INTERNET DAS COISAS E OS PRINCIPAIS PROTOCOLOS

Anderson Roberto de França Menezes[1]; Rafael Antônio Teles Barbosa[2]; Mayka de Souza Lima[3]; Sidney Cassemiro do Nascimento[4]

[1] Estudante, Instituto Federal de Sergipe, andersonroberto89@hotmail.com; [2] Estudante, Instituto Federal de Sergipe, rafael.teles80@hotmail.com; [3] Professor, Instituto Federal de Sergipe, mayka.lima@ifs.edu.br; [4] Professor, Instituto Federal de Sergipe, sidney.nascimento@ifs.edu.br.

RESUMO: A Internet das Coisas ou Internet of Things (IoT) pode ser definida como uma rede de interligação de objetos ou coisas, assim sendo considerada como um dos estados mais avançados a que a Internet pode chegar. As soluções IoT são caracterizadas por uma variedade de dispositivos com diferentes capacidades computacionais e de comunicação, ou seja, são heterogêneos. Além disso, a necessidade de interação leva a outra questão: a interoperabilidade. A maneira tradicional de tratar a heterogeneidade e a interoperabilidade é o emprego de padrões, protocolos e *middlewares*. Com base nisso, uma série de protocolos foram criados, ou têm sido adaptados, para prover a interoperabilidade de objetos na IoT. Da mesma forma, plataformas de *middleware* também têm sido propostas. Porém, ainda há uma falta de padronização, fazendo com que essas soluções não tratem de forma adequada uma série de funcionalidades importantes no contexto da IoT, como nomeação, gerenciamento dos dispositivos, segurança, modelos de programação etc. Considerando a relevância atual da IoT e sua importância nesse contexto, ter *middlewares* é um modelo arquitetural de referência. Tomando como base artigos já publicados, o objetivo deste artigo é, inicialmente, esclarecer o que é a Internet das Coisas, apresentar as áreas de aplicação, para, posteriormente, tratar os requisitos e as funcionalidades necessárias aos *middlewares* para IoT, além de discutir alguns desafios, como protocolos, segurança, privacidade e atividades de pesquisa relacionadas a essa área.

Palavras-chave: Rede. Conectividade. Interoperabilidade. *Middlewares*. Objetos.

Abstract: The Internet of Things (IoT) can be defined as a network of interconnection of objects or things, thus being considered as one of the most advanced states that the Internet can reach. IoT solutions are characterized by a variety of devices with different computational and communication capacities, that is, they are heterogeneous. In addition, the need for interaction leads to another question: interoperability. The traditional way of addressing heterogeneity and interoperability is the use of standards, protocols, and middleware. Based on this, a series of protocols have been created, or have been adapted, to provide interoperability of objects in IoT. Similarly, middleware platforms have also been proposed. However, there is still a lack of standardization, so that these solutions do not adequately address a number of important functionalities in the IoT context, such as naming, device management, security, programming models, etc. Considering the current relevance of IoT and its importance in this context, having middlewares is an architectural model of reference. Based on previously published articles, the purpose of this article is initially to clarify what the Internet of Things is, to present the areas of application, to later treat the requirements and functionalities necessary for IoT middleware, and to discuss some challenges such as protocols, security, privacy and research activities related to this area.

Keywords: Network. Connectivity. Interoperability. Middlewares. Objects.

INTRODUÇÃO

Ao longo dos anos, a rede mundial de computadores, a Internet, tem sido confundida como sinônimo de uma de suas mais importantes aplicações: a *World Wide Web*, ou apenas, *Web*. Enquanto a Internet em si é uma infraestrutura que permite a inter-

conexão de centenas de milhares de computadores, a *Web* é um repositório fantástico de informações e do conhecimento humano, que foi evoluindo com o passar dos anos. Inicialmente, no que alguns autores denominam *Web* 1.0, o foco era a busca e entrega de informações às pessoas, ou seja, informações eram disponibilizadas por poucos indivíduos e acessadas por um número significativamente maior usuários. Na *Web* 2.0, as pessoas passam de consumidoras de informações para serem também fornecedoras de informações. O foco passou a ser a colaboração e o compartilhamento das informações, onde o principal fenômeno é a criação e a disseminação das mais diferentes redes sociais. Nessa linha evolutiva, o passo seguinte é a *Web* 3.0, também denominada de *Web* semântica (BERNERS, 2001), caracterizada, de forma simplificada, pela obtenção e pelo processamento automático de informações. Uma forma diferente de analisar essa evolução é através da própria Internet, que passou de uma rede que interligava computadores, para ser vista como um repositório de documentos e, na sequência, uma rede de interconexão de pessoas e, agora, mais recentemente de objetos (ou coisas) (CARISSIMI, 2016).

A Internet das Coisas ou Internet of Things (IoT) é o ambiente no qual objetos e mesmo os seres vivos têm a habilidade de interagir e colaborar entre si, usando uma conectividade em rede, para agregar valor às informações que possuem (CARISSIMI, 2016). Assim, uma maneira simples de entender o que é a Internet das Coisas é pensar que agora são os mais variados objetos do dia a dia que geram e consomem informações na *Web* e, através disso, interagem e oferecem serviços às pessoas. Porém, essa visão já vem sido abordada. Em 1991, Mark Weiser, pai da computação ubíqua, preconizava a existência de objetos inteligentes. Da mesma forma, o termo Internet of Things foi criado em 1999, por Kevin Ashton, como uma forma de monitorar a existência de recursos físicos, minimizar desperdícios e, com isso, reduzir perdas e custos, principalmente, no setor de logística.

A Internet das Coisas, ou IoT, acrônimo do inglês Internet of Things, não possui uma definição única. A ITU Internet *Reports* define a Internet das Coisas como "a capacidade de conectividade a qualquer momento, de qualquer lugar, por qualquer um e por qualquer coisa". A Comissão Europeia, por sua vez, define como sendo "objetos de identidade única operando em espaços inteligentes para conectar e comunicar em contextos sociais, ambientais e de usuários". A origem dessas diferentes definições é a forma como se enxerga a Internet das Coisas e a abstração utilizada: orientada a coisas, orientada a Internet e orientada a conhecimento (ATZORI, 2010). Na visão orientada a coisas, a abordagem é relacionada aos sensores usados para monitorar e rastrear condições através de objetos ditos inteligentes. Na visão orientada a Internet, o foco é a interconexão desses objetos inteligentes, sua integração e gerenciamento através de *middlewares*. Por fim, a visão orientada a semântica, onde o ponto principal é o conhecimento obtido através de representação, armazenamento, busca, organização e uso das informações. Mais adiante, será desenvolvido o funcionamento por trás das Internet das Coisas por meio de uma explicação de alguns dos principais protocolos que são utilizados atualmente, que são o MQTT, o CoAP, o UPnP e o ALLJOYN.

MATERIAIS E MÉTODOS

Nesse trabalho, foi feito um levantamento dos principais artigos disponíveis e publicados que abordam o tema Internet das coisas e seus principais protocolos. O objetivo foi abordar os conceitos para um melhor entendimento sobre o assunto e detalhar o funcionamento dos protocolos da Internet das Coisas, mostrando como está o avanço sobre a solução para achar um padrão de comunicação visando à expectativa sobre o desenvolvimento de infraestrutura da IoT e a criação de protocolos e *softwares* necessários para a sua eficiência. No final, criou-se uma tabela comparativa dos protocolos utilizados e, por fim, foram propostos novos temas com base no presente artigo.

RESULTADOS E DISCUSSÃO

Além de expandir a percepção, o homem con-

seguiu, com suas invenções, grandes avanços no campo das comunicações e, assim, diminuir significativamente a distância entre as pessoas. A Internet é, sem dúvida, a tecnologia que mais evoluiu e está evoluindo, no que se refere à comunicação das pessoas não importando quantos quilômetros as separem umas das outras. (MARTINS; ZEM , 2014).

Criada em meados da década de 1950, a Internet deixou de ser uma rede estritamente militar para ganhar as universidades e, posteriormente, interligar computadores pessoais (PC) no mundo todo conforme a figura 1.

Figura 1 - Internet das coisas, conexão mundial.

Fonte: Portal GSTI, 2015.

O advento da tecnologia sem fio trouxe mobilidade à rede de uma forma que abriu precedentes para explorar a possibilidade de adicionar outros dispositivos à rede, que não fossem exclusivamente computadores. Assim, nos últimos anos, a Internet passou a conectar outros dispositivos (como *smartphones* e *tablets)*, aumentando consideravelmente a população de nós na Internet. É nesse cenário que surge o paradigma de Internet of Things (IoT).

Segundo Bandyopadhyay *et al*. (2011), "coisas" são dispositivos (físicos ou virtuais) que possuem identidades, atributos e personalidades virtuais e são capazes de utilizar interfaces inteligentes.

Conforme citado anteriormente, existem diversos objetos criados pelo homem com intuito de fornecer informações que não são possíveis de perceber diretamente. Contudo, estas informações são colhidas de forma mecânica e cabe ao indivíduo que coletou tratá-las, armazená-las e/ou retransmiti-las a algum destino. Tendo isso em mente, pode-se revelar definições de alguns autores sobre IoT:

Internet das Coisas integra um grande número de tecnologias e visiona uma variedade de coisas ou objetos ao nosso redor que, através de esquemas únicos de endereçamento e protocolos de comunicação padrão, são capazes de interagir uns com os outros e cooperar com seus vizinhos para atingirem objetivos comuns (ATZORI *et al*., 2012).

Internet das coisas refere-se a uma maneira singular de endereçar objetos e suas representações virtuais em uma estrutura similar à Internet. Tais objetos podem encadear informações sobre si mesmos ou podem transmitir dados em tempo real de sensores sobre seu estado ou outras propriedades úteis associadas a esse objeto (AGGARWAL, 2013).

Internet das coisas é uma combinação de Internet do futuro e computação ubíqua. Ela demanda interações com sensores heterogêneos, agregadores, atuadores e um diversificado domínio no contexto de aplicações conscientes, preservando segurança. (BANDYOPADHYAY *et al*., 2011).

Interconexão de dispositivos sensores e atuadores provendo a habilidade de compartilhar informações através de plataformas por meio de um *framework* unificado, desenvolvendo um cenário operacional comum possibilitando aplicações inovadoras. (GUBBI et al., 2013).

A Internet das coisas surge, então, como uma rede de nós composta na sua maioria por objetos comuns (isto é, sem recursos computacionais), mas que possui recursos sensoriais ou de medição, por exemplo, que podem ser disponibilizados ou compartilhados com seus vizinhos. Uma vez que estes recursos são capazes de circular na rede, eles podem ser utilizados por uma aplicação para armazenamento em algum local, exibição em uma tela ou retransmissão para um computador a quilômetros de distância. Tudo isso sem que o usuário final interfira no sensor/medidor, na aplicação ou

na transmissão dos dados, pois tudo que irá interessar a ele no final das contas é o dado obtido. Isso remete ao conceito de computação ubíqua.

Objetos Inteligentes

Segundo Carissimi (2016), a Internet das Coisas, como seu próprio nome diz, é formada por "coisas" e quando se fala nisso o que vem em mente é exatamente: "o que são essas coisas que formam a internet das coisas?". De forma genérica, uma "coisa" é um objeto físico composto por um identificador único, por um transdutor, por mecanismos de comunicação e por um processador, que pode variar do mais simples ao mais complexo. Uma característica fundamental da Internet, tal qual como conhecemos, é que cada elemento que a compõe possui um endereço IP. O endereço IP nada mais é que um nome que identifica, de forma única, um elemento na Internet e, como tal, pertence a um sistema de nomes.

Um sistema de nomes é uma maneira de referenciar simbolicamente, de forma inequívoca, objetos obedecendo a uma determinada sintaxe e semântica. O conjunto de nomes válidos é denominado de espaço de nomes. São exemplos cotidianos de espaço de nomes, entre outros, as placas de nossos automóveis, compostas por três letras, seguidas de quatro dígitos decimais (0-9); os endereços IPv4 ou IPv6.

Um nome identifica um objeto de forma única em um contexto. Esse contexto pode ser local, como o nome de uma rua em uma cidade (nada impede que outra cidade tenha uma rua com o mesmo nome), ou *Global*, como os endereços IP na Internet. As principais características de um nome são unicidade, persistência e longevidade, ou seja, um nome deve identificar um objeto de forma inequívoca e durar, pelo menos, o mesmo tempo de vida desse objeto. Na Internet das coisas é comum que os objetos sejam identificados por etiquetas RFID (*Radio Frequency IDentification*), por endereços IP ou através de URIs (*Uniform Resource Identifiers*).

Uma etiqueta RFID é um microchip com uma antena acoplada que responde a uma requisição externa fornecendo sua identificação, via sinal de rádio. A fonte de energia empregada pelas etiquetas RFID pode ser externa ou interna a ela e, em função disso, elas são classificadas como passiva, semipassiva ou ativa. Uma etiqueta RFID passiva não possui fonte de energia, o sinal eletromagnético da própria requisição gera uma corrente elétrica que fornece a energia necessária para o envio da identificação.

Por sua vez, as etiquetas semipassivas e ativas possuem uma fonte interna (bateria). No primeiro caso, semipassiva, a bateria é suficiente apenas para a etiqueta receber o sinal de requisição, a resposta. Como no caso anterior, é enviada com a energia do campo elétrico decorrente da própria requisição. Já nas etiquetas ativas, a bateria possui energia suficiente para receber o sinal de requisição e para transmitir a identificação.

As etiquetas RFID armazenam um código de 96 bits, o *Electronic Product Code* (EPC), que serve como identificador único da etiqueta e segue um padrão aberto (GID- 96). As etiquetas RFID são bastante difundidas, sendo usadas, inclusive, como mecanismo antifurto em lojas de departamento e em livrarias. Outros exemplos de códigos usados para identificar objetos são *QR-Codes* e códigos de barra. Normalmente, as etiquetas RFID identificam um objeto dentro de um contexto local.

Porém, no momento em que se deseja uma identificação em contexto *Global*, torna-se necessário o uso de algum outro mecanismo. Nesse ponto, entram as tecnologias Internet, como os endereços IP. Um endereço IP, na sua versão 4, é um número de 32 bits que, teoricamente, fornece até 232 nomes diferentes. No entanto, na prática, essa capacidade é menor devido à semântica dada a um endereço IPv4 em possuir dois campos, o prefixo e o sufixo, que servem, respectivamente, para identificar uma rede na Internet e uma interface de rede dentro desta. Além disso, o IPv4 já enfrenta há anos o problema de esgotamento de endereços, o que fez surgir o IPv6. Um endereço IPv6 é um número de 128 bits, ou seja, fornece cerca de 340 undecilhões de nomes (2128 endereços). Assim como o IPv4, essa é capacidade bruta, já que também há uma divisão de campos em

prefixo e sufixo, 64 bits cada, e que são usados conforme as regras de atribuição de endereços IPv6.

Outra forma de identificar objetos é através de URI (*Uniform Resource Identifier*). Um URI é um *string* empregado para identificar o nome de um recurso. Na prática, um URI fornece informações sobre a localização de um objeto e seu nome em um sistema distribuído. A sintaxe de um URI é definida no Internet Standard 66 e na RFC 3986 sendo composta, basicamente, por um esquema (*scheme*), uma parte hierárquica e, opcionalmente, por uma requisição (*query*) e um fragmento (*fragment*). As formas mais comuns de URI são o *Uniform Resource Locator* (URL) e o *Uniform Resource Name* (URN).

Assim, quando o *scheme* usado for o http, estamos na presença de um URL que é empregado para localizar e acessar um recurso na Internet, ou seja, o URL informa onde encontrar um recurso. Se o *scheme* for *urn*, estamos identificando um objeto dentro de um espaço de nome específico. Tipicamente, um URN fornece um identificador de espaço de nome (*Namespace IDentifier* – NID) e um nome válido dentro desse espaço de nome (*Namespace Specific String* – NSS) como, por exemplo, *urn*:isbn:978-85-8143-677-7. O próximo elemento que compõe um objeto inteligente é um transdutor. Um transdutor é um dispositivo que converte uma forma de energia em outra, como os sensores e os atuadores. Os sensores são capazes de converter uma fonte de energia como mecânica, térmica, acústica ou eletromagnética (inclui luz), entre outras, em corrente ou tensão elétrica.

Há uma variedade enorme de sensores que são capazes de "sentir" características de um meio físico e transformar essa característica em valores de tensão, ou corrente, que podem ser lidos e convertidos em valores binários através de conversores analógicos digitais. Um atuador, por sua vez, transforma energia elétrica em movimento para, por exemplo, acionar o fechamento de válvulas. Uma das funcionalidades básicas dos objetos inteligentes é a sua capacidade de interação, ou seja, modificar alguma situação no mundo físico ou reportar um estado desse mundo físico para que ele seja monitorado.

Como os objetos que compõem a Internet das Coisas, por questões de praticidade, de custo, e mesmo de projeto, têm capacidades reduzidas de processamento e de autonomia (duração de sua bateria), os mesmos se re*string*em a observar o meio e enviar as informações para sistemas de maior capacidade para avaliação dessas informações e tomada de decisões. Surge, então, a necessidade de conectividade, ou seja, os objetos devem ter capacidade de comunicação que variam desde barramentos específicos, interligando os objetos a sistemas de maior capacidade, até as tecnologias de comunicação via rede celular (GSM, LTE), de redes locais (*WiFi* e *Ethernet*) e de redes pessoais (*Bluetooth, ZigBee*, infravermelho, 6LowPAN, RFID etc.).

Por fim, por mais simples que possam ser, os objetos inteligentes possuem a necessidade de realizar algum tipo de processamento. Esse processamento, dependendo da complexidade do objeto e de seu custo, pode variar desde uma lógica de máquina de estados, ou programas simples executados por um processador dedicado de baixo custo, como aqueles que atendem a indústria de linha branca (eletrodomésticos), até processadores de maior capacidade, como ARM e Intel. Justamente em função de questões relacionadas com o consumo de energia, os processadores de baixo consumo têm se tornado uma opção bastante interessante e são cada vez mais empregados em placas e kits de desenvolvimento como Arduíno, Raspberry, Cubieboards, entre outras. Esses kits também contam com várias interfaces, como portas seriais, paralelas, conversores A/D, de uma gama de sensores e atuadores e conectividade de rede (*WiFi*, *Ethernet*, *Bluetooth*, *ZigBee*, infravermelho etc.), tornando-se uma plataforma interessante para comporem os elementos básicos da Internet das Coisas, assim como os nossos *smartphones*.

Protocolos IOT

Um dos aspectos mais importantes para o desenvolvimento da Internet das Coisas é a padronização da comunicação. Esse ponto tem sido discutido nos últimos anos, trazendo consigo um conjunto de protocolos para atender os requisitos das

aplicações da melhor maneira possível. Os protocolos para IoT são categorizados em: dispositivo a dispositivo (*device Data device* - D2D), dispositivo a servidor (*device Data server* - D2S) e servidor a servidor (*server Data server* - S2S). Os protocolos D2D servem para interconectar dispositivos diretamente entre si garantindo uma série de requisitos como tempo real, garantias de entrega, alto desempenho, etc. (SANTONI, 2005).

As áreas que se beneficiam dessas características incluem sistemas militares, hospitais, indústria automotiva e aviônica, entre outras. Genericamente, esses sistemas são denominados de *Data Distribution System* (DDS) e são, na verdade, mais associados a atividades de controle. Já os protocolos D2S são destinados a coletar dados e enviar a sistemas externos (servidores). Para completar, os protocolos S2S são empregados para gerenciamento e integração das informações entre servidores de aplicação, ou seja, estão em um nível gerencial de controle (TEZA, 2002).

Baseado na visão "Internet" do IoT, em que se espera uma integração entre os dispositivos IoT e a Internet que conhecemos, a escolha óbvia para endereçamento é o IP. Entretanto, é necessário definir um protocolo de aplicação a ser empregado para permitir que dispositivos IoT enviem seus dados, ou seja, para fazer a coleta de dados (D2S). Uma opção inicial é empregar o HTTP para transportar mensagens e, através de seus verbos e comandos, como GET e PUT, interagir com os dispositivos da IoT. Entretanto, essa opção traz alguns inconvenientes, como o fato de não ter nenhuma qualidade de serviço, e que, por ser um protocolo *request-reply*, necessita de *polling* explícito para consultar estados dos dispositivos e, principalmente, por dificultar *parsing*, já que há muitas opções em seu cabeçalho. A segurança também é um problema, pois as questões de privacidade, autenticidade e integridade devem ser resolvidas com o auxílio de SSL/TLS. Tudo isso implica questões de processamento, tamanho de código, capacidade de memória e de conectividade que nem sempre os dispositivos IoT apresentam (TEZA, 2002).

Em função disso, novos protocolos foram sugeridos para os ambientes IoT, muitos deles baseados em um modelo *publish-subscriber*, justamente para evitar *polling*, demandar menor largura de banda e resolver a questão de conectividade. A seguir, são apresentados alguns protocolos normalmente citados como solução para aplicações IoT, com especial atenção a dois deles, o MQTT e o CoAP, por terem se tornado as principais opções.

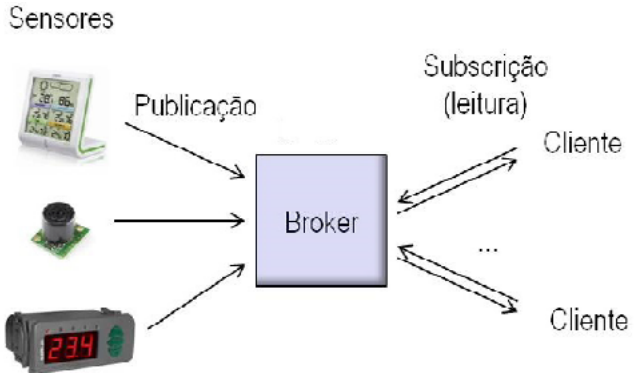
Messaging Queue Telemetry Transport (MQTT)

O MQTT é um protocolo de transporte fim-a-fim, ou seja, permite a comunicação de entidades de um mesmo nível em sistemas finais. O MQTT é baseado em um modelo *publish-subscriber*, onde clientes publicam (*publish*) informações que podem ser acessadas por outros clientes (*subscriber*s). Essas informações são enviadas em mensagens que são disponibilizadas em um endereço, chamado de tópico, que tem um formato semelhante a uma estrutura de diretórios de um sistema de arquivos como, por exemplo, casa/sala/temperatura. O sistema é assíncrono, ou seja, tanto a produção de informações (*publish*) como a leitura das mesmas pode ocorrer sem nenhum aviso prévio entre as partes. Para permitir esse desacoplamento entre a divulgação e a leitura de informações, os sistemas *publish-subscriber* precisam de um intermediário, o *broker*, que armazena as informações até a sua leitura. Assim, o *broker* é o responsável por distribuir mensagens para os clientes com base no tópico da mensagem. Além dessa distribuição, o *broker* é responsável por validar, transformar e encaminhar as mensagens. A figura 2 ilustra esse funcionamento.

O MQTT foi projetado para ser empregado em dispositivos de capacidade computacional reduzida, com baixa largura de banda e conectividade não garantida. A PDU (*Protocol Data Unit*) do protocolo MQTT é encapsulada pelo protocolo TCP, ou seja, o cabeçalho e os dados do MQTT são enviados na área de dados do TCP. Há uma versão do MQTT, denominada de MQTT-SN (MQTT Sensor Network), em que sua PDU é encapsulada pelo protocolo UDP, que, por sua vez, é encapsulada pelo IP ou pelo protocolo 6LowPAN. O MQTT prevê, ainda, diferentes

garantias de entrega, denominado de QoS (*Quality of Service*), com as semânticas: no máximo uma vez, pelo menos uma vez e exatamente uma vez.

Figura 2 - Esquema de funcionamento do MQTT



Fonte: Alexandre Carissimi, 2016.

Na versão 3.1, a especificação do MQTT (IBM; *Eurotech*, 2010) apresenta uma série de características do protocolo, algumas delas listadas abaixo:

*Uso de TCP/IP para fornecer conectividade;

*Pequena sobrecarga de transporte e trocas minimizadas de protocolos para reduzir tráfego na rede; e

*Mecanismo que notifica partes interessadas quando um cliente se desconecta da rede anormalmente.

Como visto, uma solução baseada em MQTT tem dois componentes: o *broker* e os clientes, que publicam e assinam tópicos. Há várias implementações em *software* livre para o *broker* (HiveMQ, ActiveMQ, RabbitMQ, CloudMQTT, Mosca...). Uma das implementações mais populares de *broker* MQTT é o Mosquitto2 e, para clientes, o Paho3.

Constrained Application Protocol (CoAP)

O *Constrained Application Protocol* (CoAP) é um protocolo de troca de mensagens focado especificamente em dispositivos limitados computacionalmente. O CoAP foi criado dentro de um grupo de trabalho do IETF denominado *Constrained RESTful Environments* (CoRE), projetado para ser uma alternativa ao HTTP para aplicações *machine to machine* (M2M), como por exemplo sistemas de automação residencial. CoAP dá suporte a uma comunicação entre aplicações em objetos inteligentes seguindo o paradigma requisição/resposta. Possui um serviço de descoberta já implementado, baseado no conceito de diretórios de dispositivos. Sua estrutura é baseada no HTTP, facilitando, assim, a integração com os recursos disponíveis na *WEB*. Porém, diferente do HTTP, o CoAP cumpre alguns requisitos específicos para dispositivos com limitações computacionais, como o baixo overhead na troca de mensagens (TEZA, 2002).

Uma lista interessante de pacotes que implementam o CoAP, em diversas linguagens de programação, é fornecida no Wikipedia. Importante observar que existem dois tipos de implementação que participam de uma solução IoT: o lado do dispositivo (*constrained device*) e o lado servidor. Clientes se utilizam de servidores CoAP para acessar o serviço de descoberta. Uma vez conhecendo o endereço do servidor, o cliente pode acessar a lista de dispositivos mantida por ele. Cada objeto inteligente é representado por uma URI, seguindo o formato especificado pelo *Constrained RESTful Environments* (CoRE). Essa especificação também é responsável pelo serviço de descoberta presente no CoAP.

A busca por objetos inteligentes pode ser realizada com a utilização de filtros, que são parâmetros adicionados à *string* de consulta por dispositivos, enviada ao respectivo diretório de recursos. O CoRE também define um conjunto de atributos que representam os recursos presentes em um diretório. Os principais atributos são: *Resource Type*, responsável por identificar a função de um determinado recurso (temperatura, luminosidade, impressora, etc.); *Interface Description*, o qual indica os métodos que podem ser utilizados para a comunicação com esse recurso (GET, OST, etc); *Context Type*, que representa o formato dos dados fornecidos pelo recurso. Como o CoAP já é um protocolo bastante utilizado em IoT e possui inúmeras implementações disponíveis para as mais diversas plataformas, entre as quais é possível citar o *Californium, Copper* e o *Erbium*, isso

faz com que exista uma grande quantidade de produtos que sigam suas especificações. Com base nisso, criar soluções que também utilizem o CoAP pode garantir a interoperabilidade com essa gama imensa de dispositivos já ativos. Embora essa interoperabilidade não possa ainda ser estendida para IoT em geral, garantir a compatibilidade com o CoAP é uma estratégia que potencializa a interoperabilidade (TEZA, 2002).

O CoAP segue um modelo cliente/servidor e é baseado no modelo arquitetural REST. No CoAP, os servidores disponibilizam recursos por meio de um URL e os clientes acessam esses recursos usando métodos pré-definidos como *GET, PUT, POST e DELETE*. Como tanto o HTTP quanto o CoAP usam o modelo REST, eles podem ser facilmente integrados usando proxies, de forma que, por exemplo, uma aplicação cliente pode nem ficar sabendo que está acessando um sensor. Assim como o HTTP, a área de dados do CoAP pode transportar dados codificados com XML, JSON, CBOR ou qualquer outro formato de dados definido pela aplicação. Por ter sido projetado para dispositivos de baixo custo e poder computacional, o CoAP emprega uma pilha de protocolos "enxuta", baseada em UDP sobre IP, ou sobre 6LowPAN (padrão para conectividade IPv6 para dispositivos sem fio de baixo custo). O cabeçalho CoAP possui um tamanho fixo de 4 bytes e suas mensagens causam nenhuma, ou muito pouca, fragmentação na camada de enlace. Em relação aos aspectos de segurança, o CoAP optou por usar DTLS (*Datagram Transport Layer Security*), que é equivalente ao uso de chaves RSA de 3072 bits, o que lhe confere uma excelente segurança com pouco consumo computacional (se comparado com outros métodos).

UPnP - Universal Plug and Play

Criado em 1999 pelo Forum UPnP, este protocolo de comunicação é formado atualmente por mais de 380 fabricantes e profissionais ligados à automação residencial, computação, eletrodomésticos, redes, segurança e dispositivos móveis para definição e controle dos padrões UPnP. Foi desenvolvido a partir da tecnologia PnP - *Plug and Play* - da *Microsoft Corp* e foi concebido para suportar configurações automaticamente e já está embutido no sistema operacional *Microsoft Windows* ME e XP. Além da Microsoft, segundo Teza (2002) e Santoni (2005), outras empresas de informática e eletroeletrônicos já possuem produtos para esta tecnologia. Dentre elas, podemos citar a Intel, LG, Sony, Matsushita, Panasonic, Toshiba e GE.

Para Teza (2002), o UPnP baseia-se em padrões existentes de Internet para possibilitar que PC e dispositivos inteligentes em redes domésticas sejam conectados automaticamente entre si, sem maiores complicações. O autor (op. cit.) explica que o UPnP pode funcionar por rede com fio ou sem fio, utilizando um conjunto padrão do protocolo IP para trabalhar no meio físico da rede. Assim, dispositivos UPnP podem ser conectados à rede incluindo Rádio Frequência - RF e *Wireless*, linha telefônica, rede elétrica, infravermelho - IrDA, *Ethernet* e *FireWire* - IEEE 1394. A maior dádiva deste protocolo é a utilização das diversas mídias acima mencionadas e a utilização de protocolos padrão e abertos como o TCP/IP, HTTP e XML. Outras tecnologias podem ser usadas, como: HAVi, CEBus, LonWorks, EIB e X-10, que podem fazer parte da rede UPnP através da utilização de pontes (*bridges*) ou conversores (*proxys*) (SANTONI, 2005).

Estão definidos no padrão UPnP três componentes básicos:

- Dispositivo UPnP: contém serviços UPnP e podem conter outros dispositivos UPnP aninhados. Por exemplo, uma impressora (dispositivo UPnP) pode consistir em um serviço de impressão e um dispositivo scanner aninhado, que, por sua vez, oferece um serviço de fotocópia;

- Serviço UPnP: expõe ações que podem ser aplicadas durante sua invocação, por meio de um servidor de controle residente no dispositivo que hospeda o serviço, bem como uma tabela que armazena um conjunto de variáveis de estado do serviço (tabela de estados). A tabela de estados do serviço UPnP pode ser monitorada por um servidor de eventos (também residente no dispositivo que hospeda o serviço), que tem como função publicar para outras

entidades interessadas a modificação de variáveis de estado desse serviço;

- Ponto de Controle UPnP: atua, em parte, como servidor de diretório, tendo como tarefa descobrir e controlar os dispositivos UPnP presentes na rede.

Este protocolo nos impõe facilidade no uso e gerenciamento, de forma que imediatamente após a conexão de qualquer dispositivo UPnP, este equipamento é descoberto pelos gerenciadores ou ele mesmo procura pelos gerenciadores. Este protocolo possui inúmeras vantagens e agrega a utilização da conveniência para cada tipo de aplicação, como, por exemplo:

- Milhares de pessoas conhecem o protocolo TCP/IP e desenvolvem produtos em XML e HTTP, tornando-se fácil a implementação de soluções para automação residencial;

- Utilização dos conhecimentos e tecnologias pré-existentes em rede de computadores para aplicação em automação residencial, tornando-a mais barata e eficaz;

- Homogeneização e simplificação dos sistemas computacionais e residenciais;

- Este protocolo possibilita uma instalação fácil e segura, apenas conectando o equipamento (que deve dispor de suporte ao UPnP) a qualquer mídia de comunicação (incluindo os cabos de corrente elétrica);

- Por empregar tecnologia computacional clássica, é de mais fácil utilização pelos internautas no momento de instalar e configurar um sistema de automação residencial baseado em UPnP (TEZA, 2002).

Se, por um lado, o UPnP tem diversas vantagens, principalmente no uso em automação industrial, por outro lado, a segurança desse protocolo já se mostrou duvidosa. De acordo com uma pesquisa disponibilizada no site da IDG NOW (2013), pesquisadores em segurança da Rapid7 encontraram mais de 80 milhões de endereços de IP públicos únicos que responderam a solicitações de descoberta de UPnP por meio da Internet entre os meses de junho e novembro de 2012. Além disso, identificaram também que 20%, ou 17 milhões, desses endereços de IP correspondiam a dispositivos que expunham o Protocolo Simples de Acesso a Objeto (SOAP ou *Simple Object Access Protocol*) para a Internet. Isso permite que crackers ataquem os sistemas por trás do firewall e exponham as informações sigilosas sobre eles. Foi identificado que mais de um quarto dos dispositivos tinham o UPnP implementado por meio de uma biblioteca chamada Portable UPnP SDK. Oito vulnerabilidades que podem ser exploradas remotamente foram encontradas nessa SDK, incluindo uma que pode ser utilizada para a execução de código remoto, disseram os pesquisadores.

As vulnerabilidades foram corrigidas na versão 1.6.18. Falhas adicionais, incluindo aquelas que podem ser utilizadas em ataques de negação de serviço (DDoS) e execução de código remoto, também existiam em uma biblioteca chamada de MiniUPnP. Elas foram corrigidas em 2008 e 2009, porém, 14% dos dispositivos com UPnP expostos utilizavam a versão do MiniUPnP 1.0 (vulnerável). Foi possível identificar mais de 6900 versões de produtos vulneráveis por conta do UPnP. Essa lista engloba mais de 1500 fornecedores e leva em conta apenas dispositivos que expõem o serviço SOAP da UPnP à Internet, o que é uma vulnerabilidade grave por si só.

Provedores de Internet (ISP) foram aconselhados a forçar atualizações para as configurações ou firmware para dispositivos de assinantes, a fim de desabilitar os recursos UPnP ou substituir os dispositivos por outros configurados de forma segura, que não expõem o UPnP à Internet. “Usuários domésticos e de dispositivos móveis devem garantir que a função UPnP dos seus roteadores e dispositivos de banda larga móvel esteja desabilitada”, disseram os pesquisadores (IDG NOW, 2013).

Além de garantir que nenhum dispositivo exponha a UPnP à Internet, as empresas foram aconselhadas a realizar uma revisão cuidadosa sobre o potencial impacto de segurança para todos os dispositivos compatíveis com UPnP encontrados em suas redes (impressoras de rede, câmeras IP, sistemas de armazenamento etc.) e considerar segmentá-los da rede interna até que uma atualização de firmware

esteja disponível pelo fabricante.

A Rapid7 lançou uma ferramenta gratuita chamada ScanNow para Universal Plug and Play, bem como um módulo para o teste de penetração Metasploit Framework, que pode ser usado para detectar serviços UPnP vulneráveis que estejam rodando dentro de uma rede.

AllJoyn

Segundo informações do site da Convergência Digital (2014), o protocolo AllJoyn de "código aberto" (*open source*) foi inicialmente desenvolvido pela Qualcomm e apresentado pela primeira vez no famoso Mobile World Congress de 2011, em Barcelona. Depois de alguns anos de sucesso mediano com AllJoyn, a Qualcomm passou o código-fonte para a Fundação Linux, em dezembro de 2013. A partir daí, a Qualcomm e a Fundação Linux formaram a AllSeen Alliance, um consórcio dedicado à construção e manutenção de um framework de código aberto que permite que dispositivos de todas as formas e tamanhos se comuniquem perfeitamente um com o outro incluindo nomes bem diversos, como a LG, Panasonic, Haier, Silicon Image ,TP-LINK, Cisco, Sears, Wilocity, entre outros.

O protocolo AllJoyn fornece ferramentas para todo o processo de conexão e manutenção de dispositivos em uma rede Wi-Fi. Os fabricantes podem usar a estrutura AllJoyn para criar seus próprios aplicativos personalizados para dispositivos conectados em uma rede Wi-Fi, completos com serviços de controle e de notificação. Então, os usuários podem ligar uma máquina de café antes de ir para a cama, pedir para preparar uma xícara de café para eles na parte da manhã e receber uma notificação no *smartphone* quando o copo estiver pronto. Isto é o que muitos imaginaram quando a Internet das "Coisas" começou a ganhar impulso em mercados de consumo, e o consórcio AllSeen Alliance visa a estabelecer como o protocolo AllJoyn fará com que isso aconteça.

Sendo o primeiro dos protocolos de IoT (Internet of Things) voltados ao consumidor, o padrão AllJoyn recebeu críticas elogiosas na imprensa, especialmente após a formação do AllSeen Alliance. Ele prometeu resolver um problema que qualquer pessoa que tenha lutado com conectividade Wi-Fi ou o emparelhamento Bluetooth tenha experimentado, e, usando essa solução, sugeriu novas possibilidades na Internet das Coisas.

Para o SVP da Qualcomm, Rob Chandhok, a Internet das Coisas estava falhando devido ao fato de os fabricantes terem projetado seus celulares e aparelhos inteligentes para se comunicarem apenas com suas próprias aplicações proprietárias em vez de trabalhar em conjunto. Ao invés de construir um ecossistema de dispositivos que pudessem conversar um com o outro, eles apenas construíram para si mesmos. Uma lâmpada inteligente é realmente "inteligente" se você também precisa de um interruptor especial? (TECMUNDO, 2011)

Com a ajuda da Fundação Linux, a Qualcomm acredita que pode resolver esse problema com base na formação do AllSeen Alliance, que é baseada em uma peça da tecnologia Qualcomm. Depois de não ter conseguido um dano com a tecnologia AllJoyn nos últimos dois anos, a empresa está renunciando à posse do código para a AllSeen Alliance.

AllJoyn pode fazer tudo, descobrindo automaticamente dispositivos e negociando conexões com os protocolos disponíveis. Como o mecanismo de renderização do navegador *Web*Kit, como o Eclipse, como o Hadoop, e como o próprio Linux, a expectativa da Qualcomm é que o AllSeen possa se tornar um padrão ao conseguir que as empresas compartilhem o fardo de construir algo que acabem precisando de seus dispositivos e serviços de qualquer maneira.

Embora o problema típico com os padrões tenha sido bem documentado, a AllSeen pode ter mais chances do que a maioria. Uma vez que a sua principal tarefa de negociar conexões é dispositivo, sistema operacional e agnóstico de rede, não deve tornar-se obsoleto quando as novas tecnologias se apresentam. Mesmo que cada fabricante chame AllSeen de algo diferente na caixa - um obstáculo para a tecnologia de compartilhamento de tela do Miracast - pode não importar tanto aqui. Uma vez que os dispositivos AllSeen são projetados para en-

contrar-se automaticamente entre qualquer conexão disponível, o seu *smartphone* deve teoricamente ser capaz de dizer que o Smart Share da LG e o AllShare da Samsung são a mesma coisa.

Com as empresas membros atualmente no estábulo, Chandhok acha que a Aliança poderia ter interfaces padrão para controlar a iluminação, o ar condicionado, até mesmo os painéis automáticos antes de muito tempo, e ele imagina um futuro não muito distante onde os dispositivos podem dar inteligência a seus usuários ao controle. Quando um automóvel detecta que os passageiros estão dentro de um veículo, talvez com base na proximidade de seus telefones, ele poderia deixá-los tocar música e ajustar o clima sem alcançar um mostrador. Tudo isso é um processo que está muito próximo, mas ainda vai demorar para ser realizado da forma idealizada.

De acordo com o estudo, podemos estabelecer campos de características em comum (ou não) dos quatro protocolos mostrados, com informações específicas de cada um deles. Como pode ser visto na Tabela 1:

Tabela 1 - Comparação entre os principais protocolos IOT

Protocolos	Trabalhos Pesquisados	Características	Pontos Positivos	Pontos Negativos
MQTT	Estudos dos Protocolos de Comunicação MQTT e CoAP para Aplicações Maquineto Maquine e Internet das Coias; Internet das Coisas, middlewares e outras coisas.	Protocolo de transporte fim-a-a-fim, baseado em um modelo publish-subscriber,com Sistema assícrono e tem dois componentes: o broker e os clientes, que publicam e assinam tópicos.	Permite a comunicação de entidades de mesmo nível em sistemas finais. As informações publicadas por clientes podem ser acessadas por outros clientes.	Projetado para ser empregado em dispositivos de capacidade computacional reduzida, com baixa largura de banda e conectividade não garantida.
CoAP	Estudos dos Protocolos de Comunicação MQTT e CoAP para Aplicações Maquineto Maquine e Internet das Coias; Internet das Coisas, middlewares e outras cois	Protocolo de troca de mensagens focado especificamente em dispositivos limitados computacionalmente. É uma alternativa ao HTTP para aplicações M2M. Segue o paradigma requisição/ resposta.	Facilita a integração com recursos disponíveis na WEB, pois é baseado no HTTP e no conceito de diretórios de dispositivos. Emprega uma pilha de protocolos enxuta e tem uma excelente segurança com pouco consumo computacional.	O computador deve ter um baixo overhead na troca de mensagens para suportar o CoAP.

UPnP	A Domótica como Instrumento para a Melhoria da Qualidade de vida dos Portadores de deficiência; Uma Contribuição ao Gerenciamento de Recursos de Sensoriamento e Atuação no Middleware EXEHDA	Desenvolvido a partir da tecnologia Plug and Play da Microsoft Corp., baseia-se em padrões existentes na Internet no qual PCs e dispositivos inteligentes em rede domésticas são conectados. Pode funcionar com rede com fio ou sem fio. Dispositivos UPnP podem ser conectados à rede Rádio Frequência, IrDA, Ethernet e FireWire entre outras.	Pode ser utilizadas por diversas mídias e tem protocolos padrão aberto como o TCP/IP, HTTP e XML. Impõe facilidade no uso e gerenciamento. Imediatamente após a conexão de qualquer dispositivo, o equipamento é descoberto ou ele mesmo procura pelos gerenciadores. Proporciona Fácil implementação de soluções para automação residencial além de ser a mais barata e eficaz para esse fim.	O UPnP Já apresentou falhas de segurança que deixou cerca de 6900 produtos vulneráveis porém essas falhas já foram solucionadas na versão disponibilizada atualmente.
AllJoyn	Qualcomm demonstra allJoyn, a nova tecnologia de compartilhamento P2P; Internet das Coisas: Uma 'Babel' de Protocolos.	Desenvolvido pela Qualcomm, foi o primeiro protocolo de IoT voltado ao consumidor oferece ferramentas para todo o processo de conexão e manutenção de dispositivos em uma rede Wi-Fi, com serviços de controle e de notificação. sua principal tarefa é a de negociar conexões entre dispositivo, sistema operacional e agnóstico de rede.	Tem código aberto. Por ser utilizado pelo consórcio AllSeen Alliance que é formado por várias empresas do ramo tecnológico faz com que o AllJoyn seja mais fácil de chegar a um padrão de interoperabilidade entre dispositivos de tamanhos e marcas distintas.	A previsão para que essa tecnologia venha a ser disseminada, de fato, ainda é de um futuro não muito próximo, pois tudo o que ela promete condiz exatamente com o que a Internet das coisas vem a ser.

Fonte: Elaborado pelo autor (2017).

CONCLUSÕES

A Internet das Coisas, ou IoT, interconecta pessoas e objetos do mundo real a aplicações e dados, proporcionando conforto, qualidade de vida e oportunidade de negócios. A IoT se tornou um mercado emergente com alto potencial, pois pode-se imaginar uma série de aplicações, nas mais diversas áreas do conhecimento humano e, principalmente, no quotidiano das pessoas.

À medida que se tem, cada vez mais, objetos inteligentes interconectados, há uma geração massiva de informações que precisa ser armazenada, processada e disponibilizada. As soluções atuais para tratar essa necessidade apontam para o uso de computação em nuvem, onde os recursos computacionais podem ser obtidos por demanda, e a disponibilidade dessas informações é garantida pela infraestrutura redundante aos *data centers* dos grandes provedores de solução de nuvem.

A proliferação dos dispositivos IoT gera uma série de desafios tecnológicos, de legislação e comportamentais. Os pontos fundamentais estão relacionados à privacidade e segurança das informações. Da mesma forma, apesar das diferentes capacidades computacionais dos vários tipos de dispositivos IoT existentes, é desejável que eles interajam entre si. Surgem, então, os problemas de heterogeneidade e de disponibilidade que são tratados com o desenvolvimento de padrões e adoção de *middlewares* e protocolos que abstraem uma série de características físicas. Levando-se em conta a quantidade exagerada de protocolos que há atualmente, cada qual com a sua importância e facilidades de uso, seria necessária uma padronização e para isso é preciso se estudar e desenvolver um protocolo que seja o mais adequado para a interoperabilidade de objetos que se diversificam em formas, tamanhos, materiais e principalmente marcas.

Assim, entre os protocolos aqui estudados, o que mais se aproxima de tais características é o protocolo AllJoyn por já estar sendo estudado e implementado a diversos dispositivos por meio da AllSeen Alliance. Em outra visão, por uma analogia, as linguagens de programação são muitas, têm suas vantagens e peculiaridades e podem ser utilizadas para diversos fins. Cada protocolo de IoT pode ser empregado na área em que mais se adeque, como temos o UPnP que estabelece melhor economia e eficácia para instalações residenciais. Por fim, é sugerido que se continue o estudo de outros protocolos para a Internet das Coisas, como o *Advanced Message Queuing Protocol* (AMQP) e o *eXtensible Messaging and Presence Protocol* (XMPP), em futuros trabalhos acadêmicos para que haja melhor entendimento sobre os avanços dos estudos nessa área.

REFERÊNCIAS

AGGARWAL, Charu C. **The Internet of Things:** a survey from the data-centric perspective. In: Managing and Mining Sensor Data. Springer, 2013. p. 383-428.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: a survey. **Computer networks**, v. 54, n. 15, p. 2787–2805, 2010.

ATZORI, Luigi. *et al***.** The Social Internet of Things (SIoT) when social networks meet the Internet of Things: concept, architeture and network characterization. **The International Journal of Computer and Telecommunications Networking**, Amsterdam, v. 54, 2012. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1389128612002654>. Acesso em: 05 ago. 2017.

BANDYOPADHYAY, Soma. *et al*. Role of middleware for Internet of Things: a study. **International Journal of Computer Science and Engineering Survey**, Bhopal, v. 2, n. 3, 2011. Disponível em: <http://airccse.org/journal/ijcses/papers/0811cses07.pdf>. Acesso em: 05 ago. 2017.

BERNERS-LEE, T.; HENDLER, J. The semantic web: a new form of web content that is meaningful to computers will unleash a revolution of new possibilities. **Scientific American Magazine**, p. 34–43, 2001.

CARISSIMI, Alexandre. **Internet das Coisas:** middleware e outras coisas**.** 2016. Universidade Federal do Rio Grande do Sul. Rio Grande do Sul, 2016.

Disponível em: <https://www.researchgate.net/publication/301298394> Acesso em: 13 jun. 2017.

GUBBI, Jayavardhana; et al. Internet of Things (IoT): a vision, architectural elements and future directions. **The international journal of grid computing and Science**, vol. 29, n. 7, Elsevier, 2013. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167739X13000241>. Acesso em: 05 ago. 2017.

MARTINS, Ismael Rodrigues; ZEM, José Luís. Estudo dos protocolos de comunicação MQTT e COaP para aplicações machine-to-machine e Internet das Coisas. **Revista Tecnológica da Fatec Americana**, v. 3, n. 1, p. 24, 2016. Disponível em: < http://fatec.br/revista_ojs/index.php/RTecFatecAM/article/view/41> Acesso em: 13 jul. 2017.

SANTONI, P. **Tecnologia e ricerca in domotica oggi**. Trabalho de Conclusão de Curso (Graduação em Informática). Universidade Degli Studi di Trento. Itália, 2005.

TECMUNDO. **Qualcomm demonstra allJoyn, a nova tecnologia de compartilhamento P2P**. Disponível em: <com.br/qualcomm/8618-qualcomm--demonstra-alljoyn-a-nova-tecnologia-de-compartilhamento-p2p.htm> Acesso em 05 jul. 2017.

TEZA, V. R**. Alguns aspectos sobre a automação residencial – Domótica.** Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Santa Catarina. Florianópolis, 2002.