UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

Estudo e Simulação do Protocolo *Slotted Aloha* Multicanal aplicado a VANETs

João Paulo José Vicente da Silva

Trabalho de Graduação

RECIFE
Dezembro de 2018

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA

João Paulo José Vicente da Silva

Estudo e Simulação do Protocolo *Slotted Aloha* Multicanal aplicado a VANETs

Trabalho apresentado ao Programa de GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO do CENTRO DE INFORMÁTICA da UNIVERSIDADE FEDERAL DE PERNAMBUCO como requisito parcial para obtenção do grau de Bacharel em Engenharia da Computação.

Orientador: *Renato Mariz de Moraes*

RECIFE
Dezembro de 2018

Agradecimentos

À minha mãe, Dôra, e meu pai, Getúlio, maiores incentivadores da minha vida acadêmica, seres humanos exemplares e inspiradores, responsáveis primeiros por todas as minha conquistas.

À minha irmã, Maria Raíza, a melhor companhia que qualquer pessoa poderia querer e pessoa que mais amo neste mundo.

Aos outros membros da minha família, que ajudaram a formar meu caráter e me ensinaram muitas coisas. Em especial meus avós, João Côrreia e Tereza Cristina, de quem só tenho as lembranças e vivências mais doces.

Ao meu orientador, Professor Renato Mariz, por sua grande competência e paciência em me ajudar e ensinar durante toda minha vivência acadêmica, desde as Iniciações Científicas até este trabalho.

Aos meus amigos de graduação, Ana Lima, Augusto Queiroz, Bruno Filho, Carolina Cruz, Everlaynne Melo, Flávio Mattos, Gabriel D'Luca, Igor Carneiro, Jacqueline Alves, Jaílson Dias, Jorge Salvador, Luana Nunes, Lucca França, Mateus Nunes, Matheus de La Rocque, Moabe Renato, Ramom Pereira, Thomas Anderson e Vinícius de Moraes, que foram minhas companhias de muitos projetos, e em especial a Rogério Santos, por ter me acompanhado em quase tudo que fiz na universidade, e a Alliny Alves, por há anos me dar suporte e carinho incríveis.

Ao meu cachorro Darwin, por ser sempre uma fonte de alegria.

E por fim, a todos que me ajudaram direta ou indiretamente, minha gratidão.

Resumo

Acidentes de trânsito são responsáveis por inúmeros prejuízos financeiros e em vidas humanas todos os anos, além disso frequentemente causam sequelas com as quais muitas pessoas devem conviver pelo resto de suas vidas, em especial aos jovens. Uma das abordagens para tentar evitar situações de risco é a implementação de *Vehicular Ad Hoc Networks* (VANETs), que são redes nos quais os veículos são os nós de comunicação e através da qual podem trocar informações referentes à segurança da via. Mas as aplicações de segurança são reguladas e requisitos de desempenho estritos são exigidos. Muitos trabalhos já foram propostos acerca disso e este em particular baseia-se nas propostas de Rivera de protocolos adaptados do *Slotted Aloha* [1]. Neste trabalho faremos um estudo detalhado e rigoroso do *Slotted Aloha* para um contexto multicanal e estenderemos os protocolos de Rivera para múltiplos canais. Além disso, argumentaremos que em certos casos estes protocolos são passíveis de reformulações ou correções, e validaremos todas as propostas desenvolvidas com simulações em *software* projetadas para representar os eventos e não as equações. Mostraremos que todas as alterações sugeridas conseguem melhorar os requisitos de desempenho para as VANETs sem introduzir suposições artificiais na modelagem. Mais especificamente, obteremos a probabilidade ótima de acesso ao meio para os nós da rede e a consequente probabilidade de entrega com sucesso de mensagens de emergência empregando a estratégia de difusão (*broadcast*) com o protocolo *Slotted* Aloha.

Palavras-chave: *Broadcast*, Multicanal, Redes *Ad Hoc*, Segurança Veicular, *Slotted Aloha*, VANETs.

Abstract

Traffic accidents are responsible for a great loss of both human lives and financial values every year, and frequently cause major injury with which many people have to live their entire lives, a fate which is more likely to occur to young adults well within their productive years. On of the many ways to address this problem is by creating Vehicular Ad Hoc Networks (VANETs), which are networks with vehicles as nodes, and over which they can exchange safety information about the road. But safety applications are regulated and demand strict performance requirements. Many works in the literature have already addressed that, and this one is based on the work by Rivera [1] which proposes protocols adapted from Slotted Aloha. In this work we will proceed with a detailed and rigorous study of Multichannel Slotted Aloha and extend Rivera proposals for the multichannel case. We will also argue that there are cases when these protocols should be revised, and we validate our proposals with software simulation using MATLAB to represent the events themselves, not the equations. We will show that all suggestions achieve better results for performance requirement of safety VANET applications without imposing unnatural supositions on the models. More specifically, we obtain the optimum probability of channel access for the nodes and its consequent probability of successful emergency message delivery employing the broadcast strategy with the Slotted Aloha protocol.

Keywords: *Ad Hoc Networks, Broadcast, Multichannel, Slotted Aloha, VANETs, Vehicle Safety.*

Sumário

1 Introdução **1**
- 1.1 Motivação 1
- 1.2 Objetivos 2
- 1.3 Contribuições 2
- 1.4 Estrutura do Documento 3

2 Fundamentação Teórica **4**
- 2.1 VANETs 4
- 2.2 Confiabilidade em VANETs 5
  - 2.2.1 Restrições sobre a Probabilidade de Sucesso 6
  - 2.2.2 Restrições sobre a Latência 6
- 2.3 O Protocolo *Slotted* Aloha 7
  - 2.3.1 Vazão do *Slotted* Aloha 8
- 2.4 O Problema do Terminal Escondido 8
- 2.5 Camada Física (PHY) e as VANETs 9
- 2.6 VANETs e Difusão de Mensagens de Segurança 10
  - 2.6.1 Rebroadcasting 10
- 2.7 Os Modelos de Rivera 11
  - 2.7.1 Premissas Fundamentais 11
  - 2.7.2 Topologia da Rede 12
  - 2.7.3 Modelo Não-Periódico 13
    - 2.7.3.1 Probabilidade de Sucesso 13
  - 2.7.4 Modelo Periódico com Distribuição Geométrica 15
    - 2.7.4.1 Probabilidade de Sucesso 16
- 2.8 Conclusões 19

3 Slotted Aloha Multicanal **20**
- 3.1 Premissas 20
- 3.2 Vazão 22
- 3.3 Probabilidade Ótima de Transmissão 24

4 Protocolo de *Broadcast* Não-Periódico **26**
- 4.1 Modelo Não-Periódico Multicanal 26
  - 4.1.1 Resultados 27
- 4.2 Modelo Não-Periódico Alternativo 29
  - 4.2.1 Resultados 31

5 Protocolo de *Broadcast* Periódico **34**
5.1 Correção 34
5.2 Modelo Multicanal 35
5.2.1 Infinitos Canais 35
5.3 Resultados 36

6 Considerações Finais **41**
6.1 Trabalhos Futuros 41

Lista de Figuras

2.1 Configuração possível de VANET. Fonte: [11] 5
2.2 Período vulnerável do pacote em cinza no protocolo Aloha. O período τ é a duração em tempo do pacote. Fonte: baseado em gráfico similar presente em [19]. 7
2.3 Período vulnerável do pacote em cinza no protocolo *Slotted* Aloha. O período τ é a duração em tempo do pacote. 7
2.4 Exemplo da ocorrência de terminais escondidos. 9
2.5 Distribuição dos nós na rede. Fonte: Reprodução baseada no original de Rivera [1]. 12
2.6 Exemplos do Modelo Não-Periódico, calculado pela equação (2.11). 14
2.7 Diagrama de retransmissões. Fonte: [1]. 15
2.8 p_s em função de M para o modelo geométrico com p_f fixo em 10% e $D_f = 500$ slots, variando-se o número de repetições N. 17
2.9 p_s em função de M para o modelo geométrico com com N fixo em 20 e $D_f = 500$ slots, variando-se a probabilidade falha na recepção p_f. 18
2.10 p_s em função de M para os modelo geométrico e não-periódico com N fixo em 10 e $D_f = 500$ *slots*, com $p_f = 0$. 18

3.1 Diferentes possibilidades de tentativas de envio para 3 canais e 3 *slots*. τ representa a duração de um pacote no tempo e as setas indicam pacotes direcionados para o *slot*. 21

4.1 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 1$, o que equivale a aproximadamente $M = 13$. 27
4.2 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 3$, o que equivale a aproximadamente $M = 38$. 28
4.3 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 5$, o que equivale a aproximadamente $M = 63$. 28
4.4 Exemplo de esgotamento da estratégia do multicanal, com $\lambda = 4$. 29
4.5 Comparativo entre políticas de transmissão. 30
4.6 Comparativo entre modelos não-periódicos considerando $p_f = 0$ e $\lambda = 3$. $M =$ 38, aproximadamente. Apenas 1 Canal de comunicação é considerado. 31
4.7 Comparativo entre modelos não-periódicos considerando $p_f = 0$ e $\lambda = 6$. $M =$ 75, aproximadamente. São considerados 3 canais. 32
4.8 Estudo de aderência da simulação com o modelo alternativo para $\lambda = 3$, $p_f = 0$ e 1 canal. 1000 rodadas de simulação. 32

4.9 Estudo de aderência da simulação com o modelo alternativo para $\lambda = 3$, $p_f = 0$ e 3 canais. 1000 rodadas de simulação. 33

5.1 Validação da correção ao modelo geométrico proposto por Rivera [1], com $N = 10$, 1 canal e $p_f = 0,1$. 1000 rodadas de simulação. 37
5.2 Validação da correção ao modelo geométrico proposto por Rivera [1], com $N = 5$, 1 canal e $p_f = 0,1$. 1000 rodadas de simulação. 37
5.3 Comparação entre simulação e modelo para 3 canais, considerando $p_f = 0,1$. 1000 rodadas de simulação. 38
5.4 Comparação pela quantidade de canais, com $N = 10$ e $p_f = 0,1$. 38
5.5 Comparação da aderência aos requisitos de entrega do pacote pela quantidade de canais, com $N = 10$ e $p_f = 5\%$. 39
5.6 Comparação da aderência aos requisitos de entrega do pacote pela quantidade de canais, com $N = 10$ e $p_f = 10\%$. 39

CAPÍTULO 1

Introdução

1.1 Motivação

De acordo com o último relatório global sobre o estado da segurança viária da Organização Mundial da Saúde (OMS), em 2015 foram contabilizadas 1,25 milhões de mortes nos 180 países pesquisados devido a acidentes de trânsito [2]. Além disso, de acordo com o relatório, as lesões decorrentes são a maior causa de morte global entre jovens de 15 a 29 anos, com aproxidamente 350.000 vítimas fatais apenas no ano de 2012. Mesmo entre a população em geral, os acidentes de trânsito ainda estão entre as 10 causas de morte mais comuns, com projeções de se tornarem a sétima causa mais comum em todo o globo por volta de 2030.

O último estudo do Departamento de Transporte dos EUA, referente ao ano de 2015 e publicado em 2016, contabilizou mais de 6 milhões de acidentes de trânsito segundo relato das forças policiais, resultando em aproximadamente 35 mil mortos e 2,5 milhões de feridos. É esperado que nos EUA a cada 100 condutores habilitados 1 sofra algum tipo de ferimento devido a acidentes de trânsito. Dentre todos os possíveis acidentes as colisões entre veículos foram o mais comum e as principais responsáveis por mortes e ferimentos. O custo econômico anual dos acidentes de trânsito foi estimado na ordem de centenas de milhões de dólares, apenas nos EUA, e custos semelhantes são esperados devido aos congestionamentos de tráfego. O estudo estimou também que os custos financeiros para a economia americana, já levando em consideração a existência de casos não reportados, foram de aproximadamente US$ 242 bilhões apenas em 2010 [3].

Muitas das colisões ocorrem em circunstâncias evitáveis, como por excesso de velocidade, avanço de semáforos e descuido em cruzamentos com outros veículos que se aproximam por via lateral. É claro que um sistema de notificação prévia que avaliasse riscos *in loco* poderia reduzir significativamente a quantidade de acidentes e ajudar a mitigar os custos econômicos e humanos envolvidos. Uma das abordagens que permite a criação de um sistema como este é a implementação de Redes *Ad Hoc* Veiculares (VANETs, do inglês *Vehicular Ad Hoc Networks*). Nas VANETs os veículos atuam como nós numa rede estabelecida através de um canal sem fio, comunicando-se entre si sem a necessidade de pontos de acesso ou uma infraestrutura estabelecida. Uma importante aplicação das VANETs é alertar rapidamente todos os veículos de uma determinada área sobre informações de segurança, de assistência ao condutor e/ou sobre as condições da via. Isso normalmente é feito difundindo mensagens de *broadcast* que carregam essas informações pela rede sem fio [4].

Embora as mensagens de *broadcast* tenham muitas outras aplicações diversas, incluindo manutenção da topologia da rede [5] e disseminação de informações de roteamento [6], no contexto das VANETs existe uma preocupação primordial com a segurança, e é possível es-

palhar mensagens de *broadcast* para várias aplicações desta natureza, como avisos a sistemas de emergência, indicação de condições adversas na estrada, notificação automática de colisões, etc. Decorre disso que, ao contrário do que acontece em geral nas Redes *Ad Hoc*, o consumo de energia dos nós não é um problema (uma vez que estão conectados aos veículos), mas sim as restrições rigorosas no prazo final de entrega da mensagem em *broadcast* para todos os nós da rede, que precisam respeitar um determinado prazo (*deadline*) para manter sua utilidade e evitar acidentes [7].

E dado ao aspecto de, em geral, ausência de infraestrutura na rede sem fio para estes veículos, é importante se investigar novos protocolos de comunicação que sejam simples e eficientes em atingir as restrições de entrega de mensagens. Assim este trabalho considera o protocolo *Slotted* Aloha para esta aplicação em VANETs.

1.2 Objetivos

O objetivo **geral** deste trabalho é estudar o desempenho do protocolo *Slotted* Aloha na entrega de mensagens de *broadcast* para os nós numa VANET com um prazo de entrega final rígido, utilizando mais de um canal independente de comunicação. A principal medida considerada é a probabilidade de que todos os receptores dentro do alcance de um nó interessado em transmitir uma mensagem de *broadcast* efetivamente recebam os dados enviados sem erro.

São objetivos **específicos** deste projeto:

- Formular o modelo teórico do protocolo *Slotted* Aloha multicanal;
- Simular o protocolo *Slotted* Aloha multicanal;
- Alterar os experimentos de Rivera e Moraes [1], [8] considerando o protocolo *Slotted* Aloha multicanal para estudar seu desempenho, tanto em modelo teórico quanto em simulação por *software*;
- Comparar os protocolos *Slotted* Aloha monocanal e multicanal com base nos resultados obtidos;
- Escrever um artigo científico a ser submetido para publicação na área.

1.3 Contribuições

Este trabalho propõe como contribuições a modelagem formal do protocolo *Slotted* Aloha multicanal (considerando canais com características idênticas, como capacidade e etc), a extensão dos modelos de Rivera para o caso multicanal, um modelo de transmissão de *broadcast* não-periódico alternativo ao proposto por Rivera e que atinge resultados significativamente melhores quanto à probabilidade de sucesso da mensagem, e também propõe uma correção ao modelo de transmissão utilizando distribuição geométrica, com a qual também se obtém resultados melhores. Além disso, as extensões e melhorias propostas são todas simuladas por *software* e suas predições são validadas.

1.4 Estrutura do Documento

O restante deste trabalho está organizado da seguinte forma: O *Capítulo 2* revisa os conceitos fundamentais sobre VANETs, suas aplicações mais comuns, trata de problemas típicos de Redes *Ad Hoc* como o Terminal Escondido e falhas devidas a fenômenos de camada física (PHY), refaz o estudo do protocolo *Slotted* Aloha em termos de sua vazão e apresenta a modelagem dos terminais escondidos publicada por Rivera e Moraes [8] e detalha os modelos de protocolo propostos por Rivera [1]. O *Capítulo 3* apresenta uma generalização para *Slotted* Aloha multicanal e avalia o quanto o acréscimo de canais melhora a vazão do protocolo. O *Capítulo 4* generaliza o modelo de transmissões não-periódicas proposto por Rivera [1] para o caso multicanal e além disso reinterpreta as premissas adotadas de maneira a construir outro protocolo, que obtém melhores resultados. O *Capítulo 5* trata do modelo de retransmissões periódicas seguindo distribuição geométrica também proposto por Rivera [1], introduzindo uma correção importante nas equações do modelo e generalizando-o para o caso multicanal. O *Capítulo 6* apresenta as conclusões e considerações finais do estudo, indicando os trabalhos futuros.

CAPÍTULO 2

Fundamentação Teórica

Neste capítulo abordaremos conceitos relativos às VANETs (*Veicular Ad Hoc Networks*), com foco nas preocupações de segurança veicular e em especial na confiabilidade de se usar mensagens de *broadcast* para atingir os requisitos de segurança. Também faremos uma discussão breve sobre o Slotted Aloha clássico. Problemas típicos de redes *Ad Hoc* como Terminais Escondidos e perda de pacotes por erros na camada física também serão discutidos.

2.1 VANETs

As VANETs são redes sem fio onde os nós em comunicação são os veículos e possivelmente unidades de controle presentes nas vias. As VANETs também são chamadas ocasionalmente de *Inter-Vehicle Communications* (IVC) ou *Vehichle to Vehicle Communications* (V2V) [9] e o alcance de transmissão de cada nó é determinado pelo protocolo IEEE 802.11p como sendo de 1km [10].

Sendo redes *Ad Hoc*, as VANETs não requerem nenhum tipo de infraestrutura, mas é comum que se cogite algum tipo de infraestrutura fixa nas vias com o objetivo de melhorar a comunicação devido às características diferentes que as VANETs costumam ter em comparação com os outros de tipos de *Mobile Ad Hoc Networks* (MANETs), das quais as mais importantes são:

- Os nós (veículos) possuem velocidade média muito maior que em outros tipos mais gerais de MANETs, o que acarreta numa topologia de rede muito dinâmica, com nós entrando e saindo da área de alcance uns dos outros muito rapidamente.
- A área de cobertura da rede tende a ser muito grande, uma vez que os veículos costumam se deslocar através de grandes distâncias
- O consumo de energia e o custo de cada nó, preocupações típicas em redes *Ad Hoc*, não são majoritárias em VANETs, uma vez que os veículos já são caros e o custo adicional de equipá-los com a tecnologia necessária não impacta muito significativamente seu preço final. Além disso, todos os veículos possuem baterias de longo prazo e são capazes de recarregá-las pelo próprio motor do veículo.

A Figura 2.1 mostra uma das configurações possíveis que uma VANET pode assumir, com a comunicação ocorrendo majoritariamente entre os veículos mas com ocasionais trocas de dados entre os veículos e estações fixas (infraestrutura) ao longo da via. A utilização ou não da comunicação entre veículos e infraestrutura (V2I/I2V) depende principalmente da aplicação da

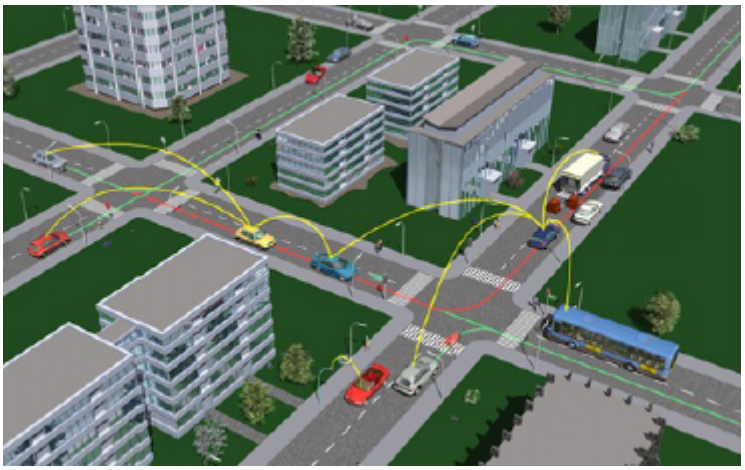

Figura 2.1 Configuração possível de VANET. Fonte: [11]

VANET em questão, e geralmente essa forma de comunicação é mais comum em aplicações de conveniência, como entretenimento, pagamentos, otimização de tráfego e/ou cálculo de melhores rotas. O escopo deste trabalho se restringe exclusivamente à aplicações de segurança, que se distinguem em dois tipos [12]:

- *Safety-critical*: Se referem à situações críticas em que acidentes podem ser iminentes, estas aplicações possuem máxima prioridade e possuem regulação estrita sobre o *delay* (latência) máximo com o qual um nó deve entregar sua mensagem aos outros dentro do seu alcance (**100ms**), por isso a probabilidade de que uma mensagem de *broadcast* seja corretamente recebida pelos outros nós deve ser muito alta.

- *Safety-related*: Se referem à aplicações onde o risco é considerado ou pequeno ou até mesmo alto, porém muito previsível. As restrições sobre a latência nesse caso não são rígidas.

As aplicações críticas são as de maior interesse para este trabalho, cujo objetivo mais geral é avaliar se é possível respeitar as restrições de segurança usando o protocolo *Slotted* Aloha.

2.2 Confiabilidade em VANETs

Em aplicações críticas de segurança é essencial que os protocolos de comunicação forneçam mensagens de *broadcast* de entrega confiável e respeitando *deadlines* específicos [13]. Para as VANETs, a preocupação principal é desenvolver protocolos que possam entregar uma mensagem que parte de um único nó para todos os outros dentro de seu alcance de transmissão com a maior probabilidade de sucesso e com a menor latência possível [14]. Definidas mais formalmente, as duas métricas de desempenho mais importantes são:

- Probabilidade de Sucesso: Probabilidade de que todos os nós receptores recebam com sucesso a mensagem de *broadcast*. Esta métrica descreve um requisito bastante específico, se apenas um nó não receber a mensagem o evento não será contabilizado como um

quase sucesso mas como uma falha e significa tanto quanto se ocorresse de algum nó não receber a mensagem, mesmo que apenas um.

- Latência: O tempo total necessário para que uma única mensagem de *broadcast* seja recebida por todos os nós dentro do alcance de transmissão. Mais uma vez, esta é uma restrição completamente severa. A latência máxima permissível é muitas vezes referida como *deadline*, uma nomenclatura adotada neste trabalho.

2.2.1 Restrições sobre a Probabilidade de Sucesso

Como a distribuição de informações locais sobre a segurança da via é a preocupação principal em aplicações críticas de segurança em VANETS, vários órgãos reguladores analisaram a questão e propuseram restrições. No SAE-J2735, a Sociedade de Engenheiros Automotivos (SAE) argumentou que todos os vizinhos de um salto (dentro do alcance de transmissão) do nó que transmite em *broadcast* devem receber com sucesso a mensagem, uma vez que mesmo que apenas um nó fique faltando ele representa um veículo não notificado sobre o risco iminente, e pode se transformar num evento de risco adicional para todos os outros.

Usando o mesmo pressuposto, o Ministério de Transportes e Telecomunicações do Japão determinou em 2010 que a probabilidade de falha das mensagens de segurança numa VANET não poderia exceder 0,01, o que equivale a uma taxa de entrega de pacotes de **99,9%** [15]. Esta mesma exigência foi sugerida também pelo *Car-2-Car Communication Consortium Europe* (C2C), que definiu que para aplicações de segurança uma mensagem de *broadcast* deve atingir o maior número possível de destinatários [16].

2.2.2 Restrições sobre a Latência

Um sistema de segurança construído sobre uma VANET é tão robusto quanto a sua capacidade de reconhecer e alertar sobre uma situação de perigo iminente antes que os condutores dos veículos ao redor se envolvam num acidente. Contudo, devido às altas velocidades que os veículos podem atingir e do período necessário para que os condutores reajam, não há muito tempo disponível para que isso aconteça. A duração do período de processamento mental de um condutor, que envolve perceber um risco e tomar a decisão do que fazer com relação a ele, demora entre 500ms e 1,2s, de acordo com o quão inesperado era o evento [17]. Como a própria mensagem de alerta requer um tempo de processamento no transmissor e em cada um dos receptores, o tempo de entrega da mensagem de segurança foi determinado em **100ms**, de modo a não atrasar significativamente as ações de mitigação de risco [18].

2.3 O Protocolo *Slotted* Aloha

O protocolo *Slotted* Aloha foi proposto para melhorar a eficiência do *Aloha* básico, o qual permite a um nó começar uma transmissão a qualquer momento sem absolutamente nenhum tipo de controle, desde que acerte uma cara (ou coroa) ao lançar uma moeda com probabilidade p pré-definida de ocorrer e igual para todos os nós. A ideia do *Slotted* Aloha é restringir qualquer transmissão para sempre no início de períodos de tempo de duração fixa chamados de *slots* de comunicação. Sempre que um nó tiver um pacote para enviar, ele deve esperar o início do próximo *slot* e além disso os tamanhos dos pacotes de dados são determinados de forma a casar perfeitamente com a duração de um *slot*.

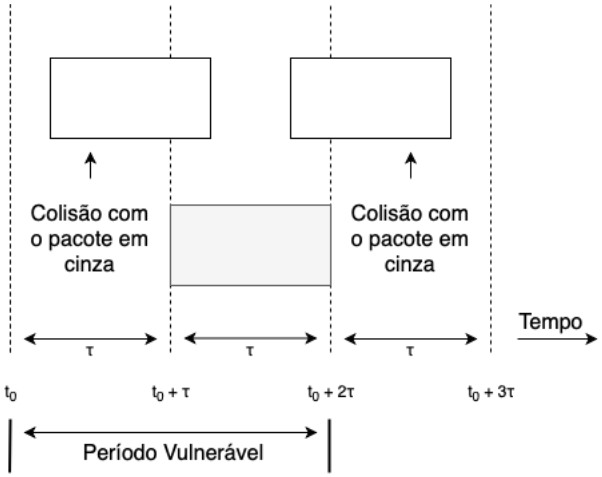

Figura 2.2 Período vulnerável do pacote em cinza no protocolo Aloha. O período τ é a duração em tempo do pacote. Fonte: baseado em gráfico similar presente em [19].

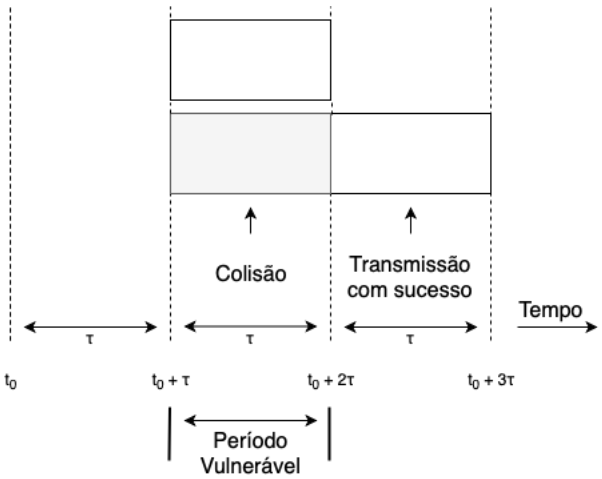

Figura 2.3 Período vulnerável do pacote em cinza no protocolo *Slotted* Aloha. O período τ é a duração em tempo do pacote.

As Figuras 2.2 e 2.3 mostram o quanto limitar as transmissões para o ínicio dos *slots* de comunicação pode ser benéfico para evitar colisões. Na Figura 2.2, o pacote em cinza se envolve em colisões com o fim e início de outros pacotes, enquanto na Figura 2.3 como os pacotes estão limitados a serem transmitidos no início de um *slot*, ao menos um deles será transmitido corretamente sem colisão, em vez de os três falharem. Considerando τ como o período de tempo que dura um *slot*, nota-se que o período vulnerável para cada pacote no protocolo Aloha é de τ, enquanto no *Slotted* Aloha é de τ.

2.3.1 Vazão do *Slotted* Aloha

A vazão (S) representa o número médio de pacotes transmitidos com sucesso por unidade de tempo. Para determiná-la, pode-se focar num pacote específico e calcular a probabilidade de que seja entregue com sucesso. Considerando um total de N usuários no sistema, com todos os pacotes tendo duração de transmissão $\boldsymbol{T}$ e uma probabilidade p de transmissão por *slot* (a rede é presumida em saturação, todos os nós têm infinitos pacotes em suas respectivas filas para transmitir) ao focarmos num período de tempo $\boldsymbol{T}$ o máximo que se pode conseguir é transmitir um pacote com sucesso. São esperadas N tentativas de transmitir, cada uma com probabilidade p, e dado que uma transmissão ocorrerá, todas as outras devem não ocorrer, portanto

$$S = Np(1-p)^{N-1}. \tag{2.1}$$

Para encontrar a probabilidade p que maximiza S, basta derivar a equação (2.1) com relação a p e igualá-la a zero, donde se obtém

$$\frac{dS}{dp} = N\left[(1-p)^{N-1} + p(N-1) + (1-p)^{N-1}(-1)\right] = 0 \tag{2.2}$$

e resolvendo-a tem-se

$$p = \frac{1}{N}. \tag{2.3}$$

Substituindo o valor ótimo de p na equação (2.1), obtém-se a vazão ótima a depender da quantidade de nós N como

$$S = \frac{(1-\frac{1}{N})^N}{1-\frac{1}{N}} \tag{2.4}$$

e tomando o limite com N tendendo ao infinito, chega-se no resultado final

$$S = \lim_{N\to\infty} \frac{(1-\frac{1}{N})^N}{1-\frac{1}{N}} = \frac{1}{e}. \tag{2.5}$$

2.4 O Problema do Terminal Escondido

Apesar de que numa rede *Ad Hoc* é possível que múltiplas transmissões possam ocorrer com sucesso ao mesmo tempo, essa capacidade pode ser ofuscada muito frequentemente pelo pro-

blema do terminal escondido. Um par de terminais escondidos ocorre quando dois nós não estão ao alcance de comunicação um do outro, mas compartilham um ou mais nós intermediários que estão dentro do alcance de ambos.

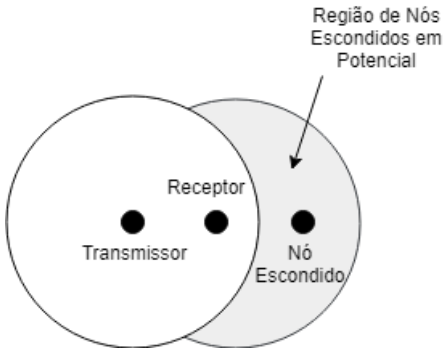

Figura 2.4 Exemplo da ocorrência de terminais escondidos.

Como mostra a Figura 2.4, o nó transmissor e o escondido formam um par de terminais escondidos, se qualquer um deles tentar transmitir para o receptor ao mesmo tempo em que o outro também está tentando ocorrerá uma colisão no receptor. Contudo, nenhum dos nós pertencentes ao par pode saber que o outro está transmitindo mesmo detecção de portadora (*carrier sense*), uma vez que não estão ao alcance um do outro. Para o caso de transmissões em *broadcast* este problema é severamente aumentado, uma vez que a região potencial para nós escondidos se estende por uma coroa circular em volta de toda a região de alcance do nó transmissor.

Como os terminais escondidos têm um impacto bastante grande sobre o desempenho de redes *Ad Hoc* em geral, vários protocolos adotaram estratégias para mitigar seus efeitos. O protocolo IEEE 802.11 por exemplo dá suporte ao mecanismo RTS/CTS (*request to send* e *clear to send*) cujo objetivo é estabeler uma comunicação prévia de controle entre transmissor e receptor para que este último confirme ao transmissor que ele pode enviar sua mensagem sem risco de colisões. Embora esse mecanismo combata o efeito dos terminais escondidos em transmissões *unicast*, não está disponível para o caso *broadcast*.

2.5 Camada Física (PHY) e as VANETs

O canal de comunicação enquanto meio físico tem um impacto muito grande na recepção dos pacotes de comunicação. O efeito onipresente é a perda pelo caminho entre o transmissor e os receptores, que é causada pela dissipação de potência irradiada ao longo da distância [20] que os separa. Outros efeitos de camada PHY também ocorrem frequentemente, como o sombreamento, que acontece por influência de obstáculos materiais entre transmissor e receptor que atenuam a potência do sinal por absorção, reflexão, refração ou espalhamento. Tanto o sombreamento como a perdo por caminho são considerados efeitos de longa distância, em contraste com o efeito de multicaminho, que se manifesta mais fortemente em distância de menor escala e consiste na recepção de várias versões do sinal transmitido, deslocadas em fase

e/ou frequência em comparação com o sinal da linha de visada direta (*Line of Sight* - LOS) [21].

Neste trabalho, e conforme foi usado em [1], será introduzido um termo constante p_f que representa a probabilidade de falha em cada um dos receptores, de maneira a representar de maneira simplificada o conjunto de diversas falhas que podem acontecer na camada PHY.

2.6 VANETs e Difusão de Mensagens de Segurança

Qualquer aplicação crítica de segurança usando VANETs exige que os veículos transmitam mensagens de alerta aos seus vizinhos [22], mas como já foi discutido em sessões anteriores existem restrições bastante rígidas sobre a confiabilidade na entrega destas mensagens e na latência com que isso acontece. Existe uma certa Qualidade de Serviço (QoS) que deve ser garantida para as mensagens de segurança em *broadcast*.

Algumas simulações já foram realizadas com o protocolo 802.11p para redes veiculares e embora os requisitos de latência tenham sido respeitados, o protocolo não obteve probabilidade de sucesso nas recepções suficientemente grande [23], além disso estudos posteriores relataram que modelagens mais realistas da propagação da informação em camada PHY indicaram uma influência maior dos terminais escondidos e resultados em geral piores [24].

Extensões do mecanismo RTS/CTS, eficiente para evitar terminais escondidos em condições *unicast* foram propostas. Uma das abordagens utilizadas foi tomar o mecanismo para todos os receptores ao alcance do transmissor [25] e a outra foi eleger como representante o vizinho mais distante e usá-lo para estimar o comportamento do grupo [26]. Essas abordagens não foram consideradas satisfatórias uma vez que os pacotes de controle tendem a ser maiores que os de segurança e por isso gastam muito os recursos da rede, além disso a inundação da rede com pacotes de controle adiciona à latência porque exige um período de negociação entre os nós e adicionalmente cria muitas chances de colisões entre os próprios pacotes de controle.

2.6.1 Rebroadcasting

Trabalhos mais recentes propuseram o reenvio de mensagens de *broadcast* como uma técnica viável para melhorar a confiabilidade na entrega dos pacotes [27]. O trabalho pioneiro que adotou essa abordagem definiu seis protocolos de camada MAC como candidatos a resolver as dificuldades das aplicações de segurança com VANETs [28]:

- *Asynchronous Fixed Repetition* (AFR): repete a mensagem de *broadcast* em todos os *slots* até um certo número fixo de tentativas;
- *Asynchronous P-persistent Repetition* (APR): o nó transmissor joga um moeda com probabilidade configurável *p* em todos os *slots*, transmitindo sempre que obtiver cara;
- *Synchronous Fixed Repetition* (SFR): Faz o mesmo que o AFR mas todos os nós são sincronizados globalmente;
- *Synchronous P-persistent Repetition* (SPR): Faz o mesmo que o APR mas todos os nós são sincronizados globalmente;

- *Asynchronous Fixed Repetition with Carrier Sensing* (AFR-CS): Faz o mesmo que o AFR porém também usa *carrier sense*;
- *Asynchronous P-persistent Repetition with Carrier Sensing* (APR-CS): Faz o mesmo que o APR porém também usa *carrier sense*.

Os próprios autores que propuseram os protocolos argumentaram contra SFR e SPR, por julgar que a sincronização global era um suposição muito incoveniente e se posicionaram em favor do AFR-CS como a melhor opção. Apesar de ser o primeiro trabalho que considerou seriamente a retransmissão como uma opção viável, uma rota que seria recomendada no futuro, todos os protocolos propostos pecam por não levarem em consideração o problema dos terminais escondidos.

2.7 Os Modelos de Rivera

Baseado no trabalho original de Bae [29], Rivera propôs melhorias ao modelo que abordassem o problema dos terminais escondidos e que possivelmente se aproveitassem de estratégias adicionais sugeridas na literatura, como *rebroadcasting* [1]. A subseção seguinte detalha as premissas assumidas por Rivera.

2.7.1 Premissas Fundamentais

De maneira a comparar de forma justa sua modelagem com a de Bae [29], Rivera [1] assumiu as mesmas premissas, conforme descritas a seguir:

- O canal de comunicação sem fio é organizado em *slots* de tempo e utiliza o protocolo *Slotted* Aloha;
- Existem múltiplos usuários competindo pelo canal com uma probabilidade de acesso comum a todos e com o objetivo de enviar mensagens em *broadcast* para todos os outros usuários;
- Nenhuma mensagem de *broadcast* tem seu recebimento confirmado por qualquer mecanismo;
- As mensagens de *broadcast* possuem um tempo de vida (D_f) que se comporta como um *deadline* rígido depois do qual a mensagem perde sua utilidade para aplicações críticas de segurança. Este tempo de vida D_f é definido como o tempo máximo permitido entre o momento que chega ao início da fila de transmissão do nó até o momento em que é recebido com sucesso por todos os receptores que este nó alcança.

As condições necessárias para que um nó tenha sua transmissão considerada como bem sucedida em um *slot* são:

- O nó ganha no cara-ou-coroa com probabilidade a;

- Nenhum outro nó vence o cara-ou-coroa no mesmo *slot*;
- A transmissão acontece em um *slot* anterior ao *deadline* Df.

2.7.2 Topologia da Rede

Estabelecer as premissas sobre as quais o sistema de comunicação vai funcionar por si só não é suficiente para desenvolver o seu modelo completamente numa rede *Ad Hoc*. Isso ocorre porque os nós não têm em geral nenhum tipo de configuração pré-determinada e frequentemente são móveis. Rivera [1] aborda esta questão fazendo uma escolha tradicional de topologia para a rede, que é reproduzida neste e nos próximos capítulos deste trabalho. Os nós são dispostos de forma aleatória numa área infinita de acordo com uma distribuição bi-dimensional de Poisson cujo parâmetro λ representa o número médio de nós por unidade de área, e a probabilidade $p(i,A)$ de encontrar i nós numa área de tamanho A (u.a.) é dada por

$$p(i,A) = \frac{(\lambda A)^i}{i!} e^{-\lambda A}. \tag{2.6}$$

Conforme mostra a Figura 2.5, para qualquer nó transmissor seu alcance de transmissão determina uma região de *broadcast* com todos os seus potenciais receptores e o alcance idêntico dos nós próximos desta região (e que conseguem causar colisões nos receptores dela) determina uma região de potenciais nós escondidos. Qualquer modelo que deseje abordar o problema do terminal escondido deve levar em consideração ambas as regiões.

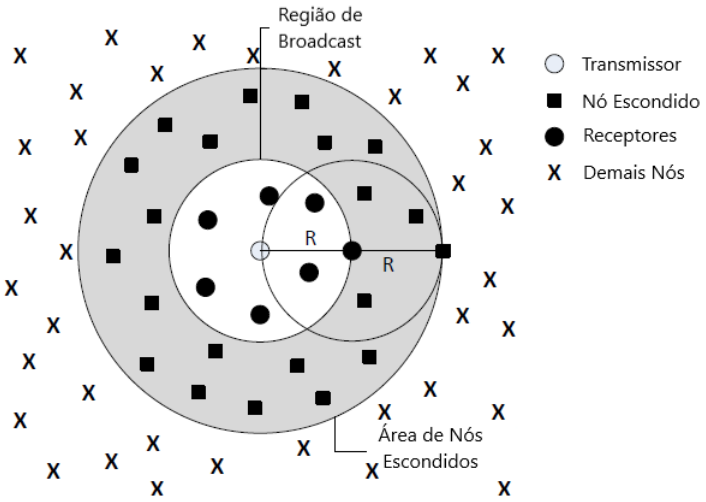

Figura 2.5 Distribuição dos nós na rede. Fonte: Reprodução baseada no original de Rivera [1].

Devido à distribuição de Poisson, o número médio de nós dentro da região de *broadcast* determinada pelo raio R de alcance do transmissor é dado por

$$N_R = \lambda A = \lambda \pi R^2. \tag{2.7}$$

Onde se considera A a área da região de *broadcast*. Já para a região dos terminais escondidos em potencial, a quantidade média de nós presentes é dada em função da coroa circular, ou seja,

$$N_H = 4\pi R^2 - \pi R^2 = 3\pi R^2 = 3\lambda A. \tag{2.8}$$

O alcance de transmissão dos nós numa VANET é de aproximadamente 1km [10]. Considerando que a velocidade média dos carros em condições normais não passa de 100km/h não é esperado que nenhum nó se desloque muito mais que 3 metros dentro dos 100ms de *deadline* para a transmissão de uma mensagem de *broadcast*. É um deslocamento muito pequeno comparado ao alcance da transmissão, portanto um modelo seguindo uma distribuição de probabilidade com nós fixos, como o adotado, é adequado como uma primeira aproximação para aplicações de segurança, dentro do tempo de um *deadline*.

Baseado nas premissas e na topologia descritas, Rivera [1] produziu algumas variantes de protocolo de camada de enlace usando como base o *Slotted* Aloha, cada uma delas assumindo outras premissas auxiliares para explorar ideias particulares distintas. Neste trabalho discutiremos e expandiremos duas destas variantes, o modelo chamado de não-periódico e o periódico de distribuição geométrica.

2.7.3 Modelo Não-Periódico

Este caso é uma reprodução da proposta original de Bae [29], estendida apenas devido à inclusão dos terminais escondidos. As premissas adicionais envolvidas são três. A primeira é que as única fonte de erro de recepção considerada é a colisão de pacotes (devido a múltiplas transmissões atingirem o mesmo receptor). A segunda é que cada um dos nós na rede tenta transmitir uma mensagem de *broadcast* em todos os *slots* jogando uma moeda (cara ou coroa) de acordo com uma probabilidade de acesso comum a todos (a). E a última é que não há nenhuma retransmissão de mensagem de *broadcast*. Ou seja, um nó que obteve sucesso no cara ou coroa num dado *slot k* não jogará a moeda nos *slots* posteriores.

2.7.3.1 Probabilidade de Sucesso

A probabilidade de sucesso referente a uma mensagem de *broadcast* (analisada individualmente) é a probabilidade com a qual esta mensagem é entregue à todos os receptores dentro do alcance do nó transmissor antes do *deadline* D_f, depois do qual ela é considerada inútil. Esta análise é feita tomando um nó arbitrário cuja mensagem de *broadcast* é marcada e seu destino é analisado.

A argumentação de Bae [29] e Rivera [1] sobre o fenômeno é que, dado que a probabilidade de transmissão para o nó marcado (ou qualquer um dos outros) é a, uma transmissão bem sucedida da mensagem de *broadcast* em avaliação ocorre num *slot k* quando ela não foi transmitida nos $k-1$ *slots* anteriores, será transmitida neste *slot k* e quando nenhum dos outros nós dentro da área de *broadcast* ou na região dos terminais escondidos também transmite no *slot k*. A probabilidade de sucesso ($p_s(a, D_f, \lambda)$) considerando os D_f *slots* é obtida argumentando que as transmissões bem sucedidas para cada *slot* são eventos mutualmente excludentes, portanto, aplicando a lei da probabilidade total, se obtém

$$p_s(a,D_f,\lambda) = \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{N_R-1}(1-a)^{N_H}$$
$$= (1-a)^{4\lambda A-1}\left[1-(1-a)^{D_f}\right]. \tag{2.9}$$

A probabilidade ótima de acesso a^* foi determinada por Rivera [1] simplesmente achando o ponto de máximo da equação (2.9) com relação a a através da sua derivada, que é igualada a zero e resolvida para a, obtendo-se

$$a^* = 1 - \left(\frac{4\lambda A-1}{4\lambda A-1+D_f}\right)^{\frac{1}{D_f}}. \tag{2.10}$$

Por fim, ao substituir a^* na equação (2.9), obtém-se a probabilidade de sucesso otimizada

$$p_s(a^*,D_f,\lambda) = \left(\frac{4\lambda A-1}{4\lambda A-1+D_f}\right)^{\frac{4\lambda A-1}{D_f}}\left(\frac{D_f}{4\lambda A-1+D_f}\right). \tag{2.11}$$

A Figura 2.6 demonstra alguns casos do modelo não-periódico, que estão em função da densidade de nós λ para demonstrar concordar exatamente com a modelagem de Rivera [1]. Contudo, é mais fácil analisar os resultados pensando na quantidade total esperada de nós dentro da região de interesse (*broadcast* + terminais escondidos), $\lambda = 2$, $\lambda = 3$ e $\lambda = 4$ correspondem respectivamente a aproxidamente 25, 38 e 50 nós na região, o que mostra que o modelo não obtém resultados suficientes para a probabilidade de sucesso maior ou igual a 99,9% conforme exigido pelos órgãos regulatórios mesmo considerando apenas colisões como fontes de erros de transmissão, uma vez que estas quantidades de nós não chegam a ser irrealistas.

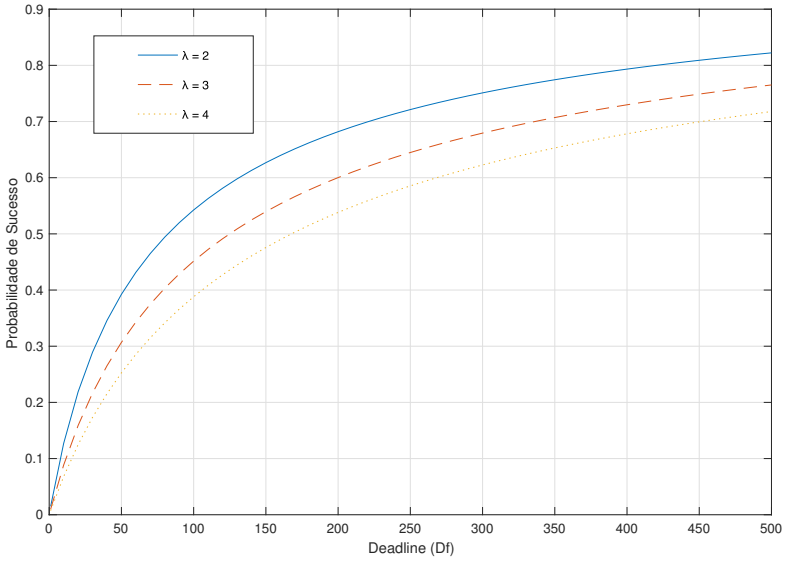

Figura 2.6 Exemplos do Modelo Não-Periódico, calculado pela equação (2.11).

Convém notar que tanto a modelagem original de [29] sem terminal escondido quanto a de Rivera [1] extendida para terminais escondidos compartilham uma simplificação implícita, que é assumir que qualquer transmissão na região dos terminais escondidos deve impactar algum dos receptores na região de *broadcast*. Isso não é necessariamente verdade, uma vez que devido à distribuição dos nós ser aleatória, pode ocorrer simplesmente de não haver um nó na região onde aquele terminal escondido em potencial está interferindo. Devido a isso, os resultados reais esperados de um protocolo conforme o modelado, mantendo todas as outras variáveis intactas, devia ser até um pouco melhor do que mostram as equações, contudo não é provável que esse fenômeno tenha efeitos realmente significativos nos resultados.

2.7.4 Modelo Periódico com Distribuição Geométrica

Devido a sugestões na literatura de que realizar *rebroadcasting* era uma estratégia promissora para aplicações de segurança em VANETs [27], [28], Rivera [1] propôs uma variante de protocolo de camada de enlace baseado em *Slotted* Aloha que fizesse uso de um *rebroadcast* periódico, e modelou sua probabilidade de sucesso p_s através de uma distribuição geométrica de probabilidade. O objetivo desta variante era atingir o resultado para o qual o modelo não-periódico da subseção anterior não se provou adequado, uma probabilidade de sucesso acima de 99,9% dentro de um *deadline* de 100ms, que são os requisitos para aplicações críticas de segurança em VANETs.

Rivera definiu o modelo periódico com distribuição geométrica (chamado de modelo geométrico em diante, por simplicidade) como uma variante do protocolo SPR [28] na qual são definidos dois parâmetros básicos:

- D_p: *deadline* parcial, define o período de repetição das mensagens de *broadcast* em número de *slots*;
- D_f: conserva o significado de *deadline* final a partir do qual a mensagem de segurança se torna inútil.

Das definições de D_p e D_f, e indicados na Figura 2.7, decorre imediatamente que haverão $N = \frac{D_f}{D_p}$ tentativas de retransmissão (ou repetições) por período de vida de uma mensagem de segurança (D_p é suposto divisor inteiro de D_f). Aqui D_f (e D_p) será dado em número de slots que pode ser mapeado em um um tempo em unidades de segundos. É importante frisar que num período D_p só pode haver uma tentativa de transmissão, uma vez que um nó vença o cara-ou-coroa e transmita neste ciclo só podera transmitir novamente no próximo ciclo. Contudo, esta transmissão pode nem sequer acontecer, já que depende da probabilidade a de acesso ao canal.

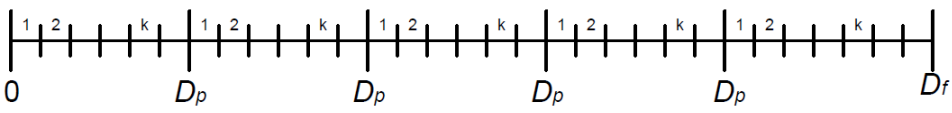

Figura 2.7 Diagrama de retransmissões. Fonte: [1].

Neste modelo também é introduzido um termo constante p_f que representa a probabilidade de falha em cada um dos receptores, de maneira a representar de maneira simplificada o conjunto de diversas falhas que podem acontecer na camada PHY.

2.7.4.1 Probabilidade de Sucesso

Como acontecem N tentativas de transmissão bem sucedidas por *deadline*, Rivera [1] abordou a modelagem do protocolo usando uma distribuição geométrica, construída a partir da probabilidade de que o primeiro sucesso tenha sido no ciclo x, onde $1 \leq x \leq N$ e a probabilidade de sucesso em cada um dos ciclos em particular é representada por um certo p_{sc}. Com essas considerações, a probabilidade de sucesso para um ciclo x é

$$P_r(X = x) = (1 - p_{sc})^{x-1} p_{sc}. \tag{2.12}$$

É importante notar que o sucesso de um ciclo é determinado pela transmissão bem sucedida da mensagem de *broadcast* para todos os receptores neste mesmo ciclo. Ainda que falte apenas um receptor num dado ciclo o modelo não considera nenhuma memória disso e continuará exigindo nas próximas tentativas que a transmissão seja recebida corretamente por todos os nós na região de alcance da mensagem de *broadcast*.

Para descrever a probabilidade p_{sc} de sucesso em um único ciclo, Rivera [1] usa diretamente a equação (2.9), argumentando que um ciclo do modelo geométrico é basicamente uma versão mais curta do modelo não-periódico. Depois de incluir o termo p_f e definir $M = 4\lambda A$, onde M é a quantidade de nós em toda a região de interesse (*broadcast* + terminal escondido), chega-se na relação

$$\begin{aligned} p_{sc}(a, D_p, M, N_R, p_f) &= \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-a)^{M-1}(1-p_f)^{N_R-1} \\ &= (1-a)^{M-1}[1-(1-a)^{D_p}](1-p_f)^{N_R-1}. \end{aligned} \tag{2.13}$$

Por conveniência de notação, toma-se

$$y = (1-a)^{M-1}[1-(1-a)^{D_p}](1-p_f)^{N_R-1}, \tag{2.14}$$

e partir da aplicação de y na equação (2.12), chega-se na probabilidade p_s de sucesso para todo o *deadline* D_f

$$\begin{aligned} p_s(y, N) &= \sum_{x=1}^{N} (1-y)^{x-1} y \\ &= y \sum_{x=1}^{N} (1-y)^{x-1}. \end{aligned} \tag{2.15}$$

Como $0 \leq y \leq 1$, sabe-se que

$$\sum_{x=1}^{N} (1-y)^{x-1} = \frac{1-(1-y)^N}{y}, \tag{2.16}$$

e combinando este resultado com a equação (2.15), tem-se que

$$p_s(y,N) = 1-(1-y)^N. \tag{2.17}$$

E finalmente combinando as equações (2.14) e (2.17), Rivera [1] chega em seu trabalho na equação desenvolvida para o modelo geométrico

$$p_s(a,D_p,M,N_R,p_f) = 1-\left[1-\left(1-(1-a)^{D_p}\right)(1-a)^{M-1}(1-p_f)^{N_R-1}\right]^N. \tag{2.18}$$

A determinação da probabilidade de acesso a^* que maximiza a probabilidade de sucesso é feita como no modelo não-periódico, derivando a expressão e igualando a zero. Contudo neste caso não se chega numa expressão com solução expressa em fórmula fechada, e o resultado é obtido numericamente. Como a longa derivação não contribui em nada para o entendimento do modelo e constitui apenas um exercício algébrico, a omitiremos.

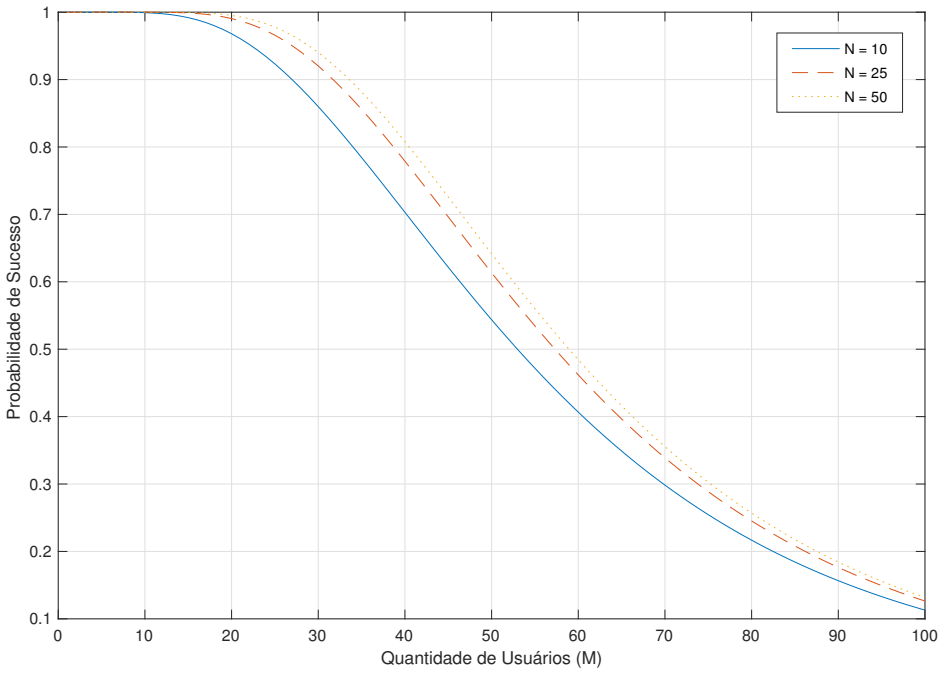

Figura 2.8 p_s em função de M para o modelo geométrico com p_f fixo em 10% e $D_f = 500$ slots, variando-se o número de repetições N.

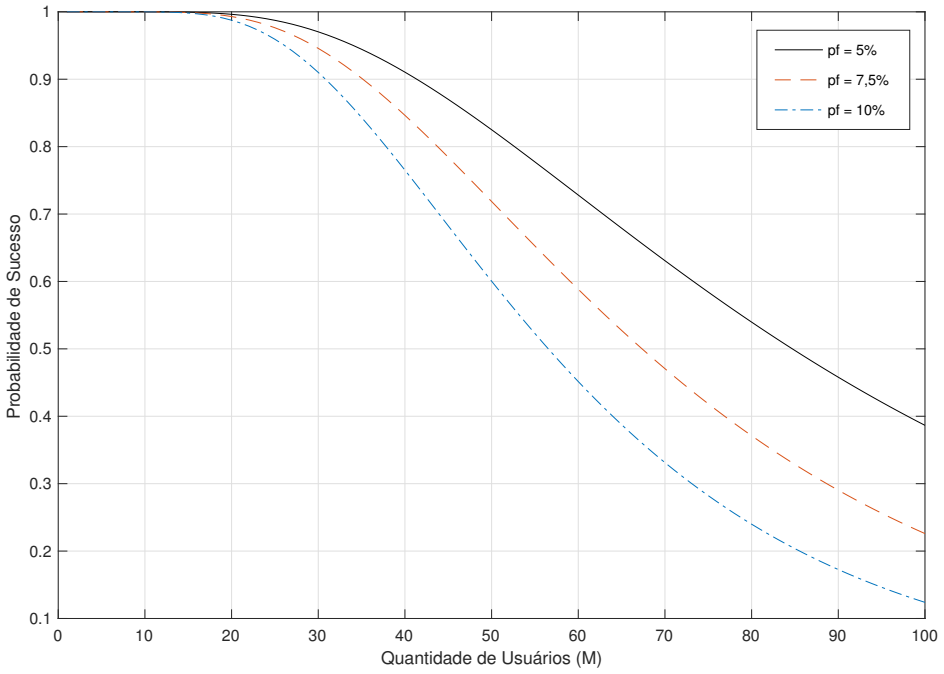

Figura 2.9 p_s em função de M para o modelo geométrico com com N fixo em 20 e $D_f = 500$ slots, variando-se a probabilidade falha na recepção p_f.

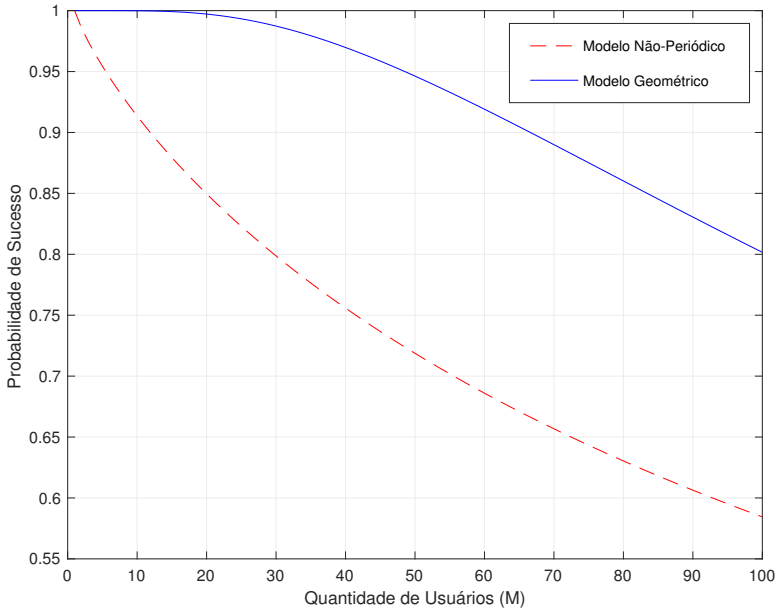

Figura 2.10 p_s em função de M para os modelo geométrico e não-periódico com N fixo em 10 e $D_f = 500$ *slots*, com $p_f = 0$.

Pela inspeção da Figura 2.10 podemos ver que o modelo geométrico é superior ao não-periódico, uma vez que ele tem resultados melhores para toda a faixa de 0 a 100 usuários. Também é fácil notar observando as figuras 2.8 e 2.9 que apesar de que aumentar o número N de repetições tem um efeito em geral positivo sobre os resultados, ele se torna irrelevante muito rapidamente. O salto de 10 para 25 repetições resulta num melhoramento sensível, mas de 25 para 50 repetições o ganho é muito pequeno. Além disso, a influência de uma probabilidade de falha de camada PHY p_f muito alta nos receptores inviabiliza o protocolo de forma decisiva para uma quantidade muito grande de nós, embora probabilidades como 10% ou até mesmo 7,5% sejam mais altas do que se espera na prática em geral.

2.8 Conclusões

Nesta capítulo abordamos as principais características das VANETs, e explicitamos que este trabalho se posiciona entre as aplicações críticas de segurança. Os requisitos que uma aplicação deste tipo deve obedecer foram explicados em profundidade e serão as métricas de julgamento de mérito dos resultados atingidos nos capítulos seguintes.

Também foi feito um estudo do protocolo *Slotted* Aloha por meio de sua comparação com o *Aloha* básico e da demonstração de sua vazão e probabilidade ótima de transmissão. Além disso foram estudados problemas típicos das redes *Ad Hoc* em geral, como os terminais escondidos e os erros associados com a camada PHY. Tentativas anteriores na literatura de lidar com mensagens de *broadcast* no contexto das VANETs foram citadas, incluindo abordagens que trouxeram a ideia de fazer *rebroadcasting*.

No final do capítulo dedicamos uma seção a discutir as propostas de Rivera [1], sobre as quais este trabalho procurou desenvolver. Mostramos em detalhes as modelagens e rediscutimos conclusões presentes na publicação original. Nos *capítulos 4* e *5* proporemos nossas próprias alterações e extensões para estes modelos.

CAPÍTULO 3

Slotted Aloha Multicanal

Devido ao avanço das tecnologias de camada física (PHY), alguns protocolos da família IEEE 802.11 já suportam múltiplos canais de comunicação sem sobreposição, inclusive o 802.11p, desenvolvido especialmente para o contexto das VANETs [30]. Como o objetivo deste trabalho é avaliar o quão adequado é um protocolo adaptado a partir do *Slotted* Aloha para lidar com as restrições rígidas das aplicações de seguranças em VANETs, seria proveitoso estender a análise para lidar com mais de um canal de comunicação. Por isso, é necessário estudar o *Slotted* Aloha para o contexto multicanal. Na literatura é possível encontrar discussões breves sobre o assunto com demonstrações intuitivas e relativamente informais, como em [31]. Uma das contribuições deste trabalho e tema deste capítulo é uma prova formal de características fundamentais de um protocolo *Slotted* Aloha multicanal, como vazão, probabilidade ótima de acesso e períodos médios de ocupação, ociosidade e utilização.

3.1 Premissas

Dado que é possível definir várias formas pelas quais os nós podem interagir com os múltiplos canais, é preciso escolher algumas premissas que pareçam naturais para generalizar o protocolo *Slotted* Aloha para mais de um canal respeitando esta escolha em particular. Neste trabalho foram adotadas as seguintes premissas:

- Cada nó tenta transmitir com uma probabilidade p, e o faz jogando uma moeda (cara e coroa).
- Se o nó acertar na moeda, sorteará de maneira uniforme um entre os C canais disponíveis para transmitir. Ou seja, cada canal tem probabilidade $\frac{1}{C}$ de ser escolhido e necessariamente algum canal será escolhido.
- Uma colisão ocorre quando dois ou mais nós transmitem no mesmo canal. No caso do protocolo multicanal é possível então que haja mais de uma transmissão bem sucedida por *slot*.

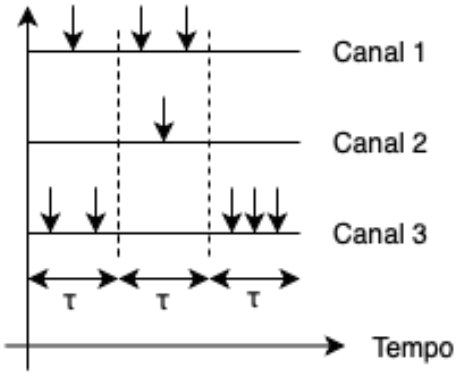

Figura 3.1 Diferentes possibilidades de tentativas de envio para 3 canais e 3 *slots*. τ representa a duração de um pacote no tempo e as setas indicam pacotes direcionados para o *slot*.

Para o cálculo da vazão do *Slotted* Aloha multicanal é mais conveniente usar uma técnica ligeiramente diferente da usada com o protocolo *Aloha* básico, que consiste em determinar os períodos médios de utilização/*utilization* (U), ocupação/*busy* (B) e ocioso/*idle* (I). Estes períodos estão relacionados com a vazão do protocolo (S) pela equação

$$S = \frac{U}{I+B}. \tag{3.1}$$

Mas definir o que exatamente representam os períodos de utilização efetiva do canal, ocupação e ociosidade não é imediatamente evidente quando se considera mais de um canal. Neste trabalho adota-se uma abordagem individualizando cada um dos canais, e analisando-os separadamente. A ideia é que as noções para apenas um canal são descomplicadas, e portanto seria mais simples analisar o sistema a nível de canais individuais e depois somar os resultados do que considerar diretamente todas as possibilidades multicanal. O fato de que os canais são independentes entre si garante que os eventos em um não influenciam nenhum evento nos outros.A Figura 3.1 representa alguns dos eventos possíveis com relação a distribuição das tentativas de transmissão entre os canais disponíveis. Podemos ver que houve colisão no segundo *slot* do canal 1, assim como no primeiro e terceiro *slots* do canal 3, mas com colisões ou não o canal teve transmissões, e esses eventos fazem parte do período ocupado. No primeiro *slot* do canal 1 e no segundo *slot* do canal 2 houve uma transmissão bem sucedida, o que caracteriza eventos pertecentes ao período de utilização. Em todos os outros *slots* não houve nenhuma transmissão, portanto fazem parte do período ocioso de seus respectivos canais.

A análise da Figura 3.1 sugere que nada muda conceitualmente do caso multicanal para o caso com canal único se a modelagem abordar a questão avaliando um canal de cada vez. Um canal não sofre qualquer influência dos demais, e portanto é como se houvesse apenas uma mudança em sua carga particular. Por padrão, a abordagem que parte da equação (3.1) para calcular a vazão modela a carga da rede (G) como um Processo de Poisson, onde $G = \ell T$ por definição, ℓ é o parâmetro das chegadas de pacotes para a rede inteira e T é a duração do *slot*. Diretamente da distribuição de Poisson que é muito bem conhecida, a probabilidade de que ocorram n chegadas na rede no intervalo T é dada por

$$P_n(T) = \frac{G^n e^{-G}}{n!} = \frac{(\ell T)^n e^{-\ell T}}{n!}. \tag{3.2}$$

3.2 Vazão

Usando as considerações da seção anterior, podemos escrever a probabilidade de que um período ocioso em apenas um canal tenha um tamanho de N slots, que para cada um dos canais tomados separadamente é

$$Pi_{1c}\{I = N\,slots\} = \left(\underbrace{e^{-G} + \sum_{i=1}^{\infty} \left(\frac{C-1}{C}\right)^i \frac{G^i}{i!} e^{-G}}_{\alpha} \right)^{N-1} \times (1-\alpha)\,. \tag{3.3}$$

O termo α representa a possibilidade de nenhuma chegada para o canal. Ora, isto ocorre quando não há nenhuma chegada na rede em si ou quanto todas as chegadas foram distribuídas para os outros canais. Para determinar o termo somatório e então calcular α, considera-se a Série de Taylor para as exponenciais

$$e^x = \sum_{i=0}^{\infty} \frac{x^n}{n!}. \tag{3.4}$$

Observando a equação (3.4), pode-se fazer uma escolha apropriada de exponencial

$$e^{G(1-\frac{1}{C})} = \sum_{i=0}^{\infty} \frac{[G(1-\frac{1}{C})]^n}{n!} = \sum_{i=0}^{\infty} \left(\frac{C-1}{C}\right)^n \frac{G^n}{n!}, \tag{3.5}$$

e aplicando este resultado na equação (3.3), obtém-se $\alpha = e^{-\frac{G}{C}}$, e portanto

$$Pi_{1c} = \left(e^{-\frac{G}{C}}\right)^{N-1} (1 - e^{-\frac{G}{C}}). \tag{3.6}$$

O valor esperado para o intervalo ocioso é trivialmente calculado por se tratar de uma distribuição geométrica de probabilidade, assim

$$I = \frac{1}{1 - e^{-\frac{G}{C}}}. \tag{3.7}$$

Para calcular o valor esperado em *slots* do período ocioso B para um canal, as equações são análogas e se obtém

$$Pb_{1c} = (1 - e^{-\frac{G}{C}})^{N-1} \left(e^{-\frac{G}{C}}\right). \tag{3.8}$$

Mais uma vez aparece uma distribuição geométrica, cujo valor esperado é facilmente calculado como

$$B = e^{\frac{G}{C}}. \tag{3.9}$$

Para calcular o valor esperado do período de utilização para um canal (U), é preciso lembrar que este período é um fração do período ocupado, que considera apenas os casos de transmissão bem sucedida, sem colisões, portando $U = B \cdot P_s$, onde P_s é a probabilidade de sucesso dado que houve uma ou mais transmissões no canal. A probabilidade P_s deve indicar o caso em que dada qualquer quantidade de chegadas na rede, apenas uma foi distribuída para o canal em questão, logo

$$P_s = \frac{\sum_{i=1}^{\infty} \frac{i}{C} \left(\frac{C-1}{C}\right)^i \frac{G^i}{i!} e^{-G}}{1 - e^{-\frac{G}{C}}}. \tag{3.10}$$

O termo somatório que aparece para P_s é muito parecido com os tratados anteriormente, o que sugere que a Série de Taylor para as exponenciais deve ser utilizada mais uma vez. Após simplificar obtém-se

$$\sum_{i=1}^{\infty} \frac{i}{C} \left(\frac{C-1}{C}\right)^i \frac{G^i}{i!} e^{-G} = \frac{G}{C} e^{-G} \sum_{i=1}^{\infty} \left(\frac{C-1}{C}\right)^{i-1} \frac{G^{i-1}}{(i-1)!}, \tag{3.11}$$

e em seguida usando a série de Taylor (equação (3.4)) na equação (3.11) e substituindo na equação (3.10), chega-se a

$$P_s = \frac{\frac{G}{C} e^{-\frac{G}{C}}}{1 - e^{-\frac{G}{C}}}. \tag{3.12}$$

Usando P_s para calcular U e substituindo na equação (3.1), temos a vazão para apenas um dos canais

$$S_{1c} = \frac{G}{C} e^{-\frac{G}{C}}. \tag{3.13}$$

Como são considerados k canais, a vazão total é

$$S = G e^{-\frac{G}{C}}. \tag{3.14}$$

É fácil mostrar que o valor máximo para esta vazão ocorre quando $G = k$, e seu valor é dado por

$$S_{max} = \frac{C}{e}. \tag{3.15}$$

Analisando estes resultados, vê-se que parecem coerentes. A vazão máxima obtida para apenas um canal é numericamente igual ao valor do *Slotted* Aloha clássico ($\frac{1}{e}$), e de maneira geral o que as equações mostram é que o potencial de cada canal considerado pode ser explorado ao máximo, com cada um deles entregando com sucesso em média $\frac{1}{e}$ pacotes por *slot*. Isso era esperado pois a distribuição de pacotes, aleatória da forma como foi proposta, naturalmente tenderá a distribuir quantidades iguais de pacotes para cada canal, e com isso a vazão máxima será obtida quando a carga da rede for numericamente igual a quantidade de canais, o que faz a carga de cada canal ser numericamente igual a 1, caso ótimo para o *Slotted* Aloha [19].

3.3 Probabilidade Ótima de Transmissão

Embora a análise de vazão por Processo de Poisson seja muito útil, ela é feita considerando que sempre que há chegadas na rede todas elas serão necessariamente distribuídas para transmissão em algum canal, o que não é verdade numa implementação real do protocolo *Slotted* Aloha. O que acontece realmente é que cada nó tem uma probabilidade de transmitir, e essa probabilidade é o fator determinante da carga (quantidade média de pacotes a serem transmitidos por *slot*) que é entregue à rede. Como usando apenas o método de Poisson não é possível obter diretamente a probabilidade ótima de transmissão que maximiza a vazão do protocolo, é preciso obtê-la através da carga ótima demonstrada na seção anterior. Portanto, seja X variável aleatória que descreve a carga, queremos que $E\{X\} = C$ para obter a vazão máxima. A equação que descreve este valor esperado é

$$E\{X\} = \sum_{i=0}^{n} i \binom{n}{i} p^i (1-p)^{n-i}, \tag{3.16}$$

onde p é a probabilidade de transmissão por parte de um nó da rede em particular e n é a quantidade de nós. É preciso determinar este valor esperado para daí calcular p. A técnica utilizada para isso é a indução matemática. Tomemos a hipótese

$$\sum_{i=0}^{n} i \binom{n}{i} p^i (1-p)^{n-i} = np \tag{3.17}$$

que é trivialmente verdadeira para o caso base $n = 1$, então é necessário provar o passo indutivo. Expandindo os termos apropriadamente, obtém-se

$$\begin{aligned}\sum_{i=0}^{n+1} i \binom{n+1}{i} p^i (1-p)^{n+1-i} = (1-p) \sum_{i=1}^{n} i \binom{n}{i} p^i (1-p)^{n-i} \\ + \sum_{i=1}^{n} i \binom{n}{i-1} p^i (1-p)^{n+1-i} + (n+1)p^{n+1}\end{aligned} \tag{3.18}$$

Usando a hipótese e fazendo a substituição $j = i - 1$, tem-se

$$\begin{aligned}\sum_{i=0}^{n+1} i \binom{n+1}{i} p^i (1-p)^{n+1-i} = \\ \sum_{j=0}^{j-1} j \binom{n}{j} p^j (1-p)^{n-j} + (1-p)np + (n+1)p^{n+1}\end{aligned} \tag{3.19}$$

e ao expandir o termo somatório e usar mais uma vez a hipótese aliada ao Teorema Binomial, chega-se a

$$\begin{aligned}\sum_{i=0}^{n+1} i \binom{n+1}{i} p^i (1-p)^{n+1-i} = \\ p(np - np^n + 1 - p^n) + (1-p)np + (n+1)p^{n+1}.\end{aligned} \tag{3.20}$$

Simplificando, resulta em

$$\sum_{i=0}^{n+1} i\binom{n+1}{i} p^i (1-p)^{n+1-i} = (n+1)p. \tag{3.21}$$

Este resultado prova o passo indutivo e com isso a hipótese. Agora que está provado que $E\{X\} = np$, é possível obter facilmente que o valor ótimo para p é (naturalmente considerando $n > C$)

$$p = \frac{C}{n}. \tag{3.22}$$

Com o resultado da equação (3.22), a modelagem do *Slotted* Aloha multicanal fica completa.

CAPÍTULO 4

Protocolo de *Broadcast* Não-Periódico

Este capítulo estende o modelo de *broadcast* não-periódico proposto por Rivera [1] para o caso multicanal sendo uma contribuição original e compara os ganhos dessa abordagem com relação ao modelo original de Rivera. Também propomos uma variante do modelo não-periódico que em comparação com o original obtém resultados melhores, e simulamos esta variante através de *software* (MATLAB) para validação. É importante frisar que a simulação não é das equações mas sim dos eventos, então são geradas representações dos nós que se comportam de acordo com as premissas a partir das quais os modelos matemáticos foram extraídos.

4.1 Modelo Não-Periódico Multicanal

O primeiro passo necessário para estender o modelo para o caso multicanal é estabelecer as premissas. Nesse caso, basta simplesmente combinar o que assumem o modelo de Rivera e a demonstração do protocolo *Slotted* Aloha que fizemos no capítulo anterior. Em nome da clareza, repetiremos as premissas fundamentais:

- Os nós têm probabilidade comum de acesso ao canal e igual a a;
- Ao vencer o cara-ou-coroa para transmitir com probabilidade a, o nó sorteia em qual canal transmitirá, com cada dos canais tendo probabilidade idêntica e igual a $\frac{1}{C}$, onde C é a quantidade de canais;
- As mensagens de *broadcast* têm um tempo de vida D_f e sua recepção bem sucedida não é confirmada nem as mensagens são retransmitidas.

Para começar a análise do modelo não-periódico multicanal, comecemos por um resultado discutindo anteriormente. A equação (2.9) descreve o caso básico para um canal e é equivalente a

$$p_s(a, D_f, \lambda) = \sum_{k=1}^{D_f} a(1-a)^{k-1}(1-a)^{4\lambda A-1}, \tag{4.1}$$

onde cada um dos termos mantém o seu significado usual. Ao ponderar sobre cada um dos termos que compõem o somatório, procuremos onde se dá a influência do multicanal. Nosso nó marcado transmitirá com probabilidade de acesso a, e podemos facilmente interpretar essa probabilidade como sendo de acesso a todos os canais, de modo que nada mude. Mas então se a é a probabilidade de transmissão por si só (sem definir em qual canal), a probabilidade de que a

transmissão ocorra num canal específico é $a \cdot \frac{1}{C}$. Como agora o contexto é multicanal, para que duas ou mais mensagens de *broadcast* venham a colidir, não basta que ambas sejam transmitidas, precisam ser transmitidas no mesmo canal. Então a equação (2.9) pode ser generalizada para C canais da seguinte maneira

$$\begin{aligned} p_s(a, D_f, \lambda, C) &= \sum_{k=1}^{D_f} a(1-a)^{k-1} \left(1 - \frac{a}{C}\right)^{4\lambda A - 1} \\ &= \left(1 - \frac{a}{C}\right)^{4\lambda A - 1} \sum_{k=1}^{D_f} a(1-a)^{k-1} \\ &= [1 - (1-a)^{D_f}] \left(1 - \frac{a}{C}\right)^{4\lambda A - 1}. \end{aligned} \tag{4.2}$$

A partir da equação (4.2) podemos calcular a probabilidade ótima de acesso a^* derivando e igualando a zero, conforme o mesmo procedimento de capítulos anteriores. A derivada com relação a a da equação (4.2) é

$$\frac{dp_s}{da} = D_f(1-a)^{D_f - 1} \left(1 - \frac{a}{C}\right)^{4\lambda A - 1} - \frac{(4\lambda A - 1)[1 - (1-a)^{D_f}](1 - \frac{a}{C})^{4\lambda A - 2}}{C}. \tag{4.3}$$

Ao igualar esta expressão a zero não obtemos uma fórmula fechada para a, mas a probabilidade ótima de transmissão ainda pode ser (e é) calculada numericamente. Também é importante notar que a equação (4.2) recai exatamente na equação (2.9) para $C = 1$, conforme o esperado devido a esta equação representar um caso particular do modelo multicanal.

4.1.1 Resultados

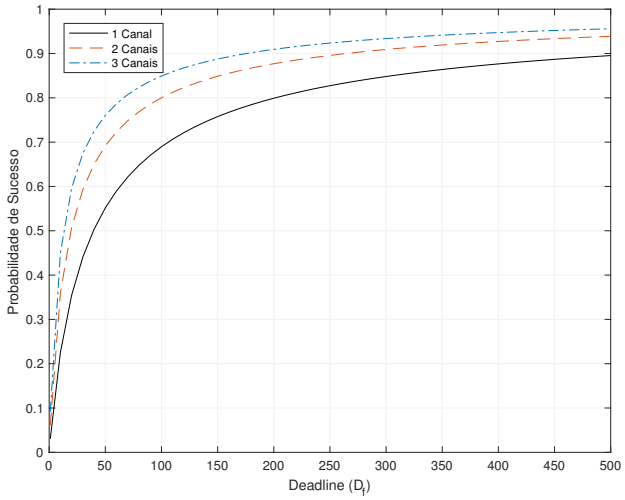

Figura 4.1 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 1$, o que equivale a aproximadamente $M = 13$.

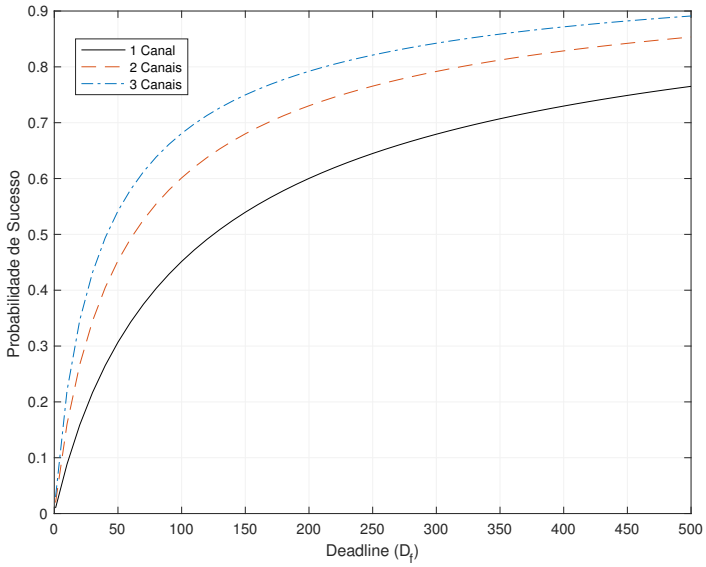

Figura 4.2 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 3$, o que equivale a aproximadamente $M = 38$.

Devidos aos resultados obtidos na modelagem do protocolo *Slotted* Aloha multicanal realizada no capítulo anterior, era esperado que estender os modelos de Rivera [1] para múltiplos canais traria uma melhora significativa nos resultados. Isto é o que ocorre de fato, como mostram as Figuras 4.1, 4.2 e 4.3.

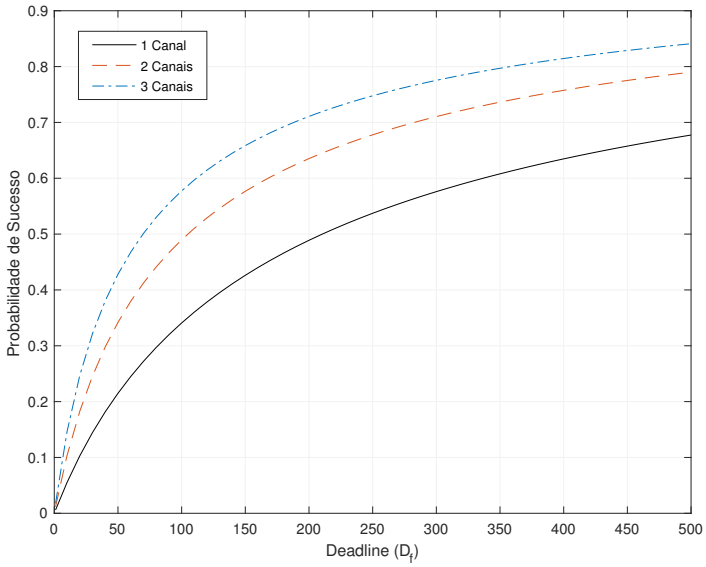

Figura 4.3 Exemplo de p_s considerando 1, 2 e 3 canais, com $\lambda = 5$, o que equivale a aproximadamente $M = 63$.

Além da evidente melhora na probabilidade de sucesso, pode-se identificar duas tendências pela análise das figuras. A primeira é que a utilização de múltiplos canais é uma estratégia que apesar de muito poderosa se esgota rápido, isto é, fica claro que aumentar cada vez mais o número de canais começa a trazer retornos cada vez menos significativos em termos de probabilidade de sucesso, o salto de 1 para 2 canais é muito grande, e de 2 para 3 já nem tanto. A Figura 4.4 mostra claramente o fenômeno, nota-se que o salto de 5 para 10 canais fornece uma melhora próxima a do salto de 3 para 5, e em termos absolutos os resultados para 5, 7 ou 10 canais estão todos próximos. Além disso, se observa um ganho proporcional maior ao partir de 1 canal para 3 do que ao partir de 3 para 10.

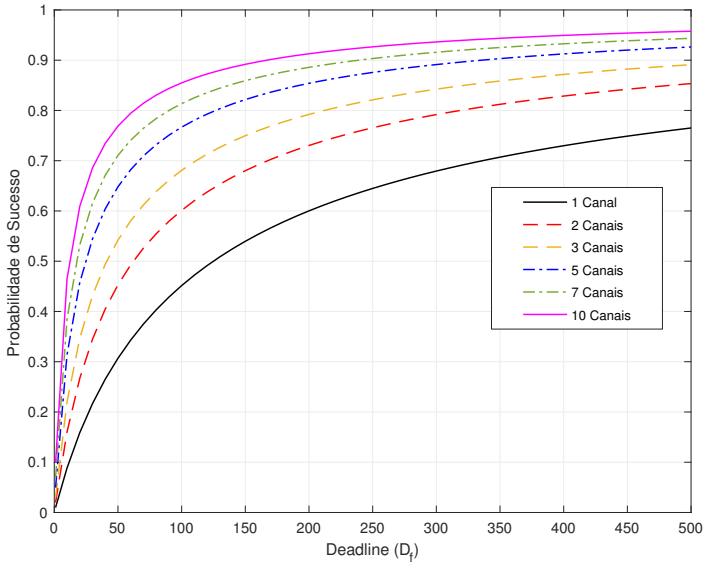

Figura 4.4 Exemplo de esgotamento da estratégia do multicanal, com $\lambda = 4$.

A segunda tendência é que os múltiplos canais melhoram especialmente os casos onde existem mais nós na rede. Para o caso $\lambda = 1$, representado na Figura 4.1, a diferença ao final do *deadline* nem chega a ser grande. Mas no caso $\lambda = 5$ já se observam diferenças muito maiores ao final do *deadline*, conforme mostra a Figura 4.3.

4.2 Modelo Não-Periódico Alternativo

Ao analisar o modelo não-periódico proposto por Rivera [1], notamos que a sua premissa de não permitir retransmissões da mensagem de *broadcast* pode ser relaxada sem nenhuma perda de realismo e com potenciais melhorias na probabilidade de sucesso. É verdade que Rivera [1] propõe em seu trabalho versões de seu modelo considerando *rebroadcasting* periódico, mas vamos propor aqui um modelo de *rebroadcasting* não-periódico.

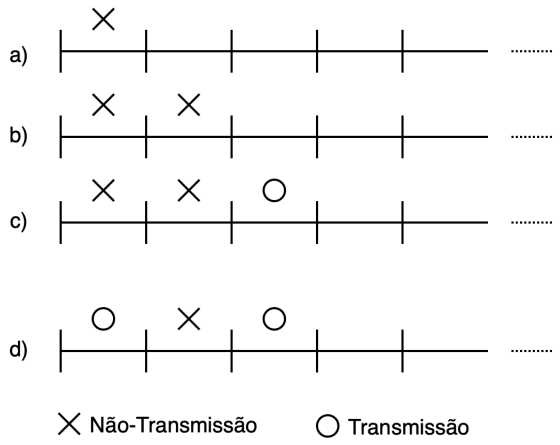

Figura 4.5 Comparativo entre políticas de transmissão.

Nossa sugestão parte do estudo da equação (4.2), onde o termo $a(1-a)^{k-1}$ explicita uma política de transmissão na qual um nó transmissor só transmite no máximo uma vez sua mensagem de *broadcast* durante todo o *deadline* D_f. A Figura 4.5 ilustra a diferença do que acontece no modelo de Rivera e no que estamos propondo: para transmitir no terceiro *slot* [*c)*], no modelo de Rivera o nó necessariamente precisa não ter transmitido nos dois anteriores [*b)*, *a)*], enquanto que na proposta apresentada nesta seção, pode ocorrer algo como [*d)*], em que o nó transmitiu no primeiro e terceiro *slots*, e pode transmitir quantas vezes conseguir dentro do *deadline*.

Temos então um modelo não-periódico com retransmissões, que se organiza de forma mais simples que o discutido na seção anterior. A regra é que quem vencer no cara-ou-coroa transmite, independentemente de *deadlines* ou do histórico anterior de transmissões. De acordo com o comportamento desejado para o protocolo, podemos escrever a probabilidade de que uma transmissão seja bem sucedida num dado *slot* como

$$p_{s1} = a(1-a)^{4\lambda A-1}(1-p_f)^{\lambda A-1}. \tag{4.4}$$

Por conveniência, este modelo já considera uma taxa de falha na camada física (PHY) p_f, e para comparação direta com o modelo não-periódico da seção anterior basta considerar $p_f = 0$. A probabilidade de sucesso para todo o *deadline* deve expressar o fato de que a transmissão foi bem sucedida em pelo menos um *slot*, e por isso pode ser expressa utilizando o complemento, isto é, $1-$*probabilidade de falha para todos os slots*, então

$$p_s = 1-(p_{s1})^{D_f} = 1-\left(1-a(1-a)^{4\lambda A-1}(1-p_f)^{\lambda A-1}\right)^{D_f}. \tag{4.5}$$

Da mesma forma que em todas as discussões anteriores, é preciso derivar a expressão para obter a probabilidade ótima de acesso a^*. O passo da derivação não oferece nenhum *insight* sobre o modelo, por isso omitimos as manipulações algébricas e escrevemos apenas o resultado final.

$$\frac{dp_s}{da} = D_f(1-a)^{4\lambda A-2}(1-a4\lambda A)(1-p_f)^{\lambda A-1}\left(1-a(1-a)^{4\lambda A-1}(1-p_f)^{\lambda A-1}\right)^{D_f-1}. \quad (4.6)$$

A equação (4.6) não pode ser resolvida para a numa fórmula fechada, por isso a probabilidade ótima de acesso é calculada numericamente.

4.2.1 Resultados

A Figura 4.6 mostra uma diferença bastante significativa entre os modelos não-periódicos. Simplesmente não restringir o nó transmissor de modo a fazer apenas uma tentativa bem sucedida em todo o *deadline* melhora os resultados. Quando se consideram múltiplos canais, como na Figura 4.7, naturalmente ambos os modelos têm um desempenho melhorado, mas conforme o esperado a diferença entre os dois persiste num patamares distantes em mais de 15% ao fim do *deadline*.

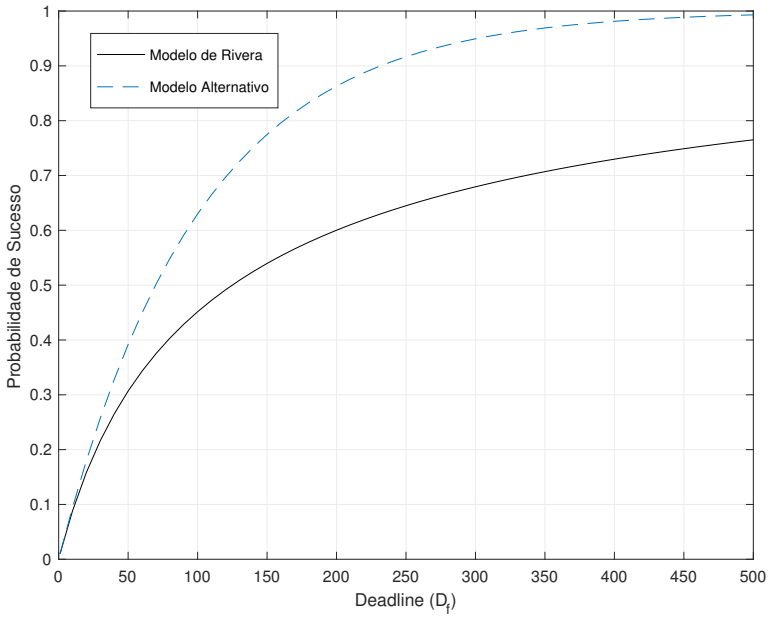

Figura 4.6 Comparativo entre modelos não-periódicos considerando $p_f = 0$ e $\lambda = 3$. $M = 38$, aproximadamente. Apenas 1 Canal de comunicação é considerado.

Como o modelo alternativo trouxe uma melhora muito significativa para a probabilidade de sucesso, convém validá-lo de alguma maneira. Realizamos simulações em *software* (MATLAB) dos eventos do modelo (em contraste com simular as equações) com esse propósito. As Figuras 4.8 e 4.9 mostram os resultados da simulação para 1000 rodadas (os eventos foram simulados 1000 vezes, cada uma das rodadas foi classificada de acordo com ter sido uma falha ou sucesso, e a média de todas as rodadas foi tomada). A simulação aderiu muito bem ao

modelo tanto para o caso de 1 canal (Figura 4.8) quanto para o caso de 3 canais (Figura 4.9), validando a nossa proposta.

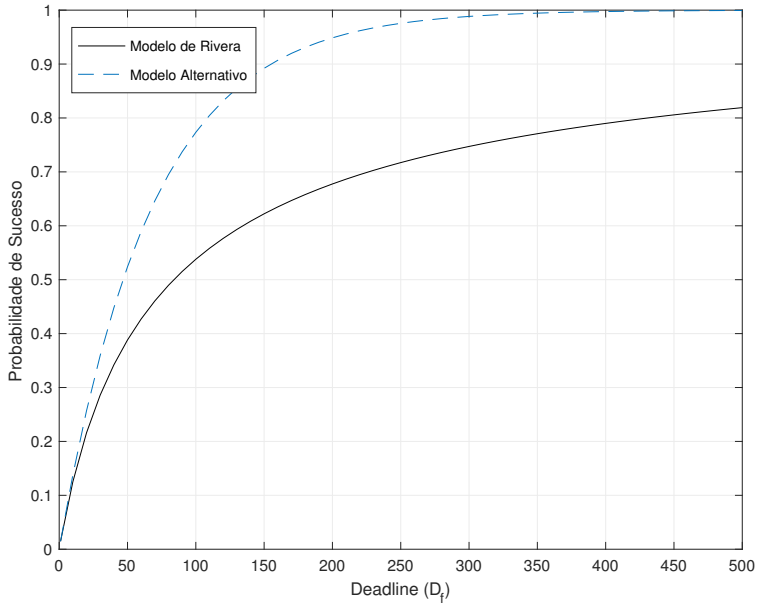

Figura 4.7 Comparativo entre modelos não-periódicos considerando $p_f = 0$ e $\lambda = 6$. $M = 75$, aproximadamente. São considerados 3 canais.

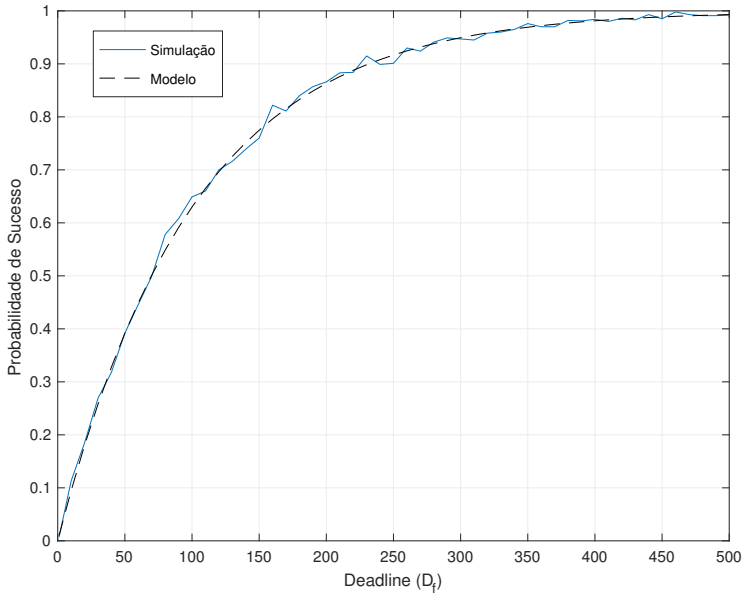

Figura 4.8 Estudo de aderência da simulação com o modelo alternativo para $\lambda = 3$, $p_f = 0$ e 1 canal. 1000 rodadas de simulação.

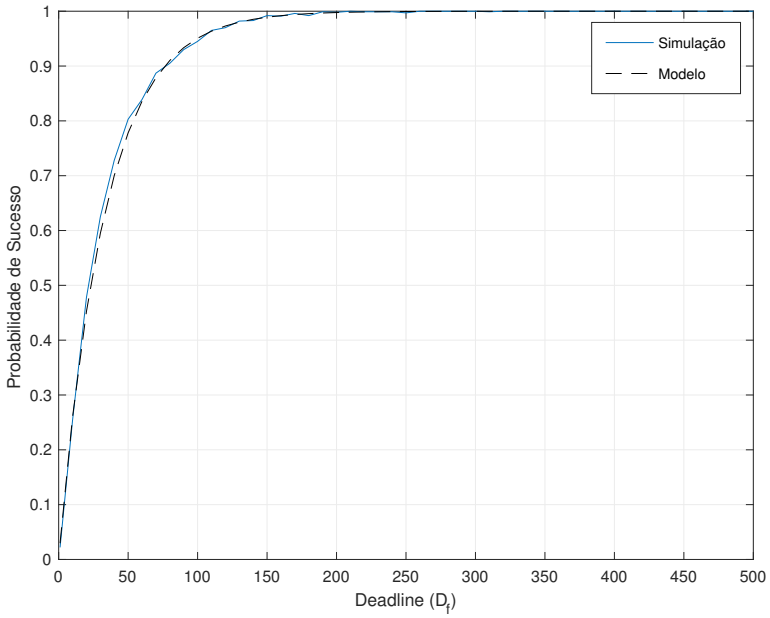

Figura 4.9 Estudo de aderência da simulação com o modelo alternativo para $\lambda = 3$, $p_f = 0$ e 3 canais. 1000 rodadas de simulação.

CAPÍTULO 5

Protocolo de *Broadcast* Periódico

Este capítulo estende o modelo de *broadcast* periódico proposto por Rivera [1] para o caso multicanal, numa das contribuições originais deste trabalho, mas antes disso propõe uma correção ao modelo, que é validada por simulação. Mostraremos que a generalização multicanal e a correção proposta ao modelo melhoram a probabilidade de sucesso do protocolo de forma muito significativa.

5.1 Correção

Na descrição do modelo geométrico conforme formulado por Rivera [1] e reproduzido neste trabalho, a equação (2.18) que modela a probabilidade de sucesso de um ciclo D_p inclui o termo $(1-a)^{M-1}$, que representa que quando o nó marcado transmitir, nenhum outro nó na região de interesse (*broadcast* + terminais escondidos) pode transmitir, do contrário haverá colisão em algum dos receptores. Embora à primeira vista isto pareça óbvio e correto, este não é o caso. O que ocorre é que nas premissas do modelo é dito que um nó que transmita uma mensagem de *broadcast* não irá transmitir novamente dentro do mesmo ciclo, apenas no próximo ciclo este nó terá "permissão" para tentar novamente.

Então qual o problema do termo $(1-a)^{M-1}$? Ele assume implicitamente que todos os nós no ciclo nunca transmitem e de alguma forma se guardam para o momento especial de colidir com o nó que marcamos para análise. Ora, se por exemplo dois destes nós já tivessem transmitido em *slots* anteriores não seriam mais candidatos a transmitir no *slot* atual, portanto o termo que apareceria devia ser $(1-a)^{M-1-2}$. Naturalmente, existem muitas combinações possíveis de quantos nós já transmitiram, o que torna a modelagem muito mais complexa. É preciso fazer a substituição

$$(1-a)^{M-1} -> \sum_{i=0}^{M-1} \binom{M-1}{i} [1-(1-a)^{k-1}]^i (1-a)^{(k-1)(M-1-i)} (1-a)^{M-1-i} = x. \quad (5.1)$$

Chamamos este somatório de x apenas por conveniência. A ideia por trás da substituição é que i representa a quantidade de nós que já transmitiram em *slots* anteriores ao presente, e a combinação de M - 1 para i indica que esta é a quantidade de maneiras que se pode escolher i nós dentre os M - 1 possíveis. O termo $[1-(1-a)^{k-1}]$ representa a probabilidade de que cada um desses nós tenha transmitido num *slot* anterior, e o termo é elevado a i porque são i nós. O termo $(1-a)^{(k-1)(M-1-i)}$ indica que todos os outros M - 1 - i não devem ter transmitido em nenhum *slot*, por fim, o termo $(1-a)^{M-1-i}$ representa que todos estes M - 1 - i nós também não podem transmitir neste *slot*.

5.2 Modelo Multicanal

Seguindo o exemplo dos casos anteriores, a única coisa necessária para generalizar o protocolo é que não ocorram colisões no *mesmo* canal em que o nó marcado está transmitindo. Sendo assim, a generalização da equação (5.1) para C canais é

$$\begin{aligned} x(C) &= \sum_{i=0}^{M-1} \binom{M-1}{i} \left[1-(1-a)^{k-1}\right]^i \left(1-a\right)^{(k-1)(M-1-i)} \left(1-\frac{a}{C}\right)^{M-1-i} \\ &= \frac{C\left(1-\frac{a}{C}\right)\left(1-a\right)^{(k-1)(M-1)} \left(\frac{(1-a)^{-k}[a((1-a)^k+C)-C]}{a-C}\right)^{M-1}}{C-a}. \end{aligned} \tag{5.2}$$

A manipulação que resulta na equação (5.2) é omitida por ser muito longa e não adicionar ao entendimento do fenômeno. Aplicando a equação (5.2) na equação (2.18) que define a probabilidade de sucesso do modelo geométrico para um ciclo D_p e já considerando a substituição discutida obtemos (considerando N_R com o significado usual da quantidade de nós dentro da região de *broadcast*)

$$y = \sum_{k=1}^{D_p} a(1-a)^{k-1}(1-p_f)^{N_R-1}x(C). \tag{5.3}$$

Seguindo o raciocínio da distribuição geométrica e assumindo $N = \frac{D_f}{D_p}$, a probabilidade de sucesso para o ciclo D_f inteiro é dada por

$$p_s = 1-(1-y)^N. \tag{5.4}$$

A derivada da equação (5.4), da qual precisamos para calcular a probabilidade ótima de acesso a^*, é uma equação extremamente grande e inconveniente de se manipular textualmente, a omitimos e deixaremos que as simulações validem o modelo. Contudo, é possível calcular a derivada e o seu zero (com relação a a) numericamente via *software*, e esta foi a estratégia utilizada neste trabalho.

5.2.1 Infinitos Canais

Ao generalizar o modelo geométrico para múltiplos canais é natural ponderar até onde esta estratégia pode melhorar os resultados. Convém fazer uma análise com infinitos canais. Já discutimos nesta seção que o termo que encapsula toda a informação sobre a quantidade de canais é $x(C)$, tomemos então seu limite

$$\begin{aligned} \lim_{C\to\infty} x(C) &= \sum_{i=0}^{M-1} \binom{M-1}{i} \left[1-(1-a)^{k-1}\right]^i \left(1-a\right)^{(k-1)(M-1-i)} \\ &= 1. \end{aligned} \tag{5.5}$$

A equação (5.5) pode ser demonstrada algebricamente mas o seu resultado também pode ser entendido *a priori* com qualquer um de dois argumentos. O primeiro é que o somatório está contando todas as possibilidades de que qualquer quantidade de nós (até o total de M - 1) tenha transmitido em algum *slot*. Ora, ao se contar todas as possibilidades de um evento aleatório é obrigatório que o resultado seja 1. O outro argumento se refere ao fato de que o termo $x(C)$ modelava a probabilidade do nó marcado como de interesse transmitir sozinho no canal (sem ocorrência de colisão com outros). Uma vez que se tenha infinitos canais para transmitir, um número finitos de nós e uma probabilidade comum para a escolha de um canal é intuitivo imaginar que a probabilidade de dois nós sejam sorteados para o mesmo canal tende a zero, portanto as colisões tendem a nunca ocorrer e o termo $x(C)$ tende a 1.

Combinando as equações (5.5) e (5.3), obtemos a probabilidade de sucesso para infinitos canais em um ciclo com D_p *slots*

$$y = (1-p_f)^{N_R-1} \sum_{k=1}^{D_p} a(1-a)^{k-1}, \tag{5.6}$$

e resolvendo o somatório obtemos

$$y = (1-p_f)^{N_R-1}[1-(1-a)^{D_p}]. \tag{5.7}$$

Ao observar a equação (5.7) vemos que para maximizá-la com relação a a só importa o termo $[1-(1-a)^{D_p}]$. E ao considerar que $0 \leq a \leq 1$, o máximo valor que este termo pode assumir é 1, e o fará justamente quando $a = 1$. Mais uma vez isto faz perfeito sentido, pois se uma quantidade finita de nós tem uma quantidade infinita de canais para transmitir à disposição o melhor é jogar a moeda com probabilidade total de vencer para transmitir sempre que possível, já que as colisões tendem a nunca ocorrer.

Com estas considerações em mente, podemos chegar na equação final que descreve o modelo otimizado para infinitos canais

$$p_s = 1-[1-(1-p_f)^{N_R-1}]^N. \tag{5.8}$$

5.3 Resultados

A primeira preocupação é validar se a alteração proposta ao modelo de Rivera [1] está correta. Esta não é uma questão estritamente evidente em si mesma, uma vez que o modelo de Rivera modela um protocolo possível, o que este trabalho argumenta é que a interpretação que adotamos das premissas é mais realista e atinge resultados melhores. Simulamos o nosso modelo corrigido e fizemos a comparação entre os três dados. As Figuras 5.1 e 5.2 mostram que o nosso modelo obtém resultados melhores e valida sua corretude ao aderir muito firmemente às simulações. Também de acordo com o esperado é o fato de que a diferença entre os modelos original e corrigido é maior com mais repetições, uma vez que a correção melhora a probabilidade de sucesso de cada repetição, então com mais repetições a correção aparece mais.

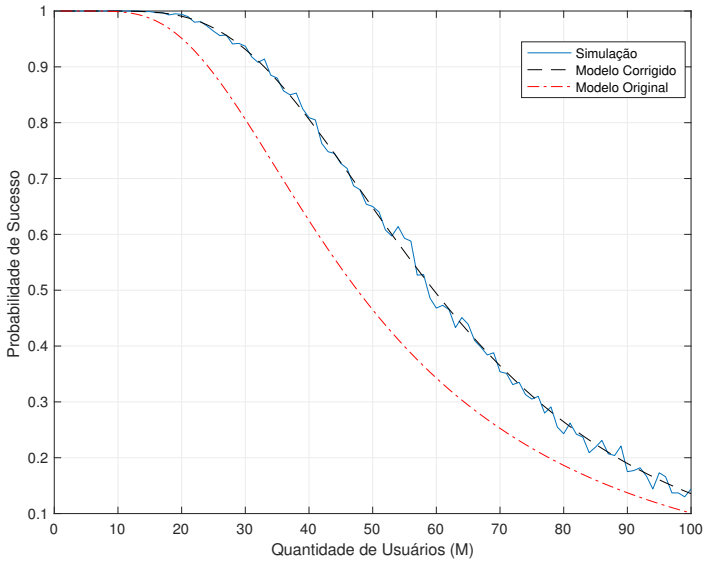

Figura 5.1 Validação da correção ao modelo geométrico proposto por Rivera [1], com $N = 10$, 1 canal e $p_f = 0,1$. 1000 rodadas de simulação.

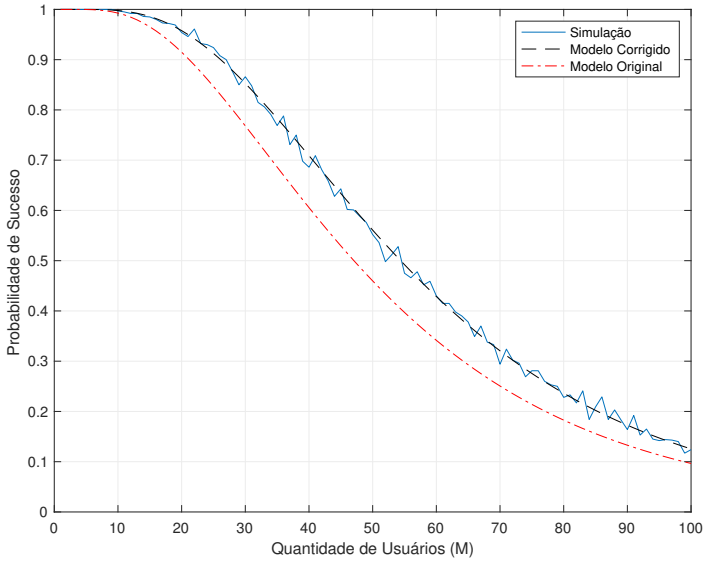

Figura 5.2 Validação da correção ao modelo geométrico proposto por Rivera [1], com $N = 5$, 1 canal e $p_f = 0,1$. 1000 rodadas de simulação.

Uma vez certos de que a correção proposta é coerente ao menos para o caso de um canal, podemos analisar se o modelo multicanal ainda está de acordo com a simulação para um quantidade maior de canais. A Figura 5.3 corrobora a aderência do modelo com a simulação para três canais e para duas opções diferentes de quantidade de repetições.

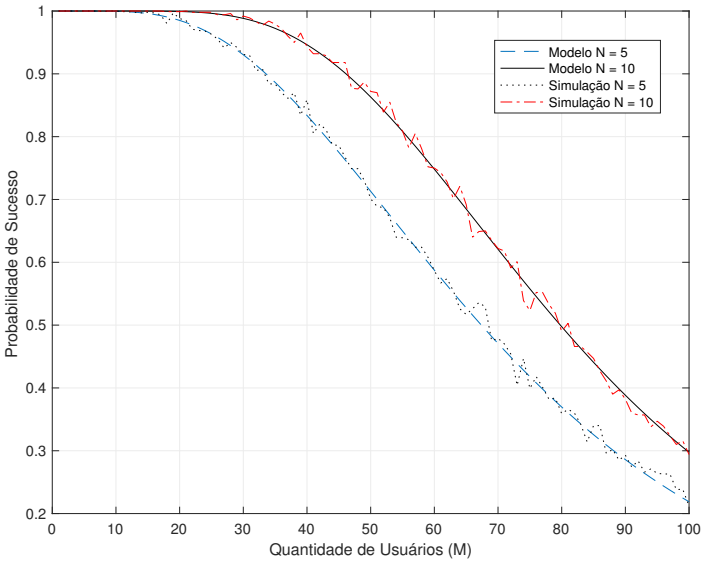

Figura 5.3 Comparação entre simulação e modelo para 3 canais, considerando $p_f = 0,1$. 1000 rodadas de simulação.

A Figura 5.4 ilustra o ganho de se utilizar mais de um canal independente de comunicação. A estratégia se prova útil, com ganhos de aproximadamente 20% já com 2 canais no ponto de maior ganho (por volta de 60 a 80 usuários) e de até aproximadamente 25% ao considerar 3 canais.

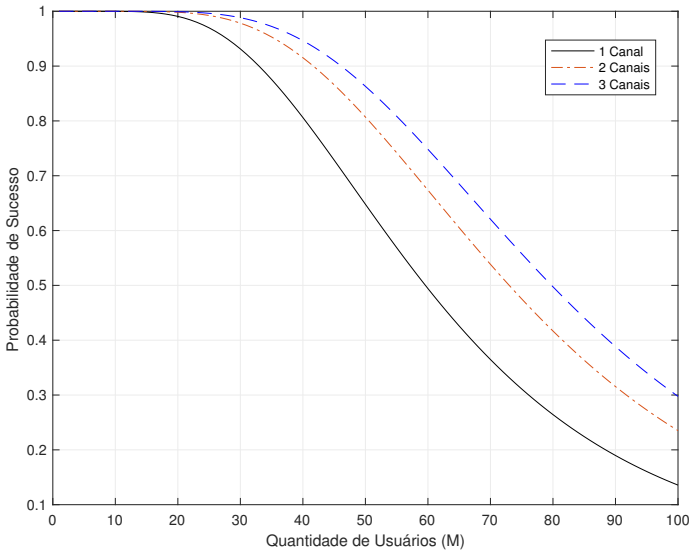

Figura 5.4 Comparação pela quantidade de canais, com $N = 10$ e $p_f = 0,1$.

Contudo, é claro na Figura 5.4 que um pouco antes de 40 nós as restrições de segurança das

VANETs não são respeitadas nem mesmo para 3 canais, e por isso todos os ganhos posteriores a esse ponto apenas validam o potencial da abordagem multicanal, mas não resolvem o problema. Convém avaliar o quanto efetivamente é possível adicionar em quantidade de usuários ao sistema sem desrespeitar as restrições.

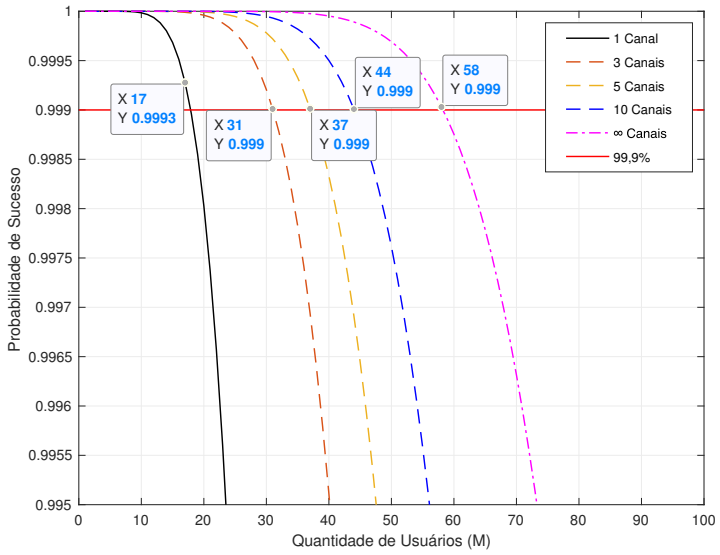

Figura 5.5 Comparação da aderência aos requisitos de entrega do pacote pela quantidade de canais, com $N = 10$ e $p_f = 5\%$.

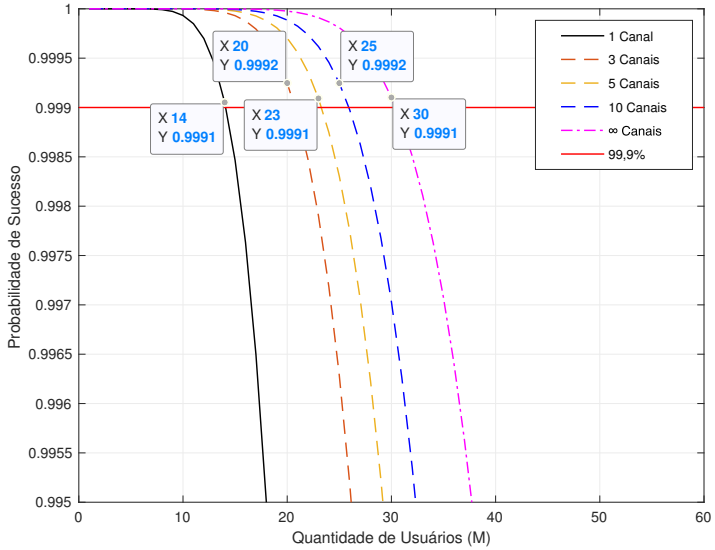

Figura 5.6 Comparação da aderência aos requisitos de entrega do pacote pela quantidade de canais, com $N = 10$ e $p_f = 10\%$.

As Figuras 5.5 e 5.6 dão a informação que queremos diretamente, vemos que para uma taxa de falha de 5% usar 3 canais quase dobra a quantidade de usuários que podemos ter na rede, enquanto sob uma taxa irrealisticamente pessimista de 10% ainda é possível um ganho de quase 50%. Também se observa a tendência de desgaste rápido da abordagem multicanal, nos dois casos apresentados o ganho proporcional de partir de 1 canal para 10 é mais que o dobro de partir de 10 canais para infinitos.

CAPÍTULO 6

Considerações Finais

Neste trabalho reintroduzimos alguns dos temas relevantes para o estudo das aplicações de segurança em VANETs, incluindo resultados prévios da literatura e noções teóricas fundamentais. Também demonstramos as características essenciais do protocolo *Slotted* Aloha e as reestudamos para o contexto multicanal, numa análise completa e formal. A partir disso, tomamos o trabalho de Rivera [1] como base e estendemos seus resultados para uma modelagem multicanal, propondo e incluindo reformulações completas e correções pontuais quando necessário.

A primeira proposta de reformulação realizada foi a de relaxar as premissas do modelo não-periódico de Rivera (baseado no trabalho de Bae [29]), de modo a obter um protocolo com menos controle e com mais possibilidade dos nós disputarem o canal pela transmissão. Obtivemos resultados com melhoras significativas e um modelo que em nada faz menos sentido que o original, e argumentamos que na verdade ele possui premissas mais realistas. Também encontramos circunstâncias nas quais o modelo geométrico de Rivera parece não obedecer estritamente às suas próprias premissas e propusemos a correção. Com isso, obtivemos outro ganho significativo na probabilidade de sucesso da transmissão, tornando o modelo viável para uma quantidade maior de nós.

Todas as nossas contribuições foram validadas através de simulações via *software* (MATLAB) dos eventos em si, com representações para os nós da rede e suas interações. Isto nem sempre é feito na literatura, mas é muito importante porque permite corrigir os modelos. De fato, só encontramos as possibilidades descritas de melhorar os resultados de Rivera porque as simulações apontavam situações adicionais e caminhos promissores que os modelos não capturavam.

6.1 Trabalhos Futuros

A linha de pesquisa perseguida neste trabalho parece promissora e possui muitas oportunidades ainda inexploradas. Pode-se citar por exemplo que é necessário refinar as simulações. O uso de um simulador de rede tradicional como o *Network Simulador 3* (NS-3) é recomendado para se chegar ainda mais perto do comportamento real dos nós numa rede que interajam de acordo com os protocolos modelados.

Além disso, existem muitos modelos que tentam prever erros de camada física, que este trabalho representou como uma constante p_f por simplicidade. Utilizar um (ou vários) destes modelos tornaria a modelagem mais rica e realista. Outra opção ainda melhor seria implementar o protocolo em dispositivos físicos e medir o desempenho real que emergiria de diferentes configurações.

Por fim, podemos considerar também que existem muitas possibilidades de se modelar um protocolo de comunicação multicanal. Nossa abordagem foi de certa forma simétrica, pois todos os canais eram iguais em capacidade, probabilidade de erro e acesso e todos os demais parâmetros possíveis de caracterização. É possível imaginar situações interessantes onde essa suposta simetria não acontece, uma questão que não abordamos.

Bibliografia

[1] J. C. Montealegre Rivera, "Difusão periódica ótima em redes veiculares com restrição de tempo considerando o terminal escondido", diss. de mestrado, Universidade de Brasília, 2015.

[2] Organização Mundial de Saúde, *Relatório global sobre o estado da segurança viária 2015*, 2015.

[3] N. H. T. S. Administration et al., "2015 motor vehicle crashes: overview", *Traffic safety facts research note*, vol. 2016, pp. 1–9, 2016.

[4] M. Khabazian, S. Aıssa e M. Mehmet-Ali, "Performance modeling of safety messages broadcast in vehicular ad hoc networks", *IEEE transactions on intelligent transportation systems*, vol. 14, nº 1, pp. 380–387, 2013.

[5] B. Chen, K. Jamieson, H. Balakrishnan e R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", *Wireless networks*, vol. 8, nº 5, pp. 481–494, 2002.

[6] C. E. Perkins, E. M. Royer, S. R. Das e M. K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks", *IEEE Personal communications*, vol. 8, nº 1, pp. 16–28, 2001.

[7] H. Cheng e Y. Yamao, "Reliable inter-vehicle broadcast communication with sectorized roadside relay station", em *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*, IEEE, 2013, pp. 1–5.

[8] J. C. Montealegre Rivera, M. M. Carvalho e R. M. de Moraes, "Deadline-constrained optimal broadcasting under hidden terminals in cognitive networks", em *Proceedings of the Latin America Networking Conference on LANC 2014*, ACM, 2014, p. 13.

[9] F. Li e Y. Wang, "Routing in vehicular ad hoc networks: A survey", *IEEE Vehicular technology magazine*, vol. 2, nº 2, 2007.

[10] K. Bilstrup, E. Uhlemann, E. G. Ström e U. Bilstrup, "On the ability of the 802.11 p MAC method and STDMA to support real-time vehicle-to-vehicle communication", *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 5, 2009.

[11] X. Ma, X. Yin e K. S. Trivedi, "On the Reliability of Safety Applications in VANETs.", *International Journal of Performability Engineering*, vol. 8, nº 2, 2012.

[12] Y. Toor, P. Muhlethaler, A. Laouiti e A. De La Fortelle, "Vehicle ad hoc networks: Applications and related technical issues", *IEEE communications surveys & tutorials*, vol. 10, nº 3, pp. 74–88, 2008.

[13] M. Torrent-Moreno, D. Jiang e H. Hartenstein, “Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks”, em *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ACM, 2004, pp. 10–18.

[14] X. Ma, X. Chen e H. H. Refai, “Performance and reliability of DSRC vehicular safety communication: a formal analysis”, *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 3, 2009.

[15] S. Oyama, “Vehicle safety communications: Progresses in Japan”, em *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, IEEE, 2008, pp. 241–241.

[16] J. Zhang, “A survey on trust management for vanets”, em *Advanced information networking and applications (AINA), 2011 IEEE international conference on*, IEEE, 2011, pp. 105–112.

[17] M. Green, “"How long does it take to stop?"Methodological analysis of driver perception-brake times”, *Transportation human factors*, vol. 2, nº 3, pp. 195–216, 2000.

[18] B. Xu, A. Ouksel e O. Wolfson, “Opportunistic resource exchange in inter-vehicle ad-hoc networks”, em *Mobile Data Management, 2004. Proceedings. 2004 IEEE International Conference on*, IEEE, 2004, pp. 4–12.

[19] A. S. Tanenbaum et al., “Computer networks, 4-th edition”, *ed: Prentice Hall*, 2003.

[20] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[21] J. G. Proakis, M. Salehi, N. Zhou e X. Li, *Communication systems engineering*. Prentice Hall New Jersey, 1994, vol. 2.

[22] K. N. Nakorn e K. Rojviboonchai, “Comparison of reliable broadcasting protocols for vehicular ad-hoc networks”, em *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, IEEE, 2010, pp. 1168–1171.

[23] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan e T. Talty, “Performance evaluation of safety applications over DSRC vehicular ad hoc networks”, em *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ACM, 2004, pp. 1–9.

[24] M. Torrent-Moreno, S. Corroy, F. Schmidt-Eisenlohr e H. Hartenstein, “IEEE 802.11-based one-hop broadcast communications: understanding transmission success and failure under different radio propagation environments”, em *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems*, ACM, 2006, pp. 68–77.

[25] M.-t. Sun, L. Huang, S. Wang, A. Arora e T.-H. Lai, “Reliable MAC layer multicast in IEEE 802.11 wireless networks”, *Wireless Communications and Mobile Computing*, vol. 3, nº 4, pp. 439–453, 2003.

[26] G. Korkmaz, E. Ekici e F. Ozguner, “Black-burst-based multihop broadcast protocols for vehicular networks”, *IEEE Transactions on Vehicular Technology*, vol. 56, nº 5, pp. 3159–3167, 2007.

[27] B. Hassanabadi e S. Valaee, "Reliable periodic safety message broadcasting in VANETs using network coding", *IEEE transactions on wireless communications*, vol. 13, nº 3, pp. 1284–1297, 2014.

[28] Q. Xu, T. Mak, J. Ko e R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC", em *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ACM, 2004, pp. 19–28.

[29] Y. H. Bae, "Analysis of optimal random access for broadcasting with deadline in cognitive radio networks", *IEEE Communications Letters*, vol. 17, nº 3, pp. 573–575, 2013.

[30] D. Jiang e L. Delgrossi, "IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments", em *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, IEEE, 2008, pp. 2036–2040.

[31] P. W. de Graaf e J. S. Lehnert, "Performance comparison of a slotted ALOHA DS/SSMA network and a multichannel narrow-band slotted ALOHA network", *IEEE Transactions on Communications*, vol. 46, nº 4, pp. 544–552, 1998.

Anexo A: Casos de Teste das Simulações

```
rng 'shuffle';

% CASO DE TESTES GEOMÉTRICO
maxNodes = 100;
nodeNumber = 1:maxNodes;
pf = 0.1;
Df = 500;
N = [5, 10];
C = 3;
qtdRepetitions = 1000;
registry = zeros(maxNodes, qtdRepetitions);
meansRegistry = zeros(numel(N), maxNodes);
for k = 1:numel(N)
    meansRegistry(k,1) = 1;
    for i = 2:numel(nodeNumber)
        M = nodeNumber(i);
        a = correctedGeometricprobpi1(N(k), pf, M/4, Df, M, C);
        parfor j = 1:qtdRepetitions
            protocol = SimplifiedSlottedAloha(M, N(k), Df/N(k), pf, a, C, 100);
            registry(i,j) = protocol.geometric();
        end
        disp(i);
        meansRegistry(k,i) = mean(registry(i,:));
    end
end

% CASO DE TESTES NÃO-PERIÓDICO
% Dp = [1, 10:10:500];
% lambda = 1:7;
% pf = 0;
% N = 1;
% C = 1:3;
% qtdRepetitions = 1000;
% registry = zeros(1, qtdRepetitions);
% simNonPeriodic = zeros(numel(C), numel(Dp), numel(lambda));
% for k = 1:numel(C)
%     Ch = C(k);
%     for i = 1:numel(lambda)
%         lamb = lambda(i);
%         for j = 1:numel(Dp)
%             Df = Dp(j);
```

```
%             a = correctedSolveACnumeric(Df, lamb, Ch);
%             parfor x = 1:qtdRepetitions
%                protocol = SimplifiedSlottedAloha(round(4*lamb*pi), N, Df, pf, a, Ch, 1
%                registry(x) = protocol.nonPeriodic()
%             end
%             simNonPeriodic(k, i, j) = mean(registry);
%         end
%         disp(i);
%     end
% end
```

Anexo B: Simulação dos Modelos de *Slotted* Aloha

```
classdef SimplifiedSlottedAloha < handle
% Esta classe representa o protocolo Slotted Aloha
% com canais e nós

properties
    M,
    N,
    Dp,
    a,
    Df,
    Nr,
    Nh,
    pf,
    Ch,
    allNodes,
    maxRadius
end

methods

    function obj = SimplifiedSlottedAloha(M, N, Dp, pf, a, Ch, maxRadius)
        obj.M = M;
        obj.N = N;
        obj.Dp = Dp;
        obj.Df = N*Dp;
        obj.maxRadius = maxRadius;
        obj.Nr = 1;
        obj.Nh = 0;
        obj.pf = pf;
        obj.Ch = Ch;
        centralNode = SimplifiedNode(maxRadius);
        centralNode.radius = 0;
        obj.allNodes = [centralNode];

        % sorteio dos nós para região de
        % broadcast ou terminal escondido
        for i = 1:(M-1)
            node = SimplifiedNode(maxRadius);
            obj.allNodes = [obj.allNodes, node];
            if (node.isPositionInsideInterest(maxRadius))
```

```
                obj.Nr = obj.Nr + 1;
            else
                obj.Nh = obj.Nh + 1;
            end
        end
        obj.a = a;
    end

    % reset no estado dos nós

    function resetNodes(obj)
        for i = 1:obj.M
            obj.allNodes(i).reset;
        end
    end

    % distribui as transmissões e contabiliza
    % quantos nós transmitiram junto com o nó
    % marcado

    function count = makeTransmissions(obj)
        count = 0;
        nodesTransmitting = [];
        channel = 0;
        for i = 1:obj.M
            if (rand() <= obj.a && ~obj.allNodes(i).transmitted)
                if (i == 1)
                    channel = randi([1, obj.Ch]);
                    count = count + 1;
                elseif (randi([1, obj.Ch]) == channel)
                    count = count + 1;
                end

                obj.allNodes(i).transmitted = true;
                nodesTransmitting = [nodesTransmitting, obj.allNodes(i)];
            end
        end
    end

    % modelo geométrico

    function didSucced = geometric(obj)
        didSucced = false;
%         disp(obj.Nr);
        for r = 1:obj.N
            if (didSucced)
```

```
                    break;
                else
                    currentSlot = 1;
                    obj.resetNodes();
%                     disp(r);
                    while currentSlot <= obj.Dp
                        currentSlot = currentSlot + 1;
                        count = obj.makeTransmissions();
                        if (obj.allNodes(1).transmitted)
                            if (count == 1)
                                if (rand() <= (1-obj.pf)^((obj.Nr + obj.Nh)/4 - 1))
                                    didSucced = true;
                                end
                            end
                            break;
                        end
                    end
%                     rng 'shuffle';
                end
            end
        end

        % modelo não-periódico alternativo

        function didSucced = nonPeriodic(obj)
            didSucced = false;
            currentSlot = 1;
            obj.resetNodes();
            while currentSlot <= obj.Df
                currentSlot = currentSlot + 1;
                count = obj.makeTransmissions();
                if (obj.allNodes(1).transmitted)
                    if (count == 1)
                        didSucced = true;
                        break;
                    end
                end
                obj.resetNodes();
            end
        end

    end
    end
```

Anexo C: Simulação de um Nó do Protocolo *Slotted* Aloha

```
classdef SimplifiedNode < handle
%SIMPLIFIEDNODES Summary of this class goes here
%   Detailed explanation goes here

properties
    radius
    angle
    transmitted
end

methods

    function obj = SimplifiedNode(maxRadius)
        obj.radius = rand()*maxRadius;
        obj.angle = rand()*2*pi;
        obj.transmitted = false;
    end

    % detecta se o nó foi pra região de broadcast
    % ou de terminal escondido

    function evaluation = isPositionInsideInterest(obj, maxRadius)
        if (obj.radius <= (maxRadius/4))
            evaluation = true;
        else
            evaluation = false;
        end
    end

    % reset do nó

    function reset(obj)
        obj.transmitted = false;
    end
end
end
```