloads over multiple radio hops and support layer-two forwarding. The mesh addressing header includes three fields: Hop Limit, Source Address, and Destination Address. The Hop Limit field is analogous to the IPv6 Hop Limit and limits the number of hops for forwarding. The Hop Limit field is decremented by each forwarding node, and if decremented to zero the frame is dropped. The source and destination addresses indicate the end-points of an IP hop. Both addresses are IEEE 802.15.4 link addresses and may carry either a short or extended address.

Header compression (RFC4944) RFC 4944 defines HC1, a stateless compression scheme optimized for link-local IPv6 communication. HC1 is identified by an encoding byte following the Compressed IPv6 dispatch header, and it operates on fields in the upper-layer headers. 6LoWPAN elides some fields by assuming commonly used values. For example, it compresses the 64-bit network prefix for both source and destination addresses to a single bit each when they carry the well-known link-local prefix. 6LoWPAN compresses the Next Header field to two bits whenever the packet uses UDP, TCP, or ICMPv6. Furthermore, 6LoWPAN compresses Traffic Class and Flow Label to a single bit when their values are both zero. Each compressed form has reserved values that indicate that the fields are carried inline for use when they dont match the elided case. 6LoWPAN elides other fields by exploiting cross-layer redundancy. It can derive Payload Length which is always elided from the 802.15.4 frame or 6LoWPAN fragmentation header. The 64-bit interface identifier (IID) for both source and destination addresses are elided if the destination can derive them from the corresponding link-layer address in the 802.15.4 or mesh addressing header. Finally, 6LoWPAN always elides Version by communicating via IPv6.

The HC1 encoding is shown in Figure 11. The first byte is the dispatch byte and indicates the use of HC1. Following the dispatch byte are 8 bits that identify how the IPv6 fields are compressed. For each address, one bit is used to indicate if the IPv6 prefix is linklocal and elided and one bit is used to indicate if the IID can be derived from the IEEE 802.15.4 link address. The TF bit indicates whether Traffic Class and Flow Label are both zero and elided. The two Next Header bits indicate if the IPv6 Next Header value is 7UDP, TCP, or ICMP and compressed or carried inline. The HC2 bit indicates if the next header is compressed using HC2. Fully compressed, the HC1 encoding reduces the IPv6 header to three bytes, including the dispatch header. Hops Left is the only field always carried inline.

RFC 4944 uses stateless compression techniques to reduce the overhead of UDP headers. When the HC2 bit is set in the HC1 encoding, an additional 8-bits is included immediately following the HC1 encoding bits that specify how the UDP header is compressed. To effectively compress UDP ports, 6LoWPAN introduces a range of wellknown ports (61616 61631). When ports fall in the well-known range, the upper 12 bits may be elided. If both ports fall within range, both Source and Destination ports are compressed down to a single byte. HC2 also allows elision of the UDP Length, as it can be derived from the IPv6 Payload Length field.

The best-case compression efficiency occurs with link-local unicast communication, where HC1 and HC2 can compress a UDP/IPv6 header down to 7 bytes. The Version,

Traffic Class, Flow Label, Payload Length, Next Header, and linklocal prefixes for the IPv6 Source and Destination addresses are all elided. The suffix for both IPv6 source and destination addresses are derived from the IEEE 802.15.4 header.

However, RFC 4944 does not efficiently compress headers when communicating outside of link-local scope or when using multicast. Any prefix other than the linklocal prefix must be carried inline. Any suffix must be at least 64 bits when carried inline even if derived from a short 802.15.4 address. As shown in Figure 8, HC1/HC2 can compress a linklocal multicast UDP/IPv6 header down to 23 bytes in the best case. When communicating with nodes outside the LoWPAN, the IPv6 Source Address prefix and full IPv6 Destination Address must be carried inline.

Header compression Improved (draft-hui-6lowpan-hc-01) To provide better compression over a broader range of scenarios, the 6LoWPAN working group is standardizing an improved header compression encoding format, called HC. The format defines a new encoding for compressing IPv6 header, called IPHC. The new format allows Traffic Class and Flow Label to be individually compressed, Hop Limit compression when common values (E.g., 1 or 255) are used, makes use of shared-context to elide the prefix from IPv6 addresses, and supports multicast addresses most often used for IPv6 ND and SLAAC. Contexts act as shared state for all nodes within the LoWPAN. A single context holds a single prefix. IPHC identifies the context using a 4-bit index, allowing IPHC to support up to 16 contexts simultaneously within the LoWPAN. When an IPv6 address matches a contexts stored prefix, IPHC compresses the prefix to the contexts 4-bit identifier. Note that contexts are not limited to prefixes assigned to the LoWPAN but can contain any arbitrary prefix. As a result, share contexts can be configured such that LoWPAN nodes can compress the prefix in both Source and Destination addresses even when communicating with nodes outside the LoWPAN.

The improved header compression encoding is shown in Figure 8. The first three bits (011) form the header type and indicate the use of IPHC. The TF bits indicate whether the Traffic Class and/or Flow Label fields are compressed. The HLIM bits indicate whether the Hop Limit takes the value 1 or 255 and compressed, or carried inline.

Bits 8-15 of the IPHC encoding indicate the compression methods used for the IPv6 Source and Destination Addresses. When the Context Identifier (CID) bit is zero, the default context may be used to compress Source and/or Destination Addresses. This mode is typically when both Source and Destination Addresses are assigned to nodes in the same LoWPAN. When the CID bit is one, two additional 4-bit fields follow the IPHC encoding to indicate which one of 16 contexts is in use for the source and destination addresses. The Source Address Compression (SAC) indicates whether stateless compression is used (typically for link-local communication) or stateful context-based compression is used (typically for global communication). The Source Address Mode (SAM) indicates whether the full Source Address is carried inline, upper 16 or 64-bits are elided, or the full Source Address is elided. When SAC is set and the Source Addresses prefix is elided, the identified context is used to restore those bits. The Multicast (M) field indicates whether the Destination Address is a unicast or multicast address. When the Destination Address is a unicast address, the DAC and DAM bits are analogous to the SAC and SAM bits. When the Destination Address is a multicast address, the DAM bits indicate different forms of multicast compression. HC also defines a new framework for compressing arbitrary next headers, called NHC. HC2 in RFC 4944 is only capable of compressing UDP, TCP, and ICMPv6 headers, the latter two are not yet defined. Instead, the NHC header defines a new variable length Next Header identifier, allowing for future definition of arbitrary next header

compression encodings. HC initially defines a compression encoding for UDP headers, similar to that defined in RFC 4944. Like RFC 4944, HC utilizes the same well-known port range (61616-61631) to effectively compress UDP ports down to 4-bits each in the best case. However, HC no longer provides an option to carry the Payload Length in line, as it can always be derived from the IPv6 header. Finally, HC allows elision of the UDP Checksum whenever an 10upper layer message integrity check covers the same information and has at least the same strength. Such a scenario is typical when transportor application-layer security is used. As a result, the UDP header can be compressed down to two bytes in the best case.

RPL

RPL is a Distance Vector IPv6 routing protocol for LLNs that specifies how to build a Destination Oriented Directed Acyclic Graph (DODAG) using an objective function and a set of metrics/constraints. The objective function operates on a combination of metrics and constraints to compute the best path.

An RPL Instance consists of multiple Destination Oriented Directed Acyclic Graphs (DODAGs). Traffic moves either up towards the DODAG root or down towards the DODAG leafs. The graph building process starts at the root or LBR (LowPAN Border Router). There could be multiple roots configured in the system. The RPL routing protocol specifies a set of ICMPv6 control messages to exchange graph related information. These messages are called DIS (DODAG Information Solicitation), DIO (DODAG Information Object) and DAO (DODAG Destination Advertisement Object). The root starts advertising the information about the graph using the DIO message. The nodes in the listening vicinity (neighbouring nodes) of the root will receive and process DIO messages potentially from multiple nodes and makes a decision based on certain rules (according to the objective function, DAG characteristics, advertised path cost and potentially local policy) whether to join the graph or not. Once the node has joined a graph it has a route toward the graph (DODAG) root. The graph root is termed as the parent of the node. The node computes the rank of itself within the graph, which indicates the coordinates of the node in the graph hierarchy. If configured to act as a router, it starts advertising the graph information with the new information to its neighbouring peers. If the node is a leaf node, it simply joins the graph and does not send any DIO message. The neighbouring peers will repeat this process and do parent selection, route addition and graph information advertisement using DIO messages. This rippling effect builds the graph edges out from the root to the leaf nodes where the process terminates. In this formation each node of the graph has a routing entry towards its parent (or multiple parents depending on the objective function) in a hop-by-hop fashion and the leaf nodes can send a data packet all the way to root of the graph by just forwarding the packet to its immediate parent. This model represents a MP2P (Multipoint-to-point) forwarding model where each node of the graph has reach-ability toward the graph root. This is also referred to as UPWARD routing. Each node in the graph has a rank that is relative and represents an increasing coordinate of the relative position of the node with respect to the root in graph topology. The notion of rank is used by RPL for various purposes including loop avoidance. The MP2P flow of traffic is called the up direction in the DODAG.

The DIS message is used by the nodes to proactively solicit graph information (via DIO) from the neighbouring nodes should it become active in a stable graph environment using the poll or pull model of retrieving graph information or in other conditions. Similar to MP2P or up direction of traffic, which flows from the leaf towards the root there is a need for traffic to flow in the opposite or down direction. This traffic may originate

from outside the LLN network, at the root or at any intermediate nodes and destined to a (leaf) node. This requires a routing state to be built at every node and a mechanism to populate these routes. This is accomplished by the DAO (Destination Advertisement Object) message. DAO messages are used to advertise prefix reachability towards the leaf nodes in support of the down traffic. These messages carry prefix information, valid lifetime and other information about the distance of the prefix. As each node joins the graph it will send DAO message to its parent set. Alternately, a node or root can poll the sub-dag for DAO message through an indication in the DIO message. As each node receives the DAO message, it processes the prefix information and adds a routing entry in the routing table. It optionally aggregates the prefix information received from various nodes in the subdag and sends a DAO message to its parent set. This process continues until the prefix information reaches the root and a complete path to the prefix is setup. Note that this mode is called the storing mode of operation where intermediate nodes have available memory to store routing tables. RPL also supports another mode called non-storing mode where intermediate node do not store any routes.

4.2.5 Application protocol

COAP (COnstrained Application Protocol)

The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. More detailed information about the protocol is given in the Contiki OS CoAP section.

Overview Like HTTP, CoAP is a document transfer protocol. Unlike HTTP, CoAP is designed for the needs of constrained devices. The packets are much smaller than HTTP TCP flows. Packets are simple to generate and can be parsed in place without consuming extra RAM in constrained devices. CoAP runs over UDP, not TCP. Clients and servers communicate through connectionless datagrams. Retries and reordering are implemented in the application stack. It follows a client/server model. Clients make requests to servers, servers send back responses. Clients may GET, PUT, POST and DELETE resources. CoAP implements the REST model from HTTP, with the primitives GET, POST, PUT and DELETE.

Coap Methods CoAP extends the HTTP request model with the ability to observe a resource. When the observe flag is set on a CoAP GET request, the server may continue to reply after the initial document has been transferred. This allows servers to stream state changes to clients as they occur. Either end may cancel the observation. CoAP defines a standard mechanism for resource discovery. Servers provide a list of their resources (along with metadata about them) at /.well-known/core. These links are in the application/link-format media type and allow a client to discover what resources are provided and what media types they are.

Coap Transactions

Coap Messages The CoAP message structure is designed to be simpler than HTTP, for reduced transmission data. Each field responds to a specific purpose.

4.2.6 Workspace ant tools

4.3 Sentilo

Sentilo is an open source platform to store sensor and actuators information. This platform is designed for the smart cities environment, to be used as a sensor data server that stores the data from different providers and different components within the providers.

4.3.1 Definitions

Provider: A Sentilo account in the server. It stores the published data, and sends the data to his subscribers.

Publisher: A device that sends data to the server. It publish the data into a provider account.

Subscriber: A device that receives data. It is subscribed to a certain data from a provider

Worker: A threat in the server that executes a programed task

Redis: A in-memory data structure store. It is used as a Publisher/Subscriber implementation to store the data in the memory of the server.

MongoDB: A database that stores the data as 'documents'. A 'document' is a JSON object.

4.3.2 Sentilo Architecture

The platform has 3 distinct parts:

PubSub Server (Core)

Web Catalog Application (A web interface to check the information of the PubSub Server)

Extensions (Also called Agents, they extend the capabilities of the PubSub Server)

The core platform, listens and responds to requests specified in the API. By default, it listens the TCP port 8081

- For a publisher, it registers the data sent, in one of the platform items.

- For subscribers, it responds with a JSON with the requested data of an item.

The web catalog, is a web interface to manage and see the information on the PubSub Server. It listens the TCP port 8080. The platform supports some extensions in order to extend the base functionalities such as alerts or data storage.

PubSub Server

The Core of the platform is a running process, that listens to the requests and creates workers (Threads) to do the tasks. There are 2 requesters:

Publishers: Send data from sensors, and alerts.

Subscribers: First, they request a subscription. Then waits for the data they are subscribed is sent. The platform is separated in 2 different layers: Transport and Service. The transport layer manages the incoming requests (as published data, data requests or subscription requests) and generates a queue with tasks containing the information of the request. Then, a limited pool of workers handles the requests, every time each finishes the previous task.

When a client sends an Http request to the platform, the process is: (Fig. 76). 1.The server accepts the request. 2.Queues the request on the list of pending requests. 3.When

a Worker is available, a pending task is assigned to it for processing(removing it from the queue) (a) delegates the request to an element of the service layer (b) constructs the HTTP response from the information received. 4.Sends the response to the client's request

The service layer manages the workers information and processes it and registers the data or delivers the data depending on the request. (Fig. 77)

1.The Worker delegates the request to the associated handler depending on the type of request (data, order, alarm, ...)

2.The following validations are performed on each request: (a) Integrity of credential: checks the received token sent in the header using the internal database in memory containing all active credentials in the system. (b) Authorization to carry out the request: validate that the requested action can be done according to the permission database.

3.Stores the data in Redis (in memory), and depending on the type of data (a) Publish the data through publish mechanism (b) Register of the subscription in the ListenerMessageContainer (A list of all subscribers) and into Redis as a subscriber.

4. If any new data is received, Redis publish the data to the subscribers, otherwise this step is skipped.

5. The container notifies the event to each subscriber associated with it by sending an HTTP Request to them.

Web Catalog Application

The catalog application platform is a web application that uses MongoDB as data storage database. The Web App has 2 parts:

- A public console for displaying public data of components and sensors and their data

- A secured part for resources administration: providers, client apps, sensors, components, alerts, permissions, ...

It is fully integrated with the Publish/Subscribe platform for data synchronization:

- Permission and authentication data

- Register statistical data and the latest data received for showing it in different graphs of the Web application.

Extensions (Agents)

The extensions of Sentilo add functionalities to the Core application. The extensions are subscribed to the Redis module for all the incoming notifications.

When Redis receives a publication of data, sends a message to all subscribers, including all the agents. The agent gets the data, and carries out his task. Currently there are 3 Sentilo agents:

- Relational database agent

- Stores all the incoming data in a external database Alarm agent

- Manages the internal alerts defined into the Web Catalog and published an alert if the condition is met.

- Location updater agent

Is responsible of updating automatically the component location according to the location of the published observations.

4.3.3 Sentilo structure

The platform has 5 main items: - Component - Sensor - Alert - Alarm - Order A component is the item where a set of sensors is attached. A sensor is a representation of a physical sensor, it is attached to a component. The data published is sent for a specific sensor. An alert is a trigger registered in Sentilo when an event happens. There a 2 types of alerts: internal and external. The internal alerts are related to specific sensors and it's logic is defined using basic math rules or configuring an inactivity time. The external alerts are defined by third party entities, which will be the responsible of calculating their logic and throw the related alarms when applies. An alarm is the message sent to the subscribers of an alert when it is triggered. Must be attached to an alert. An order is a message registered for a specific sensor or component. It is received by the subscribers of the sensor or component orders.

4.3.4 Sentilo API

The Application Programming Interface (API) define a set of commands, functions and protocols that must be followed by who wants to interact with the platform from external systems, like sensors/actuators or applications. The requests are HTTP requests with 3 fields in the header:

- The Request Method: GET, POST, PUT
- IDENTITYKEY: The authentication token
- Content-Type: application/json

The platform has 3 operations for publishers:

-Retrieve data: Using the GET method, any kind of data can be consulted, the response is in JSON format

-Register data: Using the POST method, can be registered components, sensors alerts, alarms or orders.

-Update data: Using the PUT method, components, sensors alerts, alarms and orders data can be updated. Also sensor data can be published. It also has 3 kind of subscriptions:

- To sensor data - To orders - To alerts

All the documentation of the Application Programming Interface can be found in:

- http://www.sentilo.io/xwiki/bin/view/APIDocs/WebHome

4.4 Evaluation

4.4.1 Environment description

The objective of this scenario is to connect a Wireless Sensor Network to a running Sentilo server. There are 2 sides of the network, with the border router in the middle of both. The WSN uses CoAP to extract the sensors information, and the sensor data. The Sentilo server uses HTTP requests, with JSON objects. The JSON (JavaScript Object Notation) is a text format transmit data objects consisting of attributevalue pairs. It is one of most widely used by programming languages to send data over HTTP.

Sensor Network

The wireless sensor network is composed by Z1 motes connected by a border-router.

Border Router The Border Router manages the RPL (Routing Protocol for Low-Power and Lossy Networks), and is connected to a computer using Tunslip, a tool used to bridge IP traffic between 2 devices, over the serial line. Tunslip creates a virtual network interface (tun) on the host side and uses SLIP (serial line internet protocol) to encapsulate and pass IP traffic to and from the other side of the serial line.

Nodes Each of the motes has a CoAP server running, and has a resource for each sensor attached to the mote. In this environment 2 Sentilo items will be used:

Component: The hardware where a sensor is attached.

Sensor: A physical sensor. It must be attached to a component For the Sentilo server, each component, sensor, and alert must have a unique id. In this setup, each mote is a component in the server, the mote id is used for the unique id in sentilo. For this example, the mote 3 will have the id MOTE03. Each sensor has his unique id too, using the component id and the type of sensor. In this setup the temperature sensor of the mote 3 will have the id MOTE03TMP. Every sensor has a CoAP resource defined in the mote. A location resource is defined to set the mote location

Network connector

In the computer connected with the border-router, there's a Java application that pulls the information in the WSN using CoAP, and communicates with the Sentilo server to register the sensor and send the data. A provider must be registered manually in Sentilo in order to get the authentication token. For every request sent, the authorization token is checked.

Application workflow The Java application that connects the 2 networks, follows 5 steps:
1. Searches for all the Motes of the specified network in the border router, by sending an HTTP GET to the border router. It responds with an XML with the information of all the motes.

Discovers all the sensors in each Mote, by sending a CoAP discover to each mote.

Gets the information of each sensor, by sending a CoAP GET to the resources on the mote.

Registers each sensor in Sentilo, by sending a HTTP POST to the server with the information of the sensor.

Starts collecting data from the sensors, and registers it in Sentilo, by sending a CoAP observe to each Mote resource, and for each observation, sends a HTTP PUT with the data to Sentilo.

Sensor registration Once the application has a list of all the motes and the sensors of each one, sends a GET request every mote for each one of the sensors resources, to get the information of the resource. The sensor resource has defined the information needed to register.

Once the information of the sensor is gathered, it creates a JSON Object to register the sensor into the Sentilo server via the API.

Sensor data publish The application starts an OBSERVE on the mote for each sensor resource. At this point, the application starts to listen for messages from the CoAP resource. The sensor periodic resource sends information of the sensor data periodically. The period of observation is defined in the mote. In every observation, the data is sent to Sentilo in a JSON Object via the API.

The parameters sent in the JSON to the server are:

4.5 Discussion

4.5.1 The prototype

Results

Range

Response time

Connection speed

Power consumption

4.5.2 Project execution

4.6 Conclusion

The Contiki OS, collects all the technologies needed for the development of centralized data collectors, for the sensors. This platform combined with Sentilo, creates a real application platform, to be able to deploy in several possible real environments. The main advantages of Contiki, are how easy is to create code, and generate concurrent scenarios inside the same mote, being able to have a web server at the same time a root node of a WSN is running, without complexity. At the same time , the application level library as COAP, with the complete examples of this libraries, makes this system a powerful and versatile tool. A disadvantage of this platform, is the lack of documentation and examples, outside the inner code. There's a lot of time and test to make, for a more complex application. Secondly, the Sentilo platform, is an easy to install, use and program applications with. It has a wide set of options and tools, that need to be understand carefully for a rich application that uses all the functionalities properly. The combinations of both, makes a good, simple and potentially improvable scenario, for centralize data collection.

4.6.1 Future lines of work

There are some future lines of work in this experimental environment:

1. Test the CoAP server in the new release of Contiki. Contiki 3.0 A new release of Contiki was released in September 2015, with some changes and improvements overall, specially with CoAP. The new release supports CoAP 18.

2. A Java connector with a dynamic network. The Java connector finds the motes in a stable WSN, if a node is missing or replaced, it needs a manual interaction to find all the motes gain, by erasing all the network, and start to find all the motes again. Besides, the protocol handling the routes, is IP and the protocol handling the links is RPL. The IP routes in the border router expire every certain time, that means that if a mote is missing, a route is still present for a certain time, even if the RPL is aware of the missing mote. As a possible solution, there are repairing route methods in CoAP that are used to repair the broken links between nodes.

5 | MEC: Chapter 4

5.1 Introduction & problem statement

5.1.1 Background

5.1.2 Purpose (Goal)

5.1.3 Limitations

5.1.4 Method

5.2 Background

5.2.1 Selection of technology

Requirements

Hardware

Operating system

Communication protocol

Hardware

Operating system

Communication protocol

Workspace and tools

5.3 Prototype

5.3.1 Drivers and firmware

5.3.2 CoAP server

Testing

Final prototype

5.4 Evaluation

5.4.1 Environment description

5.4.2 Results exploitation

5.4.3 Range

5.4.4 Response time

5.4.5 Connection speed

5.4.6 Power consumption

5.5 Discussion

5.5.1 The prototype

Results

Range

Response time

Connection speed

Power consumption

5.5.2 Project execution

5.6 Conclusion

6 | Conclusion

6.1 Conclusion

6.2 Perspectives

7 | Publications

7.1 List of publications

A | Appendix A

A.1 Introduction & problem statement

A.2 Background

A.3 Approach

A.4 Performance evaluation

A.4.1 Environment description

A.4.2 Results exploitation

A.5 Conclusion

B | Appendix B

Year		**Factors**	**Computation Model**	**Results interpretation**
2018	[23]	-Closeness Centralityjhjhjhjhjhjh -Degree Centrality	Estimation	**Closeness** have a high degree of nbnbnbnbnbnbnb correlation with **privacy score**

Table B.1: An example table.

Bibliography

Others

[1] *Évaluation et Amélioration Des Plates-Formes Logicielles Pour Réseaux de Capteurs sans-Fil, Pour Optimiser La Qualité de Service et l'énergie*. 00000. URL: http://docnum.univ-lorraine.fr/public/DDOC_T_2016_0051_ROUSSEL.pdf (visited on 04/17/2019) (p. 1).

[2] Enrique Alba. " Intelligent Systems for Smart Cities ". In: *Proceedings of the 2016 on Genetic and Evolutionary Computation Conference Companion - GECCO '16 Companion*. The 2016. 00004. Denver, Colorado, USA: ACM Press, 2016, pp. 823–839 (p. 1).

[3] *Waspmote Lora 868mhz 915mhz Sx1272*. 00000 (p. 3).

[4] Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, and Hicham Lakhlef. " Internet of Things Security: A Top-down Survey ". In: *Computer Networks* 141 (Aug. 4, 2018). 00029, pp. 199–221 (p. 3).

[5] Pierre Merdrignac. " Système Coopératif de Perception et de Communication Pour La Protection Des Usagers Vulnérables ". In: (2015). 00003, p. 253 (p. 4, 5).

[6] Industrial Internet of Things. *Executive Summary*. 01455. URL: http://wef.ch/1Ce8qay (visited on 04/17/2019).

[7] *Short Term Traffic Prediction Models*. 00000. 2007 (p. 7).

[8] Fayssal Bendaoud, Marwen Abdennebi, and Fedoua Didi. " Network Selection in Wireless Heterogeneous Networks: A Survey ". In: *Journal of Telecommunications and Information Technology* 4 (Jan. 2019). 00000, pp. 64–74 (p. 7).

[9] Atefeh Meshinchi. " QOS-Aware and Status-Aware Adaptive Resource Allocation Framework in SDN-Based IOT Middleware ". 00000. masters. École Polytechnique de Montréal, May 2018 (p. 7).

[10] Abishi Chowdhury and Shital A. Raut. " A Survey Study on Internet of Things Resource Management ". In: *Journal of Network and Computer Applications* 120 (Oct. 15, 2018). 00002, pp. 42–60 (p. 7).

[11] Ala Al-Fuqaha et al. " Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications ". In: *IEEE Communications Surveys & Tutorials* 17.4 (24–2015). 02482, pp. 2347–2376 (p. 8, 11, 16).

[12] H. A. A. Al-Kashoash and Andrew H. Kemp. " Comparison of 6LoWPAN and LPWAN for the Internet of Things ". In: *Australian Journal of Electrical and Electronics Engineering* 13.4 (Oct. 2016). 00010, pp. 268–274 (p. 9).

[13] Zhijing Qin et al. " A Software Defined Networking Architecture for the Internet-of-Things ". In: *2014 IEEE Network Operations and Management Symposium (NOMS)*. NOMS 2014 - 2014 IEEE/IFIP Network Operations and Management Symposium. 00258. Krakow, Poland: May 2014, pp. 1–9 (p. 8).

[14] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke. “ A Survey on Software-Defined Wireless Sensor Networks: Challenges and Design Requirements ”. In: *IEEE Access* 5 (2017). 00135, pp. 1872–1899 (p. 8).

[15] Musa Ndiaye, Gerhard Hancke, and Adnan Abu-Mahfouz. “ Software Defined Networking for Improved Wireless Sensor Network Management: A Survey ”. In: 17.5 (May 4, 2017). 00053, p. 1031 (p. 9, 10).

[16] Samaresh Bera, Sudip Misra, and Athanasios V. Vasilakos. “ Software-Defined Networking for Internet of Things: A Survey ”. In: *IEEE Internet of Things Journal* 4.6 (Dec. 2017). 00057, pp. 1994–2008 (p. 10).

[17] Tie Luo, Hwee-Pink Tan, and Tony Q. S. Quek. “ Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks ”. In: *IEEE Communications Letters* 16.11 (Nov. 2012). 00341, pp. 1896–1899 (p. 10).

[18] Salvatore Costanzo et al. “ Software Defined Wireless Networks (SDWN): Unbridling SDNs ”. In: (2012). 00181, p. 25 (p. 10).

[19] Laura Galluccio et al. “ SDN-WISE: Design, Prototyping and Experimentation of a Stateful SDN Solution for WIreless SEnsor Networks ”. In: *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE INFOCOM 2015 - IEEE Conference on Computer Communications. 00173. Kowloon, Hong Kong: Apr. 2015, pp. 513–521 (p. 10).

[20] Gerhard Hancke, Bruno Silva, and Gerhard Hancke Jr. “ The Role of Advanced Sensing in Smart Cities ”. In: 13.1 (Dec. 27, 2012). 00318, pp. 393–425 (p. 12).

[21] Johan Bregell. “ Hardware and Software Platform for Internet of Things ”. In: *Master of Science Thesis in Embedded Electronic System Design* (2015). 00002 (p. 15, 25).

[22] *Contiki Applications for Z1 Motes for 6LowPAN*. 00000. 2016. URL: https://upcommons.upc.edu/bitstream/handle/2117/82767/Master%20Thesis.pdf?sequence=1&isAllowed=y (visited on 01/14/2019) (p. 39).

[23] Pascal Thubert, Maria Rita Palattella, and Thomas Engel. “ 6TiSCH Centralized Scheduling: When SDN Meet IoT ”. In: *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2015 IEEE Conference on Standards for Communications and Networking (CSCN). 00033. Tokyo, Japan: Oct. 2015, pp. 42–47 (p. 63).