



UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE
TELECOMUNICAÇÕES

RICARDO MOURA FIRMINO

Um Protocolo de Roteamento Multitabelas
para Monitoramento de Sinais Vitais em
Cenários de Operações Militares

NITERÓI

2021

UNIVERSIDADE FEDERAL FLUMINENSE
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA E DE
TELECOMUNICAÇÕES

RICARDO MOURA FIRMINO

Um Protocolo de Roteamento Multitabelas para Monitoramento de Sinais Vitais em Cenários de Operações Militares

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre em Engenharia Elétrica e de Telecomunicações. Área de concentração: Sistemas de Telecomunicações.

Orientadora:
Dianne Scherly Varela de Medeiros

NITERÓI

2021

Ficha catalográfica automática - SDC/BEE
Gerada com informações fornecidas pelo autor

F525p Firmino, Ricardo Moura
Um Protocolo de Roteamento Multitabelas para Monitoramento de Sinais Vitais em Cenários de Operações Militares / Ricardo Moura Firmino ; Dianne Scherly Varela de Medeiros, orientadora. Niterói, 2021.
88 f.
Dissertação (mestrado)-Universidade Federal Fluminense, Niterói, 2021.
DOI: <http://dx.doi.org/10.22409/PPGEET.2021.m.09870643710>
1. Redes Móveis Ad-Hoc. 2. Protocolos de comunicação de redes. 3. Roteamento multicaminhos. 4. Militar. 5. Produção intelectual. I. Medeiros, Dianne Scherly Varela de, orientadora. II. Universidade Federal Fluminense. Escola de Engenharia. III. Título.

CDD -

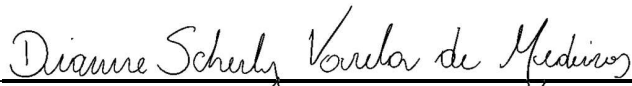
RICARDO MOURA FIRMINO

UM PROTOCOLO DE ROTEAMENTO MULTITABELAS PARA
MONITORAMENTO DE SINAIS VITAIS EM CENÁRIOS DE OPERAÇÕES
MILITARES

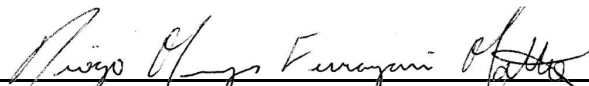
Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a Obtenção do Grau de Mestre em Engenharia Elétrica e de Telecomunicações.
Área de concentração: Sistemas de Telecomunicações.

Aprovado em 29 de outubro de 2021.

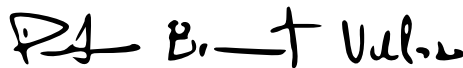
BANCA EXAMINADORA



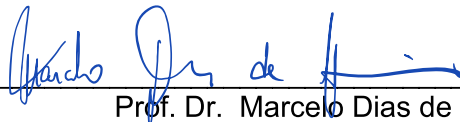
Prof. Dra. Dianne Scherly Varella de Medeiros - Orientador
Universidade Federal Fluminense - UFF



Prof. Dr. Diogo Menezes Ferrazani Mattos
Universidade Federal Fluminense - UFF



Prof. Dr. Pedro Braconnot Velloso
Sorbonne Université



Prof. Dr. Marcelo Dias de Amorim
Centre National de la Recherche Scientifique - CNRS

Niterói
2021

*Dedico o trabalho à minha querida avó Anna Firmino,
à minha tia e madrinha Sandra Eugênia Moura
e ao meu saudoso primo João Pedro Moura,
que durante minha jornada no curso,
partiram para a vida eterna.*

Agradecimentos

Primeiramente, agradeço a Deus, por minha vida, família e amigos.

À minha esposa Andreia e aos nossos filhos Eduardo, Bernardo e João, pelo incentivo e por toda paciência e compreensão pela ausência nesse período. Agradeço aos meus pais Maria do Rosário e Reinaldo por toda dedicação na minha formação. Agradeço a toda minha família pelo carinho, em especial ao meu irmão Ronaldo, pelos aconselhamentos.

À minha orientadora Dianne por toda sabedoria, confiança, amizade, cooperação e dedicação para a pesquisa que culminou neste trabalho. Ao professor Diogo pelos conselhos e ajuda na superação de obstáculos. Ao professor Pedro Velloso pelas orientações e direcionamentos da pesquisa.

À Marinha do Brasil e seus integrantes que me ajudaram a tornar esse sonho realidade. Em especial, aos Almirantes Koga e Luciana, aos Comandantes Rafael Dutra, Herbert e Ferreira Jesus, e ao Suboficial Moura Junior. Ao Capitão-Tenente(FN) Felipe Miranda e demais fuzileiros navais pela informações e imagens cedidas.

Aos professores do Mídiacom por toda força, incentivo e conversas.

Aos amigos que fiz durante o curso, pela excelente convivência.

Aos professores da banca examinadora pela disponibilidade em participar da defesa, pelos comentários e contribuições para melhoria dessa dissertação.

Aos demais funcionários do PPGEET que participam direta e indiretamente na formação dos alunos.

Resumo

As Redes Móveis *Ad-Hoc* (*Mobile Ad-Hoc NETWORKS* – MANETs) beneficiam aplicações em cenários militares ao possibilitarem o monitoramento de sinais vitais dos militares em operações de campo e, assim, aumentam a chance de sucesso da operação por auxiliar no processo de tomada de decisão. A comunicação intermitente e a volatilidade de rotas tornam a transmissão de dados desafiadora em MANETs. Desconexões frequentes e consequentes falhas geram atrasos significativos e erros na entrega de mensagens. O objetivo deste trabalho é ampliar a disponibilidade de caminhos durante a comunicação entre os nós que executam uma aplicação em uma rede *ad-hoc* móvel. Para tanto, propõe-se o *Multi-Tables Ad-hoc On Demand Distance Vector* (MT-AODV), um protocolo de roteamento reativo que evolui o protocolo AODV, amplamente utilizado na literatura. O MT-AODV adiciona a capacidade de gerenciar múltiplas rotas, visando aumentar o desempenho da comunicação em cenários de operações militares com mobilidade de tropas. O *Multi-Tables Ad-hoc On Demand Distance Vector* (MT-AODV) calcula múltiplas rotas para encontrar múltiplos caminhos possíveis na rede para fornecer maior resiliência e menor latência na comunicação. O desempenho do MT-AODV é comparado ao de outros protocolos tradicionais de MANETs, através de simulação em cenários distintos, com mobilidade e com falha de nós. Os resultados mostram que o protocolo proposto apresenta melhor desempenho se comparado ao protocolo AODV original devido ao aumento da disponibilidade de rotas em suas tabelas.

Palavras-chave: MANET, protocolos de roteamento, redes sem-fio, roteamento multi-caminhos.

Abstract

Mobile Ad-Hoc NETWORKS (MANETs) benefit applications in military scenarios by enabling the monitoring of military's vital signs in battlefields, and thus increase the mission's chance of success by assisting the decision-making process. Intermittent communication and route volatility make data transmission challenging in MANETs. Frequent disconnections and consequent failures lead to significant delays and errors in message delivery. This work aims to expand the availability of paths during the communication of nodes running an application in a mobile ad-hoc network. We propose MT-AODV, a reactive routing protocol that evolves the AODV protocol, widely used in the literature. MT-AODV adds the ability to manage multiple routes, aiming to increase communication performance in military operations scenarios with troop mobility. MT-AODV calculates multiple routes to find multiple possible paths in the network to provide greater resiliency and lower latency in communication. The performance of MT-AODV is compared to other traditional MANET protocols, through simulation in different scenarios, with node mobility and node failure. The results show that the proposed protocol presents better performance compared to the original AODV protocol due to the increased availability of routes through new tables.

Keywords: MANET, routing protocols, wireless networks, multipath routing.

Lista de Figuras

2.1	Dispositivos vestíveis em um combatente.	8
2.2	Cenário de combate com os diversos tipos de comunicação em WBANs. . .	10
2.3	Formato da Mensagem RREQ. Adaptado da RFC 3561.	17
2.4	Formato da Mensagem RREP. Adaptado da RFC 3561.	18
2.5	Formato da Mensagem RERR. Adaptado da RFC 3561.	19
3.1	Manutenção de rotas alternativas na proposta de Nasipuri e Das. A rota primária consiste em L_1, L_2, \dots, L_k . Cada nó na rota primária n_i , tem um caminho alternativo C_i para o destino. Adaptado.	26
3.2	Hierarquia de camadas para roteamento no LBMR. O <i>gateway</i> de dados é o nível mais alto das camadas, os nós mais próximos do <i>gateway</i> estão nas camadas superiores e os mais distantes estão nas camadas inferiores. Adaptado.	30
3.3	Fase de descoberta de rota do RMPR. Utiliza-se a potência do sinal recebido para cálculo do Fator de Energia (SF) dos caminhos. Adaptado.	32
4.1	Fluxograma simplificado de funcionamento do MT-AODV. A descoberta de rotas é realizada apenas quando um nó possui interesse em transmitir dados para outro nó. A manutenção de rotas atualiza as tabelas de acordo com o recebimento das mensagens de erro.	39
4.2	Topologia hipotética que exemplifica a configuração das tabelas de roteamento do nó de origem S . Nas tabelas de roteamento 2 e 3, são mostradas apenas as rotas para o nó destino Z . Existem dois caminhos principais e um caminho alternativo para salvaguarda registrados nas tabelas consolidadas.	42

4.3	Topologia que exemplifica a configuração dos predecessores associados a rotas registradas nos nós. São mostradas apenas as rotas dos nós intermediários. No caso de interrupção de um enlace, o nó intermediário encaminha mensagem de erro aos nós predecessores que possuem como <i>gateway</i> o nó do enlace interrompido.	43
5.1	Topologia da rede com nós em grade 4×5 . Apenas um coletor está configurado e todos os nós enviam dados para o nó coletor.	53
5.2	Proporção de pacotes de dados recebidos e perdidos em relação aos pacotes de dados transmitidos. O MT-AODV supera o AODV em todos os cenários. A perda de pacotes aumenta em caso de falha de nó próximo ao coletor. .	54
5.3	Média de pacotes recebidos pelo coletor em função da proximidade com o nó de origem quando ocorrem falhas em nós de acordo com a distância até o coletor. A tendência é de que quanto mais distante do nó coletor a falha ocorre, menor é o impacto em nós mais próximos ao coletor. Os nós do MT-AODV conseguem entregar mais pacotes ao coletor que o AODV. (a) No caso de falhas alternadas em nós vizinhos ao coletor, todos os nós são influenciados. (b) Falhas em nós com 2 saltos de distância do coletor não influenciam os nós a 1 salto de distância do coletor. (c) Com falhas em nós a 3 saltos do coletor, os nós a 1 e 2 saltos de distância não são influenciados pelas falhas e o número de caminhos que podem ser encontrados é maior.	55
5.4	Proporção de pacotes de controle recebidos sobre todos os pacotes recebidos. MT-AODV envia menos pacotes de controle do que AODV.	56
5.5	Atraso fim-a-fim de pacotes de dados recebidos. O atraso máximo diminui em MT-AODV em comparação com AODV.	57
5.6	Atraso fim-a-fim médio em função da distância até o nó coletor para cada cenário de falha. Quanto maior a distância ao coletor, maior é o atraso. O MT-AODV apresenta menor atraso em todos os cenários, exceto quando a falha ocorre em nós a 2 saltos do coletor. Nesse caso, os nós a 7 saltos do coletor apresentam maior atraso com o MT-AODV. Os nós a 2 saltos do coletor também apresentam maior atraso independentemente do cenário. .	58
5.7	Vazão de pacotes de dados recebidos. MT-AODV possui valores mínimos e máximos superiores ao AODV nos 3 cenários.	59

-
- 5.8 Vazão média em função da distância dos nós ao nó coletor para cada cenário. O MT-AODV apresenta melhor desempenho em todos os cenários. (a) Falha alternada nos vizinhos do nó coletor causa maior impacto no desempenho da rede pela limitação de caminhos disponíveis. (b) Falha nos nós a 2 saltos de distância do coletor. Os nós vizinhos não são afetados, atingindo vazão máxima. MT-AODV tem melhor desempenho. (c) Falha nos nós a 3 saltos de distância. Os nós a até 2 saltos do coletor não são impactados. 60
- 5.9 Número de pacotes recebidos. O MT-AODV supera os demais protocolos nos cenários com 3 falhas, mobilidade e mobilidade com falhas. A resiliência a falhas do MT-AODV depende da quantidade de rotas encontradas. . . . 61
- 5.10 Taxa de pacotes perdidos. MT-AODV obtém melhor desempenho comparado ao AODV nas condições de falhas permanentes e mobilidade. Nas demais condições, o resultado é equivalente ao AODV. 63
- 5.11 Atraso fim-a-fim. O MT-AODV obtém melhor desempenho que o AODV nos cenários de falha em 4 nós e de mobilidade. O OLSR apresenta os melhores resultados nos casos de falhas intermitentes, por ser um protocolo proativo e de estado de enlace. 64
- 5.12 Vazão média da rede. MT-AODV supera o AODV nos cenários de falhas intermitentes e mobilidade. 65

Lista de Tabelas

4.1	Arquivos de código fonte e cabeçalho modificados para a implementação do MT-AODV.	46
5.1	Resumo dos parâmetros de configuração usados na simulação do primeiro experimento.	50
5.2	Resumo dos parâmetros de configuração usados na simulação do segundo experimento.	52
5.3	Comparação AODV x MT-AODV quanto ao número de saltos e de tabelas na rede de topologia de grade 4x5.	59

Lista de Abreviaturas e Siglas

AODV	<i>Ad-hoc On Demand Distance Vector</i>
AOMDV	<i>Ad-hoc On-demand Multipath Distance Vector</i>
CBR	<i>Constant Bit-Rate</i>
CCC	Centro de Comando e Controle
DSDV	<i>Destination-Sequenced Distance Vector</i>
DSR	<i>Dynamic Source Routing</i>
ECG	Eletrocardiograma
EMG	Eletromiograma
IEEE	<i>Institute of Electrical and Electronics Engineers</i>
LBMR	<i>Load-Balanced Multipath Routing</i>
LEA	<i>Load Estimation Algorithm</i>
LoRa	<i>Long Range</i>
LRC	<i>Layer Routing Construction</i>
LR-WPAN	<i>Low Rate Wireless Personal Area Networks</i>
MAC	<i>Media Access Control</i>
MANET	<i>Mobile Ad-hoc NETWORKS</i>
MP-OLSR	<i>Multi-Path Optimized Link State Routing</i>
MPR	<i>MultiPoint Relay</i>
MT-AODV	<i>Multi-Tables Ad-hoc On Demand Distance Vector</i>
NS-3	<i>Network Simulator 3</i>
OAOMDV	<i>Optimized Ad-hoc On-demand Multipath Distance Vector</i>
OLSR	<i>Optimized Link State Routing Protocol</i>
OTAN	Organização do Tratado do Atlântico Norte
QoS	<i>Quality of Service</i>

RERR	<i>Route Error</i>
RM	<i>Route Maintenance</i>
RMPR	<i>Reliable Multi-path Routing</i>
RREP	<i>Route Reply</i>
RREP-ACK	<i>Route Reply Acknowledgement</i>
RREQ	<i>Route Request</i>
RREQ ID	Identificador de Broadcast
SMR	<i>Split Multipath Routing</i>
SpO₂	Saturação periférica de Oxigênio
UDP	<i>User Datagram Protocol</i>
WBAN	<i>Wireless Body Area Networks</i>
WSN	<i>Wireless Sensor Networks</i>
SF	<i>Strength Factor</i>

Sumário

1	Introdução	1
1.1	Objetivo	2
1.2	Contribuições	3
1.3	Estrutura da Dissertação	4
2	Roteamento Multicaminhos para Monitoramento de Sinais Vitais	5
2.1	Monitoramento de sinais vitais em operações de campo	5
2.2	Redes Corporais Sem Fio	9
2.2.1	Roteamento em redes corporais sem fio	10
2.3	Protocolos de roteamento tradicionais em MANETs	12
2.3.1	<i>Ad-hoc On Demand Distance Vector</i> (AODV)	16
2.4	Roteamento multicaminhos em MANETs	20
3	Protocolos de Roteamento Sem Fio com Múltiplos Caminhos	24
3.1	Protocolos de roteamento multicaminho em MANETs	24
3.1.1	Protocolos baseados no DSR	25
3.1.2	Protocolos baseados no AODV	27
3.1.3	Protocolos baseados no OLSR	28
3.2	Protocolos de roteamento multicaminhos em WBANs	29
3.3	Diferencial do MT-AODV	31
4	O protocolo de Roteamento Multi-Tables Ad-hoc On Demand Distance Vector	33

4.1	Visão geral do MT-AODV	33
4.1.1	Aspectos relevantes para o desenvolvimento	34
4.1.2	Funcionamento do MT-AODV	38
4.2	Detalhamento do protocolo	38
4.2.1	Descoberta de rotas	40
4.2.2	Manutenção de rotas	42
4.3	Implementação do MT-AODV	44
5	Resultados e Discussão	48
5.1	Primeiro experimento: posição inicial dos nós em grade	48
5.2	Segundo experimento: posição inicial aleatória	49
5.3	Avaliação de desempenho	52
5.3.1	Posição inicial dos nós em grade	53
5.3.2	Posição inicial dos nós aleatória	61
6	Conclusão e Trabalhos Futuros	66
	Referências	68

Capítulo 1

Introdução

O cumprimento de uma missão militar depende de fatores heterogêneos que atuam harmonicamente entre si e que estão associados a eventos previsíveis ou imprevisíveis. Um dos pilares para o sucesso da missão é a informação da vitalidade dos militares em operação. As decisões táticas em operações militares são efetivadas por um Centro de Comando e Controle (CCC). Adriano [1] define o Comando e Controle como sendo uma atividade que permite o compartilhamento de informações, a tomada de decisão e a condução de avaliações de forma coordenada, desde a fase do planejamento até a fase de execução de uma operação militar. Além disso, o autor define que a matéria-prima para essa atividade é a informação, que pode ser acessada pelos níveis de decisão envolvidos em uma operação, transformando-a em elemento vital para a eficácia da atividade. Assim, a informação célere sobre a saúde dos combatentes durante uma operação de campo auxilia o líder da tropa e o comando na tomada de decisão no futuro imediato. Nesse contexto, sensores e dispositivos inteligentes que coletam e transmitem informações em tempo real tendem a ser cada vez mais empregados para a comunicação móvel militar em cenários de operação. Dessa forma, contribui-se para a execução bem sucedida da operação.

Dentre os dispositivos mais comuns utilizados em operações militares pode-se citar câmeras portáteis, geolocalizadores, processador de dados táticos, rádios comunicadores e sensores de sinais vitais. O monitoramento de combatentes em ambientes de operações militares fornece previsões sobre a saúde e o desempenho de um indivíduo a partir de seu estado fisiológico em tempo real [2]. Com essas informações, um CCC pode tomar decisões que melhorem o desempenho da missão, assim como a capacidade de sobrevivência dos combatentes. Nesse contexto, as redes móveis sem fio, que dispensam a instalação de um ponto de acesso comum aos dispositivos e são conhecidas como Redes Móveis *Ad-hoc* (*Mobile Ad-hoc NETWORKS* - MANET), podem trazer benefícios para as operações. As

MANETs vêm evoluindo para implementação de serviços em tempo real em vários setores para uso civil ou militar [3]. Essas redes podem ser empregadas para comunicação em áreas remotas, interação entre veículos, dispositivos vestíveis (*wearables*), redes de sensores e diversas outras aplicações. Devido à autonomia das *Mobile Ad-hoc NETWORKS* (MANET)s em relação à necessidade de implantação de uma infraestrutura, há uma tendência de aplicar essas redes no ambiente de operação militar para monitoramento de saúde [4]. No entanto, a comunicação em MANETs é desafiadora devido à complexidade do ambiente de propagação e à mobilidade constante dos nós na rede, sendo necessário desenvolver novos protocolos ou adaptar os já existentes para apresentarem desempenho adequado em cenários dinâmicos.

Os protocolos de roteamento afetam diretamente o desempenho das aplicações devido à busca por rotas e à indisponibilidade de rotas que influenciam a vazão, a taxa de entrega e a latência dos pacotes transmitidos [5]. A escolha do melhor caminho e a manutenção de rotas são exemplos de desafios que os protocolos de roteamento *ad-hoc* superam de maneiras diferentes em redes sujeitas a falhas de enlaces ou de nós. Assim, os protocolos atuais buscam melhorar a eficiência da comunicação nas redes de acordo com suas particularidades. No caso das MANETs, é necessário que o protocolo de roteamento seja capaz de lidar com a topologia dinâmica e resulte em baixa perda de pacotes e baixa latência fim-a-fim. O uso de protocolos de roteamento com múltiplos caminhos pode melhorar o desempenho das aplicações em redes dinâmicas, uma vez que a disponibilidade de rotas é ampliada em comparação ao uso de protocolos com caminhos únicos. Ademais, é possível atingir uma melhor distribuição do tráfego de dados. Contudo, a complexidade e gerenciamento de múltiplas rotas impõem desafios adicionais.

1.1 Objetivo

Esta dissertação tem como objetivo geral aumentar a resiliência a falhas em MANETs, para aplicações de monitoramento de sinais vitais dos combatentes em operações militares. Para isso, propõe-se o MT-AODV, um protocolo de roteamento multicaminhos gerenciado por múltiplas tabelas, que agrega resiliência à comunicação sem aumentar a sobrecarga de mensagens de controle. O funcionamento do protocolo é derivado do protocolo *Ad-hoc On Demand Distance Vector* (AODV), evoluindo esse protocolo para gerenciar rotas de forma a possibilitar o encaminhamento dos pacotes de dados por mais de um caminho de mesmo custo. Por utilizar as mensagens originais do AODV, a retrocompatibilidade é mantida.

1.2 Contribuições

A proposta desta dissertação contribui para o avanço do estado-da-arte ao permitir o gerenciamento de múltiplas rotas através de múltiplas tabelas de roteamento e a distribuição simultânea de tráfego de dados por todas as rotas disponíveis. Não é necessário criar novas mensagens de controle, o que mantém a retrocompatibilidade com o protocolo AODV. O MT-AODV constrói múltiplas tabelas de roteamento para gerenciamento de múltiplas rotas com o objetivo de aumentar a disponibilidade da comunicação entre nós em uma rede propensa a falha e mobilidade dos nós. A ideia é permitir que o tráfego seja distribuído por mais de uma rota. Além disso, o MT-AODV permite que rotas alternativas estejam prontamente disponíveis quando uma falha em nó é detectada, ou quando um enlace é interrompido. As tabelas de roteamento são criadas sob demanda e as rotas registradas podem ser mais custosas do que o caminho de menor custo. Além de aumentar a disponibilidade da comunicação, é possível aumentar a vazão da comunicação ao utilizar as múltiplas rotas simultaneamente. O protocolo é implementado no *Network Simulator 3* (NS-3) e seu desempenho é avaliado através de simulações em cenários distintos. Assim, esta dissertação contribui com o desenvolvimento de um módulo adicional para o NS-3.

A avaliação de desempenho do protocolo é feita de forma comparativa, utilizando como referência protocolos de roteamento para MANETs bem conhecidos, como *Destination-Sequenced Distance Vector* (DSDV), *Optimized Link State Routing Protocol* (OLSR) e AODV. Varia-se a quantidade de nós transmissores com 1 a 4 falhas permanentes e falhas intermitentes em todos os nós. Também verifica-se o desempenho do protocolo em cenários com falhas intermitentes e mobilidade. Avalia-se, ainda, o desempenho do protocolo em um cenário mais controlado a fim de medir os resultados da simulação com mínima influência de aleatoriedade. Para isso, constrói-se um cenário em que os nós estão distribuídos em grade (*grid*) e estão propensos a falhas. Os resultados mostram que o MT-AODV tem um desempenho melhor do que o protocolo original devido à maior disponibilidade de caminhos em suas tabelas de roteamento.

A pesquisa realizada nesta dissertação originou as seguintes publicações:

- *Aplicações em redes de sensores na área da saúde e gerenciamento de dados médicos: tecnologias em ascensão*, XX Simpósio Brasileiro de Computação Aplicada à Saúde (SBCAS), 2020;
- *MT-AODV: Provendo Resiliência em Redes Ad-Hoc Móveis Militares através de Múltiplas Tabelas de Roteamento sob Demanda*, XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT), 2021.

- *MT-AODV: Resilient Communication in Military Mobile Ad-Hoc Networks through On-demand Multiple Routing Tables*, 5th Conference on Cloud and Internet of Things (CIoT), 2022 (aceito para publicação).

1.3 Estrutura da Dissertação

Esta dissertação está organizada da seguinte forma. O Capítulo 2 apresenta a fundamentação teórica do roteamento multicaminhos para monitoramento de dados de saúde em cenários de operação militar. Em seguida, o Capítulo 3 descreve os principais trabalhos relacionados a pesquisa, e suas respectivas limitações. No Capítulo 4, são apresentados o protocolo MT-AODV, seu funcionamento, suas vantagens e limitações. O Capítulo 5 descreve os cenários de simulação utilizados nas análises e discute os resultados das simulações realizadas. Por fim, o Capítulo 6 conclui a dissertação, destacando as principais contribuições e estabelecendo as direções futuras.

Capítulo 2

Roteamento Multicaminhos para Monitoramento de Sinais Vitais

Este capítulo introduz os temas que compõem esta dissertação. Primeiramente, descreve-se o monitoramento de sinais vitais e é feita uma breve introdução às redes corporais sem fio. Em seguida, os protocolos de roteamento tradicionais em MANETs são detalhados e, por fim, descreve-se a importância do roteamento multicaminhos em MANETs.

2.1 Monitoramento de sinais vitais em operações de campo

A coleta de dados críticos durante as operações em campos de batalha permite que os comandantes sejam capazes de gerar estratégias melhores e tomar decisões mais adequadas e com maior rapidez. Fornecer informações médicas atualizadas, como a aptidão física e psicológica de cada combatente, pode ajudar significativamente nessas decisões. A maior parte do sistema atual de coleta de informações médicas está em formato de voz ou texto. Para coletar esses dados com dispositivos móveis e propagá-los ao comandante, é necessária uma solução de transferência de dados eficiente, com baixo consumo de energia, segura e leve [6].

Em cenários de combate, a comunicação existente entre tropa e comando é limitada. Primeiramente, o combatente precisa interromper o engajamento para se comunicar, deve estar em local abrigado e precisa inserir os dados que deseja enviar. Com uma rede de sensores onde os dados coletados são transmitidos automaticamente para central de controle e comando, a fluidez da comunicação torna-se mais eficiente. Contudo, estabelecer

e manter uma rede de sensores disponível para comunicação em tempo real traz diversos desafios. Os principais desafios para comunicação entre combatente e o centro de comando e controle são listados a seguir.

- **Ausência de infraestrutura:** os locais onde são realizadas operações militares e policiais geralmente são desprovidos de infraestrutura fixa para comunicação [7] e o acesso para instalação prévia é complexo, sendo frequentemente inviável.
- **Distância:** não existe uma distância fixa nos cenários de operações, podendo variar de centenas de metros a centenas de quilômetros.
- **Mobilidade:** os combatentes movem-se constantemente durante o período de operação, alterando a topologia da rede frequentemente.
- **Ocultação da localização:** existem ambientes onde o espectro eletromagnético é monitorado pelo inimigo. Por isso, deve-se ser cuidadoso com a potência do sinal transmitido e o momento de transmissão.
- **Propagação do sinal:** ambientes geralmente com materiais que aumentam a atenuação do sinal eletromagnético, como areia, lama, árvores e concreto.
- **Segurança da informação:** deve-se considerar a interceptação do sinal e evitar sua decodificação, assim como garantir a integridade da informação recebida.
- **Latência:** a comunicação deve ser célere para que as informações atualizadas estejam disponíveis no centro de comando e controle.

Tendo em vista os desafios supracitados, a utilização de redes *ad-hoc* é ideal, uma vez que não precisam de infraestrutura, são formadas por nós móveis para auto-rotear o tráfego de rede entre si [8], podem alcançar maiores distâncias com o uso de múltiplos saltos e é possível restringir a comunicação até determinado número de nós, além de parametrizar a potência de transmissão.

Os setores de defesa e segurança têm investido cada vez mais em equipamentos e sensores modernos para coleta e transmissão de informações em tempo real que auxiliem no controle, monitoramento e tomada de decisão de uma operação. Câmeras de gravação, equipamentos geolocalizadores e comunicadores de rádio estão presentes nos campos de batalhas e operações policiais [9]. No contexto de monitoramento de dados médicos, as redes de sensores têm se tornado cada vez mais populares na área de saúde devido à ampla

disseminação dos celulares e acessórios aptos a captar dados médicos e ao crescimento de iniciativas de monitoramento remoto de pacientes. Entre as redes de sensores utilizadas para monitorar a saúde humana, observa-se um uso mais amplo das redes de sensores sem fio (*Wireless Sensor Networks* - WSN). Essas redes são caracterizadas como um conjunto de sensores especializados distribuídos espacialmente que, simultaneamente, são capazes de monitorar, registrar e comunicar dados representando medições de variáveis ambientais ou de um determinado sistema. Nesse sentido, cabe destaque às redes corporais sem fio (*Wireless Body Area Networks* - WBAN) que permitem a comunicação entre diversos sensores e atuadores corporais [10]. Essas redes são detalhadas na Seção 2.2.

Uma *Wireless Body Area Networks* (WBAN) abrange nós sensores que monitoram os sinais vitais dos indivíduos. Várias aplicações dependem de WBANs, compreendendo desde entretenimento até cuidados de saúde onipresentes e passando por aplicações de condicionamento físico e esportes de alto desempenho [11]. A maioria desses aplicativos requer o uso de dispositivos vestíveis (*wearables*) de monitoramento de integridade. Embora as aplicações médicas estejam no centro das pesquisas da WBAN, com foco em vida assistida, prevenção, diagnóstico, prognóstico, entre outros usos, as WBANs têm grande potencial para auxiliar os setores de defesa e segurança. A Figura 2.1 mostra um exemplo de configuração de dispositivos vestíveis de um combatente. Além dos sensores de monitoramento de sinais vitais, outros equipamentos estão afixados no uniforme do militar, como câmera, geolocalizador, rádio comunicador e áudio (fone e microfone). Nesta dissertação, devido à diferença de taxa de transmissão requerida pelos diversos equipamentos, é tratado apenas os sensores de monitoramento de sinais vitais, representados em verde na Figura 2.1. Contudo, para continuação do trabalho desenvolvido, deve-se levar em conta a implantação de uma rede capaz de suportar outros serviços, conforme previsto no Capítulo 6. O monitoramento de sinais vitais contribui para melhorar o desempenho de uma missão e a capacidade de sobrevivência dos soldados.

Os nós sensores WBAN comunicam-se autonomamente entre si, por meio de saltos únicos ou por múltiplos saltos. Nesse sentido, os protocolos de roteamento têm papel fundamental. Esses protocolos afetam diretamente o desempenho das aplicações devido aos diferentes algoritmos implementados que influenciam as métricas de desempenho da rede, como vazão, taxa de entrega de pacotes e latência, bem como outros aspectos, por exemplo a segurança da rede, privacidade e consumo de energia dos dispositivos.

Além das informações operacionais, as forças armadas e de segurança estão cada vez mais interessadas nos dados de saúde dos combatentes durante o treinamento e a missão,



Figura 2.1: Dispositivos vestíveis em um combatente.

como pressão arterial, glicose, temperatura, Saturação periférica de Oxigênio (SpO₂), Eletromiograma (EMG) e Eletrocardiograma (ECG). Monitorar a saúde dos combatentes é um desafio, uma vez que o equipamento de monitoramento deve considerar o tamanho, o peso, a intensidade do sinal e a resistência ao impacto, à água e à areia. O posicionamento e a mobilidade dos combatentes variam, e a transmissão de longa distância nem sempre é possível. Portanto, a WBAN surge como uma solução apropriada para monitoramento da vitalidade dos militares em operações.

Como as informações sobre a saúde do combatente estão disponíveis, o CCC verifica em tempo real as condições de saúde do militar antes, durante e depois da missão. É possível, por exemplo, saber se os componentes da tropa são capazes de se engajar em um cenário de combate enquanto ocorre a missão. Esses dados são coletados por sensores instalados no corpo do combatente, compondo a WBAN. Cada nó sensor tem baixa potência de transmissão, o que limita a comunicação a um alcance muito curto. Uma WBAN comumente implementa um nó coletor (*sink*), também conhecido como nó coordenador, que atua como um *gateway* entre os dispositivos da rede corporal, entre esses dispositivos e outras redes, ou entre os dispositivos de redes corporais distintas e próximas. Portanto, os nós sensores devem atuar como roteadores, permitindo que cada nó transmissor alcance o nó coletor. Essa configuração descreve uma pequena rede *ad-hoc*.

O monitoramento de dados médicos de múltiplos indivíduos é uma aplicação de tempo real que produz um fluxo contínuo de dados, mas não necessitam de alta taxa de transmissão. É imperativo, no entanto, que o atraso no recebimento dos dados atenda aos

requisitos do serviço. Além disso, essas aplicações devem permitir a mobilidade dos indivíduos monitorados, de forma que é essencial que a comunicação seja sem fio.

2.2 Redes Corporais Sem Fio

As WBANs consistem de vários dispositivos heterogêneos próximos do corpo humano e que se comunicam por meio de uma rede sem fio. Esses dispositivos têm potencial para se comunicar com aplicativos em sistemas para monitoramento da saúde humana [12]. Cada dispositivo geralmente é composto por um transceptor rádio com uma antena para comunicação sem fio, um microprocessador, uma memória, uma bateria para alimentação elétrica do dispositivo e sensores de monitoramento, podendo contar também com atuadores. Normalmente, o dispositivo utiliza sistema operacional com capacidade de processamento limitada, poucos requisitos de memória e que causa baixa sobrecarga no dispositivo [13].

A comunicação das WBANs pode ser classificada em três classes diferentes:

- **Classe 1 - Comunicação intra-WBAN:** troca de informações entre os dispositivos que monitoram o mesmo corpo;
- **Classe 2 - Comunicação inter-WBAN:** troca de informações entre dispositivos de diferentes WBANs através de seus *gateways*;
- **Classe 3 - Comunicação extra-WBAN:** troca de informações entre a WBAN e redes externas.

A Figura 2.2 ilustra a comunicação WBAN para monitoramento de saúde em um possível cenário de campo de batalha, considerando as classes de comunicação nas WBANs. No caso representado, os combatentes possuem dispositivos que se comunicam entre si. Apenas um combatente possui um enlace de comunicação com o CCC, e esse militar pode ser denominado como combatente coletor de dados, representando o nó coletor (*sink*). Em zonas hostis, os militares restringem sua comunicação de longo alcance para não serem detectados pelos inimigos. É possível usar tecnologia de telefonia móvel ou enlaces baseados na tecnologia de Longo Alcance (*Long Range* - LoRa) para comunicação com o CCC. Contudo, a comunicação extra-WBAN não se restringe apenas a essas tecnologias, qualquer tecnologia de longa distância pode ser utilizada desde que consiga transmitir os dados coletados. A comunicação intra-WBAN depende das tecnologias de curta distância

como as padronizadas pelo *Institute of Electrical and Electronics Engineers* (IEEE), por exemplo, IEEE 802.11 (*Wi-Fi*), IEEE 802.15.1 (*Bluetooth*) [14] e IEEE 802.15.4 (*Low Rate Wireless Personal Area Networks - LR-WPAN*) [15], dentre outras. A propagação do sinal em cenários de operação militar é restringida pela mobilidade do nó, distância e tempo de comunicação, deteriorando o desempenho da comunicação. As redes móveis de múltiplos saltos ajudam a melhorar esse desempenho. No entanto, o desempenho dos protocolos de roteamento não foi exaustivamente estudado em cenários militares somente com o uso de dispositivos vestíveis para determinar os protocolos de roteamento mais adequados para cada situação. O foco desta dissertação é voltado para a comunicação inter-WBAN, onde os dispositivos operam no padrão IEEE 802.11 (*Wi-Fi*) sem a necessidade de infraestrutura fixa. A composição dos cenários estudados está detalhada no Capítulo 5.

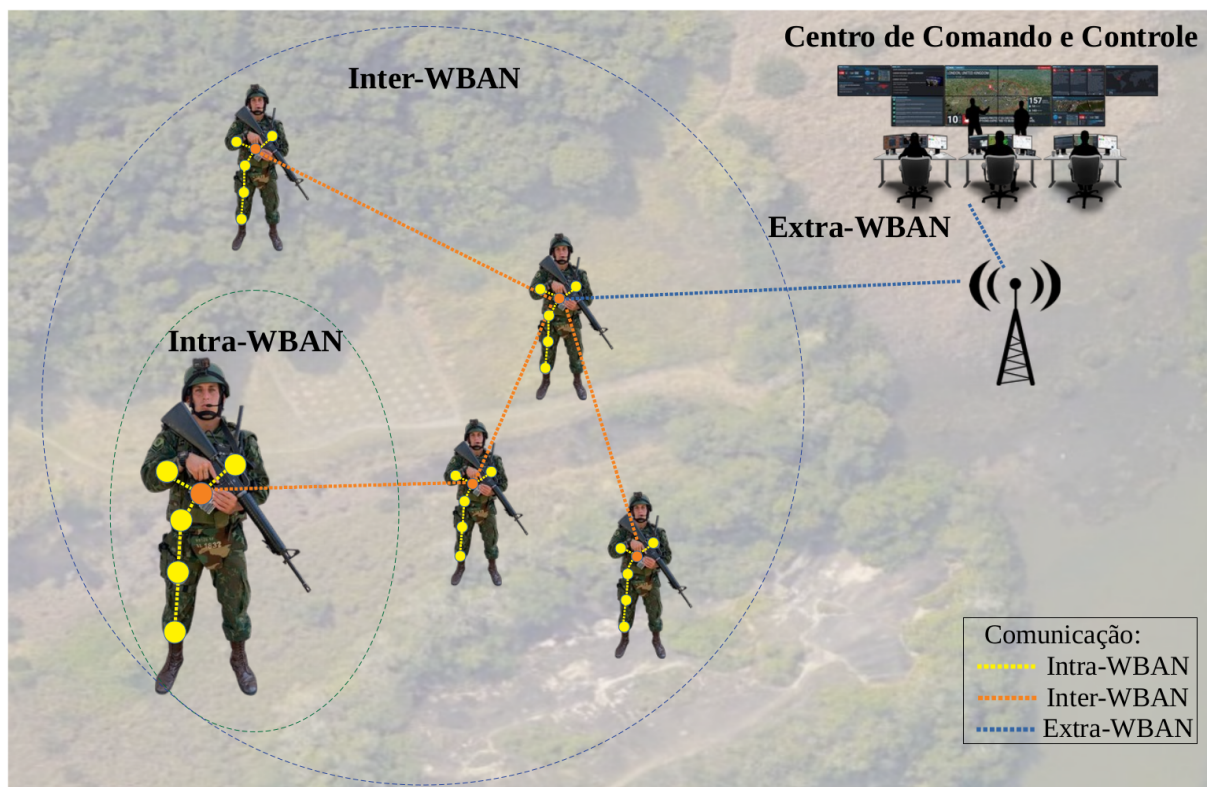


Figura 2.2: Cenário de combate com os diversos tipos de comunicação em WBANs.

2.2.1 Roteamento em redes corporais sem fio

Os aspectos relativos ao roteamento em WBANs ainda não estão definidos em nenhuma norma padronizada pelo IEEE. Por esse motivo, e impulsionados por buscar soluções para enfrentar os desafios de WBAN, diversos trabalhos de pesquisa foram realizados nos últimos anos focados no desenvolvimento de novos protocolos de roteamento

para WBANs [16]. Os protocolos de roteamento propostos para WBANs foram inicialmente classificados em cinco tipos [17, 18] e estão relacionados com os principais desafios identificados em WBANs. Esses grupos são categorizados como algoritmos de roteamento baseados em (i) agrupamentos (*clusters*), (ii) qualidade de serviço, (iii) camada cruzada (*cross-layered*), (iv) movimentos corporais e (v) temperatura.

Os protocolos baseados em agrupamentos tentam juntar os nós da rede em agrupamentos diferentes e atribuir a um dos nós a função de cabeça de agrupamento (*cluster head*). Esse nó tem a missão de encaminhar dados dos sensores de seu agrupamento, para o nó coletor (*sink*) ou estação base. Essa transmissão pode ser direta desde o nó cabeça de agrupamento até o coletor ou através de outros nós cabeça de agrupamento. Esses protocolos visam minimizar o número de transmissões diretas de nós sensores para o nó coletor. No entanto, a sobrecarga de número de saltos e atrasos exigidos para a seleção de agrupamentos são as principais desvantagens desses protocolos. Já os protocolos baseados em qualidade de serviço fornecem módulos separados para diferentes métricas de qualidade de serviço (*Quality of Service* - QoS) que operam de maneira coordenada. Assim, eles podem oferecer maior confiabilidade, menor latência fim-a-fim e maior taxa de entrega de pacotes do que protocolos comuns, a depender da métrica utilizada. Esses protocolos sofrem principalmente com a alta complexidade devido aos vários módulos que operam simultaneamente e às diferentes métricas de *Quality of Service* (QoS) que possuem.

Os protocolos de camada cruzada abordam os desafios das camadas de rede e de controle de acesso ao meio (*Media Access Control* - MAC), ao mesmo tempo para melhorar o desempenho geral da rede WBAN. Embora esses protocolos tenham alta produtividade, baixo consumo de energia e um atraso fim-a-fim relativamente fixo, eles não podem fornecer alto desempenho em casos de movimento do corpo, devido às perdas de caminho associadas aos tecidos do corpo humano em alguns cenários [17, 19]. Já para os protocolos baseados em movimentos corporais, as características de WBANs, como a baixa potência de transmissão para evitar o aquecimento dos tecidos e poupar energia, unidas aos movimentos do corpo humano, criam um cenário onde podem acontecer perdas dos enlaces e mudanças na topologia da rede. Os protocolos baseados nos movimentos corporais tentam enfrentar esse problema de particionamento topológico ou desconexão dos enlaces, causados pelo movimento corporal [20]. Por fim, os protocolos baseados na temperatura são projetados com o objetivo principal de minimizar o aumento da temperatura local ou geral do sistema. De fato, a ideia subjacente a esses protocolos é rotear dados em diferentes rotas para evitar um aumento acentuado da temperatura em alguns nós, os quais podem causar danos aos tecidos humanos [21].

As classificações anteriores são baseadas na comunicação intra-WBAN. Contudo, para comunicação inter-WBAN, os algoritmos de roteamento baseados em agrupamentos, em qualidade de serviço e em camadas cruzadas são mais adequados que os protocolos baseado em movimentos corporais e temperatura, pois os algoritmos desses dois tipos de protocolo dependem da posição dos sensores no corpo e da temperatura de cada sensor corporal, respectivamente. Para a comunicação inter-WBAN, geralmente emprega-se um único sensor corporal, portanto, não há posição relativa em relação a sensores no mesmo corpo nem parâmetros de comparação de temperatura.

Protocolos de MANETs aplicados a WBANs

As redes corporais surgiram para atuar de maneira autônoma, com nós sensores de pequenas dimensões e limitados em processamento. Do ponto de vista do roteamento, pode-se considerar que uma WBAN é uma rede *ad-hoc* móvel de pequena dimensão. Contudo, alguns trabalhos afirmam que, conceitualmente, devido às restrições de uma WBAN, como a restrição de energia e heterogeneidade dos dispositivos com requisitos rigorosos de tempo real, protocolos de roteamento desenvolvidos para redes *ad-hoc* comuns não poderiam atender a WBANs [22, 17]. Por isso, as pesquisas relativas aos protocolos de roteamento para WBAN têm sido focadas primariamente no desenvolvimento de novos protocolos para enfrentar algum dos desafios definidos para WBAN, sem considerar os protocolos já desenvolvidos para redes *ad-hoc*.

Por outro lado, outros trabalhos [23, 24] provam por meio de avaliações de desempenho que é possível a utilização de protocolos já existentes para MANETs em redes corporais. Normalmente, o estudo do roteamento em WBANs é focado para a comunicação intra-WBAN. Contudo, para a comunicação inter-WBAN, na qual se utilizam dispositivos com capacidade de processamento menos restrita, a limitação é menor e não impossibilita o roteamento dessas redes por meio de protocolos tradicionais de redes *ad-hoc* móveis. A vantagem de utilizar esses protocolos como base é que eles são projetados para oferecerem alto desempenho em redes com mobilidade sem a necessidade de heurísticas complexas.

2.3 Protocolos de roteamento tradicionais em MANETs

Os protocolos de roteamento para MANETs podem ser classificados quanto ao modo de operação em dois tipos, os protocolos proativos e os reativos. Os proativos são os protocolos nos quais os nós registram rotas para alcançar todos os nós da rede, mesmo que

possuam interesse de comunicação com apenas um subconjunto desses nós. Para manter as tabelas atualizadas, os nós trocam informações periódicas entre si com informações que permitem obter as rotas para cada nó. A principal vantagem dos protocolos proativos é ter as rotas disponíveis quando um nó deseja se comunicar. A principal desvantagem é a sobrecarga de mensagens de controle necessárias para manter as rotas atualizadas. Essa sobrecarga de mensagens causa maior processamento nos nós e uso excessivo de banda passante. Diferentemente dos protocolos proativos, os reativos descobrem as rotas sob demanda, isto é, um nó transmissor descobre uma rota para o destino apenas no momento em que deseja se comunicar. Assim, os protocolos reativos possuem baixa sobrecarga de mensagens de controle, contudo, a latência fim-a-fim é acrescida do tempo de descoberta de rota. Dentre os protocolos de roteamento tradicionais desenvolvidos para atender às MANETs, destacam-se: DSDV, *Dynamic Source Routing* (DSR), AODV, e OLSR.

O DSDV [25] é um protocolo de roteamento proativo baseado em vetor de distância. O algoritmo do DSDV é baseado no algoritmo distribuído de Bellman-Ford, que, após convergir, permite alcançar os nós pelo caminho de menor custo. A métrica de custo usada é o de número de saltos até o destino. Os pacotes são transmitidos entre os nós da rede usando tabelas de roteamento que são armazenadas em cada nó. Cada tabela de roteamento lista todos os destinos disponíveis e o número de saltos para cada um. Cada entrada de rota é marcada com um número de sequência que é originado pelo nó de destino. Quando um nó recebe alguma atualização, ele a envia a todos os seus vizinhos. Essas mensagens de atualização são enviadas com frequência para permitir a atualização da topologia constantemente. No entanto, a elevada frequência no envio de mensagens aumenta o consumo de energia e de processamento dos nós. Para eliminar os laços (*loops*) de roteamento, cada atualização de nó é marcada com um número de sequência. O número de sequência inicial para cada nó é escolhido aleatoriamente, mas deve ser incrementado sempre que ocorrer uma atualização periódica.

O DSR [26, 27] é um protocolo de roteamento reativo e iniciado na fonte, projetado especificamente para uso em MANETs com múltiplos saltos. O protocolo consiste em dois mecanismos: *descoberta de rota* e *manutenção de rota*, que operam juntos para permitir que os nós descubram e mantenham rotas da origem para seus destinos. O processo de *descoberta de rota* busca e decide o melhor caminho entre a origem e o destino. Com o processo de *manutenção da rota*, é garantido que o melhor caminho permanece uma escolha possível e permanece sem laços, mesmo que o caminho mude durante a transmissão. A descoberta e a manutenção de rotas operam inteiramente sob demanda. O processo de descoberta de rota é iniciado quando um nó deseja transmitir dados a um nó de des-

tino desconhecido. Uma mensagem *Route Request* (RREQ) é enviada a seus vizinhos em modo de difusão com limitação de 1 salto. Cada mensagem RREQ possui informação sobre a origem, o destino e a identificação da solicitação (`request id`) determinada pelo originador da mensagem. Cada RREQ também contém um registro que lista o endereço de cada nó intermediário através do qual uma cópia particular da mensagem RREQ foi encaminhada. Esse registro de rota é inicializado em uma lista vazia pelo originador da descoberta de rota. Os nós intermediários encaminham a mensagem para seus vizinhos, acrescentando o próprio endereço na lista de registros. Caso a mesma mensagem seja recebida novamente, o nó poderá identificar através do `request id`, e descarta a mensagem. Quando o destino recebe a mensagem RREQ, ele retorna uma mensagem *Route Reply* (RREP) ao iniciador do processo de descoberta de rota, com a cópia do registro de rota acumulado da mensagem RREQ. Ao receber a RREP, o nó de origem registra uma rota na sua *cache* de rotas para envio das mensagens subsequentes. Cada nó associa um temporizador à rota encontrada. Caso a rota fique ociosa por determinado período de tempo, ela é excluída da tabela de roteamento. O processo de manutenção de rotas é iniciado caso haja falha em algum enlace da rede. O nó que detecta a falha encaminha uma mensagem *Route Error* (RERR) para o nó de origem. Os nós intermediários e o nó de origem excluem as rotas que utilizam aquele enlace e um novo processo de descoberta de rota é iniciado pelo nó de origem.

O DSR não requer pacotes periódicos em nenhum nível da rede. Por exemplo, o DSR não usa nenhum anúncio de rotas periódico, detecção de estado do enlace ou pacotes de detecção de proximidade, e não depende de nenhum protocolo de rede subjacente. À medida que os nós estão se movendo mais ou que os padrões de comunicação mudam, a sobrecarga dos pacotes de roteamento do DSR é automaticamente dimensionada para o que é necessário para rastrear as rotas atualmente em uso [28]. O DSR possui, ainda uma função de “escuta promíscua” que permite aos nós intermediários receber e processar as mensagens que não são destinados a eles. Com essas mensagens, os nós conseguem atualizar as rotas armazenadas com a informação recebida mesmo sem ser o destino da mensagem.

O AODV [29] é um protocolo reativo que atua sob demanda, tendo suas rotas calculadas apenas quando necessário. O AODV responde rapidamente às mudanças topológicas que afetam as rotas ativas, sendo adequado para redes dinâmicas [30]. Possui suporte para transmissão de pacotes *multicast* e *unicast*, mesmo para nós em movimento constante. O AODV funciona principalmente em duas fases: descoberta de rotas e manutenção de rotas. Na primeira fase, o AODV usa um mecanismo de descoberta de rota semelhante ao

usado no DSR, com algumas modificações. No entanto, em vez do roteamento baseado na origem, o AODV depende do estabelecimento dinâmico de entradas da tabela de rotas em nós intermediários. Essa diferença compensa o uso em redes densas, nas quais há uma carga maior no transporte das rotas de origem em cada pacote de dados [30]. Na segunda fase, os nós disponíveis enviam uma resposta sobre o seu estado de disponibilidade para o nó solicitado e, em seguida, o nó solicitado envia os dados para o nó vizinho. Mensagens de erro são enviadas quando a rota falha ou ocorre um erro durante a transmissão. Em contraste com o DSR, as mensagens de erro no AODV informam todos os nós que usam o enlace quando a falha ocorre [31]. Semelhante ao DSDV, o AODV usa um campo de número de sequência para evitar laços de roteamento. No entanto, cada nó na rede mantém um contador de número de sequência crescente, usado para substituir rotas em cache antigas. A combinação das técnicas gera um algoritmo que usa largura de banda de forma eficiente, minimizando a carga da rede para controle e tráfego de dados, responde às mudanças na topologia e garante um roteamento sem laços. O AODV-v2¹ é a segunda versão do AODV [32]. A principal modificação do AODV-v2 é permitir que cada nó intermediário na rota entre a origem e o destino armazene a rota para todos os nós predecessores, diminuindo assim a sobrecarga de roteamento.

O OLSR [33] é um protocolo de roteamento proativo, otimizado a partir de um protocolo de estado de enlace de redes cabeadas. O OLSR compacta o tamanho da informação enviada nas mensagens e reduz o número de retransmissões. Para reduzir o número de retransmissões, o protocolo usa a técnica de retransmissão multiponto (*MultiPoint Relay* - MPR) para inundar de forma eficiente e econômica suas mensagens de controle. O objetivo é fornecer as melhores rotas em termos de número de saltos, e que essas rotas estejam disponíveis imediatamente quando necessário. O OLSR mantém suas rotas atualizadas usando mensagens periódicas trocadas entre nós vizinhos sobre informações da rede. A mensagem *Hello* é utilizada para descobrir os vizinhos até 2 saltos de distância. A partir das informações de vizinhança é que os nós *MultiPoint Relay* (MPR) são determinados para cada transmissor. As mensagens *Topology Control* são difundidas pela rede e enviadas periodicamente pelos nós, contudo, apenas os nós MPR encaminham essas mensagens, reduzindo o número de retransmissões na rede e evitando a inundação. Existe um atraso inicial para convergência do protocolo, uma vez que primeiramente é necessário estabelecer os nós MPR e disseminar toda a topologia da rede entre os nós.

O protocolo OLSR é mais adequado para MANETs grandes e densas [34]. Sua principal desvantagem é a necessidade de envio de mensagens periódicas, o que aumenta a

¹AODV-v2 inicialmente foi chamado de DYMO.

quantidade de mensagens de controle, o uso do processamento e, conseqüentemente, o consumo de energia. A versão 2 do OLSR [35] retém os mesmos mecanismos e algoritmos básicos, aprimorados pela capacidade de usar uma métrica de enlace diferente da contagem de saltos na seleção das rotas mais curtas. O OLSRv2 também usa uma estrutura de sinalização mais flexível e eficiente e inclui algumas simplificações das mensagens que estão sendo trocadas.

Estudos comparativos [31, 36] realizados para verificar o desempenho dos protocolos tradicionais de MANETs mostram que nos cenários de mobilidade, os protocolos proativos possuem menor latência e os protocolos reativos conseguem maior taxa de entrega de pacotes. Outros trabalhos realizados com foco em aplicações para WBANs [23, 24] mostram que o protocolo AODV se destaca em termos de resultados de desempenho. A proposta deste trabalho tem o AODV como base de desenvolvimento e, portanto, há maior detalhamento sobre os principais processos do AODV na seção seguinte. A ideia é prover uma base teórica para elucidar o funcionamento do AODV e melhorar a compreensão do protocolo proposto MT-AODV.

2.3.1 *Ad-hoc On Demand Distance Vector (AODV)*

Os principais processos existentes no protocolo AODV são a descoberta de rotas e a manutenção de rotas.

Processo de descoberta de rota

O AODV é um protocolo sob demanda e, por isso, a descoberta de uma rota para o destino é iniciada somente quando necessário. Por exemplo, se um nó transmissor S deseja se comunicar com o nó coletor Z , e não possui uma rota disponível em sua tabela de roteamento, S envia uma mensagem RREQ em modo de difusão para seus vizinhos. A Figura 2.3 ilustra o formato da mensagem RREQ enviada.

O campo *Tipo* especifica o tipo de mensagem como sendo RREQ, esse campo é preenchido com 1. O campo de *Flags* indica o uso da mensagem da seguinte forma: *Join (J)* e *Repair (R)* são reservadas para o modo de multidifusão (*multicast*); *Gratuitous RREP (G)* indica que a mensagem pode ser respondida por nó intermediário; *Destination only (D)* indica que somente o destino deve responder à mensagem; e *Unkown Sequence Number (U)* indica que o número de seqüência do destino é desconhecido. O campo *Reservado* é enviado como 0 e é reservado para uso futuro. O campo *Número de saltos* indica a

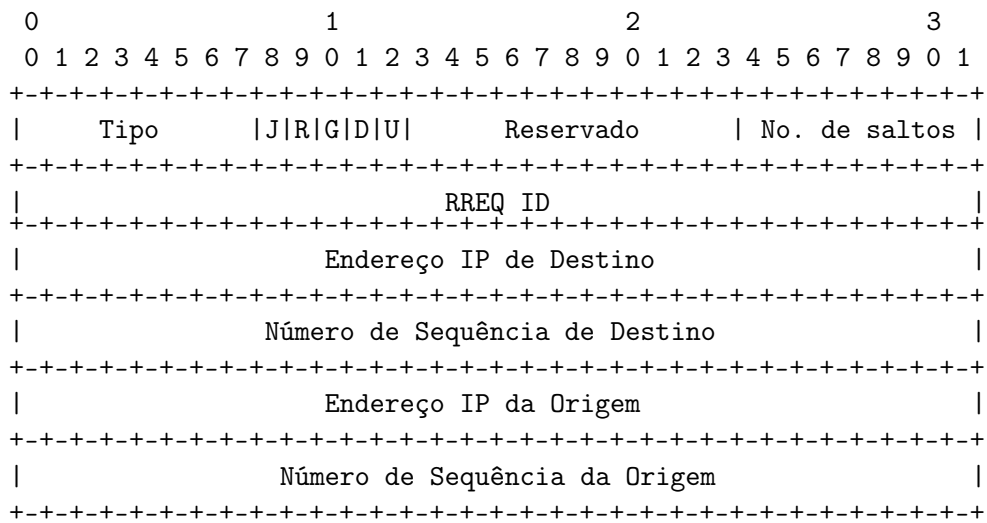


Figura 2.3: Formato da Mensagem RREQ. Adaptado da RFC 3561 [29].

quantidade de saltos do nó de destino até o receptor da mensagem. Caso a mensagem seja encaminhada, o número de saltos é incrementado de 1 pelo nó intermediário. O campo *Identificador de Broadcast (RREQ ID)* é um contador local mantido por cada nó e incrementado sempre que uma nova mensagem RREQ é transmitida [37]. O *Endereço IP da Origem* é preenchido com o endereço IP da origem da mensagem, isto é, o nó originador da requisição. Esse campo, juntamente com o RREQ ID identificam de forma exclusiva uma mensagem RREQ. O *Número de Sequência da Origem* é usado para manter as informações mais recentes do caminho reverso para a origem e o *Número de Sequência de Destino* especifica o quão recente uma rota deve estar antes de ser aceita pela origem. O campo *Endereço IP de Destino* indica o endereço do nó com o qual o nó de origem deseja se comunicar. Essa mensagem é propagada até uma determinada quantidade de saltos.

A mensagem RREQ é respondida por um nó intermediário I que possui uma rota até o nó coletor, caso o campo G esteja habilitado, ou pelo próprio nó coletor Z . A resposta é devolvida por meio de uma mensagem RREP, em modo *unicast*, pelo caminho reverso até a origem. A Figura 2.4 apresenta o formato da mensagem RREP.

No campo *Tipo* do RREP é atribuído valor 2. O campo de *Flags* pode indicar *Repair (R)*, usado para multidifusão, e se a mensagem exige reconhecimento o *flag Acknowledgment required (A)* é ativado. O campo *Reservado* é enviado com valor 0 e é reservado para uso futuro. O campo *Prefixo* especifica que o próximo salto indicado pode ser usado para quaisquer nós com o mesmo prefixo de roteamento. O campo *Número de Saltos* indica a quantidade de saltos da origem até o destino. O *Endereço IP de Destino* identifica o destinatário da mensagem. O *Número de Sequência de Destino* serve para indicar o quão recente uma rota deve estar antes de ser aceita pela origem. O *endereço IP da Origem*

2.4 Roteamento multicaminhos em MANETs

Os protocolos de roteamento tradicionais de MANETs buscam o melhor caminho entre cada par de nós e transmitem os dados através de um único caminho entre esses nós. Contudo, devido à natureza dinâmica e imprevisível das MANETs, a utilização de múltiplos caminhos é útil nessas redes [38]. Isso porque é comum a ocorrência de falhas nas rotas, devido à complexidade da propagação do sinal no ambiente sem fio. Essa complexidade é resultante dos diversos mecanismos de propagação que afetam o sinal, da existência de obstáculos no ambiente e da constante movimentação dos nós. Assim, torna-se atrativo o uso de protocolos de roteamento que apresentem maior tolerância a falhas.

O roteamento por múltiplos caminhos pode beneficiar aplicações em MANETs implantadas em ambientes de operação militar [39], melhorando a (i) tolerância a falhas, promovendo o (ii) balanceamento de carga e a (iii) agregação de largura de banda, ou (iv) reduzindo a latência. (i) Os protocolos de roteamento por múltiplos caminhos podem fornecer tolerância a falhas por possibilitar que informações redundantes sejam roteadas para o destino por caminhos alternativos. Assim, se reduz a probabilidade de interrupção da comunicação em caso de quebra de enlace. Algoritmos sofisticados empregam codificação de origem [40] para reduzir a sobrecarga de tráfego causada quando há elevada redundância, enquanto mantém o mesmo grau de confiabilidade. Esse aumento da resiliência de rota depende muito de métricas como a disjunção dos caminhos disponíveis. (ii) Os protocolos de roteamento por múltiplos caminhos podem escolher desviar o tráfego por caminhos alternativos para aliviar a carga do enlace congestionado quando esse enlace recebe mensagens em excesso. Também é possível considerar a carga de cada nó para tomada de decisão do roteamento. (iii) Ao dividir os dados para o mesmo destino em vários fluxos, cada pacote é roteado por meio de um caminho diferente, e a largura de banda efetiva pode ser agregada. Essa estratégia é particularmente benéfica quando um nó tem vários enlaces com pequena largura de banda, mas requer uma largura de banda maior do que aquela que um enlace individual pode fornecer. (iv) A latência fim-a-fim também pode ser reduzida como resultado direto de uma largura de banda maior. Além disso, para redes sem fio que empregam protocolos de roteamento sob demanda com caminho único, uma falha de rota significa que um novo processo de descoberta de caminho precisa ser iniciado para encontrar uma nova rota. Isso resulta em um atraso na descoberta da rota. Esse atraso pode ser minimizado pelo roteamento por múltiplos caminhos, uma vez que o nó já possui rota alternativa disponível. Dessa forma, a utilização de múltiplos cami-

nhos em redes sem fio tende a melhorar a resiliência e a vazão da comunicação, afetando também positivamente a latência na entrega de pacotes.

Pode-se dividir o roteamento por múltiplos caminhos em três rotinas básicas: descoberta de rotas, distribuição de tráfego e manutenção de rotas. Na **descoberta de rotas**, as rotas para os destinos são encontradas. Frequentemente, ocorre a interrupção de uma rota por falha de nó ou devido à quebra de um enlace nas MANETs. A **manutenção de rotas** é o processo que regenera rotas após a descoberta inicial da rota. Esse processo pode ser iniciado após cada falha de rota ou quando todas as rotas falharem. O processo para encontrar e estabelecer rotas para o tráfego de dados em roteamento por múltiplos caminhos é similar aos algoritmos de caminho único. Todavia, deve-se estabelecer critérios para alocação de rota em vez de substituição na tabela de roteamento. Dessa forma, é necessário armazenar os diferentes caminhos aprendidos no processo. O critério mais comumente usado para a alocação de caminhos é por meio da disjunção de caminhos, que classifica a independência de caminhos em termos de recursos compartilhados. Existem três tipos principais de disjunção de caminho, estabelecidos de acordo com os elementos da rede: caminhos disjuntos em enlaces, caminhos disjuntos em nós e caminhos não-disjuntos. Caminhos disjuntos em enlaces é o conjunto de caminhos que não possuem enlaces comuns, mas podem compartilhar os mesmos nós intermediários. De forma análoga, caminhos disjuntos em nós não possuem nós intermediários comuns, e portanto, também não compartilham do mesmo enlace. Já os caminhos não-disjuntos, podem ter enlaces e nós em comum. Desde que estejam disponíveis, os caminhos disjuntos em nós são geralmente preferidos porque utilizam os recursos de rede mais disponíveis e, portanto, considerar esses caminhos no projeto de protocolos e de redes aumenta a tolerância a falhas. Em princípio, quando um nó intermediário em um caminho disjunto em nós falha, apenas o caminho que contém o nó com falha é afetado, portanto, há um impacto mínimo na diversidade das rotas. Uma quebra de enlace só derruba um dos vários caminhos, sejam eles disjuntos em enlaces ou em nós. No entanto, uma falha de nó pode desativar vários enlaces e interromper vários caminhos de enlaces separados. Os caminhos não disjuntos oferecem o menor grau de tolerância a falhas, pois a falha do nó ou do enlace pode afetar vários caminhos. Nem sempre é possível encontrar caminhos disjuntos, especialmente quando a escolha dos caminhos é limitada pela topologia da rede. Nesse cenário, os protocolos costumam usar a noção de desconexão máxima para minimizar a probabilidade de uma falha de enlace ou nó afetar vários caminhos. Em redes sem fio, devido ao impacto significativo no desempenho do uso de vários saltos, os caminhos disjuntos em nós podem não ser a melhor solução se os caminhos consistirem em muitos

saltos. Essa compensação entre disponibilidade e desempenho deve ser considerada ao projetar protocolos de caminhos múltiplos para redes sem fio de vários saltos.

Existem várias estratégias de alocação para **distribuição de tráfego** entre as rotas disponíveis. Um protocolo de múltiplas rotas pode decidir encaminhar o tráfego usando apenas a rota com a melhor métrica e manter outras rotas descobertas como *backup*, ou as rotas podem ser usadas simultaneamente. As mensagens podem ser enviadas com ou sem redundância. O algoritmo de seleção de rota é usado para escolher um subconjunto de rotas disponíveis de acordo com a qualidade das rotas. A contagem de saltos tem sido a métrica mais comum para computar o custo de uma rota. Outras opções são a confiabilidade da rota, a disjunção de rotas, a largura de banda disponível, o grau de acoplamento de rota ou uma combinação dessas e de outras métricas. O acoplamento de rota pode ser causado por interferência de rádio ou contenção entre caminhos. Esse acoplamento pode impactar no desempenho de protocolos de roteamento por múltiplos caminhos [41], mesmo que os caminhos sejam topologicamente disjuntos. Em uma rota de rede cabeada, o acoplamento é medido pela disjunção do caminho, mas em uma rede sem fio as rotas também são consideradas fortemente acopladas se a transmissão em uma rota impedir diretamente a qualidade da outra. O acoplamento de rota pode ser aliviado fazendo alterações nas camadas físicas e de enlace, como o uso de canais múltiplos [42] ou antenas direcionais [43].

O número de caminhos e a granularidade da alocação dos dados são fatores de grande influência para a estratégia de distribuição de tráfego em protocolos de roteamento por múltiplos caminhos. Em relação ao número de caminhos, a quantidade de rotas pode ser limitada pelo protocolo para que se reduza o processamento e registros de informações pelos dispositivos. Se várias rotas forem usadas simultaneamente para transportar o tráfego, o protocolo precisa decidir como o tráfego é dividido entre as rotas e como lidar com os pacotes fora de ordem no destino. Também é possível adicionar um grau de redundância ao distribuir o tráfego por várias rotas. No entanto, o envio de mensagens redundantes causa sobrecarga de mensagens na rede. Bart et al. [44] descrevem um esquema de codificação de diversidade M-para-N. Nesse esquema de codificação, M linhas de transmissão extras são usadas para aumentar a redundância de um sistema de N linhas de transmissão. O tráfego nas $M + N$ linhas de transmissão é codificado de forma que o sistema possa tolerar menos de M falhas de linha simultâneas a qualquer momento. Essa ideia é estendida para o roteamento por múltiplas rotas em redes de pacotes por Tsirigos et al. [45]. Quanto à granularidade de alocação, algumas opções possíveis incluem: por par origem-destino, por fluxo, por pacote e por segmento. Quanto mais fina a granularidade,

mais preciso pode ser o balanceamento de carga, uma vez que a flutuação de tráfego pode ser adaptada rapidamente [46]. No entanto, a granularidade por pacote, ou ainda mais fina, exige reordenamento dos pacotes recebidos no destino, o que pode não ser adequado para algumas aplicações.

Os benefícios do roteamento por múltiplos caminhos em relação à tolerância a falhas e à redução do atraso são decorrentes da identificação de rotas alternativas durante a fase de descoberta de rotas. Ao ocorrer falha na rota principal, um protocolo de roteamento de caminho único deverá primeiramente computar uma nova rota antes de encaminhar novos dados. No protocolo de roteamento por múltiplas rotas, apenas a fração dos dados transmitidos pela rota principal é perdida e novos dados são automaticamente redirecionados para a rota alternativa ativa, sem a necessidade de computar novas rotas. Dessa forma, não há necessidade de buscar por uma rota quando ocorre falha na rota principal, o que reduz o atraso fim-a-fim. Contudo, comparado ao uso de uma rota única ativa e sem falha, o uso simultâneo de múltiplas rotas pode elevar o tempo para recebimento de todos os pacotes de um fluxo, uma vez que nem todos os caminhos usados são os de menor latência.

Capítulo 3

Protocolos de Roteamento Sem Fio com Múltiplos Caminhos

Em uma MANET não existe uma relação de dependência com nenhum controle central [47], as estações comunicam-se diretamente entre si. Devido à mobilidade, dois nós podem estar próximos e serem vizinhos um do outro em um instante e no momento seguinte estarem distantes e precisarem se comunicar através de nós intermediários. A função de um protocolo de roteamento é encontrar, estabelecer e manter rotas entre dois nós que desejam se comunicar. A obtenção e a manutenção dos endereços, por onde e através de quais nós uma origem consegue transmitir dados para um determinado destino, é uma das questões chaves do bom funcionamento das MANETs [48]. Este capítulo discute os trabalhos relacionados que focam no desenvolvimento de métodos de obtenção e manutenção de rotas baseados em protocolos de roteamento tradicionais de MANETs. Além disso, são apresentados protocolos de roteamento multicaminhos desenvolvidos especificamente para WBANs.

3.1 Protocolos de roteamento multicaminho em MANETs

Diversos protocolos para MANETs que utilizam múltiplos caminhos surgiram com base nos protocolos tradicionais discutidos na Seção 2.3. É relevante destacar que, em MANETs nas quais existe comunicação através de múltiplos saltos, a mobilidade é o principal fator que influencia negativamente a qualidade da comunicação. Devido à falta de infraestrutura fixa implantada, não há possibilidade de *handover*, nem de gerenciamento centralizado na rede quando os nós se movem. Portanto, a convergência da rede depende

exclusivamente dos próprios nós e de seus protocolos de roteamento.

3.1.1 Protocolos baseados no DSR

Nasipuri e Das [49] propõem um protocolo multicaminho como extensão do DSR. A principal motivação do trabalho é reduzir e controlar de forma eficiente a frequência de inundações das mensagens de descoberta de rota, uma vez que essas tarefas intrínsecas de protocolos reativos ocupam uma fração significativa de largura de banda disponível na rede. O artigo apresenta duas versões ligeiramente diferentes de extensão ao DSR para caminhos múltiplos e um modelo analítico para avaliar a qualidade de protocolos sob demanda.

Na primeira variação proposta, o destino responde apenas a um conjunto selecionado de consultas. Muitas cópias da mensagem de consulta inundada chegam ao destino por meio de rotas diferentes. As consultas que são respondidas são aquelas que carregam uma rota de origem que é disjunta em enlace da rota primária. A rota de origem primária é a rota percorrida pela primeira consulta que chega ao destino. Isso geralmente define a rota de menor custo entre a origem e o destino. O destino usa o registro da rota primária, a fim de descobrir a quais solicitações posteriores responder. Apenas rotas disjuntas em enlaces são escolhidas, pois uma falha de enlace em uma rota não afeta as outras. Isso também controla implicitamente o número total de respostas, evitando assim uma inundação de respostas. A origem mantém todas as rotas recebidas nos pacotes de resposta em uma *cache* de rotas. Quando a rota principal é interrompida, a rota alternativa mais curta restante é usada. Esse processo continua até que todas as rotas sejam interrompidas, quando uma nova descoberta de rota é iniciada.

O número de rotas alternativas usadas pode ser um parâmetro selecionável do protocolo. Apenas o nó de origem registra as rotas alternativas. Um nó intermediário da rota primária ainda envia um pacote de erro de volta ao nó de origem, caso haja uma quebra de enlace, e o nó de origem então usará uma rota alternativa. Isso causa uma perda temporária de rota para os pacotes de dados que já estão em trânsito no caminho do enlace com falha. Para evitar isso, uma segunda variação da extensão é explorada. Nessa segunda variação, todos os nós intermediários registram uma rota alternativa disjunta para que os pacotes de dados em trânsito não enfrentem mais nenhuma perda de rota. Para que isso seja possível, o destino passa a responder a cada nó intermediário na rota primária com uma rota disjunta alternativa para o destino. Dessa forma, qualquer resposta desse tipo é uma resposta a uma consulta do nó de origem que passou por aquele

nó intermediário. A resposta é direcionada ao nó intermediário em vez da origem.

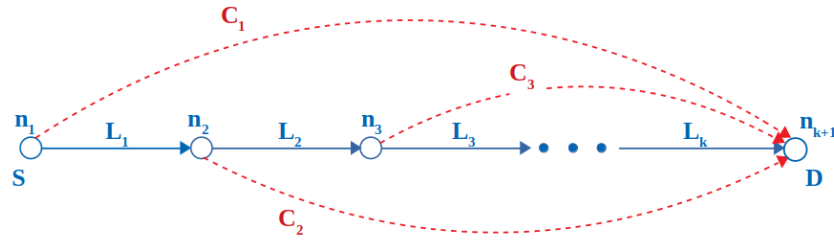


Figura 3.1: Manutenção de rotas alternativas na proposta de Nasipuri e Das. A rota primária consiste em L_1, L_2, \dots, L_k . Cada nó na rota primária n_i , tem um caminho alternativo C_i para o destino. Adaptado [49].

A Figura 3.1 ilustra como as rotas são mantidas. Nem sempre é possível para todos os nós intermediários obter uma rota disjunta alternativa, porque pode não haver caminho disjunto ao primário. Portanto, isso ainda pode resultar em perda temporária de rotas em caso de falhas de enlace até que um nó de origem alterne para uma rota alternativa. O nó de origem S usa a rota primária para transmitir pacotes de dados para D até que a rota seja interrompida em algum ponto, por exemplo L_i . Quando o enlace L_i é quebrado, o nó n_i responde à situação substituindo a parte não utilizada da rota, $L_i - L_k$, no cabeçalho do pacote de dados pela rota alternativa C_i . Isso continua até que um enlace em C_i seja interrompido, provocando a transmissão de um pacote de erro de volta para o nó n_{i-1} . Esse nó descarta o pacote de erro e encaminha todos os pacotes de dados posteriores para sua própria rota alternativa C_{i-1} modificando a rota de origem no cabeçalho do pacote como era anteriormente.

Split Multipath Routing (SMR) [50] também é um protocolo multicaminhos baseado no DSR. Em vez de manter caminhos múltiplos como rotas *backup*, o SMR utiliza caminhos múltiplos simultaneamente, dividindo o tráfego em no máximo duas rotas disjuntas. Quando uma das rotas falha, independentemente do destino, cada entrada na tabela de roteamento da origem que compartilha nós intermediários comuns com a rota com falha é removida. O SMR pode adotar duas políticas distintas para recuperação de rota. Na primeira, o processo de recuperação de rota é iniciado caso uma das rotas apresente falha. A segunda política inicia a recuperação somente quando ambas as rotas apresentem falha. Os autores mostram por meio de simulação que o SMR supera o DSR em termos de latência e entrega de pacotes em uma MANET.

3.1.2 Protocolos baseados no AODV

O protocolo *Ad-hoc On-demand Multipath Distance Vector* (AOMDV) [51] é proposto com o objetivo de fornecer maior tolerância a falhas, no sentido de recuperação de rotas mais rápida e eficiente em redes dinâmicas. Para isso, o AOMDV calcula múltiplos caminhos livre de laços (*loops*) e disjuntos em enlace (*link-disjoint*). A tabela de roteamento do AOMDV usa uma lista de rotas disjuntas em enlaces na sua tabela de roteamento, contendo o endereço do próximo salto e o número de saltos. O AOMDV mantém as rotas apenas para o número de sequência de destino mais alto conhecido. Para manter vários caminhos para o mesmo número de sequência, o AOMDV usa o conceito de contagem de saltos anunciada (*advertised hop count*). Cada nó mantém uma variável chamada contagem de saltos anunciada para cada destino. Essa variável é definida para o tamanho do caminho mais longo disponível para o destino no momento do primeiro anúncio para um número de sequência de destino específico. Conseqüentemente, a contagem de saltos permanece inalterada até que um caminho para um número de sequência de destino mais alto seja recebido. Desde que um nó nunca divulgue uma rota mais curta do que uma já anunciada, e nunca aceite uma rota mais longa do que uma já anunciada, o algoritmo é livre de laços.

No AOMDV, não é realizada distribuição do tráfego de dados por suas rotas. A troca de uma rota é realizada apenas quando a rota principal se torna indisponível. Para garantir que as rotas da tabela de roteamento sejam disjuntos em enlaces, um nó descarta um anúncio de rota que tem um próximo salto comum ou um último salto comum com um já registrado na tabela de rota. Dessa forma, desde que cada nó cumpra esta regra, todos os caminhos para o mesmo número de sequência de destino são garantidamente disjuntos em enlaces. Caminhos disjuntos em nós podem ser obtidos com uma restrição adicional da seguinte forma: se nós comuns em um conjunto de caminhos disjuntos de enlace impedem que nós de origem tenham mais de um caminho através deles, então obtém-se caminhos disjuntos em nós. Isso pode ser alcançado estipulando que, para um determinado número de sequência de destino, cada nó sempre anuncia um único caminho designado para outros nós. A manutenção da rota no AOMDV é semelhante à do AODV. Uma mensagem RERR para um destino é gerada quando o último caminho para esse destino falha.

O *Optimized Ad-hoc On-demand Multipath Distance Vector* (OAOMDV) [52] é uma otimização do AOMDV, desenvolvido para resolver o problema de *route cutoff* do AOMDV. Esse problema ocorre quando há um ou mais nós intermediários comuns em um par de

caminhos disjuntos em enlaces. Quando isso ocorre, o AOMDV não é capaz de encontrar ambos os caminhos reversos. Para evitar o problema de *route cutoff*, os autores propõem um esquema no qual uma mensagem de reconhecimento de resposta de rota *Route Reply Acknowledgement* (RREP-ACK) é adicionada para ser transmitida ao longo do caminho. Assim que um nó intermediário receber o pacote, um caminho reverso para a origem é configurado. Assim, quando o destino recebe o pacote, o caminho reverso omitido é configurado. Quando o nó de origem recebe um RREP, ele determina se o destino omitiu um caminho reverso. Isso é feito através da comparação do campo *ACK* no RREP com o vizinho do qual recebe o RREP. Se eles forem o mesmo nó, significa que nenhum caminho reverso foi omitido. Se eles forem nós diferentes, isso significa que um caminho reverso disjunto em enlace foi omitido. Nesse último caso, o nó de origem transmitirá uma mensagem de controle RREP-ACK ao longo do caminho de encaminhamento configurado por esse RREP para formar um novo caminho reverso. Diferentemente do RREP-ACK no AODV, que é um pacote transmitido a um salto e só é usado para confirmar a recepção de RREP, o RREP-ACK no OAOMDV desempenha um papel adicional. Ele contém o último salto do caminho reverso omitido e o último salto do caminho direto. Ambos são obtidos com a mensagem RREP. O último salto do caminho reverso é usado para compor o caminho reverso disjunto em enlace omitido. O último salto do caminho direto é usado para encontrar um caminho disjunto em enlace ao longo do qual a mensagem RREP-ACK é encaminhada salto a salto e um novo caminho reverso é configurado.

3.1.3 Protocolos baseados no OLSR

O protocolo *Multi-Path Optimized Link State Routing* (MP-OLSR) [53, 54] resulta da alteração do OLSR para o cálculo de múltiplos caminhos entre o nó de origem e o nó de destino. Assim como o OLSR clássico, o MP-OLSR envia as mensagens de controle periodicamente para manter a topologia conhecida da rede sempre atualizada. Todavia, o MP-OLSR não mantém tabela de roteamento todo o tempo. Os caminhos são calculados somente quando um nó precisa enviar pacotes, se tornando um protocolo sob demanda ou reativo. Por isso, MP-OLSR pode ser considerado um tipo de protocolo de roteamento de múltiplos caminhos híbrido que combina os recursos proativos e reativos.

A funcionalidade principal do MP-OLSR tem duas partes: monitoramento da topologia (*topology sensing*) e cálculo de rota (*route computation*). O monitoramento da topologia serve para tornar os nós cientes das informações de topologia da rede. Isso é feito utilizando os MPRs como o OLSR. O cálculo da rota usa o algoritmo de Dijkstra

de caminhos múltiplos para calcular os caminhos baseado nas informações obtidas no monitoramento da topologia. O caminho entre origem e destino contendo todos os saltos intermediários é salvo no cabeçalho dos pacotes de dados. O monitoramento da topologia e o cálculo da rota tornam possível encontrar vários caminhos da origem ao destino. Em teoria, os caminhos gerados pelo algoritmo de Dijkstra no MP-OLSR são livres de laços. Porém, na prática, a situação é mais complexa devido à mudança da topologia e à variabilidade do meio sem fio. Assim, a recuperação de rotas e a detecção de laços também são propostas como funcionalidades auxiliares para melhorar o desempenho do protocolo. A recuperação de rota pode reduzir efetivamente a perda de pacotes e a detecção de laços pode ser usada para evitar a existência de laços na rede.

3.2 Protocolos de roteamento multicaminhos em WBANs

Diversos protocolos foram desenvolvidos para suporte às WBANs [19, 20, 21]. Contudo, devido à pequena quantidade de nós em uma rede intra-WBAN, poucos esquemas focam na utilização de múltiplos caminhos. Os protocolos de roteamento multicaminhos são interessantes para aplicações de monitoramento de saúde por se preocuparem com a resiliência da comunicação em ambientes vulneráveis a falhas e desconexões. Tseng [55] propõe o *Load-Balanced Multipath Routing* (LBMR), um protocolo de roteamento multicaminhos para monitoramento de saúde baseado no tráfego de dados estimado de cada nó. O principal objetivo é evitar gargalos de tráfego na rede. O LBMR é composto por três processos principais: (i) Construção de Roteamento de Camada (*Layer Routing Construction* - LRC), (ii) Algoritmo de Estimativa de Carga (*Load Estimation Algorithm* - LEA) e (iii) Manutenção de Rota (*Route Maintenance* - RM). Existe uma hierarquia de camadas para o roteamento, conforme exemplifica a Figura 3.2. No processo **LRC**, o *gateway* de dados é o nível mais alto das camadas e é definido que os nós mais próximos do *gateway* estão nas camadas superiores, enquanto os nós mais distantes do *gateway* estão nas camadas inferiores. Assim, cada nó sensor pode desempenhar funções de nó de camada inferior e superior, dependendo da distância relativa até o *gateway* em comparação com seus vizinhos. Cada nó da camada inferior precisa saber apenas as informações locais dos nós do próximo salto na camada superior imediata, e o caminho do nó de origem ao *gateway* é construído salto a salto. Esse relacionamento estruturado e indutivo entre duas camadas estabelece o serviço de roteamento confiável. O **Load Estimation Algorithm** (LEA) permite que cada nó da camada inferior calcule qual nó da camada

superior tem a menor carga de tráfego. O nó da camada superior com menos tráfego é selecionado como o próximo salto para o *gateway*. Por meio da cooperação entre *Layer Routing Construction* (LRC) e LEA, a otimização do balanceamento de carga local é realizada.

Na tabela de roteamento do LBMR, vários caminhos são registrados e isso permite agregar resiliência quando o próximo salto falha. Além disso, outra garantia de qualidade de entrega é o mecanismo **Route Maintenance (RM)**. Quando qualquer nó deixa de operar normalmente, o RM permite que os nós da camada inferior recomputem seus melhores nós da camada superior em direção ao *gateway* sem transmitir mensagens de erro de rota. Portanto, o LBMR pode adaptar rapidamente os nós sensores a mudanças dinâmicas de fluxo e mau funcionamento dos enlaces. Os resultados mostram melhor desempenho da taxa de entrega de pacotes em comparação ao AODV e AOMDV. Contudo, o LBMR necessita de um gerenciamento das camadas dos nós da rede, sendo ideal para redes pouco dinâmicas.

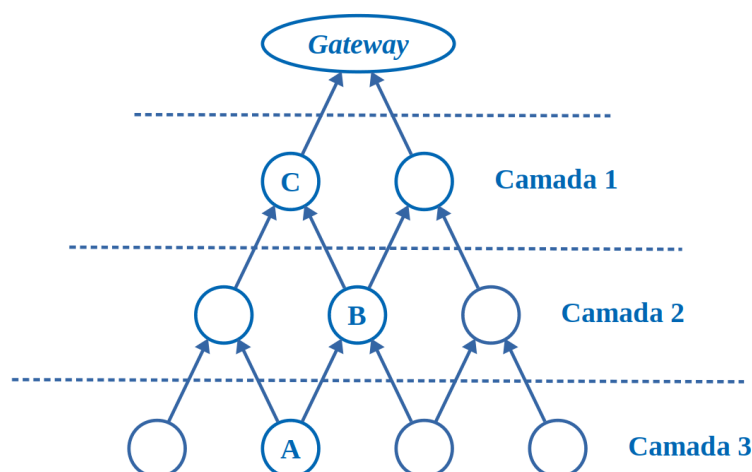


Figura 3.2: Hierarquia de camadas para roteamento no LBMR. O *gateway* de dados é o nível mais alto das camadas, os nós mais próximos do *gateway* estão nas camadas superiores e os mais distantes estão nas camadas inferiores. Adaptado [55].

Birgani *et al.* [56] apresentam o protocolo *Reliable Multi-path Routing* (RMPR) para monitoramento de saúde em pacientes, utilizando a camada física da rede para construção das rotas. O RMPR visa melhorar o procedimento de roteamento e de descoberta de rota, além de descobrir e comunicar vários caminhos entre cada nó e o destino (normalmente nó coletor). Cada nó tenta enviar o máximo de dados por meio de três caminhos até o destino. No RMPR, todos os nós armazenam uma tabela dos RREQs recebidos, com o objetivo de evitar a criação de laços. Assim, em cada tabela as especificações dos RREQs recebidos são registradas por cada nó. Nesse caso, quando um nó intermediário recebe

um RREQ, ele busca suas especificações em sua própria tabela RREQ. Se o pacote for novo, primeiro as especificações são listadas na tabela RREQ, e a seguir envia-se o pacote para os vizinhos. Com essa abordagem, apenas os caminhos disjuntos em nó na origem são descobertos. O nó de destino retorna os pacotes de resposta de rota (RREPs) após receber os RREQs através do caminho reverso de cada RREQ para a origem. O RMPR utiliza a potência do sinal para cálculo das rotas. Calcula-se um Fator de Energia (*Strength Factor* - SF) subtraindo da potência do sinal recebido a potência mínima aceitável, e depois divide-se pela potência do sinal recebido. A Figura 3.3 mostra um exemplo de cálculo para descoberta das rotas a partir do nó de origem S . O nó S envia uma mensagem RREQ para seus vizinhos, A , B e C , usando um método de inundação. Cada um desses três nós verifica primeiro a tabela RREQ para verificar se o pacote é repetido. Em seguida, eles calculam o *Strength Factor* (SF). Por exemplo, o nó de origem S inicializa o campo SF com o número 1 e encaminha a mensagem RREQ. O nó A calcula o SF do pacote que é 0,8, assim que recebe o pacote RREQ e multiplica o SF que está presente no pacote. Assim, o nó A atualiza o SF no campo. O processo continua até que o pacote de solicitação alcance o destino, que é o nó D . Por fim, o SF do caminho S-A-D é calculado como 0,56, pois o SF calculado por D é 0,7 e o campo está marcado com 0,8. Para os outros dois caminhos descobertos S-B-D e S-C-D, o SF é calculado da mesma maneira. O objetivo final é melhorar os parâmetros de atraso e a taxa de perda de pacotes com a utilização das rotas de maior potência recebida, de forma que o custo de sobrecarga de controle seja compensado. O nó de origem sempre tenta enviar seus dados ao destino por meio de duas rotas simultaneamente. Para isso, distribui os pacotes de transmissão de forma alternada entre duas rotas. Os resultados mostram melhor desempenho de entrega de pacotes em troca de acréscimo na quantidade de mensagens de controle.

3.3 Diferencial do MT-AODV

Assim como os protocolos descritos neste capítulo, o MT-AODV visa descobrir múltiplos caminhos para roteamento de pacotes. Outras similaridades com os outros protocolos multicaminhos apresentados são as seguintes. O MT-AODV é baseado no protocolo reativo AODV, assim como AOMDV e OAOMDV; pode manter rota alternativa como *backup* assim como a extensão do DSR, o AOMDV, o OAOMDV e o LBMR; e pode distribuir a carga de dados por mais de um caminho, como o SMR e o RMPR. No entanto, diferentemente desses protocolos, o MT-AODV (i) não modifica as mensagens de controle originais e os parâmetros da tabela de roteamento, visando manter a compatibilidade com

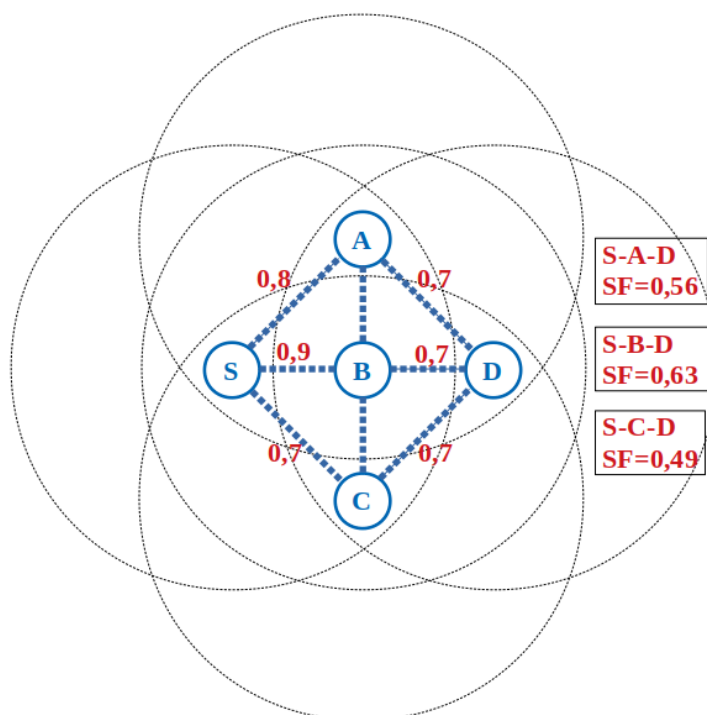


Figura 3.3: Fase de descoberta de rota do RMPR. Utiliza-se a potência do sinal recebido para cálculo do Fator de Energia (SF) dos caminhos. Adaptado [56].

o protocolo original. O MT-AODV (ii) foca em não aumentar a sobrecarga de pacotes de controle para não aumentar o tráfego na rede e manter o protocolo eficiente. (iii) A fim de manter a autonomia dos nós, evita-se o aumento da complexidade para gerenciamento dos nós. O funcionamento do protocolo proposto (iv) não tem dependência de informações de outras camadas, evitando a modificação das mensagens entre as camadas da arquitetura TCP/IP e a mantendo a independência entre as camadas. O protocolo (v) aproveita as rotas múltiplas rotas descobertas para distribuir o tráfego. (vi) Não se considera a obrigatoriedade de caminho alternativo, visando manter a versatilidade da rede. Por fim, o MT-AODV (vii) não computa caminhos disjuntos para que não seja necessário manter a todo instante informações sobre os caminhos completos existentes até o destino. Dessa forma, não sobrecarrega os recursos de memória para que as múltiplas tabelas possam ser implementadas. Assim, o protocolo proposto melhora a resiliência da rede a falhas por disponibilizar rotas ativas durante a transmissão de dados e se diferencia dos demais ao manter a retrocompatibilidade com o AODV, utilizar múltiplas tabelas para gerenciamento das rotas, distribuir a carga por n rotas disponíveis e ao flexibilizar o registro de rotas sob demanda.

Capítulo 4

O Protocolo de Roteamento *Multi-Tables Ad-hoc On Demand Distance Vector (MT-AODV)*

As vantagens do roteamento por múltiplos caminhos discutidas no Capítulo 2 motivaram o estudo e a implementação de um protocolo capaz de descobrir e manter mais de uma rota para o destino. Ademais, o protocolo proposto é habilitado a distribuir o tráfego de dados entre as melhores rotas encontradas e ainda manter rotas com maior custo como *backup*. Os cenários estudados para avaliação do protocolo proposto têm quebras de enlace como uma de suas características. Apesar dos protocolos reativos terem bom desempenho para rede móveis sem fio, tais protocolos exigem um tempo de reação para recálculo de rotas na ocasião de falha de enlace ou nó da rede. Dessa forma, o protocolo proposto visa aumentar a disponibilidade da rede permitindo registrar e usar múltiplas rotas, mantendo as principais características do protocolo original no qual se baseia, como descoberta de rotas sob demanda e número de saltos como métrica de custo. Assim, o protocolo MT-AODV é desenvolvido sem modificação das mensagens de controle do protocolo AODV, mantendo-se a retrocompatibilidade, mas sendo capaz de manter múltiplas rotas e realizar a distribuição de tráfego. Este capítulo apresenta uma visão geral sobre o MT-AODV e uma descrição mais detalha do funcionamento desse protocolo.

4.1 Visão geral do MT-AODV

O MT-AODV é proposto para roteamento de pacotes em MANETs estabelecidas para monitorar sinais vitais de combatentes durante operações militares. Deve-se destacar que as rotas encontradas pelo MT-AODV são armazenadas em múltiplas tabelas de

roteamento, gerenciadas pelo próprio protocolo. Assim, rotas diferentes para um mesmo destino são mantidas em tabelas de roteamento separadas. Da perspectiva de gerenciamento, a propriedade do destino estar presente apenas uma vez em cada tabela facilita a implementação da limitação de tabelas, pois não é necessário gerenciar a quantidade de rotas para cada destino. A ideia das múltiplas tabelas é reduzir as modificações no protocolo original, a fim de manter a retrocompatibilidade [57].

4.1.1 Aspectos relevantes para o desenvolvimento

O desenvolvimento do MT-AODV tem como base as características dos ambientes aos quais o protocolo deve atender. Assim, os seguintes aspectos são considerados: disponibilidade de rota, mobilidade, taxa de transmissão, tempos de descoberta de rota, distribuição de tráfego, sobrecarga de mensagens de controle, limite de tabelas e de número de saltos, retrocompatibilidade, prevenção de laços, tempo de vida e latência fim-a-fim. Cada aspecto é discutido a seguir.

Disponibilidade de rota

A disponibilidade de rota representa o quanto uma rota está pronta para uso durante o funcionamento da rede. Trata-se de uma métrica comumente empregada para avaliação de serviços de comunicação em tempo real. O foco principal do MT-AODV é aumentar a disponibilidade de rota de um protocolo de roteamento reativo sob demanda. Com o armazenamento de mais rotas nas tabelas de roteamento, a falha em um nó ou interrupção de uma rota por qualquer motivo pode ser mitigada pelo uso das outras rotas disponíveis e registradas nas tabelas. Dessa forma, a disponibilidade de rotas é ampliada no MT-AODV em relação ao AODV. Evita-se, ainda, novo cálculo para descoberta de rota, o que contribui para a redução da latência fim-a-fim. A implementação atual do MT-AODV não se preocupa com a disjunção entre as rotas. Dessa forma, uma única interrupção pode invalidar mais de uma rota, dependendo da topologia da rede.

Mobilidade

A mobilidade é um dos principais requisitos dos protocolos de roteamento para redes sem fio. No cenário em estudo, os nós comunicadores são portados por combatentes em ambientes de operação de campo. Dessa forma, a limitação da mobilidade dos nós está intrinsecamente associada à mobilidade do combatente na operação. Portanto, é razoável

considerar que os nós se movem com a velocidade de uma pessoa caminhando ou correndo em qualquer ritmo.

Taxa de transmissão

As aplicações WBAN para monitoramento de sinais vitais utilizam baixa taxa de transmissão contínua para envio dos pacotes. No caso da comunicação inter-WBAN, os nós encaminham para um coletor todos os dados de sensores que estão no combatente. Cada nó coletor envia os dados com uma taxa de transmissão que deve ser suficiente para suportar o agregado de todos os nós sensores que estão no combatente para que não haja congestionamento. Assim, é razoável considerar uma taxa de transmissão relativa ao somatório das taxas de transmissão de cada nó sensor.

Tempo de descoberta de rota

O tempo de descoberta de rota é o período necessário para um nó ter disponível um destino desconhecido inicialmente. Um dos requisitos impostos ao MT-AODV é não aumentar significativamente o tempo médio de descoberta de rota em relação ao protocolo original, pois além de aumentar a latência fim-a-fim, as rotas precisam ser atualizadas rapidamente para que não haja perda de pacote nem sobrecarga por enfileiramento. Dessa forma, o tempo de descoberta do AODV é a referência para o MT-AODV. As rotas no MT-AODV são disponibilizadas à medida que são encontradas, não existe tempo de resguardo para descobrimento de todas as rotas para tomada de decisão. Assim, mantém-se o tempo de descoberta de rota do protocolo original.

Distribuição de tráfego

A distribuição do tráfego de pacotes pode reduzir gargalos e congestionamentos na rede. Além disso, para uma rede de sensores autônomos, a distribuição de tráfego é importante devido às limitações energéticas dos sensores, pois se um nó for utilizado em excesso sua bateria será descarregada mais rapidamente do que as baterias dos outros nós. O encaminhamento do tráfego pelo MT-AODV resulta em uma carga de dados mais distribuída comparada à do protocolo AODV. Isso ocorre devido à utilização de múltiplas rotas para o nó de destino. Com isso, a probabilidade de gargalos e congestionamentos na rede é diminuída. Uma das características do AODV é utilizar sempre os mesmos nós intermediários para diversos nós transmissores. Isso ocorre porque o AODV permite que

uma rota seja inserida na tabela de um nó que recebeu uma mensagem RREP destinada a outro nó. Assim, por vezes, pode existir um nó intermediário sobrecarregado, enquanto um nó sem tráfego está disponível. No caso do MT-AODV, isso não ocorre porque o tráfego é distribuído entre as rotas de menor custo existentes disponíveis.

Sobrecarga de mensagens de controle

Uma das vantagens dos protocolos sob demanda é que não precisam enviar mensagens periódicas com a informação de toda a topologia da rede. As mensagens são enviadas somente quando necessário. Contudo, a cada interrupção de enlace durante uma transmissão, é necessário recalculas as rotas para o destino. Assim, um dos requisitos impostos ao MT-AODV é não elevar o número médio de mensagens de controle necessárias para operação da rede. O MT-AODV é capaz de reduzir o envio de mensagens RREQ se o nó possuir outra rota disponível. Contudo, caso haja uma quebra de enlace em uma rota após um nó intermediário, todos os *gateways* para o nó transmissor receberão uma mensagem RERR informando que a rota não está mais disponível. Assim, do ponto de vista de mensagens de controle, o MT-AODV reduz a quantidade de mensagens RREQ e aumenta o número de mensagens RERR. Contudo, as mensagens RREQ são enviadas em modo de difusão (*broadcast*), enquanto as mensagens RERR são *unicast*. Devido a essa diferença, as mensagens de requisição superam as mensagens de erro na ocasião de uma quebra de enlace. Dessa forma, pode-se afirmar que o MT-AODV reduz a sobrecarga de mensagens de controle em relação ao protocolo original.

Limitação de rotas e tabelas

Sabe-se que quanto maior a quantidade de nós na rede, maior é a quantidade de caminhos e destinos possíveis. Assim, o incremento de um nó tem potencial para aumentar exponencialmente a quantidade de rotas em uma rede *ad-hoc*. No caso do MT-AODV, uma rota secundária pode significar uma tabela nova. Uma nova tabela será criada apenas se não houver uma rota a ser atualizada. Contudo, o aumento de registros pode sobrecarregar a capacidade de memória dos dispositivos. Assim, uma das funcionalidades implementadas no MT-AODV é limitar o número de tabelas criadas. Dessa forma, pode-se optar pela quantidade de rotas desejadas. A escolha deve estar de acordo com a quantidade de nós na rede. No caso de uma rota nova descoberta, o protocolo avalia se atualiza uma de suas rotas ou a descarta.

Retrocompatibilidade

A modificação de um protocolo geralmente o torna incompatível com seu protocolo original. Um dos objetivos do MT-AODV é prover múltiplas rotas mantendo as mesmas mensagens de controle do protocolo base, o AODV. Dessa forma, o MT-AODV tem como um de seus requisitos manter a retrocompatibilidade com o AODV. Isso permite que a rede possa ter nós que atuam tanto com AODV quanto com MT-AODV.

Prevenção de laços

O MT-AODV se preocupa com a prevenção de laços na rede. Para tanto, além dos mecanismos do AODV, o MT-AODV também utiliza 2 mecanismos adicionais. Considera-se o encaminhamento dos pacotes preferencialmente pelas rotas de menor custo. Considera-se também que os nós intermediários são proibidos de encaminhar mensagens pelo *gateway* do nó de origem.

Tempo de vida

O tempo de vida da rede depende da autonomia dos nós em se manterem ativos. Ou seja, a bateria do nó é o principal elemento limitante do tempo de vida da rede. Assim, o protocolo não deve sobrecarregar o processamento do nó, a fim de não aumentar o consumo de energia dos nós. A distribuição do tráfego de dados empregada pelo MT-AODV pode evitar que um único nó seja sobrecarregado pela rede caso haja outras rotas disponíveis.

Latência fim-a-fim

A métrica utilizada para calcular o custo de uma rota no MT-AODV é o número de saltos. O protocolo influencia na latência fim-a-fim de três modos distintos. Primeiro, caso haja uma falha de rota e outra rota já registrada na tabela de roteamento seja utilizada, o protocolo MT-AODV reduz o tempo de descoberta de rota, que potencialmente leva à redução da latência fim-a-fim. Essa redução pode não ocorrer caso a nova rota utilizada tenha elevado atraso. Com isso, a latência fim-a-fim depende da rota escolhida. Segundo, os pacotes são encaminhados por múltiplos caminhos. Por utilizar os caminhos de menor número de saltos, a latência nessa comunicação por múltiplos caminhos é medida pela média da latência de cada caminho, ou, no pior caso, pela maior latência. A tendência é reduzir a latência fim-a-fim, devido às múltiplas rotas usadas. Por fim, a terceira influência

está na escolha da rota. O MT-AODV precisa analisar as rotas antes de encaminhar os pacotes, e essa análise necessita de um tempo de processamento. Assim, o tempo para escolher a rota gera um acréscimo na latência fim-a-fim. A Organização do Tratado do Atlântico Norte (OTAN) classifica os limites do atraso fim-a-fim são de acordo com a classe do serviço oferecido [58]. Para serviços de tempo-real em redes sem fio, o atraso fim-a-fim deve ser menor que 250 ms.

4.1.2 Funcionamento do MT-AODV

O MT-AODV é desenvolvido com base nos aspectos discutidos. A Figura 4.1 mostra a visão geral do funcionamento do protocolo. O fluxograma é iniciado com uma requisição para transmissão de dados. Essa requisição é iniciada na camada de aplicação e o protocolo de roteamento é responsável por indicar a rota para o destino dos dados. Assim, quando um nó possui interesse em transmitir dados, o MT-AODV verifica nas suas tabelas de roteamento se possui alguma rota disponível para o destino. Caso haja uma ou mais rotas disponíveis, o tráfego é encaminhado pelas rotas com menor número de saltos. Caso ainda não tenha rota ativa disponível em suas tabelas de roteamento, inicia-se o processo de descoberta de rotas, destacado na cor laranja. Nesse processo, o nó de origem envia mensagens de requisição de rota para seus vizinhos. Ao receber resposta a essas mensagens de requisição, atualiza-se a tabela de roteamento com a adição das rotas encontradas. São registradas as rotas de menor número de saltos para cada *gateway*. Após a atualização, os dados podem ser transmitidos pelas rotas encontradas que possuem menor número de saltos. Contudo, caso nenhuma rota seja encontrada no processo, os dados são descartados após um período de tempo. O processo de manutenção de rotas, destacado na cor rosa, ocorre em caso de falha de um enlace ou falta de uma rota para transmissão dos dados, quando uma mensagem de erro é gerada para o nó de origem. Nesse caso, o nó de origem atualiza suas tabelas, removendo a rota indisponível. No caso em que o nó de origem possui outras rotas disponíveis para o destino, elas são usadas para ajudar a escoar o tráfego.

4.2 Detalhamento do protocolo

Assim como o AODV, o MT-AODV é um protocolo de múltiplos saltos que utiliza os métodos de descoberta de rotas e manutenção de rotas, contudo, consegue manter mais de uma rota para o destino. Isso é possível por meio da criação de diferentes tabelas durante

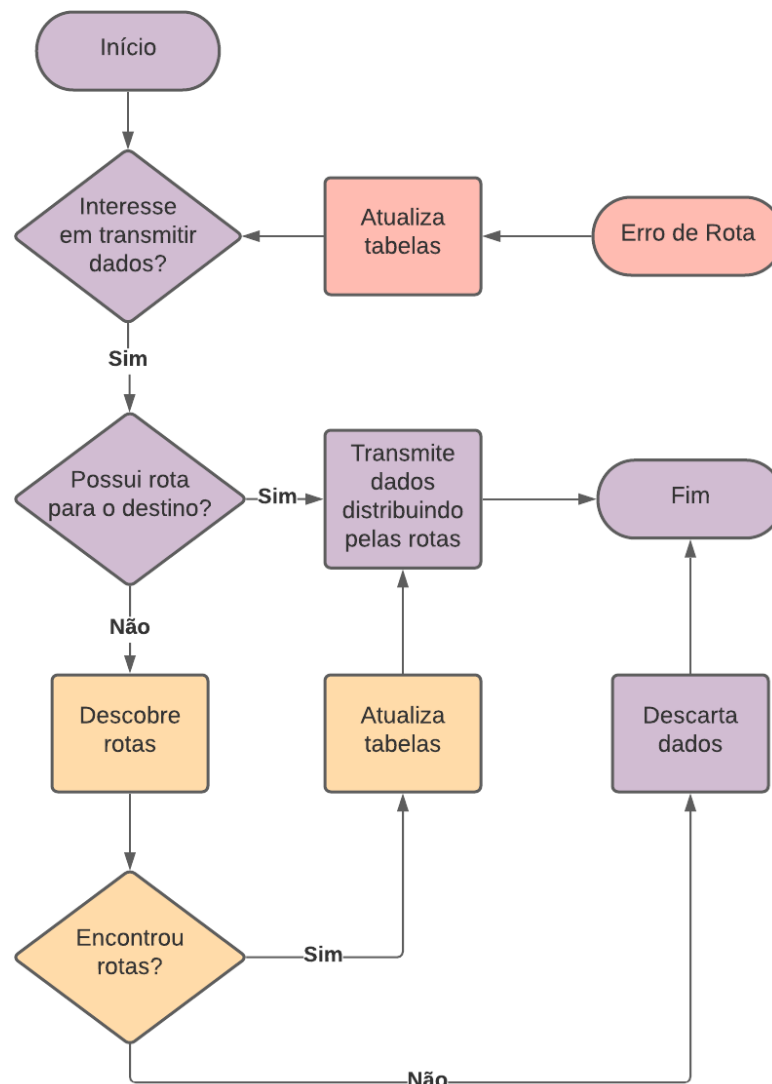


Figura 4.1: Fluxograma simplificado de funcionamento do MT-AODV. A descoberta de rotas é realizada apenas quando um nó possui interesse em transmitir dados para outro nó. A manutenção de rotas atualiza as tabelas de acordo com o recebimento das mensagens de erro.

a descoberta de rotas para um mesmo destino. As tabelas de roteamento em cada nó é construída a partir da troca de mensagens enviadas via *User Datagram Protocol* (UDP) pela porta 654. Para fins didáticos, classifica-se os nós em três tipos:

- **Nó transmissor:** corresponde ao nó de origem da mensagem;
- **Nó intermediário:** equivale a um *gateway* que encaminha a mensagem do nó transmissor para um próximo nó intermediário ou para o nó coletor. Pode haver mais de um nó intermediário no caminho;

- **Nó coletor:** corresponde ao nó de destino da mensagem.

Os principais mecanismos responsáveis pelo funcionamento do protocolo proposto são apresentados de forma detalhada nas seções seguintes.

4.2.1 Descoberta de rotas

A descoberta de rotas no MT-AODV, assim como no AODV, é feita sob demanda. O processo de descoberta de rotas também é semelhante ao do AODV. A modificação está na forma como o MT-AODV registra as rotas encontradas na tabela de roteamento [59]. O MT-AODV cria múltiplas tabelas de roteamento sob demanda, à medida em que as rotas são descobertas. O Algoritmo 1 mostra o procedimento implementado para incluir e atualizar rotas nas tabelas de roteamento quando uma mensagem **RREP** é recebida.

Algoritmo 1 Tratamento das mensagens **RouteReply** para incluir e atualizar rotas nas tabelas de roteamento.

Entrada: **RouteReply**, tabelas

```

1: procedimento RecebeRREP(RouteReply)
2:   k ← COMPRIMENTO(tabelas)
3:   max ← COMPRIMENTO MÁXIMO(tabelas)
4:   rota ← EXTRAIR INFO ROTA(RouteReply)
5:   existe_rota, atualizar_rota, adicionar_rota, adicionar_tabela,
6:     indice_tabela ← VERIFICAR ROTA(tabelas, rota, max)
7:   se existe_rota == FALSO então
8:     ADICIONAR ROTA(rota, tabelas[0])
9:     ENVIAR ROUTE REPLY ACK( )
10:    retorna
11:   senão
12:     se atualizar_rota == VERDADEIRO então
13:       ATUALIZAR ROTA(rota, tabelas[indice_tabela])
14:       ENVIAR ROUTE REPLY ACK( )
15:       retorna
16:     senão
17:       se adicionar_rota == VERDADEIRO então
18:         se adicionar_tabela == VERDADEIRO & k < max então
19:           CRIAR TABELA( )
20:           ADICIONAR ROTA(rota, tabelas[k+1])
21:           ENVIAR ROUTE REPLY ACK( )
22:           retorna
23:         senão
24:           ADICIONAR ROTA(rota, tabelas[indice_tabela+1])
25:           ENVIAR ROUTE REPLY ACK( )
26:           retorna

```

Ao receber a mensagem **RREP**, a função **RecebeRREP** é ativada para tratar a mensagem. O resultado final da execução da função é a inclusão ou a atualização da rota encontrada

nas tabelas de roteamento de S . A inclusão de rota pode ser feita em uma tabela nova ou em uma já existente. Cada registro de rota em uma tabela deve conter os parâmetros de rota. Esses parâmetros são extraídos da mensagem usando a função `ExtrairInfoRota` (linha 4). Destaca-se que o custo da rota nesta dissertação é calculado em números de saltos. Ao receber uma mensagem `RREP` e extrair as informações sobre a rota, S deve verificar se a rota já está presente em uma de suas tabelas. Isso é feito através da função `VerificarRota` (linha 6) que percorre as tabelas existentes. Caso não exista rota, a nova rota encontrada é adicionada à tabela de índice 0. Caso exista uma rota com o mesmo *gateway*, a função `VerificarRota` retorna o índice da tabela em que a rota com o mesmo *gateway* existe. Essa função também retorna informações sobre qual ação deve ser tomada, atualizar ou adicionar rota, e se uma nova tabela deve ser criada. Se a ação for uma atualização, a rota é atualizada na tabela na qual foi encontrada (linha 12). A rota também é atualizada caso a nova rota encontrada possua número de saltos menor que a rota existente, independentemente do *gateway*. Isso também é verificado na função `VerificarRota`. Se S possuir uma rota para o mesmo destino Z , mas com um *gateway* diferente, com número de saltos igual ou maior que a rota existente, a rota encontrada é registrada na tabela de roteamento subsequente, de forma que cada tabela possuirá uma rota distinta para o mesmo destino (linha 24). Se porventura não houver uma tabela sem uma rota para aquele destino, e a quantidade limite de tabelas ainda não tiver sido excedida, uma nova tabela de roteamento é criada e a rota é adicionada em seguida (linha 19).

Uma vez que o nó transmissor pode possuir mais de uma rota para o destino, é possível estabelecer a distribuição do tráfego entre as rotas existentes. Nessa proposta, a distribuição é feita de forma uniforme entre as n melhores rotas ativas nas tabelas de roteamento, doravante chamada como rotas principais. Assim, os dados são transmitidos apenas entre os caminhos que possuem o menor número de saltos. As demais rotas encontradas atuam como caminhos alternativos para salvaguarda (*backup*) e são usados apenas em caso de falha de todas as rotas principais. A Figura 4.2 exemplifica as tabelas de roteamento criadas para um nó em uma topologia hipotética, e como ocorre a distribuição das mensagens. As rotas para o destino são inseridas a partir do recebimento das mensagens `RREP`. As tabelas são criadas sob demanda à medida em que uma nova rota precise ser inserida. Para os nós intermediários, as rotas para o nó transmissor são criadas a partir do recebimento da mensagem `RREQ`. O procedimento para inclusão de rotas é similar ao procedimento de recebimento da `RREP`. No caso do exemplo, o nó S transmite os dados para o Z pelos nós A e B , sendo esse tráfego dividido igualmente pelas

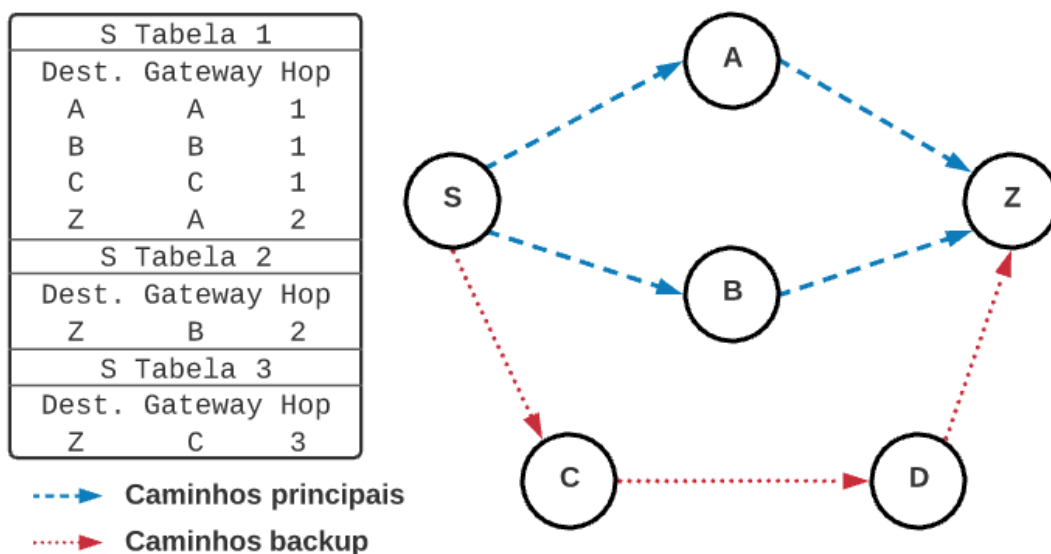


Figura 4.2: Topologia hipotética que exemplifica a configuração das tabelas de roteamento do nó de origem S . Nas tabelas de roteamento 2 e 3, são mostradas apenas as rotas para o nó destino Z . Existem dois caminhos principais e um caminho alternativo para salvaguarda registrados nas tabelas consolidadas.

duas rotas. Isso ocorre porque nas tabelas de roteamento de S , o nó Z pode ser alcançado com 2 saltos pelo *gateway* A (Tabela 1) e também com 2 saltos pelo *gateway* B (Tabela 2). Portanto, essas duas rotas são consideradas rotas principais por possuírem o menor número de saltos até o destino. Apesar da Tabela 3 também possuir uma rota para o nó Z , essa rota precisa de 3 saltos para alcançar o destino e por isso ela será usada apenas caso as duas rotas principais fiquem indisponíveis. Assim, essa terceira rota opera como rota de salvaguarda ou rota *backup*.

4.2.2 Manutenção de rotas

No caso de quebra de um enlace, independentemente do motivo da interrupção, o nó intermediário deve comunicar aos nós que utilizam o enlace falhante sobre essa interrupção. Assim, ao perceber uma queda de enlace, o nó encaminha uma mensagem **RERR** para os nós transmissores de dados e seus respectivos *gateways*. Ao receber a mensagem **RERR**, caso não exista outra rota ativa, uma nova rota precisa ser calculada pelo nó de origem. Esse processo é possível devido a uma lista de **predecessores** criada durante a descoberta de rotas e armazenada pelos nós intermediários. Ou seja, os nós intermediários guardam os endereços IP dos nós que utilizam cada rota, que são justamente os predecessores. Assim, cada rota possui associada a ela, uma lista de predecessores. A Figura 4.3 mostra um exemplo com predecessores associados a rotas. Com a lista de predecessores é

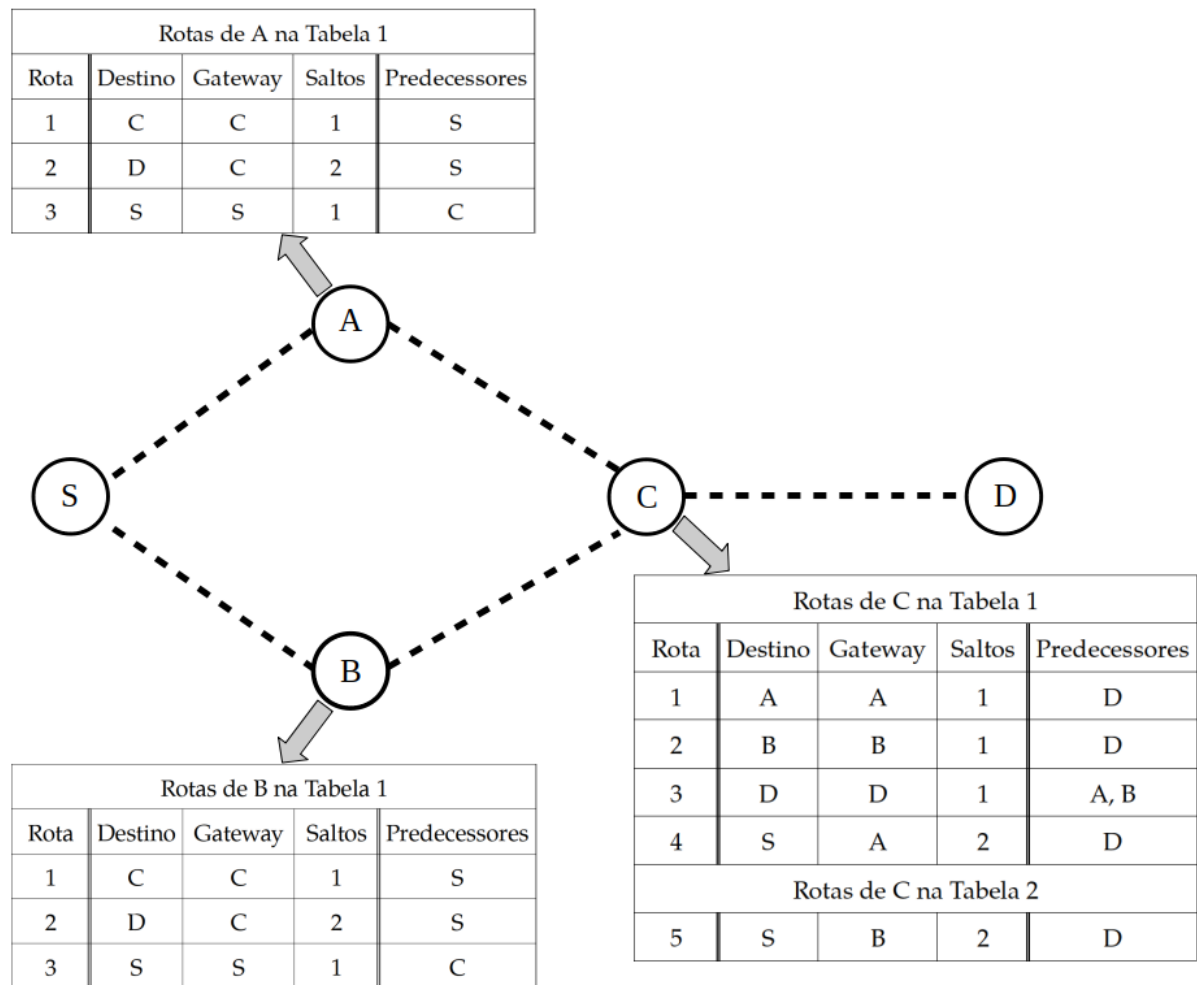


Figura 4.3: Topologia que exemplifica a configuração dos predecessores associados a rotas registradas nos nós. São mostradas apenas as rotas dos nós intermediários. No caso de interrupção de um enlace, o nó intermediário encaminha mensagem de erro aos nós predecessores que possuem como *gateway* o nó do enlace interrompido.

possível encaminhar mensagem de erro para os nós que estão utilizando uma rota que foi interrompida. O nó que detecta a interrupção é responsável por informar a todos os nós que dependiam dessa conexão por meio da mensagem RERR. Por exemplo, se ocorrer uma falha no enlace entre os nós *A* e *C* da Figura 4.3, o nó *A* verifica os predecessores dessa rota (Rota 1 da Tabela 1 de *A*). No exemplo, *S* é o único predecessor. Com essa informação, a mensagem de erro é encaminhada para todos os destinos das rotas que possuem *S* como *gateway*. Nesse caso, apenas a Rota 3 da Tabela 1 de *A* possui *S* como *gateway*. Então a mensagem RERR é enviada ao destino *S*. Da mesma forma, o nó *C* verifica os predecessores das rotas que possuem o enlace com o nó *A* como *gateway*. Nesse exemplo, as Rotas 1 e 4 da Tabela 1 de *C* possuem *A* como *gateway*. *D* é o único predecessor dessas rotas, e apenas a Rota 3 utiliza-o como *gateway*, e também como destino, a mensagem de erro é encaminhada por *C* apenas para esse nó.

4.3 Implementação do MT-AODV

O protocolo proposto nesta dissertação é implementado no NS-3, um simulador de redes de eventos discretos, direcionado principalmente para pesquisa e uso educacional. Esse simulador é escolhido por ser uma ferramenta de código aberto, licenciado sob a licença GNU GPLv2 e mantido por uma comunidade mundial. Além disso, o *software* é modular e possui bom desempenho para simulações de rede. O objetivo do projeto NS-3 é desenvolver um ambiente de simulação aberto para pesquisa em rede, alinhado com as necessidades de simulação da pesquisa em rede moderna. Como a criação de um simulador de rede que possua uma quantidade suficiente de modelos validados e mantidos de alta qualidade exige muito trabalho, o projeto NS-3 tenta distribuir essa carga de trabalho por uma grande comunidade de usuários e desenvolvedores. A cada três meses, uma nova versão estável do simulador é disponibilizada, com novos modelos desenvolvidos, documentados, validados e mantidos por pesquisadores. Assim, o projeto encoraja a contribuição da comunidade, revisão por pares e validação do *software* [60]. A ideia do projeto é construir um núcleo de simulação sólido que seja bem documentado, fácil de usar e depurar e que atenda às necessidades de todo o fluxo de trabalho da simulação, desde a configuração da simulação até a coleta e análise de traços. Com estudos baseados em simulação, a proposta pode ser estudada em detalhes em escalas variáveis, com aplicações de dados e condições de campo variáveis, conduzindo a resultados reproduzíveis e analisáveis [61].

A programação do NS-3 é feita em linguagem C++. A estrutura de *software* incentiva o desenvolvimento de modelos de simulação que sejam suficientemente realistas para permitir que o simulador seja usado como um emulador de rede em tempo real, interconectado com o mundo real, permitindo que as implementações de protocolos existentes no mundo real sejam reutilizadas dentro do NS-3. O NS-3 também oferece suporte a um agendador em tempo real que facilita uma série de casos de uso de “simulação em *loop*” para interagir com sistemas reais. Por exemplo, os usuários podem emitir e receber pacotes gerados pelo simulador em dispositivos de rede reais, e o simulador pode servir como uma estrutura de interconexão para adicionar efeitos de enlace entre máquinas virtuais.

Devido a sua modularidade, o NS-3 é um simulador que permite que novas funcionalidades sejam implementadas. Seu funcionamento básico consiste na criação de nós, seus canais de comunicação e a geração de tráfego na rede. O nó é uma abstração de um dispositivo computacional básico. Essa abstração é representada pela classe `Node` que fornece métodos para gerenciar as representações de dispositivos computacionais nas si-

mulações. Pode-se criar um conjunto de nós que possuem as mesmas características por meio da classe `NodeContainer`. As funcionalidades do nó, tais como aplicativos, pilhas de protocolos e periféricos devem ser associadas a ele. Para isso, deve-se configurar os nós, associando a eles desde a camada física, com a definição de parâmetros importantes como a frequência da portadora, potência de transmissão e limiar de sensibilidade de recepção, até a aplicação, com a definição de parâmetros como tamanho máximo do pacote e a taxa de transmissão. O meio sobre o qual os dados trafegam é chamado de canal. Cada canal é implementado em uma classe de canal diferente, que fornece métodos para configurar a comunicação no canal de acordo com o tipo de canal e tecnologia, por exemplo canal sem-fio Wi-Fi ou canal cabeado ponto-a-ponto.

No NS-3, a abstração básica para um programa de usuário que gera alguma atividade a ser simulada é a aplicação. Essa abstração é representada por classes de aplicações que são dependentes do tipo de aplicação desejada. A classe de aplicação fornece métodos para gerenciar a representação de suas versões de aplicações a serem simuladas. A aplicação interage diretamente com o protocolo de transporte por meio de soquetes. A abstração do dispositivo de rede é representada pela classe `NetDevice`, e fornece métodos para gerenciar conexões entre nós e canais. Essa abstração do dispositivo de rede cobre tanto o *hardware* quanto o *software*. Os dispositivos de rede, assim como os canais e as aplicações, também podem ser especializados. Durante a simulação, a comunicação gera registros pertinentes às configurações parametrizadas no ambiente simulado. A partir desses registros, os resultados da simulação são gerados e armazenados. Os resultados podem ser armazenados externamente ao simulador para posterior análise e construção de gráficos.

Nesta dissertação, utiliza-se a versão 3.33 do NS-3. Os códigos fonte de todos os módulos do simulador ficam armazenados no diretório `ns-3.33/src`. Para implementação do protocolo MT-AODV¹, os seguintes arquivos referentes ao módulo que implementa o AODV são usados como base: `aodv-rtable.cc`, `aodv-rtable.h`, `aodv-routing-protocol.cc` e `aodv-routing-protocol.h`. A Tabela 4.1 descreve brevemente os arquivos modificados para a implementação do MT-AODV.

As modificações realizadas são detalhadas a seguir:

- `mt_aodv-rtable.h`: criado um método que tem como entrada o endereço IP de destino, o endereço IP do *gateway* para o destino e a tabela de roteamento;

¹Os códigos implementados no NS-3 para funcionamento do MT-AODV estão disponíveis em https://github.com/ricmofi/ns-3_mt-aodv.

Tabela 4.1: Arquivos de código fonte e cabeçalho modificados para a implementação do MT-AODV.

Arquivos	Descrição
<code>mt_aodv-rtable.h</code>	Define os métodos da tabela de roteamento do MT-AODV
<code>mt_aodv-rtable.cc</code>	Define a operação da tabela de roteamento do MT-AODV
<code>mt_aodv-routing-protocol.h</code>	Define os métodos para operação do MT-AODV
<code>mt_aodv-routing-protocol.cc</code>	Define a operação do roteamento MT-AODV

- `mt_aodv-rtable.cc`: a partir do recebimento das entradas, é possível verificar se existe uma rota na tabela de roteamento para um destino com o *gateway* especificado;
- `mt_aodv-routing-protocol.h`: criado um método que tem como entrada o endereço IP de destino, o tempo de expiração de rota e o índice do vetor tabela de roteamento;
- `mt_aodv-routing-protocol.cc`: diversas modificações no código fonte original são necessárias para operação do MT-AODV. As principais são:
 - Criação de vetor para armazenar tabelas de roteamento (`TableRoutingList`)
O AODV utiliza uma classe `TableRouting` para inserir e manter a tabela de roteamento. Contudo, o MT-AODV opera com mais de uma tabela. Assim, opta-se pela criação do vetor `TableRoutingList` para registro das tabelas de roteamento, interferindo minimamente na criação da tabela de roteamento do protocolo AODV. O MT-AODV inicia com um vetor de tamanho 1. As demais tabelas são inseridas à medida em que as rotas são encontradas.
 - Modificação do método de atualização de tempo de expiração de rota (`UpdateRouteLifeTime`)
Para que a rota seja atualizada é necessário informar a tabela à qual a rota está registrada. Por isso, o método de atualização de rota é modificado e passa a informar também a tabela que deve ser atualizada.
 - Modificação do método de envio de RREQ (`SendRequest`)
O código verifica todas as tabelas antes do envio da mensagem RREQ.
 - Modificação do método de recebimento de RREQ (`RecvRequest`)
Ao receber a mensagem RREQ, o algoritmo verifica em todas as tabelas se possui rota para o destino e para a origem. A inclusão da rota e seleção de rota de

resposta também são alteradas.

- Modificação do método de envio de RREP pelo nó intermediário (`SendReplyByIntermediateNode`)
Esse método passa a receber o índice das tabelas do nó de destino e do nó de origem para encaminhamento das mensagens de resposta.
- Modificação do método de recebimento de RREP (`RecvReply`)
A inclusão e a atualização das rotas no nó de origem são realizadas nesse método.
- Modificação do método de envio de RERR quando há quebra de enlace (`SendRerrWhenBreaksLinkToNextHop`)
No protocolo original, a mensagem de erro é encaminhada sempre que há um quebra de enlace. No MT-AODV, a mensagem é enviada apenas se não houver outra rota para o destino.
- Modificação do método de envio de RERR (`SendRerrMessage`)
A mensagem de erro é enviada para todos os predecessores da rota quebrada.
- Modificação do método de encaminhamento de pacotes (`RouteOutput`)
Método modificado para que o pacote seja transmitido apenas pelo caminho de menor custo.
- Modificação do método de roteamento de pacotes (`Forwarding`)
Modificação análoga à `RouteOutput`. Esse método é usado apenas por nós intermediários.

Capítulo 5

Resultados e Discussão

O MT-AODV é avaliado através de uma análise comparativa dos resultados obtidos em simulações realizadas para cenários distintos. As avaliações são divididas em dois experimentos. No primeiro experimento, varia-se os nós falhantes de acordo com a proximidade ao nó coletor. No segundo experimento, variam-se a posição inicial dos nós, a mobilidade dos nós, o tipo de falha, os nós falhantes e o número de falhas. Este capítulo descreve os experimentos, os respectivos cenários simulados e discute os resultados obtidos.

5.1 Primeiro experimento: posição inicial dos nós em grade

O primeiro experimento tem como objetivo comparar o MT-AODV com seu protocolo base em cenários controlados, isto é, com pequeno grau de aleatoriedade no ensaio. Dessa forma, define-se um cenário onde os nós formam uma topologia em grade fixa. Nesse cenário, 20 nós estão dispersos formando uma grade 4 por 5 em uma área de $150\text{ m} \times 200\text{ m}$. A taxa de dados de tráfego *Constant Bit-Rate* (CBR) é de 10 kb/s e o tempo de simulação é de 600 s . A cada cenário, falhas são inseridas em nós que estão a 1, 2 ou 3 saltos de distância do nó coletor. Os parâmetros utilizados estão descritos na Tabela 5.1. A análise comparativa do MT-AODV é feita em relação ao AODV. Apenas 1 nó está configurado como coletor de dados e os demais são nós transmissores e/ou intermediários.

Os cenários com topologia em grade são avaliados segundo a proporção de pacotes de dados recebidos e perdidos em relação ao total de pacotes de dados transmitidos, a sobrecarga de mensagens de controle, o atraso médio fim-a-fim, o número máximo de saltos, o número máximo de tabelas e a vazão média da rede. A **proporção de pacotes**

de dados recebidos e perdidos em relação ao total de pacotes de dados transmitidos pelos nós mostra a capacidade de entrega de pacotes de cada protocolo para os cenários simulados. A **sobrecarga de pacotes de controle** é medida pelo percentual de pacotes de controle recebidos em relação ao total de pacotes recebidos. O **atraso médio fim-a-fim** mede o tempo médio que cada pacote leva para chegar ao nó coletor. O **número máximo de saltos** informa, dentre todos os nós transmissores, qual foi o maior valor do número de saltos encontrado nas tabelas de roteamento necessário para alcançar o nó coletor. O **número máximo de tabelas** mostra a maior quantidade de tabelas configuradas por um nó durante a simulação. Por fim, a **vazão** mostra a média da quantidade de bits recebidos por segundo no coletor. Como não há aleatoriedade nesse experimento, apenas uma rodada da simulação para cada cenário é executada.

Nos cenários em topologia de grade, são geradas falhas de acordo com a proximidade do nó coletor. Assim, os cenários são organizados da seguinte forma:

- 3 cenários fixos com falhas intermitentes. A cada 40 segundos uma falha é gerada em um dos nós por um período de 30 segundos.
 - Falha em nós 1 salto distante do coletor;
 - Falha em nós 2 saltos distante do coletor; e
 - Falha em nós 3 saltos distante do coletor.

Os parâmetros de configuração da simulação do primeiro experimento estão descritos na Tabela 5.1. A área é de 30000m^2 , com 20 nós posicionados em uma grade 4 por 5, com a distância entre vizinhos de 50 m e o alcance de transmissão de 60 m. O tempo de simulação é de 600 segundos, e a taxa de transmissão de 10 kb/s.

5.2 Segundo experimento: posição inicial aleatória

A fim de comparar os protocolos em cenários com topologias dinâmicas, o segundo experimento é configurado para avaliar os desempenhos dos protocolos em cenários onde existem rápidas alterações na topologia. Nesse experimento, a avaliação do protocolo é feita em 7 cenários distintos, nos quais podem existir, ou não, mobilidade e falhas. Em todos os cenários, a posição inicial dos nós é escolhida aleatoriamente. Em relação às **falhas**, elas podem ser permanentes ou intermitentes e ocorrem em momentos arbitrados em tempo de execução. *Falha permanente* significa que a falha gerada no nó não é retirada,

Tabela 5.1: Resumo dos parâmetros de configuração usados na simulação do primeiro experimento.

Parâmetro	Descrição
Simulador	NS-3 Versão 3.33
Posicionamento inicial	Pré-definido em grade
Área	150 m × 200 m
Nós transmissores	19
Nó coletor	1
Alcance de transmissão dos nós	60 m
Distância entre os nós vizinhos	50 m
Modelo de propagação	Espaço livre
Perda de propagação	Modelo de Friis
Protocolo de camada de enlace e física	802.11g
Tipo de tráfego	CBR
Protocolo da camada de transporte	UDP
Tempo de simulação	600 segundos
Tamanho do pacote de dados	256 bytes
Taxa de dados	10kb/s
Protocolos de Roteamento	AODV e MT-AODV
Mobilidade	Sem mobilidade

ou seja, a partir daquele momento, o nó torna-se inoperante até o final da simulação. Na *falha intermitente*, o nó permanece em falha durante 5 segundos, retornando ao funcionamento normal após esse período. O nó falhado é escolhido de forma aleatória. Na falha permanente, escolhe-se aleatoriamente 1, 2, 3 ou 4 nós. Em relação à **mobilidade**, os nós podem ser *fixos*, isto é, são colocados em uma determinada localização e permanecem nela durante toda a simulação, ou podem ser *móveis*, e nesse caso todos os nós se movem aleatoriamente em uma determinada área. Assim, os cenários são organizados da seguinte forma:

- 5 cenários fixos: a posição do nó é escolhida aleatoriamente.
 - Falha permanente em 1 nó transmissor/intermediário;
 - Falha permanente em 2 nós transmissores/intermediários;
 - Falha permanente em 3 nós transmissores/intermediários;
 - Falha permanente em 4 nós transmissores/intermediários; e
 - Falhas intermitentes em todos os nós transmissores/intermediários: uma falha é gerada em um nó aleatoriamente. Após 5 segundos, a falha é desfeita e uma nova falha é gerada em outro nó escolhido aleatoriamente;
- 2 cenários com mobilidade: a posição do nó é escolhida aleatoriamente. A cada 10

segundos, uma nova posição aleatória é escolhida para cada nó, que se desloca com velocidade aleatória, entre 1 e 5 m/s.

- o Sem falhas: nenhuma falha é gerada intencionalmente. As quebras de enlace são provenientes apenas da mobilidade dos nós; e
- o Falhas intermitentes em todos os nós transmissores/intermediários: Além das quebras de enlace, nesse cenário, são geradas falhas intermitentes em nós aleatórios a cada 5 segundos;

A avaliação do MT-AODV é feita através de uma análise comparativa com os protocolos DSDV, OLSR e AODV, utilizando o NS-3 [60]. Esses protocolos já estão disponíveis nesse simulador e são usadas as configurações padrão fornecidas pelo NS-3 [62]. O cenário simulado é composto por uma rede com 9 nós transmissores/intermediários sem fio e apenas 1 nó coletor de dados, sendo que cada nó representa um dispositivo de monitoramento colocado em um combatente que está em uma operação de campo. É inferido que esse dispositivo reúne todos os dados dos sinais vitais monitorados. Ou seja, os 9 nós transmissores representam 9 combatentes espalhados em um campo de operação e enviam as informações dos sinais vitais dos respectivos combatentes para o dispositivo em um 10^o combatente que, além de monitorar os sinais vitais também atua como nó coletor desse cenário de comunicação inter-WBAN. Todos os nós são alocados aleatoriamente em um plano de 900m². A transmissão dos dados até o nó coletor é feita usando a tecnologia IEEE 802.11g e, a partir do coletor os dados são enviados para o CCC. O cenário simulado foca na transmissão apenas até o nó coletor. A transmissão dos 9 nós é realizada simultaneamente com uma pequena diferença aleatória de tempo inserida na simulação para reduzir as colisões no início da execução. Os nós transmissores geram um tráfego de Taxa de Bits Constante (CBR) de 50 kb/s para o nó coletor, sendo a carga útil do pacote igual a 256 bytes. Esse tipo de tráfego foi escolhido na simulação para representar os serviços de monitoramento em tempo-real. O tráfego CBR gerado é superior aos valores encontrados na literatura para tráfego de monitoramento da saúde. Contudo, deve-se considerar que o valor é relativo ao tráfego agregado de todos os sensores de monitoramento do combatente. Cada execução da simulação dura 120 segundos e são feitas 30 execuções. A potência de transmissão é reduzida, a fim de dificultar a detecção por sistemas de varredura do espectro eletromagnético. Os parâmetros de configuração da simulação do segundo experimento estão descritos na Tabela 5.2.

Nessa avaliação, a análise de desempenho é baseada no número total de pacotes recebidos, na taxa de pacotes perdidos, no atraso fim-a-fim, e na vazão da rede ou taxa de

Tabela 5.2: Resumo dos parâmetros de configuração usados na simulação do segundo experimento.

Parâmetro	Descrição
Simulador	NS-3 Versão 3.33
Posicionamento inicial	Aleatório
Área	30m x 30m
Nós transmissores	9
Nó coletor	1
Alcance de transmissão dos nós	10m
Modelo de propagação	Espaço livre
Perda de propagação	Modelo de Friis
Protocolo de camada de enlace e física	802.11g
Tipo de tráfego	CBR
Protocolo da camada de transporte	UDP
Tempo de simulação	120 segundos
Tamanho do pacote de dados	256 bytes
Taxa de dados	50kb/s
Protocolos de Roteamento	DSDV, OLSR, AODV e MT-AODV
Mobilidade	Sem mobilidade e Aleatória
Velocidade	0 a 5m/s

transferência. O **número total de pacotes recebidos** é o somatório do número de pacotes enviados por cada nó transmissor e que é recebido pelo coletor. A **taxa de pacotes perdidos** representa a razão entre o total de pacotes perdidos e o total de pacotes esperados pelo destino. O **atraso fim-a-fim** mede o tempo médio que cada pacote leva para chegar ao coletor. Por fim, a **vazão** mostra a média da quantidade de bits recebidos por segundo no nó coletor. Os resultados são médias apresentadas com intervalo de confiança de 95% considerando a distribuição t de Student.

5.3 Avaliação de desempenho

Esta seção está subdividida em duas. Na primeira, são apresentados os resultados da primeira parte da avaliação, na qual podem existir falhas e os nós são posicionados inicialmente em uma grade 4 por 5 e permanecem fixos durante toda a simulação. Na segunda seção, são apresentados os resultados da segunda parte da avaliação, na qual os cenários estudados podem ter falha ou não e possuem 10 nós que podem ser móveis ou não, mas são distribuídos inicialmente em uma determinada área de forma aleatória.

5.3.1 Posição inicial dos nós em grade

No primeiro experimento, são realizadas simulações em um cenário tipicamente controlado. Para isso, uma topologia de nós numa grade 4 por 5 é usada para comparar os protocolos MT-AODV e AODV. A topologia em grade é usualmente empregada para simulação de redes de múltiplos saltos porque reduz alguns fatores de influência aleatória, como a variação da distância entre os nós e variação inicial do número de saltos, ao contrário do que ocorre na distribuição aleatória de nós em uma determinada região. Não há aleatoriedade nos cenários e, por isso, as simulações de um cenário têm sempre o mesmo resultado. Uma vez que os cenários do primeiro experimento são determinísticos, apenas uma rodada de simulação para cada protocolo em cada cenário é realizada. As falhas são aplicadas aos nós de acordo com a proximidade ao nó coletor. A topologia consiste em 20 nós e 31 enlaces como mostrado na Figura 5.1. Cada nó é representado por um combatente e possui uma identificação única. Cada enlace é ilustrado por uma linha tracejada na cor laranja e todos os enlaces têm o mesmo custo. Nessa topologia, o nó 19 é o mais distante do nó coletor, tendo que percorrer 7 saltos se o caminho mais curto for sempre escolhido. Cada um dos 19 nós transmissores/intermediários transmite tráfego CBR de 10 kb/s para o nó coletor. Além disso, a cada 40 segundos, uma falha de 30 segundos é

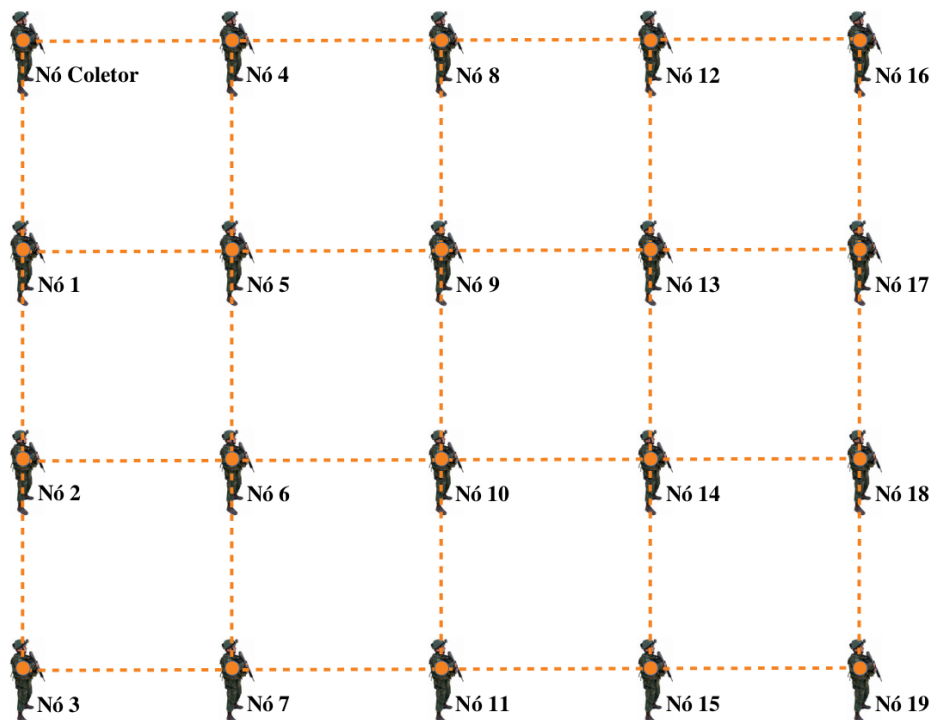


Figura 5.1: Topologia da rede com nós em grade 4×5 . Apenas um coletor está configurado e todos os nós enviam dados para o nó coletor.

inserida em um nó escolhido.

Os nós que falham são escolhidos de acordo com o número de saltos até o nó coletor. No primeiro caso, as falhas são inseridas nos nós 1 ou 4 alternadamente, pois são os únicos vizinhos do nó coletor. Ou seja, somente esses nós estão a 1 salto de distância do nó coletor. Assim, quando um desses nós falha, o nó coletor pode ser alcançado somente por um caminho alternativo que passa pelo outro nó vizinho ativo. No segundo cenário, as falhas são inseridas alternadamente em nós que estão a 2 saltos de distância do nó coletor, ou seja, nos nós 2, 5 ou 8. No terceiro cenário, os nós de falha estão na distância de 3 saltos, resultando em falhas nos nós 3, 6, 9 ou 12 alternadamente. A Figura 5.2 mostra a **proporção de pacotes de dados recebidos e perdidos** em relação aos pacotes de dados transmitidos. Analisando o primeiro cenário, com falha em nós distantes de 1 salto, o protocolo MT-AODV atinge uma taxa de entrega de pacote de dados de 62,87 %, enquanto o AODV alcança 54,75 %. Isso se deve ao fato do MT-AODV possuir mais de uma rota principal disponível em sua tabela de roteamento. Assim, alguns dos nós transmissores/intermediários possuem mais de uma rota para chegar ao destino, e ao ocorrer uma quebra de enlace todo o tráfego é redirecionado para a rota ativa sem necessidade de realizar um recálculo para descoberta da rota, diferentemente do AODV que utiliza apenas uma rota para transmissão e precisa calcular uma nova rota no caso de quebra de enlace. Para os cenários com nós falhantes a 2 e 3 saltos distantes, a diferença entre os protocolos é pequena. Observa-se que à medida que os nós falhantes estão mais distantes do nó coletor, a proporção de pacotes recebidos aumenta. Isso ocorre pelas duas razões a seguir: quanto mais próximo do nó coletor está o nó falhante, menos

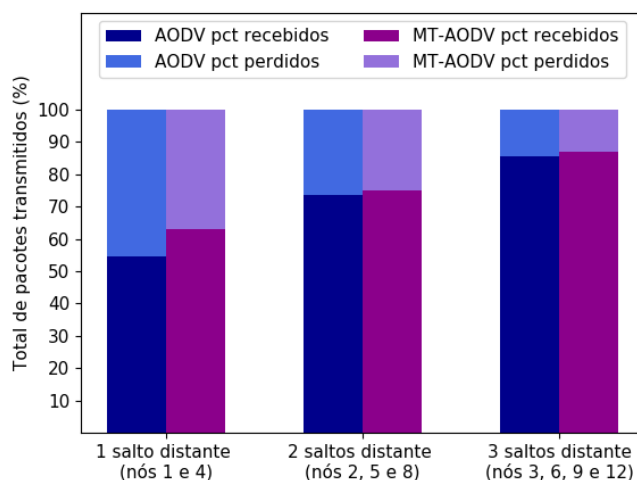


Figura 5.2: Proporção de pacotes de dados recebidos e perdidos em relação aos pacotes de dados transmitidos. O MT-AODV supera o AODV em todos os cenários. A perda de pacotes aumenta em caso de falha de nó próximo ao coletor.

rotas alternativas existem para alcançá-lo; e os nós mais próximos do coletor não são influenciados pelas falhas que ocorrem nos nós mais distantes. A Figura 5.3 corrobora a última explicação. Observa-se na Figura 5.3(a) que todos os nós são influenciados pelas falhas nos nós distantes de 1 salto do nó coletor, uma vez que o número de pacotes recebidos é bastante reduzido para os nós que estão a qualquer número de saltos até o nó coletor. Quando a falha ocorre em nós mais distantes, os nós mais próximos não são

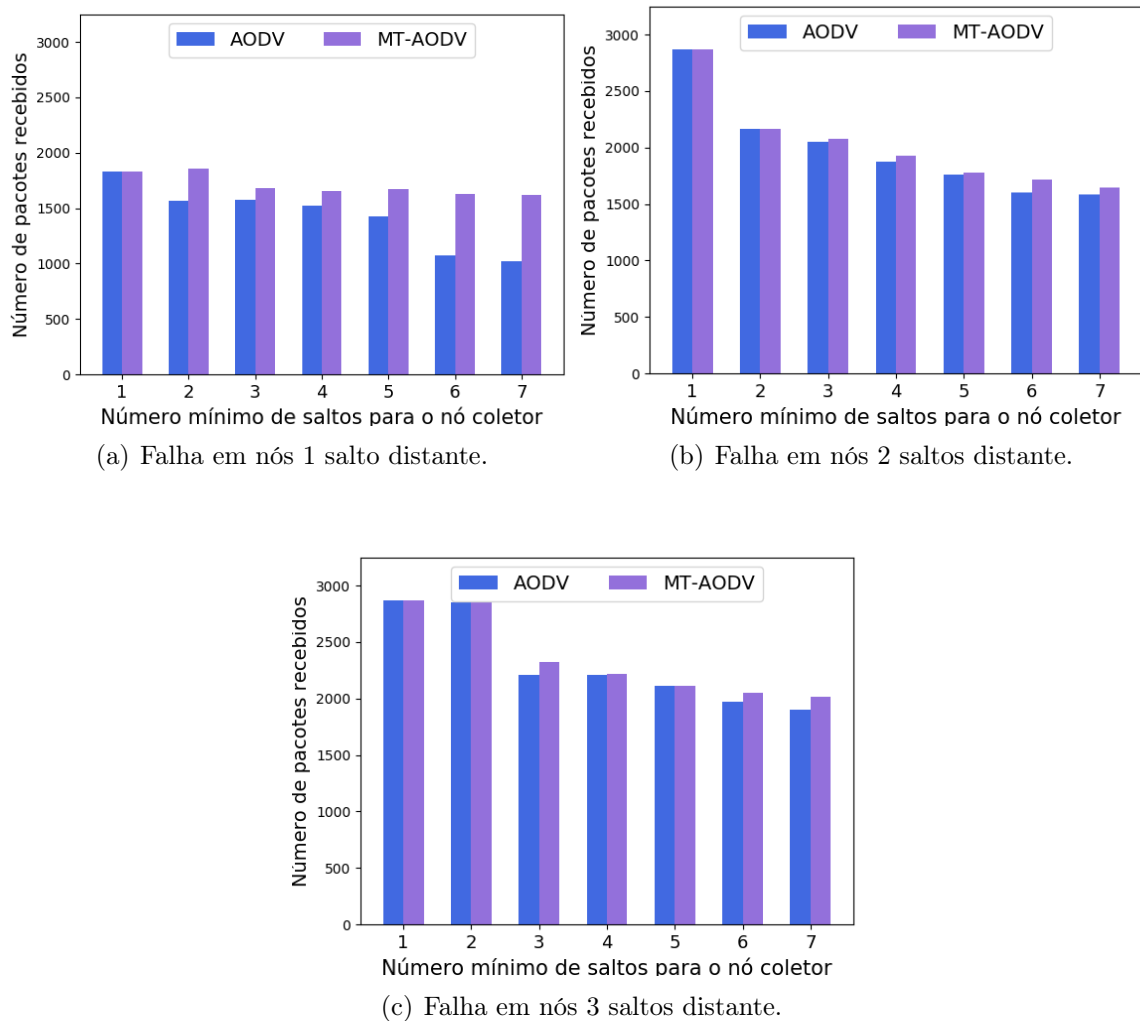


Figura 5.3: Média de pacotes recebidos pelo coletor em função da proximidade com o nó de origem quando ocorrem falhas em nós de acordo com a distância até o coletor. A tendência é de que quanto mais distante do nó coletor a falha ocorre, menor é o impacto em nós mais próximos ao coletor. Os nós do MT-AODV conseguem entregar mais pacotes ao coletor que o AODV. (a) No caso de falhas alternadas em nós vizinhos ao coletor, todos os nós são influenciados. (b) Falhas em nós com 2 saltos de distância do coletor não influenciam os nós a 1 salto de distância do coletor. (c) Com falhas em nós a 3 saltos do coletor, os nós a 1 e 2 saltos de distância não são influenciados pelas falhas e o número de caminhos que podem ser encontrados é maior.

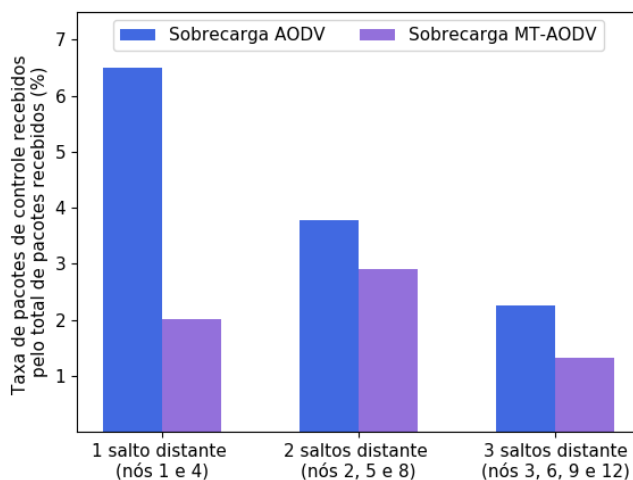


Figura 5.4: Proporção de pacotes de controle recebidos sobre todos os pacotes recebidos. MT-AODV envia menos pacotes de controle do que AODV.

afetados, como mostram as Figuras 5.3(b) e 5.3(c).

A Figura 5.4 mostra o percentual de **sobrecarga de pacotes de controle**, que é o total de pacotes de controle recebidos em relação ao total de pacotes recebidos. No cenário com falha em nós a 1 salto de distância, o AODV precisa encaminhar 1837 pacotes de controle durante os 600 segundos de simulação, o que representa 6,5 % do total de pacotes recebidos, contra 651 pacotes de controle do MT-AODV, o que representa 2 % do total de pacotes recebidos. Assim, o percentual de mensagens de controle que o MT-AODV necessita é menos de três vezes do percentual de mensagens de controle necessários para o AODV. Dessa forma, pode-se afirmar que o MT-AODV reduz significativamente a sobrecarga de pacotes de controle em relação ao protocolo original. Isso ocorre porque os nós que tinham uma segunda rota principal registrada não precisam recalculá-la para o nó coletor em caso de interrupção de uma rota. Tal recálculo gera obrigatoriamente novas mensagens RREQ e RREP. Para os segundo e terceiro cenários, o MT-AODV também tem melhor desempenho que o AODV, porém, em menor proporção, pois há menor quantidade de nós dependentes dos nós que falham a 2 e 3 saltos de distância do nó coletor. Assim, a quantidade de recálculos de rotas é menor.

O resultado de **atraso fim-a-fim** médio dos pacotes de dados é mostrado na Figura 5.5. Os diagramas de caixas mostram a variação do atraso dos pacotes transmitidos por cada nó. Observa-se que as caixas para o AODV possuem formato mais alongado, indicando uma maior variabilidade do atraso fim-a-fim. Os valores máximos do AODV são maiores que os do MT-AODV. As médias para o protocolo AODV são de 3,6 ms,

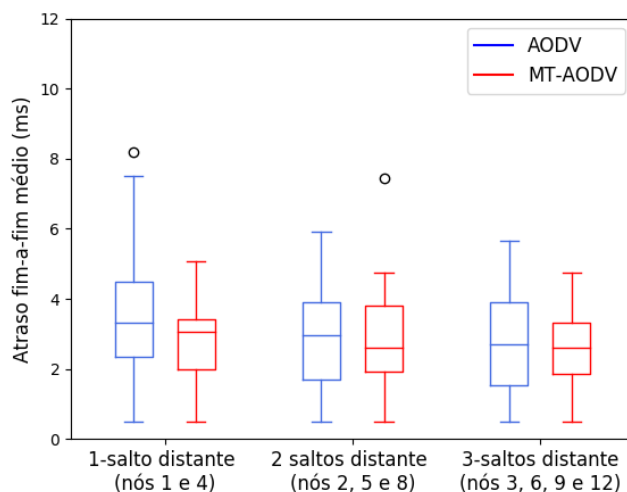


Figura 5.5: Atraso fim-a-fim de pacotes de dados recebidos. O atraso máximo diminuiu em MT-AODV em comparação com AODV.

2,9 ms e 2,7 ms para os cenários de falhas em nós a 1, 2 e 3 saltos distantes do coletor, respectivamente. Para o MT-AODV as médias são de 2,8 ms, 2,8 ms e 2,5 ms para os mesmos cenários. Entende-se que a variabilidade observada nessa figura se deve principalmente às diferentes distâncias resultantes de caminhos com número de saltos distintos que provocam atrasos maiores ou menores de acordo com a distância até o coletor. Para verificar essa afirmação, avalia-se o atraso médio fim-a-fim em cada cenário de acordo com o número mínimo de saltos do nó de origem até o coletor. A Figura 5.6 mostra esse resultado. É possível observar que o atraso médio do AODV é maior para todas as distâncias em todos os cenários, exceto para os nós a 2 saltos do coletor independentemente da distância do nó falhante, e para os nós a 7 saltos do coletor quando ocorre falha nos nós que estão a 2 saltos do coletor.

O número máximo de saltos e o número máximo de tabelas são apresentados na Tabela 5.3. Em relação ao número máximo de saltos, ocorre que, após a quebra de um enlace, os nós que estavam usando uma rota com o enlace interrompido precisam recalcular suas rotas. Contudo, nem sempre o trajeto encontrado é o trajeto mais curto disponível. Isso se deve principalmente por dois motivos: a mensagem RREP pode chegar primeiro ao nó transmissor por um nó em caminho mais longo enquanto a rota mais curta está inativa; ou se o pacote de controle da rota mais curta for perdido por algum motivo. Assim, o número de saltos máximo indica o maior número de saltos encontrado para chegar ao nó coletor dentre as rotas registradas na tabela de roteamento de todos os nós transmissores. O MT-AODV registra rotas com até 8 saltos no cenário de falhas alternadas dos nós vizinhos, enquanto o AODV armazena rotas com até 11 saltos para

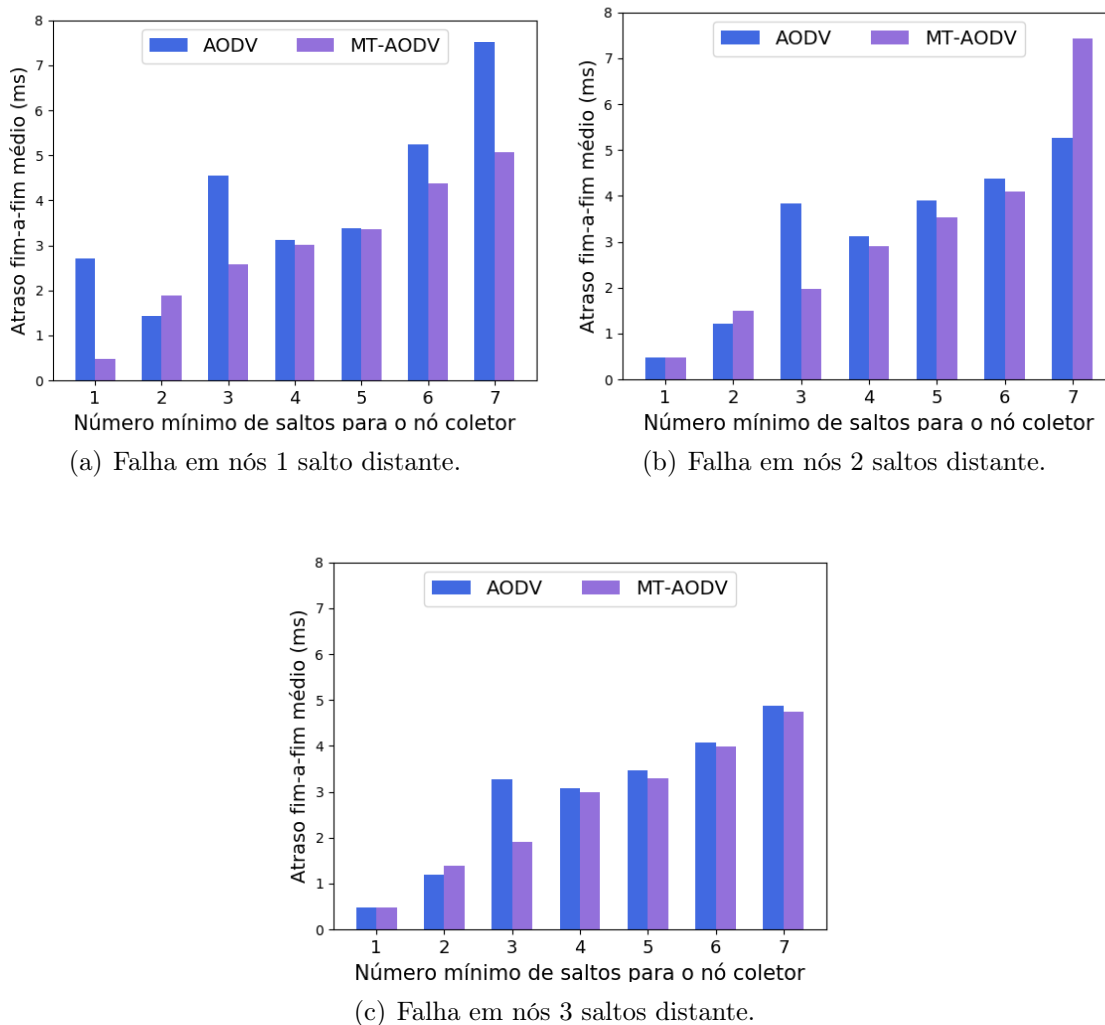


Figura 5.6: Atraso fim-a-fim médio em função da distância até o nó coletor para cada cenário de falha. Quanto maior a distância ao coletor, maior é o atraso. O MT-AODV apresenta menor atraso em todos os cenários, exceto quando a falha ocorre em nós a 2 saltos do coletor. Nesse caso, os nós a 7 saltos do coletor apresentam maior atraso com o MT-AODV. Os nós a 2 saltos do coletor também apresentam maior atraso independentemente do cenário.

o nó coletor. No cenário com falhas em nós 2 saltos distantes, para o MT-AODV existe uma rota com 9 saltos para chegar ao nó coletor, enquanto o número máximo de saltos do AODV é 8. Essa quantidade de saltos justifica um maior atraso fim-a-fim para um dos cenários do MT-AODV. Para o cenário de falhas alternadas nos nós 3, 6, 9 e 12, que estão a 3 saltos de distância do nó coletor, o AODV apresenta o número de saltos máximo de 7, enquanto o MT-AODV apresenta rotas com até 8 saltos. Contudo, essa rota esteve disponível durante pouco tempo da simulação, pois uma rota de menor custo foi encontrada, e por isso, esse resultado não é percebido na métrica de atraso fim-a-fim.

Tabela 5.3: Comparação AODV x MT-AODV quanto ao número de saltos e de tabelas na rede de topologia de grade 4x5.

Nós de falha	Métrica	AODV	MT-AODV
1 e 4	Máx. saltos	11	8
	Máx. tabelas	1	2
2, 5 e 8	Máx. saltos	8	9
	Máx. tabelas	1	3
3, 6, 9 e 12	Máx. saltos	7	8
	Máx. tabelas	1	2

Quanto ao número de tabelas utilizadas, o MT-AODV registra até 2 tabelas para os cenários de falha nos nós a 1 e 3 saltos distantes do nó coletor. Contudo, o número de rotas distintas registradas por um nó transmissor é 3 no cenário de falhas nos nós distantes de 2 saltos do coletor, conforme mostrado na Tabela 5.3. Ou seja, em um determinado momento da simulação um dos nós transmissores possui 3 tabelas de roteamento. Isso quer dizer que um dos nós possui até 3 rotas distintas para encaminhamento do tráfego nesse cenário. O AODV sempre usa uma única tabela, pois foi projetado para operar dessa forma, e por isso, o resultado é igual a 1 para todos os cenários.

A vazão média é a última métrica avaliada. O resultado é apresentado na Figura 5.7. No cenário de falha de nós a 1 salto do coletor, o MT-AODV ultrapassa o AODV, atingindo 6,07 kb/s, contra 5,26 kb/s para AODV, representando um ganho de vazão de 15% sobre o AODV. O diagrama de caixas mostra que os valores de vazão mínimo e máximo são mais altos no MT-AODV, isso significa que o MT-AODV pode fornecer maior largura de banda agregada do que o AODV. A Figura 5.8 apresenta a vazão média dos nós em

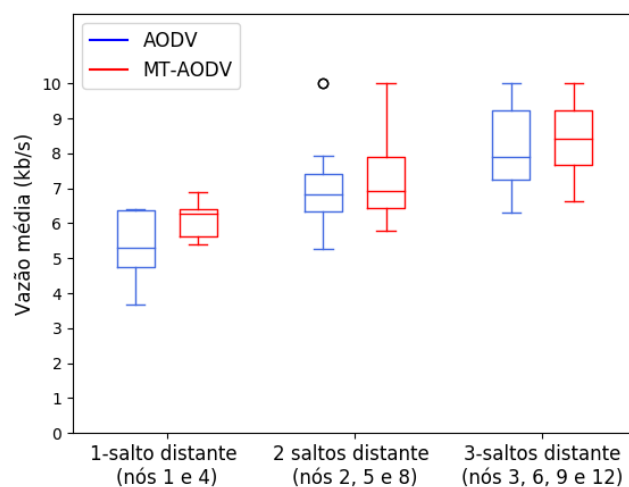


Figura 5.7: Vazão de pacotes de dados recebidos. MT-AODV possui valores mínimos e máximos superiores ao AODV nos 3 cenários.

função da distância ao nó coletor nos cenários simulados. Observa-se que o MT-AODV possui melhor desempenho em todos os cenários, com destaque para o cenário onde as falhas alternadas ocorrem nos vizinhos do nó coletor (Figura 5.8(a)). No MT-AODV, os nós mais distantes, por possuírem rotas alternativas para encaminhamento dos pacotes de dados, conseguem desviar todo o tráfego para a rota ativa, enquanto que, no AODV, as rotas precisam ser recalculadas. Nos outros dois cenários, como pode ser visto nas Figuras 5.8(b) e 5.8(c), o MT-AODV também possui melhor desempenho, mas em menor proporção. Isso se deve ao fato de ter mais caminhos disponíveis para descoberta de rotas,

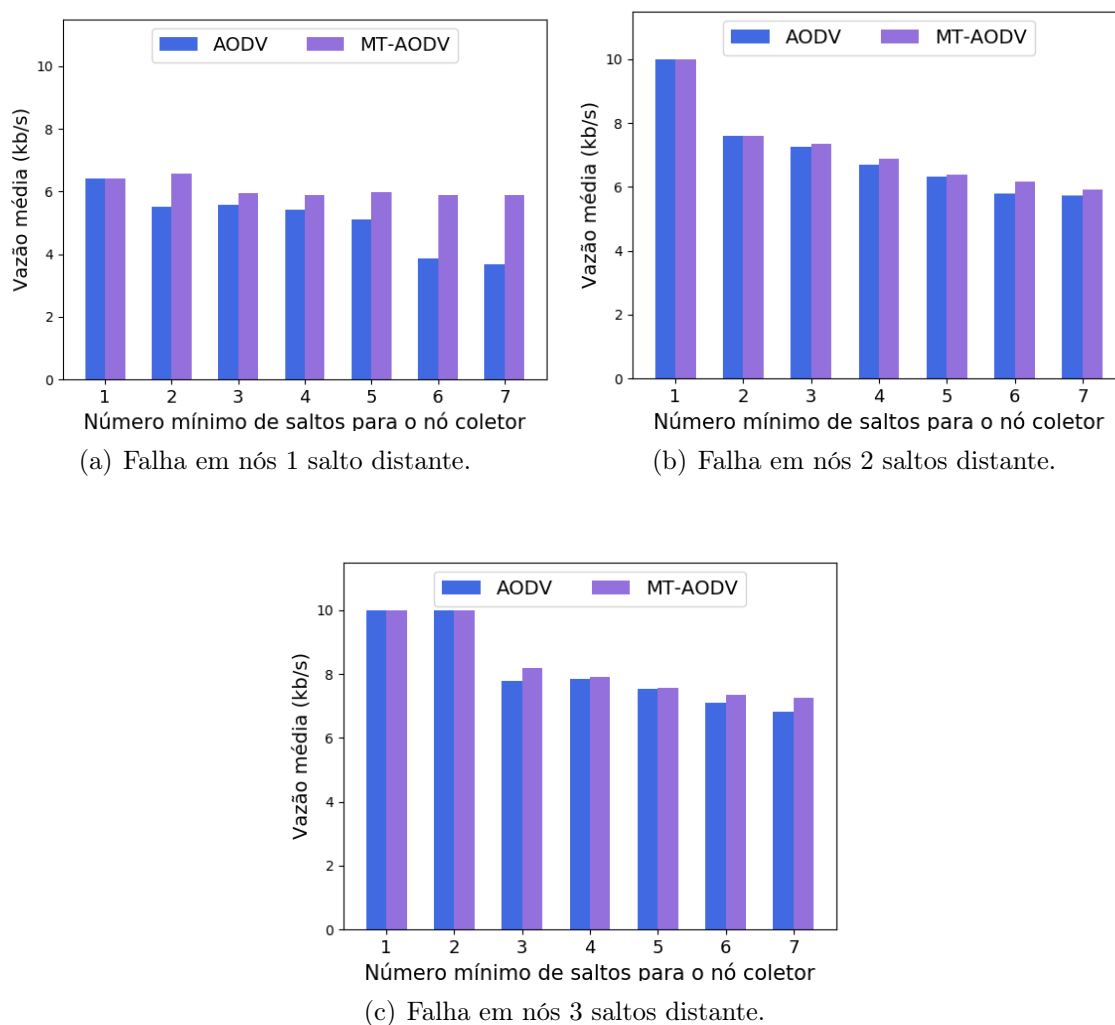


Figura 5.8: Vazão média em função da distância dos nós ao nó coletor para cada cenário. O MT-AODV apresenta melhor desempenho em todos os cenários. (a) Falha alternada nos vizinhos do nó coletor causa maior impacto no desempenho da rede pela limitação de caminhos disponíveis. (b) Falha nos nós a 2 saltos de distância do coletor. Os nós vizinhos não são afetados, atingindo vazão máxima. MT-AODV tem melhor desempenho. (c) Falha nos nós a 3 saltos de distância. Os nós a até 2 saltos do coletor não são impactados.

fazendo com que novas rotas sejam encontradas rapidamente. Além disso, a falha ocorre somente em 1 nó por vez, sendo a falha nos nós vizinhos ocorrendo nos nós alternadamente 1 e 4, nos nós a 2 saltos de distância, nos nós 2, 5 e 8, e nos nós 3, 6, 9 e 12 para 3 saltos de distância. Isso faz com que a probabilidade de uso de outros caminhos pelos nós mais distantes seja maior do que o caminho com o nó em falha.

5.3.2 Posição inicial dos nós aleatória

A segunda parte da avaliação é realizada nos cenários com a posição inicial dos nós aleatória. A Figura 5.9 apresenta o **total de pacotes recebidos** pelo nó coletor durante a simulação. Nos cenários com falha permanente em 1 nó e com falha permanente em 4 nós, o DSDV e o OLSR apresentam melhor desempenho. O MT-AODV supera os demais protocolos nos cenários de falha permanente em 3 nós, mobilidade sem falhas e mobilidade com falhas intermitentes. Para falha permanente em 2 nós, o MT-AODV supera o AODV mas empata com o OLSR e, no cenário com falhas intermitentes, o MT-AODV tem desempenho estatisticamente equivalente ao AODV e ao OLSR. É sabido que nos protocolos proativos, a topologia de rede é conhecida pelos nós. Assim, em cenários fixos a escolha de uma nova rota em caso de uma falha permanente é rapidamente identificada. Dessa forma, esses protocolos possuem vantagem em relação aos protocolos reativos. Ainda assim, o MT-AODV consegue se equiparar a protocolos proativos quanto

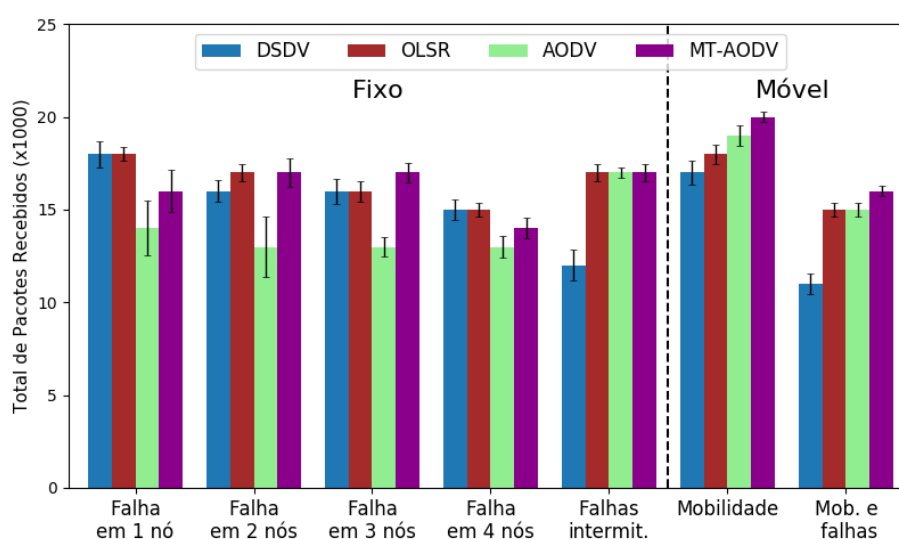


Figura 5.9: Número de pacotes recebidos. O MT-AODV supera os demais protocolos nos cenários com 3 falhas, mobilidade e mobilidade com falhas. A resiliência a falhas do MT-AODV depende da quantidade de rotas encontradas.

ao total de pacotes recebidos nesses cenários devido ao armazenamento de mais de uma rota para o destino.

No cenário fixo com falhas intermitentes, um maior dinamismo na rede é gerado. Para o protocolo DSDV, que é baseado em vetor de distância e é proativo, há certa dificuldade em manter as tabelas atualizadas, uma vez que os enlaces estão sofrendo quedas intermitentemente, e o desempenho do protocolo é prejudicado. Já para o OLSR, que é baseado em estado de enlace, as falhas são rapidamente identificadas e uma nova rota é selecionada para encaminhamento dos pacotes. No AODV, uma nova rota é rapidamente encontrada a cada queda de enlace. O MT-AODV tem desempenho similar ao OLSR e AODV nesse cenário. Apesar de possibilitar o uso de mais de uma rota para o nó transmissor, a dinâmica de falhar um nó por vez, acaba forçando o protocolo a permanecer com uma única rota em sua tabela. Dessa forma, nesse cenário, após a primeira rodada de falhas, o MT-AODV atua de forma similar ao AODV.

No cenário com mobilidade sem falhas, os protocolos reativos se destacam. Devido à não obrigatoriedade de conhecer toda a topologia da rede, esses protocolos encontram mais rapidamente os caminhos até o destino durante o descolamento dos nós. Uma vez que o MT-AODV aloca mais de um caminho, o desempenho nesse cenário é superior. O cenário com mobilidade e falhas intermitentes acumula as características dos dois cenários anteriores. Assim, o desempenho é prejudicado pelas falhas e pelo deslocamento do nós. O MT-AODV possui melhor desempenho nesse cenário devido à mobilidade dos nós. Diferentemente das falhas no cenário fixo, onde sempre as mesmas rotas podem ser encontradas, no cenário móvel, é possível que novas rotas estejam disponíveis no caso de falhas.

A **taxa de pacotes perdidos** representa a razão entre o total de pacotes perdidos e o total de pacotes esperados pelo destino. Matematicamente, a taxa de pacotes perdidos é definida pela Equação 5.1.

$$PLR = \frac{\#Pacotes\ esperados - \#Pacotes\ recebidos}{\#Pacotes\ esperados} \times 100\% \quad (5.1)$$

A Figura 5.10 mostra os resultados para a taxa de pacotes perdidos. Para os cenários fixos, o MT-AODV tem melhor desempenho se comparado ao AODV, nos cenários de falhas permanentes. Esse resultado é consequência da descoberta de mais de uma rota para encaminhamento das mensagens. Para o cenário fixo de falhas intermitentes, o resultado do MT-AODV é estatisticamente equivalente ao do AODV. Isso se deve ao fato do MT-AODV agir como o AODV após a primeira rodada de falhas. Contudo, os protocolos

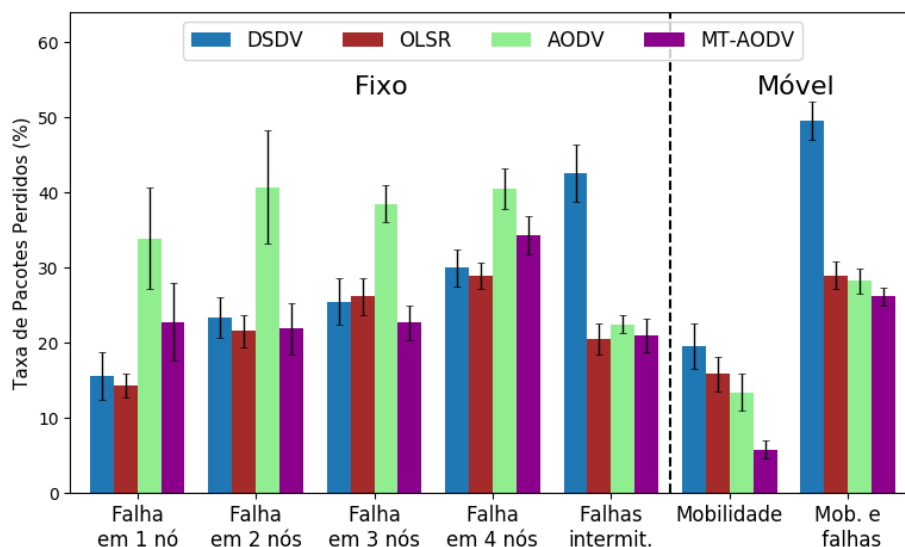


Figura 5.10: Taxa de pacotes perdidos. MT-AODV obtém melhor desempenho comparado ao AODV nas condições de falhas permanentes e mobilidade. Nas demais condições, o resultado é equivalente ao AODV.

proativos têm resultado superior ou similar ao MT-AODV nos cenários fixos de falhas permanentes, pelo fato de conhecerem a topologia da rede e disponibilizarem uma rota rapidamente.

No cenário fixo de falhas intermitentes, o DSDV não consegue atualizar as tabelas de roteamento dos nós rapidamente a cada falha e, por isso, tem resultado próximo a 40% de perda de pacotes, enquanto os demais têm resultados em torno de 20% de perda dos pacotes esperados. Para o cenário com mobilidade sem falhas, o MT-AODV possui desempenho de 6% enquanto o AODV tem 15% dos pacotes esperados perdidos. Dos protocolos proativos, o OLSR tem 17% e o DSDV 20% de perda nesse cenário, pois a dinâmica de alterações da topologia dificulta a convergência desses protocolos. No cenário de mobilidade com falhas intermitentes, os protocolos OLSR, AODV e MT-AODV estão estaticamente equivalentes. A vantagem que o MT-AODV possui com a mobilidade dos nós não é suficiente em condições de falha, considerando o intervalo de confiança calculado.

A Figura 5.11 mostra o **atraso fim-a-fim** médio dos pacotes recebidos pelo nó coletor. Apesar de o MT-AODV depender de menos tempo calculando uma nova rota, o encaminhamento por mais de um caminho pode aumentar o atraso, uma vez que percursos diferentes podem usar rotas de maior latência. O MT-AODV encaminha o tráfego de dados apenas para os caminhos de menor custo, ou seja, menor número de saltos. Porém a distância entre os nós pode variar, causando diferença no tempo de propagação dos pa-

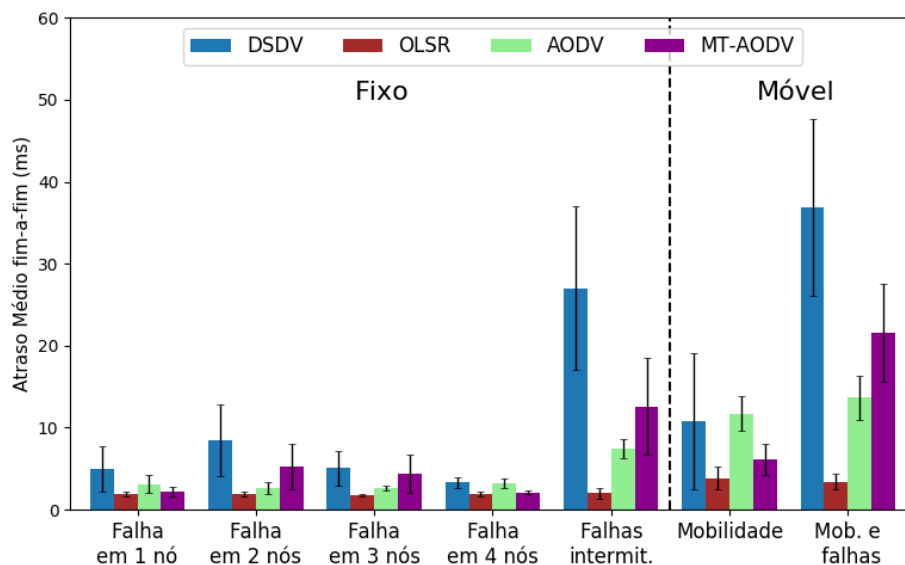


Figura 5.11: Atraso fim-a-fim. O MT-AODV obtém melhor desempenho que o AODV nos cenários de falha em 4 nós e de mobilidade. O OLSR apresenta os melhores resultados nos casos de falhas intermitentes, por ser um protocolo proativo e de estado de enlace.

cotes. Comparado ao AODV, o protocolo proposto tem melhor desempenho nos cenários de falha em 4 nós e mobilidade sem falhas, e é estatisticamente equivalente nos demais cenários, considerando o intervalo de confiança. Isso ocorre devido ao grande número de recuperações de rota necessário em condições mais dinâmicas da rede. O protocolo OLSR apresenta melhores resultados que os demais protocolos. Esse resultado é esperado porque o OLSR é um protocolo proativo, que mantém a topologia da rede sempre atualizada, com rotas disponíveis sempre que elas existirem, não sendo necessário calcular rotas no momento do envio do pacote. Além disso, por ser um protocolo de estado de enlace, o OLSR detecta as falhas rapidamente. Dessa forma, o atraso fim-a-fim tende a ser menor do que o de protocolos reativos como o AODV e o MT-AODV. Mesmo sendo reativo e baseado em vetor de distância, o MT-AODV mantém um atraso fim-a-fim estatisticamente equivalente ou muito próximo ao do OLSR na maioria dos cenários, exceto quando há falhas intermitentes. Nesses casos, os protocolos sob demanda procuram uma nova rota ao perceberem a falha, provavelmente de maior custo, mas não retornam para a rota original após término da falha até que a rota atual expire. Em razão disso, o atraso médio fim-a-fim dos protocolos reativos é maior que o do OLSR.

A métrica de **vazão da rede** mede a quantidade de bits recebidos em média pelo nó coletor em um segundo, enviados por cada nó transmissor. O cálculo da vazão média da rede é definido pela Equação 5.2, em que i é o índice do nó transmissor e n é o número

total de nós transmissores.

$$VM = \frac{\sum_{i=1}^n \frac{\#Bits\ recebidos_i}{Tempo\ do\ último\ pacote\ recebido_i - Tempo\ do\ primeiro\ pacote\ recebido_i}}{n} \quad (5.2)$$

Os resultados são apresentados na Figura 5.12. O gráfico mostra que não há queda significativa de desempenho do MT-AODV na maioria dos cenários. Apesar de existir potencial para reduzir o atraso médio na transferência de dados ao utilizar caminhos distintos, na maioria dos cenários estudados o uso de mais de um caminho para transferência dos dados aumenta ligeiramente o atraso médio fim-a-fim. Ainda assim, a vazão média do MT-AODV é pouco afetada. Nos cenários sem mobilidade, o protocolo alcança resultados similares a alguns dos protocolos comparados. Se comparado especificamente ao AODV, o MT-AODV tem menor vazão no cenário de 4 falhas permanentes, e empata nos demais. Nos cenários de mobilidade sem falhas e com falhas intermitentes, o MT-AODV alcança maior vazão comparado aos demais protocolos. Os resultados obtidos mostram que o MT-AODV é vantajoso em diferentes métrica e condições, tendo destaque nos cenários de mobilidade. Dessa forma, o emprego desse protocolo em operações militares, onde a mobilidade dos combatentes está constantemente presente, pode trazer benefícios no desempenho das aplicações de redes de monitoramento de sinais vitais dos militares em operação de campo.

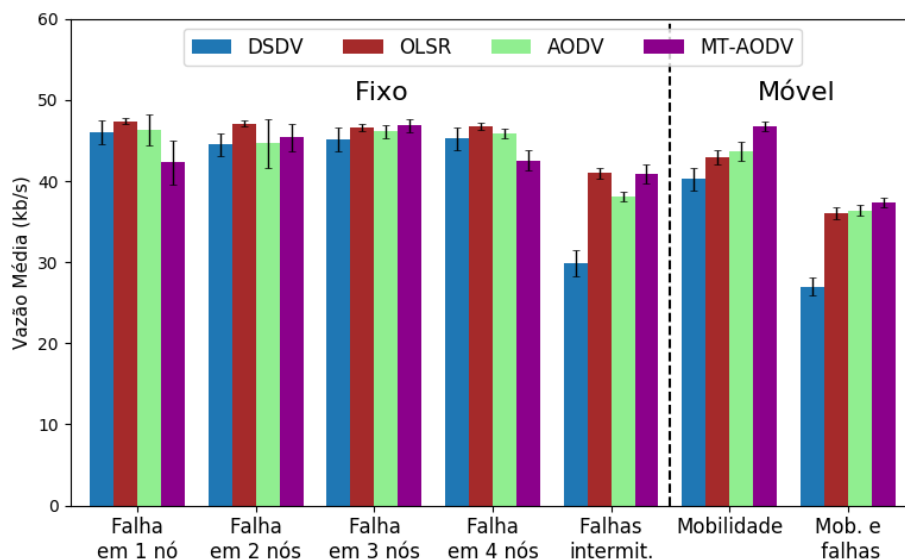


Figura 5.12: Vazão média da rede. MT-AODV supera o AODV nos cenários de falhas intermitentes e mobilidade.

Capítulo 6

Conclusão e Trabalhos Futuros

O uso de protocolos de roteamento multicaminhos em MANETs para aplicações de monitoramento de saúde de militares em operações contribui para aumentar a resiliência da rede em locais desprovidos de infraestrutura. Esta dissertação propôs o MT-AODV, um protocolo reativo resiliente, no qual as rotas são gerenciadas por meio de múltiplas tabelas de roteamento. O MT-AODV evolui o protocolo AODV tradicionalmente usado em MANETs, mantendo a retrocompatibilidade. Para implementação e avaliação, foi utilizado o simulador de redes de eventos discretos *Network Simulator 3* (NS-3). A partir dos códigos-fonte do AODV, a solução proposta foi adaptada com a modificação dos arquivos criados em linguagem C++, responsáveis pelo roteamento dos pacotes e criação e armazenamento das entradas de rotas e tabelas de roteamento. Dessa forma, os métodos que tratam dos processos de descoberta e manutenção de rotas, assim como os métodos de transmissão e encaminhamento de dados do AODV foram transformados em métodos capazes de suportar a criação e o armazenamento de múltiplas rotas voláteis em diferentes tabelas, sendo o número máximo de tabelas configurável, além de permitir o encaminhamento pelas rotas com o menor número de saltos.

O protocolo proposto é avaliado por meio de simulações que representam diversos cenários e são separados em dois experimentos distintos. No primeiro experimento, os nós são alocados em uma topologia em grade e os cenários diversificam-se pela distância dos nós falhantes em relação ao nó coletor de dados. Os resultados evidenciam que o MT-AODV apresenta melhor desempenho que o AODV em relação à proporção de pacotes de dados recebidos, sobrecarga de pacotes de controle, atraso fim-a-fim médio e vazão média. No cenário com falha de nós 1 salto distante do nó coletor, o MT-AODV atinge uma taxa de entrega de pacotes de dados de 62,87%, enquanto AODV atinge 54,75%, transmite 651 mensagens de controle enquanto o AODV envia 1837 mensagens de controle, tem um

atraso médio inferior em 10% em relação ao AODV e uma vazão de 6,07 kb/s contra 5,26 kb/s do AODV.

No segundo experimento, o posicionamento de cada nó é escolhido aleatoriamente, e os cenários distinguem-se pelos tipos e quantidades de falhas variáveis e pela mobilidade configurada. As avaliações mostraram que, em comparação com dois protocolos proativos, DSDV e OLSR, além do protocolo reativo AODV, o MT-AODV consegue melhores resultados nos cenários de mobilidade quanto ao total de pacotes recebidos, taxa de pacotes perdidos e vazão. Na condição de mobilidade sem falhas, o MT-AODV alcança aproximadamente 10% a mais do total de pacotes recebidos e 50% menos perda de pacotes se comparado aos demais protocolos.

Vislumbram-se como trabalhos futuros verificar o comportamento do protocolo em aplicações com taxas de transmissão mais altas, a fim de formar uma rede híbrida para comunicação do combatente, incluindo a transmissão de dados multimídia; avaliar o desempenho em redes mais densas; utilizar modelos reais de mobilidade em ambientes de operações militares, verificar o impacto na qualidade da comunicação ao variar o número máximo de caminhos; e analisar o impacto no desempenho da comunicação quando parte dos nós da rede implementa o MT-AODV e outra parte implementa o AODV.

Referências

- [1] ADRIANO, M. S. *COMANDO E CONTROLE: sua importância para a guerra moderna e para uma força-tarefa no mar*. Monografia (Curso de Estado-Maior para Oficiais Superiores - C-EMOS) — Escola de Guerra Naval, Rio de Janeiro, RJ, Brasil, 2009.
- [2] FRIEDL, K. E. Military applications of soldier physiological monitoring. *Journal of Science and Medicine in Sport*, v. 21, n. 11, p. 1147–1153, 2018. ISSN 1440-2440. 4th International Congress on Soldiers' Physical Performance. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S144024401830255X>>.
- [3] RAHMAN, T.; ULLAH, I.; REHMAN, A. U.; NAQVI, R. A. Notice of violation of iee publication principles: Clustering schemes in manets: Performance evaluation, open challenges, and proposed solutions. *IEEE Access*, v. 8, p. 25135–25158, 2020.
- [4] HARION, W.; FRIEDL, K. E.; BULLER, M. J.; ARANGO, N.; HOYT, R. Evolution of physiological status monitoring for ambulatory military applications. In: *Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities*. [S.l.]: Oxford Univ. Press, 2018. p. 142.
- [5] MATTOS, D. M. F.; FERRAZ, L. H. G.; COSTA, L. H. M. K.; DUARTE, O. C. M. B. Evaluating virtual router performance for a pluralist future internet. In: *Proceedings of the 3rd International Conference on Information and Communication Systems*. New York, NY, USA: Association for Computing Machinery, 2012. (ICICS '12). ISBN 9781450313278.
- [6] CHO, D.-K.; CHANG, C.-W.; TSAI, M.-H.; GERLA, M. Networked medical monitoring in the battlefield. In: *MILCOM 2008 - 2008 IEEE Military Communications Conference*. [S.l.: s.n.], 2008. p. 1–7.
- [7] RAJABHUSHANAM, C.; KATHIRVEL, A. Survey of wireless manet application in battlefield operations. *IJACSA) International Journal of Advanced Computer Science and Applications*, Citeseer, v. 2, n. 1, 2011.
- [8] LUU, B. B.; O'BRIEN, B. J.; BARAN, D. G.; HARDY, R. L. A soldier-robot ad hoc network. In: *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. [S.l.: s.n.], 2007. p. 558–563.
- [9] SILVA, J. da; CAMPOS, J. R. Monitoramento das ações policiais por meio do uso de câmeras de porte individual: uma análise de sua utilização nas atividades operacionais. *Revista Ordem Pública*, v. 8, n. 2, p. 233–253, 2015.
- [10] SANTOS, A. C.; FIRMINO, R. M.; SOTO, J. C.; MEDEIROS, D. S.; MATTOS, D. M.; ALBUQUERQUE, C. V.; SEIXAS, F.; MUCHALUAT-SAADE, D. C.; FERNANDES, N. C. Aplicações em redes de sensores na área da saúde e gerenciamento de dados médicos: tecnologias em ascensão. *Sociedade Brasileira de Computação*, 2020.

- [11] MOVASSAGHI, S.; ABOLHASAN, M.; LIPMAN, J.; SMITH, D.; JAMALIPOUR, A. Wireless Body Area Networks: A Survey. *IEEE Communications Surveys Tutorials*, v. 16, n. 3, p. 1658–1686, 2014.
- [12] RODGERS, M. M.; PAI, V. M.; CONROY, R. S. Recent advances in wearable sensors for health monitoring. *IEEE Sensors Journal*, IEEE, v. 15, n. 6, p. 3119–3126, 2015.
- [13] FERREIRA, V. C. *Agendamento de Transmissões em Redes Corporais Sem Fio Ciente de Movimentos do Corpo Humano*. Tese (Doutorado) — IC/UFF, Niterói, RJ, Brasil, 2021.
- [14] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS. *IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)*. [S.l.], 2005.
- [15] INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS. *IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)*. [S.l.], 2006. 1–320 p.
- [16] FERREIRA, V. C.; CABALLERO, E.; LIMA, R.; BALBI, H.; SEIXAS, F. L.; ALBUQUERQUE, C.; MUCHALUAT-SAADE, D. C. *Redes corporais sem fio e suas aplicações em saúde*. *Sociedade Brasileira de Computação*, 2018.
- [17] MOVASSAGHI, S.; ABOLHASAN, M.; LIPMAN, J. A review of routing protocols in wireless body area networks. *Journal of Networks*, 2013.
- [18] EFFATPARVAR, M.; DEHGHAN, M.; RAHMANI, A. M. A comprehensive survey of energy-aware routing protocols in wireless body area sensor networks. *Journal of medical systems*, Springer, v. 40, n. 9, p. 1–27, 2016.
- [19] NABI, M.; BASTEN, T.; GEILEN, M.; BLAGOJEVIC, M.; HENDRIKS, T. A robust protocol stack for multi-hop wireless body area networks with transmit power adaptation. In: . New York, NY, USA: Association for Computing Machinery, 2010. ISBN 9781450300292. Disponível em: <<https://doi.org/10.1145/2221924.2221941>>.
- [20] KHAN, Z. A.; SIVAKUMAR, S.; PHILLIPS, W.; ASLAM, N. A new patient monitoring framework and energy-aware peering routing protocol (epr) for body area network communication. *Journal of Ambient Intelligence and Humanized Computing*, Springer, v. 5, n. 3, p. 409–423, 2014.
- [21] TAKAHASHI, D.; XIAO, Y.; HU, F.; CHEN, J.; SUN, Y. Temperature-aware routing for telemedicine applications in embedded biomedical sensor networks. *EURASIP Journal on Wireless Communications and Networking*, Springer, v. 2008, p. 1–11, 2007.
- [22] ULLAH, S.; HIGGINS, H.; BRAEM, B.; LATRE, B.; BLONDIA, C.; MOERMAN, I.; SALEEM, S.; RAHMAN, Z.; KWAK, K. S. A comprehensive survey of wireless body area networks. *Journal of medical systems*, Springer, v. 36, n. 3, p. 1065–1094, 2012.

- [23] HE, P.; LI, X.; YAN, L.; YANG, S.; ZHANG, B. Performance analysis of wban based on aodv and dsdv routing protocols. In: IEEE. *2015 2nd International Symposium on Future Information and Communication Technologies for Ubiquitous HealthCare (UbiHealthTech)*. [S.l.], 2015. p. 1–4.
- [24] TIWARI, R.; SHRIVASTAVA, S.; DAS, S. Performance analysis of mobile patient network using aodv and dsr routing algorithms. In: IEEE. *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCCE)*. [S.l.], 2014. p. 1–6.
- [25] PERKINS, C. E.; BHAGWAT, P. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM computer communication review*, ACM New York, NY, USA, v. 24, n. 4, p. 234–244, 1994.
- [26] JOHNSON, D. B. The dynamic source routing protocol for mobile ad hoc networks. *IETF Internet Draft*, <https://datatracker.ietf.org/doc/html/draft-ietf-manet-dsr-04>, 2000.
- [27] JOHNSON, D. B.; MALTZ, D. A.; HU, Y.-C. *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*. 2007. Internet RFC 4728. Disponível em: <<https://www.ietf.org/rfc/rfc4728.txt>>.
- [28] JOHNSON, D. B.; MALTZ, D. A.; BROCH, J. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, v. 5, n. 1, p. 139–172, 2001.
- [29] PERKINS, C. E.; BELDING-ROYER, E. M.; DAS, S. R. *Ad hoc On-Demand Distance Vector (AODV) Routing*. 2003. Internet RFC 3561. Disponível em: <<https://www.ietf.org/rfc/rfc3561.txt>>.
- [30] PERKINS, C. E.; ROYER, E. M. Ad-hoc on-demand distance vector routing. In: IEEE. *Proceedings WMCSA '99. Second IEEE Workshop on Mobile Computing Systems and Applications*. [S.l.], 1999. p. 90–100.
- [31] DAS, S. R.; PERKINS, C. E.; ROYER, E. M. Performance comparison of two on-demand routing protocols for ad hoc networks. In: IEEE. *Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No. 00CH37064)*. [S.l.], 2000. v. 1, p. 3–12.
- [32] PERKINS, C. E.; RATLIFF, S.; DOWDELL, J.; STEENBRINK, L.; MERCIECA, V. *Ad Hoc On-demand Distance Vector Version 2 (AODVv2) Routing*. [S.l.], 2016. Work in Progress. Disponível em: <<https://datatracker.ietf.org/doc/html/draft-ietf-manet-aodvv2-13>>.
- [33] CLAUSEN, T. H.; JACQUET, P. *Optimized Link State Routing Protocol (OLSR)*. 2003. Internet RFC 3626. Disponível em: <<https://www.ietf.org/rfc/rfc3626.txt>>.
- [34] JACQUET, P.; MUHLETHALER, P.; CLAUSEN, T.; LAOUITI, A.; QAYYUM, A.; VIENNOT, L. Optimized link state routing protocol for ad hoc networks. In: IEEE. *Proceedings. IEEE International Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century*. [S.l.], 2001. p. 62–68.

- [35] CLAUSEN, T. H.; DEARLOVE, C.; JACQUET, P.; HERBERG, U. *The Optimized Link State Routing Protocol Version 2*. 2014. Internet RFC 7181. Disponível em: <<https://www.ietf.org/rfc/rfc7181.txt>>.
- [36] MOHAPATRA, S.; KANUNGO, P. Performance analysis of aodv, dsr, olsr and dsdv routing protocols using ns2 simulator. *Procedia Engineering*, Elsevier, v. 30, p. 69–76, 2012.
- [37] TANENBAUM, A. S.; WETHERALL, D. *Redes de Computadores*. trad. 5 ed. Rio de Janeiro: Pearson, 2011.
- [38] MUELLER, S.; TSANG, R. P.; GHOSAL, D. Multipath routing in mobile ad hoc networks: Issues and challenges. In: CALZAROSSA, M. C.; GELENBE, E. (Ed.). *Performance Tools and Applications to Networked Systems*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 209–234. ISBN 978-3-540-24663-3.
- [39] TSAI, J.; MOORS, T. A review of multipath routing protocols: From wireless ad hoc to mesh networks. In: CITESEER. *ACoRN early career researcher workshop on wireless multihop networking*. [S.l.], 2006. v. 30.
- [40] AYANOGLU, E.; CHIH-LIN, I.; GITLIN, R. D.; MAZO, J. E. Diversity coding for transparent self-healing and fault-tolerant communication networks. *IEEE Transactions on communications*, IEEE, v. 41, n. 11, p. 1677–1686, 1993.
- [41] WU, K.; HARMS, J. Performance study of a multipath routing method for wireless mobile ad hoc networks. In: IEEE. *MASCOTS 2001, Proceedings Ninth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*. [S.l.], 2001. p. 99–107.
- [42] PEARLMAN, M. R.; HAAS, Z. J.; SHOLANDER, P.; TABRIZI, S. S. On the impact of alternate path routing for load balancing in mobile ad hoc networks. In: IEEE. *2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No. 00EX444)*. [S.l.], 2000. p. 3–10.
- [43] SAHA, D.; TOY, S.; BANDYOPADHYAY, S.; UEDA, T.; TANAKA, S. An adaptive framework for multipath routing via maximally zone-disjoint shortest paths in ad hoc wireless networks with directional antenna. In: IEEE. *GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489)*. [S.l.], 2003. v. 1, p. 226–230.
- [44] BRAEM, B.; CLEYN, P. D.; BLONDIA, C. Supporting mobility in body sensor networks. In: IEEE. *2010 International Conference on Body Sensor Networks*. [S.l.], 2010. p. 52–55.
- [45] TSIRIGOS, A.; HAAS, Z. J. Multipath routing in the presence of frequent topological changes. *IEEE Communications Magazine*, IEEE, v. 39, n. 11, p. 132–138, 2001.
- [46] KRISHNAN, R.; SILVESTER, J. A. Choice of allocation granularity in multipath source routing schemes. In: IEEE. *IEEE INFOCOM'93 The Conference on Computer Communications, Proceedings*. [S.l.], 1993. p. 322–329.

- [47] KUROSE, J. F.; W., R. K. *Redes de Computadores e a Internet: Uma Abordagem Top-Down*. trad. 6 ed. [S.l.]: Pearson, 2013.
- [48] BAGATELLI, R. *Projeto Formal de Protocolos de Acesso ao Meio e de Roteamento para Redes Ad-Hoc*. Dissertação (Mestrado) — COPPE/UFRJ, Rio de Janeiro, RJ, Brasil, 2003.
- [49] NASIPURI, A.; DAS, S. R. On-demand multipath routing for mobile ad hoc networks. In: IEEE. *Proceedings Eight International Conference on Computer Communications and Networks (Cat. No. 99EX370)*. [S.l.], 1999. p. 64–70.
- [50] LEE, S.-J.; GERLA, M. Split multipath routing with maximally disjoint paths in ad hoc networks. In: IEEE. *ICC 2001. IEEE international conference on communications. Conference record (Cat. No. 01CH37240)*. [S.l.], 2001. v. 10, p. 3201–3205.
- [51] MARINA, M. K.; DAS, S. R. On-demand multipath distance vector routing in ad hoc networks. In: IEEE. *Proceedings Ninth International Conference on Network Protocols. ICNP 2001*. [S.l.], 2001. p. 14–23.
- [52] YUAN, Y.; CHEN, H.; JIA, M. An optimized ad-hoc on-demand multipath distance vector(aomdv) routing protocol. In: *2005 Asia-Pacific Conference on Communications*. [S.l.: s.n.], 2005. p. 569–573.
- [53] YI, J.; ADNANE, A.; DAVID, S.; PARREIN, B. Multipath optimized link state routing for mobile ad hoc networks. *Ad hoc networks*, Elsevier, v. 9, n. 1, p. 28–47, 2011.
- [54] YI, J.; PARREIN, B. *Multipath Extension for the Optimized Link State Routing Protocol Version 2 (OLSRv2)*. 2017. Internet RFC 8218. Disponível em: <<https://www.ietf.org/rfc/rfc8218.txt>>.
- [55] TSENG, C. H. LBMR: Load-Balanced Multipath Routing for wireless data-intensive transmission in real-time medical monitoring. *International journal of environmental research and public health*, Multidisciplinary Digital Publishing Institute, v. 13, n. 6, p. 547, 2016.
- [56] BIRGANI, Y. G.; JAVAN, N. T.; TOURANI, M. Mobility enhancement of patients body monitoring based on wban with multipath routing. In: *2014 2nd International Conference on Information and Communication Technology (ICoICT)*. [S.l.: s.n.], 2014. p. 127–132.
- [57] FIRMINO, R. M.; MATTOS, D. M.; MEDEIROS, D. S. MT-AODV: Provendo resiliência em redes ad-hoc móveis militares através de múltiplas tabelas de roteamento sob demanda. In: *XXXIX Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT)*. [S.l.: s.n.], 2021. p. 1–5.
- [58] STREET, M.; SZCZUCKI, F. Wireless communications architecture (land): scenarios, requirements and operational view. *NATO C3 Agency, Tech. Note*, v. 1246, 2006.
- [59] FIRMINO, R. M.; VELLOSO, P. B.; MATTOS, D. M.; MEDEIROS, D. S. MT-AODV: Resilient communication in military mobile ad-hoc networks through on-demand multiple routing tables. In: IEEE. *5th Conference on Cloud and Internet of Things (CIoT)*. [S.l.], 2022. To be published.

-
- [60] FOUNDATION N.S. et al. *Network Simulator NS-3*. Disponível em: <<http://www.nsnam.org>>. Acesso em: 30/09/2021.
- [61] RILEY, G. F.; HENDERSON, T. R. The ns-3 network simulator. In: *Modeling and tools for network simulation*. [S.l.]: Springer, 2010. p. 15–34.
- [62] FOUNDATION N.S. et al. *Network Simulator NS-3 Documentation*. Disponível em: <<https://www.nsnam.org/docs/release/3.30/doxygen/index.html>>. Acesso em: 30/09/2021.