ROSANA LACHOWSKI

PROTOCOLOS CENTRADOS EM INFORMAÇÃO PARA REDES DE SENSORES SEM FIO DE LARGA ESCALA

Curitiba - PR, Brasil

2020

ROSANA LACHOWSKI

PROTOCOLOS CENTRADOS EM INFORMAÇÃO PARA REDES DE SENSORES SEM FIO DE LARGA ESCALA

Tese apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de doutor em Informática.

Pontifícia Universidade Católica do Paraná - PUCPR

Programa de Pós-Graduação em Informática - PPGIa

Orientador: MARCELO EDUARDO PELLENZ

Coorientador: EDGARD JAMHOUR

Curitiba - PR, Brasil

2020

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Pamela Travassos de Freitas – CRB 9/1960

L138p 2020

Lachowski, Rosana
Protocolos centrados em informação para redes de sensores sem fio de larga escala / Rosana Lachowski ; orientador: Marcelo Eduardo Pellenz ; coorientador: Edgard Jamhour.– 2020.
87 f. : il. ; 30 cm

Tese (doutorado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2020
Bibliografia: f. 78-87

1. Internet. 2. Comunicação - Inovações tecnológicas. 3. Internet das coisas. 4. Redes de informação. 5. Rede de computador – Protocolos. 6. Sistemas de comunicação sem fio. I. Pellenz, Marcelo Eduardo. II. Jamhour, Edgard. III. Pontifícia Universidade Católica do Paraná. Pós-Graduação em Informática. IV. Título.

CDD 22. ed. – 004.699

Pontifícia Universidade Católica do Paraná
Escola Politécnica
Programa de Pós-Graduação em Informática

12-2021

DECLARAÇÃO

Declaro para os devidos fins que a aluna **ROSANA LACHOWSKI**, defendeu sua tese de doutorado intitulada **"PROTOCOLOS CENTRADOS EM INFORMAÇÃO PARA REDES DE SENSORES SEM FIO DE LARGA ESCALA"**, na área de concentração Ciência da Computação, no dia 09 de dezembro de 2020, no qual foi aprovada.

Declaro ainda que foram feitas todas as alterações solicitadas pela Banca Examinadora, cumprindo todas as normas de formatação definidas pelo Programa.

Por ser verdade, firmo a presente declaração.

Curitiba, 03 de março de 2021.

Prof. Dr. Emerson Cabrera Paraiso
Coordenador do Programa de Pós-Graduação em Informática
Pontifícia Universidade Católica do Paraná

AGRADECIMENTOS

É difícil para mim expressar em poucas palavras a grande gratidão que sinto pelas pessoas que fizeram parte de minha caminhada nos dez últimos anos na Pontifícia Universidade Católica do Paraná. Todas foram especiais e importantes desde o primeiro dia.

Primeiramente agradeço à Deus, fonte de toda sabedoria, pela inspiração, força nas adversidades e principalmente pelas pessoas que colocou em meu caminho para que eu tivesse a oportunidade de concretizar um grande sonho.

Gostaria de expressar minha profunda admiração ao meu orientador Prof. Dr. Marcelo E. Pellenz, coorientador Prof. Edgard Jamhour e Prof. Manoel Camillo Pena. Agradeço pelo incentivo, paciência, apoio e amizade. Serei para sempre grata por guiarem meus passos na grande aventura do conhecimento. Sem vocês este trabalho não seria possível.

Agradeço à todos os colegas pelas conversas sobre as coisas da vida, pelas sugestões e críticas e pela amizade que levarei para sempre. Especialmente Allan, Andreia, Cheila, Edenilson, Franciele, Irapuru, Jhonatan, Marisa, Sediane, Tania e Viviane.

Agradeço à Pontifícia Universidade Católica do Paraná por ter me acolhido tão bem durante tantos anos e pelo apoio financeiro.

Além disso, gostaria de agradecer a todos os funcionários, que provavelmente não imaginam como seus pequenos e grandes gestos significaram tanto para mim.

Agradeço aos pesquisadores da Fundação Agrária de Pesquisa Agropecuária (FAPA) por bondosamente compartilharem seus conhecimentos.

Finalmente, agradeço minha família pela compreensão e apoio. Especialmente às minhas filhas Ana Vitória e Ana Thereza que foram a principal fonte de incentivo. Agradeço ainda aos meus pais Romoaldo e Tereza, ao meu esposo Marcus e à minha querida tia Elza por sempre acreditarem em mim.

Obrigada!!

Se eu vi mais longe, foi por estar sobre ombros de gigantes. Isaac Newton

Para Ana Vitória e Ana Thereza

A maravilhosa disposição e harmonia do universo só pode ter tido origem segundo o plano de um Ser que tudo sabe e tudo pode. Isso fica sendo a minha última e mais elevada descoberta. Isaac Newton

RESUMO

Redes de Sensores sem Fio (RSSF) são um elemento essencial da Internet das Coisas (Internet of Things - IoT), cujas aplicações com enorme potencial para melhorar a vida humana podem envolver implantação massiva de dispositivos e grandes volumes de dados. RSSFs de larga escala apresentam diversos desafios e requerem que as abordagens tradicionais nas áreas de redes, computação, fornecimento e gerenciamento de serviços sejam repensadas. Um dos principais desafios está relacionado com a construção de rotas para entrega de dados. Os protocolos de rede convencionais apresentam estratégias inviáveis para redes de larga escala e podem não ser diretamente aplicáveis aos ambientes IoT. Especialmente com relação ao envio de comandos e consultas para a rede, é urgente propor soluções escaláveis, confiáveis e eficientes. Outras dificuldades estão relacionadas com a comunicação com múltiplos dispositivos e ao ambiente altamente dinâmico. Embora comunicar-se com grupos de dispositivos seja essencial em muitas situações, este modo de comunicação recebeu pouca atenção, levando a soluções que apresentam severas limitações. Neste trabalho, propomos protocolos de comunicação inspirados no paradigma Rede Centrada em Informações (Information-Centric Networking - ICN) para superar os desafios enfrentados por RSSFs de larga escala: ICENET (Information Centric Protocol for Big Data Wireless Sensor Networks) e ICENET-PB (ICENET-Priority Based). ICN é uma abordagem revolucinária proposta para a Internet do Futuro cuja principal característica é o foco nas informações fornecidas pelos nós da rede. Os protocolos propostos representam soluções eficientes, confiáveis e escaláveis para o encaminhamento de consultas para a rede e coleta de grandes volumes de dados. Adotamos um mecanismo de estado flexível (*soft-state*) para tratar perdas de pacotes e mudanças na topologia da rede devido ao ambiente dinâmico das comunicações em fio. ICENET-PB estende as funcionalidades do ICENET para aplicações que não requerem dados de todos os dispositivos implantados em uma determinada área ou que monitoram determinados parâmetros físicos, mas um determinado subconjunto de dados que represente significativamente a informação solicitada. Resultados mostram que as os protocolos apresentam uma sobrecarga significativamente menor, enquanto coletam aproximadamente a mesma quantidade de dados de um número maior de nós do que o CoAP, um popular protocolo para ambientes IoT.

Palavras-chave: Redes de Sensores sem Fio, Redes Centradas em Informação, Internet das Coisas, Redes de larga escala.

ABSTRACT

Wireless Sensor Networks (WSNs) are an essential element of the Internet of Things (IoT), whose applications present huge potential to improve human life and may involve massive device deployment and large volumes of data. Large-scale WSNs involve several challenges and require to rethink traditional approaches in the areas of networking, computing, service delivery and management. One of the main challenges is related to the construction of routes for data delivery. Conventional network protocols present unfeasible strategies for large-scale networks and may not be directly applicable to IoT environments. Especially with regard to sending commands and queries to the network, it is urgent to propose scalable, reliable and efficient solutions. Other difficulties are related to the communication with multiple devices and the highly dynamic environment. Although communicating with groups of devices is essential in many situations, this mode of communication has received little attention, leading to solutions that have severe limitations. In this thesis, we propose communication protocols inspired by the Information-Centric Networking (ICN) paradigm in order to overcome challenges faced by large-scale WSNs: ICENET (Information Centric Protocol for Big Data Wireless Sensor Networks) e ICENET-PB (ICENET-Priority Based). ICN is a revolutionary approach proposed for the Internet of the Future whose main characteristic is the focus on information provided by network nodes. The proposed protocols represent efficient, reliable and scalable solutions for forwarding queries to the network and collecting large volumes of data. A soft-state mechanism is adopted in order to handle packet losses and changes in the network topology due to the dynamic environment of wireless communications. ICENET-PB extends the functionality of ICENET to attend applications that do not require data from all devices deployed in a given area or that monitor certain physical parameters, but a certain subset of data that significantly represents the requested information. Results show that ICENET and ICENET-PB present significantly less overhead, while collecting approximately the same amount of data from a larger number of nodes than CoAP (Constrained Application Protocol), a popular protocol for IoT environments.

Keywords: Wireless Sensor Networks, Information-Centric Networking, Internet of Things, large-scale networks.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ATTR	atributo
CSMA/CA	Carrier sense multiple access with collision avoidance
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
CS	Content Store
dB	decibel
dBm	decibel milliwatt
DAO	Destination Advertisement Object
DD	Directed Diffusion
DIO	DODAG Information Object
DIS	DODAG Information Solicitation
DODAG	Destination Oriented Directed Acyclic Graph
DS	fontes de dados
EM	Entity Manager
ET	data de expiração
FIB	Forwarding Information Base
HTTP	Hypertext Transfer Protocol
Icache	Interest Cache
ICENET	Information Centric Protocol for Big Data Wireless Sensor Networks
ICENET-PB	ICENET-Priority Based
ICN	Information-Centric Networking – Redes Centradas em Informação
ID	identificação

IEEE	Institute of Electrical and Electronics Engineers – Instituto de Engenheiros Eletricistas e Eletrônicos
IETF	Internet Engineering Task Force
IoT	Internet of Things – Internet das Coisas
IP	Internet Protocol – Protocolo da Internet
LLNs	Low Power Lossy Networks – Redes de baixa potência e com alta probabilidade de perda de pacotes
MAC	Media Access Control – Controle de Acesso ao Meio
M2M	machine-to-machine – máquina-para-máquina
M2P	multiponto-para-ponto
MPL	Multicast Protocol for Low-Power and Lossy Networks
MQTT	Message Queue Telemetry Transport
MQTT-SN	MQTT for Sensors Networks
PHY	camada Física
PIT	Pending Interest Table
P2M	ponto-para-multiponto
P2P	ponto-a-ponto
REST	Representational State Transfer
RPL	Routing Protocol for Low Power and Lossy Networks
RSSF	Redes de Sensores sem Fio
SMRF	Stateless Multicast RPL Forwarding
SNR	signal-to-noise ratio – relação sinal-ruído
SP	sample period – período de amostragem
SR	sample rate – taxa de amostragem de dados
TCP	Transmission Control Protocol
TS	timestamp
UDP	User Datagram Protocol
URI	Universal Resource Identifier

LISTA DE SÍMBOLOS

c	contador de consistências
d_{ij}	distância entre os nós i e j
h_{ij}	ganho do canal
I	intervalo de tempo corrente
$I_{\max}$	intervalo de tempo máximo
$I_{\min}$	intervalo de tempo mínimo
k	nós filhos que deveriam enviar dados em resposta a um Interesse (fontes de dados)
N	potência do ruído
N	número de nós
p	nível de prioridade
P_r	potência média recebida
$P_r(d_0)$	potência recebida a uma distância de referência d_0
$parent_i$	nó pai de i
R	região de implantação
t	ponto de tempo aleatório
S	sombreamento
T_u	temporizador local
γ_{ij}	relação sinal-ruído instantânea
α	expoente de perda de percurso
σ^2	variância

SUMÁRIO

1 INTRODUÇÃO

Nos últimos tempos, as Redes de Sensores sem Fio (RSSF) tornaram-se um elemento essencial da Internet das Coisas (Internet of Things - IoT), cujas aplicações podem envolver implantação massiva de dispositivos e um grande volume agregado de dados. A IoT permite que dispositivos simples capazes de monitorar parâmetros físicos do ambiente possam trocar dados, interagir com usuários e com o ambiente, além de tomar decisões coordenadas a fim de oferecer uma classe totalmente nova de aplicações e serviços: cidades inteligentes (Smart Cities) (Arasteh et al., 2016; LV; HU; LV, 2020), redes de transmissão e distribuição de energia inteligentes (Smart Grids) (KABALCI, 2016; ZHOU et al., 2020), monitoramento ambiental, agricultura inteligente (Smart Agriculture - SA) (MAZZETTO; GALLO; SACCO, 2020) e Indústria 4.0 (AHMED et al., 2016; WEN; GAO; LI, 2019), assim como outros sistemas ciber-físicos inteligentes (TAVCAR; HORVATH, 2018). Estas novas aplicações possuem potencial para melhorar drasticamente a maneira como as pessoas vivem, aprendem, trabalham e se divertem. Além disso, a IoT tornou a Internet sensorial (medidas de temperatura, pressão, vibração, luz, umidade) e deste modo permitiu ações mais proativas e menos reativas (EVANS, 2011).

Os recursos oferecidos para facilitar a vida humana são tão numerosos que a revolução causada pela IoT tem sido comparada com a construção de estradas e ferrovias durante a Revolução Industrial dos séculos 18 e 19 (MARTIN, 2014). Entretanto, a interconexão de um número massivo de dispositivos físicos com capacidade de comunicação e sensoriamento, a fim de oferecer determinado serviço, exige repensar abordagens tradicionais nas áreas de redes, computação, fornecimento e gerenciamento de serviços (MIORANDI et al., 2012).

Os nós sensores são dispositivos simples, que apresentam recursos computacionais restritos e comunicam-se por meio de ondas de rádio de curto alcance. Em implantações de larga escala, os nós sensores são densamente implantados em áreas geográficas extensas. Nestes cenários, a comunicação direta com o destino final é frequentemente inviável. Além disso, certas tecnologias de comunicação emergentes de baixo custo requerem comunicação a curtas distâncias. Por este motivo, os nós necessitam organizar-se para colaborativamente construir rotas e entregar seus dados. Para isto, cada um dos dispositivos envia os dados monitorados e recebidos para um determinado nó vizinho em direção ao destino. Como os dados percorrem múltiplos enlaces, este modo de comunicação é denominado múltiplos saltos (*multi-hop*).

As RSSFs possuem ainda outras características muito específicas: os dispositivos são propensos a falhas e comunicam-se por enlaces não confiáveis com baixa taxa de dados. Estas características tornam o ambiente altamente dinâmico e favorecem a ocorrência de

perdas de pacote. Além disso, os nós sensores podem exaurir suas reservas energéticas e deixar de exercer suas atividades. Por isto, um dos principais requisitos é a utilização eficiente dos recursos energéticos (Shahid; Aneja, 2017).

Tradicionalmente o endereço dos nós é utilizado para a construção das rotas e entrega dos dados. Porém, considerando as particularidades e limitações das RSSFs e especialmente em implantações de larga escala, esta abordagem é complexa e inadequada (LOCKE, 2010). Significa que os nós necessitam ter o conhecimento de uma grande número de endereços em um ambiente dinâmico. Esta exigência implica alto consumo energético para manter as informações atualizadas e a utilização pouco eficiente dos escassos recursos dos nós sensores (memória, armazenagem e processamento).

Outra dificuldade apresentada pelas RSSFs diz respeito ao volume dos dados coletados. Os nós sensores produzem um imenso conjunto de dados, que é extremamente dificil de ser coletado, armazenado, processado e analizado utilizando-se metologias e abordagens de computação tradicionais (MISIC; ALI; MISIC, 2018). A coleta de grandes volumes de dados por uma rede que apresenta recursos restritos é uma tarefa dificil e apresenta vários desafios (RANI et al., 2017; TAKAISHI et al., 2014). Um destes desafios está relacionado com a coleta de dados de múltiplos dispositivos.

Aplicações IoT usualmente requerem comunicação com múltiplos dispositivos ao mesmo tempo (SINGH; AL-TURJMAN, 2014; OIKONOMOU; PHILLIPS; TRYFONAS, 2013; RAHMAN; DIJK, 2014). Às vezes, é necessário obter dados de todos os dispositivos implantados em uma área específica ou de todos os dispositivos que monitoram determinados parâmetros físicos. Em outros casos, é suficiente obter um conjunto de dados que representem significativamente as informações. Apesar disso, a comunicação com múltiplos dispositivos na IoT recebeu pouca atenção, levando a soluções que apresentam limitações severas e inviáveis para redes de larga escala (ZHONG; LIANG, 2018; IOVA et al., 2016; ISHAQ et al., 2016; ISTOMIN; KIRALY; PICCO, 2015). Ademais, a coleta dos dados não envolve apenas o envio de dados até o destino final, mas também o encaminhamento de consultas e comandos para a rede (XIAO et al., 2019). Neste sentido, é cada vez mais urgente propor soluções escaláveis, confiáveis e eficientes para o tráfego descendente de dados nas aplicações emergentes das RSSFs de larga escala (ZHONG; LIANG, 2018).

As dificuldades apresentadas acima podem ser superadas por meio de uma abordagem centrada em informações. Redes Centradas em Informação (Information-Centric Networking - ICN) é um paradigma promissor para a arquitetura da Internet do Futuro, no qual o roteamento de dados está baseado nas informações fornecidas pelos nós (conteúdo) ao invés de baseado no endereço dos nós. Dados são enviados apenas em resposta a uma solicitação que especifica o nome dos dados a serem recuperados.

O paradigma ICN possui um modelo de comunicação especialmente adequado para RSSFs, uma vez que a principal tarefa destas redes é a coleta de dados. Em uma

RSSFs centrada em informações, consultas enviadas ao nós solicitam que o ambiente seja monitorado a uma determinada taxa e por um certo período de tempo. Os dados correspondentes são enviados ao nó gateway (*sink*). A comunicação de dados baseada em informações é escalável, facilita a coleta de dados e também o desenvolvimento de aplicativos, pois os dados são solicitados pelo nome e o endereço dos nós é transparente. O potencial e os benefícios do paradigma ICN nas RSSFs foram investigados em (AL-TURJMAN, 2016; SINGH et al., 2014; SINGH; AL-TURJMAN, 2014; XU; NGAI; LIU, 2014; AMADEO et al., 2013; DINH; KIM, 2013; DO; KIM, 2013). O paradigma ICN representa uma abordagem revolucionária na área de redes de comunicação (JABER; KACIMI; GAYRAUD, 2017; VIRGILIO; MARCHETTO; SISTO, 2013).

Nesta tese, propomos protocolos inspirados no paradigma ICN para atender os requesitos de RSSFs de larga-escala: ICENET (Information Centric Protocol for Big Data Wireless Sensor Networks) (LACHOWSKI et al., 2019) e ICENET-PB (ICENET-Priority Based)(LACHOWSKI et al., 2020). ICENET é uma solução eficiente, confiável e escalável para o encaminhamento de consultas para a rede e coleta de grandes volumes de dados. ICENET-PB estende as funcionalidades do ICENET para atender aplicações que não requerem dados de todos os dispositivos implantados em uma determinada área ou que monitoram determinados parâmetros físicos. Nestes casos, um determinado subconjunto confiável e preciso de dados é suficiente.

1.1 Motivação

Segundo o último relatório da Cisco sobre a Internet, o número de dispositivos conectados excederá três vezes a população global até 2023 (CISCO, 2020). Isto gerará uma rede global de dispositivos de dimensões sem precedentes. Entretanto, protocolos de rede convencionais apresentam estratégias inadequadas para redes de larga escala considerando escalabilidade, eficiência energética, comunicação com vários dispositivos e ambiente altamente dinâmico. Além disso, as soluções atuais para a IoT não permitem que clientes interajam semanticamente com a rede.

Protocolos tradicionais para IoT centrados no endereço dos nós apresentam uma das seguintes arquiteturas: requisição-resposta (*request-response*), publicar-inscrever (*publish-subscribe*) e recurso-observar (*resource-observe*). Na arquitetura requisição-resposta as informações são requisitadas para a rede e os nós enviam dados em reposta à estas requisições. O dispositivo responsável por encaminhar as requisições para a rede deve ter conhecimento sobre as informações fornecidas por cada um dos nós da rede. Esta exigência é ineficiente e gera alta sobrecarga de comunicação para manter as informações sobre os nós atualizadas. Para viabilizar a comunicação com múltiplos nós ao mesmo tempo, os protocolos agrupam dispositivos de acordo com parâmetros específicos. É mais eficiente

enviar uma única mensagem *multicast* para múltiplos dispositivos do que enviar múltiplas mensagens *unicast* para dispositivos individuais. Entretanto, esta estratégia apresenta várias limitações em termos de confiabilidade, flexibilidade e capacidade de gerenciamento destes grupos de dispositivos (ISHAQ et al., 2014). A arquitetura requisição-resposta não oferece suporte para monitoramento periódico de dados. Isto ocorre porque os dados são enviados somente em resposta à uma requisição.

As arquiteturas publicar-inscrever e recurso-observar permitem manifestar o interesse em determinadas informações e receber notificações quando estas informações são fornecidas ou modificadas. Os nós que fornecem informações enviam dados continuamente para um dispositivo central, ainda que não existam manifestações de interesse. Este modo de operação acarreta o consumo desnecessário dos recursos da rede.

Em (INTANAGONWIWAT; GOVINDAN; ESTRIN, 2000), os autores propuseram o primeiro protocolo baseado no paradigma ICN para RSSFs (INTANAGONWIWAT; GOVINDAN; ESTRIN, 2000). Entretanto a solução proposta depende do *flooding* de mensagens, uma estratégia inviável para redes RSSFs de larga escala. Recentemente, outras soluções ICN para RSSFs foram propostas na literatura (JIN et al., 2016; REN; HAIL; HELLBRCK, 2013). No entanto estas soluções igualmente dependem do *flooding* de mensagens ou não apresentam uma solução completa que contempla tanto os pedidos de informação para a rede como o posterior recebimento dos dados.

1.2 Objetivos

O objetivo principal deste trabalho é a concepção e implementação de soluções baseadas nos princípios ICN para RSSFs de larga-escala no ambiente da IoT. As soluções propostas devem superar as limitações dos protocolos tradicionais centrados no endereço dos dispositivos. Para isto, as seguintes características devem ser apresentadas: escalabilidade, robustez, tolerância a perdas, eficiência e capacidade de comunicação com múltiplos dispositivos ao mesmo tempo. Além disso, deve-se evitar a inundação da rede e a alta sobrecarga de comunicação. Os objetivos específicos da pesquisa são:

1. Levantar as aplicações atuais e futuras da IoT.
2. Identificar os requisitos para coleta de dados em RSSFs de larga-escala.
3. Pesquisar e avaliar as vantagens e limitações dos protocolos para IoT tradicionais.
4. Estudar a abordagem ICN e a aplicabilidade em redes sem fio.
5. Propor, implementar e avaliar protocolos de comunicação que apresentem características que possam ser utilizadas na na construção da solução proposta.
6. Realização de experimentos, coletas de dados e validação da solução proposta.

1.3 Publicações

- LACHOWSKI, Rosana; PELLENZ, Marcelo E.; JAMHOUR, Edgard; PENNA, Manoel C.; BRANTE, Glauber; MORITZ, Guilherme; SOUZA, Richard D. Icenet: An information centric protocol for big data wireless sensor networks. Sensors, v. 19, n. 4, 2019. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/19/4/930>.

- LACHOWSKI, Rosana; PELLENZ, Marcelo E.; JAMHOUR, Edgard; PENNA, Manoel C.; MORITZ, Guilherme; BRANTE, Glauber; SOUZA, Richard D. Information centric protocols to overcome the limitations of group communication in the iot. In: BAROLLI, Leonard; AMATO, Flora; MOSCATO, Francesco; ENOKIDO, Tomoya; TAKIZAWA, Makoto (Ed.). Advanced Information Networking and Applications. Cham: Springer International Publishing, 2020. p. 1227–1238. ISBN 978-3-030-44041-1.

1.4 Estrutura do documento

Este documento está estruturado da seguinte forma:

- Capítulo 2 – apresenta os principais conceitos, características e requisitos associados às RSSFs. Além disso, este capítulo esclarece a relevância e essencialidade das RSSFs para a IoT e apresenta os requerimentos das aplicações emergentes. Investigamos ainda o paradigma ICN e sua aplicabilidade nas redes sem fio. Por último, examinamos as vantagens e deficiências do Routing Protocol for Low Power and Lossy Networks (RPL) (WINTER et al., 2017), considerado o protocolo de roteamento padrão para a IoT.

- Capítulo 3 – investiga protocolos de comunicação para ambientes IoT propostos na literatura. Os protocolos são divididos em duas classes: centrados em informação e centrados em endereço. Os principais protocolos representantes das duas classes são apresentados e discutidos.

- Capítulo 4 – descreve os protocolos propostos ICENET e ICENET-PB. Apresentamos a arquitetura, explicamos o funcionamento e a estratégia utilizada para o mecanismo de confiabilidade. Propomos e descrevemos uma estratégia para identificar a informação fornecida por um determinado nó.

- Capítulo 5 – descreve as simulações realizadas para avaliar a eficiência, escalabilidade e confiabilidade das soluções propostas.

- Capítulo 6 – discute as direções futuras deste trabalho e apresenta as conclusões finais.

2 FUNDAMENTAÇÃO TEÓRICA

Este Capítulo descreve os principais conceitos relacionados às RSSFs e sua relevância para a IoT. Além disso, o paradigma ICN é investigado e os fundamentos do *Routing Protocol for Low Power and Lossy Networks* (RPL) (WINTER et al., 2017) são apresentados. O RPL é considerado o protocolo de roteamento de facto para a IoT e é um dos componentes das soluções ICN propostas neste trabalho.

2.1 Redes de Sensores sem Fio

As RSSFs se enquadram na categoria de redes de baixa potência e com alta probabilidade de perda de pacotes (*Low Power Lossy Networks* - LLNs). Uma LLN é uma rede formada por um grande número de dispositivos com recursos limitados (energia, armazenamento e processamento) que se comunicam por enlaces não confiáveis com baixa taxa de dados (VASSEUR, 2014). Os nós sensores devem possuir baixo custo de produção, serem autônomos e operar sem assistência. Devido às restrições impostas pelos nós, as RSSFs requerem soluções específicas e eficientes.

A principal atividade das RSSFs é o monitoramento periódico de condições físicas e ambientais e o encaminhamento dos dados até o *gateway* ou *sink*, encarregado de disponibilizar os dados coletados para os usuários por meio da Internet. No entanto, o envio de comandos e consultas para os nós sensores está se tornando cada vez mais fundamental (IOVA et al., 2016). Frequentemente, aplicações emergentes requerem que comandos e consultas possam ser encaminhados para um conjunto de dispositivos. Os usuários devem ser capazes de se comunicar com a rede e solicitar informações ou enviar comandos para nós implantados em certa área ou que monitoram determinado parâmetro (XIAO et al., 2019; BOUBICHE et al., 2018). São exemplos de aplicações que requerem o envio de comandos e consultas para a rede: Agricultura Inteligente (Smart Agriculture - SA), Monitoramento Ambiental (Smart Environment), Cidades Inteligentes (Smart Cities), Redes Elétricas Inteligentes (Smart Grids), Indústria 4.0 dentre outros.

Devido ao grande número de dispositivos, áreas de implantação extensas e eventualmente de difícil acesso, a construção de uma infraestrutura cabeada de rede pode ser inviável. Por este motivo, os dispositivos comunicam-se por ondas de rádio e trabalham colaborativamente para enviar os dados até o *gateway* e entregar consultas e comandos para os nós da rede. A comunicação direta entre dois nós, especialmente a longas distâncias, pode ser proibitiva em termos de energia despendida. Isto ocorre porque a comunicação de dados é a atividade que mais consome energia dos nós sensores e impacta diretamente

no tempo de vida da rede (Raza et al., 2016; Song; Li, 2018). Os dispositivos geralmente utilizam baterias e podem exaurir suas reservas energéticas, ainda que técnicas de captação de energia sejam utilizadas.

A Figura 1 exibe a arquitetura de referência de uma RSSF no contexto da Agricultura de Precisão. Nestes cenários, os nós sensores podem estar densamente implantados nos campos, nas máquinas, equipamentos e até mesmo nos animais.

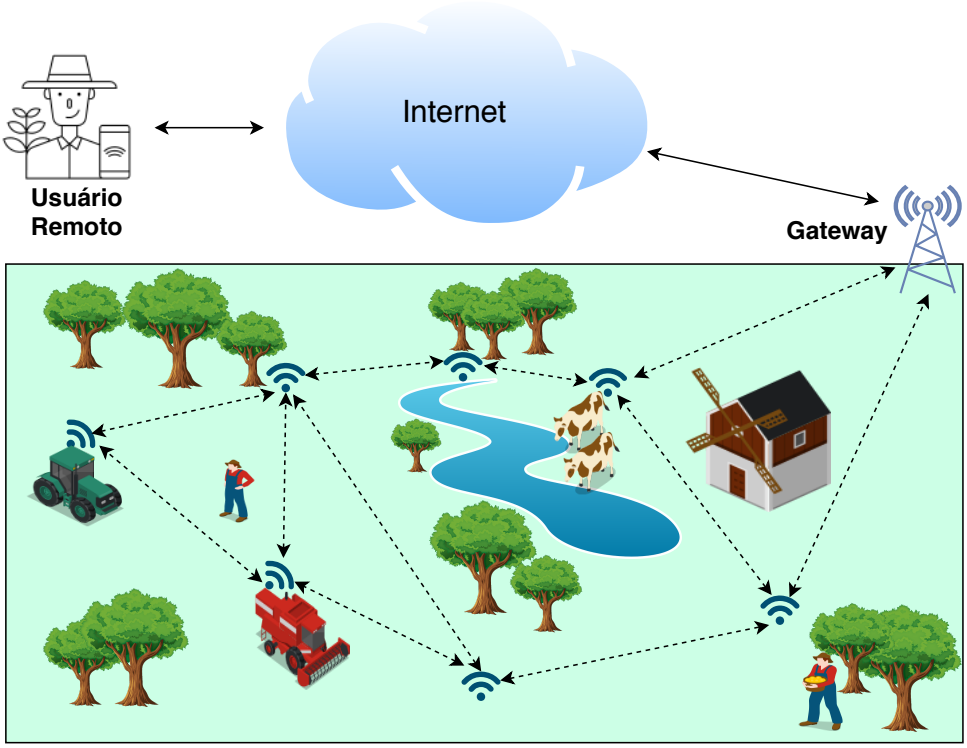


Figura 1 – Arquitetura de referência de uma RSSF.

A necessidade da utilização eficiente dos escassos recursos energéticos dos nós sensores é um dos mais importantes aspectos das RSSFs. O esgotamento da energia dos nós pode impedir que a rede execute suas atividades. Isto ocorre não somente porque o nó sensor deixa de exercer as atividades de monitoramento e coleta de dados, mas também porque os nós dependem uns dos outros para a manutenção das rotas e o encaminhamento dos pacotes de dados. Logo, as soluções devem ser simples e eficientes, especialmente com relação à comunicação entre os nós. Para as RSSFs, o custo de comunicação é várias ordens de magnitude superior ao custo de computação (KARP; KUNG, 2000). Diante disto, o número de mensagens trocadas entre os nós é uma métrica utilizada para mensurar a eficiência de algoritmos e protocolos para RSSFs (LACHOWSKI et al., 2015). Uma das estratégias utilizadas pelos nós sensores para poupar energia é a desativação temporária de seus componentes.

É essencial que soluções para RSSFs sejam escaláveis e mantenham a eficiência e viabilidade em aplicações de larga-escala. O termo *larga-escala* refere-se ao fato de que a área

monitorada é extensa e os nós sensores estão densamente implantados (DJEDOUBOUM et al., 2018). Várias aplicações demandam implantações em larga-escala: agricultura inteligente, monitoramento ambiental, sistemas inteligentes de vigilância, cidades inteligentes dentre outros (JAGANNATH et al., 2019). Nestes cenários, um dos maiores desafios é a coleta de grandes volumes de dados (RANI et al., 2017; TAKAISHI et al., 2014).

Outro grande desafio das RSSFs é o ambiente altamente dinâmico. A instabilidade dos enlaces sem fio causada por mobilidade, esgotamento de recursos energéticos, falhas e efeitos do canal sem fio torna a perda de pacotes um evento comum. Além disso, as RSSFs podem ser implantadas em regiões que apresentam condições climáticas adversas. Por estes motivos, a topologia da rede pode alterar-se rapidamente e consequentemente tornar as informações armazenadas nos nós ultrapassadas. Os nós sensores utilizam estas informações para construir as rotas ascendentes e descendentes a fim de encaminhar dados e consultas. Portanto, a instabilidade do ambiente exige soluções robustas e mecanismos de confiabilidade para manter a rede operacional. Estes mecanismos devem tratar tanto a perda de pacotes de dados quanto a manutenção de informações atualizadas nos nós da rede.

Uma das características mais marcantes das RSSFs é o foco nas informações fornecidas pela rede. Ao contrário das redes de comunicação tradicionais, o endereço ou identidade dos dispositivos que fornecem a informação não são relevantes. As RSSFs são inerentemente centradas em dados (HOLGER; WILLIG., 2005). A importância está na informação, que pode ser o resultado de dados monitorados por vários dispositivos distintos.

2.2 Internet das Coisas

A Internet das Coisas é considerada a primeira grande evolução da Internet. Esta evolução está fortemente associada à comunicação entre usuários e máquinas e máquina a máquina (machine-to-machine - M2M) (Khan et al., 2012; EVANS, 2011). A IoT incorpora inteligência à Internet ao permitir que dispositivos com capacidade de tomar decisões e realizar ações sem intervenção humana possam se comunicar, trocar informações obtidas por meio do monitoramento de parâmetros físicos e ambientais, além de interagir com os usuários. Deste modo, foi possível propor um crescente número de aplicações inteligentes capazes de melhorar o bem-estar econômico e social dos seres humanos. São alguns exemplos de aplicações inteligentes:

- Cidades Inteligentes (Smart Cities) (Arasteh et al., 2016; Cook et al., 2013) – controle de tráfego e mobilidade, monitoramento de parâmetros que impactam na qualidade de vida (poluição, ruído, qualidade do ar entre outros), tempo de resposta rápido a emergências, gestão de resíduos, segurança, gestão inteligente de vagas de esta-

cionamento, automação residencial e monitoramento de vibrações e condições dos materiais em edifícios, pontes e monumentos históricos.

- Redes Elétricas Inteligentes (Smart Grids) (KABALCI, 2016) – monitoramento e controle do sistema de energia elétrica, detecção precoce de colapsos e vulnerabilidades, integração da energia renovável à sistemas de distribuição da energia elétrica e monitoramento do consumo energético.

- Agricultura Inteligente (Smart Agriculture - SA) (MAZZETTO; GALLO; SACCO, 2020) – rastreamento de animais, elaboração de mapas de produção de cereais, monitoramento de pragas, pestes, condições do solo e qualidade da água, estudo das condições meteorológicas e previsão de chuva, neve, vento e gelo, gerenciamento de sistemas de irrigação, uso controlado de fertilizantes e pesticidas e monitoramento de máquinas e equipamentos agrícolas.

- Monitoramento Ambiental (Smart Environment) (EL-BENDARY et al., 2013) – monitoramento de regiões que oferecem perigos aos seres humanos (vulcões, regiões de instabilidade sísmica, regiões suscetíveis a ocorrência de furacões), monitoramento de regiões inóspitas, monitoramento da qualidade do ar e da água, previsão e detecção de desastres naturais (incêndios, inundações, tsunamis e terremotos), rastreamento e monitoramento de animais, monitoramento de mudanças climáticas e previsão do tempo.

- Indústria 4.0 (AHMED et al., 2016) – monitoraramento dos processos de produção para otimização e prevenção de falhas, monitoramento da integridade estrutural das instalações, controle dos espaços de armazenamento, gerenciamento do fluxo de pessoas e monitoramento das operações, funcionalidades e taxa de produtividade das máquinas.

- Saúde Digital (E-healthcare) (Boric-Lubecke et al., 2014) – consultas remotas, monitoramento remoto de pacientes, idosos, gestantes e instalações de vida assistida.

- Turismo Inteligente (Smart Tourism) (Tripathy et al., 2018) – mobilidade independente, segurança, monitoramento de parâmetros biométricos em espaços públicos e monitoramento da taxa de ocupação e do distânciamento social em centros comerciais, prédios e espaços públicos.

O principal objetivo da IoT é facilitar a vida humana. Neste sentido, as cidades inteligentes podem melhorar a qualidade de vida dos cidadãos em muitos aspectos: controle de tráfego, monitoramento da poluição e qualidade do ar, segurança e tempo de resposta rápido a emergências, entre outros. Grandes quantidades de dados coletados podem ser utilizados para construir modelos preditivos e planejar estratégias específicas (JAYARAMAN et al., 2016). A agricultura, por exemplo, pode aumentar a produtividade, otimizar

recursos (água, energia, fertilizantes, pesticidas etc.), controlar pragas e reduzir os custos e o impacto ambiental (OJHA; MISRA; RAGHUWANSHI, 2015). Ao possibilitar amplo acesso à informação e conhecimento, a IoT impulsionou a quarta revolução industrial, denominada Indústria 4.0 (SCHUTZE; HELWIG; SCHNEIDER, 2018).

A Indústria 4.0 apresenta vários benefícios obtidos por meio de dados gerados em todos os níveis do processo de produção: redução de custos operacionais e do desperdício, alta eficiência operacional, flexibilidade e maior produtividade de pessoas e equipamentos (LU, 2017). Isso não seria possível sem sensores inteligentes que além de gerar informações possuem outras funcionalidades, como o auto-monitoramento e autoconfiguração (SCHUTZE; HELWIG; SCHNEIDER, 2018).

Um dos principais objetivos da Indústria 4.0 é atingir um alto nível de automatização (LU, 2017) para que grupos de máquinas produzam produtos com rapidez, precisão e mínimo envolvimento humano. Para isto, é necessário controlar e monitorar as operações, funcionalidades e taxa de produtividade das máquinas (AL-FUQAHA et al., 2015). As mudanças causadas pela Indústria 4.0 são capazes de impactar diversos setores, como infraestrutura, economia, saúde, segurança e meio ambiente (IIC, 2020).

Na área da saúde, a IoT revolucionou a prática médica e a prevenção de doenças por meio da telemedicina (Boric-Lubecke et al., 2014). Exemplos incluem o monitoramento remoto de gestantes, pacientes com doenças crônicas, idosos e instalações de vida assistida. Em (ROBLEK; MESKO; KRAPEZ, 2016), os autores apresentam uma aplicação para que profissionais da saúde possam monitorar os pacientes por meio de aplicativos móveis, sensores em roupas e câmeras de vigilância. Alguns parâmetros biométricos que podem ser mensurados: saturação arterial de oxigênio, frequência cardíaca, temperatura corporal, pressão arterial e nível de glicose no sangue.

A saúde digital pode ser especialmente valiosa em situações extremas, como calamidades naturais, enchentes, incêndios e epidemias. Governos ao redor do mundo estão empregando a telemedicina no combate ao COVID-19, com o objetivo de reduzir o número de internações e quebrar a cadeia de propagação do vírus por meio do contato pessoal (PATIL, 2020). No Brasil, a pandemia de COVID-19 agilizou o processo de adoção da telemedicina (SANTOS et al., 2020).

O turismo é outro setor que pode beneficiar-se da IoT para superar os impactos causados pela pandemia de COVID-19. A indústria do turismo é um componente importante da economia de muitos países (Tripathy et al., 2018). Entretanto, foi severamente afetada pela pandemia. Ações que podem minimizar este impacto visam aumentar segurança e confiança. A IoT permite monitorar parâmetros biométricos em lugares públicos, detectar elevação da temperatura corporal, medir a taxa de ocupação e o distânciamento social em centros comerciais, prédios e espaços públicos.

Figura 2 – Exemplo de aplicação inteligente voltada para a agricultura (FAPA, 2016).

A Figura 2 exibe um exemplo de aplicação inteligente voltada para a agricultura, cujo objetivo é o monitoramento de populações de pragas e a utilização eficiente de pesticidas. Ferômonios são utilizados para atrair os insetos a armadilhas espalhadas nas plantações. Sensores implantados nas armadilhas coletam as imagens que são então enviadas para a Internet. Em seguida, as imagens são processadas para realizar a contagem e identificação dos insetos. As informações obtidas são combinadas à informações relativas ao clima na região a fim de predizer a probabilidade da ocorrência de determinadas pragas. Isto permite a tomada de ações proativas, como por exemplo a utilização eficiente de defensivos agrícolas.

Em determinadas regiões, o acesso à Internet por meio da comunicação celular não está disponível. Além disso, os custos envolvidos neste modo de comunicação ou na construção de infraestruturas de rede podem inviabilizar aplicações. Por estes motivos, as RSSFs são um elemento essencial da IoT que pode ser vista como uma coleção de redes distintas para fins específicos (EVANS, 2011). A Figura 3 exibe uma visão geral da IoT. Alguns pesquisadores preveem uma *Terra Inteligente* e o gerenciamento de dados fornecidos por uma Rede de Sensores sem fio Global composta por um grande número de RSSFs distintas (ABERER, 2007).

Em (CHEBUDIE; MINERVA; ROTONDI, 2014), os autores explicam que sistemas IoT possuem diferentes escopos e níveis de complexidade, como mostra a Figura 3. O sistema de menor complexidade é formado por um dispositivo unicamente identificável, com capacidade de sensoriamento e programável conectado à Internet. Devido à possibilidade de idenficar este dispositivo de modo único e sua capacidade de monitoramento, informações podem ser coletadas e o estado do dispositivo pode ser modificado de qualquer lugar, a qualquer hora, por qualquer outro dispositivo ou pessoa.

Sistemas de alta complexidade envolvem implantações em larga escala de um imenso número de dispositivos a fim de entregar serviços avançados. Nestes casos, a IoT pode ser definida como uma rede complexa, auto configurável e adaptativa que conecta dispositivos a Internet por meio de protocolos de comunicação padrão. Os dispositivos interconectados possuem representação física ou virtual no mundo digital contendo informações relativas à

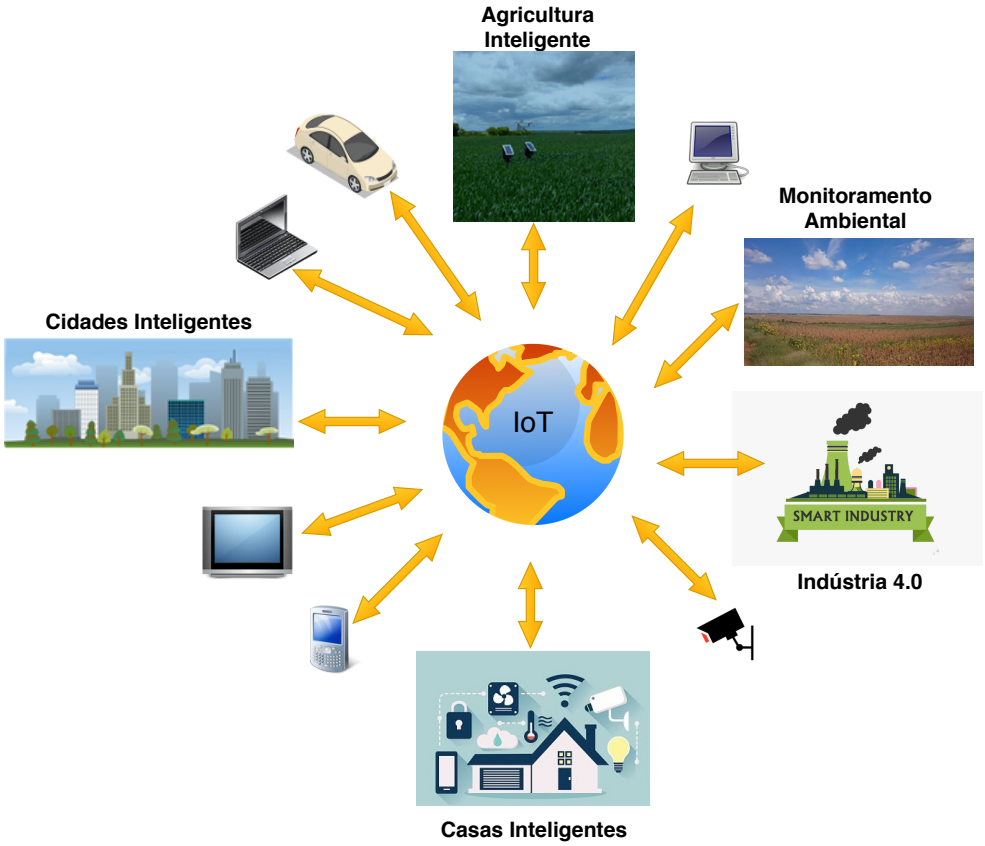


Figura 3 – Visão geral da IoT. Adaptado de (Khan et al., 2012).

identidade, status, localização ou qualquer outra informação relevante. Neste contexto, a alta complexidade exige eficiência, escalabilidade e soluções distribuídas. Além disso, exige que abordagens tradicionais para gerenciar confiabilidade, nomenclatura, descoberta de recursos, dentre outros, sejam completamente repensadas.

Cenários complexos são capazes de produzir enormes volumes de dados. O conjunto de dados produzido pelo grande número de sensores implantados em seres humanos, animais, plantas, veículos, computadores, telefones, dentre outros dispositivos, é denominado "Big Data"(AL-FUQAHA et al., 2015). Este imenso volume de dados é muito difícil de se coletar, formatar, armazenar, gerenciar, analisar e visualizar usando as metodologias das abordagens tradicionais de computação (BOUBICHE et al., 2018). Apesar das dificuldades, a coleta de Big Data representa uma grande vantagem competitiva. Por meio de ferramentas de inteligência analítica é possivel extrair informações relevantes, conhecimento e consequentemente obter um suporte valioso para tomadas de decisão (AL-FUQAHA et al., 2015).

A coleta de dados em ambientes IoT pode envolver o encaminhamento de consultas e comandos para a rede. Especialmente cenários de alta complexidade apresentam um número crescente de aplicações que requerem esta habilidade (XIAO et al., 2019; IOVA et al., 2016). Em várias situações é necessário obter dados de nós específicos ou enviar

pacotes de controle para os dispositivos (ZHONG; LIANG, 2018). Comumente consultas são utilizadas para obter dados em uma região definida ou de dispositivos que monitoram determinado parâmetro (WANG et al., 2019). Por estes motivos, a IoT não está somente associada à comunicação entre máquinas, mas também entre usuários e máquinas. Nestes casos, é coerente que os usuários possam comunicar-se semanticamente com a rede.

As principais características da IoT estão resumidas na lista abaixo (CHEBUDIE; MINERVA; ROTONDI, 2014; Singh; Singh, 2015):

- Pervasividade e ubiquidade – A IoT é capaz de conectar tudo e todos e deste modo criar um vínculo entre os mundos físico e digital. Serviços e informações estão disponíveis sempre que necessário, para quem precisar e em qualquer lugar.
- Autonomia e Inteligência– Dispositivos são capazes de coletar informações, tomar decisões e realizar ações sem intervenção humana.
- Rede de redes – A IoT conecta redes de comunicação distintas, capazes de gerenciar comunicações complexas e grandes volumes de dados a fim de oferecer serviços avançados.
- Miniaturização e simplificação – Os dipositivos podem ser tão pequenos a ponto de ficarem invisíveis quando incorporados ao ambiente. O objetivo é incluir apenas as funcionalidades necessárias no contexto da aplicação. Geralmente, os dispositivos possuem baixo custo, apresentam baixo consumo energético e poucas funções: monitoramento, armazenamento e comunicação de uma quantidade limitada de informações.
- Diferentes contextos – Dados são coletados não somente no ambiente físico, mas também no ambiente digital. Neste contexto, são coletadas informações sobre a rede e aplicativos. A coleta de grandes volumes de dados é um dos principais desafios da IoT e que pode ser superado por meio de uma abordagem centrada em informações.

2.3 Redes Centradas em Informação

Redes Centradas em Informação (Information-Centric Networking - ICN) é um paradigma de rede que representa uma das inovações mais significativas na definição dos protocolos de rede modernos (VIRGILIO; MARCHETTO; SISTO, 2013). No paradigma ICN os dados são o foco, diferentemente da arquitetura atual da Internet que segue um conceito centrado no host.

Os protocolos TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e IP (Internet Protocol - Protocolo da Internet) são dois dos protocolos mais importantes da Internet (KUROSE; ROSS, 2007). O TCP/IP considera que o papel da rede

é criar e manter o enlace lógico entre as entidades comunicantes para que a transferência dos dados possa ocorrer (KRISHNA, 2019). Para isso, a ênfase é colocada nos hosts e não nos dados transportados pela rede. O ICN altera o foco do host para os dados.

As abordagens centradas em informação geralmente identificam os dados armazenados nos hosts com nomes que são utilizados para o encaminhamento dos dados na rede. Ao contrário, a abordagem tradicional atribui uma identificação (endereço) para cada host e utiliza esta identificação para o encaminhamento dos dados. Em cenários ICN, consumidores não necessitam de endereços de rede para obter dados tampouco as mensagens contém a identificação de consumidores ou hosts.

O paradigma ICN foi inicialmente concebido para atender as demandas da Internet do Futuro (KRISHNA, 2019). O número crescente de aplicações introduziu vários novos desafios, incluindo distribuição escalável de conteúdo, segurança, mobilidade, dentre outros (Qiao et al., 2019). Os usuários destas aplicações estão interessados em obter o conteúdo desejável independemente de onde esteja localizado. Para isso, o paradigma ICN oferece um mecanismo de *caching* que juntamente com o roteamento baseado em informações tornam muitas aplicações mais efetivas (Qiao et al., 2019).

O roteamento baseado em informações permite a recuperação dos dados de qualquer hospedeiro que possua uma cópia válida do conteúdo solicitado, dissociando consumidores e produtores de informações. Isto leva à distribuição escalável e eficiente de conteúdo, suporte à mobilidade e aperfeiçoamento da tolerância a falhas (KRISHNA, 2019).

Os princípios do paradigma ICN não são recentes. Em (CHERITON; GRITTER, 2000), os autores propuseram uma nova arquitetura para a Internet denominada TRIAD. Este trabalho é considerado um importante precursor de todos os projetos ICN (GHODSI et al., 2011). Alguns anos após, várias iniciativas foram tomadas para melhorar a arquitetura e o desempenho das redes centradas em informação. Existem vários projetos ICN representando diferentes abordagens sendo ativamente desenvolvidos em todo o mundo (AMADEO et al., 2014; AHLGREN et al., 2012). Embora estas abordagens sejam diferentes com relação aos detalhes, compartilham muitas suposições, propriedades arquitetônicas e objetivos (AHLGREN et al., 2012). Neste contexto, Van Jacobson apresentou uma arquitetura denominda Rede Centrada em Conteúdo (Content-Centric Networking - CCN) (JACOBSON et al., 2009), financiada pela empresa de pesquisas PARC e que despertou um grande interesse (GHODSI et al., 2011). Recentemente, a abordagem CCN chamou a atenção dos pesquisadores pela aplicação nas RSSFs (JABER; KACIMI; GAYRAUD, 2017; WALTARI; KANGASHARJU, 2016; AMADEO et al., 2014; ABIDY et al., 2014; AMADEO et al., 2013; REN; HAIL; HELLBRCK, 2013). Apesar das vantagens, a abordagem CCN foi concebida para a Internet e requer modificações apropriadas para ser aplicada em LLNs.

2.3.1 Redes Centradas em Conteúdo

Em (JACOBSON et al., 2009), os autores explicam que os principais objetivos da abordagem CCN são manter a simplicidade e escalabilidade do IP e oferecer melhorias com relação à segurança, entrega de dados e tolerância a falhas e interrupções. Para a abordagem CCN, os dados armazenados pelos nós da rede são denominados *conteúdo*. Cada conteúdo possui um nome único, persistente e hierárquico que é utilizado para o roteamento dos dados. A Figura 4 destaca a diferença entre o roteamento de dados na abordagem tradicional e na abordagem CCN.

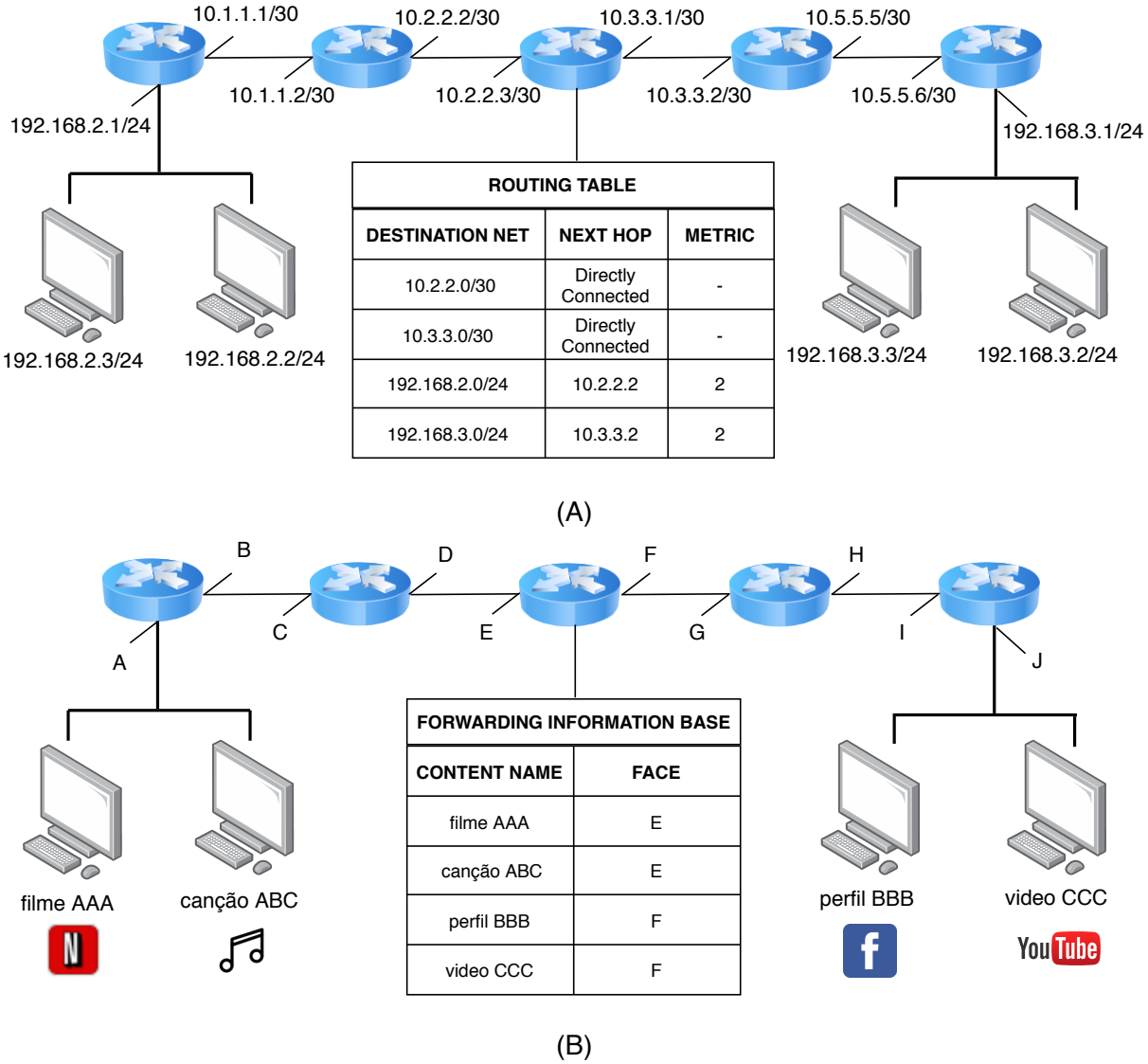


Figura 4 – (a) roteamento de dados na abordagem tradicional, (b) roteamento de dados na abordagem ICN.

A Figura 4 (A) representa a abordagem tradicional e exibe uma rede formada por cinco roteadores e a tabela de roteamento de um destes roteadores. A Figura 4 (B) representa a abordagem CCN e exibe a mesma rede, porém mostra uma estrutura

denominada *Forwarding Information Base* (FIB) equivalente à tabela de roteamento da abordagem baseada em endereços. O campo FACE da tabela FIB é uma representação abstrata para troca de dados, portanto pode representar tanto uma interface de rede física como uma aplicação ou qualquer outro dispositivo. Esta abstração permite que uma solução ICN seja implantada como uma camada *overlay* sobre o protocolo IP (JACOBSON et al., 2009).

Cada nó CCN apresenta três estruturas de dados: (i) FIB (Forwarding Information Base) - utilizada para encaminhar solicitações de dados (interesses) , (ii) PIT (Pending Interest Table) - utilizada para encaminhar pacotes de dados recebidos para os solicitantes e (iii) CS (Content Store) - utilizada para o armazenamento em *cache* de conteúdo. Um nó CCN pode apresentar também múltiplas *faces* para troca de dados. A Figura 5 exibe o modelo de um nó CCN.

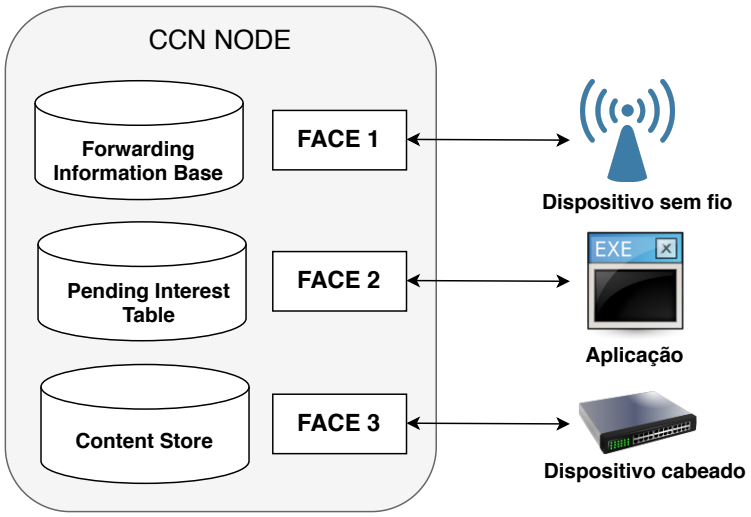


Figura 5 – Modelo de um nó CCN (Ma et al., 2013).

O mecanismo de processamento e encaminhamento de mensagens na abordagem CCN é descrito na Figura 6. Existem duas mensagens CCN: *Interesse* e *Dados*. Mensagens Interesse são enviadas em *broadcast* para coletar informações. Se um nó receber uma mensagem Interesse e verificar que a informação solicitada está armazenada em *cache*, uma mensagem Dados é enviada em resposta. Como o CCN foi concebido para a Internet, mensagens Interesse e Dados mantém um relacionamento um-para-um: os nós transmitem uma mensagem Dados somente em resposta a um Interesse. A mensagem Dados consome o Interesse atendido. Considerando RSSFs, este modo de operação não é eficiente, pois os usuários geralmente estão interessados em dados fornecidos por vários nós e em fluxos contínuos de observações. Caso um nó não possa responder à uma mensagem Interesse, a tabela PIT é verificada. Uma entrada correspondente na PIT significa que o nó já recebeu o mesmo Interesse de outro usuário ou a mensagem é duplicada. Neste caso, o Interesse é descartado e a *face* pela qual o Interesse foi recebido é adicionada à entrada existente na

PIT. Por fim, se não houver uma entrada correspondente na PIT, a regra *correspondência ao prefixo mais longo* (longest prefix matching) é utilizada para selecionar uma entrada na tabela FIB a fim de encaminhar o Interesse recebido para uma possível fonte de dados. Após a seleção da entrada na tabela FIB, uma nova entrada na PIT é criada.

Ao receber uma mensagem Dados, o nó armazena o conteúdo em CS e em seguida verifica as entradas na PIT. Caso não haja uma entrada na PIT, então os dados recebidos não foram solicitados e a mensagem é descartada. Ao contrário, a mensagem é encaminhada para as *faces* correspondentes à entrada na PIT.

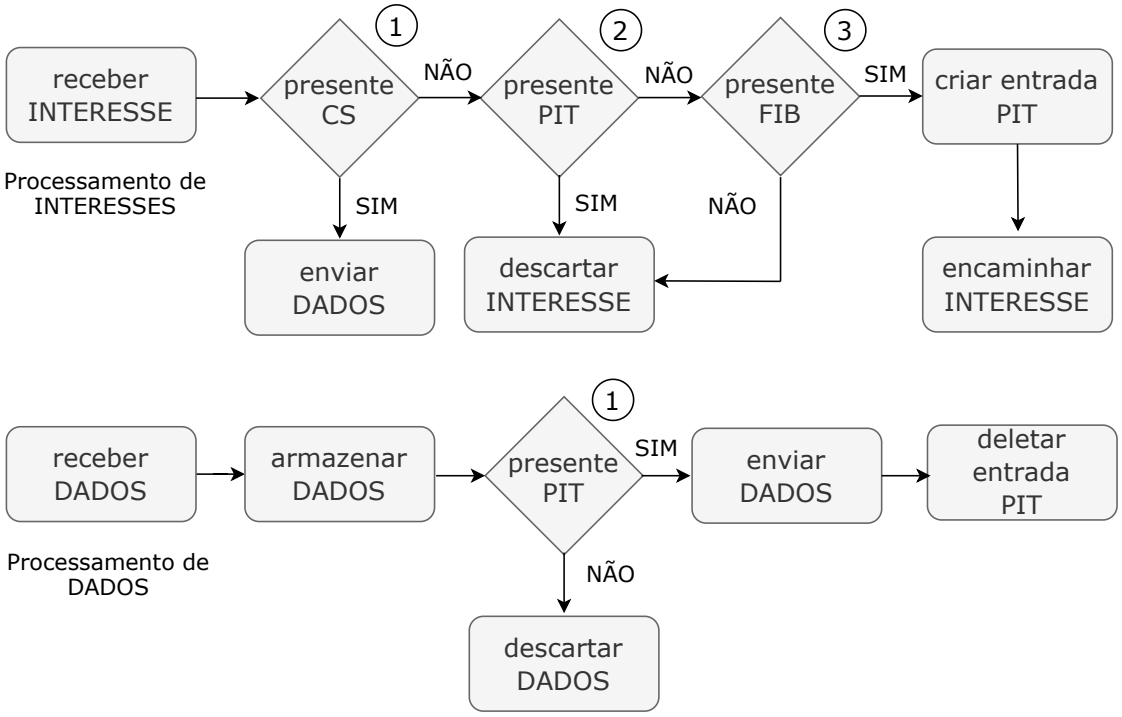


Figura 6 – Processamento e encaminhamento de mensagens na abordagem CCN (JACOBSON et al., 2009).

Certas características apresentadas pela abordagem CCN exigem modificações para a aplicação nas RSSFs. Primeiramente, os usuários devem expressar interesse por cada pacote de dados. Este modo de operação é inadequado para ambientes restritos e não oferece suporte para alertas e notificações de emergência. Além disso, os roteadores CCN necessitam manter tabelas que armazenam cada requisição de dados encaminhada, o que implica em considerável sobrecarga de armazenamento.

Capítulo 04

2.4 Fundamentos do RPL

Em 2012, o grupo de trabalho IETF (Internet Engineering Task Force) ROLL publicou o documento “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks"(WINTER

et al., 2017). O RPL foi projetado para atender os requisitos de LLNs e rapidamente tornou-se o protocolo de roteamento de fato para a IoT (IOVA et al., 2016; GADDOUR; KOUBAA, 2012).

O RPL apresenta uma solução energeticamente eficiente para construir e manter uma topologia de roteamento baseada em árvore com caminhos redundantes que reagem rapidamente a mudanças de conectividade chamada DODAG (*Destination Oriented Directed Acyclic Graph*) (WINTER et al., 2017). A topologia de rede pode apresentar múltiplas DODAGs enraizadas em diferentes *gateways*. Por padrão, cada nó sensor possui um nó pai preferencial para encaminhar pacotes de dados em direção ao *gateway* e vários pais alternativos para manutenção de rotas *backup* (IOVA et al., 2016). A DODAG suporta três padrões de tráfego: (i) tráfego *upstream* dos nós para o *gateway* (M2P), (ii) tráfego *downstream* do *gateway* para os nós (P2M) e (iii) tráfego entre nós (P2P).

2.4.1 Processo da Construção da DODAG

Para construir e manter uma DODAG, três mensagens diferentes são utilizadas:

- **DIO** – *DODAG Information Object*;
- **DIS** – *DODAG Information Solicitation*;
- **DAO** – *Destination Advertisement Object*;

A Figura 7 exibe o processo de construção da DODAG que inicia quando o nó raiz (*gateway*) envia para a rede uma mensagem DIO contendo parâmetros de configuração e métricas de roteamento (*rank*). Essas informações são usadas pelos nós para avaliar o custo dos caminhos e selecionar os pais preferenciais e alternativos. Ao receber uma mensagem DIO, o nó calcula seu próprio *rank* e em seguida propaga a mensagem recebida com o novo valor. O modo de calcular o *rank* depende de uma Função Objetiva (OF), que define como os nós traduzem uma ou mais métricas em valor. Várias métricas de roteamento foram propostas pelo IETF (FORCE, 2017):

- Métricas relativas aos nós: características do nó, energia residual e número de saltos até o *gateway*;
- Métricas relativas aos enlaces: *throughput*, latência, confiabilidade e *link color*, que é uma restrição administrativa usada para evitar ou atrair enlaces específicos para determinados tipos de tráfego;

Mesmo após a construção do DODAG, os nós continuam transmitindo mensagens DIO para manter a topologia de roteamento. O Algoritmo Trickle (LEVIS et al., 2017) é

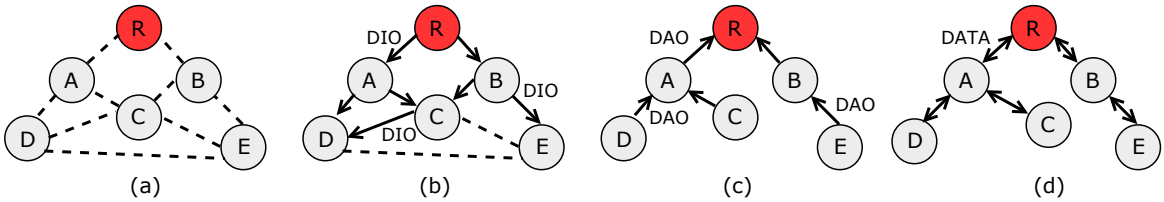


Figura 7 – Construção da DODAG - (a) uma rede sem fio, (b) construção de rotas descendentes, (c) construção de rotas ascendentes, (d) tráfego de dados

executado pelos nós para determinar a taxa de envio das mensagens DIOs. Mensagens DIS são utilizadas pelos nós para solicitar aos nós vizinhos o envio de mensagens DIOs, a fim de ingressar no DODAG ou atualizar as informações de roteamento. Mensagens DAO são usadas para estabelecer rotas descendentes (do nó raíz em direção aos outros nós da rede).

2.4.2 Modos de Operação

O RPL suporta dois modos de operação para tráfego descendente: *storing* e *non-storing*. Em ambos os modos, o RPL apresenta sérios problemas de escalabilidade (ZHONG; LIANG, 2018; IOVA et al., 2016).

No modo de operação *storing*, a mensagem DAO é enviada em *unicast* para o pai preferencial. Essas mensagens carregam informações sobre os prefixos acessíveis através do nó emissor. Os nós receptores utilizam estas informações para construção de uma tabela de roteamento. Portanto, os nós armazenam entradas para todos os destinos em sua subárvore. Especialmente em redes de larga escala, a tabela de roteamento pode não ser capaz de armazenar todas as entradas (*buffer overflow*) e a rede pode colapsar.

No modo de operação *non-storing*, a mensagem DAO é enviada em *unicast* para o root. Nós pais intermediários não armazenam informações, apenas inserem o próprio endereço na informação de rota e encaminham a mensagem para o nó pai. Somente o nó raíz mantém uma tabela de roteamento e os pacotes de dados armazenam a rota explícita até o destino. Para coletar dados de múltiplas fontes de dados, é necessário endereçar uma mensagem distinta para cada nó. É necessário também que a aplicação tenha conhecimento sobre as informações fornecidas pelos nós. Estas duas exigências acarretam uma sobrecarga de comunicação considerável. Além disso, protocolos da camada física de redes LLNs são projetados para apresentar pequenos tamanhos de quadro. A medida que o tamanho da rede aumenta, armazenar rotas em pacotes de dados pode tornar-se inviável. Outra desvantagem do modo de operação *non-storing* esta relacionada à confiabilidade. Devido ao ambiente dinâmico das RSSFs, as rotas podem tornar-se obsoletas e indisponíveis antes que o pacote de dados seja entregue ao nó destino.

A habilidade de enviar comandos e consultas de uma unidade central para os nós

da rede está se tornando cada vez mais essencial. Apesar disto, os padrões de comunicação P2M (ponto-para-multiponto) e P2P (ponto-a-ponto) não receberam a devida atenção no protocolo RPL, produzindo implementações com baixa performance e prevenindo a adoção do protocolo nas crescentes aplicações IoT que requerem o envio de comandos e consultas para os nós da rede (IOVA et al., 2016).

2.4.3 Comunicação com Múltiplos Dispositivos

Para habilitar a comunicação com múltiplos dispositivos, o RPL adota mensagens *multicast* endereçadas para grupos de dispositivos. Entretanto, a especificação do RPL não fornece um nível suficiente de detalhes sobre a comunicação *multicast* (OIKONOMOU; PHILLIPS; TRYFONAS, 2013).

Somente o modo de operação *Storing with multicast support* permite a propagação de mensagens *multicast*. Neste caso, mensagens DAO podem transportar prefixos *multicast*. Para ingressar em um grupo *multicast*, os nós anunciam o endereço *multicast* nas mensagens DAO. Ao receber uma mensagem contendo um endereço *multicast*, o nó pai insere uma entrada na tabela de roteamento e informa o novo prefixo ao próprio pai na DODAG. Conceitualmente, a entrada na tabela de roteamento indica que um dos nós na subárvore é um membro do referido grupo. Esta estratégia resolve o problema da propagação de informações sobre os membros dos grupos em direção ao nó raíz da DODAG. Entretanto, não impede que um nó da rede receba o mesmo datagrama mais de uma vez.

A especificação do RPL determina que cada nó deve enviar datagramas *multicast* somente para nós vizinhos. Portanto, somente para o nó pai e para os nós filhos pertencentes ao grupo *multicast*. Esta filtragem só pode ser alcançada por meio do envio de uma mensagem *unicast* para cada um dos destinatários (OIKONOMOU; PHILLIPS; TRYFONAS, 2013). Logo, seria necessário transmitir o mesmo datagrama múltiplas vezes, o que incorreria em gasto energético, atrasos e utilização ineficiente do canal sem fio. Para superar esta deficiência, em (OIKONOMOU; PHILLIPS; TRYFONAS, 2013) os autores propõe o algoritmo *Stateless Multicast Forwarding* (SMRF).

O SMRF opera com base nas informações fornecidas pelo RPL, especialmente com relação ao nó pai preferencial e participação dos nós em grupos *multicast*. Os nós SMRF aceitam somente mensagens enviadas pelo nó pai preferencial, que são posteriormente processadas caso o nó seja membro do grupo multicast para o qual a mensagem fora enviada. Caso algum dos nós filhos seja membro do referido grupo, então a mensagem é encaminhada. Em (FADEEL; SAYED, 2015), uma versão aperfeiçoada do algoritmo SMRF é proposta a fim de permitir o tráfego ascendente de mensagens *multicast*.

Devido às limitações do RPL com relação à comunicação com múltiplos dispositivos, o IETF propôs um protocolo *multicast* especialmente adequado para LLNs denominado

Multicast Protocol for Low-Power and Lossy Networks (MPL) (HUI; KELSEY, 2021). O MPL foi projetado para executar, sem modificações, juntamente com qualquer protocolo de roteamento. Além disso, não requer a construção e manutenção de uma topologia de roteamento ou grupos de comunicação para a disseminação das mensagens *multicast*. No entanto, devido à ausência de manutenção de uma topologia de roteamento e de grupos de comunicação, nós MPL encaminham as mensagens recebidas para toda rede (*flooding*), causando o uso ineficiente dos recursos energéticos e do canal de comunicação. Para evitar duplicações, os nós MPL não encaminham mensagens recebidas imediatamente. Cada nova mensagem é armazenada em *cache* e a transmissão é agendada de acordo com temporizadores mantidos pelo algoritmo Trickle (LEVIS et al., 2017), cujo objetivo é otimizar a frequência de transmissão das mensagens de acordo com as condições da rede. Este atraso no encaminhamento das mensagens impacta no desempenho do MPL e é fortemente influenciado pela parametrização do Trickle.

2.5 Considerações Finais

As RSSFs são um elemento essencial da IoT, cujo principal objetivo é facilitar a vida humana por meio de um crescente número de aplicações inteligentes. No entanto, as RSSFs apresentam recursos computacionais restritos e demandam soluções energeticamente eficientes, robustas e preparadas para um ambiente altamente dinâmico. Além disso, as aplicações emergentes frequentemente demandam implantações em larga-escala. O imenso volume de dados gerado nestes cenários complexos é extremamente difícil de coletar, formatar, armazenar, gerenciar, analisar e visualizar usando as metodologias das abordagens tradicionais de computação.

A alta complexidade das aplicações em larga-escala demanda além de eficiência, escalabilidade e soluções distribuídas. Outra exigência está relacionada ao gerenciamento da confiabilidade, nomenclatura e descoberta de recursos.

Um dos principais desafios das aplicações emergentes envolve a capacidade de enviar comandos e consultas para a rede. O RPL, protocolo de roteamento padrão para redes LLNs, apresenta um mecanismo pouco eficiente para o tráfego descendente de dados. Outra dificuldade está relacionada com a comunicação com múltiplos dispositivos. A especificação do protocolo não é suficientemente detalhada e supõe a retransmissão de datagramas *multicast* múltiplas vezes.

As RSSFs são inerentemente centradas em dados. Diferentemente de outras redes de comunicação de dados, a importância está nas informações fornecidas pelos nós e não na identidade dos dispositivos. Geralmente, a informação é o resultado do monitoramente de múltiplos dispositivos.

Considerando as características e requisitos das RSSFs, o paradigma Redes Centra-

das em Informação possui potencial para superar os vários desafios. O paradigma ICN representa uma grande inovação no campo das redes de comunicação. Ao contrário das abordagens tradicionais que seguem um conceito centrado na identidade dos hospedeiros, o ICN apresenta uma abordagem centrada nas informações fornecidas pela rede. Para as RSSFs, o foco está nos parâmetros monitorados pelos nós, cujos nomes são utilizados para o encaminhamento dos dados. Apesar da conveniência de aplicar os conceitos do paradigma ICN para superar os desafios das RSSFs, modificações são necessárias. O ICN foi especialmente concebido para a Internet do Futuro e algumas de suas características são inadequadas para o ambiente das RSSFs.

3 TRABALHOS RELACIONADOS

Protocolos para RSSFs em ambientes IoT podem ser divididos em duas classes: **centrados em endereço** e **centrados em informação**.

A abordagem clássica centrada em endereço utiliza o endereço dos dispositivos para o roteamento dos dados. Para permitir a comunicação com múltiplos nós ao mesmo tempo, os dispositivos são tipicamente agrupados de acordo com parâmetros específicos. Mensagens *multicast* são enviadas para os grupos de comunicação a fim de utilizar eficientemente os recursos da rede.

Protocolos centrados em informação utilizam as informações fornecidas pelos dispositivos para roteamento de dados e não dependem da construção e manutenção de grupos. Entretanto, a abordagem centrada em informações foi concebida para a Internet e, por este motivo, nem todos os protocolos centrados em informação permitem o envio de uma única mensagem para múltiplos destinos ou oferecem suporte ao envio periódico de dados.

Neste trabalho, o foco está em protocolos que permitem comunicação com múltiplos dispositivos ao mesmo tempo. Nas próximas sessões as dificuldades relacionadas à comunicação em grupo são detalhadas e os principais protocolos representantes das duas classes são apresentados e discutidos.

3.1 Limitações da Comunicação em Grupo

Devido às restrições dos dispositivos, uma das principais limitações relacionadas à comunicação em grupo refere-se à escalabilidade (ISHAQ et al., 2014). Os nós que executam a implementação *multicast* do Contiki podem ingressar em apenas um grupo de comunicação por padrão, além de quatro grupos criados automaticamente. Especialmente com relação à memória, as restrições são fatores limitantes em implantações de larga escala, pois o número de possíveis grupos pode rapidamente se tornar muito grande. Além disso, existem restrições com relação ao tamanho dos grupos (ISHAQ et al., 2016), uma vez que as colisões aumentam à medida que os grupos se tornam maiores.

A falta de flexibilidade e capacidade de gerenciamento dos grupos de comunicação também são limitações importantes. Geralmente, os nós são configurados manualmente para pertencer a determinados grupos antes da implantação da rede. No entanto, em ambientes dinâmicos, é difícil definir os grupos de comunicação pois os requisitos mudam com frequência. A falta de flexibilidade e gerenciamento impede que consultas e comandos sejam enviados para os dispositivos de acordo com as necessidades dos clientes. O envio

de mensagens apenas para dispositivos capazes de atender uma consulta ou comando reduz o número de mensagens na rede. Como a comunicação de dados é a atividade que mais consome energia dos nós dos sensores (Raza et al., 2016), a redução no número de mensagens afeta diretamente o tempo de vida da rede. Protocolos não energeticamente eficientes podem não ser diretamente aplicáveis ao ambiente restrito da IoT (AMADEO et al., 2014).

Outra restrição refere-se à confiabilidade. A comunicação com os membros do grupo não é confiável e não há garantia de que uma mensagem será entregue a todos os membros. Como algumas aplicações requerem entrega garantida (ISHAQ et al., 2014), a comunicação em grupo não é adequada para todos os casos de uso.

Por fim, a comunicação em grupo geralmente depende da construção e manutenção de rotas para os grupos *multicast*. No entanto, pouca atenção foi dedicada à comunicação *multicast* para redes que apresentam recursos restritos.

3.2 Soluções Centradas em Endereço

Vários protocolos centrados em endereço foram propostos para o ambiente da IoT. Os dois protocolos mais populares são: *Constrained Application Protocol* (CoAP) e *Message Queue Telemetry Transport* (MQTT). O CoAP apresenta menor sobrecarga e recebeu ampla aceitação (Subramanian; Pasquale; Polyzos, 2017). Foi projetado por um grupo de trabalho do *Internet Engineering Task Force* (IETF) denominado *Constrained RESTful Environments* (CoRE) em 2010 (BORMANN; CASTELLANI; SHELBY, 2012). O MQTT foi apresentado por Andy Stanford-Clark, da IBM, e Arlen Nipper, da Eurotech, em 1999 (LOCKE, 2010). Tanto o MQTT como o CoAP são protocolos da camada de aplicação. A principal diferença entre eles é que o CoAP utiliza o protocolo de transporte UDP (User Datagram Protocol), enquanto o MQTT é executado sob TCP (THANGAVEL et al., 2014). O motivo para projetar um protocolo de camada de aplicação baseado em UDP é evitar a sobrecarga para estabelecimento e fechamento das conexões TCP, o que torna o protocolo mais adequado para o ambiente da IoT. O MQTT-SN (MQTT for Sensors Networks) (STANFORD-CLARK; TRUONG, 2013), considerado uma versão adaptada do MQTT para dispositivos que apresentam recursos computacionais restritos, pode operar sob qualquer protocolo da camada de transporte.

O CoAP é um protocolo de transferência *web* baseado no estilo REST (*Representational State Transfer*) e projetado para interagir com o HTTP (*Hypertext Transfer Protocol*). REST é um estilo arquitetônico que disponibiliza as informações fornecidas pelos dispositivos como recursos identificados por URIs (*Universal Resource Identifiers*). A Figura 8 mostra que quando os protocolos CoAP e HTTP operam conjuntamente, um proxy intermediário pode disponibilizar os recursos do CoAP transparentemente para

clientes WEB. Como o UDP não fornece entrega confiável de mensagens, o CoAP implementa seu próprio mecanismo de confiabilidade. Mensagens podem ser "confirmáveis" ou "não-confirmáveis". Mensagens confirmáveis requerem uma confirmação do nó receptor.

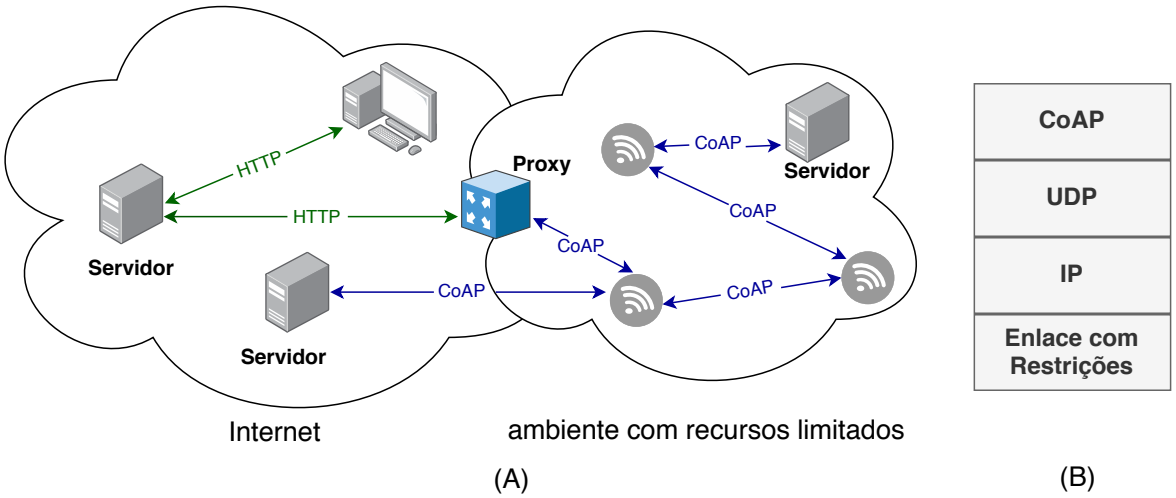


Figura 8 – Implementação da arquitetura WEB com HTTP e CoAP (BORMANN; CASTELLANI; SHELBY, 2012). (a) HTTP e CoAP operam conjuntamente; (b) Pilha de protocolos do CoAP.

Duas arquiteturas são suportadas: **recurso-observar** e **requisição-resposta**. A arquitetura recurso-observar permite que um cliente (observador) registre seu interesse em um determinado recurso indicado por um URI. Quando um dispositivo atualiza o URI com um novo valor, todos os observadores são notificados. Como exibe a Figura 9, os dados fluem dos dispositivos IoT para os observadores como um fluxo de notificações (MISIC; ALI; MISIC, 2018). Não é possível atribuir um único URI a múltiplos dispositivos (SHELBY; HARTKE; BORMANN, 2018). Caso a arquitetura requisição-resposta seja adotada, os clientes enviam requisições a um servidor e recebem dados em resposta à estas requisições.

Para atender à necessidade de comunicação com vários dispositivos, o *IETF CoRE Working Group* desenvolveu o *Group Communication for CoAP Internet Draft* (RAHMAN; DIJK, 2014). Nesse contexto, mensagens *multicast* UDP/IP são usadas para solicitações e mensagens *unicast* UDP/IP para respostas. Mensagens *multicast* não são confirmáveis. Além disso, a arquitetura requisição-resposta não oferece suporte para o monitoramento periódico dos dados.

Em (HOU; LI; QIU, 2014), os autores propõem SeaHTTP a fim de estender o CoAP para que os dispositivos possam ingressar e sair de grupos de acordo com as necessidades dos clientes. Embora a estratégia proposta reduza o número de mensagens, os dispositivos precisam ser reprogramados sempre que ingressam em um grupo. Portanto, os nós da rede devem ter inteligência necessária para decidir participar ou sair de um determinado grupo.

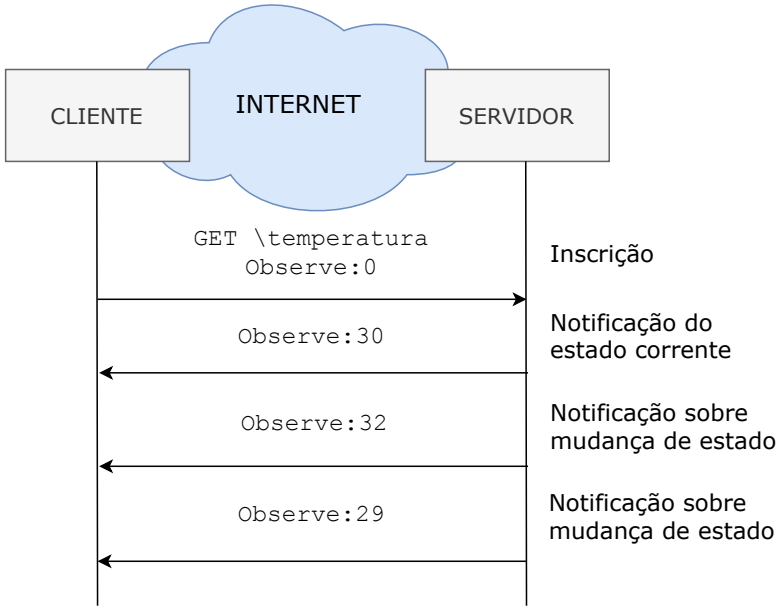


Figura 9 – CoAP – arquitetura recurso-observar.

Em (ISHAQ et al., 2014), uma solução para comunicação em grupo baseada no CoAP é apresentada. A solução proposta adota lotes de mensagens *unicast* como alternativa à soluções baseadas em mensagens *multicast*. Para isto, um componente extra chamado *Entity Manager* (EM) atua como um proxy entre os clientes e a rede. O EM analisa as solicitações recebidas, cria uma entidade (um grupo de recursos), atribui um URI e armazena no banco de dados da entidade para uso futuro. Então, o EM envia solicitações individuais para os respectivos dispositivos usando mensagens *unicast*. Como a solução não requer a criação e manutenção de grupos de comunicação e utiliza uma abordagem baseada em mensagens *unicast*, a falta de flexibilidade e confiabilidade são superadas. No entanto, lotes de mensagens *unicast* usualmente implicam em latência e alta sobrecarga de comunicação. Em (ISHAQ et al., 2016), a solução baseada em mensagens *unicast* é estendida com suporte a comunicação *multicast*, permitindo que os clientes escolham a abordagem mais apropriada de acordo com suas necessidades. O EM é responsável por solicitar que membros individuais participem e saiam de grupos *multicast*. A solução baseada em *multicast* fornece escalabilidade e menor tempo de resposta às custas de confiabilidade reduzida.

O MQTT (LOCKE, 2010) é um protocolo simples e leve, particularmente adequado para conexões M2M. A arquitetura publicar-inscrever baseada em tópicos é utilizada. Os dispositivos inteligentes (publicadores) enviam mensagens para um endereço denominado tópico em determinado servidor (*broker*). Os clientes se inscrevem nos tópicos disponibilizados pelo *broker* para receber as mensagens enviadas para os referidos tópicos. Portanto, os publicadores são fontes de dados que transmitem informações para os clientes

por meio do *broker*. O MQTT fornece uma maneira particular de comunicação em grupo, permitindo que vários publicadores enviem mensagens para um mesmo tópico. A Figura 10 exibe um exemplo de uma rede simples formada por três clientes e um broker (JAFFEY, 2018). Inicialmente os clientes "B"e "C"inscrevem-se no tópico temperatura. Em seguida, "A"publica o valor "30.5"para o tópico temperatura e o broker notifica "B"e "C".

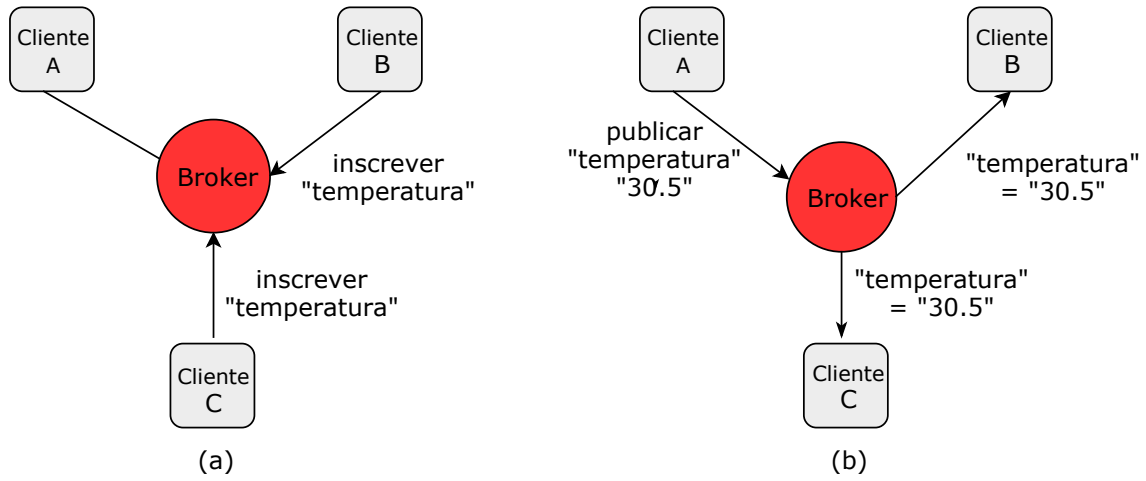


Figura 10 – Uma rede com três clientes e um broker executando o MQTT (JAFFEY, 2018).

A confiabilidade das mensagens é alcançada por três níveis de Qualidade de Serviço (QoS):

1. *Fire and Forget* - A mensagem é enviada uma única vez e não requer confirmação do nó receptor.
2. Entregue pelo menos uma vez - A mensagem é enviada ao menos uma vez e requer confirmação do nó receptor.
3. Entregue exatamente uma vez - Um mecanismo de *handshake* é utilizado garantir que a mensagem seja entregue exatamente uma vez.

Embora o MQTT seja projetado para apresentar baixo *overhead*, os publicadores enviam dados para o *broker* mesmo que não hajam clientes inscritos. Este modo de operação causa o consumo desnecessário dos recursos da rede. Além disso, o MQTT utiliza o TCP como protocolo de transporte a fim de obter sequências ordenadas e sem perda de pacotes. Entretanto, o TCP é muito complexo para dispositivos simples e que apresentam recursos computacionais restritos.

As principais diferenças entre o MQTT e o MQTT-SN envolvem a independência para operar sob qualquer protocolo da camada de transporte e a a redução no tamanho das

mensagens. Para atender as exigências relacionadas ao tamanho das mensagens e largura de banda limitada das redes sem fio, o MQTT-SN utiliza códigos (IDs) associados aos nomes dos tópicos. Ao registrar um tópico, o publicador obtém o código correspondente. As mensagens posteriores enviadas ao *broker* contém apenas o código do referido tópico. Quando um cliente se inscreve em determinado tópico, o *broker* envia o código associado ao nome do tópico que será incluído nas mensagens subsequentes. O MQTT-SN também oferece suporte para dispositivos que desativam seus componentes e entram em estado de dormência para economizar energia. Todas as mensagens destinadas a eles são armazenadas em *buffer* e entregues posteriormente quando acordam.

3.3 Soluções Centradas em Informação

Van Jacobson (JACOBSON et al., 2009) sugeriu as ideias iniciais que levaram ao projeto do primeiro protocolo que aplicou conceitos de roteamento centrado em informação para RSSFs. O protocolo denominado *Directed Diffusion* (DD) foi apresentado por Intanagonwiwat (INTANAGONWIWAT; GOVINDAN; ESTRIN, 2000) e outros e tornou-se uma solução de roteamento clássica. Recentemente, a busca por arquiteturas alternativas para a Internet do Futuro e o crescente número de aplicações para IoT mais uma vez chamaram a atenção para a abordagem centrada em informação.

Embora seja uma solução clássica, o DD depende do *flooding* de mensagens que incorre em *overhead* considerável. Portanto, o protocolo não é adequado para RSSFs de larga escala. A Figura 11 exibe o mecanismo empregado para a coleta de dados. Para solicitar informações os usuários injetam consultas chamadas *Interesses* em algum nó arbitrário (nó sink) da rede. Uma única mensagem de Interesse coleta dados de vários nós distintos. Inicialmente, o sink envia em *broadcast* o Interesse recebido solicitando baixa taxa de envio de dados. Esta mensagem inicial é exploratória e tem como objetivo determinar se existem nós que podem enviar dados em resposta à consulta recebida. Os nós sensores também transmitem em *broadcast* os Interesses recebidos de tal forma que as mensagens de Interesse inundam a rede. Se um nó é uma fonte de dados para um Interesse, ele encaminha uma mensagem de dados para cada nó vizinho do qual o Interesse foi recebido. As mensagens de dados retornam ao longo do caminho reverso da propagação dos Interesses. Deste modo, o sink eventualmente recebe dados vindos de múltiplos caminhos. O DD adota um mecanismo chamado *reinforcement* para garantir a utilização de rotas ótimas entre os sensores e o sink e também para realizar o reparo de rotas. Após receber mensagens de dados de múltiplos caminhos, o sink seleciona um nó vizinho de acordo com regras locais e reenvia o Interesse solicitando taxa de envio de dados mais alta. Um exemplo de regra é reforçar qualquer nó que entregue dados antes que os outros.

Para monitorar a qualidade das rotas e garantir a entrega de dados, o sink permanece

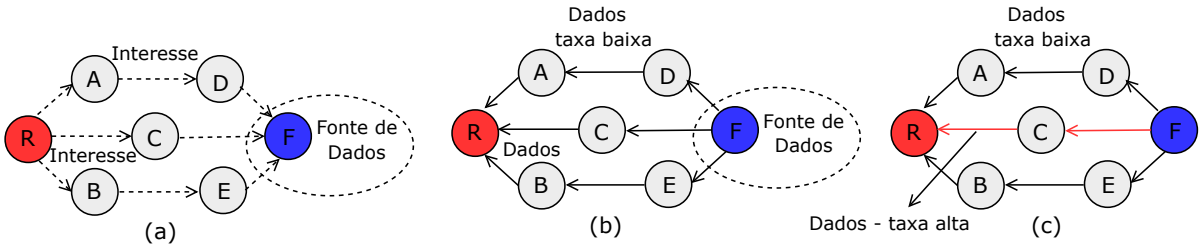


Figura 11 – Coleta de Dados no DD - (a) Propagação do Interesse, (b) Estabelecimento de Rotas, (c) Reforço de rota.

recebendo dados de múltiplos caminhos. No entanto, o caminho selecionado envia dados a uma taxa mais alta. O DD implementa um mecanismo simples de *caching* que não é suficiente para minimizar o dano de inundar constantemente uma rede com recursos limitados.

O CCN-WSN proposto em (REN; HAIL; HELLBRCK, 2013) é uma variante do protocolo CCNx projetado para microcomputadores. O protocolo CCNx não é aplicável às RSSFs, entretanto as alterações apresentadas pelo protocolo CCN-WSN incluem apenas modificações no formato das mensagens para atender os requisitos do protocolo da camada de enlace IEEE 802.15.4 e uma estratégia de nomenclatura para as informações fornecidas pelos nós. Os autores propõem a utilização imediata do CCN-WSN no topo do IEEE 802.15.4, evitando protocolos de camada superior a fim de reduzir o *overhead*. No entanto, o protocolo CCN-WSN ainda apresenta alta sobrecarga uma vez que depende de *flooding* e os nós têm que manter uma tabela listando cada solicitação de informação encaminhada. Para requisitar dados, ós nós enviam mensagens de Interesse em *broadcast*. Se o nó receptor possui a informação solicitada, uma mensagem *Content Object* é enviada em *broadcast*. Os dados são enviados somente em resposta a um Interesse e consomem o Interesse. Portanto, o protocolo não oferece suporte ao envio periódico de dados (*convergecast*). Assim como o DD, os dados retornam ao longo do caminho reverso da propagação de Interesses e um mecanismo simples de *caching* é adotado. O protocolo não implementa um mecanismo para entrega confiável de dados.

3.4 Principais Características das Soluções

As cinco principais características das soluções para RSSFs em ambientes IoT são exibidas na Tabela 1: abordagem, protocolo de transporte, protocolo de roteamento, arquitetura e mecanismo de confiabilidade.

Inicialmente, as soluções são divididas conforme a abordagem: Centrada em Endereço ou Centrada em Informação. Soluções Centradas em Endereço utilizam o endereço dos nós para o roteamento dos dados e usualmente constroem grupos de comunicação

Tabela 1 – Características de soluções para RSSFs em ambientes IoT

PROTOCOLO		**DD**	**CCN-WSN**	**CoAP**	**SeaHttp**	***unicast-based***	**MQTT**	**MQTT-SN**
Abordagem	Centrada Informação	X	X					
	Centrada Endereço			X	X	X	X	X
Transporte	UDP			X	X	X		
	TCP						X	
	Específico	X	X					
	Agnóstico							X
Roteamento	*Flooding*	X	X					
	RPL			X	X	X	X	X
Arquitetura	requisição-resposta	X	X	X	X	X		
	publicar-inscrever						X	X
	recurso-observar			X	X	X		
Confiabialidade	múltiplos caminhos	X						
	não implementado		X					
	mensagens confirmáveis			X	X	X		
	níveis de QoS						X	X

para obter dados de múltiplos dispositivos. Soluções Centradas em Informação utilizam informações fornecidas pelos nós para obter dados e não dependem da construção de grupos de comunicação.

O protocolo de transporte adotado é a principal diferença entre as soluções clássicas centradas no endereço dos dispositivos. Ao adotar o UDP busca-se evitar a sobrecarga para estabelecimento e fechamento das conexões TCP, enquanto a adoção do TCP pretende obter sequencias ordenadas e sem perdas de pacotes. A independência com relação ao protocolo de transporte pretende flexibilizar a solução para que possa atender diferentes requisitos.

A abordagem Centrada em Informação permite injetar uma única requisição na rede e obter dados fornecidos por múltiplos nós. Esta característica representa uma economia considerável em termos de energia e recursos de rede, especialmente em implantações de larga escala. Entretanto, são dependendes do *flooding* para roteamento dos dados. A abordagem Centrada em Endereço usualmente adota o RPL para roteamento de dados. O RPL apresenta uma solução energeticamente eficiente para construir e manter uma estrutura de roteamento com caminhos redundantes que reagem rapidamente à mudanças de conectividade.

Com relação à arquitetura, existem três possíveis alternativas: enviar requisições para a rede e aguardar o recebimento dos dados (requisição-resposta), inscrever-se em determinado tópico de interesse e aguardar a publicação de informações (publicar-inscrever) e registrar o interesse em determinado recurso para receber notificações quando houver modificações no referido recurso (recurso-observar). Nas arquiteturas publicar-inscrever e recurso-observar os produtores de dados enviam dados continuamente para uma unidade

central, ainda que não existam inscritos/observadores.

Três diferentes tipos de mecanismos de confiabilidade foram identificados nas soluções analisadas: recebimento de dados por múltiplos caminhos, confirmação das mensagens recebidas e utilização de diferentes níveis de QoS que envolvem tanto a confirmação de mensagens como a utilização de mecanismos de *handshake*. O recebimento de dados por múltiplos caminhos implica na transmissão e recebimento redundante de dados. Por outro lado, a exigência de mensagens de confirmação ou mecanismos de *handshake* aumenta o número de mensagens em trânsito na rede, uma vez que as próprias mensagens de confirmação podem ser perdidas.

3.5 Considerações Finais

Neste Capítulo foram analisadas as características, vantagens e deficiências de soluções propostas na literatura para coleta de dados em RSSFs em ambientes IoT. RSSFs em ambientes IoT requerem protocolos energeticamente eficientes para coletar a enorme quantidade de dados produzida por um grande número de dispositivos. Entretanto, as estratégias adotadas pelos protocolos tradicionais não são adequadas. A inundação da rede ou o envio periódico de dados para um dispositivo central causam atrasos, interferências e reduzem o tempo de vida da rede. A construção de grupos de comunicação em RSSFs de larga escala apresenta sérias limitações. A mais relevante diz respeito à escalabilidade, pois o número de grupos possíveis pode rapidamente tornar-se muito grande. Outra dificuldade está relacionada às restrições com relação ao tamanho dos grupos devido a colisões e interferências. Além disso, a construção e manutenção de rotas para os grupos de comunicação não recebeu a devida atenção.

Com relação a mecanismos de confiabilidade, nenhum dos protocolos mencionados considera o ambiente altamente dinâmico das comunicações sem fio e a escassez de recursos computacionais e energéticos dos nós sensores.

4 PROTOCOLOS PROPOSTOS

Este Capítulo apresenta os protocolos ICENET (Information Centric Protocol for Big Data Wireless Sensor Networks) e ICENET-PB (ICENET-Priority Based). Os protocolos propostos adotam o paradigma Centrado em Informações e são inspirados na abordagem CCN. O objetivo principal é fornecer soluções eficientes e robustas para coleta de dados em RSSFs de larga escala.

O roteamento baseado em informações permite que clientes interajam semanticamente com a rede. Neste contexto, os clientes podem requisitar dados por meio de consultas que são internamente processadas. Uma única mensagem coleta dados de múltiplos nós durante um período de tempo predeterminado. Não existe a necessidade de construir e manter grupos de comunicação.

Um mecanismo de estado flexível (*soft-state*) torna os protocolos robustos e preparados para perdas de pacotes e alterações na topologia de rede. Mensagens usadas para solicitar dados e para manter os *estados da rede* (informações armazenadas nos nós) atualizados são periodicamente reenviadas, de acordo com temporizadores que se adaptam à estabilidade da rede. O objetivo é enviar poucas mensagens quando a rede estiver estável para economizar energia e enviar mensagens agressivamente durante períodos de instabilidade, permitindo rápida reação a alterações topológicas. Protocolos de estado flexível apresentam grande robustez e adaptam-se rapidamente a mudanças nas condições da rede (SHARMA et al., 1997).

ICENET e ICENET-PB adotam uma estrutura de roteamento baseada em árvore. Árvores são estruturas de roteamento hierárquicas e, portanto, adequadas para economizar energia em RSSFs de larga escala (WAN; ZHANG; CHEN, 2016; RANI et al., 2015; LI et al., 2011). Em um contexto ICN, os nós pai encaminham as consultas com base na informação fornecida por seu filhos. Essa estratégia reduz significativamente o número de mensagens transmitidas e garante o uso eficiente da largura de banda do canal sem fio e dos recursos energéticos da rede.

ICENET-PB propõe reduzir o *overhead* da coleta de dados quando não é necessário obter dados de todos os dispositivos implantados em uma determinada área. Os nós sensores são usualmente implantados densamente, o que leva a uma grande quantidade de dados redundantes (VERMA; SINGH, 2018). Algumas aplicações, como Monitoramento Ambiental e Cidades Inteligentes, geralmente não requerem dados de todos os nós da rede. Em vez disso, estas aplicações podem exigir apenas um conjunto de dados que representa significativamente as informações. ICENET-PB permite que os clientes especifiquem estas exigências.

4.1 ICENET – Information Centric protocol for sEnsors NETworks

ICENET é composto por três elementos distintos que operam independentemente: *(i)* uma estrutura de roteamento baseada em árvore, construída e mantida pelo RPL, para encaminhamento das mensagens de dados (mensagens *Data*) até o gateway, *(ii)* uma topologia de roteamento sobreposta (*overlay*) centrada em informações para propagação de consultas (mensagens *Interest*) e *(iii)* um mecanismo de controle de estado flexível para confiabilidade. A Figura 12 exibe a função atribuída para cada componente do ICENET.

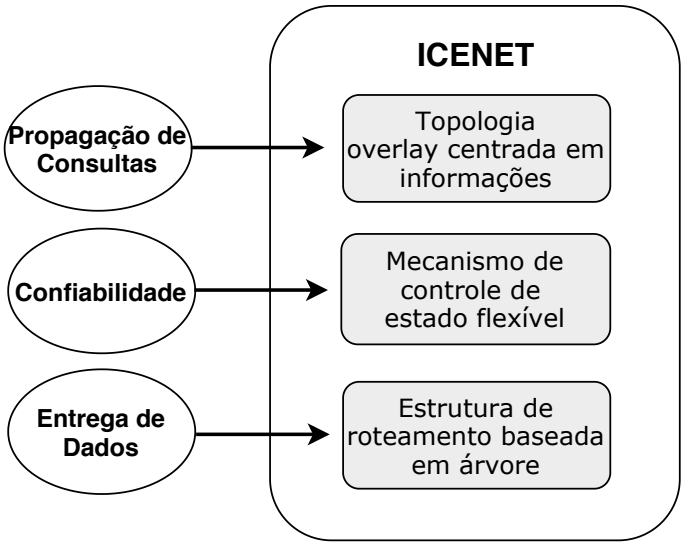


Figura 12 – Função atribuída para cada componente do ICENET.

O mecanismo de controle utilizado para confiabilidade é encarregado das retransmissões e atualizações dos Interesses armazenados na Icache. A intenção é atualizar as informações armazenadas pelos nós de acordo com as mudanças no ambiente e na topologia da rede. Ao assumir a característica de protocolos de estado flexível, ICENET e ICENET-PB tornam-se robustos e preparados para perdas de pacotes de dados devido aos ambientes dinâmicos. A estrutura de roteamento baseada em árvore é construída e mantida pelo RPL, considerado o protocolo de roteamento padrão para LLNs.

Assume-se que as consultas são injetadas na rede por um nó *gateway* (raiz) e que os nós sensores enviam dados somente em reposta a uma consulta. A estrutura baseada em árvore construída pelo RPL é encarregada de entregar mensagens *Data* para o *gateway*, enquanto a topologia baseada em informações é encarregada de encaminhar as consultas para as fontes de dados.

As mensagens de dados são retransmitidas dos nós filhos para o nó pai até chegarem ao *gateway*. Consultas são encaminhadas dos nós pai somente para os nós filhos, com base nas informações fornecidas por eles. Os nós ICENET trabalham em colaboração em uma abordagem distribuída para entregar as consultas para possíveis fontes de dados.

Abordagens centralizadas são inviáveis em implantações em larga escala, pois frequentemente requerem informações globais sobre a rede. Em ambientes dinâmicos, as abordagens centralizadas são ainda mais prejudiciais porque introduzem atrasos e sobrecarga de comunicação para manter as informações da rede atualizadas.

Para evitar a inundação da rede, que deve ser evitada em implantações IoT de larga escala (GARCIA-LUNA-ACEVES, 2017), o nó pai encaminha uma consulta somente se os nós filhos possuirem rotas para fontes de dados. Para isso, os nós mantêm uma tabela de encaminhamento denominada **FIB** (*Forwarding Information Base*) que armazena as informações fornecidas por seus nós filhos. Em comparação com outras abordagens, o tamanho desta tabela é significativamente reduzido, pois não armazena rotas para toda a rede. Se aplicarmos uma abordagem convencional em redes de larga escala, as tabelas mantidas pelos nós podem transbordar e levar ao colapso da rede. Outra vantagem de estruturas hierárquicas como árvores, é evitar o uso frequente de um mecanismo para descoberta de rotas. Além disso, árvores são a estrutura mais apropriada para agregação de dados e transmissão periódica de dados (WAN; ZHANG; CHEN, 2016).

O paradigma centrado em informações permite que os clientes obtenham dados sem o conhecimento dos endereços dos nós da rede. Assim como em (YAO; GEHRKE, 2002), assume-se que a informação é extraída da rede por meio de uma linguagem de consulta. Considerando, por exemplo, uma RSSF Ambiental implantada em uma área extensa. Um exemplo de consulta para coletar informações sobre temperatura e umidade no lago é exibido na Figura 13.

```
SELECT value FROM sensors
WHERE ATTR      = temperatura, umidade
AND REGION      = lago
starts at       2017-06-21 10:45:00
expires at      2017-06-21 23:00:00
sample rate     2 samples/min
```

Figura 13 – Exemplo de consulta para extrair informações de uma RSSF Ambiental.

Os nós decidem encaminhar uma mensagem *Interest* com base na informação armazenada localmente na FIB, cujas entradas são compostas por atributo (ATTR), região acessível (REGION) e fontes de dados (DS):

$$\textbf{FIB Entry} = \{\text{ATTR}, \text{REGION}, \text{DS}\}$$

O campo ATTR refere-se ao parâmetro físico monitorado, REGION refere-se a uma localização específica e DS representa o conjunto de nós filhos que fornecem as informações. Somente mensagens *Interest* recebidas do nó pai são processadas. Mensagens *Interest* enviadas por outros nós da rede são descartadas.

Os nós armazenam Interesses recebidos em uma tabela local denominada **Icache** (*Interest Cache*) até que expirem. As entradas da tabela Icache são compostas por identificação (ID), *timestamp* (TS), atributo (ATTR), região REGION, data de expiração (ET) e taxa de amostragem de dados (SR):

$$\textbf{Icache Entry} = \{\text{ID}, \text{TS}, \text{ATTR}, \text{REGION}, \text{ET}, \text{SR}\}$$

O campo ID refere-se a uma identificação atribuída ao Interesse pelo *gateway* e TS determina um ponto de tempo específico para iniciar a coleta de dados.

Se um nó recebe uma mensagem *Interest* e possui os dados requisitados, então uma mensagem *Data* é enviada para o nó pai. O armazenamento dos dados em *cache* é realizado apenas no *gateway*. Como a topologia da rede é baseada em árvore, Interesses são primeiramente recebidos pelo nó raiz (*gateway*) e os dados sempre convergem para a raiz. Portanto, o *cache* de dados realizado no *gateway* reduz o número de mensagens transmitidas pelos nós da rede.

Para tornar o ICENET robusto e adequado a um ambiente dinâmico, um mecanismo de estado flexível periodicamente atualiza Interesses armazenados em Icaches e as informações armazenadas nas FIBs. Os princípios do algoritmo Trickle (LEVIS et al., 2017) são incorporados para determinar a taxa de atualização dos Interesses. Os temporizadores Trickle adaptam-se dinamicamente às condições da rede, de modo que a taxa de mensagens aumenta durante períodos de instabilidade e diminui ao contrário.

A Figura 14 e o Algoritmo 1 explicam o mecanismo de processamento e encaminhamento de mensagens *Interest* no ICENET. Interesses são processados internamente pelos nós da rede, aumentando a escalabilidade da solução proposta. Além disso, uma única mensagem pode coletar dados de vários nós e por um determinado intervalo de tempo.

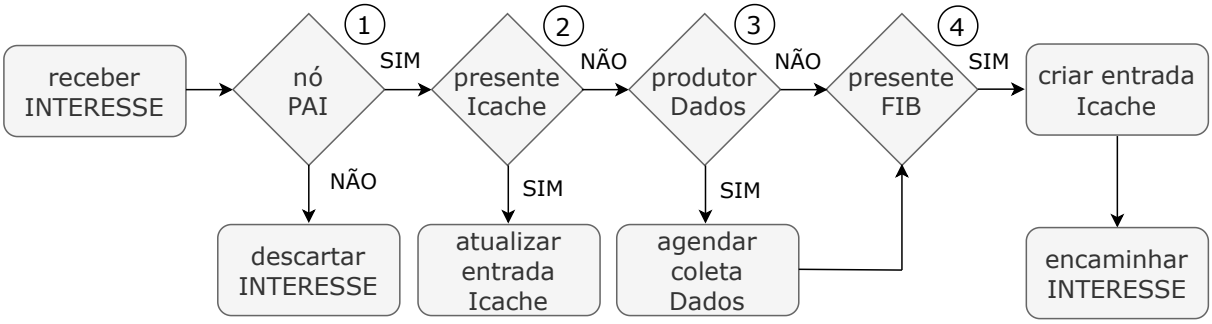


Figura 14 – Processamento e encaminhamento de mensagens *Interest*.

Os nós sensores processam somente os Interesses enviados pelo nó pai (condição 1 na Figura 14). Então, o nó receptor verifica a Icache (condição 2). Um ID correspondente na tabela significa que o interesse já foi recebido. Portanto, o nó somente atualiza a entrada

na tabela Icache se novas informações forem fornecidas. Caso contrário, o nó verifica se pode fornecer os dados solicitados (condição 3) e agenda a coleta de dados. Em seguida, o nó verifica a FIB (condição 4) para encaminhar o Interesse às fontes de dados. Se fontes de dados forem encontradas, o nó cria uma entrada na Icache, envia o Interesse em *broadcast* e inicia a execução do algoritmo Trickle.

Algoritmo 1: Interest Processing

```
1: When nó i recebe mensagem Interest do nó j
2: if parent_i = j then
3:    if existe uma entrada em Icache para o Interesse then
4:       Atualize a entrada em Icache
5:    else
6:       if i = Produtor de Dados then
7:          Agende o envio dos dados
8:       end if
9:       if existe uma entrada na FIB para os dados requisitados then
10:         Crie uma entrada em Icache
11:         Encaminhe a mensagem Interest para as fontes de dados
12:         Inicie a execução do Trickle
13:      end if
14:   end if
15: end if
```

4.1.1 Algoritmo Trickle para Interesses

O algoritmo Trickle é um mecanismo escalável, poderoso e simples que pode ser aplicado a uma ampla variedade de problemas de projeto de protocolos de rede (LEVIS et al., 2008). É um algoritmo genérico que pode ser utilizado em vários contextos, como controle de tráfego, propagação de mensagens *multicast*, descoberta e manutenção de rotas, dentre outros. O Trickle permite que nós implantados em um ambiente que apresenta alta probabilidade de perda de pacotes, possam trocar informações de modo robusto, eficiente, simples e escalável (LEVIS et al., 2008). O RPL adota o Trickle para determinar a taxa de envio de mensagens DIOS após a construção da DODAG, a fim de manter a topologia de roteamento. O ICENET por sua vez, adota os princípios do Trickle para eficientemente atualizar os Interesses armazenados na Icache. Esta flexibilidade do algoritmo Trickle decorre da possibilidade da definição específica de eventos de *consistência* e *inconsistência*.

Mensagens ou eventos consistentes não alteram a percepção do nó sobre a topologia da rede ou as condições do canal e, portanto, refletem estabilidade. Mensagens ou eventos inconsistentes indicam a necessidade de atualização. Além dos eventos de *consistência* e *inconsistência*, o Trickle possui três parâmetros de configuração:

- $I_{\min}$ – Intervalo de tempo mínimo, definido em unidades de tempo.

- $I_{\max}$ – Intervalo de tempo máximo, descrito como e o número máximo de duplicações de $I_{\min}$.
- k – Uma constante inteira positiva.

Além destes parâmetros, o algoritmo Trickle mantém três variáveis:

- I – Intervalo de tempo corrente.
- t – Ponto de tempo aleatório no intervalo $[I/2,\ I]$.
- c – Contador de consistências.

A descrição do funcionamento do algoritmo Trickle envolve seis regras:

1. Ao iniciar a execução, o algoritmo atribui à variável I um valor no intervalo $[I_{\min},\ I_{\max}]$. Então, o primeiro intervalo de tempo é iniciado.
2. Quando um intervalo de tempo inicia, o algoritmo redefine $c = 0$ e atribui a t um valor aleatório no intervalo $[I/2,\ I]$.
3. Sempre que uma mensagem ou evento consistente é detectado, c é incrementado.
4. No tempo t, os nós transmitem caso $c < k$.
5. Quando o intervalo I expira, o intervalo de tempo corrente dobra para reduzir exponencialmente a taxa de comunicação. Caso o novo intervalo I seja maior que o intervalo especificado por $I_{\max}$, então $I = I_{\max}$.
6. Sempre que uma *inconsistência* é detectada, o Trickle redefine o intervalo de tempo I para o valor inicial ($I = I_{\min}$) e inicia um novo intervalo de tempo, a fim de aumentar a taxa de envio para que os nós se adaptem rapidamente às mudanças nas condições da rede.

A Tabela 2 exibe as principais operações do algoritmo Trickle. O único momento em que o Trickle transmite é no tempo t. Por este motivo, ocorre um atraso entre a detecção de uma inconsistência e a transmissão de informações. Porém, este atraso é intencional e busca evitar que múltiplos nós transmitam ao mesmo tempo. Múltiplas transmissões simultâneas poderiam congestionar a rede, o que levaria à perda de pacotes de dados, utilização ineficiente do canal de comunicação e dos recursos dos nós.

Para adotar o algoritmo Trickle, um protocolo precisa primeiramente especificar os valores padrão para $I_{\min}$, $I_{\max}$ e k. Além disso, é necessário definir mensagens e eventos de *consistência* e *inconsistência*. O protocolo pode também definir ações adicionais a serem

Evento	**Ação**
I Expira	$I = 2 \cdot I$, onde $I \leq I_{\max}$ $c = 0$ e atribua aleatoriamente $t \in [I/2,\ I]$
t Expira	Se $c < k$ então transmita
Consistência Detectada	$c = c + 1$
Inconsistência Detectada	$I = I_{\min}$ e atribua aleatoriamente $t \in [I/2,\ I]$

Tabela 2 – Operações do algoritmo Trickle (LEVIS et al., 2008).

tomadas quando uma inconsistência é detectada. É também necessário especificar quais informações os nós transmitem nas mensagens Trickle.

Os nós ICENET consideram que receber uma mensagem *Data* de um de seus filhos representa uma *consistência*, enquanto não receber nenhuma mensagem *Data* de qualquer um de seus nós filhos durante o intervalo I representa uma *inconsistência*. Logo, o Interesse é retransmitido no tempo t. Com relação aos parâmetros de configuração, o ICENET atribui inicialmente ao parâmetro $I = I_{\min}$ e ao parâmetro $I_{\min} = \text{SP}$ (período de amostragem) do Interesse. A intuição é que após enviar um Interesse, o nó começaria a receber pacotes de dados após um tempo aproximadamente igual ao período de amostragem. Essa suposição implica condições ideais para o canal sem fio, o que significa que não ocorrem erros nos enlaces e na camada MAC. No entanto, em ambientes reais, a mensagem *Interest* pode não ser recebida por todos os nós filhos. Por este motivo, o ICENET não exige que todos os nós filhos respondam a um Interesse. Isso pode ser parametrizado por meio da constante k, que para o ICENET representa o número de nós filhos que devem responder à um determinado Interesse.

As Figuras 15, 16 e 17 exibem a execução do mecanismo de confiabilidade do ICENET para retransmissão de Interesses em diferentes cenários.

A Figura 15 apresenta uma rede formada por 8 nós e o comportamento específico do nó 3. Inicialmente, um Interesse é propagado na rede (a). O nó 3 atribui valores aos parâmetros do Trickle e aguarda o recebimento dos dados. Considera-se que todos os nós filhos podem responder ao Interesse recebido, logo $k = 3$. Em seguida, o nó 3 recebe dados de um de seus filhos e incrementa o contador de consistências c (b). Então, os nós 7 e 8 enviam dados ao nó 3 e novamente o contador de consistências é incrementado (c). No tempo t, o nó 3 compara os valores dos parâmetros c e k e verifica que não existe a necessidade de retransmitir o Interesse, pois todos os nós filhos enviaram dados. Ao expirar o intervalo de tempo I, o nó 3 dobra o valor do intervalo, atribui um novo valor ao parâmetro t dentro do novo intervalo de tempo I, zera o contador de consistências c e aguarda o recebimento de novos dados (d).

A Figura 16 exibe a execução do ICENET em uma rede formada por 8 nós e

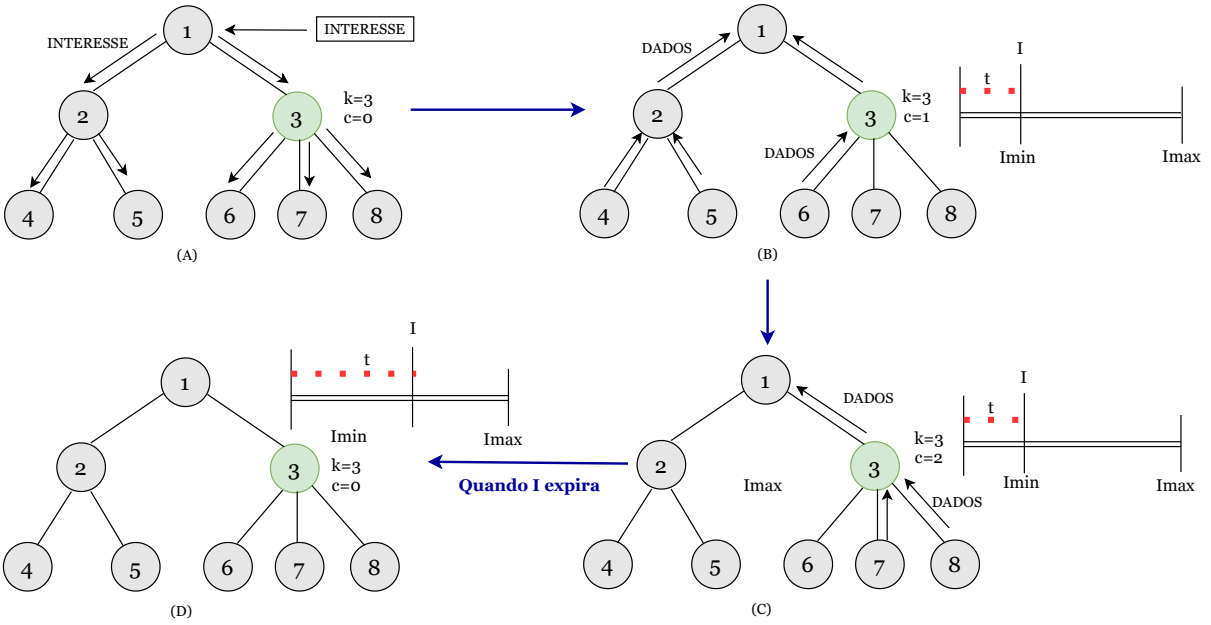


Figura 15 – Execução do mecanismo de confiabilidade do ICENET para retransmissão de Interesses – (a) Interesse propagado na rede, (b) Nó 3 recebe dados de um de seus filhos, (c) Nó 3 recebe dados dos nós 7 e 8, (d) Nó 3 inicia um novo intervalo de tempo.

o comportamento específico do nó 3. Assim como no exemplo anterior, um Interesse é propagado na rede enquanto o nó 3 atribui valores aos parâmetros do Trickle e aguarda o recebimento dos dados (a). Considera-se que todos os nós filhos podem responder ao Interesse recebido, logo $k = 3$. Os nós 6 e 8 transmitem dados ao nó 3 (b). No tempo t, o nó 3 compara os valores dos parâmetros c e k e verifica que existe a necessidade de retransmitir o Interesse, pois nem todos os nós filhos enviaram dados (c). Ao expirar o intervalo de tempo I, o nó 3 dobra o valor do intervalo, atribui um novo valor ao parâmetro t dentro do novo intervalo de tempo I, zera o contador de consistências c e aguarda o recebimento de novos dados (d).

Assim como nos exemplos anteriores, a Figura 17 exibe a execução do ICENET em uma rede formada por 8 nós e o comportamento específico do nó 3. No entanto, neste exemplo o Interesse já fora propagado e o nó 3 aguarda dados durante um novo intervalo de tempo I (a). Nenhum dos nós filhos do nó 3 envia dados em resposta ao Interesse propagado (b). No tempo t, o nó 3 compara os valores dos parâmetros c e k e verifica que existe a necessidade de retransmitir o Interesse (c). Ao expirar o intervalo de tempo I, o nó 3 detecta uma inconsistência, pois não recebeu dados de nenhum de seus filhos. Então, o nó 3 redefine o intervalo de tempo I para o valor inicial ($I = I_{\min}$) e inicia um novo intervalo de tempo para recebimento dos dados.

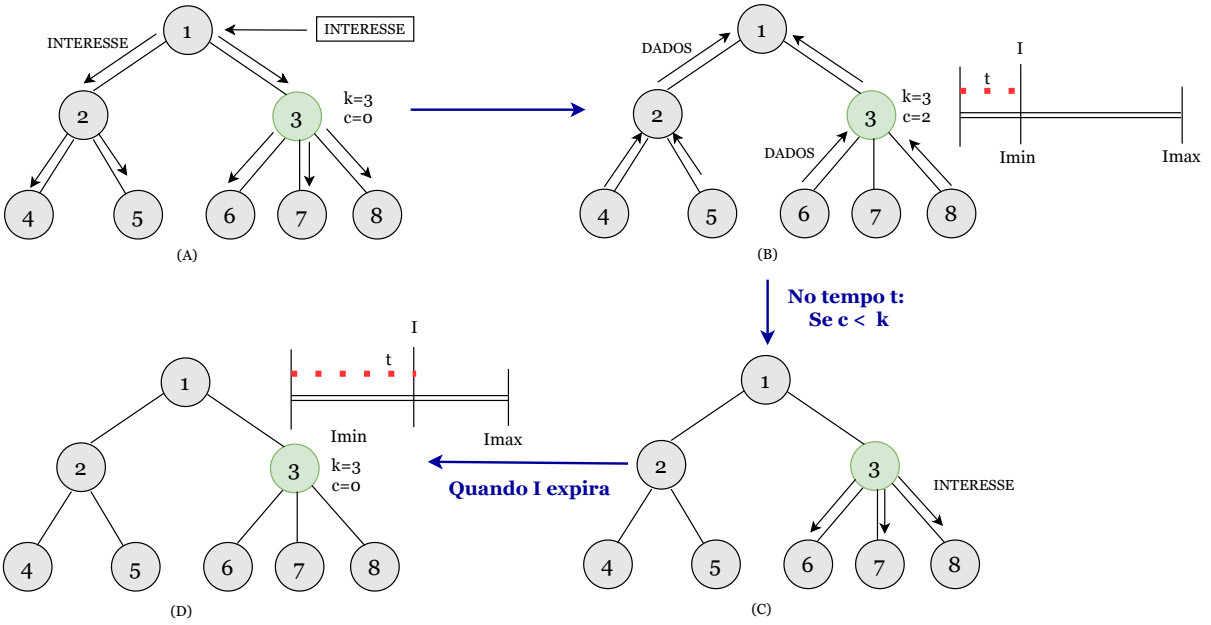


Figura 16 – Execução do mecanismo de confiabilidade do ICENET para retransmissão de Interesses – (a) Interesse propagado na rede, (b) Nó 3 recebe dados de dois nós filhos, (c) No tempo t, o nó 3 retransmite o Interesse, (d) Nó 3 inicia um novo intervalo de tempo.

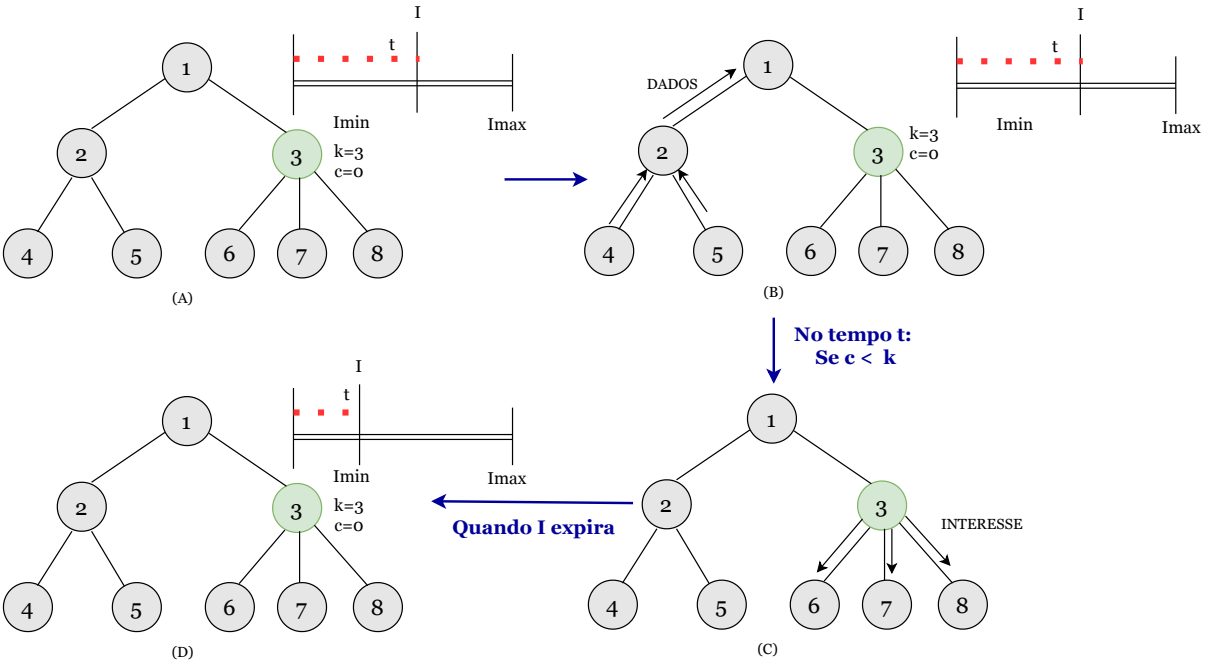


Figura 17 – Execução do mecanismo de confiabilidade do ICENET para retransmissão de Interesses – (a) Nó 3 aguarda o recebimento de dados durante um novo intervalo de tempo, (b) Nenhum dos nós filhos do nó 3 enviam dados, (c) No tempo t, o nó 3 retransmite o Interesse, (d) Nó 3 inicia um novo intervalo de tempo.

4.1.2 Estratégia para Nomenclatura da Informação

No paradigma Centrado em Informação, o elemento *nome* identifica a informação fornecida por um determinado nó da rede. Portanto, desempenha um papel fundamental na comunicação. Para o ICENET, o *nome* de uma informação é composto por dois elementos: **atributo** (ATTR) e **região** (REGION). Estes elementos descrevem o parâmetro físico monitorado e a localização do nó, respectivamente. O atributo de um nó é um nome alfanumérico plano e região é uma estrutura hierárquica de nomes, composta por um ou mais componentes alfanuméricos separados por "\". A região de implantação é sucessivamente dividida em sub-regiões representadas por diferentes componentes. A hierarquia de nomes de componentes é dependente da aplicação e deve ser definida antes da implantação da rede.

A Figura 18(a) exibe um exemplo de topologia de rede baseada em árvore, indicando os elementos ATTR e REGION em cada nó. O nó 2, por exemplo, monitora o parâmetro *umidade* e a região apresenta três níveis: *Cidade*, *Universidade* e *Biblioteca*. Um nó envia dados em resposta a um Interesse sempre que o campo REGION da mensagem corresponde parcialmente à região do nó. Portanto, o campo REGION da mensagem *Interest* define o escopo das consultas. Considerando a Figura 18, o cliente solicita informações sobre o parâmetro *nível de ruído* na região *Área Residencial* (Cidade\Área Residencial). Consequentemente, a mensagem é encaminhada para os nós 6 e 4. Caso o cliente solicitasse o mesmo parâmetro especificamente na *Area 2* (Cidade\Área Residencial\Área 2), somente o nó 4 receberia e processaria a mensagem a fim de enviar os dados para o *gateway*. A Figura 18(b) exibe a Árvore de Nomes (hierarquia de nomes dos componentes) para a topologia de rede exibida na Figura 18(a).

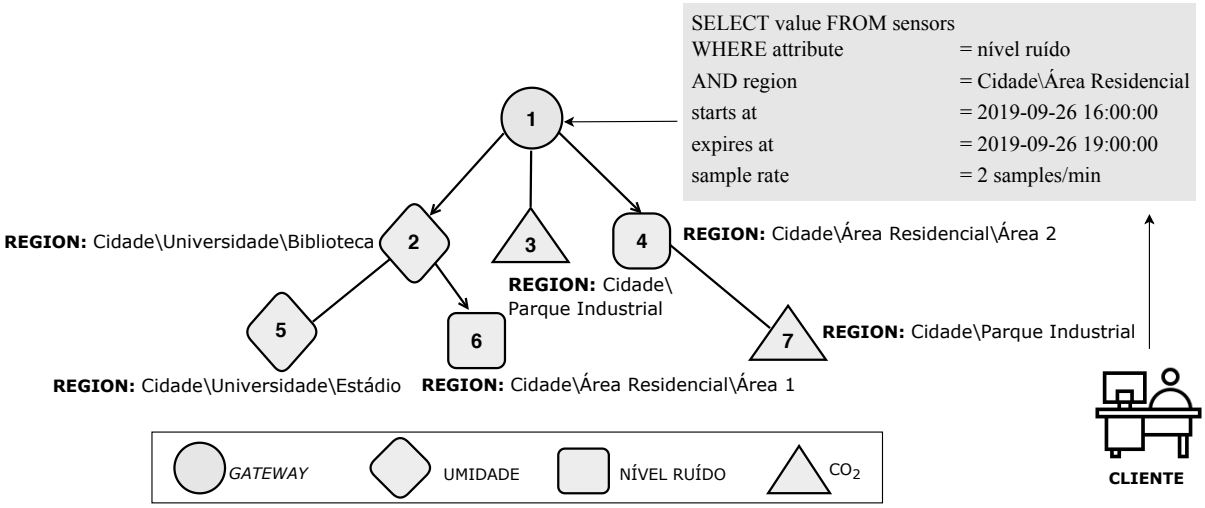
4.1.3 Procedimento para Construção e Atualização da FIB

O ICENET utiliza mensagens *Update* para preencher e atualizar as entradas da FIB, além de informar sobre a presença de novos nós ou monitoramento de novos parâmetros. Quando a execução do ICENET inicia, todos os nós sensores enviam em *unicast* uma mensagem *Update* para o nó pai. Esta mensagem contém todas as regiões distintas atualmente alcançáveis pelo nó e respectivos atributos. Nós sensores implantados após o inicio de operação da rede também enviam mensagens *Update* para o nó pai a fim de informar sua presença, regiões alcançáveis e atributos. A Figura 18 mostra um exemplo de FIB armazenada pelo nó *gateway*.

Um temporizador local T_u e um parâmetro de configuração $n > 0$ são utilizados pelos nós para definir a taxa de transmissão de mensagens *Update*. Quando T_u expira, o nó verifica a ocorrência de alterações topológicas. Se o nó pai mudou ou a FIB foi atualizada por meio da inserção ou remoção de regiões ou atributos, o nó envia uma mensagem *Update* para informar o nó pai. Deste modo, caso nós implantados após o inicio de operação

da rede apresentem atributos ainda não conhecidos, as informações sobre estes novos atributos são difundidas por toda rede. Os nós também enviam uma mensagem *Update* após $n \cdot T_u$, pois as entradas da FIB expiram após este período para evitar a utilização de rotas inválidas.

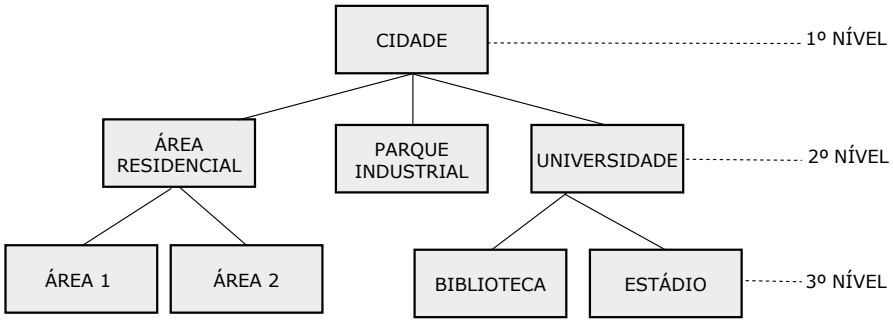
FIBs permitem o uso de diferentes rotas para cada informação fornecida pela rede. A construção de diferentes rotas reduz o tráfego de dados, prolonga a vida útil da rede, melhora a escalabilidade e o uso eficiente do canal sem fio.



FIB Nó 1

ATTR	REGION	DS
NÍVEL RUÍDO	Cidade\Área Residencial\Área1	2
NÍVEL RUÍDO	Cidade\Área Residencial\Área2	4
UMIDADE	Cidade\Universidade\Biblioteca	2
UMIDADE	Cidade\Universidade\Estádio	2
CO_2	Cidade\Parque Industrial	3-4

(A)



(B)

Figura 18 – (a) Exemplo de roteamento baseado em informação sobre uma estrutura baseada em árvore. (b) Árvore de Nomes.

4.1.4 Arquitetura do ICENET

A pilha de protocolos do ICENET é exibida na Figura 19. A comunicação nas camadas Física (PHY) e Controle de Acesso ao Meio (MAC) são suportadas pelo IEEE 802.15.4 (IEEE, 2006), considerado o protocolo padrão para as camadas mais baixas em arquiteturas IoT. A camada de adaptação 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*) (KUSHALNAGAR; MONTENEGRO; SCHUMACHER, 2007) permite a transmissão de pacotes IPv6 sobre IEEE 802.15.4, cujas funcionalidades mais pertinentes são: compressão, fragmentação e remontagem de pacotes IPv6. A razão para a escolha do UDP como protocolo de transporte é evitar a sobrecarga e complexidades do TCP. Além disso, como o ICENET possui seu próprio mecanismo de confiabilidade adequado para RSSFs, as funções de confiabilidade do TCP não são necessárias.

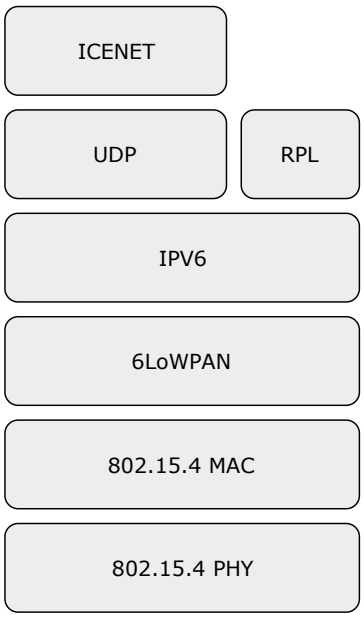


Figura 19 – Pilha de protocolos do ICENET

4.2 ICENET-Priority Based

RSSFs de larga escala usualmente apresentam uma grande quantidade de dados redundantes. A redundância é útil para fornecer confiabilidade e precisão. Por outro lado, esgota a energia dos nós sensores e diminui a vida útil da rede devido à aquisição e comunicação de dados duplicados. Certas aplicações, como Monitoramento Ambiental e Cidades Inteligentes, geralmente requerem um conjunto de dados que represente significativamente a informação solicitada.

Para atender aplicações que não exigem dados de todos os nós da rede , ICENET-PB permite especificar níveis de prioridade para as consultas realizadas pelos clientes. O

nível mais alto requer dados de todas as fontes de dados. Níveis mais baixos requerem dados de um determinado subconjunto de fontes de dados. Portanto, Interesses de alta prioridade exigem mais recursos da rede. Os níveis de prioridade são parametrizados de acordo com os requisitos das aplicações. A Figura 20 exibe um exemplo de consulta cujo nível de prioridade é especificado.

```
SELECT value FROM sensors
WHERE atributo  = temperatura, umidade
AND região      = lago
priority level  = 2
starts at       2017-06-21 10:45:00
expires at      2017-06-21 23:00:00
sample rate     2 samples/min
```

Figura 20 – Exemplo de consulta com nível de prioridade.

O nível de prioridade requisitado é informado na mensagem *Interest* e controla o mecanismo de confiabilidade do ICENET, descrito na subseção 4.1.1. A Figura 21 exibe a função atribuída para cada componente do ICENET-PB. Diferentemente do ICENET, o mecanismo de confiabilidade do ICENET-PB apresenta uma Camada de Adaptação para definição do número de filhos que deveriam responder determinado Interesse considerando o nível de prioridade informado.

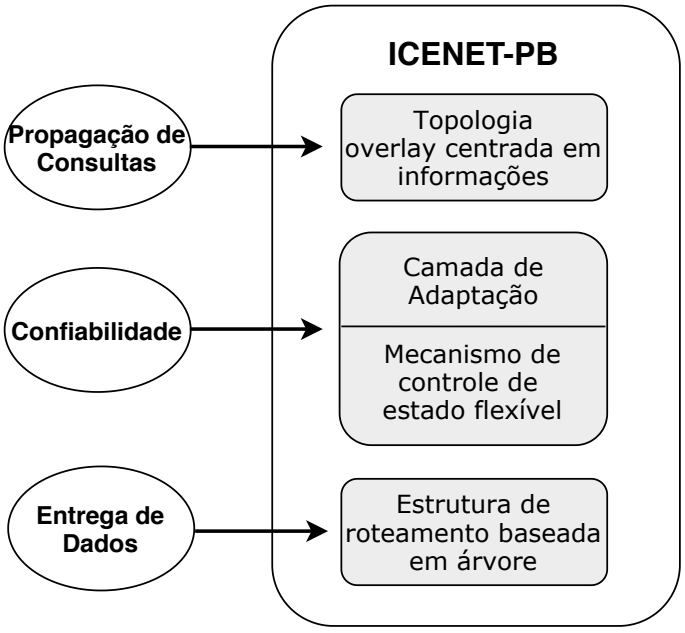


Figura 21 – Função atribuída para cada componente do ICENET-PB.

Para o mecanismo de confiabilidade dos protocolos ICENET e ICENET-PB, o parâmetro k representa o número de *nós filhos que deveriam enviar dados em resposta a*

um Interesse (fontes de dados). Para o ICENET-PB, o cálculo de k dependente do *valor correspondente ao nível de prioridade* (p):

$$k = \sum |\text{nós filhos fontes de dados}| * 0 < p < 1 \tag{4.1}$$

O nível de prioridade mais alto corresponde a $p = 1$ e equivale ao ICENET original. As informações sobre os nós filhos que podem enviar dados em resposta a um Interesse são extraídas da FIB.

O valor do parâmetro k impacta diretamente no comportamento dos protocolos propostos. Isto ocorre porque o mecanismo de confiabilidade compara k e o número de filhos que enviaram dados (c) dentro de um determinado espaço de tempo para decidir sobre o reenvio de um Interesse, como descrito na subseção 4.1.1. Caso $c < k$, o mecanismo de confiabilidade entende que a rede apresenta instabilidade. As principais causas de instabilidade da rede são: alterações de topologia, efeitos de canal sem fio e perda de mensagens. Portanto, o valor de k impacta tanto na propagação dos Interesses na rede como no posterior recebimento de dados. Quando não existe a exigência de que todos os nós da rede enviem dados, o valor de k implica em uma economia considerável de energia relacionada ao envio de mensagens. Além disso, receber um grande número de dados não significa alta precisão e confiabilidade. Geralmente é mais importante receber poucos pacotes de dados de N sensores espalhados por uma certa área geográfica do que muitos pacotes de um único sensor (HULL; JAMIESON; BALAKRISHNAN, 2004).

4.3 Considerações Finais

Este capítulo apresentou os protocolos distribuídos ICENET e ICENET-PB para coleta de grandes volumes de dados em RSSFs de larga escala. Ambos os protocolos adotam o paradigma Centrado em Informações e permitem que os clientes interajam semanticamente com a rede. Além disso, as soluções propostas não dependem da construção e manutenção de grupos de comunicação.

Uma topologia de roteamento baseada em informações é utilizada para a propagação de consultas, enquando uma estrutura de roteamento baseada em árvore é encarregada do encaminhamento dos dados até o *gateway*. Nós pais enviam consultas com base nas informações fornecidas pelos nós filhos. Esta estratégia evita algumas dificuldades apresentadas por soluções clássicas, como a inundação da rede e o consumo desnecessário de energia.

Um mecanismo de confiabilidade de estado flexível é incorporado para tornar os protocolos adequados ao ambiente dinâmico das comunicações sem fio. As informações

sobre a rede e sobre as consultas realizadas são armazenadas nos nós e periodicamente atualizadas por meio de temporizadores que adaptam-se à estabilidade da rede.

ICENET-PB representa uma solução para aplicações que não exigem dados de todos os nós da rede e supõe uma economia considerável de energia. Ainda assim, o mecanismo de confiabilidade garante a precisão dos dados ao garantir que são oriundos de um subconjunto de nós e não de um único dispositivo.

5 RESULTADOS

Para avaliar eficiência, escalabilidade e confiabilidade, ICENET e ICENET-PB ($p \in \{0.8, 0.7\}$) são comparados com o CoAP, selecionado por representar um dos protocolos mais populares para ambientes IoT (Raza et al., 2016; KARAGIANNIS et al., 2015). As simulações apresentam duas fases. A primeira fase compara o ICENET e o CoAP em um cenário que apresenta implantações de larga escala onde a construção de grupos de comunicação é inviável. Nesta situação, a inviabilidade ocorre tanto pelo número de possíveis grupos quanto pelo número de membros que podem fazer parte de um determinado grupo. A segunda fase compara ICENET, ICENET-PB e CoAP com suporte para construção de grupos de comunicação e comunicação *multicast*. As implentações do CoAP adotam o RPL para o roteamento dos dados. Durante a segunda fase, o modo de operação do RPL é *Storing with multicast support*, como descrito em (WINTER et al., 2017; OIKONOMOU; PHILLIPS; TRYFONAS, 2013). A partir deste ponto, assumimos que o termo "consulta"representa uma solicitação de informações para todos os protocolos avaliados.

5.1 Modelagem de rede e ambiente de simulação

As seguintes suposições são feitas sobre a rede:

1. Os enlaces entre os nós são simétricos: para cada enlace $i \Rightarrow j$ existe um enlace reverso $j \Rightarrow i$.
2. O *gateway* está localizado no centro da topologia.
3. Os nós sensores são idênticos em termos de processamento, tecnologia de rádio, bateria e memória.
4. O nó *gateway* possui energia ilimitada e capacidade de armazenamento e processamento superiores.
5. O protocolo CSMA/CA (*Carrier sense multiple access with collision avoidance*) é adotado para o controle de acesso ao meio.

As suposições **01** e **03** são usuais em simulações para RSSFs e visam simplificar a interpretação de resultados. A suposição **02** não afeta a comparação entre os protocolos. O nó *gateway* foi posicionado no centro da topologia porque a distribuição das mensagens na rede se torna mais uniforme à medida que o número de nós próximos ao *gateway* aumenta. A suposição **04** também é usual em ambientes de simulações para RSSFs porque

o *gateway* geralmente apresenta energia ilimitada e maior ecapacidade de armazenamento e processamento em cenários reais. A suposição **05** refere-se à adoção do IEEE 802.15.4 para controle de acesso ao meio.

Considera-se topologias de rede no formato grade com perturbações aleatórias na posição dos nós. A Figura 22 exibe um exemplo da topologia de rede adotada.

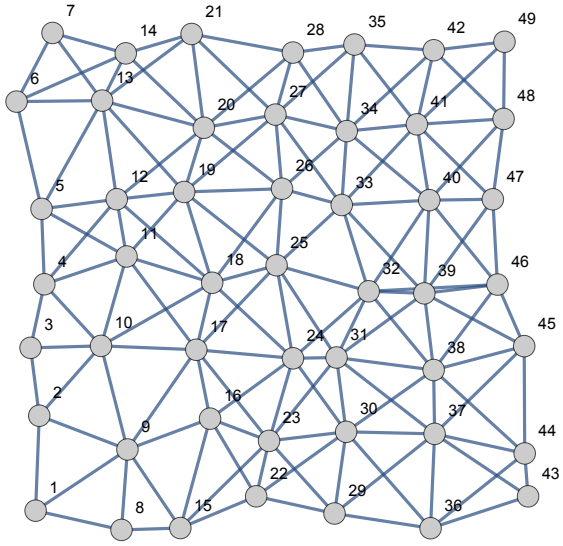


Figura 22 – Topologia no formato grade com perturbações aleatórias na posição dos nós

O *software* Mathematica (RESEARCH, 2012) juntamente com a biblioteca *SensorSim* (JAMHOUR, 2011) foram utilizados para executar as simulações. A biblioteca *SensorSim* adota os parâmetros de transmissão do IEEE 802.15.4. A Tabela 3 exibe os parâmetros adotados para controlar a taxa de encaminhamento de Interesses e de mensagens *Update*. O valor atribuído para $I_{\max}$ descreve o número máximo de duplicações de $I_{\min}$ (intervalo de tempo mínimo).

Tabela 3 – Parâmetros para atualizar Interesses e FIBs.

Parâmetro	**Descrição**
$I_{\min}$	SP (período de amostragem) do Interesse
$I_{\max}$	4
consistência	receber uma mensagem de dados de um nó filho
inconsistência	não receber nenhuma mensagem de dados
T_u	1 s
n	$0,004$ s

5.2 Modelo do canal sem fio

Assumimos um canal sem fio sujeito ao desvanecimento quase-estático. A relação sinal-ruído instantânea (SNR) medida por um nó j por meio de um pacote de dados recebido do nó i é dada por (GOLDSMITH, 2005):

$$\gamma_{ij} = |h_{ij}|^2 \, \frac{P_r}{N}, \tag{5.1}$$

onde P_r é a potência média recebida, N é a potência do ruído e h_{ij} é o ganho do canal. O desvanecimento do canal h_{ij} segue a distribuição Nakagami-m, enquanto $|h_{ij}|^2$ segue a distribuição Gamma. A função densidade de probabilidade de γ_{ij} é portanto

$$f_{\gamma_{ij}}(x) = \frac{(m/\overline{\gamma}_{ij})^m \; x^{m-1}}{\Gamma(m) \; e^{mx/\overline{\gamma}_{ij}}}, \tag{5.2}$$

com $\Gamma(a) = \int_0^\infty y^{a-1} \; e^{-y} dy$ sendo a função Gamma e $\overline{\gamma}_{ij} = P_r/N$. A potência média recebida é dada por

$$P_r(d_{ij}) \text{ [dBm]} = P_r(d_0) \text{ [dBm]} - 10 \, \alpha \log_{10} \left(\frac{d_{ij}}{d_0} \right) + S, \tag{5.3}$$

onde d_{ij} é a distância entre os nós i e j, $P_r(d_0)$ representa a potência recebida a uma distância de referência d_0, o parâmetro α é o expoente de perda de percurso e S representa o sombreamento, que segue uma distribuição Gaussiana com média zero e variância σ^2 em dB (Chen et al., 2010). Assume-se um ambiente homogêneo, com expoente de perda de percurso $\alpha = 3$, desvanecimento Nakagami-m com parâmetro $m = 2$ e variância de sombreamento $\sigma^2 = 5$ dB, para todos os nós.

5.3 Configuração da simulação

Para realizar as simulações, considerou-se topologias geradas aleatoriamente com número de nós $N \in \{100, 200, 300\}$. A região de implantação R apresenta três níveis: {City\Residential Area\Area 1}. Quatro parâmetros físicos são monitorados pela rede, mas cada nó monitora um único parâmetro. Durante uma rodada de simulação, uma única consulta solicitando um parâmetro físico por 300 s é injetada na rede. A mesma consulta é processada por todos os protocolos avaliados.

Durante a Fase I, para cada N foram executadas 18 simulações divididas em três grupos de seis rodadas. Cada grupo de simulação assume uma taxa de amostragem diferente SR $\in \{5, 10, 30\}$ s. Dentro dos grupos de simulação, as consultas injetadas são distribuídas uniformente entre os três níveis da região de implantação R.

Durante a Fase II, para cada N foram executadas 30 simulações divididas em três grupos de 10 rodadas. Cada grupo representa um nível da região de implantação R. Para o CoAP, cada um dos níveis corresponde a um grupo *multicast* distinto e SR = 10 s.

5.4 Resultados - Fase I

A Figura 23 exibe o número médio de consultas encaminhadas pelos nós por rodada de simulação. Esta é uma métrica importante porque impacta diretamente no tempo de vida da rede, uma vez que a comunicação de dados é a atividade que mais consome a energia dos nós sensores (Raza et al., 2016; Song; Li, 2018). Além disso, o número de mensagens propagagadas está relacionado ao uso eficiente do canal sem fio, interferência e atrasos. É possível observar que quanto maior o número de nós, mais significativa é a diferença entre o número de consultas encaminhadas pelos dois protocolos. Em um cenário com 100 nós, os nós ICENET encaminham 75.60 consultas, enquanto os nós CoAP encaminham 245.44 mensagens. Em um cenário com 300 nós, os nós ICENET encaminham 129.33 consultas, enquanto os nós CoAP encaminham 1079.61 mensagens. Comparando os dois cenários, o ICENET aumenta o número de consultas encaminhadas em 71% quando o número de nós aumenta de 100 para 300, enquanto o CoAP apresenta um aumento de aproximadamente 340%. Em outras palavras, em um cenário com 300 nós, o CoAP encaminha aproximadamente 8 vezes mais consultas que o ICENET. Esta diferença ocorre porque o CoAP envia uma solicitação para cada nó que monitora o parâmetro físico requisitado. Além do maior número de consultas encaminhadas inicialmente por cada nó, comunicações *unicast* causam a retransmissão de mensagens perdidas pela camada MAC.

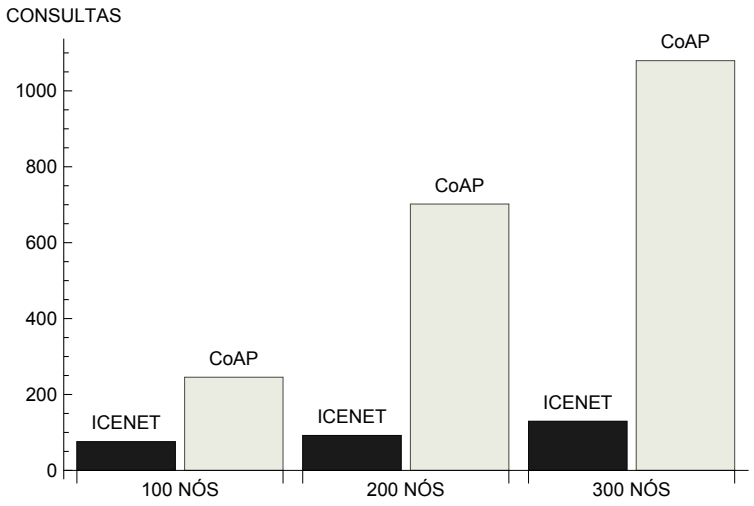


Figura 23 – Número médio de consultas encaminhadas pelos nós da rede.

A Figura 29 mostra o número médio de mensagens de dados recebidas pelo nó *gateway* por rodada de simulação. Embora os nós CoAP encaminhem mais consultas, em

cenários com 200 e 300 nós o *gateway* ICENET recebe maior número de mensagens de dados. Em um cenário com 100 nós, o servidor CoAP recebe aproximadamente 6% mais mensagens de dados que o *gateway* ICENET. No entanto, em um cenário com 300 nós, o gateway ICENET recebe aproximadamente 47% mais mensagens de dados. Quando N é maior, o ICENET apresenta os melhores resultados porque o grande número de mensagens de consulta enviadas pelo CoAP congestiona a rede. O congestionamento da rede está relacionado a atraso, interferência e perda de dados. O resultado apresentado pelo cenário com 100 nós mostra que a estratégia adotada pelo CoAP para encaminhar consultas apresenta melhor desempenho para redes formadas por poucos nós. Nestes casos, o número de mensagens necessárias para encaminhar uma consulta para cada nó que monitora o parâmetro físico solicitado e as retransmissões subsequentes executadas pela camada MAC não são suficientes para congestionar a rede e, portanto, o CoAP entrega um número maior de mensagens de dados.

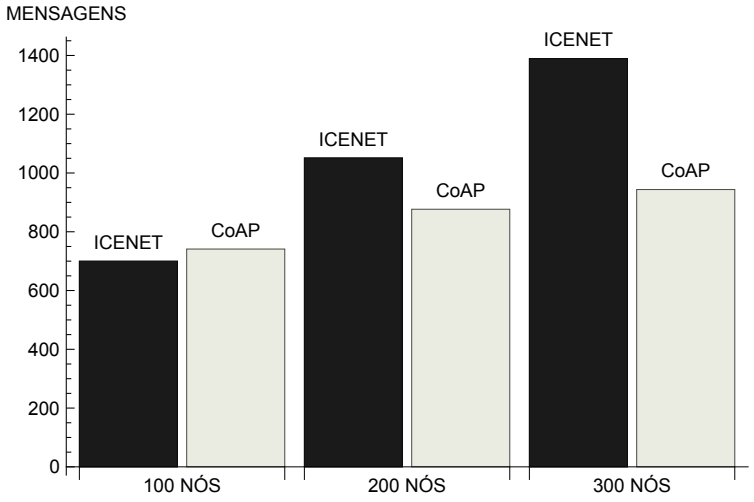


Figura 24 – Número médio de mensagens de dados recebidas pelo *gateway*.

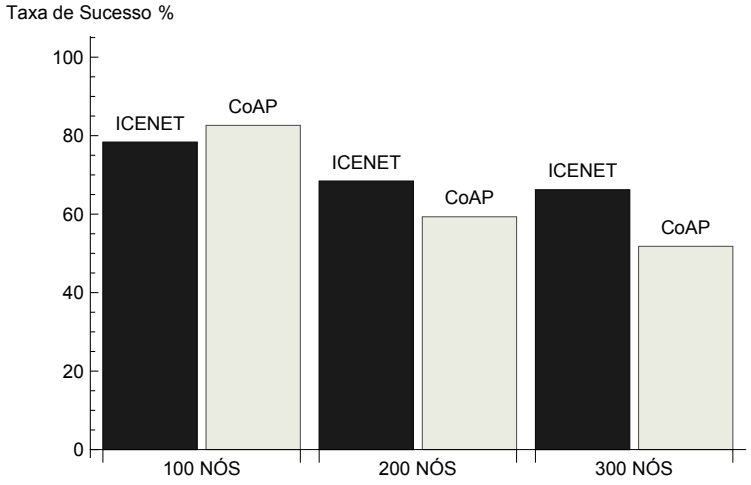


Figura 25 – Taxa de Sucesso Média.

A Figura 25 exibe a taxa de sucesso média alcançada pelos protocolos avaliados. Taxa de sucesso é a relação entre o número teórico de mensagens de dados e o número de mensagens de dados realmente recebidas. O número teórico de mensagens de dados corresponde ao número de mensagens que seriam recebidas pelo *gateway* em um cenário ideal, sem perda de pacotes devido aos efeitos do canal sem fio, interferências ou acesso múltiplo. Em um cenário com 100 nós, o CoAP apresenta uma taxa de sucesso 5% superior à taxa de sucesso apresentada pelo ICENET. No entanto, em cenários com 200 e 300 nós, o ICENET apresenta os melhores resultados. No cenário com 300 nós, o ICENET apresenta taxa de sucesso 21% superior.

A Figura 26 apresenta a sobrecarga média associada aos protocolos avaliados. Sobrecarga refere-se à relação entre o número de consultas encaminhadas e o número de mensagens de dados recebidas. O ICENET demonstra ser uma solução escalável, pois reduz a sobrecarga à medida que o número de nós aumenta. Isto ocorre porque encaminhar consultas levando em consideração os nós que podem fornecer as informações, torna-se mais eficiente à medida que aumenta o número de nós capazes de responder à consulta. Pelo contrário, a estratégia adotada pelo CoAP leva a um aumento significativo de sobrecarga à medida que a rede se torna maior. Comparando os cenários com 100 e 300 nós, o ICENET reduz a sobrecarga média em 15%, enquanto o CoAP aumenta a sobrecarga em aproximadamente 52%. No cenário com 300 nós, o ICENET apresenta uma sobrecarga média de 7%, enquanto o CoAP apresenta uma sobrecarga média de 91%.

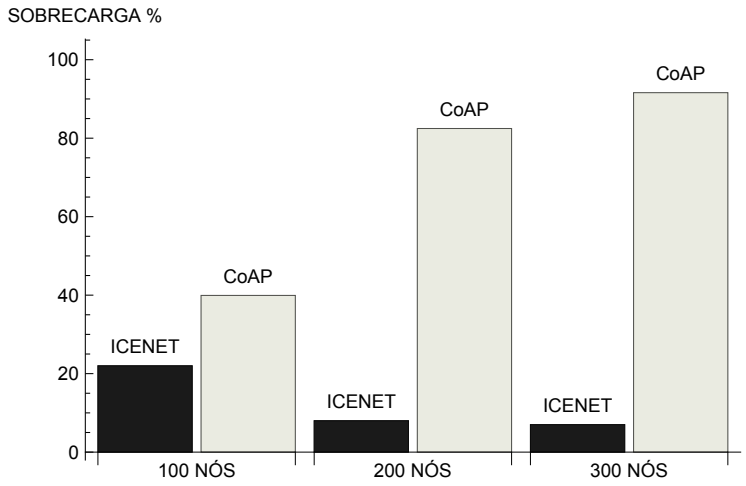


Figura 26 – Sobrecarga Média.

5.5 Resultados - Fase II

Durante a segunda fase das simulações, ao compararmos ICENET, ICENET-PB e CoAP com suporte para comunicação *multicast*, a primeira métrica avaliada é a cobertura da rede média. Cobertura de rede é definida como a relação entre o número teórico de

nós que devem responder a uma consulta e o número de nós que de fato responderam à consulta. É uma métrica importante para muitas aplicações IoT. Para alcançar alta precisão e confiabilidade, é preciso receber dados do maior número possível de sensores (HULL; JAMIESON; BALAKRISHNAN, 2004). Alcançar alta cobertura em redes sem fio multi-hop é uma tarefa difícil.

A Figura 27 apresenta a cobertura de rede média alcançada pelos protocolos avaliados. ICENET e ICENET-PB apresentam alta cobertura de rede em todos os cenários. Além disso, o ICENET apresenta aproximadamente cobertura de rede = 1.0 em todos os cenários, provando ser uma solução escalável. No cenário com maior número de nós, o ICENET-PB apresenta uma cobertura de rede 7% superior à cobertura de rede apresentada pelo CoAP. Isto ocorre porque o ICENET e o ICENET-PB adotam um mecanismo de confiabilidade, enquanto a comunicação em grupo não garante que as mensagens sejam entregues a todos os membros. O impacto da falta de um mecanismo eficiente de confiabilidade aumenta juntamente com o número de nós devido aos efeitos do canal sem fio, interferência e múltiplo acesso.

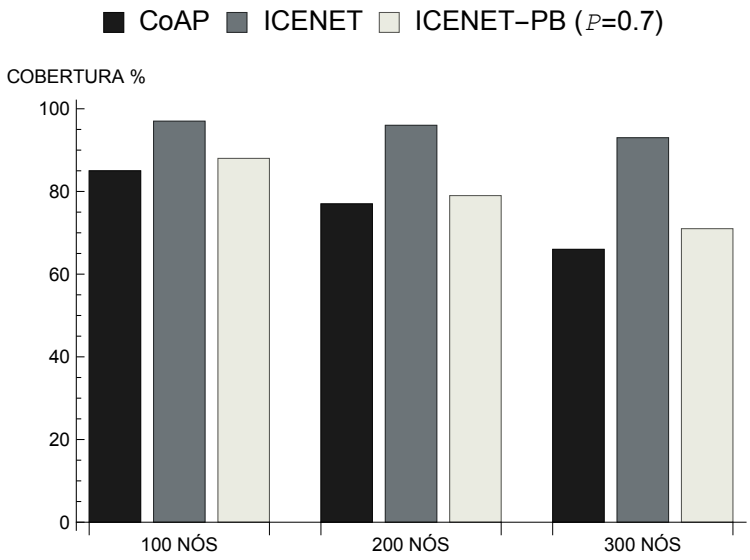


Figura 27 – Cobertura de Rede.

A Figura 28 mostra o número médio de consultas encaminhadas pelos nós por rodada de simulação. Em um cenário com 100 nós, os nós ICENET e ICENET-PB encaminharam 64 e 46 consultas em média, respectivamente, enquanto os nós CoAP encaminharam 152 mensagens em média. Em um cenário com 300 nós, os nós CoAP encaminharam aproximadamente três vezes mais mensagens que o ICENET-PB.

Figura 29 exibe o número de mensagens de dados recebidas pelo *gateway*. Considerando o cenário com maior número de nós, o *gateway* ICENET recebeu o maior número de mensagens de dados. O *gateway* ICENET-PB recebeu o menor número de mensagens de dados. No entanto, em comparação com o CoAP, a diferença no número de mensagens não

excede 10% enquanto a redução no número de consultas atinge aproximadamente 65%. Novamente, isto ocorre porque a comunicação com os membros do grupo de comunicação não é confiável. Na topologia com o maior número de nós, as consultas percorrem maior número de enlaces para alcançar as fontes de dados. Neste contexto, aumenta a possibilidade de uma consulta ser perdida antes de alcançar o destino. ICENET e ICENET-PB tratam esta possibilidade por meio de seu mecanismo de confiabilidade, o que resulta em mais mensagens de dados entregues ao *gateway*.

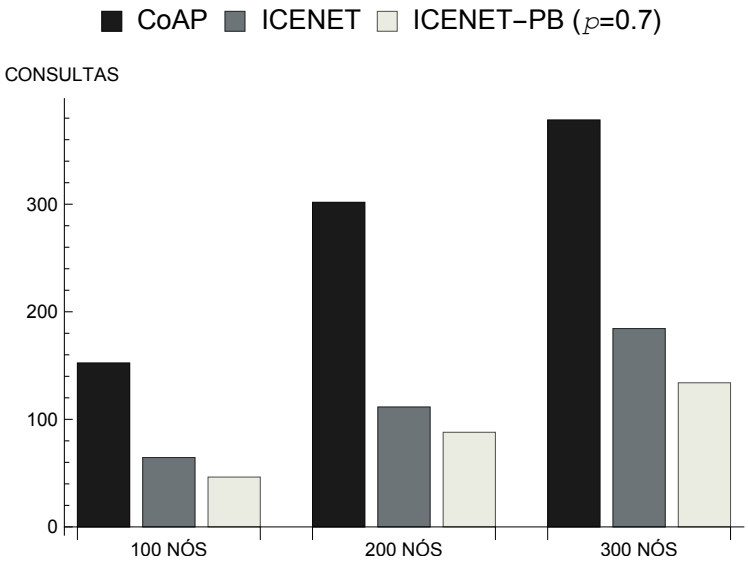


Figura 28 – Número médio de consultas encaminhadas pelos nós.

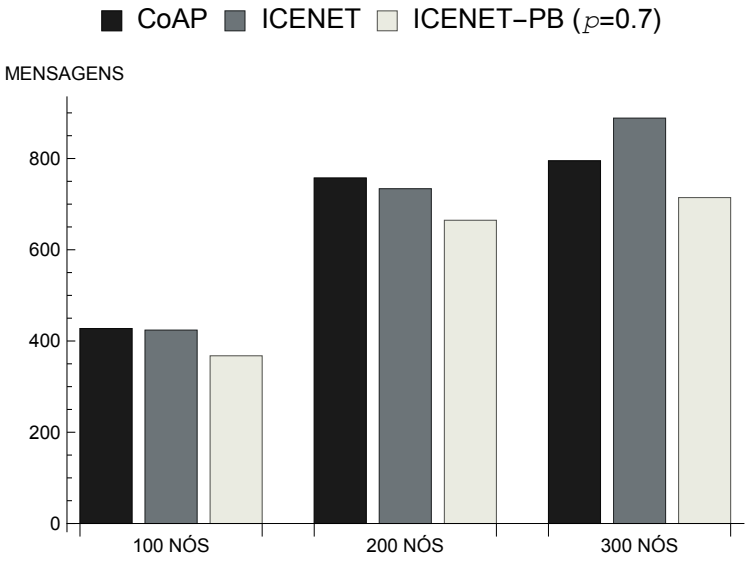


Figura 29 – Número de mensagens de dados recebidas pelo *gateway*.

A Tabela 4 apresenta um resumo da simulação e exibe o número total de consultas encaminhadas pelos nós da rede e mensagens de dados recebidas pelo *gateway*. A tabela

também compara os ganhos do ICENET-PB ($p = 0.7$) sobre o CoAP e o ICENET. Nota-se que o ganho no número de consultas em comparação com o CoAP é maior que 64% em todos os cenários. Este ganho no número de consultas afeta o número de mensagens de dados recebidas pelo *gateway*. Portanto, o *gateway* ICENET-PB recebe um número menor de mensagens de dados. No entanto, a perda no número de mensagens de dados é sempre menor que 14% e diminui à medida que o número de nós aumenta. Além disso, a redução no número de mensagens nem sempre é um aspecto negativo. As implantações em larga escala frequentemente apresentam nós redundantes e algumas aplicações não exigem dados de todos os nós, mas um conjunto de dados que representa as informações de modo confiável. A Figura 27 mostra que o ICENET e o ICENET-PB apresentam maior cobertura de rede que o CoAP em todos os cenários, o que está diretamente relacionado à precisão e confiabilidade.

Tabela 4 – Resumo da simulação.

Topologia	Mensagem	CoAP	ICENET	ICENET-PB p=0.8	ICENET-PB p=0.7	Ganho sobre CoAP	Ganho sobre ICENET
100 Nós	Consulta	4570	1935	1722	1390	0.6958	0.2817
	Dados	12822	12715	12660	11029	-0.1398	-0.1326
200 Nós	Consulta	9052	3344	2811	2639	0.7085	0.2108
	Dados	22720	22016	18504	19940	-0.1224	-0.0943
300 Nós	Consulta	11348	5532	4667	4020	0.6458	0.2733
	Dados	23855	26652	23751	21431	-0.1016	-0.1932

5.6 Considerações Finais

Este Capítulo apresentou os resultados das simulações envolvendo os protocolos ICENET, ICENET-PB e CoAP. O CoAP foi selecionado porque representa uma solução clássica e popular projetada especialmente para ambientes IoT. Além disso, permite que os clientes enviem consultas para a rede. Os protocolos propostos demonstram ser soluções mais eficientes, escaláveis e adequadas devido a vários fatores.

Durante a primeira fase das simulações, ICENET apresenta significativamente menos sobrecarga para propagação de consultas, enquanto coleta maior quantidade de dados. Além disso, demonstra ser mais escalável uma vez que a sobrecarga diminui à medida que o número de nós aumenta. Durante a segunda fase das simulações, ICENET e ICENET-PB foram comparados ao CoAP em cenários envolvendo a construção de grupos de comunicação. O principal objetivo do ICENET-PB é a redução no número de mensagens e consequente prolongamento do tempo de vida da rede quando não existe a exigência de receber dados de todos os nós implantados em determinada área, mas de um subconjunto que represente significativamente a informação solicitada. Nesta situação, ICENET e ICENET-PB apresentam menor sobrecarga enquanto coletam aproximadamente a mesma quantidade de dados oriundos de um maior número de nós, garantindo deste modo a

precisão e confiabilidade das informações. Além disso, a abordagem ICN permite que os usuários interajam semanticamente com a rede e não requer a construção e manutenção de grupos de comunicação. Por último, um mecanismo de confiabilidade eficiente torna os protocolos propostos preparados para ambientes dinâmicos. Este é um recurso importante, pois a perda de mensagens é um evento comum em redes sem fio e os nós dos sensores estão sujeitos a falhas.

6 CONCLUSÃO E TRABALHOS FUTUROS

Devido à capacidade de impactar diversos setores da sociedade, a Internet das Coisas é considerada uma revolução. Objetos físicos tradicionais são conectados à Internet e transformados em objetos inteligentes com capacidade de monitoramento, troca de informações, interação com usuários e execução de tarefas sem intervenção humana. Esta transformação impulsionou e possibilitou um grande número de aplicações com grande potencial para melhorar o bem-estar econômico e social dos seres humanos.

Diversas tecnologias conjuntamente possibilitaram o surgimento da IoT. Entretanto, as RSSFs tornaram-se um elemento essencial ao permitir que objetos que apresentam recursos computacionais restritos possam se comunicar, trabalhar colaborativamente e desempenhar tarefas complexas.

As RSSFs possuem caraceterísticas muito específicas e enfrentam diversos desafios (Capítulo 2.1). Especialmente no ambiente da IoT, as aplicações podem requerer implantação massiva de dispositivos e coleta de grandes volumes de dados. Porém, o conjunto de dados produzido em aplicações de larga escala é extremamente dificil de ser coletado, armazenado, processado e analizado utilizando-se as metodologias e abordagens de computação tradicionais. Além disso, várias aplicações emergentes requerem o envio de comandos e consultas para a rede. Existe uma necessidade crescente de interação entre os usuários e a rede. Frequentemente, comandos e consultas são enviados para conjuntos de dispositivos. Apesar disso, o tráfego descendente de dados e a comunicação com conjuntos de dispositivos receberam pouca atenção e permanecem questões de pesquisa desafiadoras.

Outro importante aspecto das RSSFs é o ambiente altamente dinâmico. Os dispositivos são propensos a falhas, comunicam-se por enlaces não confiáveis, apresentam recursos energéticos escassos e podem ser implantados em regiões inóspitas. Estes fatores podem alterar alterar rapidamente a topologia da rede e favorecer a perda de pacotes de dados.

Considerando as características particulares das RSSFs e os requisitos das aplicações emergentes, torna-se urgente propor soluções escaláveis, confiáveis, robustas e energeticamente eficientes que contemplem tanto a coleta de dados, como o envio de comandos e consultas para grupos de dispositivos.

Redes Centradas em Informação (Information-Centric Networking - ICN) é um paradigma de rede inovador concebido para atender as demandas da Internet do Futuro que recentemente chamou a atenção dos pesquisadores pela aplicação nas RSSFs (Capítulo 2.3). No paradigma ICN, o roteamento de dados está baseado nas informações fornecidas pelos nós ao invés de baseado no endereço dos nós. Este modelo de comunicação é especialmente adequado para RSSFs, pois estas redes são inerentemente centradas em

dados. O roteamento baseado em informações é escalável, facilita a coleta de dados e a comunicação com conjuntos de dispositivos, além de possibilitar a interação com a rede. Entretanto, a abordagem centrada em informações foi concebida para a Internet e requer modificações para aplicação em LLNs.

A fim de identificar vantagens e dificuldades, investigamos na literatura protocolos de comunicação tradicionais e centrados em informação para ambientes IoT (Capítulo 3). Além disso, implementamos e avaliamos os principais protocolos representantes das duas abordagens. Os protocolos convencionais centados em endereço apresentam estratégias inadequadas para redes de larga escala considerando escalabilidade, eficiência energética, comunicação com vários dispositivos e ambiente altamente dinâmico. Por outro lado, as soluções centradas em informação dependem da inundação da rede ou não apresentam uma solução completa que contempla tanto os pedidos de informação para a rede como o posterior recebimento dos dados.

Nesta tese, propomos protocolos inspirados no paradigma ICN para atender os requesitos de RSSFs de larga-escala: ICENET (Information Centric Protocol for Big Data Wireless Sensor Networks) (LACHOWSKI et al., 2019) e ICENET-PB (ICENET-Priority Based)(LACHOWSKI et al., 2020) (Capítulo 4). Os protocolos foram avaliados por meio de simulações em diferentes situações e comparados ao CoAP, um protocolo de comunicações popular para ambientes IoT (Capítulo 5).

O CoAP, assim como outros protocolos tradicionais para IoT, agrupa dispositivos de acordo com parâmetros específicos para viabilizar a comunicação com múltiplos dispositivos. Nestes cenários, uma única mensagem pode ser enviada para todos os membros de um determinado grupo ao invés de enviar uma mensagem distinta para cada dispositivo. Entretanto, a comunicação em grupo apresenta várias limitações (Capítulo 3.1). Particularmente em implantações de larga escala, esta estratégia pode ser inviável.

Em cenários onde a construção dos grupos de comunicação é inviável, comparamos ICENET e CoAP. ICENET encaminha um número significativamente menor de consultas, enquanto coleta maior quantidade de dados. O número de mensagens encaminhadas está intrinsicamente ligado à sobrecarga e eficiência energética, pois a comunicação de dados é a atividade que mais demanda energia dos dispositivos. Além disso, ICENET prova ser uma solução escalável pois o número de consultas diminui à medida que o número de nós aumenta. Ao contrário, o CoAP apresenta um aumento significativo de sobrecarga na mesma situação.

Considerando hipoteticamente a viabilidade da construção de grupos de comunicação, comparamos ICENET, ICENET-PB e CoAP. ICENET-PB estende as funcionalidades do ICENET para atender aplicações que não requerem dados de todos os dispositivos implantados em uma determinada área ou que monitoram determinados parâmetros físicos. Para estas aplicações, um determinado subconjunto confiável e preciso de dados é suficiente.

Nestes cenários, ICENET e ICENET-PB apresentam menor sobrecarga enquanto coletam aproximadamente a mesma quantidade de dados coletados pelo CoAP. Entretanto, os dados são oriundos de um maior número de nós distintos, garantindo deste modo maior precisão e confiabilidade das informações. Considerando o cenário com maior número de nós, ICENET coleta a maior quantidade de dados, enquanto ICENET-PB coleta aproximadamente a mesma quantidade de dados que o CoAP. Porém, comparativamente ao CoAP, ICENET-PB reduz significativamente o número de consultas encaminhadas pelos nós da rede.

O desempenho das soluções propostas deve-se em partes ao mecanismo de confiabilidade adotado, que juntamente com a abordagem ICN orientou o projeto dos protocolos. O mecanismo de confiabilidade utiliza uma abordadem de estado flexível e periodicamente atualiza as informações armazenadas pelos nós de acordo com temporizadores que adaptam-se às condições da rede. Deste modo, os protocolos tornam-se robustos e adequados para ambientes dinâmicos. Além disso, ambos os protocolos permitem interação semântica com a rede e não requerem a construção e manutenção de grupos de comunicação.

6.1 Resumo das Contribuições

A principal contribuição desta tese foi a concepção, implementação e validação dos protocolos de comunicação ICENET e ICENET-PB. Os protocolos propostos visam atender os requisitos das RSSFs de larga-escala no ambiente da IoT e apresentam várias novas características: abordagem centrada em informações, mecanismo de confiabilidade que adota uma abordagem de estado flexível (*soft-state*) e construção de uma estrutura hierárquica para nomenclatura das informações fornecidas pelos nós da rede.

No paradigma Centrado em Informação, o *nome* atribuído aos dados fornecidos pelos nós da rede possui um papel fundamental. A identificação dos dados é utilizada para requisitar informações e também para o roteamento de dados. Para os protocolos propostos, o "nome"de uma informação é composto pelo parâmetro monitorado pelo nó e sua localização. Dividimos a região de implantação em múltiplos níveis a fim de construir uma estrutura hierárquica de modo que uma única requisição de dados possa ser enviada para múltiplos nós. Ao especificar um nível superior na estrutura, uma requisição de dados é encaminhada também para todos os nós localizados nos níveis inferiores. Esta estratégia reduz o tráfego de dados e o consumo energético. Além disso, oferece flexibilidade para especificar diferentes requisições.

Outras contribuições desta tese incluem a identificação dos requisitos das aplicações das RSSFs de larga escala, avaliação das vantagens e limitações dos protocolos para IoT tradicionais, avaliação da aplicabilidade da abordagem ICN em RSSFs e definição de métricas de avaliação. Especificamente, nossas métricas de avaliação foram:

- Número de consultas encaminhadas pelos nós.
- Número de mensagens de dados recebidas pelo gateway.
- Taxa de sucesso – relação entre o número teórico de mensagens de dados e o número de mensagens de dados realmente recebidas.
- Sobrecarga – relação entre o número de consultas encaminhadas e o número de mensagens de dados recebidas.
- Cobertura da rede – relação entre o número teórico de nós que devem responder a uma consulta e o número de nós que de fato responderam à consulta.

Nossas avaliações indicaram que ambos os protocolos propostos apresentam alta eficiência energética e superam os resultados apresentados pelo CoAP. À medida que o número de nós aumenta, as vantagens tornam-se mais evidentes. ICENET e ICENET-PB apresentam ainda outras características importantes para as aplicações no contexto da IoT: escalabilidade, robustez e tolerância a perdas.

6.2 Trabalhos Futuros

Finalmente, é importante destacar que os protocolos de comunicação apresentados nesta tese representam as tentativas iniciais da aplicação do paradigma ICN nas RSSFs no ambiente da IoT. Abaixo, os trabalhos futuros que estão planejados para aperfeiçoar o desempenho das soluções:

1. A agregação de dados em RSSFs de larga escala representa uma solução eficiente para tratar a transmissão de grandes volumes de dados e reduzir o consumo dos recursos disponíveis na rede (BOUBICHE et al., 2018). Nestas redes, os dados transmitidos apresentam grande similaridade e redundância (Cheng et al., 2016). A agregação de dados combina dados oriundos de diferentes fontes para eliminar a redundância e consequentemente utilizar eficientemente a largura de banda, reduzir latência e prolongar o tempo de vida da rede. Estruturas hierárquicas, como as árvores empregadas pelos protocolos propostos, são a estrutura mais adequada para a agregação de dados (WAN; ZHANG; CHEN, 2016). Nestas estruturas, os nós pais executam a agregação dos dados e podem empregar diferentes funções de agregação, como MAX, MIN, MEAN, MEDIAN, SUM ou diferentes métodos de compressão (Cheng et al., 2016). Geralmente a correlação dos dados é espacial e temporal e ambas podem ser utilizadas para remover dados redundantes. Porém no caso da abordagem ICN, a correlação dos dados ocorre também com relação às informações armazenadas nos nós. Uma possível estratégia seria realizar a agregação

periodicamente. Cada nó pai aguardaria por um período de tempo predeterminado para coletar as informações e em seguida executar a agregação dos dados. A versão atual dos protocolos propostos empregam temporizadores para decidir sobre o reenvio de requisições de dados (consultas) na rede. Estes mesmos temporizadores poderiam ser empregados para a coleta e agregação de dados.

2. A fim de maximizar as vantagens alcançadas por meio da agregação de dados, o paradigma ICN pode ser integrado ao RPL. Para isto, o cálculo realizado pelo RPL para a construção das rotas poderia considerar novas métricas, como as informações fornecidas pelos nós e respectiva localização. Estes parãmetros poderiam ainda ser combinados com métricas clássicas de roteamento, como o ETX (Expected Transmission Count). A intuição é de que deste modo, pacotes de dados contendo as mesmas informações tendem a percorrer os mesmos enlaces e tornar o processo de agragação de dados mais eficiente.

3. O congestionamento da rede ocorre quando a carga de tráfego excede a capacidade da rede (HULL; JAMIESON; BALAKRISHNAN, 2004). Particularmente para as RSSFs, o congestionamento da rede degrada a qualidade do canal, abrevia o tempo de vida da rede devido ao consumo ineficiente dos recursos energéticos, favorece a saturação dos *buffers* e consequente descarte de pacotes e atrasos na entrega dos dados. O congestionamento é especialmente prejudicial em redes de larga escala, pois os pacotes de dados podem percorrer vários enlaces até serem descartados, um fenômeno denominado *livelock* (HULL; JAMIESON; BALAKRISHNAN, 2004). Na abordagem ICN original proposta para a Internet, requições de dados (Interesses) e entrega de dados mantém uma relação 1:1. Porém, para atender os requisitos das RSSFS, as soluções propostas neste trabalho permitem que uma única requisição possa coletar dados oriundos de vários dispositivos e por um certo intervalo de tempo. Portanto, mecanismos de detecção e controle de congestionamento são inevitavelmente necessários para que a rede permaneça operacional. Esta afirmação é válida para qualquer solução ICN proposta para RSSFs. Dois mecanismos tradicionalmente utilizados para detecção de congestionamento em redes sem fio são o monitoramento da ocupação do *buffer* local e da carga do canal de comunicação (WAN; EISENMAN; CAMPBELL, 2003). O canal de comunicação fornece informações precisas sobre o congestionamento da rede ao redor, porém é um mecanismo de detecção de congestionamento local. Uma solução simples e elegante de detecção e controle de congestionamento para o ICENET e ICENET-PB seria o monitoramento e gerenciamento dos *buffers* de mensagens. A capacidade total do *buffer* de cada um dos nós da rede seria igualmente compartilhada entre os Interesses armazenados pelo nó e que aguardam o envio de dados. Esta estratégia dividiria de modo justo os recursos dos nós entre os Interesses e impediria que ataques ou solicitações mal

dimensionadas congestionassem toda a rede. Pacotes de dados cujo recebimento esgotasse a cota de *buffer* destinada a certo Interesse, seriam descartados. Ao detectar que a taxa de ocupação do *buffer* excede determinado limite, os nós enviariam para seus filhos uma mensagem de notificação a fim de reduzir a taxa de envio de dados. Esta mensagem de notificação é denominada na literatura *backpressure*. (GHAFFARI, 2015). Mensagens *backpressure* são propagadas na rede até que as fontes de dados sejam alcançadas, a fim de evitar o gasto energético associado a pacotes de dados que fatalmente serão descartados.

REFERÊNCIAS

ABERER, Karl. Smart earth: Networked information management in a wireless world. In: . [S.l.: s.n.], 2007. p. 1–1. ISBN 953-184-111-X. Citado na página 28.

ABIDY, Y.; SAADALLAHY, B.; LAHMADI, A.; FESTOR, O. Named data aggregation in wireless sensor networks. In: *2014 IEEE Network Operations and Management Symposium (NOMS)*. [S.l.: s.n.], 2014. p. 1–8. ISSN 1542-1201. Citado na página 31.

AHLGREN, B.; DANNEWITZ, C.; IMBRENDA, C.; KUTSCHER, D.; OHLMAN, B. A survey of information-centric networking. *IEEE Communications Magazine*, v. 50, n. 7, p. 26–36, July 2012. ISSN 0163-6804. Citado na página 31.

AHMED, E.; YAQOOB, I.; GANI, A.; IMRAN, M.; GUIZANI, M. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, v. 23, n. 5, p. 10–16, October 2016. ISSN 1536-1284. Citado 2 vezes nas páginas 17 e 26.

AL-FUQAHA, A.; GUIZANI, M.; MOHAMMADI, M.; ALEDHARI, M.; AYYASH, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, v. 17, n. 4, p. 2347–2376, Fourthquarter 2015. ISSN 1553-877X. Citado 2 vezes nas páginas 27 e 29.

AL-TURJMAN, Fadi M. Information-centric sensor networks for cognitive iot: an overview. *Annals of Telecommunications*, Springer, p. 1–16, 2016. Citado na página 19.

AMADEO, M.; CAMPOLO, C.; MOLINARO, A.; MITTON, N. Named data networking: A natural design for data collection in wireless sensor networks. In: *2013 IFIP Wireless Days (WD)*. [S.l.: s.n.], 2013. p. 1–6. ISSN 2156-9711. Citado 2 vezes nas páginas 19 e 31.

AMADEO, Marica; CAMPOLO, Claudia; MOLINARO, Antonella; RUGGERI, Giuseppe. Content-centric wireless networking: A survey. *Computer Networks*, v. 72, n. Supplement C, p. 1 – 13, 2014. ISSN 1389-1286. Citado 2 vezes nas páginas 31 e 41.

Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-khah, M.; Siano, P. Iot-based smart cities: A survey. In: *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*. [S.l.: s.n.], 2016. p. 1–6. Citado 2 vezes nas páginas 17 e 25.

Boric-Lubecke, O.; Gao, X.; Yavari, E.; Baboli, M.; Singh, A.; Lubecke, V. M. E-healthcare: Remote monitoring, privacy, and security. In: *2014 IEEE MTT-S International Microwave Symposium (IMS2014)*. [S.l.: s.n.], 2014. p. 1–3. Citado 2 vezes nas páginas 26 e 27.

BORMANN, C.; CASTELLANI, A. P.; SHELBY, Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Computing*, v. 16, n. 2, p. 62–67, March 2012. ISSN 1089-7801. Citado 3 vezes nas páginas 9, 41 e 42.

BOUBICHE, S.; BOUBICHE, D. E.; BILAMI, A.; TORAL-CRUZ, H. Big data challenges and data aggregation strategies in wireless sensor networks. *IEEE Access*, v. 6, p. 20558–20571, 2018. Citado 3 vezes nas páginas 23, 29 e 77.

CHEBUDIE, Abiy Biru; MINERVA, Roberto; ROTONDI, Domenico. *Towards a definition of the Internet of Things (IoT)*. Tese (Doutorado), 08 2014. Citado 2 vezes nas páginas 28 e 30.

Chen, Y.; Yang, J.; Trappe, W.; Martin, R. P. Detecting and localizing identity-based attacks in wireless and sensor networks. *IEEE Transactions on Vehicular Technology*, v. 59, n. 5, p. 2418–2434, 2010. Citado na página 66.

Cheng, L.; Guo, S.; Wang, Y.; Yang, Y. Lifting wavelet compression based data aggregation in big data wireless sensor networks. In: *2016 IEEE 22nd International Conference on Parallel and Distributed Systems (ICPADS)*. [S.l.: s.n.], 2016. p. 561–568. Citado na página 77.

CHERITON, D.; GRITTER, Mark. Triad: A new next-generation internet architecture. 01 2000. Citado na página 31.

CISCO. *Cisco Annual Internet Report (20182023) White Paper*. 2020. Disponível em: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html>. Citado na página 19.

Cook, D. J.; Crandall, A. S.; Thomas, B. L.; Krishnan, N. C. Casas: A smart home in a box. *Computer*, v. 46, n. 7, p. 62–69, 2013. Citado na página 25.

DINH, N. T.; KIM, Y. Potential of information-centric wireless sensor and actor networking. In: *2013 International Conference on Computing, Management and Telecommunications (ComManTel)*. [S.l.: s.n.], 2013. p. 163–168. Citado na página 19.

DJEDOUBOUM, Asside Christian; ARI, Ado Adamou Abba; GUEROUI, Abdelhak Mourad; MOHAMADOU, Alidou; ALIOUAT, Zibouda. Big data collection in large-scale wireless sensor networks. *Sensors*, v. 18, n. 12, 2018. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/18/12/4474>. Citado na página 25.

DO, Truong-Xuan; KIM, Younghan. Information-centric wireless sensor and actor network in the industrial network. In: IEEE. *2013 International Conference on ICT Convergence (ICTC)*. [S.l.], 2013. p. 1095–1096. Citado na página 19.

EL-BENDARY, Nashwa; FOUAD, Mohamed; RAMADAN, Rabie; BANERJEE, Soumya; HASSANIEN, Aboul Ella. Smart environmental monitoring using wireless sensor networks. In: _____. [S.l.: s.n.], 2013. ISBN 9781466518100. Citado na página 26.

EVANS, Dave. *The Internet of Things - How the Next Evolution of the Internet Is Changing Everything*. 2011. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Citado 3 vezes nas páginas 17, 25 e 28.

FADEEL, Khaled Qorany Abdel; SAYED, Khaled El. Esmrf: Enhanced stateless multicast rpl forwarding for ipv6-based low-power and lossy networks. In: *Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems*. New York, NY, USA: Association for Computing Machinery, 2015. (IoT-Sys '15), p. 1924. ISBN 9781450335027. Disponível em: <https://doi.org/10.1145/2753476.2753479>. Citado na página 37.

FAPA, Fundação Agrária de Pesquisa Agropecuária. Aplicação inteligente voltada para a agricultura. 2016. Citado 2 vezes nas páginas 9 e 28.

FORCE, Internet Engineering Task. 2017. Disponível em: <tools.ietf.org/pdf/draft-ietf-roll-routing-metrics-19.pdf>. Citado na página 35.

GADDOUR, Olfa; KOUBAA, Anis. Rpl in a nutshell: A survey. *Computer Networks*, v. 56, n. 14, p. 3163 – 3178, 2012. ISSN 1389-1286. Citado na página 35.

GARCIA-LUNA-ACEVES, J. J. Adn: An information-centric networking architecture for the internet of things. In: *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. New York, NY, USA: ACM, 2017. (IoTDI '17), p. 27–36. ISBN 978-1-4503-4966-6. Disponível em: <http://doi.acm.org/10.1145/3054977.3054995>. Citado na página 51.

GHAFFARI, Ali. Congestion control mechanisms in wireless sensor networks: A survey. *Journal of Network and Computer Applications*, v. 52, p. 101 – 115, 2015. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804515000557>. Citado na página 79.

GHODSI, Ali; SHENKER, Scott; KOPONEN, Teemu; SINGLA, Ankit; RAGHAVAN, Barath; WILCOX, James. Information-centric networking: Seeing the forest for the trees. In: *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*. New York, NY, USA: Association for Computing Machinery, 2011. (HotNets-X). ISBN 9781450310598. Disponível em: <https://doi.org/10.1145/2070562.2070563>. Citado na página 31.

GOLDSMITH, Andrea. *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005. ISBN 0521837162. Citado na página 66.

HOLGER, Karl; WILLIG., Andreas. *Protocols and architectures for wireless sensors networks*. [S.l.]: John Wiley & Sons, 2005. Citado na página 25.

HOU, CD.; LI, D.; QIU, JF. et al. Seahttp: A resource-oriented protocol to extend rest style for web of things. *J. Comput. Sci. Technol.*, v. 29, p. 205–215, 2014. Citado na página 42.

HUI, J.; KELSEY, R. *Multicast Protocol for Low-Power and Lossy Networks (MPL)*. 2021. Disponível em: <https://tools.ietf.org/html/rfc7731>. Citado na página 38.

HULL, Bret; JAMIESON, Kyle; BALAKRISHNAN, Hari. Mitigating congestion in wireless sensor networks. In: *Proceedings of the 2Nd International Conference on Embedded Networked Sensor Systems*. New York, NY, USA: ACM, 2004. (SenSys '04), p. 134–147. ISBN 1-58113-879-2. Citado 3 vezes nas páginas 62, 70 e 78.

IEEE. Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, p. 1–320, Sept 2006. Citado na página 60.

IIC. *Industrial Internet Consortium - Fact Sheet*. 2020. Disponível em: <https://www.iiconsortium.org/docs/IIC_FACT_SHEET.pdf>. Citado na página 27.

INTANAGONWIWAT, Chalermek; GOVINDAN, Ramesh; ESTRIN, Deborah. Directed diffusion: A scalable and robust communication paradigm for sensor networks. In: *Proceedings of the 6th Annual International Conference on Mobile Computing and*

Networking. New York, NY, USA: ACM, 2000. (MobiCom '00), p. 56–67. ISBN 1-58113-197-6. Citado 2 vezes nas páginas 20 e 45.

IOVA, O.; PICCO, P.; ISTOMIN, T.; KIRALY, C. Rpl: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, v. 54, n. 12, p. 16–22, December 2016. ISSN 0163-6804. Citado 6 vezes nas páginas 18, 23, 29, 35, 36 e 37.

ISHAQ, Isam; HOEBEKE, Jeroen; ABEELE, Floris Van den; ROSSEY, Jen; MOERMAN, Ingrid; DEMEESTER, Piet. Flexible unicast-based group communication for coap-enabled devices. *Sensors*, v. 14, p. 9833–9877, 06 2014. Citado 4 vezes nas páginas 20, 40, 41 e 43.

ISHAQ, Isam; HOEBEKE, Jeroen; MOERMAN, Ingrid; DEMEESTER, Piet. Experimental evaluation of unicast and multicast coap group communication. *SENSORS*, v. 16, n. 7, p. 1137:1–1137:28, 2016. ISSN 1424-8220. Citado 3 vezes nas páginas 18, 40 e 43.

ISTOMIN, Timofei; KIRALY, Csaba; PICCO, Gian Pietro. Is rpl ready for actuation? a comparative evaluation in a smart city scenario. In: ABDELZAHER, Tarek; PEREIRA, Nuno; TOVAR, Eduardo (Ed.). *Wireless Sensor Networks*. Cham: Springer International Publishing, 2015. p. 291–299. ISBN 978-3-319-15582-1. Citado na página 18.

JABER, G.; KACIMI, R.; GAYRAUD, T. Data freshness aware content-centric networking in wsns. In: *2017 Wireless Days*. [S.l.: s.n.], 2017. p. 238–240. Citado 2 vezes nas páginas 19 e 31.

JACOBSON, Van; SMETTERS, Diana K.; THORNTON, James D.; PLASS, Michael F.; BRIGGS, Nicholas H.; BRAYNARD, Rebecca L. Networking named content. In: *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*. New York, NY, USA: ACM, 2009. (CoNEXT '09), p. 1–12. ISBN 978-1-60558-636-6. Disponível em: <http://doi.acm.org/10.1145/1658939.1658941>. Citado 6 vezes nas páginas 9, 31, 32, 33, 34 e 45.

JAFFEY, Toby. *MQTT and CoAP, IoT Protocols*. 2018. Disponível em: <http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php>. Citado 2 vezes nas páginas 9 e 44.

JAGANNATH, Jithin; POLOSKY, Nicholas; JAGANNATH, Anu; RESTUCCIA, Francesco; MELODIA, Tommaso. Machine learning for wireless communications in the internet of things: A comprehensive survey. *Ad Hoc Networks*, Elsevier BV, v. 93, p. 101913, Oct 2019. ISSN 1570-8705. Citado na página 25.

JAMHOUR, Edgard. A symbolic model to traffic engineering in wireless mesh networks. In: *Proceedings of the 44th Annual Simulation Symposium*. San Diego, CA, USA: Society for Computer Simulation International, 2011. (ANSS '11), p. 32–38. ISBN 1-930638-56-6. Citado na página 65.

JAYARAMAN, P.P.; YAVARI, A.; GEORGAKOPOULOS, D.; MORSHED, A.; ZASLAVSKY, A. Internet of things platform for smart farming: Experiences and lessons learnt. *Sensors*, v. 16, 2016. Citado na página 26.

JIN, Yichao; GORMUS, Sedat; KULKARNI, Parag; SOORIYABANDARA, Mahesh. Content centric routing in iot networks and its integration in rpl. *Comput. Commun.*,

Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 89, n. C, p. 87–104, 2016. ISSN 0140-3664. Citado na página 20.

KABALCI, Yasin. A survey on smart metering and smart grid communication. *Renewable and Sustainable Energy Reviews*, v. 57, p. 302 – 318, 2016. ISSN 1364-0321. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1364032115014975>. Citado 2 vezes nas páginas 17 e 26.

KARAGIANNIS, Vasileios; CHATZIMISIOS, Periklis; VAZQUEZ-GALLEGO, Francisco; ALONSO-ZARATE, J. A survey on application layer protocols for the internet of things. v. 3, p. 11–17, 01 2015. Citado na página 64.

KARP, Brad; KUNG, Hsiang. Gpsr: Greedy perimeter stateless routing for wireless networks. *Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM*, 10 2000. Citado na página 24.

Khan, R.; Khan, S. U.; Zaheer, R.; Khan, S. Future internet: The internet of things architecture, possible applications and key challenges. In: *2012 10th International Conference on Frontiers of Information Technology*. [S.l.: s.n.], 2012. p. 257–260. Citado 3 vezes nas páginas 9, 25 e 29.

KRISHNA, M.B. *User-Centric and Information-Centric Networking and Services: Access Networks, Storage and Cloud Perspective*. [S.l.]: CRC Press, 2019. ISBN 9781351801324. Citado na página 31.

KUROSE, J.F.; ROSS, K.W. *Redes de computadores e a Internet: uma abordagem top-down*. [S.l.]: ADDISON WESLEY BRA, 2007. ISBN 9788588639188. Citado na página 30.

KUSHALNAGAR, N.; MONTENEGRO, G.; SCHUMACHER, C. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*. 2007. Citado na página 60.

LACHOWSKI, Rosana; PELLENZ, Marcelo E.; JAMHOUR, Edgard; PENNA, Manoel C.; BRANTE, Glauber; MORITZ, Guilherme; SOUZA, Richard D. Icenet: An information centric protocol for big data wireless sensor networks. *Sensors*, v. 19, n. 4, 2019. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/19/4/930>. Citado na página 19.

LACHOWSKI, Rosana; PELLENZ, Marcelo E.; JAMHOUR, Edgard; PENNA, Manoel C.; MORITZ, Guilherme; BRANTE, Glauber; SOUZA, Richard D. Information centric protocols to overcome the limitations of group communication in the iot. In: BAROLLI, Leonard; AMATO, Flora; MOSCATO, Francesco; ENOKIDO, Tomoya; TAKIZAWA, Makoto (Ed.). *Advanced Information Networking and Applications*. Cham: Springer International Publishing, 2020. p. 1227–1238. ISBN 978-3-030-44041-1. Citado na página 19.

LACHOWSKI, Rosana; PELLENZ, Marcelo E.; PENNA, Manoel C.; JAMHOUR, Edgard; SOUZA, Richard D. An efficient distributed algorithm for constructing spanning trees in wireless sensor networks. *Sensors*, v. 15, n. 1, p. 1518–1536, 2015. ISSN 1424-8220. Disponível em: <http://www.mdpi.com/1424-8220/15/1/1518>. Citado na página 24.

LEVIS, Philip; BREWER, Eric; CULLER, David; GAY, David; MADDEN, Samuel; PATEL, Neil; POLASTRE, Joe; SHENKER, Scott; SZEWCZYK, Robert; WOO, Alec. The emergence of a networking primitive in wireless sensor networks. *Commun. ACM*, ACM, New York, NY, USA, v. 51, n. 7, p. 99–106, 2008. ISSN 0001-0782. Citado 3 vezes nas páginas 11, 53 e 55.

LEVIS, P.; CLAUSEN, T.; HUI, J.; GNAWALI, O.; KO, J. *The Trickle Algorithm*. 2017. Disponível em: <https://tools.ietf.org/html/rfc6206>. Citado 3 vezes nas páginas 35, 38 e 52.

LI, Changle; ZHANG, Hanxiao; HAO, Binbin; LI, Jiandong. A survey on routing protocols for large-scale wireless sensor networks. *Sensors*, v. 11, n. 4, p. 3498–3526, 2011. ISSN 1424-8220. Citado na página 49.

LOCKE, Dave. *MQ Telemetry Transport (MQTT) V3.1 Protocol Specification*. 2010. Disponível em: <https://www.ibm.com/developerworks/webservices/library/ws-mqtt/>. Citado 3 vezes nas páginas 18, 41 e 43.

LU, Yang. Industry 4.0: A survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, v. 6, p. 1 – 10, 2017. ISSN 2452-414X. Disponível em: <http://www.sciencedirect.com/science/article/pii/S2452414X17300043>. Citado na página 27.

LV, Z.; HU, B.; LV, H. Infrastructure monitoring and operation for smart cities based on iot system. *IEEE Transactions on Industrial Informatics*, v. 16, n. 3, p. 1957–1962, 2020. Citado na página 17.

Ma, G.; Chen, Z.; Liu, H.; Cao, B. Large-scale emulation for content centric network. In: *2013 Fourth International Conference on Networking and Distributed Computing*. [S.l.: s.n.], 2013. p. 100–104. Citado 2 vezes nas páginas 9 e 33.

MARTIN, Glen. *How the internet of things is more like the industrial revolution than the digital revolution*. 2014. Disponível em: <https://www.forbes.com/sites/oreillymedia/2014/02/10/more-1876-than-1995/#9352ecc66d26>. Citado na página 17.

MAZZETTO, Fabrizio; GALLO, Raimondo; SACCO, Pasqualina. Reflections and methodological proposals to treat the concept of information precision in smart agriculture practices. *Sensors*, v. 20, n. 10, 2020. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/20/10/2847>. Citado 2 vezes nas páginas 17 e 26.

MIORANDI, Daniele; SICARI, Sabrina; PELLEGRINI], Francesco [De; CHLAMTAC, Imrich. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, v. 10, n. 7, p. 1497 – 1516, 2012. ISSN 1570-8705. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1570870512000674>. Citado na página 17.

MISIC, J.; ALI, M. Z.; MISIC, V. B. Architecture for iot domain with coap observe feature. *IEEE Internet of Things Journal*, v. 5, n. 2, p. 1196–1205, April 2018. Citado 2 vezes nas páginas 18 e 42.

OIKONOMOU, George; PHILLIPS, Iain; TRYFONAS, Theo. Ipv6 multicast forwarding in rpl-based wireless sensor networks. *Wirel. Pers. Commun.*, Kluwer Academic Publishers,

Hingham, MA, USA, v. 73, n. 3, p. 1089–1116, dez. 2013. ISSN 0929-6212. Citado 3 vezes nas páginas 18, 37 e 64.

OJHA, Tamoghna; MISRA, Sudip; RAGHUWANSHI, Narendra Singh. Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture*, v. 118, p. 66 – 84, 2015. ISSN 0168-1699. Citado na página 27.

PATIL, Mallikarjunagouda B. Distance and remote healing a new development: Telemedicine and covid-19 -review. *International Journal of Advanced Science and Engineering*, v. 6, n. 4, p. 1500–1504, 2020. Citado na página 27.

Qiao, X.; Wang, H.; Tan, W.; Vasilakos, A. V.; Chen, J.; Blake, M. B. A survey of applications research on content-centric networking. *China Communications*, v. 16, n. 9, p. 122–140, 2019. Citado na página 31.

RAHMAN, A.; DIJK, E. *Group Communication for the Constrained Application Protocol (CoAP)*. 2014. Disponível em: <https://tools.ietf.org/html/rfc7390>. Citado 2 vezes nas páginas 18 e 42.

RANI, S.; AHMED, S. H.; TALWAR, R.; MALHOTRA, J. Can sensors collect big data? an energy-efficient big data gathering algorithm for a wsn. *IEEE Transactions on Industrial Informatics*, v. 13, n. 4, p. 1961–1968, Aug 2017. ISSN 1551-3203. Citado 2 vezes nas páginas 18 e 25.

RANI, Shalli; TALWAR, Rajneesh; MALHOTRA, Jyoteesh; AHMED, Syed Hassan; SARKAR, Mahasweta; SONG, Houbing. A novel scheme for an energy efficient internet of things based on wireless sensor networks. *Sensors*, v. 15, n. 11, p. 28603–28626, 2015. ISSN 1424-8220. Citado na página 49.

Raza, S.; Seitz, L.; Sitenkov, D.; Selander, G. S3k: Scalable security with symmetric keys: Dtls key establishment for the internet of things. *IEEE Transactions on Automation Science and Engineering*, v. 13, n. 3, p. 1270–1280, July 2016. ISSN 1545-5955. Citado 4 vezes nas páginas 24, 41, 64 e 67.

REN, Z.; HAIL, M. A.; HELLBRCK, H. Ccn-wsn - a lightweight, flexible content-centric networking protocol for wireless sensor networks. In: *2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*. [S.l.: s.n.], 2013. p. 123–128. Citado 3 vezes nas páginas 20, 31 e 46.

RESEARCH, Inc. Wolfram. *Mathematica*. [S.l.]: Wolfram Research, Inc., 2012. Citado na página 65.

ROBLEK, Vasja; MESKO, Maja; KRAPEZ, Alojz. A complex view of industry 4.0. *SAGE Open*, v. 6, n. 2, p. 2158244016653987, 2016. Disponível em: <https://doi.org/10.1177/2158244016653987>. Citado na página 27.

SANTOS, W. S.; JúNIOR, J. H. Souza; SOARES, J. C.; RAASCH, M. Reflexões acerca do uso da telemedicina no brasil: Oportunidade ou ameaça? *Rev. gest. sist. saúde*, v. 9, p. 433–453, 2020. Citado na página 27.

SCHUTZE, A.; HELWIG, N.; SCHNEIDER, T. Sensors 4.0 – smart sensors and measurement technology enable industry 4.0. *Journal of Sensors and Sensor Systems*, v. 7, n. 1, p. 359–371, 2018. Disponível em: <https://jsss.copernicus.org/articles/7/359/2018/>. Citado na página 27.

Shahid, N.; Aneja, S. Internet of things: Vision, application areas and research challenges. In: *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. [S.l.: s.n.], 2017. p. 583–587. Citado na página 18.

SHARMA, P.; ESTRIN, D.; FLOYD, S.; JACOBSON, V. Scalable timers for soft state protocols. In: *INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE*. [S.l.: s.n.], 1997. v. 1, p. 222–229 vol.1. ISSN 0743-166X. Citado na página 49.

SHELBY, Z.; HARTKE, K.; BORMANN, C. *The Constrained Application Protocol (CoAP)*. 2018. Disponível em: <https://tools.ietf.org/html/rfc7252>. Citado na página 42.

SINGH, G.; ABU-ELKHEIR, M.; AL-TURJMAN, F.; TAHA, A. E. M. Towards prolonged lifetime for large-scale information-centric sensor networks. In: *2014 27th Biennial Symposium on Communications (QBSC)*. [S.l.: s.n.], 2014. p. 87–91. Citado na página 19.

SINGH, G. T.; AL-TURJMAN, F. M. Cognitive routing for information-centric sensor networks in smart cities. In: *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*. [S.l.: s.n.], 2014. p. 1124–1129. ISSN 2376-6492. Citado 2 vezes nas páginas 18 e 19.

Singh, S.; Singh, N. Internet of things (iot): Security challenges, business opportunities reference architecture for e-commerce. In: *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. [S.l.: s.n.], 2015. p. 1577–1581. Citado na página 30.

Song, X.; Li, Y. Data gathering in wireless sensor networks via regular low density parity check matrix. *IEEE/CAA Journal of Automatica Sinica*, v. 5, n. 1, p. 83–91, 2018. Citado 2 vezes nas páginas 24 e 67.

STANFORD-CLARK, Andy; TRUONG, Hong Linh. *MQTT For Sensor Networks (MQTT-SN) Protocol Specification*. 2013. Disponível em: <http://www.mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf>. Citado na página 41.

Subramanian, S. S.; Pasquale, J.; Polyzos, G. C. Coap for content-centric networks. In: *2017 14th IEEE Annual Consumer Communications Networking Conference (CCNC)*. [S.l.: s.n.], 2017. p. 467–472. ISSN 2331-9860. Citado na página 41.

TAKAISHI, D.; NISHIYAMA, H.; KATO, N.; MIURA, R. Toward energy efficient big data gathering in densely distributed sensor networks. *IEEE Transactions on Emerging Topics in Computing*, v. 2, n. 3, p. 388–397, Sept 2014. ISSN 2168-6750. Citado 2 vezes nas páginas 18 e 25.

TAVCAR, J.; HORVATH, I. A review of the principles of designing smart cyber-physical systems for run-time adaptation: Learned lessons and open issues. *IEEE Transactions on*

Systems, Man, and Cybernetics: Systems, p. 1–14, 2018. ISSN 2168-2216. Citado na página 17.

THANGAVEL, D.; MA, X.; VALERA, A.; TAN, H. X.; TAN, C. K. Y. Performance evaluation of mqtt and coap via a common middleware. In: *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. [S.l.: s.n.], 2014. p. 1–6. Citado na página 41.

Tripathy, A. K.; Tripathy, P. K.; Ray, N. K.; Mohanty, S. P. itour: The future of smart tourism: An iot framework for the independent mobility of tourists in smart cities. *IEEE Consumer Electronics Magazine*, v. 7, n. 3, p. 32–37, 2018. Citado 2 vezes nas páginas 26 e 27.

VASSEUR, JP. *Terms Used in Routing for Low-Power and Lossy Networks*. 2014. Disponível em: <https://tools.ietf.org/html/rfc7102>. Citado na página 23.

VERMA, Neetu; SINGH, Dinesh. Data redundancy implications in wireless sensor networks. *Procedia Computer Science*, v. 132, p. 1210–1217, 01 2018. Citado na página 49.

VIRGILIO, Matteo; MARCHETTO, Guido; SISTO, Riccardo. Pit overload analysis in content centric networks. In: *Proceedings of the 3rd ACM SIGCOMM Workshop on Information-centric Networking*. New York, NY, USA: ACM, 2013. (ICN '13), p. 67–72. ISBN 978-1-4503-2179-2. Citado 2 vezes nas páginas 19 e 30.

WALTARI, O.; KANGASHARJU, J. Content-centric networking in the internet of things. In: *2016 13th IEEE Annual Consumer Communications Networking Conference*. [S.l.: s.n.], 2016. p. 73–78. Citado na página 31.

WAN, Chieh-yih; EISENMAN, Shane; CAMPBELL, Andrew. Coda: Congestion detection and avoidance in sensor networks. In: . [S.l.: s.n.], 2003. p. 266–279. Citado na página 78.

WAN, S.; ZHANG, Y.; CHEN, J. On the construction of data aggregation tree with maximizing lifetime in large-scale wireless sensor networks. *IEEE Sensors Journal*, v. 16, n. 20, p. 7433–7440, Oct 2016. ISSN 1530-437X. Citado 3 vezes nas páginas 49, 51 e 77.

WANG, Xing; LIU, Xuejun; WANG, Meizhen; NIE, Yunfeng; BIAN, Yuxia. Energy-efficient spatial query-centric geographic routing protocol in wireless sensor networks. *Sensors*, v. 19, n. 10, 2019. ISSN 1424-8220. Disponível em: <https://www.mdpi.com/1424-8220/19/10/2363>. Citado na página 30.

WEN, L.; GAO, L.; LI, X. A new deep transfer learning based on sparse auto-encoder for fault diagnosis. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, v. 49, n. 1, p. 136–144, 2019. Citado na página 17.

WINTER, Ed T.; THUBERT, Ed P.; BRANDT, A.; HUI, J.; KELSEY, R.; LEVIS, P.; PISTER, K.; STRUIK, R.; VASSEUR, JP.; ALEXANDER, R. *RPL: IPv6 Routing Protocol for Low power and Lossy Networks*. 2017. Disponível em: <https://tools.ietf.org/html/rfc6550>. Citado 4 vezes nas páginas 21, 23, 35 e 64.

XIAO, Yingyuan; JIAO, Xu; WANG, Hongya; HSU, Ching-Hsien; LIU, Li; ZHENG, Wenguang. Efficient continuous skyline query processing in wireless sensor networks. *Sensors*, v. 19, p. 2902, 06 2019. Citado 3 vezes nas páginas 18, 23 e 29.

XU, G.; NGAI, E. C. H.; LIU, J. Information-centric collaborative data collection for mobile devices in wireless sensor networks. In: *2014 IEEE International Conference on Communications (ICC)*. [S.l.: s.n.], 2014. p. 36–41. ISSN 1550-3607. Citado na página 19.

YAO, Yong; GEHRKE, Johannes. The cougar approach to in-network query processing in sensor networks. *SIGMOD Rec.*, ACM, New York, NY, USA, v. 31, n. 3, p. 9–18, 2002. ISSN 0163-5808. Disponível em: <http://doi.acm.org/10.1145/601858.601861>. Citado na página 51.

ZHONG, Xiaoyang; LIANG, Yao. Scalable downward routing for wireless sensor networks and internet of things actuation. *CoRR*, abs/1802.03898, 2018. Citado 3 vezes nas páginas 18, 30 e 36.

ZHOU, Z.; WANG, B.; DONG, M.; OTA, K. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, v. 50, n. 1, p. 43–57, 2020. Citado na página 17.