UNIDADE ITUIUTABA | UEMG
Intercursos Revista Científica
Ciências Exatas

PROTOCOLOS DE COMUNICAÇÃO PARA INTERNET OF THINGS (IOT)

COMMUNICATION PROTOCOLS FOR INTERNET OF THINGS (IOT)

Lucas Lima Freire Brito; Milton Miranda Neto; Monica Rocha Ferreira De Oliveira; Ígor Andrade Moraes; Vinicius Angelo De Oliveira Muniz

RESUMO:

Este trabalho apresenta uma revisão dos protocolos de comunicação utilizados entre dispositivos inteligentes apoiados pelo conceito de IoT, uma vez que os protocolos de comunicação podem influenciar no projeto IOT devido a suas características de funcionamento, tais como eficiência energética, baixo consumo de banda, conexões geograficamente distantes e dependendo dos requisitos do ambiente.

Palavras-Chave: IoT, Protocolos. Comunicação. Revisão.

ABSTRACT:

The main goal of this paper is to analyze the communication protocols used for smart devices supported by the concept of IoT, considering that these communication protocols might cause a change on the project, such as energy efficiency, bandwidth, geographically distant regarding the requirements of the project.

Keywords: IoT, Protocols, Communication, Review.

I. INTRODUÇÃO

As redes de computadores são o núcleo da comunicação, onde empresas, casas, fazendas, universidades, hospitais, entre outros ambientes, podem possuir vários computadores e dispositivos conectados entre si através das tradicionais redes LAN e também pelas WLAN, quando conectados na internet ou estão em locais distantes geograficamente. “Redes de computadores como um conjunto de computadores autônomos interconectados por uma única tecnologia” [1]. As redes possuem várias aplicações tais como: computadores ligados a sistemas distribuídos

utilizando servidores sem limites de localidade no globo terrestre, aplicações comerciais, aplicações domésticas, acesso a informações remotas, comunicação entre pessoas, entretenimento interativo, comércio eletrônico, usuários com dispositivos móveis como: notebook, smartphones, wearabletechnology e gadgets.

Desta forma a arquitetura cliente-servidor é um modelo de comunicação utilizado na internet é baseado em duas atribuições principais na comunicação: 1) Cliente; 2) Servidor. O servidor precisa ter alta disponibilidade à espera da iniciativa do cliente. O cliente aciona o servidor todas as vezes que é preciso fazer a comunicação [2].

O Servidor é um software que mantém uma porta de comunicação aberta à espera do cliente, sendo que sua localização é pelo seu endereço ou nome, devem ser conhecidas por todos clientes que querem ter o acesso [2]. Um servidor pode receber muitas solicitações simultâneas de clientes, por este motivo, normalmente são executados por sistemas distribuídos de alto desempenho. Isto não impede que um dispositivo IoT execute a função de servidor, apesar do hardware limitado, podendo receber solicitações de clientes.

O cliente é um software ou processo, normalmente acionado por um usuário, por este motivo é comum possuir uma interface gráfica amigável [2]. Onde o cliente inicia a comunicação com o servidor, seja acionado por um usuário ou de forma automática, em resposta a um evento ou uma ação externa. Um dispositivo IoT pode atuar como um cliente, acessando servidores para atualizar informações sobre seu funcionamento ou mandar uma instrução qualquer.

Na Figura 1 a comunicação é demonstrada na forma de um processo cliente que envia uma mensagem pela rede ao servidor. Então, o processo cliente espera por uma mensagem de resposta. Quando o processo servidor recebe a solicitação, ele executa o envio da transferência de dados para o cliente [1].

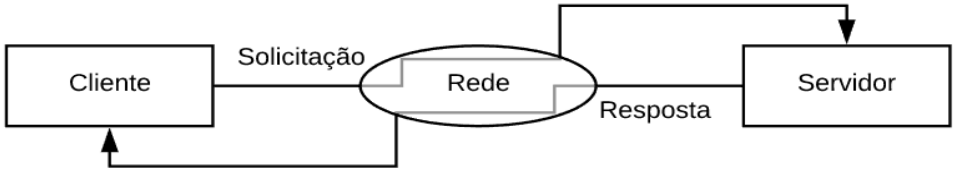

Figura 1 - O modelo cliente-servidor, demonstrando as solicitações e respostas. Autoria própria adaptado de [1].

II. MATERIAIS E MÉTODOS

A. Protocolos

Os protocolos são análogos a um idioma, como por exemplo, o inglês, onde para que ocorra troca de informações ou dados é imprescindível que os dispositivos conectados conheçam o mesmo vocabulário e a estrutura da linguagem, caso contrário os pacotes não serão entregues corretamente. Os protocolos possibilitam a transmissão da informação entre as camadas e entre equipamentos [3]. Um protocolo de rede é um conjunto de regras e padrões utilizado para possibilitar a comunicação entre dispositivos diferentes [3]. Os protocolos são responsáveis por dividir dados em pacotes onde serão transmitidos pela rede, sendo assim dentro de cada pacote deve conter, endereçamento do ponto de destino do pacote, numeração de sequência tornando cada pacote único, estabelecimento de um canal fechado entre transmissor e receptor, controle de erros de comunicação e correção, retransmissão ou confirmação e conversão de código com adequações de pacotes enviados ou recebidos.

O Internet Enginee ring Task Force (IETF) é o principal órgão de padrões da Internet, desenvolvendo padrões abertos por meio de projetos abertos.

B. TCP/IP

Com a variedade de sistemas operacionais e uma extensa quantidade de hardwares diferentes, havia a necessidade de uma padronização dos protocolos de envio e recebimento de dados. Para comunicação entre dois dispositivos a ISO (International Organization for Standardization) propôs o modelo OSI (Open System Interconnection) com sete camadas: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física [1]. Na pratica o modelo TCP/IP, criado pelo DoD (Departamento de Defesa dos Estados Unidos) tornou-se o mais popular. O modelo TCP/IP (Protocolo de Controle de Transmissão / Protocolo de Internet) possui apenas quatro camadas: Aplicação, Transporte, Internet e Host/rede ou Acesso à rede [2] [4].

A figura 2 é a equivalência entre cada camadas do modelo OSI/ISO e o modelo TCP/IP [1].

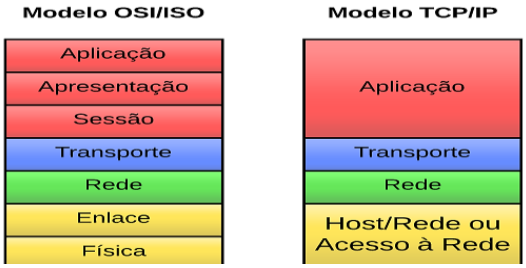

Figura 2 - Pilha de protocolos e suas equivalências. Autoria própria adaptado de [1].

A figura 3 é apresentada para facilitar o entendimento dos protocolos e redes por camadas do TCP/IP IP [1].

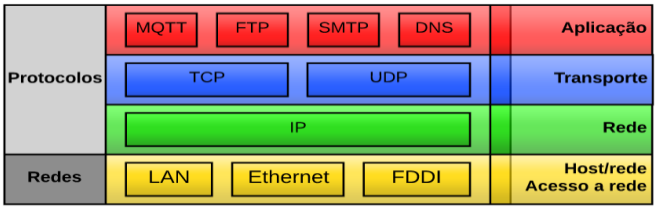

Figura 3 - O modelo cliente-servidor, demonstrando as solicitações e respostas. Autoria própria adaptado de [1].

C. Camada de Aplicação

A camada de aplicação define como os diversos programas ou processos em execução vão se comunicar. E dependendo algumas aplicações tais como fluxo de vídeo (VNC) ou chamadas de voz (VoIP) pela internet, assim necessitam manter a conexão durante toda a transmissão. Outras aplicações como trocas de mensagem (SMTP) precisam conectar periodicamente para verificar se há novas mensagens [2]. Muitos outros protocolos foram incluídos ao decorrer dos anos como o sistema de nomes de domínio (DNS), que mapeia os nomes de hosts para seus respectivos endereços de redes, os protocolos HTTP e HTTPS são utilizados para buscar páginas na World Wide Web, protocolo MQTT que é utilizado para conectividade máquina a máquina (machine-to-machine (M2M)), entre muitos outros protocolos [1] [5].

Um dispositivo de IoT executando a função de servidor necessita de alta disponibilidade e deve estar sempre pronto para receber solicitações de acionamentos ou as informações por ele processadas disponíveis. Na prática, a confiabilidade destes dispositivos pode estar comprometida, em virtude de confiabilidade da rede, dos roteadores e de todos equipamentos pertencentes no

cenário. É difícil garantir até mesmo a alimentação de energia dos dispositivos IoT, pois geralmente os dispositivos estão inseridos em ambientes instáveis [2].

D. Camada de Transporte

O objetivo principal é entregar o fluxo de dados às aplicações. Possui a função de chavear os diversos pacotes de dados que chegam ao dispositivo, para as várias aplicações que fazem acesso à rede. Aplica também a função para controle de fluxo de congestionamento, garantia de entrega dos pacotes, incluindo a retransmissão de pacotes perdidos e reordenamento dos pacotes.

Para o chaveamento dos pacotes pela aplicação é utilizado um número entre 0 e 65535 (16 bits) como referência. Estes números são utilizados por processos e podem ser chamados de endereço de transporte ou também são chamados de porta de transporte [1]. A maioria das aplicações ou processos usam endereços fixos para facilitar o acesso. Existem diversas aplicações que possuem endereços fixos bem conhecidos tais como: HTTP (80), DNS (53), SSH (22), FTP (20 e 21), MQTT (1883) e entre outros [2].

O protocolo de transporte mais utilizado é o TCP, entretanto não é o único. O protocolo de datagrama do usuário (UDP) é usado em aplicações que não necessitam de garantia de entrega, reordenamento de pacotes ou qualquer controle de fluxo ou congestionamento [2]. Existe também o protocolo de mensagens de controle de internet (ICMP), usando apenas em aplicações de testes, como a famosa aplicação ping para verificar se um dispositivo está ativo e acessível.

E. Camada de Rede

A camada de redes é responsável pelo endereçamento universal dos dispositivos que estão conectados à rede. Isto é, necessita definir endereços de origem e destino dos pacotes que, a princípio, não deveriam ser alterados até seu destino [2]. O protocolo utilizado nesta camada é o protocolo de Internet (IP). Atualmente, duas versões desse protocolo estão ativas: IPv4 e IPv6.

Os 32 bits de endereçamento do IPv4 suportam na teoria 4,295x10^9 de elementos conectados, número que já é insuficiente em um cenário de IoT Mundial.

Além do mais, os endereços estão mal distribuídos pelo mundo, e ainda existem vários endereços reservados que não podem ser usados por ter funções especiais. Os 128 bits de endereçamento do IPv6 suportam na teoria 3,403x10^38 de dispositivos, ou seja, mais do que o necessário para o cenário previsto do crescimento no número de equipamentos IoT no cenário de desenvolvimento, onde cada equipamento poderia ter seu próprio IP.

F. Camada de Host/Rede ou Acesso à Redes

A camada de host/rede ou acesso a redes, encontrar-se abundantemente despedaçada em um grande vácuo. “O modelo de referência TCP/IP não especifica muito bem o que acontece ali, exceto o fato de que o host tem de se conectar à rede utilizando algum protocolo para que seja possível enviar pacotes IP. Esse protocolo não é definido e varia de host para host e de rede para rede.” [1]. Os livros e documentação que tratam do modelo TCP/IP raramente relatam ou descrevem sobre esta camada.

G. DHCP e DNS

Suponha que um cliente liga seu notebook, smartphone ou um dispositivo IoT e faz a conexão via Ethernet ou Wi-Fi em sua universidade. O roteador da universidade é conectado a um provedor de serviço de internet (ISP), que neste caso é a Telecom.

Quando o cliente conecta na rede pela primeira vez, não consegue fazer nada (por exemplo, abrir uma página Web ou um Web Services) sem um endereço IP. Assim, a primeira ação relacionada à rede, tomada pelo notebook é executar o protocolo DHCP para obter um endereço IP, bem como outras informações do servidor DHCP local [6]. Então o protocolo DHCP por meio de um servidor tem a função de distribuir automaticamente endereços IP diferentes a computadores à medida que eles fazem solicitações de conexão à rede [7].

Após o dispositivo do cliente possui um IP da rede, adquirido pela configuração manual ou automática pelo protocolo DHCP, o cliente está pronto para acessar a intranet ou internet, em seguida o cliente deseja se conectar em um website ou servidor, entretanto não se sabe qual o IP do site desejado, para facilitar

o acesso a este IP foi criado o protocolo DNS. O protocolo para sistema de nomes de domínio (DNS) é responsável por traduzir nomes que são mais fáceis de memorizar, para endereços IP. O acesso pode ser feito por meio de um nome que pode estar diretamente ligado ao serviço que queira acessar. Assim nomes como www.google.com.br, www.facebook.com, www.uemg.br, ou qualquer outro, podem ser localizados na internet com facilidade. Para que um dispositivo, consiga acessar serviços pelo nome, é preciso que o nome esteja devidamente registrado e que um servidor de DNS esteja ativo, possua alta disponibilidade e bem configurado [8].

A coordenação global da Raiz do DNS, o endereçamento IP e outros recursos do protocolo da Internet são executados conforme as funções da IANA (Internet Assigned Numbers Authority).

H. Meios de Comunicação

Os meios de comunicação em rede referem-se a cabos, fios e outros recursos usados para transmitir dados, onde vários bits são transportados de sua origem a seu destino. Os meios mais comuns para a comunicação de dados são o cabo de par trançado, o cabo coaxial, o cabo de fibra óptica e as conexões sem fio [6].

I. Padrão IEEE 802.11

O padrão IEEE 802.11 é internacionalmente conhecido como Wi-Fi, acrônimo para Wireless Fidelity. O termo Wi-Fi quer dizer um conjunto de especificações para redes locais sem fio (Wireless Local Área Network (WLAN)). Sua proposta, é conectar dispositivos em redes locais sem fio, é bastante questionado em seus vários aspectos, entretanto não impediu o padrão IEEE 802.11 de se tornar tão popular quanto a internet [2].

Possui vários padrões de rede sem fio como 802.11(a/b/g/n/ac) que precisam ser reestruturados para que não seja substituído por outra tecnologia que atenda melhor à evolução de IoT [2]. Esses padrões trabalham em uma faixa definida 2,4GHz a 5GHz, e essas redes possuem um número finito de elementos conectados na rede.

O Ponto de Acesso (Access Point (AP)) ou roteador wireless, é um dispositivo que interliga a rede ethernet à rede Wi-Fi para prover ao cliente o acesso à internet ou rede local. Na pilha de protocolos TCP/IP ocupa a camada de host/rede.

A escolha do padrão IEEE 802.11 elimina vários problemas da rede cabeada para dispositivos IoT, essa comunicação via Wi-Fi em relação às tradicionais LANs ou redes cabeadas. Adicionar novos clientes ou dispositivos via Wi-Fi é menos complicado e não perdem a conexão pelo motivo de cabos defeituosos. E mesmo sofrendo com ruídos eletromagnéticos é possível obter uma boa conexão para transferência de dados na rede, podendo também reposicionar o dispositivo inteligente pelo ambiente sempre que necessário no raio de alcance do sinal.

J. Redes Mesh

Um ecossistema IoT pode possuir diversos dispositivos conectados em uma grande área, de forma que pode se tornar muito difícil posicionar todos os dispositivos dentro do alcance da rede sem fio. Uma forma para ampliar o alcance do rádio e atender dispositivos que não estão próximos ao roteador, é usar a rede Mesh.

Em uma rede Mesh os dispositivos passam a exercer a função como roteadores, encaminhando mensagens de outros dispositivos para um AP que esteja a seu alcance ou, ainda, a outro dispositivo que esteja mais próximo de um AP, quando um dispositivo encaminha mensagem para outro dispositivo é popularmente conhecido como salto (Hop) [9].

A inteligência de roteamento é formada como uma única estrutura e autocorretiva distribuindo os clientes entre pontos de acesso, evitando gargalos na rede e melhorando o desempenho da rede. A tecnologia em malha ou padrão IEEE 802.11s também melhora a robustez e velocidade da rede, uma vez que o cliente está conectado em um nó e o mesmo para de funcionar ou possua muitas requisições gerando a concorrência, o sistema se realoca automaticamente, desviando o nó defeituoso com transparência, sem que o usuário perceba ou perca a conexão [10].

K. RFID e Padrão RFC

A tecnologia de identificador por radiofrequência é conhecida como RFID (Radio FrequencyIdentifier), é uma identificação automática sem fio e tecnologia de captura de dados (AutomaticI dentification and Data Capture (AIDC)). Um sistema RFID é composto por três componentes principais: 1) Etiquetas (tags) onde a informação fica armazenada; 2) Sistema para leitura/gravação; 3) O sistema interessado na informação, geralmente um hardware midd leware aplicativo que decide o que fazer [11].

Existem ainda dois tipos de Tags: 1) Passivas; 2) Ativas. As tags passivas utilizam a rádio frequência do leitor para transmitir o seu sinal e normalmente têm suas informações gravadas permanentemente quando são fabricadas, entretanto algumas destas etiquetas são regraváveis. As tags ativas são muito mais sofisticadas e caras e contam com uma bateria própria para transmitir seu sinal sobre uma distância razoável, além de permitir armazenamento em memória RAM capazes de armazenar até 32KB [11]. O RFID possui diversas frequências na tabela 1 é demonstra as frequências do RFID e suas faixas de alcances [12].

Tabela 1 - Frequências RFID

Nome	Frequência	Faixa de alcance
Baixa frequência	125KHz	50 centímetros
Alta frequência	13,56MHz	3 metros
ultra alta frequência	860-960MHz	9 metros
Micro-ondas	2,45GHz	10 metros

A figura 4 apresenta o funcionamento de um sistema RFID conhecido no Brasil como “SEM PARAR”. Após instalar no veículo, a tag Sem Parar usa o sistema de radiofrequência para liberar automaticamente as cancelas nas praças de pedágios e estacionamentos, ou mesmo identificar e autorizar transações em estacionamentos que não contam com cancelas [13].

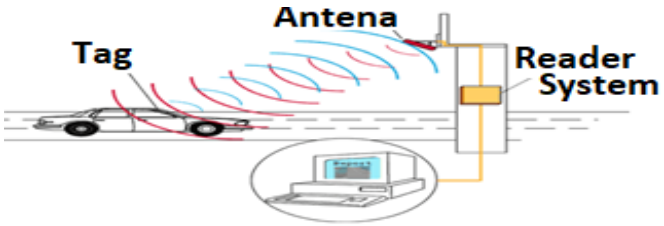

Figura 4 - Funcionamento do RFID.

O padrão de comunicação por proximidade ou campo próximo (Near Field Communication, NFC), foi projetado para comunicação entre dispositivos muito próximos, da ordem de centímetros. Este padrão está disponível em vários tipos de dispositivos, desde smartphones, caixas eletrônicos, porteiros eletrônicos, equipamentos portáteis, e suas aplicações são mais diversificadas que o RFID, pode ser usado também para, transferir arquivos ou manter a comunicação de quaisquer outras aplicações, assim sua proposta de curtas distancia o torna mais seguro. As aplicações do NFC são geralmente para transações comercias, como transferência de recursos, possivelmente substituíndo cartões de credito e outras formas de pagamento [2].

O RFID e NFC são fundamentais para IoT. São usadas em aplicações de controle de acesso, logística, controle de estoque, transferência de recursos, comercio eletrônico e físico, entre outros tipos que se possam inventar agregando as tecnologias de RFID e NFC às demais tecnologias embarcadas e com comunicação sem fio previstas em IoT.

L. Protocolos Específicos para IOT

Existem diversos modelos de referência, o modelo TCP/IP é usado para os protocolos na internet. Pelo fato da IoT ter sido baseado com os princípios da internet. O modelo TCP/IP possui apenas quatro camadas: Aplicação, Transporte, Internet e Rede [1].

Existem alguns protocolos propostos exclusivamente para os ambientes automatizados, ou ainda para redes de sensores sem fio, que é parecido com o conceito IoT, com baixa demanda de largura de banda, presença de muitos dispositivos na rede, alcance limitado a poucos metros e necessidade de eficiência

energética. Percebe-se que essas propostas são muito diferentes dos objetivos previstos inicialmente em redes Wi-Fi.

Os protocolos IEEE 802.15 foram desenvolvidos para as redes conhecidas como redes sem fio que alcançam poucos metros de distância (Wireless Personal Area Network (WPAN)). O protocolo Bluetooth está incluindo nesse padrão. Fazem parte desse padrão os protocolos ZigBee, 6LoWPAN, Wireless Hart, ISA100.11a, ESP-NOW, ESP-MESH e MQTT.

a. Bluetooth e Bluetooth Low Energy

O protocolo Bluetooth, definido no padrão IEEE 802.15 foram projetados para as redes conhecidas como WPAN a se tornar comercial e se popularizar, utilizado. Onde facilmente encontrado em vários dispositivos dispositivo. Aplicações que popularizou o Bluetooth foi transferência de dados, ligação de periféricos como fones de ouvidos, sistemas de som, teclados e mouse, tanto a celulares, gadgets, dispositivos IoT [2].

Uma variação do Bluetooth é conhecida como BLE (Bluetooth Low Energy) sua característica é o baixo consumo de energia, assim muito utilizado para aplicações que exigem um tempo de vida elevado de bateria. Embora alguns recursos do BLE sejam herdados do controlador Bluetooth clássico, os dois tipos de controlador são atualmente incompatíveis. Opera na banda Industrial Scientific Medical (ISM) de 2,4GHz e define 40 canais de radiofrequência (RF) com espaçamento de 2MHz. Alcance limitado a 50m [14].

b. ZigBee

O padrão ZigBee utiliza os protocolos definidos no padrão 802.15.4 na camada de enlace e na camada física. Suas características incluem baixo consumo de energia, baixa taxa de transmissão e baixo custo de implementação. O alcance é limitado no máximo 100m. Para atingir distancias maiores, conta com o repasse das informações pelos nós da rede, em múltiplos saltos até alcançar o seu destino [15].

c. 6LoWPAN

O 6LoWPAN, que significa IPv6 (Over Low Power Wireless Personal Area Networks). A proposta é encapsular o protocolo IPv6 para redes sem fio de curto alcance, utilizando o padrão IEEE 802.15.4 nas camadas de enlace e física. Para isso, os cabeçalhos IPv6 devem ser fragmentados, compactados e reagrupados, não é uma questão fácil, por que os cabeçalhos IPv6 possuem 128bits, logo são muito extensos, entretanto isso torna cada dispositivo IoT tenha um endereço único [15].

d. LoRaWAN

Para atender as redes IoT de longa distância, existe a Lo RaWAN (Long Range Wide Area Network), essa proposta está focada em acessos a dispositivos a até 15 quilômetros de distância, utilizando uma estação de rádio de longo alcance. Para atingir distancias maiores as frequências estão entre 433 e 915MHz, há diversas aplicações que podem ter grandes utilidades no futuro para serviços de tarifação como agua, energia, gás encanado entre outros tipos de serviços [15].

e. ESP-MESH

O avanço da IoT requer um número vasto de nós para se conectar à internet. No entanto, apenas um número limitado de nós (geralmente menos de 32) pode se conectar diretamente ao mesmo roteador [16]. Existem diversos protocolos que foram criados para resolver este problema. Assim o protocolo ESP-MESH criado pela empresa ESPRESSIF, em uma rede mesh, onde cada dispositivo IoT se torna um nó, os nós podem estabelecer uma rede e encaminhar pacotes. Como resultado, um grande número de nós se conectar à Internet sem melhoria no roteador atual.

A figura 5 é um exemplo de rede mesh, utilizando o protocolo ESP- Mesh utilizando apenas uma conexão ao roteador [16]. O uso do protocolo ESP- Mesh, pode se tornar um protocolo emergente para controlar uma grande rede de dispositivos como lâmpadas e interruptores IoT, utilizando apenas poucas conexões diretas ao roteador.

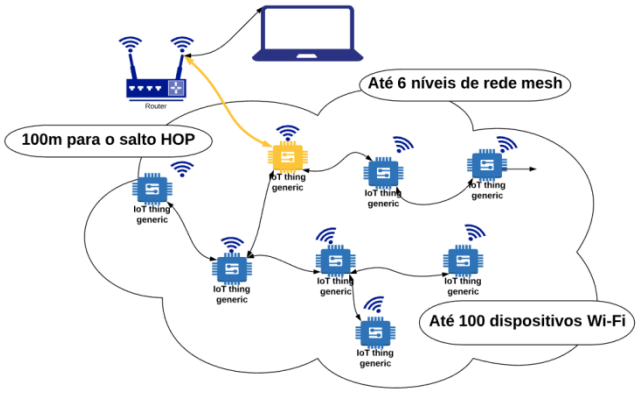

Figura 5 - Protocolo de rede ESP-Mesh. Autoria própria.

f. ESP-NOW

O ESP-NOW é um tipo de protocolo de comunicação Wi-Fi sem conexão que é definido pela ESPRESSIF, não faz uso do protocolo TCP. No ESP-NOW os dados da aplicação são encapsulados no quadro de ação específico do fornecedor e depois transmitidos de um dispositivo Wi-Fi para outro sem conexão. O protocolo CBC-MAC (CCMP (Cryptography) é usada para proteger o quadro de ação para segurança. ESP-NOW é amplamente utilizado em ambientes de iluminação inteligente, controle remoto, sensores, atuadores, entre outros dispositivos IoT [17].

O ESP-Now permite que vários dispositivos se comuniquem sem usar o roteador Wi-Fi transmissão entre os dispositivos. O protocolo é semelhante à conectividade sem fio de baixa potência de 2,4 GHz que é frequentemente implantada em mouses sem fio. Assim, o emparelhamento entre dispositivos é necessário antes da comunicação. Após o pareamento, a conexão é persistente, peer-to-peer (P2P), e nenhum handshake é necessário [18], e torna o protocolo mais eficiente e veloz na comunicação entre dispositivos IoT.

g. MQTT

O protocolo MQTT (Message Queue TelemetryTransport) está localizado na camada de aplicação do TCP/IP. A porta TCP/IP 1883 é reservada com a IANA para uso com o MQTT. A porta TCP/IP 8883 também está registrada, para usar o MQTT sobre SSL [5].

MQTT é um protocolo de mensagens extremamente simples e leve de publicação / assinatura (publish / subscribe), projetado para dispositivos restritos e redes de baixa largura de banda, alta latência ou não confiáveis. Os princípios de design são minimizar a largura de banda e os requisitos de recursos dos dispositivos, ao mesmo tempo em que tentam garantir a confiabilidade e um certo grau de garantia de entrega [5]. Esses princípios tornam o protocolo ideal para as tecnologias emergentes no mundo de dispositivos conectados “máquina a máquina” (M2M) ou “Internet das Coisas” de dispositivos inteligentes conectados, e para aplicações moveis onde a largura de banda e bateria são essenciais, também conta com segurança de entrega de mensagens por QoS (Quality of Service).

h. INTERNET

A internet nasceu da ARPANET, uma rede experimental financiada pelos militares dos Estados Unidos, sendo que a mesma nasceu interligando universidades e centros de pesquisa, permitindo aos pesquisadores compartilhar a capacidade de processamento dos seus equipamentos [19]. A internet está sofrendo diversas transformações desde seu início.

A Internet pode ser dividida em três níveis, no primeiro nível era apenas uma rede de computadores, no segundo nível se tornou uma rede de pessoas e comunidades, atualmente estamos começando a presenciar o terceiro nível que é a Internet das Coisas [20]. Vários tipos de dispositivos inteligentes interligados capturando, analisando e processando dados podendo executar ações, tornando o cotidiano cada vez mais fácil.

RESULTADOS E DISCUSSÃO

A internet e os computadores estão parecem estar desaparecendo, esta impressão é justamente porque cada vez mais, eles estão presentes em tudo a nossa volta e nem reparamos mais neles, simplesmente esperamos que estejam lá [20]. Para Mark Weiser “As tecnologias mais importantes são aquelas que desaparecem. Elas se integram à vida do dia a dia, ao nosso cotidiano, até serem

indistinguíveis dele.” [21]. Assim resultando também no conceito de computação pervasiva ou ubíqua, onde existe a onipresença da tecnologia no cotidiano das pessoas.

CONSIDERAÇÕES FINAIS

Para manter a confiabilidade dos serviços prestados pelos dispositivos IoT é importante considerar a presença de um dispositivo intermediário, que possua alta disponibilidade e confiabilidade, que faça a interface entre as solicitações recebidas pelos usuários e as informações disponibilizadas pelos dispositivos IoT [2]. O protocolo MQTT atende a todas essas demandas através de equipamentos que são denominados de brokers, que fazem essa intermediação e são os chamados hardwares midd leware.

Existem vários brokers disponíveis na internet de forma gratuita. Nessa configuração associa-se o conceito de IoT ao conceito de Computação na nuvem (Cloud Computing), visto que o broker está na “nuvem”, ou seja, em algum lugar da internet cuja localização não é importante, apenas o serviço que ele disponibiliza [5].

Os protocolos de comunicação influenciam muito dependendo do projeto. Pois geralmente os dispositivos IoT estão em ambientes completamente hostis, por meios da precariedade da rede onde são imersos, os protocolos podem prevenir o congestionamento da rede, no caso de possuir um baixo consumo de banda, ou pela falta de energia, existe a necessidade de eficiência energética dos dispositivos inteligentes, para uma duração maior das baterias. A utilização de brokers On-Premise e Cloud Server são também a solução para garantir a confiabilidade de entrega dos pacotes de dados para os dispositivos.

REFERÊNCIAS

TANENBAUM, A. S. “Redes de Computadores”. Tradução de Vandenberg D. de Souza. Quarta Edição. Ed. Rio de Janeiro: Elsevier, vol. 1, 2003.

OLIVEIRA, S. D. “Internet das Coisas com ESP8266, Arduino e Raspberry Pi”, Novatec,1ª Edição, vol. 1, São Paulo, 2017.

CASTELUCCI, D. (2011). Protocolos de comunicação em redes de computadores. Acedido em 23 de Março de 2018, em:https://daniellacastelucci.wordpress.com/2011 / 04 / 08 / protocolos - de - comunicação – em – redes – de - computadores.

I
NTERNET-GUIDE.CO.UK. DOD TCP/IP. Acedido em 06 de Abril de 2018, em: http://www.internet-guide.co.uk/dod.html.

A. STANFORD - CLARK, A. NIPPER (2014), MQTT, MQTT.ORG, Acedido em 07 de Abril de 2018, em: http://mqtt.org.

J. KUROSE, K. ROSS, “Redes de computadores e a internet: uma abordagem top-down.”, Pearson Education do Brasil, Tradução de Daniel Vieira. vol. 1, 6ª Edição, São Paulo, 2013.

R. DROMS (1997), Dynamic Host Configuration Protocol, IETF: Network Working Group, Acedido em 09 de Abril de 2018, em: https://www.ietf.org/rfc/rfc2131.txt.

P. MOCKAPETRIS (1987), Domain Names – implementation and specification, IETF: Network Working Group, Acedido em 09 de Abril de 2018, em: https://www.ietf.org/rfc/rfc1035.txt.

T. M. CARDOSO, P. C. F. MARQUES, “Rede Mesh: topologia e aplicação”, Revista iTEC, Osório, vol. 4, no. 4, pp. 16-25, Julho 2012.

D. CRISTINA, D. et al; “Multihop MAC: Desvendando o Padrão 802.11s”, Livro de Minicursos do Simpósio Brasileiro de Redes de Computadores, Rio de Janeiro, vol. 1, no. 26, pp. 13-59, Maio 2008.

L. CASTRO, S. F. WAMBA, “An Inside Look At RFID Technology”, Journal of Technology Management &Innovation, Santiago, vol. 2, no. 1, pp. 128-141, Janeiro 2007.

J. S. ROCHA (2014), Funcionamento da RFID, Sala da Automação, Acedido em 12 de Abril de 2018, em: http://saladaautomacao.com.br/funcionamento-da-rfid.

SEMPARAR (2018), Como Funciona: Sobre a Tecnologia, Acedido em 13 de Abril de 2018, em: https://www.semparar.com.br/como-funciona.

C. GOMES, J. OLLER, J. PARADELLS, “Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology”, Sensors, Basileia, vol. 1, no. 12, pp. 11734-11753, Agosto 2001.

Y. DING, S. H. HONG, R. LU, J. KIN, Y. H. LEE, A. XU, L. XIAOBING, “Experimental Investigation of the Packet Loss Rate of Wireless Industrial Networks in Real Industrial Environments”, 2015 IEEE International Conference on Information and Automation, Lijiang, vol. 1, no. 1, pp. 1048-1053, August/October 2015.

ESPRESSIF (2018), ESP- Mesh, ESPRESSIF, Acedido em 10 de Abril de 2018, em: https://www.espressif.com/en/products/software/esp-mesh/overview.

ESPRESSIF (2016), ESP-NOW User Guide, ESPRESSIF, Acedido em 13 de Abril de 2018, em: https://www.espressif.com/sites/default/files/documentation/esp-now_user_guide_en.pdf.

ESPRESSIF (2018), ESP-NOW, ESPRESSIF, Acedido em 15 de Abril de 2018, em: https://www.espressif.com/en/products/software/esp-now/overview.

A. MACHADO, (2009), Há 40 anos, surgia a Arpanet, o embrião da internet, NIC.br, Acedido em 25 de Março de 2018, em: https://www.nic.br/noticia/na-midia/ha-40-anos-surgia-a-arpanet-o-embriao-da-internet.

NIC.br, A Internet das Coisas, explicada pelo NIC.br, Youtube, 16 de Julho de 2014, É uma explicação do nic.br, Acedido em 25 de Março de 2018 em: https://www.youtube.com/watch?v=jlkvzcG1UMk.

F. L. DOMINGUES (2008), Computação Ubíqua, Guia do Hardware, Acedido em 03 de Abril de 2018, em: https://www.hardware.com.br/artigos/computacao-ubiqua/.

AUTORES:

Lucas Lima Freire Brito: Bacharel em Engenharia de Computação da UEMG – Unidade Ituiutaba. lucas.lfreire@gmail.com

Ígor Andrade Moraes: Bacharel em Engenharia de Computação da UEMG – Unidade Ituiutaba da UMG – Unidade Ituiutaba. igorandradesystem@gmail.com

Maria Luiza Trindade Moraes:

Milton Miranda Neto: Coordenador do Curso de Sistemas de Informação da UEMG – Unidade Ituiutaba. voidmmn@gmail.com

Mônica Rocha Ferreira de Oliveira: Docente na UEMG – Unidade Ituiutaba. Monica.oliveira@uemg.br

Vinicius Angelo De Oliveira Muniz: Bacharel em Engenharia de Computação da UEMG – Unidade Ituiutaba. vinnyangelo@gmail.com