



Instituto Politécnico de Tomar

Escola(s) Superior de Tecnologia de Tomar

Daniel João Santos Domingues Henriques
(aluno 20760)

Implementação de um sistema de Rega Inteligente

Novembro de 2019

Projeto Final 2º Ano
Orientado por: **Ana Lopes e Luís Oliveira**

Trabalho realizado no âmbito da disciplina de Projeto
do curso Mestrado em Engenharia Informática – Internet das Coisas



RESUMO



ABSTRACT

AGRADECIMENTOS

Gostava de agradecer a todos aqueles que ao longo dos últimos dois anos me apoiaram e tornaram este trabalho possível.

Aos meus orientadores, Eng.^a Ana Lopes e Eng.^o Luís Oliveira, pela disponibilidade demonstrada durante todo o mestrado e particularmente durante o desenvolvimento deste projeto.

Ao Município de Tomar, minha entidade empregadora, e ao Instituto Politécnico de Tomar, meu estabelecimento de ensino, por me terem disponibilizado as ferramentas necessárias para que fosse possível desenvolver este projeto.

Por último, mas não menos importante, agradeço à minha família, principalmente aos meus pais, esposa e filhos. A eles devo muito, pois proporcionaram-me as condições necessárias e sempre me apoiaram ao longo deste percurso.



ÍNDICE GERAL

RESUMO.....	3
ABSTRACT	4
AGRADECIMENTOS	5
ÍNDICE GERAL.....	7
ÍNDICE DE FIGURAS	9
ÍNDICE DE TABELAS	10
1 - INTRODUÇÃO	11
1.1 - Sumário	11
1.2 - Contexto e motivação	11
1.3 – Objetivos do projeto	13
1.4 – Contribuições	16
1.5 - Estado atual do projeto	17
2 - ESTADO DA ARTE EM TECNOLOGIAS IOT impar	19
2.1 - Introdução	19
2.2 - Tecnologias emergentes	20
2.3 – Protocolos e métodos de comunicação.....	24
2.3.1 – Protocolos IoT das camadas física e de ligação	26
2.3.1.1 – NB-IoT – Narrowband IoT	26
2.3.1.2 - LoRa – Long Range	33
2.3.1.3 - 802.15.4 (6LowPAN)	41
2.3.5 – Protocolos IoT da camada de transporte.....	45
2.3.5 – Protocolos IoT da camada de aplicação	48
3 – PLATAFORMA PARA REGA INTELIGENTE	55
3.1 - Requisitos	55
3.2 - Arquitetura global da solução.....	58
3.3 - Redes de sensores – Dispositivos e gateways	60
3.4 - Plataforma de gestão de dispositivos.....	67
3.5 - Plataformas de integração (Node-RED).....	71
4 – RESULTADOS EXPERIMENTAIS	81
4.1 – Cenário e instalação de sistemas	81
4.2 – Testes de validação.....	82



4.3	- Resultados dos testes de validação	90
5	- CONCLUSÕES	99
	REFERÊNCIAS – ver ordem	101

ÍNDICE DE FIGURAS

Figura 1 - Ilustração representativa do conceito de Smart Cities	11
Figura 3 - Gráfico comparativo entre Sigfox, LoRa e NB-IoT (retirado de [20])	13
Figura 4 - Ilustração representativa das comunicações do sistema de rega inteligente	20
Figura 5 – Camadas protocolares das várias camadas dos principais protocolos IoT	24
Figura 6 - Ilustração representativa de uma arquitetura de rede Narrowband-IoT	26
Figura 7 - Ilustração representativa dos processos de uplink e de downlink em NB-IoT	29
Figura 8 - Ilustração representativa do ciclo de vida de um terminal NB-IoT.....	30
Figura 9 - Gráficos da ocupação do canal de UL e DL.....	31
Figura 10 – Gráficos com percentagem de recursos livres e ocupação da rede.....	32
Figura 11 - Ilustração representativa de arquitetura de uma rede LoRa.....	33
Figura 12 - Fotos de dispositivo terminal e de gateway LoRa.....	35
Figura 13 – Gráfico representativo dos RSSIs face a fatores de spreading diferentes	36
Figura 14 - Mapa representativo das localizações do gateway e dos dispositivos terminais.....	37
Figura 15 - Gráfico com rácio de pacotes entregues com locais e spreadings diferentes	37
Figura 16 - Gráfico comparativo da taxa de transferência média com 1 único dispositivo.....	39
Figura 17 - Canais e frequências da camada física do protocolo 802.15.3	42
Figura 18 – Comparativo entre modelo TCP/IP e 6LowPAN	43
Figura 19 – Dispositivo terminal e border-router	44
Figura 20- Representação da comunicação entre uma rede IPv6 e uma rede IPv4	Erro!
Marcador não definido.	
Figura 21 - Cabeçalhos TCP e UDP	46
Figura 22 - Ilustração representativa de transmissão de dados entre 1 sensor e 2 clientes.....	50
Figura 23 - Ilustração representativa da arquitetura de comunicação com os sensores	59
Figura 24 - Ilustração representativa da arquitetura de comunicação com os atuadores	60
Figura 25 – Cenário montado para testar comunicação com electroválvula	62
Figura 26 - Equipamentos LoRa utilizados no survey realizado no concelho de Tomar	63
Figura 27 - Localização das antenas NB-IoT atualmente ativadas no concelho de Tomar	65
Figura 28 - Sensor NB-IoT instalado em caixa estanque	65
Figura 29 – Dashboard de registo e gestão de dispositivos do Watson IoT.....	68
Figura 30 – Dashboard de logs de conexão do Watson IoT	68
Figura 31 - Menu de aprovisionamento e gestão de dispositivos NB-IoT	69
Figura 32 - Dashboard do sistema de rega inteligente	70
Figura 33 - Aprovisionamento e gestão de dispositivos na aplicação LoRaWAN Server	71
Figura 34 – Dashboard de acesso à lista de recursos disponíveis no IBM Cloud	72
Figura 35 – Fluxo desenvolvido para envio de dados do Watson IoT para o Cloudbant	75
Figura 36 – Fluxo de tratamento e validação de dados da camada de middleware	76
Figura 37 – Fluxo que realiza o log dos valores excluídos pelas regras de validação	77
Figura 38 - Fluxo que trata as previsões meteorológicas da API do IPMA.....	78
Figura 39 – Fluxo de validação e atuação com Arduino.....	79
Figura 40 – Segurança das plataformas da camada de gestão de dispositivos	87
Figura 41 - Camadas protocolares TCP/IP, 6LowPAN, LoRaWAN e NB-IoT.....	90
Figura 42 – Local elevado de instalação de antena e gateway LoRa	93

ÍNDICE DE TABELAS

Tabela 1 - Comparativo entre NB-IoT, LoRaWan e 802.15.4	26
Tabela 2 – Bandas de frequência licenciadas para NB-IoT.....	27
Tabela 3 – Comparativo entre LTE, LTE-M e LTE NB-IoT.....	28
Tabela 4 - Tabela comparativa de especificações LoRa em vários locais do mundo	34
Tabela 5 – Especificações por canal da camada física do protocolo 802.15.4.....	42

1 - INTRODUÇÃO

1.1 - Sumário

Este trabalho foi desenvolvido no âmbito do Mestrado em Engenharia Informática – Internet das Coisas e consiste no estudo e no desenvolvimento de um sistema de rega inteligente, a instalar nos espaços verdes do Complexo Desportivo Municipal de Tomar.

O foco principal deste projeto será a utilização de tecnologias *Internet of Things* (IoT), uma vez que no final da sua instalação se pretende realizar uma análise às opções tecnológicas tomadas e utilizar o estudo e a experiência adquirida como fundamentação para as escolhas tecnológicas a adotar em projetos futuros de *Smart Cities* (cidades inteligentes).

1.2 - Contexto e motivação

A Internet das coisas tem como principal objetivo ligar à internet equipamentos eletrónicos utilizados no quotidiano. A ideia consiste em massificar a presença de objetos IoT na sociedade (conforme representado metaforicamente na figura 1), tal como sensores, atuadores, ou outros equipamentos que sejam capazes de executar tarefas sem necessidade de interação humana. Ou seja, uma sociedade onde a Internet marca presença em todos os locais e equipamentos [1].



Figura 1 - Ilustração representativa do conceito de Smart Cities [2]

A IoT tem o potencial de influenciar a forma como vivemos, através de alterações significativas dos ambientes domésticos e empresariais. A nível doméstico pode ser aplicada em diversas áreas, nomeadamente em casas automatizadas, *assisted living*, *e-health* e *enhanced learning*, entre outros. Na esfera empresarial e corporativa, as mais valias afetarão essencialmente áreas como a automação, a produção, a logística e o transporte, melhorando a eficiência e rentabilidade [1].

O conceito de *Smart Cities* está a crescer em todo o mundo e a IoT é uma peça essencial para a sua viabilização.

As soluções de *Smart Cities* têm por objetivo transformar a vida das cidades, dos seus habitantes e dos turistas que as visitam. Através da utilização das tecnologias é possível tornar as populações mais seguras, eficientes, económicas e amigas do ambiente [3].

Existem no mercado nacional diversas empresas a competir e a oferecer serviços no mercado das *Smart Cities*, mas os valores das soluções propostas são muito elevados. Em grande parte das situações os custos de investimento e manutenção dos projetos são tão elevados que inviabilizam a sua concretização.

A relevância do trabalho aqui proposto destaca-se essencialmente pela mais-valia dos conhecimentos adquiridos, fundamentados pela utilização e pelos testes realizados às diversas tecnologias, equipamentos, dispositivos e protocolos de comunicação.

Para o Município de Tomar, este projeto vai permitir chegar a uma melhor arquitetura IoT, com especial relevância na plataforma de integração agnóstica, que não olhe a marcas, patentes ou licenças de propriedade. Só assim será possível desenvolver uma solução que permita integrar equipamentos IoT (sensores, routers, atuadores, etc.) de todas as marcas e modelos, independentemente dos protocolos de comunicação utilizados.

Como complemento pretende-se que a solução proposta seja desenvolvida não só a pensar na rega inteligente dos espaços verdes do Município, mas também a pensar em futuros projetos no âmbito da gestão de consumos energéticos, de consumo de água, de recolha de resíduos, ou de qualquer outra área da competência dos Municípios.

Através da comparação a realizar às diversas tecnologias de comunicação, exemplo: Lora/LoraWan, NB-IoT, Ethernet, WiFi, etc. pretende-se perceber em que circunstâncias e em que locais melhor se adaptam cada uma delas (ex. figura 3).

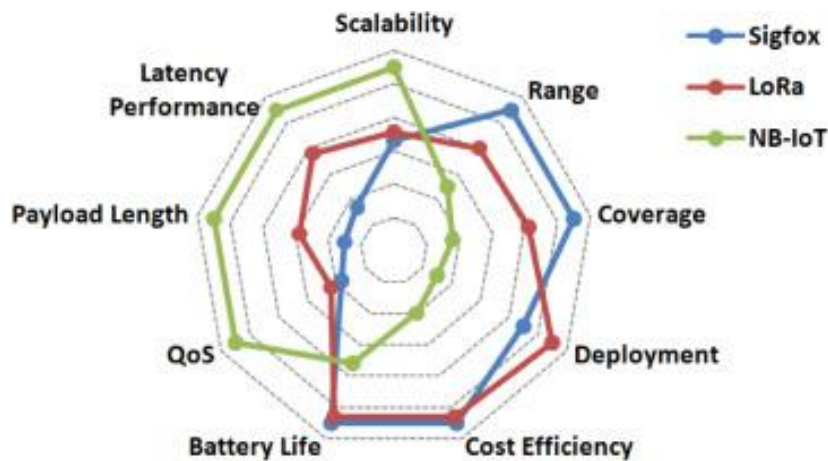


Figura 2 - Gráfico comparativo entre Sigfox, LoRa e NB-IoT [4]

O custo benefício financeiro da solução adotada é um fator decisivo no momento em que, uma empresa, um município ou uma pessoa individual, opta pela escolha de uma determinada tecnologia.

Um dos aspetos que serão analisados no final deste projeto serão os custos de desenvolvimento e de manutenção associados a cada tecnologia instalada.

1.3 – Objetivos do projeto

Enquadrados no âmbito da implementação de uma solução dedicada à gestão de sistemas de rega inteligente, com recurso a dispositivos IoT, a instalar nos espaços verdes do Complexo Desportivo Municipal de Tomar, foram propostos os seguintes objetivos para o projeto descrito neste relatório:

1 – Definir a arquitetura global para a solução de rega inteligente:

Este objetivo é fundamental para o sucesso deste projeto. O desenho de uma arquitetura adequada e a escolha das tecnologias mais indicadas vão permitir o sucesso presente e futuro da solução.

O diagrama de arquitetura global deverá ser projetado por forma a responder às necessidades existentes, com foco especial na compatibilidade entre as tecnologias de comunicação e entre as plataformas integrantes deste projeto IoT .

Para que tal aconteça é necessário que os dispositivos escolhidos sejam capazes de comunicar com a camada de gestão de dispositivos e que as soluções IoT possuam capacidade de comunicação com a camada de integração.

A primeira para que dispositivos de vários fornecedores e tecnologias se possam autenticar centralmente de forma segura e a segunda para que seja possível integrar dados de vários projetos e soluções (adicionando funcionalidades e inteligência). Para que tal seja possível, um dos requisitos obrigatórios é que as soluções a implementar permitam a criação de APIs (Application programming interface).

A escolha das tecnologias a integrar na arquitetura deste projeto deverá ter em conta o requisito de comunicação com qualquer equipamento IoT, sem olhar ao protocolo de comunicação (MQTT, COAP, HTTP, etc.) ou à tecnologia de comunicação (NB-IoT, LoRa/LoRaWan, 802.15.4 (6LowPAN), 3G/4G, WiFi, Ethernet, etc).

2 - Especificar o funcionamento da plataforma de gestão de dispositivos:

O objetivo é que esta camada seja responsável pelo registo e autenticação de todos os dispositivos na plataforma central.

Neste projeto pretende-se utilizar o Watson IoT e o Vodafone/Thinkdigital AEP, e verificar se ambas estas ferramentas reúnem os requisitos técnicos necessários para registo e gestão de dispositivos IoT.

Todos os sensores e atuadores, independentemente da sua tecnologia, deverão ser registados nesta plataforma. Só assim deverá ser possível aos mesmos enviar e receber dados.

Aqui serão registados e controlados de uma forma eficiente e segura, mediante a atribuição de um Token individual por dispositivo.

Esta camada servirá de ponte entre os dispositivos IoT e a plataforma de integração. Para a comunicação entre plataformas serão criadas APIs (MQTT, COAP ou REST).

3 - Desenvolver uma plataforma de integração e validação de dados (middleware em Node-RED)

Os objetivos desta camada passam pelo desenvolvimento de uma solução que permita realizar a integração de diversas plataformas IoT e que permita realizar o tratamento e a validação dos dados recolhidos pelos sensores e enviados para os atuadores.

Independentemente da plataforma IoT ou do protocolo de comunicação utilizado, será esta ferramenta que fará a ponte entre os dados enviados por todos os sensores, sem qualquer tratamento e validação, e as plataformas IoT de controlo e gestão.

No processo de tratamento de dados poderão ser efetuadas conversões, cálculos ou outro tipo de operações.

No processo de validação poderão ser efetuadas análises de intervalos de valores, valores com variações acima do normal, valores nulos, valores enviados com frequências demasiado elevadas, etc.

Pretende-se que a exclusão deste tipo de dados traga mais fiabilidade ao conjunto dos dados recolhidos e, mediante o tipo de contrato realizado com as plataformas de armazenamento, contribuir para uma eventual redução nos custos, uma vez que ao excluir valores errados ou com uma frequência demasiado elevada, irá diminuir o volume de dados armazenados.

Será também através desta plataforma que deverão ser realizados os backups dos dados recolhidos pelos sensores.

No sentido inverso, na comunicação das plataformas para os atuadores instalados no terreno, esta ferramenta virá a ter uma importância elevada, uma vez que terá capacidade para contrariar as ordens dadas pelas plataformas de gestão. A análise das variáveis ambientais ou das previsões meteorológicas poderá resultar no cancelamento dessas instruções.

4 - Efetuar testes de validação, discutir e analisar resultados.

Neste capítulo é pretendido realizar testes a todos os componentes envolvidos neste projeto.

Na componente física é pretendido testar as redes de sensores e respetivos dispositivos de sensorização e atuação, incluindo os protocolos e métodos de comunicação.

Na componente aplicacional é pretendido testar a plataforma de gestão de dispositivos, a camada de integração, as aplicações de gestão e IoT.

No final dos testes realizados deverá ser possível reunir dados que permitam suportar escolhas tecnológicas para projetos futuros, dando especial foco à comparação entre as tecnologias utilizadas.

1.4 – Contribuições

A realização deste projeto permitiu reunir as seguintes contribuições:

- Apoio no aprofundamento de conhecimentos na área de projetos IoT, especialmente direcionados para trabalhadores da área das tecnologias de informação dos municípios.
- Análise e comparação entre as várias tecnologias de comunicação IoT, nomeadamente Lora, NB-IoT e 802.15.4 (6LoWPAN), quer ao nível das características das próprias tecnologias e da sua adaptação aos vários espaços, como também no que diz respeito aos custos de desenvolvimento e manutenção das infraestruturas tecnológicas respeitantes.
- Definir a arquitetura para o sistema de rega inteligente, realizada de acordo com os objetivos do projeto
- Desenvolver uma plataforma de integração e perceber que, através do Node-RED é possível integrar diversas plataformas IoT, de diversos fornecedores, nomeadamente de consumo energético, consumo de água, recolha de resíduos, ou outra área IoT.
- Estudar e implementar diversas plataformas de gestão IoT.
- Testar e validar vários protocolos da camada de aplicação em ambiente IoT, nomeadamente MQTT, COAP, HTTP.
- perceber as vantagens financeiras e operacionais de cada tecnologia, concluindo que as posições das empresas variam aparentemente de acordo com os seus interesses económicos e os conhecimentos dos seus quadros técnicos.

Em suma, sendo o foco principal a utilização de tecnologias IoT, através da realização deste projeto foi possível reunir conhecimentos técnicos e realizar testes, de modo a poder escolher e fundamentar as melhores opções tecnológicas a adotar em projetos futuros.

1.5 - Estado atual do projeto

Este projeto foi iniciado com o estudo das necessidades, com a definição de objetivos, com o desenho da arquitetura global da solução e a definição da equipa de projeto. De seguida estudaram-se projetos semelhantes e por fim efetuou-se um estudo às tecnologias existentes.

Efetuada as escolhas tecnológicas e definida a arquitetura do projeto, passou-se à fase de desenvolvimento e instalação da solução, quer ao nível das redes de sensores como ao nível aplicacional.

Paralelamente à realização deste projeto, o Município de Tomar está a realizar as alterações necessárias ao sistema de rega existente e iniciou diligências no sentido de proceder à instalação do depósito subterrâneo para aproveitamento das águas pluviais e das lavagens das piscinas.

Atualmente o projeto encontra-se em fase de análise das tecnologias escolhidas para realização deste projeto. No decorrer dos próximos 12 meses o sistema estará em produção e serão analisados os desempenhos e comportamentos das diversas opções tecnológicas tomadas, tendo como objetivo perceber as vantagens e desvantagens de cada tecnologia e projeto a implementar de futuro.



2 - ESTADO DA ARTE EM TECNOLOGIAS IOT impar

O objetivo deste capítulo é apresentar uma visão geral sobre plataformas e protocolos IoT, com especial foco nas tecnologias LoRa, NB-IoT e 802.15.4 (6LoWPAN).

2.1 - Introdução

Os principais desafios deste projeto passaram pela criação da rede de sensores, pelo estudo das diversas tecnologias IoT, pelos testes aos diversos protocolos de comunicação entre sensores e plataformas, e pelo desenvolvimento e implementação de uma plataforma de integração de sistema IoT, de modo a responder às necessidades do Município de Tomar.

Só assim seria possível no futuro, perceber das tecnologias emergentes, quais serão as melhores apostas para implementação de projetos IoT, no âmbito do conceito de *Smart Cities*.

Uma das principais componentes deste projeto passa pela criação de uma rede de sensores bem dimensionada, de modo a garantir fiabilidade e bom desempenho nas comunicações entre os dispositivos (tendo em conta todas as questões da segurança aplicada à Internet das Coisas).

Redes de sensores sem fios (RSSF) são conjuntos de nós-sensores autoalimentados capazes de recolher informações e detetar eventos do meio onde estão instalados e via canais rádio transmitir os dados processados.

Uma das valias de uma RSSF é que esta pode ser utilizada para a monitorização de áreas onde não é viável utilizar uma infraestrutura de rede com fios (ex. zonas remotas, zonas de acesso restrito ou difícil e zonas potencialmente hostis).

Embora os equipamentos utilizados neste projeto comuniquem através de protocolo 6LowPan, NB-IoT, LoRa e Ethernet, a solução implementada não limita a utilização de outra qualquer tecnologia ou protocolo de comunicação, conforme representado na figura 4.

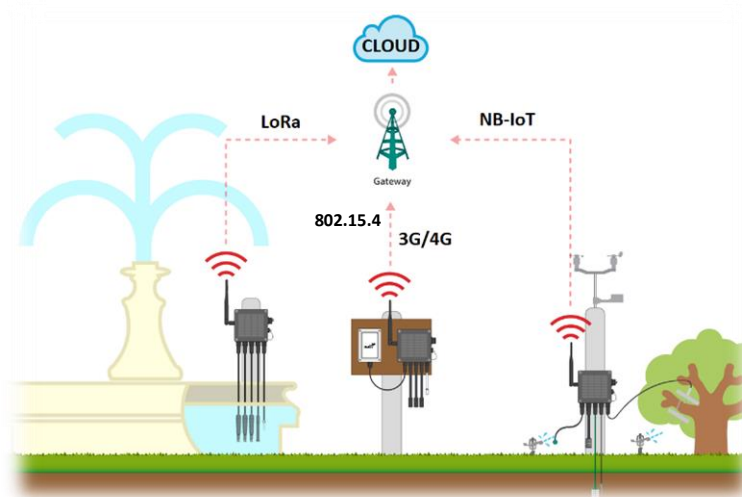


Figura 3 - Ilustração representativa das comunicações do sistema de rega inteligente

A solução de integração, alojada na Cloud, tem como objetivo integrar as diversas tecnologias e equipamentos IoT, orquestrando a comunicação entre os diversos dispositivos e as diversas plataformas IoT, por forma a que seja possível atuar sobre os mesmos num ambiente centralizado.

Considerou-se essencial que o desenvolvimento da solução de gestão central IoT, por questões de segurança e normalização, permitisse apenas a receção de dados a partir de APIs.

A plataforma é aberta a todas as tecnologias de comunicação, suportando diversos protocolos, entre eles MQTT, COAP ou HTTP.

Um dos requisitos fundamentais é a capacidade da solução conseguir atuar sobre os equipamentos instalados no terreno. [14]

Deste modo, neste capítulo, o principal foco passa pela análise de vários protocolos e métodos de comunicação utilizados em sistemas IoT, dando especial relevância aos que mais impacto terão no desenvolvimento do projeto final, e aos que se encontram com mais frequência associados a projetos de IoT, nomeadamente LoRa, NB-IoT e 802.15.4 - 6LowPAN.

2.2 - Tecnologias emergentes

Num mundo tecnológico em constante evolução, o desenvolvimento de novas tecnologias IoT acontece cada vez com maior frequência.

Termos como *Internet of Things*, *Big Data*, *Mobile & Social Internet*, *Artificial Intelligence*, *Virtual Reality*, *Automation*, *Robots*, *Cloud Computing* e muitos outros, estão cada vez mais presentes no nosso dia-a-dia e o seu impacto em áreas como a cultura, os mercados e as sociedades será enorme no decorrer da próxima década. [3]

Desde o aparecimento do conceito de *Internet of Things*, diversas tecnologias de comunicação foram desenvolvidas e testadas para suportar soluções e aplicativos IoT.

Por muitos considerada a quarta revolução industrial, a era da nova geração de redes sem fios vai permitir conectividade entre bilhões de máquinas e objetos.

Para dar resposta a este paradigma, os sistemas de comunicação sem fios precisam de suportar a conectividade de um enorme número de dispositivos.

Prevê-se que no próximo ano (2020), mais de vinte e cinco bilhões de dispositivos estejam conectados através de redes sem fios. [12]

O rápido crescimento do mercado da internet das coisas (IoT), faz com que as tecnologias de comunicação sem fios de baixa potência e de baixa largura de banda se tornem cada vez mais populares.

Dentro das tecnologias de comunicação de baixo consumo energético, podemos de uma forma geral fazer uma separação dentro de duas categorias:

- Redes de área local - Com alcance inferior a 1000 metros, onde incluímos IEEE 802.15.4, IEEE P802.1ah, Bluetooth / LE, etc.

- Redes de área alargada - Com alcance superior a 1000 metros, onde incluímos LoRaWAN, Sigfox, DASH7, NB-IoT, etc. [11]

O aparecimento das redes de grande alcance e de baixa potência (LPWAN), com um consumo de energia reduzido e uma baixa taxa de transferência de dados, projetadas e desenvolvidas especificamente para IoT, iniciou-se com o lançamento do Sigfox em 2009 (baseada em tecnologias proprietárias, atua como um provedor de serviços IoT).

De seguida surgiu o IngenuTM, formalmente designado como On-Ramp, que surge como um provedor de serviços de LPWAN via redes de IoT públicas e privadas, baseadas em tecnologias proprietárias (The Random Phase Multiple Access). Mais

recentemente, surgem muitas outras tecnologias LPWAN, sendo 2 dos exemplos mais consolidados o LoRa e o NB-IoT. [3]

Resumo das tecnologias e métodos de comunicação mais utilizadas em IoT:

LoRa (*Long Range*) - LoRa é uma tecnologia de comunicação sem fios para redes de longa distância / área alargada, baixa potência e de baixa largura de banda (LPWAN) onde os dispositivos comunicam diretamente com os gateways. É atualmente considerada uma das tecnologias mais adaptadas para IoT, essencialmente devido ao baixo custo dos equipamentos e dispositivos, ao baixo consumo de energia e devido ao seu modelo de negócio.

NB-IoT (*Narrowband IoT*) - É uma tecnologia de comunicação sem fios, padronizada pelo 3GPP, desenvolvida especificamente para comunicações máquina em grande quantidade "*Massive Machine-Type Communications*".

802.15.4 (*6LowPAN*) - É um padrão que especifica a camada física e a camada de ligação (MAC) em redes do tipo de área pessoal sem fios (*low-rate wireless personal area networks*). Foi desenvolvido para sistemas de comunicações de baixo custo, em redes de curta distância (entre 10 e 100 metros) e com pouca infraestrutura, tendo como principal objetivo reduzir ao máximo o consumo de energia.

Zigbee – É um protocolo mais utilizado em ambientes industriais do que residenciais. É baseado no padrão IEEE802.15.4, que é basicamente um padrão para redes wireless industriais na faixa de 2.4GHz. O alcance vai de 10 a 100 metros. A taxa de transmissão alcança um máximo de 250kbps. O protocolo é mantido pela Zigbee Alliance.

SigFox – É uma alternativa intermedia entre o WiFi e as redes de longo alcance, como as redes móveis (3G, 4G, etc.). A banda utilizada é a ISM (industrial, scientific and medical band). A tecnologia base do Sigfox é chamada de UNB (Ultra Narrowband) e foi projetada apenas para níveis de transferência entre 10 bit/s e 1 kbit/s. O seu alcance vai até 50Km.

Neul – O protocolo Neul baseia-se num conceito similar ao Sigfox e é baseado no chip IcenI. A tecnologia base é a chamada Weightless, é baseada em redes WAN e desenhada para competir com as já existentes GPRS, 3G, CDMA e LTE WAN. A taxa

de transferência de dados vai até 100 kbps. Possui um alcance de até 10 km e consumo de cerca de 20-30 mA.

NFC (Near Field Communication) - É uma tecnologia para troca de informações entre dois equipamentos eletrônicos. Basicamente é uma extensão da tecnologia de cartões RF (RFIDs) que permite aos equipamentos trocarem informações a distâncias de alguns centímetros. É especialmente interessante para *smartphones*, pois pode ser utilizada para transferir dados entre equipamentos. O alcance geral do protocolo é de 10 cm, e a taxa de transmissão vai até 420 kbps.

Wi-Fi - É um protocolo LAN (Local Area Network) e tem capacidade transferências com altas taxas de transmissão. Os padrões mais usados são o 802.11ac e o 802.11n, que já oferecem velocidades que podem ultrapassar 1 Gbps. Este protocolo tem um consumo energético elevado para dispositivos IoT. O alcance das redes WiFi é de aproximadamente 50 metros em espaços interiores e 100 metros em espaços exteriores.

Thread - Desenvolvido para o ramo da automação residencial (domótica), é baseado no protocolo 6LoWPAN. Do ponto de vista das suas aplicações, pode-se considerar um protocolo complementar ao WiFi para ambientes residenciais.

Z-Wave - Desenvolvido para o ramo da automação residencial. Possui taxas de transmissão até 100 kbps e permite redes mesh com 232 nós. O protocolo é mantido pela Z-Wave Alliance, opera na faixa de 900 MHz e tem um alcance de 30 m.

Bluetooth - Protocolo mantido pelo Bluetooth SIG (*Special Interest Group*). Possui uma extensa documentação e inúmeros exemplos de aplicações. O alcance varia conforme a classe do módulo: a classe 1 alcança até 100 metros e tem uma potência de 100 mW, a classe 2 tem alcance de até 10 metros e uma potência de 2,5mW, e a classe 3 que tem um alcance de 1 metro e dissipa no máximo 1 mW. Já teve várias versões lançadas, mas foi no 4.0 (*Bluetooth Low Energy*) e na mais recente 5.0 que o foco se concentrou na Internet das Coisas. O baixo consumo energético das últimas versões foi um requisito colocado exatamente pelas novas aplicações IoT. [16]

2.3 – Protocolos e métodos de comunicação

Neste ponto apresenta-se um estudo com foco nos protocolos e métodos de comunicação mais utilizados em IoT.

A necessidade de criação de novos protocolos, dimensionados de acordo com as necessidades e especificidades dos equipamentos IoT, surgiu como uma solução para o grande crescimento do número de objetos M2M, que trouxeram inúmeros desafios de interoperabilidade e comunicação. [1]

Nos últimos anos, a chegada da Internet das coisas, estimulou o desenvolvimento de dispositivos IoT cada vez mais potentes e mais autónomos, em grande parte justificados pelas potencialidades de alcance e largura de banda das comunicações sem fio.

Neste capítulo serão analisadas diferentes formas de transmissão de dados no universo de IoT, assim como os seus padrões de comunicação e protocolos, com especial foco em 802.15.4 (6LowPAN), LoRaWan e NB-IoT.

Na figura 5 apresenta-se uma visão das várias camadas protocolares que compõe as principais tecnologias IoT, comparativamente com o protocolo TCP/IP (*Transmission Control Protocol / Internet Protocol*).

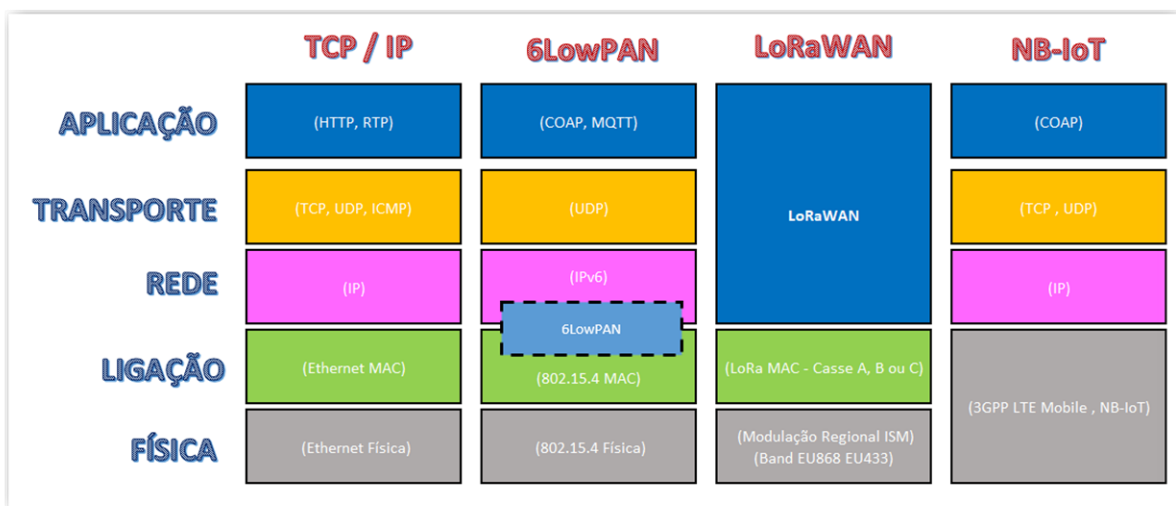


Figura 4 – Camadas protocolares das várias camadas dos principais protocolos IoT

Camada física

Define especificações elétricas e físicas dos dispositivos na relação entre os dispositivos e os meios de transmissão (por cabo ou sem fios).

A camada física define se a transmissão pode ser realizada nos dois sentidos em simultâneo. Sendo a camada mais baixa, representa a transmissão e receção de dados brutos não-estruturados.

Nos protocolos IoT a comunicação na camada física baseia-se em comunicações sem fios (802.15.4, 3GPP, LoRa, etc.).

Camada de ligação

Esta camada deteta e corrige erros que possam ocorrer na camada física. É responsável por controlar o fluxo e também estabelece um protocolo de comunicação entre sistemas. A tarefa desta camada é entregar os pacotes para o destino definido, através do endereçamento e entrega.

Por exemplo, no protocolo 802.15.4, para que seja possível comunicar através do protocolo IPv6, foi criada uma camada intermédia entre esta e a camada de rede, denominada 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks).

Camada de transporte

A finalidade desta camada é fazer a transferência de dados entre duas máquinas, independentemente da aplicação usada e do tipo, topologia ou configuração das redes físicas existentes entre elas.

Na camada de transporte IoT utiliza-se essencialmente UDP, devido à mais baixa necessidade de processamento e ao mais baixo volume de dados.

Camada de aplicação

Esta camada engloba os diversos protocolos que realizam a comunicação entre aplicações, sendo o HTTP o mais utilizado para serviços web. No entanto, uma vez que o HTTP possui muita complexidade computacional, requer muita largura de banda e um consumo de energia elevado, no contexto IoT não é muito utilizado, sendo os protocolos mais utilizados o CoAP e o MQTT.

2.3.1 – Protocolos IoT das camadas física e de ligação

Nesta subsecção são apresentadas as especificações e características das três tecnologias de comunicação que são utilizadas no projeto, nomeadamente NB-IoT e LoRaWan como protocolos de rede de longo alcance, e 802.15.4 (6LowPAN) que atua no quadro das redes de curto alcance.

Embora estas tecnologias de comunicação trabalhem com modelos de arquitetura bastante diferentes, todas elas se adaptam aos requisitos e necessidades de comunicação de projetos IoT, nomeadamente no que se refere às larguras de banda, conforme se apresenta na tabela 1.

Tabela 1 - Comparativo entre NB-IoT, LoRaWan e 802.15.4 (retirado de [22])

	NB-IoT		LoRaWan	6LowPAN
Protocolo	LTE Cat NB1	LTE Cat NB2	LoRa	802.15.4
Downlink	26 kbit/s	127 kbit/s	50 kbit/s	250 kbit/s
Uplink	66 kbit/s	159 kbit/s	50 kbit/s	250 kbit/s
	16,9 kbit/s			

2.3.1.1 – NB-IoT – Narrowband IoT

Neste subcapítulo é efetuada uma descrição do protocolo NB-IoT e da sua arquitetura (representada na figura 6), juntamente com a análise e avaliação de desempenho desta tecnologia, com base nos artigos [5] e [12].



Figura 5 - Ilustração representativa de uma arquitetura de rede Narrowband-IoT

NB-IoT é uma tecnologia de comunicação sem fios, padronizada pelo 3GPP, desenvolvida especificamente para comunicações máquina em grande quantidade “Massive Machine-Type Communications”.

Em comparação com as tecnologias 3G/4G desenvolvidas para utilização pessoal, o NB-IoT tem características de concepção que proporcionaram um aumento da cobertura e uma maior economia no consumo energético, em contrapartida com uma redução das funcionalidades disponíveis.

Conforme podemos verificar na tabela 2, as frequências de uplink e downlink possuem várias bandas licenciadas, variando também a respetiva largura de banda.

Tabela 2 – Bandas de frequência licenciadas para NB-IoT [23]

Bandas de frequências NB-IoT				
NB-IoT Band	Uplink Band	Downlink Band	Bandwidth	Duplex Mode
B1	1920 - 1980 MHz	2110 - 2170 MHz	60 MHz	HD-FDD
B2	1850 - 1910 MHz	1930 - 1990 MHz	60 MHz	HD-FDD
B3	1710 - 1785 MHz	1805 - 1880 MHz	75 MHz	HD-FDD
B4	1710 - 1755 MHz	2110 - 2155 MHz	45 MHz	HD-FDD
B5	824 - 849 MHz	869 - 894 MHz	25 MHz	HD-FDD
B8	880 - 915 MHz	925 - 960 MHz	25 MHz	HD-FDD
B11	1427.9 - 1447.9 MHz	1475.9 - 1495.9 MHz	20 MHz	HD-FDD
B12	699 - 716 MHz	729 - 746 MHz	17 MHz	HD-FDD
B13	777 - 787 MHz	746 - 756 MHz	10 MHz	HD-FDD
B14	788 - 798 MHz	758 to 768 MHz	10 MHz	HF-FDD
B17	704 - 716 MHz	734 - 746 MHz	12 MHz	HD-FDD
B18	815 - 830 MHz	860 - 875 MHz	15 MHz	HD-FDD
B19	830 - 845 MHz	875 - 890 MHz	15 MHz	HD-FDD
B20	832 - 862 MHz	791 - 821 MHz	30 MHz	HD-FDD
B25	1850 - 1915 MHz	1930 - 1995 MHz	65 MHz	HD-FDD
B26	814 - 849 MHz	859 - 894 MHz	35 MHz	HD-FDD
B28	703 - 748 MHz	758 - 803 MHz	45 MHz	HD-FDD
B31	452.5 - 457.5 MHz	462.5 - 467.5 MHz	5 MHz	HD-FDD
B66	1710 - 1780 MHz	2110 - 2200 MHz	70/90 MHz	HD-FDD
B70	1695 - 1710 MHz	1995 - 2020 MHz	25 MHz	HD-FDD
B71	633 - 698 MHz	617 - 783 MHz	65 MHz	HD-FDD
B72	451 - 456 MHz	461 - 466 MHz	5 MHz	HD-FDD
B73	450 - 455 MHz	461 - 466 MHz	5 MHz	HD-FDD
B74	1427 - 1470 MHz	1475 - 1518 MHz	43 MHz	HD-FDD
B85	698 - 716 MHz	728 - 746 MHz	10 MHz	HD-FDD

Comparativamente ao LTE comum, o LTE cat NB-IoT apresenta uma capacidade de transferência de dados muito mais reduzida, apresenta uma latência muito maior, só trabalha em half-duplex e não permite a mobilidade dos dispositivos terminais (tabela 3). Por outro lado, possui maior economia de energia e um custo mais baixo.

Tabela 3 – Comparativo entre LTE, LTE-M e LTE NB-IoT (retirado de [22])

	LTE Cat 1	LTE-M				NB-IoT	
		LC-LTE	eMTC			LTE Cat NB1	LTE Cat NB2
		LTE Cat 0	LTE Cat M1	LTE Cat M2	non-BL		
3GPP Release	Release 8	Release 12	Release 13	Release 14	Release 14	Release 13	Release 14
Downlink	10 Mbit/s	1 Mbit/s	1 Mbit/s	~4 Mbit/s	~4 Mbit/s	26 kbit/s	127 kbit/s
Uplink	5 Mbit/s	1 Mbit/s	1 Mbit/s	~7 Mbit/s	~7 Mbit/s	66 kbit/s (multi-tone) 16,9 kbit/s (single-tone)	159 kbit/s
Latencia	50–100ms	not deployed	10ms–15ms			1.6s–10s	
Numero de Antenas	2	1	1	1	1	1	1
Modo de Duplex	Full Duplex	Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex
Bandwidth	1.4 – 20 MHz	1.4 – 20 MHz	1.4 MHz	5 MHz	5 MHz	180 kHz	180 kHz
Transmissão	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	14 / 20 / 23 dBm

Estas características permitiram que fosse possível garantir a conectividade de mais dispositivos, em localizações mais remotas, diminuindo as necessidades de processamento e de complexidade dos dispositivos terminais, possibilitando o aumento da duração da bateria dos dispositivos.

Mas o NB-IoT não pode ser encarado como a solução tecnológica ideal para todos os cenários. Sistemas que necessitem de transferir grandes volumes de dados e que necessitem de tempos de resposta muito reduzidos não podem ser implementados com as normas e padrões existentes atualmente.

O facto de as operadoras já possuírem infraestruturas de comunicações compatíveis com NB-IoT reflete o seu enorme potencial. Este foi o principal fator de aposta nesta tecnologia. Esta é sem dúvida a principal vantagem face às restantes tecnologias de comunicação desenvolvidas para IoT.

De seguida vamos resumir as possíveis configurações do NB-IoT e discutir os procedimentos para transmissão e receção de dados, e analisar a latência e ocupação de recursos, de acordo com o artigo [5]

Na figura 7 encontram-se representados os processos de uplink e de downlink.

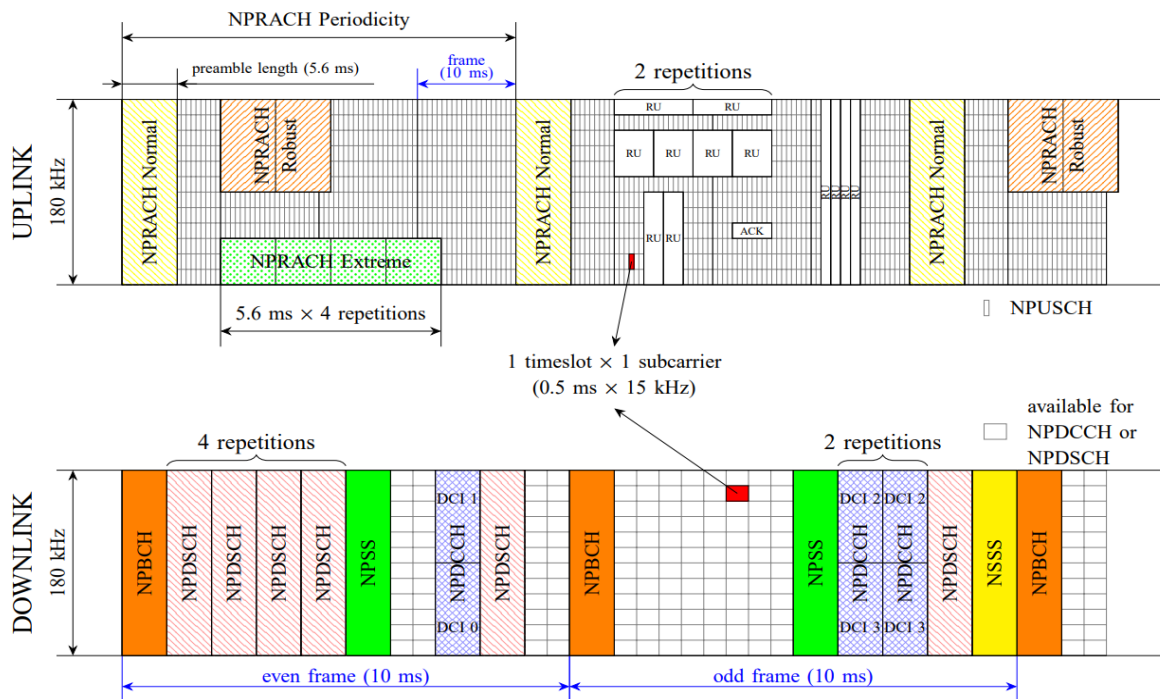


Figura 6 - Ilustração representativa dos processos de uplink e de downlink em NB-IoT [5]

A tecnologia NB-IoT permite uma maior cobertura de 20dB GSM / GPRS, através da utilização de sinais de uma banda mais estreita e através da diversidade de tempo de transmissão. Um sinal de banda estreita permite que o recetor filtre mais ruído, melhorando assim o “Signal to Interference and Noise Ratio” (SINR).

Para aumentar a probabilidade de sucesso na transmissão do sinal, são permitidas até 2048 repetições em Downlink e 128 repetições em Uplink. Cada réplica pode ser decodificada separadamente ou várias réplicas podem ser combinadas para aumentar ainda mais a probabilidade de receção.

O NB-IoT permite ainda flexibilidade na configuração do serviço, definindo três classes de cobertura: Normal, Robusta e Extrema.

As classes são diferenciadas através de limiares baseados em sinal/força, definidas para introduzir três níveis de extensão de cobertura GSM / GPRS: 0dB, 10dB e 20dB, para Normal, Robusto e Extremo, respetivamente.

Técnicas para economia de energia - Além de reduzir a potência máxima de transmissão de 23dB para 14dB, o NB-IoT introduziu duas técnicas de economia de

energia: a recepção descontínua estendida eDRX (extended Discontinuous Reception) e o modo de poupança de energia PSM (Power Saving Mode).

Em estado inativo, o terminal verifica periodicamente o canal para analisar os dados recebidos. Essa periodicidade, ou seja, o Ciclo DRX, foi estendido de 2,56s (valor máximo em LTE) até um máximo de eDRX de ~175 minutos em NB-IoT, conforme podemos comprovar na figura 8 (eDRX cycle < 2.9 hours).

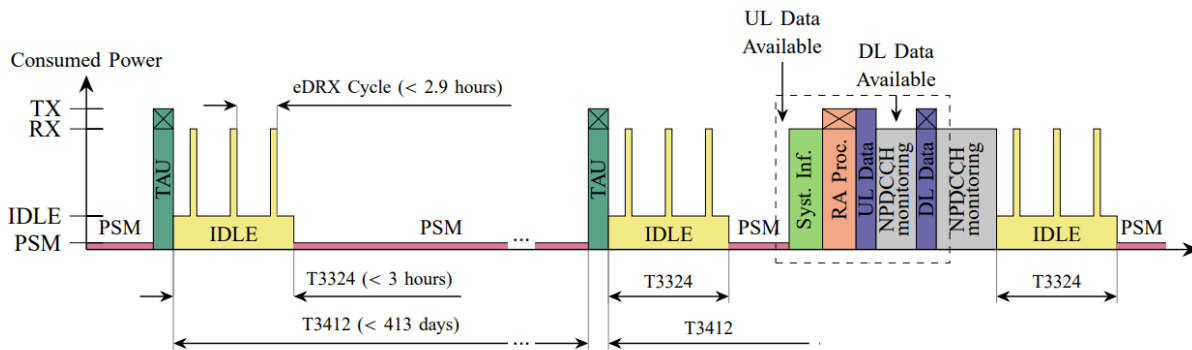


Figura 7 - Ilustração representativa do ciclo de vida de um terminal NB-IoT [5]

A um terminal também pode ser permitido mudar para PSM, sendo que o equipamento está registrado na rede, mas não acessível.

No final do ciclo de PSM, o terminal realiza uma Atualização da Área de Rastreo TAU (Tracking Area Update).

No que se refere à avaliação da performance, o desempenho da tecnologia NB-IoT varia em cenários com densidade diferente, periodicidade diferente (RP) e Carga diferente (PS), que determinam a percentagem de terminais em classes Normal, Estendido e Extrema.

O total de sobrecarga (considerando o protocolo UDP / IP e 3GPP) é de 65B. Os terminais acordam aleatoriamente considerando a sua periodicidade (RP), decodificam, executam o procedimento random access (RA) para enviar um relatório de uplink.

O cenário de implantação considera estações base de três setores, implantadas numa grelha hexagonal, com uma distância entre locais que foi variando, considerando 500m, 1000m e 1732m, conforme se pode verificar na figura 9.

O número de repetições utilizadas é calculado considerando -100dB e -110dB como potência de sinal recebida.

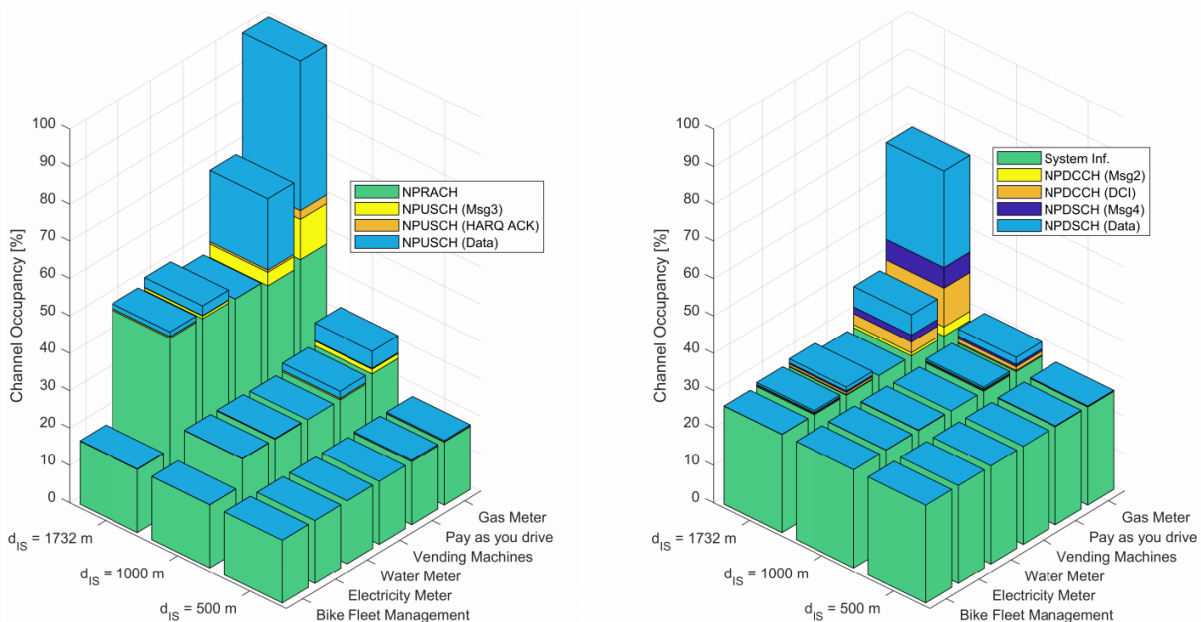


Figura 8 - Gráficos da ocupação do canal de UL e DL [5]

NPRACH (NB-IoT physical random access channel) refere-se à frequência de tempo na qual os preâmbulos de acesso aleatório são transmitidos.

Transmitir um preâmbulo de acesso aleatório é o primeiro passo do procedimento de comunicação. Este permite a um equipamento estabelecer ligação à rede [6].

Impacto da configuração do NPRACH - A fim de investigar o trade-off entre a rede, a taxa de transferência e a quantidade de recursos disponíveis de uma rede NB-IoT, foi realizada uma análise, aumentando a quantidade de dispositivos e variando a configuração da periodicidade NPRACH.

Na figura 10 são mostrados dois gráficos representativos da percentagem de recursos livres face à evolução do tráfego gerado pelos terminais.

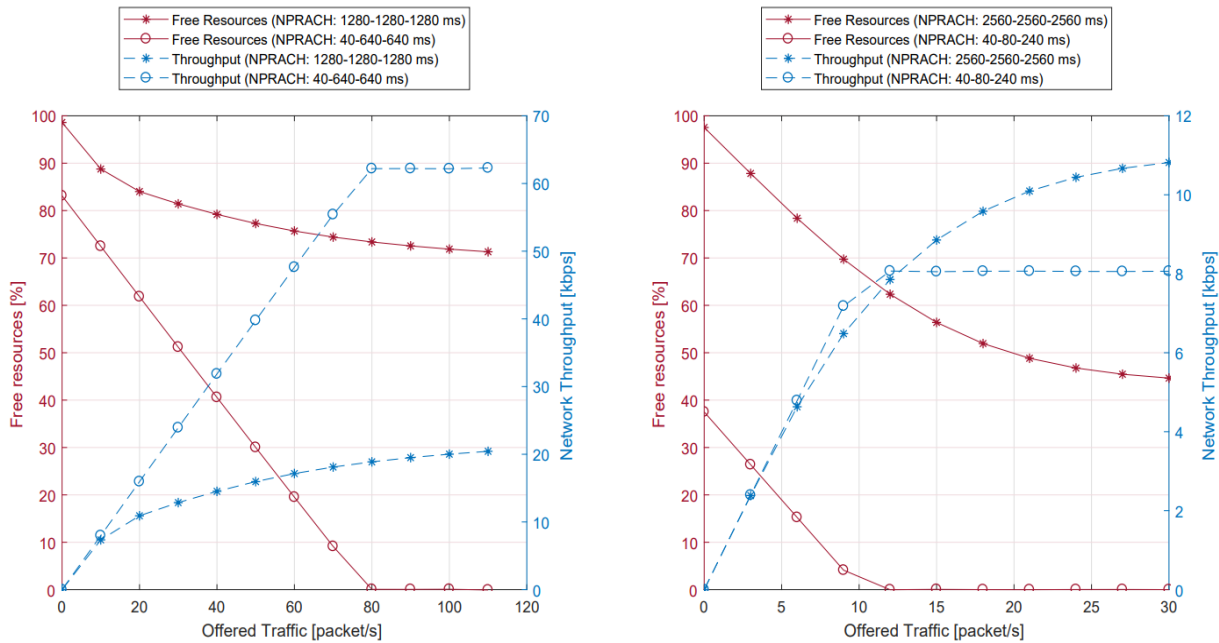


Figura 9 – Gráficos com percentagem de recursos livres e ocupação da rede [5]

O eixo dos x representa o tráfego gerado pelos terminais, enquanto o eixo y mostra a percentagem de recursos livres e a ocupação da rede.

A rede satura a uma taxa de transferência de 62 kbps (curva a tracejado) porque todos os recursos rádio foram usados (curva em sólido). As curvas com os marcadores em forma de estrela representam configuração onde o NPRACH é significativamente menor.

Neste caso, a rede satura para uma taxa de transferência muito menor, 20 kbps, porque apenas alguns terminais podem completar o procedimento RA (cerca de 70% dos recursos não foram utilizados).

Neste subcapítulo apresentou-se uma descrição detalhada das principais características da NB-IoT e dos procedimentos de transmissão e recepção de dados com fontes de latência associados.

Discutiou-se como a configuração dos parâmetros de rede afeta o desempenho de latência do NB-IoT e discutiu-se também como podem ser ajustados de modo a melhorar as suas capacidades. [5] e [12]

2.3.1.2 - LoRa – Long Range

LoRa é uma tecnologia de comunicação sem fios para redes de longa distância / área alargada, baixa potência e de baixa largura de banda (LPWAN).

Os dispositivos comunicam diretamente com os gateways. Estes, por sua vez, funcionam como pontes transparentes na retransmissão das mensagens para o servidor de rede central (LoRaWAN Server), que se encarrega de as processar e disponibilizar para a camada aplicacional (conforme exemplo de sistema de controlo de estacionamento representado na figura 11).

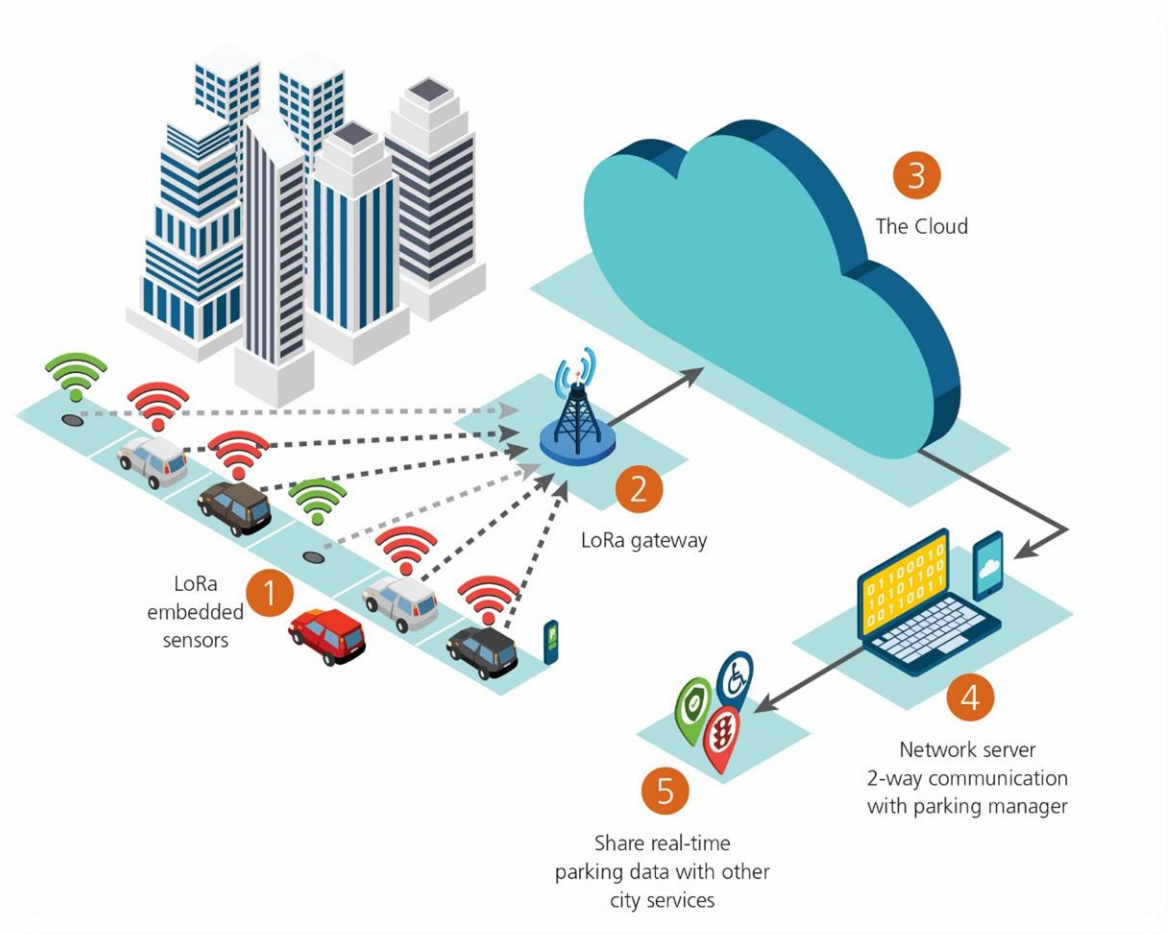


Figura 10 - Ilustração representativa de arquitetura de uma rede LoRa [24]

É atualmente considerada uma das tecnologias mais utilizadas em projetos IoT, essencialmente devido à capacidade de cobertura, ao baixo custo dos equipamentos, ao baixo consumo de energia e à grande quantidade de empresas especializadas no fornecimento e instalação deste tipo de soluções.

Podemos separar o LoRa em duas camadas distintas: a camada física da rede, utilizando a técnica de modulação de rádio Chirp Spread Spectrum (CSS), e a camada lógica da rede, que define a arquitetura e os parâmetros da comunicação (LoRaWAN - protocolo da camada MAC).

A camada física da rede, desenvolvida pela Semtech, permite comunicações de longa distância, baixo consumo energético e comunicações de baixa largura de banda.

Utilizada há décadas sobretudo em sistemas militares e em radares, por possibilitar longo alcance e grande resistência a ruídos, sempre fez parte de sistemas muito críticos no que diz respeito à estabilidade da frequência e a altos custos.

Com o avanço das tecnologias passou a ser viável utilizar estas mesmas técnicas usando cristais e outros componentes mais baratos, sendo a tecnologia LoRa a primeira implementação de baixo custo desenvolvida para uso comercial.

Opera em bandas ISM que variam dependendo da região em que se encontra instalado, podendo a taxa de transmissão de dados chegar aos 50 Kbps (conforme tabela 4).

Tabela 4 - Tabela comparativa de especificações LoRa em vários locais do mundo [25]

	EUROPA	AMERICA	CHINA	COREIA	JAPÃO	ÍNDIA
FREQUENCIA	867-869 MHz	902-869 MHz	470-510 MHz	920-925 MHz	920-925 MHz	865-867 MHz
CANAIS	10	64 + 8 + 8	Em definição pelo "Technical Committee"			
UPLINK	125 / 250 KHz	125 / 500 KHz				
DOWNLINK	125 KHz	500 KHz				
TRANSMISSÃO	50 kbps	21.9 kbps				

A camada lógica da rede, através de um protocolo da camada MAC (LoRaWAN), fornece um mecanismo de MAC, permitindo que muitos dispositivos comuniquem com um único gateway.

As características e especificações do LoRaWAN apresentam mais valias ao nível de operações de camada de Controlo de Acesso Médio (MAC), oferecendo bom desempenho nas comunicações entre dispositivos IoT [8].

O protocolo LoRaWAN implementa os detalhes do funcionamento, segurança, qualidade do serviço, ajustes de potência visando maximizar a duração da bateria dos módulos, e os tipos de aplicações tanto do lado dos dispositivos como do lado do servidor LoRaWAN.

Enquanto a modulação LoRa é proprietária, o LoRaWAN é um padrão aberto desenvolvido pela Aliança LoRa. [11]

Avaliação de desempenho – Foram analisados os testes do artigo em questão [11], com objetivo de verificar o desempenho dos dispositivos LoRa.

O ambiente de testes foi desenvolvido com recurso a uma placa de desenvolvimento Freescale KRDM-KL25Z com escudo Semtech SX1276 MBED como dispositivo terminal, e um router industrial Cisco 910 usado como o Gateway (figura 12).



Figura 11 - Fotos de dispositivo terminal e de gateway LoRa [11]

Neste teste foram enviados de um dispositivo LoRa para o gateway cerca de 10.000 pacotes, tendo os indicadores de intensidade do sinal (RSSI) dos pacotes recebidos sido registrados.

O gateway foi instalado dentro de uma casa, e os dispositivos foram testados ao ar livre, num ambiente urbano. Todos os pacotes foram enviados na frequência de 125 kHz. A potência de transmissão do dispositivo terminal foi definida para o mínimo (2 dBm, com uma antena de 3 dBi), a fim de limitar a distância a cobrir antes de alcançar baixos RSSIs. A ordem de magnitude da distância entre o dispositivo final e o gateway

em que os pacotes se começaram a perder foi de 100 metros. Os RSSIs mínimos observados estão representados na figura 13.

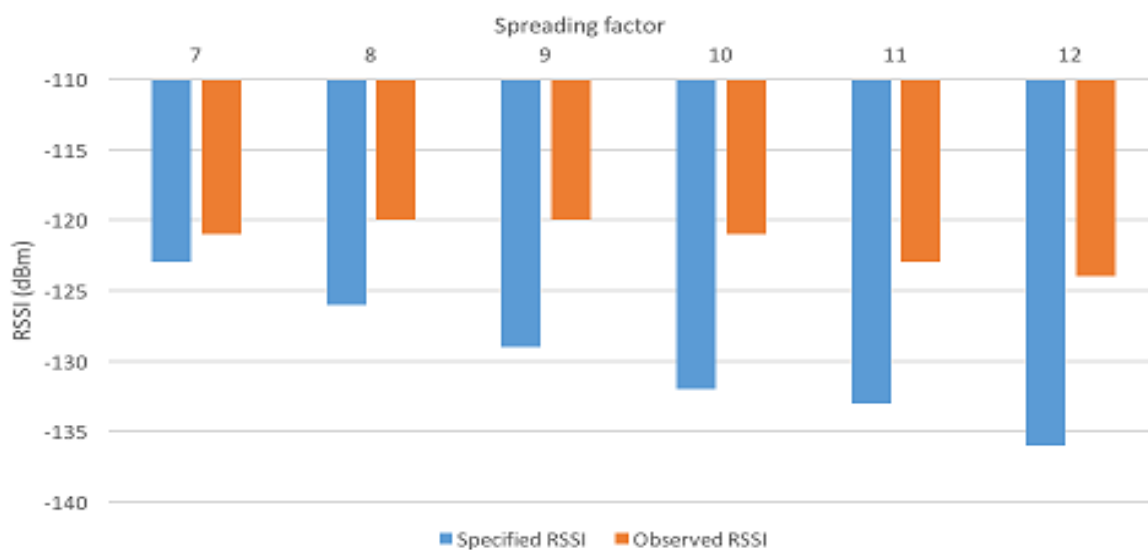


Figura 12 – Gráfico representativo dos RSSIs face a fatores de spreading diferentes [11]

Os resultados obtidos estão ligeiramente acima dos valores esperados e a diminuição esperada face ao aumento do fator de spreading (duração do chirp, que é um sinal em que a frequência aumenta ou diminui com o tempo) não é tão evidente.

No entanto, os pacotes que atingiram os RSSIs mais baixos também foram recebidos com um alto SINR, próximo a 20 dB. Isto deveu-se provavelmente ao facto do gateway estar dentro de casa.

Cobertura de rede - Esta experiência testou a cobertura de rede do LoRa. Os testes foram conduzidos nos subúrbios de Paris, com residências principalmente baixas. A temperatura era de cerca de 15 ° C e a humidade do ambiente era de cerca de 55%. O gateway ficou no segundo andar de uma casa.

Foram escolhidos cinco pontos para testes, sempre com distâncias diferentes em relação ao gateway, conforme figura 14.

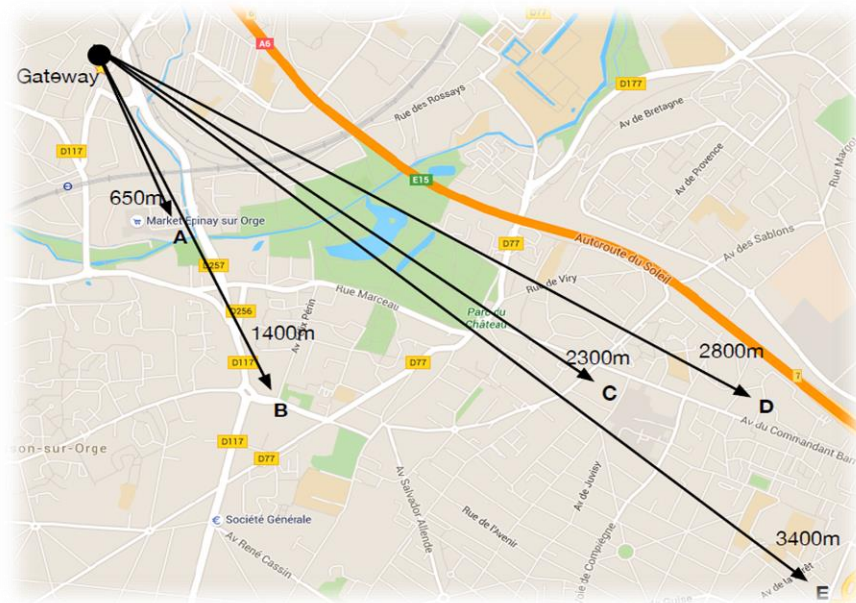


Figura 13 - Mapa representativo das localizações do gateway e dos dispositivos terminais [11]

A potência de transmissão do dispositivo final foi configurada para 14 dBm, que é o valor padrão indicado. Para testar o desempenho de diferentes fatores de spreading (de 7, 9 e 12), o reconhecimento de pacotes e a retransmissão foram desativados. A verificação de links também foi desativada, sendo que, por padrão, o LoRa irá adaptar o fator de propagação de acordo com a qualidade do link.

A gráfico representado na figura seguinte (15), mostra a taxa de entrega de pacotes com diferentes fatores de spreading e com várias distâncias. Cerca de 100 pacotes foram transmitidos para o servidor de rede em cada teste.

Os maiores fatores de spread têm melhor cobertura: para um fator de expansão de 12, mais de 80% dos pacotes foram recebidos no Ponto D (2800 m), enquanto nenhum pacote foi recebido com um fator de propagação de 7.

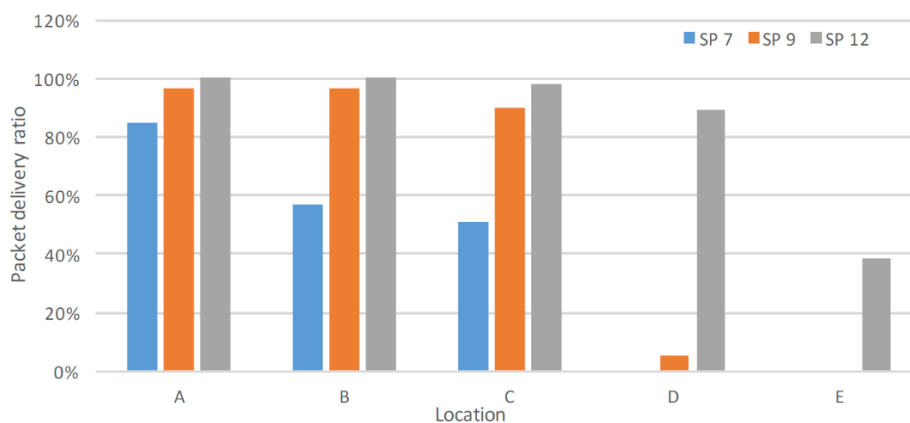


Figura 14 - Gráfico com rácio de pacotes entregues com locais e spreadings diferentes [11]

Vale a pena referir que o gateway estava localizado no segundo andar, que ficava a cerca de 5 m acima do solo (normalmente, essa estação base estaria localizada em altitude para obter uma melhor cobertura), e o ponto de teste D estava logo atrás de um prédio de sete andares.

De acordo com os resultados obtidos no ambiente de testes, chegou-se à conclusão de que uma taxa de entrega elevada, alcançada através de um aumento do fator de spreading, tem como consequência a redução da largura de banda.

Por outro lado, verificou-se que a cobertura da rede diminui fortemente à medida que vão baixando os fatores de propagação.

LoRaWAN

É um protocolo MAC, criado com base na utilização da camada física LoRa. Foi projetado principalmente para sensores que trabalhem em redes com baixa capacidade de transferência de dados e com intervalos de transmissão bastante espaçados (de uma transmissão por hora até vários dias).

O LoRaWAN possui três classes diferentes de dispositivos:

- Classe A (sensores): os dispositivos podem transmitir dados de acordo com as suas próprias necessidades, mas a recepção de dados só se efetua mediante pedido do terminal, originando um menor consumo de energia.
- Classe B (atuadores): os dispositivos possuem comunicações agendadas no tempo. O gateway envia um beacon para saber que terminais estão à escuta.
- Classe C: os dispositivos finais de classe C têm um funcionamento de recepção de dados quase contínuo, sendo, portanto, a Classe que tem um maior consumo de energia.

O LoRaWAN não permite comunicação direta de dispositivos para dispositivos: os pacotes só podem ser transmitidos de um dispositivo para o servidor de rede, ou vice-versa. Comunicações de dispositivo para dispositivo devem ser “disparadas” através do servidor de rede, originando duas transmissões de dados por parte do gateway (recepção do dispositivo A e envio para o dispositivo B).

As especificações indicam que as redes LoRaWAN devem usar frequências sujeitas a regulamentações referentes à potência do sinal de transmissão e ao ciclo de serviço. Essas limitações do ciclo de trabalho traduzem-se em atrasos dos dados enviados pelos dispositivos. Se a limitação é de 1%, o dispositivo terá que esperar 100 vezes a duração do último envio até enviar novamente no mesmo canal.

Análise ao desempenho de LoRaWAN – Nesta secção vamos analisar e discutir o desempenho de LoRaWAN com base nos resultados obtidos em [7].

O objetivo deste teste é avaliar o rendimento máximo que um dispositivo pode obter. Os testes foram efetuados com seis canais de 125 kHz e utilizando fatores de propagação de 7 a 12. Como nenhum comando MAC foi enviado, então o tamanho do cabeçalho MAC foi sempre 13 bytes.

Os resultados, dependendo do tamanho da carga útil, são visíveis na figura 16 (cerca de 100 pacotes transmitidos em cada teste).

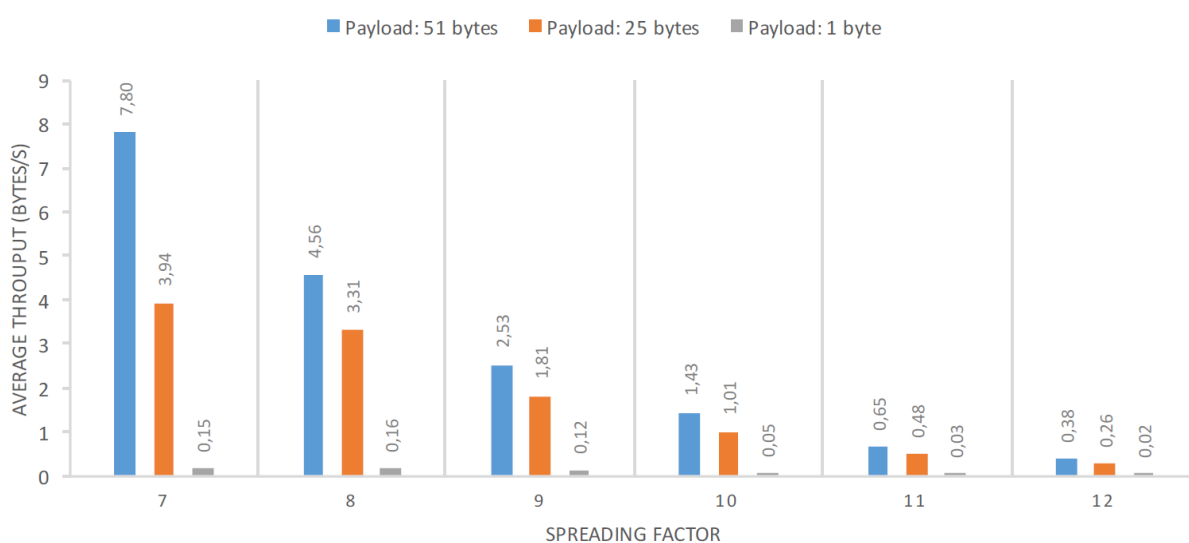


Figura 15 - Gráfico comparativo da taxa de transferência média com 1 único dispositivo [11]

Esta experiência revelou que em pacotes pequenos, o fator limitador não foi canal, como poderia ter sido esperado, mas a duração das janelas de receção.

A maior limitação deveu-se ao facto de o dispositivo ter que esperar pelas duas janelas de receção de downlink após a transmissão ter acabado, para depois poder enviar outro pacote.

No entanto, uma vez que o LoRaWAN foi projetado para gerir grandes quantidades de dispositivos, com transmissão de pequenos volumes de dados espaçados no tempo, ao enquadrarmos esta tecnologia neste âmbito, chegamos à conclusão de que este fator limitador do LoRaWan não pode ser considerado como uma menos valia na implementação de projetos IoT.

Capacidade total e carga do canal - A capacidade total da rede não está relacionada apenas com o tamanho da carga útil. Como duas transmissões na mesma frequência, mas com diferentes fatores de propagação, podem ser decodificadas em simultâneo, é definido um canal lógico por par (frequência e fator de spreading).

A capacidade total de transmissão de uma rede LoRaWAN é a soma das capacidades de todos os canais lógicos. Numa frequência de 125 kHz, existem seis possíveis fatores de propagação (de 7 a 12), o que aumenta a capacidade total de um canal de 125 kHz para 12.025 bps.

Como a taxa de transferência depende do fator de spreading, nem todos os canais lógicos têm a mesma capacidade.

A carga para um canal é definida pela média temporal da quantidade de dispositivos LoRa que estão a tentar enviar dados. Isto coincide com a definição natural da carga: nas condições ideais, ou seja, com uma sincronização perfeita dos dispositivos, a carga total poderá ser alcançada, saturando o canal.

Neste subcapítulo apresentou-se uma descrição detalhada das principais características da tecnologia de comunicação LoRaWan.

Verificamos que o LoRaWan é um protocolo de comunicações de longo alcance e de baixa potência, com características e especificações adaptadas ao conceito de “Internet das Coisas” e que a camada física usa a modulação LoRa.

O LoRaWAN é um “open standard” que disponibiliza as suas especificações gratuitamente e que se encontra consolidado em todo o mundo, conforme podemos confirmar na figura 20 (<https://loro-alliance.org>).

Conclui-se então que, de acordo com testes analisados, graças à modulação do espectro de propagação chirp e à alta sensibilidade dos receptores, o LoRa oferece boa resistência a interferências.

Testes de campo mostram que o LoRa pode oferecer uma cobertura de rede satisfatória até 3 km, em áreas com moradias residenciais densas.

O fator de propagação tem impacto significativo na cobertura de rede e na taxa de transferência, mas o desempenho degrada-se rapidamente à medida que a carga do link aumenta. [9] [11]

3.1.3 - 802.15.4 (6LowPAN)

O IEEE 802.15.4 é um padrão que especifica a camada física e a camada de ligação (MAC) em redes do tipo de área pessoal sem fios (low-rate wireless personal area networks).

Foi desenvolvido para sistemas de comunicações de baixo custo, em redes de curta distância e com pouca infraestrutura, com o principal objetivo de reduzir ao máximo o consumo de energia.

O IEEE 802.15.4 trabalha nas bandas de frequências ISM (Industrial, Scientific and Medicine), que são gamas abertas e que não necessitam de licenciamento.

Na Europa, na gama de frequências 868MHz, só existe um canal de comunicação e a taxa de transmissão de dados pode chegar aos 20 Kbps.

Nos EUA, na gama dos 902-928Mhz existem 10 canais com espaçamento de 2 Mhz e a taxa de transmissão pode chegar aos 40 Kbps.

Já no que se refere à gama dos 2.400-2.4835 Ghz, que é a mais utilizada, existem 16 canais de 5MHz e o débito pode chegar aos 250kbps. Na figura 17 são representados estes canais e as frequências da camada física do protocolo 802.15.4.

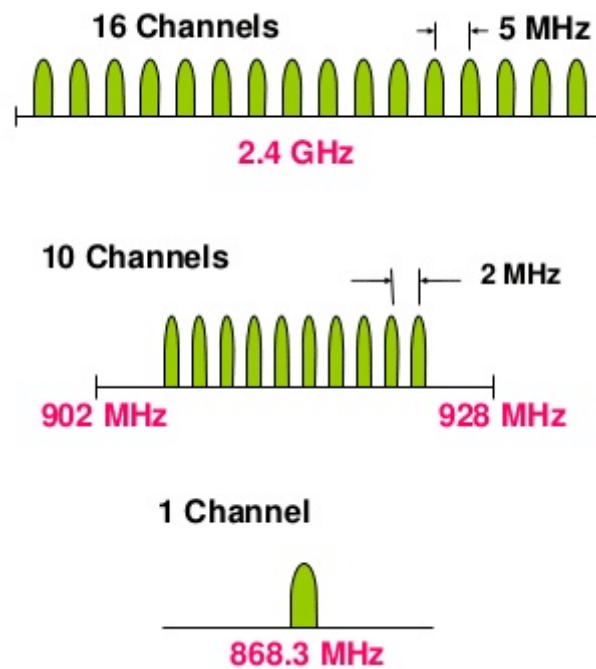


Figura 16 - Canais e frequências da camada física do protocolo 802.15.4 [26]

Estes três conjuntos totalizam os 27 canais disponíveis, sendo cada um deles identificado pela combinação do número da página e do número do canal (conforme tabela 5).

Tabela 5 – Especificações por canal da camada física do protocolo 802.15.4 [27]

Página	Número de canal	Frequência	Taxa de transmissão	Modulação
0	0	868 MHz	20	BPSK
	1-10	915 MHz	40	BPSK
	11-26	2,4 GHz	250	O-QPAK
1	0	868 MHz	250	ASK
	1-10	915 MHz	250	ASK
	11-26	Reservado		
2	0	868 MHz	100	O-QPSK
	1-10	915 MHz	250	O-QPSK
	11-26	Reservado		
3-31	Reservado	Reservado		

6LowPAN (IPv6 over Low-power wireless Personal Area Network) é uma camada que define o encapsulamento, os cabeçalhos e os mecanismos de compressão, utilizado em

redes de sensores com limitações energéticas, de baixo alcance, baixas taxas de transmissão e baixo custo.

Foi criado para que fosse possível comunicar através de IPv6 em protocolos de rede como é o caso do padrão 802.15.4.

6LowPAN cria uma camada de adaptação entre o IEEE 802.15.4 e o IPv6, com cabeçalhos específicos para cada uma dessas funções.

Está localizado numa camada intermédia entre a camada de ligação e a camada de rede (conforme representado na figura 18).

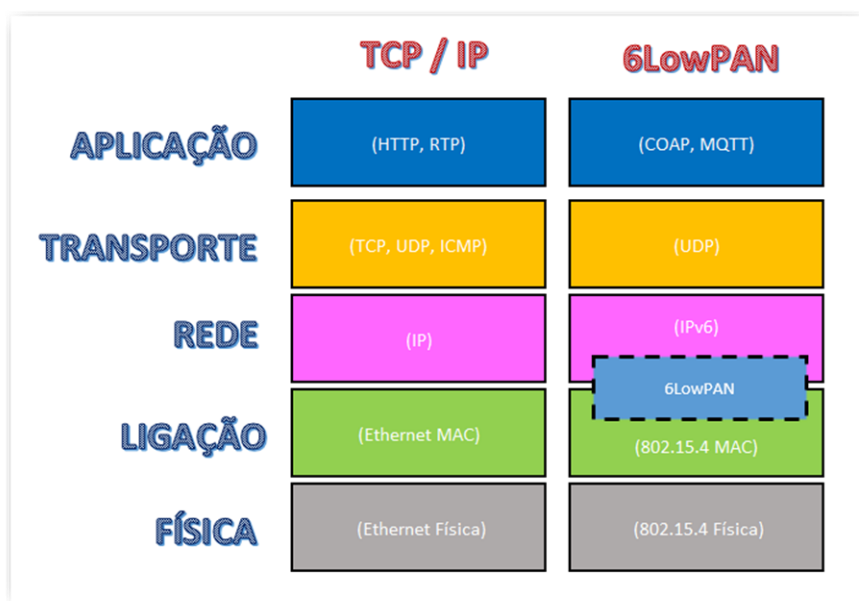


Figura 17 – Comparativo entre modelo TCP/IP e 6LowPAN [28]

Como suporta IPv6, tornou possível atribuir a cada objeto ou equipamento do mundo um IP único e conectá-lo à internet. Desta forma todos os dispositivos passam a fazer parte no mundo da Internet ou "Internet of Things".

Cada pequena rede 6LowPAN é independente da Internet, ou seja, os pacotes transmitidos na mesma não são transmitidos para redes diferentes.

Todos os pacotes com destino a redes externas terão obrigatoriamente que ser encaminhados através de um coordenador (border router) até à rede de destino.

Cada rede 6LoWPAN partilha o mesmo prefixo do endereço IPv6 (os primeiros 64 bits) e está limitada a 64000 dispositivos.

Este limite é imposto pelo endereçamento utilizado pelo IEEE 802.15.4, que usa 16 bits de endereços para cada dispositivo na rede.

Existem três classes de redes 6LoWPAN:

- Ad-Hoc – Redes sem conexão à Internet e que funcionam sem qualquer infraestrutura;
- Simples – Redes interligadas a outras redes através de um border-router;
- Extendidas – Múltiplas redes interligadas por múltiplos border-routers e à Internet.

O border-router é essencial no encaminhamento da informação, sendo responsável por:

- Conexão entre redes;
- Controlo de fluxos;
- Fragmentação / desfragmentação;
- Compressão / descompressão dos pacotes IPv6;
- Registo dos endereços através do Neighbor Discovery.

Nas fotos apresentadas na figura 19, podemos visualizar à direita os equipamentos Raspberry PI e Zolertia, que desempenham as funções de border-router.



Figura 18 – Dispositivo terminal e border-router

É necessária a existência de um border-router sempre que uma rede 6LoWPAN necessita de comunicar com uma rede IPv4. Só este nó permite a interligação entre estas duas redes (conforme representado nas imagens 20).

Neste subcapítulo demonstra-se que 6LowPAN é uma camada que trabalha sobre outros protocolos de rede, nomeadamente o protocolo 802.15.4, não se podendo comparar diretamente com NB-IoT ou com LoRaWan.

2.3.5 – Protocolos IoT da camada de transporte

A camada de transporte é responsável pela transferência de dados entre equipamentos, independente da aplicação, do tipo, topologia ou configuração das redes físicas.

A camada de transporte faz a ponte entre as camadas aplicacionais e as camadas físicas. As camadas de nível aplicacional enviam os dados contidos nos pacotes para as aplicações de destino, e as camadas de nível físico encarregam-se da forma como os dados serão transmitidos pela rede.

A transferência de dados nesta camada pode ser realizada mediante a utilização de conexões ou através de datagramas. Os protocolos desta camada podem ou não oferecer confiabilidade, garantia de entrega, controle de fluxo, entre outros.

Embora existam vários protocolos da camada de transporte, como por exemplo, RTP, DCCP, SCTP ou RSVP, os dois protocolos mais utilizados desta camada são o UDP e o TCP.

Nas soluções e projetos IoT, o protocolo da camada transporte mais utilizado é o UDP. Esta opção deve-se essencialmente a uma dimensão mais reduzida dos pacotes, comparativamente com o protocolo TCP.

O cabeçalho dos pacotes do protocolo TCP utiliza um número mais elevado de bits do que o do UDP.

Por exemplo, conforme se consegue verificar na figura 21, o cabeçalho do protocolo TCP indica o *Sequence number* e o *Acknowledgment Number*, que permitem garantir a ordem e a confirmação de entrega do pacote.

Já no cabeçalho do protocolo UDP esses dados não aparecem uma vez que cada pacote UDP é único e indivisível.

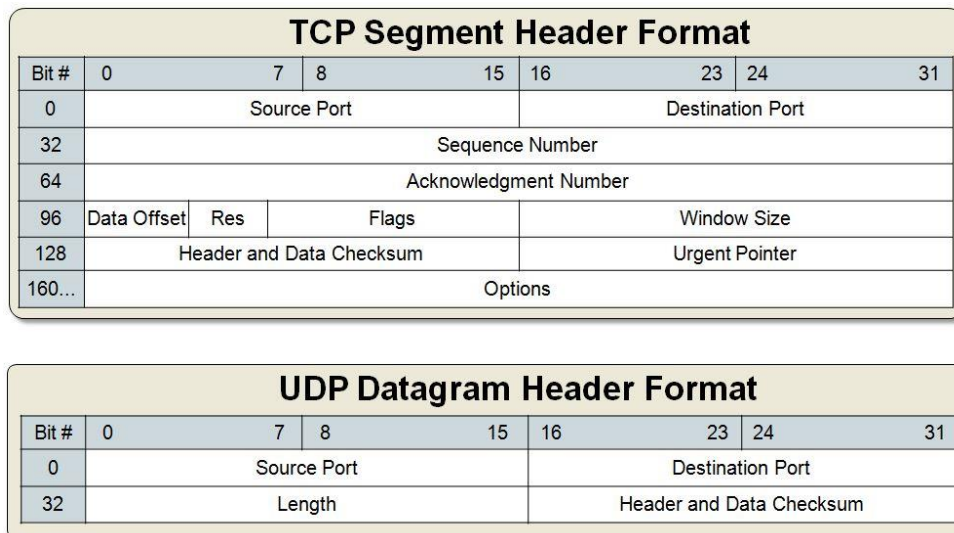


Figura 19 - Cabeçalhos TCP e UDP [29]

A diminuição do número de bits utilizados permite reduzir a largura de banda necessária para transmissão dos pacotes e reduzir as necessidades de processamento no encapsulamento (baixando também o consumo energético dos dispositivos).

O protocolo UDP (User Datagram Protocol)

Situa-se na camada de transporte, descrito na RFC 768 e permite à camada de aplicação encaminhar datagramas encapsulados em pacotes IPv4 ou IPv6.

Porém, este protocolo não apresenta garantias de entrega de pacotes no destino, não apresentando confiabilidade. Caso sejam necessárias garantias de entrega de pacotes, é necessário proceder à implementação de várias estruturas de controlo, tais como *timeouts*, retransmissões, *acknowledgements*, controlos de fluxo, etc.

Ao contrário do TCP, que é um protocolo orientado a fluxos de bytes sem início e sem fim, cada datagrama UDP é único e pode ser considerado como um registo indivisível.

É um serviço sem conexão, pois não necessita de manter um relacionamento entre o cliente e o servidor. Assim, o cliente UDP pode criar um socket, enviar dados para um

servidor e de seguida enviar um outro datagrama com o mesmo socket para um outro servidor. Da mesma forma, através de um único socket é possível a um servidor poder receber informação vinda de diversos clientes.

O UDP também fornece os serviços de broadcast e multicast, permitindo que um único cliente envie pacotes para vários outros clientes da rede [19].

O protocolo UDP não suporta SSL / TLS. Em alternativa, para fornecer segurança nas transferências de dados, este utiliza o DTLS, Datagram Transport Layer Security.

A utilização do protocolo UDP faz-se principalmente nos serviços que não precisam de garantir a chegada de pacotes. Streamings de vídeo e serviços de voz sobre IP são exemplos de utilização UDP.

Protocolo TCP (Transmission Control Protocol)

O TCP é um protocolo de nível da camada de transporte e é sobre este que assentam a maioria dos protocolos da camada de aplicação, como o SSH, FTP, HTTP.

O protocolo de controlo de transmissão faz a ponte dos dados transferidos entre as camadas físicas e as camadas aplicacionais, e garante confiabilidade, sequência correta de entrega de pacotes e verificação de erros.

Aplicações que não necessitem de um serviço com confiabilidade de entrega de pacotes podem utilizar de protocolos mais simples como o User Datagram Protocol (UDP) [4].

Embora não seja o mais adequado para projetos IoT, continua a ser muito utilizado neste tipo de projetos.

A utilização deste protocolo verifica-se mais na comunicação entre plataformas do que nas comunicações entre dispositivos IoT.

Contrariamente à grande maioria das plataformas aplicacionais, os dispositivos IoT possuem baterias de baixa capacidade, o que obriga a restrições no consumo energético e na largura de banda.

A utilização deste protocolo deve-se em grande parte à utilização massificada da Internet, que é suportada por este, e ao facto de muitas das plataformas IoT alojadas na cloud comunicarem através de APIs HTTP (REST).

2.3.5 – Protocolos IoT da camada de aplicação

Com a massificação da comunicação entre dispositivos e plataformas IoT, foi necessário recorrer à utilização de conceitos e protocolos que exigem baixa largura de banda e baixo processamento de dados.

Embora os protocolos mais adaptados para IoT sejam o MQTT e o CoAP, existem muitos projetos IoT implementados com recurso ao protocolo HTTP (Hypertext Transfer Protocol) e ao conceito RESTful APIs (Representational State Transfer).

A utilização desta última deve-se em grande parte à utilização massificada que esta tem no desenvolvimento das soluções Web modernas, justificada pela sua simplicidade e pelo conhecimento já adquirido por parte dos programadores.

Tanto o MQTT como o CoAP são normas abertas, mais adequados para ambientes com restrições de processamento, de largura de banda e de consumo energético, do que o HTTP (REST), que consome mais recursos e necessita de mais recursos por parte dos dispositivos e das redes. O MQTT oferece flexibilidade nos padrões de comunicação e atua apenas como um canal para dados binários, enquanto que o CoAP foi projetado para interoperabilidade com a web. [14]

Em projetos IoT é comum recorrer-se à utilização de APIs (Application Programming Interface) para efetuar e controlar a transferência de informação entre os sensores, gateways, atuadores e plataformas IoT de controlo/gestão.

Uma API é um conjunto de padrões de programação que permitem a construção de aplicativos mais seguros e eficazes. Sendo invisível para os utilizadores e funcionando como suporte às aplicações informáticas, esta interface permite definir comportamentos e permissões de acesso aos sistemas, aumentando a segurança no acesso aos dados e diminuindo os riscos de manipulação de dados. [14]

Existem atualmente online diversas ofertas de APIs, desenvolvidas especificamente para IoT (ex. <https://www.programmableweb.com/category/internet-things/api>).

MQTT (Message Queue Telemetry Transport)

Desenvolvido pela IBM no final dos anos 90, com base no protocolo TCP/IP, acabou por se tornar um padrão para comunicações IoT. É um protocolo de mensagens com suporte para a comunicação assíncrona e utiliza um modelo de publicação / assinatura. No final de 2014, tornou-se oficialmente um padrão aberto, com suporte nas linguagens de programação mais populares e usado em diversas implementações de soluções de software [17].

O MQTT é um protocolo de rede leve e flexível, que oferece o equilíbrio ideal para os programadores IoT, permitindo implementações em hardware com baixas capacidades e em redes com largura de banda limitada e alta latência.

Embora a maioria dos serviços da Web corram via HTTP, este padrão tem algumas limitações graves, nomeadamente o facto de ser síncrono, de ser unidirecional, de ser um-para-um e de ser um protocolo pesado com muitos cabeçalhos e regras.

O protocolo MQTT define dois tipos de entidades na rede: um message broker e os clientes. O broker é um servidor que recebe todas as mensagens dos clientes e, em seguida, direciona essas mensagens para os clientes de destino relevantes. Um cliente é qualquer dispositivo que possa interagir com o broker e receber mensagens.

Como as mensagens do MQTT são organizadas por tópicos, o programador pode especificar que determinados clientes somente podem interagir com determinadas mensagens. Por exemplo, os sensores publicarão as suas leituras no tópico "sensor_data" e assinarão o tópico "config_change".

Os aplicativos de processamento de dados que salvam os dados do sensor numa base de dados assinaram o tópico "sensor_data", conforme figura 22.

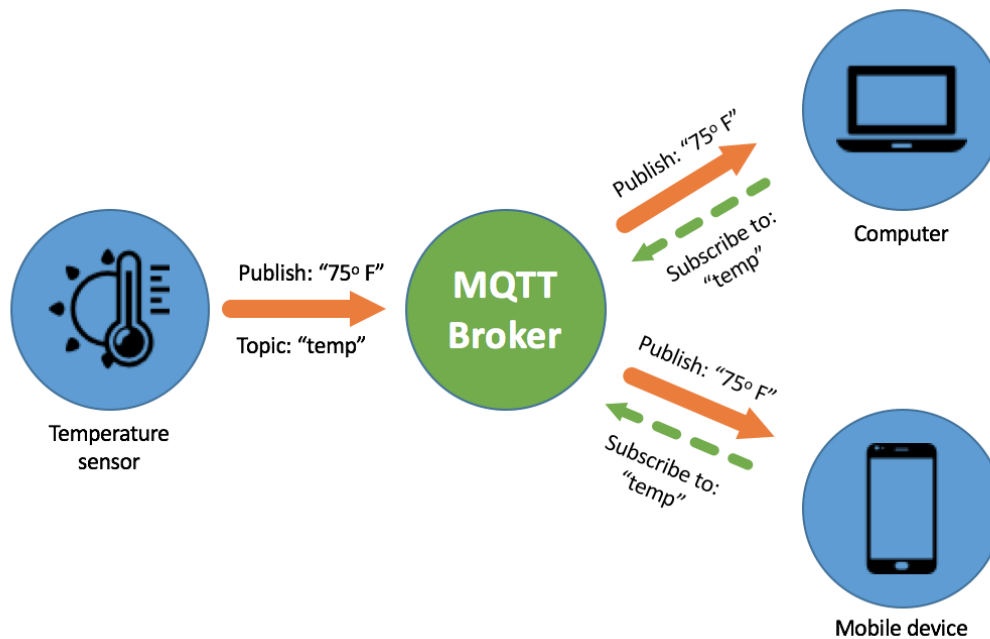


Figura 20 - Ilustração representativa de transmissão de dados entre 1 sensor e 2 clientes [30]

Ao mesmo tempo, o MQTT é leve, uma vez que tem um cabeçalho simples. Pode usar qualquer formato de dados, quer seja JSON, XML, binário criptografado ou Base64, desde que os clientes de destino o possam interpretar.

A grande vantagem do MQTT é a simplicidade. Não há restrições quanto ao tipo de tópico ou de mensagem que se pode usar. Isso permite alguns casos de uso interessantes. Por exemplo, para executar mensagens de um para um com o MQTT, o nome do tópico pode conter os IDs dos dois clientes para garantir a sua exclusividade. Outro exemplo é como proteger as comunicações. A ligação do cliente com o broker pode ser criptografada através de TLS, ou com um método de criptografia e um mecanismo de atualização de chaves. [15]

COAP (Constrained Application Protocol)

Tal como o protocolo HTTP, o CoAP é um protocolo de transferência de dados. Ao contrário do HTTP, o CoAP foi projetado tendo em conta as restrições de capacidade de processamento e de largura de banda.

O CoAP é executado sobre UDP. Clientes e servidores comunicam através de datagramas sem ligação. O CoAP permite que broadcast e multicast UDP sejam usados

para endereçamento, seguindo um modelo cliente / servidor. Os clientes fazem solicitações e os servidores devolvem respostas (GET, PUT, POST e DELETE). [17]

O CoAP foi projetado para operar com o HTTP e a Web REST por meio de proxies simples. Como o CoAP é baseado em datagramas pode ser usado tanto em SMS como noutros protocolos de comunicação baseados em pacotes.

A nível de aplicação QoS, as solicitações e mensagens de resposta podem ser marcadas como “confirmable” ou “nonconfirmable”. Mensagens confirmadas são respondidas pelo recetor com um pacote ack e mensagens não-confirmadas são esquecidas.

Como o CoAP trabalha sobre UDP e não sobre TCP, o SSL / TLS não está disponível para fornecer segurança. Neste caso utiliza-se o DTLS, Datagram Transport Layer Security, que fornece as garantias semelhantes ao TLS, mas para transferências de dados por UDP.

No CoAP, um sensor é tipicamente um servidor e não um cliente (embora possa ser ambos). Isto deve-se ao facto de o sensor fornecer recursos que podem ser acedidos pelos clientes, quer seja para ler ou alterar o estado do sensor. Como os sensores CoAP são servidores, eles podem receber pacotes de entrada.

Embora o CoAP não exija o IPv6, é mais fácil de implementar em ambientes IP, onde os dispositivos são diretamente rastreáveis. [13]

HTTP / REST (Hypertext Transfer Protocol / Representational State Transfer)

É um protocolo de comunicação massificado pela utilização em transferência de páginas HTML.

Para que a transferência de dados seja realizada, o protocolo HTTP necessita estar agregado a outros dois protocolos de rede: TCP (Transmission Control Protocol) e IP (Internet Protocol).

Embora não possa ser considerado um protocolo IoT, devido às suas necessidades de computação e de largura de banda, mesmo assim verifica-se que existem muitos projetos IoT desenvolvidos com recurso ao protocolo HTTP, principalmente devido à grande quantidade de programadores que trabalham atualmente com o mesmo no desenvolvimento de solução Web.

O REST, considerado um conceito e não um protocolo, é atualmente a principal base de comunicação com a maior parte das APIs existentes na Internet.

As APIs RESTful estão massificadas nas soluções Web modernas e a transferência de dados é efetuada através de JSON ou XML. É um conceito stateless, ou seja, os clientes conectam-se e consomem dados a pedido, transmitindo todos os dados no momento, sem que seja mantida uma ligação aberta.

Os aplicativos que são RESTful são aqueles cujas APIs seguem um conjunto universal de requisitos de arquitetura, de modo a que várias linguagens de programação se possam interligar facilmente, através de uma abordagem unificada.

As APIs REST trabalham via HTTP para executar ações, como por exemplo, POST, GET, PUT e DELETE. Estas ações podem ser mapeadas para as funções SQL CREATE, SELECT, UPDATE e DELETE (conhecido como CRUD).

O REST desempenha um papel crucial e tornou-se um “protocolo” normalizado, interpretado por quase todos os terminais e servidores Web.

Considerada uma forma quase universal de comunicação entre dispositivos e aplicações alojadas na Internet (via serviços RESTful), as APIs REST são consistentes e apresentam uma forma simples e padrão para ligar equipamentos, e processar/armazenar dados. Desempenho, Escalabilidade, Simplicidade, Modificabilidade, Visibilidade, Portabilidade e Fiabilidade são as principais características e mais-valias deste conceito.

Uma vez que trabalha sobre HTTP, qualquer dispositivo que se possa ligar à web e fazer pedidos através de uma página Web, pode usar uma API REST.

Neste contexto, não fossem as elevadas necessidades de recursos computacionais e de rede, o REST poderia ser considerado um bom modelo para IoT, uma vez que cada dispositivo pode facilmente disponibilizar as suas informações de estado e padronizar a maneira de criar, ler, atualizar e excluir registos.

Os programadores podem criar rapidamente um modelo REST para muitos dispositivos IoT. Podem por exemplo, obter facilmente o estado de uma lâmpada: se ela está desligada, então podemos enviar um pedido a ligar.

Tornar mais fácil desenvolver soluções informáticas sem ter de conhecer os dispositivos e as suas complexidades ou protocolos tornará a IoT mais acessível aos programadores.

As APIs resolvem esse desafio abstraindo as especificações do objeto e expondo-o como se fosse uma interface, permitindo programar dispositivos da mesma forma que trabalham com sistemas de back-end existentes ao criar aplicativos móveis.

Neste conceito, para um programador de software, acender uma lâmpada é exatamente igual a adicionar dados num outro tipo de sistema.

A camada da API é utilizada pela arquitetura de IoT para garantir a ligação aos servidores Web, fornecendo a consistência, o controlo, a orientação e a segurança necessários. [14]

RESUMO

Os protocolos MQTT e CoAP são dois protocolos desenvolvidos e otimizados para ambientes IoT.

O protocolo HTTP, embora não se possa considerar adequado a projetos IoT, é muito utilizado nesta área, principalmente devido à sua simplicidade e à grande quantidade de programadores que possuem conhecimentos de desenvolvimento nesta tecnologia (REST é considerado um conceito e não um protocolo).

O MQTT é um protocolo de comunicação muitos-para-muitos utilizado essencialmente para transmitir mensagens entre vários clientes através de um intermediário central (broker). Os clientes publicam mensagens e o servidor decide para onde os deve encaminhar, mediante a utilização de rotas.

O CoAP é, principalmente, um protocolo um-para-um criado para transferir informações entre um cliente e um servidor. Embora tenha capacidade para a

observação de recursos, o CoAP é mais adequado para um modelo de transferência de estados e não para comunicações baseadas em eventos. [13]

HTTP é um protocolo que necessita estar agregado a outros dois protocolos de rede: TCP (Transmission Control Protocol) e IP (Internet Protocol).

As APIs REST trabalham via HTTP para executar ações. Estão massificadas nas soluções Web modernas e a transferência de dados pode ser efetuada através de JSON ou XML.

REST é um conceito stateless, ou seja, os clientes ligam-se e consomem dados a pedido através da API, transmitindo dados sem que seja necessária uma conexão aberta. [14]

3 – PLATAFORMA PARA REGA INTELIGENTE

Neste capítulo é apresentado o trabalho realizado, de acordo com os objetivos estabelecidos para o projeto.

3.1 - Requisitos

Considerando que os principais desafios que se colocaram no desenvolvimento deste projeto foram a definição da arquitetura global da solução, a implementação de uma plataforma de gestão de dispositivos IoT agnóstica e o desenvolvimento de uma plataforma middleware de integração, será dado principal destaque aos requisitos destes pontos.

Requisitos da arquitetura global da solução:

O diagrama de arquitetura global foi projetado por forma a responder às especificidades de um sistema de rega inteligente. O cumprimento deste requisito é fundamental para o sucesso deste projeto.

Todos os dispositivos a instalar, sejam eles sensores ou atuadores, deverão estar autenticados na plataforma de gestão de dispositivos, sendo esta agnóstica a todos os protocolos e tecnologias de comunicação.

O objetivo é que dispositivos de vários fornecedores e tecnologias se possam autenticar centralmente de forma segura.

Relativamente às plataformas IoT, para além das funcionalidades genéricas deste tipo de produtos, as mesmas deverão ter capacidade de comunicar com a camada de integração (Node-RED). O objetivo é tornar possível a integração de dados de vários projetos e soluções (adicionando funcionalidades e inteligência).

Para que tal seja possível, um dos requisitos obrigatórios é que as soluções aplicacionais a implementar permitam comunicar via API (Application programming interface).

A escolha das tecnologias a integrar na arquitetura deste projeto deverá ter em conta o requisito de comunicação com qualquer equipamento IoT, sem olhar ao protocolo de comunicação (MQTT, COAP, HTTP, etc.) ou à tecnologia de comunicação (NB-IoT, LoRa/LoRaWan, 802.15.4 (6LowPAN), 3G/4G, WiFi, Ethernet, etc).

Requisitos da plataforma de gestão de dispositivos:

O requisito principal desta camada é que esta seja responsável pelo registo e autenticação de todos os dispositivos numa plataforma central.

Deste modo o principal requisito é que a mesma seja capaz de integrar todos os dispositivos, sejam eles sensores ou atuadores, todas as plataformas IoT e todos os protocolos e tecnologias de comunicação.

Esta camada deverá:

- Ser agnóstica, não limitando acessos e funcionalidades, independentemente do fornecedor ou de questões tecnológicas;
- Aprovisionar todos os dispositivos, sensores e atuadores, independentemente da sua tecnologia;
- Ter a capacidade de registar e controlar de uma forma eficiente e segura estes acessos, mediante a atribuição de um Token individual por dispositivo.
- Servir de ponte entre os dispositivos IoT e a plataforma de integração.
- Estar alojada na cloud.
- Ter capacidade disponibilizar APIs de comunicação entre plataformas. Os requisitos de comunicação da camada de aplicação deverão ser MQTT, CoAP e HTTP (REST).

Requisitos da plataforma de integração:

O requisito central desta camada passa pelo desenvolvimento de uma plataforma em Node-RED, com capacidade para integrar as diversas plataformas IoT e funcionalidades de tratamento dos dados recolhidos pelos sensores e de gestão dos atuadores.

Esta plataforma deverá ser desenvolvida em software de código aberto e sem custos de licenciamento.

Esta ferramenta deverá permitir efetuar a ponte entre os dados enviados por todos os sensores e as plataformas IoT de controlo e gestão, e comunicar através dos protocolos MQTT, CoAP e HTTP (REST).

Um dos requisitos será a capacidade de efetuar tratamento e validação de dados, nomeadamente:

- Conversões de valores
- Cálculos por aplicação de fórmulas
- Análises de intervalos de valores
- Variações de dados acima do normal
- Exclusão de valores nulos
- Limitar a frequência das comunicações dos dispositivos
- Etc.

Esta plataforma deverá permitir a realização dos backups dos dados recolhidos pelos sensores LoRa, NB-IoT e 802.15.4 para um repositório central (IBM Cloudant).

Outro dos requisitos que esta camada deverá possuir passa pela capacidade de agir diretamente sobre os atuadores instalados no terreno e de ter capacidade para contrariar as ordens dadas aos mesmos pelas plataformas de gestão.

Deverá também ter a capacidade de automaticamente recolher as previsões meteorológicas do IPMA, através da consulta realizada à API disponibilizada.

3.2 - Arquitetura global da solução

A definição da arquitetura para o sistema de rega inteligente foi realizada tendo em conta os objetivos do projeto e amadurecida à medida que foram sendo analisadas as tecnologias existentes.

Os principais módulos que foram considerados para a definição da arquitetura do sistema de rega são os seguintes:

- Rede de sensores composta por:
 - Sensores e gateways LoraWan;
 - Sensores NB-IoT;
 - Sensores e gateways 6LowPAN.

- Plataformas de gestão de dispositivos:
 - IBM Watson IoT;
 - Vodafone/Thinkdigital AEP;
 - Wavesys LoraWan Server.

- Plataformas de Integração em Node-RED:
 - Cloud Node-RED;
 - IBM Watson IoT
 - IBM CloudAnt.

- Plataformas analíticas e de gestão IoT
 - IBM Watson IoT;
 - IBM IOC;
 - IBM Cloudant;
 - Vodafone/Thinkdigital Plataforma IoT;
 - Vodafone/Thinkdigital AEP (Coletores e APIs);
 - Vodafone/Thinkdigital GTC (SCADA).

O diagrama abaixo (figura 23) representa de uma forma global, quais os principais módulos envolvidos no processo de recolha e tratamento de dados e o respetivo sentido do fluxo de dados.

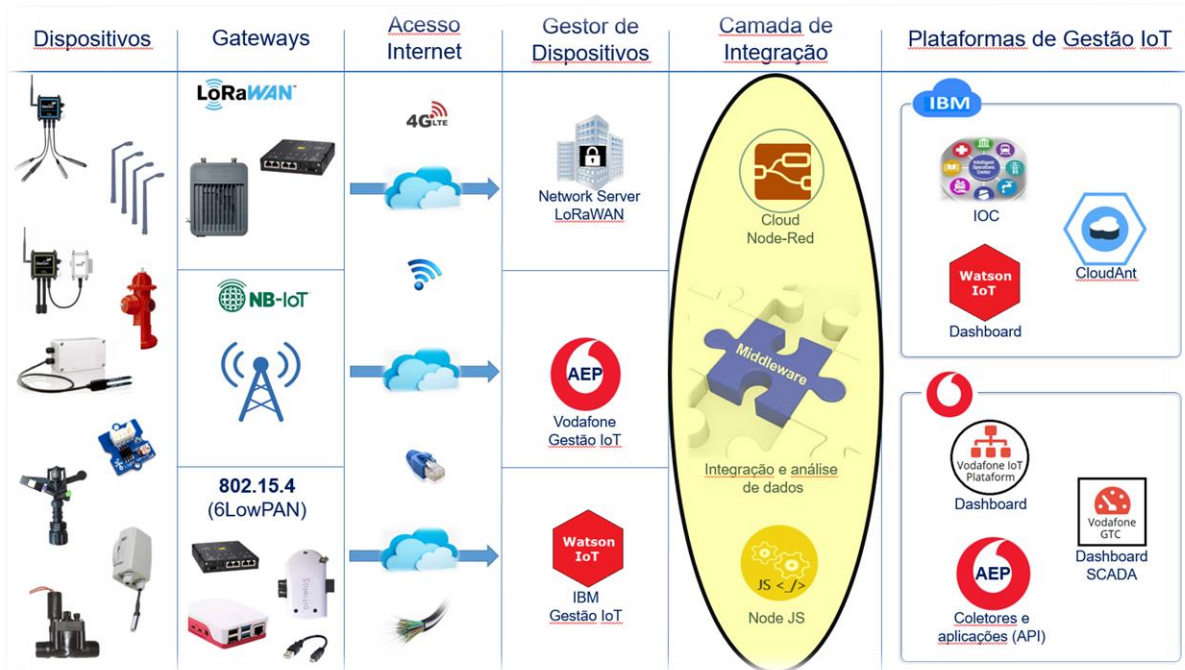


Figura 21 - Ilustração representativa da arquitetura de comunicação com os sensores

Na componente física, representada na figura 23 nas colunas “Dispositivos” e “Gateways”, encontram-se representados os sensores e as tecnologias das respetivas redes de sensores.

Na camada aplicacional foram representados os protocolos de comunicação IoT, as plataformas de gestão IoT, as soluções utilizadas na camada de integração e as plataformas de análise e analítica (com especial destaque para a camada de integração desenvolvida em Node.js e Node-RED).

O objetivo principal de um sistema de rega inteligente é ser mais eficiente do que o sistema tradicional. Para tal, o requisito principal é evitar o desperdício de água.

Através de rotinas e algoritmos que analisam as diversas variáveis ambientais (temperatura, humidade, previsões meteorológicas etc.), podemos evitar regar quando está demasiado calor, quando está a chover ou quando vai chover, e até regar tempos diferentes em espaços diferentes, de acordo com as percentagens de humidade do ar e do solo verificadas nos diversos locais.

No diagrama abaixo (figura 24) é feita uma representação, de uma forma global, de quais os principais módulos envolvidos no processo de atuação e qual o respetivo sentido do fluxo de dados.

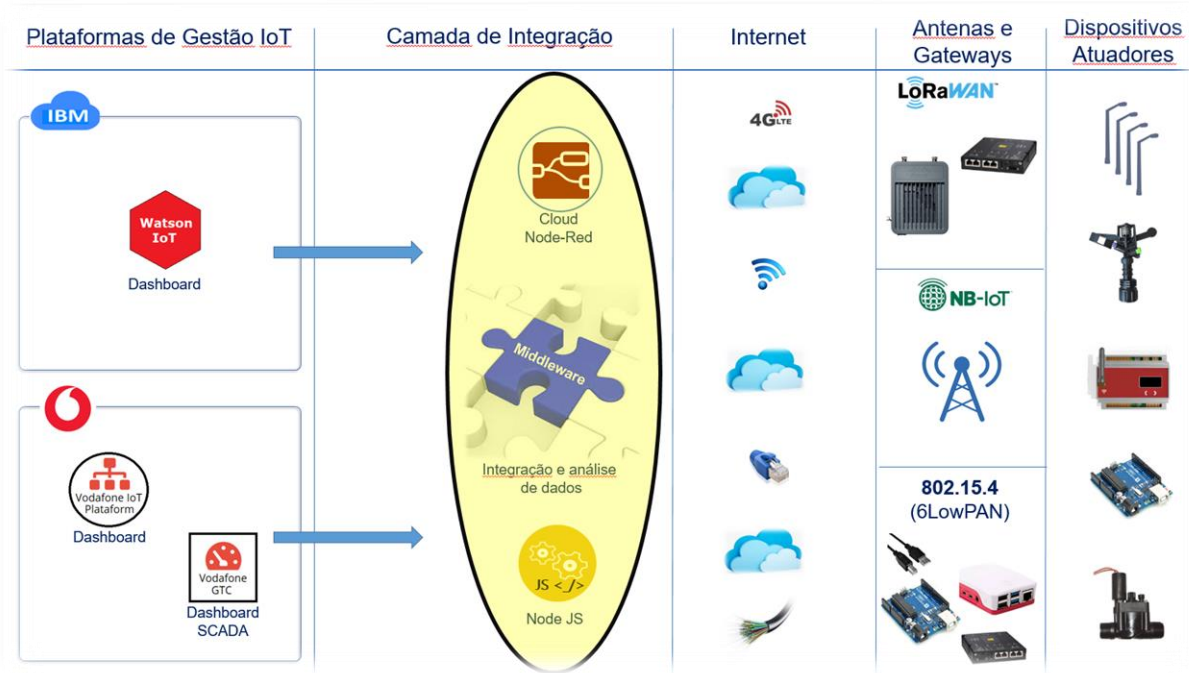


Figura 22 - Ilustração representativa da arquitetura de comunicação com os atuadores

Na componente física, representada na figura 24 nas colunas “Dispositivos” e “Gateways”, foram representados os atuadores e as tecnologias das respectivas redes de sensores.

Na camada aplicacional foram representados os protocolos de comunicação IoT, as plataformas de gestão IoT, as soluções utilizadas na camada de integração e as plataformas de dashboard e SCADA (com especial destaque para a camada de integração desenvolvida em Node.js e Node-RED).

Desde as redes de comunicação, aos sensores, aos atuadores, às plataformas de middleware, e às plataformas de armazenamento e tratamento de dados, todas as abordagens, foram sempre efetuadas no contexto IoT e enquadradas no âmbito da temática das *Smart Cities*, tendo como principal requisito a compatibilidade e capacidade de integração entre todos os módulos.

3.3 - Redes de sensores – Dispositivos e gateways

No âmbito deste projeto foram instalados e testados dispositivos 6LowPAN, NB-IoT e LoRaWAN.

Dispositivos 802.15.4 6LowPAN (sensores e atuadores)

Nos trabalhos realizados com esta tecnologia foi montado um cenário onde foram utilizados 6 dispositivos Zolertia (temperatura do ar, humidade do ar e luminosidade), 2 Raspberry PI (Contiki, Node-JS e Node-RED), 1 Arduino Uno, 1 Eletroválvula e 1 Relé.

Foi criada uma rede 6LowPAN IPv6 de 5 sensores Zolertia utilizando o protocolo de encaminhamento RPL sobre UDP.

Neste cenário os dados ambientais recolhidos são enviados para o nó border router (Zolertia). Este, por sua vez, através de um túnel USB (tunslip6 script) transfere os dados recolhidos para o Raspberry PI, que processa a informação e a encaminha, através do protocolo IPv4, para a plataforma de gestão de dispositivos (Watson IoT).

Nesta rotina, desenvolvida em Node.js, em tempo real, é efetuado o parse ao JSON capturado, e os valores dos sensores são separados pelos MACs dos respetivos dispositivos Zolertias. De seguida, através da ligação MQTT, os dados tratados são enviados via API para o IBM Watson IoT.

O Watson foi a ferramenta escolhida para efetuar o registo dos sensores e obter o respetivo TOKEN, uma vez que reunia os requisitos técnicos e funcionais que se procuravam. Nesta decisão também pesou o facto de o Município de Tomar estar a planear implementar um projeto de eficiência energética com esta solução e de ficar responsável pela gestão da solução.

De seguida, através do Node-RED cloud, os dados são analisados, tratados e encaminhados para o IBM Cloudant (para feed de backup) e para as plataformas IoT.

Por sua vez, no sentido inverso, no que diz respeito aos atuadores (comando de electroválvulas), foram utilizados um RaspBerry Pi e um Arduino.

O sistema operativo utilizado no RaspeBerry foi o Debian e o firmware carregado no Arduino foi o *StandardFirmdata* (carregado através do IDE Arduino).

No Rasperry Pi foi instalado o Node-RED e foi criado um fluxo que ciclicamente faz consultas à plataforma de IoT, com o objetivo de saber se tem ordem para regar.

A verificar-se essa confirmação, o Node-RED dá ordem ao Arduino para passar energia para o pin onde está ligado a relé.

Ao receber este impulso, a relé ativa o circuito principal dos 9V que faz atuar a electroválvula (abrir ou fechar o circuito de rega).

A ligação entre o RaspBerry e o Arduino foi realizado por USB. Já a comunicação entre o Arduino e a relé que ativa a electroválvula foi efetuada através da ligação a um pino digital de saída.

Neste último foi ligado um relé de 2 circuitos, que através da entrada de 5V provenientes do Arduino, ativa ou inativa o circuito elétrico de 9V de uma electroválvula de 1 ½" (conforme figura 25).

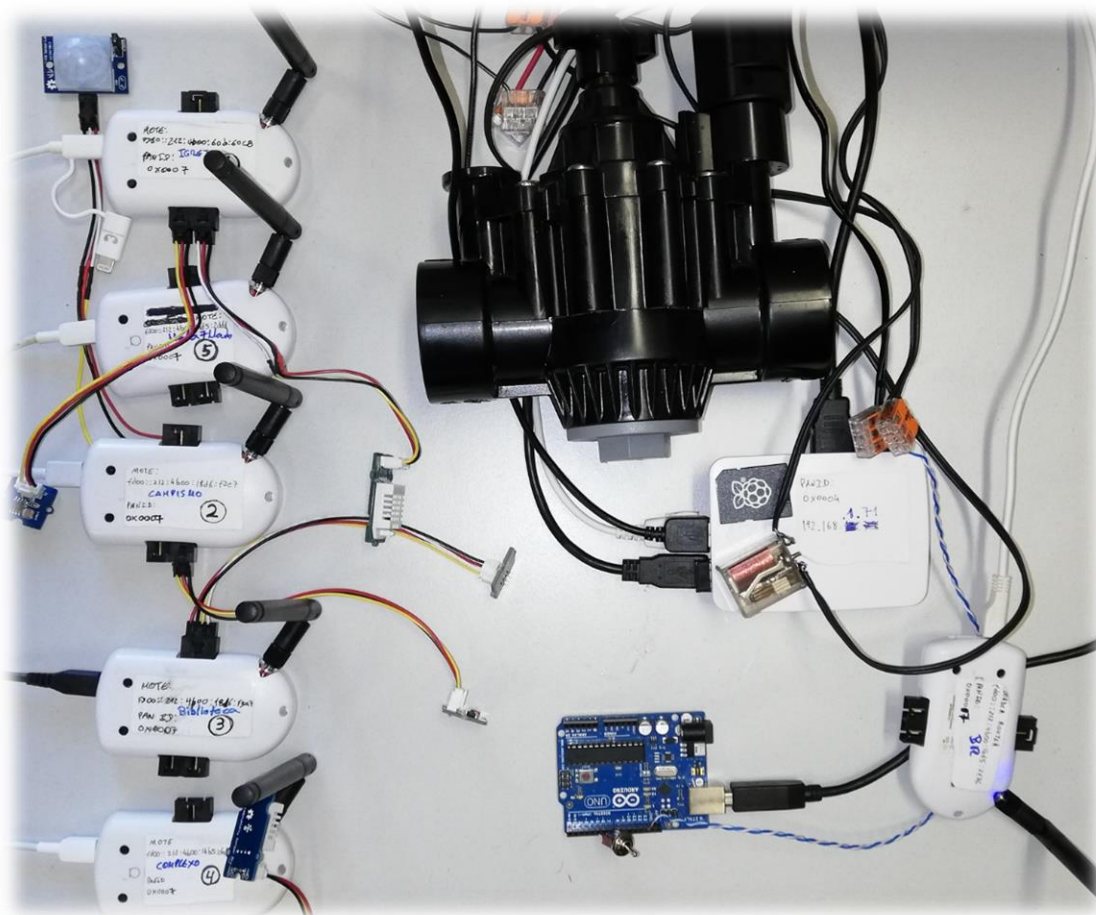


Figura 23 – Cenário montado para testar comunicação com electroválvula

Dispositivos LoRaWan (sensores)

Nos trabalhos realizados com esta tecnologia foram utilizados sensores de medição LoRa (temperatura, humidade e luminosidade), um gateway LoRa e um LoRaWan Server alojado na cloud.

Nesta componente do projeto foram realizados trabalhos em duas vertentes:

- O primeiro projeto focou-se na definição da arquitetura e no início da instalação dos gateways LoRa, de modo a garantir a cobertura da totalidade do território do concelho.

Os equipamentos utilizados para o survey e para os testes foram fornecidos pela IBM, no âmbito de um projeto de eficiência energética em implementação para Tomar (figura 26).



Figura 24 - Equipamentos LoRa utilizados no survey realizado no concelho de Tomar

O Município está a substituir todas as luminárias tradicionais da via pública por luminárias led, com capacidade para controlar centralmente a intensidade da iluminação individualmente por cada luminária.

Para comunicar com os atuadores existentes nas luminárias está a ser instalada uma rede LoRaWAN. O objetivo desta rede é servir não só este projeto mas também projetos futuros que possam vir a necessitar de conectividade LPWAN.

Ao responsável pelas tecnologias de informação do município de Tomar, nomeado gestor deste projeto, cabe a função de planear, acompanhar e fiscalizar

o desenvolvimento e a implementação do mesmo, participando ativamente na realização do survey que serviu de base para a definição dos locais ideais para instalação das antenas (gateways).

Nesta fase, a rede LoRaWAN vai servir para conectar os sensores de todas as luminárias da rede pública de iluminação, um sensor que mede o nível da água do rio Nabão, um sensor que controla a utilização da água de uma boca de incêndio e um sensor que mede a qualidade do ar.

Embora o município fique como responsável pela gestão da solução, a empresa fornecedora dos equipamentos fica obrigada contratualmente a substituir qualquer equipamento avariado durante os próximos 16 anos.

- A segunda vertente deste projeto, em que foram realizados trabalhos com tecnologia LoRa, passou pela utilização de 2 sensores (temperatura e humidade), 1 gateway e 1 LoRaWAN Server alojado na cloud, com um registo de domínio provisório.

Para além de questões físicas, como o alcance, a largura de banda, etc., este projeto piloto também serviu para perceber como se aprovisionam dispositivos no servidor LoRaWAN. Este procedimento consiste em adicionar, o mac address na lista de equipamentos que se podem registar na rede LoRa. A partir desse momento o dispositivo passa a estar disponível para utilização.

Para que os dados recolhidos nesta rede pudessem ser encaminhados para a plataforma de integração, foi disponibilizada na plataforma IoT da Wavecom o envio de dados via API. Através desta é possível enviar dados para a plataforma de gestão de dispositivos (Watson IoT).

Por sua vez, a plataforma de integração (Node-RED), automaticamente, trata e envia os dados recebidos para a plataforma de backup (Cloudant) e para as plataformas IoT desejadas.

Relativamente à comunicação com atuadores LoRa, não foram efetuados quaisquer testes.

Dispositivos NB-IoT (sensores e atuadores)

Nos trabalhos realizados com esta tecnologia foram utilizados 6 sensores NB-IoT (2 de temperatura do ar, 2 de humidade do ar e de humidade solo) e 2 controladoras GPRS de 254 canais (2 x 254 circuitos para electroválvulas).

Os sensores foram fornecidos pela Vodafone e ativação dos serviços nas antenas de telecomunicações móveis demorou cerca de três meses. Na figura 27 estão representadas as antenas de telecomunicações do concelho de Tomar onde já está ativo o serviço do protocolo NB-IoT.

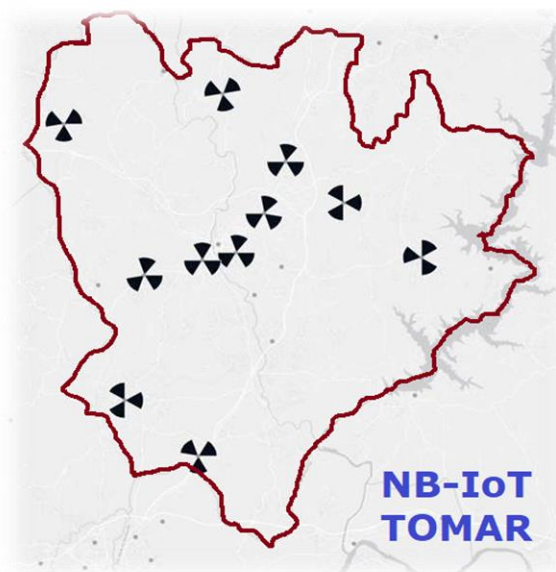


Figura 25 - Localização das antenas NB-IoT atualmente ativas no concelho de Tomar

Os sensores IoT fornecidos foram instalados dentro de caixas estanques, com as sondas de medição derivadas para o exterior das mesmas, conforme representado na figura 26. De seguida foram enterrados em localizações definidas tendo em conta as questões geográficas e morfológicas do terreno.



Figura 26 - Sensor NB-IoT instalado em caixa estanque

As controladoras IoT fornecidas, foram instaladas em quadros elétricos exteriores e fixadas nos barramentos dos disjuntores, tendo as cablagens de controlo das electroválvulas sido passadas até às caixas de chão onde foram efetuadas as derivações dos circuitos de rega e onde as mesmas foram instaladas.

Conforme podemos verificar na figura 27, estes equipamentos assemelham-se fisicamente a disjuntores trifásicos, fixados em calha DIN, e foram desenvolvidos pela empresa Thinkdigital para uma utilização profissional.

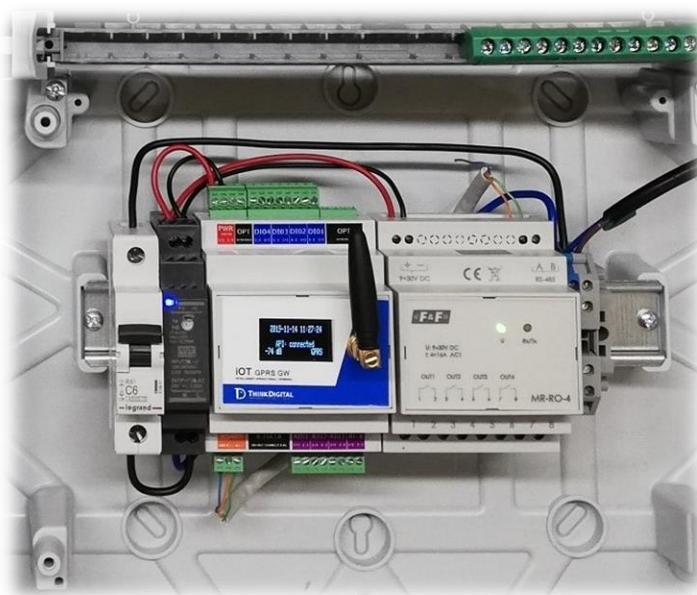


Figura 27 - Atuador GPRS Modbus de 254 canais

Uma vez que esta tecnologia utiliza as infraestruturas de comunicação das operadoras de comunicações móveis, não foi necessário proceder à instalação de equipamentos gateway.

Nos equipamentos fornecidos pela Vodafone, tanto os sensores como os atuadores possuem um cartão de comunicações semelhante ao de um telemóvel e são autenticados na rede através do IMEI e do MAC Address. Os sensores possuem um router NB-IoT e os atuadores comunicam por GPRS.

A transmissão de dados entre dispositivos Narrowband é efetuada, na camada de transporte, através do protocolo UDP. Já na camada de aplicação, a informação é transferida entre aplicações através do protocolo de comunicação CoAP.

Nesta tecnologia, a arquitetura de comunicações utilizada na camada de aplicação foi muito semelhante à efetuada nos trabalhos realizados com a tecnologia LoRa.

Os dados recolhidos dos sensores são diretamente enviados para a plataforma de gestão de dispositivos da Vodafone (AEP IoT Vodafone).

De seguida, através da camada de integração (middleware desenvolvido em Node-RED) os dados são automaticamente tratados e encaminhados para a Cloudant da IBM (para backup) as para as plataformas IoT para gestão.

3.4 - Plataforma de gestão de dispositivos

Esta camada é responsável pelo registo e autenticação de todos os dispositivos e pela disponibilização das APIs necessárias para receção e envio dos dados recolhidos por todos os sensores e pelos atuadores.

O objetivo é centralizar a gestão de todos os dispositivos numa só plataforma, gerida pelo Município. Para tal foram escolhidas as plataformas IBM Watson IoT, o Vodafone/Thinkdigital AEP e o Wavesys LoraWan Server. Todas estas ferramentas reúnem os requisitos técnicos necessários para registo e gestão de dispositivos IoT de uma forma segura.

IBM Watson IoT (Plataforma Internet das Coisas da IBM) – A criação da instância de trabalho (recurso na cloud) que suporta esta plataforma foi realizada através da área de lista de recursos, disponibilizada na plataforma IBM CLoud.

Na figura 29 podemos ver a área do Watson IoT onde se registam os dispositivos. No status da ligação podemos confirmar que os dispositivos se encontram conectados através de MQTT.

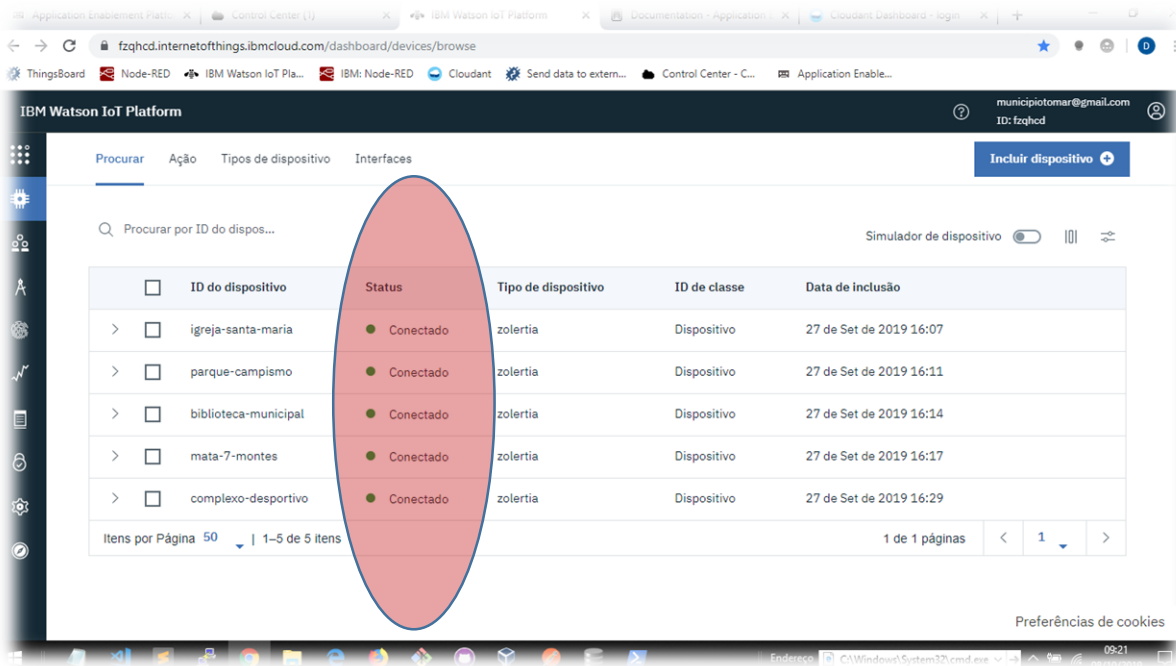


Figura 28 – Dashboard de registo e gestão de dispositivos do Watson IoT

Na figura 30 é possível ver o registo dos logs de conexão do sensor Zolertia da “igreja-santa-maria”, com referência à autenticação por Token.

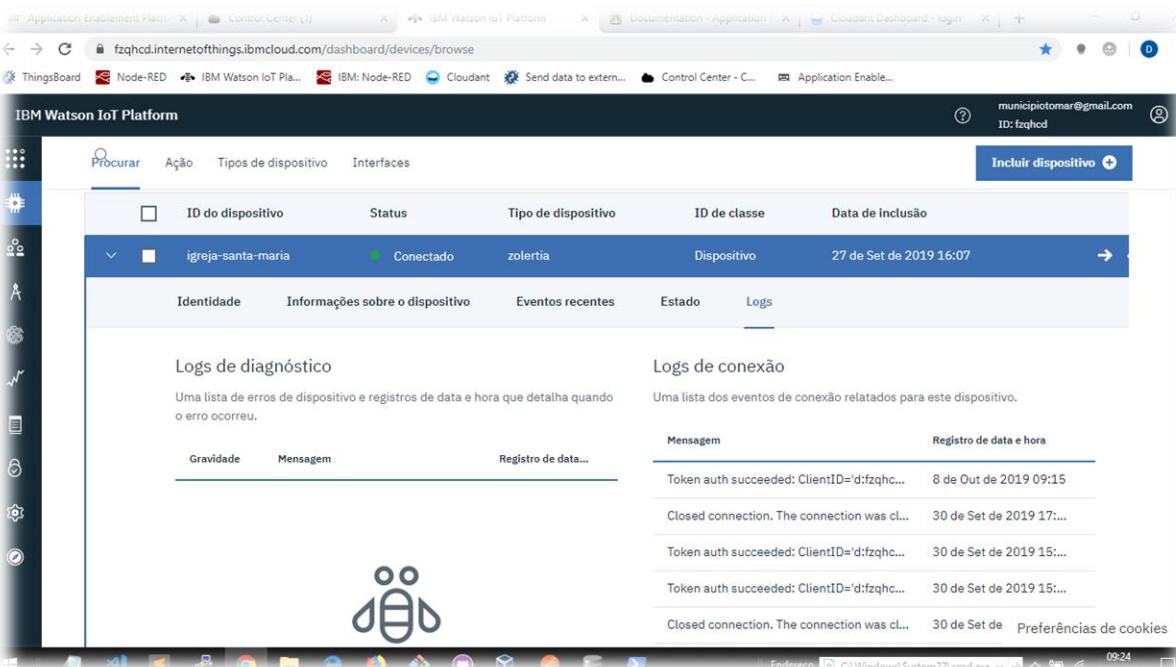


Figura 29 – Dashboard de logs de conexão do Watson IoT

Na arquitetura atual esta camada serve de ponte (para todos os sistemas que se pretendam integrar) entre os dispositivos IoT e a plataforma de integração.

Para a comunicação entre plataformas são disponibilizadas APIs (MQTT, COAP ou REST).

AEP Vodafone/Thinkdigital (Plataforma de Gestão de Dispositivos) – O acesso a esta plataforma foi disponibilizado pela Vodafone.

O primeiro passo, para podermos centralizar o aprovisionamento de sensores e atuadores nesta ferramenta, passou pela criação de uma instância de coletores. Após este passo passou a ser possível criar dispositivos e definir os seus sensores. Por último, no que diz respeito à gestão de dispositivos, foram criadas as respetivas aplicações de comunicação (APIs).

No que diz respeito às credenciais de autenticação, para adicionar dispositivos NB-IoT à plataforma AEP, é possível utilizar o IP público, o Mac Address que identifica o dispositivo e o IMEI (identidade internacional de equipamento móvel) do cartão SIM. Normalmente para dispositivos móveis são utilizados o IMEI e o MSISDN (conhecido normalmente por número de telefone).

Para dispositivos LoRa e 802.15.4, as credenciais de segurança para comunicação são geradas na plataforma e a transferência de dados é efetuada através de APIs REST, MQTT ou COAP.

Na figura 31 podemos ver a área do AEP Vodafone/Thinkdigital onde se registam os dispositivos.

Na coluna “Ligado” podemos ver a data da última comunicação do dispositivo e se a mesma respeita o intervalo de segurança definido.

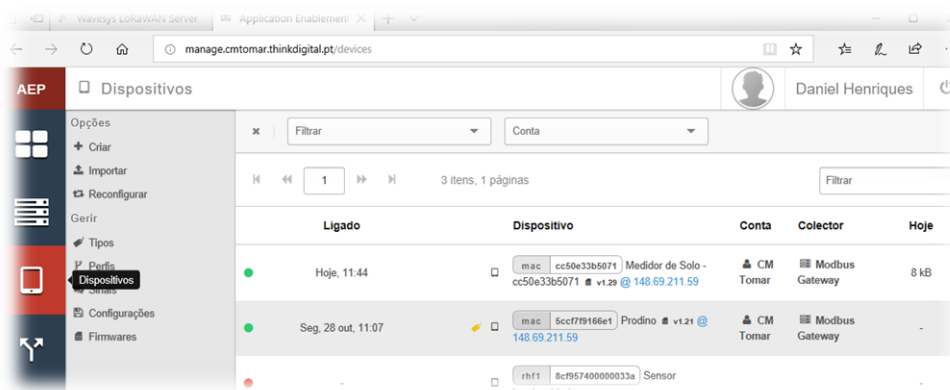


Figura 30 - Menu de aprovisionamento e gestão de dispositivos NB-IoT

Em apoio à gestão dos dispositivos, foi desenvolvido um dashboard de controlo do sistema de rega inteligente, que permite também apoiar na visualização do histórico dos dados recebidos e na localização dos dispositivos instalados no terreno, através de georreferenciação (figura 32).

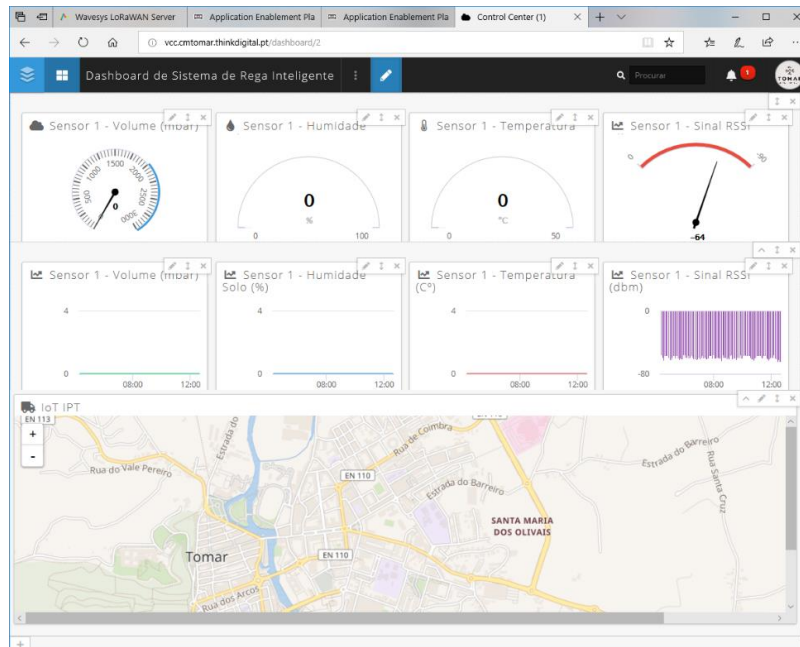


Figura 31 - Dashboard do sistema de rega inteligente

Uma vez que os dispositivos NB-IoT comunicam através do protocolo CoAP, não é possível manter uma conexão aberta. A única forma de controlar a conectividade e o funcionamento de um dispositivo é através do controlo e verificação do cumprimento do agendamento predefinido das comunicações. Por exemplo, se um determinado dispositivo está configurado para comunicar de duas em duas horas e falhar numa dessas comunicações, então poderá estar a ocorrer uma falha de conectividade.

Já no caso dos atuadores IoT, tratando-se de equipamentos GPRS, como a comunicação é bidirecional, a plataforma faz um registo calendarizado da qualidade do sinal da rede, sendo possível analisar o histórico de registos e validar a qualquer momento a conectividade dos dispositivos.

No caso da plataforma LoraWan, o aprovisionamento dos dispositivos LoRa é efetuado diretamente no equipamento de gateway Cisco.

O procedimento para adicionar um dispositivo LoRa à rede, partindo do pressuposto que o mesmo está ao alcance de do gateway LoRa, é feita através da seleção do MAC Address do dispositivo.

Já na plataforma de gestão de dispositivos Wavesys LoRaWAN Server, só após a criação da aplicação que gera a *application key* é que é possível proceder à criação de dispositivos e receber os dados recolhidos pelos mesmos.

A criação de dispositivos é efetuada mediante a introdução do nome, da descrição e do *EUI* do equipamento. Após estes passos, para poder comunicar com o sensor é necessário introduzir um *application key* (que pode ser constante ou variável) de modo a poder ativar a comunicação com o sensor.

Na figura 33 é possível observar a área do Wavesys LoRaWAN Server onde se registam os dispositivos e se criam as aplicações de acesso e comunicação.

Na coluna “Last seen” podemos ver a data da última comunicação dos dispositivos.

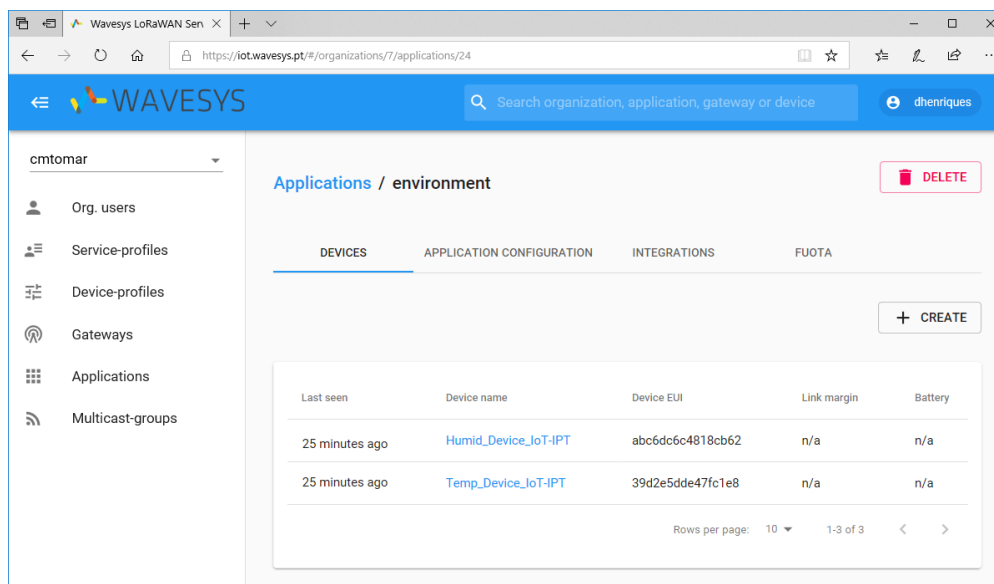


Figura 32 - Aprovisionamento e gestão de dispositivos na aplicação LoRaWAN Server

3.5 - Plataformas de integração (Node-RED)

É nesta camada que é realizada a integração entre as diversas plataformas IoT e que é efetuado o tratamento e a validação dos dados recolhidos pelos sensores.

As escolhas das soluções tecnológicas para esta camada, procuraram ferramentas open-source e com capacidade para desenvolvimento de funções, com facilidade na conexão de dispositivos de hardware e na criação de APIs de comunicação.

Após análise das várias ferramentas, a escolha recaiu sobre o Node-RED (local e na cloud).

Node-RED é uma ferramenta de desenvolvimento baseada em fluxos e nós, com uma interface que permite realizar programação com algum apoio visual.

Foi desenvolvida originalmente pela IBM para conectar dispositivos, para comunicar via APIs e para aceder a serviços online.

Apresenta um editor de fluxos que corre em ambiente Web, que tem a capacidade de criar e interpretar funções JavaScript (podendo os elementos desenvolvidos ser guardados e partilhados para outras reutilizações).

O compilador é construído “em cima” da framework do Node.js, sendo os fluxos gerados e armazenados no formato JSON.

Relativamente aos trabalhos desenvolvidos nesta plataforma, os mesmos foram iniciados ainda na fase da escolha das tecnologias para o desenvolvimento deste projeto. Foram utilizadas duas versões de Node-RED. A versão local, instalada no disco rígido e a correr sobre a framework node.js local, e a versão na nuvem, a correr na IBM Cloud.

Na camada de integração, a versão cloud foi utilizada para a comunicação e tratamento dos dados recolhidos pelos sensores. Já a versão local foi utilizada para comunicação e gestão dos atuadores, após ter-se concluído que a versão alojada na cloud não permite a comunicação com equipamentos Arduino via porta USB.

Para poder trabalhar online com o Node-RED, optou-se por utilizar a versão suportada pela cloud da IBM. Para tal foi necessário proceder previamente à criação de uma conta. De seguida foi necessário proceder à criação do *Starter Kit* que permitiu gerar os dados de acesso e autenticação. Na figura 34 podemos ver a instância de Node-RED criada na cloud da IBM.

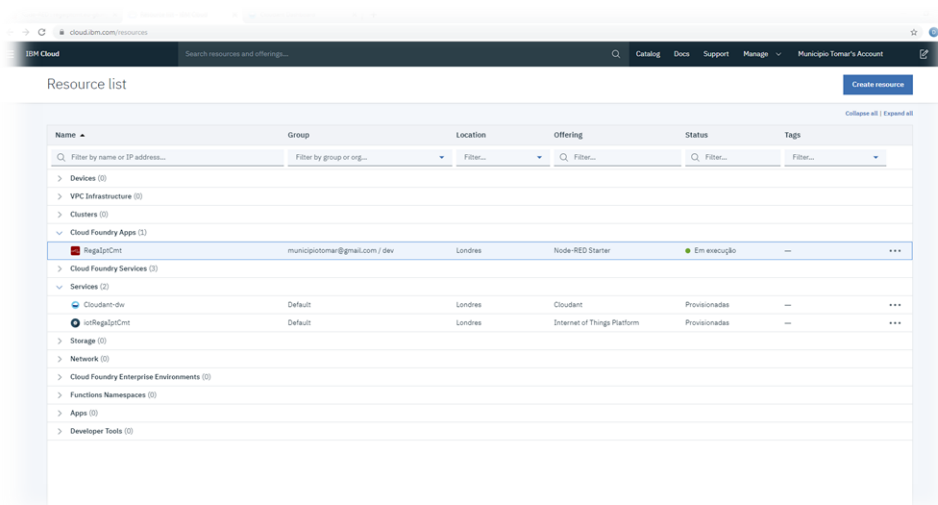


Figura 33 – Dashboard de acesso à lista de recursos disponíveis no IBM Cloud

Para tentar perceber se esta ferramenta cumpria os requisitos técnicos e funcionais necessários, foram efetuados diversos fluxos de teste, como por exemplo:

1 - Fluxo de envio de dados via REST para o EmonCMS



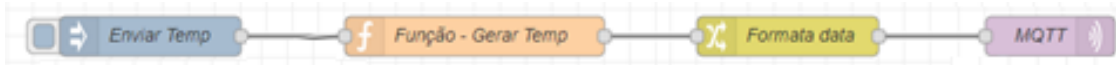
“Enviar Temp” - Nó do tipo inject, que permite iniciar a função

“Função – Enviar Temp” – Nó do tipo função em JavaScript:

```
var basic_url = "https://emoncms.org";
var apikey = "a78c34207046097575ce46e9c4ac9ad6";
var nomenode = "Portugal";
var Temperatura = Math.floor((Math.random() * (30 - 10)) + 10);
var final_url = "/input/post?node=" + nomenode +
"&data={Temperatura:" + Temperatura + "}&apikey=" + apikey;
msg.url = (basic_url + final_url);
return msg;
```

“POST – Recebe Temp” – Nó do tipo pedido HTTP

2 - Fluxo de envio de dados via MQTT para o Watson IoT



“Enviar Temp” - Nó do tipo inject, que permite iniciar a função

“Função – Gerar Temp” – Nó do tipo função em JavaScript:

```
var Temperatura = Math.floor((Math.random() * (30 - 10)) + 10);
msg.payload = Temperatura;
return msg;
```

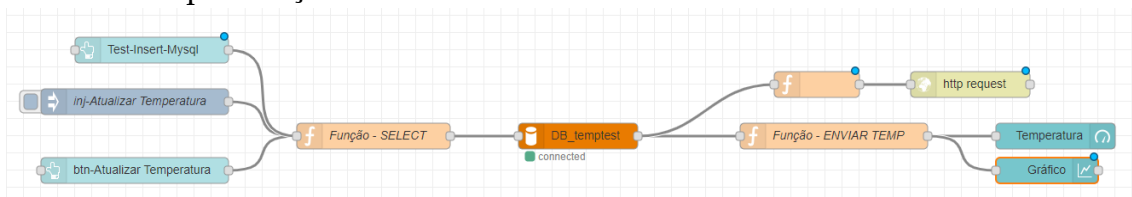
“Formata data” Nó que permite converter a mensagem em formato JSON

```
Msg.topic
iot-2/eot/Temperatura/fmt/json
```

“MQTT” – Nó de conexão ao broket de MQTT

```
Server: bq261t.messaging.internetofthings.ibmcloud.com
Client ID: d:bq261t:testDeviceType1:testDevice1
User: use-token-auth
Pass: testDevice1
```

3 - Fluxo de leitura de registos em BD MySQL e envio via REST para o EmonCMS / publicação no Node-RED Dashboard



“inj-Atualizar-Temperatura” - Nó do tipo inject, que permite iniciar a função

“Função – SELECT” – Nó do tipo função em JavaScript:

```
msg.topic = "select valor from temphistory order by id desc";
return msg;
```

“DB_temptest” – Nó do tipo conexão de leitura em DB

“Função – ENVIAR TEMP” - Nó do tipo função em JavaScript:

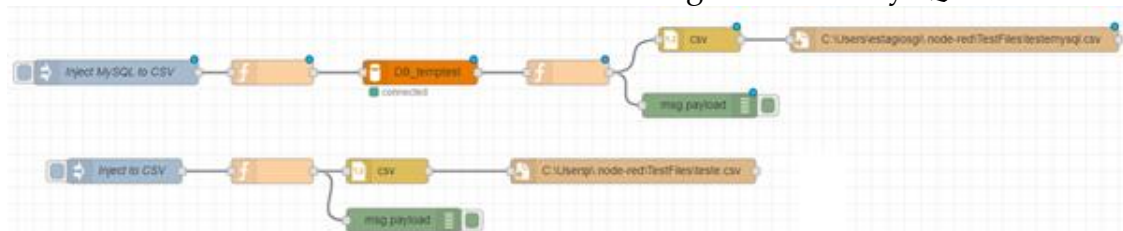
```
var str = msg.payload;
var temp = str[0]['valor'];
msg.payload = temp;
return msg;
```

“Função – sem título” - Nó do tipo função em JavaScript

```
var str = msg.payload;
var temp = str[0]['valor'];
var basic_url = "https://emoncms.org";
var apikey = "a78c34207046097575ce46e9c4ac9ad6";
var nomenode = "Portugal";
var final_url = "/input/post?node=" + nomenode + "&data={Temperatura:" +
temp + "}&apikey=" + apikey;
msg.url = (basic_url + final_url);
return msg;
```

“http request” – Nó do tipo pedido HTTP

4 - Fluxo de escrita em ficheiro CSV de 1 registo de BD MySQL



“inject MySQL to CSV / inject to CSV” - Nó do tipo inject que permite iniciar a função

“Função – sem título 1” – Nó do tipo função em JavaScript:

```
msg.topic = "select valor from temphistory order by id desc";
return msg;
```

“DB_temptest” – Nó do tipo conexão de leitura em DB

“Função – sem título 2” – Nó do tipo função em JavaScript:

```
var str = msg.payload;
var time = str[0]['timestamp'];
var idOrg = str[0]['idOrg'];
var idLocal = str[0]['idLocal'];
var idDisp = str[0]['idDisp'];
var unid = str[0]['unid'];
var temp = str[0]['valor'];
var all = [time, idOrg, idLocal, idDisp, unid, temp];
msg.payload = all;
return msg;
```

“csv” – Nó de conversão de dados em CSV

Foram ainda realizados outros fluxos de testes, nomeadamente:

- Pesquisar dados num CSV por coordenadas;
- Escrever dados num CSV;
- Chamar e executar rotinas e ficheiros remotamente no servidor;
- Pesquisar registos numa BD de MySQL;
- Escrever e ler registos do Watson IoT;
- Escrever e ler registos do IBM Cloudant Bluemix;
- Enviar instruções para um Arduino Uno;

Estes desenvolvimentos também serviram para compreender melhor o funcionamento da ferramenta Node-RED e quais as suas potencialidades.

Após a análise aos testes realizados, concluiu-se que esta seria a plataforma ideal para desenvolvimento da camada de integração.

Desenvolvimento e implementação da camada de integração - O primeiro fluxo desenvolvido (conforme imagem 35), permitiu capturar os dados dos dispositivos autenticados no Watson IoT (camada de gestão de dispositivos) e proceder ao respetivo encaminhamento para o IBM Cloudant.

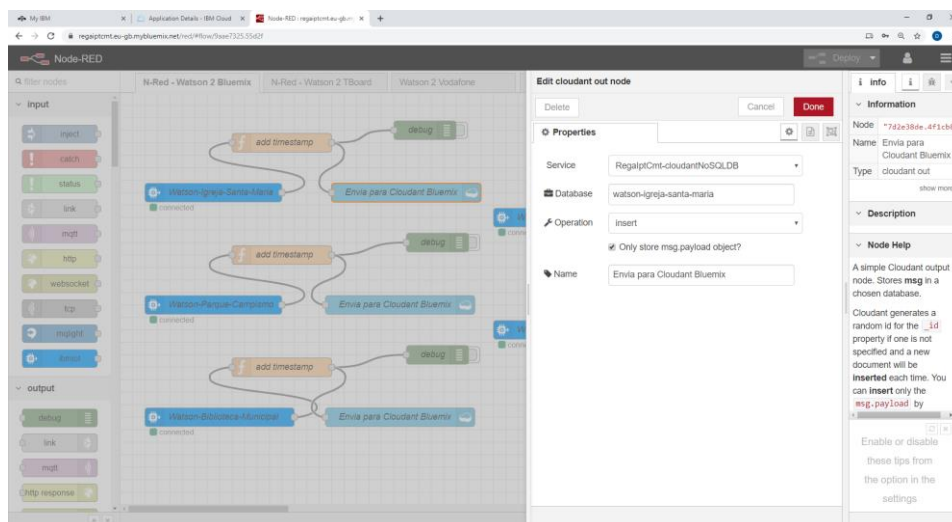


Figura 34 – Fluxo desenvolvido para envio de dados do Watson IoT para o Cloudant

Antes de adicionar e configurar os nós de conexão, foi necessário proceder à configuração do Watson e do Cloudant da IBM.

Enquanto que no IBM Watson IoT foi necessário criar a instância e os dispositivos individualmente, no IBM Cloudant as bases de dados de armazenamento dos dados

recolhidos e tratados pelo Node-RED são criadas em tempo real, no momento em que são enviadas.

Relativamente aos desenvolvimentos efetuados no Node-RED, foi adicionado e configurado um nó *ibmiot* por cada dispositivo autenticado no Watson e procedeu-se à configuração da respetiva API MQTT.

De seguida foi adicionado um nó de função, onde foi desenvolvido o código necessário para adicionar um *timestamp* ao *payload* recebido pelo nó *ibmiot*.

Para concluir foi incluído um nó *Cloudant Out*. Através deste nó foi realizado o envio dos dados tratados para uma base dados de backup (IBM Cloudant).

Após o desenvolvimento deste fluxo, todos os dados enviados pelos dispositivos para a plataforma de gestão de dispositivos passaram a ser encaminhados automaticamente para a plataforma de backups (IBM Cloudant).

De seguida, procedeu-se ao desenvolvimento de um fluxo que efetuasse o tratamento de dados, nomeadamente, validações, conversões, cálculos, ou outro tipo de operações (intervalos de valores, valores nulos, valores enviados com frequências demasiado elevadas, etc.).

Na figura 35 conseguimos ver o fluxo que analisa valores aleatórios enviados para o sensor “Watson-Igreja-Santa-Maria”.

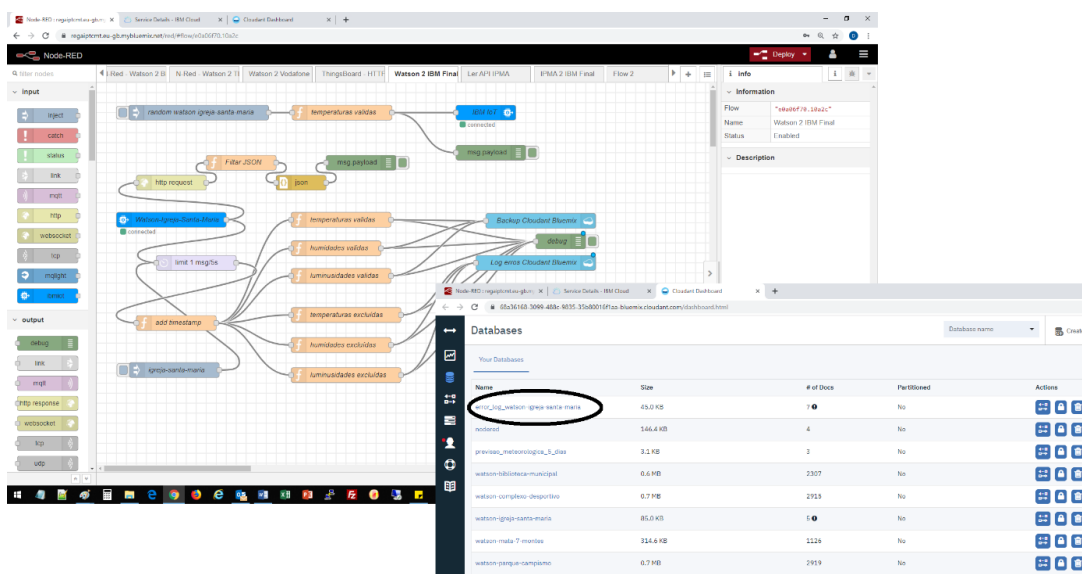


Figura 35 – Fluxo de tratamento e validação de dados da camada de middleware

Os valores das temperaturas, humidades e luminosidades, que são validados são enviados para a plataforma de backup e os valores que são excluídos, por não cumprirem alguma das regras de validação, são enviados para uma base de dados *error_log_watson-igreja-santa-maria*, criada para fazer o log dos registos excluídos

A figura 36 mostra o fluxo desenvolvido em Node-RED e a base de dados do IBM Cloudant onde é efetuado o backup dos valores excluídos.

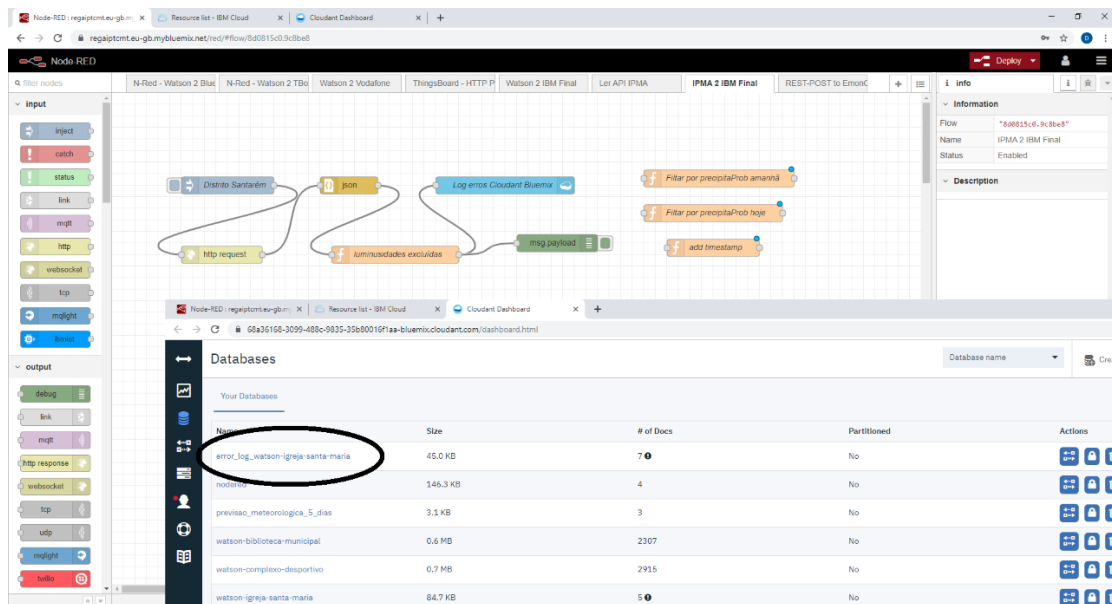


Figura 36 – Fluxo que realiza o log dos valores excluídos pelas regras de validação

É também na camada de gestão de dispositivos que é efetuada a cópia automática dos dados recolhidos pelos dispositivos registados na camada de gestão de dispositivos, fazendo validações, tratamento e envio automático para a plataforma de backups (IBM Cloudant).

Para feed dos registos de backup pretende-se utilizar o IBM Cloudant e testar as respetivas funcionalidades disponíveis.

Para evitar regar nos períodos de tempo que antecedem as chuvas, reduzindo os desperdícios de água, desenvolveu-se também um fluxo que permite ler as previsões meteorológicas disponibilizadas pelo IPMA, mediante a utilização de uma API REST, e que as envia para o IBM Cloudant, para consulta por parte dos atuadores (figura 38).

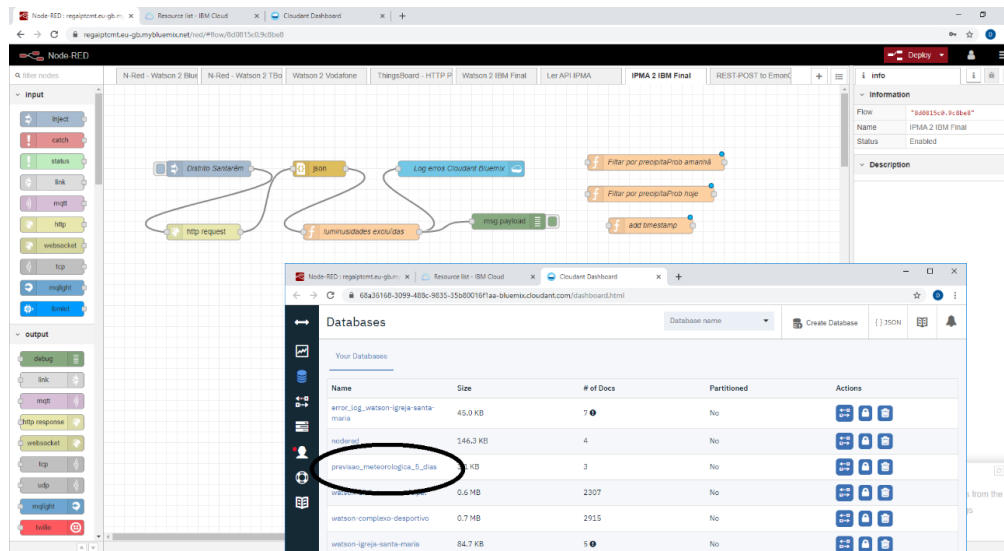


Figura 37 - Fluxo que trata as previsões meteorológicas da API do IPMA

Nos pedidos efetuados à API são passados parâmetros de localização e de intervalos de tempo. Desta forma são filtrados os valores das previsões meteorológicas regionais do presente dia e dos próximos 4 dias.

Estes valores são armazenados no Cloudant, na base de dados “previsão_meteorologica_5_dias”, estando depois à disposição de serem utilizados pelos atuadores, no condicionamento das ordens de rega.

Esses dados, em conjunto com as instruções dadas pelas plataformas IoT, são analisados pelos atuadores, de acordo com os agendamentos predefinidos e de acordo com as ordens de atuação recebidas.

Para operacionalizar este cenário foi desenvolvido um fluxo que avalia todas as variáveis existentes e decide qual a ação a executar.

Conforme figura 39, este fluxo foi desenvolvido com recurso aos seguintes nós:

- *Cloudant in* - que realiza consultas às bases de dados do IBM Cloudant;
- *Delay* - que limita o intervalo de leitura da base de dados;
- *Função* - que analisa as instruções dadas pela plataforma IoT;
- *Http request* – que efetua a consulta à API do IPMA e analisa as previsões meteorológicas armazenadas na base de dados “previsão_meteorologica_5_dias”;
- *JSON* – que converte o formato dos dados recebidos;
- *Função* – que analisa os dados recebidos e dá as ordens de atuação”
- *Arduino out* - palette adicionada que comunica com a camada de hardware e que transmite ao Arduino informação de quais os circuitos a ativar.

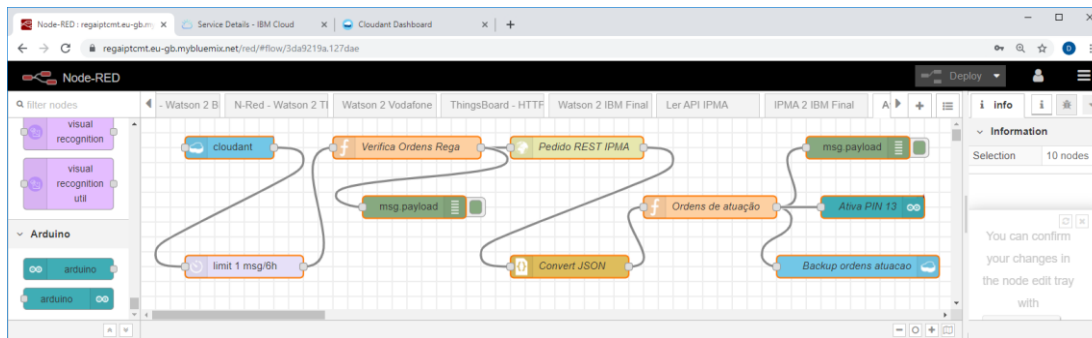


Figura 38 – Fluxo de validação e atuação com Arduino

Esta camada poderá contrariar ordens ou instruções dadas pelas plataformas de gestão e controlo IoT.

Por exemplo, de acordo com um determinado agendamento, pode ser dada ordem de rega para um atuador de uma electroválvula. No entanto, considerando que esta camada se encontra entre o dispositivo e a plataforma IoT e que esta tem capacidade de interferir nessas decisões, as validações desenvolvidas nas rotinas dos fluxos Node-RED poderão anular ou alterar essas ordens.

Questões como as previsões meteorológicas, avarias, manutenção de espaços ou realização de eventos em espaços públicos, são alguns desses exemplos.

A impossibilidade de criar múltiplos dashboards e múltiplos perfis de utilizador, foram as principais limitações encontradas nesta ferramenta (eventualmente motivados pelo facto de estar a ser utilizada a versão de testes e de avaliação). Também o facto de não ter sido viável comunicar por usb com um Arduino na versão cloud do Node-RED, criou algumas dificuldades, obrigado à instalação da versão local num Raspberry Pi.

4 – RESULTADOS EXPERIMENTAIS

Neste capítulo apresenta-se os resultados experimentais dos trabalhos realizados e das tecnologias adotadas no projeto, nomeadamente o cenário e instalação de sistemas, os testes de validação, os resultados dos testes de validação e a discussão de resultados.

Para além de permitirem validar a arquitetura e as opções tecnológicas efetuadas para este projeto, os resultados encontrados também servirão de suporte a futuras escolhas tecnológicas.

4.1 – Cenário e instalação de sistemas

O cenário montado para este projeto teve como principal preocupação a escolha e implementação de dispositivos e plataformas compatíveis com as diversas tecnologias e protocolos de comunicação IoT, que melhor se enquadrassem no âmbito de um projeto de rega inteligente.

O local escolhido para execução do projeto foi o Complexo Desportivo Municipal de Tomar. Este espaço possuía um sistema de rega obsoleto e desativado há já alguns anos e foi eleito por reunir as condições ideais para a execução deste projeto piloto.

Os trabalhos iniciaram-se com o estudo e a análise das soluções tecnológicas que melhor se enquadravam nos objetivos do projeto, quer na componente física como aplicacional.

Concluída esta fase iniciaram-se os trabalhos de desenvolvimento e implementação da solução de rega inteligente. Paralelamente, em colaboração com os serviços do município, procedeu-se à elaboração do projeto de rega e à instalação das respetivas infraestruturas necessárias (tubagens, cablagens, electroválvulas, aspersores, etc.)

A primeira etapa da componente IoT do projeto passou pela criação das redes de sensores e atuadores, compostas por dispositivos LoraWan, NB-IoT e 6LowPAN.

Seguiu-se a fase do estudo, configuração e desenvolvimento das plataformas de gestão de dispositivos, nomeadamente o IBM Watson IoT, o Vodafone/Thinkdigital AEP e Wavesys LoraWan Server.

Através desta camada passou a ser possível autenticar dispositivos e utilizar os dados recolhidos pelos mesmos.

A fase seguinte passou pelo desenvolvimento da camada de middleware de integração (Cloud Node-RED, IBM Watson IoT e IBM CloudAnt). Esta camada está no core deste projeto, acumulando as funções de controlo e integração dos vários sistemas do projeto.

Após o desenvolvimento deste middleware (camada de integração), passou a ser possível recolher e tratar os dados dos sensores autenticados no Watson IoT, no Wavesys LoraWan Server e no AEP da Vodafone. Esta camada permitiu também realizar o envio de toda a informação para a base de dados de backup (Cloudant) e para as restantes aplicações IoT utilizadas no trabalho.

Por último e para concluir o cenário de instalação dos sistemas da camada aplicacional, procedeu-se à configuração das plataformas IoT. Esta componente envolveu diversas plataformas, nomeadamente, IBM Watson IoT, IBM IOC, IBM Cloudant, Vodafone/Thinkdigital Plataforma IoT, Vodafone/Thinkdigital AEP (Coletores e APIs) e Vodafone/Thinkdigital GTC (SCADA).

4.2 – Testes de validação

Neste capítulo são apresentados os testes efetuados aos componentes envolvidos neste projeto, nomeadamente os testes efetuados às plataformas utilizadas e aos protocolos de comunicação das camadas físicas e de aplicação.

Relativamente à componente física é efetuada uma descrição do resultado dos testes efetuados às redes de sensores e aos respetivos dispositivos, incluindo protocolos e métodos de comunicação.

Na componente aplicacional é apresentado um resumo do resultado dos testes efetuados à plataforma de gestão de dispositivos, à camada de integração e às aplicações de gestão e IoT.

Testes à camada física

Nos testes efetuados foram utilizadas três tecnologias de comunicação, nomeadamente NB-IoT, LoRaWan e 802.15.4-6LowPAN.

De um lado temos NB-IoT e LoRaWan como protocolos de rede de longo alcance e por outro temos 802.15.4 (6LowPAN) que atua no quadro das redes de curto alcance.

NB-IoT (sensores e atuadores)

Nos testes realizados com esta tecnologia foram utilizados sensores NB-IoT de medição de variáveis ambientais e 2 controladoras de atuação.

Foi criada uma rede de sensores fornecidos pela Vodafone, onde foi possível testar as configurações disponíveis, a conectividade e o desempenho.

No survey realizado verificou-se que o protocolo utilizado pelos dispositivos NB-IoT para transferência de dados dos dispositivos, na camada de aplicação, é o COAP.

Nos testes de cobertura foram efetuados ensaios com apoio de um equipamento de teste. Foram realizadas medições de sinal em campo aberto, dentro de edifícios e enterrados no solo.

Para realização dos testes subterrâneos, os sensores foram instalados dentro de caixas estanques, com as sondas de medição derivadas para o exterior das mesmas.

Foram também efetuados testes em várias localizações do concelho e dentro de vários edifícios.

No caso das controladoras, foram testadas as capacidades de comunicação dentro de quadros elétricos e testada a ativação das respetivas electroválvulas através da cloud.

Para comunicação entre as controladoras e as electroválvulas foram testadas cablagens de controlo passadas através de infraestruturas subterrâneas, até às caixas onde estas se encontravam.

Dispositivos LoRaWan (sensores)

Os testes realizados com esta tecnologia permitiram utilizar vários sensores de medição de temperatura, humidade e luminosidade, um gateway LoRa e um LoraWan Server alojado na cloud.

Os testes desta componente foram realizados no âmbito de dois projetos distintos:

- O projeto de eficiência energética em implementação no concelho de Tomar, onde os testes realizados se centraram principalmente nos testes de cobertura e no survey de definição dos locais para instalação das antenas e gateways LoRa.

Foram analisados e testados os equipamentos de gateway, nomeadamente na sua capacidade de cobertura e nas funcionalidades disponibilizadas no aprovisionamento de dispositivos LoRa.

- O segundo projeto, onde o cenário foi montado especificamente para este trabalho, foram realizados trabalhos com tecnologia LoRa, os testes passaram pela utilização de sensores de variáveis ambientais, 1 gateway e 1 LoRaWAN Server alojado na cloud.

Nesta componente não foram testados alcances, uma vez que o gateway era um equipamento de indoor. Foram testados os procedimentos de aprovisionamento de sensores no servidor LoRa e validados aspetos de configuração e compatibilidade com as soluções tecnológicas escolhidas para este projeto.

Relativamente à comunicação com atuadores LoRa, não foram efetuados quaisquer testes.

Dispositivos 802.15.4 6LowPAN (sensores e atuadores)

Nesta tecnologia foram realizados testes com seis dispositivos Zolertia (equipados com sensores de temperatura do ar, humidade do ar e luminosidade), 2 Raspberry PI (S.O. Debian/Contiki, Node-JS e Node-RED), 1 Arduino Uno, 1 Eletroválvula 50mm de 9V e 1 Relé de dois circuitos 5V/9V.

Nestes testes foi criada uma rede 6LowPAN IPv6, utilizando o protocolo de encaminhamento RPL sobre UDP. Foi testado o envio dos dados ambientais recolhidos através do nó border router.

Mediante a criação de um túnel USB (tunslip6 script), os dados recolhidos são enviados para o Raspberry PI. Neste último os dados são processados, tratados e transferidos através do protocolo TCP/IPv4 para a plataforma de gestão de dispositivos (Watson IoT).

Nos testes realizados foram analisados os alcances dos dispositivos, a duração das baterias, a capacidade de processamento de dados do border-router, etc.

Foi testada a comunicação via protocolos MQTT e HTTP (REST) e a compatibilidade e capacidade de integração com as plataformas da camada de gestão de dispositivos. Este teste foi efetuado com recurso a uma rotina desenvolvida em Node.js., que trata os dados recebidos e os encaminha para o feed respetivo.

Testes à Camada de aplicação

Nos testes efetuados foram analisadas as funcionalidades, compatibilidades e potencialidades de cada uma das plataformas utilizadas no projeto, nomeadamente as ferramentas de gestão de dispositivos, a plataforma de integração e as plataformas IoT de gestão e controlo.

Os trabalhos realizados com cada uma destas plataformas permitiram testar as operações de criação de perfis de utilizadores, de ambientes de trabalho, de gestão de dispositivos e de bases de dados, e a criação de conectores de ligação, etc.

Relativamente aos protocolos da camada de aplicação, foram testadas as comunicações através de APIs MQTT, COAP e HTTP (REST).

Plataforma de gestão de dispositivos

Considerando como principal requisito desta camada o registo e autenticação de dispositivos de forma centralizada, estes testes centraram-se mais nas questões de conectividade e de segurança das plataformas tecnológicas (Watson IoT, AEP Vodafone/Thinkdigital e Wavesys LoraWan Server).

Foram testados o registo e a integração de dispositivos NB-IoT, LoRa e 802.15.4 (sensores ou atuadores), assim como a integração de todas as plataformas IoT adotadas no projeto, através da utilização de protocolos e tecnologias de comunicação IoT.

Os testes efetuados pretenderam concluir se esta camada cumpria os requisitos para se poder considerar agnóstica, conforme definido nos objetivos do projeto, tendo capacidade de aprovisionar todos os dispositivos, independentemente da sua tecnologia ou proprietário.

Relativamente à questão da segurança na comunicação via APIs, nas transferências de dados realizadas através de protocolo MQTT, CoAP e HTTP (REST), conforme imagem abaixo (40), foram testados diversos dispositivos e validadas as funcionalidades de atribuição do Tokens, de validação de MACs, de IPs, etc.

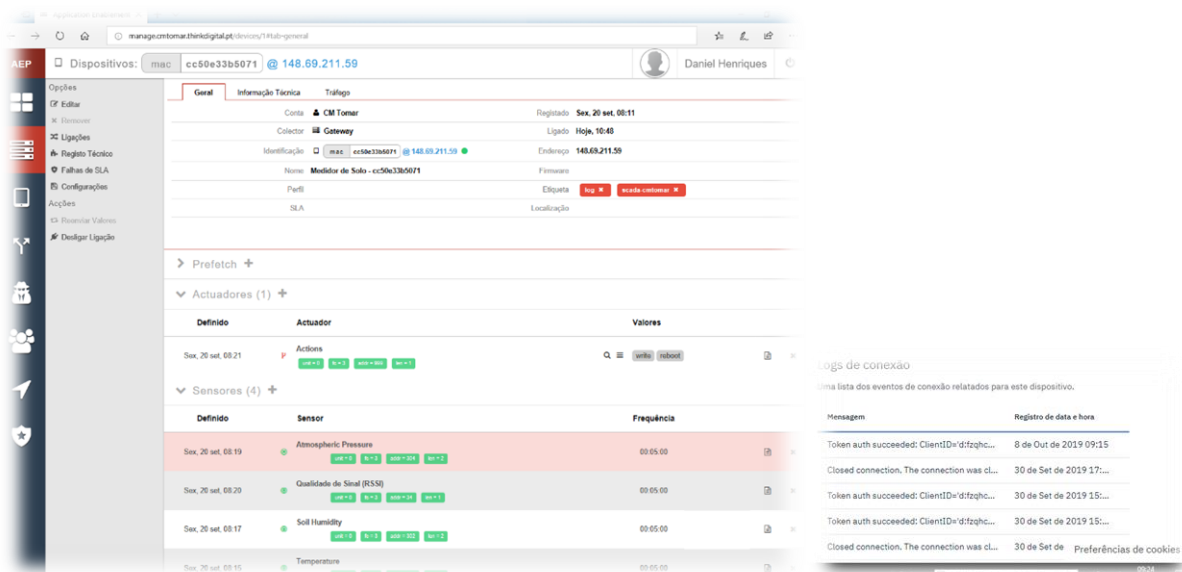


Figura 39 – Segurança das plataformas da camada de gestão de dispositivos

Para conseguir cumprir o objetivo de utilizar esta camada como ponte entre os dispositivos IoT e a plataforma de integração, foram utilizadas e testadas 3 plataformas de gestão de dispositivos (Watson IoT, AEP Vodafone/Thinkdigital e Wavesys LoraWan Server), onde foram realizadas as abordagens necessárias.

Considerando que um dos requisitos para esta solução seria o alojamento na cloud, foram realizados diversos testes de disponibilidade, fiabilidade e desempenho.

Plataforma de Integração

Os testes efetuados nesta camada incidiram sobre as capacidades de desenvolvimento e sobre as compatibilidades do Node-RED (alojado na cloud).

À medida que foi sendo efetuado o desenvolvimento da solução foram efetuadas as validações necessárias.

Por se tratar de uma ferramenta de código aberto, as funcionalidades do Node-RED são de acesso público e indiscriminado. Assim sendo, os testes foram efetuados no sentido de perceber se os desenvolvimentos efetuados respondiam às necessidades de desenvolvimento e se cumpriam os requisitos do projeto.

Foram realizados testes de integração das diversas plataformas, nomeadamente no que diz respeito à comunicação através dos protocolos da camada de aplicação MQTT, CoAP e HTTP (REST).

No que respeita à capacidade para efetuar tratamento e validação de dados, foram desenvolvidas, com sucesso, as rotinas para conversões de valores, cálculos por aplicação de fórmulas, análises de intervalos de valores, variações de dados acima do normal, exclusão de valores nulos, limitação das frequências de comunicação dos dispositivos, etc.

Para testar se esta solução se encontra habilitada para desempenhar funções de backup para um repositório de dados centralizado, foi desenvolvido de um fluxo que copia todos os dados recolhidos pelos sensores LoRa, NB-IoT e 802.15.4, e os replica para as diversas bases de dados criadas no IBM Cloudant.

Foi também testada a capacidade de desenvolver um fluxo que automaticamente recolhe as previsões meteorológicas do IPMA, através de consultas realizadas à API disponibilizada.

Quanto à capacidade de agir diretamente sobre os atuadores instalados no terreno e à capacidade para contrariar as ordens dadas aos mesmos pelas plataformas de gestão IoT, foi desenvolvido um fluxo que analisa as variáveis ambientais e que se consegue sobrepor, eventualmente negando essas ordens.

Já na área de atuação, foram testados fluxos no Node-RED alojado na cloud para tratar as ordens de atuação das plataformas IoT.

No Node-RED local, instalado nos Raspberry Pi, foram realizados testes para o comando do Arduino utilizado para controlo das eletroválvulas.

A necessidade de instalação da versão local deveu-se ao facto de não ter sido possível interagir com o Arduino na versão cloud do Node-RED, através da portas usb.

Para validação dos testes de abertura e o fecho de electroválvulas através de um Raspberry Pi, foi efetuada a instalação do Node-RED local e da criação de um fluxo em JavaScript, que ciclicamente, para saber se deve atuar, faz consultas à plataforma de IoT.

Plataformas de controlo e gestão IoT

Os testes realizados nas soluções escolhidas para esta camada foram centrados nas funcionalidades, nomeadamente no desenvolvimento de feeds e dashboards, na capacidade de comunicação com a camada de integração e na comunicação com os atuadores instalados no terreno.

Testes realizados por plataforma:

IBM Watson IoT – Criação de instâncias de trabalho, gestão de dispositivos IoT, comunicação através dos diversos protocolos da camada de aplicação e integração com as plataformas da camada de integração e de backup (Node-RED e Cloudant).

IBM Cloudant - Criação de recursos de trabalho, criação de bases de dados (sensores, backups, previsões meteorológicas, ordens de atuação, etc.), comunicação através dos diversos protocolos da camada de aplicação e integração com a plataforma da camada de integração (Node-RED).

Vodafone/Thinkdigital AEP (Coletores e APIs) - Criação de aplicações e conectores, criação de dispositivos IoT, comunicação através dos diversos protocolos da camada de aplicação e integração com as plataformas da camada de integração e de gestão (Node-RED e Vodafone/Thinkdigital Plataforma IoT).

Vodafone/Thinkdigital Plataforma IoT - Criação ambiente de projeto, gestão de dispositivos IoT, comunicação através dos diversos protocolos da camada de aplicação e integração com as plataformas da camada de integração (Node-RED e Vodafone/Thinkdigital AEP), criação de dashboards com gráficos e widgets.

Vodafone/Thinkdigital GTC (SCADA) - Comunicação com as plataformas da camada de integração (Node-RED e Vodafone/Thinkdigital AEP), criação de dashboards com gráficos, widgets e esquemas tipo SCADA.

Outras plataformas – Foram ainda realizados testes de integração de outras plataformas, nomeadamente ThingsBoard, IBM IOC, etc. mas foram excluídas do presente projeto por questões de enquadramento tecnológico.

4.3 – Resultados dos testes de validação

Neste capítulo são apresentados os resultados dos testes efetuados aos componentes envolvidos neste projeto, nomeadamente às plataformas utilizadas e aos protocolos de comunicação das camadas físicas e de aplicação.

Relativamente à componente física é apresentado o resultado dos testes efetuados às redes de sensores e aos dispositivos (incluindo protocolos e métodos de comunicação).

Na componente aplicacional é apresentado o resultado dos testes efetuados à plataforma de gestão de dispositivos, à camada de integração e às aplicações de gestão e IoT.

No que diz respeito às camadas protocolares (Física, Ligação, Rede, Transporte e Aplicação), LoRa, NB-IoT e 802.15.4 apresentam arquiteturas muito diferentes.

Na figura 41 é representado de forma ilustrada um esquema dos vários protocolos e padrões utilizados por cada camada protocolar.

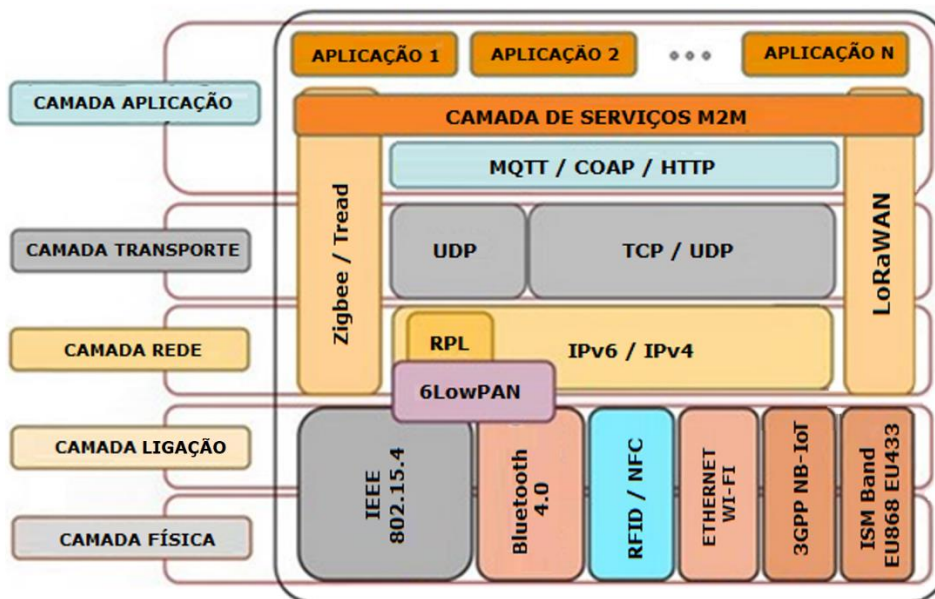


Figura 40 - Camadas protocolares TCP/IP, 6LowPAN, LoRaWAN e NB-IoT

Resultado dos testes efetuados à camada física

Neste ponto são apresentados os testes efetuados às três tecnologias de comunicação, nomeadamente NB-IoT, LoRaWan e 802.15.4-6LowPAN.

NB-IoT (sensores e atuadores)

Nesta tecnologia foram realizados testes com dois sensores NB-IoT de medição de variáveis ambientais e duas controladoras de atuação.

Confirmou-se que não foi necessário da parte da Vodafone proceder à instalação de antenas ou gateways, tendo sido apenas necessário ativar as licenças NB-IoT nas antenas de comunicações móveis. Neste projeto a ativação destes serviços demorou cerca de 3 meses. Foram efetuados testes em várias localizações do concelho e confirmou-se que o sinal apenas estava ativo nas antenas indicadas pela Vodafone.

No contacto com as empresas envolvidas neste projeto, ficou a ideia de que embora o NB-IoT tenha surgido em 2017, ainda hoje a sua cobertura a nível nacional é muito reduzida e a sua implementação no território nacional está abaixo das expectativas das operadoras de telecomunicações.

Verificou-se que NB-IoT opera em frequências licenciadas, o que permite que os clientes usufruam dos sistemas de segurança disponibilizados pelas operadoras de telecomunicações (neste caso a Vodafone).

Pelos testes efetuados, embora realizados durante um curto espaço de tempo, verificou-se bastante fiabilidade na transmissão de dados, uma vez que não se registam percas de dados.

Relativamente à cobertura e alcance do sinal, verificou-se que efetivamente, mesmo dentro de edifícios e debaixo do solo, esta é das três tecnologias testadas a que apresenta melhor desempenho. Nos testes subterrâneos os sensores foram instalados dentro de caixas estanques e mesmo assim o sinal NB-IoT apresentava boa conectividade.

Comparativamente com as outras tecnologias testadas, os equipamentos NB-IoT têm a particularidade de possuir uma maior capacidade de penetração de sinal, permitindo

enterrar os dispositivos, reduzindo assim a probabilidade de furto e de atos de vandalismo.

No caso das controladoras, foram testadas as capacidades de comunicação dentro de quadros elétricos e testada a ativação das respetivas electroválvulas através da cloud. Para comunicação entre as controladoras e as electroválvulas foram testadas cablagens de controlo passadas através de infraestruturas subterrâneas, até às caixas onde estas se encontravam.

Nos testes realizados não foi possível aceder ao firmware dos dispositivos, uma vez que se trataram de equipamentos proprietários da Vodafone. O firmware destes dispositivos já vem instalado de fábrica, consistindo os trabalhos da parte dos clientes apenas na instalação física dos mesmos no terreno.

Ainda não foi possível testar a capacidade da bateria, mas de acordo com as especificações disponibilizadas pelo fabricante será muito semelhante à dos dispositivos LoRa.

Face aos testes efetuados, tirando a facilidade com que se adicionam novos dispositivos aos projetos, não se encontram vantagens em termos de funcionalidades, concluindo-se que o recurso a esta tecnologia faz mais sentido nos locais onde seja difícil instalar infraestruturas de comunicação sem fios, ou nas situações em que o baixo número ou a dispersão de dispositivos não justifiquem o investimento em antenas e gateways.

Por outro lado, sendo que o custo desta tecnologia tem a tendência de baixar nos próximos anos, a curto prazo poderá vir a ser economicamente mais vantajosa do que as outras tecnologias que obrigam a investimentos em infraestruturas.

Verificou-se que tanto os sensores como os atuadores vêm equipados com um router NB-IoT, ao qual é atribuído um 1 IP público por parte da operadora de telecomunicações fornecedora do serviço. Tal como os routers 3G/4G, estes equipamentos necessitam de um cartão SIM semelhante ao de um telemóvel, e autenticam-se através de um IMEI.

Confirmou-se que, em dispositivos Vodafone, a transmissão de dados entre dispositivos Narrowband é efetuada, na camada de transporte, através do protocolo UDP e que na camada de aplicação o protocolo de comunicação utilizado é COAP.

Relativamente à componente financeira, verificamos que os dispositivos NB-IoT são mais caros do que os dispositivos LoRa, mas uma vez que dispensam a instalação de antenas e gateways, estes ficam mais económicos em projetos com menor quantidade de equipamentos e com maior dispersão geográfica.

Dispositivos LoRaWan (sensores)

Nesta tecnologia foram realizados testes, com sensores de medição de temperatura, humidade e luminosidade, um gateway LoRa e um LoraWan Server alojado na cloud.

Verificou-se que os dispositivos LoRa utilizados tinham a capacidade para operar nas bandas de frequências ISM dos 863MHz aos 870MHz.

Resultados dos testes obtidos no âmbito dos dois projetos desenvolvidos:

No projeto de eficiência energética, nos testes de cobertura efetuados não se confirmaram as distâncias de alcance de sinal divulgado nas especificações desta tecnologia, mesmo colocando as antenas em locais muito elevados e com linha de vista (conforme imagem abaixo).



Figura 41 – Local elevado de instalação de antena e gateway LoRa

Os testes efetuados durante o survey confirmaram que existe qualidade de sinal em distancias até 5km e em zonas urbanas e de locais de baixa quota, como por exemplo o vale da Roda Grande e da Roda Pequena, o sinal diminui de intensidade e chega até a perder-se.

No projeto montado especificamente para este trabalho, foram realizados trabalhos com dois sensores de variáveis ambientais, 1 gateway e 1 LoRaWAN Server alojado na cloud.

Nos testes de aprovisionamento de dispositivos LoRa verificou-se que o registo dos mesmos se efetua no gateway LoRa, através do MAC Address do dispositivo.

Nesta componente não foram testados alcances, uma vez que o gateway era um equipamento de indoor mas deu para testar a fiabilidade das comunicações, confirmando-se as melhores espetativas, uma vez que não foram registadas percas de dados.

No que diz respeito aos testes com atuadores LoRa, nestes dois projetos ainda não foi possível efetuar qualquer teste, tendo sido simulada esta componente do projeto.

Dispositivos 802.15.4 6LowPAN (sensores e atuadores)

Nesta tecnologia foram realizados testes com seis dispositivos Zolertia, 2 Raspberry PI, 1 Arduino Uno, 1 Eletroválvula e 1 Relé.

Os testes foram realizados à rede 6LowPAN IPv6 montada com recurso a equipamentos Zolertia.

Foi testado o protocolo de encaminhamento RPL sobre UDP e foi testado o envio dos dados ambientais recolhidos através do nó border router com sucesso.

Também foi possível fazer chegar ao Raspeberry PI os dados recolhidos pelo border-router, através de um túnel USB (tunslip6 script).

Neste último, através de uma rotina desenvolvida em Node.js foi possível ultrapassar a dificuldade de estabelecer comunicação via protocolo MQTT (já através do protocolo TCP/IPv4) para a plataforma de gestão de dispositivos (Watson IoT), e efetuar a separação dos pacotes recebidos pelos respetivos MAC Address dos dispositivos.

Nos testes realizados foi analisada a cobertura dos dispositivos, verificando-se que o alcance máximo é inferior a 50 metros.

Mesmo assim concluiu-se que a qualidade do sinal é aceitável, uma vez que se cumpre as especificações do protocolo 802.15.4 (entre 10 e 100 metros).

A duração das baterias destes equipamentos, mesmo reduzindo a frequência das comunicações, foi muito baixa, tendo o equipamento com maior duração permanecido ligado menos de 2 dias.

Quanto à capacidade de processamento, não foram realizados testes.

Na componente de atuação, os testes efetuados vieram a confirmar que não foi possível conectar a versão Node-RED Cloud aos vários Arduinos testados.

Em alternativa teve que ser instalada a versão local num Raspberry Pi, permitindo desta forma a realização da ligação.

Para além deste constrangimento, como o Arduino debita 5V e a electroválvula utilizada trabalha a 9V, foi necessário recorrer à utilização de uma relé de dois circuitos. Ao receber o impulso dos 5V, a relé ativa o circuito principal dos 9V e faz acionar a electroválvula.

Resultado dos testes efetuados à camada de aplicação

Nesta área são apresentados os resultados dos testes decorrentes da análise às funcionalidades, compatibilidades e potencialidades de cada uma das plataformas utilizadas no projeto, nomeadamente as ferramentas de gestão de dispositivos, a plataforma de integração e as plataformas IoT de gestão e controlo.

Plataforma de gestão de dispositivos

Foi testado com sucesso o registo e autenticação de dispositivos de forma centralizada. Os testes de conectividade e de segurança das plataformas tecnológicas (Watson IoT, AEP Vodafone/Thinkdigital e Wavesys LoraWan Server) foram realizados com sucesso.

Foi possível gerir dispositivos NB-IoT, LoRa e 802.15.4 (sensores ou atuadores) e foi testada com sucesso a integração com todas as plataformas IoT adotadas no projeto. Desta forma concluiu-se que a solução implementada se poderia considerar agnóstica, uma vez que possui capacidade de aprovisionar todos os dispositivos e plataformas, independentemente da sua tecnologia ou proprietário.

Os testes de segurança na comunicação via APIs MQTT, CoAP e HTTP (REST) foram efetuados entre diversos dispositivos e foram validadas as funcionalidades de atribuição do Tokens, de validação de MACs e de IPs, etc.

O requisito de encontrar uma solução alojada na cloud que cumprisse os diversos testes de disponibilidade, fiabilidade e desempenho foi cumprido para as três soluções, exceto na comunicação usb com o Arduino.

Comparando diretamente as três plataformas, concluiu-se que a plataforma da Vodafone apresenta como vantagem principal o facto de disponibilizar mais módulos e funcionalidades que as restantes, e como desvantagem os custos de licenciamento associados.

O Watson IoT apresenta como principais vantagens a estabilidade, as funcionalidades de segurança, o desempenho da solução (alojado na infraestrutura IBM) e a integração com o IBM Cloudant.

A solução Wavesys LoraWan Server apresenta como principal vantagem o facto de ser desenvolvido em código aberto, sobre a plataforma *LoRaWAN Network Server stack*, possuir uma interface web muito simples e amigável, especificamente desenvolvida para gestão de dispositivos IoT e APIs de comunicação.

Plataforma de Integração

Os resultados dos testes efetuados nesta camada vieram comprovar que o Node-RED possui os requisitos e funcionalidades entendidos como necessários, servindo para o cumprimento dos objetivos definidos para esta camada do projeto.

Grande parte dos testes foram efetuados com sucesso à medida que ia sendo efetuado o desenvolvimento da solução.

Foi validado o facto de se tratar de uma ferramenta de código aberto, não havendo funcionalidades bloqueada por questões de licenciamento.

Os testes de integração das diversas plataformas, através dos protocolos da camada de aplicação MQTT, CoAP e HTTP (REST), foi realizado com sucesso, sendo os trabalhos de desenvolvimento e configuração muito simples e com apoio gráfico na configuração dos nós dos fluxos.

Todas as rotinas de tratamento e validação de dados definidas nos objetivos foram desenvolvidas com sucesso.

O fluxo de realização de backups foi realizado, habilitando esta plataforma para desempenhar funções de backup para o Cloudant.

Com recurso a mais um fluxo de Node-RED, foi desenvolvido com sucesso um fluxo que automaticamente recolhe as previsões meteorológicas do IPMA, através de consultas realizadas à API disponibilizada e as guarda numa base de dados do Cloudant.

Na área de atuação, os testes vieram mostrar que o Node-RED alojado na cloud não consegue agir diretamente sobre equipamentos Arduino ligados por USB. Para ultrapassar esta limitação foi necessário utilizar um Raspberry Pi com a instalação do Node-RED local.

Plataformas de controlo e gestão IoT

Neste ponto é apresentado o resultado dos testes realizados às plataformas de controlo e gestão IoT.

Os testes efetuados às plataformas de gestão de dispositivos IoT vieram confirmar que as escolhas efetuadas cumprem os objetivos do projeto, nomeadamente na comunicação através dos diversos protocolos da camada de aplicação.

Desde os testes de criação de instâncias e recursos de trabalho, à gestão de dispositivos, à ligação com a plataforma de integração, todos os objetivos foram executados com sucesso.

De acordo com os trabalhos e testes realizados a adoção do Node-RED como plataforma principal da camada de integração foi um sucesso, uma vez que para além de todas as capacidades de integração com dispositivos e plataformas, também apresentou os recursos necessários para o desenvolvimento da programação e desenvolvimento de algoritmos

Já a opinião que fica do IBM Cloudant, é que para plataforma de backups serve perfeitamente, para armazenamento de dados também, mas fica a ideia que as funcionalidades disponíveis são muito limitadas (eventualmente por se tratar da versão gratuita de demonstração/testes).

De acordo com os testes realizados, esta ferramenta, no contexto deste trabalho, tem como principal vantagem o facto de integrar diretamente com o Node-RED e com o Watson IoT.

Relativamente às plataformas da Vodafone/Thinkdigital, tanto na camada de gestão de dispositivos, na camada de integração ou na camada de gestão IoT, a conclusão a que se chega é que as mesmas são muito robustas e apresentam muitas funcionalidades desenvolvidas à medida para projetos IoT.

Uma das funcionalidades que esta ferramenta apresenta com muita qualidade, que não foram abordadas neste relatório por não fazerem parte dos objetivos do projeto, mas que apresentam uma enorme mais valia a este produto, é o módulo de desenvolvimento de dashboards.

5 – CONCLUSÕES

Num mundo tecnológico em constante evolução surgem regularmente novos desafios, novas tendências, novas oportunidades de negócio e novas tecnologias, que influenciam diretamente o nosso modo de vida, transformando a vida nas cidades. O conceito de Smart Cities (cidades inteligentes) está a crescer em todo o mundo e a IoT (Internet das Coisas) é uma peça essencial na viabilização da implementação de projetos, quer seja na área da redução do consumo de água, de energia, da recolha de resíduos, etc.

De acordo com a investigação e com os testes realizados no âmbito protocolos IoT das camadas física e de ligação, conclui-se que o LoRa e o NB-IoT competem no quadro dos projetos IoT para redes de longo alcance e que o 802.15.4 compete na área das redes de curta distância. Enquanto o LoRa e o 802.15.4 têm o seu lugar consolidado no mercado IoT, o NB-IoT ainda está em fase de expansão e consolidação.

O NB-IoT apresenta uma elevada cobertura e capacidade de penetração. O custo dos dispositivos é elevado, mas como não necessita de investimento em equipamentos gateway, em projetos com poucos dispositivos ou muito dispersos no terreno, acaba por se tornar a opção mais vantajosa. O facto de as operadoras possuírem infraestruturas de comunicações compatíveis com NB-IoT é um fator de vantagem face às restantes tecnologias IoT. Encontra-se mais direcionado para projetos implementados em áreas de maior dimensão, que exijam um QoS mais elevado e necessitem de uma mais baixa latência

O LoRa apresenta dispositivos com baixo consumo energético e baixo custo. A necessidade de instalação de infraestruturas de comunicação (gateways) e a baixa largura de banda são alguns dos obstáculos encontradas na utilização deste protocolo. Separada em duas camadas, uma camada física da rede, que utiliza a técnica de modulação de rádio Chirp Spread Spectrum (CSS) e na camada lógica, que define a arquitetura e os parâmetros da comunicação (LoRaWAN - protocolo da camada MAC). Concentra-se principalmente em projetos de longa duração e com maior densidade e quantidade de dispositivos face à área de implantação

O 802.15.4 (6LowPAN) especifica a camada física e a camada de ligação (MAC) e foi desenvolvido para sistemas de comunicações de baixo custo em redes de curta distância, apresentando baixas necessidades de infraestruturas e baixo consumo de energia. Para ultrapassar o baixo alcance desta tecnologia, permite a implementação de redes de tipologia mesh, reduzindo o número de gateways. Enquadra-se principalmente em projetos de pequenas áreas e dimensão.

De acordo com o estudo e com os trabalhos realizados no âmbito das camadas aplicacionais, conclui-se que é viável centralizar a gestão de diversos projetos IoT através de uma única plataforma de integração. Através do Node-RED, que possui os requisitos técnicos e as funcionalidades necessárias para desenvolvimento da camada de integração, tanto ao nível da integração com plataformas IoT (ex. IBM Watson IoT, AEP Vodafone/Thinkdigital, IBM Cloudant, etc.), como ao nível da integração com dispositivos de hardware (ex. Arduino), é possível utilizar diversas soluções, de diversos fornecedores e tecnologias, integradas e a comunicar entre si via API.

No que respeita a limitações encontradas no desenvolvimento do projeto, foram identificadas questões como a impossibilidade de alterar configurações dos dispositivos NB-IoT, uma vez que o acesso ao seu firmware se encontra barrado pela operadora de comunicações, a impossibilidade de testar um atuador LoRa por falta de acesso a equipamento, e a incapacidade para testar a duração das baterias dos protocolos LPWAN, uma vez que o tempo de projeto não foi suficiente para poder chegar a alguma conclusão.

Na camada aplicacional foi verificada a impossibilidade de garantir segurança na autenticação de alguns dispositivos, motivada pelo facto de estarem a ser testados dispositivos de diversas tecnologias e proprietários.

Como trabalho futuro no âmbito deste projeto, serão realizados testes durante os próximos 12 meses e será desenvolvido um dashboard de gestão e controlo de sistemas de rega. Paralelamente, com a infraestrutura tecnológica à disposição no concelho de Tomar, será possível avançar com a expansão desta solução de rega inteligente para os restantes espaços verdes do concelho, e eventualmente para outras áreas de atuação no âmbito de atuação dos Municípios.

Concluindo, o conceito de Smart Cities está em constante evolução, com novos sistemas e equipamentos IoT a surgir frequentemente, suportados por redes de longa distância de baixa potência (LPWAN) com custos cada vez mais baixos. Estes sistemas continuarão a revolucionar o nosso dia-a-dia, na forma como nos relacionamos com os equipamentos e objetos que temos à nossa volta.

A escolha das tecnologias certas é essencial para que os recursos disponibilizados se adaptem às necessidades dos projetos, evitando custos desnecessários e projetos sem viabilidade técnica e económica.

REFERÊNCIAS – ver ordem

- [1] The Internet of Things: A survey. (2010, outubro). Comput. Netw. pp. 2787-2805.
- [2] Smart cities of the future (2012). Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, Y.
- [3] The Top 30 Emerging Technologies 2018–2028 (Abril 30, 2018) Sean Moffitt.
- [4] The Internet in IoT-OSI, TCP/IP, IPv4, IPv6 and Internet Routing. (2017).
- [5] Narrowband-IoT: A Survey on Downlink and Uplink Perspectives, Luca Feltrin, Galini Tsoukaneri, Massimo Condoluci, Member, Chiara Buratti, Toktam Mahmoodi, Mischa Dohler, Fellow, and Roberto Verdone
- [6] Random Access Preamble Design and Detection for 3GPP Narrowband IoT Systems, 2016, Xingqin Lin, Ansuman Adhikary, and Y.-P. Eric Wang
- [7] LoRaWAN Specification V1.0. LoRa Alliance, 2015. (August 2016).
- [8] LoRa technology - MAC layer operations and Research issues. Chékra El Fehria,, Mohamed Kassabb,, Slim Abdellatifc, Pascal Berthouc, Abdelfettah Belghithd. (2018)
- [9] Long-Range Communications in Unlicensed Bands: The Rising Stars in the IoT and Smart City Scenarios Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi (outubro 2016)
- [10] LoRa - A Survey of Recent Research Trends, M. Saari*, A. Muzaffar bin Baharudin **, P. Sillberg*, S. Hyrynsalmi* and W. Yan** (maio 2018)
- [11] A Study of LoRa: Long Range & Low Power, Networks for the Internet of Things Aloÿs Augustin¹, Jiazi Yi ¹, Thomas Clausen ¹ and William Mark Townsley ²
LORA vs NB
- [12] A survey on LPWA technology: LoRa and NB-IoT, (21 março 2017), Rashmi Sharan Sinha, Yiqiao Wei, Seung-Hoon Hwang (setembro 2016)
- [13] Toby Jaffey, Eclipse Foundation Newsletter, 2014, MQTT and CoAP, IoT Protocols
- [14] Alexandra Bowen, (setembro 2018), IoTZone, IoT Is Eating the World: APIs and REST
- [15] Michael Yuan, (outubro 2017, Conhecendo o MQTT)
- [16] Vitor Vidal, (nov. 2017), Desenvolvimento de Software, Internet of Things (IoT)
- [17] A Gentle Introduction to IoT Protocols: MQTT, CoAP, HTTP & WebSockets, (June 14, 2017), Antonio Almeida and Jaime González-Arintero
- [18] Postscapes (maio de 2019, IoT Standards and Protocols)
- [19] E. Ferreira, Rubem. (jan. 2013) Linux:guia do adminitrador do sistema.

- [20] Kais Mekkia, Eddy Bajica, Frederic Chaxela, Fernand Meyer, (Dec. 2017), A comparative study of LPWAN technologies for large-scale IoT deployment
- [21] Vaishali Maru (February 13, 2019), 10 Best Opinions about IoT based Smart Cities
- [22] Standardization of NB-IOT completed. 3gpp.org. 3GPP. June 22, 2016. p. 1. Retrieved August 19, 2016.
- [23] NB-IoT - The choice of Frequency, Deployment Mode and Coverage
March 22, 2017 | By Junaid Afzal @ SIGFOX
- [24] EW Staff (30th August 2018), IoT smart cities: the long-range forecast for wireless connectivity
- [25] osoyoo, (jul 20018), What is LoRa Radio Network?
- [26] Pablo Melo, (May 2017), Padrão IEEE 802.15.4 - A base para as especificações Zigbee, WirelessHart e MiWi
- [27] Thanh-Dien Tran · Ricardo Silva · David Nunes · Jorge Sa Silva, (2011) Characteristics of Channels of IEEE 802.15.4 Compliant Sensor Networks
- [28] Alfadoni Prisantama, Widyawan, and I. Wayan Mustika, (july 2016), Tunneling 6LoWPAN protocol stack in IPv6 network
- [29] Microchip Technology, Inc. (2019), Wi-Fi and Ethernet, TCP/IP Protocol Suite, TCP vs. UDP
- [30] Leor Brenman, (March 2018), API Builder and MQTT for IoT – Part 1