UNIVERSIDADE DO VALE DO RIO DOS SINOS — UNISINOS
UNIDADE ACADÊMICA GRADUAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

MATEUS RAUBACK AUBIN

UM SISTEMA DE GESTÃO DE DISPOSITIVOS INTELIGENTES BASEADO EM PROTOCOLOS DE GERÊNCIA DE REDES VOLTADO PARA A INTERNET DAS COISAS

São Leopoldo
2013

Mateus Rauback Aubin

UM SISTEMA DE GESTÃO DE DISPOSITIVOS INTELIGENTES BASEADO EM PROTOCOLOS DE GERÊNCIA DE REDES VOLTADO PARA A INTERNET DAS COISAS

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação pela Universidade do Vale do Rio dos Sinos — Unisinos

Orientador:
Prof. Dr. Rafael Bohrer Ávila

São Leopoldo
2013

LISTA DE SIGLAS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
ARPANET	Advanced Research Projects Agency Network
CDMA	Code division multiple access
CMIP	Common Management Information Protocol
FCAPS	Fault Configuration Accounting Performance Security
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSO	IP for Smart Objects Alliance
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
M2M	Machine-To-Machine
MIB	Management Information Base
NFC	Near Field Communication
OSI	Open Systems Interconnection
PC	Personal Computer
PDU	Protocol Data Unit
RFC	Request For Comments
SLA	Service Level Agreement
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TI	Tecnologia da Informação
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network

SUMÁRIO

1 INTRODUÇÃO

"In the nineteenth century, machines learned to do;
in the twentieth century, they learned to think;
and in the twenty-first century, they are learning
to perceive — they actually sense and respond"
Sundmaeker et al. (2010)

Desde a Revolução Industrial há uma crescente busca pela automação das tarefas humanas. Através de máquinas cada vez mais sofisticadas foi possível obter significativo avanço nas tecnologias e nos métodos de produção ao passo que diversas tarefas deixaram de ser realizadas manualmente. Seguindo esta filosofia, máquinas computacionais foram projetadas e as bases da ciência da computação estabelecidas. Conceitos como a Álgebra Booleana de Boole (2003), publicado originalmente em 1854, servem até hoje como fundamentos deste campo de estudos.

Durante a segunda guerra mundial houve um expressivo progresso na computação graças ao incentivo das organizações de defesa para melhorar métodos de cálculo e criptografia. Neste período publicações como as de Shannon (2001), Turing (1937) e Von Neumann (1945) definiram a ciência da computação como é conhecida hoje.

Ainda com objetivos de defesa, pesquisas no campo de redes de computadores começaram a ser desenvolvidas nos anos que seguiram. A IBM, nos anos 50, desenvolveu para os EUA o SAGE[1], um dos primeiros exemplos de computadores conectados em rede, caracterizado pela "transmissão de dados digitais em linhas telefônicas de voz a 1300 bits por segundo" (ASTRAHAN; JACOBS, 1983, p. 348).

Contudo, o SAGE comunicava-se através do conceito de circuitos, que, mais tarde, mostrou-se inferior à troca de pacotes (*packet switching*). Explorada pela agência de defesa americana nos anos 70, a comunicação via troca de pacotes originou a ARPANET, uma rede nacional descentralizada utilizada para interligar universidades e centros de pesquisas (BARAN, 1964), assim como os protocolos TCP/IP, a base da atual internet.

A contínua ampliação da capacidade de processamento dos dispositivos computacionais, aliada a redução de custos, possibilitou uma nova revolução tecnológica (ATZORI; IERA; MORABITO, 2010), abrindo caminho para a Era da Informação. Munidos de circuitos integrados e *microchips*, os computadores estão cada vez mais presentes nas atividades humanas, avançando em direção à ubiquidade (KAKU, 2007).

No atual cenário tecnológico já é possível, de maneira economicamente viável, colocar em prática algumas das ideias vislumbradas por Weiser (1991). Apesar de representar um desafio para diversas áreas do conhecimento, as barreiras para a efetiva integração entre dispositivos computacionais e a vida cotidiana têm diminuído, possibilitando a criação de novos produtos e

[1] Semi-Automatic Ground Environment, um sistema nacional de defesa do espaço aéreo e um dos mais importantes projetos da IBM. Disponível em: <www.ibm.com/ibm/history/ibm100/us/en/icons/sage/>. Acesso em: set. 2013.

serviços, resultando em soluções para os mais diversos problemas.

Ainda que não seja uma proposta nova, Turck (2013) pontua que a implementação de uma rede composta de dispositivos embarcados em objetos do dia-a-dia, ou seja, a Internet das Coisas (do inglês Internet of Things, IoT), não era viável devido a fatores como complexidade e custo. Entretanto, tomando por referência a lei de Moore (1998), a qual dita que o número de transístores em um circuito integrado dobra aproximadamente a cada dois anos, é improvável que se reverta a tendência de dispositivos cada vez menores e mais baratos.

Diversas são as semelhanças entre a Internet das Coisas e as Redes de Sensores sem Fio, porém, enquanto as redes de sensores são implantadas principalmente com o intuito de monitorar variáveis em um ambiente (SAKTHIDHARAN; CHITRA, 2012), a Internet das Coisas expande este conceito ao próximo nível. A capacidade de tornar cada dispositivo individualmente endereçável na internet favorece o compartilhamento de informações entre sistemas, resultando em uma modalidade de comunicação chamada por ETSI (2010) de comunicação Máquina-a-Máquina (M2M).

Motivados pelas oportunidades e pelo alto impacto social da computação pervasiva[2], impulsionada com a ajuda da IoT, pesquisadores tanto da academia quanto da indústria se mobilizaram em torno deste conceito (ATZORI; IERA; MORABITO, 2010). Entidades governamentais reconheceram também a IoT como um paradigma promissor, fomentando iniciativas de pesquisa e desenvolvimento em países como China, Japão, Estados Unidos e da União Europeia (SUNDMAEKER et al., 2010).

Entretanto, com grandes poderes vêm grandes responsabilidades[3]. Para realizar sua visão, a Internet das Coisas deve superar uma série de desafios, entre eles: privacidade, padronização tecnológica e escalabilidade (COETZEE; EKSTEEN, 2011). Percebe-se, portanto, que a cooperação entre academia, indústria e governo é fundamental para que a IoT possa demonstrar seu verdadeiro potencial.

Este trabalho está organizado da seguinte forma: no Capítulo 2 serão abordadas questões relativas à gerência de redes e seu principal protocolo, o SNMP; no Capítulo 3 é apresentado e detalhado o conceito de Internet das Coisas, detalhando desde sua origem e definição, até os desafios e as oportunidades proporcionadas por este paradigma; o Capítulo 4 apresenta a proposta deste trabalho para unir os conceitos anteriormente apresentados, combinando as estratégias da gerência de redes com a Internet das Coisas; o Capítulo 5 versa sobre o planejamento do desenvolvimento deste trabalho, ou seja, como ele prosseguirá de forma a atingir seus objetivos.

[2] A computação ubíqua e/ou pervasiva é uma área de estudo que tem como objetivo tornar a interação homem computador invisível, ou seja, integrar a informática com as ações e comportamentos naturais das pessoas. Disponível em: <https://en.wikipedia.org/wiki/Pervasive_computing>. Acesso em: nov. 2013.

[3] Lição dada a Peter Parker por seu tio Ben na história em quadrinhos Homem-Aranha, escrita por Stan Lee.

1.1 Justificativa e Definição do Problema

Em um mundo cada vez mais conectado e dependente da internet, a quantidade de dispositivos capazes de integrar esta rede já representa uma fatia considerável entre os aparelhos usados diariamente (ACCENTURE, 2012). Computadores, *laptops*, *tablets*, *smartphones* e televisores integram uma crescente classe de produtos comercialmente chamados de Dispositivos Inteligentes (*Smart Devices*) e que permitem, dentre outras funções, acesso a redes e, consequentemente, à internet.

Paralelamente a esta tendência e seguindo as previsões de Gilder (2007) e Moore (1998), por exemplo, a capacidade de equipamentos e redes continua a aumentar, resultando na visão de um atraente e economicamente viável mundo conectado (DING, 2009). Tais mudanças influenciam direta e indiretamente a sociedade, seus costumes, e, conforme afirma Carr (2010), até mesmo o pensamento humano.

Tamanha difusão de aparelhos capazes de acessar a internet deu origem a um novo paradigma que está transformando a gestão da Tecnologia da Informação (TI) (ZDNET, 2013). Este aumento apresenta-se como um desafio para as áreas de segurança da informação e gerência de redes, convidando grandes empresas como Bradley et al. (2012), Hewlett-Packard (2013) e Motorola (2011) a criar novas soluções de forma a atender demandas de mercado.

Apesar de constituir um desafio de gestão, não há indícios da redução no número de dispositivos nas redes. A Internet das Coisas trará consigo uma vasta gama de novos aparelhos que carecem de diretivas de gestão (ATZORI; IERA; MORABITO, 2010) e, ainda que novas soluções estejam em desenvolvimento, não há um acordo sobre mecanismos específicos de gerência, resultando em soluções proprietárias e que não colaboram entre si.

Visando manter a interoperabilidade entre dispositivos, há, nas pesquisas de IoT, um consenso referente ao uso do Protocolo de Internet (IP), mais especificamente o IPv6, como o protocolo padrão de comunicação (DUNKELS; VASSEUR, 2008; MATTERN; FLOERKEMEIER, 2010; FENG; HUANG; SU, 2011; PAVENTHAN et al., 2012). Compartilhando desta motivação, autores como Sundmaeker et al. (2010), Mattern e Floerkemeier (2010) e Wang, Jäntti e Ali (2012) afirmam que os protocolos de gerenciamento de redes devem, também, manter a compatibilidade com os padrões já existentes, sendo, se necessário, estendidos para dar suporte aos desafios da IoT.

Para tanto, é de grande interesse da indústria e da academia que um protocolo de gerência de redes possa desempenhar seu papel em conjunto com a infraestrutura já existente sem deixar de atender às restrições e características da IoT. É nesta tarefa que concentram-se os esforços deste trabalho, buscando melhorias específicas para este novo cenário e, ao mesmo tempo, mantendo a interoperabilidade com padrões já estabelecidos.

1.2 Objetivos

Corroborando a visão apresentada, o presente trabalho se propõe a estudar e criar mecanismos que possibilitem o emprego de protocolos e modelos da gerência de redes tradicional aplicados ao contexto de Internet das Coisas.

Nos alicerces da IoT encontram-se computadores associados a objetos do cotidiano denominados dispositivos embarcados e que são caracterizados, na definição de Bormann, Ersue e Keranen (2013), pela escassez de recursos computacionais e atuação praticamente autônoma, requerindo pouca ou nenhuma configuração. Observa-se ainda que tais dispositivos não contam com interfaces de usuário, fazendo com que toda sua gestão deva ser realizada remotamente ou de forma automatizada.

Enquanto, idealmente, um dispositivo deveria ser auto-gerenciável, é improvável que tais métodos sejam apropriados ou até mesmo possíveis em todas as situações. Desta forma, eventualmente será necessária a intervenção manual sobre um ou mais destes dispositivos.

Devido a ausência de padrões de gerenciamento para IoT e a constante competição entre grandes empresas, existe a possibilidade de que cada fabricante proponha diferentes maneiras de realizar esta gestão, criando implementações incompatíveis e de padrão fechado. Esta filosofia vai diretamente de encontro à mentalidade da internet, que é composta por padrões livres e abertos, para que todos, tanto indivíduos quanto organizações, possam acessá-los.

Porém, a gestão da Internet das Coisas apresenta características únicas não contempladas pelos padrões já estabelecidos, entre elas estão a grande quantidade de dispositivos presentes na rede e a reduzida capacidade de processamento. Surge, então, a necessidade de estudar e ajustar os protocolos para este contexto, de forma que melhor atendam às necessidades da IoT.

Uma vez encontradas as fraquezas da gerência de redes tradicional no contexto de IoT, este trabalho apresenta sugestões de melhorias ao processo de gestão. Tais funcionalidades devem, idealmente, manter a compatibilidade com o protocolo, funcionando como extensões. O resultado final deve conter o detalhamento das melhorias propostas e uma implementação realizada a título de prova de conceito.

1.2.1 Objetivo Geral

Propor uma solução que permita o uso de modelos da gerência de redes tradicional (protocolos e sistemas) para gerir dispositivos em um contexto de Internet das Coisas.

1.2.2 Objetivos Específicos

- Projetar uma arquitetura de gerência para Internet das Coisas compatível com ferramentas e protocolos da gerência de redes tradicional;
- Desenvolver um protótipo da solução projetada como prova de conceito;

- Avaliar a solução em termos de suas forças, fraquezas e futuras oportunidades.

1.3 Método de Pesquisa

Para atingir seus objetivos, a presente pesquisa é caracterizada por uma abordagem quantitativa "que tem suas raízes no pensamento positivista lógico, tende a enfatizar o raciocínio dedutivo, as regras da lógica e os atributos mensuráveis" (GERHARDT; SILVEIRA, 2009, p. 33), e busca "traduzir em números opiniões e informações para classificá-las e analisá-las" (SILVA; MENEZES, 2005, p. 20). Ao estabelecer como contexto as áreas de Gerência de Redes e Internet das Coisas, atribui-se a natureza de pesquisa aplicada, onde os resultados serão adequados para a "aplicação prática e dirigidos à solução de problemas específicos" (SILVA; MENEZES, 2005, p. 20).

Quanto aos seus procedimentos técnicos, esta será uma pesquisa experimental. Neste aspecto, Silva e Menezes (2005) e Gerhardt e Silveira (2009) apoiam-se em Gil (2007), que a define como o processo de determinar um objeto de estudo, selecionar variáveis capazes de influenciá-lo e definir formas de controle e observação destas variáveis. Um maior detalhamento ainda é possível na visão de Fonseca (2002), onde deve-se dividir a pesquisa experimental em duas categorias, a de campo e a de laboratório, realizada neste trabalho.

Desta forma, pode-se classificar o presente trabalho como uma proposta de melhoria na abordagem de gerência de redes e, considerando que "não é necessário, porém, que o autor de algum método novo demonstre que o seu método é melhor do que outro método do estado da arte para toda e qualquer situação" (WAZLAWICK, 2008), sua abrangência é intencionalmente limitada ao domínio da Internet das Coisas.

2 GERÊNCIA DE REDES

O crescimento explosivo das redes de computadores nos anos oitenta trouxe à tona uma série de desafios para os administradores de sistemas, de um lado as facilidades e a agilidade na troca de informações e do outro a dificuldade em gerir a grande quantidade de recursos computacionais (STALLINGS, 1999). Impulsionada pelo crescimento e evolução das redes de computadores, as técnicas de gerência de redes, ainda que primitivas e sem padronização, se tornaram fundamentais para garantir o funcionamento e a qualidade dos serviços prestados.

Cada vez mais importantes para as atividades humanas, as redes de computadores (especialmente a internet) obtiveram grande êxito nas atividades comerciais, onde "têm catalizado a inovação e favorecido a emergência de novos e disruptivos modelos de negócio" (DING, 2009, p. 23). Portanto, observa-se uma crescente dependência de empresas e organizações nos serviços de conectividade, demonstrando o seu valor e provando, na prática, que "manter estes serviços funcionando torna-se sinônimo de manter o negócio funcionando" (CLEMM, 2006, p. xix).

De acordo com Clemm (2006), a gerência de redes pode ser definida como "as atividades, métodos, procedimentos, e ferramentas que dizem respeito a operação, administração, manutenção e provisionamento de sistemas de rede". Uma definição extensiva do conceito de gerência de redes é fornecida por Ding (2009, p. 64):

> a execução de um conjunto de funções requeridas para controlar, planejar, alocar, implantar, coordenar, e monitorar os recursos de uma rede de telecomunicações ou de computadores, incluindo a realização de funções como planejamento inicial da rede, atribuição de frequências, roteamento predefinido de tráfico para suportar balanceamento de carga, autorização de distribuição de chaves criptográficas, gerência de configuração, gerenciamento de falhas, gestão da segurança, gerência de performance e gestão de contabilização.

O reconhecimento da importância das técnicas de gerência de redes provocou esforços por parte de órgãos reguladores, como a Organização Internacional para Padronização (ISO). Em sua normativa 7498-4, a ISO (1989) define as cinco principais categorias da gerência de redes, conhecidas como o modelo FCAPS e que contempla o gerenciamento de:

- ***Fault* – Falhas:** Engloba todas as ações de detecção e correção de falhas que possam ocorrer na rede e em seus equipamentos. Segundo Ding (2009), é composta por três passos fundamentais: detecção, isolamento e correção. Em suma, o "gerenciamento de falhas está portanto interessado no monitoramento da rede para garantir que tudo esteja funcionando regularmente e reagir quando este não for o caso" (CLEMM, 2006, p. 132);

- ***Configuration* – Configuração:** Responsável por manter uma lista completa e atualizada de todos os ativos que compõem a rede, guardando informações como: Configurações de

Hardware, Versões de Sistemas, Serviços e Documentação (CLEMM, 2006; DING, 2009; MAURO; SCHMIDT, 2009). A manutenção de tal inventário não é uma tarefa trivial, devendo contemplar a inclusão, remoção e atualização de dados sobre cada dispositivo que compõe a rede. Portanto, uma boa gerência de configuração, "para realizar estas atividades deve monitorar todas as mudanças feitas aos recursos" (WANG; JÄNTTI; ALI, 2012, p. 2);

- ***Accounting* – Contabilização:** Contempla principalmente a coleta de estatísticas sobre usuários e/ou grupos de usuários. Apontada por Hunt (1997) como desejável para o repasse de custos do uso de recursos aos usuários, esta categoria é de especial importância para empresas pois auxilia na cobrança a clientes internos e externos (CLEMM, 2006). O valor da contabilização está em "possibilitar que o uso por indivíduos ou grupos seja regulamentado de forma adequada. Tal regulamentação minimiza problemas de rede (pois os recursos de rede podem ser repartidos com base nas suas capacidades) e maximiza a equidade de acesso à rede dentre todos os usuários" (DING, 2009, p. 93);

- ***Performance* – Desempenho:** Interessada principalmente na qualidade dos serviços de rede, a finalidade desta categoria é "garantir que os objetivos de níveis de serviço (SLA) sejam alcançados ao mesmo tempo em que os recursos de rede sejam utilizados de maneira economicamente eficiente" (WANG; JÄNTTI; ALI, 2012, p. 2). Depende quase exclusivamente de métricas que mensurem as características da rede, sendo as principais: *throughput*, *delay*, porcentagem de erros e uso de *links* (CLEMM, 2006; WANG; JÄNTTI; ALI, 2012; DING, 2009; HUNT, 1997). Pode, ainda, ser discriminada em três passos: Coleta de dados, Estabelecimento de valores de referência e Monitoramento destes valores (MAURO; SCHMIDT, 2009). Alterações nos parâmetros inicialmente definidos podem indicar recursos congestionados e/ou subutilizados, desencadeando processos de gerência de falhas e configuração (WANG; JÄNTTI; ALI, 2012);

- ***Security* – Segurança:** Abrange procedimentos para prover controle de acesso, proteção de dados, autenticação, autorização e auditoria sobre as ações ocorridas em determinada rede (WANG; JÄNTTI; ALI, 2012). Ou, nas palavas de Ding (2009, p. 94), "um conjunto de funções que protege redes e sistemas de acessos não autorizados por pessoas, atos ou influências". Ainda segundo o autor, tais funções contemplam desde a autorização de um login a um usuário, até a disseminação de chaves criptográficas e a distribuição de registros sobre eventos de segurança. Em suma, o objetivo desta categoria é duplo, sendo tanto garantir o controle de acesso quanto prevenir e detectar ataques aos recursos de rede (MAURO; SCHMIDT, 2009).

Redes são naturalmente compostas por um conjunto de dispositivos interconectados. A gerência de redes ocorre, portanto, nestes dispositivos, tendo como requisito para seu sucesso a existência de uma infraestrutura de suporte aos processos envolvidos. Não há uma fórmula

de sucesso para a implantação de processos de gerência de redes, contudo, há uma série de requisitos necessários. Ding (2009) os define como:

- **Dispositivo:** Todo e qualquer equipamento conectado à rede e que deseja-se que faça parte da gerência. Deve conter um software denominado Agente;
- **Agente:** Um programa que reside no dispositivo gerenciado e que facilita a execução das tarefas solicitadas pelo gerente. Deve coletar e manter dados de gerência referentes ao dispositivo onde encontra-se e reportá-los ao gerente na forma de respostas a solicitações ou alertas. Cada equipamento da rede pode abrigar um ou mais agentes;
- **Gerente:** Responsável por emitir requisições e receber notificações dos agentes. Pode ser pensado como um software que realiza as ações solicitadas pelo usuário, servindo como centralizador. Deve, também, ter uma visão geral da rede e facilitar a obtenção de informações de alto nível para embasar a tomada de decisão. Geralmente existem poucos gerentes na rede;
- **Protocolo de Gerência:** Responsável por mediar a comunicação entre os dispositivos da rede e seus agentes e gerentes;
- **Estação de Gerência de Redes:** Dispositivo onde o usuário terá acesso ao gerente, executando as aplicações de gerência para monitoramento e controle dos elementos da rede. É constituído, geralmente, por uma máquina com abundância de recursos;
- **Objeto Gerenciado:** Representa algum recurso presente em um dispositivo que é de interesse do usuário. Pode ser exemplificado como a lista de conexões TCP de determinado dispositivo da rede. Este objeto será de interesse do agente e do gerente e estará presente em uma MIB representado através da SMI;
- **Estrutura das Informações de Gerenciamento (SMI):** Linguagem usada para descrever as regras de nomenclatura e codificação dos dados de um objeto gerenciado. É base para toda informação codificada no sistema e é usada tanto por agentes quanto por gerentes;
- **Base de Informações de Gerenciamento (MIB):** Banco de dados para os objetos gerenciados, abrigando-os em uma estrutura hierárquica (árvore) que estabelece as possíveis operações e relações entre eles. Também compartilhada entre agentes e gerentes, define as funcionalidades que um agente disponibiliza e estes podem conter mais de uma MIB.

Em suma, a disciplina de gerência de redes pode ser definida como:

> O propósito da gerência de redes é de reunir informações sobre o estado e o comportamento dos elementos da rede. Dados a serem reunidos incluem informações estáticas, relacionadas a configuração; informações dinâmicas, relacionadas aos eventos na rede; e informações estatísticas, resumida a partir de

> informações dinâmicas. Tipicamente, cada dispositivo gerenciado na rede inclui um módulo agente responsável por coletar informações locais de gerência e transmití-las a uma ou mais estações de gerência. Cada estação de gerência inclui software de aplicação de gerência de rede e software para comunicação com os agentes. Informações podem ser coletadas de maneira ativa, através de *pooling* pela estação de gerenciamento, ou passivamente, através de relatórios de eventos gerados pelos agentes (STALLINGS, 1999, p. 45).

2.1 Simple Network Management Protocol

A internet impulsionou o crescimento das redes e tornou sua gestão ainda mais complicada, uma vez que tais redes podem conter centenas de dispositivos geograficamente distribuídos e heterogêneos em suas funcionalidades e recursos (STALLINGS, 1999). Reconhecendo estas dificuldades, diversos grupos de trabalho se formaram em entidades padronizadoras buscando criar soluções, ou pelo menos mitigar, o problema nas mãos dos administradores de redes (LEINWAND; CONROY, 1996).

Neste cenário, duas vertentes dominavam as iniciativas de gerência de redes. De um lado os padrões ISO com seu modelo OSI de protocolos e, consequentemente, um modelo de gerência com base no CMIP *(Common Management Information Protocol)*. E, de outro lado, a IETF *(Internet Engineering Task Force)* com o suporte ao modelo TCP/IP e sugerindo o SNMP *(Simple Network Management Protocol)* como uma medida tapa-buraco enquanto uma solução melhor não ficasse pronta.

Com essa premissa, o SNMP seguiria como uma solução temporária, simplificada e focada, tratando apenas das áreas de gerência de falhas e configuração, enquanto no longo prazo o CMIP assumiria seu lugar como uma solução completa (LEINWAND; CONROY, 1996; STALLINGS, 1999). Entretanto, tal desejo nunca se concretizou e o desenvolvimento dos padrões ISO passou por grandes dificuldades e incompatibilidades com o TCP/IP. Este desfecho é atribuído por Hunt (1997, p. 77) ao fato de que "o programa de desenvolvimento OSI foi muito lento e a implementação de produtos ainda mais lenta, com o resultado inevitável de que o SNMP aproveitou a janela de oportunidade e foi implementado rapidamente por uma série de fornecedores".

Ainda sobre porquê o SNMP se tornou o protocolo padrão para gerência de redes, Stallings (1999) corrobora com a visão de Hunt (1997):

> O Protocolo Simples de Gerência de Rede foi projetado para ser uma ferramenta básica e facilmente implementável de gerência de redes que poderia ser utilizado para atender num curto prazo as necessidades de gerência. Devido ao progresso lento na gerência de sistemas OSI, o SNMP preencheu a lacuna e acabou se tornando o método dominante padronizado de gerência de rede em uso atualmente (STALLINGS, 1999, p. 83).

Apesar de ser projetado como uma solução rápida e fácil para os principais problemas enfrentados na época, o sucesso do SNMP deve-se também, em parte, à sua estrutura de dados projetada para acomodar o crescimento e proporcionar flexibilidade para a inclusão de novos objetos (STALLINGS, 1999). Graças a esta flexibilidade, o protocolo pôde ser adaptado para atender as necessidades de diversos casos de uso, sendo utilizado em produtos que vão desde servidores a roteadores e *no-breaks*. Neste contexto, a gestão baseada em SNMP

> é inerentemente genérica de forma que ela pode ser usada para gerir diversos tipos de sistemas. Esta abordagem pode ser usada com redes computacionais de dados, redes de tráfego automotivo, redes de controle de calefação e arrefecimento, redes de irrigação, ou fábricas de produtos químicos. Portanto, vê-se que quase qualquer sistema de tempo real consistindo de uma coleção de elementos independentes se comunicando pode usar SNMP (PERKINS; MCGINNIS, 1996, p. 2).

Como nenhuma solução é perfeita para todos os casos, o SNMP também sofreu grandes críticas. A comunidade de profissionais que efetivamente fazem a gerência de redes expressa opiniões negativas sobre o protocolo e sua implementação, questionando a existência do termo "simples" em seu nome. Até mesmo na literatura não é incomum encontrar questionamentos a respeito das decisões de projeto do protocolo e sobre a complexidade de operar um sistema de gerenciamento baseado em SNMP. Nas palavras de Stallings (1999, p. 111), "os resultados são desanimadores para o cliente/usuário que acredita no *simples* em SNMP".

Entretanto, Clemm (2006) argumenta que a simplicidade do SNMP foi pensada em termos das operações que o protocolo suporta, conforme ilustra a Tabela 1, o que facilita a implementação de agentes mas move a complexidade para as aplicações de gerência.

> Como tantas vezes é o caso na engenharia, é tudo sobre *tradeoffs*. Os projetistas originais do SNMP decidiram que era mais importante manter a implementação de agentes simples e, como consequência, empurrar um pouco mais de complexidade para a lógica da aplicação de gerenciamento. Primeiro, haveria um menor número de aplicações de gerência (talvez uma dúzia) do que implementações de agentes (talvez centenas, senão milhares). Além disso, aplicações de gerência não estariam sujeitas às mesmas restrições de recursos computacionais de um dispositivo de rede. Portanto, esta complexidade se acomodaria mais facilmente nos gerentes do que nos agentes (CLEMM, 2006, p. 250).

Esta transferência na complexidade é, ainda segundo Clemm (2006), uma das responsáveis pela rápida disponibilidade de agentes SNMP, facilitando a aceitação do protocolo nos anos que seguiram sua padronização. A decisão de manter o agente como a parte simplificada do modelo SNMP é também muito útil no contexto de Internet das Coisas, uma vez que estes dispositivos compartilham das mesmas (se não piores) restrições de poder computacional que os dispositivos

de rede que são objeto da gerência.

Ainda que existam outras tecnologias para gerência de redes, o SNMP segue como a principal delas no contexto pessoal e empresarial. As informações apresentadas até aqui apenas confirmam esta hipótese e tornam o SNMP o protocolo de escolha para esta pesquisa. Deste ponto em diante apresenta-se um detalhamento sobre o protocolo de forma a apresentar ao leitor suas principais características, além de uma visão mais detalhada das suas funcionalidades.

2.1.1 Versões

Devido ao seu surgimento como uma solução interina para o problema da gerência de redes, o SNMP passou por diversas versões e revisões. Ao ser padronizado através do uso de RFCs *(Request For Comments)* da IETF, seu desenvolvimento passou por diversas iterações em comitês específicos para este fim. Hoje, existem em uso três principais versões do protocolo, abordadas a seguir:

- **SNMPv1:** Versão inicial do protocolo, padronizada pela RFC 1157 e publicada em 1990. Hoje está obsoleta e é mantida apenas como um padrão histórico, porém, implementações desta versão ainda são encontradas em dispositivos (MAURO; SCHMIDT, 2009; DING, 2009). Focava principalmente na detecção de falhas e no monitoramento da rede, não dando a devida importância à segurança (CLEMM, 2006), fazendo com que as senhas para configuração de dispositivos fossem transmitidas em *plaintext*, ou seja, visíveis a qualquer equipamento na rede (HUNT, 1997; DING, 2009). Ainda que com algumas falhas, estabeleceu as bases do que viria a ser o SNMP e a gerência de redes como conhecemos hoje;

- **SNMPv2:** Com o uso já difundido do SNMP e o mapeamento de suas deficiências, iniciou-se, no final de 1992, o trabalho para a definição de um sucessor (HUNT, 1997). O crescimento das redes trouxe novas necessidades para os gerentes, agravando o fato de que o "SNMPv1 é notoriamente ineficiente na busca de grandes quantidades de informações gerenciais" (CLEMM, 2006, p. 258) e expondo ainda mais suas fragilidades de segurança. Sendo assim, esta versão introduziu dois novos tipos de operação (*get-bulk* e *inform*) além de redefinir o formato dos pacotes (de modo à uniformizá-los) e melhorar os metadados utilizados para descrever os objetos gerenciados (HUNT, 1997; STALLINGS, 1999; MAURO; SCHMIDT, 2009). Apesar do interesse por melhorias na segurança o processo de padronização encontrou dificuldades e divergências nas soluções, causando com que tais funcionalidades fossem removidas do padrão, revertendo aos moldes de segurança do SNMPv1, baseado em senhas (CLEMM, 2006; DING, 2009);

- **SNMPv3:** Após quase uma década de uso do protocolo, sua terceira versão é concluída trazendo uma solução completa de segurança, o que "finalmente torna o SNMP um protocolo seguro" (CLEMM, 2006, p. 260). Se fosse necessário sumarizar esta versão, Clemm

(2006, p. 260) afirma que ela "pode essencialmente ser pensada como SNMPv2 mais segurança". Apesar das funcionalidades de criptografia, integridade e autenticação serem destaque nesta versão, Mauro e Schmidt (2009) ponderam que não são as únicas. Outra novidade é a "introdução de novas convenções textuais, conceitos e terminologia" (MAURO; SCHMIDT, 2009, p. 73), possibilitando que as especificações sejam mais precisas e se relacionem melhor, facilitando o entendimento e a implementação do padrão. Tais novidades, apesar de mostrarem um amadurecimento do protocolo, tornaram o SNMP muito mais complexo do que inicialmente planejado e, devido ao longo tempo de desenvolvimento da versão, gerentes deixaram de usar o protocolo no contexto de configuração (recorrendo a outras ferramentas) e mantendo-o apenas para monitoramento (CLEMM, 2006). Outra dificuldade identificada é devida aos fornecedores de equipamentos que são "notoriamente lentos em adotar novas versões do protocolo" (DING, 2009, p. 76). Portanto, "resta saber se o SNMPv3 impulsionará o uso do protocolo para outros propósitos além do monitoramento" (CLEMM, 2006, p. 261).

2.1.2 Operações

Simplicidade é um dos objetivos de projeto do SNMP, portanto espera-se que suas operações sejam simples também. Desta forma, as ações realizadas sobre um determinado dispositivo devem ser expressas de maneira compacta e precisa, evitando a complexidade associada a decisão de qual operação é válida dado o estado do objeto. Apesar do conjunto limitado, Stallings (1999) elenca três operações básicas que devem estar disponíveis em qualquer protocolo de gerência de redes, e que são contempladas pelo SNMP, sendo elas: *get*, *set* e *trap*.

No SNMP as operações podem afetar mais de um objeto, isto deve-se a sua estrutura de pacotes, explicada à seguir na seção Mensagens. Desta forma uma operação *get*, por exemplo, pode buscar o valor de diversos objetos em uma única requisição. Adicionalmente define-se que as operações são atômicas, causando com que a falha em um ou mais itens invalide a requisição inteira (SIMONEAU, 1999).

A decisão de manter a complexidade no gerente e simplificar os agentes já foi elogiada por Clemm (2006) e, no que diz respeito às operações, Perkins e McGinnis (1996) corroboram ao afirmar que, embora limitadas, as operações do SNMP são muito poderosas.

> Possuir apenas algumas poucas e simples operações permitiu que as implementações dos mecanismos do protocolo fossem muito pequenas e exigissem menos recursos para seu desenvolvimento quando comparadas a outros protocolos de gerência (PERKINS; MCGINNIS, 1996, p. 185).

A seguir apresenta-se um detalhamento[1] das operações que o protocolo SNMP prevê.

[1] Adaptadas a partir de: Perkins e McGinnis (1996), Simoneau (1999), Stallings (1999), Clemm (2006) e Mauro e Schmidt (2009).

Tabela 1: Principais operações do protocolo SNMP

Operação	De – Para	Mensagem
GET	Gerente – Agente	get-request
GETNEXT	Gerente – Agente	get-next-request
GETBULK	Gerente – Agente	get-bulk-request
SET	Gerente – Agente	set-request
TRAP	Agente – Gerente	trap
INFORM	Qualquer – Gerente	inform-request

Fonte: Adaptado pelo autor de Perkins e McGinnis (1996).

- ***Get*:** Contempla a obtenção do valor de uma informação de gerência. Nesta operação o gerente solicita um dado sobre um determinado objeto a um agente;

- ***Get-Next*:** Assim como o *get*, contempla uma obtenção, porém, neste caso, o gerente está solicitando o próximo objeto, potencialmente desconhecido, a partir de outro objeto. Esta operação é útil para explorar MIBs desconhecidas ou obter valores de objetos tabulares;

- ***Get-Bulk*:** Constitui uma melhoria em relação ao *get-next* pois possibilita representar grandes requisições, principalmente de tabelas, de forma mais econômica. Atinge este objetivo através de uma indicação de repetições;

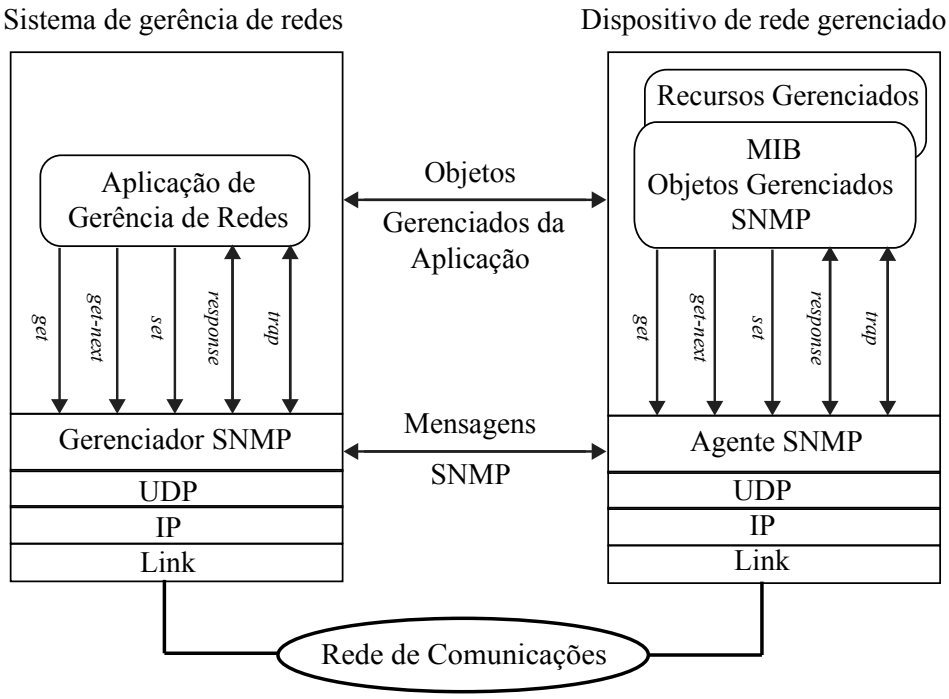
- ***Inform*:** Assim como o *trap*, é utilizada para relatar eventos. Contudo, esta operação exige uma confirmação de recebimento e pode ser usada para comunicação entre agente–gerente assim como gerente–gerente. Contudo, a necessidade de confirmação incorre um custo extra no controle de mensagens e, portanto, faz com que esta operação seja indicada apenas para comunicação entre gerentes;

- ***Report*:** Contempla a comunicação de mensagens de controle entre gerentes e agentes, sendo responsável pela comunicação de erros de processamento. Tem como objetivo informar o originador de uma requisição que um erro interno ocorreu durante o processamento no receptor e não deve ser gerada por operação do usuário;

- ***Set*:** Define o valor de uma determinada informação de um objeto gerenciado. Esta operação é indispensável para a gerência e a compatibilidade com o modelo FCAPS. Devido a sua simplicidade, o SNMP não contempla ações de criação ou remoção de objetos gerenciados, sendo realizadas, quando possível, pelo próprio *set*;

- ***Trap*:** Representa um aviso enviado de maneira autônoma do agente para o gerente. Usado para relatar condições excepcionais e gerar alertas. Esta operação, ao contrário do *inform*, não é confirmada, portanto não há como garantir que foi recebida pelo gerente. Com a chegada do SNMPv2 e as alterações no formato da mensagem, a operação passou a se chamar *notification*, porém esta nomenclatura é pouco usada.

Figura 1: Estrutura de funcionamento do SNMP



Fonte: Adaptado pelo autor de Ding (2009).

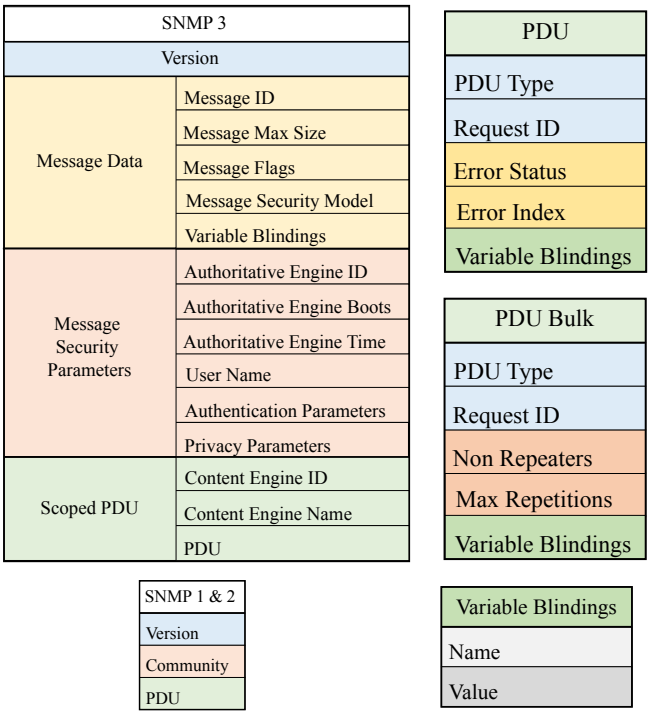
2.1.3 Mensagens

Projetado desde o princípio para ser o protocolo de gerência de redes associado aos protocolos de internet (TCP/IP), o SNMP trabalha nativamente sobre o serviço de datagramas UDP (*User Datagram Protocol*). Ao contrário do TCP, que exige o estabelecimento de uma conexão antes de comunicar-se, o UDP evita este custo enquanto não garante a entrega nem a ordenação das mensagens. Apesar dessas deficiências, os ganhos obtidos são suficientes para justificar sua escolha pois, um vez que os metadados do pacote são menores, seu uso reduz o impacto na operação normal da rede e aumenta as chances de sucesso na comunicação em redes sobrecarregadas (MAURO; SCHMIDT, 2009).

Entretanto a situação torna-se mais delicada quando *traps* são consideradas. A ausência de confirmação por parte do UDP faz com que não seja possível ao emissor saber se sua mensagem chegou ao destino o que, no caso das *traps*, pode significar a perda de um evento importante (CLEMM, 2006). Para casos onde é estritamente necessária a confirmação de um evento, foi adicionada a operação *inform* que realiza este controle através da aplicação ao invés do protocolo de transporte.

Apesar de projetado para o funcionamento sobre redes TCP/IP, o SNMP, devido ao seu sucesso, ganhou compatibilidade com outras plataformas como AppleTalk e IPX, além de projetos para interoperabilidade com o modelo ISO assim que ele entrasse em uso (HUNT, 1997). Entretanto tais tecnologias perderam espaço e hoje não têm mais relevância nas redes de computadores e tampouco na sua gerência. Para comunicação sobre UDP, o SNMP utiliza a porta

Figura 2: Estrutura dos Pacotes SNMP



Fonte: Adaptado pelo autor com base em Perkins e McGinnis (1996), Stallings (1998), Stallings (1999) e Mauro e Schmidt (2009).

161 para todas operações exceto *traps* e *informs*, quando usa a porta 162 (MAURO; SCHMIDT, 2009).

Ao longo de sua evolução o SNMP passou por revisões na estrutura de suas mensagens, com a principal delas ocorrendo na transição entre as versões 1 e 2. Tais correções tiveram por objetivo unificar a arquitetura e simplificar o seu tratamento tanto no agente quanto no gerente (PERKINS; MCGINNIS, 1996). Apesar das alterações no formato das mensagens, a arquitetura do modelo SNMP, como ilustrada pela Figura 1, não foi alterada, seguindo estável desde seu projeto inicial.

Com a padronização de sua terceira versão o SNMP passou a contar com funcionalidades maduras de segurança, entretanto esta evolução trouxe consigo um significativo aumento na complexidade do protocolo (MAURO; SCHMIDT, 2009). Este crescimento fica evidente quando inspeciona-se a estrutura de um pacote SNMP das versões 1 e 2 comparado com a versão 3. Com a ajuda da Figura 2, percebe-se que as funcionalidades de segurança incorrem um custo tanto no tamanho dos pacotes quanto na simplicidade do protocolo.

Apesar da mudança no pacote SNMP, a estrutura da PDU (*Protocol Data Unit*, ou, em tradução livre, Unidade de Dados do Protocolo) manteve-se estável. A PDU é responsável por encapsular os dados de requisições e respostas realizadas através do SNMP e, para isso, conta com campos de metadados e dados (PERKINS; MCGINNIS, 1996).

Todas as operações disponibilizadas pelo SNMP compartilham a mesma PDU, com ressalvas no caso do *get-bulk*, sendo esta uma prova concreta da simplicidade do SNMP, uma vez que

a estrutura compartilhada facilita a implementação de agentes (CLEMM, 2006) Na Tabela 2 é detalhado o significado de cada um dos campos da PDU conforme a operação realizada. Cabe destacar que os campos *error status* e *error index* adquirem outro significado quando usados na requisição *get-bulk*, informando quais dos itens nos *variable bindings* devem ser interpretados como repetidos ou não (PERKINS; MCGINNIS, 1996).

Cabe, também, atenção especial aos *variable bindings*, que indicam os objetos de interesse da requisição e da resposta. Neste campo espera-se uma lista contendo os nomes (identificadores na MIB) e os valores dos campos sobre os quais o gerente deseja operar (SIMONEAU, 1999). No caso de respostas, *sets* e *traps* (considerando também *informs* e *reports*) estarão presentes os valores que definem os objetos, enquanto nas requisições devem conter um indicador de campo vazio, NULL (CLEMM, 2006). Nessa estrutura reside a capacidade do SNMP de obter e definir diversas informações de gerência em uma única requisição e de maneira atômica.

2.2 MIB

Parte integral da gerência de redes é a definição de um idioma comum que será usado entre gerentes e agentes. O protocolo, seja SNMP ou qualquer outro, faz parte da solução mas sozinho não é capaz de preencher todos os requisitos necessários para o estabelecimento de uma linguagem compreendida por todos os interessados na gerência e, apesar de especificar o formato das mensagens, o protocolo não determina como as informações serão representadas. Esta é a função da Base de Informações de Gerência (em inglês *Management Information Base*, MIB).

O papel da MIB é especificar a organização lógica e quais são os dados disponíveis para que aplicações se comuniquem de maneira padronizada (SILVA, 2005). Sua importância deve-se ao fato de ser "uma definição precisa das informações acessíveis através de um protocolo de gerência de redes" (LEINWAND; CONROY, 1996, p. 152) e de que as "informações de gerência estão no cerne da comunicação que ocorre entre gerentes e agentes" (CLEMM, 2006, p. 227).

Sua origem "deriva do modelo OSI/ISO de gerência de redes" (DING, 2009, p. 46) e indica que "como um conceito, uma MIB não depende de nenhum protocolo de gerência" (CLEMM, 2006, p. 222). Porém este nem sempre é o caso e, como o próprio Clemm (2006, p. 201) explica, "apesar de, em teoria, MIBs poderem ser definidas de forma verdadeiramente independente do seu protocolo, na prática diferentes protocolos exigem sua própria maneira" . Este foi o caso do SNMP e do modelo ISO, onde inicialmente previa-se que ambos compartilhariam as mesmas MIBs, porém diferenças nos protocolos forçaram o desenvolvimento independente (HUNT, 1997; STALLINGS, 1999; LEINWAND; CONROY, 1996).

Estruturada como uma árvore, a MIB abriga e define todas as informações de gerência para determinado dispositivo ou classe de dispositivos, ou seja, as "MIBs são especificações contendo as definições das informações de gerenciamento para que sistemas em rede possam ser

Tabela 2: Relação dos campos da PDU e seu uso de acordo com a operação

	response	***set***	***trap***	***inform***	***report***	***get***	***get-next***	***get-bulk***
PDU Type	0xA2	0xA3	0xA7	0xA6	0xA8	0xA0	0xA1	0xA5
Request ID	Copia o valor da requisição	Número gerado pelo solicitante para identificar a requisição						
Error Status / Non Repeaters	Indica o código do erro ocorrido no processamento da resposta	Não utilizado, deve ser enviado zerado						Assume o papel de Non Repeaters, indicando quantos dos itens presentes nos Variable Bindings devem retornar apenas uma ocorrência
Error Index / Max Repetitions	Indica a posição do item nos Variable Bindings que causou o erro	Não utilizado, deve ser enviado zerado						Assume o papel de Max Repetitions, indicando quantas vezes deve obter os itens restantes nos Variable Bindings
Variable Bindings	Lista de Nomes e Valores conforme recebido na requisição porém com os valores preenchidos com os dados atuais do dispositivo	Lista de Nomes e Valores contendo os valores que deseja-se definir para os objetos no dispositivo destino	Lista de Nomes e Valores contendo os dados relevantes à notificação e obrigatoriamente informando o uptime do dispositivo e o tipo de notificação			Lista de Nomes e Valores contendo os identificadores dos objetos aos quais deseja-se obter o valor e com o valor na requisição definido como NULL	Lista de Nomes e Valores contendo os identificadores parciais dos objetos aos quais deseja-se obter o valor e com o valor na requisição definido como NULL	

Fonte: Adaptado pelo autor com base em Perkins e McGinnis (1996) e Stallings (1999).

monitorados, configurados e controlados" (PERKINS; MCGINNIS, 1996, p. 1). Outra forma de visualizar a MIB é como uma coleção de objetos em um banco de dados virtual usado para gerir entidades de rede, tais como computadores, roteadores e impressoras (DING, 2009), permitindo representar uma visão lógica do dispositivo sendo gerenciado e criando uma camada de abstração especificamente para fins de gerência de redes (CLEMM, 2006). Desta forma "qualquer tipo de informação estatística ou de estado que pode ser acessada pelo gerente está definida na MIB" (MAURO; SCHMIDT, 2009, p. 4).

É importante notar que um agente pode, e é encorajado a, implementar mais de uma MIB concorrentemente (CLEMM, 2006), isto é possível pois "permite-se a indivíduos e fornecedores definir MIBs para seu próprio uso" (MAURO; SCHMIDT, 2009, p. 5). Grandes fabricantes como Cisco e 3Com (agora HP), além de suportar um conjunto básico de MIBs, fornecem, juntamente com seus equipamentos, MIBs próprias e específicas para determinados produtos. Desta forma podemos concluir que uma MIB "pode ser pensada como a especificação que define os objetos gerenciados que um dispositivo ou fornecedor suporta" (MAURO; SCHMIDT, 2009, p. 27).

3 INTERNET DAS COISAS

A Internet das Coisas pode ser caracterizada como um paradigma no qual uma infinidade de dispositivos, embarcados em objetos cotidianos, podem coletar dados sobre seu ambiente e, através de esquemas de endereçamento, comunicar-se entre si em busca de um objetivo comum (ATZORI; IERA; MORABITO, 2010). Indústria e academia estão cientes das possibilidades que este modelo apresenta e cooperam em prol do alcance desta visão através de parcerias e trocas de experiência (ITU, 2005). Apesar dos esforços, a tecnologia atual não permite, de maneira economicamente viável, alcançar as proporções necessárias para a criação de uma verdadeira Internet das Coisas, tornando os experimentos não mais do que protótipos de escala reduzida (SMITH, 2012).

Neste capítulo são apresentados os principais conceitos que possibilitaram a concepção da ideia de uma Internet das Coisas e sua definição conforme interpretada neste trabalho. Ainda é abordada aqui a importância da IoT para revolucionar a maneira como a sociedade adquire informações e conhecimento sobre si mesma, transformando-os em sabedoria, assim como os principais desafios e oportunidades ligados à realização deste paradigma.

3.1 Origem

Diversas tecnologias contribuíram com os avanços necessários para o desenvolvimento da Internet das Coisas. A partir dos estudos em áreas como etiquetas de Identificação por Radiofrequência (RFID), Redes de Sensores sem Fio (WSN), Protocolo de Internet versão 6 (IPv6) e *Smart Objects* foi possível atingir o atual nível de maturidade da IoT. A seguir são apresentadas as principais tecnologias nas quais o conceito de Internet das Coisas se apoia e que possibilitaram o seu desenvolvimento.

3.1.1 RFID

Etiquetas RFID representam uma nova geração dos mecanismos de identificação de objetos (BROCK, 2001). Diferentemente dos códigos de barras, as *tags* RFID utilizam comunicação via radiofrequência, o que, segundo Want (2006), possibilita uma maior distância de leitura e, adicionalmente, elimina a necessidade de visada direta. O autor afirma ainda que é possível que as etiquetas contenham memória de leitura e escrita, permitindo descrever estados do objeto identificado, além de sensores que podem indicar informações sobre o item (se ele sofreu quedas ou se permaneceu dentre os limites de temperatura, por exemplo).

Iniciativas preliminares no campo da Internet das Coisas contemplaram principalmente o uso de RFIDs para realizar o rastreamento de objetos em um ambiente dotado de diversos leitores RFID ou para ativar determinados comportamentos em um sistema computacional de acordo com dados obtidos através da leitura de uma etiqueta. Os trabalhos de Want et al. (1999),

Floerkemeier, Roduner e Lampe (2007) e Welbourne et al. (2009) apresentam implementações concretas utilizando-se de RFIDs.

3.1.2 WSN

Diferentemente das *tags* RFID, que não realizam processamento e são geralmente passivas (ATZORI; IERA; MORABITO, 2010), as Redes de Sensores sem Fio são compostas de pequenos dispositivos que, apesar da capacidade reduzida, efetuam coleta e processamento de dados (SAKTHIDHARAN; CHITRA, 2012). Segundo Sung, Lopez e Kim (2007), boa parte das aplicações de WSNs são voltadas para o monitoramento de ambientes físicos, contemplando fins militares, ecológicos e industriais (SUHONEN, 2012). Pesquisas relacionando RFID e WSNs, em direção a uma visão de Internet das Coisas, foram realizadas por Sung, Lopez e Kim (2007), Zhang e Zhu (2011) e Hada e Mitsugi (2011), comprovando a viabilidade da proposta.

De acordo com Liu e Zhou (2012), a capacidade de coletar e processar dados de maneira autônoma é uma das fundações da IoT, tornando as WSNs uma das áreas de pesquisa que mais contribuíram para o seu desenvolvimento. Perera et al. (2013) corroboram ao afirmar que a IoT não pode existir sem o apoio das WSNs, pois elas fornecem a maior parte da infraestrutura de hardware para a comunicação e coleta de informações contextuais.

3.1.3 Gateway IoT

Apesar do sucesso das WSNs para a comunicação em curta distância, Zhu et al. (2010) afirmam que existe dificuldade em conectar redes de sensores à internet devido a falta de padronização nos protocolos de comunicação. Para superar esta dificuldade foi estabelecido o conceito de dispositivo coordenador, também chamado de *gateway* (STEENKAMP; KAPLAN; WILKINSON, 2009). Assim como as WSNs, os protótipos iniciais de IoT conectavam-se à internet através do coordenador, um dispositivo mais potente que faz o papel de roteador na rede (KURYLA, 2010) e, por não apresentar as mesmas restrições dos sensores, é encarregado de prover conectividade externa (através de tecnologias como GSM, CDMA e WLAN, por exemplo) (LIU; ZHOU, 2012).

As implementações de Zhu et al. (2010), Steenkamp, Kaplan e Wilkinson (2009) e Hada e Mitsugi (2011) apresentam resultados e percepções sobre o uso de *gateways* entre WSNs e a internet, viabilizando a criação de aplicações que demonstram, na prática, o conceito de Internet das Coisas.

3.1.4 IPv6

Uma vez cumprido o objetivo de conectar as WSNs a internet o próximo passo consiste em propiciar conectividade para cada dispositivo individualmente (ATZORI; IERA; MORABITO,

2010), efetivamente tornando-o parte da internet. Para tanto, a escolha considerada mais sábia por Mattern e Floerkemeier (2010) é de utilizar-se dos mesmos protocolos já estabelecidos pela internet, favorecendo a interoperabilidade. Sobre o uso de endereços IP como forma de identificação Sundmaeker et al. (2010) dizem que:

> a ideia de atribuí-los a cada um dos aproximadamente 5 mil objetos diários que nos cercam, é bastante atraente. Com a tecnologia certa em cada objeto (uma etiqueta RFID, por exemplo) e a rede certa nos arredores, será fácil localizar e catalogar itens em poucos segundos e colher os benefícios da vasta quantidade de novas informações que a comunicação entre eles vai prover. IPv6 é indiscutivelmente um dos passos para tornar a Internet das Coisas uma realidade (SUNDMAEKER et al., 2010, p. 15).

Orientadas por esta visão, companhias como Intel, Cisco e SAP formaram em 2008 a aliança "IP para Objetos Inteligentes" (IPSO), reforçando o interesse da indústria pela conectividade direta entre dispositivos (DUNKELS; VASSEUR, 2008; MATTERN; FLOERKEMEIER, 2010). Aliada a esse interesse, a Força Tarefa de Engenharia da Internet, IETF, vem desenvolvendo o protocolo IPv6 sobre Rede Local Pessoal Sem Fio de Baixo Consumo, 6LoWPAN, que define os mecanismos para troca de mensagens IPv6 sobre redes IEEE 802.15.4, especialmente projetada para o caso da Internet das Coisas (GOMEZ; PARADELLS, 2010).

3.1.5 *Smart Objects*

Contrastando com as etiquetas RFID, o conceito de Objetos Inteligentes (*Smart Objects*) compreende objetos físicos/digitais autônomos aumentados com capacidades sensoriais, de processamento e rede (BEIGL; GELLERSEN; SCHMIDT, 2001). Estes objetos foram classificados, no trabalho de Kortuem et al. (2010), em três grandes grupos de acordo com seu grau de percepção e, consequentemente, complexidade. Sendo eles: consciência à nível de atividade, de política e de processo. Segundo Dunkels e Vasseur (2008), a adoção e popularização dos Objetos Inteligentes tem sido dificultada pela grande quantidade de sistemas fechados e proprietários, o que dificulta, ou até mesmo impossibilita, a integração entre soluções.

Espera-se que as principais habilidades de um Objeto Inteligente digam respeito ao compartilhamento de informações (entre dispositivos e usuários) e a consciência do contexto em que estão inseridos (BEIGL; GELLERSEN; SCHMIDT, 2001). Os autores ainda enfatizam que tais objetos "serão deliberadamente limitados em sua capacidade computacional, memória e poder de processamento a níveis adequados para um propósito específico". Seguindo esta tendência, Mattern e Floerkemeier (2010) prevêem que a tecnologia caminha em direção a um modelo onde Objetos Inteligentes efetivamente se comuniquem entre eles mesmos, serviços na internet e seus usuários.

Experiências no planejamento e execução de aplicações compostas por *Smart Objects* po-

dem ser encontradas nos trabalhos de Beigl, Gellersen e Schmidt (2001), Gellersen et al. (2004), Holmquist et al. (2004), através do projeto Smart-Its, e Kortuem et al. (2010), abordando questões de saúde e segurança, gestão de processos e modelos de negócio por intermédio de um único dispositivo aplicado ao ramo da construção civíl.

3.2 Definição

Diversas são as definições disponíveis para o termo Internet das Coisas (IoT). Atzori, Iera e Morabito (2010) atribuem a grande variedade de definições às diferentes visões que cada organização, dependendo dos seus objetivos, tem, geralmente sendo orientadas a internet ou as coisas. Apesar das diferenças o conceito de IoT é, para Coetzee e Eksteen (2011):

> uma visão onde objetos se tornam parte da internet: onde cada objeto é unicamente identificável e acessível à rede, sua posição e status conhecidos, onde serviços e inteligência são acrescidos a esta internet expandida, fundindo o mundo físico e o digital (COETZEE; EKSTEEN, 2011).

Segundo Sundmaeker et al. (2010), dentre as mais citadas estão as definições por Kevin Ashton (2009) e David Brock (2001) do Auto-ID Labs e da União Internacional de Telecomunicações, ITU (2005). Enquanto a primeira é focada na identificação e detecção de objetos através do uso de RFIDs, a segunda aborda uma definição mais ampla, detalhada a seguir.

Em sua definição, a ITU (2005) sugere que a Internet das Coisas, através de suas tecnologias, será capaz de conectar objetos de maneira inteligente e sensorial, combinando avanços nos campos de:

- **Identificação – *Tagging things*:** Tecnologias para reconhecimento e rastreamento de objetos, baseadas principalmente em RFID. Possibilitam uma forma primitiva de integração entre o real e o virtual;

- **Sensores – *Feeling things*:** Tecnologias relacionadas a WSNs, utilizando-se dos conhecimentos já adquiridos pelas pesquisas nesta área. Sensores ampliam a quantidade de informações contextuais para aplicações, possibilitando um melhor mapeamento do seu ambiente por meio de parâmetros como: temperatura, luminosidade, vibração, nível de ruído, entre outros;

- **Sistemas embarcados – *Thinking things*:** Refere-se a crescente capacidade de embutir microcontroladores e processadores em objetos da vida cotidiana, efetivamente possibilitando a criação de objetos inteligentes. Com a redução de custo e tamanho, a substituição de circuitos de propósito específico por processadores multipropósito é favorecida, criando uma nova geração de objetos;

- **Nanotecnologia – *Shrinking things*:** Abordando o impacto e as possibilidades do uso altamente difundido de tecnologias de nano escala. Dentre as previsões estão circuitos menores, mais econômicos e baratos, além do uso de novos materiais, como grafeno e nanotubos, na fabricação destes dispositivos.

Entretanto, a riqueza de possibilidades abertas pela IoT pode ser explicada simplesmente pela análise individual de seus termos constituintes, ou seja, a combinação de internet e coisas. Segundo Simpson e Weiner (2005), no Oxford English Dictionary, a internet é "uma rede global de computadores provendo diversos serviços de informação e comunicação, constituída de redes interconectadas usando protocolos padronizados de comunicação".

Coisas, por outro lado, não tem uma definição precisa, podendo variar conforme o contexto e o foco da aplicação. Coetzee e Eksteen (2011) apresentam uma definição abrangente direcionada para IoT:

> A definição de "coisas" na visão da IoT é muito ampla e inclui uma variedade de elementos físicos. Estes incluem objetos pessoais que carregamos como *smartphones*, *tablets* e câmeras digitais. Ela também inclui elementos em nosso ambiente (seja em casa, no carro ou no trabalho) assim como coisas equipadas com *tags* (RFID ou outras) que se tornam conectadas através de um portal de acesso (um *smartphone*, por exemplo) (COETZEE; EKSTEEN, 2011).

Identifica-se uma mudança gradual na definição do conceito de Internet das Coisas, inicialmente contemplando apenas mecanismos de identificação e, impulsionado pela evolução tecnológica, passando a versar sobre dispositivos inteligentes e diretamente conectados à internet sem a necessidade de intermediários. Segundo Buckley (2006) a transformação no conceito de IoT é resultado tanto de avanços tecnológicos quanto de interesse mercadológico impulsionado pelos potenciais benefícios.

3.3 Importância

Uma vez estabelecida a definição de Internet das Coisas, é possível compreender o impacto social e tecnológico deste conceito. A internet causou uma revolução na maneira com que compartilhamos informação e conhecimento, gerando, de acordo com Carr (2010), mudanças até mesmo em nossa estrutura cerebral.

Classificada como a terceira onda da computação (REGISTER, 2013), os conceitos de IoT poderão ser aplicados a diversos setores produtivos, desde a indústria ao setor público. Os possíveis benefícios obtidos através de uma vasta rede de dispositivos interconectados fez com que especialistas como Hung e Mahoney (2012), da Gartner, classificassem a IoT como um paradigma transformacional.

Evans (2011) ressaltam que a importância da IoT está profundamente interligada com a

Figura 3: Hierarquia do conhecimento

Fonte: Evans (2011)

maneira como a humanidade se desenvolveu: “Humanos evoluem porque se comunicam. Assim que o fogo foi descoberto e compartilhado, por exemplo, ele não precisou ser redescoberto, apenas comunicado”. Ainda sob este ponto de vista, afirmam que com a aplicação dos conceitos de IoT, haverá um aumento exponencial na quantidade de dados disponíveis e na forma como utilizamos estes dados (representada pela Figura 3):

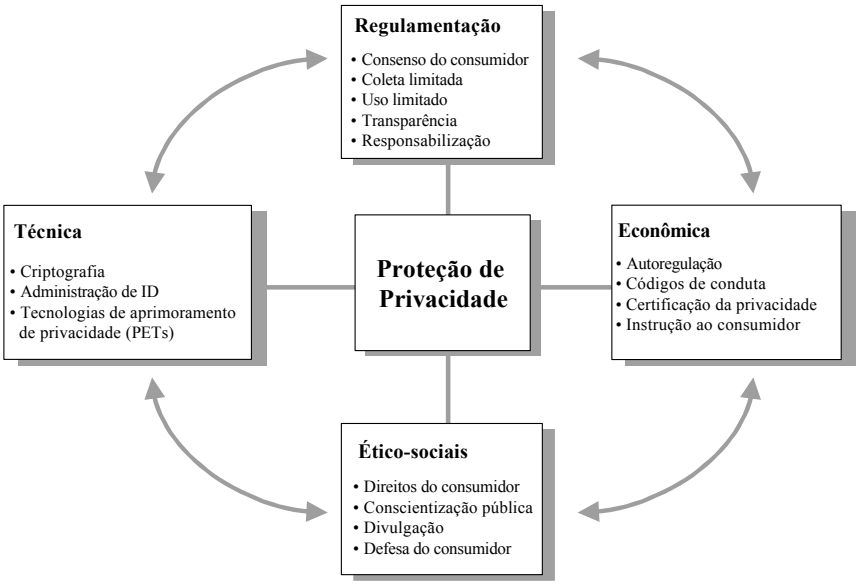
> considere que a IoT representa a próxima evolução da internet, levando a um enorme salto na sua habilidade de coletar, analisar e distribuir dados que podemos transformar em informação, conhecimento e, finalmente, sabedoria. (EVANS, 2011, p. 2).

3.4 Desafios

A realização de uma visão de Internet das Coisas não ocorrerá sem desafios, tanto sociais e políticos quanto tecnológicos. As implicações ligadas a existência de uma infinidade de dispositivos coletando e transmitindo informações sobre a vida de seus usuários já causa grandes preocupações entre membros da indústria e da academia. Desenvolvimentos tecnológicos, necessários para viabilizar a difusão do conceito de IoT, também representam grandes barreiras no avanço deste paradigma.

No âmbito social, as dificuldades em tornar real a visão da Internet das Coisas concentram-se principalmente em torno da privacidade. Diversos autores demonstram receio quanto a ma-

Figura 4: Estratégias para proteção de privacidade



Fonte: Adaptado pelo autor de ITU (2005).

neira com que os dados obtidos serão utilizados, havendo, inclusive, propostas de códigos de conduta específicos para este paradigma (ITU, 2005). Existe a noção de que há um balanço a ser atingido através dessas tecnologias, de um lado a proteção à privacidade, e de outro o conforto obtido através do uso destas informações (ATZORI; IERA; MORABITO, 2010).

Assim como a revolução industrial causou um aumento na dependência da civilização na energia elétrica, Mattern e Floerkemeier (2010) ponderam que a implantação de uma Internet das Coisas a nível global trará um aumento na dependência de conectividade. Há de se convir que atualmente já percebe-se um aumento na dependência por computadores e conectividade, como nota Carr (2010), contudo o aumento explosivo na quantidade de dispositivos, previsto por Evans (2011) para a casa de 50 bilhões em 2020, vai agravar ainda mais a situação.

O medo de viver em uma era Orwelliana[1], com vigilância integral sobre o indivíduo, torna-se uma possibilidade real e factível. Desta forma, há grandes receios por parte da comunidade acadêmica sobre a forma com que tais dados serão utilizados e, conforme aponta a Figura 4, como serão protegidos. A respeito da privacidade, Buckley (2006) argumenta que dentre as principais questões em aberto neste contexto encontram-se: a propriedade dos dados, quem é o dono dos dados coletados; a gestão de acessos, quem pode acessar e qual é o nível de acesso aos dados; a autorização para transmissão, quem está ciente e/ou autoriza a transmissão dos dados para terceiros; e a neutralização de objetos, como desabilitá-los de forma permanente.

Relacionada a privacidade, existem ainda questões de segurança que previnem a difusão da

[1] George Orwell era um escritor inglês que, em seu livro 1984, caracterizou um ditador totalitário que vigiava a todos através de câmeras e denominava-se Big Brother.

Internet das Coisas. Dada a reduzida capacidade de processamento dos dispositivos que integram o paradigma da IoT, técnicas de criptografia e segurança de dados acabam sendo de aplicabilidade limitada, portanto ainda são necessários desenvolvimentos nesta área (SUNDMAEKER et al., 2010). Mecanismos de identificação, como chaves pública-privadas, por exemplo, devem também ser melhorados e padronizados para o uso no contexto de IoT, uma vez que serão responsáveis por manter o controle e permissionamento necessário para o acesso aos dados contidos nos dispositivos, assim como mecanismos para revogação destas identificações (BUCKLEY, 2006). Ainda permeando a segurança está a preocupação com a clonagem de *tags* e dispositivos, algo que pode comprometer toda uma rede assim como colocar em risco a segurança de outras pessoas, como no caso de um passaporte clonado (ITU, 2005).

A quantidade de dados gerados através dos dispositivos que compõem a Internet das Coisas também apresenta seus próprios desafios. Coetzee e Eksteen (2011) definem este fenômeno como "dilúvio de dados", onde deve-se provisionar desde espaço de armazenamento até capacidade de rede para tratar do volume de informação. Existe, ainda, o problema de como interpretar todos estes novos dados que, devido ao seu volume, nem sempre fazem sentido com técnicas simples de análise (ITU, 2005). Apesar de diretamente relacionado às questões de segurança e privacidade, o problema da quantidade de informação gerada permeia, também, questões técnicas.

Os desafios de âmbito técnico apresentados pelo paradigma da Internet das Coisas são muitos e diversificados, caracterizando, em alguns casos, uma área de estudo própria. Portanto são apresentados na lista abaixo uma compilação dos desafios técnicos conforme definidos por ITU (2005), Buckley (2006), Mattern e Floerkemeier (2010) e Sundmaeker et al. (2010):

- **Energia:** Melhorias na capacidade de baterias e nas técnicas de conversão de energia a partir de outras fontes (como vibração, luz e calor) são necessárias para aumentar a utilidade dos dispositivos, uma vez que a limitação energética faz com que outras características do aparelho também tenham que ser limitadas;

- **Antenas:** Visando aumentar o alcance das comunicações e a duração das baterias, desenvolvimentos em técnicas de processamento de sinais e no projeto de antenas também são desejáveis para dispositivos da IoT;

- **Protocolos:** Reduções no custo das comunicações e métodos de tolerância a falhas são necessários para tornar a comunicação sem fio mais confiável, ocasionando, ainda, uma redução no gasto energético (uma vez que mensagens não precisarão ser retransmitidas);

- **Sensores:** Melhorias na precisão e a redução no consumo energético de sensores são, também, áreas onde deseja-se desenvolvimento tecnológico. Dado que geralmente mais de um sensor integra um dispositivo da Internet das Coisas e considerando, também, as limitações de sensores (como GPS em ambientes fechados), a superação destas barreiras possibilitaria grandes avanços para a IoT;

- **Atuadores:** Complementando o trabalho dos sensores, os atuadores são responsáveis por efetivamente realizar as ações (a partir das decisões tomadas com base nos dados de sensores), portanto o seu desenvolvimento traz melhorias para os dispositivos e novas possibilidades de produtos e serviços;

- **Endereçamento:** A identificação de dispositivos, não só através de endereços como o IP, também é área de estudo relacionada à IoT. O desenvolvimento de ontologias e maneiras de endereçar as "coisas" conforme a aplicação em questão são necessárias, uma vez que o IP não é eficiente para memorização humana e não fornece características sobre o dispositivo identificado;

- **Busca:** Da mesma forma como existem algoritmos de busca para documentos na internet, é necessário o desenvolvimento de formas de buscar os dispositivos que compõem a Internet das Coisas, possivelmente utilizando-se das diferentes técnicas de endereçamento e das características de cada um destes dispositivos.

3.5 Oportunidades

Conceitos atuais como Big Data fornecem uma amostra das possibilidades de extração de conhecimento a partir de grandes conjuntos de dados. Com uma Internet das Coisas funcional, e utilizando-se destas técnicas, por exemplo, é possível aumentar a quantidade e a qualidade dos dados obtidos, melhorando, consequentemente, a qualidade e a precisão das análises. Projetos como Hadoop e SAP Hana já encontram-se em uso em diversas organizações e contribuem para a gestão e otimização de processos, possibilitando a tomada de decisões em tempo real a partir de dados vindos de fontes heterogêneas.

A grande quantidade de sensores distribuídos geograficamente poderá também desempenhar um papel importante na tomada de decisão, possibilitando, em conjunto com atuadores, a automação de tarefas baseadas em dados do ambiente. Tais decisões, por mais simples que pareçam, são necessárias ao longo de toda a cadeia produtiva na forma de processos industriais, seja no controle de umidade do solo, de temperatura ou de peso. Apesar de já serem possíveis hoje, tais controles terão maior valor de negócio, uma vez que a integração na Internet das Coisas possibilita o processamento e o compartilhamento dessas decisões com outros dispositivos, potencialmente servindo como dados de entrada para os demais processos (ITU, 2005).

Grandes corporações também se apropriam do conceito de Internet das Coisas para a criação de diversos projetos de controle e automação, seja a nível residencial, comercial e industrial, expandindo até mesmo à iniciativas globais. HP, IBM e Microsoft através de seus projetos, respectivamente, CeNSE, Smarter Planet e Eye-On-Earth demonstraram o interesse e investimento em direção à realização do conceito de Internet das Coisas (COETZEE; EKSTEEN, 2011). O projeto CeNSE traz, em sua definição, uma descrição da visão de Internet das Coisas que vai ao encontro de autores como Atzori, Iera e Morabito (2010), Smith (2012) e Perera et al. (2013):

> CeNSE consiste de uma rede altamente inteligente de bilhões de sensores de nanoescala projetados para sentir, provar, cheirar, ver e ouvir o que está acontecendo no mundo. Quando completamente implantados, estes sensores irão rapidamente reunir dados e transmití-los a potentes motores computacionais, que irão, em tempo real, analisar e agir de acordo com as informações usando uma nova geração de serviços e aplicações de negócios (HEWLETT-PACKARD, 2009).

Os domínios de aplicação afetados pelo paradigma da Internet das Coisas são variados e atingem grande parte da população e da indústria. A difusão de computadores e sistemas de informação pode ser apontada, em parte, como responsável pelo grande alcance das tecnologias de IoT, uma vez que tais sistemas podem sempre ser aprimorados. Na lista abaixo encontra-se uma seleção de domínios[2] onde são previstas melhorias pelo uso de conceitos e tecnologias da Internet das Coisas.

- **Aviação e Aeroespacial:** identificação de peças falsificadas, monitoramento através de redes de sensores (dentro e fora da aeronave), identificação de passagens;
- **Automotiva:** sistemas de monitoramento (pressão dos pneus, temperatura do óleo, etc), direção autônoma, comunicação veículo–veículo e veículo–infraestrutura;
- **Telecomunicações:** redes peer-to-peer, NFC, carteira digital;
- **Prédios Inteligentes:** automação residencial (luzes e ar-condicionado, por exemplo), monitoramento de consumo, assistência a idosos, compras automatizadas;
- ***Smart Grids*:** medição de energia, monitoramento da rede elétrica,
- **Médica e Saúde:** monitoramento de pacientes, distribuição de medicamentos, medição e monitoramento de parâmetros vitais (pulso, temperatura, pressão), dispositivos implantados (marcapassos, por exemplo);
- **Farmacêutica:** rastreamento, identificação de produtos falsificados, monitoramento das condições de transporte / armazenamento;
- **Varejo, Logística e Gestão da Cadeia de Suprimentos:** monitoramento de entregas, recebimentos e estoque, detecção de furto, rastreamento de produtos;
- **Manufatura e Gestão de Ciclo de Vida de Produtos:** otimização do processo de produção, monitoramento do ciclo de vida, localização de itens, reciclagem;
- **Óleo e Gás:** monitoramento de barris e contêineres, identificação de produtos tóxicos, monitoramento de maquinário e processos, monitoramento de parâmetros de operação;

[2] Elaborada com base nos dados apresentados por ITU (2005), Atzori, Iera e Morabito (2010), Sundmaeker et al. (2010), Smith (2012) e Perera et al. (2013).

- **Segurança, Proteção:** vigilância ambiental (chuvas, queimadas, poluição, etc), monitoramento de infraestrutura (vazamentos e rachaduras, por exemplo), controle de acesso, alertas de catástrofes;
- **Monitoramento Ambiental:** monitoramento de desmatamentos e queimadas, monitoramento da qualidade do ar e da água, rastreamento de animais;
- **Transporte de Pessoas e Mercadorias:** sistemas de pedágio e passagens, identificação e triagem de pessoas e mercadorias, controle de tráfego, identificação de bagagens;
- **Rastreabilidade de Alimentos:** rastreamento de matéria prima, reconstrução da cadeia de suprimentos, identificação de produtos/lotes contaminados, monitoramento das condições de armazenamento e transporte;
- **Criação e Agricultura:** identificação e rastreamento de animais, controle e prevenção de doenças e pragas, vacinação, redução de intermediários entre produtor e consumidor;
- **Mídia, Entretenimento e Bilhetagem:** geração autônoma de notícias, interatividade através de etiquetas, cobrança automatizada de bilhetes e entradas, propagandas interativas;
- **Seguros:** monitoramentos de parâmetros de operação (em troca de descontos, por exemplo), acionamento automático da seguradora, previsão de manutenções e trocas;
- **Reciclagem:** monitoramento de emissão de poluentes, logística reversa, rastreamento de itens não descartados corretamente.

4 PROPOSTA PARA IOT

Uma vez apresentado o conceito de Internet das Coisas e conhecidos seus desafios e oportunidades, torna-se possível identificar pontos de melhoria. A grande quantidade de dispositivos previstos no contexto de IoT torna sua gerência e configuração uma tarefa não trivial e altamente vulnerável a erros humanos. Apesar das iniciativas em busca de autoconfiguração e gestão automatizada, é improvável que tais esforços possibilitem uma gerência livre da intervenção de operadores.

Ainda que a autoconfiguração forneça um objetivo de longo prazo, a necessidade de configurar e gerenciar dispositivos, mesmo que em situações experimentais e de escala reduzida, é um problema que já se enfrenta atualmente. Desta forma, percebe-se o desejo por um método padronizado para a gerência destes dispositivos, principalmente no que diz respeito à configuração, uma vez que cada sistema operacional (por vezes específico para o domínio de aplicação) apresenta mecanismos próprios de gestão e configuração.

Tais necessidades são deveras semelhantes aquelas encontradas nos anos 1980, onde profissionais e acadêmicos passavam por grandes dificuldades na gestão de suas infraestruturas, seja na forma de um escritório ou de um laboratório. Devido a falta de maturidade das aplicações para a Internet das Coisas existem, ainda, grandes divergências e falta de padronização dos próprios dispositivos, dificultando a integração entre eles. Semelhanças como estas tornam ainda mais explícita a relação da IoT com a gerência de redes clássica e o SNMP.

Os problemas semelhantes, no contexto de Internet das Coisas e de gerência de redes, tornam oportuno o reuso de estratégias reconhecidamente eficazes e postas à prova ao longo dos anos através do SNMP, que acabou tornando-se o protocolo *de facto* e sinônimo de gerência de redes. Contudo, as peculiaridades características da IoT exigem adaptações e revisões das antigas estratégias, de forma que aproveite-se também a oportunidade para revisitar partes problemáticas do modelo clássico de gerência de redes.

A união dos conceitos de IoT e gerência de redes traz benefícios pois possibilita o reuso de ferramentas, protocolos e estratégias de gestão e, mesmo que ainda não estejam adaptadas para a Internet das Coisas, permite obter boa parte dos ganhos provenientes do seu uso. Ainda é possível citar, como um subproduto da mescla proposta entre SNMP e IoT, a aderência ao paradigma FCAPS de gerência de redes, viabilizando o reuso de todo um arcabouço de conhecimento frente aos novos desafios apresentados pela Internet das Coisas.

Portanto objetiva-se, neste trabalho, provar que é possível reaproveitar boa parte dos conhecimentos adquiridos com a gerência de redes clássica e viabilizar a interoperabilidade entre as suas ferramentas e o paradigma da Internet das Coisas. Para atingir este objetivo é necessária a criação de um modelo que forneça denominadores comuns entre estes paradigmas, intermediando sua integração. O funcionamento deste modelo será demonstrado através da implementação de um protótipo da solução, servindo como prova de conceito e dispensando o uso de simuladores na avaliação. Uma vez criado o modelo de integração, implementado na forma de

protótipo e testado, é necessária uma avaliação crítica de suas forças e fraquezas, possibilitando verificar a adequação desta proposta ao seu uso no contexto de Internet das Coisas e de gerência de redes.

4.1 Escopo

De forma a melhor delimitar os objetivos, necessidades e critérios de avaliação, este trabalho tem seu escopo de atuação intencionalmente limitado à automação residencial. Neste contexto estão inseridos processos tais como a coleta de dados, ou seja, o monitoramento do ambiente (temperatura, umidade, iluminação), seus dispositivos (consumo energético, estado) e o controle sobre estes dispositivos (ligar, desligar, alterar a temperatura).

Esforços de automação residencial auxiliam na caminhada rumo a casas e prédios inteligentes e que regulam, de forma autônoma, parâmetros ambientais como temperatura e iluminação baseados em dados a respeito dos hábitos de seus moradores. Entre os ganhos ocasionados por este tipo de automação é possível citar a economia de energia e a consequente redução no impacto ambiental, além do aumento nos níveis de conforto e segurança das residencias.

A este contexto pertencem as ideias de casas futuristas, vistas em feiras e nas obras de ficção-científica, onde, por exemplo, moradores são recebidos com torradas e café prontos ao chegar do trabalho, ou com um banho quente à sua espera. Contudo, devido às dificuldades tecnológicas e as incompatibilidades entre padrões e fornecedores esta visão manteve-se limitada a experimentos. Entretanto a Internet das Coisas fornece meios que possibilitam chegar ainda mais perto da realização desta visão.

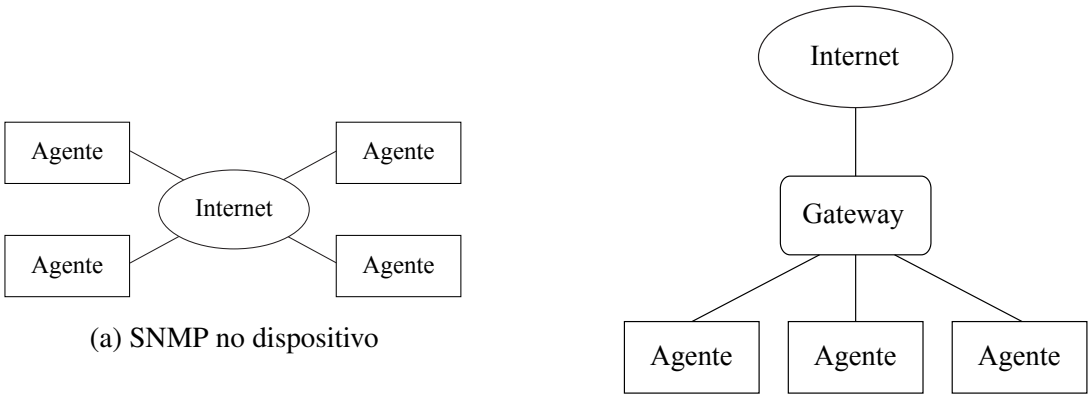
4.2 Arquitetura

Definidos os objetivos do trabalho, é necessária a criação de uma arquitetura que suporte seus objetivos, possibilitando reaproveitar as técnicas, protocolos e sistemas de gerência de redes e, ao mesmo tempo, empregá-los na gestão dos dispositivos em uma Internet das Coisas. Em um cenário ideal, com abundância de recursos, a tarefa em questão poderia ser solucionada de forma trivial, simplesmente incluindo os softwares de gerência de redes diretamente nos dispositivos.

Contudo, dados os recursos limitados dos dispositivos da Internet das Coisas, conforme detalhado por Bormann, Ersue e Keranen (2013), a execução de um agente SNMP no dispositivo deixa de ser uma tarefa trivial. Esforços como os de Choi, Kim e Cha (2009) e Kuryla (2010) demonstram que embutir um agente SNMP em um dispositivo para Internet das Coisas é possível, entretanto a implementação ocupa grande parte dos recursos do dispositivo, fazendo com que este seja incapaz de executar aplicações de usuário, efetivamente inutilizando-o.

Em contrapartida, os trabalhos de Steenkamp, Kaplan e Wilkinson (2009) e Zhu et al. (2010) sugerem o uso de um dispositivo dedicado a prover conectividade e interoperabilidade aos nós

Figura 5: Arquiteturas de Integração SNMP–IoT



(a) SNMP no dispositivo

(b) Gateway

Fonte: Elaborado pelo autor.

da rede, um *gateway*. Este dispositivo deve prover comunicação com a internet e servir como um tradutor, possibilitando a comunicação em diferentes protocolos, desta forma os dispositivos continuariam com suas aplicações de usuário intactas, concentrando o custo da tradução no *gateway*.

Cada modelo, seja de conectividade direta ou através de um *gateway*, ilustrados pela Figura 5, tem suas vantagens e desvantagens. Assim como a conectividade direta reduz o número de dispositivos envolvidos em uma ação e concentra um maior número de funcionalidades no dispositivo, seu preço é um aumento significativo na complexidade de implementação e na quantidade de recursos necessários. Da mesma forma o modelo com *gateway* impõem restrições e, principalmente, instaura um ponto único de falha na arquitetura enquanto provê facilidades como o controle centralizado e a possibilidade de aliviar as restrições de processamento da rede como um todo de maneira economicamente viável, aumentando os recursos de um único dispositivo ao invés de diluir este aumento entre todos os nós.

No contexto deste trabalho, direcionado à automação residencial, a arquitetura com *gateway* foi escolhida pois exige um menor número de alterações nos dispositivos já presentes e pelo fato de que é comum a presença de algum tipo de dispositivo com papel análogo ao do *gateway*, como um modem ou *set-top box* de televisão a cabo, e que poderia ser incorporado na solução proposta. É comum que tais dispositivos sejam baseados em micro–distribuições Linux, permitindo que o usuário possa incorporar a funcionalidade desejada diretamente no *gateway*. Distribuições como BusyBox, DD–WRT, OpenWRT e Tomato[1], específicas para esta classe de dispositivos, fornecem a infraestrutura necessária para a execução de aplicações de usuário como se estivessem em um ambiente nativo Linux. A arquitetura proposta contempla três elementos principais, sendo eles:

[1] Maiores informações podem ser encontradas diretamente nas páginas dos projetos, respectivamente: `http://www.busybox.net`, `http://www.dd-wrt.com`, `https://openwrt.org`, `http://www.polarcloud.com/tomato`.

- **Dispositivo Inteligente:** Qualquer dispositivo que disponha de conectividade e de uma API[2] para leitura e definição de informações e configurações a seu próprio respeito ou dos objetos aos quais ele se relaciona;

- ***Gateway*:** Um dispositivo com maior poder de processamento capaz de servir como intermediário e tradutor das comunicações entre dispositivos e gerentes, criando uma ponte entre os protocolos específicos de Internet das Coisas e de gerência de redes, neste caso o SNMP;

- **Gerente:** Aplicativo de gerência de redes capaz de utilizar o protocolo SNMP e, portanto, possa comunicar-se com o *gateway* de forma a gerenciar os dispositivos da Internet das Coisas.

4.3 Agrupamento de Dispositivos

A presença de um *gateway* entre a internet e os dispositivos permite que operações como filtrar e agregar dados sejam facilmente desempenhadas na rede. A existência de um grande número de dispositivos torna estas operações ainda mais desejáveis, uma vez que os dados de interesse podem encontrar-se apenas em um subconjunto dos dispositivos da rede, não fazendo sentido a obtenção desses dados de todos os integrantes da rede.

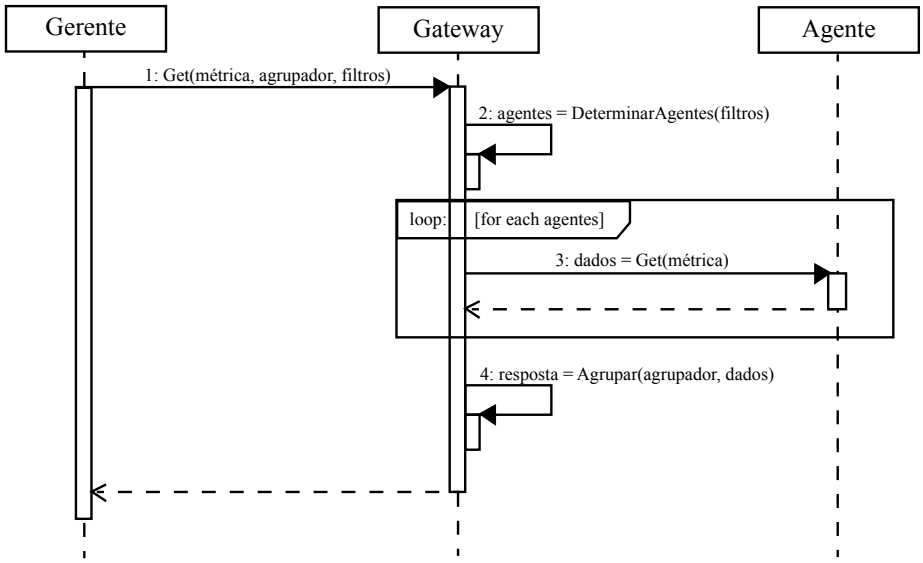
Há, então, a necessidade de uma maneira de agrupar conjuntos de dispositivos em entidades lógicas (denominadas, a partir de agora, grupos) e controladas pelo usuário, através do gerente. Possibilita-se, graças a esta funcionalidade, a classificação de um dispositivo ao associá-lo a um grupo que represente uma categoria, por exemplo ao classificar o dispositivo televisão à categoria eletrônico. Além de fazer parte de diferentes grupos, um dispositivo pode ser classificado de acordo com sua localização, estando na sala ou no quarto, por exemplo.

Entretanto esta classificação ainda apresenta-se limitada no contexto de automação residencial, uma vez que um televisor, por exemplo, pode pertencer a múltiplos grupos representando desde categorias (como eletrônico, áudio e vídeo) até sua localização (apartamento 203, quarto do João ou cozinha). Percebe-se, portanto, que este controle deve permitir a associação de um mesmo dispositivo a mais de um grupo simultaneamente, funcionando nos moldes das *tags*, ou etiquetas, popularizadas na internet.

Tal estratégia permite que um único dispositivo, representando um objeto, seja associado a mais de uma categoria, possibilitando uma descrição mais flexível e detalhada das propriedades deste objeto. Ainda com o exemplo do televisor, uma série de *tags* possíveis para a sua classificação seriam: eletrônico; áudio; vídeo; digital; apartamento 203; cozinha. Por intermédio das *tags* torna-se possível a realização de buscas filtradas de acordo com os grupos aos quais os dispositivos pertencem.

[2] Uma API, ou Interface de Programação de Aplicativos, é um conjunto de padrões e regras que estabelece a forma como ocorrerá a comunicação entre diferentes softwares.

Figura 6: Diagrama de uma requisição SNMP conforme a proposta



Fonte: Elaborado pelo autor.

Adicionalmente, de forma a melhor apresentar os resultados, cria-se a necessidade de agrupar os dados resultantes da busca. Operações de agrupamento como mínimo, máximo, e média (entre outras), podem ser usadas para representar o estado de toda uma classe de dispositivos e seus respectivos objetos, aumentando o poder de expressão das consultas. Como produto final da proposta, representado pela Figura 6, é criada a possibilidade de realizar consultas que abrangem todo um conjunto de dispositivos, filtrados por suas *tags* e com seus valores agrupados.

4.4 Validação

A proposta será validada através do seu efetivo uso em situações hipotéticas no contexto de automação residencial, conforme especificado no escopo da proposta. Tal avaliação será possível pois é objetivo deste trabalho a implementação de um *gateway* a título de protótipo, o que viabiliza a criação de um cenário real de comunicação entre dispositivos, sem necessitar do uso de simuladores.

Assim como definido na arquitetura, a avaliação contará, também, com três elementos principais, sendo eles:

- **Dispositivo Inteligente:** Um dispositivo que disponha de conectividade e utilize protocolos da Internet das Coisas, podendo assumir papéis como o de sensor, atuador, entre outros. Caso seja possível obter um dispositivo de uso específico para IoT planeja-se usá-lo na validação, contudo há grande dificuldade em encontrar estes dispositivos e, caso não seja possível, pretende-se emular seu comportamento em um dispositivo comum, como um PC por exemplo;

- **Gateway:** Um PC ou outro dispositivo com maior poder de processamento do que os Dispositivos Inteligentes, preferencialmente executando uma das distribuições Linux específicas para esta classe de dispositivos, como o OpenWRT, ou um ambiente Linux. Este dispositivo estará executando o protótipo da solução e deverá fornecer a comunicação tanto entre dispositivos inteligentes como gerentes, funcionando como uma ponte entre eles;

- **Gerente:** Aplicativo de gerência de redes que se comunique usando SNMP e executando em um PC. Nesta máquina não há restrições quanto a sistema operacional ou arquitetura, desde que o aplicativo de gerência a suporte. Não serão realizadas nenhum tipo de alterações no dispositivo gerente e seus softwares, executando versões disponibilizadas diretamente pelo fabricantes de forma a atestar a interoperabilidade da solução proposta, ou seja, seu funcionamento em um cenário de Internet das Coisas.

Uma vez montado um ambiente com todos os elementos acima descritos será possível avaliar o funcionamento do protótipo e, consequentemente, da proposta. Esta avaliação será realizada na forma de testes através do gerente da execução das diversas ações previstas na proposta como: adição e remoção de *tags*; execução de requisições com e sem filtros; execução de requisições com e sem critérios de agrupamento (como mínimo, máximo e média); e a execução de requisições padrão do SNMP. O sucesso na realização destas tarefas representa o sucesso da validação como um todo e, consequentemente, da ideia proposta por este trabalho.

5 PLANEJAMENTO DA IMPLEMENTAÇÃO

O desenvolvimento deste trabalho se dará conforme o cronograma apresentado pela Figura 7, tendo como principal atividade o desenvolvimento do protótipo de um software para o *gateway* IoT—SNMP. Observando-se de maneira mais ampla, o desenvolvimento pode ser detalhado com base nas seguintes etapas:

- **Artigo:** Assim como o protótipo do *gateway*, o artigo final compõe um dos entregáveis deste trabalho. Seu desenvolvimento se dará na segunda metade do tempo previsto em cronograma por depender das decisões, experiências e resultados do desenvolvimento do protótipo. Ao final da escrita do artigo, detalhando o acontecido no desenvolvimento da solução e os resultados encontrados, haverá a apresentação do mesmo para a banca avaliadora;

- **Análise:** Prevê-se logo no começo do tempo alocado em cronograma um período que compreenderá atividades de análise e planejamento do desenvolvimento. Entre as atividades previstas estão a definição de ambientes e linguagens de desenvolvimento, assim como as bibliotecas necessárias. Ainda nesta fase haverá um detalhamento técnico da solução proposta, visando seguir padrões de desenvolvimento de software e obter maior qualidade no resultado final que, mesmo em caráter de protótipo, pode ser útil à comunidade, tanto profissional quanto acadêmica;

- **Desenvolvimento:** Ocupando quase a metade do tempo previsto em cronograma, as atividades de desenvolvimento caracterizam a efetiva codificação e integração da solução proposta. Como produto final desta fase objetiva-se por obter um software capaz de executar em ambientes embarcados, predominantemente Linux, e desempenhar a função de

Figura 7: Cronograma da implementação

Atividades	janeiro	fevereiro	março	abril	maio	junho
Análise e planejamento da implementação						
Criação da MIB						
Desenvolvimento de um ou mais agentes com protocolos IoT						
Desenvolvimento da camada IoT do Gateway						
Desenvolvimento da camada SNMP do Gateway						
Desenvolvimento da camada de tradução de protocolos do Gateway						
Desenvolvimento dos módulos de filtro (tags) e agregação no Gateway						
Testes e validação da solução						
Artigo						
Entrega e apresentação do artigo						

Fonte: Elaborado pelo autor.

integrador entre redes da Internet das Coisas e ambientes de gerência de redes. Esta atividade foi dividida, no cronograma, em cinco outras atividades menores em termos dos principais componentes do protótipo, sendo eles: agente experimental em protocolo de IoT; camada de comunicação com protocolos de IoT; camada de comunicação com protocolo SNMP; camada de tradução entre os diferentes protocolos; e os módulos de filtro e agrupamento de requisições. Todas estas atividades são fundamentais para a obtenção do resultado esperado, ou seja, o protótipo de *gateway* IoT—SNMP;

- **MIB:** De forma a atingir os objetivos de filtro e agregação de valores das consultas SNMP, conforme detalhado na proposta deste trabalho, é necessário o desenvolvimento de uma MIB própria e criada especificamente para este fim. Assim como a análise, este é um dos passos iniciais e que definirá o rumo do restante do trabalho, merecendo especial atenção;

- **Validação:** A fim de comprovar a funcionalidade do protótipo, e, consequentemente, a viabilidade da proposta deste trabalho, está previsto o tempo de um mês ao fim do desenvolvimento. Neste momento serão realizados testes integrados em um ambiente que simule um contexto de automação residencial e permita, entre outros, avaliar as forças, as fraquezas e as oportunidades relativas a solução proposta.

REFERÊNCIAS

ACCENTURE. **Always on, always connected**: finding growth opportunities in an era of hypermobile consumers. [S.l.: s.n.], 2012.

ASHTON, K. **That 'Internet of Things' Thing**. Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: mai. 2013.

ASTRAHAN, M. M.; JACOBS, J. F. History of the Design of the SAGE Computer — The AN/FSQ-7. **IEEE Annals of the History of Computing**, [S.l.], v. 5, n. 4, p. 340—349, Oct. 1983.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: a survey. **Computer Networks**, [S.l.], v. 54, n. 15, p. 2787—2805, Oct. 2010.

BARAN, P. **On distributed communications**. Santa Monica: RAND Corporation, United States Air Force, 1964.

BEIGL, M.; GELLERSEN, H.-W.; SCHMIDT, A. Mediacups: experience with design and use of computer–augmented everyday artefacts. **Computer Networks**, [S.l.], v. 35, n. 4, p. 401—409, Mar. 2001.

BOOLE, G. **The Laws of Thought**. Cork: Prometheus Books, 2003. 424 p. (Great Books in Philosophy).

BORMANN, C.; ERSUE, M.; KERANEN, A. **Terminology for Constrained Node Networks**. [S.l.]: Active Internet–Draft, Internet Engineering Task Force (IETF)., 2013.

BRADLEY, J.; LOUCKS, J.; MACAULAY, J.; MEDCALF, R.; BUCKALEW, L. **BYOD**: a global perspective. [S.l.]: Cisco Internet Business Solutions Group (IBSG), 2012.

BROCK, D. L. **The Electronic Product Code (EPC)**: a naming scheme for physical objects. Cambridge: Auto–ID Center, 2001.

BUCKLEY, J. From RFID to the Internet of Things: pervasive networked systems. In: PERVASIVE NETWORKED SYSTEMS CONFERENCE, 2006, Brussels. **Proceedings...** [S.l.: s.n.], 2006. p. 32.

CARR, N. G. **The Shallows**: what the internet is doing to our brains. 1ª. ed. New York: W W Norton, 2010. 276 p.

CHOI, H.; KIM, N.; CHA, H. 6LoWPAN–SNMP: simple network management protocol for 6lowpan. In: IEEE INTERNATIONAL CONFERENCE ON HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS, 11., 2009, Seoul. **Proceedings...** IEEE, 2009. p. 305—313.

CLEMM, A. **Network management fundamentals**. 1ª. ed. Indianapolis: Cisco Press, 2006. 552 p.

COETZEE, L.; EKSTEEN, J. The internet of things-promise for the future? an introduction. In: IST-AFRICA CONFERENCE, 2011, Gaborone. **Proceedings...** IEEE, 2011. p. 1—9.

DING, J. **Advances in Network Management**. Boca Raton: Auerbach Publications, 2009. 390 p.

DUNKELS, A.; VASSEUR, J.-P. **IP for Smart Objects**. [S.l.]: Internet Protocol for Smart Objects (IPSO) Alliance, 2008.

ETSI. **Machine to Machine Communications**. Sophia Antipolis: European Telecommunications Standards Institute, 2010.

EVANS, D. **The Internet of Things**: how the next evolution of the internet is changing everything. [S.l.]: Cisco Internet Business Solutions Group (IBSG), 2011. (April).

FENG, K.; HUANG, X.; SU, Z. A network management architecture for 6LoWPAN network. In: IEEE INTERNATIONAL CONFERENCE ON BROADBAND NETWORK AND MULTIMEDIA TECHNOLOGY, 2011, Shenzhen. **Proceedings...** IEEE, 2011. p. 430—434.

FLOERKEMEIER, C.; RODUNER, C.; LAMPE, M. RFID Application Development With the Accada Middleware Platform. **IEEE Systems Journal**, [S.l.], v. 1, n. 2, p. 82—94, Dec. 2007.

FONSECA, J. **Metodologia da pesquisa científica**. Fortaleza: Universidade Estadual do Ceará, 2002. 127 p.

GELLERSEN, H.; KORTUEM, G.; SCHMIDT, A.; BEIGL, M. Physical prototyping with smart–its. **IEEE Pervasive Computing**, [S.l.], v. 3, n. 3, p. 74—82, 2004.

GERHARDT, T.; SILVEIRA, D. **Métodos de Pesquisa**. 1ª. ed. Porto Alegre: UFRGS, 2009. 120 p. (Educação a Distância).

GIL, A. C. **Como elaborar projetos de pesquisa**. 4ª. ed. São Paulo: Atlas, 2007. 176 p.

GILDER, G. **Ten Laws Of The Telecosm Redux**. Disponível em: <`http:` `//www.forbes.com/2007/01/09/telecosm-jdsu-intel-pf-soapbox-in_gg_0109soapbox_inl_print.html`>. Acesso em: jun. 2013.

GOMEZ, C.; PARADELLS, J. Wireless home automation networks: a survey of architectures and technologies. **IEEE Communications Magazine**, [S.l.], v. 48, n. 6, p. 92—101, June 2010.

HADA, H.; MITSUGI, J. EPC based internet of things architecture. In: IEEE INTERNATIONAL CONFERENCE ON RFID–TECHNOLOGIES AND APPLICATIONS, 2011, Sitges. **Proceedings...** IEEE, 2011. p. 527—532.

HEWLETT-PACKARD. **CeNSE**. Disponível em: <`http:` `//www8.hp.com/us/en/hp-information/environment/cense.html`>. Acesso em: nov. 2013.

HEWLETT-PACKARD. **A holistic approach to your BYOD challenge**. Austin: Hewlett–Packard Development Company, 2013.

HOLMQUIST, L. E.; GELLERSEN, H.; KORTUEM, G.; SCHMIDT, A.; STROHBACH, M.; ANTIFAKOS, S.; MICHAHELLES, F.; SCHIELE, B.; BEIGL, M.; MAZE, R. Building intelligent environments with smart–its. **IEEE Computer Graphics and Applications**, [S.l.], v. 24, n. 1, p. 56—64, 2004.

HUNG, L.; MAHONEY, J. **Hype Cycle for Big Data**: internet of things. [S.l.]: Gartner, 2012. 101 p.

HUNT, R. SNMP, SNMPv2 and CMIP — the technologies for multivendor network management. **Computer Communications**, [S.l.], v. 20, n. 2, p. 73—88, Mar. 1997.

ISO. **ISO/IEC 7498-4**:1989. Geneva: International Organization for Standardization, 1989.

ITU. **The Internet of Things**. Geneva: International Telecommunication Union, 2005.

KAKU, M. **The Intelligence Revolution**. [S.l.]: BBC Four, 2007.

KORTUEM, G.; KAWSAR, F.; FITTON, D.; SUNDRAMOORTHY, V. Smart objects as building blocks for the Internet of things. **IEEE Internet Computing**, [S.l.], v. 14, n. 1, p. 44—51, Jan. 2010.

KURYLA, S. **Implementation and Evaluation of the Simple Network Management Protocol over IEEE 802.15.4 Radios under the Contiki Operating System**. 2010. 46 p. Dissertação (Mestrado em Ciência da Computação) — Jacobs University, 2010.

LEINWAND, A.; CONROY, K. F. **Network management**: a practical perspective. 2ª. ed. San Jose: Addison–Wesley, 1996. 338 p. (UNIX and open systems series).

LIU, Y.; ZHOU, G. Key Technologies and Applications of Internet of Things. In: FIFTH INTERNATIONAL CONFERENCE ON INTELLIGENT COMPUTATION TECHNOLOGY AND AUTOMATION, 2012, Zhangjiajie. **Proceedings...** IEEE, 2012. p. 197—200.

MATTERN, F.; FLOERKEMEIER, C. From the Internet of Computers to the Internet of Things. In: SACHS, K.; PETROV, I.; GUERRERO, P. (Ed.). **From Active Data Management to Event–Based Systems and More**. [S.l.]: Springer, 2010. n. 2, p. 242—259. (LNCS, v. 6462).

MAURO, D.; SCHMIDT, K. **Essential SNMP**. 2ª. ed. [S.l.]: O'Reilly Media, 2009. 462 p.

MOORE, G. Cramming More Components Onto Integrated Circuits. **Proceedings of the IEEE**, [S.l.], v. 86, n. 1, p. 82—85, Jan. 1998.

MOTOROLA. **BYOD**: bring your own device. [S.l.]: Motorola Solutions, Inc, 2011.

PAVENTHAN, A.; ALLU, S.; GAYATHRI, V.; BARVE, S.; RAM, N. Leveraging CoAP towards monitoring agriculture sensors network. In: INTERNATIONAL CONFERENCE ON WIRELESS COMMUNICATION AND SENSOR NETWORKS, 8., 2012, Phitsanulok. **Proceedings...** [S.l.: s.n.], 2012. p. 6.

PERERA, C.; ZASLAVSKY, A.; CHRISTEN, P.; GEORGAKOPOULOS, D. Context Aware Computing for The Internet of Things: a survey. **IEEE Communications Surveys & Tutorials**, [S.l.], v. PP, n. 99, p. 41, 2013.

PERKINS, D. T.; MCGINNIS, E. **Understanding SNMP MIBs**. [S.l.]: Prentice Hall, 1996. 528 p.

REGISTER, T. **Salesforce**: internet of things is 'third wave of computing'. Disponível em: <http://www.theregister.co.uk/2013/04/23/salesforce_gets_social/>. Acesso em: mai. 2013.

SAKTHIDHARAN, G. R.; CHITRA, S. A survey on wireless sensor network: an application perspective. In: INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATION AND INFORMATICS, 2012, Coimbatore. **Proceedings...** IEEE, 2012. p. 1—5.

SHANNON, C. E. A mathematical theory of communication. **ACM SIGMOBILE Mobile Computing and Communications Review**, New York, v. 5, n. 1, p. 3, Jan. 2001.

SILVA, E. L. da; MENEZES, E. M. **Metodologia da Pesquisa e Elaboração de Dissertação**. 4ª. ed. Florianópolis: UFSC, 2005. 138 p.

SILVA, J. M. A. da. **Construção de Agentes SNMP em ambiente Linux**. 2005. 114 p. Dissertação (Mestrado em Ciência da Computação) — Universidade Federal de Lavras, 2005.

SIMONEAU, P. **SNMP Network Management**. New York: McGraw–Hill, 1999. 477 p.

SIMPSON, J.; WEINER, E. **Oxford English Dictionary**. 3ª. ed. New York: Oxford University Press, 2005. 22000 p.

SMITH, I. G. **The Internet of Things 2012**: new horizons. Halifax: CASAGRAS2, 2012. 360 p.

STALLINGS, W. SNMPv3: a security enhancement for snmp. **IEEE Communications Surveys & Tutorials**, [S.l.], v. 1, n. 1, p. 2—17, 1998.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2**. 3ª. ed. Boston: Addison—Wesley, 1999. 619 p.

STEENKAMP, L. d. T.; KAPLAN, S.; WILKINSON, R. H. Wireless sensor network gateway. In: AFRICON, 2009, Nairobi. **Proceedings...** IEEE, 2009. p. 1—6.

SUHONEN, J. **Designs for the Quality of Service Support in Low–Energy Wireless Sensor Network Protocols**. 2012. 112 p. Tese (Doutorado em Ciência da Computação) — Tampere University of Technology, 2012.

SUNDMAEKER, H.; GUILLEMIN, P.; FRIESS, P.; WOELFFLé, S. **Vision and challenges for realising the Internet of Things**. 1ª. ed. Belgium: European Union, 2010. 230 p.

SUNG, J.; LOPEZ, T. S.; KIM, D. The EPC Sensor Network for RFID and WSN Integration Infrastructure. In: ANNUAL IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, 5., 2007, White Plains. **Proceedings...** IEEE, 2007. p. 618—621.

TURCK, M. **Making Sense Of The Internet Of Things**. Disponível em: <http://techcrunch.com/2013/05/25/making-sense-of-the-internet-of-things/>. Acesso em: mai. 2013.

TURING, A. M. On Computable Numbers, with an Application to the Entscheidungsproblem. **Proceedings of the London Mathematical Society**, London, v. s2–42, n. 1, p. 230—265, Jan. 1937.

Von Neumann, J. **First draft of a report on the EDVAC**. Los Alamos: Los Alamos National Laboratory, 1945.

WANG, Q.; JÄNTTI, R.; ALI, Y. On Network Management for the Internet of Things. In: SWEDISH NATIONAL COMPUTER NETWORKING WORKSHOP, 8., 2012, Stockholm. **Proceedings...** [S.l.: s.n.], 2012. p. 4.

WANT, R. An Introduction to RFID Technology. **IEEE Pervasive Computing**, [S.l.], v. 5, n. 1, p. 25—33, Jan. 2006.

WANT, R.; FISHKIN, K. P.; GUJAR, A.; HARRISON, B. L. Bridging physical and virtual worlds with electronic tags. In: SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS THE CHI IS THE LIMIT, 1999, New York, New York, USA. **Proceedings...** ACM Press, 1999. p. 370—377.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier, 2008. 155 p.

WEISER, M. The Computer for the 21st Century. **Scientific American**, [S.l.], v. 265, n. 3, p. 94—104, Sept. 1991.

WELBOURNE, E.; BATTLE, L.; COLE, G.; GOULD, K.; RECTOR, K.; RAYMER, S.; BALAZINSKA, M.; BORRIELLO, G. Building the Internet of Things Using RFID: the rfid ecosystem experience. **IEEE Internet Computing**, [S.l.], v. 13, n. 3, p. 48—55, May 2009.

ZDNET. **BYOD and the Consumerization of IT**. Disponível em: <`http:` `//www.zdnet.com/topic-byod-and-the-consumerization-of-it/`>. Acesso em: jun. 2013.

ZHANG, H.; ZHU, L. Internet of Things: key technology, architecture and challenging problems. In: IEEE INTERNATIONAL CONFERENCE ON COMPUTER SCIENCE AND AUTOMATION ENGINEERING, 2011, Shanghai. **Proceedings...** IEEE, 2011. p. 507—512.

ZHU, Q.; WANG, R.; CHEN, Q.; LIU, Y.; QIN, W. IOT Gateway: bridgingwireless sensor networks into internet of things. In: IEEE/IFIP INTERNATIONAL CONFERENCE ON EMBEDDED AND UBIQUITOUS COMPUTING, 2010, Hong Kong. **Proceedings...** IEEE, 2010. p. 347—352.