UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE COMPUTAÇÃO

Um Algoritmo Anticolisão para RFID de Larga Escala em Ambientes Ruidosos

Israel Eduardo de Barros Filho

Orientador: Prof. Dr. Ivanovitch Medeiros Dantas da Silva

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Computação da UFRN (área de concentração: Telecomunicações) como parte dos requisitos para obtenção do título de Doutor em Ciências.

Número de ordem PPgEEC: D284
Natal, RN, Novembro de 2020

Divisão de Serviços Técnicos
Catalogação da Publicação na Fonte. UFRN - Biblioteca Central Zila Mamede

Barros Filho, Israel Eduardo de.
Um algoritmo anticolisão para RFID de larga escala em ambientes ruidosos / Israel Eduardo de Barros Filho. - 2020.
91f.: il.

Tese (Doutorado) - Universidade Federal do Rio Grande do Norte, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia Elétrica e de Computação. Natal, RN, 2020.
Orientador: Prof. Dr. Ivanovitch Medeiros Dantas da Silva.

1. IoT industrial - Tese. 2. GSPN - Tese. 3. RFID- Tese. 4- Modelagem de Erro - Tese. I. Silva, Ivanovitch Medeiros Dantas da. II. Título.

RN/UF/BCZM CDU 621.3

A minha esposa e companheira de todas as horas, Terezinha Barros, que sempre me apoiou. E também ao meu filho, Miguel, que teve que suportar minha ausência em diversos momentos, para que este trabalho pudesse ser realizado.

Agradecimentos

Ao Prof. e orientador Dr. Ivanovitch Medeiros Dantas da Silva, o meu sincero agradecimento pela valiosa orientação, confiança e amizade e, antes de tudo, por ter acreditado neste trabalho e ter me ajudado a realizar um sonho, que faz parte do meu projeto de vida.

Aos meus pais, Israel e Miriam, meu profundo agradecimento.

À minha esposa e companheira Terezinha Barros, meu eterno agradecimento por acumular muitas das minhas responsabilidades com o nosso filho durante esses últimos tempos e por compreender todos os meus momentos e dificuldades. Seu valioso e incansável apoio foi definitivo em todos os momentos deste trabalho.

Ao meu filho Miguel, agradeço as demostrações de afeto ao requisitar minha presença, que ainda não tem idade para entender o que é uma tese, agradeço pela espontaneidade, carinho e amor incondicional que sempre me estimularam nos momentos difíceis.

Aos amigos Thales Lima e Rodrigo Ramos, pela amizade e disponibilidade em ajudar a compreender o uso do software.

À minhas irmãs Prissila e Mikarla pelo apoio em continuar seguindo com este trabalho.

Aos meus colegas e familiares que de forma direta ou indireta contribuíram para a realização deste trabalho.

Resumo

A Internet das Coisas Industrial (IIoT) é frequentemente apresentada como um conceito que está mudando significativamente o cenário tecnológico das indústrias, através de procedimentos de automação e identificação de objetos relevantes. Para tanto, problemas de confiabilidade e desempenho devem ser considerados ao se fornecerem os serviços de comunicação previstos. Ao empregar a Identificação por Radiofrequência (RFID) no contexto da IIoT, diversas pesquisas anteriores atuaram para melhorar a eficiência dos seus sistemas de comunicação, geralmente definindo modelos matemáticos para o planejamento e a avaliação da qualidade. No entanto, tais modelos são projetados com base em comunicações livres de erros, o que de fato é irreal quando se considera a natureza propensa às falhas das comunicações sem fio em plantas industriais. Portanto, esta tese propõe um novo algoritmo anticolisão para RFID, juntamente com um modelo formal baseado em Redes de Petri Estocásticas Generalizadas (GSPN) para avaliar as comunicações RFID, modelando diferentes possibilidades de erros entre leitores e etiquetas. Uma vez que essa proposta emprega os parâmetros *EPCGlobal UHF Classe 1 Gen2* como referência, que já são adotados pelo protocolo anticolisão *Dynamic Frame Slotted Aloha* para sistemas RFID passivos, esse modelo pode ser explorado para avaliar o desempenho e a confiabilidade de diferentes protocolos de acesso ao meio RFID ao assumir canais ruidosos, suportando melhores comparações entre diferentes algoritmos e protocolos. Os resultados demonstraram que o algoritmo proposto consegue apresentar melhor resultado em relação aos demais protocolos avaliados, principalmente na presença de canais ruidosos e de um grande número de etiquetas para serem lidas. Os cenários de simulação são definidos para apresentar resultados de confiabilidade e desempenho, ao avaliar as leituras da etiqueta RFID, que são essenciais ao projetar e manter aplicações IIoT.

Palavras-chave: IoT industrial. GSPN. RFID. Desempenho. Confiabilidade. Modelagem de Erro.

Abstract

The Industrial Internet of Things (IIoT) is often presented as a concept that is significantly changing the technological landscape of industries, through automation procedures and identification of relevant objects. Therefore, reliability and performance problems must be considered when providing the communication services provided. By using Radio Frequency Identification (RFID) in the context of IIoT, several previous researches have worked to improve the efficiency of their communication systems, generally defining mathematical models for planning and quality assessment. However, such models are designed based on error-free communications, which is in fact unrealistic when considering the fault-prone nature of wireless communications in industrial plants. Therefore, this thesis proposes a new anti-collision algorithm for RFID, together with a formal model based on Generalized Stochastic Petri Nets (GSPN) to evaluate RFID communications, modeling different possibilities of errors between readers and tags. Since this proposal uses the EPCGlobal UHF Class 1 Gen2 parameters as a reference, which are already adopted by the Dynamic Frame Slotted Aloha anti-collision protocol for passive RFID systems, this model can be explored to assess the performance and reliability of different access protocols to the RFID means by assuming noisy channels, supporting better comparisons between different algorithms and protocols. The results showed that the proposed algorithm is able to present a better result in relation to the other evaluated protocols, mainly in the presence of noisy channels and a large number of tags to be read. The simulation scenarios are defined to present results of reliability and performance, when evaluating RFID tag readings, which are essential when designing and maintaining IIoT applications.

Keywords: Industrial IoT. GSPN. RFID. Performance. Reliability. Error Modeling.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Publicações

Filho, I. E. Barros, I. Silva & C. M. D. Viegas (2018), 'An Effective Extension of Anti-Collision Protocol for RFID in the Industrial Internet of Things (IIoT)', Sensors 18 (4426).

Filho, I. E. Barros, I. Silva, Daniel G. Costa & Carlos M. D. Viegas (2020), 'Um Modelo de Performabilidade para Protocolos Anticolisão de Etiquetas RFID', *X Conferência Nacional em Comunicações, Redes e Segurança da Informação* (Aprovado).

Filho, I. E. Barros, I. Silva, D. G. Costa, C. M. D. Viegas & P. Ferrari (2020), 'A GSPN-based Performability Model for Anti-Collision RFID Algorithms Under Noisy Chan nels in Industrial Internet of Things', *Computers in Industry (Elsevier)* (Submetido).

Lista de Símbolos e Abreviaturas

ACK: Acknowledgement

BAP: Battery Assisted Passive

CDMA: Acesso Múltiplo por Divisão de Código

CRC16: Verificação de redundância cíclica de 16 bits

DFSA: Dynamic Framed Slotted ALOHA

DNS: Domain Name System

EPC: Electronic product code

FDMA: Acesso Múltiplo por Divisão de Frequência

GSPN: Generalized Stochastic Petri Nets

HF: High Frequency

ID: Identificação

IEC: International Electrotechnical Commission

IIoT: Industrial Internet of Things

IoT: Internet of Things

ISM: Industrial, Scientific e Medical

ISO: International Organization for Standardization

LF: Low Frequency

MAC: Controle de Acesso ao Meio

ONS: Object Naming Service

RFID: Identificação por Radiofrequência

RISSF: Rede Industrial de Sensores Sem Fio

RN16: Número aleatório de 16 bits

SAN Rede de Atividade Estocástica

SDMA: Acesso Múltiplo por Divisão de Espaço

TDMA: Acesso Múltiplo por Divisão de Tempo

UHF: Ultra High Frequency

UUID: Universally Unique Identifier

Capítulo 1

Introdução

A identificação por radiofrequência (RFID - Radio Frequency IDentication) é conhecida como uma tecnologia de comunicação sem fio que identifica objetos de maneira automática e eficiente. Desse modo, sistemas de RFID vêm sendo amplamente adotados nas mais diversas áreas, incluindo rastreamento de objetos, sistemas de controle de acesso, automatização industrial e biomedicina [Finkenzeller 2010]. Cada vez mais, aplicações de Internet das Coisas Industrial (IIoT) demandam necessidades de gerenciar múltiplos objetos de forma rápida e precisa. Com isso, os sistemas de identificação automática vêm evoluindo e substituindo sistemas antigos, como códigos de barra, cartões com leitura magnética, crachás de identificação, entre outros.

O objetivo deste capítulo é apresentar uma breve contextualização da tecnologia RFID, apontando os principais desafios de quando ela é submetida a ambientes industriais para a identificação de vários objetos. Em seguida, serão abordados os principais requisitos exigidos em aplicações industriais, como: escalabilidade, desempenho e confiabilidade. Ao final do capítulo, serão descritos os objetivos, as motivações e as contribuições da presente tese, além da organização deste documento nos capítulos posteriores.

1.1 Contextualização

A Internet das Coisas (IoT) é uma tecnologia bastante promissora que oferece soluções inteligentes para transformar o modo de operação e funcionalidade de muitos sistemas industriais existentes. O termo IoT foi inicialmente proposto para se referir a objetos interoperáveis, conhecidos como “identificáveis”, de maneira única com a tecnologia de identificação por radiofrequência (RFID) [Jia et al. 2012]. A IoT tem como propósito principal atuar no desenvolvimento de um ambiente onde todos os objetos envolvidos são conectados à Internet e podem se comunicar entre si com o mínimo de intervenção humana.

Essa nova abordagem de sistemas conectados é composta por objetos físicos inteligentes, como, por exemplo: sensores, atuadores, eletrodomésticos, dispositivos eletrônicos, veículos, aviões, produtos em supermercados e produtos industrializados em geral que podem, dependendo da aplicação utilizada, realizar comunicações autônomas, interagir entre si e efetuar a comunicação de dados com a Internet [Al-Fuqaha et al. 2015]; [Lin et al. 2017] a qualquer hora e em qualquer lugar, utilizando a rede e os serviços disponíveis.

Em alguns setores da indústria, o uso de esquemas para a implantação de serviços inteligentes pode ser feito com a utilização do identificador único universal (UUID), necessário para cada serviço ou dispositivo. Um dispositivo com UUID exclusivo pode ser facilmente identificado e recuperado. Assim, UUIDs são essenciais para serviços de sucesso implantados em uma grande rede com diversos nós, como é o caso de um cenário IoT [Al-Fuqaha et al. 2015].

Recentemente, o paradigma da Internet das Coisas (IoT) ganhou cada vez mais espaço, à medida que sistemas embarcados se tornaram acessíveis e novos padrões de comunicação foram sendo desenvolvidos [Lin et al. 2017], [Costa & Duran-Faundez 2018]. Diante desse cenário, dispositivos autônomos inteligentes e interações homem-máquina estão desbravando novos caminhos para transformações importantes, modificando profundamente a concepção e as operações das indústrias modernas [Santos et al. 2015], [Filho et al. 2018], [Bertelli et al. 2017]. O cenário resultante da Internet das Coisas Industrial (IIoT) será permeado por diferentes soluções e por uma grande variedade de contextos.

Dentre as diversas tecnologias de identificação e rastreamento envolvidas no contexto de IIoT, o RFID vem recebendo destaque. Ele tem a capacidade de identificar e rastrear dispositivos e objetos físicos com baixo custo de implantação, suportando um grande conjunto de aplicações. O sistema RFID está cada vez mais sendo adotado no cenário industrial, como logística, gestão da cadeia de suprimentos e monitoramento de serviços de saúde [Jia et al. 2012], [Lim et al. 2013].

Outros benefícios além do uso de comunicação sem fio oferecidos pelo sistema RFID incluem o fornecimento de informações precisas e em tempo real sobre os objetos envolvidos, reduzindo o custo de mão de obra, simplificando o processo de negócios, aumentando a precisão das informações no inventário e melhorando a eficiência dos negócios de modo geral. Atualmente, sistemas baseados em RFID têm sido utilizados com sucesso por diversos fabricantes, distribuidores e varejistas em muitas indústrias [Sun 2012], [Lim et al. 2013]. Porém, alguns requisitos rigorosos de redes industriais, quando relacionados a questões de confiabilidade e desempenho, devem servir de referência para o desenvolvimento de soluções [Garrido-Hidalgo et al. 2019].

1.2 Principais Desafios

Apesar das vantagens destacadas na seção anterior para os sistemas RFID, existem alguns desafios que precisam ser enfatizados. Um deles é o problema de acesso ao meio quando o número de etiquetas para serem identificadas aumenta, pois é certo que se eleva a probabilidade de atrasos e erros no processo de identificação, comprometendo o desempenho do sistema devido ao surgimento de colisões. Desse modo, é necessário o uso de um protocolo anticolisão eficiente para auxiliar no processo de identificação, principalmente quando há um grande número de etiquetas [Klair et al. 2010].

Porém, outro desafio bastante relevante em aplicações IIoT é a capacidade de um sistema de fornecer os serviços conforme o esperado, mesmo com falhas, o que geralmente é definido como uma propriedade conhecida por "dependabilidade". A percepção da dependabilidade pode ser alcançada associando requisitos de confiabilidade e disponibilidade, sendo, para tanto, avaliada e aprimorada como uma forma de assegurar um nível de operação aceitável ao longo do tempo, com desenvolvimentos importantes nos últimos anos [Silva et al. 2013], [Costa et al. 2014]. No entanto, a confiabilidade por si só pode ser insuficiente quando se trata de cenários de comunicação complexos, uma vez que o desempenho dos protocolos também deve ser contabilizado [Silva et al. 2008], [Filho et al. 2018]. Nesse sentido, características como o número de pacotes em colisões e de *slots* de tempo alocados também são bastante relevantes para garantir que os serviços esperados estão sendo atendidos.

Para que seja possível a utilização de sistemas RFID em ambiente industrial, é preciso garantir satisfação na qualidade de serviço conforme o acordo no nível de serviço das aplicações. Para tanto, alguns requisitos são exigidos, como: escalabilidade, desempenho e confiabilidade.

1.2.1 Escalabilidade

A escalabilidade em IIoT se refere à capacidade de adicionar novos dispositivos, serviços e funções para usuários sem comprometer negativamente a qualidade dos serviços já existentes. Adicionar novas operações e suportar novos dispositivos não é uma tarefa fácil, especialmente na presença de diversas plataformas de *hardware* e protocolos de comunicação. Aplicações IoT devem ser projetadas antes mesmo de operar, para permitir com previsibilidade serviços e operações [Uckelmann et al. 2010]. Um fator bastante relevante sobre a questão da escalabilidade em sistemas RFID é a utilização do protocolo de acesso ao meio, para efetuar o processo de leituras simultâneas de várias etiquetas

na mesma área de radiofrequência do leitor. Diversos trabalhos têm utilizado o TDMA como método de acesso ao meio, devido a sua popularidade, simplicidade e baixo custo computacional [Klair et al. 2010]. Porém, a escalabilidade é um critério importante a ser considerado quando se avaliam soluções integradas em qualquer sistema de comunicação sem fio, principalmente em soluções baseadas no RFID.

1.2.2 Desempenho

Um problema crucial que afeta diretamente o desempenho nos sistemas RFID, além das interferências, é o processo de detecção múltipla de um conjunto de etiquetas. Conforme a rede se expande, os leitores atuam para resolver de forma eficiente o problema de colisões que ocorrem durante o processo de identificação, pois são elas as principais responsáveis pelo aumento do consumo de recursos, pela probabilidade de atrasos e erros e pela degradação do desempenho [Su et al. 2016]. Para minimizar os problemas de colisões, os leitores RFID devem implementar algum mecanismo anticolisão [Wang et al. 2012]. Cenários como os de ambientes industriais exigirão cada vez mais um desempenho acurado de todas as tecnologias envolvidas, especialmente no tratamento de colisões em sistemas RFID, pois esses mecanismos definem o desempenho global da tecnologia.

Os parâmetros utilizados para medir o desempenho pelos algoritmos anticolisão de etiquetas são de fato um grande desafio, devido à heterogeneidade de técnicas adotadas por diferentes autores, além da diversidade de características e requisitos dos mais diversos cenários de aplicações, como ambientes industriais. Assim, a análise de desempenho dos algoritmos anticolisão para RFID baseia-se em quatro categorias principais, como: *slots*, tempo, tráfego e precisão. A categoria de *slots* representa o tipo mais frequente na literatura, pois se baseia na contagem do número de *slots* que são utilizados no conjunto dos quadros gerados no processo de identificação. Já a categoria *tempo* visa medir o tempo gasto no processo de identificação que, em algumas situações, é dependente dos *hardwares* utilizados. A métrica de tráfego tem como objetivo contabilizar a troca de mensagens entre o leitor e as etiquetas, também no processo de identificação. Por fim, a precisão visa medir o quão precisos são os algoritmos em estimar a quantidade de etiquetas em relação ao tamanho do quadro ideal.

1.2.3 Confiabilidade

Confiabilidade refere-se ao bom funcionamento do sistema com base em sua especificação [Silva et al. 2013]. Ela visa aumentar a taxa de sucesso da entrega de serviços em

IoT. Tem uma relação estreita tanto com a disponibilidade assim como com a confiabilidade, garantindo a disponibilidade das informações e dos serviços ao longo do tempo. A confiabilidade é ainda mais crítica e possui requisitos mais rigorosos quando se trata de aplicações com necessidade de tempo de resposta emergencial [Costa et al. 2014]. Nesses sistemas, a parte crítica é a rede de comunicação, que deve ser resiliente a falhas para realizar uma distribuição confiável das informações. A confiabilidade deve ser implementada tanto em *software* quanto em *hardware* para todas as camadas de IoT. Para ter uma IIoT eficiente, a comunicação subjacente deve ser confiável, porque, por exemplo, em uma percepção não confiável, a coleta, o processamento e a transmissão de dados podem levar a longos atrasos, à perda de dados e, eventualmente, a decisões erradas, o que proporciona cenários desastrosos e, consequentemente, torna a IIoT menos confiável, inviabilizando a sua utilização.

Para garantir a confiabilidade, o sistema deve ser capaz de continuar operando corretamente. Em sistemas baseados em RFID, é esperado que uma etiqueta possa ser lida independentemente da situação atual do canal de comunicação, mesmo após algum atraso na resposta. Na verdade, se uma etiqueta está sendo lida por um leitor que não está recebendo os dados solicitados, é possível que o sistema esteja apresentando uma falha temporária. Em geral, essas falhas podem produzir diferentes condições de erro, impactando de modo deficiente na qualidade percebida nas aplicações [Pradhan 1996].

1.3 Motivação

A seção anterior apresentou uma discussão sobre os principais desafios enfrentados pela tecnologia RFID diante do contexto industrial, principalmente quando o número de etiquetas que precisam ser identificadas aumenta exponencialmente. Nesse sentido, é preciso manter impreterivelmente uma boa qualidade na comunicação das diversas aplicações, para que seja viável a sua usabilidade.

Tipicamente, aplicações industriais têm sido desenvolvidas para explorar o uso de tecnologias de comunicação com fio [Cairó et al. 2018]. Nessa perspectiva, conforme o aumento constante do número de soluções, vem surgindo uma mudança por opções de infraestruturas que utilizam padrões de comunicação sem fio, visando extrair benefícios importantes, como redução de custos e escalabilidade. Considerando tal cenário, um desafio passa a ser mais evidente: garantir o mesmo nível de confiabilidade e desempenho antes assegurados em conexões com fio, mesmo quando todas as conexões passam a ser sem fio. Como se sabe, a presença constante de probabilidades de erro em comunicações sem fio dificulta a confiabilidade do sistema [Abdelgawad & Bayoumi 2011], colocando tais

questionamentos sobre a usabilidade em aplicações industriais. Além disso, a presença de desempenho abaixo do esperado pode ser levada em consideração, quando comparado às conexões com fio, possivelmente reduzindo o rendimento dos sistemas [Avizienis et al. 2004]. Então, esse cenário adverso demanda o surgimento de novas propostas para melhorar a qualidade das comunicações sem fio, de modo geral, para aplicações industriais.

Para a IIoT, a tecnologia RFID também pode ser explorada em diferentes cenários, oportunizando diversas possibilidades de aplicações. Entretanto, uma vez que as redes industriais e os sistemas de automação exigem algum nível de tolerância a falhas e de eficiência mínima atingível, de acordo com os requisitos das aplicações, a adoção da tecnologia RFID deve considerar essas particularidades. Na verdade, para canais ruidosos comumente percebidos em plantas industriais, deseja-se obter o maior número de leituras bem-sucedidas de etiquetas RFID com o menor tempo, independentemente de erros no canal de comunicação.

No entanto, é importante destacar que somente a confiabilidade não é suficiente para avaliar cenários de comunicação complexos, que demandam a necessidade de mensurar o desempenho dos protocolos anticolisão [Filho et al. 2018]. Diante disso, métricas como números de *slots* em colisão, tempo de identificação, entre outras, também são bastante relevantes para garantir que os serviços esperados sejam cumpridos.

A fim de abordar o desempenho e confiabilidade das comunicações baseadas em RFID, que será mais difícil de ser alcançada quando o número de etiquetas que necessitam ser identificadas for bastante significativo, esta tese propõe um modelo capaz de realizar uma modelagem de canais ruidosos de forma realista, considerando, para tanto, a presença de rajadas de erro e o impacto do tamanho do *payload* da etiqueta. Trabalhos anteriores nessa área de pesquisa assumiram o uso de canais de comunicação livres de erros [Klair et al. 2010], ignorando eventuais problemas comuns que ocorrem em ambientes de comunicação sem fio. Na prática, tornam o sistema menos realista, sendo um grande desafio implementá-los em cenário real.

Adicionalmente, o modelo desenvolvido se apoia no algoritmo anticolisão, baseado em DFSA, proposto para identificar um grande volume de etiquetas. Apresenta-se como técnica o uso do fator de envelhecimento, que atua como um agente recompensador ou penalizador de *slots*, aproveitados de acordo com o desempenho obtido no processo de identificação anterior. Para realizar comparações mais realistas, foi feita uma avaliação de confiabilidade e desempenho com outros algoritmos da literatura, utilizando simulações com o modelo que foi proposto.

1.4 Objetivos

O primeiro objetivo desta tese é apresentar um novo algoritmo anticolisão para sistemas RFID. Considerando os diversos desafios de acesso ao meio para identificar um grande volume de etiquetas, foi desenvolvido junto ao algoritmo uma técnica (fator de envelhecimento) que atua como um agente recompensador ou penalizador dos *slots* aproveitados de acordo com o desempenho obtido no processo de identificação anterior. Esse mecanismo atua como um filtro, diminuindo o número de *slots* em colisões, mesmo quando a taxa de transmissão aumenta durante o canal de comunicação.

O segundo objetivo é propor uma modelagem para canais ruidosos, considerando para isso a presença de erros em rajadas e o impacto do tamanho do *payload* da etiqueta. Para tanto, o modelo proposto é definido explorando o formalismo de modelagem de Redes de Petri Estocásticas Generalizadas (GSPN). Fazendo isso, facilitamos experimentos de simulação com resultados mais factíveis. O canal de comunicação foi modelado tomando como referência os parâmetros *EPCGlobal UHF Classe 1 Gen2*, que são adotados pelo protocolo de acesso ao meio anticolisão DFSA, utilizado nas comunicações RFID.

O terceiro objetivo é realizar a implementação dos algoritmos da literatura que abordam o protocolo DFSA como forma de acesso ao meio e compará-los.

1.5 Contribuições

As principais contribuições desta tese são destacadas a seguir:

- Estudo sistematizado sobre os principais algoritmos anticolisão que avaliam a confiabilidade e o desempenho;
- Proposta de um algoritmo anticolisão capaz de identificar uma grande população de etiquetas, reduzindo o número de *slots* colididos por meio do fator de envelhecimento;
- Desenvolvimento de uma modelagem para o protocolo DFSA em comunicações RFID, utilizando, para tanto, o formalismo GSPN. Esta modelagem visa permitir uma avaliação mais realista de algoritmos anticolisão baseados no protocolo DFSA;
- Definição de diferentes cenários de comunicação assumindo um conjunto de configurações de erro;
- Avaliação da confiabilidade e desempenho de diferentes algoritmos anticolisão;
- Análise de falhas de comunicações RFID.

1.6 Estrutura da Tese

Neste primeiro capítulo, apresentam-se uma contextualização geral, os principais desafios, as motivações, os objetivos, e as contribuições da presente tese. Adicionalmente, o trabalho é complementado por mais cinco outros capítulos, os quais são brevemente descritos a seguir:

- Capítulo 2 apresenta de forma geral os principais conceitos da tecnologia RFID. Como também os protocolos de acesso ao meio, tendo como foco o protocolo DFSA. A fundamentação teórica sobre o estado da arte, que trata da confiabilidade e o desempenho em comunicações sem fio. Além disso, são discutidos nesse capítulo detalhes da modelagem baseada em GSPN.
- Capítulo 3 aborda os trabalhos relacionados que avaliam a confiabilidade e o desempenho em sistemas RFID. O objetivo é avaliar a qualidade das comunicações RFID.
- Capítulo 4 descreve o algoritmo proposto e o modelo desenvolvido para avaliar a confiabilidade e o desempenho dos algoritmos baseados em DFSA. O seu objetivo é detalhar as propostas da respectiva tese.
- Capítulo 5 realiza uma avaliação do desempenho e da confiabilidade dos algoritmos anticolisão baseados no DFSA, utilizando o modelo que foi proposto como ferramenta de avaliação para análise dos resultados.
- Capítulo 6 finaliza o documento com as conclusões e os trabalhos futuros a serem desenvolvidos.

Capítulo 2

Fundamentação Teórica

Neste capítulo apresenta os fundamentos básicos dos sistemas RFID, assim como os tipos de etiquetas e colisões. Para resolver o problema de acesso ao meio, foram expostos as técnicas de acesso múltiplo ao meio juntamente com o protocolo anticolisão DFSA. Também será abordado conceitos relacionados à problemas no canal de comunicação. O capítulo finaliza apresentando o modelo formal de Redes de Petri Estocásticas Generalizadas (GSPN) aplicado a sistemas de RFID. Modelagem, confiabilidade e desempenho também serão descritos.

2.1 Identificação por Radiofrequência - RFID

Atualmente, existe cada vez mais a necessidade de gerenciar vários objetos de forma rápida, segura, eficiente e precisa. De acordo com esse propósito, a tecnologia RFID surge como uma opção bastante interessante para realizar tarefas como identificação, rastreamento e automação de objetos. Uma vantagem do RFID em relação a outros sistemas de identificação refere-se ao alcance de leitura, uma vez que não é necessária a aproximação do objeto para sua completa identificação [Klair et al. 2010].

Apesar de ter se desenvolvido em abrangência nos anos 2000, a notoriedade por trás do RFID foi contemplada nos anos de 1940. Seu desenvolvimento surgiu na época da segunda guerra mundial, no sistema de identificação de "aliados ou inimigos"(*Friend or Foe*) [Finkenzeller 2010]. A proposta nesse sistema era permitir, por exemplo, a identificação de aviões, determinando se eles eram aliados. Nesse sentido, o processo de requisição era realizado através de sinais modulados em frequências bem definidas e eram previstas respostas padronizadas. Com esse intuito, as aeronaves aliadas eram providas de *transponders*, que tinham capacidade de decifrar sinais recebidos e responder com seus identificadores. Caso as respostas não fossem as esperadas ou se não houvesse nenhuma resposta, concluía-se que as aeronaves não eram conhecidas, embora isso não significasse

que fossem inimigas [Lumpkins 2015].

Este capítulo tem por objetivo apresentar os principais fundamentos básicos dos sistemas RFID, assim como a classificação das etiquetas, os padrões, os problemas de acesso ao meio e as possíveis soluções em sistemas RFID. Por fim, serão mostrados alguns cenários de aplicações que exigem grande volume de etiquetas RFID.

2.2 Arquitetura

O RFID apresenta sistemas adaptáveis e completos, formado por diversos elementos e configurações, podendo variar desde sistemas mais simples até complexos e sofisticados, determinados apenas pela aplicação utilizada. Um sistema RFID básico consiste em três elementos principais, sendo eles: leitores, etiquetas (ou *tags*) e uma base de dados, dependendo do tipo de aplicação.

O leitor é um equipamento cuja função é identificar as etiquetas e, através disso, extrair informações nelas contidas, desde que estejam no seu raio de alcance para a realização correta do processo de leitura. Sua comunicação com as etiquetas é realizada por meio de ondas de radiofrequência. Outra função também importante de responsabilidade do leitor diz respeito ao gerenciamento do controle de acesso ao meio das etiquetas, que, por sua vez, é realizado com o auxílio dos protocolos anticolisão.

A base de dados é a entidade centralizadora do sistema RFID. Ela tem a função de armazenar e também de processar informações, que serão transformadas em inteligência de negócios de acordo com as necessidades de cada aplicação. Em geral, é um banco de dados no qual se armazenam e se acessam informações de todas as etiquetas e leitores presentes no sistema. Uma característica fundamental do banco de dados é que ele pode estar embutido no próprio leitor, dependendo do modelo de dispositivo utilizado.

As etiquetas são os elementos mais simples do sistema. Têm o papel principal de armazenar informações dos objetos que estão inseridos no ambiente que estão associados a elas (anexados em cada objeto). Cada etiqueta possui um identificador exclusivo próprio chamado de (ID), pelo qual podem ser identificadas quando interrogadas pelo leitor.

O processo de comunicação funciona da seguinte forma: quando as etiquetas são colocadas na área de leitura do leitor, passam a ser energizadas por meio de ondas de radiofrequência contínuas e enviam suas informações de volta para o leitor. Este, por sua vez, recebendo as informações das etiquetas, enviam-nas para o sistema de aplicação para processamento das informações recebidas [Zhang, Xiang, Tang, Li & Yan 2018]. A descrição funcional de um sistema RFID básico é apresentada pela 2.1. e possui os seguintes componentes básicos: uma ou mais etiquetas equipadas com antenas e um leitor

RFID capaz de enviar comandos por sinais de rádio, para extrair informações necessárias das etiquetas. O leitor pode estar associado ou não a um servidor para controlar os dados capturados através do gerenciador de banco de dados.

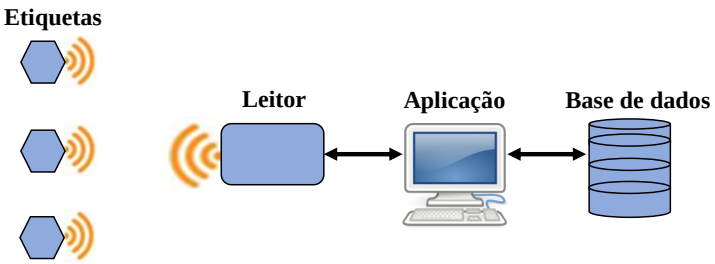

Figura 2.1: Exemplo de sistema básico de RFID.

2.3 Etiquetas RFID

As etiquetas são os componentes mais presentes no sistema RFID. Elas são anexadas a cada objeto que será gerenciado, podendo estar disponíveis nos mais diversos tamanhos, formatos, materiais e capacidade de armazenamento, dependendo do contexto da aplicação em que serão aproveitadas. Fundamentalmente, são formadas pelos seguintes componentes essenciais: um microchip; uma antena para comunicação; e uma pequena memória [Klair et al. 2010].

O microchip é um circuito integrado que oferece funcionalidade à etiqueta. É bem semelhante à funcionalidade de um microprocessador encontrado em qualquer computador ou *smartphone*, porém sem muita "sofisticação"de processamento. Para algumas etiquetas, principalmente as mais simples, seu microchip apresenta apenas o propósito de transmitir o identificador único da etiqueta. [Jia et al. 2012].

A principal funcionalidade da antena na etiqueta RFID é transmitir e receber ondas de rádio para a comunicação. Esse dispositivo é também conhecido como um mecanismo acoplado, que consegue transformar a energia em forma de radiação eletromagnética [Senadeera et al. 2013]. Essa é a forma pela qual a etiqueta e o leitor RFID se comunicam.

2.3.1 Classificação das Etiquetas

As etiquetas RFID podem ser classificadas de três principais formas: quanto ao método de energia; quanto a capacidade de leitura e escrita dos dados; e quanto à frequência de operação utilizada. Conforme detalhado pelas seguintes Tabelas 2.1, 2.2 e 2.3. Há

também a subdivisão em quatro categorias de etiquetas: Passivas, Ativas, SemiAtivas e SemiPassivas [Senadeera et al. 2013].

Tabela 2.1: Categorização de etiquetas quanto à forma de energia [Senadeera et al. 2013].

Tipo de etiqueta	**Atributos**
Passivas	Não possuem fonte própria de energia, sendo energizadas pelo sinal do leitor.
Ativas	Possuem fonte própria de energia podendo iniciar uma comunicação com o leitor.
Semi-Ativas	Possuem fonte de energia própria, mas necessita do auxilio do leitor para ser ativada.
Semi-Passivas	Possuem fonte de energia própria, porém se não tiver fonte de energia continuará em modo passivo.

Etiquetas passivas são mais comuns, duráveis e de baixo custo. Elas não possuem fonte de alimentação energética, como bateria interna, isto é, utilizam o sinal emitido do próprio leitor como fonte de energia, através do processo de indução eletromagnética, para alimentar o seu microchip interno e, com isso, realizar a comunicação com ele. Desse modo, não é necessário a realização de manutenção desse tipo de etiqueta, porém, devido à simplicidade oferecido pelo seu *hardware*, possui um alcance de cobertura bem menor em relação as etiquetas ativas.

As etiquetas ativas, diferentemente das passivas. Apresentam uma fonte própria de energia, de modo geral, uma bateria interna que tem como finalidade auxiliar na realização de todas as funções do processamento interno, possuindo a habilidade de iniciar sua própria comunicação com o leitor e com outras etiquetas. Apresenta maior alcance de leitura em relação às etiquetas passivas e semipassivas, bem como melhor poder computacional e, consequentemente, maior custo financeiro de implementação.

As semiativas possuem fonte de energia própria para alimentar seu microchip central e, assim, realizar também operações internas, mas ainda utilizam o sinal enviado pelo leitor como fonte de energia para transmissão. Nessa perspectiva, esse tipo de etiqueta somente irá transmitir algum sinal de comunicação se antes houver uma transmissão realizada pelo leitor para o estabelecimento de comunicação.

O grupo das semipassivas utiliza um mecanismo chamado *Battery Assisted Passive*

(BAP), o qual possui a funcionalidade de apenas auxiliar no processo de leitura quando o leitor não consegue transmitir um sinal com intensidade suficiente para acioná-las. Trabalham de maneira similar às etiquetas semiativas, porém, quando a sua bateria interna deixa de funcionar, elas continuam operando normalmente, em modo de etiqueta passiva.

Outra forma de classificação das etiquetas é por características computacionais disponíveis, como: capacidade de memória e leitura/escrita. Segundo o padrão [EPCGlobal 2013] as etiquetas são constituídas por cinco classes bem definidas, conforme está descrito pela Tabela 2.2.

Tabela 2.2: Categorização de etiquetas quanto à capacidade de leitura e escrita [EPCGlobal 2013].

Classe	**Atributos**
Classe 0	Somente leitura dos dados. (Etiquetas passivas)
Classe 1	Somente leitura dos dados. (Etiquetas passivas)
Classe 2	Leitura/escrita dos dados acima de 65 kb (Etiqueta passivas)
Classe 3	Leitura/escrita dos dados (Etiquetas semipassivas)
Classe 4	Leitura de outras etiquetas (Etiquetas ativas)
Classe 5	Capacidade de comunicação com outros dispositivos (Etiquetas ativas)

O método utilizado pelo padrão *EPCGlobal* para classificar as etiquetas RFID está de acordo com capacidade de leitura e escrita dos dados que elas podem oferecer para registrar as informações dos objetos, como também a forma de utilização como fonte de energia, sendo elas: ativas, semipassivas ou passivas. É importante destacar que os elementos envolvidos no processo de comunicação como as etiquetas, os leitores e outros dispositivos podem ou não ser compatíveis com ambos os padrões e protocolos existentes, ficando, assim, a cargo do usuário verificar a compatibilidade disponível para a aplicação no sistema de identificação.

Com relação à categorização para o tipo de frequência apresentado pela Tabela 2.3, percebe-se que, quanto menor a frequência de operação, menor será o alcance de cobertura da etiqueta (com exceção de micro-ondas). Essa informação é fundamental para determinar a escolha da frequência que será utilizada no projeto em questão. A utilização de etiquetas de Baixa Frequência (LF) ocorre em aplicações de controle de acesso e controle de inventários, como, por exemplo, em um ambiente onde funcionários de uma empresa precisam aproximar seu cartão de acesso, equipado com etiqueta RFID, de uma

catraca que contém um leitor que realiza o procedimento de liberar ou não a passagem ao local desse funcionário. Etiquetas que possuem Alta Frequência (HF) se encaixam melhor em cartões inteligentes. Nos sistemas de pagamento de transporte público, cada vez que um passageiro precisa entrar no ônibus, é necessário efetuar o pagamento utilizando o seu cartão inteligente. Após a realização da transação, o valor é debitado diretamente do cartão, o qual pode ser recarregado quantas vezes forem necessárias.

Tabela 2.3: Categorização de etiquetas quanto à faixa de frequência [Klair et al. 2010].

Tipo de etiqueta	**Frequência**	**Alcance**	**Taxa de transferência**
Baixa Frequência - LF	125 - 134kHz	0.5m	< 10kbit/s.
Alta Frequência - HF	13.56MHz	1.5m	< 100kbit/s.
Ultra Alta Frequência - UHF	860 - 960MHz	4m - 7m	< 100kbit/s.
Micro-ondas	2,45GHz	1m	< 200kbit/s.

As etiquetas de Ultra Alta Frequências (UHF) são mais bem aplicadas a contextos industriais para rastreamento e localização de modo geral. São as mais consolidadas comercialmente, devido à eficácia em diversas aplicações. Os cenários de uso são bastante amplos, principalmente por apresentarem as vantagens de ler várias etiquetas ao mesmo tempo, assim como de oferecer maior distância de identificação, transferência rápida de dados e tolerância a ambientes agressivos ao ar livre.

As etiquetas UHF podem ser usadas para gerenciamento de ativos, gerenciamento de linha de produção, gerenciamento da cadeia de suprimentos, armazenamento, todos os tipos de rastreabilidade de segurança de mercadorias (como tabaco, álcool, remédios etc.), varejo e gerenciamento de veículos, além de possuírem uma padronização bem definida [Finkenzeller 2010]. Por fim, as etiquetas com maior taxa de transmissão de dados são as que utilizam frequências de micro-ondas, porém, estas também apresentam maior custo em relação às demais citadas, o que torna inviável sua aplicação quando é necessária a utilização de milhares de etiquetas.

É importante ressaltar que as etiquetas passivas UHF estão cada vez mais sendo utilizadas em diversas aplicações RFID, por serem pequenas e de simples fabricação, além de possuírem algumas vantagens com relação aos outros grupos de etiquetas, como baixo custo de produção, maior durabilidade e alcance de leitura. Conforme a série de benefícios mencionada e a maior viabilidade comercial para aplicabilidade com grandes quan-

tidades de objetos, as etiquetas passivas *EPCGlobal UHF Class 1 Generation 2* serão o foco de pesquisa desta tese.

2.4 Padronização em RFID

Com o aumento do uso comercial em aplicações RFID, surgiu a necessidade de desenvolver padrões para a tecnologia em si, trazendo benefícios como aumento da produtividade, melhor utilização dos recursos e melhoria na qualidade das soluções de forma geral. As principais entidades responsáveis por desenvolver normas e padrões para a tecnologia RFID foram a ISO (*International Organization for Standardization*) e a *EPCGlobal*. A primeira organização representa uma série de normas e protocolos para a comunicação sem fio. Esses padrões abrangem as atuais frequências utilizadas no RFID em diversos países [ISO 2013]. Já a *EPCGlobal* tem por finalidade gerenciar o sistema de numeração dos *IDs* exclusivos para cada etiqueta, o qual é representado pela classe de codificação EPC (*Electronic Product Code*), bem como desenvolver padrões de protocolos de comunicação, frequências de operações e pesquisas voltadas para o RFID [EPCGlobal 2013].

Apesar de haver características comuns entre os padrões *ISO 18000* e *EPCglobal*, alguns aspectos técnicos descritos em ambas as propostas apresentaram incompatibilidades, principalmente quando se referiam à utilização de protocolos para a interface aérea capaz de trocar informações entre o leitor e a etiqueta. Portanto, a *EPCGlobal* disponibilizou sua especificação *EPC Gen2*, também denominada *EPCGlobal UHF Class 1 Generation 2*, que, por sua vez, passou a ser utilizada com o mínimo de modificações pelo então padrão ISO 18000-6C, em 2006 [Cerciello et al. 2014]. O aceite por parte da ISO para a norma *EPCGlobal Gen2* significa que equipamentos de acordo com a normatização *Gen2* também estão em conformidade com os padrões ISO.

Os padrões ISO e *EPCglobal* representam um papel importante na evolução da tecnologia RFID, proporcionando compatibilidade, interoperabilidade e segurança entre os diversos componentes envolvidos no sistema RFID. A padronização tem sido um componente fundamental no desenvolvimento comercial da tecnologia RFID.

2.4.1 Padrões ISO

A ISO é uma organização de abrangência mundial que contribui na publicação e no desenvolvimento de padrões e normas internacionais, sendo formada por uma rede de institutos nacionais de normalização presente em 165 países. É uma organização não governamental que atua nos diversos segmentos dos setores públicos e privados, formando

um consenso a ser alcançado em soluções que atendam os requerimentos de negócios de acordo com as necessidades da sociedade [ISO 2013].

As normas da ISO têm contribuído no crescimento de pesquisas técnicas em quatro domínios específicos para a tecnologia RFID. Eles são: utilização das respectivas faixas de frequências, que são regulamentadas para aplicação e uso; interface aérea (comunicação entre etiqueta e leitor); conteúdo e codificação de dados (sistemas de numeração); testes de conformidade, desempenho e interoperabilidade entre as diversas aplicações voltadas para RFID.

Normalmente, a frequência selecionada para operação de leitura das etiquetas precisa estar de acordo com a norma de comunicação, para que seja possível realizar seu processo de identificação com qualidade. Esse padrão é o que define qual linguagem será utilizada para a troca de mensagens, conforme apresentado pela Tabela 2.4 [Klair et al. 2010].

Tabela 2.4: Especificação de frequências com diferentes padrões ISO.

Faixa de Frequência	**Especificação ISO**
125 - 134kHz (Baixa Frequência - LF)	ISO/IEC 18000-2
13.56MHz (Alta Frequência - HF)	ISO/IEC 18000-3
2,45GHz (Micro-ondas)	ISO/IEC 18000-4
5,8GHz (Micro-ondas)	ISO/IEC 18000-5
860 - 960MHz (Ultra Alta Frequência - UHF)	ISO/IEC 18000-6

Até a adoção do padrão *EPCGlobal Gen 2 Class 1* haviam outros dois padrões que utilizavam a mesma de frequência: 18000-6A e 18000-6B. Porém, a principal distinção entre eles é a utilização do protocolo anticolisão de etiquetas, que pode ser evidenciado pela Tabela 2.5.

Tabela 2.5: Especificação dos protocolos anticolisão ISO/IEC 18000-6x.

Frequência 860 - 960MHz (Ultra Alta Frequência - UHF)	
Padrão ISO/IEC	**Protocolo Anticolisão**
18000-6A	ALOHA
18000-6B	Árvore Binária
18000-6C (EPCglobal Gen 2 Class 1)	Slot Randômico (ou QAlgoritmo)

2.4.2 Padrão EPCglobal

O *EPCGlobal* é uma instituição sem fins lucrativos sucessora da *Auto-ID center*, cujo papel é desenvolver e administrar soluções voltadas para a tecnologia RFID. Entre as mais diversas aplicações desse segmento, tem como foco principal desenvolver padrões voltados para a indústria, mais precisamente em sistemas para gerenciamento de cadeia de suprimentos. Um dos principais padrões desenvolvidos foi o código eletrônico de produto ou simplesmente EPC, que serve como um identificador único utilizado para especificar cada objeto [EPCGlobal 2013]. Além disso, o padrão EPC regulamenta a comunicação entre os diversos elementos envolvidos, incluindo o armazenamento de informações e o formato dos dados para transferência.

O padrão EPC conta com um serviço de rastreabilidade de produtos conhecido como Serviço de Nomes para Objetos (*ONS - Object Naming Service*), semelhante ao Serviço de Domínios de Nomes da Internet (DNS). A finalidade do ONS é disponibilizar um serviço de busca global por meio de um código EPC, que simplesmente o traduz para um endereço de URL específico, no qual mais informações detalhadas do objeto podem ser encontradas, como fabricante, data fabricação, modelo etc. Com isso, o EPC provou que é possível agilizar os processos e aumentar a visibilidade dos produtos por meio da disponibilização de informações, criando o conceito de rastreamento total de produtos e não somente de um processo ou de uma empresa, mas de cada produto individualmente, em toda a cadeia de suprimentos.

A especificação do protocolo de comunicação *EPCGlobal UHF Class 1 Generation 2* define quais são os requisitos físicos e lógicos obrigatórios para a etiqueta passiva. Nesse sentido, o leitor fica responsável sempre por iniciar todo o processo de comunicação com as etiquetas, estabelecendo como frequência de operação para o sistema RFID de 860 MHz - 960 MHz e uma comunicação caracterizada por ser do tipo *half-duplex* [Duan et al. 2015*a*]. Atualmente, diversos países fazem uso de aplicações na indústria com etiquetas passivas *EPCGlobal UHF Class 1 Generation 2*, devido aos benefícios garantidos pelo padrão. Na seção 2.9, será detalhado o seu funcionamento de comunicação com os protocolos anticolisão de etiquetas passivas.

2.5 Colisões em Sistemas RFID

Como os sistemas RFID utilizam o meio sem fio para comunicação, existem alguns problemas que surgem durante o compartilhamento de acesso ao meio, como colisões e interferência de sinais [Xu & Chen 2015] [Duan et al. 2015*b*] [Gong et al. 2018] [Zhang,

Xiang & Tang 2018]. Em geral, as colisões comprometem a comunicação dos sistemas RFID, pois podem ocorrer erros no processo de identificação das etiquetas. Além disso, quando ocorrem colisões, uma estratégia de retransmissão precisa ser utilizada, o que impacta no consumo de energia, aumentando o uso da largura de banda e retardando, consequentemente, o tempo total de identificação das etiquetas RFID [Zhong et al. 2012]. Ao considerar o uso de etiquetas passivas, o problema de colisão pode ser ainda maior, devido à sua limitação computacional. Na maioria dos casos, a comunicação se torna impossível de ser realizada, sendo este um problema a ser resolvido.

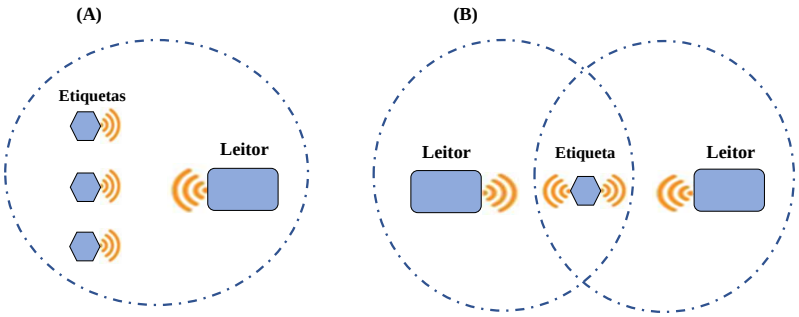

Figura 2.2: Tipos de colisões.

Existem dois tipos de colisões que precisam ser resolvidos, conforme descritos pela Figura 2.2: colisões entre etiquetas (A) e colisões entre leitores (B). De um lado, colisões entre etiquetas ocorrem quando duas ou mais etiquetas enviam informações simultaneamente para um único leitor. Por outro lado, as colisões entre leitores ocorrem quando os sinais de dois ou mais leitores se sobrepõem [Su et al. 2016], tornando confuso para as etiquetas identificarem a qual leitor elas devem responder primeiro.

Problemas de acesso ao meio estão diretamente ligados às colisões de etiquetas nos sistemas de RFID. Para resolver os problemas de colisões, soluções têm adotado o papel primordial de coordenar a forma de comunicação entre leitor e etiquetas, realizando um sincronismo entre as partes envolvidas através do uso de protocolos anticolisão. Algumas soluções de acesso múltiplo ao meio serão expostas na seção a seguir.

2.6 Protocolos de Acesso Múltiplo ao Meio

Em virtude do crescimento cada vez mais maior de novas aplicações, o processo de leituras simultâneas de várias etiquetas na mesma área de radiofrequência do leitor vem se tornando um grande desafio. Podemos citar como exemplos práticos supermercados,

indústrias, bibliotecas, bagagens aéreas, vestuários e lojas. Problemas de acesso múltiplo vêm acompanhando a tecnologia sem fio durante muito tempo. Por essa razão, diversas soluções, como protocolos de acesso ao meio, têm sido pesquisadas e ampliadas, com o propósito fundamental de separar a presença individual de cada etiqueta das demais, quando envolvidas no processo de leitura para identificação pelo leitor.

A Figura 2.3 ilustra como são definidos os quatro principais protocolos de acesso ao meio (MAC): acesso múltiplo por divisão de espaço (SDMA), acesso múltiplo por divisão de código (CDMA), acesso múltiplo por divisão de frequência (FDMA) e acesso múltiplo por divisão de tempo (TDMA).

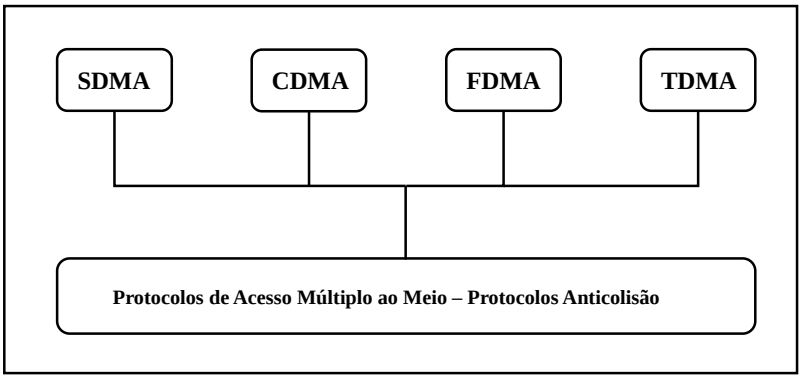

Figura 2.3: Métodos de controle de acesso múltiplo ao meio.

O protocolo SDMA [Finkenzeller 2010] tem como principal função distribuir diferentes faixas de frequência para diferentes áreas de abrangência vizinhas. Essa técnica é amplamente utilizada para a realização de cobertura de sinal entre células adjacentes, assim como pela rede de telefonia móvel. Porém, sua aplicação em sistemas RFID é praticamente inviável, devido à necessidade de se usar diversas antenas e leitores setoriais, o que significa aumento de complexidade e custo do sistema [Klair et al. 2010].

O protocolo CDMA [Vahedi et al. 2014] tem por finalidade utilizar técnicas de propagação espectral que são distribuídas uniformemente e aplicadas aos elementos envolvidos na rede com a mesma potência e frequência. Cada elemento possui um código diferente para modular o sinal recebido pelo emissor. Porém, ao considerar seu uso em sistemas RFID, esse protocolo apresenta alguns problemas, uma vez que a divisão do código requer um alto custo computacional.

O protocolo FDMA realiza a divisão da largura de banda disponível em várias bandas de frequência. Com isso, cada usuário possui uma faixa de frequência reservada, que pode ser utilizada até o final de sua transmissão. No entanto, o uso de diversas bandas de frequência aumenta o custo de dispositivos como etiquetas e leitores [Bang et al. 2009].

No protocolo TDMA [Mingliang & Shun 2010], o canal de comunicação é dividido em vários *slots* de tempo que possuem tamanho fixo, em que cada elemento transmite um determinado *slot* por vez, evitando, assim, interferências. Devido a sua popularidade, simplicidade e baixo custo computacional, esse protocolo tornou-se a opção mais adequada para sistemas RFID. Com o uso do TDMA, os intervalos de tempo disponíveis para transmissão de etiquetas são classificados de três formas: *slot* vazios, quando não há transmissão; *slot* de sucesso, quando apenas uma etiqueta pode transmitir sua identificação; e *slot* em colisão, quando duas ou mais etiquetas tentam transmitir simultaneamente dentro do mesmo intervalo de tempo.

2.7 Protocolo Anticolisão de Etiquetas

Com o objetivo de resolver problemas causados por colisões de etiquetas, existem diversos protocolos que podem ser encontrados na literatura [Klair et al. 2010], de acordo com a limitação computacional imposta pelas etiquetas passivas e grande usabilidade em diversas aplicações pelo baixo custo oferecido. Então, torna-se mais viável a adoção de soluções como o TDMA para gerenciar a forma de acesso múltiplo nos sistemas de RFID. Desse modo, o TDMA pode ser dividido em três grandes categorias de protocolos anticolisão de etiquetas: protocolos baseados em árvores, protocolos baseados em ALOHA e protocolos híbridos [Klair et al. 2010].

Os protocolos de anticolisão baseados em árvore atuam de forma determinística. Em virtude disso, atrasos no processo de identificação crescem exponencialmente à medida que o número de etiquetas aumenta, devido à forma como tratam as colisões. No entanto, exige-se, por parte da etiqueta, maior capacidade de memória e dependência de *hardware* mais sofisticado.

Os baseados em ALOHA possuem a característica de serem probabilísticos. Apresentam simplicidade de implementação em nível de hardware e consequentemente menor complexidade de implantação, atributos essenciais para sua utilização em larga escala.

Os protocolos híbridos têm como característica principal utilizar a combinação das vantagens que são oferecidas pelos protocolos baseados em árvore e ALOHA. Porém, o desafio dessa proposta de protocolo continua sendo manter um baixo custo computacional para as etiquetas passivas.

Como o objetivo principal dessa tese consiste em avaliar a confiabilidade e o desempenho em sistemas RFID, compostos por um grande número de etiquetas passivas *EPCglobal UHF Class 1 Generation 2*, serão abordados na seção seguinte os protocolos baseados em ALOHA.

2.8 Classificação dos Protocolos Baseados em ALOHA

Os protocolos baseados em ALOHA nos sistemas RFID têm como função dividir o tempo em diversos *slots* e alocar cada etiqueta em seu respectivo *slot* de tempo, para extrair suas informações, reduzindo, portanto, a possibilidade de colisões [Xinqing & Fan 2010]. Os protocolos ALOHA são simples de se implementar e podem ser utilizados para identificar qualquer número de etiquetas. Por essa razão, essa classe de protocolos é amplamente abordada em sistemas RFID.

2.8.1 Pure ALOHA (PA)

O protocolo ALOHA foi um dos primeiros sistemas anticolisão desenvolvidos para resolver problemas de acesso múltiplo ao meio, tradicionalmente, em redes de computadores. De acordo com o seu funcionamento, o emissor começa a enviar quadros de informações para o receptor. Após o envio desses quadros, o emissor escuta o meio para ter a certeza de que a sua informação chegou ao destino, ou seja, ele obtém um retorno que sua informação foi enviada. Para essa finalidade, o emissor gera um tempo aleatório de espera para saber se a sua informação de fato chegou ao seu destino. Se por acaso não houve resposta durante esse tempo de espera, o emissor irá repetir novamente uma outra transmissão da mesma informação, isto é, irá reenviar o quadro em específico, do qual não obteve resposta [Tanenbaum 2003].

Como os protocolos anticolisão baseados em ALOHA são chamados de probabilísticos ou aleatórios, eles têm o papel fundamental de estimar uma certa quantidade de etiquetas. Para tanto, separam-nas de um grupo total, que irá disputar por *slots* de tempo, e as alocam nas suas respectivas transmissões.

Os problemas de ocorrências de colisões no *pure ALOHA* em sistemas de RFID são resolvidos da seguinte forma [Zhong et al. 2012]: se, durante uma transmissão, duas ou mais etiquetas enviarem suas informações simultaneamente para o leitor, ocorrerá certamente uma colisão. Dessa forma, é gerado um período de tempo aleatório no qual as etiquetas que se envolveram na colisão atual possam retransmitir novamente apenas uma única etiqueta por vez. Um exemplo do funcionamento do *pure ALOHA* é destacado na Figura 2.4.

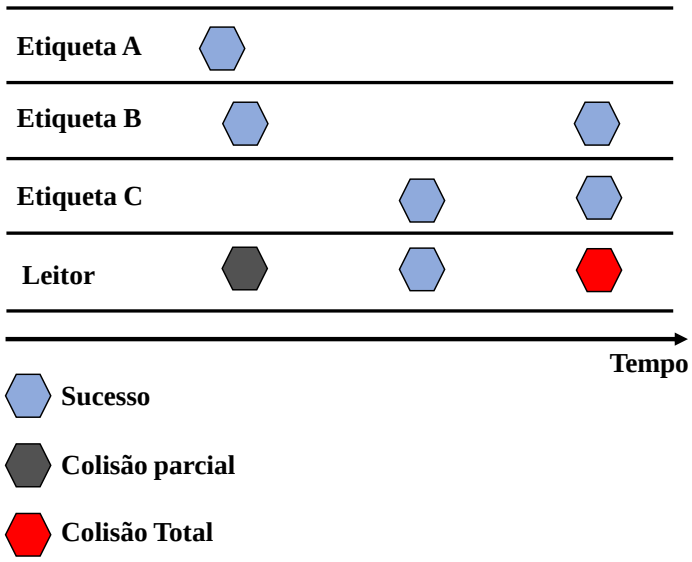

Figura 2.4: Transmissão no pure ALOHA.

Observa-se que as etiquetas A e B fazem uma colisão parcial logo na sua primeira transmissão. Nota-se que, no momento em que a etiqueta A transmite suas informações, parte dela colide com a etiqueta B, que está disputando o acesso ao meio simultaneamente, como pode ser observado na Figura 2.4. As colisões parciais são problemas que podem acontecer no protocolo *pure ALOHA*, devido à falta de *slots* de tempo com tamanho fixo. Essa adversidade é característica comum do próprio protocolo, enquanto as etiquetas B e C apresentam uma colisão total e apenas a etiqueta C consegue ser identificada com sucesso. De acordo com o que foi mostrado, existe uma problemática em relação ao uso do *pure ALOHA* para RFID. Imaginemos que há milhares de etiquetas a serem identificadas, dessa forma, poderá ocorrer uma demora muito significativa na identificação de todas as etiquetas do inventário. Em virtude da falta de gerenciamento do tempo para a transmissão das etiquetas, elas passam a transmitir informações a todo momento, gerando diversas colisões sucessivas, o que compromete sua utilização.

2.8.2 Slotted ALOHA

Diferentemente do *Pure ALOHA*, o protocolo anticolisão *Slotted ALOHA* utilizou como solução o método de fragmentação do tempo para transmissões em várias partes de tamanhos iguais, chamando-os de *slots* de tempo [Tsao et al. 2011]. Para tanto, é primordial que todas as etiquetas envolvidas estejam sincronizadas com o leitor, no intuito de saber quando se inicia ou finaliza um determinado *slot* antes de realizar qualquer tipo de transmissão.

A Figura 2.5 mostra um exemplo do protocolo com três possíveis situações que podem ser encontradas: *slots* em colisão, quando duas ou mais etiquetas transmitem ao mesmo tempo; *slots* com sucesso, quando apenas uma única etiqueta transmite; e *slots* vazio, quando não há transmissão de etiquetas. A ilustração expõe, de forma geral, o funcionamento do protocolo *Slotted ALOHA*. Nota-se que as etiquetas A, B e C disputam o acesso ao meio. A etiqueta A transmite sozinha, no primeiro *slot*; as etiquetas B e C colidem no segundo *slot*; no terceiro *slot*, nenhuma etiqueta transmite informações; e no quarto *slot* apenas a etiqueta C transmite normalmente.

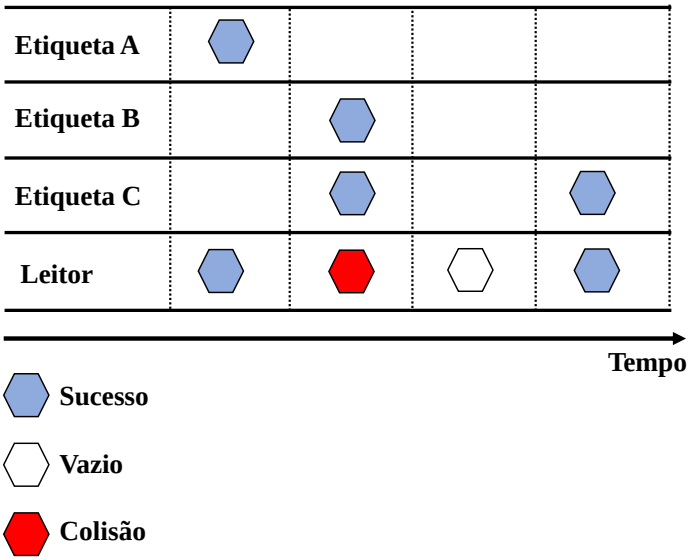

Figura 2.5: Transmissão no slotted ALOHA.

2.8.3 Framed slotted ALOHA

O protocolo *Framed Slotted ALOHA* é uma evolução do *Slotted ALOHA*, cuja função é implementar a utilização de quadros que possuem tamanho fixo compostos por diversos *slots*. Assim, cada transmissão de etiquetas poderá ser alocada em apenas um único *slot* por quadro [Eom et al. 2008]. Se houver a necessidade de uma etiqueta transmitir em um *slot* ocupado, ocorrerá uma colisão. Vale salientar que a forma de alocação de etiquetas em *slots* acontece de maneira aleatória, o que pode dificultar a previsão de acomodação das etiquetas aos respectivos *slots* de tempo.

A Figura 2.6 apresenta, de maneira geral, o exemplo de utilização do protocolo *Framed Slotted ALOHA*. Verifica-se que inicialmente são gerados dois quadros, ambos de tamanhos fixos com quatro *slots* cada. As etiquetas A, B e C vão disputar transmissões por *slots* no primeiro quadro. Observa-se que apenas a etiqueta A é identificada com su-

cesso logo no primeiro *slot*. Já no segundo, as etiquetas B e C provocam uma colisão, porque realizaram uma transmissão em único *slot*, simultaneamente. O terceiro e quarto *slots* apresentam-se como vazios, porque não houve nenhuma sinalização de transmissão de etiquetas.

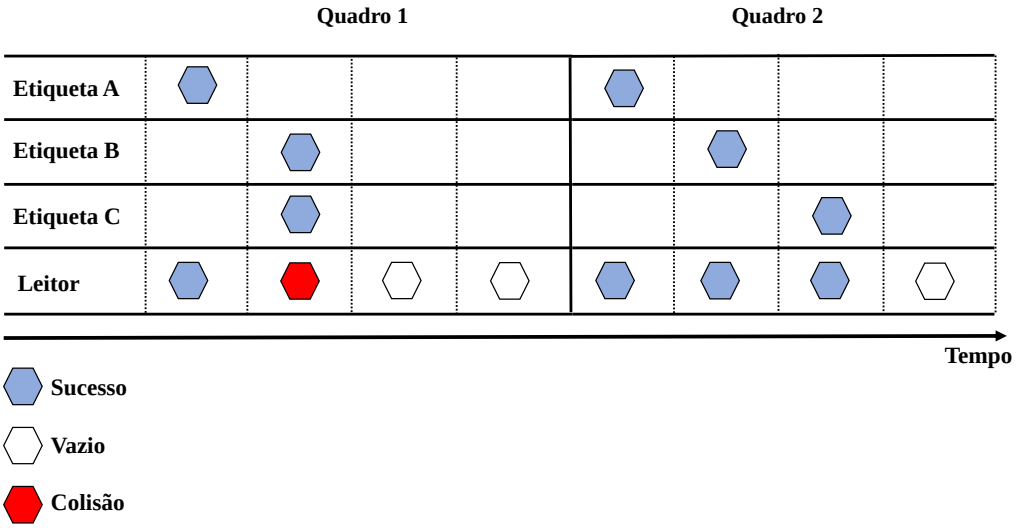

Figura 2.6: Transmissão no framed slotted ALOHA.

Devido à existência de colisão ocorrida no primeiro quadro, nesse caso, ainda restam identificar as etiquetas B e C, gerando-se, para isso, um quadro seguinte com essa finalidade. No segundo quadro, as etiquetas A, B e C são identificadas com sucesso, uma em cada *slot*, separadamente. Já o último *slot* aparece como vazio, porque não houve transmissão de nenhuma etiqueta.

No entanto, existe um dilema quando se utiliza esse protocolo. Para uma determinada quantidade de etiquetas a serem identificadas, caso se apresente um quadro com um tamanho grande, ou seja, com vários *slots*, poderá causar um número excessivo de *slots* vazios, provocando, assim, um desperdício desnecessário de largura de banda. Já se o tamanho do quadro for pequeno, poderá ocorrer um número alto de *slots* em colisões, significando novos procedimentos de leitura de etiquetas, o que acarretará em maior tempo gasto nessa etapa.

2.8.4 Dynamic Frame Slotted ALOHA (DFSA)

Conforme discutido anteriormente sobre o problema da utilização de um quadro com tamanho fixo, surgiu, então, a necessidade de se criar uma alternativa para resolver tal

problema, como um protocolo que utiliza quadros de tamanho variável de acordo com a necessidade de identificação das etiquetas.

O protocolo *Dynamic Frame Slotted ALOHA*, ou simplesmente DFSA, é bastante eficiente em relação a outras extensões propostas para os protocolos anticolisão baseados em ALOHA [Wang et al. 2012]. O protocolo DFSA tem como característica realizar o ajuste dinâmico no tamanho do seu quadro antes de cada ciclo de leitura. Com isso, ele consegue identificar um maior número de etiquetas em menor tempo, devido à utilização de um tamanho de quadro teoricamente proporcional ao número de etiquetas que fazem parte do processo de identificação. Em tese, não se sabe ao certo quantas etiquetas precisam ser identificadas.

O DFSA funciona da seguinte forma: inicialmente, é criado um quadro com o tamanho de apenas um *slot*, representado de quadro L = 1. As etiquetas A, B e C vão transmitir todas nesse único *slot*, gerando obviamente uma colisão. O protocolo DFSA percebe então a necessidade de ajustar dinamicamente o quadro atual com base nas etiquetas que competiram por *slots* nesse quadro. Logo, é gerado um novo quadro com o tamanho de dois *slots* representado por L = 2; assim, apenas a etiqueta A é identificada com sucesso, de modo que e as demais geram uma colisão. Novamente, em uma nova transmissão, é gerado outro quadro, agora com o tamanho de três *slots*, formado por L = 3, no qual apenas a etiqueta B é identificada com sucesso e as demais geram uma colisão. Por fim, no último quadro, de tamanho L = 3 novamente, todas as etiquetas, A, B e C são identificadas com sucesso. O exemplo do protocolo DFSA pode ser visualizado na Figura 2.7.

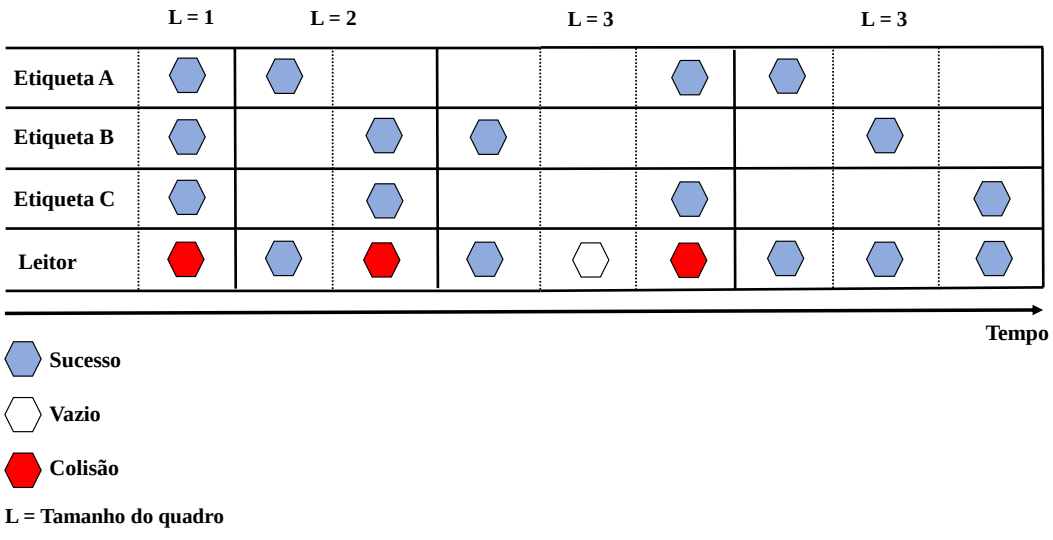

Figura 2.7: Transmissão no Dynamic framed slotted ALOHA.

Para o DFSA conseguir obter um bom desempenho no gerenciamento do novo quadro, é preciso primeiramente observar a quantidade de etiquetas que disputaram por *slots* no quadro anterior. Esse resultado é obtido através de algoritmos chamados de estimadores, os quais são capazes não somente de estimar, como também de gerar um próximo quadro, com o tamanho ideal para a quantidade de etiquetas que foram estimadas.

2.9 *EPCGlobal UHF Class-1 Gen-2* aplicado ao DFSA

A especificação do padrão *EPCglobal UHF Class 1 Generation 2* define os requisitos físicos obrigatórios de comunicação entre leitor e etiquetas. O protocolo anticolisão DFSA foi adotado pela norma *EPCglobal UHF Class-1 Gen-2* para resolver o problema de colisão de etiquetas passivas para sistemas RFID [Fraj et al. 2018]. Sua principal estratégia é permitir o ajuste dinâmico no tamanho do quadro a cada realização de ciclos de leitura durante o processo de identificação das etiquetas [Wu et al. 2018], [Tan et al. 2018] e [Yong et al. 2017]. Esse ajuste tem impacto significativo no desempenho do protocolo DFSA, que, por sua vez, está diretamente relacionado ao comprimento do quadro. Conforme já foi mencionado anteriormente, o leitor tem como funcionalidade coordenar o acesso ao meio e, assim, ajustar dinamicamente o comprimento do quadro a cada processo de identificação. No entanto, isso também depende da estimativa populacional das etiquetas que competem por *slots* em um quadro.

2.9.1 Funcionamento

Na implementação do DFSA, além do controle de acesso ao meio, existem alguns comandos definidos pela norma *EPCGlobal UHF Class-1 Gen-2* que auxiliam no processo de leitura das etiquetas. Por sua vez, esses comandos são divididos em duas formas de comunicação. Para a comunicação do leitor com as etiquetas, estão disponíveis os seguintes comandos: *Select*, para indicar um grupo de etiquetas que estão posicionadas dentro da área de leitura do leitor; *Query*, para identificar uma ou mais etiquetas; *QueryAdjust*, para ajustar o tamanho do superquadro atual; *QueryRep*, para avançar para o próximo *slot*; e *ACK*, para fins de confirmação. No que diz respeito às comunicações das etiquetas com o leitor, os comandos disponíveis são: *RN16*, para informar o *ID* de 16 bits da etiqueta; e *payload*, para transmitir os dados efetivos associados à etiqueta.

Primeiramente, no DFSA, o leitor inicia o processo de comunicação enviando uma transmissão em *broadcast* para identificar um determinado grupo de etiquetas que estão em seu raio de cobertura, enviando o comando *Select*. Logo em seguida, é enviado o co-

mando *Query*, para identificar as etiquetas que foram selecionadas anteriormente, o qual especifica um intervalo mínimo e máximo do número de etiquetas que estão relacionadas ao tamanho do quadro inicial. Esse quadro deve ser obrigatoriamente uma potência de 2. Portanto, quando uma etiqueta recebe um comando *Query*, ela gera um número aleatório de 16 bits (RN16) e extrai parte de um subconjunto de consultas *Q-bit*, resultando em um contador para responder a consulta. Esse contador é decrementado de menos 1, à medida que as etiquetas recebem um comando *QueryRep*. Por fim, quando esse contador chega a zero, a etiqueta envia seu *RN16*. Na verdade, o *ID* real de uma etiqueta é composto por 96 bits de EPC (dependendo da aplicação). Assim, o *RN16* pode ser considerado como um *ID* temporário, com o objetivo de reduzir a frequência de colisões. Após o envio do comando *Query*, o leitor passa a verificar os registros ocorridos em cada *slot* para uma possível recepção de comunicação *RN16*.

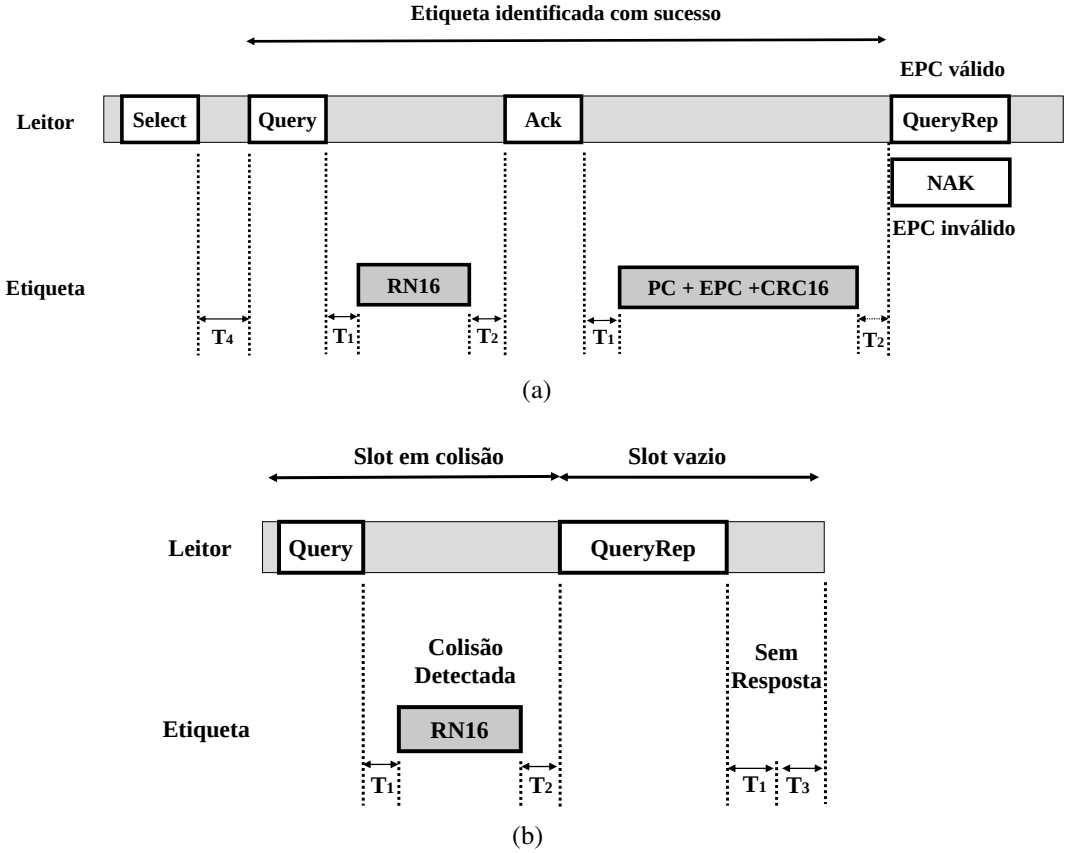

Figura 2.8: Possibilidades de respostas das etiquetas. (**a**) Resposta de um *slot* identificado com sucesso, e (**b**) Resposta de um *slot* em colisão e um *slot* vazio.

Para cada resposta das etiquetas ao *slot* de tempo, existem as seguintes possibilidades de transmissões: *slot* bem-sucedido, quando a etiqueta é identificada com sucesso; *slot*

em colisão, quando duas ou mais etiquetas competiram no mesmo slot de tempo; e *slot* vazio, quando não há transmissão (ver Figura 2.8a, b). Quando um *slot* ou etiqueta é identificado com sucesso, o leitor reconhece a etiqueta com um comando *ACK*. Em seguida, a etiqueta transmite seu EPC de 96 bits ao leitor. Se houver uma colisão de RN16, portanto, nenhuma etiqueta é identificada. O leitor, então, termina o *slot* de tempo de transmissão, verifica todos os *slots* de tempo do quadro 2^Q e inicia um novo ciclo de transmissões de consulta, agora com o novo Q atualizado.

2.10 Cenários de aplicações com RFID

A principal motivação para a utilização da tecnologia RFID vem da necessidade de obter informações de objetos em movimento, em locais insalubres ou em qualquer tipo de processo que impeça a utilização de código de barra. Atualmente, essa tecnologia tem ampla aplicabilidade em inúmeros setores industriais, de distribuição, de identificação e controle de acesso, possibilitando eficácia e eficiência.

Existem diversos cenários que podem utilizar os benefícios proporcionados pela tecnologia RFID. Entre eles, destacam-se o gerenciamento de logística e varejo, a manutenção de aeronaves, a autenticidade de produtos, e o controle de bagagens e saúde [Sun 2012], [Ding et al. 2018], [Song et al. 2016], [Zullig et al. 2017] e [Wang & Wang 2020].

Diversas organizações estão explorando o RFID em suas principais operações para alavancar os processos de automação e reduzir custos. Por exemplo, o grupo Walmart vem utilizando a tecnologia na cadeia de suprimentos, alcançando um eficiência operacional que possibilite a redução de custos. Com isso foi possível reduzir os problemas de logística operacional em 30% devido a utilização do sistema de RFID em sua cadeia produtiva [Ali 2012]. Throttleman resolveu problemas de restrições de espaço para armazenamento de objetos, identificando de forma ágil e fácil determinados itens que entram e saem dos estoques [Throttleman 2014]. O Metro Group obteve uma melhor gestão de controle e manipulação de materiais [Ali 2012]. já Cold Chain Logistics reduziu significativamente os danos causados por falhas nos contêineres frios, devido ao monitoramento ineficiente de temperatura interna [Emenike et al. 2016].

A Tabela 2.6 apresenta possíveis cenários de utilização da tecnologia RFID nos diversos segmentos, expondo como característica principal o número estimado de etiquetas por aplicação. Esse número pode variar de acordo com aplicabilidade em questão.

Tabela 2.6: Cenários de aplicações da tecnologia RFID.

Atividades	**Aplicação**	**Quantidade de etiquetas**
Varejo [Ali 2012]	• Redução na montagem de paletes; • Automatização de processos; • Aumento de produtividade; • Eliminação do código de barras; • Eficiência no monitoramento de produtos; • Disponibilidade de informações do produto.	Centenas
Vestuário [Throttleman 2014]	• Redução de roubo de produtos; • Redução no tempo de estoque; • Precisão de taxa de leitura de 99%; • Problemas de armazenamento solucionados.	Milhares
Logística [Emenike et al. 2016]	• Aumento das exportações de alimentos; • Monitoramento de contêiner em tempo real; • Rastreamento do produto até o cliente final; • Redução de produtos danificados.	Dezenas
Indústria 4.0 [Fernández-Caramés & Fraga-Lamas 2018]	• Melhoria no processo de identificação; • Rastreabilidade de peças e equipamentos; • Benefícios no processo de fabricação; • Segurança de produtos.	Milhares
Agricultura [Wang & Wang 2020]	• Rastreamento e rotulagem de transgênicos; • Gerenciamento do plantio; • Controle de pragas; • Logística de produtos agrícolas.	Milhares

2.11 Canais ruidosos

Ambientes industriais são constituídos por diversos tipos de dispositivos eletrônicos, os quais são fontes diretas de algumas interferências eletromagnéticas que podem pro-

duzir falhas de comunicação. Na verdade, tal interferência pode comprometer o recebimento dos pacotes na rede, resultando consequentemente em seu descarte e prejudicando o processo de leitura das etiquetas. Portanto, esse tipo de falha apresenta um impacto significativo nos sistemas baseados em RFID, o que tem exigido um planejamento cada vez mais eficiente de topologia da rede, garantias de redundância e robustez para aplicações de segmentos industriais.

2.11.1 Falhas

De modo geral, uma falha (*fault*) é compreendida por uma ação em que pode resultar como consequência um erro. Quando uma falha está em plena atividade, ela pode levar a um erro, do contrário, ela está de prontidão. No contexto baseado em sistemas RFID, as falhas podem acontecer por diversos fatores, como mau funcionamento do hardware (podendo ser mais evidente em ambientes críticos como plantas industriais), surtos de interferência eletromagnética e *bugs* de *software*.

A presença de falhas nos dispositivos ou canais de comunicação podem produzir uma falha temporária (transiente) ou permanente [Laprie 1995]. Essas falhas podem conduzir a diferentes situações de erro, impactando de forma alterada a qualidade do serviço, o que é percebido nas aplicações [Pradhan 1996]. Em suma, as falhas esperadas podem ser classificadas da seguinte forma:

- Transiente: quando a falha possui um tempo de duração limitado, resultante de um mau funcionamento temporário ou de uma interferência externa temporária;
- Intermitente: uma falha que tem como duração um curto período de tempo, mas repetidamente;
- Permanente: essas falhas têm longa duração, com profundo impacto no funcionamento de um sistema.

Será abordado como o foco de pesquisa desta tese o uso de falhas transientes, as quais prejudicam diretamente o canal de comunicação entre os dispositivos envolvidos por um curto intervalo de tempo, tendo como representação em milissegundos (ms) [Willig et al. 2002]. Esse tipo de falha pode ser provocado por diversas fontes de interferências eletromagnéticas ou ruídos ocasionados pelo ambiente aplicado.

2.11.2 Erros

Erro é um conceito básico e fundamental que se aplica diretamente na análise de confiabilidade, o qual serve para identificar o mau funcionamento por parte da aplicação.

Erros, no geral, podem levar a defeitos, entretanto, sua causa pode levar a falhas [da Silva 2013]. Os defeitos são percebidos, de fato, quando os erros são espalhados por todo o sistema.

Em sistemas de RFID, erro pode se relacionar com falha e defeito, como, por exemplo, durante a transmissão de um pacote enviado de um leitor para uma etiqueta. No determinado instante de transmissão, houve uma interferência eletromagnética que provocou uma falha, alterando-se, em consequência disso, parte do pacote enviado (erro). Consequentemente, a etiqueta não foi capaz de entender o sinal que lhe foi enviado e simplesmente não responde ao leitor, que deixa de identificar tal objeto (defeito).

No contexto desta tese, todos os erros são percebidos durante transmissão e/ou recepção de pacotes entre leitor e etiqueta RFID, através do uso de mensagens de controle pelos próprios protocolos anticolisão de etiquetas.

2.11.3 Defeito

Um sistema pode apresentar defeito quando não consegue ser capaz de fornecer um serviço de forma correta, ou seja, a finalidade do serviço se desvia da especificação imposta pelo sistema. O defeito é o acontecimento que causa a mudança de estado do serviço de um sistema de correto para incorreto, como, por exemplo, uma atividade que não implementa a especificação do sistema. O defeito somente ocorre quando um erro existente no sistema se espalha internamente, chegando a ser percebido pelo usuário da aplicação.

Defeitos podem até ser tolerados, mas devem ser evitados, para que o sistema não apresente defeitos. É possível que os defeitos sejam evitáveis, utilizando métodos de tolerância a falhas [Weber 2002].

De acordo com [Avizienis et al. 2004], o domínio dos defeitos é classificado por três principais categorias:

- Defeitos em relação à informação: dados transmitidos estão fora da especificação prevista.
- Defeitos quanto ao tempo: a temporização do serviço é desviada da especificação prevista (mais rápida ou mais lenta).
- Defeitos híbridos (informação e tempo): nenhum serviço é completado ou, caso seja, desvia-se da especificação prevista.

2.11.4 Confiabilidade

Confiabilidade é um conceito que está diretamente relacionado com o termo dependabilidade. De forma geral, pode ser definida como a capacidade de um sistema (elementos) de atender uma especificação dentro de condições predefinidas, durante um intervalo de tempo (t) e condicionado a estar operacional nesse período. [Avizienis et al. 2004]. A Equação 2.1 tem como representação a confiabilidade R(t), que é igual à probabilidade de ocorrência de defeitos até um determinado instante (t), uma variável aleatória (T) que simboliza o tempo de ocorrência de defeitos no sistema e (F) corresponde uma função distribuída acumulativa de ocorrência de falhas no sistema [Kuo & Zuo 2003].

$$R(t) = P(T > t) = 1 - F(t) \tag{2.1}$$

Para se atingir um nível acurado de confiabilidade, é necessária a utilização combinada de conceitos específicos, que auxiliam na evolução para se ter um sistema confiável [Avizienis et al. 2004], como, por exemplo, o uso do método de tolerância a falhas em conjunto com outras técnicas, como prevenção de falhas, remoção de falhas e previsão de falhas. A seguir, será descrito o papel de cada técnica citada.

Prevenção de falhas tem como principal funcionalidade atuar para prevenir a ocorrência ou a adição de falhas. A prevenção de falhas pode ser abordada durante etapas de especificação do projeto, escolha da metodologia correta, seleção dos componentes adequados e operação no uso do sistema. Porém, é preciso enfatizar que essa técnica não evita completamente todas as possíveis ameaças de falhas. Na verdade, é quase impossível assegurar que um sistema não apresente falhas [Portugal 2004].

Tolerância a falhas é um conceito que possui como características formas de evitar defeitos, mesmo que haja existência de falhas. Para que seja possível cumprir o seu papel, é preciso o uso de duas outras técnicas em conjunto, sendo primeiramente necessário identificar o erro, com a técnica de detecção de erros, e, na sequência, a correção do problema, com o método de recuperação de sistema.

Remoção de falhas apresenta como propósito reduzir o número ou a severidade de falhas durante etapas de evolução e manipulação do sistema. Em meio à evolução, a remoção de falhas é dividida em três metodologias: verificação, diagnóstico e correção. Por outro lado, já na fase operacional, a remoção de falhas é assegurada pela realização de manutenção dos elementos envolvidos.

Por fim, o método de **Previsão de falhas** tem por objetivo principal a realização de uma análise comportamental do sistema em relação à ocorrência e à ativação de falhas.

Essa análise pode ser feita de duas formas: qualitativa, buscando identificar, categorizar e ordenar por relevância os motivos do defeito no sistema, e quantitativa, que mensura os termos probabilísticos referentes aos atributos da dependabilidade do sistema.

No contexto de RFID, alguns métodos são utilizados para aumentar a confiabilidade das comunicações. Uma vez que todas as transmissões de dados precisam ser confirmadas, as etiquetas que não estão respondendo adequadamente podem ser identificadas e, com isso, novas leituras são necessárias [EPCGlobal 2013]. No entanto, esse atraso no processo de leitura geral também pode comprometer a eficiência de um sistema baseado em RFID.

Para garantir a confiabilidade, o sistema deve ser capaz de continuar operando corretamente. Em outras palavras, é esperado que uma etiqueta possa ser lida independentemente da situação atual do canal, mesmo após algum atraso. Na verdade, se uma etiqueta está sendo lida por um leitor que não está recebendo os dados solicitados, é possível que o sistema esteja apresentando uma falha temporária. Em geral, essas falhas podem produzir diferentes condições de erro, impactando de forma deficiente na qualidade percebida nas aplicações [Pradhan 1996].

2.11.5 Desempenho

Um problema crítico que afeta o desempenho dos sistemas RFID é a leitura de várias etiquetas. Na verdade, os leitores podem realizar uma série de leituras sucessivas durante um curto intervalo de tempo. No entanto, uma vez que as falhas podem acontecer de forma imprevisível, tais leituras sucessivas podem ser prejudicadas por ocorrência de falhas, que são responsáveis pelo dispêndio de recursos adicionais, aumentando os atrasos de leitura, e pela degradação geral do desempenho [Wu et al. 2013]. Portanto, confiabilidade e desempenho são conceitos bem relacionados.

Para minimizar os problemas de colisões, os leitores RFID implementam algum mecanismo anticolisão de etiqueta [Wang et al. 2012]. Em cenários como de ambientes industriais, exige-se cada vez mais um desempenho acurado de todas as tecnologias envolvidas, especialmente no tratamento de colisões em sistemas RFID, pois esses mecanismos definem o desempenho da tecnologia.

Os parâmetros utilizados pelos algoritmos anticolisão de etiquetas para medir o desempenho são, de fato, grandes desafios, devido à heterogeneidade de técnicas adotadas por diferentes autores, além da diversidade de características e requisitos dos mais distintos cenários de aplicações. Assim, a análise de desempenho dos algoritmos anticolisão para RFID baseia-se em quatro principais categorias de métricas, como: *slots*, tempo,

tráfego e precisão. Todos esses parâmetros são considerados para a avaliação de confiabilidade e desempenho desta tese.

- **Slots -** É a mais comum na literatura, sendo realizada por contabilizar o número de *slots* alocados.
- **Tempo -** Visa medir os diversos tempos gasto no processo de identificação em algumas situações é dependente dos *hardwares* utilizados (leitores e etiquetas).
- **Tráfego -** Essa métrica tem como objetivo contabilizar as transmissões de pacotes entre o leitor e a etiqueta durante o processo de identificação.
- **Precisão -** É usado quando se deseja estimar com precisão o número de etiquetas de acordo com o tamanho dos quadros.

Uma metodologia bastante utilizada para mensurar a avaliação de desempenho em sistemas RFID refere-se à taxa de transferência (Throughput), ou seja, à capacidade que as etiquetas possuem em responder ao leitor através do envio de seus dados toda vez em que for solicitado por ele. Essa métrica está representada pela Equação 5.1, em que taxa de transferência T_{hput} é igual ao número de *slots* bem-sucedidos N_{Ss} sobre o número total de *slots* consumidos (número de *slots* bem-sucedidos, N_{Ss}, número de *slots* em colisão, N_{Cs}, e número de *slots* vazio, N_{Es}). Porém, vale pontuar que a métrica descrita corresponde ao desempenho do sistema, resultando em um canal de comunicação livre de erros.

$$T_{hput} = \frac{N_{Ss}}{N_{Ss} + N_{Cs} + N_{Es}} \tag{2.2}$$

2.12 Modelagem baseada em GSPN

O modelo de avaliação de sistemas deve garantir dois principais requisitos: a representação comportamental do sistema de forma bastante rígida e a possibilidade de avaliação completa, utilizando como atributo fundamental a confiabilidade durante o seu funcionamento [Portugal 2004]. Para isso, seu desenvolvimento ocorre a partir do conjunto de características funcionais voltadas para a possibilidade de ocorrência das falhas e respectivas consequências, como comprometimento gradativo no desempenho da aplicação. Diante disso, o modelo representa a atuação do sistema em situação de ocorrência de falhas, que repercutem no funcionamento de todos os seus elementos. No entanto, a partir do modelo criado, são colocados em prática métodos apropriados, os quais permitem extrair medidas de confiabilidade de interesse.

As particularidades para adoção do modelo têm como resultado a utilização do formalismo na modelagem durante o processo de desenvolvimento. O formalismo matemático tem como característica essencial a capacidade de modelar comportamentos, desde que não se apresente alguma restrição, como tipo de medidas que não podem ser adquiridas. Entretanto, é corrente o uso de comportamento estocástico por parte do sistema, o que pode resultar na dependência de outros processos com característica estocástica. Esses podem se apresentar de forma externa ao sistema, como é o caso de correções, ou de maneira interna, que ocorre normalmente durante o funcionamento geral do sistema.

Um método eficiente de representar confiabilidade de sistemas complexos é o uso de modelo de estados. Possui como característica principal a representação do comportamento de sistema através do uso de um conjunto de estados e eventos que estabelecem transações entre eles. Essas transações utilizam valores representativos de probabilidades, taxas ou funções de distribuição [Dantas et al. 2012]. Esse modelo pode reproduzir sistemas complexos, com dependência de uso de subsistemas e restrição de recursos, apresentando relações bem definidas a partir do estado do sistema. A seguir, será discutido o conceito de Redes de Petri Estocásticas Generalizadas (GSPN) e suas variações.

2.12.1 Redes de Petri Estocásticas Generalizadas (GSPN)

Redes de Petri (PN) são ferramentas gráficas e matemáticas que permitem realizar modelagem formal e análise de sistemas dinâmicos [Murata 1989]. Para tanto, elas manipulam eventos seguindo algumas regras predefinidas, considerando que os *eventos* são modelados por transições e que as *regras* são arcos direcionados a locais marcados. Para esse formalismo, quando características probabilísticas são adicionadas aos eventos, a Rede de Petri resultante é referida como Redes de Petri Estocásticas Generalizadas (GSPN).

O conceito de GSPN pode ser definido como uma extensão do formalismo das Redes de Petri, acrescentando possibilidade de utilizar transições temporizadas e imediatas para representar o mesmo problema. Com isso, é possível adicionar ainda mais recursos à Rede de Petri, mantendo a sua característica de realizar análise comportamental de sistemas e avaliação de desempenho, que permite, através de detalhes temporais, o desenvolvimento de modelos formais probabilísticos [Marsan et al. 1995].

Uma Rede GSPN possui os mesmos elementos que o modelo de Rede de Petri (PN) convencional (não temporizada), representados graficamente por: lugares (círculos), transições (retângulos), arcos direcionados (setas) e *tokens* (círculos fechados ou setas) [Marsan et al. 1995] [Murata 1989]. Lugares (círculos) corresponde a uma variável que armazena

temporariamente os estados do sistema modelado. Já os estados têm como característica a representação dos elementos conhecidos como *tokens*. A marcação de um lugar é a identificação do seu estado, podendo está vazio ou não, sendo possível uma mudança de estado quando se adicionam ou retiram *tokens*. Assim, essa mudança é conhecida como transição de estados. A Figura 2.9 (a), (b), (c), (d) e (e) apresenta os principais elementos básicos que formam uma rede GSPN.

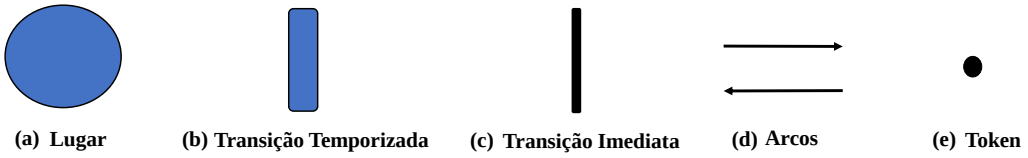

Figura 2.9: Rede GSPN - Elementos básicos

Uma transição corresponde como agente atuante sobre os estados. Para que seja possível uma mudança de estado, é necessário que os elementos estejam conectados de alguma forma, o que indica o conceito de rede. Essas conexões são realizadas por meio de arcos direcionados, que associam os vértices (lugares e transações) a regras pré ou pós-definidas, oportunizando a existência de uma ação. Porém, nesse caso, uma transição pode ser representada de duas formas. A primeira consiste em transição temporizada, sendo simbolizada por um retângulo (*t1*), e a segunda é composta por uma transição imediata, que dispara quando se torna habilitada, simbolizada por uma linha (*t1*), conforme descrita pela Figura 2.10(a) e (b).

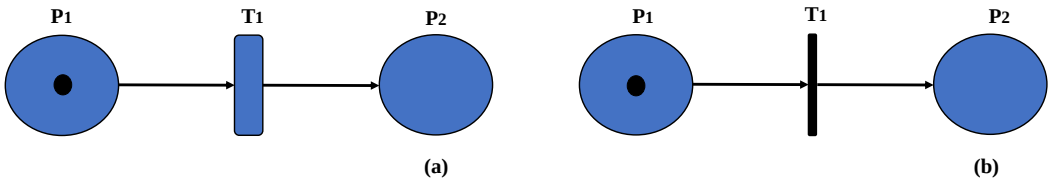

Figura 2.10: Exemplo de transição em GSPN. (**a**) Transição temporizada, e (**b**) Transição imediata.

A transição temporizada é denotada por um retângulo na Figura 2.10 (a) e possui uma característica temporal recebida de uma variável aleatória com distribuição exponencial. Nessa situação, as transições disparam certo tempo após sua habilitação e somente nesse ponto é removida a marca do lugar de entrada, destinando-se para o lugar de saída. Como esses disparos são eventos estocásticos, seu tempo de atuação ocorre de forma contínua. Com isso, a probabilidade de haver dois disparos de forma simultânea é zero, ou seja,

inexistente. Desse modo, se houver situação na qual ocorra conflito por disputa de *tokens* nas transições, imediatamente, será solucionado de forma a priorizar as transições que tenham o menor tempo de disparo.

Um aspecto interessante que pode ser considerado é que o modelo GSPN mantém uma configuração não determinística como principal característica, tornando-se uma interessante solução para a análise de comportamento no contexto de aplicações com problemas reais. Portanto, essa particularidade estocástica transforma-se em uma opção para a resolução de problemas cotidianos, nos quais uma abordagem determinística apresenta tal limitação em avaliar o comportamento de sistemas dinâmicos.

O grau de habilitação de uma transição é representado como importante característica em redes GSPN. Esse atributo corresponde diretamente à possibilidade de diversos *tokens* habilitarem uma transição, tendo como resultado um cenário com vários disparos concomitantes. Diante disso, a semântica de disparo levará em consideração o número de *tokens* que podem ser disparados simultaneamente. Segundo [Marsan et al. 1995], as possibilidades de semânticas oportunizadas são:

- *Exclusive Server:* a transição dispara em série, ou seja, somente depois de um disparo ela se torna habilitada novamente, emancipando-se do grau da transição;
- *Infinite Server:* uma única habilitação de uma transição suporta a transferência de infinitos *tokens* de forma simultânea;
- *Multiple Server:* o grupo completo de *tokens* será computado de maneira paralela, até que se atinga o limiar máximo permitido do grau de paralelismo, sendo representado por *k-tokens* e definido por essa semântica.

Considerando a existência de uma situação de transição imediata habilitada para o disparo, pode-se afirmar que sua marcação corresponde a não tangível (*vanishing*). Em consequência desse aspecto, todas as transições temporizadas permanecem desabilitadas, para que a imediata seja por padrão, priorizada pelo fato de não ter custo de tempo. No entanto, não existindo nenhuma transição imediata habilitada, pode-se classificar essas marcações como sendo tangíveis *(tangible)*, que têm como prioridade no disparo quem de fato apresentar o menor tempo.

2.12.2 Representação formal GSPN

De acordo com [Marsan et al. 1995], o modelo GSPN pode ser representado formalmente por uma 8-tupla, sendo descrito da seguinte forma:

$M_{GSPN} = (P, T, \Pi, I, O, H, W, M_o)$, tal que:

- P é composto por um conjunto finito dos lugares, onde $P = p_1, p_2, ..., p_n$;
- T é com por um conjunto finito de transições, onde $T = t_1, t_2, ..., t_n$;
- $\Pi : T \longrightarrow$ N corresponde a uma função de prioridade que mapeia uma transição imediata a um número natural que representa a sua prioridade;
- I $\subseteq$ (P x T) corresponde a um conjunto de arcos que marca relação de fluxo de entrada;
- O $\subseteq$ (T x P) corresponde a um conjunto de arcos que marca relação de fluxo de saída;
- H : P x T $\longrightarrow$ N representa a função estrutural dos arcos inibidores;
- W : T $\longrightarrow R^+$ é a função que realiza o mapeamento de uma transição para uma função real positiva, com imagem no conjunto dos números reais;
- M_o : P $\longrightarrow$ Representa a marcação inicial dos lugares.

Neste trabalho, os modelos propostos para a avaliação de confiabilidade e desempenho em sistemas RFID têm como finalidade utilizar o modelo GSPN, com o intuito de obter métricas para os resultados a partir de simulações e análise em estado estacionário e transiente, baseados na Cadeia de Markov embutida no modelo. Portanto, algumas descrições práticas desse formalismo são oportunizadas para representar um problema real, as quais serão consideradas no Capítulo 4.

2.12.3 Ferramenta de Modelagem - Möbius

O Möbius é uma ferramenta de software com finalidade de modelar o comportamento de sistemas complexos. Embora tenha sido originalmente desenvolvido para analisar confiabilidade, disponibilidade e desempenho de sistemas computacionais e rede, seu uso se expandiu para diversas outras áreas, incluindo uma ampla gama de sistemas de eventos discretos, desde reações bioquímicas dentro de genes até os efeitos de invasores maliciosos em sistemas seguros, além dos aplicativos originais [Sanders 2005].

Essa heterogeneidade de uso é possível devido à flexibilidade e à capacidade disponíveis no Möbius, que contém suporte para vários tipos de formalismos, com modelagem de alto nível e diversas técnicas de soluções. Essa versatilidade permite que engenheiros e cientistas representem seus sistemas em linguagens de modelagem apropriadas para seus domínios de problema e, com isso, resolvam os problemas de forma precisa e eficiente, usando as técnicas de solução mais adequadas ao tamanho e à complexidade dos sistemas [Daly et al. 2000]. Simulação de eventos discretos com eficiência de tempo e espaço e solução numérica, baseada em processos de Markov, são atributos importantes suportados pela ferramenta.

Devido às inúmeras possibilidades de representações de modelagem para sistemas complexos fornecidos pelo Möbius, serão apenas descritos a seguir os atributos que foram utilizados para atender as expectativas de desenvolvimento desta tese.

2.12.4 Modelo Atômico - SAN

Redes de atividade estocástica (SANs) são extensões estocásticas para Redes de Petri. Elas utilizam primitivas gráficas para fornecer um formalismo de modelagem com alto nível, criando modelos detalhados de desempenho e confiabilidade que podem ser especificados de forma simples.

As SANs são compostas de quatro objetos primitivos básicos, sendo eles: locais, transições, entrada e saída de *tokens*. As transições representam ações do sistema modelado e são divididas em temporizada, com característica temporal, e instantânea, que entra em atividade quando se torna habilitada. Os locais representam o estado do sistema modelado. As entradas são usadas para controlar a habilitação de atividades e, por fim, as saídas, para alterar o estado do sistema quando uma atividade é concluída. A Figura 2.11 detalha um exemplo desse modelo.

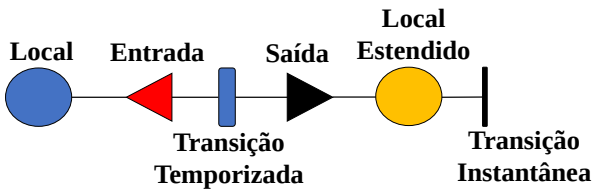

Figura 2.11: Elementos do modelo SAN.

2.12.5 Modelo Composto

A ferramenta Möbius permite a construção de modelos compostos a partir de modelos previamente definidos. Com isso, é possível adotar uma abordagem hierárquica para modelagem, construindo submodelos como unidades significativas e, em seguida, combinando-os de maneira bem definida para construir um modelo de um sistema maior. No entanto, às vezes, é usado como técnica conveniente para tornar o modelo modular mais simples de desenvolver. Em outras palavras, as formas como os modelos são compostos podem levar à eficiência no processo de solução.

O método composto utiliza uma abordagem de compartilhamento de estado. Nessa abordagem, os submodelos são vinculados por meio de sobreposição, ou seja, pelo com-

partilhamento de variáveis de estado correspondentes, incluindo apenas uma única variável de estado para cada submodelo. Isso permite que os submodelos interajam de modo que cada um deles possa efetuar operações nas variáveis de estado compartilhadas. Qualquer gravação realizada na variável de estado compartilhada estará, consequentemente, disponível para todos os submodelos que contêm essa variável de estado. Por exemplo, é possível conectar dois modelos SAN, fazendo com que eles tenham um determinado lugar em comum, conforme evidenciado pela Figura 4.3.

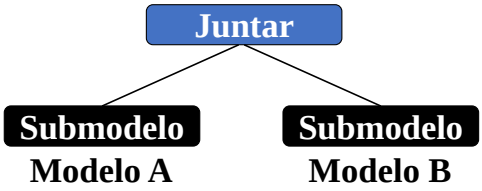

Figura 2.12: Exemplo do modelo composto.

A Figura 4.3 apresenta um nó de união que interliga outros dois submodelos, indicando a existência de um relacionamento de compartilhamento entre ambos. Isso significa que um modelo composto também é um modelo em si e, portanto, pode ser fundido posteriormente com outros submodelos para produzir modelos maiores e otimizados.

2.12.6 Modelo de Recompensa

Os formalismos de recompensa definem funções que medem informações sobre o sistema que está sendo modelado. No geral, as variáveis de desempenho são utilizadas para avaliar o desempenho do sistema através de métricas bem definidas, fatores importantes que determinam na prática a qualidade do sistema em questão. Para especificar essas variáveis, o Möbius possui alguns atributos, que são: submodelos, recompensa de taxa, recompensa de impulso, tempo e simulação.

- Submodelos: quando existe N instâncias para o submodelo selecionado no modelo de nível superior, a função de recompensa será avaliada N vezes. Para alguns tipos de funções de recompensa, é desejável dividir a função de recompensa pelo número de instâncias no modelo, de modo que a recompensa represente a média das N instâncias.
- Recompensa de taxa: é usada para definir recompensas com base no tempo em cada estado, sendo implementada em código C++, que deve terminar com uma instrução de retorno ao valor da função.

- Recompensa de impulso: define as funções de recompensa que são avaliadas quando as ações no modelo filho são disparadas. Podem ser facilmente usadas para contar o número de vezes que uma ação é disparada durante um intervalo de tempo.
- Tempo: esse parâmetro define os tipos de resultados a serem mensurados para os tempos de interesses específicos.
- Simulação: é usada para definir dois aspectos das variáveis de recompensa que são exclusivos da simulação: estimativa de variável e definição de intervalo de confiança.

2.12.7 Modelo de Estudo

O modelo de estudo permite examinar o efeito de vários parâmetros (variáveis globais) no desempenho do sistema. Em um modelo de estudo, um ou mais experimentos podem ser definidos com base nos diferentes valores que os parâmetros podem assumir. Mais precisamente, um experimento é uma tupla com valores de parâmetros para os quais um modelo pode ser resolvido.

O parâmetro intervalo de estudo permite que cada variável global seja atribuída a um valor fixo ou a um intervalo de valores. Em um intervalo de valores representativos, os experimentos são criados automaticamente pelo Möbius como o produto vetorial de todos os valores possíveis que as variáveis globais podem assumir. Por exemplo, se houver duas variáveis globais, cada uma com intervalo de seis valores atribuídos, o estudo será composto ao todo por 36 experimentos.

2.12.8 Modelo de Simulação

O modulo simulador é utilizado para testar e validar modelos desenvolvidos, usando como procedimento a simulação de eventos discretos. Ele realiza uma avaliação do modelo utilizado juntamente com parâmetros especificados pelo modelo estudo, o qual vincula as suas bibliotecas à biblioteca do simulador e realiza o processo de execução. O simulador pode ser utilizado para tratar qualquer modelo especificado no Möbius e tem potencial para analisar modelos com estados transitórios ou estáveis.

A simulação fornece soluções estatisticamente precisas dentro de um intervalo de confiança especificável pelo usuário. Os parâmetros de simulação podem ser divididos em quatro subcategorias, a saber:

- **Seleção de estudo e experimento**: escolhe quais são os experimentos que serão avaliados;

- **Parâmetros de execução de simulação**: corresponde ao uso de atribuições predefinidas durante o processo de simulação;
- **Opções de compilação**: controla como a simulação é compilada e executada, permitindo otimizações, saída de rastreamento e especificação do nome da execução.
- **Caixas de seleção**: controla a saída do simulador, gerando arquivos que contém os resultados.

Capítulo 3

Trabalhos Relacionados

Este capítulo tem como propósito fundamental apresentar as metodologias dos trabalhos relacionados, destacando suas principais contribuições de pesquisa. No geral, para garantir qualidade nas diversas aplicações oferecidas pela tecnologia RFID, é preciso apresentar um nível satisfatório de confiabilidade e desempenho, tornando viável sua utilização prática nos mais diversos segmentos industriais.

Tradicionalmente, diversas soluções industriais têm sido desenvolvidas para explorar o uso de tecnologias de comunicação com fio [Cairó et al. 2018]. No entanto, com o aumento do número aplicações, vem ocorrendo uma migração para opções de infraestruturas que utilizam padrões de comunicação sem fio, visando obter benefícios como redução de custos e larga escalabilidade. Nesse contexto, o desafio tem sido fornecer o mesmo nível de confiabilidade e desempenho antes garantidos em conexões com fio, mesmo quando todas as comunicações passam a ser sem fio.

Porém, a existência de maiores probabilidades de erro em comunicações sem fio dificulta a garantia da confiabilidade do sistema [Cheng et al. 2011, Abdelgawad & Bayoumi 2011], gerando questionamentos sobre a usabilidade em aplicações industriais. Além disso, a presença de desempenho abaixo do esperado pode ser levada em consideração, quando comparada às conexões com fio, podendo reduzir o desempenho dos sistemas [Avizienis et al. 2004]. Então, esse cenário adverso demanda o surgimento de novas soluções para melhorar a qualidade de forma geral das aplicações industriais sem fio.

Este trabalho tem como abordagem principal desenvolver uma modelagem capaz de avaliar questões de confiabilidade com parâmetros de desempenho, sendo processados de forma conjunta para analisar o comportamento de sistemas RFID. No geral, foi realizada uma análise abrangente na literatura, em busca de trabalhos de pesquisa que pudessem contribuir com essa investigação. Embora a proposta [Filho et al. 2018] não tenha sido abordada anteriormente, trabalhos de pesquisa cobrindo questões de dependabilidade, confiabilidade e avaliação na qualidade em comunicações sem fio podem trazer

contribuições importantes para as discussões e definições nesta tese.

As comunicações em sistemas RFID têm sido bastante exploradas há algum tempo, com diversas contribuições interessantes surgindo nos últimos anos [Su, Sheng, Leung & Chen 2019]. No entanto, para o contexto operacional de comunicação RFID, serão analisados em particular os possíveis erros de transmissão e como eles são tratados por protocolos e algoritmos anticolisão [Zhu & Yum 2011]. Alguns trabalhos associados a essas temáticas são apresentados e comparados durante esta seção.

O trabalho de [Solic et al. 2017] teve como proposta a utilização do conceito de rádio definido por *software* (SDR), para modelar a operação RFID em diferentes cenários. Os autores tiveram como objetivo avaliar o quanto de energia era necessário para ativar uma etiqueta passiva RFID.

Com o auxílio de parâmetros estatísticos, o desempenho no processo de leitura das etiquetas foi aprimorado. O trabalho de [Vogt 2002] propôs uma função de estimativa baseada em distância mínima, para gerenciar o número de leituras das etiquetas. Neste trabalho, o processo de leitura é estimado com base em uma Cadeia de Markov, visando o cálculo do tamanho de quadro mais adequado para um grupo de etiquetas não lidas.

[Chen 2014] propôs um algoritmo de fácil implementação para sistemas com limitação de recursos computacionais. A ideia era obter um nível de desempenho satisfatório considerando as restrições impostas pelo *hardware*. Para atender tal demanda, o autor abordou o fator de leitura, propondo um algoritmo anticolisão simples baseado em estimativas de erro.

O problema de colisões em sistemas RFID foi analisado por diferentes formas. Em [Su, Sheng, Liu, Han & Chen 2019], os autores propuseram uma nova estratégia para gerenciar a ocorrência de colisões em comunicações RFID, conhecida como algoritmo de divisão binária baseado em grupos. Esse método reduz o número de colisões ao dividir as etiquetas em um grupo com vários subconjuntos, permitindo, então, um processo de leitura mais coordenado.

Já os autores [Su et al. 2020] consideram que é possível reduzir o número de colisões através do uso de um protocolo baseado em árvore de consulta especializada. A ideia é separar as etiquetas que colidiram em subgrupos menores, permitindo uma leitura mais eficiente na continuidade do processo. Além disso, os autores propuseram um mecanismo chamado prefixo duplo, o qual apresenta a possibilidade de que várias etiquetas pudessem responder no mesmo intervalo de tempo.

As probabilidades de erro foram exploradas por [Xuan & Li 2019], que consideraram o tempo de duração dos *slots* de tempo em colisão e vazios para melhorar o desempenho do sistema. O objetivo era otimizar o número de leituras em um tempo menor. Abor-

dando o mesmo contexto, porém, de forma diferente, um novo algoritmo foi proposto em [Abbasiana & Safkhani 2020], baseado no protocolo ALOHA, permitindo a identificação de informações úteis mesmo em *slots* que apresentaram colisão. De forma similar, o trabalho em [Zhao et al. 2019] propôs um método que realiza transmissões intermitentes, ajustando diversas vezes o tamanho dos quadros.

Outras áreas de pesquisa relevantes também foram abordadas em trabalhos anteriores. Os autores [Munir et al. 2018] realizaram uma análise do impacto proporcionado por interferência externa, que afeta o sinal refletido (da etiqueta retornando ao leitor). Fazendo isso, esse estudo mensura o nível de comprometimento que tal interferência pode produzir na confiabilidade dos protocolos anticolisão. A interferência também foi considerada em [Valentini et al. 2020], que investigou o impacto do ambiente de propagação subjacente e o efeito de captura para leituras de etiquetas.

Em [Benedetti et al. 2019], vários leitores foram considerados juntamente com técnicas de redundância para gerenciar de maneira eficiente a carga de leitura das etiquetas RFID. Desse modo, por existir um padrão de transmissão redundante, eventuais colisões são compensadas pela divisão dos fluxos de transmissão, garantindo ainda um bom nível de confiabilidade ao sistema. O trabalho de [Xie et al. 2019] também explorou a redundância de etiquetas, mas anexando várias delas em objetos de leitura única. No entanto, o tempo total de identificação também pode ser multiplicado, devido ao aumento do número de etiquetas.

Além disso, a confiabilidade e o desempenho tiveram a possibilidade de serem aprimorados de outras formas. Em [Li et al. 2020], os autores propuseram o uso de múltiplas antenas RFID pelo leitor. Tais antenas podem se adaptar ao cenário de leitura atual, permitindo a identificação simultânea das etiquetas, embora haja algumas complexidades nesse processo. A pesquisa de [Zhang et al. 2020], de forma diferente, empregou um algoritmo para detectar etiquetas ausentes, utilizando filtros especializados. Para diminuir o número de etiquetas com informações falso positivas, os autores utilizam uma combinação de amostragem e *multi-hash* para relatar a presença das etiquetas, melhorando a probabilidade de detecção.

A Tabela 3.1 resume os trabalhos citados, destacando suas principais contribuições de pesquisa. Na verdade, os trabalhos destacados na Tabela 3.1 apresentam contribuições importantes quando abordam os requisitos de confiabilidade e desempenho em comunicações RFID. No entanto, todos eles consideram sempre que o canal de comunicação utilizado é livre de erros, o que na prática é uma suposição irreal. Portanto, esta tese propõe um novo algoritmo anticolisão que utiliza um modelo formal baseado em GSPN com cenários de falhas no canal de comunicação. Este modelo, suporta diferentes análises

dos algoritmos anticolisão baseados em DFSA ao realizar múltiplas leituras de etiquetas passivas, beneficiando os novos desenvolvimentos de pesquisa nessa área.

Tabela 3.1: Pesquisas voltadas para RFID que avaliam o desempenho e a confiabilidade.

Trabalhos	**Desempenho**	**Análise de Falhas**
[Solic et al. 2017]	*X*	
[Zhao et al. 2019]		*X*
[Munir et al. 2018]		*X*
[Su, Sheng, Liu, Han & Chen 2019]	*X*	
[Vogt 2002]	*X*	
[Chen 2014]	*X*	
[Barros Filho et al. [2018]	*X*	
[Benedetti et al. 2019]		*X*
[Xie et al. 2019]		*X*
[Li et al. 2020]		*X*
[Su et al. 2020]	*X*	
[Zhang et al. 2020]		*X*
[Xuan & Li 2019]	*X*	
[Abbasiana & Safkhani 2020]	*X*	
[Valentini et al. 2020]		*X*
Proposta	*X*	*X*

Capítulo 4

Proposta

Este capítulo apresenta como proposta um algoritmo anticolisão para resolver problemas de acesso ao meio, utilizando o modelo desenvolvido baseado em GSPN para avaliar a confiabilidade e o desempenho em protocolos DFSA para RFID. O modelo contribui na prática com simulações mais precisas, pois não ignora a ocorrência de possíveis falhas transitórias no canal de comunicação durante as transmissões. Sendo assim, é possível adotar um planejamento mais aprimorado para se implementar aplicações RFID em qualquer segmento industrial.

4.1 Algoritmo Proposto

O algoritmo anticolisão proposto é apresentado na Figura 4.1. Inicialmente, o leitor realiza o procedimento de ciclo de leitura das etiquetas, transmitindo um comando de consulta Q= 6 para todas as etiquetas dentro de sua área de cobertura. Esse comando corresponde ao comprimento do quadro 2^Q, significando que existem 2^Q *slots* no quadro de leitura atual. Ao chegar no último *slot* de tempo, o leitor começa a contabilizar o número de *slots* vazios *Sv*, o número de *slots* identificados com sucesso *Ss* e o número de *slots* em colisão *Sc*. Após esse procedimento, um número estimado de etiquetas é então gerado para ser lido no início do ciclo de leitura, de acordo com a Equação 4.1:

$$\hat{n} = \frac{L}{i} \times (\alpha \times Ss_i + k \times Sc_i) \tag{4.1}$$

Esse fator é o valor aproximado do número de etiquetas que serão transmitidas em cada *slot* de colisão no quadro finalizado, em que k representa o coeficiente do valor aproximado para o número de etiquetas que serão transmitidas em cada *slot* que colidiu no quadro finalizado, L corresponde ao tamanho do quadro e i é o último *slot* de tempo

do quadro atual. Considerando que há pelo menos duas etiquetas envolvidas em uma colisão, o coeficiente k pode ser ajustado para assumir o valor 2 como uma medida de limite mínimo para realizar a estimativa de etiqueta. Para minimizar implementações complexas, foi considerado como $k = 2,39$, que é o mesmo coeficiente usado pelo método em [Schoute 1983] que otimiza o número de *slots* em colisão.

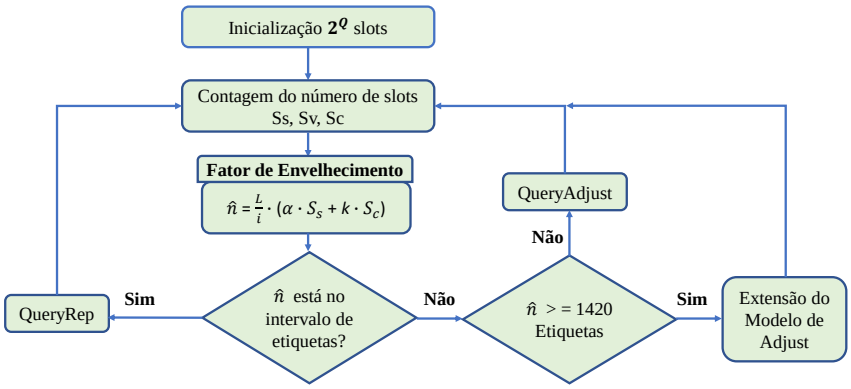

Figura 4.1: Fluxograma do algoritmo proposto.

Além disso, a proposta apresenta um fator de envelhecimento (α) que atua recompensando ou penalizando *slots*, conforme exposto na Equação 4.1, de acordo com o desempenho do ciclo de leitura anterior. O fator α é multiplicado pelo número de *slots* bem-sucedidos. Esse fator é a representação média do número de *slots* bem-sucedidos no quadro anterior, o que significa que o número de etiquetas que tiveram uma identificação bem-sucedida impactará diretamente no quadro atual. A média é a proporção entre o número de *slots* bem-sucedidos sobre o número total de *slots* em um quadro.

Inicialmente, o fator de envelhecimento α assume valor igual a 1. Como não há histórico anterior, pois o processo de identificação está começando, nas rodadas seguintes, o valor de α pode ser alterado, assumindo valores entre o intervalo 0,8 e 1,2. Esses valores foram escolhidos empiricamente, entre outros, por apresentarem melhor desempenho para o esquema fator de envelhecimento. Quando o valor de α é 0,8, indica que o número de *slots* bem-sucedidos no quadro anterior está abaixo da média esperada e, então, será penalizado. Por outro lado, se o próximo quadro tiver um valor maior ou igual à média de *slots* bem-sucedidos, então α será igual a 1,2, o que significa uma recompensa por alcançar vários *slots* de sucesso na rodada anterior. Com essa técnica, torna-se mais fácil estimar um *slot* bem-sucedido de acordo com o processo de leitura anterior.

A Figura 4.2 exemplifica o processo de funcionamento do fator de envelhecimento, em que o quadro inicial começa com α. Como no passado teve apenas um *slot* com sucesso

no quadro, então o segundo quadro receberá fator de penalização de $\alpha = 0{,}8$. Ao calcular a média de *slots* de sucesso no segundo quadro, o terceiro quadro será recompensado com $\alpha = 1{,}2$.

O leitor deve verificar se a estimativa das etiquetas está dentro do intervalo associado ao comprimento do quadro *L*, conforme listado na Tabela 4.1. Caso contrário, se o número de etiquetas for $>= 1420$, o leitor ajustará o tamanho do quadro enviando um comando *QueryAdjust* para aumentar ou diminuir o número de *slots* no próximo quadro. De outro modo, se $\hat{n}$ for menor que 1420 etiquetas, a extensão do modelo de *Adjust* será aplicado de acordo com a Tabela 4.1, enviando um comando *QueryRep*. A Figura 4.1 ilustra o algoritmo proposto.

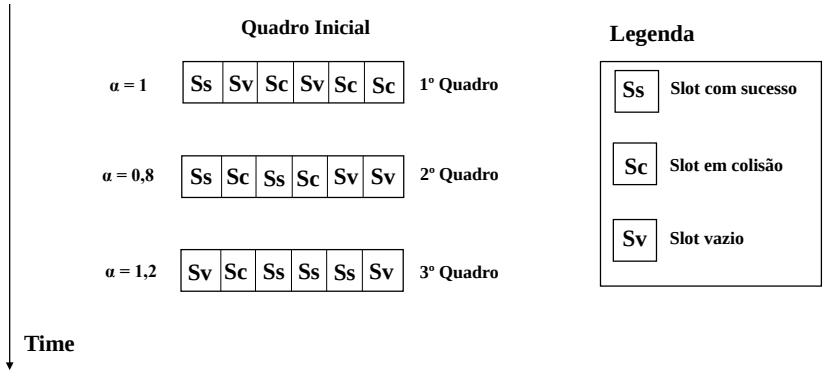

Figura 4.2: Fator de envelhecimento.

Se for necessário realizar um ajuste no tamanho do quadro, o leitor precisa definir um comprimento adequado, com base na estimativa do *backlog*, para estimar um número de etiquetas $\hat{n}$ de acordo com o número de etiquetas identificadas com sucesso (da Equação 4.2). Com base no *backlog* estimado, o leitor ajusta o tamanho do quadro usando o comando *QueryAdjust* ou um valor *Q* conforme descrito na Tabela 4.1. No entanto, se o ajuste do tamanho do quadro não ocorrer durante o processo de identificação, o leitor adota o estimador do [Schoute 1983], utilizando o fator de $2{,}39 * Sc$ para estimar o atraso, onde *Sc* é o número de *slots* em colisão no final do quadro atual.

$$backlog = \hat{n} - Ss \tag{4.2}$$

A Tabela 4.1 demonstra a relação tamanho de quadro para quantidade de etiquetas estimadas. Com essa relação, é possível fazer com que o algoritmo possa identificar

um pouco mais de 10.000 etiquetas, sendo um número razoável para atender diversas aplicações industriais.

Com vistas a avaliar a confiabilidade e o desempenho do algoritmo proposto e também dos demais algoritmos, será explicado na Seção 4.2 o desenvolvimento do modelo orientado a confiabilidade e desempenho, utilizado como ferramenta de avaliação.

Tabela 4.1: Tamanho do quadro em relação ao número de etiquetas .

Q	**Tamanho do quadro** $L = 2^Q$	**Intervalo de etiquetas** $n_{Q_1} - n_{Q_2}$
2	4	[1,5]
3	8	[6,11]
4	16	[12,22]
5	32	[23,44]
6	64	[45,89]
7	128	[90,177]
8	256	[178,355]
9	512	[356,710]
10	1024	[711,1420]
11	2048	[1421,2840]
12	4096	[2841,5680]
13	8192	[5681,11360]

4.2 Implementação do Modelo

O modelo de confiabilidade e desempenho que foi proposto é capaz de realizar simulações de forma mais realista para comunicações de sistemas RFID baseadas no protocolo anticolisão DFSA. A ideia é a de que diferentes algoritmos que seguem o padrão de comunicação de acordo com a norma *EPCGlobal UHF Class-1 Gen-2* possam ser avaliados de maneira mais completa e eficiente em termos de confiabilidade e desempenho. Para tanto, o comportamento de erro no canal e o funcionamento do leitor RFID foram modelados utilizando o formalismo GSPN, conforme será descrito no decorrer desta seção.

O modelo proposto foi desenvolvido com auxílio da ferramenta de modelagem para sistemas complexos conhecida como Möbius, que possui uma extensão direcionada para GSPN chamada Rede de Atividade Estocástica (SAN). A ferramenta Möbius é capaz de fornecer um formalismo de alto nível com mecanismos apropriados para compor diferentes modelos, disponibilizando uma maior flexibilidade ao processo de modelagem. O

detalhe da ferramenta pode ser visto na subseção 2.12.3.

Para realizar uma modelagem de forma mais precisa e detalhada do ambiente que foi investigado, é preciso primeiramente considerar alguns elementos básicos primordiais: Esses pressupostos são bastante razoáveis e apresentados da seguinte forma:

1. Foi considerado que existem no mesmo cenário um leitor e múltiplas etiquetas a serem identificadas;
2. O leitor é responsável por sempre iniciar a comunicação;
3. Quando as etiquetas são identificadas, elas são silenciadas (desconsideradas do inventário);
4. São consideradas apenas mensagens de dados como (transmissões entre leitor/etiqueta e etiqueta/leitor) através do uso de ondas de rádio contínua;
5. As falhas ocorrem de maneira independente no canal de comunicação;
6. Se houver uma falha durante a transmissão de pacotes, supõe-se que os pacotes foram comprometidos (corrompidos) através da inserção de erros, como também deve-se considerar que todos os erros são sempre detectados;
7. Todos os dispositivos têm o mesmo intervalo de transmissão, respeitando o padrão *EPCGlobal UHF Class-1 Gen2* utilizado em sistema RFID para o protocolo anticolisão DFSA.

Considerando essas proposições, a modelagem proposta foi desenvolvida com o apoio do modelo composto, disponibilizado pela ferramenta Möbius, que utiliza uma abordagem de compartilhamento de estado. Nessa abordagem, os submodelos são vinculados por meio de sobreposição, ou seja, compartilhando variáveis de estados correspondentes, incluindo apenas uma única variável de estado para cada submodelo. Com base nisso, três submodelos distintos foram criados, sendo eles: submodelo Erro, submodelo Leitor e submodelo Juntar. Todos esses submodelos são modelados utilizando o formalismo GSPN, considerando então a sua natureza probabilística. As próximas subseções vão detalhar o submodelo Erro e o submodelo Leitor, já que o submodelo Juntar tem como finalidade apenas realizar a ligação entre eles. A Figura 4.3 expõe a organização estrutural lógica do modelo proposto baseado em GSPN.

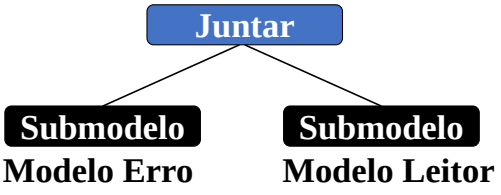

Figura 4.3: Visão geral do modelo proposto.

4.2.1 Submodelo Erro

Para esta tese, foi considerado que uma falha pode ser qualquer tipo de interferência que reproduz um erro de comunicação, o que resulta, consequentemente, no descarte de pacotes de dados. Para realizar a modelagem de ocorrência de erro, um modelo baseado em Cadeia Markov foi adotado na implementação, estendendo-se a diversos trabalhos anteriores [Willig et al. 2002]. A seguinte Figura 4.4 traz em resumo a Cadeia de Markov como referência.

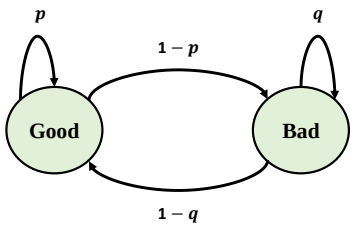

Figura 4.4: Modelo de erro Gilbert/Elliot usado como referência.

O modelo clássico baseado em Cadeia de Markov, comumente conhecido como modelo de erro Gilbert/Elliot, define dois parâmetros de estados para se modelar de forma concisa um canal de comunicação: *Good* e *Bad*. Quando o canal está no estado *Bad*, todos os pacotes são descartados imediatamente devido à ocorrência de erros durante uma transmissão de dados. Inicialmente, o modelo de erro está setado no estado *Good* e pode ocorrer uma transição, alterando-o para o estado *Bad*. Então, uma nova transição pode fazer o modelo retornar ao estado anterior *Good*. Tais transições podem se dar periodicamente, de acordo com uma probabilidade definida, conforme expresso na Figura 4.3. Nessa Figura, p é a probabilidade de permanência no estado *Good*, enquanto q é a probabilidade de permanecer no estado *Bad*, assumindo em ambos os casos que nenhuma transição de estado aconteceu.

Esse modelo de erro básico foi reproduzido neste trabalho, sendo implementado com o formalismo GSPN, incorporando elementos adicionais para melhor se modelar erros em canais ruidosos. O novo modelo de erro baseado em GPSN proposto é apresentado segundo a Figura 4.5.

No modelo de erro proposto, são apresentados dois locais estendidos, quais sejam: *Interference* e *Memory*, incorporados para armazenar o status do canal quando ele se encontra no estado *Bad*. Esses dois lugares estendidos são compartilhados pelos elementos compostos do modelo. Além disso, as transições existentes entre os estados acontecem de acordo com uma distribuição estocástica. A periodicidade e a duração dos erros são

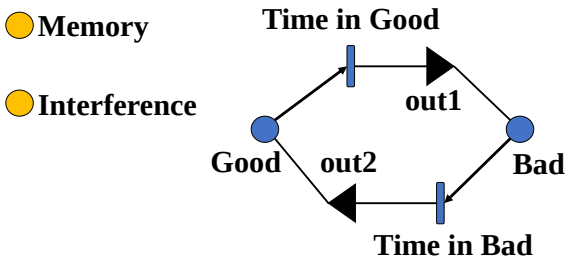

Figura 4.5: Modelo de erro proposto baseado em GSPN.

configuradas por duas atividades temporizadas: *Time in Good* e *Time in Bad*. Fazendo isso, é possível modelar erros de curta e longa duração.

Outro elemento bastante importante do modelo de erro desenvolvido é a saída, sendo duas delas representadas pelos seguintes objetos: *out1* e *out2*. Elas controlam o funcionamento do modelo de erro, conforme definido pela Figura 4.6. Nessa Figura, o valor "1" indica que houve uma permanência no estado correspondente. Portanto, o estado do local *Memory* não é alterado pela saída *out2*, visto que há uma permanência no estado *Good*. *Mark ()*) é uma função definida pela ferramenta Möbius que retorna o número de *tokens* em um determinado tempo t em um lugar p.

Out 1	**Out 2**
$Good \longrightarrow Mark() = 0$	$Good \longrightarrow Mark() = 1$
$Bad \longrightarrow Mark() = 1$	$Bad \longrightarrow Mark() = 0$
$Interference \longrightarrow Mark() = 1$	$Interference \longrightarrow Mark() = 0$
$Memory \longrightarrow Mark() = 1$	

Figura 4.6: Controlando o comportamento do modelo de erro de comunicação.

4.2.2 Submodelo Leitor

Esse submodelo representa o elemento principal do modelo proposto, sendo desenvolvido seguindo as devidas especificações do protocolo anticolisão DFSA. Assim, tem o papel de ser responsável pelos procedimentos de leitura das etiquetas, realizando o gerenciamento básico de controle de acesso ao meio durante o processo de comunicação entre os elementos envolvidos. Na verdade, uma vez que o formalismo GSPN permite a implementação de diferentes códigos com o uso linguagem de programação (C++) para controlar o disparo das transições das Redes de Petri, o submodelo Leitor se torna bastante

adaptativo e adequado a diferentes situações, segundo as regras impostas pelos protocolos anticolisão. Essa característica possibilita que o modelo proposto se torne uma ferramenta poderosa capaz de avaliar diferentes algoritmos baseados em DFSA, como também cenários com diferentes níveis de ruídos.

O protocolo anticolisão de etiquetas baseado em DFSA, o qual utiliza o TDMA como forma de acesso ao meio, funciona definindo uma estrutura de quadros, dividindo o canal de transmissão em vários *slots* de tempo de tamanho fixo. Nele, cada etiqueta irá transmitir em um intervalo de tempo, tentando evitar assim possíveis ocorrências de colisões. Nesse sentido, três diferentes situações são possíveis quanto à utilização dos *slots* de tempo: *slot* com sucesso, *slot* colidido e *slot* vazio. Todas essas situações foram modeladas. Além disso, para torná-lo mais realista e fiel para simulação, esse modelo utiliza todos os parâmetros relacionados a uma operação de comunicação leitor/etiqueta, seguindo as especificações técnicas impostas pelo padrão *EPCGlobal UHF Classe 1 Gen2*. O DFSA segue os requisitos físicos e lógicos de comunicação do padrão *EPCGlobal UHF Classe-1 Gen2*, adotado em diversas soluções para RFID. Esse padrão consiste no conjunto de regras que auxiliam no processo de identificação das etiquetas.

Na comunicação do leitor para etiqueta *(Downlink)* são utilizados os seguintes comandos:

- *Select* - inicialmente é usado para selecionar um grupo de etiquetas que estão dentro do raio de cobertura do leitor;
- *Query* - para identificar uma ou um grupo de etiquetas;
- *QueryAdjust* - com função de ajustar o tamanho do quadro atual;
- *ACK* - para confirmar o recebimento do quadro;
- *QueryRep* - para refazer uma consulta.

Já os comandos usados na comunicação de etiquetas para leitor *(Uplink)* são:

- *RN16* - que significa uma parte do *ID* da etiqueta contendo 16 bits, sendo utilizado para minimizar o número de colisões;
- *payload* - que representa o dado em si da etiqueta.

O submodelo Leitor baseado em GSPN é apresentado na Figura 4.7.

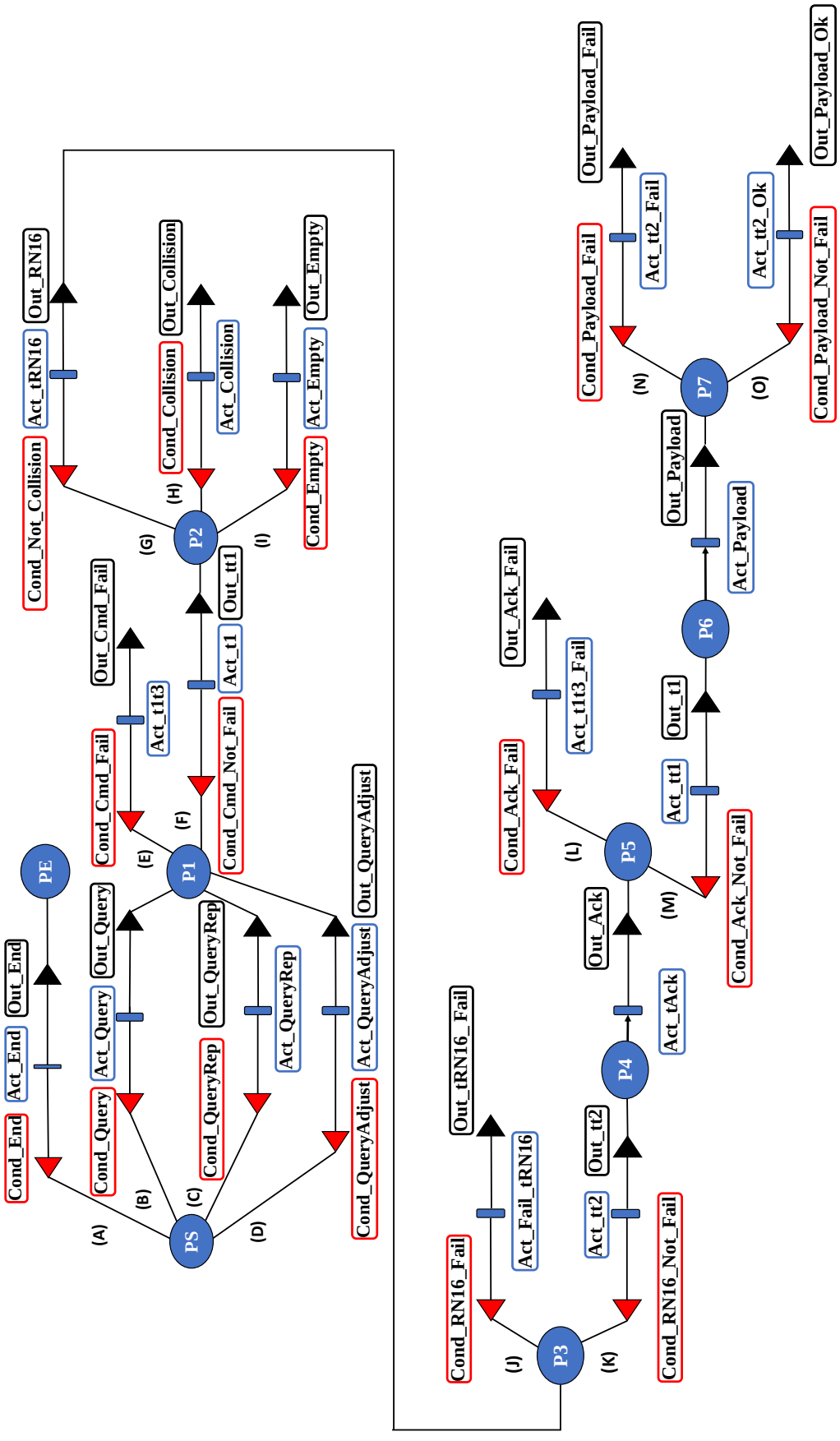

Figura 4.7: A modelagem GSPN do módulo Leitor.

4.2.2.1 Variáveis de controle

A modelagem dos *slots* de tempo foi dividida em duas partes. A primeira está associada à sua sequência lógica, sendo composta por locais padrão, atividades temporizadas, entrada e saída de dados. A segunda parte define as funcionalidades das variáveis de suporte, que são modeladas por locais estendidos. Tais variáveis são organizadas em diferentes classes: variáveis estáticas (parâmetros predefinidos considerados durante um processo de simulação), variáveis métricas (para gerenciar os resultados obtidos) e, por fim, as variáveis dinâmicas (modificadas durante a execução do procedimento de simulação). Essas variáveis são os principais elementos do modelo.

As variáveis estáticas do submodelo Leitor são compostas pelas *Tags* que representam a quantidade de etiquetas a serem identificadas e o parâmetro Q que define o tamanho inicial do quadro em execução.

Já o grupo formado por variáveis métricas é responsável por fornecer informações mensuradas para avaliação da confiabilidade e do desempenho do modelo. Essas variáveis registram a quantidade de pacotes descartados por erros de canal, o tempo necessário para a leitura das etiquetas, o número de *slots* utilizados, entre outros parâmetros, conforme definidos pela Tabela 4.2.

Tabela 4.2: Lista de variáveis métricas.

Local estendido	**Descrição**
Queryrep_fail	Número de comandos de consulta do Leitor que são repetido devido a falhas
Adjust_fail	Número de falhas que ocorrem quando o leitor solicita um ajuste no quadro
Ack_fail	Número de mensagens *ACK* com falhas
Payload_fail	Número de falhas de dados (pacotes de dados não recebidos)
RN16_fail	Número de falhas *RN16* (as respostas das etiquetas não foram recebidas pelo leitor)
Rounds	Número de oportunidades de transmissão
Silence_tags	Número de etiquetas silenciadas (etiquetas que foram identificadas)
Collisions_slots	Número de *slots* em colisão
Idle_slots	Número de *slots* vazios
Total_time	Tempo total (tempo gasto para identificar todas as etiquetas)

O conjunto de variáveis dinâmicas, apresentado na Tabela 4.3, tem o papel de auxiliar no processo de execução do sistema. Os elementos *Interference* e *Memory* também estão presentes no modelo de erro, uma vez que ambos são compartilhados pelos dois submodelos.

A variável *L* representa o tamanho do quadro ajustado dinamicamente de acordo com o número de *slots* de tempo. Esse quadro é referenciado pela variável *Frame*. Esse ajuste dinâmico é baseado no número atual de etiquetas e nas variáveis *qAdjust* ou *Adjust*. Além disso, a variável *lastSuccess* trabalha usando o número médio de *slots* bem-sucedidos no quadro anterior para influenciar na alocação do quadro atual.

Tabela 4.3: Lista de variáveis dinâmicas.

Local estendido	**Descrição**
Device	O vetor de etiquetas que serão dinamicamente alocadas no quadro
Frame	Quadro atual
L	Tamanho do quadro dinâmico
qAdjust	Função ajuste de quadro de acordo com o número de etiquetas
adjust	Ajuste sem uso do *backlog*
current_cmd	Indica o comando atual que será usado no processo de leitura da etiqueta (depende do algoritmo utilizado)
lastSucess	Fator de envelhecimento (Apenas o algoritmo proposto)
Number_Txs	Número de transmissão com sucesso (número de etiquetas que transmitem seu RN16 após o tempo t1)
Number_Txc	Número de transmissão em colisão
Number_Txi	Número de transmissão ocioso
Memory	Memorizando problemas de canal
Interference	Ruído no canal

4.2.2.2 Operação do Leitor no modelo GSPN

Essa subseção apresenta com mais detalhes o modo de operação lógica do submodelo Leitor, conforme descrito na Figura 4.7. Como essa implementação em GSPN é baseada no protocolo anticolisão DFSA (Figura 2.8), as transições e os estados do sistema modelado replicam a operação do protocolo em ambiente real. Uma preocupação importante ao modelar o protocolo é a atuação do tempo das transições. A Tabela 4.4 apresenta as variáveis temporais consideradas no modelo.

Tabela 4.4: Período das transições durante um *slot* de tempo no modelo.

Tempo das transições	**Período**
Act_Query	tquery
Act_QueryRep	tqueryrep
Act_QueryAdjust	tqueryadjust
Act_t1t3	tt1 + tt3
Act_t1	tt1
Act_tRN16	trn16
Act_Colision	trn16 + tt2
Act_Empty	tt3
Act_Fail_tRN16	tt2
Act_tt2	tt2
Act_tAck	tack
Act_t1t3_Fail	tt1 + tt3
Act_tt1	tt1
Act_Payload	tag_memory * tpri
Act_tt2_Ok	tt2

Os valores da Tabela 4.4 são definidos de acordo com o padrão *EPCGlobal UHF Class 1 Gen2* para comunicações RFID, tornando assim sua atuação de forma mais realista. Deste modo, a Tabela 4.5 demonstra os valores considerados nesse modelo.

Conforme esperado, por se tratar de uma Rede de Petri, os *tokens* podem transitar por todos os locais padrão. O estado inicial é representado pelo local *PS*, que assume como valor do seu *token* "1". De acordo com o processo de simulação podem ocorrer transições, "movendo"o *token* por toda a Rede de Petri. Na verdade, as transições para uma melhor compreensão do funcionamento do modelo foram organizadas em grupos de "fluxo", representados pela Figura 4.7, variando de **A** a **O**. Os fluxos são descritos a seguir:

- **Fluxo (A)**: é representado pela entrada *Cond_End*, essa condição exige obrigatoriamente que o número de etiquetas silenciadas seja igual ao número de etiquetas que devem ser identificadas (total do inventário). Também é necessário que não exista *slot* em colisão no quadro atual. Satisfazendo essas condições, esse fluxo segue para a transição imediada *Act_End* gerando como saída *Out_End*. Desse modo, os estados *PS* e *PE* assumem, respectivamente, valores de *token* "0"e "1". Assim, é sinalizado que o processo de identificação de todas as etiquetas foi finalizado.

- **Fluxo (B)**: a entrada de dados representada pela condição *Cond_Query* requer que o comando atual seja *Query* ou *Queryfail*, sem nenhum ajuste necessário para o quadro atual. Se essas condições forem atendidas, a atividade temporizada *Act_Query* realiza a verificação de falsos positivos e os falsos negativos em relação ao canal de transmissão (modelo de erro), seguindo para saída de dados *Out_Query*, onde o leitor envia uma consulta para as etiquetas e aguarda como retorno suas respostas. (Algoritmo 1). Em seguida, as etiquetas escolhem um *slot* aleatório dentro de um intervalo de *slots*. Somando-se as tentativas desse processo, é possível contabilizar o número de tentativas das etiquetas (0 para *slot* vazio, 1 para *slot* usado com sucesso e valor maior que 1 para *slot* em colisão). Depois disso, o fator de envelhecimento é acionado para analisar os resultados anteriores, estimando novo número de etiquetas. Então, se for necessário ajustar o tamanho do quadro, o comando *Query_Adjust* é usado (o fator de 2^Q é considerado para ajustar o quadro, com $Q = 6$ como valor inicial de 64 *slots*). Assim, os valores dos estados *PS* e *P1* passam a ser, respectivamente, "0"e "1'.

Tabela 4.5: Valores dos parâmetros de acordo com o padrão *EPCGlobal UHF Class 1 Gen2*.

Parâmetro	**Valor**	**Descrição**
ttrcal	$50\mu s$	Tempo de calibragem do leitor/etiqueta
divide ratio (dr)	8	Divide *ratio*
tpri	(ttrcal/dr)/1000	Intervalo de repetição por pulso
tquery	22·tpri	Tempo de consulta
tqueryrep	4·tpri	Tempo de consulta por repetição
tqueryadjust	9·tpri	Tempo de ajuste por consulta
trn16	16·tpri	Tempo RN16
tack	18·tpri	Tempo ACK
tepc	$max(32, tagsize)$·tpri	O tamanho da tag é um parâmetro do modelo
tt1	10·tpri	Tempo entre a solicitação do leitor e uma resposta imediata da etiqueta
tt2	20·tpri	Tempo de resposta da etiqueta
tt3	10·tpri	Tempo de espera após tt1 para a etiqueta transmitir outra resposta

- **Fluxo (C)**: aciona a condição de entrada *Cond_QueryRep* e verifica se o comando atual corresponde a *Queryrep* ou *Queryrep_fail*. Para tanto, o *token* em PS deve ter valor igual a "1"e o número de etiquetas que foram silenciadas deve ser menor que o número de etiquetas do inventário. Em seguida, o fluxo vai para a atividade temporizada *Act_QueryRep*, que verifica a presença de falso positivo (canal em *Good*) ou falso negativo (canal em *Bad*). Alcançando a saída *Out_QueryRep*, será verificado se número de etiquetas é igual ou menor que o tamanho do quadro atual. Assim sendo, o valor de *Q* permanece inalterado, conforme o (Algoritmo 2). Desse modo, os valores dos estados representados por *PS* e *P1* passam a ser, respectivamente, "0"e "1".
- **Fluxo (D)**: a condição de entrada *Cond_QueryAdjust* é acionada quando o comando atual corresponde a *QueryAdjust* ou *QueryAjust_fail*. O *token* em PS é "1"também quando o número de etiquetas silenciadas for menor do que o número de etiquetas do inventário. O fluxo vai para a transição *Act_QueryAdjust* verificar a presença de erros. Nesse processo, o tempo *tqueryadjust* será considerado. Assim, a saída *Out_QueryAdjust* tem por objetivo realizar um ajuste no quadro atual segundo o número de etiquetas, realizando uma operação chamada de *backlogEstimated*, conforme descrito pelo (Algoritmo 3), alterando o valor de *Q*. Os valores nos estados *PS* e *P1* passam a ser, respectivamente, "0"e "1".
- **Fluxo (E)**: requer o uso da variável *Memory* com valor 1, indicando erro. Conforme já foi mencionado na subseção 4.2.1, a variável Memory é utilizada para armazenar o *status* do canal no estado *Bad*, sendo *P1* com o *token* de valor “1” como entrada. A atividade temporizada *Act_t1t3* representa a soma dos tempos t1 e t3, resultando como saída *Out_Cmd_Fail* (armazenando a quantidade de comandos em falha como *Queryfail*, *QueryRep_fail* e *QueryAdjust_fail*). Em seguida, a Rede de Petri retorna ao seu estágio inicial, com *P1* com *token* "0"e *PS* com *token* "1". O processo de identificação será recomeçado.
- **Fluxo (F)**: esse fluxo significa que não houve falha durante o processo de identificação, seguindo para a entrada *Cond_Cmd_not_fail*. Neste caso, a variável *Memory* é atualizada com valor "0"e o estado e *P1* assume como valor "1". *Act_t1* tem como duração de tempo t1, aguardando na saída *Out_tt1* os seguintes possíveis comandos *Query, QueryRep* ou *QueryAdjust*, que serão contabilizados. Como não houve falhas durante o fluxo corrente, então a representação dos estados *P1* recebe como valor "0"e *P2* tem valor "1".
- **Fluxo (G)**: representa um fluxo sem ocorrência de *slot* em colisão. Sua entrada é o *Cond_Not_Collision*, representando uma transmissão para cada *slot*. Seguindo

para *Act_tRN16*, que verificará a existência de falso positivo para o canal *good* e falso negativo para o canal *bad*. Na saída *Out_RN16*, o tempo *trn16* será somado ao tempo total. *P3* agora tem seu *token* com valor igual a "1".

- **Fluxo (H)**: representa um fluxo com existência de pelo menos um *slot* em colisão. Sua entrada é descrita pela condição de entrada *Cond_Collision*, indicando que houve mais de uma transmissão no mesmo *slot*, seguindo para *Act_Collision* em que o tempo de colisão corresponde a $(t1 + trn16)$, que será contabilizado. Gera como saída *Out_Collision*, que coleta informações de quantidade de *slots* em colisões e da quantidade de *rounds* (oportunidade de transmissão). *PS* recebe o *token* com valor "1"e o comando atual passa a ser *Query*.
- **Fluxo (I)**: apresenta uma situação de fluxo contendo *slot* vazio, indicando que não houve nenhuma transmissão de etiquetas no *slot* corrente. Como a entrada é representada pela condição *Cond_Empty*, Segue para a transição temporizada *Act_Empty*, sendo tempo de um *slot* vazio contabilizado como *(t3)*. A saída do fluxo é representada por *Out_Empty* e o *PS* recebe como valor "1", alterando o comando atual para *QUERY*.
- **Fluxo (J)**: o fluxo (G) continuará o fluxo no lugar *P3*. Lá, este fluxo indica que houve um erro de transmissão no Pacote *RN16*. A condição *Cond_RN16_Fail* recebe como entrada a variável *Memory* e o lugar *P3*. Após a confirmação de tempo indicada pela transição temporizada *Act_Fail_tRN16*, o resultado é apresentado na saída *Out_tRN16_Fail*: o comando *QueryAdjust* é então utilizado. Nesse caso, o leitor considera que ocorreu uma colisão. Como resultado, o número de *Rounds* e a quantidade de pacotes *RN16* com falha também serão contabilizados. Além disso, *PS* recebe como valor "1", ou seja, o retorno para o estagio inicial.
- **Fluxo (K)**: No lugar *P3* - esse fluxo é considerado quando não há erro de transmissão de pacotes *RN16*, representados pela entrada *Cond_RN16_Not_Fail*. O tempo de resposta da etiqueta é indicado pela transição temporizada *Act_tt2*, que é contabilizada e o fluxo segue para a saída *Out_tt2*, somando-se todos os intervalos de tempo. A transmissão segue para a transição temporizada *Act_tAck*, que irá armazenar o tempo de confirmação para comunicação. Ao final deste fluxo, *P5* possui o valor “1”.
- **Fluxo (L)**: nesse fluxo é considerado quando existe uma situação em que ocorre um erro na transmissão de mensagens do tipo *ACK*, representado pelo entrada *(Cond_Ack_Fail)*. Nesse caso, a transição temporizada *Act_t1t3_Fail* contabiliza o tempo *t1* e *t3*. A saída *Out_Ack_Fail* indica o número de *rounds* como também o número de pacotes com falha *Ack*. Em decorrência da situação da perda de pa-

cote apresentada nesse fluxo, o comando selecionado é o *QueryRep* e os valores dos estados são alterados, em que *P5* recebe como valor "0"e *PS* recebe como valor "1".

- **Fluxo (M)**: esse fluxo possui como entrada a condição *Cond_Ack_Not_Fail* e a variável *Memory* com valor igual a "0", pois não ocorreu erro de comunicação. Na saída *Out_t1*, o tempo de resposta da etiqueta será contabilizado. No lugar de estado P6, a transição temporizada *Act_Payload* atualiza seus parâmetros para evitar o processamento de erros de falso positivo e falso negativo. Por fim, na saída *Out_Payload*, o tempo correspondente ao tamanho do *payload* da etiqueta é adicionado ao tempo total.
- **Fluxo (N)**: No lugar de estado *P7* - erro na transmissão da etiqueta é modelado por esse fluxo, é indicado pela condição de entrada *Cond_Payload_Fail*. Então, a transição temporizada *Act_tt2_Fail* calcula o tempo de resposta da etiqueta, gerando como saída *Out_Payload_Fail*, que indica o número de *rounds* e o número de pacotes *Payload_Fail*. Como esperado, *PS* recebe o valor "1".
- **Fluxo (O)**: por fim, esse fluxo apresenta como entrada a condição *Cond_Payload_Not_Fail* (variável *Memory* assume valor igual a "0"), pois não houve erro de comunicação. A transmissão vai para a transição temporizada *Act_tt2_Ok*, aguardando uma resposta da etiqueta. A saída *Out_Payload_OK* contabilizará o tempo de resposta da etiqueta, o número de *rounds* e o número de etiquetas que foram silenciadas. Assim, o fluxo é concluído.

Conforme foi apresentado, o submodelo Leitor é tido como elemento principal do sistema RFID, pois detalha as principais características de funcionamento de comunicação leitor/etiqueta, reproduzindo o comportamento lógico e físico para um cenário realista de ambientes industriais, incluindo comandos em falhas e confirmações bem-sucedidas que, de fato, poderão ocorrer em sistemas RFID de etiquetas passivas.

Como forma de descrever melhor alguns elementos importantes para o funcionamento operacional do submodelo Leitor, alguns algoritmos da proposta que foi desenvolvida para resolver os problemas de acesso ao meio foram definidos para realizar processamento nos principais fluxos. Desse modo, é possível representar os elementos estruturais do protocolo em funcionamento. Para tanto, primeiramente será considerado o Fluxo (B), uma vez que representa a atividade principal do submodelo, no qual o comportamento da saída *Out_Query* é descrito pelo Algoritmo 1.

Consulta no inventário de etiquetas

Algoritmo 1: Out_Query

```
1  if current_cmd→ cmd_type→ Mark() == QUERY then
2      adjust->Mark() = 0;
3      for i← 1; ((i <= L→ Mark()) && (adjust→ Mark() == 0)); i++ do
4          if i <= L→ Mark() && i == pow(2,j) then
5              //aging factor
6              if lastSucess→ Mark() ! = −1 then
7                  if lastSucess→ Mark() < sucess_slots→ Mark() z = 0.8 then
8                      ;
9                  end
10                 else if lastSucess→ Mark() > sucess_slots→ Mark() z = 1.2 then
11                     ;
12                 end
13                 else
14                     z = 1.0
15                 end
16                 ;
17             end
18             //estimate the number of tags to generate a new frame
19             n = ((z∗sucess_slots→ Mark() + k∗collisions_slots→ Mark())∗L→
                   Mark())/i;
20         end
21     end
22 end
```

Em relação ao Fluxo (C), a saída representada por *Out_QueryRep* é definida conforme o Algoritmo 2, que realiza o procedimento de validação para leitura das etiquetas, pois significa que o tamanho do quadro está de acordo com o número de etiquetas que respondem a consulta do leitor. Ou seja, não há necessidade de ajuste no tamanho do quadro atual.

O número de etiquetas está de acordo com o tamanho do quadro atual

Algoritmo 2: Out_QueryRep

```
1  if current_cmd→ cmd_type→ Mark() == QUERYREP then
2  |  Q→Mark() ! = qAdjust→Mark();
3  |  adjust→Mark() = 1;
4  |  return Query;
5  end
```

A operação *backlogEstimated*, utilizada para realizar o ajuste do tamanho do novo quadro é descrita pelo fluxo (D) e definida conforme o Algoritmo 3.

Ajustando o tamanho do novo quadro

Algoritmo 3: Out_QueryAdjust

```
1  if current_cmd→ cmd_type→ Mark() == QUERYADJUST then
2  |  if backlogEstimated <= 5 then
3  |  |  qAdjust→ Mark() = 2;
4  |  |  .
5  |  |  .
6  |  |  .
7  |  |  .
8  |  end
9  |  else if backlogEstimated <= 11360 then
10 |  |  qAdjust→ Mark() = 13;
11 |  end
12 |  return Query;
13 end
```

Depois de todas essas definições apresentadas, o modelo baseado em GSPN proposto, está apto para ser utilizado como uma ferramenta poderosa e adaptável, cujo seu principal objetivo é avaliar a confiabilidade e o desempenho do algoritmo proposto, como também dos diferentes protocolos anticolisão baseados no DFSA para RFID. Essa avaliação será apresentada no capítulo a seguir.

Capítulo 5

Resultados

Este capítulo apresenta uma análise do comportamento do algoritmo proposto juntamente com outras soluções de acesso ao meio para RFID. Para tanto, foi implementado um modelo baseado em GSPN cuja finalidade é analisar a confiabilidade e o desempenho dos algoritmos investigados em um ambiente com múltiplas etiquetas. Nesse sentido, foram considerados três seguintes cenários para a avaliação. O primeiro cenário apresenta o canal de comunicação livre de erros, o segundo cenário expõe um nível de falhas mais ponderado, e o terceiro cenário uma situação com maior incidência de falhas. Ao final do capítulo, será abordada uma avaliação comparativa entre os diversos algoritmos.

5.1 Avaliação da Confiabilidade e do Desempenho

A avaliação dessa métrica unificada verifica a probabilidade de um sistema, em um determinado instante, apresentar um desempenho igual ou superior a um nível predeterminado durante um certo período de tempo em operação. Portanto, essa avaliação em sistemas RFID contribui diretamente para a análise da eficácia do mecanismo de tolerância a falhas transitórias e acordos de nível de serviço, que são fundamentais para aplicações práticas em ambiente industrial.

Esta seção apresenta uma avaliação da confiabilidade e desempenho do algoritmo que foi proposto com outros diferentes protocolos de comunicação para RFID, explorando, para tanto, o modelo que foi desenvolvido baseado em GSPN. Tal avaliação foi realizada através de ferramenta de modelagem de sistemas complexos, conhecida como Möbius [Sanders 2005], que permite uma maior flexibilidade na visualização dos resultados obtidos. Além disso, esta seção descreve como os experimentos foram realizados, para avaliar diferentes parâmetros diretamente relacionados à confiabilidade e desempenho dos algoritmos considerados.

Para facilitar melhor a compreensão, foi ilustrado um cenário genérico de comunicação para identificação das etiquetas em sistemas RFID. Na Figura 5.1, observa-se um fluxograma que contém um leitor, o que está sendo auxiliado por um protocolo anticolisão, efetuando transmissões no canal de comunicação para realizar a leitura de diversas etiquetas. Adicionalmente, foi considerado que os elementos RFID envolvidos seguem o padrão de comunicação da *EPCGlobal UHF Classe-1 Gen-2*.

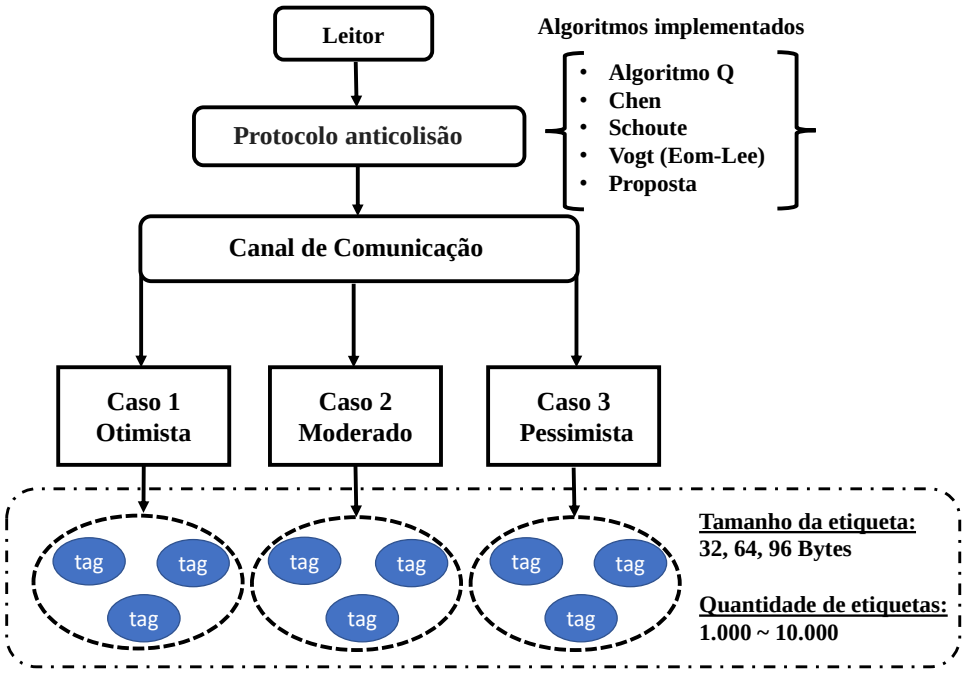

Figura 5.1: Fluxograma representando um procedimento de leitura das etiquetas.

Para permitir uma avaliação de forma mais abrangente para os quesitos de confiabilidade e desempenho usando o modelo que foi desenvolvido baseado em GSPN, além do algoritmo anticolisão que foi proposto, quatro outros algoritmos com a mesma finalidade, porém com características diferentes, foram implementados, a saber: 1) Algoritmo Q, 2) Chen, 3) Schoute e 4) Vogt (Eom-Lee). As comparações de atributos numéricos entre esses algoritmos são uma contribuição importante para uma avaliação de confiabilidade e desempenho mais realista em aplicações baseadas em RFID.

Ambientes industriais são caracterizados pela existência de uma alta diversidade de equipamentos, fonte de padrões de interferências eletromagnéticas que induzem a falhas. Nos sistemas de comunicação, essas falhas afetam o meio de transmissão e produzem erros nos pacotes transmitidos, corrompendo seu conteúdo (dados), o que pode levar a comportamentos imprevisíveis que prejudicam as comunicações entre os leitores e as etiquetas, inviabilizando a aplicação. Portanto, é importante avaliar a influência desse tipo

de falha nos sistemas de RFID, com vistas a ser possível antecipar decisões relacionadas a topologia, níveis de redundância e robustez, necessários para as aplicações de destino.

Para simular erros de comunicação, conforme já mencionado, foram definidos três cenários de interferência: otimista, moderado e pessimista. Na verdade, cada um desses cenários possui um determinado nível de interferência, que afeta diferentemente os experimentos realizados. No cenário otimista (caso 1), o canal de comunicação é definido como sendo livre de erros. No cenário moderado (caso 2), o canal de comunicação está sujeito a alguns erros. Por fim, no cenário pessimista (caso 3), o canal de comunicação está propenso a maior presença de erros.

A Tabela 5.1 apresenta os parâmetros de interferência que foram considerados em cada cenário, os quais foram definidos considerando trabalhos anteriores [Willig et al. 2002].

Tabela 5.1: Parâmetros de interferência.

Cenário	$\mathbf{P_{good}}$	$\mathbf{P_{bad}}$	$\mathbf{T_{good}}$ **(ms)**	$\mathbf{T_{bad}}$ **(ms)**
Otimista (Caso 1)	1.0	0.0	∞	0.00
Moderado (Caso 2)	0.91	0.09	65.00	10.00
Pessimista (Caso 3)	0.67	0.33	20.00	10.00

De acordo com a Tabela 5.1, os seguintes parâmetros P_{good} e P_{bad} representam a probabilidade de o canal de comunicação estar no estado Bom e no estado Ruim, respectivamente. T_{good} e T_{bad} representam o período de tempo em milissegundos (ms), em que o canal de comunicação permanece no estado Bom e no estado Ruim, respectivamente. É importante destacar que os valores de P_{good} e P_{bad} foram obtidos empiricamente através de experimentos de simulação, conforme os valores escolhidos para T_{good} e T_{bad}. Com isso, os valores escolhidos para T_{good} e T_{bad} pode impactar diretamente nos valores de P_{good} e P_{bad}.

Para o cenário otimista, a representação de um valor elevado (infinito) em T_{good} torna P_{good} com 100%, resultando em um canal de comunicação livre de erros. Por outro lado, os cenários moderado e pessimista, que apresentam valores inferiores para T_{good}, fazem com que os valores de P_{good} e P_{bad} sejam alterados de forma significativa, representando interferência no canal de comunicação.

O submodelo Leitor baseado em GSPN, que foi desenvolvido para sistemas RFID, implementa todos os cinco algoritmos anticolisão, com o objetivo de realizar a leitura das etiquetas. Para avaliar o desempenho de cada algoritmo anticolisão citado, foi considerada uma população de etiquetas constituída de 1.000, 5.000 e 10.000 etiquetas, com diferentes

tamanhos de *payload*, variando entre 32, 64 e 96 bytes. Os resultados indicam que tanto o número de etiquetas quanto o tamanho do *payload* podem influenciar de maneira crucial nas métricas que foram consideradas para a avaliação. Em seguida, visando otimizar com precisão os resultados, foi definida a utilização de um intervalo de confiança de 95%, com a média de 5.000 simulações.

As subseções que seguem neste trabalho têm como finalidade apresentar de forma completa as análises de métricas que estão relacionadas a tempo, *slots*, interferência e desempenho da taxa de transferência nas simulações. Todos esses resultados que foram extraídos durante o processo de simulação, são elementos primordiais para a avaliação da confiabilidade e do desempenho dos algoritmos. Com base nos resultados é possível perceber o quanto o fator interferência pode prejudicar a comunicação nos sistemas RFID como um todo.

5.1.1 Análise de tempo para leitura das etiquetas

O tempo máximo para a realização do processo de leitura das etiquetas segue o padrão definido pela norma *EPCGlobal*, combinado com parâmetros de velocidade de comunicação entre os dispositivos envolvidos. Com isso, torna-se possível calcular o tempo máximo total para efetuar o processo de leitura de um conjunto de etiquetas. Essas informações também servem como especificação técnica de equipamentos como leitores, pois, com base no tempo máximo de resposta de cada etiqueta, é possível determinar o número mínimo de etiquetas que um interrogador (leitor) deverá ser capaz de identificar a cada segundo.

Esta subseção tem por finalidade apresentar uma análise de tempo com todos os protocolos anticolisão implementados nesta tese, considerando os seguintes cenários: otimista, moderado e pessimista. A Figura 5.2 apresenta os tempos de leitura das etiquetas para todos os protocolos anticolisão com diferentes tamanhos de *payload* e população de etiquetas de acordo com os cenários acima mencionados.

Conforme os resultados expostos na Figura 5.2, independentemente do cenário aplicado e do tamanho da população de etiquetas, todos os protocolos anticolisão apresentaram desempenhos semelhantes, exceto o Chen. Apesar dos resultados semelhantes, a proposta se destaca por demonstrar um desempenho levemente superior quando comparada a outros protocolos (ou seja, menor tempo de leitura para identificar todas as etiquetas).

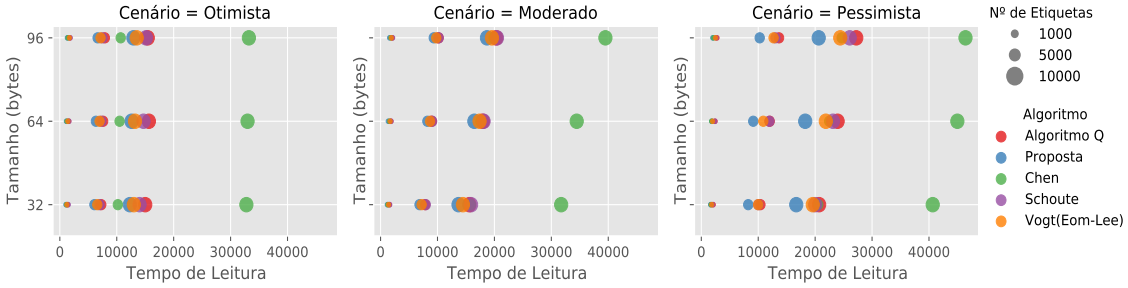

Figura 5.2: Tempos de leitura das etiquetas de todos os protocolos anticolisão considerando diferentes tamanhos de população de etiquetas nos cenários otimista, moderado e pessimista.

No cenário otimista, onde não há interferência no canal de comunicação, percebe-se que, independentemente do tamanho do *payload*, os tempos de leitura das etiquetas são quase iguais para todos os protocolos anticolisão. Por outro lado, nos cenários moderado e pessimista, que apresentam interferência no canal, pode-se constatar que o tamanho do *payload* tem impacto direto no tempo de leitura das etiquetas. Esse comportamento pode ser justificado pelo aumento do número de *slots* em colisão, uma vez que o canal de comunicação está sujeito a erros, sendo necessário o uso de retransmissões para identificar as etiquetas com sucesso.

Para compreender melhor o impacto causado pelo tamanho do *payload* nos tempos de leitura das etiquetas, a Tabela 5.2 mostra a diferença no tempo de leitura ao considerar os tamanhos do *payload* de 32 bytes e 96 bytes. Como pode ser observado, o tamanho do *payload* impacta no tempo de transmissão, uma vez que o leitor precisa de mais tempo para ler uma etiqueta com maior tamanho de *payload* (96 bytes), em comparação com o tamanho de *payload* inferior (32 e 64 bytes). Esse comportamento é ainda mais agravado quando a população de etiquetas e os níveis de interferência aumentam.

Claramente, o pior caso é apresentado pelo protocolo Chen quando o número de etiquetas varia de 5.000 a 10.000 nos cenários moderado e pessimista. Para o cenário moderado, a proposta apresenta a menor diferença no tempo de leitura das etiquetas quando a população é de 1.000 etiquetas, e o algoritmo do Schoute apresenta a menor diferença para uma população de 5.000 e 10.000 etiquetas. Em contrapartida, no cenário pessimista, a proposta aponta o melhor resultado, superando todos os demais algoritmos, independentemente do tamanho da população de etiquetas. Esse resultado indica que a proposta suporta problemas de interferência no canal melhor do que os outros algoritmos, pois é capaz de diminuir o número de *slots* em colisão, reduzindo assim o tempo de leitura das etiquetas.

Tabela 5.2: Diferença (em milissegundos) no tempo de leitura da etiqueta considerando os tamanhos de *payload* com 32 bytes e 96 bytes.

Cenário: **Otimista**

Protocolo	**Tamanho da População de Etiquetas**		
	1,000	5,000	10,000
Chen	253.06	**500.53**	443.79
Proposta	**250.03**	561.26	622.37
QAlgoritmo	394.53	629.17	**443.56**
Schoute	339.21	510.47	1,136.54
Vogt (Eom-Lee)	437.97	569.57	506.42

Cenário: **Moderado**

Protocolo	**Tamanho da População de Etiquetas**		
	1,000	5,000	10,000
Chen	513.90	3,990.88	7,771.99
Proposta	**401.13**	2,498.46	5,000.22
QAlgoritmo	472.96	2,368.76	4,728.62
Shoute	521.35	**2,261.32**	**4,550.23**
Vogt (Eom-Lee)	493.96	2,572.88	5,103.88

Cenário: **Pessimista**

Protocolo	**Tamanho da População de Etiquetas**		
	1,000	5,000	10,000
Chen	434.93	4,113.30	5,757.35
Proposta	**381.41**	**2,020.05**	**3,943.10**
QAlgoritmo	659.40	3,272.64	6,522.59
Shoute	604.22	3,021.07	6,056.22
Vogt (Eom-Lee)	654.35	2,713.05	4,832.08

Os valores destacados representam os melhores resultados para cada situação.

5.1.2 Análise de utilização dos *slots*

A métrica de quantidade de *slots* utilizados é uma das mais comuns para realizar a avaliação de desempenho em sistemas RFID, pois universaliza as medidas de desempenho dos protocolos anticolisão, independentemente da implementação, o que, de forma geral, facilita a comparação entre os mais variados algoritmos. No entanto, faz-se necessário destacar que muitas propostas podem obter resultados de desempenho semelhantes nessa métrica, porém diferenças em outros tipos de métricas.

Esta seção apresenta uma análise do uso de *slots* quanto ao seu estado (vazio, em colisão ou interferência) para todos os protocolos anticolisão, considerando os cenários

otimista, moderado e pessimista. A Figura 5.3 expõe os resultados do consumo de *slots* por todos os protocolos anticolisão considerados com diferentes tamanhos na população de etiquetas nos cenários mencionados acima.

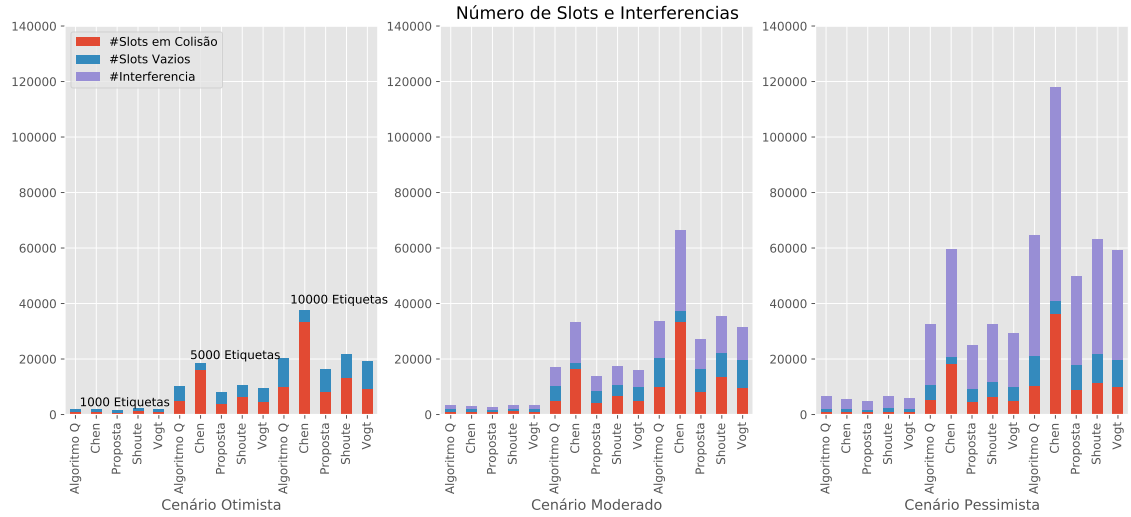

Figura 5.3: Número de *slots* em colisão, vazios e com interferência para todos os protocolos anticolisão ao considerar o tamanho da população com 1.000, 5.000 e 10.000 etiquetas para os cenários otimista, moderado e pessimista. O tamanho do *payload* considerado para esta avaliação foi de 64 bytes.

Para esta avaliação, foram consideradas as seguintes situações: *slots* vazios, onde não há transferência de dados durante sua permanência; *slots* em colisão, ocasião em que duas ou mais etiquetas iniciaram uma transmissão ao mesmo tempo e depois colidiram; e, por fim, a interferência sendo considerada como o período nos *slots*, em que ocorreram rajadas de ruído durante uma transmissão (ou seja, nessa conjuntura, os dados não são recuperáveis). A análise dessas métricas é de bastante relevância, pois acaba apresentando um fator impactante no resultado do tempo de leitura das etiquetas.

De acordo com os resultados da Figura 5.3, é possível perceber que todos os protocolos anticolisão possuem um desempenho semelhante considerando uma população de 1.000 etiquetas. Por outro lado, conforme o número de etiquetas aumenta para 5.000 e 10.000, a proposta se destaca por apresentar um melhor desempenho, quando comparada com os demais protocolos, principalmente durante o cenário pessimista.

Já o algoritmo do Chen obteve o pior resultado quando se leva em conta o número de 5.000 e 10.000 etiquetas. Esse resultado é justificado pela limitação imposta no tamanho do quadro subsequente, durante a execução do algoritmo, quando, de fato, faz-se necessária a realização de mais retransmissões, resultando, assim, em um aumento significativo do número de *slots* em colisão e interferência. Por outro lado, o Chen é capaz de reduzir

o número de *slots* vazios. Mais uma vez, é possível concluir que a proposta consegue se adaptar melhor a problemas de interferência no canal de comunicação quando comparada com os outros algoritmos anticolisão.

Para avaliar o impacto do modelo de interferência sobre o uso de *slots*, foi considerado como referência o algoritmo proposto. A Figura 5.4 demonstra o desempenho da proposta levando em consideração o tamanho da população com 10.000 etiquetas, com o uso de *payload* com tamanho de 64 bytes nos cenários moderado e pessimista.

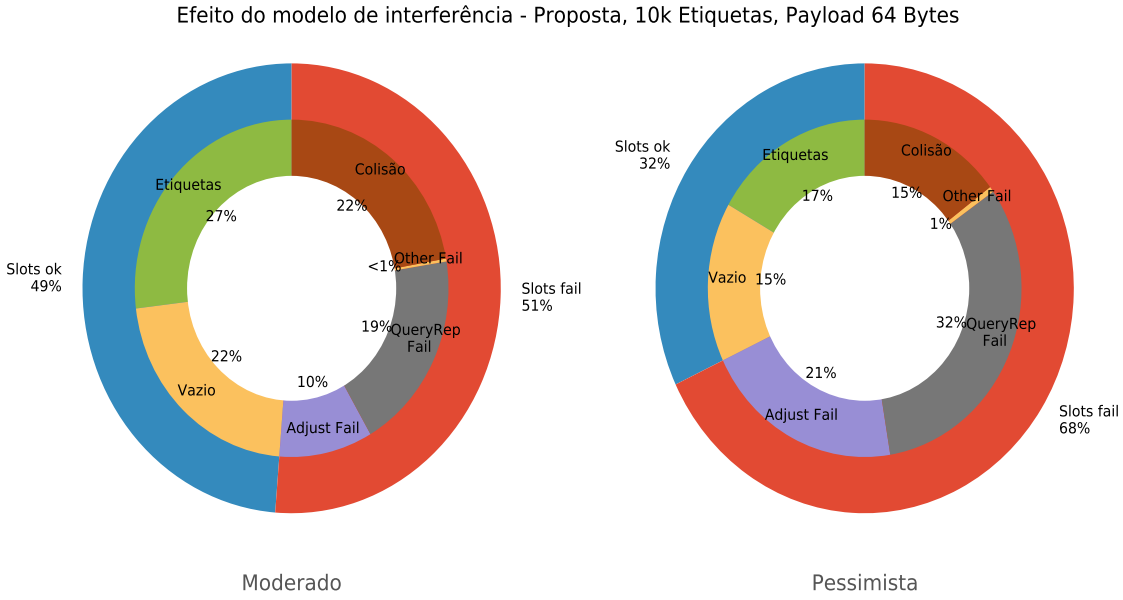

Figura 5.4: Impacto do modelo de interferência sobre o uso de *slots* com a proposta considerando o tamanho da população com 10.000 etiquetas, com tamanho de 64 bytes no *payload* para os cenários moderado e pessimista.

Na Figura 5.4, os *slots ok* representam etiquetas identificadas com sucesso (Denotada Etiquetas) e *slots* vazios. Já os *slots* fail (*slots* em falhas) correspondem por *slots* em colisão, *"QueryRep fail"*, *"Adjust fail"* e outras falhas. No cenário moderado, pode ser apontado que 49% dos *slots* são constituídos de *slots ok* (ou seja, 27% de etiquetas identificadas + 22% de *slots* vazios) e para 51% dos *slots fail* (ou seja, 22% *slots* em colisão + 19% de comando *QueryRep fail* + 10% de comando *Adjust fail* + <1% outras falhas). Vale ressaltar que, para este nível de interferência que ocorre no canal de comunicação, há um certo equilíbrio entre as porcentagens de *slots ok* e *slots fail*.

No cenário pessimista, percebe-se que há aumento na porcentagem de *slots fail* (*slots* em falha), pois o canal de comunicação está sujeito a um nível de interferência mais elevado. Desta forma, sua composição é de 32% com *slots ok* (ou seja, 17% etiquetas identificadas com sucesso + 15% de *slots* vazios) e 68% de *slots fail (*slots em falhas) (ou

seja, 15% *slots* em colisão + 32% de comandos *QueryRep fail* + 21% de comandos *Adjust fail* + 1% de outras falhas).

Segundo os resultados apresentados, é possível concluir que o nível de interferência pode impactar diretamente no processo de leitura das etiquetas, comprometendo assim o desempenho da comunicação de todo o sistema, semelhante ao que acontece em aplicações práticas de cenário real.

5.1.3 Análise de perda de pacote

Esta análise tem como objetivo avaliar o impacto da interferência por perda de pacotes em relação ao tamanho do *payload* da etiqueta. O número de perda de pacotes por causa da interferência está diretamente relacionado ao tamanho do *payload* da etiqueta. Quanto mais elevado for o nível de interferência, maior será o seu impacto nas etiquetas com maior tamanho de *payload*. A Figura 5.5 apresenta esse comportamento, destacando como métrica a perda de pacotes devido à interferência para todos os protocolos anticolisão considerando diversos tamanhos de *payload* com uma população de 10.000 etiquetas nos cenários moderado e pessimista.

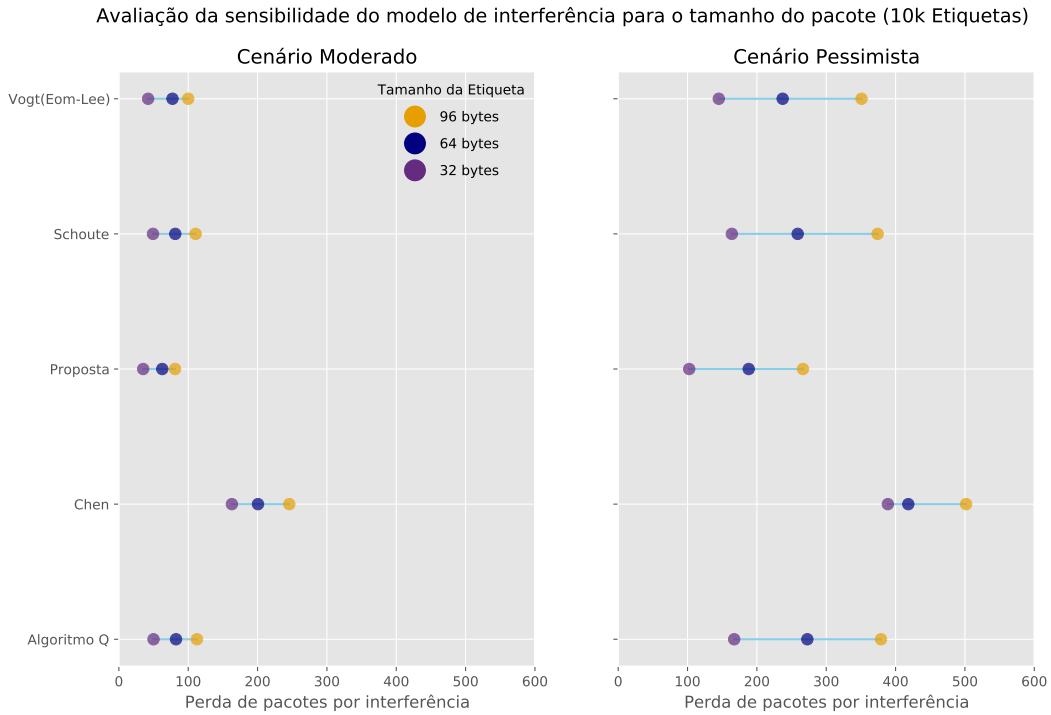

Figura 5.5: Perda de pacotes devido à interferência para todos os protocolos anticolisão considerando o tamanho do *payload* de 32, 64 e 96 bytes para uma população de 10.000 etiquetas nos cenários moderado e pessimista.

A partir dos resultados que foram expostos, pode-se compreender que a variação da perda de pacotes é bem menor para o cenário moderado quando comparada ao cenário pessimista. Além disso, fica evidente que quanto maior for tamanho do *payload*, mais suscetível a etiqueta se torna a interferências, provocando, consequentemente, mais perdas. Dessa forma, é possível concluir que, em um ambiente passível a interferências, recomenda-se a utilização de etiquetas de menor tamanho de *payload* para minimizar a perda de pacotes.

O desempenho de todos os protocolos anticolisão foi semelhante. No entanto, a proposta teve um melhor desempenho em ambos os cenários quando comparada aos demais algoritmos, pois foi capaz de reduzir significativamente a perda de pacotes. Em contrapartida, o protocolo do Chen apresentou o maior número de perdas de pacotes, mas, especificamente no cenário pessimista, o desempenho foi quase idêntico quando o tamanho do *payload* foi de 32 e 64 bytes.

5.1.4 Análise de Eficiência (Throughput)

A eficiência está diretamente relacionada com a capacidade de precisão que o sistema RFID possui para identificar o maior número de etiquetas dentro de um conjunto total. Para tanto, é preciso apresentar uma boa taxa de transmissão, tornando possível uma maior viabilidade de utilização para os diversos contextos de aplicações.

A análise de eficiência do sistema visa avaliar a capacidade máxima de transmissão de etiquetas a cada 100 *slots* de tempo para todos os protocolos anticolisão. Para esta análise, a taxa de transferência pode ser obtida da seguinte forma:

$$T_{hput} = \frac{N_{tags} \times N_{slots}}{N_{rounds^+}} \tag{5.1}$$

Nesta Equação, N_{tags} corresponde ao número de etiquetas, N_{slots} representa o número de *slots* de tempo e N_{rounds^+} refere-se ao número de ciclos de transmissões, representado pela soma de todas as oportunidades de transmissão (ou seja, a soma de todos os *slots* em colisão, *slots* vazios, *slots* bem-sucedidos, bem como falhas de comando, requisições e respostas de leitor e etiquetas durante o processo de identificação). Esta métrica é bastante relevante para avaliar a capacidade máxima de transmissão de etiquetas para todos os protocolos anticolisão, considerando os cenários otimista, moderado e pessimista. Para tanto, foi contabilizado o número de etiquetas com tamanho de *payload* de 64 bytes que podem ser transmitidas a cada 100 *slots* de tempo.

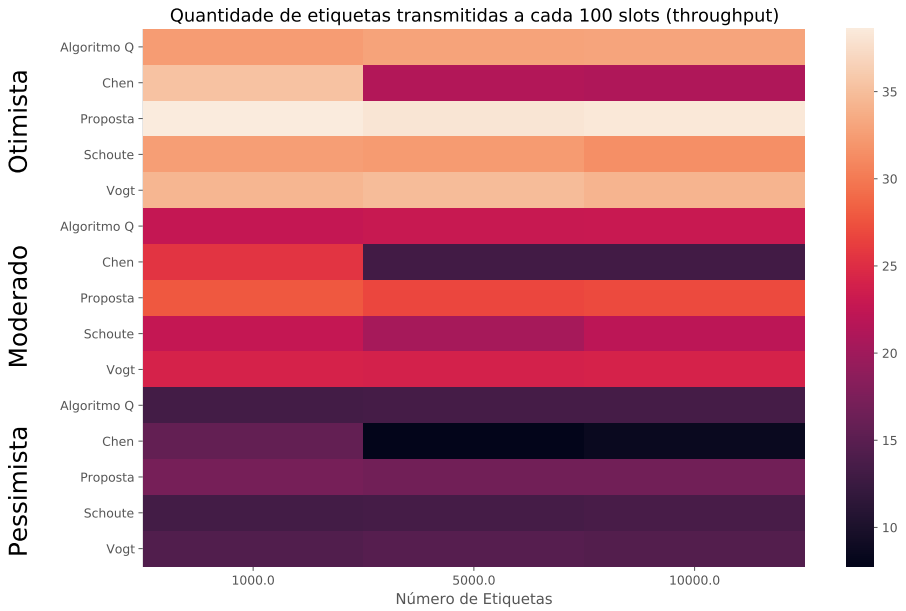

Figura 5.6: Eficiência (capacidade máxima de transmissão de etiquetas a cada 100 *slots* de tempo) com todos os protocolos anticolisão nos cenários otimista, moderado e pessimista considerando como tamanho de população de 1.000, 5.000 e 10.000 etiquetas.

O mapa de calor representado pela Figura 5.6 e os resultados conforme a Tabela 5.3 demonstram a eficiência de todos os protocolos anticolisão nos cenários otimista, moderado e pessimista considerando tamanho de população com 1.000, 5.000 e 10.000 etiquetas. As cores mais claras correspondem ao melhor desempenho, indicando que há um maior número de transmissões de etiquetas para cada 100 *slots*. De forma contrária, as cores mais escuras referem-se ao pior desempenho, em que há um número menor de transmissões de etiquetas a cada 100 *slots*.

Tabela 5.3: Eficiência (capacidade máxima de transmissão de etiqueta a cada 100 *slots* de tempo) para todos os protocolos anticolisão nos cenários otimista, moderado e pessimista, considerando como tamanho de população de 1.000, 5.000 e 10.000 etiquetas.

Algoritmo	**Cenário**								
	Otimista			**Moderado**			**Pessimista**		
	População de etiquetas			População de etiquetas			População de etiquetas		
	1,000	5,000	10,000	1,000	5,000	10,000	1,000	5,000	10,000
Chen	35.34	21.30	21.04	25.51	13.09	13.07	15.64	7.75	8.48
Proposta	**38.59**	**38.08**	**38.24**	**27.85**	**26.71**	**26.91**	**17.12**	**16.74**	**16.75**
Algoritmo Q	32.37	32.90	33.03	22.61	22.92	23.02	13.22	13.34	13.40
Schoute	32.51	32.25	31.42	22.60	20.41	22.00	13.22	13.37	13.66
Vogt (Eom-Lee)	34.35	34.85	34.15	24.02	24.00	24.11	14.37	14.64	14.49

Os valores destacados representam os melhores resultados em cada caso.

O protocolo Chen apresentou uma eficiência decrescente conforme houve um aumento do número de etiquetas, enquanto os demais apresentaram um desempenho de eficiência bastante estável, não sendo afetados pelo aumento da população de etiquetas. Os resultados expostos na Figura 5.6 e na Tabela 5.3 indicam que o algoritmo proposto é o mais eficiente, pois é capaz de transmitir um maior número de etiquetas a cada 100 *slots* de tempo, independentemente dos cenários e do tamanho da população de etiquetas, superando assim todos os demais protocolos que foram avaliados. Sem perda de generalidade, apesar de alguma similaridade no desempenho de eficiência, o algoritmo proposto provou ser uma opção de solução mais aprimorada.

5.1.5 Analisando o comportamento dos Protocolos

A utilização de um formalismo matemático, como as Redes de Petri Estocásticas Generalizadas, permite que seja possível a implementação prática de diferentes algoritmos e protocolos, realizando diversos tipos de procedimentos avaliativos com qualidade nos resultados. De fato, a adoção de modelos matemáticos pode apresentar alguns benefícios, como redução de custos durante a implantação e de tempo para fins de avaliação, favorecendo diretamente o desenvolvimento de novas abordagens. Para o contexto de comunicação RFID na Internet das Coisas Industrial, o modelo que foi proposto pode ser aplicado como ferramenta importante para auxiliar novos desenvolvimentos na área.

Os protocolos anticolisão considerados foram de grande utilidade para demonstrar como o modelo proposto baseado em GSPN pode ser explorado para realizar comparações práticas entre diferentes algoritmos. Os experimentos realizados nesta tese trouxeram resultados importantes, evidenciando que o algoritmo proposto consegue apresentar um melhor desempenho em relação aos demais protocolos, praticamente em todas as métricas avaliadas, em especial em situações como presença de canais ruidosos e grande número de etiquetas a serem lidas. Para aplicações reais, esse tipo de avaliação de qualidade é de extrema relevância.

A modelagem de canais com ruído e a forma como os leitores se comportam ao ler as etiquetas permitem a percepção de como os protocolos vão atuar quando o erro de transmissão aumenta. Como a confiabilidade é um componente do desempenho, a contabilização de pacotes descartados e a retransmissão de dados fornecem informações importantes sobre o nível de confiabilidade que pode ser alcançado pelo sistema. Paralelamente, o entendimento de desempenho também pode ser mensurado usando o modelo proposto baseado em GSPN, uma vez que erros de pacote aumentam e podem afetar diretamente no atraso da leitura das etiquetas. Portanto, o processamento combinado desses dois ele-

mentos é um argumento importante para a adoção de um modelo matemático, conforme proposto nesta tese.

Capítulo 6

Conclusão e Trabalhos Futuros

O RFID é uma das tecnologias essenciais utilizadas no contexto de (IIoT), o que está gerando um aumento significativo no uso de aplicações práticas, devido aos benefícios técnicos que lhe são proporcionados, como: recursos para detecção, eficiência energética, escalabilidade, acessibilidade de custos, confiabilidade e desempenho, os quais são atributos críticos indispensáveis para a usabilidade em ambiente industrial.

Como os sistemas RFID utilizam o meio sem fio para comunicação, existem alguns problemas que surgem no meio compartilhado, como colisões e interferência de sinais. Em geral, as colisões podem comprometer a comunicação dos sistemas RFID, pois podem ocorrer erros na identificação das etiquetas. Além disso, quando ocorrem colisões, uma estratégia de retransmissão é empregada, aumentando o consumo de energia e a largura de banda. Ao considerar etiquetas passivas, o problema de colisão pode ser agravado por sua limitação computacional. Na maioria dos casos, a comunicação se torna impossível, contudo, esse é um problema que pode ser resolvido.

Visando contribuir na resolução de problemas de acesso ao meio mantendo qualidade na comunicação dos sistemas RFID, esta tese traz como proposta um algoritmo anticolisão baseado em DFSA para identificar um grande volume de etiquetas, apresentando como técnica o uso do fator de envelhecimento que atua como um agente recompensador ou penalizador dos *slots* aproveitados de acordo com o desempenho obtido no processo de identificação anterior. Esse mecanismo atua como um filtro diminuindo o número de *slots* em colisões, mesmo quando a taxa de transmissão aumenta no canal de comunicação.

As propostas de protocolos anticolisão como DFSA surgem como possível solução para resolver os problemas de acesso ao meio. Porém, não exploram fatores importantes como confiabilidade e desempenho em conjunto, principalmente para uma escala maior de etiquetas, como é o caso de 10.000. O problema ocorre quando é preciso garantir uma boa qualidade no desempenho, mesmo que o ambiente apresente interferências no canal de comunicação que induzam a erros e falhas no sistema. Soluções para garantir

a confiabilidade e desempenho do sistema RFID foram investigadas na literatura. No entanto, elas consideram o canal de comunicação utilizado como sendo livre de erros, o que acaba ignorando eventuais problemas comuns que podem acontecer em ambientes de comunicação sem fio. Na prática, tornam o sistema menos realista, sendo um grande desafio para a implementações em cenário real.

Observando ausência de modelos precisos que avaliam a confiabilidade e desempenho em sistemas RFID, esta tese apresenta como contribuição o desenvolvimento de um modelo de simulação baseado em formalismo GSPN, buscando avaliar desempenho e confiabilidade, considerando a influência de falhas transitórias que podem afetar o canal de comunicação em sistemas RFID. Esse modelo foi cuidadosamente descrito neste trabalho, permitindo a replicação. Além disso, cinco diferentes protocolos anticolisão, inclusive o algoritmo proposto, foram implementados no referido modelo, apresentado, possibilitando realizar comparações mais realistas de desempenho e confiabilidade. Para tanto, foram concebidos vários cenários, nos quais o canal de comunicação está sujeito a apresentar diferentes níveis de interferência, para diferentes números de etiquetas e diversos tamanhos de seu *payload*.

Os experimentos realizados trouxeram resultados importantes para a avaliação de confiabilidade e desempenho. Embora não tenha sido explicitamente definido ou comparado, a avaliação combinada de parâmetros de confiabilidade e desempenho fornece dicas importantes a respeito de como avaliar os protocolos. Portanto, o modelo proposto e os experimentos realizados podem auxiliar significativamente na avaliação de confiabilidade e desempenho em aplicações reais para IIoT, potencializando a adoção de sistemas baseados em RFID para ambientes industriais.

As contribuições da respectiva tese podem ser listadas a seguir:

- Proposta de um algoritmo que utiliza como mecanismo um fator de envelhecimento que atua como fator recompensador ou penalizador dos *slots* bem-sucedidos de acordo com o desempenho no processo de identificação anterior;
- Um algoritmo que apresenta uma melhor desempenho em relação aos outros descritos nesse trabalho;
- Modelagem do protocolo DFSA em comunicações RFID, utilizando para tanto o formalismo GSPN. Esta modelagem visa permitir uma avaliação mais realista de algoritmos anticolisão baseados no protocolo DFSA;
- Definição de diferentes cenários de comunicação assumindo um conjunto de configurações de erro;
- Avaliação da confiabilidade e desempenho de diferentes algoritmos anticolisão;

- Análise de falhas de comunicações RFID.

Finalmente, como trabalhos futuros, pretende-se adotar um fator de envelhecimento que atue dinamicamente para melhorar o desempenho do algoritmo anticolisão proposto. A ideia é aprender o comportamento do canal de comunicação de acordo com uma janela deslizante de tamanho limitado. Adicionalmente, como mais uma contribuição, pretende-se desenvolver novos modelos de simulações baseados no formalismo GSPN, buscando avaliar questões de confiabilidade e desempenho para diferentes classes de protocolos anticolisão de etiquetas, como abordagens de protocolos baseados em árvore e híbridos. Resultados numéricos adicionais também são buscados, apoiando ainda mais as análises de confiabilidade e desempenho em aplicações industriais reais.

Referências Bibliográficas

Abbasiana, Amir & Masoumeh Safkhani (2020), 'Cncaa:a new anti-collision algorithm using both collided and non-collided parts of information', *Elsevier Computer Networks* **172**, 1–16.

Abdelgawad, A. & M. Bayoumi (2011), 'Remote measuring for sand in pipelines using wireless sensor network', *IEEE Transactions on Instrumentation and Measurement* **60**(4), 1443–1452.

Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari & Moussa Ayyash (2015), 'Internet of things: A survey on enabling technologies, protocols, and applications', *IEEE Communications Surveys Tutorials* **17**, 2347–2376.

Ali, Omar Massuod Salim Hassan (2012), Improved supply chain performance through RFID technology: comparative case analysis of Metro Group and Wal-Mart, Master of information systems technology - research thesis, Faculty of Informatics, University of Wollongong. Available at: `http://ro.uow.edu.au/theses/3774` [Accessed 08 set 2020].

Avizienis, A., J.-C. Laprie, B. Randell & C. Landwehr (2004), 'Basic concepts and taxonomy of dependable and secure computing', *IEEE transactions on dependable and secure computing* **1**, 11–33.

Bang, O., H. Jeon, S. Kim & H. Lee (2009), Efficient heterogeneous reader anti-collision methods for passive rfid systems, *em* '2009 IEEE 70th Vehicular Technology Conference Fall', pp. 1–5.

Benedetti, David, Gaia Maselli, Chiara Petrioli & Mauro Piva (2019), 'The impact of external interference on rfid anti-collision protocols', *IEEE Networking Letters* **1**(2), 76–79.

Bertelli, G., A. Santos, I. Silva, R. Fernandes, D. Brandao, I. Muller, J. Netto, J. Winter & C. E. Pereira (2017), 'Research activities on industrial wireless instrumentation: Brazilian perspective', *IEEE Instrumentation Measurement Magazine* **20**(2), 21–30.

Cairó, Josep-Ignasi, Jordi Bonache, Ferran Paredes & Ferran Martín (2018), 'Interference sources in congested environments and its effects in uhf-rfid systems: A review', *IEEE Journal of Radio Frequency Identification* **2**, 1–8.

Cerciello, Eleonora, Gianluca Massei & Luigi Paura (2014), Optimization of tag anti-collision algorithm for epc gen2 rfid, *em* '2014 Euro Med Telco Conference (EMTC)', pp. 1–6.

Chen, W. (2014), 'A feasible and easy-to-implement anticollision algorithm for the epc-global uhf class-1 generation-2 rfid protocol', *IEEE Transactions on Automation Science and Engineering* **11**(2), 485–491.

Cheng, T., M. Venugopal, J. Teizer & P. Vela (2011), 'Performance evaluation of ultra wideband technology for construction resource location tracking in harsh environments', *Automation in Construction* **20**(8), 1173–1184.

Costa, D. G., I. Silva, L. A. Guedes, P. Portugal & F. Vasques (2014), Selecting redundant nodes when addressing availability in wireless visual sensor networks, *em* '2014 12th IEEE International Conference on Industrial Informatics (INDIN)', pp. 130–135.

Costa, Daniel & Cristian Duran-Faundez (2018), 'Open-source electronics platforms as enabling technologies for smart cities: Recent developments and perspectives', *Electronics* **7**(12), 404.

da Silva, Ivanovitch Medeiros Dantas (2013), Uma metodologia para modelagem e avaliação da dependabilidade de redes industriais sem fio, Tese de doutorado, Universidade Federal do Rio Grande do Norte.

Daly, D., D.D. Deavours, J.M. Doyle, P.G. Webster & W.H. Mobius Sanders (2000), An extensible tool for performance and dependability modeling, *em* 'In Proceedings of the 11th International Conference on Computer Performance Evaluation: Modelling Techniques and Tools', p. 332–336.

Dantas, Jamilson, Rubens Matos, Jean Araujo & Paulo Maciel (2012), 'An availability model for eucalyptus platform: An analysis of warm-standy replication mechanism', *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* .

Ding, Kai, Pingyu Jiang & Shilong Su (2018), 'Rfid-enabled social manufacturing system for inter-enterprise monitoring and dispatching of integrated production and trans-

portation tasks', *Robotics and Computer-Integrated Manufacturing* **49**, 120 – 133. **URL:** *http://www.sciencedirect.com/science/article/pii/S073658451630196X*

Duan, H., H. Wu & Y. Zeng (2015*a*), Channel estimation for recovery of uhf rfid tag collision on physical layer, *em* '2015 International Conference on Computer, Information and Telecommunication Systems (CITS)', pp. 1–5.

Duan, H., H. Wu & Y. Zeng (2015*b*), Channel estimation for recovery of uhf rfid tag collision on physical layer, *em* '2015 International Conference on Computer, Information and Telecommunication Systems (CITS)', pp. 1–5.

Emenike, C. C., N. P. Van Eyk & A. J. Hoffman (2016), Improving cold chain logistics through rfid temperature sensing and predictive modelling, *em* '2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)', pp. 2331–2338.

Eom, Jun-Bong, Tae-Jin Lee, Ronald Rietman & Aylin Yener (2008), 'An efficient framed-slotted aloha algorithm with pilot frame and binary selection for anti-collision of rfid tags', *IEEE Communications Letters* **12**(11), 861–863.

EPCGlobal (2013), 'GS1 EPC Tag Data Standard 1.7 [Online]'. Disponível em: URL = `https://www.gs1.org/sites/default/files/docs/epc/tds_1_7-Sd.pdf` [Acessado em 01 de setembro de 2020].

Fernández-Caramés, T. M. & P. Fraga-Lamas (2018), 'A review on human-centered iot-connected smart labels for the industry 4.0', *IEEE Access* **6**, 25939–25957.

Filho, I. E. Barros, I. Silva & C. M. D. Viegas (2018), 'An effective extension of anti-collision protocol for rfid in the industrial internet of things (iiot)', *Sensors* **18**(4426).

Finkenzeller, Klaus (2010), Data Integrity, *em* 'RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication', Vol. 3, John Wiley & Sons, Ltd., capítulo 7, pp. 189–211.

Fraj, R. Ben, V. Beroulle, N. Fourty & A. Meddeb (2018), An evaluation of uhf rfid anti-collision protocols with ns2, *em* '2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)', pp. 1–6.

Garrido-Hidalgo, Celia, Teresa Olivares, F. Javier Ramirez & Luis Roda-Sanchez (2019), 'An end-to-end internet of things solution for reverse supply chain management in industry 4.0', *Computers in Industry* **112**, 103127.

Gong, W., H. Liu, J. Liu, X. Fan, K. Liu, Q. Ma & X. Ji (2018), 'Channel-aware rate adaptation for backscatter networks', *IEEE/ACM Transactions on Networking* **26**(2), 751–764.

ISO (2013), 'ISO/IEC 18000-6:2010 Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz [Online]'. Disponível em: `www.https://www.iso.org/standard/46149.html` [Acessado em 01 de setembro de 2020].

Jia, Xiaolin, Quanyuan Feng, Taihua Fan & Quanshui Lei (2012), Rfid technology and its applications in internet of things (iot), *em* '2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)'.

Klair, D. K., K. Chin & R. Raad (2010), 'A survey and tutorial of rfid anti-collision protocols', *IEEE Communications Surveys Tutorials* **12**(3), 400–421.

Kuo, Way & Ming J. Zuo (2003), 'Optimal reliability modeling: Principles and applications', *John Wiley Sons* .

Laprie, Jean-Claude (1995), Dependable computing: Concepts, limits, challenges, *em* '25th IEEE International Symposium on Fault-Tolerant Computing', pp. 42–54.

Li, Shuoming, Jianbin Lu & Shihong Chen (2020), 'A room-level tag trajectory recognition system based on multi-antenna rfid reader', *Elsevier Computer Communications* **149**, 350–355.

Lim, M. K., W. Bahr & S. Leung (2013), 'Rfid in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends', *Elsevier, International Journal of Production Economics* **145**(1), 409–430.

Lin, J., W. Yu, N. Zhang, X. Yang, H. Zhang & W. Zhao (2017), 'A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications', *IEEE Internet of Things Journal* **4**(5), 1125–1142.

Lumpkins, William (2015), 'Rfid: An evolution of change, from world war ii to the consumer marketplace', *IEEE Potentials* **34**, 6–12.

Marsan, M. A., G. Balbo, G. Conte, S. Donatelli & G. Franceschinis (1995), 'Modelling with generalized stochastic petri nets.', *Wiley Series in Parallel Computing - John Wiley and Sons* .

Mingliang, Wang & Yang Shun (2010), Improvement of anti-collision algorithm for rfid system based on tdma, *em* 'International Conference on Computational Problem-Solving', pp. 336–339.

Munir, Ahnaf, Md. Tahmid Rahman Laskar, Md. Sakhawat Hossen & Salimur Choudhury (2018), 'A localized fault tolerant load balancing algorithm for rfid systems', *Journal of Ambient Intelligence and Humanized Computing* **10**.

Murata, T. (1989), Petri nets: Properties, analysis and applications, *em* 'Proceedings of the IEEE', Vol. 77, pp. 541–580.

Portugal, Paulo José Lopes Machado (2004), Avaliação da Confiança no Funcionamento de Redes de Campo - Contribuição no Domínio dos Sistemas Industriais de Controlo, Tese de doutorado, Faculdade de Engenharia da Universidade do Porto.

Pradhan, D. K. (1996), Fault tolerant computer system design, *em* 'Prentice Hall'.

Sanders, W. H. (2005), Möbius user manual, *em* 'University of Illinois'.

Santos, A., D. Lopes, J. César, L. Luciano, A. Neto, L. A. Guedes & I. Silva (2015), Assessment of wirelesshart networks in closed-loop control system, *em* '2015 IEEE International Conference on Industrial Technology (ICIT)', pp. 2172–2177.

Schoute, F. (1983), 'Dynamic frame length aloha', *IEEE Transactions on Communications* **31**(4), 565–568.

Senadeera, Praharshin M., Numan S. Dogan, Zhijian Xie, Huseyin S. Savci, Ibraheem Kateeb & Mohammed K Ketel (2013), Recent trends in rfid transponders, *em* '2013 Proceedings of IEEE Southeastcon', pp. 4–7.

Silva, I. M. D., L. A. Guedes & F. Vasques (2008), Performance evaluation of a compression algorithm for wireless sensor networks in monitoring applications, *em* '2008 IEEE International Conference on Emerging Technologies and Factory Automation', pp. 672–678.

Silva, Ivanovitch, Rafael Leandro, Daniel Macedo & Luiz Affonso Guedes (2013), 'A dependability evaluation tool for the internet of things', *Computers & Electrical Engineering* **39**(7), 2005 – 2018.

Solic, Petar, Zoran Blazevic, Maja Skiljo, Luigi Patrono, Riccardo Colella & Joel J. P. C. Rodrigues (2017), 'Gen2 rfid as iot enabler: Characterization and performance improvement', *IEEE Wireless Communications* **24**(3), 33–39.

Song, Xiang, Xu Li, Weigong Zhang & Wencheng Tang (2016), 'Rfid application for vehicle fusion positioning in completely gps-denied environments', *Engineering Letters* **24**, 19–23.

Su, J., Z. Sheng, D. Hong & G. Wen (2016), 'An effective frame breaking policy for dynamic framed slotted aloha in rfid', *IEEE Communications Letters* **20**(4), 692–695.

Su, J., Z. Sheng, V. C. M. Leung & Y. Chen (2019), 'Energy efficient tag identification algorithms for rfid: Survey, motivation and new design', *IEEE Wireless Communications* **26**(3), 118–124.

Su, Jian, Yongrui Chen, Zhengguo Sheng, Zhong Huang & Alex X. Liu (2020), 'From m-ary query to bit query: A new strategy for efficient large-scale rfid identification', *IEEE Transactions on Communications* **68**(4), 2381–2393.

Su, Jian, Zhengguo Sheng, Alex X. Liu, Yu Han & Yongrui Chen (2019), 'A group-based binary splitting algorithm for uhf rfid anti-collision systems', *IEEE Transactions on Communications* **68**(2), 998–1012.

Sun, Chunling (2012), 'Application of rfid technology for logistics on internet of things', *AASRI Procedia* **1**, 106 – 111. AASRI Conference on Computational Intelligence and Bioinformatics.
URL: *http://www.sciencedirect.com/science/article/pii/S2212671612000200*

Tan, X., H. Wang, L. Fu, J. Wang, H. Min & D. W. Engels (2018), 'Collision detection and signal recovery for uhf rfid systems', *IEEE Transactions on Automation Science and Engineering* **15**(1), 239–250.

Tanenbaum, Andrew S. (2003), Redes de computadores.

Throttleman (2014), 'European Retailer Throttleman Improves Supply Chain with RFID [Online]'. Available at: `https://www.alientechnology.com/wp-content/uploads/Case-Study-European-Retailer-Throttleman-Improves-Supply-Chain-with-RFID.pdf` [Accessed 08 set 2020].

Tsao, Hsuan-Wei, Der-Jiunn Deng, Hsing-Wen Wang & Jung-Hsin Chang (2011), 'Runtime optimization of framed slotted aloha based rfid systems', *International Symposium on Wireless and Pervasive Computing* pp. 400–421.

Uckelmann, D., M. Isenberg, M. Teucke, H. Halfar & B. Scholz-Reiter (2010), 'Autonomous control and the internet of things: Increasing robustness, scalability and agility in logistic networks', *Unique Radio Innovation for the 21st Century* **3**, 163—-181.

Vahedi, E., R. K. Ward & I. F. Blake (2014), 'Performance analysis of rfid protocols: Cdma versus the standard epc gen-2', *IEEE Transactions on Automation Science and Engineering* **11**(4), 1250–1261.

Valentini, Roberto, Piergiuseppe di Marco, Roberto Alesii & Fortunato Santucci (2020), Exploiting capture diversity in distributed passive rfid systems, *em* '2020 10th Annual Computing and Communication Workshop and Conference (CCWC)'.

Vogt, Harald (2002), Efficient object identification with passive rfid tags, *em* F.Mattern & M.Naghshineh, eds., 'Pervasive Computing', Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 98–113.

Wang, Jianbo & Jiayue Wang (2020), 'Tracking method of agricultural products logistics based on rfid technology', *Springer* **1117**, 578–583.

Wang, Shuai, Liang Yin Weijun Hong & ShuFang Li (2012), 'A novel fast tag estimate method for dynamic frame length aloha anti-collision algorithms in rfid system', *IEEE Vehicular Technology Conference (VTC Fall)* pp. 1–5.

Weber, Taisy Silva (2002), 'Um roteiro para exploração dos conceitos básicos de tolerância a falhas', *Relatório técnico, Instituto de Informática UFRGS* .

Willig, A., M. Kubisch, C. Hoene & A. Wolisz (2002), 'Measurements of a wireless link in an industrial environment using an ieee 802.11-compliant physical layer', *IEEE Transactions on Industrial Electronics* **49**(6), 1265–1282.

Wu, H., Y. Wang & Y. Zeng (2018), 'Capture-aware bayesian rfid tag estimate for large-scale identification', *IEEE/CAA Journal of Automatica Sinica* **5**(1), 119–127.

Wu, Haifeng, Yu Zeng, Jihua Feng & Yu Gu (2013), 'Binary tree slotted aloha for passive rfid tag anticollision', *IEEE Transactions on Parallel and Distributed Systems* **24**(1), 19–31.

Xie, Xin, Xiulong Liu & Heng Qi (2019), 'Fast identification of multi-tagged objects for large-scale rfid systems', *IEEE Wireless Communications Letters* **8**(4), 992–995.

Xinqing, Yan & Zhang Fan (2010), Rapid rfid tag collision resolution with the frame slotted aloha protocol, *em* '2010 International Conference on Computer Application and System Modeling (ICCASM 2010)'.

Xu, Y. & Y. Chen (2015), An improved dynamic framed slotted aloha anti-collision algorithm based on estimation method for rfid systems, *em* '2015 IEEE International Conference on RFID (RFID)', pp. 1–8.

Xuan, Xiuwei & Kun Li (2019), 'Efcient anti-collision algorithm for rfid epc generation-2 protocol based on continuous detection', *International Journal of Wireless Information Networks* **27**, 133–143.

Yong, W., L. Qing, W. Lei & S. Hao (2017), Research on anti-collision algorithm in radio frequency identification technology, *em* '2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC)', Vol. 2, pp. 239–244.

Zhang, L., W. Xiang & X. Tang (2018), 'An efficient bit-detecting protocol for continuous tag recognition in mobile rfid systems', *IEEE Transactions on Mobile Computing* **17**(3), 503–516.

Zhang, L., W. Xiang, X. Tang, Q. Li & Q. Yan (2018), 'A time-and energy-aware collision tree protocol for efficient large-scale rfid tag identification.', *IEEE Trans. Industrial Informatics* **14**(6), 2406–2417.

Zhang, Youlin, Shigang Chen, You Zhou & Yuguang Fang (2020), 'Missing-tag detection with unknown tags', *IEEE/ACM Transactions on Networking* pp. 1–14.

Zhao, Jumin, Xiaojuan Liu & Dengao Li (2019), 'Fast and reliable burst data transmission for backscatter communications', *Sensors* **19**(5418), 1–16.

Zhong, Weifeng, Jinjin Chen, Liguo Wu & Mingyu Pan (2012), The application of aloha algorithm to anticollision of rfid tags, *em* 'Proceedings of 2012 International Conference on Measurement, Information and Control', Vol. 2, pp. 717–720.

Zhu, L. & T. P. Yum (2011), 'A critical survey and analysis of rfid anti-collision mechanisms', *IEEE Communications Magazine* **49**(5), 214–221.

Zullig, Leah L., Phil Mendys & Hayden B. Bosworth (2017), 'Medication adherence: A practical measurement selection guide using case studies', *Patient Education and*

Counseling **100**(7), 1410 – 1414.
URL: *http://www.sciencedirect.com/science/article/pii/S0738399117300654*