Internet of Things: Architectures and Technologies

Beatriz Rocha, Filipe Guimarães e Gonçalo Ferreira

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
e-mail: {a84003,a85308,a84073}@alunos.uminho.pt

Resumo Internet of Things (IoT) é o conjunto de tecnologias capaz de interligar qualquer equipamento, desde objetos do dia-a-dia a dispositivos em rede mais sofisticados. Estes aparelhos inteligentes têm a capacidade de partihar informação entre si, desde que estejam permanentemente ligados à Internet. Neste ensaio escrito, iremos enfatizar as arquiteturas que utilizam este conceito, bem como as tecnologias utlizadas de modo a torná-las executáveis, confiáveis e seguras.

1 Introdução

1.1 Contextualização

A Internet of Things (IoT) surgiu no âmbito da necessidade de criar aplicações que fossem úteis no dia-a-dia comum. Esta permite que os objetos vejam, ouçam e concretizem tarefas interagindo entre si, partilhando informação e coordenando as suas decisões. Por exemplo, sensores de estacionamento que comunicam entre si e informam aos condutores quantos lugares disponíveis existem naquele momento.

Figura 1. Diferentes áreas onde a IoT desempenha um papel fundamental

2 Principais Desafios Associados

Os dispositivos que integram IoT apresentam limitações no que toca à implementação de mecanismos de segurança. Estes equipamentos apresentam restrições de custo que afetam o seu poder computacional e a sua memória, bem como restrições energéticas, uma vez que grande parte deverá estar operacional durante anos. Estas limitações, aliadas ao elevado número existente destes dispositivos, geram a necessidade da criação de novos protocolos de comunicação que sejam compatíveis com os protocolos já existentes para a Internet e mecanismos de segurança desenhados para protegerem as comunicações com os mesmos.
Num artigo da Universidade de Coimbra acerca de segurança em IoT[1] é proposta uma stack de protocolos para cada camada de comunicação, bem como os mecanismos de segurança disponíveis para cada uma delas.

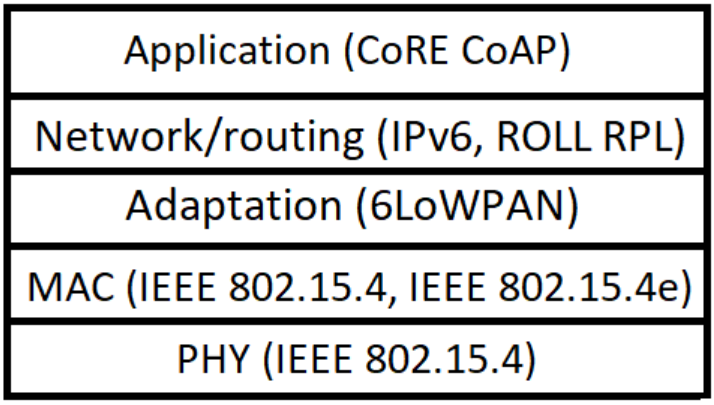

Figura 2. Stack de Protocolos de comunicação para IoT

2.1 PHY (IEEE 802.15.4) & MAC (IEEE 802.15.4, IEEE 802.15.4e)

Na camada PHY (Physical) e na MAC (Medium Access Control) é sugerido o protocolo IEEE 802.15.4, desenhado para conciliar o alcance e a velocidade das comunicações com as restrições energéticas em IoT. Este protocolo providencia vários modos de segurança na camada MAC que são diferenciados pela encriptação ou pela sua falta e pela validação da autenticidade das mensagens transmitidas. Neste protocolo, a confidencialidade da mensagem pode então ser apoiada pelos modos de segurança que implementam encriptação, onde se usarão chaves de 128 bits. A integridade e autenticidade dos dados transmitidos é fornecida nos modos que produzem um MIC (Message Integrity Code) de 32, 64 ou 128 bits, que será adicionado ao fim da mensagem a transmitir.

2.2 Adaptation (6LoWPAN)

Na camada seguinte, o protocolo 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) permite o transporte de pacotes IPv6 através de ambientes de comunicação sem fios com restrições de energia, implementando mecanismos de fragmentação e reconstrução de pacotes. Com isto, torna-se possível a comunicação através de IPv6 entre estes aparelhos limitados e entre outras entidades na Internet com mais capacidade. Nesta camada não existem mecanismos de segurança definidos para este protocolo.

2.3 Network/routing (IPv6, ROLL RPL)

O routing através de 6LoWPAN é suportado por RPL (Routing Protocol for Low-power and Lossy Networks) do grupo ROLL. RPL define como a segurança será aplicada às mensagens de controlo de routing. Para apoiar a integridade e autenticação dos dados, é utilizado o sistema de criptografia RSA com o algoritmo de hash SHA-256. É também possível a utilização de AES/CCM para encriptação e geração de MIC com chaves de 128 bits que irão apoiar a confidencialidade e a integridade dos dados. RPL também define 3 modos de segurança:

- Unsecured, onde não é aplicada segurança às mensagens de controlo de routing
- Preinstalled, apoia confidencialidade, integridade e autenticação das mensagens de controlo de routing
- Authenticated, apropriado para dispositivos a operarem como router

2.4 Application (CoRE CoAP)

Na camada Application, as comunicações podem ser suportadas pelo protocolo CoAP (Constrained Application Protocol) do grupo CoRE, podendo assim comunicar com outras entidades na Internet usando apenas CoAP ou traduzindo CoAP para HTML e vice-versa. CoAP pode adotar DTLS (Datagram Transport Layer Security) na camada de transporte para aplicar segurança nas mensagens em termos de confidencialidade, autenticação e integridade. Para além disto, ainda existem 4 modos de segurança neste protocolo que diferem na forma como é efetuada a autenticação (NoSec, PreSharedKey, RawPublicKey e Certificates).

3 Arquitetura da IoT

As arquiteturas que se baseiam no modelo das três camadas (Figura 3 (a)) não se adaptam a ambientes IoT reais, uma vez que a *Network Layer*, por exemplo, não cobre todas as tecnologias subjacentes que transferem dados para as plataformas IoT. Já no modelo das cinco camadas (Figura 3 (d)), a *Application Layer* corresponde à interface através da qual os utilizadores finais conseguem interagir com um dispositivo e requisitar dados interessantes. Este modelo providencia ainda uma interface à *Business Layer* onde análises de alto nível e relatos podem ser produzidos. Complementarmente, os mecanismos de controlo para aceder aos dados da *Application Layer* também são tratados nesta

camada. Contudo, esta apenas pode ser suportada por dispositivos poderosos devido à sua complexidade e enorme necessidade computacional.[2] Considerando estes pontos e tendo em conta a simplicidade da arquitetura, concluímos que o modelo das cinco camadas é o ideal para as aplicações IoT.

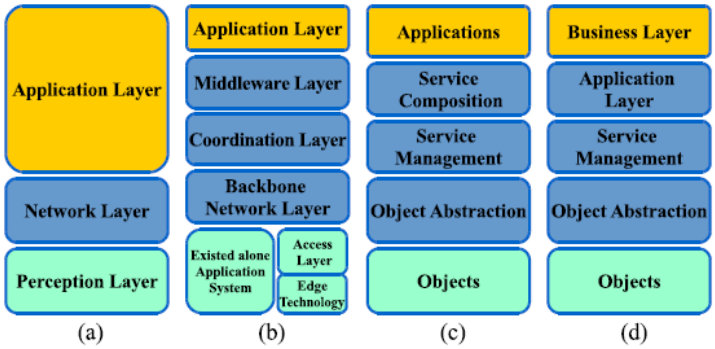

Figura 3. A arquitetura IoT

3.1 *Objects Layer*

A primeira camada representa os sensores físicos da IoT que tencionam colecionar e processar informação. Esta camada inclui sensores para executar diferentes funcionalidades tais como inquirir a localização, a temperatura, o peso, o movimento, a vibração, a aceleração, a humidade, etc. Mecanismos standard prontos a usar necessitam de ser utilizados pela *Perception Layer* para configurar objetos heterogéneos. Esta digitaliza e transfere dados à *Object Abstraction Layer* através de canais seguros. Para além disso, os grandes volumes de dados criados pela IoT são iniciados nesta camada.

3.2 *Object Abstraction Layer*

Esta camada é responsável pela tranferência de dados através de canais que usam tecnologias como RFID (Radio Frequency Identification), 3G, GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunication System), WiFi, Bluetooth LowEnergy, infravermelhos, entre outras. É também a camada onde é feita a gestão de dados e a computação na nuvem.

3.3 *Service Management Layer*

Esta camada é baseada em endereços e nomes. Permite que os programadores de IoT trabalhem com diversos objetos sem se preocuparem com o hardware em causa. Esta

também recebe dados, toma decisões e transmite os serviços que obedecem aos protocolos de rede.

3.4 *Application Layer*

Esta camada fornece os serviços requisitados pelos utilizadores, por exemplo, providencia medidas de temperatura e humidade do ar àqueles que requisitem estes dados. A importância desta camada para a IoT foca-se na capacidade de fornecer serviços inteligentes de alta qualidade, de maneira a ir de encontro às necessidades dos usuários. Esta camada cobre inúmeros mercados, nomeadamente transportes, automação industrial e serviços de saúde inteligentes.

3.5 *Business Layer*

Business Layer é a camada de gestão onde os sistemas IoT são desenhados, analisados, implementados, monitorizados e desenvolvidos. A responsabilidade desta camada consiste em construir modelos de negócio, gráficos e diagramas de fluxo dos dados recebidos da *Application Layer*, tornando possível a tomada de decisões baseada na análise de grandes volumes de dados, repeitando a privacidade dos utilizadores.

4 Projetos atuais relacionados com a temática

4.1 Monitorização de animais baseada em tecnologias IoT

Este projeto surge no âmbito das atividades de criação de gado (com especial atenção ao pasto em campos de vinha e pomares), possibilitando a monitorização da condição física, localização e comportamento do animal. O sistema deve permitir o gado pastar em áreas cultivadas sem os colocar em risco. Os dados recolhidos pelos sensores deverão ser levantados por uma rede local para um servidor (*cloud*) e, autonomamente, guardar e atualizar a informação, de modo a ser acessível pelo pastor do gado, referindo se este está seguro.
O desenho proposto para este projecto tem como base uma coleira com sensores capazes de recolher a informação útil, como postura, localização e comportamento. Essa informação é, então, transmitida para torres que cobrem a área de pasto e, por sua vez, enviada para o nodo central. Estas torres permitem ainda que as coleiras avaliem a sua localização, baseando-se em RSSI (Received Signal Strength Indication). Para um baixo consumo de energia, usa-se um sistema que segue TDMA (Time Division Multiple Access mechanism)[3]. O nodo central (gateway) funciona como um agregador de informação, responsável também pela conexão entra a rede local e a rede exterior. Para que esta conexão seja bem sucedida e eficiente, é proposto o uso das estruturas de dados JSON (JavaScript Object Notation).
Os dados são recebidos na *cloud* pelo *broker*, que suporta protocolos de mensagem de arquitetura assíncrona como AMQP (Advanced Message Queuing Protocol) e MQTT (Message Queuing Telemetry Transport)[4]. Este recebe a informação do nodo central por FIFO (First-In-First-Out), utilizando um RabbitMQ, que é um intermediário

orientado a mensagens que oferece mecanismos de segurança, como SSL/TLS (Secure Sockets Layer/Transport Layer Security). A *cloud* será dividida em 4 estágios nos quais serão usados diversos protocolos para manter uma base de dados saudável e acessível.

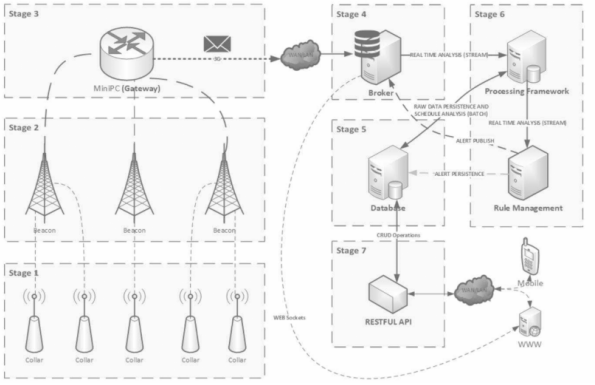

Figura 4. Arquitetura global

4.2 *Smart Homes*

Um exemplo muito comum onde podemos encontrar IoT são as *Smart Homes*. Casas com este sistema fornecem aos utilizadores a possibilidade de controlar e monitorizar a iluminação, os eletrodomésticos e as câmaras de videovigilância em qualquer instante e lugar. Estas casas são sistemas que consistem em aplicações construídas com base na infraestrutura da IoT e têm como funções principais[5]:

Alerta Monitoriza o ambiente e envia aos utilizadores notificações com os dados atuais via email, mensagem ou outro serviço de comunicação

Monitorização Avalia, com ajuda de sensores e câmaras, as condições em redor, permitindo controlar tudo constantemente

Controlo Permite que o utilizador interaja com a casa, nomeadamente desligue ou ligue a iluminação, feche e abra portas

Inteligência É responsável por tomar decisões a partir de mecanismos de inteligência artificial, face a mudanças no ambiente

O diagrama[6] da figura 5 mostra uma simples implementação das *Smart Homes*. No lado esquerdo temos o terminal onde o utilizador vai interagir, através de uma aplicação ou site, com a casa. Já no lado direito temos os dispositivos e sensores. Para conectar as duas extremidades podemos recorrer a um microcontrolador que liga a casa, através de protocolos de rede WiFi, ao utilizador final.

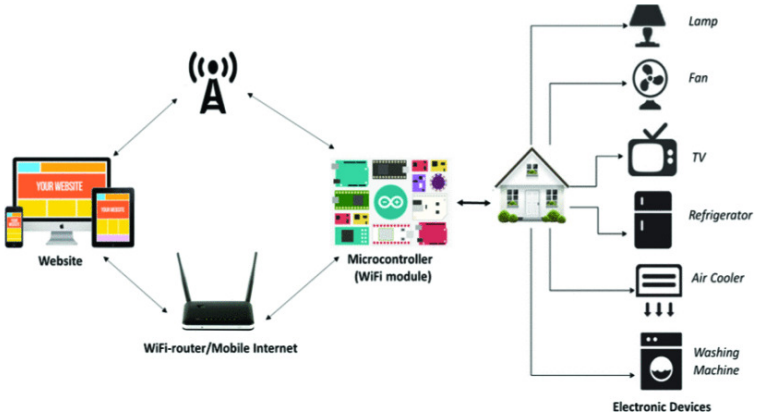

Figura 5. Arquitetura das *Smart Homes*

5 Conclusão

Em suma, a IoT não se trata de um tema simples, na medida em que vários desafios ,tais como confiança, mobilidade, desempenho, segurança e interoperabilidade necessitam de ser tidos em consideração. Contudo, acreditamos que a Internet das Coisas seja o futuro, uma vez que é capaz de revolucionar não só a vida humana, mas também inúmeras áreas de grande relevância.

Referências

1. J. Granjal, E. Monteiro, J. Sá Silva Security for the Internet of Things: A survey of Existing Protocols and Open Research Issues
2. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications
3. L. Nóbrega, P. Pedreiras, P. Gonçalves, S. Silva Energy efficient design of a pasture sensor network
4. Oasis MQTT Version 3.1.1 Plus.
5. T. Malche, P. Maheshwary Internet of Things (IoT) for building Smart Home System
6. S. Mahmud, S. Ahmed, K. Shikder A Smart Home Automation and Metering System using Internet of Things (IoT)