UNIVERSIDADE ESTADUAL DE CAMPINAS
Faculdade de Tecnologia

JOSÉ ROBERTO EMILIANO LEITE

MODELAGEM E SIMULAÇÃO DE REDES IoT, AdHoc E RFID

LIMEIRA
2019

JOSÉ ROBERTO EMILIANO LEITE

MODELAGEM E SIMULAÇÃO DE REDES IoT, AdHoc E RFID

Tese de Doutorado apresentada à Faculdade de Tecnologia da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Doutor em Tecnologia, na Área de Sistemas de Informação e Comunicação.

Orientador: Prof. Dr. Edson Luiz Ursini

Coorientador: Prof. Dr. Paulo Sérgio Martins Pedro

Este exemplar corresponde à versão final da Tese defendida por José Roberto Emiliano Leite e orientado pelo Prof. Dr. Edson Luiz Ursini.

LIMEIRA
2019

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca da Faculdade de Tecnologia
Felipe de Souza Bueno - CRB 8/8577

L533m

Leite, José Roberto Emiliano, 1956-
Modelagem e simulação de redes IoT, AdHoc e RFID / José Roberto Emiliano Leite. – Limeira, SP : [s.n.], 2019.

Orientador: Edson Luiz Ursini.
Coorientador: Paulo Sérgio Martins Pedro.
Tese (doutorado) – Universidade Estadual de Campinas, Faculdade de Tecnologia.

1. Detectores. 2. Internet das coisas. 3. Redes ad hoc (Redes de computadores). 4. Sistemas de identificação por radiofrequência. 5. Simulação (Computadores). I. Ursini, Edson Luiz, 1951-. II. Martins Pedro, Paulo Sérgio, 1967-. III. Universidade Estadual de Campinas. Faculdade de Tecnologia. IV. Título.

Informações para Biblioteca Digital

Título em outro idioma: Modeling and simulation of IoT, AdHoc and RFID networks
Palavras-chave em inglês:
Detectors
Internet of things
Ad hoc networks (Computer networks)
Radio frequency identification systems
Computer simulation
Área de concentração: Sistemas de Informação e Comunicação
Titulação: Doutor em Tecnologia
Banca examinadora:
Edson Luiz Ursini [Orientador]
Tânia Regina Tronco
Kalinka Regina Lucas Jaquie Castelo Branco
Leonardo Lorenzo Bravo Roger
Rangel Arthur
Data de defesa: 14-11-2019
Programa de Pós-Graduação: Tecnologia

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-8368-7388
- Currículo Lattes do autor: http://lattes.cnpq.br/2752503087387960

Folha de Aprovação

Abaixo se apresentam os membros da comissão julgadora da sessão pública de defesa de tese para o Título de Doutor em Tecnologia na área de concentração de Sistemas de Informação e Comunicação, a que submeteu o aluno José Roberto Emiliano Leite, em 14 de novembro de 2019 na Faculdade de Tecnologia FT/UNICAMP, em Limeira/SP.

Prof. Dr. Edson Luiz Ursini
Presidente da Comissão Julgadora

Prof. Dra. Tânia Regina Tronco

Prof. Dra.Kalinka Regina Lucas Jaquie Castelo Branco
USP São Carlos

Prof. Dr. Leonardo Lorenzo Bravo Roger
FT UNICAMP

Prof. Dr. Rangel Arthur
FT UNICAMP

Ata da defesa de Tese de Doutorado, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Tese de Doutorado e na Secretaria de Pós-Graduação da FT.

Agradecimentos

Agradeço a Deus pela conclusão desta jornada.

Agradeço à minha família (Selma, Danieli e Lucca) pelo apoio e compreensão, sendo fonte de motivação e inspiração.

Agradeço à UNICAMP e à FT pela oportunidade desta pesquisa de doutorado.

Agradeço a meus orientadores, Ursini e Paulo, pela orientação, esforço e colaboração na preparação dos artigos publicados.

Agradeço também a meus colegas de curso, Roberto Belli/Flávio Massaro/Vlademir Santos/Loreno Menezes/Rafael Neto/Max/Swift, pela ajuda e atenção dispensada nas matérias e nos documentos gerados.

José Roberto Emiliano Leite

Resumo

A Internet inicialmente possibilitou a comunicação de pessoas e computadores, estabelecendo-se como uma "rede de redes" e uma ferramenta de comunicação global. O barateamento e a diminuição no tamanho dos componentes de acesso à Internet permitiram que equipamentos e dispositivos simples do nosso cotidiano também tivessem acesso a essa rede (incluindo TV, refrigeradores, fogões, sistemas de ar-condicionado, alarmes residenciais, lâmpadas e carros); apareceu assim a Internet das Coisas (IoT) permitindo o incremento de inteligência em diversos setores da economia. Este documento apresenta o referencial teórico desse novo ambiente de rede em termos de Arquiteturas, Modelos, Tecnologias, Protocolos e Aplicações, incluindo a Revisão Bibliográfica com as novas e recentes pesquisas na área e a identificação de pontos críticos de desempenho que devem ser otimizados, preocupado com o alto volume de objetos conectados. O objetivo desta tese é criar um Modelo de Rede IoT usando a Simulação Hibrida Incremental por meio de Ferramentas de Software ARENA, MATLAB e Visual Basic.

Construiu-se um Modelo de Rede IoT/AdHoc/RFID genérico, usando uma simulação por eventos discretos (DES), o qual foi validado por Redes de Jackson, e quantitativamente apresentado por meio de 13 cenários e casos de estudo de diversas condições. O modelo e sua implementação servem como base para a análise de diversas condições que podem apoiar o projeto, planejamento, dimensionamento e evolução das futuras Redes IoT, no que diz respeito a congestionamento de tráfego. Para redes existentes, o modelo pode também ser usado para detecção ou até predição de gargalos futuros na rede IoT, ajudando assim no investimento estratégico de empresas.

Especificamente, os 13 cenários apresentados de simulação, consideram Validações Incrementais, Validação Analítica do Modelo, nós congestionados e não congestionados, mensagens com e sem prioridades, Otimização de Roteamento em VANET usando Monte Carlo e Perda de Mensagens usando os modelos de mobilidade *Two-Ray Propagation* e *Random Way Point*. O objetivo dos cenários é analisar o tráfego no equipamento Mediador para estimar sua capacidade, considerando diversos tipos de aplicações: Redes de Ambientes de Catástrofe, Dimensionamento de Redes IoT, Redução do Consumo de Energia na Rede e no Campus Universitário, Sistema de Transporte Inteligente ITS (*Smart City*) usando VANET, Gerenciamento do Mediador, Redes para Recuperação de Desastres considerando confiabilidade/disponibilidade dos nós processadores e enlaces.

Objetivamos com esses cenários determinar a Perda de Conectividade, Utilização dos Processadores e Atrasos nas Mensagens da Rede IoT. Os resultados ilustram como se pode usar o modelo para estudar o balanceamento de tráfego, a otimização de roteamento e a priorização de mensagens que são relevantes para o uso efetivo da rede.

Abstract

INTERNET, initially enabling the communication of people and computers, established itself as a network and a global communication tool. The cheapness and the decrease in size of Internet access components led to simpler equipment and devices of our everyday lives to access a broader network (including TV, refrigerators, cookers, conditioned air systems, residential alarms, lamps, and cars); then Internet of Things (IoT) has appeared to allow the increment of intelligence in the various sectors of the economy. This thesis presents this new network environment in terms of Architectures, Models, Technologies, Protocols and Applications, regarding the Bibliography Review with the recent and new researches in the area and the performance and identification of critical points that should be optimized, concerning the high volume of connected objects. The methodology to be used includes the creation of the IoT Network Simulation Model, using the ARENA/MATLAB/VISUAL BASIC Software tools.

We built a discrete-event simulation model of an IoT/AdHoc/RFID Network, which was analytically validated by Jackson networks, and quantitatively showed through 13 scenarios/case studies. The model and its implementation serve as the basis for the analysis of several conditions that may support the design, planning and dimensioning of future IoT networks regarding traffic congestion. For existing networks, it may also be used for detection or even prediction of future bottlenecks.

Specifically, the 13 simulation scenarios presented, considering congested and uncongested nodes, messages with and without priorities, and including routing optimization and message losses by using also Two-ray propagation and Random Way Point (mobility) models. The goal is to analyze the traffic of the mediator to estimate its capacity considering several kinds of applications: Smart City, ITS, Catastrophe, Energy Consumption and Network Management. We aim at determining the processor utilization and message delays in the Mediator. The results showed that balancing traffic, routing optimization and prioritization of messages are relevant to the effective resource usage of the network.

Lista de Ilustrações

Lista de Tabelas

Lista de Abreviaturas e Siglas

a) Órgãos Internacionais de Padronização
ITU-T : *International Telecommunication Union - Standardization Sector* (Telecomunicações)
ISO : *International Standardization Organization* (Informática)
IEC : *International Electrotechnical Commission*
IETF : *Internet Engineering Task Force* (Internet)
IDA : *International Digital Asset Management*
EPC-Global : Padronização RFID
IEEE : Instituto de Engenheiros Eletricistas e Eletrônicos

b) Arquitetura TCP/IP
IP : *Internet Protocol*
TCP : *Transmission Control Protocol*
UDP : *User Datagram Protocol*
SNMP : *Simple Network Management Protocol*
CMIP : *Control Management Protocol*
IPSEC : *IP Security*
IPV4 : Endereçamento IP de 32 bits
IPV6 : Endereçamento IP de 128 bits
MAC : *Media Access Control*
MIMO : *Multiple-Input Multiple-Output*
SSL : *Secure Sockets Layer*
RFC : *Request for Comments*
TLS : *Transport Layer Security*

c) Protocolos WEB
WWW : *World Wide Web*
http : *Hyper Text Transfer Protocol*
https : *Hyper Text Transfer Protocol Secure* (HTTP + SSL)
CBOR : *Concise Binary Object Representation*
CA : Autoridade Certificadora
XML : *Extensible Markup Language*
JSON : *Java Script Object Notation* (formato de troca de dados)
SaaS/IaaS/PaaS (Modelos de Serviços de TI para nuvem) : *Software as a Service*, *Infrastructure as a Service*, *Plataform as a Service*)
Protocolos WEB Restritos em CPU/Memória : COAP (*Constrained Application Protocol*), MQTT , AMQP, CBOR.
MIB : *Management Information Base*
TMN : Rede de Gerência de Telecomunicações

d) Tecnologias
RFID : *Radio Frequency Identification*
WSN : *Wireless Sensor Network*
6LowPAN (*IPv6 over Low-Power Wireless Personal Area Networks*)
GPS : *Global Positioning System*
PLC : *Power Line Communication (Smart Grid)*
UPS : *Uninterruptible Power Supply*

e) Internet das Coisas
IoT *: Internet of Things*
OSI : *Open Systems Interconnection*
RWP : *Random Way Point (Mobility Model)*
DES : *Discrete Event Simulation*
QoS : *Quality of Service*
PAS : Ponto de Acesso ao Serviço

f) Tipos de Redes AdHoc
MANET : *Mobile AdHoc Network*
VANET : *Vehicular AdHoc Network*
FANET : *Flying AdHoc Network*

g) Hierarquia de Redes
PAN : *Personal Area Network*
LAN : *Local Area Network*
MAN : *Metropolitan Area Network*
WAN : *Wide Area Network*

Sumário

Capítulo 1: Introdução

A Internet [1] consagrou-se como sendo uma "Rede de Redes" e uma ferramenta de comunicação globalizada, inicialmente possibilitando a ligação entre pessoas e entre pessoas e computadores (máquinas). Foi criada nos anos 60 com o objetivo de interligar os ambientes acadêmicos e de pesquisas; com seu crescimento, a Internet foi expandida para a área comercial, aumentando ainda mais o seu uso com o surgimento da forma de busca WEB (WWW) e das redes sociais. Atualmente, é impossível imaginarmos nossa vida sem o uso da Internet, das redes sociais e comerciais.

O barateamento e a diminuição do tamanho dos componentes de acesso à Internet possibilitaram que equipamentos e aparelhos mais simples de nosso cotidiano pudessem também acessar a rede global (TV, geladeira, fogão, ar-condicionado, alarmes residenciais, lâmpadas, automóveis, aparelhos hospitalares); surgiu então a Internet das Coisas (IoT). Essa nova forma de utilização da Internet visa interligar aparelhos de uso cotidiano, executando assim uma comunicação entre coisas/objetos/aparelhos, possibilitando uma maior automatização do nosso cotidiano, por meio do uso do acesso celular. Possibilita também o incremento de inteligência em diversos setores da economia: *Smart Grid* (Setor Elétrico), *City, Building, House,* Logística, Indústria, Hospital, Saúde e Automatização Comercial (atacado e varejo), dentre outros. A inteligência e a automação são decorrentes dos acréscimos de processamento, memória e comunicação nos objetos envolvidos.

A IoT realiza uma nova transformação digital, conectando dispositivos, incrementando valores de negócios, redefinindo organizações e gerando enorme quantidade de oportunidades. Sem dúvida, esta é uma nova onda tecnológica criando uma nova fronteira do mundo conectado com as pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais, todos conectados e capazes de interagirem entre si.

Novas tecnologias de acesso foram selecionadas pela IoT visando baratear e potencializar o uso da rede: RFID (Radio Frequency Identification), Rede de Sensores, WiFi, ZIGBEE e Bluetooth.

O conceito de Internet das Coisas (IoT) foi introduzido por Kelvin Ashton em 1999 como resultado de sua pesquisa para utilizar Etiquetas Eletrônicas RFID (*Radio-Frequency Identification*) na cadeia de produção [1]. Adicionalmente, foi introduzida a utilização de sensores e atuadores, apesar de suas restrições de energia, processamento e memória. Com o avanço da microeletrônica, o preço das interfaces de redes diminuiu e seu tamanho físico também, viabilizando a introdução de telecomunicações nesses objetos, tornando-os assim "Objetos Inteligentes e Conectados". Dessa maneira, a Internet globalizada passou a incorporar os objetos inteligentes, surgindo assim a Internet das Coisas (IoT), com a arquitetura em camadas mostradas na Figura 1. Essa arquitetura divide a comunicação em camadas de sensoriamento, rede, serviço e interface, com seus respectivos elementos.

Órgãos internacionais especificaram a padronização internacional aberta, visando a interconexão de objetos e sistemas heterogêneos, de qualquer tipo, modelo e fabricante: IoT-A (Padronização IoT), EPCglobal (Padronização RFID), IPSO (Padronização de Objetos Inteligentes), IEEE (Engenharia), 3GPP (Telefones Móveis), ITU-T (Telecomunicações),

IEC/ISO e IETF (Padronização Internet). A IoT já possui vasto conhecimento documentado em livros e padrões internacionais [1] [2] [3] [4] [5].

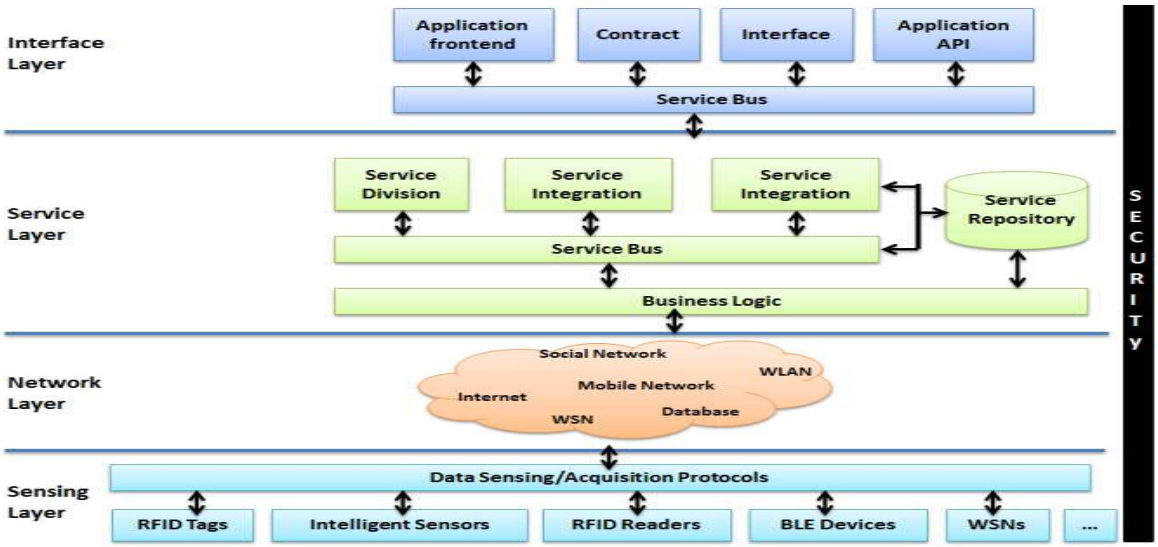

Figura 1 : Arquitetura IoT em Camadas, extraída de [15]

Foi mantida a nomenclatura inglesa para ficar compatível com as normas internacionais. Algumas tabelas e figuras estão em Inglês por serem dos Documentos de Padronização Internacionais e dos artigos já publicados. Muitas pesquisas e trabalhos de teses já foram desenvolvidos, principalmente em redes de sensores para monitoração ambiental [6].

Neste capítulo aborda-se o problema a ser estudado, os objetivos da tese, a metodologia utilizada, a visão geral da tese e a organização do documento.

1.1) O Problema

Apesar do volume de informação normalmente gerado individualmente por um sensor ou etiquetas RFID poder ser baixo (e.g. se comparado com tráfego de arquivos e multimídia em redes de alto nível), ocorre um alto congestionamento de tráfego no mediador que concentra todo tráfego das informações geradas por um grande número de sensores, etiquetas RFID e redes de sensores. Outros sensores, e.g. câmeras e sensores de amostragem de alta taxa, podem tornar esse tráfego ainda mais intenso. Portanto, **precisa-se estudar o tráfego (congestionamento/atraso) na rede para avaliar e dimensionar a capacidade do mediador, visando um bom desempenho na rede como um todo.**

Este panorama constitui-se em um desafio de pesquisa, haja visto que a IoT é um conjunto de " redes de computadores" relativamente novo que traz à tona novos elementos de projeto tais como:

- mobilidade aleatória dos nós (e de alta velocidade em alguns casos);
- a "clusterização (agrupamento)" dos nós;

- inexistência de nós centralizados (AdHoc);
- perdas de conectividade devido à relativa baixa potência de transmissão e propagação;
- heterogeneidade do tráfego e dos nós, e
- poucos recursos operacionais tais como dispositivos operados por bateria, baixa capacidade de transmissão e processamento dos nós.

Portanto, **a tese deste trabalho é de que:**

"*É possível modelar, simular, e avaliar o desempenho de uma Rede IoT incluindo AdHoc e RFID, no que tange ao tráfego e capacidade dos nós, considerando-se mobilidade, agrupamento, descentralização e escassez de recursos computacionais que caracterizam esses sistemas"*.

A defesa desta tese, mediante o estudo do tráfego (congestionamento/atraso) e a avaliação/dimensionamento da capacidade do Mediador, usando a modelagem e a simulação, pode prover ferramentas essenciais para o adequado gerenciamento, planejamento e administração de tráfego.

Dentro deste contexto, para subsidiar o argumento desta tese, neste trabalho foram propostos e analisados **13 cenários** envolvendo: Redes de Ambientes de Catástrofe, Incremento de Mobilidade, Dimensionamento de Redes IoT, Validações Incrementais, Redução do Consumo de Energia na Rede e no Campus Universitário, Sistema de Transporte Inteligente usando VANET, Validação Analítica do Modelo, Gerenciamento do Mediador, Redes para Recuperação de Desastres, Otimização de Roteamento em VANETs e confiabilidade/disponibilidade dos nós processadores e enlaces.

1.2) Objetivos

O objetivo desta tese é **desenvolver um Modelo de Simulação de Rede de Telecomunicações IoT com a RFID e Rede de Sensores AdHoc**, utilizando uma simulação de eventos discretos com teoria de filas, visando a localização de pontos críticos de comunicação que precisarão ser otimizados. Essa comunicação na rede IoT é dividida em camadas conforme mostrada na Figura 1, visando diminuir a complexidade existente.

A contribuição principal desta tese é oferecer um inovador Modelo de Simulação Híbrido Incremental de Rede de Eventos Discretos (DES) que inclui Redes IoT (Sensores, Etiquetas e Leitores RFIDs, Redes AdHoc e Redes RFID), com diversas aplicações típicas. É híbrido pelo fato de juntar Modelos de Mobilidade (Two-ray e RWP), Modelo Analítico de Jackson, Priorização de Mensagens IP e Otimização de Roteamento com Monte Carlo. É incremental pelo fato de adicionar funcionalidades pouco-a-pouco, usando diversos cenários e casos de estudo.

Modelos de Simulação têm uma grande demanda atualmente para Redes AdHoc e IoT, que são redes novas e estão sendo implantadas, e assim requerem projeto, planejamento e dimensionamento. Uma vez implantadas, as ferramentas de simulação e análise, podem modelar o tráfego em redes de dados, descobrindo pontos críticos de gargalo e qual melhor

solução pode ser usada na sua evolução. São também elementos críticos de suporte na tomada de decisão em planejamento estratégico. O desempenho dos dispositivos que compõem as Redes AdHoc, RFID e IoT são dependentes da quantidade de tráfego, medido em Erlang, e no congestionamento de tráfego nesses dispositivos, os quais são diretamente relacionados com as variações da utilização da rede. Quanto maior o congestionamento, maior o atraso dos pacotes e a lentidão da rede, devido ao custo de retransmissão e mecanismos de recuperação de erro que são utilizados quando a rede está sobrecarregada. O Modelo de Rede IoT com simulação híbrida ajuda a projetar e dimensionar a rede IoT, contendo : Eventos Discretos, Mobilidade(RWP, Two-Ray), Otimização de Monte Carlo, Lógicas Fuzzy e de Predição, Integração com Ferramentas MATLAB e VISUAL BASIC e Tratamentos Estatísticos (Replicações, Intervalos de Confiança - Margem de Segurança). Essas ferramentas foram utilizadas em 13 Cenários e Casos de Estudo.

A comunicação na rede IoT com tecnologia RFID, também é dividida em camadas [1] conforme mostrada na Fig. 2, visando diminuir a complexidade existente. Os eventos "E" ocorrem nas tags RFID; as informações das tags são enviadas ao seu respectivo Leitor que reenvia ao Mediador e posteriormente às aplicações.

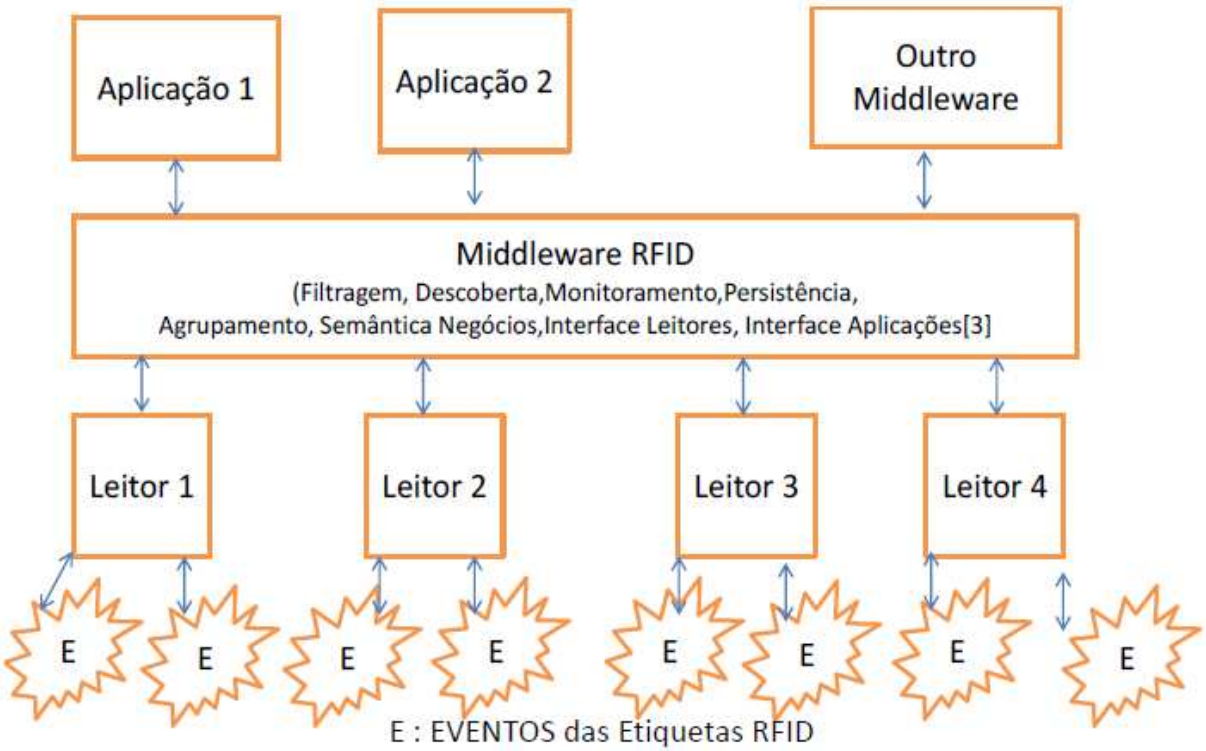

Figura 2 : Implementando RFID na cadeia de negócio [1]

Os equipamentos de rede mais sobrecarregados são aqueles que concentram o tráfego : Mediador, *Gateway* Inter Sub-redes, Internet e Aplicações. Para evitar os gargalos é necessário escalar com mais processadores esses equipamentos e elementos.

1.3) Metodologia

O objetivo desta tese é desenvolver um novo Modelo de Rede de Internet das Coisas, simulado por meio de estruturas de filas, contemplando comportamentos estatísticos, através

do uso do Software por eventos discretos ARENA. Esse modelo ajuda a descobrir e otimizar os caminhos críticos existentes nessa rede.

Os elementos participantes deste experimento de simulação são: Etiquetas RFID, Leitores RFID, Sensores, Rede de Sensores, Redes Adhoc, Mediador, Internet, Aplicações e Banco de Dados, trabalhando em um cenário simulado de Redes IoT focadas em "Monitoração Remota de Informação", usando o Software de Simulação ARENA rodando em Servidor da FT UNICAMP.

O experimento é quantitativo e relaciona as variáveis dependentes (Saída : Parâmetros de Qualidade de Serviço QoS relevantes, ou seja : Vazão (throughput), Largura de banda necessária, Latência ou Atraso de Transferência, Variação do Atraso (Jitter) e Taxa de Perda de Pacotes, às Variáveis Independentes (Entrada : Quantidade de Entradas, Tempo Entre Chegadas com respectiva Distribuição Estatística (Etiquetas RFID, Sensores e Redes de Sensores)) controlado pelas Variáveis de Controle (Usar ou não Solução de Nuvem, Segurança e Banco de Dados).

O Modelo inicial de Simulação em ARENA é mostrado na Fig. 3 que segue, contemplando os 3 Tipos de Variáveis de Entrada: Etiquetas RFID, Sensores Sem Fio e Redes de Sensores sem Fio. Adicionalmente, temos Leitor de *Tags* RFID, Mediador, Internet, Aplicações.

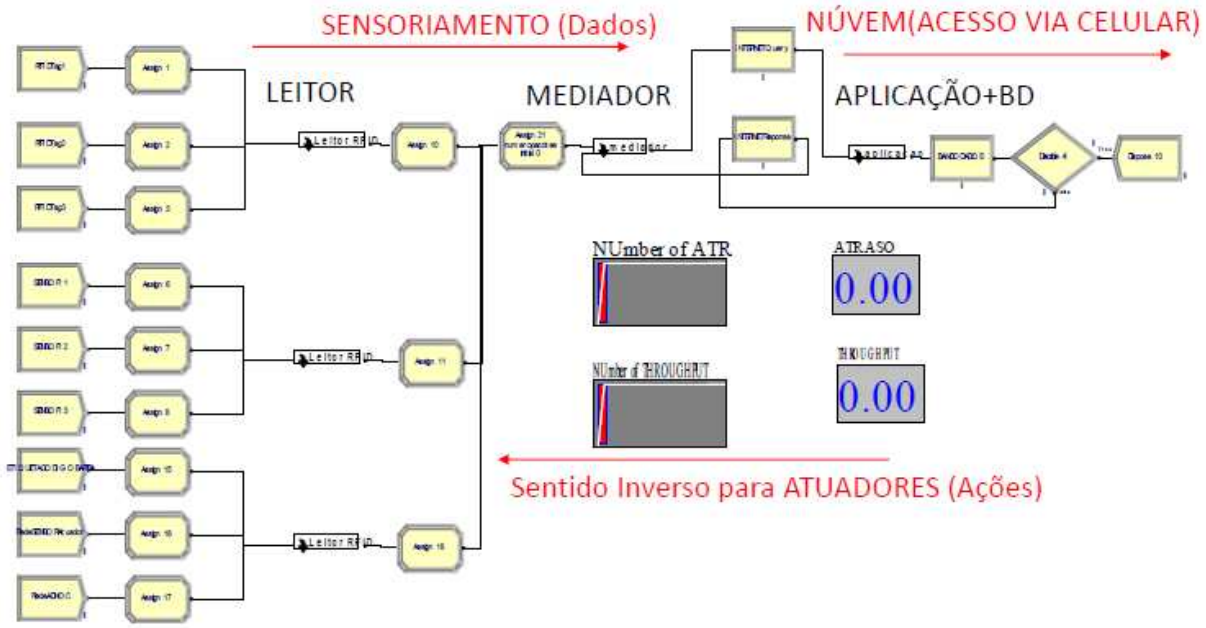

Figura 3: Modelo de Simulação da Integração da IoT com a RFID.

A Metodologia de Análise de Desempenho, para o Cenário de Redução do Consumo de Energia, pode ser vista com mais detalhe na Seção 5.6 Cenário #6.

O Congestionamento de Tráfego é relevante no projeto de dispositivos dependentes de bateria e redes, pelo fato das redes sofrerem retransmissões em altas taxas que podem aumentar o consumo de energia e assim, descartar dispositivos de baterias mais rapidamente. Neste contexto, é possível eleger parâmetros importantes de projeto para uma rede IoT com as seguintes questões:

1. Quanto congestionamento de tráfego suporta uma rede, dado um requisito de QoS (*Quality of Service*)?
2. Para tal nível de congestionamento, podemos perguntar: Qual o consumo de energia em um nó de rede arbitrário (que permite o estabelecimento da duração de suas baterias e seus tempos de vida)?
3. Quais são os gargalos de congestionamento da rede?
4. Qual é a taxa de chegada de tráfego que elimina esses gargalos?
5. Qual é a taxa de processamento de serviço nos nós que elimina esses gargalos?

A metodologia que consegue responder essas questões, e que é objeto desta tese, é a seguinte:

1. Construção de um Modelo de Simulação de Eventos Discretos (DES) para a rede completa, incluindo Redes AdHoc, Redes RFID e Redes IoT;
2. Validação do modelo DES usando o Modelo Analítico de Jackson (Rede de Jackson);
3. Avaliação de Rede Congestionada com seus gargalos;
4. Avaliação de Rede não congestionada;
5. Cálculo da Variação de tráfego (*Delta Erlang*);
6. Estimar a Redução de consumo de Energia decorrente do *Delta Erlang* usando modelos (Watt/Erlang) para diferentes tecnologias (Cenários 7 e 8).

1.4) Visão Geral da Tese

O objetivo de uma rede de telecomunicações é transportar informações de um ponto a outro de forma efetiva, isto é, as mensagens chegam ao seu destino corretamente e no tempo necessário. A quantidade de informações passadas corretamente no tempo é dita *throughput* (vazão da rede). A quantidade de tempo requerida para passar as informações é dita atraso de rede. Diversos parâmetros podem influenciar nesses valores, como por exemplo: número das mensagens transmitidas, tamanho das mensagens, número de nós na rede (topologia), protocolo e hardware de comunicação, etc. O estudo desses parâmetros de rede pode otimizar a efetividade da rede, estudo este que pode ser feito por meio de ferramentas de simulação, apesar dos protocolos de comunicações serem frequentemente muito complexos para serem modelados precisamente. De fato, não precisam ser modelados em detalhes, a mesmo de situações muito específicas, porque o que interessa são seus possíveis gargalos e contenções que podem provocar perdas e atrasos.

Modelagem e Simulação são ferramentas amplamente aceitas como técnicas de analisar sistemas do mundo real, que são muito complexos para serem modelados analiticamente, onde a maioria das redes de comunicações se apresenta. Permitem a análise de diversos cenários para o dimensionamento de novos sistemas ou o incremento e expansão de sistemas existentes. No entanto, sua credibilidade depende dos processos de verificação e validação do modelo de simulação de rede específico. Processos de verificação e validação devem ser usados para aumentar o nível de correção e exatidão da simulação, e a consequente confiança em seus resultados.

O objetivo da verificação é garantir que os requisitos e especificações projetadas de um sistema estão sendo cumpridos. **O objetivo da validação** é garantir que a simulação (e seu modelo) foi desenvolvida corretamente e que encontram as necessidades operacionais do usuário, e que pode ser realmente usada por tomadores de decisão para fazer a melhor decisão

a custo otimizado em sistemas reais. Os processos de verificação e validação podem incrementar tanto a correta simulação como a certeza colocada em seus resultados. O processo de validação deve ser aplicado tanto em sistemas existentes como em novos sistemas desenvolvidos. Validação dentro do contexto deste trabalho é tratada de forma mais ampla envolvendo inclusive a verificação pois o simulador coleta e apresenta tempo de atraso de pacotes e a utilização de processadores em cada nó do sistema, a qual é a funcionalidade exigida de especificações internas. Do ponto de vista do usuário final, o principal requisito da validação é um simulador que garanta tanto a correção da simulação como a confiança nos resultados. O modelo foi validado analiticamente pela Rede de Jackson, que será detalhado no Cenário 10.

Esta tese desenvolveu um Modelo de Rede IoT simulado, considerando aspectos essenciais para a Simulação de Redes: Redes para Catástrofes (Emergência) através das quais muitas vidas podem ser salvas, Redes de Sustentabilidade (Economia de Energia Elétrica), Redes Veiculares VANETs, Gerência de Rede e Segurança da Informação. As redes estudadas são heterogêneas, complexas, considerando clusterização, mobilidade, perdas, otimização de roteamento, redundância de links e acessos sem fio, priorização de mensagens, etc; apesar disso, é possível modelar, simular e validar esses avanços.

Esta tese apresenta 13 cenários com casos de estudo de simulação de Redes IoT, AdHoc e RFID, considerando nós congestionados e não congestionados, mensagens com e sem prioridades, e incluindo otimização de roteamento e perda de mensagens usando os modelos de mobilidade *Two-Ray Propagation* e *Random Way Point*. O objetivo desses cenários é analisar o tráfego no equipamento mediador para estimar sua capacidade, considerando diversos tipos de aplicações: *Smart City*, *Smart Green Building*, ITS (*Intelligent Transport System*), *Power Consumption*, Avisos de Catástrofe e *Network Management*. Especificamente, objetivamos determinar a utilização dos Processadores e Atrasos nas Mensagens da Rede IoT. O modelo proposto e sua simulação podem ser usados no projeto, planejamento, dimensionamento e evolução da rede IoT. Os resultados mostram que o balanceamento de tráfego, a otimização de roteamento e a priorização de mensagens são relevantes para o uso efetivo da rede.

Esta tese está focada na resolução desses problemas por meio de ferramentas de Modelagem, Simulação Híbrida por meio do uso de diversas ferramentas, validação, fazendo assim o mapeamento de uma rede real em uma rede simulada através da metodologia. Usaram-se as ferramentas integradas como: ARENA (Evento Discreto), MATLAB (Mobilidade e Otimização de Monte Carlo) e Visual Basic (Integração das Lógicas Fuzzy e de Predição do Matlab no ARENA).

1.5) Organização do Documento

O **Capítulo 2** apresenta o Referencial Teórico da Arquitetura IoT (*Overview*) com sua Arquitetura, Modelos, Tecnologias, Protocolos e Aplicações selecionados. Apresenta também a Segurança da Informação na Rede IoT e o Gerenciamento de Elementos de Redes IoT.

O **Capítulo 3** apresenta a metodologia utilizada na pesquisa bibliográfica, os resultados obtidos, a divisão funcional dos artigos selecionados, um resumo do estado atual e tendências da IoT e as conclusões desta pesquisa bibliográfica. No final, mostram-se as referências bibliográficas selecionadas. O **Capítulo 4** apresenta o Modelo de Rede IoT proposto com simulação híbrida.

O **Capítulo 5** apresenta 13 CENÁRIOS desenvolvidos na tese, com seus respectivos casos de estudo e artigos publicados/apresentados: experimento e os resultados do desenvolvimento da pesquisa. Os artigos publicados possuem um capítulo de "*Related Work*" mostrando os artigos relacionados com a pesquisa específica, sendo assim uma complementação do trabalho de Pesquisa Bibliográfica original. Apresentam-se também os Resultados Esperados e os Resultados Observados. O **Capítulo 6** apresenta as Conclusões e Futuros Trabalhos. O **Apêndice A** apresenta a Lista de Artigos Publicados e apresentados em Congressos. O **Apêndice B** apresenta as Atividades Desenvolvidas durante a Tese.

Capítulo 2 : Referencial Teórico IoT

Neste capítulo aborda-se o referencial teórico IoT com sua arquitetura, modelos, protocolos, tecnologias, aplicações, segurança e gerenciamento da rede IoT.

2.1) Arquiteturas e Modelos IoT e RFID

A Arquitetura IoT foi padronizada internacionalmente em [5] [62] e está mostrada na Fig. 4 que segue. Foram publicados os seguintes artigos [P4] [P8] [P16] com uma Visão Geral sobre a IoT: Arquitetura, Modelos, Tecnologias, Protocolos e Aplicações.

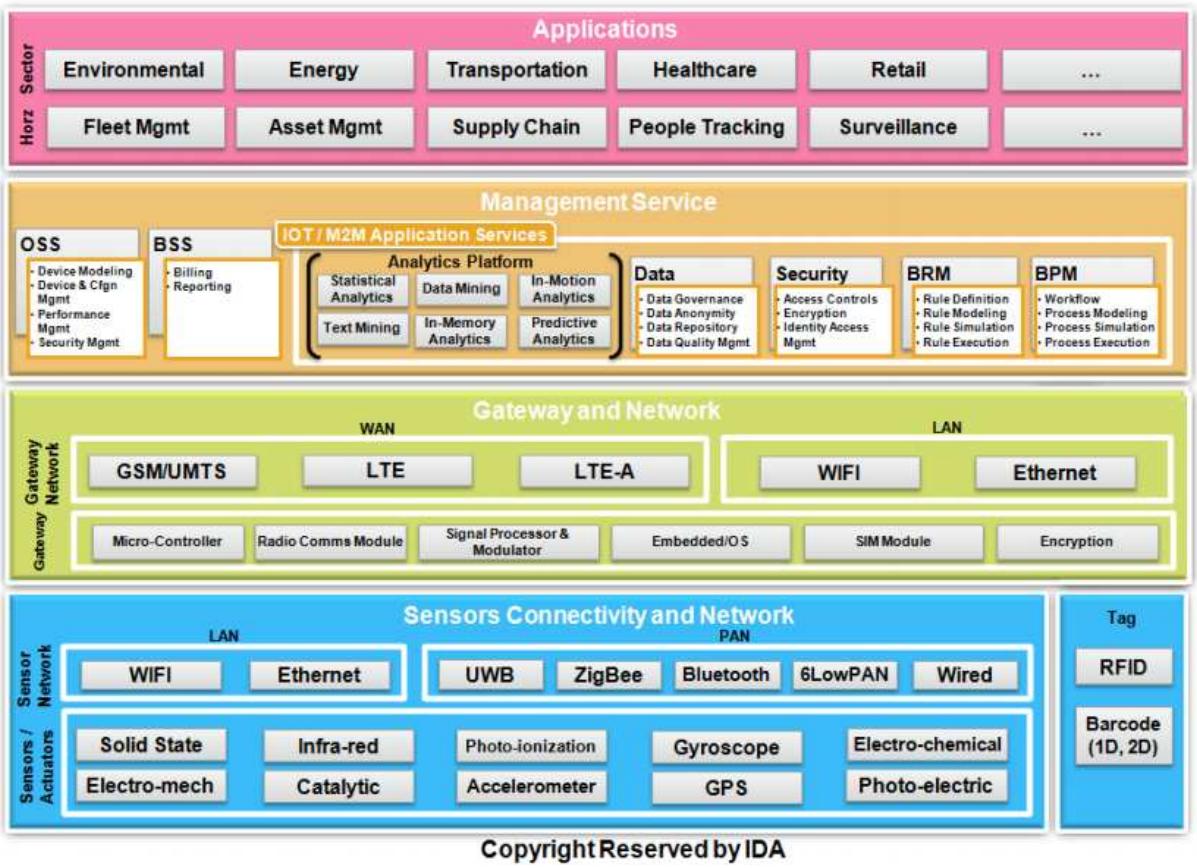

Figura 4*: Arquitetura IoT da IDA (International Digital Asset Management)* [64]

A Arquitetura RFID também foi padronizada internacionalmente pelo EPCglobal; está especificada em [2] e está mostrada na Fig. 5 que segue.

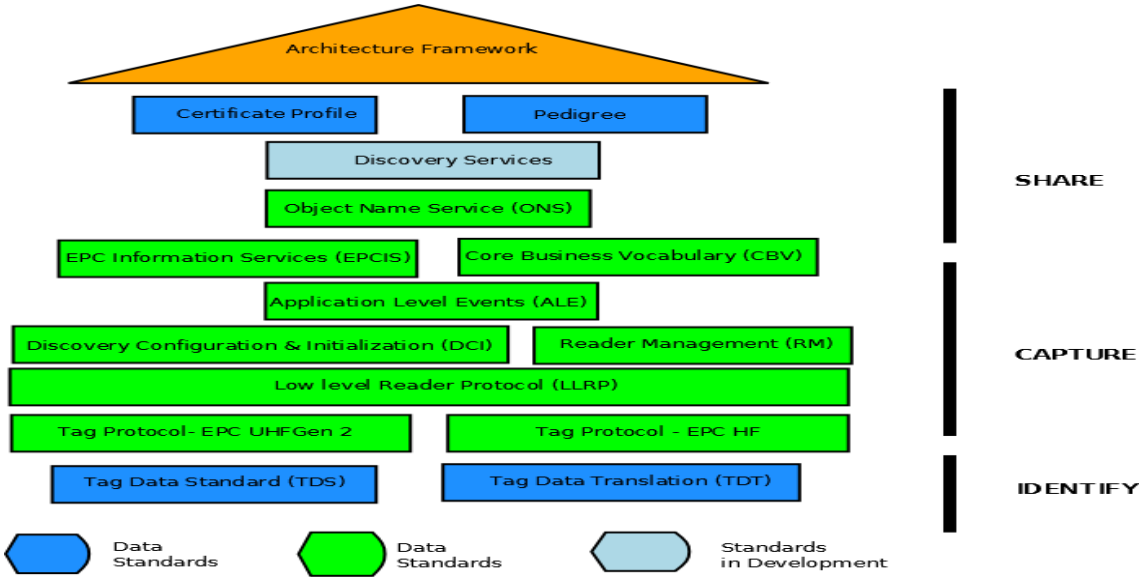

Figura 5 : Arquitetura RFID (EPCglobal/ISO) [2]

A Arquitetura IoT (Figura 1) escolheu Tecnologias Abertas, Simples, Baratas e Consagradas como Ethernet, WiFi, Ad-Hoc, ZIGBEE, Bluetooth, RFID (*Radio-Frequency Identification*), WSS (*Wireless Signal Solutions*) e Rede de Sensores. É claro que soluções cabeadas como Ethernet/*Wired* também podem ser usadas. A Arquitetura IoT selecionou outras Arquiteturas consagradas como TCP/IP e SOA (*Service Oriented Architecture*). A Arquiteura IoT separa a Comunicação nas seguintes Camadas:

- Conectividade de Sensores e Redes;
- *Gateways* e Redes;
- Serviços de Gerenciamento de Rede e Segurança da Informação;
- Aplicações.

A IoT escolheu também aplicações de utilização direta na sociedade e na Economia Mundial, como por exemplo: Ambiental, Energia (*Smart Grid*), Transporte, Saúde, Varejo/Atacado, Cadeia de Produção, Acompanhamento de Pessoas (*Healthcare*) e Segurança (*Smart Home, Building, City*), entre outros.

A Figura 5 mostra a Arquitetura RFID utilizada na IoT, dividindo em Camadas de Identificação, Captura e Compartilhamento de Informações. A Camada de Identificação é responsável em identificar as Etiquetas *TAGs* com uma numeração única. A Camada de Captura é responsável em coletar as informações recebidas das Etiquetas. A Camada de Compartilhamento é responsável em distribuir e compartilhar as informações recebidas das Etiquetas com as aplicações RFID.

A Figura 6 mostra o Modelo de Referência IoT conforme o entendimento de Telecomunicações do ITU-T [62], ISO e IEC. Como todos os modelos de referência da ITU-T, possui 2 colunas referentes a Gerenciamento de Rede e Segurança, colunas essas que tem funcionalidades espalhadas em todas as camadas do modelo.

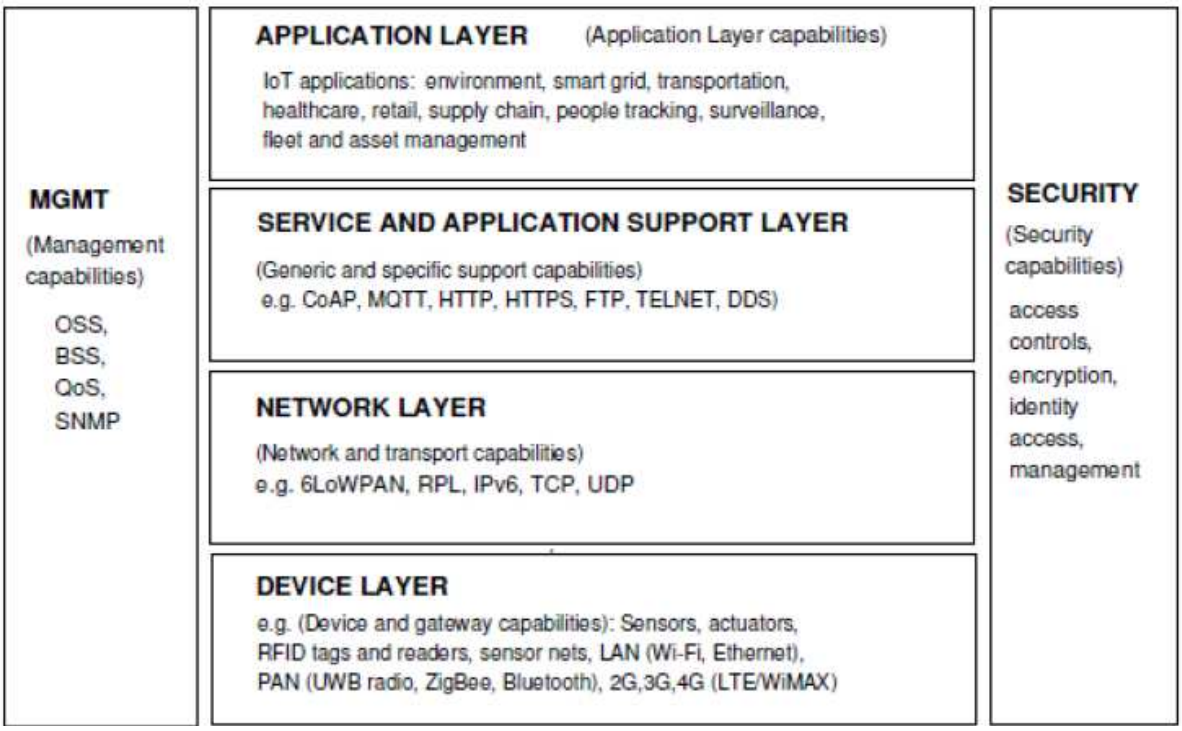

Figura 6 : Modelo de Referência IoT com seus principais protocolos (ITU-T, ISO e IEC) [62]
.

2.2) Protocolos IoT

A Figura 7 apresenta o Modelo de Comunicação IoT [2] comparado com o Modelo OSI(Open System Interconnection) da ISO [58] [59] [60] [61] [65]. As linhas tracejadas representam que existem diferenças entre as camadas IoT em relação ao Modelo OSI. O foco principal é a informação trocada ("*Data*") entre o objeto e a aplicação.

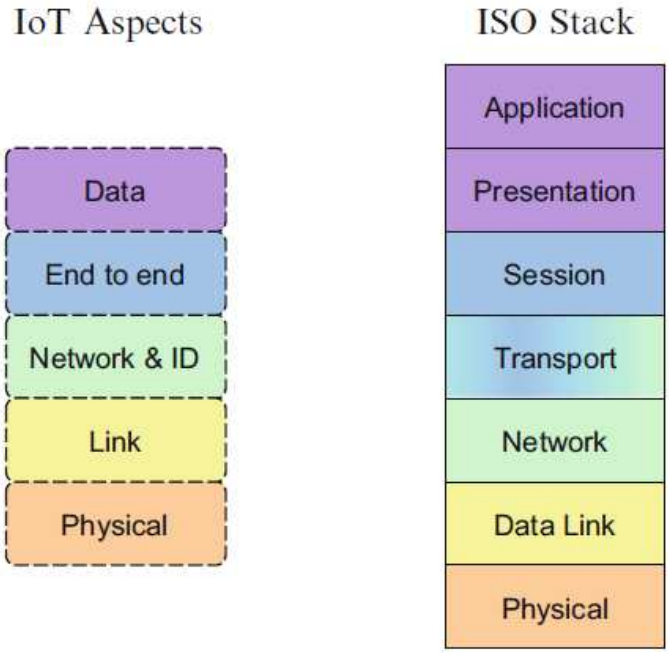

Figura 7 : Modelo de Comunicação IoT seguindo o Modelo OSI da ISO [2]

A pilha de protocolos IoT é baseada no Modelo de Referência OSI da ISO [58] com 7 camadas (Tabela 1), onde a comunicação é dividida em 7 camadas devido à sua complexidade. A Arquitetura TCP/IP, por motivos de eficiência, optou em agrupar os 3 níveis superiores em um só. A Internet, WEB e IoT seguiram o mesmo caminho.

O foco da IoT é no transporte de informações (*DATA*) gerados pelos RFIDs e Sensores. As Camadas restantes (*Physical, Link, Network ID, End to End*) importam suas funcionalidades das camadas OSI da ISO. Devido ao grande número de dispositivos conectados, o volume de dados pode ser muito grande. A Pilha de Protocolo WEB é também considerada na IoT para a busca de informação na nuvem (*Cloud* e *Fog*), usando celulares e *smartphones*. Em resumo, a Pilha TCP/IP pode ser totalmente usada. Assim sendo, protocolos das camadas 1 a 4 são bem conhecidos devido à popularidade da Arquitetura TCP/IP. Os protocolos novos da IoT são 6LowPAN (*IPv6 over Low-Power Wireless Personal Area Networks*), CoAP, MQTT, AMQP e CBOR. CoAP (*Constrained Application Protocol*) é um Protocolo especializado em Protocolo de Transferência WEB para nós limitados (processamento, memória, interfaces e energia) e dispositivos de IoT. MQTT é um protocolo *machine-to-machine* (M2M) e de conectividade IoT. Foi projetado como um transporte de mensagens *publish/subscribe* bem leve. MQTT é o AMQP ou JMS para ambientes limitados da IoT. CBOR (*Concise Binary Object Representation*) é um formato de dado projetado com o objetivo de prover a IoT com mensagens de tamanhos pequenos. É baseado no JSON. Enquanto JSON usa codificação de texto, CBOR usa codificação binaria, resultando assim em mensagens de tamanhos compactas.

Tabela 1. *Stack* de Protocolos IoT e WEB [P8]

IoT Stack	OSI	Web Stack
DATA/CoAP MQTT/XMPP, AMQP CBOR, JSON	7. Application 6.Presentation 5. Session	Web Applications HTML, XML, JSON HTTP,HTTPS, DHCP, DNS, TLS/SSL
TCP/UDP/DTLS	4. Transport	TCP, UDP
IPv6/IP routing/6LowPAN	3. Network	IPv6, IPv4, IPsec
IEEE 802.15.4 MAC	2.Data Link	Ethernet, DSL, ISDN, WLAN, Wi-Fi
IEEE 802.15.4 PHY radio	1. Physical	Physical

2.3) Tecnologias Selecionadas pela IoT

A IoT selecionou diversas tecnologias padronizadas e já utilizadas internacionalmente. Assim sendo, muito dos novos ambientes IoT são parecidos com os atuais existentes na INTERNET Residencial e Empresarial. A maioria das tecnologias é por rádio e sem fio (*Radio Access Technologies*), ou seja, utilizando os padrões IEEE 802.11, IEEE 802.15 e IEEE 802.16, por questões de flexibilidade e alcance.

As tecnologias selecionadas encontram-se agrupadas conforme a área de Cobertura da Rede: P2P, Pessoal, Local, Metropolitana e Satélite:

- ***P2P (Peer to Peer) :*** RFID, NFC;

- ***WPAN(Wireless Personal Area Network) :*** Bluetooth, Zigbee; Obs. WBAN (*Wireless Body Area Network*) está sendo pesquisada e desenvolvida;
- ***WLAN (Wireless Local Area Network):*** Wi-Fi (IEEE 802.11 a/c/n/ac, Wi-GIG (80.11.ad), AdHoc (IEEE 802.15.4);
- ***WAN-MAN (Wireless Metropolitan Area Network) :*** WiMAX 802.16 d,e,s, LTE GSM, NB-IoT, SIGFOX, LoRa, MimoMAX;
- ***WAN-RAN (Wireless Area Satellite Network):*** VSAT.

A Tabela 2 apresenta um resumo das tecnologias mais utilizadas nas Redes de Acessos (*P2P, WPAN e WLAN*). A conectividade permite a troca de dados entre participantes dentro do domínio funcional, dentro do sistema e entre sistemas. A troca de dados pode incluir atualizações de sensores, dados de telemetria, eventos, alarmes, logs, arquivos, mudanças de estado, comando de controle, e atualização de configurações.

Tabela 2: Comparação de tecnologias de acesso e seus protocolos [P4] [P8].

Technology	Protocols	Rate (bps)	Power	Range (m)	Battery	Topology	# nodes
RFID	ISO/IEC 18000	800 to 960M 2.45 or 5.8G	1 W (reader)	5 max.	not applicable	star	diverse
NFC	ISO/IEC 18092	424 k 125k, 13.56M	100+ mW (reader) –	0.01-0.1	months/years –	P2P	2
Bluetooth	IEEE 802.15.1	1 M	49m/0.2 mA	1-10+	days	star	7
ZigBee	IEEE 802.15.4	20-250k	30m/0.356 mA	100+	months/years	P2P/star/mesh	254 to 64516
Wi-Fi	IEEE 802.11b	54M	400/20m mA	1-30+	hours	star	32+ cabled
6LoWPAN	IEEE 802.15.4	250k	1 mW	100+	months/years	star and tree	100 +

2.3.1) Sensores e Redes de Sensores

Os sensores são os geradores básicos de informações em uma Rede IoT. Por sua simplicidade, só conseguem gerar informações específicas de Temperatura, Pressão, Umidade, Claridade, etc; o tráfego dessas informações é feito através das Redes de Sensores que podem ser fixas ou móveis AdHocs. Já existem sensores capazes de gerar diversas dessas informações conjuntamente e outros sensores embutidos em Etiquetas RFID, evitando o uso de bateria.

2.3.2) Redes AdHoc

O uso de protocolos de roteamento dinâmicos e adaptativos possibilitam que as redes AdHoc sejam formadas rapidamente, por diversos nós que tem proximidade para a comunicação. As Redes AdHoc sem fio podem ser classificadas por suas aplicações : *Mobile Ad-hoc Networks (MANET*), *Vehicular Ad-hoc Networks (VANETs)*, *Smartphone Ad-hoc Networks (SPANs), Internet based Mobile Adhoc Networks (iMANETs), FANETs (Flying AdHoc Network)* e *Military / Tactical MANETs* [3]. O Protocolo AdHoc tem os seguintes pontos importantes: Padrão Internacional Aberto IEEE 802.15.4, usado nas Redes MANET, VANET, FANET, *WSN (Wireless Sensor Networks)*, Redes de Catástrofe e de Emergência; adicionalmente, é a base das Arquiteturas ZIGBEE, Bluetooth e Acesso IoT. Segundo o ITU-T e o 3GPP, a rede celular 5G em instalação mundial terá também a funcionalidade AdHoc pois será incrementada com o Protocolo D2D da Arquitetura Móvel 5G e CRAN (*Cognitive Radio Ad-hoc Networks*).

2.3.3) Tecnologia RFID (Radio Frequency Identification)

O RFID utiliza campos eletro-magnéticos para automaticamente identificar e rastrear Etiquetas coladas nos objetos [2]. O sistema RFID é composto por Etiquetas, Antenas, Leitores, Mediador e Aplicações; a etiqueta (*TAG*) possui informação de identificação (EPC: *Electronic Product Code*) de um produto/equipamento/crachá e é armazenada em um *TAG* com "96 Bits de Dados"; ela pode ser passiva, ativa e Assistida com Bateria. O Leitor emite um sinal de rádio e aproveita a proximidade das *Tags;* esse sinal é recebido pelas *tags* que transmitem suas informações de identificação. Esse é um processo de indução eletro-magnética entre o Leitor e as *Tags*. Essas informações são enviadas ao mediador, responsável pela filtragem e agrupamento, enviando as informações resumidas e consolidadas para as aplicações. A RFID, assim como a IoT, também aproveitou os protocolos de sucesso existentes nas redes de telecomunicações, como por exemplo a Arquitetura TCP/IP.

2.3.4) Tecnologia NFC (Near Field Communication)

NFC (Comunicação por Campo de Proximidade) é um conjunto de tecnologias sem fio de curta distância (<10 cm) com padrão ISO/IEC 18000-3. Sua origem se deu junto com a tecnologia RFID. É muito utilizada para pagamentos móveis com Smartphone. É uma tecnologia que permite a troca de informações sem fio e de forma segura entre dispositivos compatíveis próximos. Quando os dispositivos estão próximos, a comunicação é estabelecida automaticamente. Esses dispositivos podem ser telefones celulares, *tablets*, crachás, cartões de bilhetes eletrônicos e qualquer outro dispositivo que tenha um *chip* NFC.

2.3.5) BLUETOOTH

Padrão internacional aberto IEEE 802.15.1, sinal de rádio frequência por difusão e curtas distâncias (poucos metros), alta qualidade e flexibilidade. Desenvolvido e Evoluído pelo *Bluetooth Group*, muito usado em automóveis.

2.3.6) ZIGBEE

Padrão internacional aberto IEEE 802.15.4, usa em sua base uma Rede AdHoc (*Hop to Hop*). O Zigbee é responsável pelas funções: *Network Routing, Address Translation, Packet Segmentation e Profiles*. Desenvolvido e Evoluído pelo *ZigBee Alliance*.

2.3.7) Wi-Fi

Padrão internacional aberto IEEE 802.11.b,g,n, 2.4 GHz., sinal de Radio Frequência por difusão, médias distâncias (dezenas de metros), alta qualidade e flexibilidade. Já possui uma evolução para altas taxas (*Gbps*) de comunicação, chamado de Wi-GIG.

2.3.8) IPV6

Padrão de Endereçamento TCP/IP de 128 bits; os objetos futuramente utilizarão o "Micro IP" por questões de eficiência energética (*chip* de comunicação fica desligado quando ocioso). A utilização do IPV6, ao invés do IPV4, foi necessária devido ao grande volume de objetos (*Things)* que deverão ser endereçados na rede.

2.3.9) Mobile 4G (LTE) and Mobile 5G (Em Implantação mundial)

As Redes Celulares Móveis são as mais utilizadas na busca pelas informações coletadas na rede; normalmente, essa busca é feita na nuvem, através de protocolos tipo HTTP ou HTTPS (Com Segurança e Criptografia). Adicionalmente, elas podem ser usadas para avisos de catástrofe, indicando a rota de fuga a ser seguida pela população em risco.

2.4) Aplicações Selecionadas pela IoT

A IoT selecionou diversas aplicações em diversos Setores da Economia Mundial :

- Cliente e Residência (Conforto e Conveniência);
- Prédios (Comercial e Institucional);
- Industria (automação);
- Cuidado com a Saúde;
- Energia, água, gaz e telecom;
- Mercado (Atacado e Varejo);
- Transporte;
- Segurança Publica;
- Tecnologia da Informação e Redes (TICs).

Algumas dessas aplicações serão exemplificadas a seguir na Tabela 3.

2.4.1) *Smart Home*

Essa aplicação visa oferecer automação residencial usando o *Smartphone* ou *Tablet* para acesso remoto, como por exemplo: acender e apagar luzes, saber o tempo de vida das lâmpadas, abrir e fechar portas e portões, ligar e desligar TV/Ar-Condicionado, receber a lista de mantimentos faltantes na geladeira, receber informações via *SMARTTV* e Videos, etc.

2.4.2) *Smart Building*

Essa aplicação visa a automatização em um edifício, tornando *'green"* em termos de Energia Elétrica, Agua, Aquecimento Solar, Sistemas de Baterias, etc. Equipamentos de alto consumo (Ar-Condicionado e Iluminação) poderão ser ajustados dinamicamente em função da temperatura/umidade/claridade interna e externa do prédio. Sistemas de Baterias poderão ser supervisionados visando a antecipação de troca em caso de futura falha. O artigo publicado [P13] mostra um cenário desenvolvido como Modelo de Rede IoT para um *SMART Campus*, visando a economia de energia.

2.4.3) *Smart Cities*

Essa aplicação trata de troca de informações entre carros, celulares, prédios e semáforos, visando melhorar o trânsito e fluxo de carros em uma cidade. A *Smart City* abrange as seguintes áreas:

- *Saúde das Estruturas de Prédios e Pontes;*

- *Monitoramento de Lixo;*
- *Monitoramento da qualidade do ar;*
- *Monitoramento de ruído;*
- *Monitoramento do Congestionamento de Tráfego;*
- *Consumo de energia na cidade;*
- *Estacionamentos Inteligentes;*
- *Semáforos Inteligentes;*
- *Automação e Salubridade em prédios públicos.*

O artigo publicado [P12] mostra um cenário desenvolvido para ITS (*Intelligent Transportantion System*), parte funcional da *Smart City* em estradas.

2.4.4) *Smart Grid (Energy* e *Utilities*)

Essa aplicação cuida da Automatização do Setor Elétrico visando colocar nas residências leitores inteligentes (*Smart Meters*) que passam as informações de consumo diretamente para as empresas fornecedoras, as quais utilizam a própria rede para gerenciar seus equipamentos e falhas. Utiliza uma rede específica do setor elétrico com tecnologia PLC (*Power Line Communication*), por questões de confiabilidade e tempo de resposta. Seus principais componentes são:

- Geração de Energia Elétrica;
- Transmissão de Energia Elétrica;
- Automação da Distribuição de Energia Elétrica;
- Automação da Casa do Cliente e resposta à demanda (Infraestrutura de Medição Avançada (AMI), Carros Elétricos e Gerenciamento da Energia Elétrica na Residência).

Os dispositivos envolvidos são usinas, geradores, transformadores, linhas de transmissão, estações de conversão de tensão, geradores eólicos, geradores solares, UPS, baterias, células de hidrogênio, carros elétricos, etc. Similarmente, existe a aplicação de monitoramento do fornecimento de agua, gás e Internet.

2.4.5) *Healthcare* (Assistência Médica Remota)

Essa aplicação possibilita o monitoramento e acompanhamento remoto de pacientes em suas casas, através da coleta de informações de sensores (no paciente) de temperatura/pressão arterial/ batimentos cardíacos/nível de glicose/nível de oxigenação, sensores ambientais de presença/ temperatura/pressão/movimento, RFIDs de crachás de paciente, enfermeira, cuidadora, funcionários, remédios, equipamentos, etc, informações essas que são enviadas para a nuvem e são acessadas pelos médicos e hospitais. O médico poderá acessá-las através de seu *Smartphone* e solicitar que o paciente seja deslocado para o hospital em caso de valores perigosos nos seus sinais vitais. Essa aplicação possibilita um novo modelo de negócio para Planos de Saúde, em que o paciente só vai ao Hospital em situações graves.

2.4.6) *Smart Manufacturing (Industry)*

Essa aplicação é responsável pelo controle e automação de processos fabris reais (Indústria 4.0) sobre Dispositivos Industriais (Tornos, Prensas, Controladores Numéricos, Controladores de Lógica Programáveis (PLCs), Robôs, etc), requerendo tempos de reação curtos (*Real Time*), com pouco atraso e *jitter*, e pouca quantidade de dados produzida. Adaptadores,

Bridges e Gateways são necessários devido ao grande número de Ilhas (Aplicações) existentes com protocolos proprietários.

2.4.7) *Smart Farming*

Essa aplicação automatiza a fazenda, através da sua interconexão com o mundo global. Possibilita a interconexão de tratores, colheitadeiras, *drones*, sede da fazenda, cooperativas, entidades da agricultura e aviões pulverizadores. Os funcionários e os animais são identificados através de etiquetas RFIDs. È necessário a instalação de uma Estação Rádio Base na fazenda, permitindo a interconexão dessas diversas partes que permite construir uma fazenda *ONLINE.* Esta aplicação é de grande importância para o Brasil por ser um país fortemente agrícola.

2.4.8) *Transporte e Logística*

Três maiores aspectos são incluídos nessa classe de aplicação: 1) a otimização de desempenho de veículo, 2) operações flexíveis, e 3) gerenciamento de tráfego. A inclusão da IoT nos veículos permite a instalação de novas funcionalidades como predição e monitoramento de desempenho de veículo. VANETs (*Vehicle Area Networks*) são redes AdHocs criadas para a integração desses objetos e dispositivos que suportam as funcionalidades dos veículos. O uso de sensores, processamento e comunicação, possibilitam que os veículos sejam monitorados e acompanhados em todos os lugares das ruas, estradas e estacionamentos. A predição da futura localização também será possível. A IoT permite também o acompanhamento das cargas/caminhões e obtenção de dados em tempo real, monitoramento de desempenho do transporte e redução do tempo de entrega e do atraso do transporte. A integração da IoT com a Engenharia de Tráfego ITS (*Intelligent Transport System*, parte funcional da *Smart City*), pode aumentar a segurança dos carros e diminuição do atraso no tráfego: acesso a condições de estradas e vias, gerenciamento de infraestrutura de transporte, redução do congestionamento, coordenação de Redes de Transportes assim como a provisão de serviços inovativos.

2.4.9) Outras Aplicações

Outras aplicações potenciais estão surgindo: Catástrofe (Recuperação de Desastre), Estacionamento Inteligente, Automação Comercial (Atacado e Varejo), Carro Conectado, Canteiro de Obras Conectado, Monitoramento de Tanques Industriais, Monitoramento de Oleodutos/Gasodutos, Medidor Inteligente (Luz, Agua, Gás, Internet), Segurança Pública, Aviso de Catástrofe, dentre outras. Estas demandarão muito esforço de Padronização, Especificação, Desenvolvimentos e Testes. Cada aplicação necessitará ter a sua própria padronização aberta que deverá ser gerada pelos grupos técnicos associados.

Tabela 3 : Aplicações *SMART* da IoT [P4] [P8]

Smart Applications	Environment	Functions (monitoring of)	Remote Access	Stake-holders	State-of--the-art
Home	residential	handle lighting, A/C, windows, alarms appliances, doors	smart phone	family	commercial solutions
Building	civil construction	power efficiency, water heating, solar, battery	sensors, actuators	condominiums	standards, pilot
Cities	autos, traffic lights bridges, buildings, transit, tunnels	congestion, air quality parking, lighting, noise, etc.	smart phones GPS	population police, Hall	standards, pilot
Grid	utilities energy	power generation transmission, distr.	energy meters mgmt. systems	energy companies	standardized, under implementation
Healthcare	residential	patient monitoring medicine, tags	smart-phone tablet, laptop	patients, doctors nurses, health plan	pilot implementation
Manu-factoring	industrial	robots, PLCs	management	factories automation devices	proprietary implementations
Farming	farms cattle	tractors, trucks harvesters, drones	mgmt. systems	farms silos, co-ops	proprietary implementations
Transporta--tion, Logistics	roads, fleets vehicles	vehicle downtime, performance	GPS, handhelds mgmt. systems	drivers, transport authorities, etc.	proprietary implementations

2.5) Segurança da Informação na IoT

O núcleo da IoT é formado [P14] [63] [P16] por plataformas especializadas em serviços de coleta de dados de dispositivos IoT, processamento de dados e conexão com outros serviços para tomada de decisão em atividades futuras, tais como ativação de atuadores, etc. A maioria das redes IoT utiliza tecnologia sem fio por questões de flexibilidade, sendo assim mais susceptível a ataques gerais de redes sem fio, tais como : DoS (*Denial of Service*), MITM (*Man-in-the Midle*), ESCUTA (*Eavesdroping)*, modificação de mensagem e apropriação de recurso. Adicionalmente, cada tecnologia possui também outros pontos vulneráveis que devem ser considerados na fase de projeto da aplicação.

A IoT aproveitou as arquiteturas, tecnologias e protocolos consagrados nos ambientes de TI e TELECOM, existentes na Internet e na WEB. Assim sendo, muitos mecanismos de segurança da informação puderam ser aproveitados e utilizados tanto no Modelo de Serviços na Nuvem com plataformas de serviços prontas (SaaS, PaaS e IaaS), como nas camadas de protocolos (exemplos: HTTPS, IPSEC, Criptografia na RFID, Segurança do TCP/IP, Criptografia, SSL, TLS, AES, X.509, etc). Os certificados X.509 são certificados digitais que usam a infraestrutura de chave pública X.509 padrão para associar uma chave pública a uma identidade contida em um certificado. Os certificados X.509 são emitidos por uma entidade confiável chamada CA (Autoridade de Certificação). Esse aproveitamento de protocolos de sucesso e infraestrutura existente na nuvem diminuem o investimento e o tempo de desenvolvimento de Softwares *Middleware* e Aplicações *Smart*. É esperado que as plataformas de TI da nuvem já possuam mecanismos de segurança embutidos internamente e em seus protocolos de comunicação. Esses mecanismos de segurança, assim como a Gerência de Rede, são espalhados nas diversas camadas de rede, conforme mostrado na Figura 6.

Os novos protocolos criados para ambientes restritos (*constrained)* da IoT utilizam mecanismos de segurança, conforme Tabela 4a que segue. Adicionalmente, apresentam-se as arquiteturas de protocolos para Sensores, *Tags*, *Notebooks*, *Smartphones* e Dispositivos: RFID, WiFi, Zigbee e Bluetooth (Tabela 4b).

Tabela 4 : Mecanismos de Segurança adicionados nos: **a) Protocolos Restritos**. (LIMITAÇÕES (*Constrained)* em termos de: Potência, Memória, Processador, Banda, Comunicação, Tamanho); **b) Tecnologias de Acesso** [P16]

Protocolo/ Arquitetura	**Origem**	**Modelo de Mensagem**	**Mecanismo de Segurança**	**Padronização**	**Transporte**
a) AMQP	Bancos 2003	Advertiser/Subscriber	SSL	OASIS 2012	TCP
MQTT	IBM 1999	Advertiser/Subscriber	TLS Brokers(Username + Password)	IEEE 2013	TCP
CoAP	IoT	REST [64] Request/Response Advertiser/Subscriber	DTPLS	RFC 7252	UDP
6LOWPAN	IETF	Micro IP	SubconjuntoIPSEC	RFC4919	IEEE802.15.4
b) RFID	EPCglobal	Tag Information 96bits	Autenticação, Criptografia e Assinatura	GS1 EPCglobal	RFID
WiFi	IEEE	IEEE 802.11 (a,b,g,n)	Criptografia, Filtros MAC, Protocolos e Endereços IPs	IEEE	TCP/IP
ZigBee	ZigBee Alliance	IEEE 802.15/ ISA100.11 a	Controle de Acesso, Criptografia, integridade dos quadros, sequencialidade, Trust Center	IEEE	IEEE 802.15.4 IEEE 802.15.4
Bluetooth	Bluetooth Group	IEEE 802.15.1	Autenticação, Criptografia e Autorização	IEEE	

No nível mais baixo, precisa-se acrescentar mecanismos de segurança nos dispositivos IoT, que são muito numerosos e fonte de informações na qual a funcionalidade do sistema é baseada. A tecnologia RFID já foi criada com endereçamento grande (96 bits e criptografia na leitura das informações das *tags*), sendo assim forte candidata a ocupar este espaço de dispositivos de leitura de sensores.

O uso de mecanismos de segurança depende do tipo de aplicação e precisa ser criteriosamente estudado e escolhido, pois implica sempre em aumento de *overhead* e maior atraso na comunicação.

O artigo de Grabovica et al.[45] apresenta os Mecanismos de Segurança para Redes IoT usuárias de Tecnologias ZigBee, Bluetooth, RFID e WiFi. São mecanismos já existentes nos protocolos que podem ser utilizados para dar uma melhor segurança na comunicação. O assunto Segurança da Informação está no Estado da Arte de IoT.

O artigo de Gonçalves et al.[46] apresenta uma Arquitetura de Segurança para Aplicações de *Mobile E-Health* no Controle de Medicamentos. Comenta que por motivos de segurança, a Tecnologia RFID é a melhor a ser utilizada na Área Médica; serve para Identificação de Remédios, Equipamentos e Profissionais (Médico, Enfermeiro, Cuidadora, Farmacêutico), garantindo uma Identificação única e segura usando 96 bits de Identificação. Propõe uso de Mecanismos de Segurança nos Protocolos TCP/IP/HTTPS/IPSec. Comenta também sobre a utilização de *LogIN*/Senha nos Aplicativos, garantindo a Identidade do Usuário. Comenta a necessidade de se utilizar Arquivos *LOG* contendo todas as Intervenções ocorridas com o paciente. Propõe também a utilização de Protocolos de Segurança mais sofisticados e complexos, com o uso de Chaves Públicas e Privadas, Algoritmos *HASH*, Criptografias Simétricas e Assimétricas. É um assunto de alta complexidade que proporcionará muitas novas pesquisas, estando assim no estado da arte da IoT.

a) Proteção de Dados e Mecanismos de Segurança na Arquitetura RFID da EPCglobal

A análise de segurança depende de cada aplicação, ficando assim sua análise aos proprietários e usuários do sistema baseada na Arquitetura RFID EPCglobal. A segurança é um processo pelo qual uma organização ou um indivíduo protege seu acervo de dados, visando reduzir o risco de um ataque.

A RFC 2828 apresenta que a segurança de dados é comumente subdividida em atributos: confidencialidade, integridade, disponibilidade e identificação (*accountability*). A confidencialidade de dados é uma propriedade que garante que a informação não fique disponível ou revelada para indivíduos não autorizados, entidades ou processos. A integridade dos dados é uma propriedade que os dados não foram alterados, destruídos ou perdidos de forma não autorizada ou de maneira acidental, durante o transporte ou armazenamento. Disponibilidade de Dados é a propriedade de um sistema ou recurso de um sistema ser acessível e ser utilizado sob demanda por uma entidade de sistema autorizado. Identificação (*Accountability)* é a propriedade de um sistema que permite que as ações de uma entidade de sistema possam ser identificadas unicamente para esse sistema, o qual pode ser responsável por suas ações. As técnicas de segurança como criptografia, autenticação, assinaturas digitais e serviços de não repudio são aplicadas aos dados para prover segurança. A Autenticação é pré-requisito para comunicação criptografada.

Diversas Interfaces de Redes da arquitetura RFID são baseadas em protocolos de arquitetura de rede existente incluindo as redes TCP/IP. Mecanismos de proteção de dados do protocolo TLS (*Transport Layer Security* – RFC2246 e RFC 4346), permitindo que clientes e servidores selecionem algoritmos de criptografia na troca de certificados permitindo a autenticação de identidade e compartilhem chaves para permitir a criptografia e o

compartilhamento de dados validados. Mecanismos de proteção do protocolo HTTPS (*HTTP over TLS:* RFC 2818) são utilizados para conteúdo sensível a criptografia para transferência na WEB; pode-se escolher no *browser* e o uso ou não do TLS (HTTPS ou HTTP). Todos dados HTTP podem ser enviados dentro de conexões TLS ao servidor, protegidas por mecanismos de criptografia negociados durante a conexão TLS. As Aplicações RFID (ALE: *Application Level Events*) podem utilizar o HTTPS provendo autenticação e criptografia, os quais juntos, provêm confidencialidade e integridade dos dados compartilhados. Mecanismos de "*call-back*" também podem ser utilizados para eventos assíncronos visando garantir a veracidade da comunicação, usando a Operação Segura POST via TLS. O HTTPS permite segurança a nível de link e autenticação mútua opcional. O protocolo entre o Leitor e o Mediador tem opcionalmente a possibilidade de criptografia e autenticação do link de comunicação; mais uma vez o HTTPS pode ser utilizado. Os mecanismos de autenticação X.509 ITU-T podem ser amplamente utilizados para chaves criptográficas.

O Gerenciamento do Leitor pode ser feito através do uso do protocolo SNMP (RM SNMP MIB, com mecanismos de criptografia e autenticação) ou XML.

O RFID provê 4 modos de segurança: Autenticação de *TAGs*, Autenticação do LEITOR, Comunicação Criptografada (Confidencialidade), e Comunicação com Assinatura (leitores querem receber informações somente de fontes e dispositivos confiáveis). O RFID provê 3 níveis de criptografia: Simples (Tráfego não criptografado), Moderado (Uso do Algoritmo de Criptografia DES) e Avançado (Uso do Algoritmo AES com criptografia de 128 bits).

b) Proteção de Dados e Mecanismos de Segurança no Acesso WiFi

Este tipo de tecnologia de rede é um padrão internacional aberto amplamente utilizada no mundo possuindo assim mais recursos de segurança. Existem 2 tipos de ataques mais comuns: controle de acesso da rede e segurança de dados. Utiliza-se Autenticação e Criptografia WEP. O WiFi prevê 4 níveis de criptografia: WEP 64 (criptografia de 64 bits), WEP 128 (criptografia de 128 bits), WPA (criptografia de 256 bits) e WPA 2 -PSK (TKIP e AES). O WiFi provê 4 modos de segurança: Projeto de Rede de Modo Seguro, Comunicação Criptografada (WEP, WPA e WPA2), Filtro de Endereços MACs (permite acesso somente de dispositivos desejados), Filtro de Protocolos, desabilitação de Informações SSID de *Broadcast* e Assinalamento de Endereços IPs (Estático ou Dinâmico).

c) Proteção de Dados e Mecanismos de Segurança no Acesso ZigBee

ZigBee é o padrão internacional aberto (*ZigBee Alliance*) para as redes pessoais PAN (*Personal-area networks*) visando baixo custo, baixo consumo de potência, confiabilidade, comunicação bidirecional e comunicação sem fio para aplicações de curto alcance. Possui 4 níveis de comunicação: Físico (PHY), Controle de Acesso ao Meio (MAC), Rede (NWK) e Aplicação (APL). Os 2 níveis mais baixos são especificados pelo padrão IEEE 802.15.4, ficando o ZigBee propriamente dito, nas Camadas mais altas (Rede e Aplicação). ZigBee possui uma segurança muito boa.

A camada MAC possui os seguintes serviços de segurança: Controle de Acesso (*MAC Address*), Comunicação Criptografada usando Chaves Simétricas, Integridade de Quadro através de Cheques de Redundância CRC e Sequencialidade de Quadros. Essa camada possibilita 3 modos de operação: Não seguro, Lista de Controle de Acesso com dispositivos

permitidos e Seguro. Adicionalmente, o ZigBee também especifica seu próprio modelo de segurança que inclui Estabelecimento de Chave Criptográfica, Transporte de Chave, Proteção de Quadro e Gerenciamento de Dispositivo. A Criptografia no ZigBee pode utilizar chaves de 128 bits ou AES, possuindo 3 tipos de chaves: chave de Rede (usada por todos os nós da rede), Chave de Link (chaves de sessão secretas, entre dispositivos conectados) e Chave Mestre (usada para gerar a Chave de Link). A Chave de Rede já deixa a Rede ZigBee bastante segura pois proíbe que dispositivos não autorizados entrem na rede. O uso do Centro de Controle ZigBee (TC: *Trust Center*) exige que todos os dispositivos para entrar na rede sejam cadastrado e respondam a único TC. É ele que distribui e armazena as chaves dos dispositivos da rede.

d) Proteção de Dados e Mecanismos de Segurança no Acesso Bluetooth

O Bluetooth é um padrão internacional aberto para comunicação via rádio em curtas distâncias, usado também para redes pessoais PAN. Possui os seguintes requisitos de segurança: Autenticação, Criptografia e Autorização. Trabalha com 4 modos de operação: Procedimentos de Segurança não utilizados, Autorização no estabelecimento do link, Autenticação e Criptografia para todas as conexões, e Chave de Link Autenticada e não autenticada. Além dos modos de aparelhamento e autenticação, o Bluetooth provê 3 modos de criptografia: Sem Criptografia, Chaves Criptográficas usadas somente para o tráfego endereçada individualmente (não sendo utilizada para tráfego *broadcast*) e Criptografia usando chave de *Link* Mestre para todos os tipos de tráfegos.

2.6) Gerenciamento dos Elementos da Rede IoT

O crescimento das redes de transporte [P16] e a complexidade dos equipamentos de rede, tratando diversos serviços de rede ao mesmo tempo (voz, dados e vídeo) aumentou o interesse em monitorar e otimizar o uso dessas redes e seus equipamentos e serviços, constituindo assim o Plano de Gerência [P14], adicionalmente aos Planos de Dados e de Controle. O Plano de Gerência utiliza o NMS (*Network Management System*) atuando em regime 24/7 para monitoramento remoto, operação, manutenção e análise de desempenho de redes e equipamentos. O Protocolo SNMP [4], parte da Arquitetura TCP/IP, foi o escolhido como base de comunicação internacional e aberta de gerência de redes.

As seguintes funções fazem parte da gerência da rede: supervisão e monitoração das sub-redes com seus equipamentos e recursos, medição da utilização dos recursos, configuração dos equipamentos para funcionamento, configuração dos canais de transmissão, disponibilidade de recursos, manutenção dos equipamentos, provisionamento, confidencialidade de dados, integridade de dados e controle de acesso. Adicionalmente, pode-se gerenciar falhas, tráfego e segurança.

O Gerenciamento e a Supervisão Remota de Equipamentos e Redes foram desenvolvidos nos anos 80 para as Redes de Telecomunicações e Redes de TI; teve o objetivo de agilizar a atuação remota em problemas dos equipamentos e redes, os quais passaram a ser acompanhados apenas remotamente, sem pessoal local. Inicialmente utilizava protocolos proprietários para sua execução. Ganhou muita importância mundial, o que levou a órgãos internacionais como ISO, ITU-T e IETF (*Internet Engineering Task Force*) gerarem

padronização internacional aberta para essa comunicação. Ganhou ainda maior importância com sua expansão para Gerência de Redes, contemplando novas funcionalidades de Gerência de Configuração, Falhas, Tráfego, Desempenho, Segurança, Contabilização, etc. Está espalhado por todas as camadas funcionais e camadas de protocolos de comunicação, conforme mostrado na Figura 6. O padrão que se tornou de fato no mundo da Internet foi o SNMP (*Simple Network Management Protocol*) [04], padronizado pelo IETF através da RFC 3584, Gerencia de dispositivos em Redes IPs, ainda muito utilizado atualmente em Servidores, Comutadores(*switches*), Roteadores, Repetidores, *Gateways*, Estação de Trabalho, Impressoras, *racks*, etc; pode ser utilizado inclusive para dispositivos da IoT. Trabalha com o conceito hierárquico de Gerente/Sub-Agente/Agente atuando sobre os objetos da MIB (*Management Information Base*) com Mensagens dos seguintes tipos: Comando/Resposta (Leitura e Escrita) e Mensagem Espontânea (TRAP). Adicionalmente, possibilita a manipulação de dados através do Modelo de Dados MIB (*Managment Information Base*), onde os dados são definidos de forma bilateral permitindo seu acesso e modificação.

Especifica (na versão 1) quatro tipos de unidades de dados (PDU):

1. *GET*, usado para retirar um pedaço de informação de gerenciamento.
2. *GETNEXT*, usado interativamente para retirar sequências de informação de gerenciamento.
3. *GETBULK*, usado para retirar informações de um grupo de objetos.
4. *SET*, usado para fazer uma mudança no subsistema gerido.
5. *TRAP,* usado para reportar uma notificação ou para outros eventos assíncronos sobre o subsistema gerido.

No nosso modelo de Simulação de Rede da IoT da FT (Cenário 12), foram contempladas mensagens do tipo TRAP (do Mediador para a Aplicação SNMP) e Comandos/Respostas (da Aplicação SNMP para o Mediador e depois retornando para a Aplicação SNMP). A taxa de geração das mensagens TRAP e Comandos foram de EXPO [0,6], isto é, 1,67 pacotes/segundo (= 1/0,6). Esta tese foca também em Administração de Tráfego e Planejamento de Redes.

A Rede IoT também poderá desfrutar do uso do SNMP, pois possuirá equipamentos e elementos a serem supervisionados remotamente. Devido ao grande volume de objetos/coisas/dispositivos a serem supervisionados, é interessante que sejam utilizados elementos mediadores que efetuem essa coleta de informação de estado dos dispositivos, além da coleta de informações ambientais dos mesmos, deixando assim a aplicação sem esse ônus. Poderão ser aproveitadas temporariamente soluções proprietárias deste gerenciamento/supervisão.

O artigo de Sallabi et al.[44] apresenta uma Proposta de Arquitetura para Sistemas de Gerenciamento de Redes IoT, baseada no Modelo TMN (Rede de Gerenciamento de Telecomunicações) da ITU (União Internacional de Telecomunicações), comentando que a área de Gerenciamento de Redes IoT está pouco pesquisada, devendo aparecer ainda muitos trabalhos de pesquisas. Apresenta também um Estudo de Caso para *Smart Healthcare,* aplicável a Pacientes nos contextos de Residência (Fixo), Escritório (Móvel) e Viagem. Cada um desses contextos exige requisitos de comunicações diferentes. Comenta que as Empresas de Plano de Saúde serão as grandes interessadas em oferecer esse novo tipo de serviço que objetiva retirar pacientes mais cedo do hospital, contratando Empresas de Telecomunicações ISP e Cuidadoras de Pacientes (Novo Modelo de Negócio). Comenta na utilização do

Protocolo SNMP [4] como base para a Comunicação de Gerenciamento. O assunto Gerenciamento de Rede IoT está no estado da arte sendo uma boa área de pesquisa.

O artigo de Samaniego et al.[41] apresenta o Gerenciamento de Recursos Heterogêneos da IoT, onde se obtém os dados. Esses recursos normalmente são limitados e trabalham com soluções de protocolos proprietários. Cada vendedor oferece sua própria comunicação proprietária visando compatibilidade, eficiência e segurança na comunicação do ambiente restrito até o ambiente de nuvem. A necessidade de padrões tem influenciado que usuários exijam implementações de interconexão de coisas heterogêneas seguindo os padrões de gerenciamento ITU-T M.3400. Esse artigo apresenta a criação de Recursos Virtuais rodando em Dispositivos de Computação *EDGE* na nuvem, adotando o Protocolo CoAP (*Constrained Application Protocol* : RFC 7252) na comunicação do Recurso Virtual (com estado (usando *CoAP REST* para buscar os estados) ou sem estado(usando *CoAP OBSERVE* para receber as atualizações)) e a Linguagem de Programação *GO* para construí-los. A Arquitetura foi desenvolvida em 3 Camadas: *View Abstraction Layer* (VAL), *Hardware Abstraction Layer* (HAL) e *Physical Layer* (PL: Sensores). Foi utilizada Emulação de Clientes para análise experimental.

Capítulo 3 : Levantamento Bibliográfico

Neste capítulo aborda-se o levantamento bibliográfico efetuado no início da tese para detectar as recentes pesquisas sendo feitas nos ambientes acadêmicos. A metodologia utilizada na pesquisa bibliográfica possui 7 passos [57] [P1]:

- Definição do tópico de pesquisa;
- Definição dos conceitos envolvidos;
- Fontes bibliográficas consultadas;
- Definição dos termos de busca;
- Definição da estratégia de busca;
- Definição de critérios de inclusão e exclusão;
- Apresentação do Fluxograma Prisma.

O artigo [P1] já teve até 18/agosto/2019, o total de 864 consultas/leituras no ResearchGate, mostrando assim sua boa divulgação e importância para ambientes acadêmicos.

Seguindo o Fluxograma Prisma (Identificação, Seleção, Elegibilidade e Inclusão), pesquisaram-se 3 bases de dados, conforme mostrado na Figura 8 abaixo: IEEE XPLORE, SCIENCE DIRECT e SBU(Unicamp). Foram utilizadas as seguintes palavras-chave: "IoT" + "RFID". Foi possível localizar mais 26 artigos relevantes para a área IoT/RFID. Essa metodologia deverá ser complementada com os novos artigos estudados na pesquisa da tese, localizando os novos artigos da área.

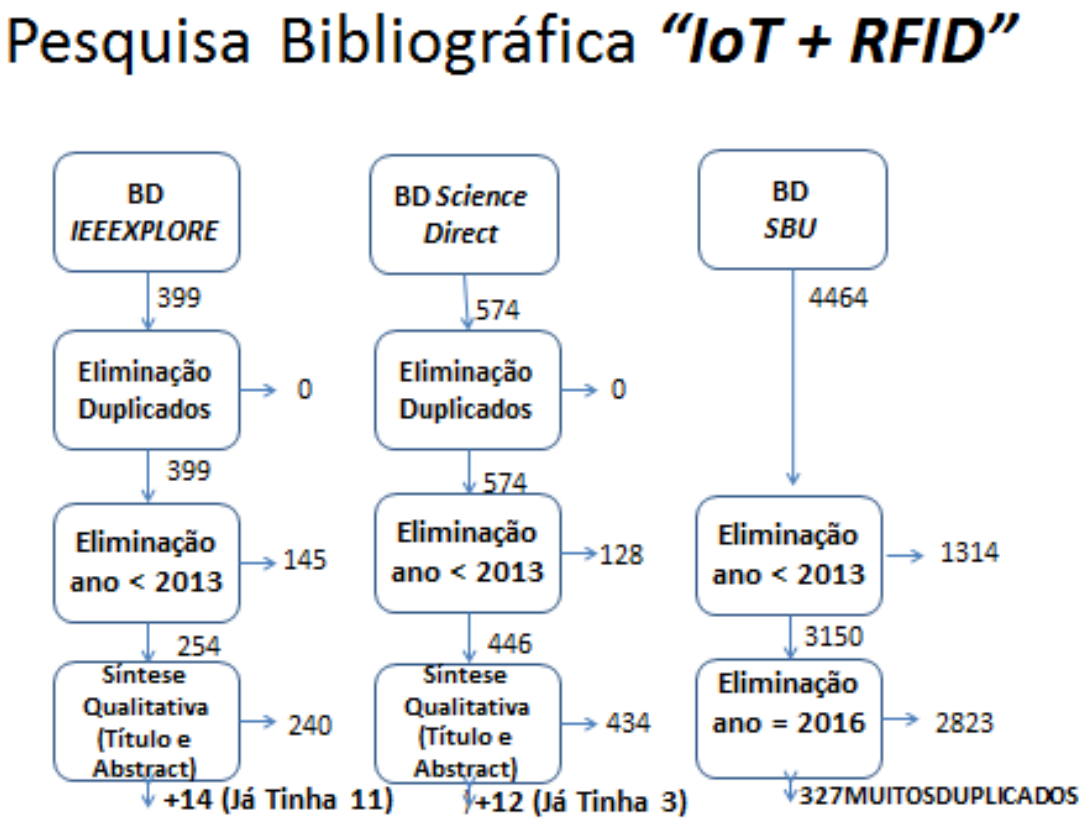

Figura 8: Fluxo de informação com as diversas fases da revisão bibliográfica [P1].

Com os filtros adequados de ano de publicação (2013 em diante) e análise de título/abstract do artigo, foram selecionados os seguintes volumes de artigos:

IEEE *XPLORE*: 399 artigos que foram filtrados por anos recentes para 254, selecionando 25 artigos por assuntos ligados à pesquisa;

SCIENCE DIRECT: 574 artigos que foram filtrados por anos recentes para 512 e depois para 446, selecionando 15 artigos por assuntos ligados à pesquisa;

SBU: 4464 artigos que foram filtrados por anos recentes para 3150, selecionando 327 artigos por assuntos ligados à pesquisa. Com muitos artigos duplicados, foram mantidos os artigos anteriores. Foram acrescentados também 9 artigos retirados anteriormente de fontes diversas.

O processo de exclusão é necessário para diminuir o volume de artigos a serem estudados e focar no assunto a ser pesquisado; utiliza-se neste processo a análise do título e do *abstract* a fim de selecionar os artigos que se aproximam da área de pesquisa.

Com a palavra-chave "IoT + RFID" existem as seguintes áreas de pesquisa nos artigos selecionados:

- IoT Aplicação : *Smart Health*, UPS(*Uninterruptible Power Supplies*), *Building*, *Manufacturing;*
- IoT Internet: nuvem, IPSO, conteúdo (HTTP), SNMP e simulação de rede;
- IoT Mediador: Qualidade de serviço (QoS), operação e manutenção, segurança;
- IoT Objetos: RFID (Leitor e etiqueta RFID), redes de sensores e atuadores.

Os artigos selecionados foram inseridos na ferramenta Mendeley, visando um registro das referências do estado da arte e acompanhamento da sua evolução. Foram organizados visualmente usando um mapa conceitual, conforme mostrado na Figura 9. As redes de sensores são mais antigas e possuem um volume muito grande de artigos; a RFID é a grande novidade e parceira da IoT. Os artigos selecionados estão apresentados e detalhados no Item 3.1.

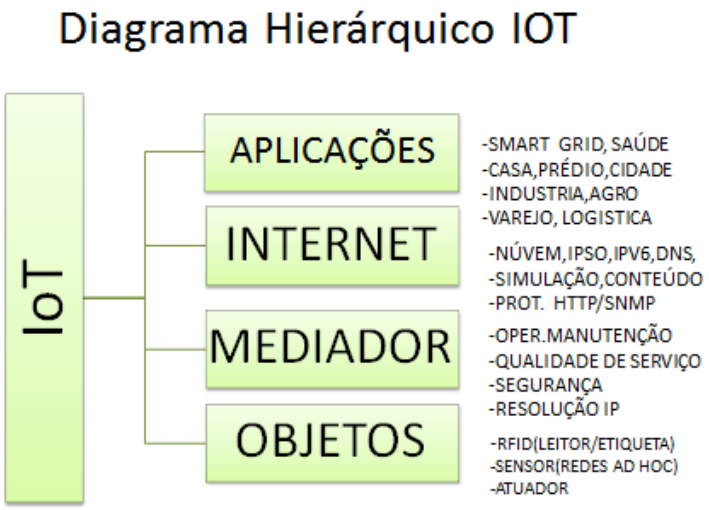

Figura 9 : Diagrama Hieráquico IoT (Mapa Conceitual) [P1].

A Figura 10 apresenta a distribuição dos artigos selecionados nos anos de suas publicações (2001-2016, sendo 1 = 2001, 2 = 2002, ...), mostrando que a maioria são artigos são recentes.

Número de Artigos/ano

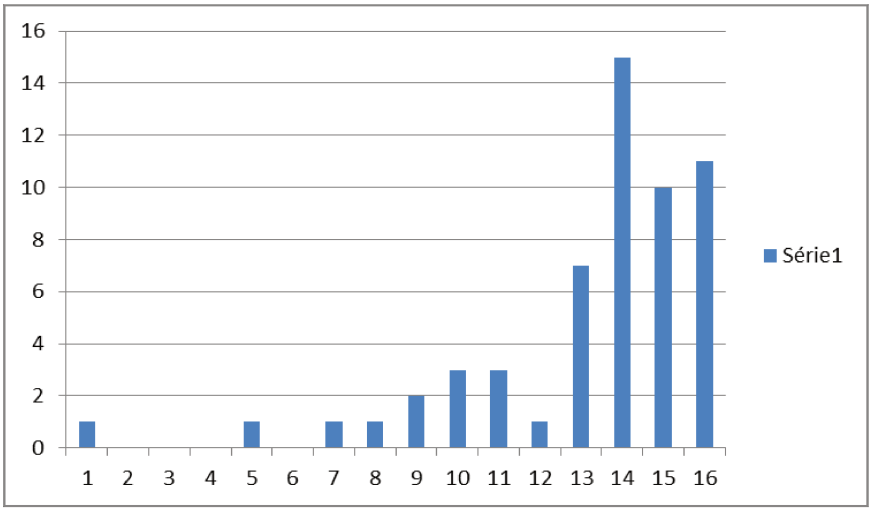

Figura 10 : Pesquisa IoT + RFID : Numero de artigos/ano(20xy) [P1].

As seguintes frentes de pesquisas atuais foram observadas na IoT :

- Padronização Internacional da IoT, RFID e IPSO;
- Desenvolvimento de redes de sensoriamento ambiental;
- Desenvolvimento de aplicações de sensoriamento industrial e *Smart Grid* (Rede Elétrica);
- Desenvolvimentos de Redes de Sensores ZIGBEE e AdHoc;
- Desenvolvimento de placas de interfaces inteligentes tipo Arduíno.

As seguintes tendências de pesquisas de desenvolvimento futuro foram observadas na IoT:

- Novas aplicações *smart;*
- Segurança da informação;
- Gerência, operação e manutenção da rede IoT;
- Qualidade de serviço (QoS) para a rede IoT;
- Novos equipamentos mediadores (*Middleware*);
- Aplicações em nuvem (*Cloud e Fog*);
- Bases de dados *Big Data*, com processo de mineração;
- Interfaces IP simplificadas (Micro IP) para comunicação dos objetos;
- Novos sensores acoplados nas etiquetas RFID;
- Leitores RFID capazes de leitura de sensores;
- Lógicas Fuzzy de mudança de modo de operação;
- Lógica de Predição.

“Frente de pesquisa” é o que está sendo feito atualmente e “Tendência de Pesquisa” é o que será feito futuramente.

Conclui-se que a IoT acoplada às tecnologias RFID, sensores e atuadores, permitirá o desenvolvimento de muitas novas aplicações, potencializando novos modelos de negócios, abrangendo todos os setores da economia, e funcionará como alavanca para o incremento

globalizado da economia, constituindo-se em um campo vasto para o incremento das atividades dos profissionais do setor de telecomunicações e de computação.

Durante os Estudos dos Cenários e Casos de Estudo, mostrados no Capítulo 5, foram pesquisados e estudados novos artigos específicos para cada assunto pesquisado, os quais foram citados e descritos resumidamente (*Related Work*) em cada artigo. Esse conjunto de novas referências forma uma complementação da Pesquisa Bibliográfica original, agora por área de pesquisa desenvolvida.

3.1) Análise dos Artigos selecionados na Pesquisa Bibliográfica, por Grupo Funcional

Apresentam-se a seguir os artigos selecionados na Pesquisa Bibliográfica, por Grupo Funcional.

3.1.1. Aplicações SMART IoT: Health, UPS, Infraestrutura, Indústria e outras

Esta seção apresenta os artigos relacionados com as aplicações *Smart* da IoT.

O artigo de Joshi et al.[7] apresenta uma revisão sobre a IoT e suas aplicações, Monitoramento Ambiental, Gerenciamento de Infraestrutura, Sistemas Médicos e de Assistência Médica, Aplicações Industriais, Gerenciamento de Energia, Sistemas de Transportes, Automação Residencial e de Prédios, Gerenciamento de Cidades (*SMART CITY*). Apresentam-se os seguintes desafios: Protocolos, Redes Limitadas, Segurança, Interoperabilidade, Limitações de Energia nos Sensores e Antenas Pequenas RFID.

O artigo de CARNOT et al.[8] apresenta a IoT formada com seus Objetos Inteligentes Interligados, com suas aplicações: Infraestrutura de Cidades, Serviços Móveis, Distribuição em Massa, Transporte e Aeronáutica e Residência Inteligente. Cita também os principais desafios atuais: Projeto e Integração das Coisas (Objetos Inteligentes), os Objetos Interconectados e Serviço de Gerenciamento.

O artigo de Vermesan et al.[9] apresenta um grande *roadmap* de Pesquisas Estratégicas da IoT : apresenta a Visão Geral da IoT, suas Tecnologias, suas Aplicações e Tendências de Tecnologias (Segurança da Informação, *Cloud e Big Data*).

O artigo de Gubbi et al.[10] apresenta uma Visão Geral da IoT com seus elementos de Arquitetura, Desafios existentes e suas tendências: Sensoriamento Eficiente de Energia, Redes Reprogramadas Seguras e com Privacidade, Qualidade de Serviço de uma Rede Heterogênea, Novos Protocolos, Sensoriamento Participativo, Mineração de Dados, Visualização baseada em GIS (Geoprocessamento), Computação em Nuvem e Atividades Internacionais de Padronização.

O artigo de Al-Fuqara et al.[11] apresenta um *survey* de IoT em Tecnologias Alavancadoras, Protocolos e Aplicações, dando ênfase a RFID, Sensores Inteligentes e Protocolos Internet. Apresentam-se as principais Aplicações IoT: Industria, Transporte, Saúde, Agricultura, Casa Inteligente, Mercado(Varejo e Atacado), Escola e Veículos. A IoT

apresenta os seguintes Elementos: Identificação, Sensor, Comunicação, Computação, Serviços e Semânticas. Comenta que os desafios aparecem em Segurança e Privacidade, Análise de Dados (*Big Data*), Computação *Cloud* e *Fog*. Comenta a necessidade de utilização de Equipamentos Mediadores e *Gateway*, visando a interoperabilidade entre sistemas heterogêneos.

a) Aplicações de Monitoramento Ambiental e de Prédios Inteligentes

O artigo de Moreno et al.[12] apresenta uma Aplicação IoT de Prédios Inteligentes para viabilizar a Eficiência Energética (Iluminação, Ar Condicionado e Segurança), tendo em vista que a Eficiência Energética é reconhecida como um objetivo internacional para promover a sustentabilidade energética do planeta. Foram selecionados 3 Prédios Inteligentes como referência onde foi instalada a Plataforma de Automação para monitorar Energia e onde foi obtido uma economia de 23% da Energia.

O artigo de Silva et al.[13] apresenta uma Aplicação de Monitoramento Ambiental utilizando Redes de Sensores Sem Fio de Baixo Custo, para monitorar Temperatura, Humidade Relativa e Pressão Atmosférica, através de 4 Nós Sensores e uma Rede ZIGBEE com um Nó Coordenador. Esse Coordenador coleta as medidas dos sensores, armazena esses dados em Memória *Flash* e envia-os através de uma Página HTML que pode ser acessada por um Endereço IP. O Coordenador também acompanha a potência do sinal de transmissão de cada sensor e coloca o *timestamp* (Carimbo de Tempo) nas informações medidas usando um relógio de tempo real; utiliza um Microcontrolador de 32 bit para processamento.

b) Aplicações Industriais

As Aplicações Industriais foram as primeiras a serem desenvolvidas na IoT.

O artigo de Kubo[14] apresenta uma Solução de RFID Industrial na IoT, focando no uso de RFIDs e de Mediadores; apresenta a tendência de aparecer novas aplicações nos setores de Alimentação (Gado e *Food*), Gerenciamento de *Container*, Hospital e Minas. Apresenta um Sistema IoT composto por *Tags* RFID ligadas a Leitores RFID, ligados ao Mediador SAVANT, o qual armazena os dados e os envia para a Internet.

O artigo de Sallabi et al.[15] apresenta um *survey* da Aplicação da IoT em Ambientes Industriais; apresenta as Tecnologias envolvidas, a Arquitetura IoT com 4 Camadas, a Arquitetura IoT orientada a Serviço (SOA), os Itens de QoS e os Desafios de Pesquisa existentes : Projeto de Arquitetura voltada a Serviço (SOA), Interoperabilidade em Redes Heterogêneas (Endereço, Identificação, Conteúdo), Métodos de Descoberta de Serviços, Interligação com Sistemas Legados, *Big Data* e Mediadores, Segurança da Informação e Proteção de Privacidade, Evolução da RFID para contemplar Sensores, Integração com Redes Sociais, Conexão com a Cloud (*Web of Things*), *Green* IoT Tecnologias (Economia em Energia), Técnicas de Inteligência Artificial para *Self-Configuration/Optimization/ Interprection/Healing.*

O artigo de Zhuming Bi et al.[16] apresenta o uso da IoT para Sistemas Empresariais de Indústrias Modernas; mostra a evolução passada pela Indústria, tipos de Sistemas Industriais, Sistema de Aquisição de Dados na Indústria (Sensores e Compartilhamento dos Dados), Requisitos Críticos para o Ambiente, Evolução da Infraestrutura de TI, Tecnologias Críticas para a IoT (Sensores, RFIDs, Redes de Sensores WSNs, Computação em Nuvem, IPV6, WiFI

e WIMax, ZigBee, Bluetooth, Plataforma Móvel, Roteamento Eficiente em termos Energéticos, Agregação de Dados, Gerenciamento de Dados) e a Criação de Novas Aplicações IoT.

O artigo de Kortuem et al.[17] apresenta a utilização de Objetos Inteligentes em Ambientes Industriais através de Blocos de Construção da IoT, Objetos Inteligentes e Tipologia de Objetos Inteligentes. A combinação da Internet com as tecnologias de Comunicação de Campo Próximo (NFC), localização em tempo real e sensores embarcados, transformaram os objetos atuais em objetos inteligentes que podem entender e reagir ao seu ambiente, possibilitando a criação de numerosas e complexas aplicações.

c) Monitoração Remota de Saúde

A Monitoração Remota de Saúde foi aplicada para Pacientes Humanos, Sistemas de Baterias e Infraestruturas da Cidade (Pontes, Rodovias, Prédios, Túneis).

O artigo de Aono et al.[18] apresenta a Monitoração de Infraestrutura utilizando uma Rede IoT com Sensores Piezoeléctrico e de 3 Eixos. Trabalha com Algoritmos de Predição de Tempo de Vida da Infraestrutura, utilizando Variáveis de Carga com Distribuição Gaussiana CDF. Esse sistema pode monitorar Pontes, Túneis, Prédios e Estradas. Os Sensores ficam espalhados dentro do Concreto e do Asfalto, comunicando-se com o Leitor RFID através de Comunicação Sem Fio.

O artigo de Laplante et al.[19] apresenta uma Solução de *Helthcare* para Monitoração de Paciente na IoT, mostrando o Potencial das Aplicações Médicas Remotas e seus desafios. Comenta que é uma solução que envolve Hospital, Plano de Saúde, Cuidadores e Empresas de Telecomunicações, com os seguintes desafios: Segurança da Informação, Perda de Privacidade e Informações Confiáveis. Comenta que a necessidade desses Serviços será cada vez mais crescente, principalmente para a população mais idosa e mais remota dos centros urbanos.

O artigo de Raiput et al.[20] apresenta uma proposta de Arquitetura IoT para Sistemas de Monitoração de Saúde, contemplando a utilização de Sensores de Temperatura e Batimento Cardíaco, Placa de Inteligência Arduíno, Envio de Dados para a Nuvem através do Protocolo HTTP, dados esses que podem ser acessados pelos *Smarthphones* Móveis.

O artigo de Lukovic et al.[21] apresenta uma Metodologia para Manutenção Proativa de UPS (*Uninterruptible Power Supplies*), baseada em Monitoração online de Estado de Saúde das baterias, utilizando Sensores para a Monitoração Remota das Baterias. Tem como evolução o uso de Sistema Preditivo e a Utilização de RFIDs. A análise analítica dos dados permite a predição de falhas de componentes. O objetivo final é aumentar a confiabilidade dos dispositivos UPS, diminuir o custo da manutenção e aumentar a disponibilidade do dispositivo.

O artigo de Kourtuem et al.[22] apresenta uma Aplicação de Monitoramento de Segurança e Saúde em um Ambiente Industrial, utilizando Redes de Sensores ou Objetos Inteligentes, mostrando que existe a possibilidade de acrescentar *tags* RFID no Equipamento, Crachás de Funcionários e Sensores de Vibração e Barulho, podendo até gerar uma Futura Patente.

O artigo de Amendola et al.[23] apresenta uma solução de Monitoração de Saúde baseada em IoT e RFID em Espaços Inteligentes. Apresenta um *survey* do Estado da Arte no uso de RFID para aplicações de Monitoramento de Saúde para coletar informações do Paciente (Temperatura, Pressão e Batimentos Cardíacos) e do Ambiente (Temperatura, Humidade e Gases). Os Espaços Inteligentes são usados para Localização dos Objetos e Paciente dentro da Residência. Comenta que ainda existem desafios na Confiabilidade de Sensores e na Autonomia de Leitores RFID, mostrando que poucos produtos estão comercialmente disponíveis para aplicações de larga escala.

O artigo de Catarinucci et al.[24] apresenta uma Arquitetura Baseada na IoT para Sistemas de *Smart Healthcare*, para Monitoração Automática e Acompanhamento de Pacientes, Profissionais da Saúde e Aparelhos Biomédicos. Propõe um Sistema Hospitalar Inteligente capaz de coletar em tempo real as informações do paciente e do Ambiente. Utiliza Protocolos de Comunicação CoAP/IPV6 sobre Redes Locais Pessoais sem fio (6LoWPAN) de baixo consumo. Oferece Serviço de Acesso de Informação local e remoto via *Web Service* REST. Utiliza uma Rede Híbrida Integrada RFID-WSN 6LoWPAN com interoperabilidade com a Internet usando o Paradigma de REST Solicitação/Resposta em Mensagens CoAP, o qual é um dos protocolos de comunicação mais usados na IoT, por ser leve e parecido com o HTTP (Modelo de Interação Solicitação/Resposta URI); possibilita também que o cliente receba Notificações de toda mudança de estado dos recursos os quais foi ligado (*subscribed).*

O artigo de Yang et al.[25] apresenta uma Plataforma IoT de Saúde baseada na Integração de Blocos Funcionais Inteligentes: Bio Sensores (Bio-Patch), a Caixa Médica Inteligente (iMedBox) e o Pacote Inteligente de Remédios (iMedPack); visa a Monitoração Remota de pacientes. Com essa solução, a Aplicação IoT de Health fica dividida em 3 partes: *Cloud, Home* e Corpo. A iMedbox funciona como uma estação que prove interoperabilidade com a Rede IoT. O iMedPack controla a Não-Conformidade no uso dos Remédios Receitados pelo Médico, avisando o paciente no horário da medicação. O Bio-Patch monitora os Sinais Vitais do Paciente.

O Artigo de Santos et al.[26] apresenta o uso da IoT e de Objetos Inteligentes para Monitoração e Controle da Saúde (*M-Health*), usando Etiquetas RFID para uma identificação rápida e precisa de cada Entidade *Smart*, possibilitando um acesso em qualquer lugar e rápido dos Registros de Saúde Pessoal (PHR). A Etiqueta RFID possui um microchip capaz de armazenar um Número de Série que identifica a pessoa, objeto ou coisa. O Leitor RFID recupera esse Número Serial sem contato físico. No contexto de Saúde, as preocupações com Segurança e Privacidade são imperativas. Esse artigo apresenta uma Nova Arquitetura de Serviço *Mobile Health*, Simples e Segura, usando Etiquetas RFID e Resolução ONS (*Object Name System).*

O artigo de Hossain et al.[27] apresenta uma Solução Industrial de IoT baseada na Nuvem (*Cloud*), possibilitando a Aplicação de Monitoração de Saúde. Com o crescimento de pessoas idosas e doentes, é urgente a utilização de Infraestrutura de Monitoramento de Saúde em Tempo Real para analisar dados de saúde de pacientes e evitar mortes. Essa solução é formada pelas tecnologias de comunicação, aplicações de interconexão, Objetos (Dispositivos e Sensores) e pessoas que vão trabalhar junto com os Sistemas Inteligentes para monitorar, acompanhar armazenar informações de saúde de pacientes.

O artigo de Lamprinakos et al.[28] apresenta uma Plataforma de Monitoração Remota Integrada para a Interoperabilidade de Serviços de *Telehealth* e *Telecare*. Comenta a

importância desses serviços devido ao aumento dos idosos, da necessidade de melhorar sua qualidade de vida e da necessidade da redução dos custos com saúde. A solução integra a Monitoração de Sinais Vitais do Paciente (*TeleHealth*) com a Análise de Sinais Ambientais baseada em Sensores da Residência do Paciente (*Telecare*), não sendo ainda uma solução de larga escala. Utiliza um *Middleware* com Arquitetura Voltada a Serviço (SOA) que coleciona os dados heterogêneos recebidos de *Gateways* de *Telehealth* e *Telecare*, além dos Alertas de emergência; envia os dados para Portais Web onde médicos e operadores podem acessá-los em Sistemas *Backend*. Observou-se que não utilizou dispositivos com Etiquetas RFID para Objetos, Pacientes, Profissionais e Equipamentos de Medidas Vitais.

d) Aplicações *SMART GRID* para o Setor Elétrico

O artigo de Kamouskos et al.[29] apresenta uma Simulação da Aplicação de *Smart Grid City* com Agentes de Software, onde foram simulados os Aparelhos de uma Residência, um Carro Elétrico e uma Usina Geradora de Energia Elétrica. Foi possível a criação de uma infraestrutura dinâmica que possa simular o ambiente da futura *Smart Grid City*.

3.1.2. INTERNET : Simulação, Conteúdo, SNMP, HTTP, Protocolos e CLOUD

Esta seção apresenta os artigos relacionados com a Internet, como Simulação, Redes Voltadas a Conteúdo, Protocolo de Supervisão de Rede SNMP, Protocolo de Web HTTP e Uso de Nuvens (*Cloud* e *Fog*).

a) Arquitetura de Protocolos

O IPT (Instituto de Pesquisa Tecnológica) apresenta o Laboratório de Testes de Protocolos de RFID e Móvel, sendo implantado no IPT [30]. A ideia é que esse laboratório sirva de referência para testes das Tecnologias utilizadas na IoT, formando uma massa crítica de conhecimento e habilidades requeridas para identificar e impulsionar novas oportunidades de negócios.

O artigo de Aguiar [31] apresenta a Arquitetura de Protocolos TCP/IP para o Plano de Dados e para o Plano de Controle: Lista todos os protocolos existentes e especificados nos padrões RFCs pelo IETF. Serve de Referência para a Evolução da IoT que terá sua base nas Redes de Arquitetura TCP/IP. Comenta que todas as redes devem ser baseadas nas Tecnologias IP: Tudo sobre IP e IP sobre tudo. Comenta também da evolução ocorrida na Arquitetura TCP/IP possibilitando a Comunicação *Multimidia, Multicast*, com Qualidade de Serviço (QOS), Segurança e Mobilidade.

b) Redes Voltadas a Conteúdo

O artigo de Cianci et al.[32] apresenta os Serviços Centrados em Conteúdo, para Cidades Inteligentes, utilizando Aplicações em Nuvem em uma Rede CCN (*Content-Centric Networking*). Esse tipo de solução pode ser utilizada em diversas aplicações de IoT: e-commerce, *Healthcare, Entertainment*, ITS e LBS. A Rede CCN é uma Rede *Overlay* sobre a Rede IP Tradicional, utilizando-se de protocolos CoAP (tipo HTTP) com simplicidade e segurança, permitindo o acesso das informações através de celulares.

O artigo de Amadeo et al.[33] apresenta uma Arquitetura de Redes Voltadas a Nomes (NDN) com a Utilização de Protocolos HTTP. A Arquitetura NDN é baseada na Arquitetura CCN, possuindo 2 tipos de pacotes: *Interest e Data.* Utiliza-se o conceito de Memória *Cache* para guardar os últimos nomes utilizados e evitar consultas desnecessárias.

O artigo de Kustscher et al.[34] apresenta o uso de Informações Identificadas por Nomes (Rede Voltada a Conteúdo CCN) utilizadas para a IoT. Essa rede é montada de forma overlay sobre a Internet e possibilita a Identificação da Informação por "nome" e não por Endereço de Nó Sensor, garantindo escalabilidade e segurança.

O artigo de Oliveira et al.[35] apresenta uma Proposta de Arquitetura para Gerência de Redes Orientadas a Conteúdo, sendo inter operável com Sistemas Legados. Apresenta uma Solução de Gerenciamento com *Proxy* SNMP CCN, de Rede Orientada a Conteúdo. As Redes CCN utilizam uma estrutura de nomes hierárquicos e legíveis (formados por sequências de caracteres e números) para identificar os conteúdos. A Rede CCN utiliza 2 tipos de Pacotes: *Interest e Data.* O Consumidor expressa seu interesse inserindo o nome do conteúdo desejado em uma mensagem do tipo *Interest* e a envia para a rede. O Produtor (ou algum *cache* no interior da rede) que possui tal conteúdo receberá essa mensagem e envia de volta ao consumidor uma mensagem do tipo *Data* como resposta. Mensagens Duplicadas são descartadas através da utilização de um Número Aleatório "*Nonce*" eliminando-se assim Loops de Rede.

O artigo de Suarez et al.[36] apresenta uma Arquitetura de Gerenciamento IoT Segura baseada em Redes Centradas em Informação (ICN). Essa arquitetura possui requisitos de nomenclatura, interoperabilidade, segurança e eficiência energética. Foi implementada uma Prova de Conceito da Arquitetura sobre uma Placa Arduíno, validando a solução, com fluxo de informação voltada a conteúdo.

c) Computação na Nuvem

O artigo de Nguyen et al.[37] apresenta uma Proposta de Desenvolvimento de Otimizações em Aplicações RFID na Nuvem, usando Algoritmos de Predição de Carga e *Load Balancing*. Comenta sobre os desafios existentes em Flutuações de Carga de um Número desconhecido de *Tags* Entrantes e Migração de Carga de Fluxos dos Leitores RFIDs. Visando resolver esses desafios, propôs um sistema que foca em Otimizações de Balanceamento de Carga (*Load Balancing*) para aplicações RFID desenvolvidas na Nuvem.

O artigo de Kafra et al.[38] apresenta uma solução segura de Autenticação para IoT rodando em Servidores da Nuvem. A solução de segurança utiliza Criptografia de Curva Elíptica (ECC) baseadas em algoritmos que dão melhor solução de segurança em comparação com Criptografia de Chave Pública (PKC), devido ao tamanho de chaves pequenas e computação eficiente. Esse artigo apresenta uma Segurança ECC baseada em protocolo de autenticação mutua para comunicação de Dispositivos Embarcados e Servidores de Nuvem usando *cockies* HTTP (*Hyper Text Transfer Protocol*), solução bem robusta contra-ataques múltiplos de segurança. A verificação formal do protocolo proposto foi executada usando a Ferramenta AVISPA, que confirmou sua segurança na presença de possíveis intrusos.

O artigo de Diaz et al.[39] apresenta um *survey* dos Componentes de Integração da IoT: Plataformas *Cloud*, Infraestrutura *Cloud* e *Middleware*. Adicionalmente, algumas propostas e técnicas analíticas de dados são apresentadas assim como diferentes desafios e pesquisas

abertas. A Computação na Nuvem possibilita acesso a redes de forma escalável a um *pool* de Recursos Computacionais Configurável. Comenta que a Computação em Nuvem complementa a IoT, tendo em vista que pode acrescentar inteligência aos simples objetos de sensoriamento; comenta também sobre a popularidade das Aplicações IoT: *Smart Home*, *Werables, Smart City, Smart Grid, Industrial, Connected Car, Connected Health, Smart Retail, Smart Supply-chain e Smart Farming*.

d) Simulação

O artigo de Lu et al.[40] apresenta um Procedimento de Otimização de Cobertura-K Fuzzy usando um Algoritmo de Simulação de Crescimento de Planta. A Otimização do Planejamento de rede é importante para o incremento de desempenho de Redes RFID. Esse artigo apresenta um Algoritmo eficiente para planejamento de Rede RFID baseado na Cobertura-K; o Modelo de Cobertura-K é formulado como um Problema de Otimização multidimensional com condições limitantes. Os resultados da Simulação mostram as medidas obtidas com o algoritmo escolhido em relação a outros algoritmos.

O artigo de Samaniego et al.[41] apresenta o Gerenciamento de Recursos Heterogêneos da IoT. Utiliza o Modelo de Recurso Virtual mapeado em Recurso Físico. Esse artigo apresenta a criação de Recursos Virtuais rodando em Dispositivos de Computação *Edge*, adotando o Protocolo CoAP (*Constrained Application Protocol* : RFC 7252) na comunicação do Recurso Virtual e a Linguagem de Programação GO para construí-los. A Arquitetura foi desenvolvida em 3 Camadas: *View Abstraction Layer* (VAL), *Hardware Abstraction Layer* (HAL) e *Physical Layer* (PL: Sensores). Foi utilizada Emulação de Clientes para análise experimental.

O artigo de Novak et al.[42]. apresenta uma Solução de Integração por simulações e Sistemas SCADA. As aplicações IoT não podem ser desenvolvidas e testadas sem os Modelos de Simulação e Acesso de Dados Online e Histórico. Esse artigo propõe uma Plataforma para Integração de Simulação e Sistemas Industriais SCADA suportando acesso a dados complexos e reuso de código de simulação. A ideia desta plataforma é conectar simulações, fontes de dados, otimizadores, outros cálculos e Sistema SCADA em um Ambiente Integrado. A maior contribuição desse artigo é o Modelo em Camadas da Arquitetura de Integração e a formulação de requisitos de integração no domínio de automação industrial. A solução proposta foi implementada e testada na Camada de Protótipo de Software.

3.1.3. MIDDLEWARE : QoS, OAM, ONS, SECURITY E SYSTEM

Esta seção apresenta os artigos relacionados com as Funcionalidades do *Middleware*.

O artigo de Mota et al.[43] apresenta um Mecanismo de QoS (Qualidade de Serviço) de RFID para Aplicações de Busca (*Tracking*) na IoT. Apresenta uma Solução de Otimização de Software da Comunicação entre a *tag* e o leitor RFID, onde as *tags* só vão responder a uma Solicitação de um novo leitor. Foi feita uma Simulação desta Otimização com a Ferramenta Ns-2 onde ficou comprovado que com o aumento do Número de *tags* conseguiu-se uma eficiência de até 43% na Redução no Número de Pacotes Transmitidos e consequente Consumo de Energia Elétrica, na Comunicação entre a *tag* e o leitor. Como trabalho seguinte, cita a pesquisa da quantidade de economia de Energia. Essa otimização de comunicação entre

TAG e Leitor RFID é algo simples, desenvolvida em software, que traz fortes economias no volume de pacotes trocados e consequente economia de energia.

O artigo de Sallabi et al.[44] apresenta uma Proposta de Arquitetura para Sistemas de Gerenciamento de Redes IoT, baseada no Modelo TMN (Rede de Gerenciamento de Telecomunicações) da ITU (União Internacional de Telecomunicações), comentando que a área de Gerenciamento de Redes IoT está pouco pesquisada, devendo aparecer ainda muitos trabalhos de pesquisas. Apresenta também um Estudo de Caso para *SMART Healthcare,* aplicável a Pacientes nos contextos de Residência (Fixo), Escritório (Móvel) e Viagem. Cada um desses contextos exige requisitos de comunicações diferentes. Comenta que as Empresas de Plano de Saúde serão as grandes interessadas em oferecer esse novo tipo de serviço que objetiva retirar pacientes mais cedo do hospital, contratando Empresas de Telecomunicações ISP e Cuidadoras de Pacientes (Novo Modelo de Negócio). Comenta na utilização do Protocolo SNMP como base para a Comunicação de Gerenciamento. O Assunto Gerenciamento de Rede IoT está no Estado da Arte, sendo uma boa área de pesquisa.

O artigo de Grabovica et al.[45] apresenta os Mecanismos de Segurança para Redes IoT usuárias de Tecnologias ZIGBEE, Bluetooth, RFID e WiFi. São mecanismos já existentes nos protocolos que podem ser utilizados para dar uma melhor segurança na Comunicação. O Assunto Segurança da Informação está no Estado da Arte de IoT.

O artigo de Gonçalves et al.[46] apresenta uma Arquitetura de Segurança para Aplicações de *Mobile E-Health* no Controle de Medicamentos. Comenta que por motivos de segurança, a Tecnologia RFID é a melhor a ser utilizada na Área Médica; serve para Identificação de Remédios, Equipamentos e Profissionais (Médico, Enfermeiro, Cuidadora, Farmacêutico), garantindo uma Identificação Única e Segura. Propõe uso de Mecanismos de Segurança nos Protocolos TCP/IP/HTTPS/IPSec. Comenta também sobre a Utilização de *LogIN*/Senha nos Aplicativos, garantindo a Identidade do Usuário. Comenta a Necessidade de se Utilizar Arquivos LOG contendo todas as Intervenções ocorridas com o Paciente. Propõe também a utilização de Protocolos de Segurança mais sofisticados e complexos, com o uso de Chaves Públicas e Privadas, Algoritmos *HASH,* Criptografias Simétricas e Assimétricas. É um assunto de alta complexidade que proporcionará muitas novas pesquisas.

O artigo de Raiput et al.[47] apresenta uma solução de *Middleware* (Mediador) para Etiquetas RFID e Rede de Sensores ZIGBEE, comentando que o Mediador tem funções de Concentração, Conversão de Protocolos, Comunicação com diversas Aplicações, Recepção de Informações, Filtragem, Agregação e Transmissão para Sistemas Aplicativos. Oferece Interfaces API para que as Aplicações não se preocupem com o Nível de Sensoriamento da Rede.

O artigo de Skorin-Kapov et al.[48] apresenta a Funcionalidade de Gerenciamento de Sensores com Eficiência Energética e Qualidade Contínua para Aplicações Móveis IoT. Apresenta as Restrições de Energia existentes em um Sensor, o grande volume de dados sensoriados e a necessidade de processamento desses dados usando *BIG Data*. Apresenta uma solução de *Middleware* chamado CUPUS para Aplicações Móveis.

O artigo de Sterle et al.[49] apresenta uma Arquitetura de Operação e Manutenção OAM voltada para Aplicações IoT para Ambientes IoT Heterogêneos. Essa arquitetura possibilita a coleta de informações de Redes Heterogêneas, do Nível Físico, Enlace, Rede e Aplicações

usando Métodos e Mecanismos de OAM, detectando Falhas e Isolamento, Medidas de Desempenho e Monitoração.

O artigo de Razzaque et al.[50] apresenta um *survey* sobre os mediadores existentes para a IoT. O mediador facilita o processo de desenvolvimento, integrando Sistemas Heterogêneos e Dispositivos de Comunicação, possibilitando a interoperabilidade de muitas aplicações e serviços. Existem diversas soluções de Mediação baseadas em Redes Sem Fio (WSNs), mas não considera os Leitores RFID, Comunicação M2M e Controle de Supervisão e Aquisição de Dados SCADA. Apresenta-se um conjunto de requisitos para o mediador IoT e mostra a lista de mediadores existentes.

O artigo de Skorin-Kapov et al.[51] apresenta uma solução de gerenciamento contínuo de sensor, voltado para qualidade, visando a eficiência energética de aplicações móveis IoT. Comenta que o grande volume de informações geradas pelo Sensor exige um bom Gerenciamento de Dados e da Energia Consumida em um sensor. Apresenta uma arquitetura de sistema baseado em *Cloud,* interconectado através do mediador do tipo *Publish/Subscribe* com a função de Gerenciamento de Sensor voltada para qualidade. O mediador gerencia com inteligência as leituras dos sensores, reduzindo atividades redundantes e consequentemente, reduzindo o consumo total de energia do sistema. A avaliação da solução foi feita utilizando simulação.

O artigo de Vinh et al.[52] investiga a Integração da IoT com a MCC (*Mobile Cloud Computing*) interconectados com dispositivos das tecnologias RFID, Redes de Sensores sem Fio e Bluetooth. A Nuvem pode ajudar a IoT nos desafios de Escalabilidade, Armazenamento de Dados, Processamento de Dados vindo de dispositivos heterogêneos e com Energia Limitada. A Computação em Nuvem oferece os serviços: *Network as a Service* (NaaS), *Infrastructure as a Service* (IaaS) *Software as a Service* (SaaS) e *Storage as a Service* (STaaS), abstraindo todos os tipos de Recurso de computação como Serviço. Funciona como se fosse uma *Utility* de Computação para que Usuários de Objetos Inteligentes possam acessar os recursos de computação necessários e pagar pelo seu uso, permitindo escalar o seu uso. A MCC é uma combinação da Computação em Nuvem com Redes Móveis para trazer benefícios para Usuários Móveis. O artigo investiga o Estado da Arte na convergência da MCC e a IoT no contexto de desenvolvimento de Aplicação *Smart Home*, apresentando sua Arquitetura de Sw. Utiliza Plataforma Arduino no *Gateway* e Tecnologia REST e BLE/Android no *Smartphone*, ajudando a autoconfiguração e a interação em tempo real.

O artigo de Sadok et al.[53] apresenta uma solução de *Middleware* para o Ambiente Industrial. Apresenta uma nova Arquitetura Distribuída para Monitoração e Controle de Sistemas de larga escala pela integração de Objetos Inteligentes Heterogêneos, o mundo dos dispositivos físicos, sensores e atuadores, dispositivos legados e subsistemas, cooperando para suportar Gerenciamento Holístico. Utiliza Arquitetura Orientada a Serviço (SOA), expondo em capacidades de Objetos por meio de *Web Services*, suportando interoperabilidade sintática e semântica entre tecnologias diferentes, incluindo Sistemas SCADA, formando um Sistema *Middleware* Orientado para a Indústria.

3.1.4. OBJETOS : RFID (LEITOR RFID, TAG, SYSTEM), SENSOR e ATUADOR

Esta Seção apresenta os artigos relacionados com os Objetos Inteligentes RFID, Sensor e Atuador.

O artigo de Capone et al. apresenta o modelamento e a simulação de melhorias de Eficiência Energética para o Padrão IEEE 802.15.4e DSME para Rede de Sensores sem Fio (WSNs) [54], usando a ferramenta de Simulação OPNET. Analisa o Consumo de Energia e propõe um conjunto de Incrementos para aplicações de Baixa Potência, permitindo uma redução de consumo de energia em 9%.

O artigo de Akyildiz et al.[55] apresenta um *survey* sobre redes de sensores sem fio com seus elementos, suas aplicações (ambientais, saúde, residencial e veicular), suas limitações (energia, processamento e memória) e camadas de protocolo. Os sensores possibilitam a medição de temperatura, humidade, movimento, claridade, pressão, liquidez, nível de barulho, presença ou ausência de algum objeto, nível de estresse, velocidade, direção e tamanho do objeto. Os sensores podem ser usados de forma contínua, detecção de evento, identificação de evento, localização e controle de atuadores. Possibilita sua atuação de aplicações militares, ambientais (incêndio em floresta e enchente), saúde e residenciais.

O artigo de Ursini et al.[56] apresenta uma metodologia de modelos analíticos e de simulação para o dimensionamento de redes de dados da FT UNICAMP, utilizando o Software de Simulação ARENA. São simulados os tipos de tráfego *Stream* e Elástico, observando os parâmetros de qualidade de serviço: vazão, atraso, variação do atraso e taxa de perda de pacotes.

O artigo de Emiliano et al.[P1] apresenta uma metodologia de execução de pesquisa bibliográfica na área de IoT+RFID, com resultados de buscas ocorridas nas bases de dados IEEExplore, Science Direct e SBU (Unicamp).

Capítulo 4 : Modelagem de uma Rede IoT Típica Usando Simulação Híbrida Incremental.

Neste capítulo será abordado o modelo de rede IoT usado na simulação híbrida incremental.

O Modelo de Rede criado [P12], principal contribuição desta tese, é hierárquico e está dividido em 3 níveis em que podem ser abrigadas as diferentes configurações do mundo real (Figura 11): Rede no Ambiente do Usuário (Casa, Automóvel (Bluetooth), Escritório, Prédio, Campus, Quarto de Paciente, Hospital), Rede Geográfica ligando o Ambiente do Usuário ao Mediador (Rede AdHoc Geográfica) usando acessos WiFi, Celular Móvel LTE ou Zigbee(AdHoc)) e Rede Internet (Ligando o Mediador a Aplicações na Nuvem).

O primeiro nível é executado dentro do Ambiente do Usuário usando Sensores, Atuadores, Etiquetas RFID/Leitores RFID, GPS e Redes de Sensores; normalmente existe um concentrador que junta essas informações em uma só mensagem; no caso do carro, é o computador de bordo. A interligação desses elementos pode ser feita por fio (*wired*) ou por rádio, através de Rede Bluetooth que tem em sua base uma rede AdHoc.

A comunicação interna pode ser feita usando Protocolos ***Bluetooth e RFID***. ***A comunicação externa*** poderá ser GLOBAL utilizando conexões ***celulares/adhoc (do tipo MANET e VANET)***, utilizando tecnologias WiFi, LTE e Zigbee (AdHoc).

O segundo nível diz respeito à Internet, conectividade do ambiente do usuário ao mundo externo, que é feita através da Rede AdHoc Geográfica, usando de tecnologias WiFi, Mobile LTE e Zigbee (AdHoc). A rede geográfica é formada por *clusters* que são compostos por N Nós Móveis (Parâmetro de Configuração), interligados com os *Cluster Heads* de saída dos pacotes para outros *clusters*. Cada *cluster* é simulado por meio de Blocos de Simulação *"Enter, Chance, Output CPU e Output"*.

O terceiro nível diz respeito à Internet, interconectando os Mediadores às respectivas Aplicações residentes na nuvem.

Existe também um quarto nível abstraído, que diz respeito à Aplicação IoT atuando sobre as emergências recebidas do ambiente do usuário.

a) Modelo da Rede Interna do Ambiente do Usuário:

O ambiente do usuário possui forte poder de computação, sensoriamento e comunicação, através do uso do Computador/Sensores/Atuadores/ Etiquetas e Leitores RFID//Interfaces de comunicação. Dessa forma, poderá coletar diversas informações internas/externas no ambiente e enviá-las agregadas para a Aplicação *Smart* na Nuvem, fazendo assim o papel de mediador usuário.

b) Modelo de Rede Geográfica

Esse modelo é usado para interconexão dos ambientes de usuários ao Mediador de Rede.

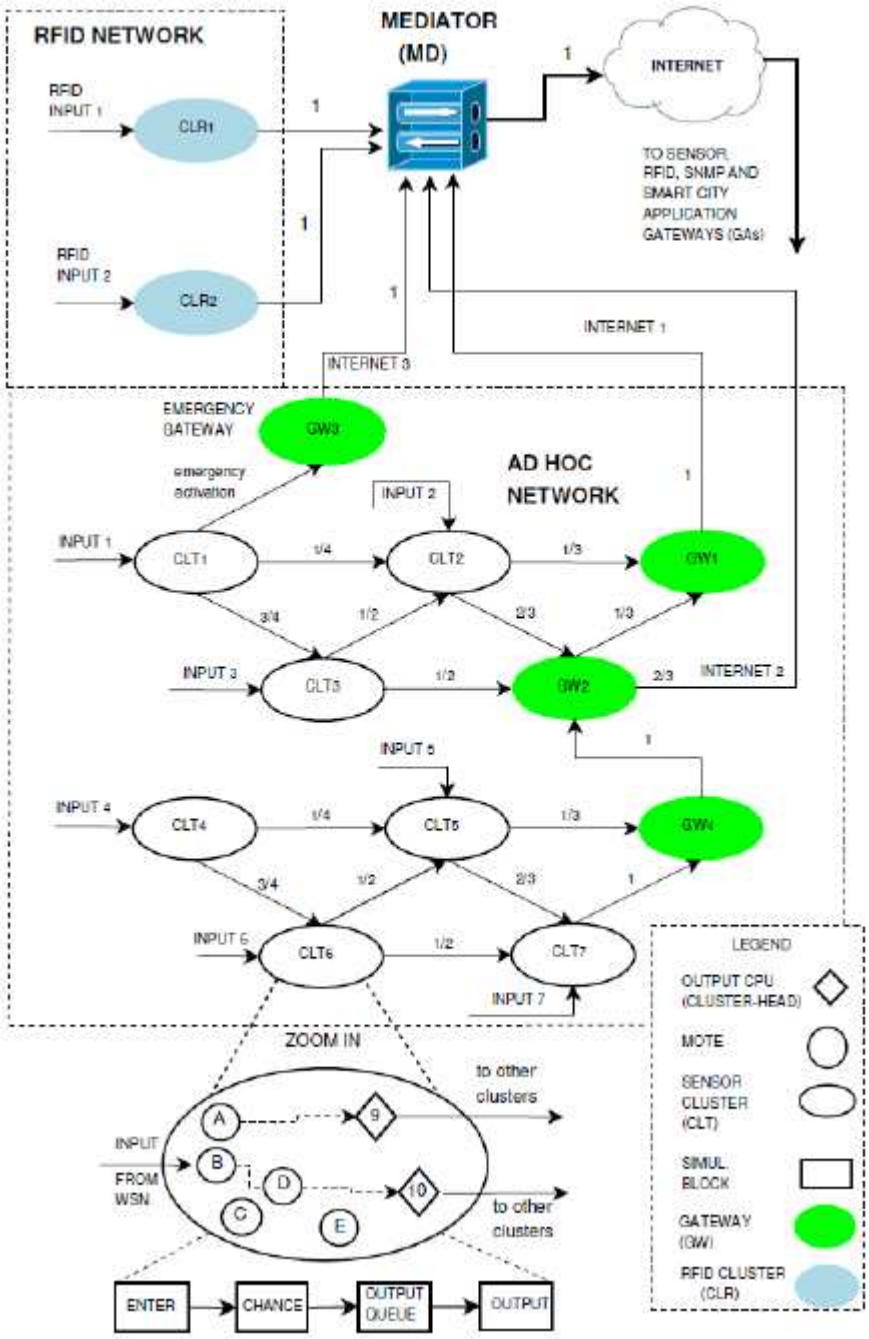

Figura 11: Modelo de Rede IoT Simulado [P12].

Um pacote IP é modelado como uma entidade que chega ao sistema e atravessa diversas filas no *cluster* antes de sua partida, isto é, antes de ser consumido pela aplicação.

O modelo de rede é hierárquico, composto por *clusters*, os quais também são hierárquicos pois contêm *motes* (nós Móveis), que por sua vez contêm CPUs múltiplas, permitindo diversas conexões em paralelo. Um *cluster* pode ter também CPUs de Saída múltiplas (*Multiple output CPUs*) permitindo diversas conexões em paralelo. Inerente a cada fila existe o Atraso de Espera antes que um pacote IP possa ser processado pelo servidor. Claramente, tanto o tempo de fila como o tempo de processamento estão sujeitos às distribuições estatísticas. Portanto, um *Cluster* de Rede pode ser visto como um conjunto de filas internas (cada uma associada com um *link* de saída).

Os componentes de rede propostos são: Mediador, Gateways e *Endpoints* (RFIDs e Sensores). A Figura 11 mostra o modelo de rede com suas entradas e saídas (pacotes IP) para cada *cluster*.

A parte superior do modelo inclui a Rede RFID com:

- 2 *clusters* RFID (CLR1 e CLR2) os quais executam a aquisição/entrada das informações das Etiquetas RFID; o número de *cluster* pode ser configurado;
- 2 entradas RFIDs as quais recebem os pacotes de dados gerados pelas Etiquetas RFID (Leitor RFID).

Inclui também a INTERNET a qual modela a Internet tradicional, com suas aplicações na nuvem. O Mediador MD também é um nó que contém uma ou mais CPUs; ele agrega e filtra as informações geradas pelas RFIDs e Sensores; é compartilhado por todas as sub-redes do modelo, isto é, ele executa as funções de mediação IoT e interconecta (fisicamente e logicamente) com outros elementos de rede com o propósito de mediar dados com as aplicações, eliminando das aplicações as funções de comunicação. Existem duas ou mais aplicações, que consomem as informações geradas pelas RFID e Sensores, como por exemplo: *Smart Green Building* (inclui o controle de atuadores de Luz, UPS (*Uninterruptible Power Supply*), ar-condicionado), *Smart City*, *Smart Transportation* ITS (*Intelligent Transportation System*), Catástrofe (*Disaster Recovery*) e Gerenciamento de Rede SNMP. Observe que o caminho das aplicações para os atuadores e os próprios atuadores em si, não são foco desta tese, e são abstraídos.

A parte inferior do modelo trata da Rede AdHoc com 2 sub-redes, que trafega informações de sensores. Consiste dos seguintes elementos:

- 7 *clusters* (CLT_1....CLT_7); eles não são móveis e homogêneos para simplificação. No entanto, o modelo não se restringe à adição de clusters heterogêneos. Cada cluster consiste de "n" nós móveis, onde n é um parâmetro de configuração; o número de *cluster* também pode ser configurado;
- 4 *gateways* ou Nós de Internet (GW_1....GW_4); ambos GW_1 e GW_2 são gateways de saída; GW_3 é um *gateway* de emergência, i.e. é usado como *gateway* sobressalente (*backup*) do GW_1. Quando o GW1 ficar sobre carregado em seus *buffers* internos; GW_4 e GW_2 são conversores de protocolos usados para integração de duas sub-redes;
- 7 Entradas: modela pacote de dados gerados pelos sensores IoT;
- 3 Saídas Internet: modelam o fluxo de pacotes IP de saída;
- Mobilidade do Nó: utiliza-se o SW MATLAB Random Way Point;
- Variáveis de Entrada: distribuições de tempo de chegada de dados e tempo de serviço no nó;
- Variáveis de Controle: probabilidade da conectividade no *cluster*; essa probabilidade é calculada pelo algoritmo *Random Way Point* (que depende de variáveis tais como *receiver threshold*, tamanho da área, tipo de antena e ganho, e coeficiente de perda de propagação do sistema, dentre outros;
- Variáveis de Saída: "*mean queue time*" e "*mean CPU utilization*" em cada *cluster* para uma dada posição dos nós dentro do *cluster*.

Cada *cluster* contém diversos nós (Figura 11) que por sua vez têm internamente uma ou mais *CPUs* (somente as *CPUs* dos nós 9 e 10 são mostradas para evitar sobrecarregar a figura, e por causa deles estarem conectados às saídas do *cluster* (*output CPUs*). O modelo é dinâmico e a Figura 11 mostra apenas uma foto representando um instante t no tempo. Por exemplo, no instante *t*+1 podem ter outros nós responsáveis pela transmissão de saída. Adicionalmente, cada *cluster* tem uma ou mais *output CPUs* que são usadas para seus canais/links de saída (Tabela 5). Essas " *CPUs* de Saída" são fixas em nosso modelo (sem comprometer as qualidades dos resultados), embora seja possível configurá-las para ter algum grau limitado de mobilidade também Os nós compartilham as *output CPUs* para retransmitir o tráfego de saída, desde que eles tenham conectividade, i.e. eles estarem com potência suficiente para acessar qualquer output *CPU* ou um nó intermediário.

Cada nó é modelado com 4 blocos de simulação conectados em série:

1. ***Enter block***: simula a chegada de um pacote no *cluster*. Conta o número de pacotes entrando no cluster;
2. ***Chance*** é um bloco Arena "DECIDE" e distribui os pacotes entre um conjunto de linhas de saída, onde cada linha é associada com uma fila de saída; um parâmetro importante neste bloco é a probabilidade de perda de pacote, e seu valor é obtido do caso de estudo. A probabilidade de um pacote ser retransmitido para um link de saída é inicialmente configurada, conforme mostrado na Fig. 11 (exemplo, 1/4 do *cluster* 1 ao *cluster* 2 e 3/4 do *cluster* 1 ao *cluster* 3);
3. ***Output queue*** representa o tempo de fila no link de saída;
4. ***Output cluster*** simula a saída (i.e. retransmissão) de pacotes de um *cluster*. É também, responsável pela contagem do número de pacotes deixando o *cluster*.

A Tabela 5 mostra o relacionamento do *cluster* / *gateways* para *output* CPUs. A coluna "*Probability*" é associada à coluna "*Output CPUs*". Cada probabilidade é usada para definir o gerenciamento de tráfego de cada nó de acordo com uma dada aplicação. Esses valores também indicam a probabilidade de um pacote ser servido por um indicado *output* CPU. Por exemplo, a probabilidade que o *cluster* CLT_2 envie um pacote para a output CPU_3 é 1/3, e essa probabilidade é 2/3 para *output* CPU_4. Esta configuração foi escolhida aleatoriamente e foi mantida durante toda a simulação. Nos casos reais medidas devem ser incorporadas para obter as probabilidades mais adequadas a cada caso.

Tabela 5: Configuração de Rede [P12].

Function	Probability	Output CPUs
GA_{12}	1	25
GA_{34}	1	28
GA_{57}	1	29,33
GA_{8}	1	19,34
AdHoc submodel	1,1,1,1	30,31,32,33
CLR_1	1	21
CLR_2	1	22
MD	1/2, 1/2	24, discard
GWI	1/3,1/3,1/3	23, 26, 27
GW_1	1	5
GW_2	1/3, 2/3	11,6
GW_3	1	14
GW_4	1	17
CLT_1	1/4, 3/4	1,2,20*
CLT_2	1/3, 2/3	3,4
CLT_3	1/2, 1/2	7,8
CLT_4	1/4, 3/4	12,15
CLT_5	1/3, 2/3	16,13
CLT_6	1/2, 1/2	9,10
CLT_7	1	18

* output-CPU 20 to GW_3 is used only in an emergency

Cada nó recebe pacotes em um *link* de entrada e retransmite-os para um dos enlaces de saída usando UDP sobre IP (*Datagram*). Como a chegada de mensagens para redes RFID e AdHoc pode ser modelada como um processo de Poisson, o volume de tráfego de cada nó individual pode ser estendido ao volume de tráfego de um *cluster* pela simples soma de taxas de chegadas Poissonianas. Assim, somamos as taxas de cada nó de um *cluster* de N nós.

O modelo adiciona duas ou mais aplicações representativas que consome a informação vinda do mediador: Gerenciamento SNMP, *Smart Green Building*, *Smart City*, ITS (*Intelligent Transportation System*). A Aplicação SNMP recebe mensagens TRAPS de supervisão vindas do mediador e troca Comandos e Respostas também. As aplicações *smart* típicas da IoT recebem informações e armazena-as em Banco de Dados na nuvem, que poderão ser acessadas posteriormente por *Smartphones* através do protocolo seguro HTTPS. As aplicações RFID recebem informações de Etiquetas RFID com 96-bit EPCglobal. As redes

configuradas nos cenários do Capítulo 5 são redes de baixa capacidade, baixo custo com dispositivos de baixa energia (isto é, *motes*), a qual tem a capacidade de sensoriar os parâmetros de interesse. O parâmetro sensoriado é retransmitido para o mediador através de rede formada com esses nós. Assim, o processamento e a velocidade de transmissão são relativamente baixos comparado com redes tradicionais. No entanto, essas características não eliminam a necessidade de planejar e dimensionar pelas seguintes razões: 1) o número de dispositivos pode ser muito grande, o que pode implicar em grande tráfego no mediador; 2) uma estimativa de tráfego permite ao projetista determinar o tempo de vida das baterias desses sistemas; 3) a capacidade dos *links* deve ser determinada para permitir um uso de canal eficiente. Adicionalmente, o modelo proposto é geral e escalável, i.e., não está restrito a essa classe de redes, e assim redes de alta velocidade com grande volume de dispositivos também podem ser analisadas por esse modelo. Todas as conexões são consideradas sem fio. Lembrando ainda que a determinação do atraso pode ser crucial no caso de Recuperação de Desastres. No entanto, o modelo não restringe o uso de conexões com fio.

c) Mapeamento do Modelo de Rede Simulado

Seguem os mapeamentos e as ferramentas utilizadas na Modelagem da Rede IoT Simulada**.**

c.1) As ferramentas de simulação existentes são muitas e as que foram consideradas mais próximas à abordagem desta tese atual e para perspectivas futuras são as seguintes:

1) Plataformas comerciais de uso geral (ARENA, SIMIO, FLEXSIM, PROMODEL): são equivalentes e caras; têm versões restritas de demo e para estudantes. Utilizou-se o ARENA pois a UNICAMP tinha licença profissional, assim como a do MATLAB. O ARENA é de caráter geral para eventos discretos (DES) e permite a incorporação de outras características via MATLAB/VBA (Mobilidade/Propagação/Otimização de Roteamento usando Monte Carlo, Lógica Fuzzy e Algoritmos de Predição, etc.);
2) NS-2 (NETWORK SIMULATOR 2): é software de uso livre (*free*) para plataforma Linux, com utilização mais complexa devido ao seu novo ambiente a ser dominado (Linux), além de ser menos amigável pois não é do tipo "clica e arrasta". É específico papa análise de redes e pode incorporar mobilidade;
3) OPNET: tem alto custo (30 mil dólares a licença, mais ou menos há 15 anos atrás) mas também tem versão restrita para estudante. O NS-2 e o OPNET são específicos para redes e podem incorporar mobilidade;
4) OMNET ++ (REDES MÓVEIS): ferramenta de software de uso livre (*free*), focada no nível de protocolo específico. Pode facilitar a análise de redes tipo MANET (IoT) pois incorpora facilidades de mobilidade;
5) PYTHON: também utilizado em ambiente Linux mais complexo; tem futuro promissor pois trabalha com bibliotecas já prontas do tipo dos softwares MATLAB e MATHEMATICA;
6) NETLOGO: software de uso livre (*free*) e orientado para simulação por "agentes".
Tanto o *PYTHON* quanto o *NETLOGO* podem servir para futuros trabalhos explorando novas características da rede e novas facilidades oferecidas por eles;
7) COOJA: Existe o conjunto ***CONTIKI/COOJA/ RPL;*** RPL é um roteador de borda, para interligar redes, que pode ser programado com o simulador COOJA. A plataforma de desenvolvimento é a CONTIKI. É focado em roteamento entre redes e bastante utilizado em

redes IoT, O Modelo de Rede Simulado nesta tese foi em nível mais alto; contemplou otimização de roteamento *OFF LINE* usando Monte Carlo, diminuindo o número de saltos (*hops*) das redes AdHoc *VANET*; o roteamento geral *ON LINE* foi abstraído e pode ser incorporado em futuro trabalho por meio de funcionalidades de perdas e reenvio de pacotes.

Usou-se ARENA por ser uma ferramenta de uso geral, ter licença na UNICAMP e poder ser complementado com o MATLAB *OFF LINE* (RWP, MONTE CARLO) E VBA (INTERFACES DINÂMICAS *ON LINE*); foi utilizado um modelo incremental, para efeito de validar os resultados da simulação, e evolutivo para englobar as funcionalidades adicionais desejadas.

c.2) Uso de Simulação Híbrida "ARENA + MATLAB + VBA": é uma solução de propósito geral e se encaixou bem no Modelo de Rede IoT Simulado, pois permite trabalhar com camadas de sensores, rede, apoio aplicativo e aplicação. Permitem a simulação de eventos discretos (DES) e o acréscimo de funções como *Random Way Point*, Modelo de Propagação (*Two-Ray e Free Space*), Otimizações de Monte Carlo, Lógica Fuzzy e Algoritmos de Predição. Podem ser usados nas fases de Planejamento, Projeto, Dimensionamento e Evolução das redes; permitem a abstração dos níveis físicos (sem fio e com perdas), enlaces, rede e aplicação. Também pode auxiliar na Administração da Rede (Engenharia de Tráfego).

c.3) Mapeamento do Modelo de Rede Simulado, com a Arquitetura TCP/IP : foram implementados os Níveis Físico, Enlace, Rede e Aplicação de comunicação, considerando Enlace sem Fio, Modelos de mobilidade *Random Way Point* e Modelos de Propagação "Two -Ray ou Free Space", Rede Datagrama UDP e Aplicação (Abstraídas nas Taxas de Chegadas e Serviço, ou seja, no tráfego gerado); a abstração para a rede TCP/IP é feita transferindo as características de rede nas taxas de chegadas e serviços (inicialmente exponenciais por facilidade de comparação com modelo analítico da Rede de Jackson) e adicionando aplicações com prioridades; as mensagens são consideradas datagramas geradas pelos sensores/etiquetas RFID e indo para o Mediador, Redes (AdHoc e Internet) e Aplicações; trabalhos futuros poderão usar distribuições estatísticas que não a exponencial;

c.4) Mapeamento do Modelo de Rede Simulado, com o Modelo de Referência IoT do ITU-T: nossa referência de implementação foi o Modelo de Referência IoT do ITU-T que divide a comunicação em 4 camadas (Figura 6): "Dispositivo", "Rede", "Serviço e Aplicação de Suporte" e "Aplicação"; ele foi todo simulado com abstrações de Sensores, Etiquetas/Leitores RFID, Redes (AdHoc, Mediador, Internet); HTTPS e aplicações de Gerenciamento de Rede, Transporte e Energia. Dependendo do caso ou da aplicação, uma ou outra característica poderá ser explorada em mais detalhes.

c.5) Mapeamento da Aplicação: perdas de conectividade reduzem o tráfego na rede devido às perdas de pacotes. A necessidade ou não das retransmissões desses pacotes depende do tipo de aplicação. Por exemplo, Medidas de Sensoriamento Cíclicas dispensam a necessidade de retransmissão pois a informação será reenviada em um novo ciclo. A Taxa de Perda de Conectividade foi estimada em 5% (com os parâmetros supostos em nossa rede, que poderão ser medidos no caso real) no *Random Way Point* a partir dos parâmetros: velocidade do móvel, área de abrangência, potência de transmissão, etc. A Taxa de Retransmissão não foi considerada, mas poderá ser facilmente incorporada em futuro trabalho. A ideia é a de que algumas mensagens são perdidas e devem ser retransmitidas quando isso ocorre. Por outro lado, mensagens maiores, compostas por vários pacotes, também podem escoar pela rede. Se

um dos pacotes da mensagem for perdido, ele deverá ser retransmitido para a composição final da mensagem. O modelo poderá supor vários tipos diferentes de mensagem e o tráfego de cada uma delas, ou adicionar uma taxa estimada (um percentual) de retransmissão de pacotes que vai depender do tipo de rede e seus tipos de roteamento (apenas MANET, IoT, etc,). Cada caminho com mensagem priorizada pode ser considerado uma aplicação específica.

Capítulo 5 : Cenários e Casos de Estudo Desenvolvidos e Publicados

O objetivo desta tese é apresentar um Modelo Simulado de Rede IoT, criado para estudar a integração da rede de telecomunicações IoT com a Rede de Sensores AdHoc, RFID e Sensores, utilizando uma simulação de eventos discretos com teoria de filas, visando a localização de pontos críticos de comunicação que precisarão ser otimizados.

Essa comunicação na rede IoT é dividida em camadas conforme mostrada na Fig. 6, visando diminuir a complexidade existente.

Neste capítulo será abordado esse novo Modelo de Rede IoT que foi criado e testado utilizando cenários (Novas Situações) com casos de estudo (Novas Configurações), conforme mostrado na Figura 12 abaixo.

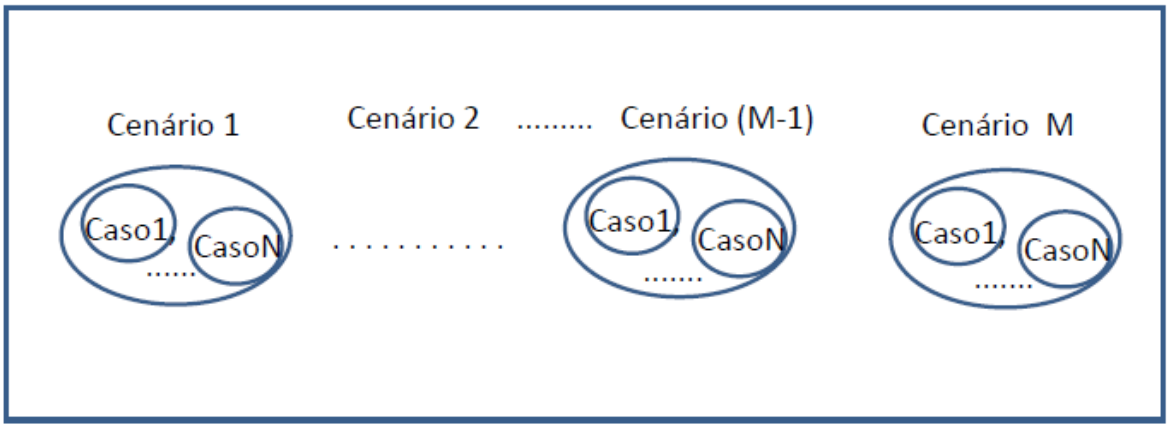

Figura 12: Cenários com seus respectivos Casos de Estudo

A Tabela 6 mostra a evolução incremental ocorrida nesses Cenários/Casos de Estudo (Conferência apresentada) sobre a Simulação do Modelo de Redes. Exemplo de Uso dos itens da tabela: para a Conferência WSC18 (Winter Simulation Conference 2018) apresenta-se um cenário com Rede AdHoc MANET, Rede RFID, Rede IoT, Simulação por Eventos Discretos (DES) ARENA, Mobilidade RWP, Validação de Jackson, Lógica Fuzzy e Algoritmo de Predição, aplicações de Gerência de Rede e Consumo de Energia, e 6 Casos de Estudo.

Tabela 6: Evolução Incremental do Modelo Híbrido de Rede IoT.

Conferência/Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
BTSYM16	S															
SBrT17			S				S	S						CA	4	S
ADHOCNOW17			S				S	S						CA	1	
BTSSYM17 #1		S														
BTSSYM17 #2			S		S	S	S	S						GR,SC	1	
SS SPECTS18			S		S	S	S	S	S	S				GR.SC	4	
SPRINGER18#1		S														
SPRINGER18#2			S		S	S	S	S	S	S				GR,CE	4	
SBrT18			S		S	S	S	S	S	S				GR,CE	6	
IEEE IEMCON18				S	S	S	S	S	S				S	GR,TI	6	
WSC18			S		S	S	S	S		S	S	S		GR,CE	6	
RESEARCH GATE(Relatório)			S		S	S	S	S						GE		
UNESP 19			S			S								CA	1	
ADHOC NOW19			S		S	S	S			S				CA	3	
IEEE IEMCON19			S	S	S	S	S	S	S	S			S	CA,GR SC,TI	7	S
BTSYM 19		S	S			S								SC,GR	1	
WSC 19			S			S								CA	3	
Conferência/Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Itens:
1 : Pesquisa Bibliográfica
2 : Arquitetura IoT (Padronização)
3 : Rede AdHoc MANET
4 : Rede AdHoc VANET
5 : Rede RFID
6 : Rede IoT
7 : Simulação por Eventos Discretos (ARENA)
8 : Simulação com Mobilidade RWP (MATLAB)
9 : Uso de Prioridades na Rede
10 : Validação Analítica Modelo Jackson
11 : Lógica FUZZY (MATLAB com Interface Visual Basic)
12 : Algoritmo de Predição (MATLAB com Interface Visual Basic)
13 : Otimização de Monte Carlo (MATLAB)
14 : Aplicações : Gerência de Rede SNMP (GR), *Smart City* (SC), *Transporte Inteligente* ITS (TI), Consumo Energia (CE), Geral (GE), Catástrofe (CA)
15 : Número de Estudos de Casos
16 : Modos; OBS : "S" representa que o item de estudo foi aplicado no artigo da conferência e na pesquisa.

5.1) Cenário # 1: Modelo de Rede Adhoc Incremental para Ambientes de Catástrofe

[P2] Performance Analysis of a Multi-Mode AdHoc Wireless Network via Hybrid Simulation;
Apresentado: ***XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais; Setembro/2017); SBrT 2017 São Pedro/SP/ BRASIL.***

O ARTIGO [P2] apresenta o modelo de rede AdHoc simulado (Figura 13).

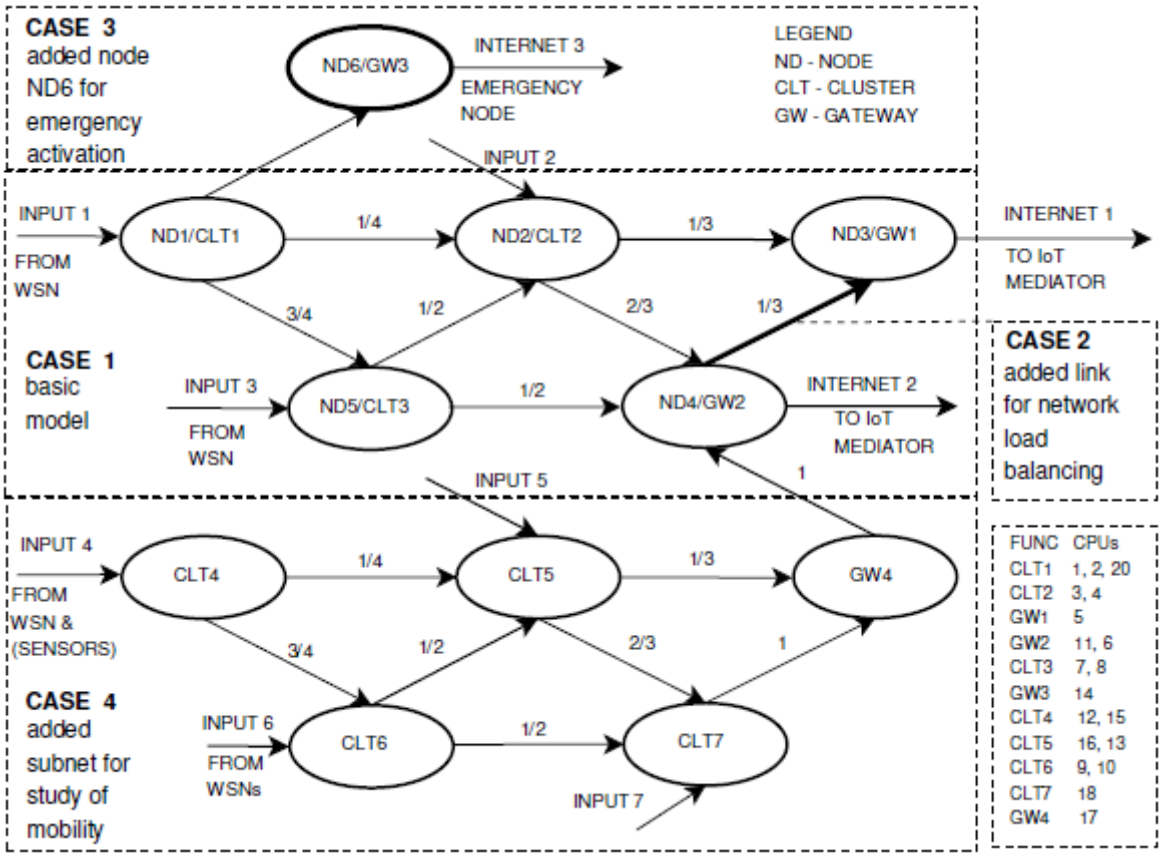

Figura 13 : Modelo de Rede AdHoc proposto [P2].

Este cenário apresenta uma Rede AdHoc bastante utilizada em ambientes de catástrofe, tendo em vista que ela não possui infraestrutura fixa e centralizada (Radio Base) e possui sua interconexão dinâmica entre nós.

Este artigo trabalha com 4 cenários incrementais na Tabela 7: 1) Rede Básica (Modos Normal e Não Balanceado), 2) Extensão da Capacidade da Rede (Modo Balanceado com acréscimo de Link), 3) Expansão da Topologia da Rede (Nó de Emergência) e 4) Rede AdHoc Completa contemplando Mobilidade (RWP) e *clusters*. A Rede AdHoc é uma rede sem fio (Radio Frequência), *multi-hop(receive, store and forward)*, descentralizada e sem Radio Base; após execução observou-se que a rede estava não balanceada (343 pacotes recebidos no Nó 3 e 1202 pacotes no Nó 4). O Modelo analisa o fluxo de pacotes na rede no que diz respeito a "*Mean Queue Time*" e "*CPU Utilization*". Acrescentou-se um "*Link*" para balancear a rede e um Nó de Emergência para Catástrofe ou Congestionamento das 2 Saídas Internet.

Tabela 7 : Casos de Estudo e Parâmetros considerados [P2].

	Case Study			
Variable #	1	2	3	4
# modes	1	2	3	4
mode name	regular	balanced	emergency	mobility
mode action	basic	new link	new node	added mobil.
balanced traffic	✗	✓	✓	✓
emergency mode	✗	✗	✓	✓
# user nodes	3	3	3	70
# gateway nodes	2	2	3	4
total # nodes	5	5	6	74
# clusters	0	0	0	7
mobility	✗	✗	✗	✓
performance parameter	CPU utilization queue time	utilization queue time	utilization queue time	util, queue time + netw. connectivity
goal: to study the impact of:	reference network	added link	added gateway 3	connectivity due to mobil.
arrival rate (packets/s)	0.5	0.5	5	1.67
service rate (packets/s)	3	3	3	10

O Caso 4 é mais completo e incremental, contendo todos os casos anteriores de expansão de link e nó de emergência, considerando adicionalmente a "mobilidade e clusterização". Utiliza a Tabela 8 de configuração dos parâmetros do *Random Way Point*.

O objetivo deste caso de estudo é analisar diferentes maneiras de aumentar a conectividade para diferentes parâmetros. Devido às características Poissonianicas para o tráfego de entrada, é possível somar as taxas de cada nó individual e então considerar um *cluster* formado por 10 nós. Assumindo que o '*mean inter-arrival time*" em um único nó é 6 segundos, o tempo médio de chegada individual de cada *cluster* se torna 0,6 sec/packet EXPO (i.e. 6/10). Assim a taxa de chegada é 1/0.6 = 1,67 packet/sec. O tempo de serviço médio é 0,1 sec/packet e a taxa de serviço (1/0,1) = 10 packets/sec. Assim, expandindo a rede considerando 7 *cluster*s de 10 nós cada e 3 nós Internet (GW1, GW2 e GW3), sendo o último um Nó de Emergência, e uma sub-rede AdHoc com 4 *cluster*s (CLT4, CLT5, CLT6 e CLT7) e um nó *Gateway* (GW4, usado para interconexão). Introduziu-se a Mobilidade do Nó através do algoritmo RWP (*Random Way Point*) para Redes Móveis AdHoc. Os parâmetros de mobilidade são configurados através da Tabela 8 que segue do Sw MATLAB, gerando a probabilidade de conexão para uma determinada configuração. A conectividade aumenta com o Nível de Sinal, com a quantidade de nós no *cluster*, com a quantidade de nós *Gateways* na rede e o menor tamanho da área. A Probabilidade de Falha é calculada pelo RWP e inserida no modelo para verificação dos resultados.

As Figuras 14 e 15 apresentam o número de nós ativos em um *cluster* por simulação para diferentes posições dos nós.

Tabela 8: Caso 4: Parâmetros de Entrada MATLAB de configuração do *Random Way Point* [P2].

Input Parameters	Values
Receiver Threshold	-88 dBm
Area size	1000 x 1000 m
Antenna type	Omnidirectional
Antenna height (ht, hr)	1.5 m
Antenna gain (G_t, G_r)	1.0
System Loss Coefficient (L)	1.0
# Mobile nodes in a Cluster	10
Mobility model	Random Waypoint
Speed interval	[0.2 - 2.2] m/s
Pause interval	[0-1] s
Walk interval (walk time)	[2-6] s
Direction interval	[-180 + 180] degrees
Transmission frequency	5.8 GHz
Transmission power (Pt)	15 dBm
Simulation time	306 s

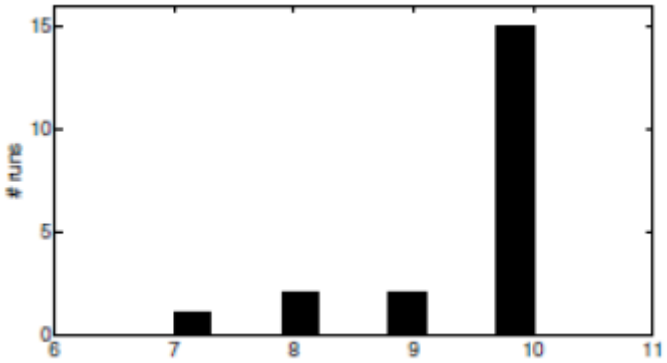

Figura 14: Caso 4: Números de Nós ativos em um cluster por rodadas de simulação [P2].

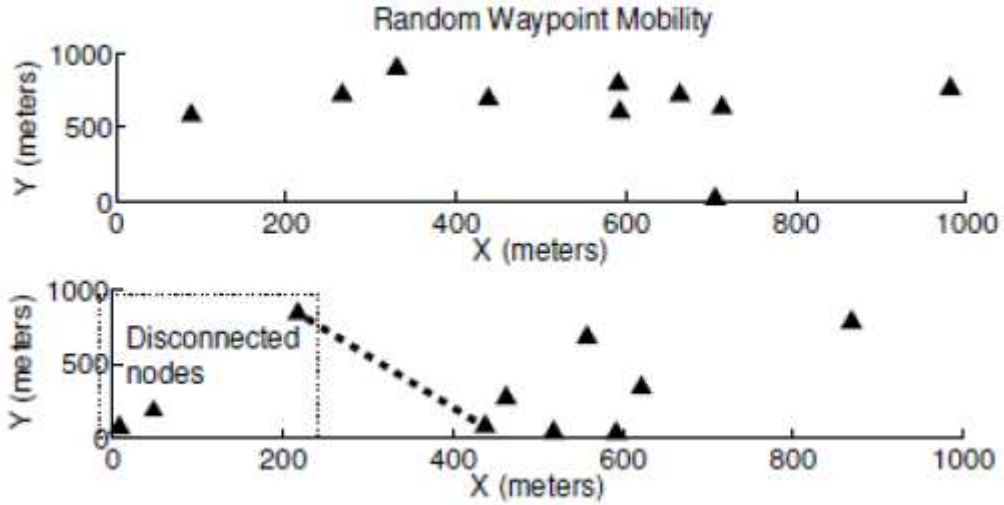

Figura 15: Posições diferentes dos nós [P2].

Este artigo apresenta os seguintes resultados de tempo médio de fila e utilização de CPU para os 4 casos de estudo (Figura 16). Observe no Caso 1 que a CPU 6 está sobrecarregada (alto tempo de fila e alta *CPU Utilization*), situação essa que mudou a partir do Caso 2 com o acréscimo de novo link e posteriormente novo nó de emergência (Caso 3). O Caso 4 apresenta os resultados com Mobilidade.

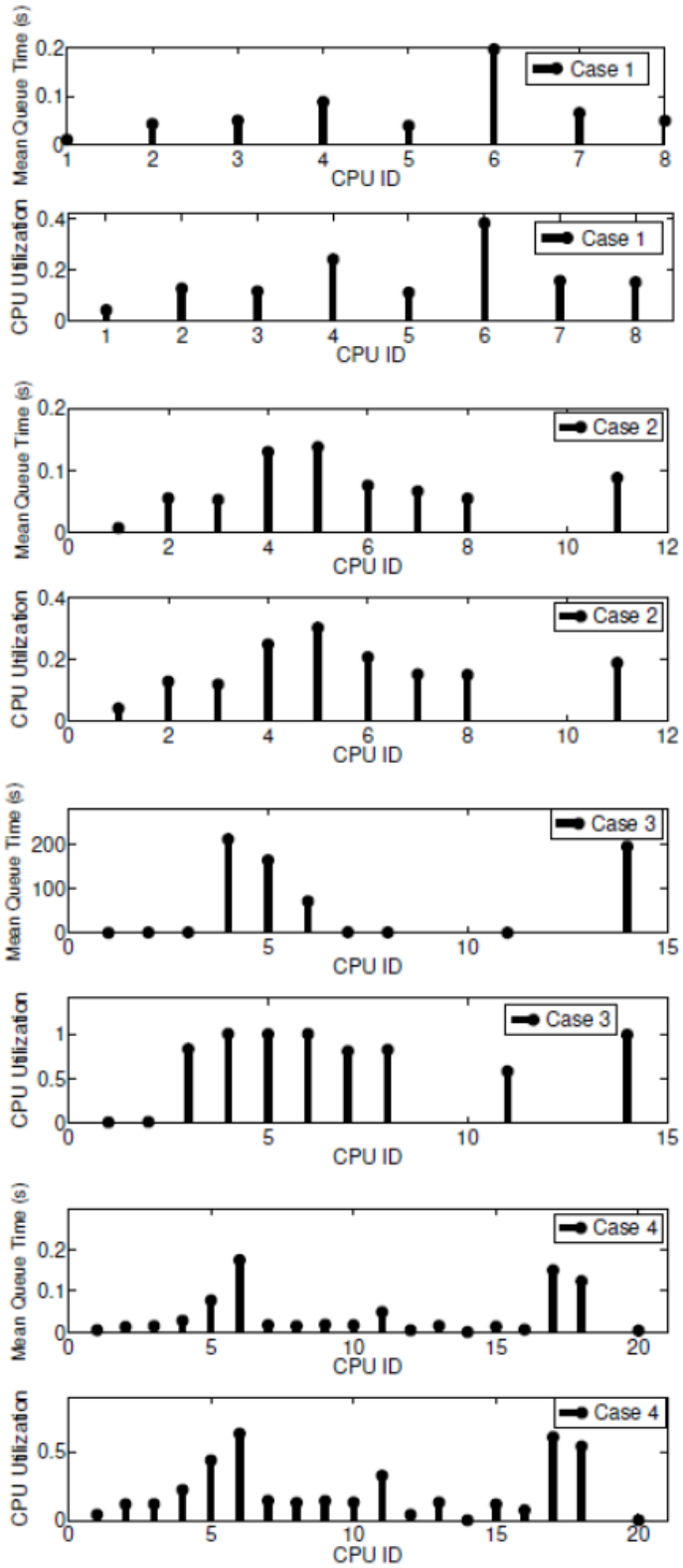

Figura 16: Tempo Médio de Espera de Fila e Utilização Média de *CPU* [P2].

5.2) Cenário # 2: Modelo de Rede AdHoc com Mobilidade (Ambientes de Catástrofe)

[P3] Simulation of AdHoc Networks Including Clustering and Mobility;
Apresentado: ***16th International Conference on Ad Hoc Networks and Wireless; Outubro/2017); ADHOC-NOW 2017; MESSINA/ITÁLIA; LIVRO SPRINGER;***

O ARTIGO [P3] apresenta o modelo de rede AdHoc. Este cenário apresenta uma Rede AdHoc bastante utilizada em ambientes de catástrofe, tendo em vista que ela não possui infraestrutura fixa e centralizada (Radio Base) e possui sua interconexão entre nós dinâmica.

Esse cenário assim como o anterior, contempla uma Rede AdHoc (Figura 17) incluindo Mobilidade e 2 casos de estudo: *first* e *second run*. Esse trabalho é parte de um esforço maior de dimensionar a capacidade de uma rede IoT, onde os gargalos nos níveis mais altos da arquitetura, isto é, no mediador, que concentra a maioria dos fluxos de dados na rede. Observe que o tráfego sob consideração neste trabalho converge para um Mediador IoT.

O Modelo de Simulação de Rede por Eventos Discretos permite a colocação de nós sensores em um *cluster*, assim como sua carga de tráfego, mas não expressa sua mobilidade. A mobilidade dos nós dentro de um *cluster* é dada pelo algoritmo RWP, com a mesma tabela mostrada no cenário anterior (Tabela 8). A degradação da conectividade para alguns nós pode causar a redução do tráfego nas camadas superiores. Pode também aumentar o tráfego nos nós vizinhos, justificando o uso de nós *gateways* de emergência, visando desafogar a degradação de desempenho em nós afetados.

O resultado mais importante deste trabalho é analisar e estimar o tráfego total na rede de *clusters* considerando o efeito de mobilidade e *fading,* isto é, o volume de tráfego sobre condições dinâmicas.

Foram executadas duas rodadas descritas a seguir:

Caso 1 (Primeira Rodada): neste caso os tempos entre chegadas para um *cluster* são EXPO (0,2), isto é, um pacote é recebido a cada 0,2 segundos (1/0,2=5), gerando assim uma taxa de chegada de 5 pacotes/segundos. Usamos uma taxa de serviço de 1/0,33, significando que a taxa de serviço é 3, isto é, 3 pacotes são processados a cada segundo. Alguns nós estavam instáveis devido à taxa de serviço ser menor que a taxa de chegada e sua utilização ser próxima de 100%. Isso causa excessivos atrasos o que pode ser resolvido com o uso de um Nó de Emergência. Então, nesta primeira rodada a situação foi forçada para que a rede apresente instabilidades, visando verificar o desempenho do nó de emergência. Rodando o modelo completo em 1.000 segundos, foram observadas as seguintes carga de tráfego nos *Gateways*: GW1 (5,2550 pacotes/segundos); GW2 (2,2350 pacotes/segundos); Gw3 de Emergência (0,3910 pacotes/segundos).

Caso 2 (Segunda Rodada): neste caso os tempos entre chegadas de um cluster são EXPO (0,6), isto é, um pacote a cada 0,6 segundos (a taxa de chegadas é 1/0,6=1,67 pacotes/segundos, isto é 10 nós x 0, 167 pacotes/s por nó). Utilizamos uma taxa de serviço de 1/0,1, significando uma taxa de serviço de 10, isto é, 10 pacotes são processados a cada segundo, maior do que na Primeira Rodada, o que foi suficiente para estabilizar o sistema.

Assim, a rede estável fez com que o Nó de Emergência (CPU 20) ficasse inativo (apenas poucos pacotes). Rodando o modelo completo em 5.000 segundos, foram observadas as seguintes carga de tráfego nos *Gateways*: GW1 (4,3828 pacotes/segundos); GW2 (6, 3736 pacotes/segundos); GW3 de Emergência (0,0030 pacotes/segundos). Nesta rodada foi executado o Modelo Analítico de Rede de Jackson que é calculado como uma Cadeia de Markov para validar o modelo de simulação com distribuições exponenciais (chegada e serviço). Desta forma, o modelo não está limitado ao uso de Distribuição Poissoniana inicialmente. No entanto, uma vez validado é possível avaliar outras distribuições. O modelo não é restrito ao uso do RWP e pode ser utilizado com outros modelos.

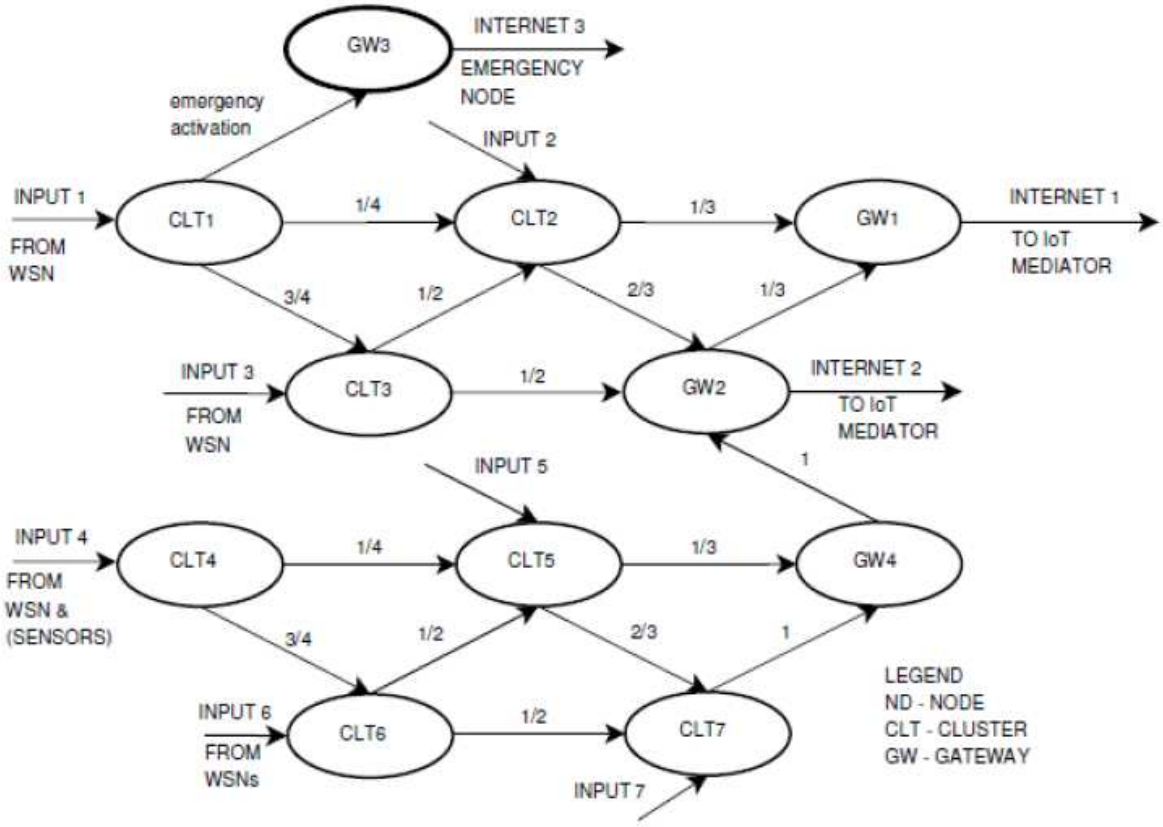

Figura 17: Modelo de Rede AdHoc Móvel [P3].

Os resultados desse cenário são mostrados na Figura 18 que segue; observa-se que a rede passou a ter estabilidade, como esperado, devido ao aumento da Taxa de Serviço.

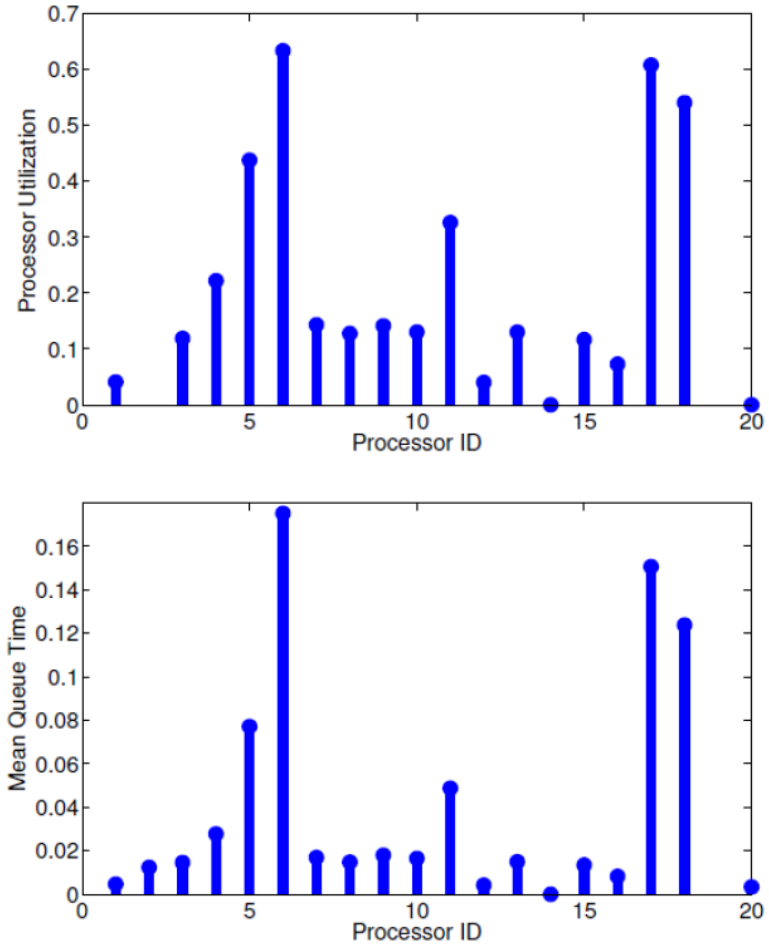

Figura 18: Utilização Média de *CPU* (processador, acima) e tempo médio de fila (abaixo) (para a segunda rodada) [P3].

5.3) Cenário # 3 : Modelo de Rede IoT com Rede Adhoc, RFIDs e Sensores

[P5] A Proposal for Performance Analysis and Dimensioning of IoT Networks; Apresentado: *BTSYM'17 Brazilian Techbology Symposium; (ISSN 2447-8326); Dezembro/2017); BTSYM 2017 Campinas/SP/ BRASIL.*

Este cenário [P5] apresenta um Modelo de Rede IoT, com sensores, RFIDs e sub-redes AdHoc. Para avaliar cada nó independentemente, uma Rotina MATLAB gera posições randômicas para os 10 nós em cada cluster, todo segundo, usando o *Random Way Point* (RWP) para simular a mobilidade no desempenho da rede. Este trabalho analisa e estima o tráfego total na rede de *clusters* considerando o efeito de mobilidade e *fading,* isto é, o volume de tráfego sobre condições dinâmicas. Foram considerados 3 Casos de Estudo:

Caso 1 (Primeiro Cenário): Mediador sobrecarregado; os tempos entre chegadas para um *cluster* é EXPO (0,6), isto é, um pacote a cada 0,6 segundos; assim, a taxa de chegada é 1/0,6 = 1,67 pacotes/s (10 nós x 0,167 pacotes/s por nó). Utiliza-se a taxa de serviço de 10 pacotes/s (isto é, 1/0,1). Alguns nós ficaram instáveis devido ao fato da taxa de serviço ser menor que a taxa de chegada e sua taxa de utilização ficar próxima de 100%. Isso causa um atraso

excessivo e pode ser visto a ativação do nó de emergência. Assim sendo, neste cenário a situação foi forçada para que a rede apresentasse instabilidade para verificar o desempenho do nó de emergência.

Caso 2 (Segundo Cenário): Mediador com Capacidade Estendida; os tempos entre chegadas para um cluster foi EXPO (0,6), isto é, um pacote a cada 0,6 segundos (com taxa de chegada de 1/0,6=1,67 pacotes/s, isto é, 10 nós x 0,167 pacotes/s por nó). Usamos a taxa de serviço de 1/0,02 significando que a taxa de serviço é 50, isto é, 50 pacotes são processados a cada segundo (velocidade 5 vezes maior que o primeiro cenário). O aumento na taxa de serviço no mediador (CPU 24) foi suficiente para estabilizar o sistema, como mostrado na Figura 19. Assim sendo, a rede estável fez com que o nó de emergência (CPU 20) ficasse praticamente inativo, isto é, apenas poucos pacotes passam por ele. Observe que no sistema atual, o atraso de processamento é diferente para cada elemento de rede. O resultado que resume o dimensionamento do mediador é mostrado na Tabela 9; mostra a diminuição do tempo médio e da utilização de CPU, na mudança do primeiro para o segundo caso (Mediador Estendido).

Caso 3 (Terceiro Cenário): Validação da simulação. O sistema foi validado sem a mobilidade, usando modelo de rede de Jackson. Observe que o nó de emergência foi removido, garantindo assim 100 % de conectividade.

Para avaliar cada nó independentemente, uma rotina MATLAB gera posições randômicas para os 10 nós dentro do cluster, cada um segundo neste caso, que utiliza o Modelo *Random Way Point* (RWP) para simular o desempenho da rede.

O resultado mais importante neste trabalho é a análise e estimativa do tráfego total em uma rede de *cluster* considerando o efeito de mobilidade e *fading*, isto é, o volume de tráfego sobre condições dinâmicas.

Os resultados são apresentados na Figura 19 e Tabela 9.

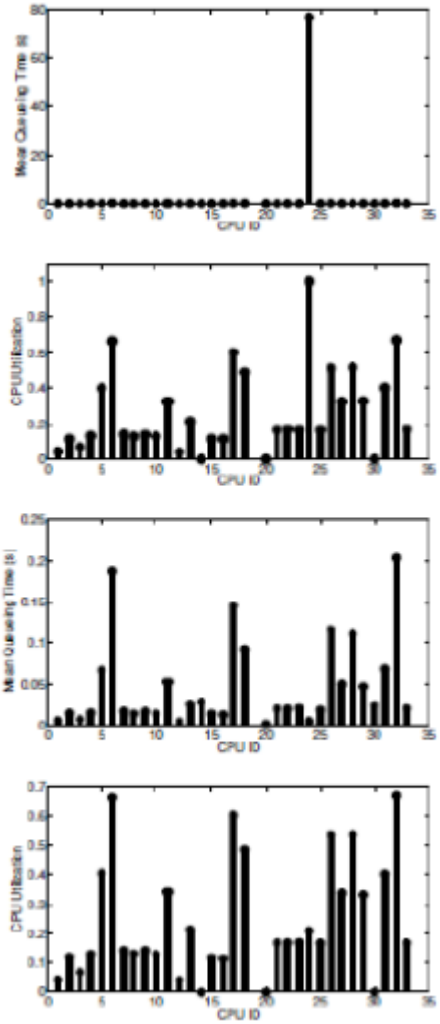

Figura 19: Tempo Médio de fila e Utilização Média de *CPU* [P5].

Tabela 9: Resultados para o mediador [P5].

Parameter	First Scenario (overloaded mediator)	Second Scenario (extended mediator)
arrival rate (packets/s)	20	20
service rate (packets/s)	10	50
mean-queue-time (s)	79	0.0056
CPU Util. (%)	100	20

5.4) Cenário # 4: Modelo de Rede IoT com Validações Incrementais

[P6] Performance Analysis of IoT Networks with Mobility via Modeling and Simulation.
Apresentado: ***SUMMERSIM 2018 – SPECTS 2018 International Symposium on Performance Evaluation of Computer and Telecommunication Systems; Junho/2018); SUMMER SIM SPECTS 2018 BORDEAUX/FRANÇA.***

O artigo [P6] faz o estudo de tráfego de uma Rede AdHoc e de Rede IoT, visando o planejamento e dimensionamento de redes futuras, ou detecção e otimização de pontos críticos nas redes existentes. Utiliza simulação hibrida de Eventos Discretos e Mobilidade usando o *Random Way Point* em MATLAB. Foram executados 3 casos de estudo utilizando validações incrementais: Regular, Balanceado, Emergência e Mobilidade. A simulação mede o desempenho do tempo de espera nas filas e o Nível de Utilização de CPU dos Nós.

Os parâmetros de mobilidade são selecionados conforme Tabela 8. Dependendo do Nível de Potência, os nós podem se comunicar, conforme mostrado nas Figuras 20 e 21. A execução foi feita em três Casos de Estudo: Mediador sobrecarregado, Capacidade Estendida do Mediador e Validação da Simulação. Os resultados estão mostrados na Figura 22 e Tabela 10 para o Mediador.

Para avaliar cada cluster independentemente, uma rotina MATLAB gera posições randômicas para 10 *motes* (nós móveis) dentro do *cluster*, todo segundo. Este caso usa o *Random Way Point Mobility Model* (RWP) para simular o desempenho da rede. Pela mudança de diferentes parâmetros, pode-se aumentar ou diminuir a conectividade. Por exemplo, pode-se aumentar a conectividade, aumentando-se o número de *motes*, aumentando-se o número de *gateways* (interconexão), potência de transmissão e a diminuição da área de simulação. A mobilidade calcula o posicionamento de cada *mote* e seleciona uma destinação randômica e caminha para ela com velocidade fixa. O *cluster* é configurado com 10 *motes*. A probabilidade de conexão é calculada passo a passo, sendo inserida no software de simulação.

Três Casos de Estudo são apresentados para avaliar o volume de tráfico sob condições dinâmicas:
Caso 1 (Primeiro Cenário): Mediador Sobrecarregado – Neste caso de estudo utiliza-se um tempo entre chegadas para um *cluster* de EXPO (0,6), isto é, um pacote a cada 0,6 segundos, com taxa de chegada de 1/0,6= 1,67 pacotes/segundos (10 motes = 0,167 pacotes/segundo por mote). Foi utilizada Taxa de Serviço de 10 pacotes/segundos (isto é, 1/0,1), incluindo o mediador. Esses valores causaram instabilidade no mediador devido à taxa de utilização se aproximar de 100%.

Caso 2 (Segundo Cenário): Mediador com Capacidade Estendida – Neste caso de estudo, mudou-se a Taxa de Serviço para 50 pacotes/segundos (= 1/0,02); o aumento da taxa de serviço no mediador (CPU 24) foi suficiente para estabilizar o sistema;

Caso 3 (Terceiro Cenário): Validação da Simulação – Neste caso de estudo, com o sistema sem mobilidade, foi validado o modelo de simulação com o modelo de rede de Filas de Jackson. A mobilidade na rede AdHoc foi eliminada para garantir 100% de conectividade, pois o modelo analítico adotado não acomoda perda de pacote e mobilidade. O Modelo analítico de Redes de Jackson foi calculado como um processo de Markov para validar o

modelo de simulação com distribuição exponencial para ambas as distribuições de chegada e de serviço. Entretanto, uma vez validada, é possível avaliar outras condições, como por exemplo, diferentes distribuições da exponencial, a inclusão de perda de conectividade e a distribuição de probabilidade no que diz respeito ao tráfego entre *cluster*.

Resumidamente, o primeiro caso de estudo com rede congestionada, o segundo caso de estudo com rede balanceada e o terceiro caso de estudo com o modelo de validação validado com o modelo analítico, acrescentando restrições de mobilidade zero e conectividade completa. O modelo proposto é genérico e pode ser instanciado para aplicações específicas. Por exemplo, as probabilidades de transmissão para os links de saídas podem ser medidas em aplicações reais e substituída no modelo. As distribuições de tempo de chegada e de serviço consideradas podem ser substituídas por outros tipos de distribuições.

A Figura 20 apresenta as conectividades para variação de valores de potência.

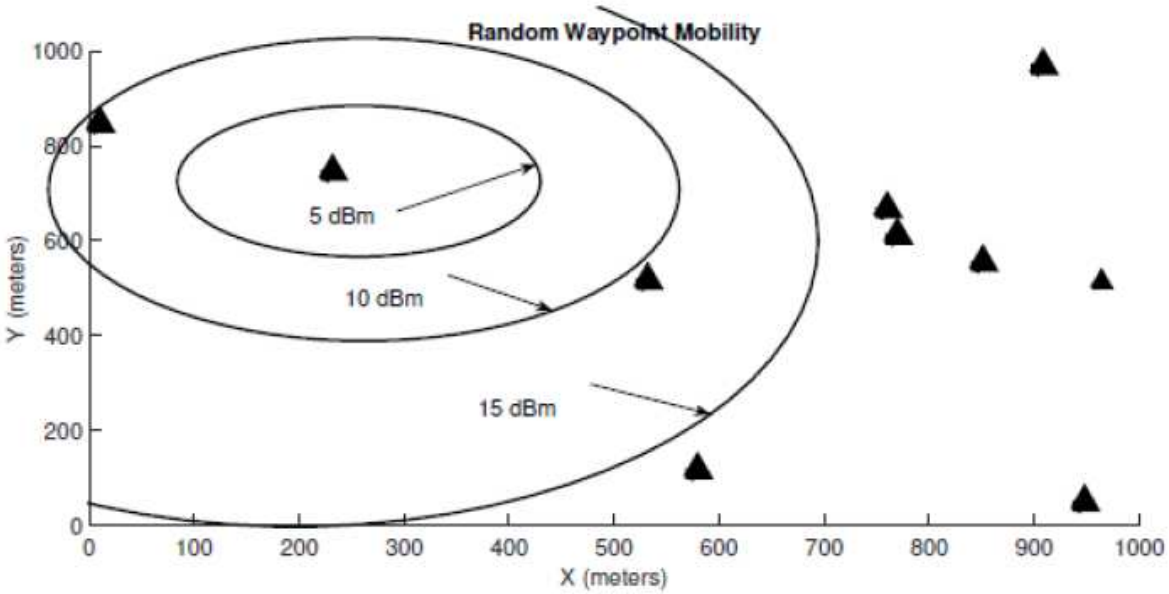

Figura 20: Variação de Potência para 5, 10 e 15 dBm (dez motes móveis) [P6].

A Figura 21 apresenta a conectividade e distância em função da variação da potência.

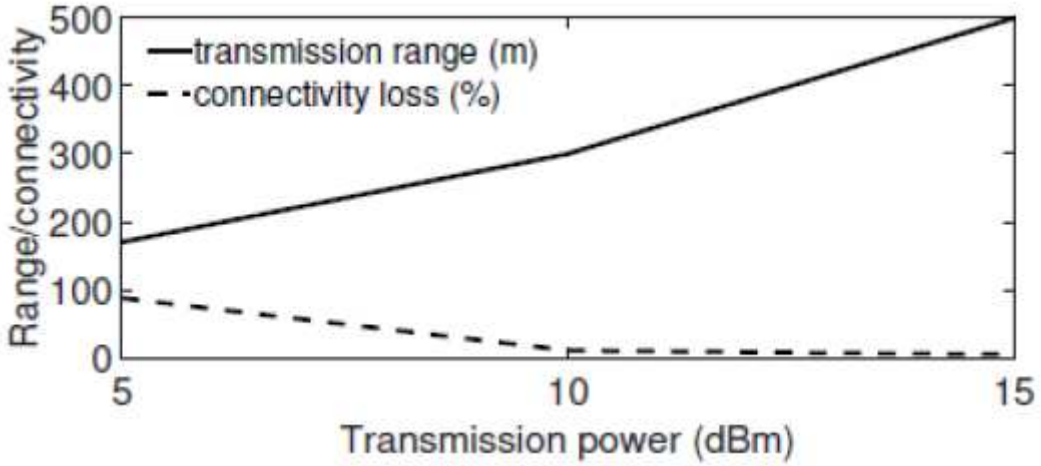

Figura 21: Conectividade e distância em função de variação de potência [P6].

Este artigo apresenta os seguintes resultados da Figura 22, com diversas Probabilidades de Bloqueio: 4,95%, 10,5%, 20.5% e 49,5%.

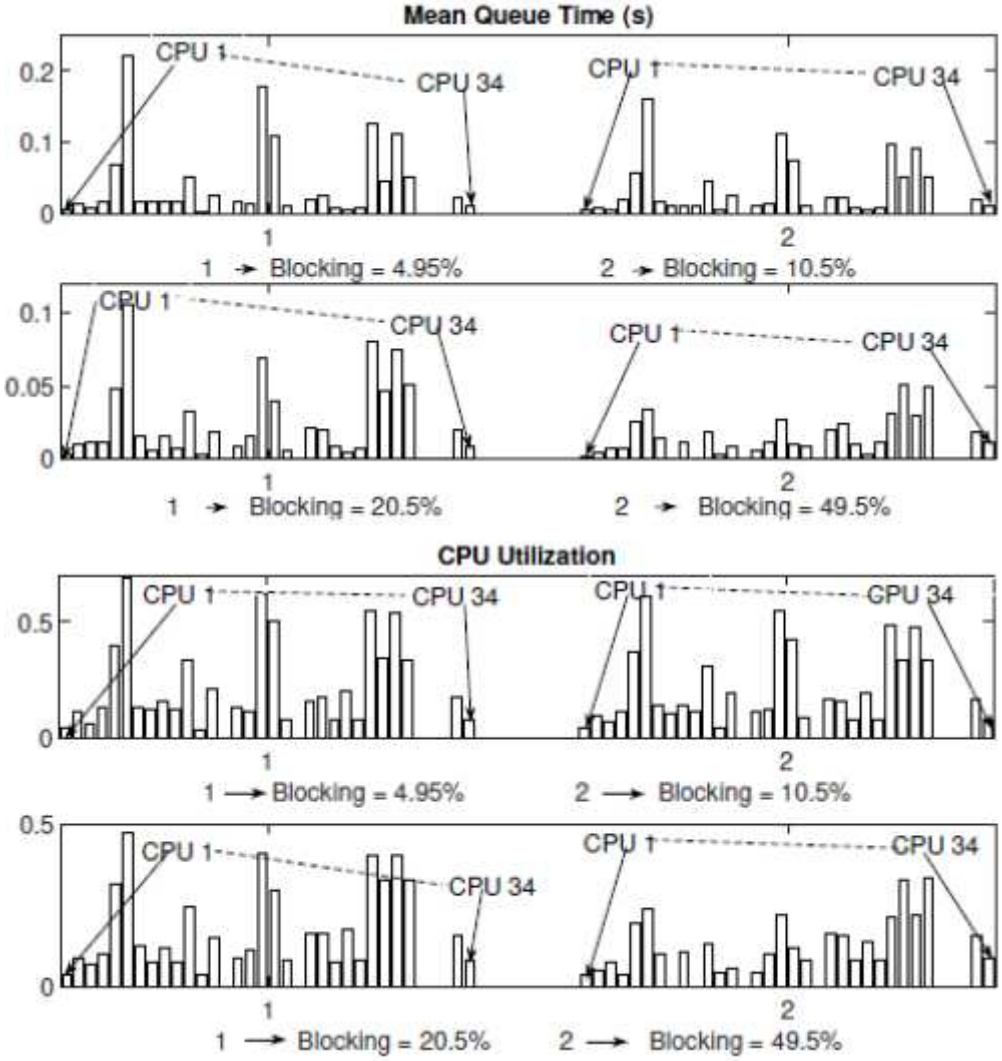

Figura 22: Tempo médio de Fila (acima) e Utilização Média de CPU (abaixo) para perda de conectividade de 4,95%, 10,5%, 20,5% e 49,5% da esquerda para a direita [P6].

A Tabela 10 apresenta (para os dois primeiros casos de estudo) os resultados de tempo médio de fila e tempo médio de fila no mediador (CPU 24).

Tabela 10: Resultados para o mediador (CPU 24) [P6].

Parameter	First Scenario (overloaded mediator)	Second Scenario (extended mediator)
arrival rate (packets/s)	20	20
service rate (packets/s)	10	50
mean-queue-time (s)	79	0.0056
CPU 24 Util. (%)	100	20

5.5) Cenário # 5: Avaliação de Atrasos de Tráfego e Utilização de Redes IoT

[P7] Evaluation of Traffic Delays and Utilization of IoT Networks considering Mobility; Publicado: ***Proceedings of the 3rd Brazilian Technology Symposium – Emerging Trends and Challenges in Technology; Maio/2019); (LIVRO SPRINGER BTSYM 2019).***

Este artigo [P7] é um subconjunto do artigo anterior. Apresenta o estudo de uma Rede IoT com validação e mobilidade. Neste cenário o modelo analítico de Rede de Jackson é utilizado, o qual foi calculado como uma cadeia de Markov para validar o modelo de simulação com uma distribuição exponencial para ambas distribuições de taxas de chegada e taxa de serviço. Observe que o modelo de simulação não está limitado ao uso de distribuição Poissoniana inicialmente assumida neste trabalho.

A análise de desempenho e o dimensionamento de uma rede IoT são apresentados, usando simulação de eventos discretos e considerando mobilidade do nó. Especificamente, a utilização do processador em cada nó e o tempo médio de atraso da rede é estimado. Adicionalmente, quanto mais baixa for a potência de transmissão, maior a perda de pacotes; a tolerância a perda de pacotes depende da aplicação; a rede IoT simulada pode prover ao projetista como um guia para especificar o mínimo de potência de transmissão requerida como função da distância do nó e perda de pacote admissível. Esse limite pequeno de potência de transmissão é crítico, em sistemas sem fio e alimentados com bateria, pois a potência de transmissão tem direto impacto na expectativa de tempo de vida.

Este trabalho se preocupa com o dimensionamento da capacidade do nó investigando através de um caso de estudo o tempo médio de fila e a utilização de CPU para cada nó, para uma dada probabilidade de conectividade de nós resultantes da mobilidade. Utiliza-se a simulação de rede por eventos discretos que permite a simulação de nós sensores e RFID em *clusters*, assim como a carga de tráfego aproximada, mas não expressa sua mobilidade dentro de um *cluster*, que é simulada através do algoritmo *Random Way Point* (RWP). A degradação na conectividade em alguns nós pode causar a redução total de tráfego em camadas superiores. Através do modelo é possível estimar o tráfego de entrada e saída para cada *cluster* e o Mediador IoT.

Para um dado nível de potência de transmissão, é possível verificar o nível correspondente de perda de pacotes (fig.21). Devido à redundância intrínseca da informação na rede, existe um nível aceitável de perda no sistema que não afeta a aplicação do ponto de vista funcional. A tolerância à perda de pacotes depende da aplicação. No entanto, com o modelo de simulação apresentado é possível analisar tais níveis quantitativamente, que prove ao projetista com um guia para configurar a potência de transmissão. Este é um parâmetro de projeto crítico, tendo em vista que sistemas sem fio e alimentados por baterias, pois a potência de transmissão tem um impacto direto no seu tempo de vida.

Na Figura 23 apresentam-se o tempo médio de fila e a utilização de todas as CPU (1 até 34). Usando as taxas de chegadas de Jackson e considerando os valores simulados e aqueles

obtidos usando um Modelo de Fila M/M/1 (Taxa de Chegada na *CPU* sendo 1/0,6=1,67 bps e taxa de serviço na *CPU* sendo 1/0,1=10 bps; o mediador tem 5 bps para taxa de chegada e 50 bps para taxa de serviço, o atraso médio da rede é Wa= 233,2 ms (modelo analítico) e Ws = 247,3 ms (modelo de simulação). No entanto, os valores atuais serão menores devido aos casos de perdas de conexões.

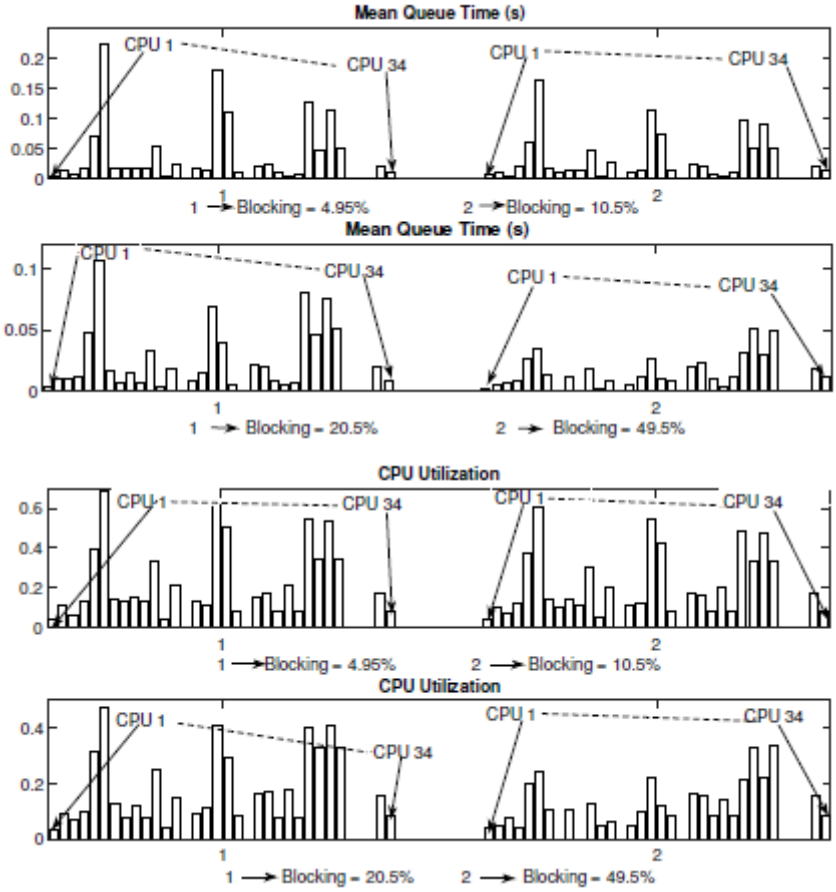

Figura 23: Tempo Médio de CPU e Utilização Média de CPU: perda de conectividade de 4,95%, 10,5%. 10,5% e 49,5% [P7].

5.6) Cenário # 6 : Impacto da Redução de Tráfego no Consumo de Energia, visando a Sustentabilidade

[P9] Evaluating the Impact of Congestion Reduction on Power Consumption in IoT Networks;
Apresentado: ***XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais; Setembro/2018); SBrT 2018 Campina Grande/PB/ BRASIL.***

O artigo [P9] apresenta um estudo de tráfego de Redes AdHoc e IoT visando a redução do congestionamento, diminuição do consumo de energia e aumento do tempo de vida dos dispositivos dependentes de baterias. Utiliza Simulação de Eventos Discretos (DES) para o Planejamento e Dimensionamento da Rede IoT, em conjunto com o Modelo *Two-ray Propagation*, Modelo de Mobilidade *Random Way Point*, possibilitando a detecção e otimização de Pontos críticos existentes (gargalos). O modelo proposto (Figura 11) foi

validado analiticamente através das Redes de Jackson. Dois casos de estudo foram analisados: Congestionado e Não Congestionado. O desempenho foi medido através das variáveis de tempo de espera nas filas e utilização de *CPUs*. Conclui-se que a redução de congestionamento implica numa redução de consumo de energia e aumento do tempo de vida dos dispositivos dependentes de bateria.

Este artigo apresenta uma Metodologia de Análise de Desempenho:

a) QUESTÕES DE PROJETO DE REDE IoT:

1. Qual tráfego pode ser suportado (Req.QoS)?
2. Qual o consumo de energia em um nó (Duração da Bateria/Tempo de Vida)?
3. Quais os gargalos de congestionamento?
4. Que Taxa de Tráfego de Chegada elimina esses gargalos?
5. Que Taxa de Serviço do Processador elimina esses gargalos?

b) Metodologia de Respostas:

1. Construir um modelo de simulação por eventos discretos (DES) para a rede IoT;
2. Validar o modelo DES usando modelo analítico da Rede de Jackson;
3. Avaliar a rede congestionada com identificação dos gargalos (caso 1);
4. Avaliar a rede não congestionada (caso 2);
5. Calcular a variação de tráfego (*erlang*);
6. Estimar a redução de consumo de energia usando modelos e equações para diversas tecnologias.

O modelo é capaz de estimar o consumo de energia tanto globalmente como individualmente nos nós, tanto na fase de projeto como na fase de operação. Esta metodologia é, na fase de projeto, a única alternativa viável para estimar o consumo de energia em grandes redes, tendo em vista que medidas e dados de redes físicas ainda não estão disponíveis e os modelos analíticos não podem capturar a complexidade de tais redes. Para redes já existentes e operacionais, é um procedimento mais fácil de estimar gargalos futuros e prever o consumo de energia devido às expansões e crescimento da rede. O desempenho é analisado através de 2 variáveis de saída, mostradas na Figura 24 que segue: Tempo médio de Fila e Utilização de *CPU*.

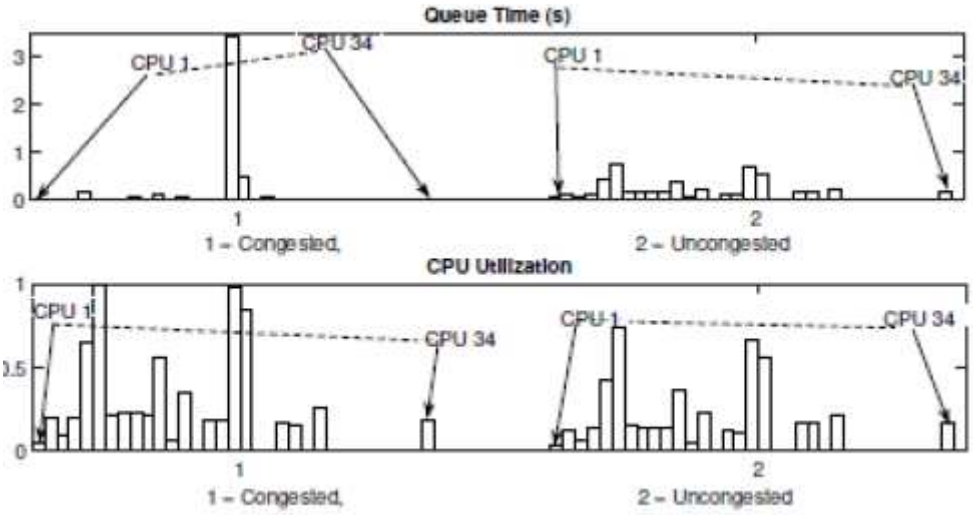

Figura 24: Tempo Médio de Fila e Utilização de *CPU*: Casos 1 e 2 [P9].

O atraso das mensagens foi medido nos dois casos: Rede Congestionada e Rede Não congestionada, mostrando uma redução de mais de 10 vezes nesse atraso (28,04 → 2,28 sec) (Tabela 11).

Tabela 11: Tempo de Atraso de Mensagem (secs) para casos de estudos [P9].

Message type	Case 1 congested	Case 2 uncongested
SNMP	0.093	0.085
sensor 1 AC sensor 2 light sensor 3 battery	28.04	2.28
RFID	2.170	2.145

O consumo de energia decorrente pode ser visto na Tabela 12, tanto para o Modelo Analítico como para o Modelo de Simulação.

Tabela 12: Impacto da Redução de Tráfego no Consumo de Energia [P9].

Equipment [ref]	Equations (W)	Busy Hour Reduction (Watts)	
		Jackson	Simul.
3G - BS [2]	$1.274 + 1.713x$	4.42	4.94
GSM900 - sector1 [3]	$581 + 11.9x$	602.9	606.5
GSM900 - sector2 [3]	$549 + 11.1x$	569.4	572.8
UMTS - 3 sectors [3]	$551 + 1.14x$	553.1	553.4
WiMAX, LTE, HSPA [4]	$493.2x$	906.5	1055.4
CDMA (forwarding link) [5]	$0.734x$	1.35	1.57

O cálculo da economia de energia diário pode ser feito, considerando:

1. Levantar a Diferença de Tráfego (*Delta* Tráfego);
2. Entrar com esse valor na fórmula *Delta* Energia = 1,274+1,713x;
3. Exemplos:
   Redução 1 (Jackson 24 *CPUs*) = 1.274+1.713(6.734-4.896) = 4.422W
   Redução 2 (Simulation 34 *CPUs*) = 1.274+1.713(7.056-4.915) = 4.94 W
   Arredondando para 4,5;
4. Calcular o valor mensal na hora de maior movimento (HMM):
   = 5hs/dia x 20 dias/mês x 4.5 =100 x 4.422= 450 W/mês.

Conclui-se que a redução do consumo de energia na rede é possível, tanto no nível de projeto como no nível de operação, através da redução de congestionamento (menos perda de pacotes (detecção/correção de erro) com menos retransmissões), que pode ser usado para estender o tempo de vida dos dispositivos.

5.7) Cenário # 7: Rede VANET para Sistema de Transporte Inteligente.

[P10] Analysis of an Adhoc Network in an Intelligent Transportation System; Apresentado*: The 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference 2018; Novembro/2018); IEEE IEMCON 2018 VANCOUVER/ CANADÁ.*

As VANETs (*Vehicle AdHoc Networks*) [P10] foram inicialmente introduzidas em 2001 para aplicações "*car-to-car AdHoc mobile communication and networking*", onde redes podem ser formadas e informações podem ser trocadas entre os veículos. A arquitetura de comunicação possibilita dois tipos de conexão: V2V (*Vehicle-to-Vehicle*) e V2I (*Vehicle-to roadside Infrastucture*). A VANET é formada por nós móveis e semi-móveis com infraestrutura, espontânea, com elementos vizinhos, de forma descentralizada, auto organizada com rotas *Multi-hop*. O Nó anda com média/alta velocidade e muitos nós (alta densidade) seguindo a estrada (ambiente restrito com direção e espaço limitado). A ITS permitirá maior segurança na locomoção, melhor navegação com menor tráfego e novos serviços. A aplicação do modelo VANET/ITS é a análise de uma rodovia sobre controle e monitoração de uma concessionária de estrada.

Este artigo [P10] apresenta a simulação hibrida de uma rede de telecomunicação (Figura 25) usada para um Sistema de Transporte Inteligente (ITS), bloco funcional de uma Rede VANET da *Smart City*. A VANET, diferentemente da MANET, possui um alto grau de mobilidade e de concentração dos nós devido à alta velocidade dos carros, necessitando um algoritmo de roteamento ágil para reconfiguração da rede. A análise de desempenho e o dimensionamento de uma rede IoT é apresentado, usando simulação por eventos discretos (DES), considerando mobilidade do nó (*Two Ray Propagation Model e Random Way Point*) e Otimização de Roteamento usando algoritmo de Monte Carlo. O modelo foi analiticamente validado usando as Redes de Jackson. O estudo da capacidade no mediador é feito visando o planejamento e o dimensionamento da rede, medindo-se Tempo Médio de Fila e Utilização de CPU.

Seis casos de estudo são mostrados: Rede Congestionada, Não Congestionada, Não Congestionada com Prioridade, Congestionada sem Prioridade, Sem otimização de Roteamento e Com otimização de Roteamento.

O Modelo da Rede VANET é um pouco diferente dos outros casos (Vide Figura 25). Possui um Modelo Físico formado pelos carros em grupos (*Cluster*), o ponto de acesso ao serviço de rede (SAP ou *Cluster Head*), o Mediador, a Internet e as Aplicações ITS. Possui também um Modelo Lógico hierárquico dividido em 4 camadas: Intravehicular (Rede Bluetooth interna ao carro, controlada pelo Computador de Bordo), Rede Geográfica VANET (Rede AdHoc interligando os carros e *cluster*), Rede Internet tradicional (interligando o Sistema Mediador da Estrada com as aplicações ITS, e Aplicações (ligando as aplicações ITS com os órgãos públicos operacionais das estradas (concessionárias, polícia rodoviária, bombeiros, ambulâncias, guinchos, etc). A primeira e a última hierarquia são abstraídas devido ao baixo tráfego e envolver diversos órgãos públicos. A configuração de rede da Figura 25 passa a ser apenas inicial pois o roteamento pode ser otimizado através do algoritmo de Monte Carlo.

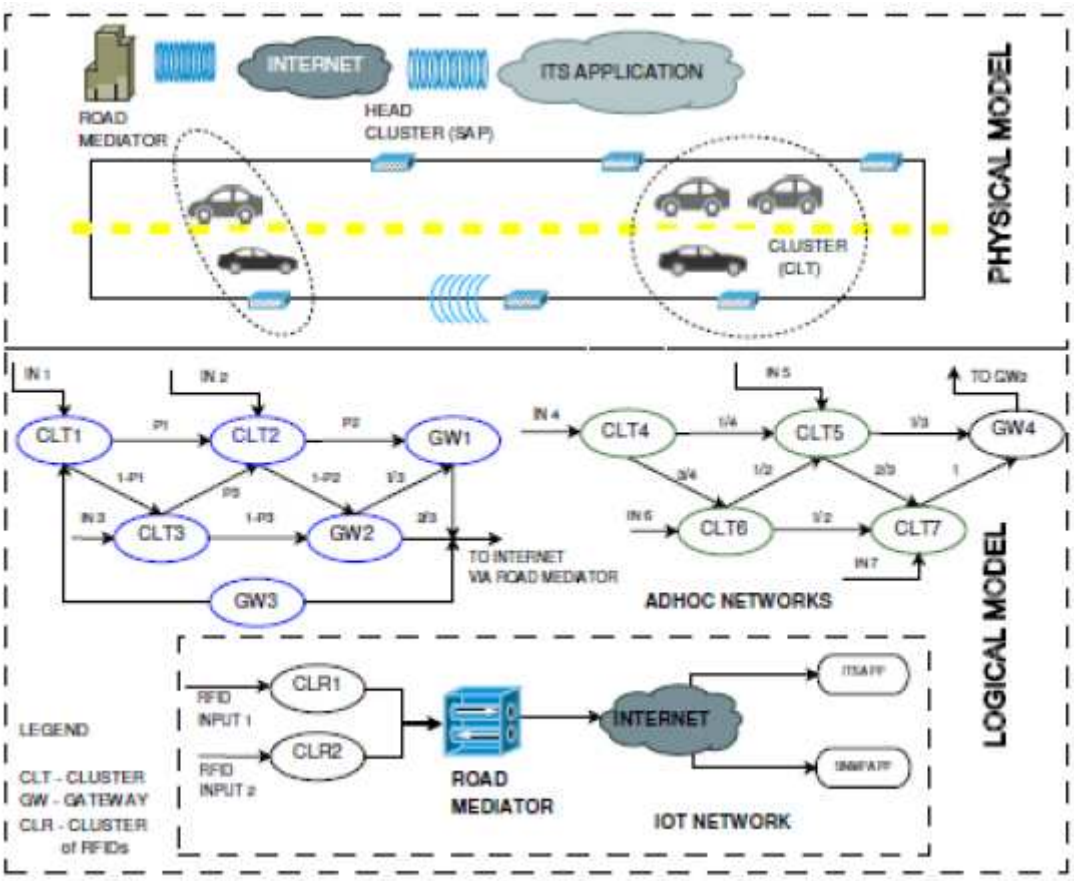

Figura 25: Modelo de Rede Físico (acima) e Lógico (abaixo) [P10].

Os parâmetros de mobilidade (Tabela 13) são diferentes dos casos anteriores MANET (Tabela 8), devido à forte mobilidade/velocidade dos automóveis e a forte concentração de veículos; a velocidade passa a ser de 20m/s (72 Km/h), Área de Cobertura (1000 x 500 m2) com um Intervalo de Direção de apenas 90 graus (-45 a + 45 graus), 20 nós por *cluster*, *range* de 250 m, usando o *Random Way Point.* O Modelo de Mobilidade Manhattan pode ser usado para Centros Urbanos.

Tabela 13 : Parâmetros de Entrada MATLAB para VANET [P10].

Input Parameters	Values
Receiver Threshold	-88 dBm
Area size	1000 x 500 m^2
Antenna type	Omnidirectional
Antenna height (h_t, h_r)	1.5 m
Antenna gain (G_t, G_r)	1.0
System Loss Coefficient (L)	1.0
# Mobile nodes in a Cluster	20
Mobility model	Random Waypoint
Speed interval	[0.2 - 20] m/s
Pause interval	[0-1] s
Walk interval (walk time)	[2-6] s
Direction interval	[-45 + 45] degrees
Transmission frequency	5.8 GHz
Transmission power (P_t)	15 dBm
Simulation time	306 s

Os sensores, RFIDs e GPSs geram informações para o Computador de Bordo que junta em pacotes a serem enviados para as aplicações ITS. Apenas 5 das mensagens são consideradas emergências e necessitam de atuação imediata da concessionária através da chamada a órgãos de polícia, bombeiros, ambulâncias e guinchos. Foram considerados 3 tipos de serviços: Localização de Carro, Descoberta de Destinação e Tratamento de Mensagens Emergenciais (Roubo, Sequestro, Acidente, Quebra do Carro, etc).

A Figura 26 e Tabela 14 apresentam os resultados da execução dos casos de estudo: Tempo Médio de Fila/Utilização de *CPU* e atraso médio das mensagens.

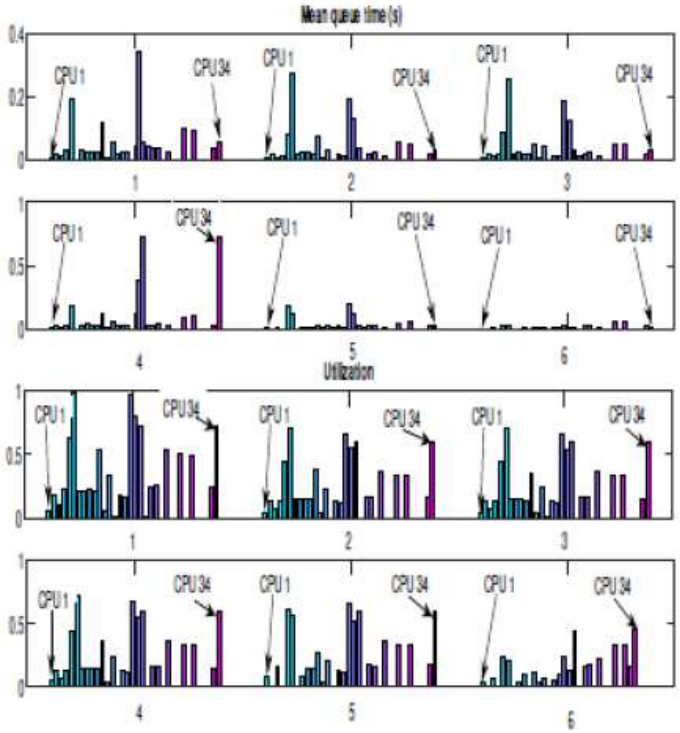

Figura 26: Tempos Médios de fila (a e c) e Utilização [P10].

Observe que ambas as variáveis medidas vão decrescendo conforme o descongestionamento da rede e o uso de priorização nas mensagens.

Tabela 14: Tempo de Atraso de Mensagem (secs) para casos de estudo [P10].

Message source type (Priority)	Case 1	Case 2	Case 3	Case 4	Case 5	Case 6
	C	NC	NC	C	NC	NC
	NP	NP	P	P	NP	NP
SNMP (PR_0, max prio)	0.093	0.085	0.085	0.09	0.085	0.085
vehicle EMERGENCY (PR_1)	28.04	2.28	2.091	2.27	2.18	2.10
ROAD SENSOR (PR_2)			3.730	4.45	2.18	2.10
vehicle NORMAL (PR_3)			3.127	84.76	2.18	2.10
ROAD RFID (PR_4)	2.170	2.145	2.145	2.15	2.145	2.145

PR=priority, NP=no-prio, C=congested NC = no congestion

Observe que os atrasos de mensagem diminuem de 28,04 secs(Congestionada) → 2,28 → 2,091 ➔ 2,27 (Rede Congestionada de novo) → 2,18 e 2,10 secs. Conclui-se que o Descongestionamento de rede, priorização de mensagens e a otimização do roteamento (diminuição de saltos) são fatores relevantes ao efetivo uso dos recursos de rede e para a queda do atraso das mensagens.

5.8) Cenário # 8: Diminuição do Consumo de Energia (Sustentabilidade) em um *Smart* CAMPUS;

[P11] Reducing Power Consumption in Smart Campus Network Applications through simulation of high-priority service, Traffic Balancing, Prediction and Fuzzy Logic; Apresentado: ***Winter Simulation Conference 2018; Dezembro/2018); WSC 2018 GOTEMBURGO/ SUÉCIA*****.**

A prioridade e o congestionamento tradicionalmente têm sido associados com qualidade de serviço em redes e sistemas de tempo real. Este artigo mostra outra face da prioridade e congestionamento, seu impacto no consumo de energia e na durabilidade das baterias.

O artigo [P11] está preocupado com a sustentabilidade; apresenta técnicas para redução de consumo de energia de dispositivos dependentes de bateria em uma aplicação *Smart Campus*, incluindo hospital. Esses dispositivos são conectados por sistemas de redes os quais podem ser sujeitos a flutuações de atrasos de mensagens que controlam equipamentos essenciais. Apresenta 5 casos de estudo usando simulação por eventos discretos (DES), mostrando que o consumo de energia pode ser reduzido usando priorização e balanceamento de tráfego emergencial de rede. Um algoritmo de Predição e um controlador de Lógica Fuzzy foram usados para indicar o nível sobre o qual o sistema deve desligar a carga a fim de reduzir o consumo de energia. A análise do caso de estudo mostra que uma redução considerável de energia é obtida através da redução do atraso de mensagens e também devido ao Controlador Fuzzy dos equipamentos de Ar-condicionado e Iluminação. Possibilita também o uso de um Algoritmo de Predição para a tomada de decisão de troca de baterias de UPS (*Uninterruptible Power Supply*). Essa pesquisa utiliza adicionalmente a IoT para controle de atuadores.

O artigo apresenta 4 estratégias de redução do consumo de energia elétrica (vide Tabela 15):

1. Baterias de dispositivos móveis (Redes IoT/AdHoc);

2. Baterias de operação em equipamentos emergências (UPS) e de alto consumo (sistemas de Ar-Condicionado AC);
3. Outros equipamentos, não emergenciais e de alto consumo;
4. Aplicações que fazem o uso de Lógica de Controle Fuzzy para controlar o nível de operação (%) dos aparelhos de ar-condicionado e iluminação, usando variáveis tais como temperatura, humidade e claridade.

Tabela 15: Estratégias para a Redução do Consumo de energia em um *Smart Campus*[P11].

Strategies →	Priorization	Network load balancing		Traffic	Fuzzy control logic	mode of operation
Energy reduction in	Delay reduction (ΔT)	Delay reduction (ΔT)	Utilization reduction (ΔU)	load		
IoT/AdHoc network (on battery) (Fig. 1)	✗	✗	✓Case 1 ✓ Case 2	high low	✗	normal, power out.
emergency equip. (on UPS battery)	✓ Case 4 ⊖ Case 3	✓ Case 1 ⊖ Case 2	✗	high low	Case 5 ✓	power outage
other equipment (power network)	✗	✗	✓	high low	✗	normal
Application power saving	⊖	⊖	⊖	⊖	Case 5 ✓	normal power off

✗= ineffective , ✓= effective, ⊖ = negligible

A Figura 27 apresenta o Tempo Médio de Fila e a Utilização de CPU de cada processador.

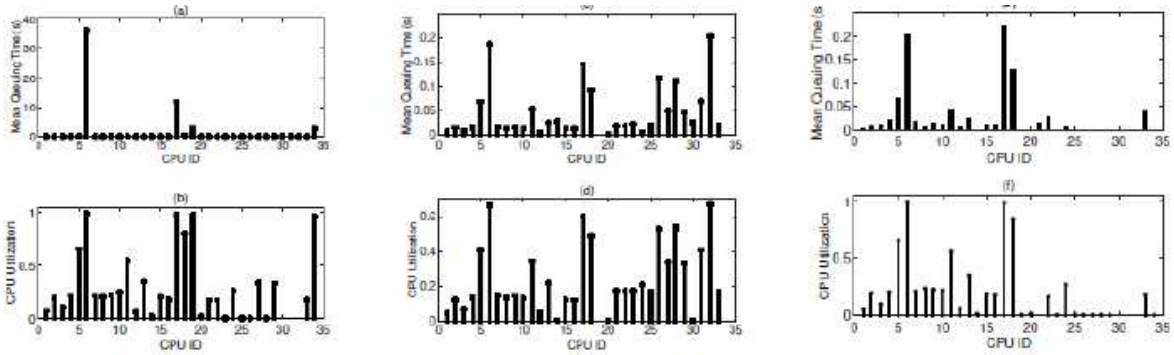

Figura 27: Tempo Médio de Fila e Utilização de CPU [P11]: Caso 1 (a,b), Caso 2 (c,d) e Caso 4(e,f) [P11].

Os 4 casos de estudo com seus atrasos de mensagem de rede são apresentados na Tabela 16. Eles são executados sobre redes congestionadas e balanceadas, com e sem prioridade nas mensagens emergenciais. Observe no Caso 1 que o atraso de mensagem na rede e a utilização de *CPU* são muito grande e vão diminuindo conforme o descongestionamento da rede e o uso de prioridades na mensagens emergenciais: 28,04 (secs) → 2,28 → 2,091 → 2,09 (secs), subindo um pouco para 2,27 sec mesmo no caso de rede congestionada devido ao uso de prioridade; mensagens com alta prioridade podem efetivamente atravessar a rede em situação de congestionamento de tráfego. Duas funções foram criadas usando logica *fuzzy* funcionando como atuadores para controles de iluminação e ar-condicionado.

Tabela 16: Tempo de Atraso de Mensagem na rede para casos de estudo 1-4 (prio=prioridade) [P11].

Message source type	Case 1	Case 2	Case 3				Case 4	
	congested	balanced	balanced		balanced		congested	
	no-prio	no-prio	(a) with 3 prio		(b) with 2 prio		with prio	
	delays	delays	delays	prio	delays	prio	delays	prio
SNMP (high)	0.093	0.085	0.085	0	———	0	0.09	0
sensor 1 AC	28.04	2.28	2.091	**1**	2.090	**1**	2.27	1
sensor 2 light			3.730	**2**	3.728	**1,2**	4.45	2
sensor 3 battery			3.127	**3**	3.127	**2**	84.76	3
RFID	2.170	2.145	2.145	4	2.144	4	2.15	4
SNMP (low)	——	——	——	5	0.086	5	—-	5

A Redução do Consumo de Energia em um Campus com 200 ACs pode chegar a:

200 ACs x 50% Economia x 8 hs x 17,1 KWh/mês = 13.680 KWh/mês.

A Figura 28 apresenta os gráficos das variáveis *Fuzzy* (via interface Visual Basic) de entrada e de saída para o Ar-Condicionado e Iluminação. A Tabela 17 apresenta exemplo de uso de regras *fuzzy*.

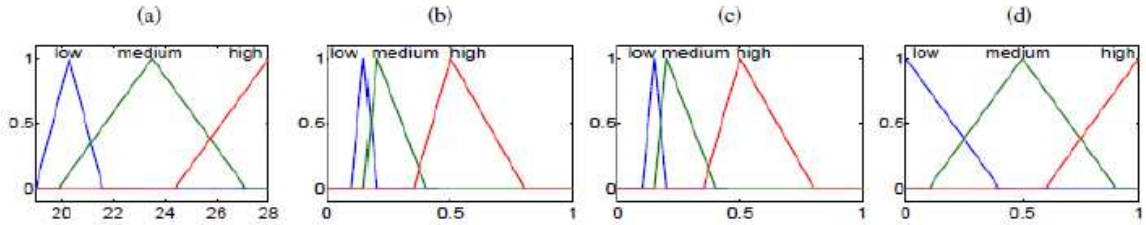

Figura 28: Variáveis de Entrada (a,b,c) e Saída (d) para Ar-Condicionado e Iluminação [P11]**.**

Tabela 17: Exemplos de Regras *Fuzzy* usando conjunção (AND) **[P11]**

Input Variables			Output Variables	
Temperature	Humidity	Clarity	AC Level	Lighting Level
L	L	L	L	H
M	L	L	M	H
H	L	L	H	H
...	...	...	...	...
M	H	H	H	L
H	H	H	H	L

e.g. RULE 1: IF TEMP=L AND HUM=L AND CLARITY=L THEN AC LEVEL=LOW

A Figura 29 mostra a redução de energia no ar-condicionado e na iluminação, chegando a ser até 50%. A Figura 30 apresenta as variáveis de controle de entrada e de saída para os sistemas UPS, visando através de Lógicas de Predição (preditor baseado em filtro de Kalman) antecipar a substituição de baterias antes que estas estraguem, monitorando a corrente e a tensão da bateria. A Lógica de Predição trabalha com variáveis de corrente e voltagem da bateria, que são parâmetros de entrada para Logica *Fuzzy* que determina a necessidade de troca de bateria.

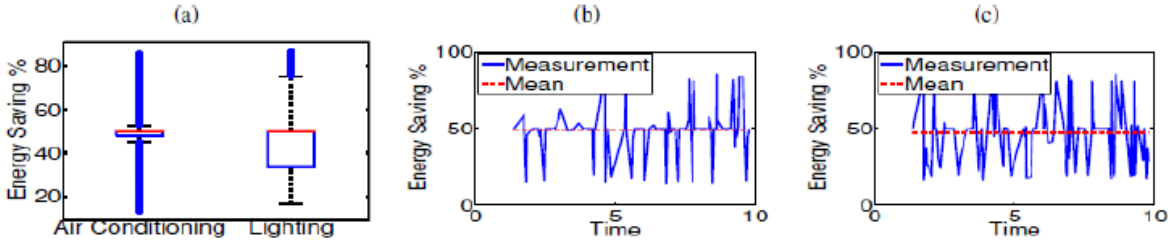

Figura 29: Redução de Potência no Ar-condicionado e Iluminação.

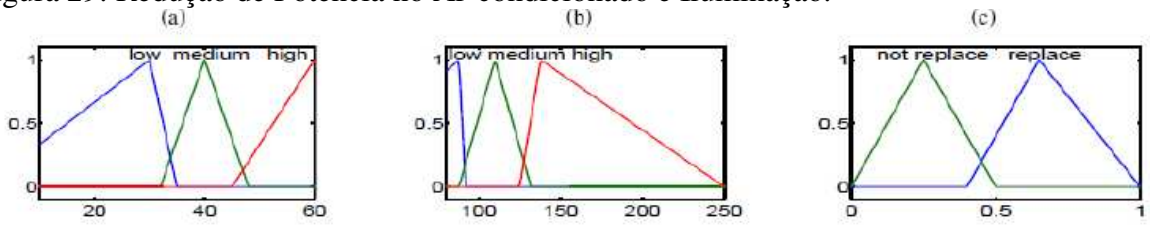

Figura 30: Entrada (a,b) e Saída (c) *Fuzzy* para Controle da UPS [P11].

5.9) Cenário # 9: Tecnologias de Telecomunicações e Simulação Matemática Computacional por Eventos Discretos, para a Redução de Risco de Mortes em Desastres Ambientais;

[P13] Tecnologias de Telecomunicações e Simulação Matemática Computacional por Eventos Discretos, para a Redução de Risco de Mortes em Desastres Ambientais

Apresentado e Publicado no: *Workshop sobre Ciências Matemáticas e Redução do Risco de Desastres; UNESP, São José dos Campos, 6/JUNHO/2019. Organização UNESP, INPE, CEMADEN.*

Este artigo [P13] apresenta as principais tecnologias existentes em telecomunicações que podem ser utilizadas para a antecipação da detecção de ocorrência de desastres, avisos imediatos de evacuação e consequente redução de riscos de mortes em desastres ambientais. Apresenta também um Modelo de Simulação Hibrida Matemática Computacional dessas redes, usando Eventos Discretos, Mobilidade, Otimização de Monte Carlo e Validação de Jackson.

A Internet das Coisas (IoT) realiza uma nova transformação digital, interligando dispositivos, incrementando valores de negócios, redefinindo organizações e gerando enorme quantidade de oportunidades. Sem dúvida, esta é uma nova onda tecnológica que cria uma nova fronteira no mundo conectado com as pessoas, computadores, dispositivos (objetos/coisas), ambientes e objetos virtuais, todos ligados e capazes de interagirem entre si, dividindo a comunicação em camadas conforme Padrão Internacional ITU-T. A IoT foi possível graças ao barateamento e a diminuição do tamanho dos componentes de acesso à Internet. Possibilita também o incremento de inteligência em diversos setores da economia através das Aplicações *SMART*, incluindo Redes de Salvamento em Catástrofe. A inteligência e a automação são decorrentes dos acréscimos de processamento, memória e comunicação nos objetos envolvidos. Novas formas simplificadas de acesso foram selecionadas pela IoT visando baratear e potencializar o uso da rede: WSS (*Wireless Systems Solutions*), rede de sensores Adhoc, aplicações ZIGBEE e redes celulares 2G/3G/4G(LTE). A simulação matemática computacional auxilia no estudo e planejamento dessas redes.

A IoT selecionou diversas tecnologias padronizadas e já utilizadas internacionalmente. Assim sendo, muito dos novos ambientes IoT são parecidos com os atuais existentes na Internet. A maioria das tecnologias é por rádio e sem fio por questões de flexibilidade e alcance, padrões IEEE 802.11/15/16. Os sensores são os geradores básicos de informações

em uma Rede IoT (Figura 6). Por sua simplicidade, só conseguem gerar informações específicas de temperatura, pressão, umidade, claridade, deslocamento, etc; o tráfego dessas informações é feito através das redes de sensores que podem ser fixas ou móveis. Já existem sensores capazes de gerar diversas dessas informações conjuntamente e outros sensores embutidos em etiquetas RFID (*Radio Frequency Identification*), evitando o uso de bateria. Essas tecnologias permitem a antecipação na detecção da ocorrência de algum desastre ambiental, possibilitando o aviso da população através de sirenes, painéis, atuadores e celulares, mostrando as rotas de fuga existentes.

O Modelo de Simulação de Rede IoT (Figura 11) usado no estudo das fases de planejamento, desenvolvimento, implantação e evolução da rede, contempla elementos como sensores, atuadores, RFIDs, Redes AdHoc e Aplicações. As redes AdHoc, parte da IoT, foram criadas para fins militares e não possuem infraestrutura fixa centralizada, possibilitando sua formação rápida, por diversos nós que tem proximidade para a comunicação. As redes celulares 2G/3G /4G (LTE) são as mais utilizadas no aviso de desastres visando saída imediata pelas rotas de fuga e na busca na nuvem das informações coletadas na rede.

As tecnologias selecionadas pela IoT são consagradas no mercado de telecomunicações e podem reduzir muito o risco de mortes em desastres ambientais. Para tal, se torna necessário o investimento na construção de novas redes e no uso de ferramentas de simulação híbrida de Eventos Discretos (junto com Modelos *Random Way Point*, *Two-Ray*, Monte Carlo e Jackson), de tráfego com processos estocásticos e quantificação de incertezas em modelagens físicas de redes (Figura 11), durante seu projeto. A simulação serve como ferramenta de gerência e estudo da rede nas fases de planejamento, desenvolvimento, implantação e evolução.

5.10) Cenário # 10: Um método de Validação de Modelos Simulados de Redes AdHoc, incluindo MANETS, VANETS e Cenários de Emergência;

[P14] Dimensioning of IoT Networks: an Incremental Validation Approach

Apresentado e Publicado na Conferência *AdHoc-Now 2019 (18th International Conference on Ad Hoc Networks and Wireless) em Luxemburgo em 1-3/Outubro/2019*

Simulação é correntemente uma técnica amplamente usada devido à sua popularidade e disponibilidade de ferramentas, permitindo o exame de diversos cenários reais para o dimensionamento de um novo sistema ou o incremento/expansão de um sistema existente. No entanto, devido aos cronogramas apertados impostos aos praticantes de simulação, esforços substanciais são gastos na medida das propriedades chaves do sistema, na construção do Modelo do Sistema, e a simulação propriamente dita do sistema real. Assim sendo, não disponibiliza tempo suficiente para estudar um dos mais importantes passos do projeto de simulação, que é a validação e a verificação do Modelo de Simulação propriamente dito.

Este artigo [P14] apresenta uma metodologia de planejamento e validação de redes AdHoc e IoT simuladas, considerando nós congestionados e não congestionados. Consiste de um conjunto de passos baseados no Modelo de Filas de Rede de Jackson: Criar Matrix R com Probabilidade de Transmissão de cada link entre os clusters, Criar Vetor Gama com a Taxa de

Geração de Pacotes, Descobrir Lâmbida com a Taxa de Chegada em cada *CPU*, Descobrir Atrasos, Rodar Modelo de Simulação e Comparar Resultados.

O Modelo de Rede AdHoc validado, composto de um número de *clusters* de rede, considera rede Móvel (MANET), Veicular (VANET) e Cenário de Recuperação de Desastres. O método proposto apresenta resultados satisfatórios e potencial para futuros incrementos e evoluções. O objetivo é analisar o tráfego de um nó de destino e estimar sua capacidade considerando uma aplicação AdHoc. Especificamente, objetivamos o uso da validação para determinar a utilização do processador e o atraso da mensagem. O Modelo Proposto e a ferramenta de simulação podem ser usados para planejamento, dimensionamento da rede, mas também como guia de gerenciamento da rede em situações críticas que podem ser antecipadas.

Adicionalmente à validação MANET, os resultados mostram que a Otimização de Roteamento de Monte Carlo (Caso VANET) e a disponibilidade/confiabilidade (Caso de Recuperação de Desastres) podem ser relevantes para o efetivo uso de recurso da rede.

5.11) Cenário # 11: Planejamento de Redes AdHoc e IoT em Operações de Emergência

[P15] Planning of AdHoc and IoT Networks under Emergency Mode of Operation

Apresentado e Publicado na Conferência IEMCON 2019 (IEEE e UBC) e futura apresentação na *Revista "SENSOR JOURNAL".*

Nos ambientes de catástrofe [P15] (Tabela 18) é desejável que existam muitos tipos de redundância, inclusive em redes de telecomunicações: Redes AdHocs (MANET, VANET, FANET), Redes RFID, Redes IoT, Redes Celulares (2G, 3G, 4G e 5G), Redes Satélites, Balões de Telecomunicações, *Walk Talk*, etc. Essa redundância é necessária pois em caso de catástrofe diversos recursos podem se perder devido às tempestades, inundações, desmoronamentos, queda de morros, arvores e postes, falta de energia, etc,

Tabela 18: Cenários 0, 1 e 2 - Otimização de Roteamento e Recuperação de Desastre [P15].

Scenario	Cases	Description	Goal	Network Part that is Analyzed	Parameters analyzed	Results
0 (MANET Network as a Reference)	1	MANET Network as a Reference	MANET Network as a Reference	All the Network	Mean queueing time and message delays(MQT+MD)	Tables II, III, IV, V and VI
1 (VANET Routing Planning Optimization)	1	VANET NETWORK	Reference Network	All the network, without the Probabilities, complete model It is the reference for the other cases	(MQT+MD)	Figures 1 and 2
	2	One ADHOC subnetwork : A – Monte Carlo considering the probabilities of hops B – considering processing capacity	To Reduce end-to-end delays from source to MEDIATOR MD	AdHoc from above is optimized	(MQT+MD)	Figures 2, 3 and 4
	3	Two ADHOC subnetwork : A – Monte Carlo considering the probabilities of hops B – considering processing capacity	To Reduce end-to-end delays from source to MD	Both AdHoc networks are optimized	(MQT+MD)	Table VII Figures 2, 3 and 4
2 (Network Redundancy in Disaster)	1	Network without disaster	Reference Network	All network	(MQT+MD)	Figures 1 and 2
	2	Disaster – adding Emergency Gateway G3 (CLTI LINK REDUNDANCY)	Availability + connectivity	Emergency Gateway + CLTI LINKS	(MQT+MD)	Tabela VIII
	3	Disaster – adding Macrocell Gateway (connectivity inside a cluster)	Availability + connectivity	Macrocell Gateway + AdHocs inside a cluster	(MQT+MD)	Connectivity Lost (RWP)

O **Cenário 0** só possui o Caso 1 (MANET Reference) e apresenta uma Rede de Referência AdHoc MANET.

O **Cenário 1** (*VANET Routing Optimization*) está preocupado em otimizar o roteamento em Rede VANET usando Monte Carlo, diminuindo o número de saltos (*hops)* no caminho das mensagens; apresenta 3 casos:

- Caso 1 sem otimização,
- Caso 2 com otimização na sub-rede Adhoc superior e
- Caso 3 com otimização nas 2 sub-redes AdHoc.

Regiões com perigos ambientais precisam ter mais atenção e se preparar para diminuir o risco de mortes em caso de catástrofe. O **Cenário 2** (*Disaster Recovery*) mostra 3 casos de estudo contemplando ambientes de catástrofe:

- Caso 1: Redes AdHoc e IoT Normais sem Catástrofe;
- Caso 2: Rede AdHoc com Redundância de *Link* para o Nó de Emergência (GW3 e Processador 14);
- Caso 3: Rede AdHoc com Redundância de Acesso *Wireless* dentro do *Cluster*, em caso de Falha de Comunicação maior que zero, indo o pacote direto para uma Macrocélula tipo Wi-Max ou LTE.

A nova configuração de rede é mostrada na Tabela 19.

Tabela 19 : Nova Configuração de Rede para Catástrofe (MANET e VANET) [P15].

Table 1: Network configuration.

Function	Probabilities			Output CPUs		
GA_{12}	1			25		
GA_{34}	1			28		
GA_{57}	1			29,33		
GA_8	1			19,34		
AdHoc submodel	1,1,1,1			30,31,32,33		
CLR_1	1			21		
CLR_2	1			22		
MD	1/2, 1/2			24, discard		
GWI	1/3,1/3,1/3			23, 26, 27		
—-	Vanet	Manet	Disaster	Manet	Vanet	Disaster
GW_1	1	1	0	5	5	0
GW_2	1/3, 2/3	1/3, 2/3	0	11,6	0	0
GW_3	1	1	1	14	14	14
GW_4	1	1	0	17	17	0
CLT_1	1	1/4, 3/4	0	1,2,20*	1, 20*	1,20*
CLT_2	1	1/3, 2/3	0	3,4	3	3
CLT_3	1	1/2, 1/2	0	7,8	8	8
CLT_4	1	1/4, 3/4	0	12,15	12	12
CLT_5	1	1/3, 2/3	0	16,13	13	13
CLT_6	1	1/2, 1/2	0	9,10	10	10
CLT_7	1	1	0	18	18	18

* output-CPU 20 to GW_3 is used only in an emergency

As Figuras 31, 32 e 33 mostram os resultados de Tempo Médio de Fila e Utilização de *CPU* para os 3 casos acima. O Caso 1 trata de uma Rede AdHoc normal dentro do cluster, sem catástrofe e sem perda de pacote no *cluster*; os *clusters* são interligados por *Links* com e sem fio formando uma Rede tipo *Mesh* fixa. Observa-se que no Caso 2 o *Gateway* de Emergência (GW3) assume todo o tráfego dos *Clusters* CLT1 a CLT7, estando assim muito sobrecarregado, a ponto de ser necessário que seu processamento seja escalado para níveis de desempenho do Mediador. No Caso 3 inicia-se o estudo da falha de comunicação dentro do *Cluster* (*FaultProbability* = 4,5 %), sendo nestes casos os pacotes desviados para uma macrocélula WiMax ou LTE. Com essas redundâncias, temos a certeza que não haverá falha na comunicação durante a catástrofe e sua recuperação. Ambas as soluções dos casos 2 e 3 são construídas montando-se redes com topologia tipo “estrela” devido à centralização no *Gateway* de Emergência (GW3) e na macrocélula.

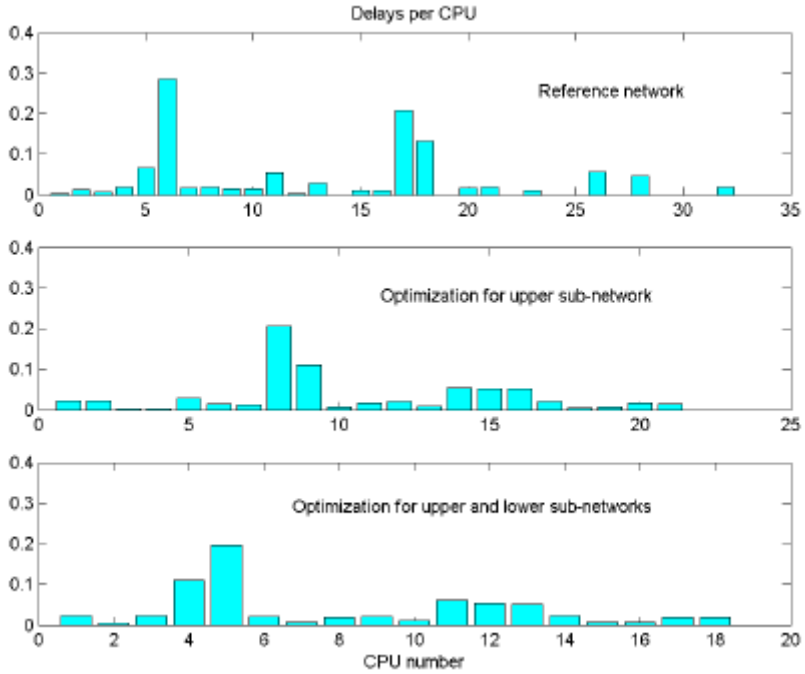

Figura 31: Cenário 1 - Otimização de Roteamento, impacto nos atrasos [P15].

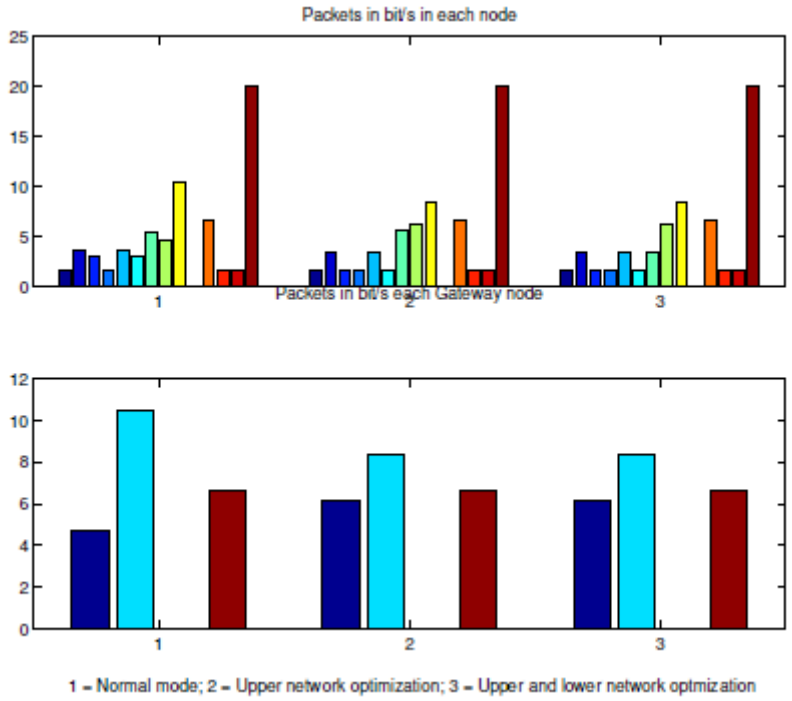

Figura 32: Cenário 1 - Otimização de Roteamento, impacto na Taxa de Pacotes [P15].

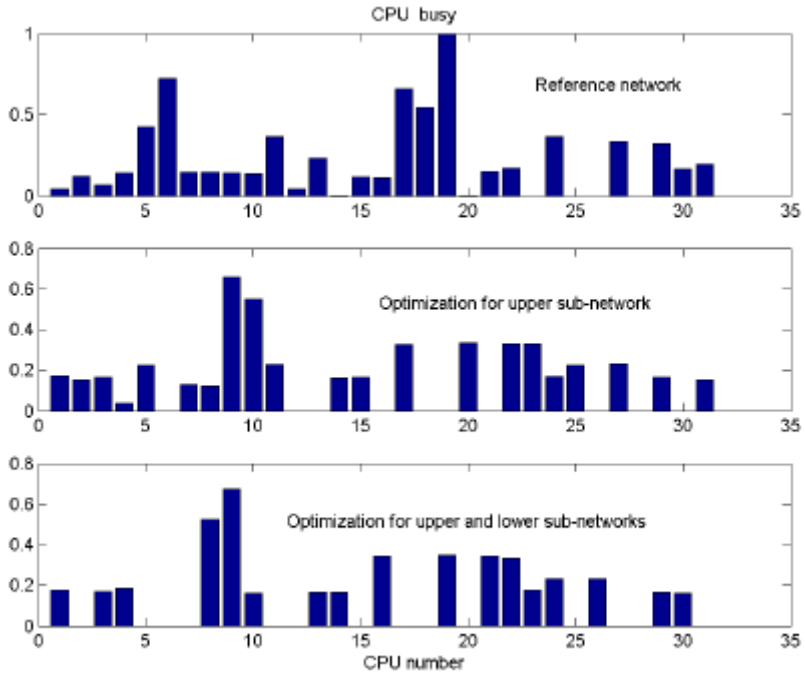

Figura 33: Cenário 1 - Otimização de Roteamento, impacto na utilização de *CPU* [P15].

Essa simulação mostra que é possível a criação de redundância visando que não ocorra nenhuma falha de comunicação durante uma catástrofe e sua recuperação, possibilitando a alta disponibilidade com baixo custo e diminuindo assim o risco de mortes nessas situações. É claro que a Aplicação *Smart Disaster Recovery* precisa se antecipar à detecção da ocorrência do desastre através de sensores de temperatura, pressão, umidade, claridade e deslocamento, e disparar avisos para a população, defesa civil, autoridades governamentais (municipal, estadual e federal), bombeiros, ambulâncias, polícias, etc. Deve disparar avisos em atuadores de Alarmes sonoros em Sirenes, Rotas de Fuga em Painéis e Celulares, e vídeo monitoramento através de câmeras IP. Todo esse ambiente diminuirá o risco de mortes. Para tal, se torna necessário o projeto, simulação e construção dessas redes de catástrofe.

As Redes de Celulares 2G, 3G, 4G e 5G, são os melhores caminhos para informar a população de desastres, pela sua capilaridade, disponibilidade e usabilidade (toda população tem seu celular). É claro que em caso de falha da rede celular precisam ser usados outros recursos como sirenes e painéis. A rede celular permite também de forma barata, confiável e simples, o acesso de informações ambientais coletadas e disponíveis na nuvem (*cloud*). A Tecnologia Celular 5G, que está no início de implantação mundial, oferecerá pela primeira vez a funcionalidade da rede AdHoc embutida, através da funcionalidade D2D.

O conhecimento e aprendizado dessas novas redes podem ser feitos através de ferramentas de simulações.

As tecnologias selecionadas pela IoT são consagradas no mercado de telecomunicações e podem reduzir muito o risco de mortes em desastres ambientais. Sendo necessário o investimento na construção e estudo dessas novas redes.

5.12) Cenário # 12: Segurança da Informação e Gerenciamento de Rede IoT

[P16] Segurança da Informação e Gerenciamento de Rede IoT

Apresentado e Publicado no *Congresso BTSYM 2019 (The Brazilian Technology Symposium) em Campinas em 22-24/Outubro/2019*

Este artigo [P16] apresenta os principais protocolos utilizados para Segurança da Informação e Gerenciamento da Rede IoT, tornando assim as redes confiáveis e a prova de *hackers*.

Muitos desses protocolos foram aproveitados da Rede INTERNET tradicional (HTTPS, IPSEc, etc) e outros foram criados e simplificados para utilização em ambientes restritos dos objetos (Tabela 20).

Tabela 20: Mecanismos de Segurança adicionados: a) Protocolos de Acessos Restritos (Limitações (*Constrained*) em termos de: Potência, Memória, Processador, Banda, Comunicação e Tamanho)) b) Tecnologias de Acesso [P16].

Protocolo/ Arquitetura	Origem	Modelo de Mensagem	Mecanismo de Segurança	Padronização	Transporte
a) AMQP	Bancos2003	Advertiser/Subscriber	SSL	OASIS 2012	TCP
MQTT	IBM 1999	Advertiser/Subscriber	TLS Brokers (Username + Password)	IEEE 2013	TCP
CoAP	IoT	REST [64] Request/Response Advertiser/Subscriber	DTPLS	RFC 7252	UDP
6LOWPAN	IETF	Micro IP	SubconjuntoIPSEC	RFC4919	IEEE802.15.4
b) RFID	EPCglobal	Tag Information 96bits	Autenticação, Criptografia e Assinatura	GS1 EPCglobal	RFID
WiFi	IEEE	IEEE 802.11 (a,b,g,n)	Criptografia, Filtros MAC, Protocolos e Endereços IPs	IEEE	TCP/IP
ZigBee	ZigBee Alliance	IEEE 802.15/ ISA100.11 a	Controle de Acesso, Criptografia, integridade dos quadros, sequencialidade, Trust Center	IEEE	IEEE802.15.4
Bluetooth	Bluetooth Group	IEEE 802.15.1	Autenticação, Criptografia e Autorização	IEEE	IEEE802.15.4

O Gerenciamento de Rede poderá ser feito pelo Protocolo SNMP tradicional da Internet ou protocolos específicos das próprias tecnologias (RFID, WiFi, Bluetooth, ZigBee).

O SNMP especifica (na versão 1) quatro tipos de unidades de dados (PDU) [4]:

1. *GET*, usado para retirar um pedaço de informação de gerenciamento.
2. *GETNEXT*, usado interativamente para retirar sequências de informação de gerenciamento.
3. *GETBULK*, usado para retirar informações de um grupo de objetos.
4. *SET*, usado para fazer uma mudança no subsistema gerido.
5. *TRAP,* usado para reportar uma notificação ou para outros eventos assíncronos sobre o subsistema gerido.

Na tese foi implementada uma pequena solução de Monitoramento SNMP do Mediador, com mensagens do tipo TRAP, Comandos e Respostas. Uma aplicação SNMP foi desenvolvida visando a geração e o tratamento das mensagens SNMP, nos quais foram priorizadas na rede.

5.13) Cenário # 13: Simulação de Redes AdHoc e IoT para Diminuição de Riscos de Mortes em Catástrofe em Cenários de Recuperação de Desastres;

[P17] Increasing Fault Tolerance in IoT and AdHoc Networks for Risk Reduction in Disaster Recovery

Publicado e apresentado no *WSC 2019 (Winter Simulation Conference 2019 - PHD Colloquium) em Maryland (USA); 8-11/Dezembro/2019.*

Em ambientes de desastres [P17] é desejável que existam muitos tipos de redundância, incluindo redes de telecomunicações tais como IoT, AdHocs, RFID, Celulares (2G, 3G, 4G, 5G) e Satélites. Essa redundância é necessária devido à possibilidade de perda de equipamentos no ambiente de desastre. Este cenário apresenta 3 casos de estudo:

Caso 1: Ambiente Normal sem catástrofe;

Caso 2: Rede AdHoc com Redundância de Link e Acesso direto dos *Cluster* de Sensores ao *Gateway* de Emergência, ativado especificamente para a Recuperação do Desastre;

Caso 3: Rede AdHoc com Redundância de Acesso Sem Fio, onde a falha de acesso é encaminhada diretamente para um Macrocélula WiMax ou LTE.

A aplicação *Smart Disater* é responsável em antecipar a detecção da ocorrência do desastre através de sensores de pressão, umidade, temperatura, luz e deslocamento, e monitoração via câmeras IP. É responsável também em acionar os atuadores para avisar a população através de sirenes, painéis e celulares, mostrando a Rota de Fuga. Adicionalmente, deverá avisar a Defesa Civil, autoridades governamentais (municipal, estadual e federal), bombeiros, ambulâncias, etc. Assim sendo, é possível diminuir o risco de mortes e feridos durante o desastre.

5.14) Sumário dos Resultados Esperados e Resultados Observados

Sabe-se que quanto maior for o tráfego de entrada (Número de entradas vezes o tráfego individual de cada entrada), maior será o congestionamento nas filas internas e pior serão os valores de QoS (maior Atraso, maior "*Jitter"*, maior Perda de Pacotes *e "Throughput"*).

5.14.1) Resultados Esperados

Quanto mais aumenta-se o número de entradas (através da diminuição do tempo entre chegadas), maior é o" *throughput*" (vazão), atraso e "*Jitter",* até uma saturação onde se verificará a manutenção da vazão e o início da perda de pacotes pelo motivo das filas estarem sobrecarregadas, conforme mostrado nas Figuras. 34, 35 e 36.

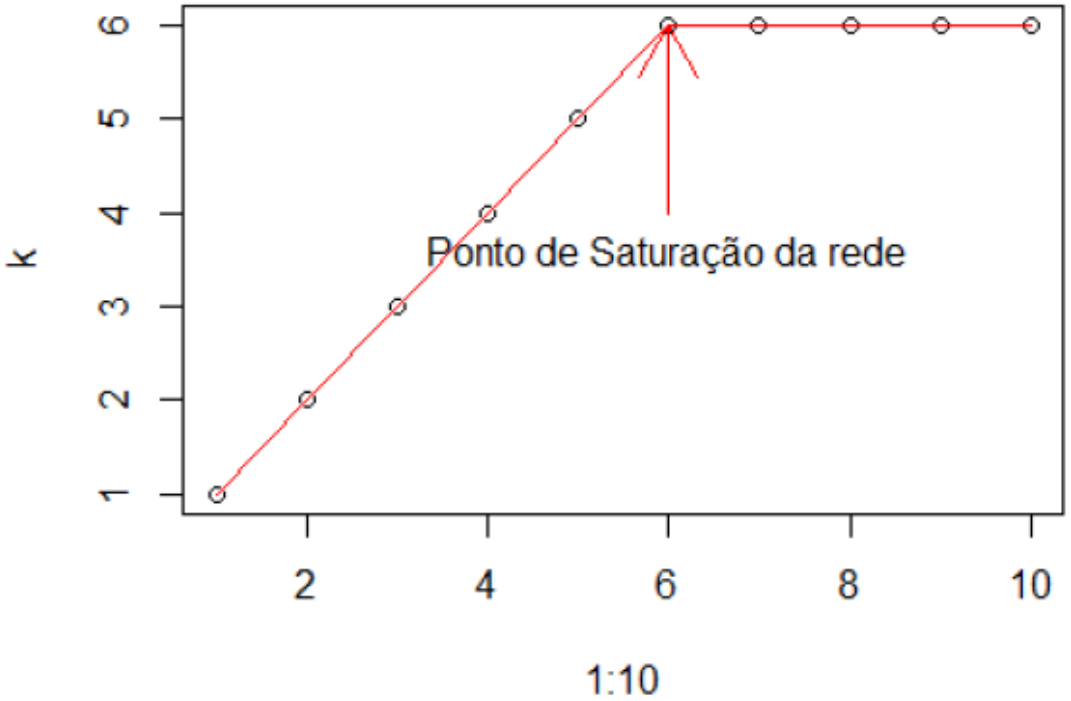

Figura 34: *Throughput*(Vazão) em função do Congestionamento na Rede (com Ponto de Saturação em 6).

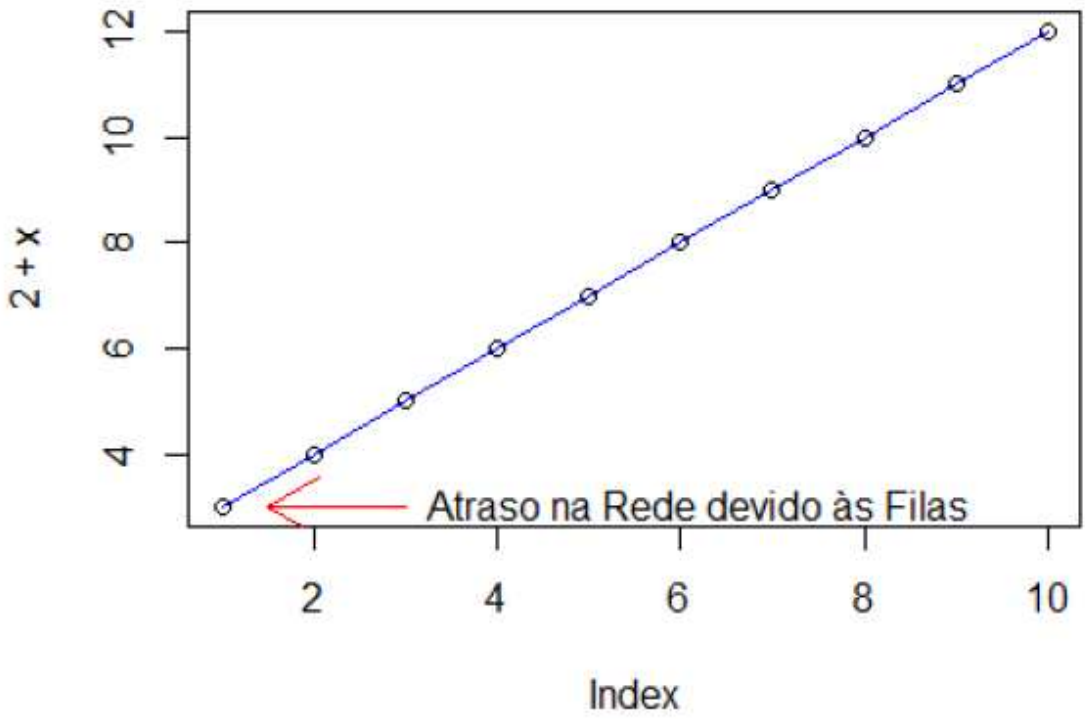

Figura 35 : Atraso e *Jitte*r em função do Congestionamento na Rede.

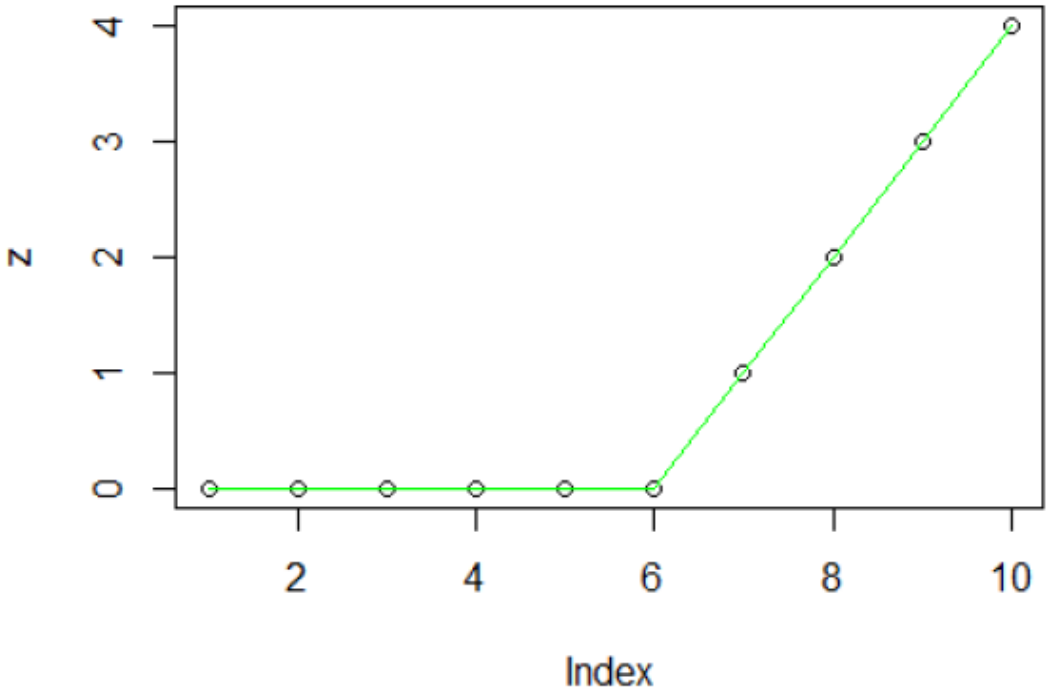

Figura 36: Perda de Pacotes em função do Congestionamento da Rede.

É possível a representação de vários sensores por meio de um único valor determinístico (única fonte ou único *CREATE*). Se a temporização é determinística e se tiver muitos sensores, é possível utilizar a fórmula 1/T= 1/T1+1/T2+....+1/Tn. Por exemplo, se forem 2 sensores, um com 10 segundos e outro com 20 segundos, teremos 1/T=1/10+1/20, ou seja T=

6,67 seg. O comportamento é similar ao de resistores em paralelo. No caso Exponencial, tem-se diversas Etiquetas RFID gerando uma exponencial resultante, com a soma dos Lambidas e o Tempo entre Chegadas de 1/Lambida Total.

O modelo analítico pode ser derivado do modelo de Jackson, para diversas filas distribuídas na rede. Considere uma rede de filas com "N" estações, cada uma com uma ou várias máquinas idênticas e capacidade de espera infinita. As Estações 1, 2,..., n são estações internas e a estação 0 é a estação externa do sistema. Para cada estação interna j, Jobs chegam da estação 0 com iid intervalos de tempo entre chagadas a0j, esperam em fila por uma máquina disponível, e são processados com iid tempos de serviço sj. Após serem processados, Jobs deixam a estação j com intervalo de tempo entre partidas dj e vão para a estação i, i==0,....,n, com probabilidade de transição definida por uma Cadeia de Markov. Assume-se que qualquer sequência de intervalos de tempo entre chegadas externas, tempos de serviço e decisões de roteamento são mutuamente independentes, e que as tarefas são processadas em cada estação, conforme a disciplina FCFS (*First Come First Service*). Se os intervalos de tempo entre chegadas externas e os tempos de serviço forem independentes e exponencialmente distribuídos (Processo de Poisson), então chama-se a rede acima de Rede de Jackson; caso contrário, tem-se uma Rede de Jackson generalizada (ou simplesmente uma OQN genérica). Redes de Jackson possuem soluções exatas na forma de produto (elegantes do ponto de vista matemático) demostradas por Jackson.

5.14.2) Resultados Observados

Os seguintes resultados foram observados:

- A rede congestionada aumenta o atraso dos pacotes e o consumo de energia devido à retransmissão dos pacotes perdidos; isso pode ser evitado com uma boa engenharia de tráfego;
- O uso de *links* e nós redundantes (ou de emergência) ajudam a desafogar a rede e evitar que esta fique congestionada;
- O atraso do pacote é fortemente dependente da topologia da rede; otimizações em topologia/roteamento normalmente implicam em diminuição de atraso;
- O primeiro nó congestionado transfere seus problemas para os nós subsequentes;
- A redução no consumo de energia na rede de telecom é possível com a redução de congestionamento, o que pode ser usada para a expansão do tempo de vida do sistema;
- O uso de mensagens priorizadas reduz fortemente o atraso de mensagens muito críticas de atuadores ou gerenciamento de rede, mesmo em situações de congestionamento;
- O uso da otimização de Monte Carlo no roteamento AdHoc é muito importante pois diminui o número de saltos dos pacotes e o consequente atraso do pacote, principalmente em redes VANET onde a mudança de posicionamento é muito grande e rápida; adicionalmente, é importante levar em consideração também a sobrecarga existente nos *gateways* das novas rotas;
- A otimização de roteamento usando Monte Carlo se mostrou eficiente para reduzir o atraso dos pacotes, diminuindo o número de saltos no caminho (*hop*); no entanto, não se mostrou eficiente em casos em que o novo caminho passe por um *Gateway* sobrecarregado; essa informação tem que ser considerada também para escolha das melhores rotas.

Capítulo 6: Conclusão

O desempenho de redes IoT é fortemente dependente da capacidade do mediador, tendo em vista ser um concentrador de dados/tráfego. Para especificar a sua capacidade, é necessário se efetuar simulações e análise de tráfego gerados pelas diversas tecnologias cobertas pelas redes IoT. Foi criado um modelo de simulação de Redes IoT, AdHoc e RFID, visando fazer esse estudo.

Nesta tese, 13 cenários foram estudados visando o dimensionamento da capacidade do mediador, considerando distintos tipos de tráfegos e a diversidade de dispositivos existentes em uma rede IoT. Para modelar o efeito da mobilidade do *mote (mobile)*, foi utilizado o algoritmo MATLAB do *Random Way Point,* complementando a simulação de modelo discreto (DES). Esse modelo captura diversas características de sistemas complexos, incluindo o mediador, *gateways*, nós de emergência, Internet e tráfego IoT, e o mais importante o tráfego gerado pelas Etiquetas RFID e Sensores. Foram analisados 13 cenários e casos de estudo, estudando o tempo médio de fila e a utilização da *CPU* de saída para cada *cluster* para uma dada probabilidade de conectividade dos *motes* (sensores) resultantes de sua mobilidade. Pelo modelo foi possível estimar o tráfego de entrada e saída para cada *cluster* e o mediador IoT, que foi o ponto focal e objetivo inicial desta tese.

O modelo proposto é **escalável**, significando que acomoda a inclusão de outros tipos e números de componentes, pelo uso do conceito de *clusters.* Desta forma, pode ser utilizado como uma ferramenta de dimensionamento de redes para diversos tipos de aplicações, inclusive o contexto de *SMART CITY*, Sistema de Transporte Inteligente ITS, *Smart Grid* (Redução de Consumo de Energia Elétrica na Rede e no Campus) e Recuperação/prevenção de Catástrofe. No caso real, as características de cada rede devem ser incorporadas no modelo de simulação; por exemplo, o tamanho do pacote e a velocidade do *link* podem ser considerados variáveis.

O modelo proposto é **flexível** pois permite essas adaptações. Utilizaram-se sensores GPS para VANET ITS e o Método de Monte Carlo para Otimização do Roteamento da Sub-rede Adhoc de Sensores. Foram utilizadas Lógicas Fuzzy e Algoritmo de Predição, para redução de energia em Campus Universitário.

A redução no consumo de energia em uma rede de telecomunicações é possível com a redução de congestionamento, e que pode ser usada para a expansão do tempo de vida dos dispositivos com baterias. Além do fato que a redução do tempo de comunicação em uma rede é essencial, principalmente no caso de catástrofes.

A tese deste trabalho foi de que:

> "*É possível modelar, simular, e avaliar o desempenho de um sistema IoT incluindo AdHoc e RFID, no que tange ao tráfego e à capacidade dos nós, considerando-se mobilidade, agrupamento, descentralização e escassez de recursos computacionais que caracterizam esses sistemas"*.

Considerando-se que:

- Os valores numéricos obtidos nas simulações para os parâmetros explicitados mantiveram-se dentro dos níveis aceitáveis (conhecimento de domínio);
- Estatisticamente, os valores apresentados mantêm sua coerência e dentro dos intervalos de confiança estabelecidos;
- Foram modelados os processos estocásticos de chegada e serviço bem como as disciplinas de atendimento;
- Os modelos de simulação foram validados por modelos analíticos conhecidos, permitindo a evolução para outras cargas de chegada e processamento;
- O modelo foi submetido a treze cenários distintos, contemplando as características da tese, e para os quais os resultados apresentaram-se dentro das expectativas;
- O modelo mostrou-se flexível e passível de extensões quanto ao tipo de aplicações e à escalabilidade de suas características,
- Itens contemplados no modelo:

    - Mobilidade Aleatória dos Nós: OK!
    - Clusterização (Agrupamento de Nós): OK!
    - Inexistência de Nós Centralizados na Rede AdHoc: OK!
    - Perdas de Conectividade (Baixa Potência de transmissão/propagação): OK!
    - Heterogeneidade do tráfego e dos nós: Sensor, Rede de Sensores, RFID, GPS: OK!
    - Poucos Recursos Operacionais nos Objetos (Bateria, *CPU*, Interfaces, Memória): OK !
    - Modos de Operação: Emergência, Congestionado, Não Congestionado, etc : OK !.
    - Pontos chaves analisados: Atrasos nas *CPUs* (*Mean Queue Time*) e Utilização de *CPU :* OK!

Conclui-se então que:

"**É possível modelar, simular, e avaliar o desempenho de um sistema IoT incluindo AdHoc e RFID, no que tange ao tráfego e à capacidade dos nós, considerando-se mobilidade, agrupamento, descentralização e escassez de recursos computacionais que caracterizam estes sistemas". Conclui-se acerca da viabilidade da tese** proposta dentro do escopo de trabalho definido.

Adicionalmente, esta tese trouxe à tona e considerou aspectos relevantes para a simulação de redes, com caráter social: Redes para Catástrofes (Emergência) por meio das quais muitas vidas podem ser salvas, Redes de Sustentabilidade (Economia de Energia Elétrica), e Segurança Veicular em Rodovias (ITS).

6.1) Limitações

As entradas foram simuladas usando distribuições estatísticas exponenciais. Com a validação analítica do modelo, usando Rede de Jackson, é possível a extensão para a utilização de outras distribuições estatísticas, de maneira bastante simples.

Nas primeiras rodadas foi observado esgotamento de memória devido à taxa de entrada ser maior que a taxa de serviço. Essa limitação teve que ser resolvida descobrindo-se a fila com congestionamento e aumentando-se sua taxa de serviço, como se fosse o incremento de processadores.

6.2) Dificuldades Encontradas

Esta tese encontrou os seguintes desafios de pesquisa:

- Integração de tecnologias muito diferentes: etiquetas, leitores, sensores, atuadores, mediadores, *gateways*, computadores, redes e servidores em *Data-Center* (Nuvem);
- Limitação das "coisas": energia, computação, memória, tamanho e comunicação;
- Necessidade de se acrescentar inteligência às "coisas" por meio de equipamentos leitores, interfaces, mediadores e *gateways*;
- Migrar da padronização abstrata para o mundo real;
- Necessidade de endereçamento único (IPv6);
- Detecção e otimização dos pontos críticos da rede;
- Utilização de simulação hibrida por eventos discretos e mobilidade (*Random Way Point* e *Two-Ray Propagation Model*);
- Integração de modelos e ferramentas DES, MATLAB e VISUAL BASIC;
- Utilização de Lógicas Fuzzy;
- Utilização de Algoritmo de Predição;
- Utilização do Modelo Analítico de Validação de Jackson;
- Utilização do Método de Otimização de Monte Carlo.

Esta tese identificou os elementos críticos na comunicação na IoT, mostrando maneiras de otimização visando reduzir suas limitações. Ajudará a simular alguns modelos de redes que poderão gerar futuras aplicações IoT, usando Etiquetas RFID e Sensores de entrada.

6.3) Contribuições

Esta tese contribuiu nos seguintes aspectos de pesquisa:

1) Apresentou uma publicação com Pesquisa Bibliográfica "IoT+RFID" para o ambiente acadêmico [P1];

2) Apresentou 3 publicações com Referencial Teórico (*Overview*) das Redes IoT, AdHoc e RFID: Padronização, Arquiteturas, Modelos, Tecnologias, Protocolos, Aplicações, Segurança e Gerenciamento de Rede. Esse material está sendo usado em curso de graduação e pós-graduação da FT [P1] [P4] [P8] [P16];
3) Desenvolvimento inovador de um Modelo de Rede Simulado IoT com aplicações típicas que servirão como orientação para novas pesquisas; oferece um Modelo de Simulação por Eventos Discretos (DES) da Rede, analiticamente validado pelo modelo matemático de Redes de Jackson, que inclui Redes IoT e AdHoc combinadas, envolvendo RFIDs, Sensores e GPS.
4) Integração de tecnologias diferentes;
5) O modelo também possibilita a **avaliação de mobilidade** por meio do SW *Random Way Point* (RWP) e os modelos de propagação *Two-Ray* (ou *Free Space*), de Redes AdHoc; Integração da Simulação continua com a discreta, via VISUAL BASIC;
6) Possibilita a **otimização do Roteamento das Redes AdHoc VANET**, por meio do uso do SW MATLAB com otimização de **Monte Carlo**;
7) Possibilita a configuração/utilização de funções de prioridades de mensagens, controle de congestionamento de tráfego, controle Fuzzy/Lógicas de Predição através de Interface VISUAL BASIC criada; Integração de Modelos feitos em diversas Ferramentas DES, MATLAB e VISUAL BASIC (Fuzzy e Predição com o preditor KSLX);
8) O modelo pode ser usado ou aplicado para diversos cenários: Economia de Energia, Sistemas de Transporte Inteligente (*Smart City*/ITS/VANET), Ambientes de Catástrofe com uso de redundâncias em *links*/nós/acessos Internets, Gerenciamento de Rede;
9) Execução de 13 cenários e casos de estudo, mostrando os resultados positivos em sua utilização; **Abstração das Camadas Física e de Enlace;** Migração da padronização abstrata para o mundo real. Aproveitamento do conhecimento AdHoc adquirido para utilizá-lo na Nova Rede Celular 5G D2D;
10) O uso desse tipo de *approach* (simulação, priorização, Controles Fuzzy e Predição) permite um caminho rápido de obter resultados qualitativos na redução do consumo de energia, do congestionamento de tráfego e atraso na rede; integração de sistemas muitos diferentes e distantes;
11) O modelo de rede possui uma estrutura flexível e pode ser usado para **projeto, planejamento e dimensionamento de novas redes; pode ser usado também para descobrir gargalos em redes existentes**, auxiliando na tomada de decisão de evolução da rede (ou em Engenharia de Tráfego); pode ser usado no estudo de desempenho de sistemas de tempo real dinâmicos.

6.4) Trabalhos Futuros

Nos trabalhos futuros, pode-se incrementar o modelo com:

- Algoritmos de Inteligência Artificial (Redes Neurais) auxiliando a IoT;
- Criar um modelo de predição crescente de tráfego que vai permitir uma estimativa mais precisa da capacidade disponível na rede que pode ser considerada no projeto do mediador;
- O modelo de mobilidade utilizado assume baixa mobilidade e baixa velocidade para MANET;
- O modelo VANET possibilitou o uso de alta mobilidade e alta velocidade para os automóveis em rodovias; mesmo assim, pode-se ampliá-lo com o uso do Modelo *Manhattan* para *Smart Cities* ao invés do RWP;

- Pode-se expandir o modelo VANET para o uso de Rede FANET (*Flying Ad- Hoc Network*) para *drones*;
- Utilização de controlador centralizado com as probabilidades de distribuição dos pacotes *nos links* entre *clusters*;
- A partir do Modelo Validado, utilização de outros tipos de distribuições, diferentes da Exponencial;
- Escalonamento do número de *Clusters*, número de *motes* nos *clusters* e número de sub-redes RFIDs e AdHocs;
- Desenvolvimento de novas aplicações, incluindo aplicações em nuvem (*cloud e fog*);
- Desenvolvimento de novos mediadores, sensores e atuadores; exemplo: sensor com fibra ótica;
- Desenvolvimento das funcionalidades de Segurança da Informação na IoT;
- Desenvolvimento adicionais das funcionalidades de gerenciamento da rede IoT;
- Interligação de novos sensores e atuadores;
- Criação de serviço de monitoração remota de informações para: Pacientes (*Mobile Health*), Baterias, Infraestrutura e Ferramentas insalubres (exemplo, barulho pela utilização de Britadeira);
- Extensão do cenário para outras aplicações, tipo *Healthcare*;
- Otimização de Roteamento considerando Quantidade de Energia nas Baterias dos Nós;
- Lógica Fuzzy para Roteamento Dinâmico monitorando as taxas de pacotes chegando no mediador e os pacotes vindo das sub-redes AdHoc.

6.5) Lista de Artigos Publicados e Apresentações em Conferências

O Apêndice A apresenta os 17 artigos ([P1] a [P17]) publicados (Conferências e Capítulos de Livros) e apresentados em conferências, com seus "*links* de leitura" para o *Research Gate* e respectivos Números de Leituras até a data de 18/agosto/2019.

Total de Artigos Publicados: 17;
Total de Leituras no *Research Gate* (até 18/agosto/2019): 2.171.

O Apêndice B apresenta as atividades desenvolvidas durante a tese.

Referências Bibliográficas:

[1] Implementando RFID na Cadeia de Negócios (Tecnologia a serviço da Excelência) Fabiano Hessel, Reinaldo Villar, Renata Rampim, Suely Baladei, *PUCRS 2011*.

[2] Enabling Things to Talk
Alessandro Bassi, Martin Bauer, Martin Fiedler,Thorsten Kramp, Rob van Kranenburg, Sebastian Lange, Stefan Meissner; IoT-A, *Spring Open, Elsevier 2013*.

[3] Interconnecting Smart Objects with IP: The Next INTERNET
Jean-Philippe Vasseus, Adam Dunkels; *Cisco; Elsevier 2010*.

[4] Essential SNMP
Douglas R.Mauro, Kevin J.Schmidt; *O'Relly 2005*.

[5] Sensor Technologies: Healthcare, Wellness and Environmental Applications
Michael J.McGrath; Cliodhna Ni Scanaill; *Intel Labs Europe; Apress Open 2013*

[6] Arquitetura para Interconexão de Redes de Sensores sem fio e a Internet através de WEB Services e o Protocolo HTTP; Daniel Adorno Gomes; David Bianchini; *PUC Campinas 2015.*

[7] Internet of Things: A Review;
Manveer Joshi; Bikram Pal Kaur;
2015 International Journal of Science Technology & Management;

[8] Smart Networked Objects & Internet of Things;
Instituts CARNOT; 2010 Association Instituts CARNOT.

[9] Internet of Things Strategic Research Roadmap;
Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harisson, Markus Eisenhauer, Pat Doody; *2009 IERC - European Research Cluster of IoT.*

[10] Internet of Things (IoT): A Vision, Architectural elements and future directions;
Jaavardhana Gubbi, Rajkumar Bua, Slaven Marusic, Marimuthu Palaniswami;
2013 Future Generation Computer Systems.

[11] Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. Ala Al-Fuqaha; Mohsen Guizani; Mehdi Mohammadi; Mohammed Aledhari; Moussa Ayyash;
IEEE Communications Surveys & Tutorials (Volume: 17, Issue: 4, Fourthquarter 2015). IEEE2015

[12] How can we Trackle energy Efficiency in IoT Based Smart Buildings?
M.Victoria Moreno, Benedito Ubeda, Antonio F. Sharmeta, Miguel A. Zamora;
Sensors 2014.

[13] Monitoramento Ambiental através de Redes de Sensores Sem Fio de Baixo Custo;
Marcel Salvioni da Silva; Fabiano Fruett;
XVI Simpósio Brasileiro de Sensoriamento Remoto 2013.

[14] The Research of IOT Based on RFID Technology; Kubo; *Intelligent Computation Technology and Automation (ICITA) 7 th International Conference on; 2014.*

[15] Internet of Things in Industries: A Survey
Li Da Xu, Wu He, Shancang Li; *IEEE Transactions on Industrial Informatics 2014*.

[16] Internet of Things for Enterprise systems of Modern Manufacturing;
Zhuming Bi, Li da Xu, Cheng Wang; *IEEE Transactions on Industrial Informatics 2014*.

[17] Smart Objects as Building Blocks for the Internet of things;
Gerard Kortuem; Daniel Fitton; Vasughi Sundramoorthy;
2010 IEEE Internet Computing.

[18] Infrastructural health monitoring using self-powered Internet-of-Things
Kenji Aono; Nizar Lajnef; Fred Faridazar; Shantanu Chakrabartty
Circuits and Systems (ISCAS), *2016 IEEE International Symposium on; IEEE 2016*.

[19] The Internet of Things in Healthcare: Potential Applications and Challenges.
Phillip A.Laplante; Nancy Laplante; *IEEE IT Pro May/June 2016.*

[20] An IoT Framework for Healthcare Monitoring Systems;
Dharmendra Singh Raiput; Rakesh Gour;
2016 International Journal of Computer Science and Information Security;

[21] A Methodology for Proactive Maintenance of Uninterruptible Power Supplies;
Slobodan Lukovic;Igor Kaitovic; Miroslaw Malek; Gerardo Lecuona;
Artigo enviado para Aprovação do IEEE.

[22] Sensor Networks or Smart Artifacts? An Exploration of Organizational Issues of An Industrial Health and Safety Monitoring System;
Gerd Kourtuem; David Alford; Linden Ball; Jerry Busby; Nigel Davies; Christos Efstratiou; Joe Finney; Marian Iszatt White; Katharina Kinder;
Ubicomp 2007: Ubiquitous Computing – Springer.

[23] RFID Technology for IoT-Based Personal Healthcare in Smart Spaces
Sara Amendola; Rossella Lodato; Sabina Manzari; Cecilia Occhiuzzi; Gaetano Marrocco;
IEEE Internet of Things Journal (Volume: 1, Issue: 2, April 2014); IEEE 2014.

[24] An IoT-Aware Architecture for Smart Healthcare Systems;
Luca Catarinucci; Danilo de Donno; Luca Mainetti; Luca Palano; Luigi Patrono; Maria Laura Stefanizzi; Luciano Tarricone
IEEE Internet of Things Journal (Volume: 2, Issue: 6, Dec. 2015); IEEE 2015.

[25] A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box;
Geng Yang; Li Xie; Matti Mäntysalo; Xiaolin Zhou; Zhibo Pang; Li Da Xu; Sharon Kao-Walter; Qiang Chen; Li-Rong Zheng;
IEEE Transactions on Industrial Informatics (Volume: 10, Issue: 4, Nov. 2014); IEEE 2014.

[26] Internet of Things and Smart Objects for M-Health Monitoring and Control;
Santos A Macedo J Costa A Nicolau M;
Procedia Technology 2014 vol: 16 (16) pp: 1351-1360; ELSEVIER 2014.

[27] Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring;
M. Shamim Hossain G;
Computer Networks, Volume 101, 4 June 2016, Pages 192-202.

[28] An integrated remote monitoring platform towards Telehealth and Telecare services interoperability; G.C. Lamprinakos, S. Asanin, T. Broden, A. Prestileo, J. Fursse, K.A. Papadopoulos, D.I. Kaklamani I; *Information Sciences*, Volume 308, 1 July 2015, Pages 23-37;

[29] Simulation of a Smart Grid City with Software Agents;
Stamatis Karnouskos, Thiago Nass de Holanda;
EMS'09 Proceedings of the 2009 Third UKSIN European Symposium on Computer Modeling and Simulation.

[30] Integrated environment for testing IoT and RFID technologies applied on intelligent transportation system in Brazilian scenarios;
Adriano Galindo Leal; Alessandro Santiago; Mario Y. Miyake; Mauro K.Noda; Matheus J.Pereira; Leandro Avanço; *2014 IEEE Brasil RFID*.

[31] Some Comments on Hourglasses;
Rui L Aguiar; *ACM SIGCOMM Computer Communication Review 2008*.

[32] Content Centric Services in Smart Cities;
I.Cianci, G.Piro, L.A.Grieco, G.Boggia, P.Camarda;
2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies.

[33] Named Data Networking for IoT: An Architectural Perspective;
Marica Amadeo, Claudia Campolo, Antonio Iera, Antonella Molinaro;
2014 European Conference on Networks and Communications.

[34] Towards an Information-Centric Internet with more Thigs;
Dirk Kustscher, Stephen Farrel; *2011 IoT Worshop*.

[35] SNMP Proxy CCN: Uma proposta de arquitetura para gerência de redes orientadas a conteúdo interoperável com sistemas legados;
Marciel de Lima Oliveira, Christian Esteve Rothenberg;
SBRC 2014.

[36] A secure IoT management architecture based on Information-Centric Networking;
Javier Suarez, Jose Quevedo, Ivan Vidal, Daniel Corujo, Jaime Garcia-Reinoso R;
Journal of Network and Computer Applications Volume 63, March 2016, Pages 190–204; ELSEVIER 2016.

[37] Optimizations for RFID-based IoT applications on the cloud;
Hoang Minh Nguyen; Seong Hoon Kim; Dinh Tuan Le; Sehyeon Heo; Janggwan Im; Daeyoung Kim; *Internet of things (IoT), 2015 5 th International Conference on the.*

[38] Secure authentication scheme for IoT and cloud servers;
Sheetal Kalra S; *Pervasive and Mobile Computing* Volume 24, December 2015, Pages 210–223 Special Issue on Secure Ubiquitous Computing; ELSEVIER 2015.

[39] State-of-art, challenges, and open issues in the integration of internet of things and cloud Computing.Manuel Diaz, Cristian Martin, Bartolomé Rubi. *Journal of Network and Computer Applications* (2016) 99-117

[40] A fuzzy k-coverage approach for RFID network planning using plant growth simulation algorithm;
Shilei Lu, Shunzheng Yu; *Journal of Network and Computer Applications* Volume 39, March 2014, Pages 280–291. ELSEVIER 2014.

[41] Management and Internet of Things; Samaniego M Deters R;
Procedia Computer Science 2016 vol: 94 pp: 137-143; ELSEVIER 2016.

[42] Integration framework for simulations and SCADA systems;
Petr Novák, Radek Šindelář R;
Simulation Modelling Practice and Theory, Volume 47, September 2014, Pages 121-140;

[43] A RFID QoS mechanism for IoT tracking applications;
Rafael Perazzo Barbosa Mota; Daniel M. Batista;
Wireless and Pervasive Computing (ISWPC), 2013 International Symposium on; IEEE 2013.

[44] Internet of things network management system architecture for smart healthcare;
Farag Sallabi; Khaled Shuaib;

Digital Information and Communication Technology and its Applications (DICTAP), *2016 Sixth International Conference on; IEEE 2016;*

[45] Provided security measures of enabling technologies in Internet of Things (IoT): A Survey; Minela Grabovica; Srđan Popić; Dražen Pezer; Vladimir Knežević; *Zooming Innovation in Consumer Electronics International Conference (ZINC), 2016; IEEEE 2016*.

[46] Security architecture for mobile e-health applications in medication control; Fabio Gonçalves; Joaquim Macedo; M. João Nicolau; Alexandre Santos; *Software, Telecommunications and Computer Networks (SoftCOM), 2013 21st International Conference on; IEEE 2013*.

[47] A Middleware of Internet of Things (IoT) based on Zigbee and RFID; Chunxiao Fan, Zhigang Wen. Fan Wang; Yuexin Wu; *IEEE Proceedings of ICCTA 2011*.

[48] Energy Efficient and Quality-Driven Continuous Sensor Management for Mobile IoT Applications;
Lea Skorin-Kapov, Kresimir Pripuzic, Martina Marjanovie, Aleksandar Anotine, Ivana Podnar Zarko;
Simulação de Gerenciamento de Sensores para Aplicações Móveis de IoT 2014.

[49] Application-Driven OAM Framework for Heterogeneous IoT Environments; Janez Sterle, Urban Sedlar, Miha Rugeli, andrej Kos, Mojca Volk;
2015 International Journal of Distributed Sensor Networks.

[50] Middleware for Internet of Things: A Survey;
Mohammad Abdur Razzaque; Marija Milojevic-Jevric; Andrei Palade; Siobhán Clarke;
IEEE Internet of Things Journal (Volume: 3, Issue: 1, Feb. 2016); IEEE 2016.

[51] Energy Efficient and Quality-Driven Continuous Sensor Mangement for Mobile IoT Applications.
Lea Skorin-Kapov, Kresimir Pripuzie, Martina Marjanovic, Aleksandar Antonie, Ivana Podnar Zarko. *IEEE 2014*

[52] Middleware to integrate mobile devices, sensors and cloud computing; Vinh T Bouzefrane S Farinone J Attar A Kennedy B; *Procedia Computer Science 2015*.

[53] A middleware for industry; Djamel F.H. Sadok, Lucas L. Gomes, Markus Eisenhauer J;
Computers in Industry, Volume 71, August 2015, Pages 58-76;

[54] Modelling and Simulation of Energy Efficient Enhancements for IEEE802.15.4.e DSME;
Silvia Capone, Fábio Ricciato, Genaro Boggin, Angelo Malvani;
2014 Wireless Telecommunication Symposium.

[55] Wireless Sensor Networks: a Survey;
I.E.Akyildiz, W.Su, Y.Sankaraubramaniam;
2001 Computer Networks;

[56] Metodologia de Modelos Analíticos e de Simulação para o Dimensionamento de Redes de Dados
Edson Luiz Ursini; Michael Soares da Silva Fonseca. *Projeto de Pesquisa PIBITI 013; UNICAMP*.

[57] Integração da Internet das Coisas (IoT) com a RFID e Redes de Sensores: Revisão da Literatura. José Roberto Emiliano Leite; Edson Luiz Ursini; Paulo S. Martins. *Brazilian Technology Symposium (BTSym 2016) e Sexto Workshop Smart Grid Energia:* 1 e 2/dezembro/2016; UNICAMP.

[58] O Modelo de Referência para a Interconexão de Sistemas Abertos. José Roberto Emiliano Leite; *Revista Telebrás*; junho/1985.

[59] A Camada de Aplicação do Modelo de Referência para a Interconexão de Sistemas Abertos. José Roberto Emiliano Leite; Revista Telebrás; março/1990.

[60] La Capa de Aplicacion del Modelo de Referência para la Interconexion de Sistemas Abiertos. José Roberto Emiliano Leite; *Revista Telebrás*; marzo/1990.

[61] Interconexão de Sistemas Computacionais Abertos em Redes Locais de Automação Industrial e de Escritórios. José Roberto Emiliano Leite; Manuel de Jesus Mendes; Luis Roberto Ferreira; *Revista Telebrás*; junho/1987.

[62] Recomendações Série Y.4000/Y.2060 : Overview of the Internet of things. *ITU-T Genebra 2016*. Obs. Standards prepared on a collaborative basis with ISO and IEC;

[63] Security Mechanisms in IoT. Ivan Tot; Dusan Bogicevic; Komlen Lalovic; Miodrag Brzakovic; Ivana Ognjanovic; *The 9th International Conference on Business Information Security (BISEC-2017*, 18th October 2017, Belgrade, Serbia.

[64] The Internet of Things (IoT); *International Digital Asset Management (IDA);* July 2012;

[65] Interconexão de Sistemas Computacionais Abertos em Automação Industrial; *Revista SBA: Controle e Automação (Sociedade Brasileira de Automação*); Janeiro/1997;

Apêndice A - Lista de Artigos Publicados e Apresentados

A seguir mostram-se os 17 artigos ([P1] a [P17]) publicados (Conferências e Capítulos de Livros) e apresentados em conferências, com seus "*LINKs* DE LEITURA" para o *Research Gate* e respectivos Números de Leituras até a data de 18/agosto/2019.

Total de Artigos Publicados: 17
Total de Leituras no *Research Gate* (até 18/agosto/2019): 2.171

[P1] Integration of RFID and IoT/WSNs: A Bibliographic Review
José Roberto Emiliano Leite, Edson L. Ursini, Paulo Martins
***BTSYM 2016 Campinas BRASIL (*Apresentado: *BTSYM'16 Brazilian Techbology Symposium; Dezembro/2016).* Obs : Artigo com 864 LEITURAS no *ResearchGate* em 18/agosto/2019;**
https://www.researchgate.net/publication/311403383_Integration_of_RFID_and_IoTWSNs_A_Bibliographic_Review

[P2] Performance Analysis of a Multi-Mode AdHoc Wireless Network via Hybrid Simulation
J.R. Emiliano Leite, Edson L. Ursini, Paulo S. Martins
SBrT 2017 São Pedro BRASIL (*Apresentado: *XXXV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais; Setembro/2017);
https://www.researchgate.net/publication/319403532_Performance_Analysis_of_a_Multi-Mode_AdHoc_Wireless_Network_via_Hybrid_Simulation

[P3] Simulation of AdHoc Networks Including Clustering and Mobility
J. R. Emiliano Leite, Edson L. Ursini, Paulo S. Martins
ADHOC-NOW 2017 MESSINA ITÁLIA (*Apresentado: *16th International Conference on Ad Hoc Networks and Wireless; Outubro/2017); LIVRO SPRINGER; Confêrência com classificação Webqualis CAPES Periódicos 2013-2016 " B1" com proceedings equivalente a publicação de REVISTA (ISSN 0302-9743) revista "Lecture Notes in Computer Science";
https://www.researchgate.net/publication/319402094_Simulation_of_AdHoc_Networks_Including_Clustering_and_Mobility

[P4] A INTERNET das COISAS (IoT) : Tecnologias e Aplicações
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
***BTSYM 2017 # 1 Campinas BRASIL (*Apresentado: *BTSYM'17 Brazilian Techbology Symposium; (ISSN 2447-8326); Dezembro/2017).* Obs : Artigo com 336 LEITURAS no *ResearchGate* em 18/agosto/2019;**
https://www.researchgate.net/publication/325807577_A_INTERNET_das_COISAS_IoT_Tecnologias_e_Aplicacoes_ISSN_2447-8326

[P5] A Proposal for Performance Analysis and Dimensioning of IoT Networks
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
BTSYM 2017 # 2 Campinas BRASIL (*Apresentado: *BTSYM'17 Brazilian Techbology Symposium; (ISSN 2447-8326); Dezembro/2017);

https://www.researchgate.net/publication/326489209_A_Proposal_for_Performance_Analysis_and_Dimensioning_of_IoT_Networks

[P6] Performance Analysis of IoT Networks with Mobility via Modeling and Simulation.
José Roberto Emiliano Leite, Edson L. Ursini, Paulo Martins
SUMMER SIM SPECTS 2018 BORDEAUX FRANÇA (*Apresentado: *SUMMERSIM 2018 – SPECTS 2018 International Symposium on Performance Evaluation of Computer and Telecommunication Systems; Junho/2018);
https://www.researchgate.net/publication/326560399_Performance_Analysis_of_IoT_Networks_with_Mobility_via_Modeling_and_Simulation

[P7] Evaluation of Traffic Delays and Utilization of IoT Networks considering Mobility
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
LIVRO SPRINGER 2019 # 1 (*Publicado: *Proceedings of the 3rd Brazilian Technology Symposium – Emerging Trends and Challenges in Technology; Maio/2019);
https://www.researchgate.net/publication/327042050_Evaluation_of_Traffic_Delays_and_Utilization_of_IoT_Networks_Considering_Mobility_Emerging_Trends_and_Challenges_in_Technology

[P8] Internet of Things : An Overview of Architecture, Models, Technologies, Protocols and Applications
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
***LIVRO SPRINGER 2019 # 2 (*Publicado: *Proceedings of the 3rd Brazilian Technology Symposium – Emerging Trends and Challenges in Technology; Maio/2019).* Obs : Artigo com 366 LEITURAS no *ResearchGate* em 18/agosto/2019;**
https://www.researchgate.net/publication/327042049_Internet_of_Things_An_Overview_of_Architecture_Models_Technologies_Protocols_and_Applications_Emerging_Trends_and_Challenges_in_Technology

[P9] Evaluating the Impact of Congestion Reduction on Power Consumption in IoT Networks
J R Emiliano Leite, Edson L Ursini, Paulo S Martins
SBrT 2018 Campina Grande BRASIL (*Apresentado: *XXXVI Simpósio Brasileiro de Telecomunicações e Processamento de Sinais; Setembro/2018);
https://www.researchgate.net/publication/325934667_Evaluating_the_Impact_of_Congestion_Reduction_on_Power_Consumption_in_IoT_Networks

[P10] Analysis of an Adhoc Network in an Intelligent Transportation System
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
IEEE IEMCON 2018 VANCOUVER CANADÁ (*Apresentado*: The 9th IEEE Annual Information Technology, Electronics and Mobile Communication Conference 2018; Novembro/2018);
https://www.researchgate.net/publication/327468356_Analysis_of_an_AdHoc_Network_in_an_Intelligent_Transportation_System

[P11] Reducing Power Consumption in Smart Campus Network Applications through simulation of high-priority service, Traffic Balancing, Prediction and Fuzzy Logic
J.R.Emiliano Leite, F.R.Massaro, Paulo S.Martins, Edson L.Ursini
WSC 2018 GOTEMBURGO SUÉCIA (*Apresentado: *Winter Simulation Conference 2018; Dezembro/2018); CONFERÊNCIA COM CATEGORIA "A2" CAPES;

https://www.researchgate.net/publication/326960199_REDUCING_POWER_CONSUMPTION_IN_SMART_CAMPUS_NETWORK_APPLICATIONS_THROUGH_SIMULATION_OF_HIGH-
PRIORITY_SERVICE_TRAFFIC_BALANCING_PREDICTION_AND_FUZZY_LOGIC

[P12] Validation of a Discrete Event IoT Simulation Model
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
RESEARCH GATE (*Publicado: *Research Gate; Junho/2018);
https://www.researchgate.net/publication/326410652_Validation_of_a_Discrete_Event_IoT_Simulation_Model

[P13] Tecnologias de Telecomunicações e Simulação Computacional por Eventos Discretos, para a Redução de Risco de Mortes em Desastres Ambientais
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
UNESP: WORKSHOP SOBRE CIÊNCIAS MATEMÁTICAS E REDUÇÃO DO RISCO DE DESASTRES (Apresentado em 6/Junho/2019; São José dos Campos); ORGANIZAÇÃO UNESP, INPE E CEMADEN;
https://www.researchgate.net/publication/334638371_Tecnologias_de_Telecomunicacoes_e_Simulacao_Matematica_Computacional_por_Eventos_Discretos_para_a_Reducao_de_Risco_de_Mortes_em_Desastres_Ambientais_Workshop_sobre_Ciencias_Matematicas_e_Reducao_do_Risco de Desastres

[P14] Dimensioning of IoT Networks: an Incremental Validation Approach
J.R.Emiliano Leite, E.L.Ursini, P.S.Martins
Apresentado no ADHOCNOW 2019 LUXEMBURGO (Outubro/2019); CONFERÊNCIA COM CATEGORIA "B1" CAPES;
https://www.researchgate.net/publication/334612908_A_Validation_Method_for_AdHoc_Networks_Including_MANETs_VANETs_and_Emergency_Scenarios

[P15] Planning of AdHoc and IoT Networks under Emergency Mode of Operation
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
Apresentado no IEEE IEMCON 19 VANCOUVER (17 a 19/Outubro/2019) e no SENSOR JOURNAL; Prêmio Recebido de BEST PRESENTER.
https://www.researchgate.net/publication/336370333_Planning_of_AdHoc_and_IoT_Networks_Under_Emergency_Mode_of_Operation

[P16] Segurança e Gerenciamento da Rede IoT
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
Apresentado no BTSYM 2019 CAMPINAS (Outubro/2019);
https://www.researchgate.net/publication/336903352_Seguranca_e_Gerenciamento_da_Rede_IoT

[P17] Increasing Fault Tolerance in IoT and AdHoc Networks for Risk Reduction in Disaster Recovery
J R Emiliano Leite, Paulo S Martins, Edson L Ursini
Apresentado no WSC (WINTER SIMULATION CONFERENCE – PHD Colloquium) MARYLAND (8 a 11/Dezembro/2019); CONFERÊNCIA COM CATEGORIA "A2" CAPES;

https://www.researchgate.net/publication/336903415_INCREASING_FAULT_TOLERANCE_IN_IOT_AND_ADHOC_NETWORKS_FOR_RISK_REDUCTION_IN_DISASTER_RECOVERY_MODE

OBS: OUTROS ARTIGOS RELACIONADOS À TESE, PUBLICADOS ANTES DA TESE:
a) **O Modelo OSI da ISO** (*Revista TELEBRÁS Junho/1985*) [58]
b) **A Camada de Aplicação do Modelo de Referência para a Interconexão de Sistemas Abertos** (*Revista TELEBRÁS Março/1990*) [59]
c) **La Capa de Aplicacion del Modelo de Referência para la Interconexion de Sistemas Abiertos** (*Revista TELEBRÁS Marzo/1990*) [60]
d) **Interconexão de Sistemas Computacionais Abertos em Redes Locais de Automação Industrial e de Escritórios** (*Revista TELEBRÁS Junho/1987*) [61]
e) **Interconexão de Sistemas Computacionais Abertos em Automação Industrial** (*Revista SBA: Controle e Automação (Sociedade Brasileira de Automação; Janeiro/1987*); co-autoria Manuel de Jesus Mendes (FEEC UNICAMP) [65].

Apêndice B: Atividades Desenvolvidas

Este apêndice apresenta o cronograma executado na tese com suas atividades (Anos 2017, 2018 e 2019) na Figura 37.

ATIVIDADES/MES	F	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O	N	D
A : Créditos e Exame de Proficiência Inglês	F	I	N	A	L	I	Z	A	D	O	S												
B : Exame de Qualificação																							
C : Análise Crítica do Material Bibliográfico																							
D : Desenvolvimento do Ambiente Simulado																							
E : Inclusão e testes do Módulo Fuzzy																							
F : Inclusão e testes do Módulo de Predição																							
G : Conclusão do Modelo Dinâmico																							
H : +13 Artigos Publicados																							
I : Escrita da Tese																							

Figura 37: Cronograma de Desenvolvimento da Tese. OBS: Novos artigos publicados em 2019.

Adicionalmente a esta tese, foram feitas as seguintes **atividades acadêmicas**:

1) Participação em 6 ***PEDs (Programas de Estágio Docente) da FT*** em Redes de Telecomunicações e Instalações Elétrica Predial (1S2015, 2S2015, 1S2016, 2S2016, 1S2017, 1S2018);
2) Criação e Manutenção do Grupo Facebook: ***Grupo IoT UNICAMP e PUCC;***
3) Criação e Participação do ***"Grupo Pesquisa e Ação em Conflitos, Riscos e Impactos Associados a Barragens (CRIAB_UNICAMP)",*** com foco em Tecnologias e Aplicações de Redes de Telecomunicações para Catástrofes Ambientais, Redes de Sensores AdHoc, Redes de Sensores ZigBee e Redes IoT. Escrita do Capítulo "IoT" do Livro CRIAB da UNICAMP;
4) Criação da EMENTA de ***Curso de Extensão UNICAMP de INTERNET DAS COISAS*** (2017);
5) Coeficiente de Rendimento (de 0 a 4) das Disciplinas Cursadas: 3.7037;
6) Utilização dos Artigos Publicados nas matérias de graduação e pós-graduação da FT UNICAMP;
7) Passagem do Modelo de Rede simulado para novos alunos da pós-graduação;
8) Prêmio de *BEST PRESENTER* recebido no IEMCON 2019 (IEEE e UBC, Vancouver/CA, 19/10/2019);
9) Convite recebido para que a publicação ITS [P10] participe na Revista Sensor.