IOT – INTERNET DAS COISAS

AULA 1

Prof. Gian Carlo Brustolin

CONVERSA INICIAL

Conheceremos uma tecnologia que tem apresentado evolução vertiginosa em aplicações e tecnologia. O uso da expressão Internet das Coisas ou IoT (*Internet of Things*, em inglês) é reputado a Kevin Ashton, cientista idealizador da padronização de RFID, em uma conferência em 1999, mas a exata definição de IoT, até o momento em que concluímos esta publicação, ainda é lacunosa e, como recurso, feita por exclusão.

Intuitivamente, imaginamos IoT como pequenos objetos relativamente autônomos conectados com a internet. Essa aproximação parece nos bastar inicialmente, embora não resista a questionamentos básicos. Por exemplo, a partir dessa definição intuitiva, podemos afirmar que televisões inteligentes ou mesmo *palmtops* são objetos IoT? Parece-nos que sim, mas de fato não o são.

A nossa dificuldade em estabelecer os limites entre objetos IoT e outras eletrônicas inteligentes não impedem, obviamente, a proliferação constante desses objetos. Essa verdadeira invasão eletrônica não se dá, entretanto, pacificamente, conforme afirma Brustolin (2022),

> a profusão de entidades ligadas à internet gerou alguns problemas clássicos como a questão do endereçamento, a princípio resolvido pelo IPV6, mas também alguns problemas inusitados, como a necessidade de conexão sem fio de pequenos entes computacionais, sem alimentação externa, de forma segura, sem configurações e de operação simplificada. Esta combinação de requisitos e exigências torna a flexibilidade de projeto bastante baixa e a seleção de protocolos viáveis bastante estrita.

Nesta etapa, considerando a necessária associação, por vezes, dicotômica entre objetos IoT e sua conectividade, abordaremos os fundamentos desses objetos, a exemplo da arquitetura básica de *hardware* e *software*, bem como os conceitos gerais de alguns protocolos de comunicação voltados a esses objetos.

No decorrer desta caminhada, veremos como esses objetos nos auxiliam em aplicações residenciais, comerciais e industriais, facilitando a aquisição de dados e a operação de máquinas, desde o acionamento remoto da refrigeração de sua casa até o controle de maquinário agrícola autônomo.

Mergulharemos também no interessante tema das cidades inteligentes indistintamente fundido com a Internet das Coisas. Não nos furtaremos ao conhecimento das soluções de conectividade para IoT, posto que tais soluções

são substancialmente diversas daquelas para redes tradicionais de computadores. Estudaremos, também, o temerário tema de segurança que assola a todos os projetistas e usuários dessa tecnologia. Desta forma, ao final desta caminhada, você terá uma visão técnica geral de IoT, conhecendo suas aplicações e desafios. Vamos, então, dar início a este empolgante estudo.

TEMA 1 – INTRODUÇÃO À IOT

Você provavelmente está imaginado que, levando em conta a tradução literal do termo IoT (*Internet of Things*, em inglês), o estudo da Internet das Coisas deveria ser um estudo de redes ou de conectividade para "objetos". Se você pensou assim, não está errado, em parte, ao menos. Podemos dizer que do ponto de vista *stricto*, IoT estuda somente a conexão de eletrônicas à internet, neste sentido, podemos citar Santos et al, 2016, p. 2:

> A Internet das Coisas, em poucas palavras, nada mais é que uma extensão da Internet atual, que proporciona aos objetos do dia a dia (quaisquer que sejam), mas com capacidade computacional e de comunicação, se conectarem à Internet. A conexão com a rede mundial de computadores viabilizará, primeiro, controlar remotamente os objetos e, segundo, permitirá que os próprios objetos sejam acessados como provedores de serviços. Estas novas habilidades, dos objetos comuns, geram um grande número de oportunidades tanto no âmbito acadêmico quanto no industrial.

Este conceito estrito precisa ser, entretanto, ampliado, englobando também os objetos inteligentes ou, ao menos, a eletrônica que confere essa inteligência a máquinas e sensores, por motivos que analisaremos em seguida.

1.1 Um pouco de história

A origem da IoT está ligada à automação industrial. As redes de sensores e atuadores industriais eram inicialmente conectadas entre si (e à rede de computadores da indústria) por protocolos proprietários de cada fabricante. Essas soluções, embora robustas e funcionais, padeciam de interoperabilidade entre fabricantes. Se a empresa adquirisse maquinário dotado de sensores/atuadores próprios, haveria necessidade de desenvolver um *gateway* de interconexão entre a rede legada e a nova máquina. Este era um trabalho de engenharia complexo, caro e demorado.

Essa realidade motivou numerosos estudos sobre interoperabilidade de redes no ambiente industrial e já várias alternativas consolidadas existem. São redes das quais se exige a operação segura, em ambientes agressivos e insalubres, com foco considerável em redução de custos, concomitante à resiliência da operação (Automation, 2011).

O compromisso entre segurança e baixo custo levou à busca de padrões, não apenas para a interconexão entre redes de sensores/atuadores, mas também para os próprios sensores/atuadores (aos quais passaremos a designar “objetos” ou “dispositivos” indistintamente).

A partir desse ponto, o estudo das redes de objetos, e dos próprios objetos, se tornou indivisível. Dotar um objeto de capacidade de conexão com protocolos genéricos, de alta complexidade (para permitir a operação sem falhas), exigiu o aporte de certa capacidade de processamento (ou inteligência) nos objetos. Uma vez que essa inteligência foi embarcada, mais usos pode-se fazer dela, a exemplo do pré-processamento de dados ou tomada de decisões elementares.

A possível interoperabilidade dos protocolos e o baixo custo dos objetos inteligentes propiciou a extrapolação das fronteiras industriais, com aplicações comerciais em residências, prédios, agricultura e em áreas públicas. Muito provavelmente, neste salto, passamos a denominar a essa tecnologia pelo adágio atual, IoT.

Neste ponto, estamos preparados para tentar, se não uma definição, ao menos um conceito lógico de IoT.

1.2 Conceito de IoT

Podemos aceitar, sem nos comprometermos com o erro, a ideia de que IoT envolve objetos eletrônicos, dotados de certa autonomia ou inteligência, conectados a uma rede que lhes permite contatar, ou serem contatados, por outros objetos. Desta forma, nosso conceito de IoT engloba não só a conectividade, mas também os objetos. Esquematicamente, podemos representar o conceito como dois macroblocos: o objeto inteligente e a interconexão desse objeto à rede, como apresentado a seguir.

Figura 1 – IoT como Conectividade + Objeto

Essa representação nos reporta a uma célula na qual o núcleo é formado pela inteligência do objeto, e a membrana celular, pela conectividade. Essa analogia é útil uma vez que toda informação externa chega ao objeto através das facilidades de conexão, da mesma forma que os dados coletados pelo objeto são transmitidos em sentido inverso.

Considerando essa dicotomia homogênea, entre objeto e conexão, podemos estudar IoT segundo essas duas aproximações. Por um lado, precisamos entender os objetos, eletrônicas que foram desenvolvidas para permitir o acesso de baixo custo ao controle ou memória de máquinas. De outro lado, estará a própria conexão composta por protocolos que garantam a conectividade segura desses objetos.

Vamos, a seguir, conhecer de maneira genérica, essas duas tecnologias para, posteriormente, mergulhar, nos capítulos seguintes, em alguns detalhes técnicos essenciais para a compreensão da tecnologia como um todo.

TEMA 2 – CONECTIVIDADE DA IoT

Ao tratarmos do tópico de conectividade de objetos inteligentes, nossa imaginação se vê roteada, involuntariamente, para os conceitos de redes tradicionais de computadores, protocolos padronizados e estruturas clássicas de conexão com a internet. A conectividade IoT é um tema mais amplo, entretanto,

visto que engloba outras formas de interligação entre dispositivos, diversas do tradicional TCP/IP.

Segundo Ideali (2021, p. 8), a conexão entre objetos e sua inteligência, seja embarcada no objeto (microcontroladores) ou dispersa na borda (*edge e fog computing*) ou internet (*cloud computing*), é hoje o maior desafio técnico da conectividade. Isto se deve a exigências bastante particulares de protocolos e técnicas de interconexão para IoT.

É importante comentarmos que as soluções de conectividade para esses objetos ainda não estão plenamente sedimentadas, ou seja, não há um protocolo, ou mesmo tecnologia, padrão de interconexão do objeto com a rede local ou internet. Assim, nosso estudo precisará contar com certezas tênues, e uma boa dose de incertezas.

Em outro momento, descreveremos alguns padrões de rede de sucesso, usados em sistemas de sensoriamento ou acionamento industrial, bem como protocolos ainda em fase de implementação ou testes. Para o momento atual, nos bastará apresentar conceitos das redes de atendimento aos objetos IoT que subsidiarão os futuros estudos.

Podemos estudar a conectividade a uma rede qualquer sob duas ópticas: física ou lógica. Do ponto de vista físico, percebemos duas classes distintas de tecnologias: com o uso de cabeamento (*wired*, em inglês) ou sem ele (wireless). Do ponto de vista lógico, enxergaremos a conectividade através dos protocolos, ou algoritmos, que tratam os dados circulantes pela interconexão, dando-lhes, ao menos, maior robustez e resiliência.

Ao ler este parágrafo, você se lembrou das camadas de redes OSI? Sim, aqui estão elas novamente. A camada física congrega as interfaces eletrônicas de conexão com o meio, que, como comentamos anteriormente, podem ser fiadas ou não. Todas as demais camadas OSI são lógicas, ou seja, códigos computacionais. Um protocolo pode envolver apenas a camada de enlace, logo acima da camada física, ou subir na pilha, estabelecendo padrões para as camadas superiores de rede, transporte etc.

Antes de tratar esse aspecto lógico, vamos descrever resumidamente as possibilidades de conectividade física.

2.1 Conectividade física com fio

A conectividade para objetos IoT nasceu com essa interface nativa. Essa escolha histórica se deu pela maior resiliência das soluções cabeadas às interferências eletromagnéticas e à agressividade do meio industrial. O robustecimento das redes sem fio, já antes da metade da década de 2010, iniciou, entretanto, um processo irreversível de mudança dessa escolha natural pelas interfaces fiadas. Sensores sem fio são economicamente mais viáveis do ponto de vista de implantação e manutenção em relação a seus antecessores cabeados (Ko *et al*., 2010).

Do ponto de vista de redes industriais, o uso de cabeamento, mormente óptico, permanece como alternativa de projeto, para conectividade em determinadas condições altamente agressivas, principalmente por sua imunidade à intensa interferência eletromagnética (IEM) presente nas linhas de produção. Quando limitações mecânicas impedem o uso de cabos ópticos, cabos coaxiais são utilizados como alternativa viável.

Para objetos inteligentes com aplicações fora desse ambiente, redes fiadas têm aplicação cada dia mais restrita. Algumas placas para IoT ainda apresentam interfaces para cabeamento metálico, disponibilizando conectores RJ45 ou USB, normalmente com foco na configuração inicial ou como alternativa de segurança. Os protocolos de comunicação adaptados para camadas físicas ópticas ou metálicas coaxiais são variados e, por estarem restritos a aplicações industriais, não serão objeto de nosso estudo aqui.

2.2 Conectividade sem fio

A conectividade sem fio é, sem dúvida, a opção mais frequente nas aplicações de objetos IoT de uso geral. Soluções não cabeadas utilizam majoritariamente radiopropagação, mas o uso de pulsos de luz é uma solução sem fio alternativa ao uso de rádio. A interface IrDA (*Infrared Data Association*), que utiliza luz infravermelha para transmissão de dados entre duas fontes próximas, é o exemplo mais frequente.

Como a solução, sem uso de radiofrequência, implica em certa proximidade restritiva, a opção por radiocomunicação é preponderante na conectividade de objetos IoT.

Em função da aplicação do objeto IoT e das condições do meio no qual ele se insere, a solução de conectividade pode variar substancialmente. Objetos

destinados ao agronegócio, como sensores de características de solo ou válvulas atuadoras de irrigação, demandam sistemas de comunicação independentes da cobertura das operadoras de telecomunicações, de baixo consumo de energia e alta resiliência.

Figura 2 – Pecuária de precisão com uso de sensores conectados

Crédito: Ruslan Zagidullin/Shutterstock.

Objetos móveis, a exemplo de sensores de veículos autônomos, por sua vez, necessitam de protocolos de comunicação capazes de tratar convenientemente a mobilidade, fornecendo conectividade ubíqua. Soluções de IoT, para uso em residências unifamiliares e prédios, demandam conectividade de baixo custo, simples e padronizada.

Podemos citar as LPWANs (tecnologias de radiopropagação de bom alcance, baixo consumo de energia e taxas de transmissão baixas), a exemplo de LoRa e Sigfox, como ideias para atendimento a objetos IoT voltados ao agronegócio.

Para permitir a operação em mobilidade, há soluções disponibilizadas pelas operadoras celulares, como NB-IoT, LTE-M, CAT NB e EC GSM, cada

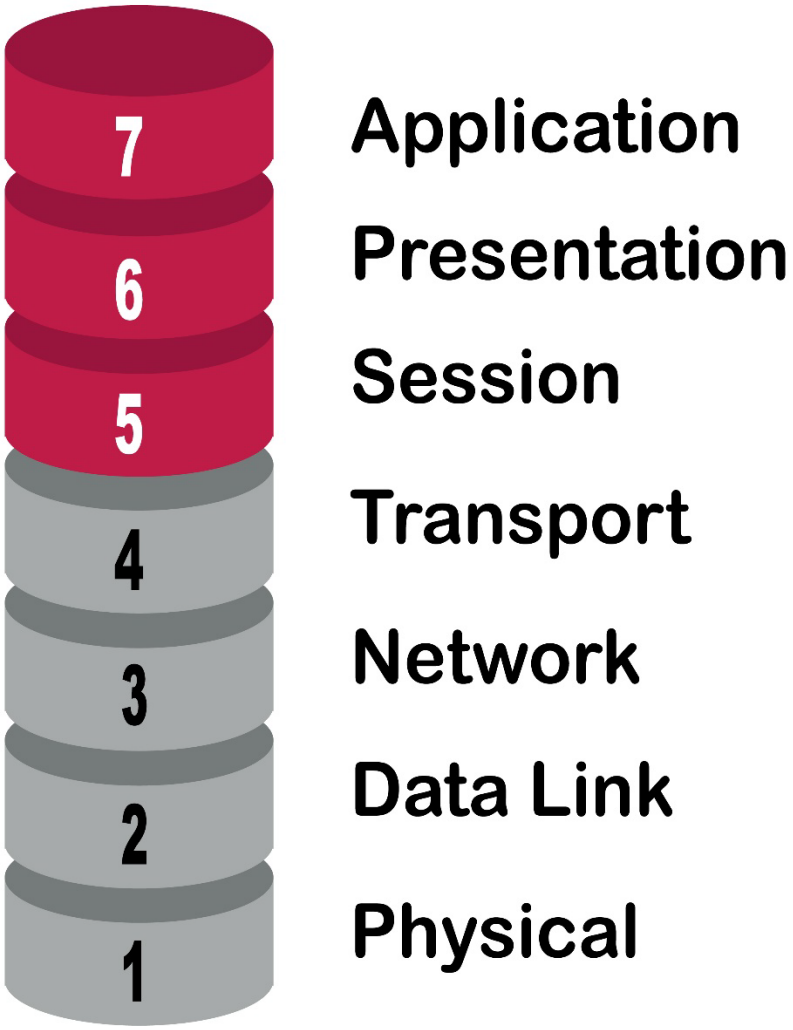
padrão operado em determinadas gerações de equipamentos celulares ou em todas as gerações celulares, a exemplo do CAT NB. Essas soluções não privadas, com uso de redes celulares, entretanto, não são boas para suporte de aplicações em residências e prédios para os quais WiSUM parece ser mais adequado.

Em outro momento, voltaremos a abordar cada grupo de tecnologia com o necessário aprofundamento. Para subsidiar esse futuro estudo, vamos, a seguir, revisar os conceitos de camadas de redes.

De forma a darmos foco naquilo que efetivamente utilizaremos neste curso, abandonaremos o modelo OSI clássico, representado a seguir, para nos focarmos nas duas primeiras camadas, nas quais os padrões de conectividade para IoT diferem das demais estruturas de redes.

Esta análise, de parte da pilha OSI certamente, não lhe é estranho. Quando você estudou o protocolo de rede IP e seu par TCP, particionou-se a pilha na camada de transporte.

Figura 3 – Modelo OSI clássico de 7 camadas



Crédito: Game art assets/Shutterstock.

Antes de iniciarmos a descrição das particularidades das duas primeiras camadas, com foco nas redes para IoT, vamos repassar o conceito de protocolo para que não pairem dúvidas sobre sua definição.

Um protocolo é um padrão de comunicação entre máquinas computacionais conectadas. Esse padrão divide os dados a serem trocados em segmentos predefinidos, ao quais designamos quadros (ou frames, em inglês). Estes quadros, possuem, ao menos, um cabeçalho de controle, endereços de origem e destino, dados úteis e indicador de fim de quadro (Ideali, 2021, p. 26).

Como já aprendemos em nossos estudos de redes de computadores, cada camada possui seu protocolo próprio e independente, desta forma, podemos falar em protocolo da camada física (que normalmente é designado pela sigla PHY) ou protocolo da camada de controle de acesso ao meio (MAC), por exemplo.

2.3 Camada física (PHY)

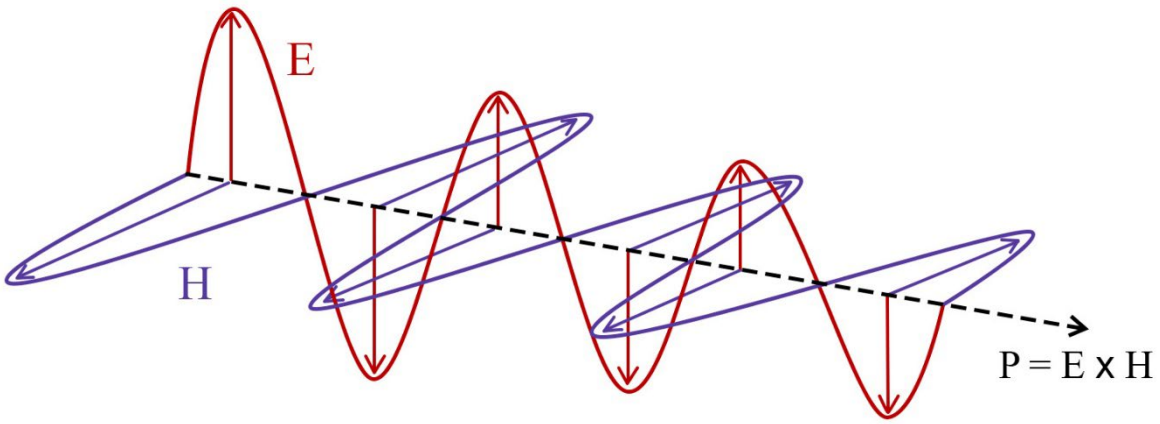
O protocolo da camada física contém os padrões de interface com o meio. No caso da interface sem fio, que nos interessa para o estudo de IoT, esse protocolo descreverá a solução técnica de radiopropagação. Em outro momento, aprofundaremos um pouco mais esse assunto sem descer aos complexos detalhamentos técnicos mais atinentes à engenharia de telecomunicações. Por hora, nos bastará uma breve conversa sobre radiocomunicação.

O uso de redes sem fio se tornou um fato corriqueiro em nossas vidas e, normalmente, não percebemos sua presença e nem nos detemos para meditar sobre sua natureza. Quando refletimos, entretanto, sobre o funcionamento de um enlace de rádio, é impossível não nos impressionarmos com a "magia" científica envolvida. Como a eletrônica é capaz de codificar a informação em pulsos elétricos e, em seguida, transmiti-los por um meio esparso como o ar ou vácuo?

O entendimento das ondas eletromagnéticas (OEM) nos permitirão explicar esse processo. Uma OEM é uma emissão de energia, composta, como se supõe, pelo nome da associação de uma oscilação elétrica e outra magnética.

Quando associamos campos oscilantes elétrico e magnéticos, como ilustrado a seguir, a energia assim composta ganha a possibilidade de propagar-se pelo espaço.

Figura 4 – Oscilação eletromagnética



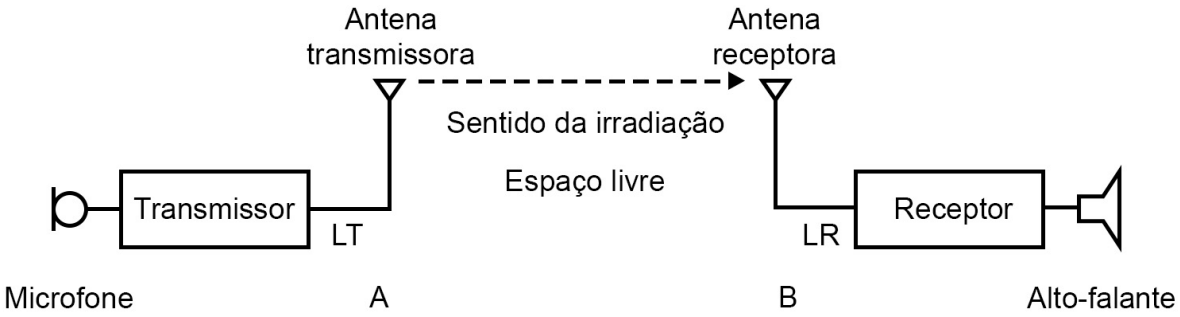
Crédito: Ramos, 2016.

De fato, o que um rádio transmissor faz é tomar uma onda senoidal pura, de frequência constante (dita onda portadora) e realiza alterações em seu formato, frequência ou fase. Essas alterações são controladas pelo sinal que desejamos transmitir.

A onda alterada (dita modulada) será então expulsa do meio metálico, onde foi gerada, para o espaço exterior através de um transdutor. Esse transdutor, que chamamos de antena, permite que a oscilação modulada seja liberada para o meio externo. A antena direciona o feixe oscilatório e dá a ele o ganho necessário para que atinja a antena de recepção.

No receptor, a antena receptora converterá a OEM captada no espaço livre para uma oscilação elétrica. A eletrônica do rádio, então, decodificará as alterações feitas na onda portadora, obtendo, finalmente, o sinal que desejávamos transmitir. As primeiras aplicações de rádio objetivavam a transmissão de sinais de voz analógicos. O diagrama a seguir ilustra um rádio enlace de voz.

Figura 5 – Radio enlace



Crédito: Medeiros, 2016, p. 99.

A transmissão sem fio de sinais digitais, ou seja, de dados binários, é, em essência, muito semelhante às transmissões analógicas que descrevemos. Acrescenta-se apenas um estágio que ajuste os dados binários às necessidades do modulador e a transmissão se dará da mesma forma que vimos anteriormente.

Transmissões digitais, entretanto, são mais flexíveis que as analógicas em relação a seu sequenciamento temporal. Podemos perder parte do trem de *bits* transmitido sem que isso implique em perda de inteligibilidade da comunicação, bastando solicitar seu reenvio. Essa flexibilidade permite a criação

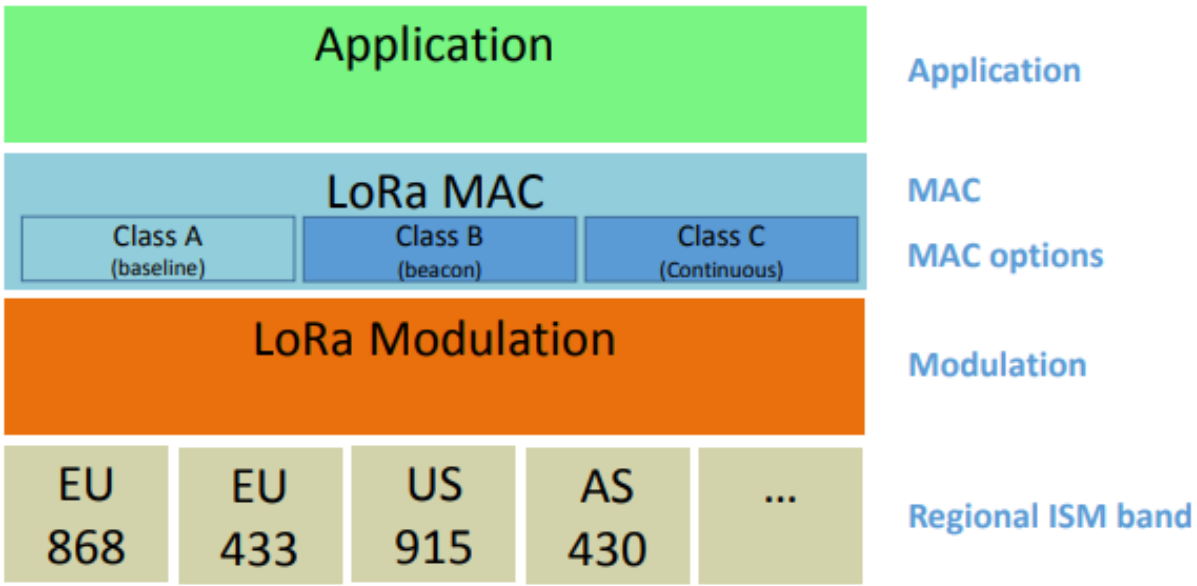
de técnicas de modulação avançadas, altamente resilientes, com alto aproveitamento do espectro de transmissão, propícias para o uso em sensores e atuadores IoT.

2.4 Camada de Controle de Acesso ao Meio (MAC)

A camada MAC, como já adiantamos, tem a função de conformar os dados coletados do meio para que a rede possa acessá-los, ordenadamente e de forma padronizada.

A figura a seguir ilustra a presença da camada MAC para o padrão LoRa de conectividade. Nesta figura, a camada de aplicação é empilhada sobre a MAC, simbolizando a presença de uma aplicação de controle, que normalmente se encontra na nuvem computacional ou em uma máquina remota.

Figura 6 – Camadas de rede para o padrão WAN



Crédito: Lora, 2017.

A camada MAC envelopa os dados, incluindo o controle do frame (preâmbulo e fim de quadro), endereço do objeto, seção (caso o objeto seja multifuncional), controle de erros do quadro e informações de controle do protocolo. Terminado esse processo, os dados são convertidos em binário (se ainda não o são) e entregues a camada PHY para transmissão.

Na camada física, os dados, empacotados pela MAC, são seccionados em tamanhos adequados ao meio de transmissão, ganham novo cabeçalho e, finalmente, passam pela modulação.

Voltaremos a esses conceitos aprimorando-os, quando descrevermos uma das interfaces mais comuns de conexão para objetos IoT de uso comercial, o WiFi.

TEMA 3 – ARQUITETURA INTERNA DOS OBJETOS IOT

Em nosso conceito de IoT, introduzimos a ideia da dicotomia entre conectividade e o objeto IoT. Estudamos, então, brevemente, a conectividade. Neste tópico, descreveremos os objetos IoT.

Podemos dizer que há objetos IoT próprios e impróprios. Os primeiros são aqueles objetos criados especificamente para a utilização em IoT. Esses objetos embarcam, nativamente, a inteligência necessária e as interfaces de comunicação apropriadas. Há, entretanto, outros, impróprios, que nascem do acréscimo voluntário de inteligência e conectividade.

Esses últimos são na verdade eletrônicas de controle de máquinas que receberam uma **placa para IoT**, que viabiliza a conexão à rede. Por esta via, objetos de uso cotidiano, como fechaduras eletrônicas, máquinas de lavar, equipamentos de refrigeração e interruptores elétricos, podem ser conectados “diretamente” à internet para que possam ser controlados a distância.

Tanto objetos próprios quanto impróprios têm uma arquitetura construtiva (interna) muito semelhante, a qual discutiremos a seguir, para depois nos debruçarmos sobre a arquitetura externa, em nosso próximo tópico.

3.1 Arquitetura interna

A arquitetura construtiva, do *hardware*, de um objeto IoT é comumente denominada arquitetura interna. Essa denominação tem por objetivo distinguir esse desenho daquele outro que engloba a conectividade e a eventual partição da inteligência com a nuvem.

Para que um objeto seja capaz de conectar-se a uma rede ou à internet, será necessária uma arquitetura de controle e atuação, ao menos, elementar. Trata-se de uma estrutura eletrônica interna ou arquitetura interna, que permita

a conexão com a rede, além de certa inteligência local. Essa inteligência facultará o sensoriamento ou a atuação do objeto no meio, tratando convenientemente o protocolo de comunicação, em ambos os sentidos.

Santos *et al*. (2016) divide a arquitetura interna em seis blocos funcionais (veja figura a seguir): comunicação, identificação, semântica, computação, sensores e atuadores (serviços). Por se tratar de blocos funcionais, podem ser, do ponto de vista eletrônico, agregados em um único ou em vários componentes eletrônicos.

Figura 7 – Blocos funcionais da arquitetura interna

3.2 Blocos funcionais da arquitetura interna

A clara definição de IoT, como já comentamos, é ainda lacunosa, desta forma, a definição dos objetos inteligentes que se conectam à rede também o será. Apesar dessa nossa falta de precisão teórica, é possível definir algumas características de desenho, necessárias à operação de um objeto IoT. A esta coleção de características, denominaremos arquitetura interna do objeto.

Seguindo o proposto por Santos *et al*. (2016), podemos dividir a arquitetura interna em seis blocos funcionais. Naturalmente, dada a aplicação do objeto, alguns blocos podem estar ausentes. Vamos, então, descrever cada possível bloco, iniciando por aqueles essenciais a um objeto IoT.

O bloco essencial de **Computação** controla os demais blocos do objeto, contém seu código fonte e determina a função do objeto. Esse bloco define quais os objetos próprios e impróprios, que antes comentamos. Todo objeto IoT deve possuir certa inteligência que permite tratar os protocolos complexos de comunicação e controla a atuação do objeto no meio.

O **bloco de serviços ou atuação** permite a ação do objeto no meio. Trata-se da eletrônica de controle do objeto. Tome o exemplo de um objeto impróprio: imagine uma máquina de lavar roupa que recebeu uma placa de IoT, a eletrônica de controle (bloco de atuação) é nativa a esse objeto. A placa IoT apenas agrega o bloco de computação e comunicação. Neste caso, a computação extrai, dos dados presentes nos *frames* do protocolo de comunicação, os comandos de operação e comanda a eletrônica de controle da máquina de lavar, como você faria se a operasse presencialmente.

O **bloco de sensores**, por outro lado, nos permite ler informações do meio que serão empacotados pelo bloco de computação e enviados para a conexão com a rede. Retomando o exemplo da máquina de lavar à qual conectamos uma placa de IoT, podemos querer receber informações sobre a fase de execução de uma lavagem, o bloco sensor será responsável por adquirir esses dados e disponibilizá-los para a computação.

Certamente, podemos imaginar objetos que possuam apenas um desses dois blocos anteriores. Um barômetro, por exemplo, pode ter apenas a função de sensor de pressão atmosférica em dado local, sem que nenhuma ação seja a ele associada. Desta forma, os blocos de atuação e serviços podem coexistir, ou não, em um mesmo objeto, mas ao menos um desses blocos é essencial à existência do objeto.

O **bloco de comunicação e de identificação** não será aqui descrito, uma vez que corresponde à parte da conectividade IoT, realizada pelo objeto. Já dedicamos todo um tópico anterior à conectividade, incluindo a descrição desse bloco. Neste ponto, basta citarmos que a conectividade é um bloco essencial a todo objeto IoT.

O **bloco "Semântica"** refere-se aos algoritmos de tratamento dos dados obtidos pelos sensores. Esses algoritmos podem estar ausentes em muitos objetos, principalmente nas versões iniciais e nas eletrônicas mais econômicas. Eles permitem a extração de conhecimento das informações colhidas, ou seja, realizam um pré-processamento dos dados, transmitindo somente a fração desses dados que possuam informações, ou alterando os dados, de forma a agregar-lhes valor.

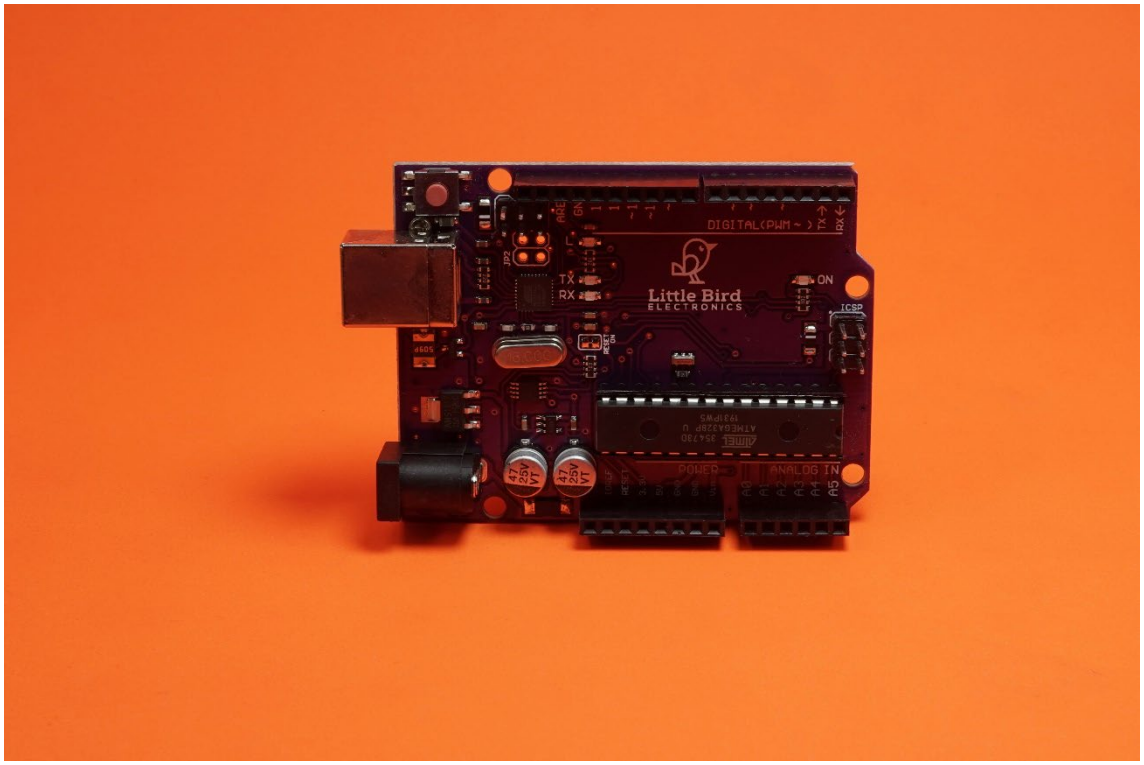
Para exemplificar o que afirmamos, imagine uma câmera de vídeo de segurança. Se esse objeto não possuir o bloco de semântica, transmitirá as imagens captadas continuamente para a rede, ocupando banda e limitando a capacidade da rede. O bloco de semântica poderá interpretar a imagem, enviando apenas quadros alterados, ou seja, a rede só será acessada para transmitir alterações da imagem.

Neste exemplo, a semântica está selecionando os dados que contém informações. Podemos imaginar uma semântica ainda mais complexa: suponha que equipemos o objeto com uma pequena rede neural capaz de identificar silhuetas humanas. Agora, as transmissões não contêm apenas informações, mas informações valoradas pela inteligência semântica.

Talvez você esteja se questionando o porquê de esse bloco não ser parte integrante do bloco de computação. Esta, de fato, é uma discussão teórica válida. A literatura científica tem preferido dividir computação e semântica, como blocos distintos dos objetos IoT, posto que todos os objetos devem possuir o bloco de computação. O bloco de semântica, por sua vez, não é essencial, sua existência é benéfica para desonerar o tráfego de rede ou mesmo para reduzir o processamento de nuvem, mas não é impositiva, na maioria dos casos.

Por outro lado, voltando aos objetos impróprios, a placa IoT, associada por nós ao sistema de controle, antes presente no equipamento, não complementará apenas as funções de gerenciamento e conectividade, mas, eventualmente, acrescentará capacidade semântica à supervisão do objeto. Na figura a seguir, temos um exemplo de placa para IoT, a famosa Arduino Uno.

Figura 8 – Placa para IoT Arduino (Uno AT mega 328)



Crédito: Hendrik Sejati/Shutterstock.

Certamente, você está curioso quanto às placas IoT, voltaremos a elas em breve, vamos agora comentar sobre a arquitetura lógica para que, em seguida, possamos examinar a arquitetura externa dos objetos.

3.3 Arquitetura Interna Lógica

Como já sabemos, um mesmo objeto pode ter blocos de sensores e atuadores. Também é possível imaginarmos dispositivos com mais de um sensor ou mais de um atuador. Examine o exemplo de um sensor de temperatura e umidade, como ilustrado a seguir. Neste caso, há dois sensores em um único objeto.

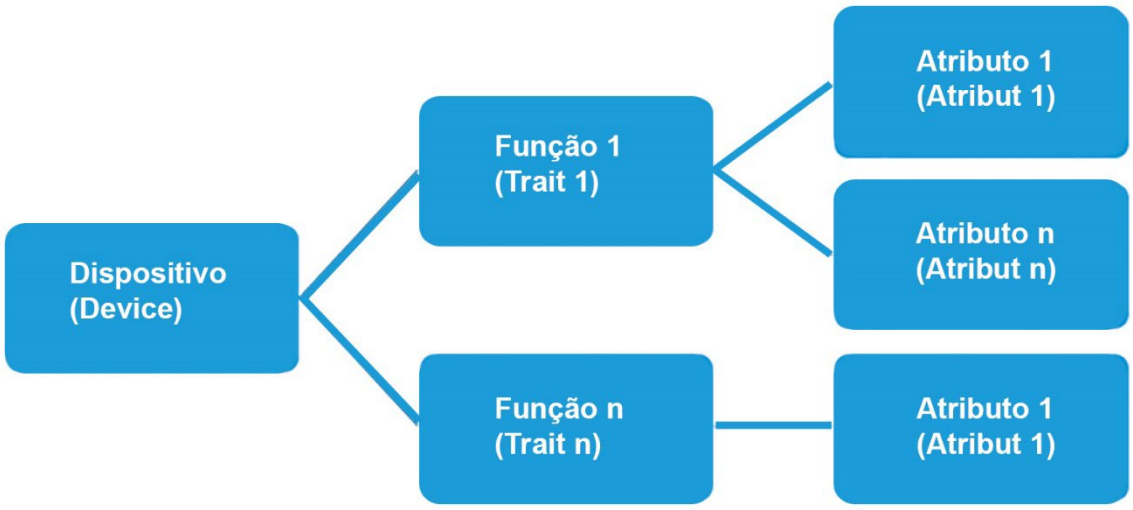
Figura 9 – Sensor de temperatura e pressão

Crédito: Jerome Quek/Shutterstock.

Do ponto de vista de arquitetura de HW e funcional trata-se de um sensor apenas, mas, para que possamos endereçar cada dado individualmente, será necessário o conceito de arquitetura lógica.

A arquitetura lógica de um objeto IoT é bastante simples, basta segregarmos em uma camada o dispositivo (*device*) e abaixo dela uma camada com as funções do objeto (*traits*, em inglês, por analogia à programação) e finalmente os atributos de cada função (*atributs*).

Figura 10 – Arquitetura lógica



Crédito: Gian Carlo Brustolin.

Desta forma, para o exemplo da Figura 9, anterior, teríamos o dispositivo com duas funções: termômetro e barômetro. A função termômetro pode ter

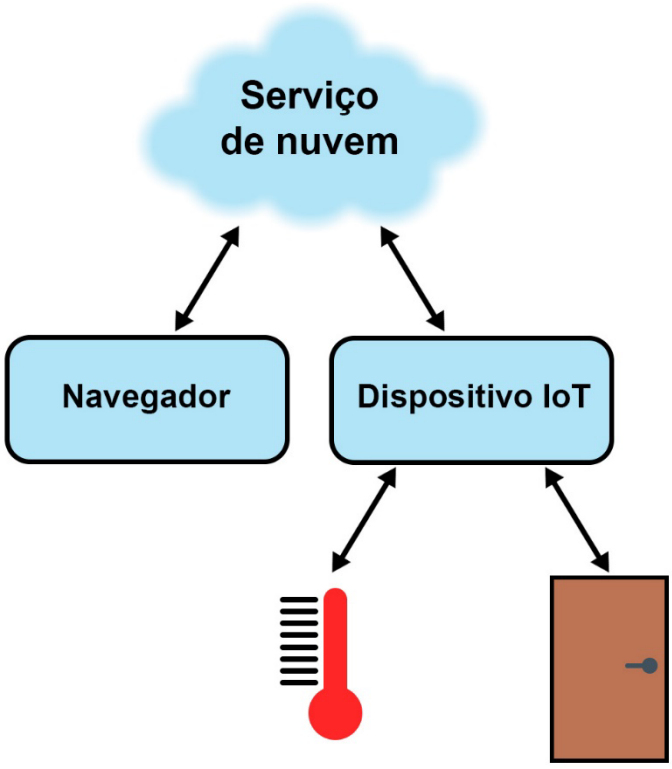
atributos como forma de medida (média horária, por exemplo) e unidade (Celsius ou Fahrenheit).

TEMA 4 – ARQUITETURA EXTERNA DOS OBJETOS IOT (IoT-A)

Já sabemos que um objeto IoT, necessariamente, embarca certa inteligência (semântica ou não), conectividade com a rede e capacidade de sensoriamento e/ou atuação. O custo de um objeto está substancialmente ligado à sua capacidade de processamento local.

Objetos simples, como lâmpadas, ventiladores ou fechaduras, precisam de eletrônicas mais espartanas e baratas, para que sejam comercialmente viáveis. Colocar parte do processamento em aplicações externas, como ilustrado a seguir, é uma solução que permite essa restrição econômica.

Figura 11 – IoT conectado a serviços de nuvem



Crédito: Monk, 2018.

Essa solução implica no vínculo do objeto, não só com sua arquitetura interna, mas com uma macroarquitetura que também contemple sua conexão e

as facilidades de processamento externas. Essa macroarquitetura é denominada IoT-A.

De forma genérica, pode-se pensar a **IoT-A como composta por três camadas: percepção, rede e aplicação**. Na camada de percepção, estariam os objetos inteligentes. Dispositivos de roteamento e *gateways* comporiam a camada de rede, ao passo que as aplicações de controle e análise de dados determinariam a última camada.

Essa IoT-A simplificada pode ser útil em algumas aproximações mais genéricas, a exemplo da definição de uma estratégia de segurança, mas será insuficiente quando desejamos entender a tecnologia de forma mais profunda.

Maschietto *et al*. (2021, p. 62 e seguintes) propõe modelos compostos por camadas funcionais que examinaremos a seguir. Antes de iniciarmos, entretanto, será útil conceituarmos superficialmente o que o autor chama de *midleware*.

Esse conceito não é exatamente uma novidade, sempre que se faz necessário interconectar uma aplicação de nuvem a distintos sistemas operacionais, é necessária a presença de um tradutor intermediário, dito *middleware* (Red Hat, 2021). O mesmo se aplica a soluções para IoT, dada a grande variação entre as implementações de HW e SW envolvidas.

Maschietto parte de um modelo de três camadas, cada acréscimo de camada, a partir dessa arquitetura básica, retira do objeto IoT parte de sua eletrônica, simplificando-o e, consequentemente, reduzindo seu custo. Esse ganho somente se justifica em soluções de escala, ou seja, acrescentar camadas externas a uma coleção de objetos IoT, só tem sentido econômico se a coleção for numerosa.

4.1 IoT-A de três camadas – *Front-Loaded*

Quando poucos objetos estão presentes em uma rede, um modelo de três camadas é mais eficiente. Neste caso, o objeto conterá todos os blocos funcionais, descritos anteriormente, embarcados. Nesta arquitetura, também chamada *front-loaded*, o dispositivo conecta-se diretamente a uma rede de transporte (a exemplo da TCP) e, posteriormente, a de aplicação, presente na rede ou a ela conectada, como ilustrado a seguir.

O primeiro modelo, IoT-A de três camadas, presume a presença do *gateway* de comunicação na eletrônica embarcada dos objetos. Serão objetos de maior custo, porém de alta flexibilidade e facilidade de uso.

Figura 12 – IoT-A de três camadas

Crédito: Elaborada com base em Maschietto *et al.*, 2021, p. 62.

Este modelo também permite estruturas de comunicação em mesh para atendimento de redes de sensoriamento mais amplas, como no caso de sensores e atuadores para agricultura de precisão. Neste caso, além da comunicação direta, existe a possibilidade de comunicação entre dispositivos a arquitetura *front loaded* recebe a segunda denominação de *smart client*.

Nestas aplicações, embora a quantidade de sensores indique o uso de uma arquitetura com mais camadas, a complexidade imposta pelas dificuldades de comunicação exige a presença de um *gateway* no dispositivo para processar o protocolo de comunicação. WMN (*Wireless Mesh Network*) são redes nas quais os objetos (ditos nós) são capazes de autoconfiguração, assumindo, quando necessário, a capacidade de gerenciamento e roteamento (Akyildiz *et al.*, 2005) dotando a rede de alta resiliência.

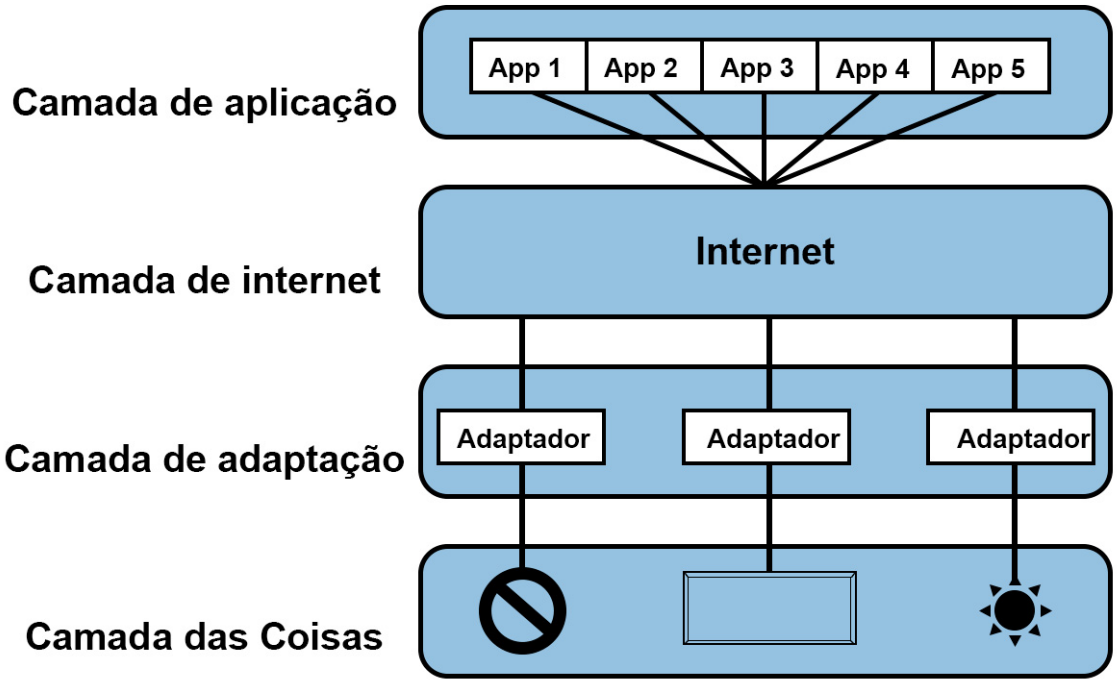
Neste modelo arquitetônico de três camadas, o processamento local, no objeto, pode conservar vários níveis de complexidade, mas sempre dependerá do controle realizado em máquina externa, como em todas as arquiteturas IoT.

4.2 IoT-A de quatro camadas – *Spoke-hub*

Como acabamos de ver, o modelo de três camadas exige uma eletrônica de certa autonomia, residente no objeto. Para soluções compostas de grande número de objetos, em operação padrão, outro modelo pode ser pensado. Sem

exigências profundas de resiliência para o bloco de comunicação, podemos reduzi-lo, inserindo uma quarta camada, que atue como interface para a conexão, conforme ilustrado a seguir. A esse modelo, chamaremos *spoke-hub*, em inglês.

Figura 13 – IoT-A de quatro camadas



Crédito: alaborada com base em Maschietto *et al.*, 2021, p. 63.

As funções de coleta e atuação seguem embarcadas no objeto, mas há uma camada de adaptação, externa aos objetos, que permitem o trânsito de informações bidirecionais, com um protocolo de comunicação de alto nível.

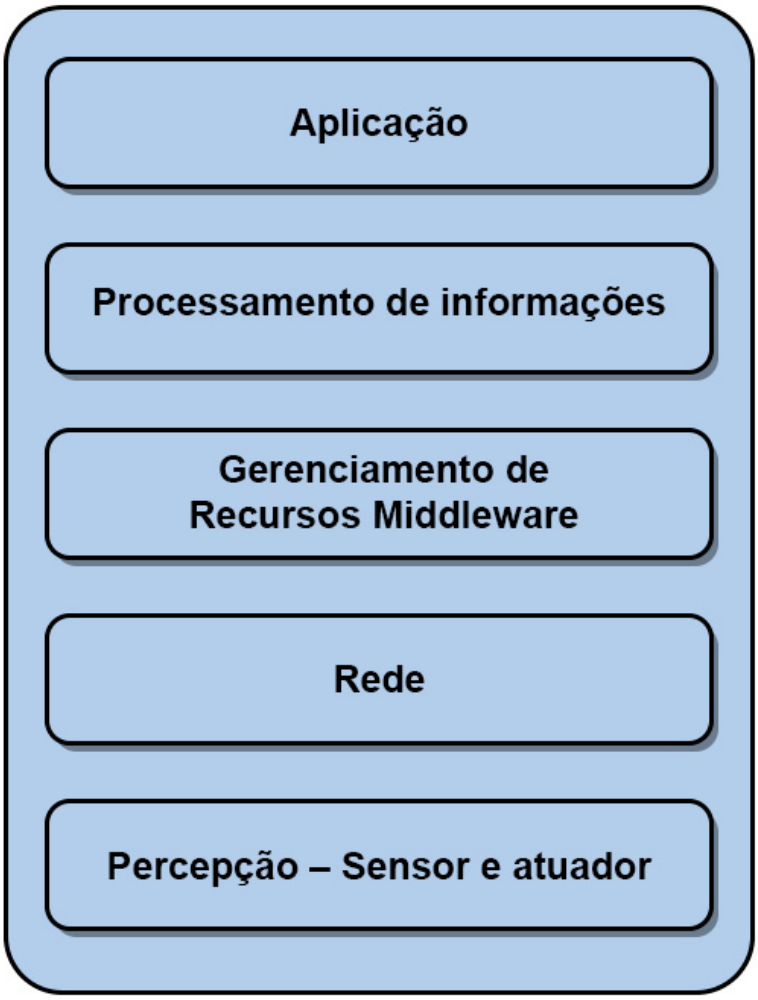
Neste modelo, assim como no de três camadas, o processamento local permanece no objeto, podendo ter complexidade discriminatória. Naturalmente, podemos simplificar ainda mais os objetos em um modelo com mais uma camada, se reduzirmos ainda mais a autonomia de comunicação e parte do processamento local.

4.3 IoT-A de cinco camadas

A arquitetura de cinco camadas, ilustrada a seguir, manterá, nos dispositivos, blocos mínimos para a operação. A camada de percepção (onde estão os objetos) inclui sensores e leitores simples conectados a um *gateway*

externo. A camada de rede faculta a conectividade dos objetos com plataformas de comunicação, como na arquitetura anterior, porém a camada de gerenciamento opera os objetos e a função semântica e de pré-processamento será assumida por camada de processamento externa.

Figura 14 – IoT-A de cinco camadas



Crédito: elaborada com base em Maschietto et al., 2021, p. 65.

Como enfatizamos ao iniciar este tópico, a escolha da IoT-A depende essencialmente da aplicação e do número de dispositivos envolvidos. Em nosso próximo tópico, vamos explorar um pouco as aplicações possíveis desses objetos, mas antes devemos comentar sobre uma camada acrescentada recentemente na estrutura IoT.

4.4 Camada de negócio

Considerando o emprego de IoT, principalmente em cidades inteligentes, como meio de extração de massas de dados, que permitem tratamentos estatísticos e de aprendizagem profunda, uma nova camada pode ser imaginada na IoT-A. Por esse viés, objetos IoT ganham valor como coletores de dados e atuadores para viabilizar ganhos de conforto, econômicos e de sustentabilidade na vida urbana.

O tratamento dos dados, entretanto, será o principal responsável pelo ajuste das decisões, que eventualmente retornam à camada de objetos, para sua concretização, por meio dos atuadores, presentes na rede. Estudaremos esses assuntos, com boa profundidade, mas, por hora, basta-nos entender que esse novo emprego da tecnologia justifica o acréscimo de uma camada de negócio, à arquitetura de cinco camadas, responsável pelo tratamento dos dados.

Santana *et al*. (2019, p. 78), sondando a literatura científica, propõem um modelo de cinco camadas no qual a camada de processamento de informações, descrita na Figura 14, é absorvida pela camada de aplicação, como pré-processamento para uso bruto da informação. Sobre a camada de aplicação surge, então, a camada de negócio, responsável pela inteligência de dados, fornecendo gráficos, análises, modelos etc. A figura a seguir ilustra esse modelo alternativo de cinco camadas.

Figura 15 – IoT-A de cinco camadas com camada de negócios

Crédito: elaborada com base em Santana et al., 2019, p. 79.

TEMA 5 – PROJETOS DE IOT E CAMADA DE APLICAÇÃO

Objetos IoT devem ser proporcionalmente baratos em relação aos demais custos de rede. Nesses custos, devemos incluir não só a aquisição, mas também os valores de operação e manutenção dos dispositivos.

As possibilidades de aplicação desses objetos inteligentes, conectados à rede, principalmente às nuvens da internet, são virtualmente infinitas. A escolha do objeto, ou seja, de sua arquitetura interna e da IoT-A, entretanto, determinarão o sucesso do projeto. Analisaremos agora algumas vantagens e desvantagens das IOT-A estudadas bem como os protocolos de comunicação da camada de aplicação.

5.1 IoT-A e Critérios de Projeto

Examinemos o exemplo de uma instalação industrial, com grande coleção de leitores RFID, sensores de esteiras e acionadores de máquinas. Leitores

RFID coletam somente dados, o processamento local se limita à verificação da validade das leituras. Sensores de esteiras, da mesma forma, apenas coletam dados, a análise de divergência precisa ser realizada pela máquina computacional que conhece quais devem ser os padrões de operação, para cada processo produtivo específico.

Se escolhermos uma arquitetura de três ou quatro camadas, dada a grande quantidade de objetos, os recursos necessários de endereçamento serão elevados, além disso, o processamento local, nesses casos, como entendemos, é pouco útil. Retirar boa parte da inteligência do objeto, senão toda, é um caminho interessante para conter custos. Neste caso, uma arquitetura de cinco camadas é uma escolha viável.

Naturalmente, essa opção arquitetônica tornará os objetos mais “rústicos”, exigindo do projetista um esforço maior para controlá-los. Certamente, será necessário agir nos níveis mais baixos de programação, entendendo a comunicação binária e as instruções de controle de cada tipo de objeto.

Vamos imaginar, agora, uma instalação predial. Neste prédio, cada sala possui um equipamento de climatização, ao qual queremos embarcar certa inteligência. Os equipamentos devem perceber, além da temperatura, a presença de pessoas no ambiente para decidir pela ativação, por exemplo. Suponha que a iluminação de cada ambiente também seja decidida em função da luminosidade local e da presença.

Neste caso, implementar uma arquitetura que retire a inteligência da borda pode ser pouco viável. Transportar todos os dados de temperatura, ocupação das salas e luminosidade, através da rede, para decisão central, apenas ocuparia a rede e o processamento do controlador. Uma arquitetura de três camadas será mais eficiente e econômica, deixando-se à aplicação de controle geral, funções de alto nível, como determinar os valores-limites de ativação ou mesmo horários de bloqueio.

Essa opção arquitetônica dará ao projetista certo distanciamento dos objetos, permitindo uma programação de mais alto nível, focada no cálculo e controle de parâmetros de operação e não no controle direto dos objetos.

Além do processamento local, podemos, nesta implantação, conceder aos objetos, também, processamento colaborativo, de borda (ou *edge computing*). Imagine que se detecta a presença de grande quantidade de pessoas em um

ambiente, tornando os esforços de refrigeração menos eficientes naquele local. Equipamentos em salas próximas podem ser acionados para complementar a demanda por refrigeração.

Essa decisão não precisa ser tomada de forma centralizada, pela aplicação de controle, mas pode ser delegada aos próprios objetos. O controle desse coprocessamento, normalmente, é deixado a cargo do *midleware*, residente em um objeto mais complexo, ou em uma máquina autônoma próxima.

Não há limites para este *downsizing*, plataformas de *middleware* podem agregar algoritmos de IA sintetizando dados ou alterando os parâmetros de decisão autonomamente.

5.2 Protocolos da camada de aplicação

Observando as várias IoT-As, a camada de aplicação se mantém inalterável, como bloco único. Isto assim se faz, para manter a interoperabilidade de uma rede IoT, em relação a seus usuários externos à rede. A camada de aplicação, entretanto, para permitir essa transparência, precisa conviver, do lado IoT da rede, com objetos cuja capacidade de processamento e memória são baixos.

Tradicionalmente, essa comunicação cliente-servidor é baseada em HTTP, para redes IP, compostas por “objetos” de alta capacidade de armazenamento e processamento. Um protocolo adaptável a essas limitações precisa ser concebido. A resposta a essa demanda são protocolos como MQTT e CoAP, vamos detalhá-los então.

5.3 CoAP

Constrained Application Protocol (CoAP) é um protocolo que busca reduzir o HTTP, mantendo as funcionalidades básicas, tais como *GET*, *POST*, *DELETE* e *PUT*, sobre comunicação sem conexão (como UDP, por exemplo). O desenho do protocolo inclui duas camadas, em sua arquitetura interna, permitindo a interação seguindo os princípios REST.

Na primeira camada, reside o controle dos mecanismos próprios de requisição/resposta. Já na segunda camada, o protocolo detecta duplicidade de mensagens, permitindo comunicação confiável, mesmo em ambientes sem

conexão. Para que essa comunicação seja possível, dois tipos de mensagens são produzidas no CoAP: confirmáveis e não confirmáveis. As mensagens confirmáveis demandarão a recepção de um *acknowledgement*, garantindo sua chegada ao destino.

A arquitetura do protocolo baseia-se na criação de *Universal Resource Identifiers* (URIs) que permitem a um sensor publicar no servidor informações sobre serviços distintos por ele disponibilizados.

Feita a publicação, a informação estará disponível no servidor para ser consumida por todos os assinantes do serviço. Essas facilidades têm um custo de processamento, que não pode ser assumido por todos os objetos IoT. Dispositivos mais restritos necessitam de um protocolo ainda mais simples, o MQTT.

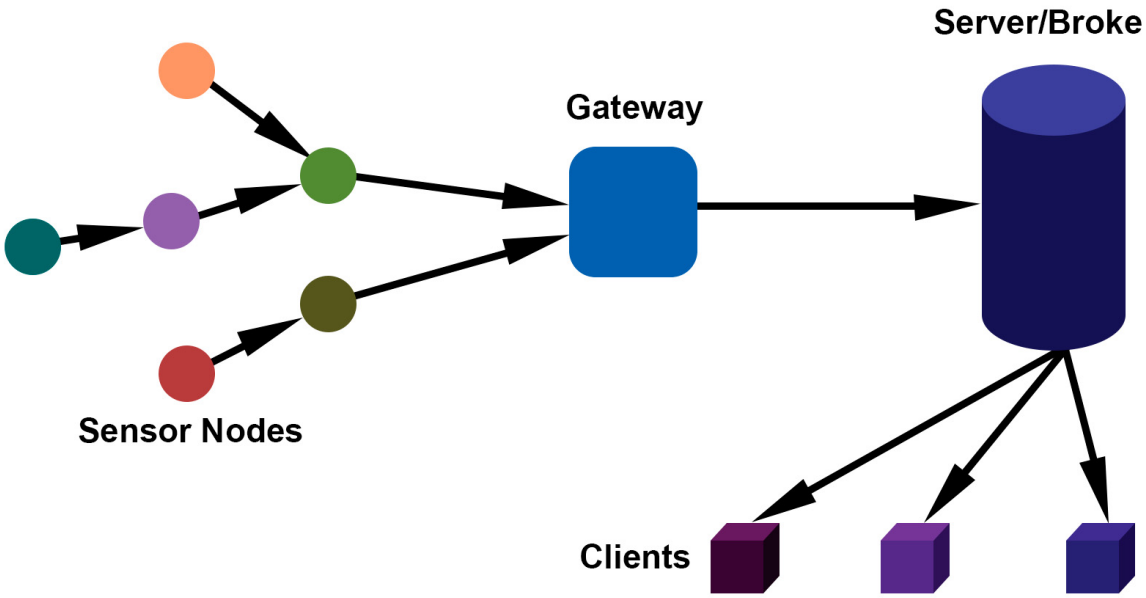
5.4 MQTT

Message Queue Telemetry Transport (MQTT) é um protocolo com foco em dispositivos limitados ao extremo. Criado inicialmente pela IBM e, posteriormente, padronizado pela norma ISO/IEC 20922.

Esse protocolo pressupõe não apenas limitações de memória e processamento, mas também de banda disponível para a transmissão, que é uma preocupação bastante razoável, para boa parte das aplicações de IoT, conforme veremos em outro momento. Desta forma, a implementação utiliza baixo *overhead*, no empacotamento de dados.

O protocolo MQTT opera em ambientes conectados (como TCP) e cria uma arquitetura com três elementos principais, ditos *subscriber*, *publisher* e *broker*. No caso do IoT, temos o *gateway* (ou servidor, dependendo da IoT-A), como *broker*, e o sensor, como *publisher*. Nesta arquitetura, o publicador insere dados no *broker* sobre determinado tema, acessível a todos os assinantes desse tópico. A figura a seguir ilustra a arquitetura.

Figura 16 – Arquitetura *Publish-Subscribe*



Fonte: Thangavel *et al*., 2014, p. 2.

Uma vez que a informação fica disponível no servidor, a comunicação entre assinantes e sensores é assíncrona, o que reduz significativamente as necessidades de uso do meio para comunicação, principalmente por parte dos publicadores. O protocolo possui alguns recursos de controle de qualidade de serviço (QoS) de rede, selecionáveis em três níveis de qualidade.

Uma implementação, bastante popular e livre desse protocolo, é o servidor Mosquito, que implementa a maioria das facilidades previstas na norma ISO/IEC 20922.

FINALIZANDO

Nesta etapa, buscamos construir um conceito de IoT associado aos objetos inteligentes e suas aplicações. Entendemos que a escolha de um objeto, para um dado uso, depende das arquiteturas interna e externa possíveis, bem como das restrições de conectividade presentes no meio. Estamos agora prontos para conhecer algumas aplicações importantes desses objetos em outros momentos.

REFERÊNCIAS

AKYILDIZ, I. F.; WANG, X.; WANG, W. **Wireless mesh networks: a survey. Computer networks**, v. 47, n. 4, p. 445-487, 2005.

AUTOMATION, R. **Converged Plantwide Ethernet (CPwE) Design and Implementation Guide**. 2011. Disponível em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.352.6198&rep=rep1&type=pdf>. Acesso em: 26 set. 2022.

BRUSTOLIN, G. C. **Redes para IoT** – Aula 1, Material Didático para Roteiro de Aprendizagem do Curso de Tecnologia em Redes de Computadores. Curitiba: Intersaberes, 2022.

IDEALI, W. **Conectividade em Automação e IoT**. Rio de Janeiro: Alta Books Editora. 2021.

KO, H-S. et al. A statistical analysis of interference and effective deployment strategies for facility-specific wireless sensor networks. **Computers in Industry**, v. 61, n. 5, p. 472-479, 2010.

LORA Alliance. **Lorawan 1.1 Specification**. 2017. Disponível em <https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1>. Acesso em: 26 set. 2022.

MASCHIETTO, L. et al. **Arquitetura e Infraestrutura de IoT**. Grupo A, 2021. (MB)

MEDEIROS, J. C. de O. **Princípios de telecomunicações**: teoria e prática. 5. ed. São Paulo: Érica, 2016.

MONK, S. **Internet das Coisas**: uma introdução com o Photon – Série Tekne. Grupo A, 2018.

RAMOS, A. **Eletromagnetismo**. Editora Blucher, 2016.

RED Hat. **O que é Middleware e para que serve**. Disponível em: <https://www.redhat.com/pt-br/topics/middleware/what-is-middleware>. Acesso em: 26 set. 2022.

SANTOS, B. P. et al. **Internet das coisas**: da teoria à prática. Belo Horizonte: UFMG, 2016.

SANTANA, C. et al. Teoria e prática de microserviços reativos: um estudo de caso na internet das coisas. **Sociedade Brasileira de Computação**, 2019.

THANGAVEL, D. et al. Performance evaluation of MQTT and CoAP via a common middleware. In: 2014 IEEE NINTH international conference on intelligent sensors, sensor networks and information processing (ISSNIP). IEEE, 2014. p. 1-6.