# Internet of Things

A *Internet of Things* (IoT) consiste num conceito onde todos os dispositivos estão ligados à internet. Este permite que os dispositivos possam enviar informações ou realizar tarefas depois de terem recebido algo remotamente.

Em uso domestico, as máquinas de lavar roupa e louça, o frigorifico, o forno, o micro-ondas, entre outros, poderiam aderir ao IoT. Num frigorifico, por exemplo, quando se observa que um alimento está em falta, seria útil enviar um alerta ao proprietário. Poder-se-ia ainda configurar o mesmo para que este encomenda-se um alimento quando a quantidade estiver abaixo da pretendida. Ou seja, de forma rápida e cómoda, o proprietário pode definir quais os alimentos críticos que o frigorifico deve ter em conta, qual a quantidade mínima destes, e quando essa for ultrapassada, encomendar uma certa quantidade predefinida, permitindo escolher qual o horário preferencial de entrega, entre outros.

Este conceito está em constante expansão, estando as entidades envolvidas a apostar, cada vez mais, em protocolos de comunicação cujas características visam beneficiar o seu uso em dispositivos IoT.

# Tecnologias de Comunicação

Para que o microcontrolador consiga comunicar com o servidor remoto, foi necessário escolher uma tecnologia de comunicação. Uma tecnologia não consegue servir todas as necessidades de todos os projetos existentes, tendo cada uma as suas características. Wifi e BTLE são os mais usados e servem aplicações relacionadas à comunicação de dispositivos pessoais, como o computador, tablets e outros. Estes têm capacidade para receber uma grande quantidade de dados, mas estão propícios a ataques. Os telemóveis têm também a sua própria tecnologia de comunicação, sendo ótima para enviar grandes quantidades de dados, existindo uma grande área de cobertura para o uso desta rede. A LPWAN permite aos seus dispositivos uma poupança de energia considerável, sendo adequada para dispositivos que enviam poucas quantidades de dados em grandes intervalos de tempo.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Local Area Network | Low Power Wide Area Network (LPWAN)  Internet of Things | Cellular Network |
| good | -Well established standards  -High data rate | -Low power consumption  -Low Cost  -high range | -Existing Coverage  -High data rate |
| bad | -Battery Live  -Network cost & dependencies  -low range | - High Data rate  - Emerging standards | -Autonomy  -Battery Live  -Medium Range |
| technology | wifi | LoRa, Sigfox | 3G, 4G |

Os protocolos que são mais usados pelos IoT neste momento são o Sigfox e o LoRaWAN, devido ao baixo consumo de bateria e à grande área de rede de comunicação (LPWAN – Low Power Wide Area Network), sendo nesses que este estudo se irá focar.

# LoRa

LoRa é uma camada física ou modulação sem fios que permite criar comunicações a grandes distâncias. Muitos sistemas sem fios usam frequency shifting keying modulation (FSK) como camada física, devido ao seu baixo consumo energético, no entanto, o LoRa usa chirp spread spectrum modulation que mantem o baixo consumo energético, mas que permite um maior alcance da área de comunicação.

**LaRaWAN**

LoRaWAN define o protocolo de comunicação e a arquitetura da rede, usando o LoRa para estabelecer comunicações. O protocolo e a arquitetura definidos têm implicações que são sentidas na duração da bateria, na capacidade de rede, na qualidade do serviço, na segurança e no número de aplicações diferentes servidas pela rede.

É o protocolo e a arquitetura da rede que tem a maior influencia na duração da bateria de um dispositivo, da capacidade da rede, da qualidade do serviço, da segurança e o número de aplicações diferentes servidas pela rede.

As especificações do LoRaWAN variam de região para região. Na europa foram definidos 10 canais, em que 8 destes são *multi data rate* (??multi-ritmo de dados), podendo ir dos 250bps até 5.5 kbps. Na europa, são permitidos, no máximo, +14dBM.

**Mensagem**

O tamanho de uma mensagem LoRaWAN é pequeno em comparação com outros protocolos de comunicação. Este protocolo ocupa, no mínimo, 12 bytes para tudo o que seja meta-informação. Este valor, pode subir se existirem campos opcionais no frame. No máximo, pode atingir os 29 bytes de tamanho do header. O tamanho máximo de uma mensagem LoRaWAN varia consoante a sua região e a sua velocidade de transmissão. O payload da mensagem pode ter um tamanho máximo de 51 bytes ou de 242 bytes, dependendo das características referidas anteriormente.

(Imagem)

**Arquitetura da rede**

Muitas redes existentes usam uma arquitetura *mesh network*, isto é, cada nó comunica com todos os outros nós que estão na mesma rede, permitindo um aumento do alcance e da quantidade de nós associados à mesma. Em contrapartida, há um aumento na complexidade da rede, dado que um nó comunica com vários outros ao mesmo tempo. Consequentemente, dá-se uma diminuição da capacidade da rede e um aumento do consumo energético, devido ao enorme tráfego entre os nós. Uma outra contrapartida, advém do facto de que cada nó deve receber e enviar informações de outros nós, mesmo que a informação não lhes seja destinada. Tal resulta no aumento do alcance e do tamanho dos nós de uma rede. Por oposição, aumenta a complexidade, dado que um nó comunica com vários nós ao mesmo tempo, diminui a capacidade da rede, uma vez que existe um enorme tráfego entre nós por haver várias ligações e existe um maior consumo de energia dado que cada nó terá que receber e enviar informações dos outros nós mesmo que a informação não lhe seja relevante.

(Imagem)

Uma arquitetura de estrela de longo alcance (arquitetura usada pelo LoRaWAN), quando comparada com a Mesh Network, aparenta ser uma melhor escolha, visto que tem um baixo consumo de bateria.

(Imagem)

Numa rede LoRaWAN os dispositivos não estão associados a uma gateway. A informação é enviada para todos os gateways que estão dentro do raio de alcance, sendo estes responsáveis por propagar o pacote recebido para um servidor colocado na cloud, por via de um backhaul (rede móvel, ethernet, wi-fi). A complexidade e tratamento inerente ao reconhecimento de chegada, verificações de segurança, adaptação da transmissão de dados, entre outros, são da responsabilidade do servidor.

**Capacidade da rede**

Como o LoRaWAN é uma tipologia estrela, para possibilitar a receção de uma quantidade considerável de mensagens de vários nós, é necessário ter gateways com uma enorme capacidade. Para garantir esta condição, é possível optar por duas técnicas, adaptive data rate, que permite adaptar a quantidade de bits enviados num intervalo de tempo, e multichannel multi-modem transceiver, em que as mensagens enviadas em multi-canais, podem ser recebidas pelo gateway.

Existem fatores de propagação que podem comprometer a capacidade de rede, como a quantidade de canais concorrentes, a frequência de bits enviados num intervalo de tempo, o tamanho do payload da mensagem e a frequência em que são enviadas as mensagens pelos nós. Como o LoRa usa spread spectrum based modulation, os sinais são praticamente ortogonais quando diferentes fatores de propagação são utilizados. Os gateways tiram proveito desta característica, dado que têm a capacidade de receber dados com diferentes ritmosno mesmo canal, ao mesmo tempo. Se um nó tem uma boa conexão e encontra-se perto do gateway, este pode aumentar a frequência de envio de bits, consumindo uma maior largura de banda. Assim o envio é mais rápido, diminuindo o tempo da transmissão e aumentando a possibilidade de outro nó começar a transmitir. De modo a que o adaptive data rate funcione, é necessário que o ritmo de envio seja igual ao ritmo de receção de mensagens.

**Tipos de Serviço**

O LoRaWan, de forma poder abranger uma grande diversidade de sistemas embebidos, cada um com as suas características próprias, dividiu-se em diferentes classes. Isto tornou possível otimizar, através, de por exemplo, variações no downlink (quanto maior, mais consumo energético), o desempenho de acordo com as necessidades de cada dispositivo.

(Imagem)

**Classe A** – Comunicação bidirecional

Os dispositivos que tem a classe A, usufruem de comunicação bidirecional. Quando um dispositivo envia informação, este terá um intervalo para receber transmissões. Esta é a classe que permite maior poupança de bateria. Não existe limite para mensagens enviadas, mas a nível de receção existe uma forte limitação, visto que tem que enviar primeiro uma mensagem e, posteriormente, irá ter um intervalo para receber dados. Assim, todas os dados enviados para o dispositivo, têm que aguardar que o dispositivo comece uma transmissão.

**Classe B** – Comunicação bidirecional com intervalos para receber dados

Esta classe tem todas as funcionalidades da classe A, mas tem uma diminuição de latência. Isto porque os dispositivos com a classe B, têm a adição de uma janela de tempo para receber dados. Para tal, este recebe uma sincronização-temporal do gateway, permitindo ao servidor saber quando o dispositivo está à escuta.

**Classe** **C** – Comunicação bidirecional a tempo inteiro

Dispositivos com a classe C não têm restrições para receber dados, podendo-os receber a qualquer instante, excecionando aqueles em que está a enviar. Esta classe é a que consome maior bateria, sendo direcionada para sistemas embebidos que necessitem de uplink e downlink sem restrições, não havendo latência nas transmissões.

**Segurança**

O protocolo LoRaWAN tem duas camadas de segurança: uma para a rede e outra para a aplicação. A camada de rede assegura que as mensagens enviadas vão autenticadas. Juntamente com a mensagem enviada, é adicionada uma marca que é o “representante” da mesma. Quando o destinatário recebe a mensagem, vai tentar recriar a marca a partir desta, se ambas as marcas, a recriada e a da mensagem rececionada, coincidirem, pode-se concluir que não se sucederam alterações, caso contrário, houve alguma alteração e a mensagem deve ser rejeitada. A camada de aplicação fornece encriptação das mensagens, isto é, antes de enviar a mensagem, esta é cifrada, impedindo assim que um *man-in-the-middle* consiga ler o conteúdo da mesma. A decifra é depois realizada ao nível da aplicação, visto que, só esta terá a chave que possibilita o mesmo. Uma vez que o servidor do operador não tem acesso à chave que permite decifrar as mensagens, mesmo que este sofra um ataque, o conteúdo das mensagens não ficará exposto.

# SIGFOX

A *Sigfox* é uma empresa francesa na área das telecomunicações. É responsável por

desenvolver redes sem fios que ligam equipamentos de baixo consumo energético à Internet ou, em casos especiais, entre si (🡨não fica bem). Alguns exemplos são, os contadores de eletricidade, água e gás, os eletrodomésticos e plataformas meteorológicas amadoras.

As comunicações entre os dispositivos respeitam o protocolo da *Sigfox*, usando como meio físico, para o envio das suas mensagens, as ondas de rádio.

No envio de mensagens para a *cloud*, é usado uma modulação DBPSK (*Differential Binary Phase Shift Keying*). Esta permite transmitir 1 bit por segundo fazendo uso de 1 *Hertz* da largura de banda. Assim, para enviar 100 bits, a ocupação só iria aumentar para 100 *Hertz*, contribuindo para que esta modulação tenha um impacto pouco significante no congestionamento da rede. Optou-se por usar a modulação para transmissão de dados oferecida pela *Sigfox*, uma vez que esta oferece uma facilidade acrescida na sua implementação, quando comparada com as restantes estudadas pelo autor. O facto de que este protocolo permite uma poupança de energia mais elevada, dada a sua baixa velocidade de envio dos bits, pesou igualmente na decisão.

A velocidade de envio das mensagens depende de região para região, podendo variar de 100 bits por segundo até 600 bits por segundo.

O *Sigfox* utiliza a tecnologia *ultra-narrow band* (UNB) para estabelecer uma comunicação bidirecional entre equipamentos e uma *base-station* proprietária. Quando um dispositivo envia uma mensagem, este fá-lo para todas as *base-stations* que estão ao seu alcance. Quando uma *base-station*, que cobre uma certa área, recebe uma mensagem de um dispositivo, esta propaga-a para a *cloud* da *Sigfox*, sendo aí tratadas eventuais mensagens repetidas. A mensagem é recebida na *cloud* do utilizador, cabendo a este escolher entre disponibilizar uma REST API para poder aceder à mesma ou o envio dessa informação para um outro servidor através de um mecanismo de *callback*.

A tecnologia UNB possibilita o envio de mensagens em canais com largura de banda, geralmente, inferior a 200 Hz. O alcance deste tipo de sinais pode superar os 30 km em meios rurais e 5 km em ambientes urbanos. Outra das vantagens da tecnologia UNB é a forte imunidade a ruído, uma vez que o sinal tem uma largura de banda muito pequena, os recetores terão filtros também com uma largura de banda pequena, removendo assim uma grande parte do ruído no sinal.

**Pilha Protocolar**

A pilha protocolar do *Sigfox* é um conjunto de camadas de *software* e *hardware*, responsáveis por construir as mensagens e envia-las para a *base-station*. A pilha do *Sigfox* é constituída por 3 camadas: *frame*, *medium access control* (MAC) e *physical layer*. A primeira recebe a mensagem que é para enviar da aplicação e gera o *frame*, no qual é adicionado um número sequencial para o identificar. A segunda camada, adiciona ao *frame* a identificação do dispositivo e parâmetros que permitem a deteção de erros. A Sigfox, contrariamente às restantes tecnologias, decidiu não colocar nenhum sinal de sincronismo, assim os dispositivos não estão sincronizados com a rede, estando livres para enviar mensagens arbitrariamente. A última camada, determina como o sinal *Sigfox* é enviado. No caso das mensagens *uplink*, é usada uma modulação DBPSK, nas mensagens *downlink* é usada a GFSK (*Gaussian Frequency Shift Keying*). Esta filtra o sinal através de um filtro gaussiano para suavizar as transições, reduzindo a interferência realizada sobre esse canal.

**Mensagens**

Uma das vantagens do protocolo *Sigfox*, é o tamanho das suas mensagens. Um *frame Sigfox* pode ter, no máximo, 12 bytes para o corpo, caso esteja a remeter a mensagem, ou 8 bytes caso seja o destinatário. O *header* tem um tamanho de 14 bytes, onde se encontra um *timestamp*, a identificação do módulo, a informação de autenticação e um código para detetar erros. Assim, um *frame* tem, no máximo, 26 bytes. Já o protocolo *IP Stack*, usa 40 bytes para o *header*. Mas estes tipos de protocolos, em que as suas mensagens têm grandes quantidades de informação, têm um consumo energético superior. Como os sinais são feitos a partir de energia, a relação entre a quantidade de dados a enviar e a energia gasta é proporcional. O tamanho reduzido do *header*, e a limitação de dados a enviar no protocolo *Sigfox*, permite otimizar a bateria.

(imagem)

**Arquitetura da rede**

A *Sigfox* usa uma tipologia estrela. Como constatado anteriormente, o sistema embebido transmite a sua mensagem para todas as estações *Sigfox* que estiverem ao seu alcance. Essas estações irão, posteriormente, propagar essa mensagem para a *Sigfox Cloud*, fazendo uso de uma ligação ponto-a-ponto. A responsabilidade de entregar a mensagem ao destinatário final, neste caso, o servidor do utilizador, cabe à *cloud*.

(imagem)

**Capacidade da rede**

Ao usar tecnologia UNB, as mensagens ocupam uma largura de banda mínima, permitindo, em comparação com os restantes protocolos de comunicação, um maior número de envio de mensagens num dado instante de tempo. Outra característica que diminui a sobrecarga na rede, é a forma das mensagens. Como foi explicado anteriormente, estas têm um tamanho reduzido, fazendo uma utilização inferior da largura de banda quando comparada com as restantes tecnologias de comunicação.

Estas características permitem que a rede da *Sigfox* consiga enviar e receber uma boa quantidade de dados entres os dispositivos e as *base-stations*.

**Tipos de Serviço**

A *Sigfox* só tem um tipo de serviço para todos os IoTs, mas tem diferentes comportamentos e limitações para cada direção de comunicação (*downlink* e *uplink*).

**Uplink**

Quando o dispositivo envia mensagens, tem uma limitação no número de dados que pode enviar. Como foi referido anteriormente, um dispositivo que use *Sigfox* tem, no máximo, 12 bytes para enviar em cada mensagem. Outra limitação, é o número de mensagens que se pode enviar por dia. Para diminuir o trafego da rede e, por consequente, diminuir o número de colisões, só é possível enviar 140 mensagens por dia, no entanto, estas podem ser enviadas a qualquer hora.

**Downlink**

Para poupar a energia do dispositivo, este não está sempre recetivo a mensagens. Para o dispositivo receber uma mensagem, tem que primeiro enviar um pedido para a *cloud* para poder rececionar as suas mensagens. De seguida, a *cloud* envia as mensagens para a *base-station* e estas, posteriormente, são transmitidas para o dispositivo. Cada dispositivo só pode receber 4 *frames* por dia, cujo corpo pode ter, no máximo, 8 bytes.

**Segurança**

A segurança é uma área na qual a Sigfox deu a devida importância. Todas as mensagens enviadas a partir do dispositivo, são autenticadas fazendo uso do MAC (*Message Authentication Code*). Quando a *cloud* recebe uma mensagem, consegue verificar se houve alguma alteração indesejada, descartando-a caso necessário. Para possibilitar o funcionamento deste método de segurança, é necessário que ambas as partes tenham conhecimento de uma chave simétrica. No caso do modulo de rede, a chave encontra-se alocada numa zona de memória não acessível, onde só é permitido fazer leituras. Vai também no *frame* enviado, um número sequencial, de modo a que um atacante não consiga enviar uma mensagem antiga. O envio do *frame* é feito por frequências aleatórias, diminuindo assim a probabilidade do atacante o conseguir observar.

Como foi referido anteriormente, o modulo *Sigfox* não está sempre recetivo a mensagens. É necessário este tomar a iniciativa. Assim, o modulo não irá estar o resto do tempo recetivo a mensagens, algumas delas que podem ser do atacante.

Os *gateways* da *Sigfox* têm uma ligação ponto a ponto com a *cloud*, fazendo uso de uma VPN cifrada.

# Conclusão

Após o estudo sobre as duas principais tecnologias de comunicação no mundo dos IoT, concluísse que, apesar de serem ambas adequadas para o uso em IoT, cada uma tem as suas características únicas que as distingue.

Em relação ao tamanho da mensagem, a Sigfox é mais limitada no número de bytes que pode enviar. Tem, no limite, 12 bytes reservados para o payload, enquanto que o LoRaWAN tem reserva 51 bytes. Neste caso, esse limite pode trazer vantagens, dado que a nossa comunicação não irá conter muita informação, os 12 bytes são suficientes. Poderia ser tentador enviar mais informação, se não houvesse limite, no entanto, o consumo de bateria iria aumentar. No LoRaWAN a mensagem também poderá conter mais bytes no header, permitindo uma menor poupança da bateria.

Ambas as tecnologias têm em comum a topologia de rede, estando a principal divergência no tipo de serviço disponibilizado. O LoRaWAN permite uma maior customização do serviço, enquanto que o Sigfox só oferece um fixo. O serviço da Sigfox tem limitação no número de mensagens que se pode enviar num dia, enquanto que o LoRaWAN não impõe qualquer limite. Contudo, essa restrição não afetaria este projeto visto que os envios das mensagens têm uma grande periodicidade.

A tecnologia de informação que será usada neste projeto será o Sigfox. Na decisão, além das suas características, pesou também o facto de que este tem uma maior cobertura que o concorrente em Portugal continental. Segundo o site do Sigfox, existe uma cobertura do sinal em todo o Portugal continental, não implicando custos adicionais ao programador para conseguir estender esse sinal. Relativamente ao LoRaWAN, não foi possível averiguar uma entidade que tivesse uma cobertura tão abrangente como a do Sigfox.

# Periféricos

## Sensores Para Medir Distância

Para saber a quantidade de lixo que um contentor tem, é necessário ter um sensor que consiga saber a distância do lixo até à tampa. Para isso, foi pensado usar um sensor ultrassónico ou ótico. Estes são os mais usados no mercado para medir distâncias de objetos e como tal foi feito um estudo sobre estes dois.

Os sensores óticos, são sensores cujo o funcionamento baseia-se na emissão de um feixe de luz. Existem três tipos de sensores óticos: i)Barreira, ii)Difuso e iii)Refletivo. O que iriamos usar é um de difusão. Neste caso, o sensor envia um feixe, este é refletido no primeiro objeto que entra em contacto, e o sensor recebe novamente esse feixe. A distância do sensor ao objeto é a metade do tempo que o sinal demorou a regressar vezes a velocidade da luz.

(Formula)

Estes tipos de sensores têm uma enorme precisão permitindo um calculo da distância mais consistente.

Um sensor ultrassônico é um dispositivo que permite medir distâncias de objetos através da emissão de ultrassons. Este, envia um ultrassom, que é refletido pelo o primeiro objeto enviado de volta para o dispositivo. Usando a mesma formula apresentada anteriormente (substituindo a velocidade da luz pela a velocidade do som) é assim possível saber a distância do objeto. O uso de ultrassons para o calculo de distâncias é ótima quando existe a probabilidade desses objetos poderem ser transparentes, visto que os objetos transparentes continuam a refletir o som, e existir poeiras no ar, onde o ultrassom não é afetado por este.

Um problema que pode causar o uso deste sensor é se houver materiais que tenham propriedades absorventes de som. Isto poderia causar um erro na obtenção da distância deste objeto.

Depois desta reflexão, foi escolhido o uso de um sensor ultrassônico. Esta escolha deve-se ao ambiente em que o sensor irá se colocado (um contentor), um ambiente onde poderá existir poeiras ou materiais transparentes que dificultam a medição da distância num sensor ótico.

## Sensor de temperatura

Devido à otimização que é realizada na recolha de lixo, existem contentores que poderão não ser recolhidos em mais de uma semana (se este mantiver o seu volume de lixo abaixo do treshold). Isto levanta problemas de salubridade. Para resolver tal problema, decidiu-se colocar com o sistema embebido um sensor que consiga medir a temperatura. (Não sei se o tiago fala do processo da fermentação do lixo).

Uns dos requisitos para escolha deste, foi o seu baixo custo (é só uma demonstração de ideia), o meu de comunicação fosse digital (se fosse analógico seria necessário realizar um conversor, algo que iria tronar o código do sistema embebido mais verboso) e por fim que aguenta-se altas temperaturas (um contentor, no verão pode chegar aos 50ºC). Assim o sensor escolhido foi e DS18B20+ digital thermometer porque tem todas as propriedades referidas anteriormente.