JOILSON ALVES JUNIOR

UM PROTOCOLO DE ROTEAMENTO RESISTENTE A ATAQUES *BLACKHOLE* SEM DETECÇÃO DE NÓS MALICIOSOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.
Orientador: Prof. Dr. Luiz Carlos Pessoa Albini

CURITIBA

2012

JOILSON ALVES JUNIOR

UM PROTOCOLO DE ROTEAMENTO RESISTENTE A ATAQUES *BLACKHOLE* SEM DETECÇÃO DE NÓS MALICIOSOS

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas, Universidade Federal do Paraná.
Orientador: Prof. Dr. Luiz Carlos Pessoa Albini

CURITIBA

2012

RESUMO

Uma rede ad hoc móvel (MANET) é uma rede sem fio que não necessita de infra-estrutura pré-existente. Nas MANETS o roteamento é uma questão complexa e deve ser estabelecido de maneira distribuída e auto-organizada. Os protocolos de roteamento utilizados nestas redes devem suportar a topologia dinâmica e a falta de operações centralizadas, garantindo a entrega dos pacotes com pequena sobrecarga e atraso. Em geral, nestas redes, os pacotes podem ser descartadas pelas seguintes razões: congestionamento, mobilidade, estouro de pilha, quebras de enlaces e ataques de nós maliciosos. Um ataque frequentemente realizado em redes ad hoc é o *blackhole*. Este tipo de ataque se caracteriza quando um ou vários nós descartam indiscriminadamente todos os pacotes de dados que passam por eles. Tal ataque pode ter um efeito destrutivo na rede, interrompendo totalmente seu funcionamento. Este trabalho apresenta um protocolo cujo objetivo é reduzir os efeitos dos descartes de pacotes causados por ataques *blackhole* em redes ad hoc. Para tanto, combina um esquema de partilha de informações baseado no teorema chinês do resto e roteamento multi-caminhos. O protocolo proposto pode evitar que nós *blackhole* prejudiquem o fluxo de dados entre dois nós, sem qualquer conhecimento prévio sobre o comportamento do nó atacante. Resultados de simulações indicam que o protocolo proposto fornece equilíbrio entre segurança e desempenho no roteamento diante de ataques de nós *blackhole*. Comparações com os protocolos *Ad hoc On Demand Distance Vector* (AODV) e *Ad hoc On-demand Distance Vector Backup Routing* (AOMDV) mostram que em cenários nos quais mais de 40% dos nós da rede são atacantes, a taxa de entrega apresenta ganhos superiores a 50%. Neste mesmo cenário, ocorre uma redução de 52% na perda de pacotes de dados resultantes de ataques *backhole*, e a vazão dos pacotes de dados é até sete vezes maior em relação aos protocolos que estão sendo comparados.

Palavras-chave: MANETs, multi-caminhos,*blackhole*, teorema chinês do resto.

SUMÁRIO

1 INTRODUÇÃO **1**

2 ROTEAMENTO EM REDES AD HOC **4**

2.1 *Ad-hoc On-demand Distance Vector* 5

2.1.1 Descoberta de rota 6

2.1.2 Manutenção das rotas 7

2.2 *Ad hoc On-demand Multipath Distance Vector Routing* 7

2.2.1 Descoberta de rota 7

2.2.2 Manutenção de rota 8

2.2.3 Liberdade de laço 8

2.2.4 Caminhos disjuntos 9

2.3 Protocolos de roteamento multi-caminhos 11

3 ATAQUE *BLACKHOLE* **13**

3.1 Trabalhos relacionados a ataques de *blackhole* 14

3.1.1 Tabela comparativa entre os trabalhos relacionados 17

4 TEORIA DOS NÚMEROS **19**

4.1 Algoritmo euclidiano 19

4.2 Algoritmo euclidiano estendido 19

4.3 Fatoração única 20

4.4 Aritmética modular 21

4.4.1 Aritmética modular 22

4.5 Sistemas de congruência 23

4.6 Teorema chinês do resto 24

5 PROTOCOLO DE ROTEAMENTO RESISTENTE A ATAQUES *BLACKHOLE* EM REDES AD HOC MÓVEIS SEM DETECÇÃO DE

NÓS MALICIOSOS **26**

5.1 Modificações realizadas no AOMDV para construção do PRAB 27

5.2 Divisão e remontagem das informações 28

5.2.1 Aplicação do algoritmo chinês do resto para divisão e reconstrução da informação 29

5.3 Sobrecarga extra dos dados transmitidos na rede 30

6 AVALIAÇÃO DO PROTOCOLO PROPOSTO **31**

6.1 Ambiente de Simulação 31

6.2 Métricas 32

6.3 Resultados e Análises 33

6.3.1 Ambiente de rede hostil - Cenário 1 35

6.3.2 Variando a densidade da rede - cenário 2 56

6.3.3 Variando o tráfego de mensagens na rede - cenário 3 65

6.4 Síntese dos resultados e análises 70

7 CONCLUSÃO **72**

BIBLIOGRAFIA **79**

LISTA DE FIGURAS

2.1 Criando caminhos disjuntos 10

3.1 Ataque *blackhole* no AOMDV 14

6.1 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós. 37

6.2 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós. 38

6.3 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós. 38

6.4 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 50 nós. 39

6.5 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 75 nós. 39

6.6 Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 100 nós. 40

6.7 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós. 41

6.8 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós. 41

6.9 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós. 42

6.10 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 50 nós. 42
6.11 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 75 nós. 43
6.12 Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 100 nós. 43
6.13 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós. 45
6.14 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós. 45
6.15 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós. 46
6.16 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 50 nós. 46
6.17 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 75 nós. 47
6.18 Quantidade de dados transferidos versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 100 nós. 47
6.19 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós. 49
6.20 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós. 49
6.21 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós. 50
6.22 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 50 nós. 50

6.23 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 75 nós. 51
6.24 Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 100 nós. 51
6.25 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós. 53
6.26 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós. 53
6.27 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós. 54
6.28 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 50 nós. 54
6.29 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 75 nós. 55
6.30 Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 100 nós. 55
6.31 Taxa de entrega dos dados versus densidade da rede - 20% de nós *blackhole* na rede. 57
6.32 Taxa de entrega dos dados versus densidade da rede - 40% de nós *blackhole* na rede. 58
6.33 Sobrecarga versus densidade da rede - 20% de nós *blackhole* na rede. 60
6.34 Sobrecarga versus densidade da rede - 40% de nós *blackhole* na rede. 61
6.35 Quantidade de pacotes de dados descartados por nós *blackhole* versus densidade da rede - 20% de nós *blackhole* na rede. 63
6.36 Quantidade de pacotes de dados descartados por nós *blackhole* versus densidade da rede - 40% de nós *blackhole* na rede. 64
6.37 Taxa de entrega dos dados versus trafego da rede - 20% de nós *blackhole* na rede. 65

6.38 Taxa de entrega dos dados versus trafego da rede - 40% de nós *blackhole* na rede. 66
6.39 Sobrecarga versus trafego da rede - 20% de nós *blackhole* na rede. 67
6.40 Sobrecarga versus trafego da rede - 40% de nós *blackhole* na rede. 67
6.41 Quantidade de pacotes descartados versus trafego da rede - 20% de nós *blackhole* na rede. 68
6.42 Quantidade de pacotes descartados versus trafego da rede - 40% de nós *blackhole* na rede. 69

LISTA DE TABELAS

2.1 Tabela de roteamento do protocolo AOMDV 9

2.2 Tabela comparativa entre protocolos de roteamento multi-caminhos 12

3.1 Tabela comparativa entre tipos de ataques *blackhole* 17

4.1 Divisões do algoritmo euclidiano estendido 20

5.1 Tabela com exemplos da sobrecarga extra de pacotes transmitidos na rede. 30

6.1 Parâmetros de simulação do cenário 1 34

6.2 Parâmetros de simulação do cenário 2 34

6.3 Parâmetros de simulação do cenário 3 35

LISTA DE ABREVIATURAS E SIGLAS

ABM	*Anti-Blackhole Mechanism*
	Mecanismo Anti-Buraco Negro
AODV	*Ad hoc On Demand Distance Vector*
	Vetor de Distância Ad Hoc Sob Demanda
AODV-BR	*Ad hoc On-demand Distance Vector Backup Routes*
	Vetor de Distância Ad Hoc Sob Demanda com Rotas de Backup
AOMDV	*Ad hoc On-demand Multipath Distance Vector*
	Vetor de Distância Multi-Caminhos Ad Hoc Sob Demanda
APR	*Alternate Path Routing*
	Caminho Alternativo de Roteamento
CBR	*Constant Bit Rate*
	Taxa de Bit Constante
CHAMP	*Caching Multipath Routing Protocol*
	Protocolo de Roteamento Multicaminhos Com Armazenamento
DSDV	*Destination Sequenced Distance Vector*
	Vetor de Distância Com Destino Sequênciado
DSR	*Dynamic Source Routing*
	Roteamento Dinâmico Pela Fonte
IEEE	*Institute of Electrical and Electronics Engineers*
	Instituto de Engenharia Elétrica e Eletrônica
ID	*Unique Identifier*
	Identificador Único
IDS	*Intrusion Detection System*
	Sistema de Detecção de Intrusão
MAC	*Medium Access Control*

	Controle de Acesso ao Meio
MDC	*Maximum Common Divisor*
	Máximo Divisor Comum
MANET	*Mobile Ad Hoc Network*
	Rede Ad Hoc Móvel
MP-DSR	*Multi-path Dynamic Source Routing*
	Roteamento Dinâmico Pela Fonte Multi-Caminhos
MSR	*Multipath Source Routing*
	Roteamento na Fonte Multi-Caminhos
NAM	*Network Animator*
	Animador de Rede
NS	*Network Simulator*
	Simulador de Rede
OTCL	*Object Tool Command Language*
	Ferramenta Orientada a Objeto Para Linguagem de Comandos
RERR	*Route Error*
	Erro de Rota
RREQ	*Route Request*
	Requisição de Rota
RREP	*Route Reply*
	Resposta de Rota
RTS	*Request to Send*
	Requisição de Envio
SMR	*Split Multipath Routing*
	Divisão de Roteamento Multi-Caminhos
TCP	*Transmission Control Protocol*
	Protocolo de Controle de Transmissões
TORA	*Temporally Ordered Routing Algorithm*

	Algoritmo de Roteamento Temporariamente Ordenado
UDP	*User Datagram Protocol*
	Protocolo de Datagrama de Usuário

CAPÍTULO 1

INTRODUÇÃO

Redes ad hoc móveis, também conhecidas como MANETs, abreviação para *Mobile Ad Hoc Networks*, são redes sem fio que podem ser construídas em qualquer lugar, pois independem da existência de infra-estrutura fixa [1]. As unidades de tais redes são, em sua maioria, pequenas, portáteis, alimentadas por baterias e se comunicam umas com as outras através de sinais de rádio.

Como o alcance dos sinais de rádio é limitado, cada nó só pode se comunicar diretamente com outros nós que estiverem dentro do raio de alcance de seus sinais. Contudo, pode existir a necessidade de um nó transmitir informações para outros nós que estão além do seu raio de alcance. Para isso, os nós devem cooperar agindo como roteadores e repassando as informações do nó origem ao nó destino [2].

Devido ao fato das unidades serem móveis, a topologia da rede pode mudar imprevisivelmente. Com efeito, as rotas estabelecidas inicialmente podem se tornar obsoletas, devendo ser recalculadas. Desta forma, o roteamento em redes ad hoc precisa usar protocolos distribuídos que calculem múltiplas rotas livres de laços e que mantenham uma baixa sobrecarga de comunicação [3].

Os protocolos tradicionais para redes fixas consomem uma quantidade significativa de banda, precisam de grande poder de processamento das unidades e não agem rapidamente em caso de mudanças de topologia [1]. Como as unidades das MANETs normalmente têm baixo poder de processamento, possuem interfaces de rede com restrições de desempenho e necessitam de cálculos rápidos de novas rotas em caso de mudança de topologia, os protocolos tradicionais podem tornar-se inadequados [2]. Isto faz do roteamento em redes ad hoc um grande desafio.

Outro desafio em redes ad hoc está relacionado à segurança dos nós. Essas redes possuem vulnerabilidades associadas principalmente à utilização do ar como meio de comu-

nicação, à ausência de infra-estrutura e ao encaminhamento colaborativo das mensagens [4]. Neste contexto, além dos ataques convencionais às redes sem fio, a comunicação colaborativa possibilita novas ameaças de segurança e a ausência de infra-estrutura dificulta a criação de mecanismos de defesa [4]. Dessa forma, os ataques de nós maliciosos podem interromper o funcionamento da rede e causar impacto na disponibilidade dos recursos e das informações. Os ataques podem ser categorizados em duas classes: ataques passivos e ataques ativos [5]. Os ataques passivos não afetam o funcionamento da rede, sendo caracterizados apenas pela espionagem dos dados. Por outro lado, os ataques ativos são aqueles em que o atacante altera, descarta ou inviabiliza o uso dos dados que estão sendo transmitidos. Um ataque ativo comumente realizado sob redes ad hoc é o *blackhole* [4, 6, 7, 8, 9, 10, 11, 12, 13, 14].

O *blackhole* é um tipo de ataque de negação de serviço cujo objetivo é interromper o funcionamento da rede. O mesmo se caracteriza quando um ou vários nós descartam deliberadamente os pacotes que passam por eles. Um nó *blackhole* pode se aproveitar da vulnerabilidade dos algoritmos de roteamento cooperativos e, através do envio de pacotes de roteamento falsos, rotear para si mesmo todos os pacotes de dados destinados a outro nó visando descartá-los. Ainda, um nó *blackhole* pode não interferir no processo de estabelecimento das rotas e somente descartar pacotes de dados que passam por ele [4].

Este trabalho apresenta um protocolo para reduzir o impacto do descarte de pacotes em redes ad hoc causados por ataques do tipo *blackhole*. Este protocolo combina um esquema de partilha de informações baseado no teorema chinês do resto e um protocolo de roteamento multi-caminhos modificado.

O protocolo proposto consiste em dividir a informação original em n partes e transmití-las de um nó de origem para um nó de destino na rede. Para reconstruir a informação original, um nó deve obter t partes, com $t \leq n$. Qualquer tentativa de reconstruir a informação com menos de t partes deve falhar.

O esquema de partilha de informações baseado no teorema chinês do resto é combinado com uma versão modificada de um protocolo de roteamento multi-caminhos. Nesta nova

versão, o protocolo de roteamento constrói várias rotas entre a origem e o destino, e usa todas elas simultaneamente para transmitir as partes da informação. Esta técnica garante que as n partes não viajarão entre a origem e o destino por um único caminho.

A combinação do esquema de partilha de informações com o roteamento multi-caminhos é usada para construir um protocolo de roteamento resistente a ataques de nós *blackhole*. Assim, evita-se que esses nós prejudiquem o fluxo dos dados entre dois nós quaisquer, sem o conhecimento prévio sobre o comportamento do nó atacante.

Esta dissertação está dividida em sete capítulos. O capítulo 2 descreve o roteamento em redes ad hoc. O capítulo 3 descreve o ataque *blackhole*. O capítulo 4 apresenta os conceitos matemáticos da teoria dos números e do teorema chinês do resto. O capítulo 5 apresenta um protocolo de roteamento resistente a ataques *blackhole* em redes ad hoc móveis. O capítulo 6 apresenta a avaliação do protocolo proposto. O capítulo 7 apresenta a conclusão.

CAPÍTULO 2

ROTEAMENTO EM REDES AD HOC

Nas redes ad hoc, os pacotes são encaminhados através de vários nós até chegarem ao destino. Este tipo de encaminhamento de mensagens também é conhecido por múltiplos saltos [3]. O encaminhamento cooperativo dos pacotes através dos múltiplos saltos faz do roteamento um serviço fundamental para o funcionamento destas redes. Tal serviço é controlado por um protocolo de roteamento, que é o responsável por descobrir e manter as rotas entre os nós de origem e destino [2]. Os protocolos de roteamento normalmente são classificados em duas classes principais:

- Proativos;
- Reativos.

Os protocolos proativos mantêm informações sobre a topologia da rede continuamente atualizadas em suas tabelas de roteamento, independente do uso das rotas armazenadas [15]. Quando um cliente necessita enviar uma mensagem na rede, ele já sabe previamente qual a rota a ser seguida. Tais protocolos podem ter alta sobrecarga de mensagens de controle, pois para manter as tabelas de roteamento atualizadas, mensagens de controle são periodicamente enviadas para todos os nós. O protocolo *Destination Sequenced Distance Vector* (DSDV) [15] é um exemplo de protocolo proativo.

Os protocolos reativos não mantêm informações de roteamento atualizadas, eles descobrem rotas apenas quando um nó de origem precisa transmitir pacotes de dados para um nó de destino [16, 17]. Quando uma origem quer enviar uma mensagem para um destino, inicia-se um processo de descoberta de rota, normalmente por inundação. Se o destino é alcançado, uma mensagem de resposta é enviada para origem. Quando a rota é estabelecida, ela é mantida na tabela de roteamento dos nós até que o destino se torne inalcançável, ou a origem não deseje mais a rota. Tais protocolos apresentam baixa

sobrecarga de mensagens de controle, embora aumentem a latência do procedimento de descoberta de rotas. O protocolo *Ad-hoc On-demand Distance Vector*(AODV) [16] é um exemplo de protocolo reativo.

O procedimento de descoberta de rotas pode resultar na formação de uma ou mais rotas entre um nó de origem e um nó de destino. Os protocolos que descobrem apenas uma rota, como o AODV, são classificados como protocolos de rota única ou caminho único. Já os protocolos que descobrem mais de uma rota, como o *Ad hoc On-demand Multipath Distance Vector Routing* (AOMDV) [17, 18], são classificados como protocolos de múltiplas rotas.

Para a realização deste trabalho, o protocolo de roteamento multi-caminhos escolhido foi o AOMDV [17, 18]. Este protocolo foi selecionado por possuir características técnicas que vão ao encontro dos objetivos deste estudo, tais como: criação de rotas totalmente disjuntas e livres de laço entre dois nós quaisquer; a origem não precisa conhecer a rota completa para o destino. As seções 2.1 e 2.2 descrevem com detalhes os protocolos de roteamento AODV, AOMDV e apresenta outros importantes protocolos tratados pela literatura.

2.1 *Ad-hoc On-demand Distance Vector*

O *Ad-hoc On-demand Distance Vector* (AODV) [16] foi projetado para o uso em redes ad hoc que possuam desde dezenas até milhares de nós móveis. O objetivo principal do protocolo é se adaptar rápida e dinamicamente às variações das condições dos enlaces da rede, descobrindo rotas de forma a se evitar o desperdício de banda e minimizar o uso de memória e processamento nos nós que atuam como roteadores.

O AODV é um protocolo que atua sob demanda, isto é, procura por rotas somente quando elas são realmente necessárias, e o faz através um mecanismo de descoberta de rotas. Cada nó possui em sua tabela de rotemento somente informações sobre o próximo salto para o qual a mensagem deve ser enviada para chegar ao destino. Desta forma, quando o nó K quer enviar uma mensagem para o nó J, ele verifica em sua tabela de roteamento qual é o próximo salto para se chegar ao nó J, e envia a mensagem para o nó

que for o próximo salto. Caso este nó não seja o J(destino), ele repete o processo até que a mensagem chegue ao destino. Quando a origem não tem próximo salto para o destino desejado, ela executa o processo de descoberta de rota.

2.1.1 Descoberta de rota

O AODV constrói rotas através de mensagens de requisição de rotas *Route Request* (RREQ) e respostas de rota *Route Reply* (RREP). Quando um nó origem necessita enviar uma mensagem de dados para um nó que ele ainda não conhece a rota, uma mensagem de RREQ é enviada em *broadcast* através da rede. Os nós que recebem esta mensagem atualizam suas tabelas de roteamento, adicionando uma entrada para informar que para chegar à origem, basta enviar a mensagem para o nó que acabou de enviar a RREQ. Os nós mantêm controle da origem da RREQ e do identificador de *broadcast*. Se eles receberem uma mensagem RREQ já processada, a mensagem é simplesmente descartada.

Um nó que recebe uma mensagem de RREQ pode enviar uma mensagem de RREP para a origem se ele é o destinatário, ou se ele conhece uma rota para o destino. Esta mensagem de RREP é enviada em *unicast* pelo caminho reverso criado pelo RREQ. Como a mensagem de RREP deve ser propagada até a origem, os nós atualizam suas tabelas de roteamento, adicionando uma entrada para informar que para chegar no destino original da RREQ (que agora é origem da RREP), basta enviar a mensagem para o nó que acabou de enviar a RREP. Quando o nó de origem receber a RREP, ele pode então transmitir pacotes de dados para o destinatário, simplesmente encaminhando mensagem para o nó que entregou a RREP.

Se a origem receber outra mensagem de RREP vinda de um nó do qual já se sabe a rota, porém contendo uma rota mais atual, ou passando por menos nós intermediários, ela pode atualizar sua tabela de roteamento para aquele destino, e utilizar a nova rota para transmitir dados.

2.1.2 Manutenção das rotas

A movimentação de um nó pode provocar a queda de um enlace que esta sendo utilizado. Nesta situação, o nó que detectou a quebra envia uma mensagem de *Route Error* (RERR) até a origem, avisando sobre a queda do enlace. Se a origem ainda deseja utilizar a rota, o processo de descoberta de rotas é reiniciado.

2.2 *Ad hoc On-demand Multipath Distance Vector Routing*

O objetivo do protocolo *Ad hoc On-demand Multipath Distance Vector Routing* (AOMDV) [18] é estender o AODV [16] para encontrar múltiplas rotas livres de laços e disjuntas entre a origem e o destino, ao invés de somente uma rota. Ao descobrir a primeira rota para o destino, a origem começa a usá-la. Todas as outras rotas descobertas são deixadas como rotas de *backup*. A origem vai tentar usar uma dessas rotas se a atual for quebrada. O AOMDV consiste nas seguintes partes: descoberta de rota e manutenção de rota.

2.2.1 Descoberta de rota

A origem inicia um processo de descoberta de rota enviando uma mensagem de *route request* (RREQ) em *broadcast*. A partir do momento que o RREQ é enviado para a rede toda, um nó pode receber várias cópias do mesmo RREQ. Em protocolos de caminho único, apenas o primeiro RREQ é usado para formar rotas inversas entre o nó que recebeu o RREQ e a origem, as cópias duplicadas que chegam depois, são simplesmente descartadas. Porém, algumas dessas cópias duplicadas podem ser utilizadas para formar caminhos inversos alternativos. Assim, todas as cópias duplicadas são examinadas no AOMDV, aquelas cópias que preservam a liberdade de laço e possuem caminhos disjuntos entre a origem e o destino, poderão ser utilizadas para formar caminhos alternativos.

Quando um nó intermediário recebe uma cópia de uma mensagem de RREQ, ele verifica em sua tabela de roteamento se existe um ou mais caminhos válidos para o destino solicitado na mensagem de RREQ. Caso exista, o nó gera uma mensagem de *route reply* (RREP) e a envia de volta para a origem no caminho inverso. Caso contrário, a mensagem

de RREQ é reencaminhada pelo nó intermediário na rede.

Quando o nó destino recebe cópias da RREQ, ele constrói caminhos inversos da mesma forma que os nós intermediários. O nó destino gera um RREP em resposta a cada RREQ que chega, através de um caminho livre de laço com a origem.

2.2.2 Manutenção de rota

Para manutenção de rotas o AOMDV usa mensagens de erro *Route Error* (RERR). Um nó gera e encaminha uma RERR para a origem quando detecta a quebra de um enlace. AOMDV também inclui uma otimização para salvar pacotes enviados através de enlaces quebrados e reenviá-los posteriormente por um caminho alternativo. Ao receber uma mensagem de RERR, a origem simplesmente escolhe outro caminho para o destino e mantém o encaminhamento dos dados. Se não houver mais rotas disponíveis, a origem deve reiniciar o processo de descoberta de rota.

2.2.3 Liberdade de laço

Um ponto importante na utilização do AOMDV é o fato deste protocolo utilizar múltiplas rotas entre a origem e o destino e conseguir garantir que estas sejam livres de laços. No AOMDV, cada RREQ e RREP define um caminho alternativo entre a origem e o destino. Múltiplos caminhos são mantidos nas tabelas de roteamento de cada nó. Cada entrada na tabela de roteamento contém uma lista do próximo salto juntamente com o número de saltos (*hop count*) para cada destino.

O AOMDV, para assegurar que os caminhos sejam livres de laços, utiliza um valor chamado de *advertised hop count*. Cada nó mantém este valor para cada destino em sua tabela de roteamento. O *advertised hop count* é definido como a contagem de saltos do caminho mais longo disponível no momento em que um nó anuncia pela primeira vez um caminho para o destino. Um caminho alternativo entre o nó J e o destino K, só é aceito se o *hop count* é menor que o *advertised hop count*. A contagem de saltos anunciados (*advertised hop count*) impede a formação de um caminho alternativo para um destino, através do nó que gerou o RREQ, e portanto, garante a liberdade de laço. Este fato

acontece pois, caso o pacote de RREQ passe novamente pelo nó que o gerou, o valor da variável *hop_ count* será maior que o valor da variável *advertised_ hop_ count* e, quando isso ocorre, um caminho alternativo entre dois nós não é formado. A tabela 2.1 ilustra os campos da tabela de roteamento do protocolo AOMDV.

AOMDV
destination
sequence number
advertised_hopcount
route_list {(nexthop1,hopcount1), (nexthop2,hopcount2),...}
expiration_timeout

Tabela 2.1: Tabela de roteamento do protocolo AOMDV

2.2.4 Caminhos disjuntos

Além de manter vários caminhos livres de laço, o AOMDV visa encontrar caminhos alternativos disjuntos entre um par de nós. A utilização de rotas disjuntas aumenta a tolerância a falhas, pois a probabilidade de falhas simultâneas é menor em comparação à utilização de caminhos alternativos compartilhados. Para o AOMDV, qualquer caminho entre um par de nós que não possua nós ou enlaces comuns é considerado disjunto.

Em protocolos de caminho único, um nó pode registrar apenas o próximo salto e a distância através do próximo salto para cada caminho. Estas informações não são suficientes para um nó determinar se dois caminhos obtidos a partir de dois vizinhos são de fato distintos. Informações adicionais são necessárias para verificar se os caminhos são totalmente diferentes. Uma possibilidade é que cada nó da rede mantenha informações completas de caminhos para cada rota, ou seja, todo o caminho com todos os nós os quais o pacote deverá percorrer. No entanto, esta solução tem uma alta sobrecarga de comunicação [17]. O protocolo AOMDV possui um mecanismo o qual não necessita que os nós mantenham informações completas de caminhos para cada rota, e mesmo assim consegue garantir que as múltiplas rotas são disjuntas.

O mecanismo proposto pelo AOMDV requer que cada nó mantenha o registro do úl-

timo salto para cada caminho, além do próximo salto. Quando um nó de origem necessita de uma rota para um destino e nenhuma rota está disponível, inicia-se um processo de descoberta de rotas. A origem gera um pacote de RREQ e envia para toda rede. Quando algum vizinho da origem recebe o pacote de RREQ, antes de retransmiti-lo, copia seu endereço para o campo *Last Hop* (último salto) do RREQ. Um nó intermediário somente aceita pacotes de RREQ com diferentes *Last Hop* e só retransmite o primeiro pacote recebido. O destino aceita todos os RREQs recebidos, mas somente cria rotas com os que possuem diferentes *Last Hop*.

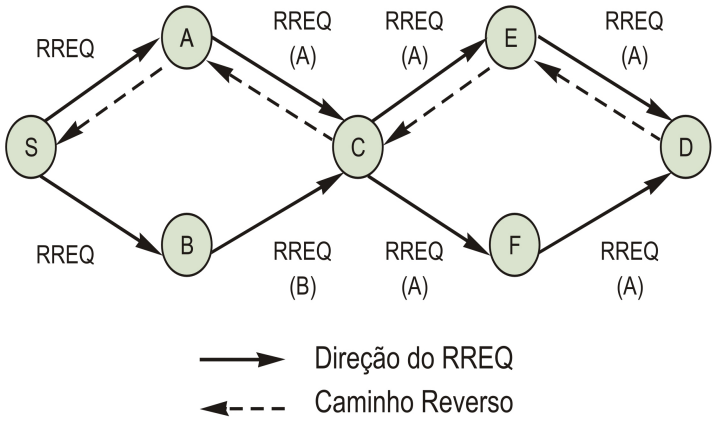


Figura 2.1: Criando caminhos disjuntos

Na figura 2.1, o nó S transmite um pacote de RREQ em seu raio de alcance. Quando os nós A e B recebem o pacote de RREQ, adicionam seus endereços no campo *Last Hop*. Em seguida, os nós criam em suas tabelas de roteamento os caminhos reversos (A-S) e (B-S) e retransmitem os pacotes de RREQ. O pacote enviado via nó A é representado por RREQ(A) e o enviado via nó B é representado por RREQ(B). Após o nó C receber os pacotes RREQ(A) e RREQ(B), ele cria em sua tabela de roteamento duas rotas reversas disjuntas:(C-A-S) e (C-B-S). Em seguida, o nó C retransmite o RREQ(A), que foi o primeiro pacote de RREQ recebido. Quando os nós E e F recebem o RREQ(A), criam as rotas reversas (E-C-A-S) e (F-C-A-S). Por fim, o nó D recebe os pacotes RREQ(A) enviados pelos nós E e F. Se D receber primeiramente o RREQ(A) enviado por E, cria a rota reversa (D-E-C-A-S). Quando receber a segunda cópia de RREQ(A) enviada por F, a qual contém o mesmo *Last Hop* do pacote enviado por E, o nó destino D não constrói

a rota reversa(D-F-C-A-S), pois esta não será disjunta.

2.3 Protocolos de roteamento multi-caminhos

Abordagens encontradas na literatura têm usado além do AOMDV, outros protocolos de roteamento multi-caminhos em redes ad hoc, conforme descrito a seguir. *Ad hoc On-demand Distance Vector Backup Routing* (AODV-BR) [19] é um protocolo de roteamento multi-caminhos no qual cada nó mantém uma tabela de roteamento alternativa, com rotas alternativas para um determinado destino. Estas rotas são usadas como rotas de *backup* e utilizadas somente quando a rota principal falhar. No AODV-BR, as várias rotas criadas não possuem garantia de disjunção.

Os protocolos *Dynamic Source Routing* (DSR) [20] e *Temporally-ordered Routing Algorithm*(TORA) [21] possuem por padrão a capacidade de criar múltiplas rotas entre a origem e o destino. Estas rotas não são disjuntas e são usadas como rotas de *backup*, utilizadas somente quando a rota principal falhar. No DSR, a origem conhece as rotas completas, salto-a-salto, para o destino. Por sua vez, o protocolo TORA constrói e mantém várias rotas livres de laço e não disjuntas entre dois nós quaisquer, sem armazenar a rota completa. Este protocolo é baseado no conceito de enlace reverso [22] e é proposto para ser utilizado em redes altamente dinâmicas.

O *Multi-path Source Routing* (MSR) [23] é usado para encontrar múltiplas rotas disjuntas entre dois nós quaisquer. O objetivo deste protocolo é distribuir a carga entre as várias rotas encontradas pelo nó de origem. Tal técnica baseia-se no algoritmo *round-robin* e em métodos heurísticos para distribuir as informações entre os vários caminhos.

O protocolo *Split Multipath Routing* (SMR) [24], constrói um protocolo de roteamento multi-caminhos, no qual a origem conhece a rota completa, salto-a-salto, para o destino. O SMR cria e mantém todas as rotas disjuntas possíveis entre dois nós. Porém, o protocolo não fornece garantia de que todas as rotas criadas são realmente disjuntas. O principal foco deste protocolo é distribuir a carga entre as rotas encontradas, por isso mantém em sua tabela rotas disjuntas e compartilhadas.

O *Caching and Multipath Routing Protocol* (CHAMP) [25] é um protocolo multi-

caminhos cujo principal objetivo é diminuir o descarte de pacotes causados pelas frequentes quebras de enlaces. Este protocolo constrói múltiplas rotas não disjuntas e uma rota alternativa só é usada se a principal falhar. Um *cache* local é criado em cada nó da rede para que os dados possam ser armazenados e retransmitidos caso um dos caminhos apresente falha. As rotas escolhidas para que os dados sejam enviados são sempre aquelas que apresentarem o menor número de saltos para o destino.

Multi-path Dynamic Source Routing Protocol (MP-DSR) [26] é um protocolo de roteamento multi-caminhos baseado no DSR, o qual cria rotas disjuntas e livres de laço entre dois nós quaisquer. As rotas criadas pelo MP-DSR são utilizadas simultaneamente para distribuir a carga entre os vários caminhos.

Protocolos	**AODV-BR**	**DRS**	**TORA**	**MSR**	**SMR**	**CHAMP**	**MP-DSR**	**AOMDV**
Liberdade de laço	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
Rotas disjuntas	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	SIM	SIM
Rotas completas	NÃO	SIM	NÃO	SIM	SIM	NÃO	SIM	NÃO
Rotas simultâneas	NÃO	NÃO	NÃO	SIM	SIM	NÃO	SIM	NÃO

Tabela 2.2: Tabela comparativa entre protocolos de roteamento multi-caminhos

Observa-se na tabela 2.2 que os protocolos são comparados quanto às seguintes métricas: liberdade de laço, rotas disjuntas e rotas completas conhecidas, salto a salto, para o destino. Os protocolos mais eficientes quanto ao desempenho e aos ataques de nós maliciosos devem possuir liberdade de laço, rotas disjuntas e não conhecer a rota completa para o destino [18] (respostas SIM, SIM e NÃO na tabela 2.2). Neste contexto, evidencia-se pela análise da tabela citada, que o único protocolo com estas características é o AOMDV, sendo assim o mais adequado entre os protocolos comparados.

CAPÍTULO 3

ATAQUE *BLACKHOLE*

Blackhole [4, 6, 7, 8, 9, 10, 11, 12, 13, 14] é um tipo de ataque que ocorre quando um ou vários nós da rede descartam indiscriminadamente os pacotes que passam por eles. Os nós *blackhole* podem se aproveitar da vulnerabilidade dos algoritmos de roteamento cooperativos e, através do envio de pacotes de roteamento falsos, induzir o envio para si mesmo de todos os pacotes de dados destinados a outro nó e então descartá-los. Ainda, um nó *blackhole* pode não interferir no processo de roteamento e somente descartar os pacotes de dados que passam por ele. Este ataque pode causar um grande impacto no desempenho da rede, podendo resultar na redução significativa da taxa de entrega de pacotes de dados.

A figura 3.1 mostra um exemplo de ataque *blackhole*. Neste exemplo, o nó C é um nó malicioso enquanto os nós S e D são os nós de origem e destino, respectivamente. Primeiramente, o nó S transmite os pacotes de RREQ para seus vizinhos com distância de um salto. Então, ao receber este pacote, cada nó vizinho pode retransmití-lo, caso não tenha uma rota disponível para o destino. No entanto, o nó C desobedece esta regra e envia um pacote RREP de volta ao nó S, afirmando ter o caminho mais curto para o destino. Assim, se o RREP enviado pelo nó D ou um nó intermediário honesto, que tem uma nova rota para o nó D (com a mesma distância ou menor da que o nó C afirmou ter) atinge o nó S antes do RREP enviado pelo nó C, tudo funciona corretamente. Caso contrário, o nó de origem S considera que a rota que passa pelo nó C é o caminho mais curto e, portanto, começa a transmitir os pacotes de dados para C, que os descarta.

Em outra estratégia de ataque, os nós *blackhole* cooperam normalmente com os nós autênticos no procedimento de descoberta de rotas, buscando se posicionar como nós intermediários das rotas. Assim, os nós *blackhole* podem participar do processo de roteamento e descartar todos os pacotes de dados enviados antes que eles cheguem aos seus

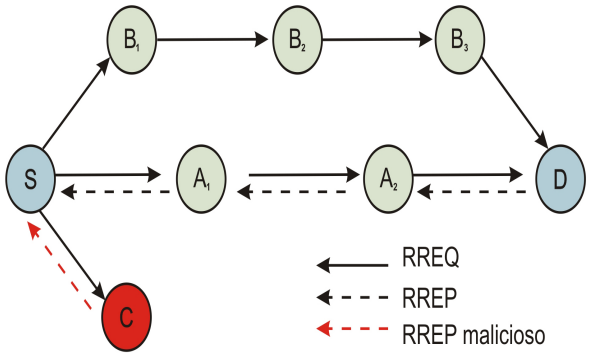


Figura 3.1: Ataque *blackhole* no AOMDV

destinos.

3.1 Trabalhos relacionados a ataques de *blackhole*

Abordagens encontradas na literatura têm tratado de ataques de *blackhole*, conforme descrito a seguir. Segundo [27] as atividades de um nó na rede podem demonstrar a sua honestidade. Assim, para que um nó possa participar do processo de transferência de dados, deve comprovar que é honesto. Neste trabalho, quando um nó entra na rede, tem permissão para transferir dados, pois o mesmo têm um tempo para provar sua idoneidade. Porém, todas as suas atividades são monitoradas por seus vizinhos. Passado este tempo, caso o novo nó tente estabelecer qualquer troca de mensagens com outro nó que já faz parte da rede, os vizinhos monitores são convocados pelo nó antigo para enviar suas opiniões sobre o novo membro. Após analisar todos os pareceres dos vizinhos, o nó antigo decide se o novo membro é um nó honesto ou malicioso. A decisão tem por base algumas regras pré-estabelecidas. As seguintes regras são utilizadas para julgar a honestidade de um nó na rede:

1. Se um nó envia muitos pacotes de dados para os destinos, é considerado honesto;
2. Se um nó recebe muitos pacotes, mas não envia a mesma quantidade, é considerado suspeito;
3. Quando a regra 2 é válida e o nó tem pacotes de RREP enviados, é considerado malicioso;

4. Quando a regra 2 é valida e o nó não enviou nenhum pacote RREP, é considerado um nó falho.

O referido estudo mostra que em uma rede com 3 nós *blackhole* ele consegue entregar 70% mais pacotes de dados do que os outros protocolos que foram comparados. Entretanto, esta mesma rede pode ter 100% de aumento de sobrecarga.

Em [28] é proposto um método que considera que todas as atividades de um usuário ou um sistema podem ser monitoradas e identificadas. Consequentemente as atividades de um nó atacante também podem ser monitoradas. Após a coleta de dados sobre um determinado nó na rede, o sistema, chamado IDAD, é invocado para analisá-las e compará-las com um conjunto de anomalias pré-estabelecidas. Assim, é possível verificar se este nó apresenta características de um nó *blackhole*. Caso apresente, será isolado pelo nó que o detectou. Neste sistema, cada nó é responsável por sua própria proteção. Segundo [28], em um ataque de *blackhole*, um nó malicioso engana o nó de origem, enviando uma mensagem RREP falsa. Esta mensagem falsa contém os seguintes parâmetros:

- Número de sequência máximo: igual ou maior ao último recebido;
- Número de saltos baixo para o destino: um salto somente;
- *life-long route*: informa que a rota existirá enquanto a rede existir;
- Endereço IP copiado do destino;
- *time-stamp*: informa o tempo em que o RREP foi gerado.

Assim, quando o nó de origem recebe um RREP, ele invoca o sistema IDAD, o qual analisa estes parâmetros com base em um banco de dados pré-gravado. Por exemplo, se no pacote de RREP existir exatamente o mesmo *time-stamp* do pacote de RREQ, este nó é considerado *blackhole*. O referido estudo mostra que uma rede com 2 nós *blackhole* tem mais de 95% de todos os pacotes entregues usando o sistema IDAD, taxa de entrega maior que a dos outros protocolos comparados. A sobrecarga de roteamento é maior que a dos outros protocolos.

No sistema *Watchdog and Pathrater* [29], cada nó da rede detecta os nós maliciosos isoladamente. O nó de origem envia o pacote para o outro nó que afirma ser o caminho mais curto para o destino. Após isso, coloca sua interface de rede no modo promíscuo e verifica se este nó realmente encaminhou seu pacote. Caso o nó não tenha encaminhado, é considerado *blackhole* e isolado da rede pela origem. Na presença de até 40% nós atacantes, está técnica pode aumentar a taxa de entrega em até 27% e a sobrecarga da rede em até 24%.

Em [30] é proposto um método de monitoramento colaborativo para a prevenção do ataque *blackhole*. Neste método, os nós da rede são classificados de três formas: confiáveis, monitoradores e *blackhole*. Todos os nós que forem eleitos monitoradores, devem observar os seus vizinhos e decidir se eles podem ser tratados como confiáveis ou maliciosos. Assim, os nós da rede podem decidir em quem confiar. Por exemplo: antes do nó de origem enviar um pacote de dados para seu vizinho que afirmou ter a melhor rota para o destino, ele convoca um nó monitor para monitorar a transmissão; caso o monitor perceba que o nó vizinho descarta os pacotes da origem, ele avisa a origem e todos os outros monitores que o referido nó é *blackhole*. O referido trabalho relata que é efetivo quanto à detecção de nós maliciosos e consegue aumentar a taxa de entrega em uma rede com até 45% de nós atacantes. A sobrecarga de roteamento é maior que a dos outros protocolos comparados.

Em [31], nós IDS (*Intrusion Detection System*) são implementados em MANETs para identificar e isolar nós *blackhole*. Neste trabalho, cada nó IDS executa um mecanismo, chamado de ABM (*Anti-Blackhole Mechanism*), o qual é utilizado para monitorar e estimar se um determinado nó é *blackhole*, de acordo com o valor da diferença entre os RREQs e RREPs transmitidos. O monitoramento é realizado em modo promíscuo pelos nós IDS. Depois que um nó *blackhole* é identificado, os nós IDS enviam uma mensagem em *broadcast* para rede, avisando que este nó deve ser isolado. O mecanismo de detecção funciona da seguinte forma: se um nó intermediário não é o nó de destino, e nunca transmitiu um RREQ para uma rota específica, mas encaminhou um RREP para esta rota, é considerado *blackhole*. Este mecanismo mostra que a taxa de pacotes descartados pode ser reduzida em mais de 80% com dois nós *blackhole* na rede. Não são apresentados re-

sultados sobre a sobrecarga de roteamento. Como existem muitas trocas de mensagem, a sobrecarga deve ser elevada.

Em [32] é proposto um sistemas para reduzir a probabilidade de sucesso em ataques realizados por nós *blackhole*. Neste trabalho, é descrito um método que aguarda todas as respostas de todos os nós vizinhos e, somente após processar as respostas decide por qual caminho deve enviar os pacotes de dados. Quando o nó de origem necessita de uma rota para o destino, envia em *broadcast* na rede uma mensagem de RREQ. Os nós que possuem uma rota para o destino desejado respondem com uma mensagem de RREP. Na maioria dos protocolos de roteamento, assim que chega um RREP com uma rota para o destino, a origem começa imediatamente a transmitir os dados. Todavia, neste trabalho, a rota não é formada imediatamente. Um tempo pré-estabelecido é aguardado, assim, muitos RREPs podem chegar, originando-se de nós honestos, bem como maliciosos. Após o recebimento, a origem analisa cada um deles para decidir por qual caminho deve enviar os pacotes de dados. Os RREPs que possuírem próximos saltos repetidos são considerados como caminhos confiáveis. O referido trabalho relata que é efetivo quanto à detecção de nós maliciosos e aumenta a taxa de entrega em até 80%. A sobrecarga de roteamento é maior que a dos outros protocolos comparados.

3.1.1 Tabela comparativa entre os trabalhos relacionados

Sistemas	**[27]**	**[28]**	**[29]**	**[30]**	**[31]**	**[32]**
Detecta nós *blackhole*	SIM	SIM	SIM	SIM	SIM	SIM
Reage aos ataques	SIM	SIM	SIM	SIM	SIM	SIM
Teve aumento de sobrecarga	SIM	SIM	SIM	SIM	SIM	SIM
Aumento da sobrecarga em (%)	80	NI	24	NI	NI	NI
Teve aumento da taxa de entrega	SIM	SIM	SIM	SIM	SIM	SIM
Aumento da taxa de entrega (%)	70	95	24	45	NI	80

Nota: NI = Não Informado

Tabela 3.1: Tabela comparativa entre tipos de ataques *blackhole*

Na tabela 3.1, os trabalhos relacionados estão apresentados([27],[28],[29],[30],[31],[32]) na ordem em que foram descritos no texto e conforme o número descrito nas referências bibliográficas. A comparação disposta na tabela 3.1 tem como parâmetro a capacidade

dos sistemas em detectar os nós *blackhole* presentes na rede, bem como uma possível ação quanto ao nó atacante após a detecção. Outrossim, a comparação tem como referência a taxa de entrega e a sobrecarga de roteamento. Observa-se que todos os sistemas analisados detectam e reagem aos nós *blackhole*, isso torna a taxa de entrega maior, contudo a sobrecarga de roteamento também aumenta.

CAPÍTULO 4

TEORIA DOS NÚMEROS

Este capítulo apresenta os fundamentos matemáticos da teoria de números [33, 34, 35], os quais são necessários para o entendimento do teorema chinês do resto.

4.1 Algoritmo euclidiano

O Algoritmo de Euclides é uma das formas de se encontrar o MDC (máximo divisor comum) de dois números inteiros. Diz-se que para calcular o máximo divisor comum entre a e b, é feita a seguinte sequência de divisões:

$$a = bq_1 + r_1 \text{ e } 0 \leq r_1 < b$$
$$b = r_1q_2 + r_2 \text{ e } 0 \leq r_2 < r_1$$
$$r_1 = r_2q_3 + r_3 \text{ e } 0 \leq r_3 < r_2$$
$$r_2 = r_3q_4 + r_4 \text{ e } 0 \leq r_4 < r_3$$

Observando a sequência de restos, nota-se que o seguinte é sempre menor que o anterior, mas todos são maiores ou iguais a zero. Escrevendo matematicamente, tem-se:

$$b > r_1 > r_2 > r_3 > r_4 ... \geq 0$$

4.2 Algoritmo euclidiano estendido

Sejam a e b inteiros positivos e d o MDC destes números, é possível encontrar inteiros α e β, tais que:

$$\alpha \cdot a + \beta \cdot b = d$$

O algoritmo euclidiano modificado que calcula α e β simultaneamente é denominado algoritmo euclidiano estendido. Portanto, para efetuar os cálculos correspondentes a uma

determinada divisão, basta guardar os dados referentes às duas divisões imediatamente anteriores. Assim, a sequência de divisões pode ser reescrita da seguinte forma:

$$a = bq_1 + r_1 \text{ e } r_1 = ax_1 + by_1$$

$$b = r_1q_2 + r_2 \text{ e } r_2 = ax_2 + by_2$$

$$r_1 = r_2q_3 + r_3 \text{ e } r_3 = ax_3 + by_3$$

$$r_2 = r_3q_4 + r_4 \text{ e } r_4 = ax_4 + by_4$$

$$\vdots$$

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1} \text{ e } r_{n-1} = ax_{n-1} + by_{n-1}$$

$$r_{n-2} = r_{n-1}q_n \text{ e } r_n = 0$$

Os números $x_1, ..., x_{n-1}$ e $y_1, ..., y_{n-1}$ são os inteiros que serão determinados e podem ser vistos na tabela 4.1. A primeira e a segunda linha são os "casos base"e por isso são denotados como linhas -1 e 0. Assim, adota-se: $x_1 = 1, y_1 = 0, x_0 = 0, y_0 = 1$.

O uso do algoritmo é necessário para preencher a tabela até encontrar a condição de parada, fazendo com que os últimos valores encontrados para x e y sejam α e β, ou seja:

$$\alpha = x_{n-1} \text{ e } \beta = y_{n-1}$$

Restos	**Quocientes**	x	y
a	$*$	$x-1$	$y-1$
b	$*$	x_0	y_0
r_1	q_1	x_1	y_1
r_2	q_2	x_2	y_2
r_3	q_3	x_3	y_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

Tabela 4.1: Divisões do algoritmo euclidiano estendido

4.3 Fatoração única

Cada número inteiro pode ser escrito como um produto de números primos. Um número natural é um número primo quando ele tem exatamente dois divisores: o número um e ele mesmo.

O teorema da fatoração única pode ser enunciado da seguinte forma: dado um inteiro positivo $n \geq 2$ pode-se sempre escrevê-lo, de modo único, na forma:

$$n = p_1^{e_1}...p_k^{e_k},$$

onde $1 < p_1 < p_2 < p_3... < p_k$ são números primos e $e_1...e_k$ são inteiros positivos.

Os expoentes $e_1...e_k$ são chamados de multiplicidades. Assim, a multiplicidade de p_1 na fatoração de n é e_1. Observa-se também que n tem k fatores primos distintos, mas que a quantidade total de fatores primos (distintos ou não distintos) é a soma das multiplicidades $e_1 + ... + e_k$.

O teorema da fatoração única demonstra duas propriedades: 1) todo inteiro pode ser escrito como um produto de primos; 2) só há uma escolha possível de primos e expoentes para a fatoração de um inteiro dado.

4.4 Aritmética modular

Dois inteiros a e b são congruentes módulo n se $a - b$ é um múltiplo de n. Se a e b são congruentes módulo n, escreve-se:

$$a \equiv b(mod\, n)$$

Pode-se verificar as propriedades da congruência módulo n. Primeiro, a propriedade reflexiva. Seja a um inteiro. Para mostrar que $a \equiv a(mod\, n)$, verifica-se, por definição, que a diferença $a - a$ é um múltiplo de n, pois 0 é múltiplo de qualquer número inteiro. Analisando a propriedade simétrica, verifica-se que se $a \equiv b(mod\, n)$, então $a - b$ é um múltiplo de n. Mas $b - a = -(a - b)$; logo $b - a$ também é múltiplo de n. Portanto $b \equiv a(mod\, n)$.

Para a propriedade transitiva, supõe-se que $a \equiv b(mod\, n)$ e $b \equiv c(mod\, n)$, onde a, b e c são inteiros. A primeira congruência mostra que $a - b$ é múltiplo de n; a segunda que $b - c$ é múltiplo de n. Somando múltiplos de n obtém-se novamente múltiplos de n; logo $(a - b) + (b - c) = (a - c)$ é um múltiplo de n. Assim, $a \equiv c(mod\, n)$.

Pela relação de congruência módulo n, o conjunto quociente de $\mathbb{Z}$ tem uma notação própria, $\mathbb{Z}_n$; e seu nome é conjunto dos inteiros módulo n. Seja $a \in \mathbb{Z}$. A classe de a é formada pelos $b \in \mathbb{Z}$ que satisfaçam $b - a$ múltiplo de n; isto é $b - a = kn$, para algum $k \in \mathbb{Z}$. Então, a classe de a pode ser descrita da forma:

$$\bar{a} = \{a + kn : k, a, b \in \mathbb{Z}\}$$

Em particular $\bar{0}$ é o conjunto dos múltiplos de n, fazendo com que se $a \in \mathbb{Z}$, então podemos dividí-lo por n, obtendo q e r inteiros, tais que:

$$a = nq + r \text{ e } 0 \leq r \leq n - 1$$

Logo $a - r = nq$ é um múltiplo de n. Portanto $a \equiv r(mod\, n)$, demonstra que o conjunto quociente $\mathbb{Z}_n$ é formado pelas classes $\bar{0}, \bar{1}, ..., \overline{n-1}$. Resumindo:

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$$

$$\bar{3} = \{... - 3, 3, 9, 15, 21...\}$$

4.4.1 Aritmética modular

A definição da soma de determinadas classes de $\mathbb{Z}_n$ é dada por: sejam $\bar{a}$ e $\bar{b}$ as classes de $\mathbb{Z}_n$ que deseja-se somar. A fórmula para a operação é a seguinte:

$$\bar{a} + \bar{b} = \overline{a + b}$$

A diferença entre duas classes é definida de modo análogo ao da adição.

Passando à multiplicação, pode-se repitir a definição matemática dada à adição. Desta forma:

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

Assim como nas operações em números inteiros, as operações com classes possuem propriedades correspondentes. As propriedades da adição são:

$$(1).\ (\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$$

$$(2).\ \bar{a}+\bar{b}=\bar{b}+\bar{a}$$

$$(3).\ \bar{a}+\bar{0}=\bar{a}$$

$$(4).\ \bar{a}+\overline{-a}=\bar{0}$$

As propriedades da multiplicidade são:

$$(1).\ (\bar{a}\cdot\bar{b})\cdot\bar{c}=\bar{a}\cdot(\bar{b}\cdot\bar{c})$$

$$(2).\ \bar{a}\cdot\bar{b}=\bar{b}\cdot\bar{a}$$

$$(3).\ \bar{a}\cdot\bar{0}=\bar{a}$$

$$(4).\ \bar{a}\cdot\overline{-a}=\bar{0}$$

Há também a propriedade que relaciona duas operações, a distributividade:

$$\bar{a}\cdot(\bar{b}+\bar{c})=\bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}$$

4.5 Sistemas de congruência

Considerando o caso de uma única equação linear

$$a\equiv b\,mod\,(n)$$

onde n é um inteiro positivo.

Estas equações são fáceis de serem resolvidas quando $\bar{a}$ tem inverso em $\mathbb{Z}_n$. Segundo o teorema da inversão, $\bar{a}$ tem inverso em $\mathbb{Z}_n$, se e somente se, a e n são primos entre si. Se $\bar{a}$ não tem inverso, pode-se dizer que $mdc(a,n)\neq 1$. Assim, se a equação $a\equiv b\,mod\,(n)$ tem solução, isto quer dizer que existem $x,y\in\mathbb{Z}$ tais que

$$ax-ny=b$$

Isto só é possível se o $mdc(a,n)$ divide b. Se $\bar{a}$ tem inverso em $\mathbb{Z}_n$ esta condição é satisfeita, porque neste caso $mdc(a,n)=1$.

Supõe-se então que $d=mdc(a,n)$ divide b. Diz-se que $a=da, b=db$ e $n=dn$. Substituindo em $ax-ny=b$ e cancelando d

$$ax - ny = b$$

que se converte na equação $ax \equiv b mod(n)$; uma nova equação em congruências. Deve-se observar que $mdc(a, n)$ é sempre 1.

4.6 Teorema chinês do resto

Considera-se o seguinte sistema:

$$(1).\ x \equiv a\, mod(m) \text{ e } (2).\ x \equiv b\, mod(n)$$

A primeira equação pode ser reescrita na forma $x = a + my$, onde y é um inteiro qualquer. Com isto, pode-se substituir x na segunda equação, obtendo

$$my \equiv (b - a)(mod\, n).$$

Para que esta equação tenha solução é preciso que o MDC entre m e n divida $b - a$. Para assegurar este fato, basta assumir que $mdc(n, m) = 1$. Com isto $\overline{m}$ tem inverso em $\mathbb{Z}_n$. Chamando $\overline{\alpha} \in \mathbb{Z}_n$ o inverso, a solução da equação acima é $y \equiv \alpha(b - a)(mod\, n)$. Assim, $y = \alpha(b - a) + nz$, onde z é um número inteiro. Substituindo na equação que dá x em função de y, tem-se

$$x = a + m\alpha(b - a) + mnz.$$

Mas $\overline{m\alpha} = \overline{1}$ em $\mathbb{Z}_n$. Logo, existe algum inteiro β tal que $1 - m\alpha = n\beta$. Assim

$$x = a(1 - m\alpha) + mb\alpha + mnz = an\beta + mb\alpha + mnz$$

De fato, $1 = m\alpha + n\beta$. Como supõe-se que $mdc(m, n) = 1$, basta aplicar o algoritmo euclidiano estendido a m e n para obter α e β. Resumindo: se $mdc(m, n) = 1$, então o sistema mostrado acima sempre tem como soluções os números $an\beta + bm\alpha + kmn$, onde k é um inteiro qualquer.

Uma equação linear pode ter mais de uma solução se o módulo for composto. O sistema acima tem infinitas soluções quando tratam-se de soluções inteiras, já que há

uma solução para cada escolha de k. Diz-se que x e y são dois inteiros que são soluções do sistema descrito acima. Então, tem-se que $x \equiv a\, mod(m)$ e $y \equiv a\, mod(m)$. Como se tratam de duas equações com mesmo módulo, pode-se realizar a subtração entre elas. Obtendo-se: $x - y \equiv 0\, mod(m)$. Assim, m divide $x - y$. Fazendo o mesmo com a segunda equação, conclui-se que n divide $x - y$. Supondo que $mdc(m, n) = 1$, tem-se que mn divide $x - y$. Assim, o sistema tem infinitas soluções inteiras, mas apenas uma solução em $\mathbb{Z}_{mn}$ quando $mdc(m, n) = 1$. Portanto, tudo isso pode ser resumido em um teorema:

Teorema Chinês do Resto. Sejam m e n inteiros positivos, primos entre si. O sistema

$$x \equiv a\, mod(m)$$

$$x \equiv b\, mod(n)$$

sempre tem uma única solução em $\mathbb{Z}_{mn}$.

Os conceitos do teorema chinês do resto serão utilizados posteriormente para divisão e remontagem da informação.

CAPÍTULO 5

PROTOCOLO DE ROTEAMENTO RESISTENTE A ATAQUES *BLACKHOLE* EM REDES AD HOC MÓVEIS SEM DETECÇÃO DE NÓS MALICIOSOS

O protocolo aqui proposto intitulado de *Multipath routing* ***P****rotocol* ***R****esistant* to **B**lackHole **A**ttacks (**PRAB**), tem como escopo inibir os efeitos dos descartes de pacotes causados por ataques *blackhole* em redes ad hoc sem a necessidade de conhecimento algum do comportamento do nó atacante. Com efeito, figura-se desnecessária a detecção e a reação contra cada um dos nós atacantes.

No PRAB, cada pacote transmitido pode ser dividido em partes menores e, cada uma destas partes pode ser enviada da origem para o destino por um caminho diferente. No destino, não são necessárias todas as partes que foram transmitidas para reconstruir a informação original, algumas destas partes podem ser descartadas por nós *blackhole*, e mesmo assim a informação original pode ser reconstruída. Generalizando a idéia descrita tem-se: dada uma informação d, o objetivo é dividir d em n partes, e enviar por n caminhos, de tal forma que d possa ser reconstruída a partir de, no mínimo k das n partes, onde $k \leq n$. Com $k-1$ ou menos partes, a informação original não pode ser reconstruída.

O PRAB utiliza o teorema chinês do resto para dividir a informação na origem e remontá-la no destino. Por sua vez, o protocolo de roteamento AOMDV levemente modificado, é usado para criar múltiplas rotas visando a transmissão simultânea das informações particionadas.

O algoritmo 1 descreve o PRAB.

Algoritmo 1 - Protocolo de roteamento multicaminhos resistente a atacantes *blackhole*

```
1:  Entrada:
2:  d = Informação original
3:  n = Número de partes que a informação original é dividida
4:  k = Número de partes necessárias para reconstruir a informação original
5:  procedure ProtocoloResistenteAtaquesBlackhole
6:      if (nó de origem) then
7:          if (descobreNCaminhosDisjuntos()==n) then        ▷ Descobre n caminhos disjuntos e livres de laço
8:              divideDEmNPartes(d,n)                        ▷ Divide d em n partes de mesmo tamanho
9:              enviaNpartesPorNCaminhos(n)                  ▷ Envia as n partes por n caminhos disjuntos
10:         else(segueDistribuicaoCiclica(n))   ▷ Se não for possível criar n caminhos disjuntos e livres de laço, segue
    distribuição cíclica através dos n caminhos existentes
11:             divideDEmNPartes(d,n)                        ▷ Divide d em n partes de mesmo tamanho
12:             enviaNpartesPorNCaminhos(n)                  ▷ Envia as n partes por n caminhos disjuntos
13:         end if
14:     end if
15:     if (nó intermediário) then
16:         escolhePrimeiraRota()                  ▷ Escolhe a primeira entrada na tabela de rotas dos nós
17:         enviaParte()                ▷ Envia a parte da informação que esta passando por este nó
18:     end if
19:     if (nó destino) then
20:         reconstroiDComKPartes(k)                 ▷ Reconstrói d com k das n partes, com k <= n
21:     end if
22: end procedure
```

5.1 Modificações realizadas no AOMDV para construção do PRAB

Em cada processo de descoberta de rotas, o protocolo AOMDV original cria no máximo três rotas disjuntas e livres de laço entre dois nós quaisquer. No entanto, no PRAB, é necessário manter nas tabelas de roteamento dos nós, um número grande de rotas. Além disso, todas as rotas disjuntas e livres de laço possíveis para um determinado destino são mantidas na tabela de roteamento do nó de origem, sendo representadas por n. Os motivos pelos quais deve-se utilizar somente rotas totalmente disjuntas são: evitar a sobrecarga excessiva de apenas alguns elementos da rede; aumentar a probabilidade de evitar nós maliciosos.

No protocolo PRAB, todas as rotas (até n) podem ser utilizadas simultaneamente para encaminhar as partes da informação original. Caso o novo protocolo não seja capaz de construir n rotas disjuntas entre a origem e o destino, as n partes da informação são transmitidas através das rotas disponíveis, seguindo uma distribuição cíclica. É importante ressaltar que o parâmetro n representa o número de partes em que a informação é dividida, bem como o número máximo de caminhos através dos quais a informação é envida da origem para o destino.

O AOMDV original permite que tanto os nós de origem como os nós intermediários criem múltiplas rotas para um mesmo destino. Porém, nas modificações realizadas no novo protocolo, somente a origem pode enviar pacotes por todas as suas rotas. Os nós intermediários devem utilizar apenas a primeira entrada para cada destino de suas tabelas de roteamento. Em outras palavras, caso o nó de origem possua múltiplas rotas para um determinado destino e, um nó intermediário que faz parte deste caminho, também possua múltiplas rotas para o mesmo destino, o nó intermediário não pode enviar pacotes por todas suas rotas, limitando-se à utilização da primeira entrada na tabela de rotas.

5.2 Divisão e remontagem das informações

Após o processo de estabelecimento das rotas, as mensagem de dados podem ser enviadas do nó de origem para o nó de destino. Na origem, cada mensagem é dividida em n partes de mesmo tamanho, as quais são envidas por n caminhos diferentes e disjuntos.

No destino, a informação original é reconstruída. A quantidade de partes necessárias para que seja possível reconstruir a informação original depende do parâmetro estabelecido, que pode ser representado por: $L = (k, n)$, onde n é o número de partes em que a informação é dividida e k é o número de partes necessárias para reconstruir a informação. Para qualquer parâmetro adotado, as seguintes propriedades são válidas:

- $(n \geq 2)$.
- O tamanho de cada parte deve ser t/k, onde t é o tamanho da informação original e k é o número de partes necessárias para reconstruir a informação original [36][37].
- Se k for mantido fixo, as parte n podem ser adicionadas ou excluídas, sem afetar o resultado final.

5.2.1 Aplicação do algoritmo chinês do resto para divisão e reconstrução da informação

Dados h números primos, inteiros e positivos, $m_1, \cdots, m_h$ chamados de módulo, e considerando $M = \prod_{p=1}^{h} m_p$ e $m_p > m_{p-1}$ para cada $p \in [2, h]$. Dado qualquer inteiro não negativo X, e sendo $x_p = X \bmod m_p$ o resíduo de X modulo m_p. A h-tupla $(x_1, \cdots, x_h)$ é chamada de representação do resíduo de X; nesta representação x_p é chamado de resíduo de p^{th}. Existem M representações de resíduos distintos e cada representação corresponde a um número inteiro único em $[0, M)$. Para cada h-tupla $(x_1, \cdots, x_h)$, o correspondente inteiro X pode ser reconstruído pelo teorema chinês do resto: $X = (\Sigma_{p=1,h} x_p \frac{M}{m_p} \cdot b_p) \mathrm{mod} M$ onde, para cada $p \in [1, h]$, b_p é o inverso multiplicativo de $\frac{M}{m_p}$ modulo m_p [38].

Dados os módulos $m_1 \cdots m_h$, $m_{h+1} \cdots m_{h+r}$, e seja $M = \prod_{p=1}^{h} m_p$, $M_R = \prod_{p=h+1}^{r} m_p$ e $m_p > m_{p-1}$ para cada $p \in [2, h+r]$. Pode-se ter o sistema numérico de resíduos redundantes (RRNS) de módulos $m_1 \cdots m_{h+r}$, no intervalo M e redundância M_R, para representar números inteiros em $[0, M)$ com as $(h+r)$-tuplas dos seus $m_1 \cdots m_{h+r}$ módulos residuais.

O legítimo intervalo de representação do RRNS é limitado em $[0, M)$, e as correspondentes $(h+r)$-tuplas, são ditas legítimas. Inteiros em $[M, M \cdot M_R]$ e as correspondentes $(h+r)$-tuplas são ditas ilegítimas. Dado um RRNS no intervalo M e redundância M_R, onde $(m_1 \cdots m_h, m_{h+1} \cdots m_{h+r})$ são $(h+r)$-tupla do módulo e $(x_1 \cdots x_h, x_{h+1} \cdots x_{h+r})$ a legítima representação de algum X em $[0, M)$. Um evento que torna indisponíveis d partes arbitrárias é chamado de eliminação da multiplicidade d. Seja $\{x_1, x_2, \cdots, x_{h+r-d}\} \subseteq \{x_1, \cdots, x_{h+r}\}$ as partes diponíveis e $\{m_1, m_2, \cdots, m_{h+r-d}\} \subseteq \{m_1, \cdots, m_{h+r}\}$ o módulo correspondente. Se $d \leq r$, o RRNS do módulo $(m_1, m_2, \cdots, m_{h+r-d})$ tem um intervalo $M = \prod_p = 1^{h+r-d}\ m_p \geq M$ e desde que $X < M$, $(x_1, x_2, \cdots, x_{h+r-d})$ é a única representação de X.

Inteiros representados por X podem ser reconstruídos para a $(h + r - d)$-tupla $(x_1, x_2, \cdots, x_{h+r-d})$ por meio do teorema chinês do resto, como segue: $X = (\Sigma_p = 1^{h+r-d} x_p \frac{M}{m_p} \cdot b_p) \bmod M$ onde b é tal que $b_p \frac{M}{m_p} \bmod m_p = 1$ para cada $p \in [1, h + r - d]$.

Isso significa que o RRNS tolera perdas de partes até a multiplicidade r [38].

5.3 Sobrecarga extra dos dados transmitidos na rede

A divisão e transmissão da informação original em partes pode gerar sobrecarga extra de dados na rede. A sobrecarga para cada pacote transmitido é calculada tendo como base o parâmetro adotado e o tamanho de cada parte com seus respectivos cabeçalhos. Cada parte transmitida tem 74 bytes [39][40] de cabeçalhos, que estão divididos da seguinte forma: 42 bytes [39][40] para o cabeçalho do protocolo da camada de enlace, 8 bytes [39][40] para o cabeçalho do protocolo da camada de transporte e 24 bytes [39][40] para o cabeçalho protocolo da camada de rede.

Considerando-se que informação original é dividida em n partes, cada uma com tamanho t/k, onde k é o número de partes necessárias para reconstruir a informação original, e como $n > k$, tem-se uma sobrecarga extra de até $(n-k)$ partes, cada uma com tamanho t/k mais cabeçalhos. Assim, se a informação original tiver t bytes, e for dividida em n partes, com k partes necessárias para reconstruí-la, a sobrecarga extra de dados para transmitir a informação no novo protocolo pode ser de até: $[(n-k)\cdot(t/k)] + [(n-k)\cdot c]$, em que c representa o custo dos cabeçalhos dos diversos protocolos utilizados. Porém, este custo extra compensa pela maior taxa de entrega e, consequentemente, menor retransmissão de dados.

Por exemplo, se a informação original tiver 1024 bytes ($t = 1024$) e os parâmetros adotados forem: $L = (2,3)(k = 2, n = 3)$,$L = (2,4)(k = 2, n = 4)$, $L = (2,6)(k = 2, n = 6)$ e $L = (3,6)(k = 3, n = 6)$, a sobrecarga extra máxima para transmitir esta informação no novo protocolo, para cada um dos parâmetros citados, é descrita na tabela 5.1.

Parâmetros	$[(n-k)\cdot(t/k)] + [(n-k)\cdot c]$	**Sobrecarga**
$L = (2,3)(k = 2, n = 3)$	$[(3-2)\cdot(1024/2)] + [(3-2)\cdot 74]$	586 bytes
$L = (2,4)(k = 2, n = 4)$	$[(4-2)\cdot(1024/2)] + [(4-2)\cdot 74]$	1172 bytes
$L = (2,6)(k = 2, n = 6)$	$[(6-2)\cdot(1024/2)] + [(6-2)\cdot 74]$	2344 bytes
$L = (3,6)(k = 3, n = 6)$	$[(6-3)\cdot(1024/3)] + [(6-3)\cdot 74]$	1246 bytes

Tabela 5.1: Tabela com exemplos da sobrecarga extra de pacotes transmitidos na rede.

CAPÍTULO 6

AVALIAÇÃO DO PROTOCOLO PROPOSTO

Este capítulo apresenta a avaliação do funcionamento do protocolo proposto com simulações em diferentes cenários de redes sob ataques de *blackhole*.

6.1 Ambiente de Simulação

A avaliação foi realizada através de simulação usando o simulador NS (*Network Simulator*) versão 2.34 [41]. O NS-2 é um simulador de eventos discretos muito utilizado em pesquisas sobre redes ad hoc. Ele suporta os protocolos de rede mais populares, tanto para redes cabeadas quanto as sem fio.

A topologia de rede criada para avaliar as simulações possui nós distribuídos aleatoriamente, os quais se movimentam livremente e sem obstáculos, seguindo o modelo de movimentação *random waypoint* [42]. No modelo *random waypoint*, os nós se movem de um ponto até um outro ponto escolhido aleatoriamente com velocidade dentro de um intervalo pré-estabelecido. Um nó pode ainda parar em um ponto durante certo período de tempo antes de se mover ao próximo ponto.

Os nós se movem nas seguintes velocidades: 1 m/s, 8 m/s, 16 m/s e sem pausas. O padrão de tráfego é composto por conexões *User Datagram Protocol* (UDP) com taxa de bits constante (*Constant Bit Rate* - CBR) entre 15 pares de nós escolhidos aleatoriamente. O modelo de propagação de rádio é o *twoRay ground* [42], enquanto a camada MAC segue as especificações IEEE 802.11 [43]. As simulações são realizadas por 600 segundos e todos os resultados apresentados são médias de 35 simulações com o mesmo modelo de tráfego, mas com diferentes cenários de mobilidade.

6.2 Métricas

As métricas abaixo são usadas para avaliação do PRAB. Através do uso destas métricas é possível analisar os ganhos de desempenho e segurança fornecidos por este protocolo diante de ataques *blackhole*.

- **Taxa de entrega dos pacotes (TEP)**: é a proporção de pacotes de dados entregues ao destino em relação à quantidade de pacotes de dados enviados pela origem.

  Para o cálculo da taxa de entrega do PRAB os seguintes parâmetros foram estabelecidos: $L = (2, 3)$, $L = (2, 4)$, $L = (2, 6)$ e $L = (3, 6)$. Para os três primeiros parâmetros cada pacote é divido em 3, 4 e 6 partes e enviados por 3, 4 e 6 rotas. Nestes três primeiros casos o pacote é considerado entregue se no mínimo 2 partes chegarem ao destino. Para o último parâmetro, cada pacote é dividido em 6 partes e enviado por 6 caminhos. Neste caso, o pacote é considerado entregue se pelo menos 3 partes chegarem ao destino.

  Através da taxa de entrega dos pacotes é possível conhecer os descartes de pacotes resultantes de ataques *blackhole*, além de pacotes descartados por congestionamento, mobilidade, *buffer overflow* e quebras de enlaces.

- **Atraso fim-a-fim dos pacotes de dados (APD)**: representa o atraso das transmissões dos pacotes de dados entregues corretamente. Para os protocolos AOMDV e AODV originais, é a diferença entre o tempo em que um pacote saiu da origem e chegou ao destino. Para o PRAB, representa o tempo em que a primeira parte saiu da origem e a última parte necessária para reconstruir a informação chegou ao destino. Somente é considerado para pacotes entregues.

- **Vazão**: representa a quantidade de dados transferidos entre dois nós durante o intervalo de tempo em que permanecem conectados. Para o PRAB, somente é considerado pacotes entregues. Cada pacote de dados entregue é considerado como tendo 1024 bytes, mesmo que mais partes do que as necessárias para a reconstrução

da informação sejam entregues.

- **Sobrecarga de roteamento (SOR)**: é a quantidade total de pacotes de roteamento transmitidos. Para os pacotes enviados através de múltiplos saltos, cada transmissão do pacote (cada salto) conta como uma transmissão.

- **Pacotes de dados descartados por ataques de nós maliciosos (PDM)**: é a porcentagem de pacotes de dados descartados pela ação de nós *blackhole* em relação à quantidade total de pacotes enviados. Esta métrica indica a tolerância do sistema contra a ação de nós maliciosos.

6.3 Resultados e Análises

As simulações buscam examinar o protocolo proposto em diversas topologias de rede, para tanto definiu-se três cenários. No **Cenário 1**, o objetivo é examinar um ambiente de rede hostil, com alto percentual de nós atacantes, variando-se o tamanho da área da rede, o número de nós, a velocidade em que os nós se movimentam e o percentual de atacantes. Neste primeiro cenário, considera-se redes com tamanhos de 1000m X 1000m (cenário 1(a)) e 1500m X 300m (cenário 1(b)). Ambas as redes possuem 50, 75 e 100 nós e 0%, 5%, 10%, 20%, 30%, 40%, 50% e 60% dos nós são atacantes *blackhole*. Cada nó transmite seus sinais de rádio frequência em um raio de 250 metros. As conexões UDP entre os nós transmitem duas mensagens por segundo. As simulações comparam o PRAB com os protocolos AOMDV e AODV originais. Como o PRAB cria em média 6 rotas disjuntas, ele utiliza os seguintes parâmetros para avaliação: $L = (2,3)$, $L = (2,4)$, $L = (2,6)$ e $L = (3,6)$. Estes parâmetros podem ser representados respectivamente por: PRAB (2,3), PRAB (2,4), PRAB (2,6), PRAB (3,6).

O tamanho de cada parte depende do parâmetro estabelecido, e é calculada da seguinte forma: t/k, onde t é o tamanho da informação original e k é o número de partes necessárias para reconstruir a informação original [36][37]. Desta forma, para os três primeiros parâmetros do PRAB, cada parte tem 512 bytes de tamanho e, para o último parâmetro cada parte tem 341 bytes. Para os protocolos AODV e AOMDV originais cada pacote

tem 1024 bytes. Os parâmetros de simulações do cenário 1 estão resumidos na tabela 6.1.

Parâmetros	**Valores(s)**
Simulador	NS-2 (2.34)
Área de simulação	1.000m X 1.000m e 1500m X 300m
Número de nós	50, 75, 100
Modelo de mobilidade	*Random waypoint*
Raio de alcance dos nós	250m
Velocidade dos nós	1m/s, 8m/s, 16m/s
Tempo de pausa dos nós	0m/s
Padrão de tráfego	UDP/CBR com 2 mensagens por segundo
Número de conexões simultâneas	15
Tempo de simulação	600s
Atacantes(%)	0%,5%,10%,20%,30%,40%,50% e 60%
Modelo de propagação de rádio	*twoRay ground*
Especificações da camada MAC	IEEE 802.11

Tabela 6.1: Parâmetros de simulação do cenário 1

O **Cenário 2** tem como objetivo investigar os resultados perante o aumento da densidade da rede. Desta forma, a rede criada possui 50, 75 e 100 nós, cada nó transmite seus sinais de rádio frequência em um raio de 120 e 250 metros, em uma área 1000m X 1000m e 1500m X 300m. As conexões UDP transmitem duas mensagens por segundo. Neste cenário foi definido que 20% e 40% dos nós são *blackhole*. Os parâmetros de simulações do cenário 2 estão resumidos na tabela 6.2.

Parâmetros	**Valores(s)**
Simulador	NS-2 (2.34)
Área de simulação	1.000m X 1.000m e 1500m X 300m
Número de nós	50, 75, 100
Modelo de mobilidade	*Random waypoint*
Raio de alcance dos nós	120 e 250m
Velocidade dos nós	1m/s, 8m/s, 16m/s
Tempo de pausa dos nós	0m/s
Padrão de tráfego	UDP/CBR com 2 mensagens por segundo
Número de conexões simultâneas	15
Tempo de simulação	600s
Atacantes(%)	20%,40%
Modelo de propagação de rádio	*twoRay ground*
Especificações da camada MAC	IEEE 802.11

Tabela 6.2: Parâmetros de simulação do cenário 2

O **Cenário 3** tem como objetivo investigar os resultados perante o aumento do tráfego

de mensagens na rede. A rede criada para este cenário possui 75 nós distribuídos em uma área de 1500m X 300m, cada nó transmite seus sinais de rádio frequência em um raio de 250 metros. As conexões UDP por sua vez transmitem 2, 8, 16, 32 e 64 mensagens por segundo. Neste cenário foi definido que 20% e 40% dos nós são *blackhole*. Os parâmetros de simulações do cenário 3 estão resumidos na tabela 6.3.

Parâmetros	**Valores(s)**
Simulador	NS-2 (2.34)
Área de simulação	1500m X 300m
Número de nós	75
Modelo de mobilidade	*Random waypoint*
Raio de alcance dos nós	250m
Velocidade dos nós	1m/s, 8m/s, 16m/s
Tempo de pausa dos nós	0m/s
Padrão de tráfego	UDP/CBR com 2,8,16,32,64 mensagens por segundo
Número de conexões simultâneas	15
Tempo de simulação	600s
Atacantes(%)	20%,40%
Modelo de propagação de rádio	*twoRay ground*
Especificações da camada MAC	IEEE 802.11

Tabela 6.3: Parâmetros de simulação do cenário 3

6.3.1 Ambiente de rede hostil - Cenário 1

As figuras 6.1 a 6.6 apresentam os resultados obtidos para a taxa de entrega dos dados versus a variação do número de nós atacantes na rede, para os cenários 1(a) e 1(b). É possível observar que a taxa de entrega de todos os protocolos diminui com o aumento do número de nós atacantes na rede, como esperado. Contudo, o PRAB obteve melhores resultados independentemente do percentual de nós atacantes da rede.

Para ambos os cenários em redes com 100 nós, a taxa de entrega do protocolo PRAB com parâmetros $L = (2,4),(2,6)$ e $(3,6)$ é superior a 50%, mesmo nos casos onde 60% dos nós da rede são atacantes. Por sua vez, nesta mesma situação, os protocolos AODV e AOMDV originais entregam apenas 20% de seus pacotes.

Em redes com 75 nós, nos cenários 1(a) e 1(b), o parâmetro que apresenta os melhores resultados é o $L = (2,6)$, entregando mais de 40% dos pacotes de dados, mesmo nos

casos onde 60% dos nós da rede são atacantes. Os parâmetros $L = (2, 4)$ e $(3, 6)$ também mantém a taxa de entrega alta, com percentuais superiores a 35% na maioria dos casos, mesmo com 60% de nós atacantes na rede. Já os protocolos AODV e AOMDV entregam no máximo 20% dos pacotes em redes com mais de 50% de nós atacantes.

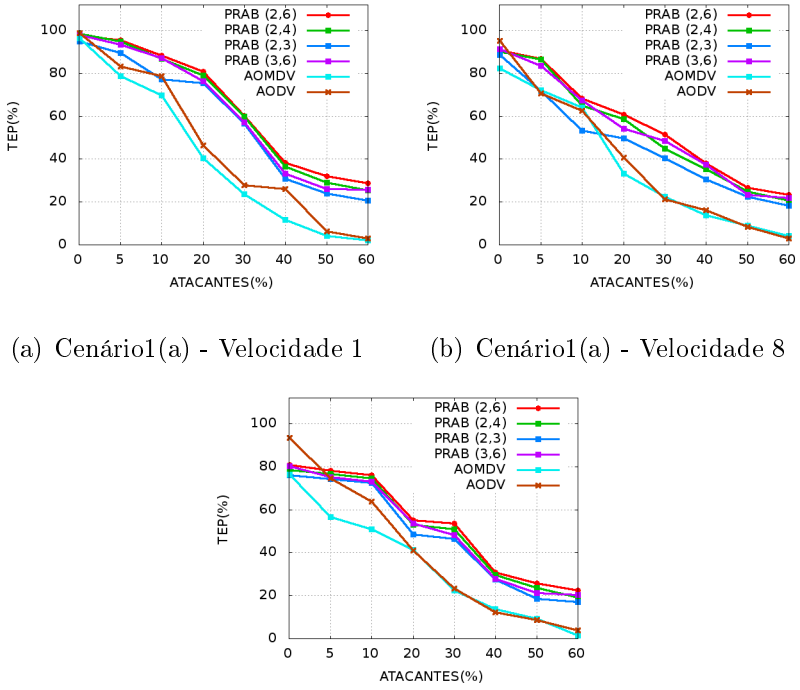
No cenário 1(b), em redes com 50 nós, onde 40% dos nós são atacantes, o PRAB com parâmetro $L = (2, 6)$ apresenta os maiores ganhos, entregando até 56,87% dos pacotes de dados. Neste mesmo caso, o cenário 1(a) com parâmetro $L = (2, 6)$ entrega mais 40% dos pacotes, enquanto o AOMDV e o AODV entregam apenas 6,6% e 10.10%, respectivamente. Os parâmetros $L = (2, 4)$ e $(3, 6)$ também foram superiores aos protocolos AOMDV e AODV em todos os percentuais analizados.

Entre os parâmetros analisados para o protocolo PRAB, o que apresenta os melhores resultados para a taxa de entrega é o $L = (2, 6)$, e o que apresenta os piores resultados é o $L = (2, 3)$. Isto ocorre porque para o parâmetro $L = (2, 6)$ cada pacote é dividido em seis partes e somente duas partes são necessárias para reconstruir a informação original, quatro destas partes podem ser descartadas por nós *blackhole*. Para o parâmetro $L = (2, 3)$, cada pacote é dividido em três partes, sendo que duas partes são necessárias para reconstruir a informação, somente uma parte pode ser descartada por nós *blackhole*.

Embora o PRAB com parâmetro $L = (2, 6)(k = 2, n = 6)$ proporcione os melhores resultados para a taxa de entrega, é o que possui o maior número de dados transmitidos pela rede, podendo ter uma sobrecarga extra de até $n-k$ partes para cada pacote de dados transmitido, ou seja, 4 partes do pacote original. O PRAB com parâmetro $L = (2, 3)$ exibe os piores resultados quando comparado aos outros parâmetros do protocolo PRAB, porém possui o menor número de dados transmitidos pela rede. Mesmo apresentando os piores resultados entre os parâmetros estudados, esta configuração entrega mais pacotes de dados que os protocolos AODV e AOMDV originais.

Nos cenários 1(a) e 1(b) com 50 nós na rede, os protocolos AODV e AOMDV tem melhor desempenho quanto a taxa de entrega em comparação ao PRAB com parâmetro $L = (2, 3)$ em apenas dois casos, com menos de 5% de nós atacantes e com 10%. Como mostra a figura 6.1(a). Com o aumento da velocidade dos nós, o protocolo AODV obtém

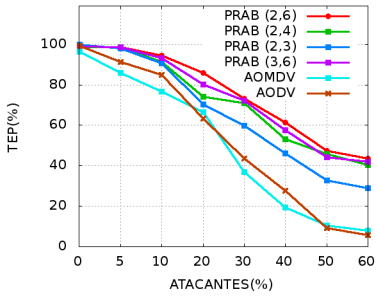
melhores resultados quando a rede possui 0% de nós atacantes, mas com o aumento da porcentagens de nós *blackhole*, o PRAB se torna superior para todos os parâmetros, com ganhos superiores a 50%.



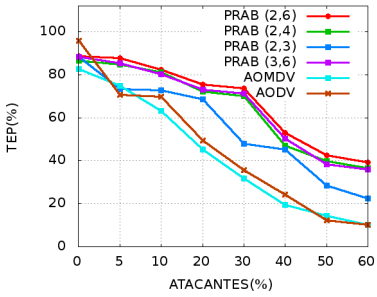
(a) Cenário1(a) - Velocidade 1 (b) Cenário1(a) - Velocidade 8

(c) Cenário1(a) - Velocidade 16

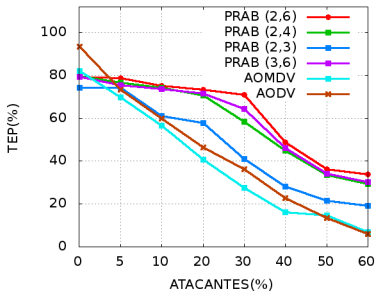
Figura 6.1: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós.



(a) Cenário1(a) - Velocidade 1

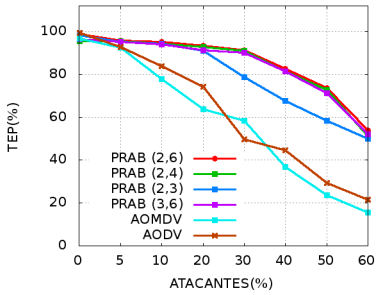


(b) Cenário1(a) - Velocidade 8

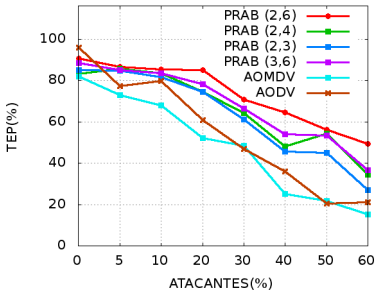


(c) Cenário1(a) - Velocidade 16

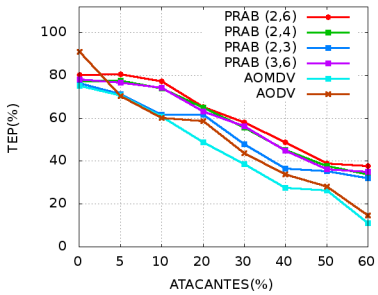
Figura 6.2: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós.



(a) Cenário1(a) - Velocidade 1

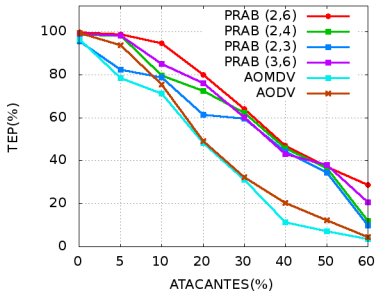


(b) Cenário1(a) - Velocidade 8

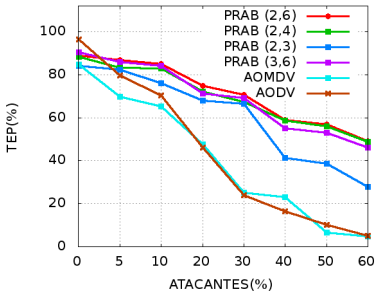


(c) Cenário1(a) - Velocidade 16

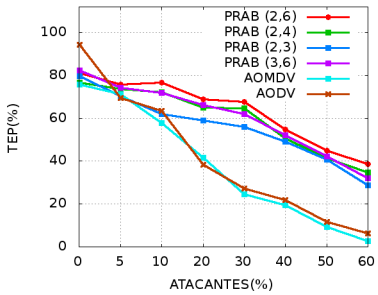
Figura 6.3: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós.



(a) Cenário1(b) - Velocidade 1

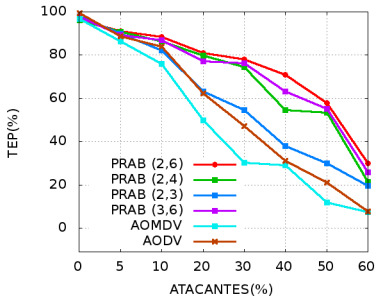


(b) Cenário1(b) - Velocidade 8

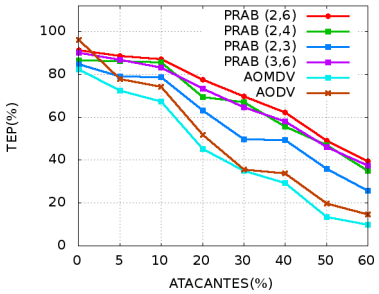


(c) Cenário1(b) - Velocidade 16

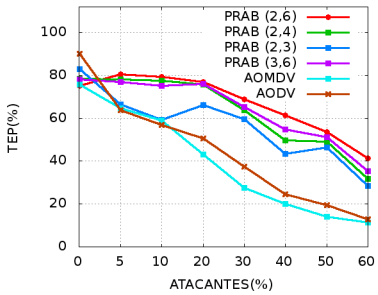
Figura 6.4: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 50 nós.



(a) Cenário1(b) - Velocidade 1

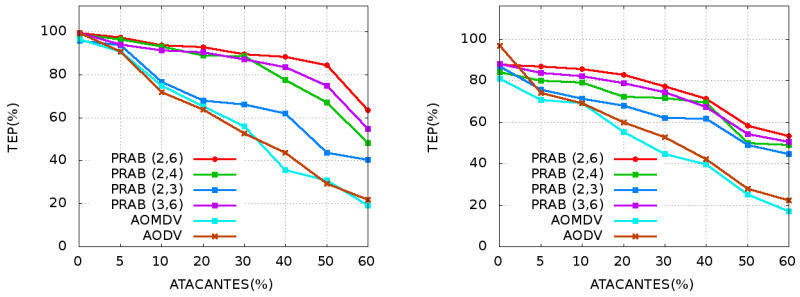


(b) Cenário1(b) - Velocidade 8

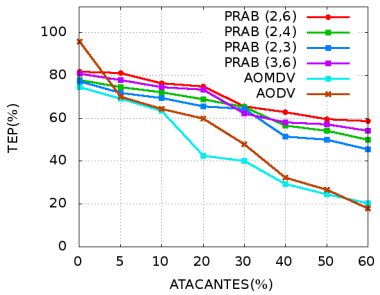


(c) Cenário1(b) - Velocidade 16

Figura 6.5: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 75 nós.



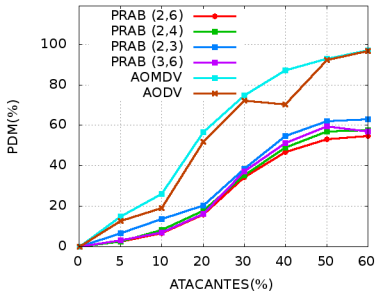
(a) Cenário1(b) - Velocidade 1 (b) Cenário1(b) - Velocidade 8



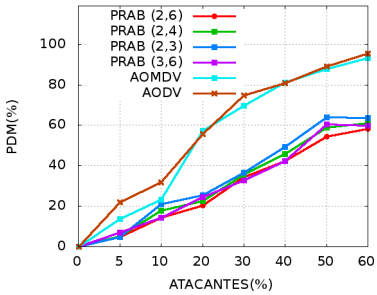
(c) Cenário1(b) - Velocidade 16

Figura 6.6: Taxa de entrega dos dados versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 100 nós.

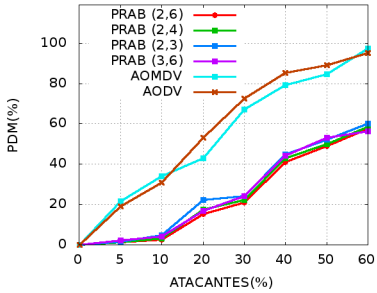
As figuras 6.7 a 6.12 apresentam os resultados obtidos para a porcentagem de pacotes de dados descartados por nós *blackhole* em relação a variação do número de nós atacantes na rede.



(a) Cenário1(a) - Velocidade 1

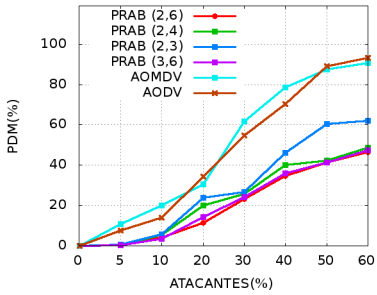


(b) Cenário1(a) - Velocidade 8

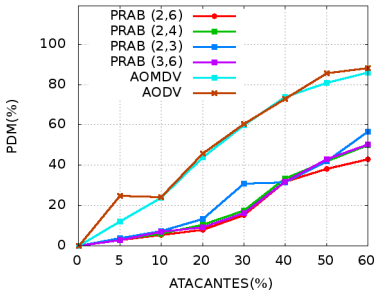


(c) Cenário1(a) - Velocidade 16

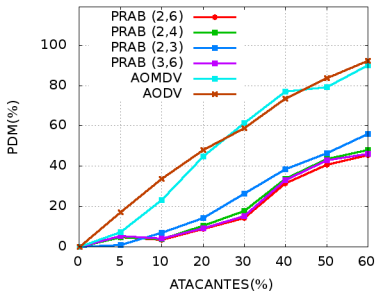
Figura 6.7: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós.



(a) Cenário1(a) - Velocidade 1

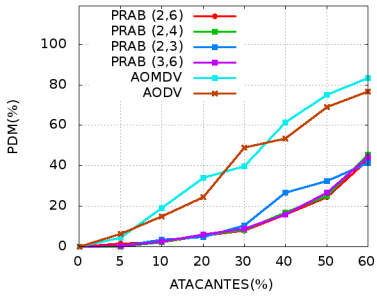


(b) Cenário1(a) - Velocidade 8

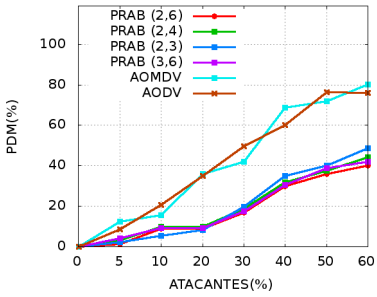


(c) Cenário1(a) - Velocidade 16

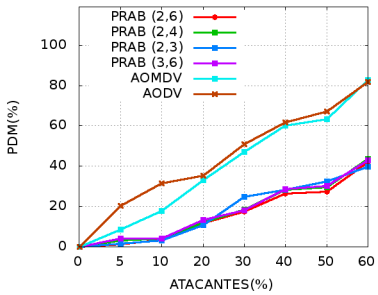
Figura 6.8: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós.



(a) Cenário1(a) - Velocidade 1

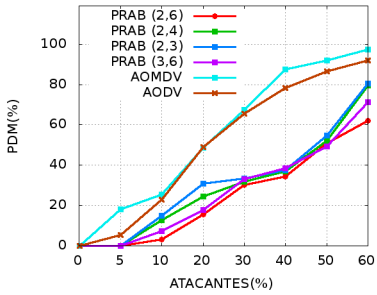


(b) Cenário1(a) - Velocidade 8

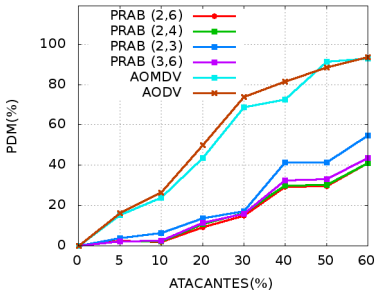


(c) Cenário1(a) - Velocidade 16

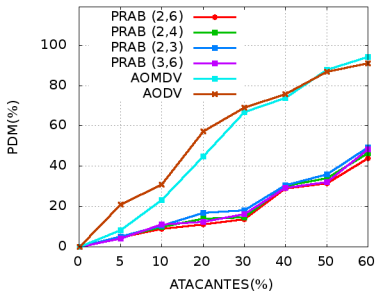
Figura 6.9: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós.



(a) Cenário1(b) - Velocidade 1

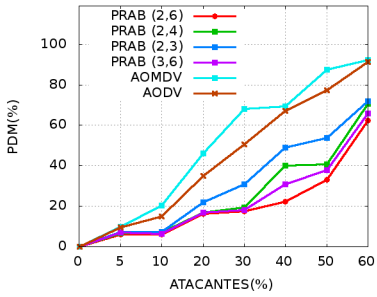


(b) Cenário1(b) - Velocidade 8

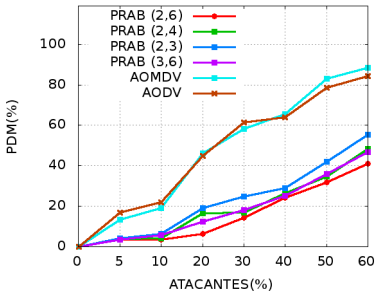


(c) Cenário1(b) - Velocidade 16

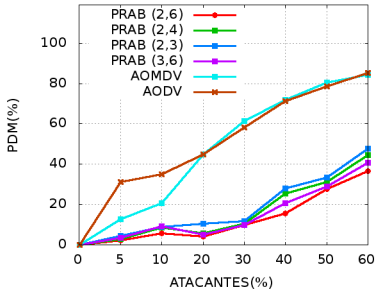
Figura 6.10: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 50 nós.



(a) Cenário1(b) - Velocidade 1

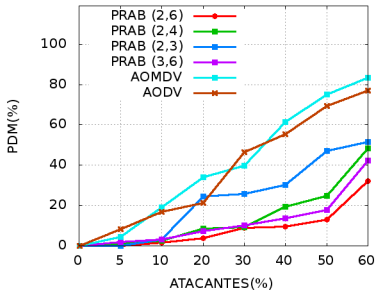


(b) Cenário1(b) - Velocidade 8

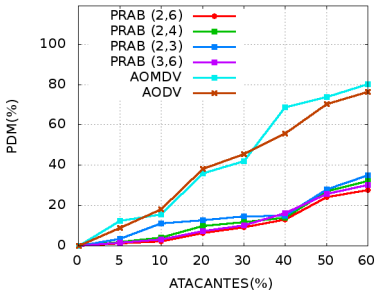


(c) Cenário1(b) - Velocidade 16

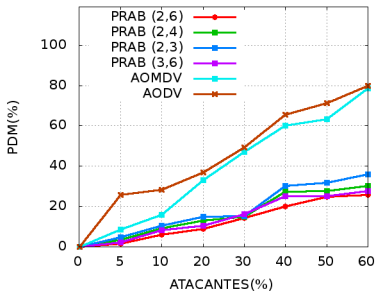
Figura 6.11: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 75 nós.



(a) Cenário1(b) - Velocidade 1



(b) Cenário1(b) - Velocidade 8



(c) Cenário1(b) - Velocidade 16

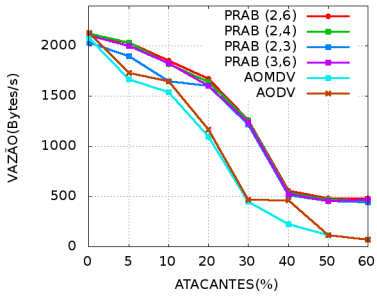
Figura 6.12: Quantidade de pacotes de dados descartados por nós *blackhole* versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 100 nós.

Percebe-se nas figuras 6.7 a 6.12 que o aumento do percentual de atacantes aumenta também a porcentagem de pacotes descartados para os cenários analisados. Este resultado é esperado porque conforme aumenta-se o número de nós atacantes, também cresce o número de rotas comprometidas pela presença deles. Contudo, nota-se que o PRAB reduz o número de pacotes descartados em relação aos descartes do AODV e do AOMDV, independentemente do percentual de atacantes. Os ganhos do PRAB com parâmetro $L = (2, 6)$ são superiores em até 45% no cenário 1(a). No cenário 1(b), os ganhos são ainda maiores, chegando a 52%.

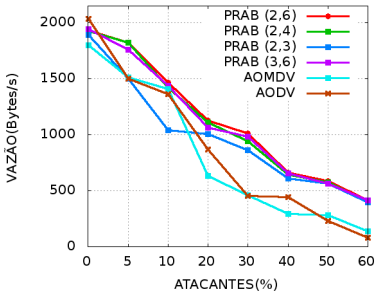
O PRAB apresenta melhores resultados para todos os seus parâmetros, independente do tamanho da área da rede, do número de nós na rede, do percentual de atacantes ou da velocidade dos nós. Dentre os parâmetros estudados, o que descarta menos pacotes de dados pela ação de *blackholes* é o $L = (2, 6)$, seguido dos parâmetros $L = (3, 6)$, $L = (2, 4)$ e $L = (2, 3)$. Com estes resultados, pode-se verificar que o protocolo PRAB, em todos os seus parâmetros, é mais tolerante à ação de nós *blackhole*. O parâmetro $L = (2, 3)$ é o menos resistente a ações de nós *blackhole*, pois tolera apenas o descarte de uma parte, enquanto o parâmetro $L = (2, 6)$, que é o mais resistente, tolera o descarte de até quatro partes.

A maioria dos descartes de pacotes de dados que ocorrem para o cenário 1 são provenientes da ação de nós *blackhole*, e não de outras naturezas, como congestionamento e estouro de pilha. Desta forma, os gráficos apresentados para a quantidade de pacotes de dados descartados por nós *blackhole* são complementos dos gráficos apresentados para a taxa de entrega dos pacotes de dados.

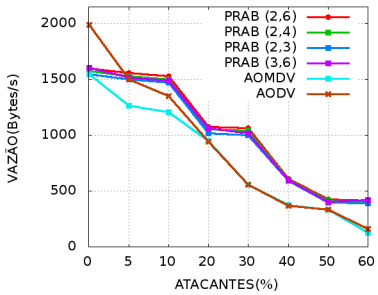
As figuras 6.13 a 6.18 mostram os resultados obtidos para a vazão com a variação do número de nós atacantes *blackhole* na rede. É importante ressaltar que a vazão é a quantidade de dados transferidos entre dois nós durante o intervalo de tempo em que permanecem conectados, enquanto a taxa de entrega é a proporção de pacotes de dados entregues ao destino em relação à quantidade de pacotes de dados enviados pela origem.



(a) Cenário1(a) - Velocidade 1

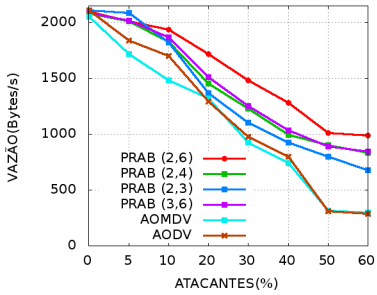


(b) Cenário1(a) - Velocidade 8

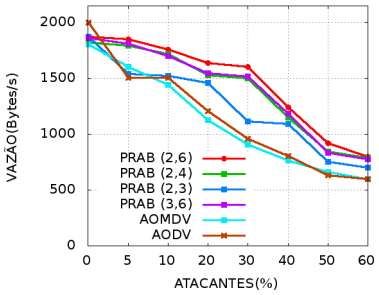


(c) Cenário1(a) - Velocidade 16

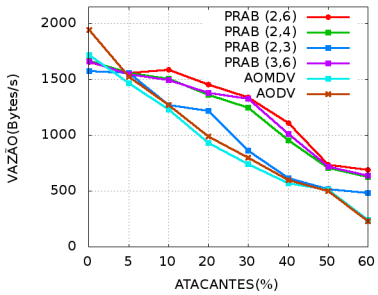
Figura 6.13: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1.000m X 1.000m e 50 nós.



(a) Cenário1(a) - Velocidade 1

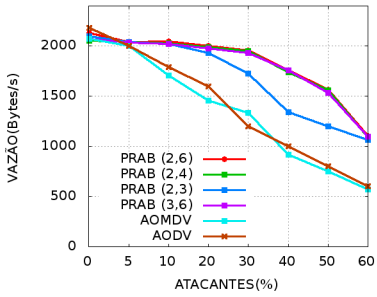


(b) Cenário1(a) - Velocidade 8

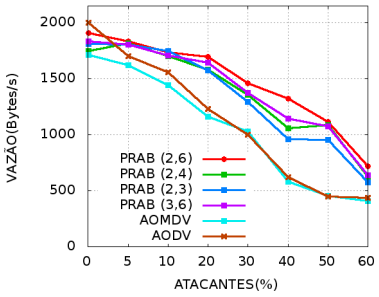


(c) Cenário1(a) - Velocidade 16

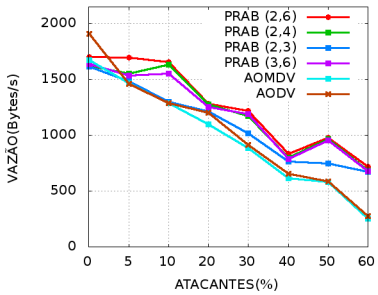
Figura 6.14: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1.000m X 1.000m e 75 nós.



(a) Cenário1(a) - Velocidade 1

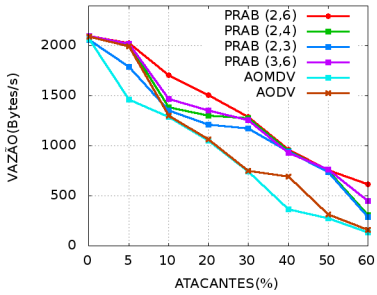


(b) Cenário1(a) - Velocidade 8

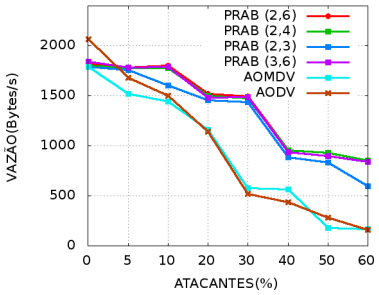


(c) Cenário1(a) - Velocidade 16

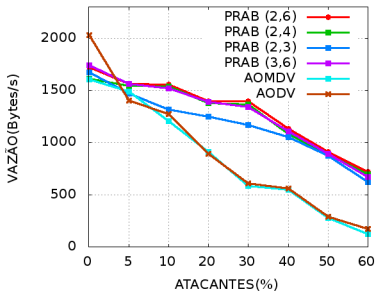
Figura 6.15: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1.000m X 1.000m e 100 nós.



(a) Cenário1(b) - Velocidade 1

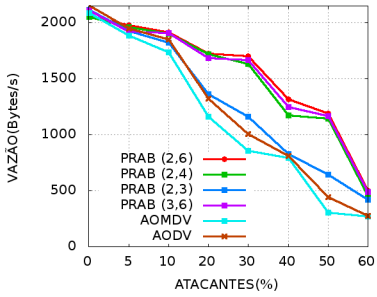


(b) Cenário1(b) - Velocidade 8

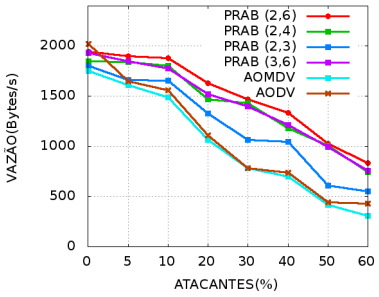


(c) Cenário1(b) - Velocidade 16

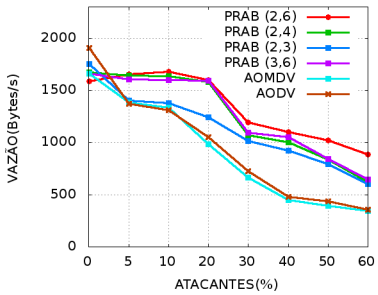
Figura 6.16: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1500m X 300m e 50 nós.



(a) Cenário1(b) - Velocidade 1

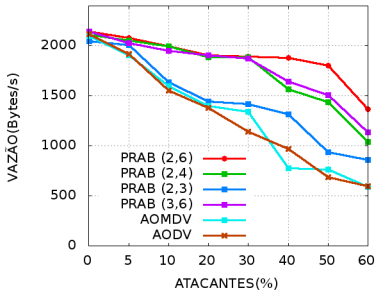


(b) Cenário1(b) - Velocidade 8

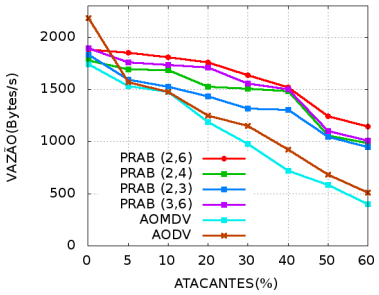


(c) Cenário1(b) - Velocidade 16

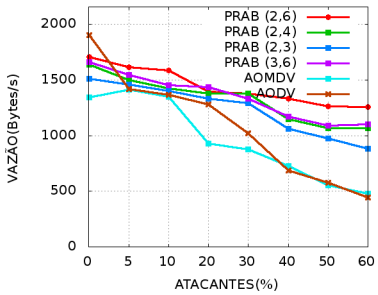
Figura 6.17: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1500m X 300m e 75 nós.



(a) Cenário1(b) - Velocidade 1



(b) Cenário1(b) - Velocidade 8



(c) Cenário1(b) - Velocidade 16

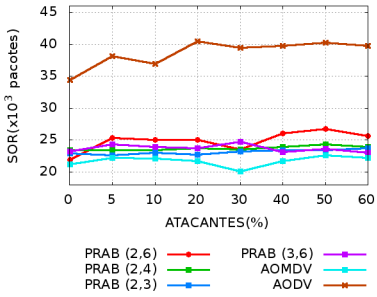
Figura 6.18: Quantidade de dados transferidos versus variação do percentual de atacantes *black-hole* - rede com 1500m X 300m e 100 nós.

Observa-se nas figuras 6.13 a 6.18, que o aumento do percentual de atacantes diminui a vazão para os cenários 1(a) e 1(b), como esperado. Entretanto, o PRAB obteve melhores resultados em relação ao AODV e AOMDV, independentemente do percentual de nós atacantes na rede.

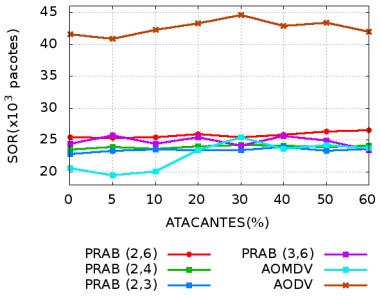
No cenário 1(b), com 50 nós na rede, velocidade de 8m/s e 60% de atacantes, o PRAB com parâmetro $L = (2, 6)$ consegue transferir até cinco vezes mais dados do que os protocolos AOMDV e AODV originais. No cenário 1(a), os ganhos são ainda maiores, pois o PRAB com parâmetro $L = (2, 6)$ consegue transferir até sete vezes mais dados do que os outros protocolos, conforme mostra a figura 6.13(a).

Em alguns poucos casos, com 50 nós na rede e com no máximo 10% de nós atacantes, os protocolos AODV e AOMDV tem melhor desempenho em comparação ao PRAB com parâmetro $L = (2, 3)$, conforme mostra a figura 6.13(a) e 6.13(b). Estes fatos são observados porque a taxa de entrega dos protocolos AODV e AOMDV são maiores. Com o aumento da velocidade dos nós, o protocolo AODV obteve melhores resultados quando a rede possui 0% de nós atacantes, mas com o acréscimo da porcentagen de nós *blackhole*, o PRAB se torna superior para todos os parâmetroes, pois consegue entregar mais dados, tendo assim uma vazão maior. Verifica-se também, na maioria do casos, que o aumento do número de nós na rede implica no crescimento da quantidade de dados transferidos, principalmente para o protocolo PRAB.

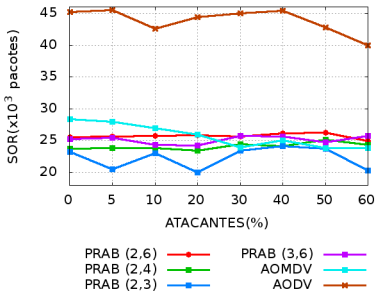
As figuras 6.19 a 6.24 demonstram os resultados obtidos para a sobrecarga de roteamento com a variação do número de nós atacantes *blackhole* na rede.



(a) Cenário1(a) - Velocidade 1

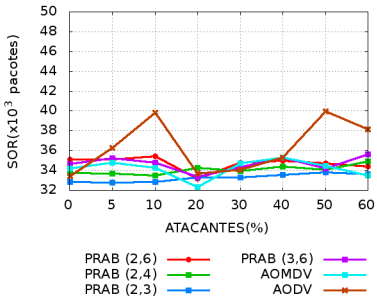


(b) Cenário1(a) - Velocidade 8

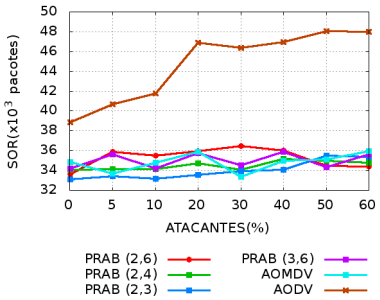


(c) Cenário1(a) - Velocidade 16

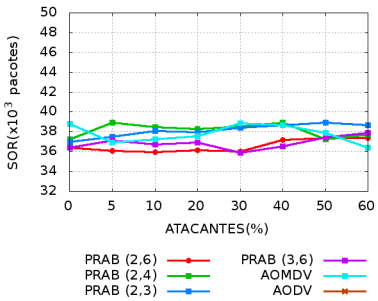
Figura 6.19: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós.



(a) Cenário1(a) - Velocidade 1

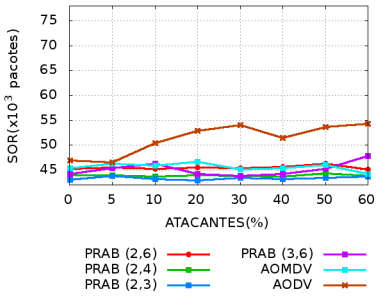


(b) Cenário1(a) - Velocidade 8

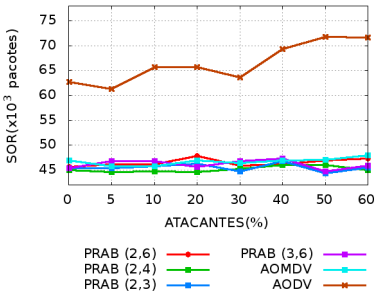


(c) Cenário1(a) - Velocidade 16

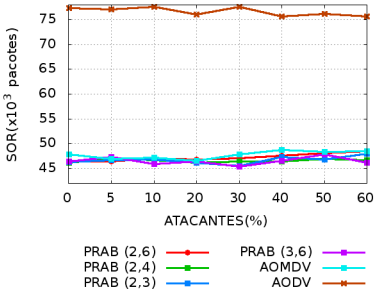
Figura 6.20: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós.



(a) Cenário1(a) - Velocidade 1

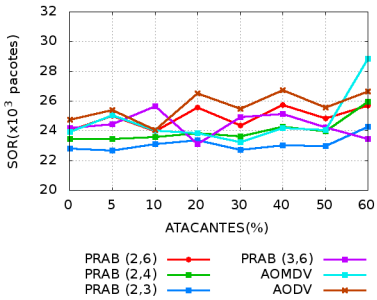


(b) Cenário1(a) - Velocidade 8

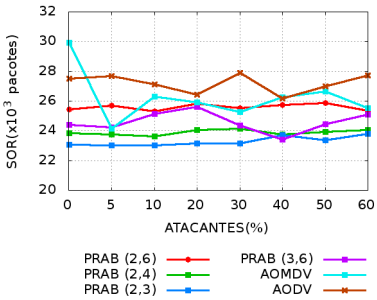


(c) Cenário1(a) - Velocidade 16

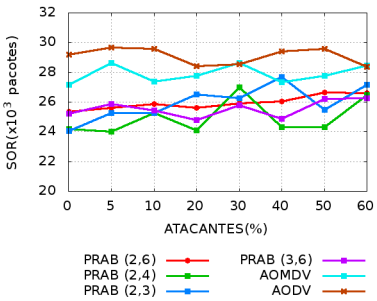
Figura 6.21: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós.



(a) Cenário1(b) - Velocidade 1

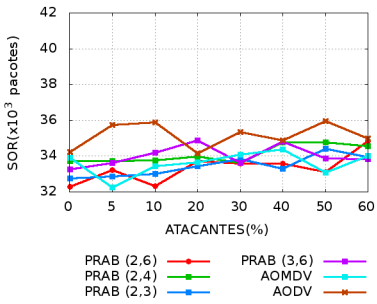


(b) Cenário1(b) - Velocidade 8

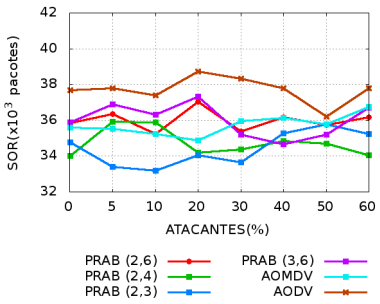


(c) Cenário1(b) - Velocidade 16

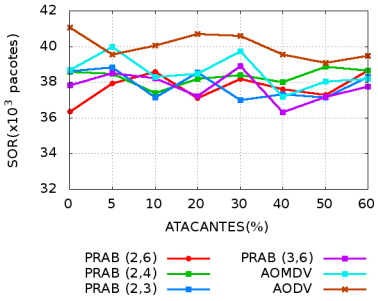
Figura 6.22: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 50 nós.



(a) Cenário1(b) - Velocidade 1

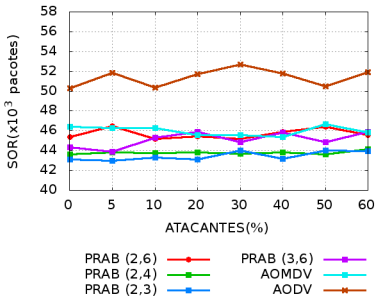


(b) Cenário1(b) - Velocidade 8

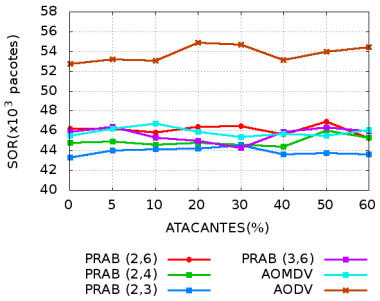


(c) Cenário1(b) - Velocidade 16

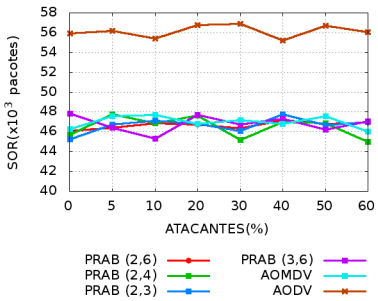
Figura 6.23: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 75 nós.



(a) Cenário1(b) - Velocidade 1



(b) Cenário1(b) - Velocidade 8



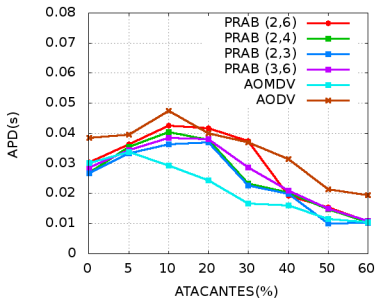
(c) Cenário1(b) - Velocidade 16

Figura 6.24: Sobrecarga versus variação do percentual de atacantes *blackhole* - rede com 1.500m X 300m e 100 nós.

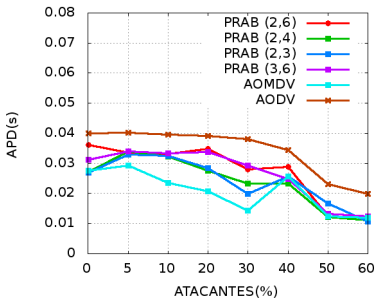
Nota-se nas figuras 6.19 a 6.24, para os cenários 1(a) e 1(b), que a sobrecarga do protocolo PRAB e AOMDV original se mantiveram semelhantes para todos os percentuais de nós atacantes da rede. Isso ocorre por que o processo de descoberta de rotas do PRAB e do AOMDV são iguais. As alterações realizadas no AOMDV para o desenvolvimento do PRAB não alteraram o processo de descoberta de rotas. Verifica-se também que a sobrecarga do protocolo AODV se manteve superior a dos outros protocolos nos cenário 1(a) e 1(b) para todos os percentuais de nós atacantes da rede, mas com maior destaque no cenário 1(a). Tal fato ocorre, pois para qualquer falha de rota o AODV precisa iniciar uma operação de descoberta de rotas, o que implica no envio de pacotes de roteamento para toda rede. O AOMDV e o PRAB, que possuem rotas alternativas em suas tabelas, não precisam iniciar uma operação de descoberta em qualquer falha, diminuindo assim o número de pacotes de roteamento transmitidos pela rede.

Outro evento que merece destaque refere-se ao crescimento da sobrecarga de roteamento quando ocorre o aumento da velocidade dos nós na rede, com maior magnitude para o AODV. Este evento decorre do aumento da mobilidade dos nós provocar o crescimento do número de rotas com falha.

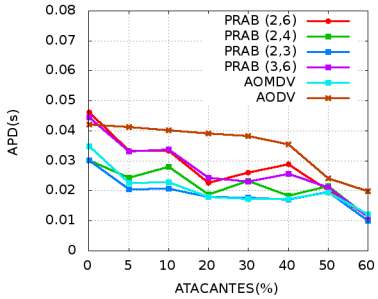
As figura 6.25 a 6.30 demonstram os resultados obtidos para a latência na entrega dos dados com a variação do número de nós atacantes *blackhole* na rede, para os cenários 1(a) e 1(b).



(a) Cenário1(a) - Velocidade 1

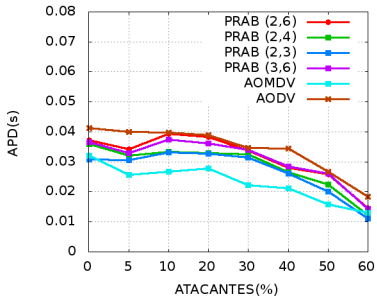


(b) Cenário1(a) - Velocidade 8

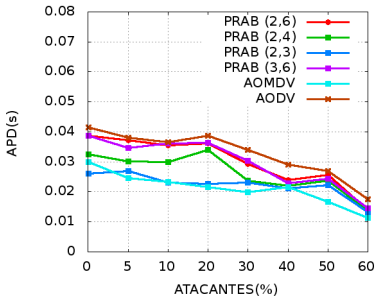


(c) Cenário1(a) - Velocidade 16

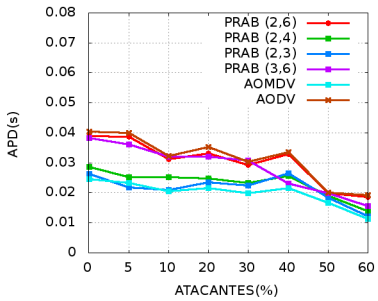
Figura 6.25: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 50 nós.



(a) Cenário1(a) - Velocidade 1

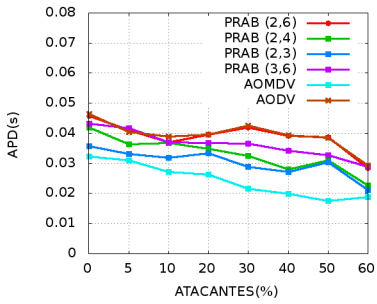


(b) Cenário1(a) - Velocidade 8

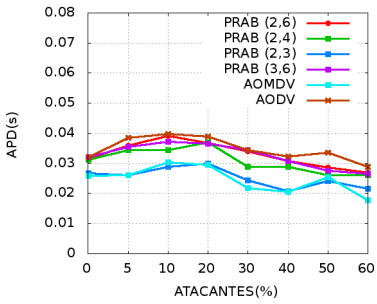


(c) Cenário1(a) - Velocidade 16

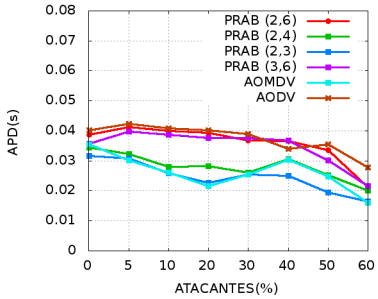
Figura 6.26: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 75 nós.



(a) Cenário1(a) - Velocidade 1

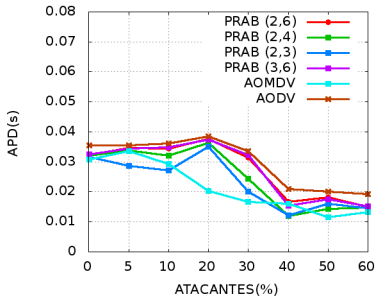


(b) Cenário1(a) - Velocidade 8

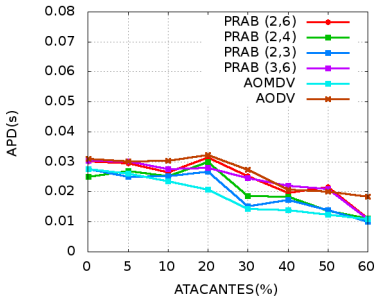


(c) Cenário1(a) - Velocidade 16

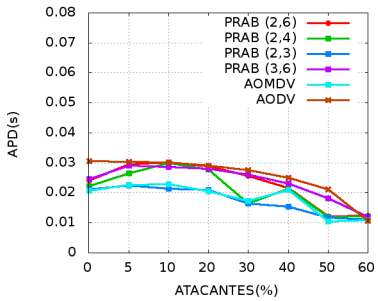
Figura 6.27: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1.000m X 1.000m e 100 nós.



(a) Cenário1(b) - Velocidade 1

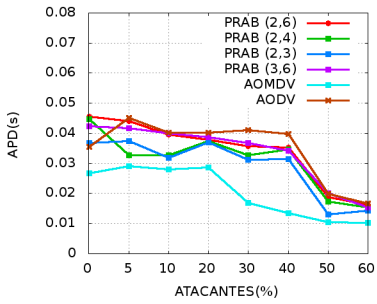


(b) Cenário1(b) - Velocidade 8

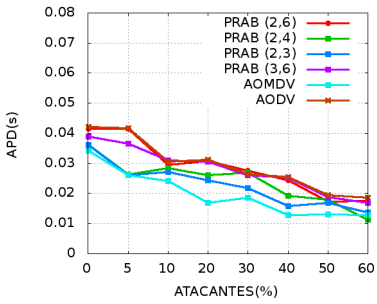


(c) Cenário1(b) - Velocidade 16

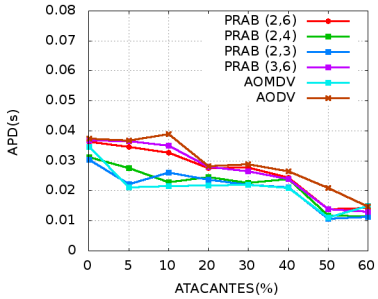
Figura 6.28: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 50 nós.



(a) Cenário1(b) - Velocidade 1

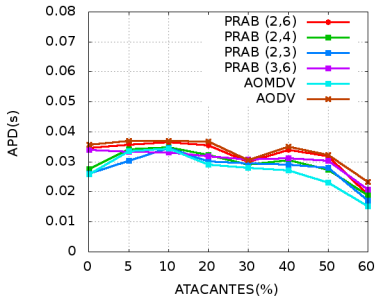


(b) Cenário1(b) - Velocidade 8

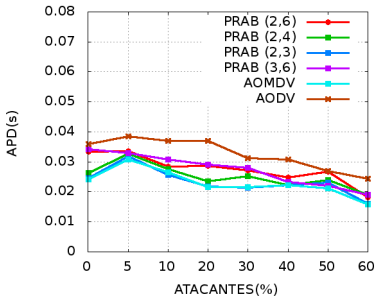


(c) Cenário1(b) - Velocidade 16

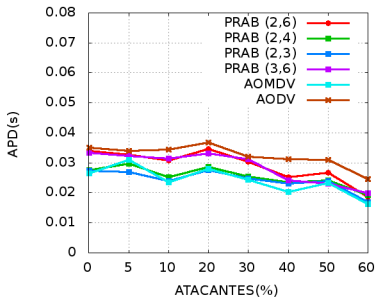
Figura 6.29: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 75 nós.



(a) Cenário1(b) - Velocidade 1



(b) Cenário1(b) - Velocidade 8



(c) Cenário1(b) - Velocidade 16

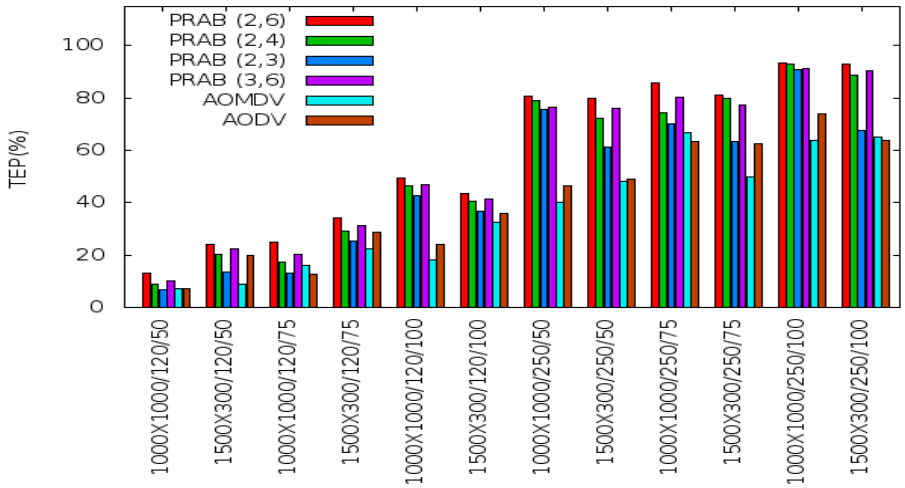
Figura 6.30: Atraso fim-a-fim dos pacotes de dados versus variação do percentual de atacantes *blackhole* - rede com 1500m X 300m e 100 nós.

Nota-se nas figuras 6.25 a 6.30, que a latência do protocolo AODV obteve valores mais elevados em relação ao AOMDV e PRAB. Isto ocorre porque a disponibilidade das rotas alternativas presente no AOMDV e PRAB, em caso de falhas de rotas, elimina a latência da descoberta de rotas, fazendo com que seus resultados sejam melhores. Como é esperado, a latência do protocolo PRAB foi maior em relação à latência do protocolo AOMDV original. Pois para o PRAB a latência é a diferença entre o tempo em que a primeira parte saiu da origem e a última parte necessária para reconstruir a informação chegou ao destino. O PRAB com parâmetro $L = (2, 6)$ teve os maiores valores de latência, seguido dos parâmetros $L = (3, 6)$ e $L = (2, 4)$. É possível observar também que com aumento do percentual de nós atacantes na rede, a latência diminui ligeiramente. Tal fato ocorre devido à redução do tráfego de dados provocada pelos descartes dos atacantes.

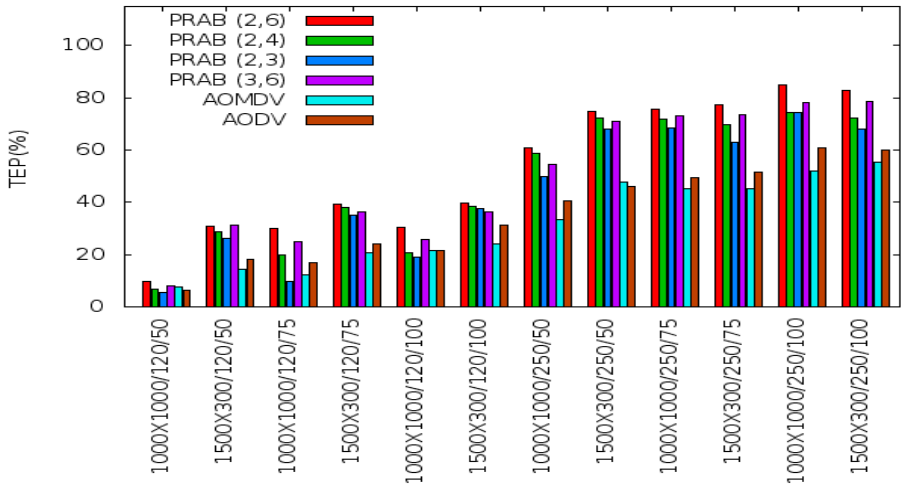
Uma análise precipitada pode levar à conclusão de que o PRAB reduz o desempenho da rede em relação ao AOMDV original por possuir uma latência mais alta. Porém, o PRAB entrega mais pacotes de dados aos destinos que o AOMDV original, o que mantém por mais tempo o tráfego de dados na rede.

6.3.2 Variando a densidade da rede - cenário 2

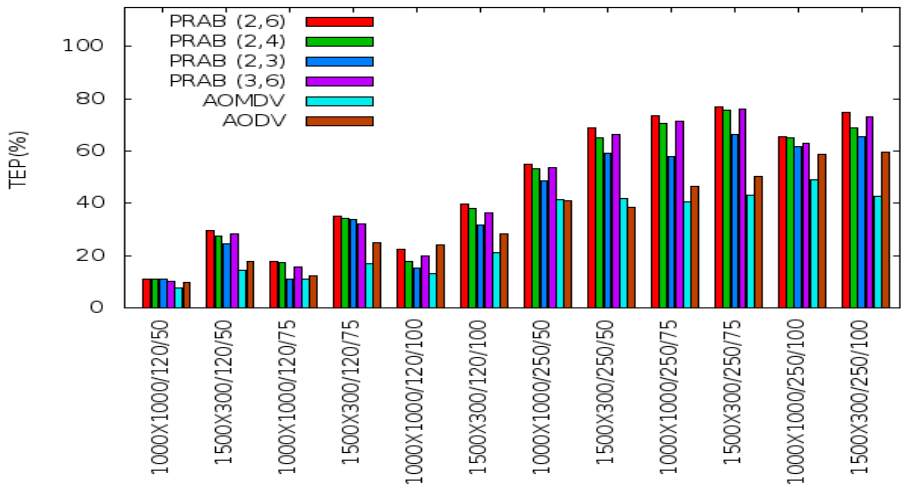
As figuras 6.31 e 6.32 mostram os resultados obtidos para a taxa de entrega dos dados com a variação da densidade na rede, em redes com 20% e 40% de nós atacantes, respectivamente. Pode-se notar que quanto mais densa a rede, maior é taxa de entrega para todos os protocolos. Contudo, o PRAB apresenta melhores resultados em relação ao AOMDV e AODV originais para todos os casos. Nos gráficos pode-se observar notações da seguinte forma: 1000X1000/120/50, 1500X300/250/100, a primeira notação significa que a rede tem uma área de 1000m X 1000m, cada nó transmite seus sinais em um raio de 120 metros e a rede possui 50 nós. A segunda notação significa que a rede tem uma área de 1500m X 300m, cada nó transmite seus sinais em um raio de 250 metros e a rede possui 100 nós. Todas a outras notações seguem este mesmo padrão.



(a) Cenário2 - Velocidade 1

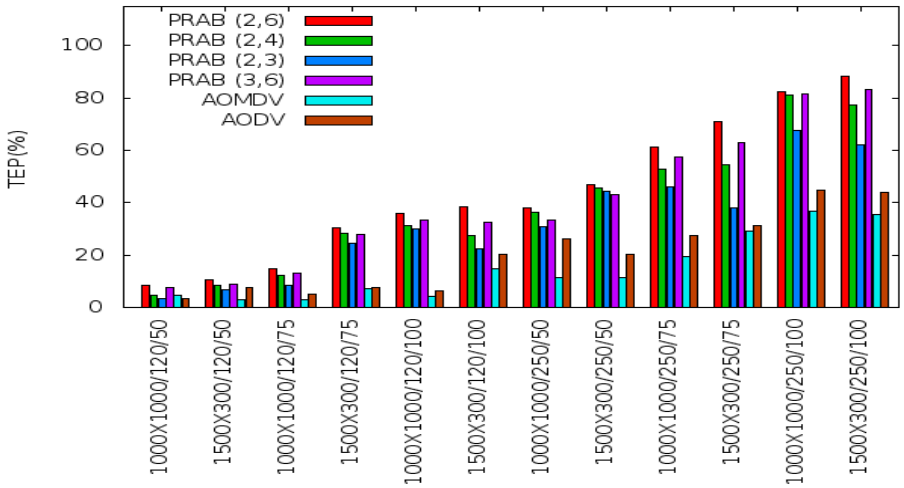


(b) Cenário2 - Velocidade 8

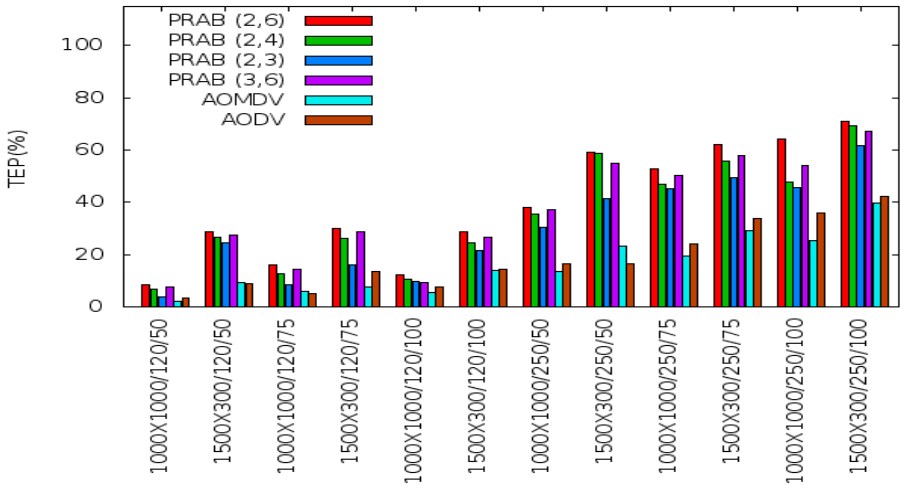


(c) Cenário2 - Velocidade 16

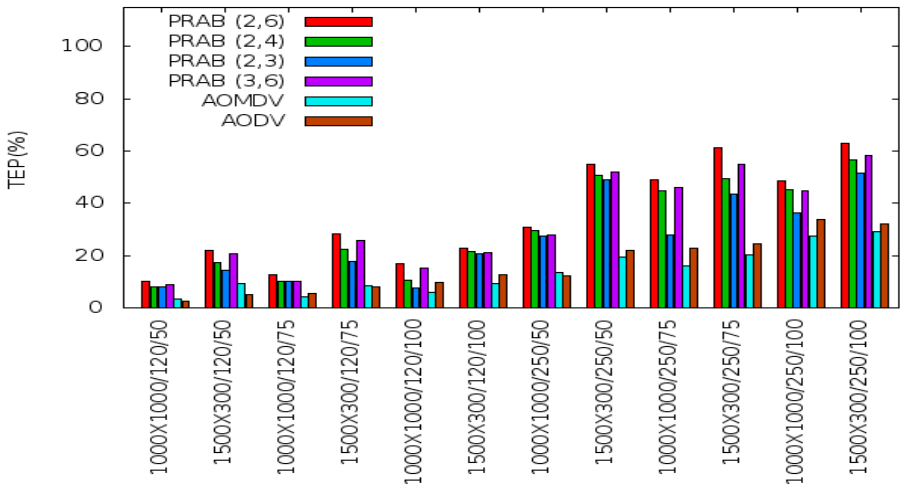
Figura 6.31: Taxa de entrega dos dados versus densidade da rede - 20% de nós *blackhole* na rede.



(a) Cenário2 - Velocidade 1



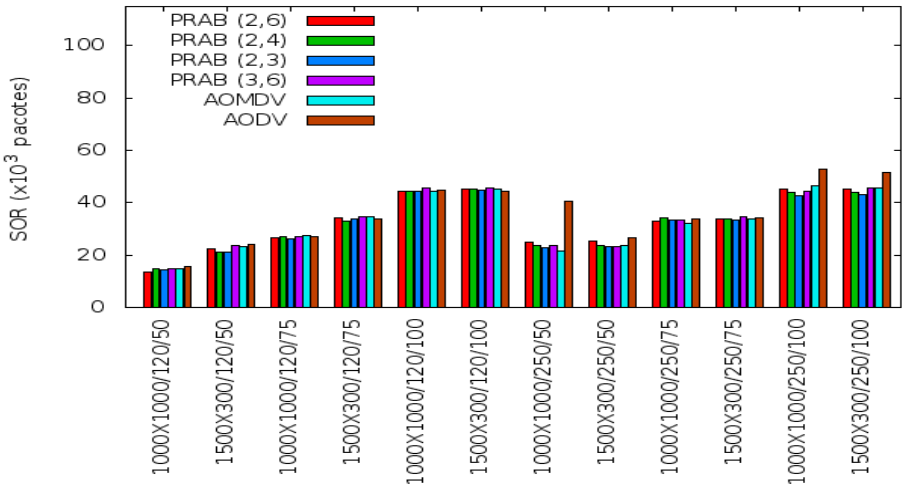
(b) Cenário2 - Velocidade 8



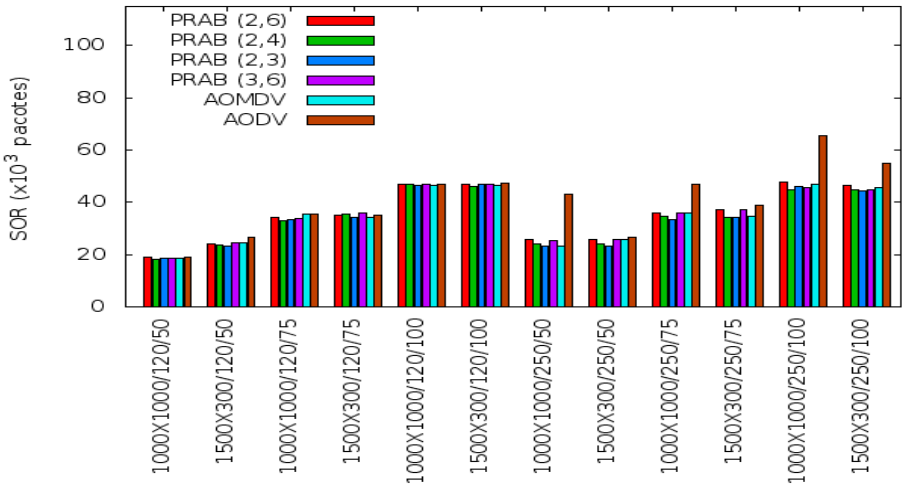
(c) Cenário2 - Velocidade 16

Figura 6.32: Taxa de entrega dos dados versus densidade da rede - 40% de nós *blackhole* na rede.

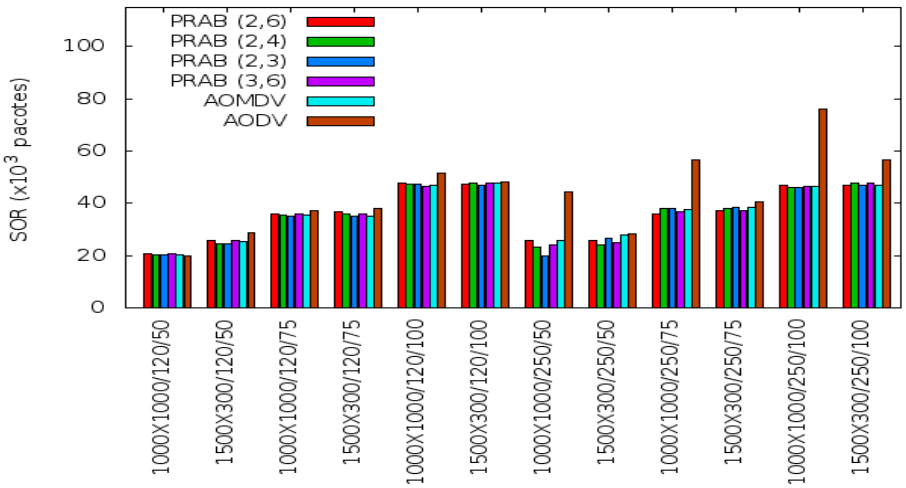
As figuras 6.33 e 6.34 mostram os resultados obtidos para a sobrecarga de roteamento com a variação da densidade na rede, em redes com 20% e 40% de nós atacantes respectivamente. É possível observar nas figuras 6.33 e 6.34, que na maioria dos casos, quanto mais densa a rede, maior é a sobrecarga de roteamento para todos os protocolos. Tal fato ocorre porque o aumento do número de nós na rede provoca o aumento do número de mensagens de roteamento enviadas. O AODV continua sendo o protocolo com maior sobrecarga, enquanto o AOMDV e o PRAB se mantém semelhantes.



(a) Cenário2 - Velocidade 1

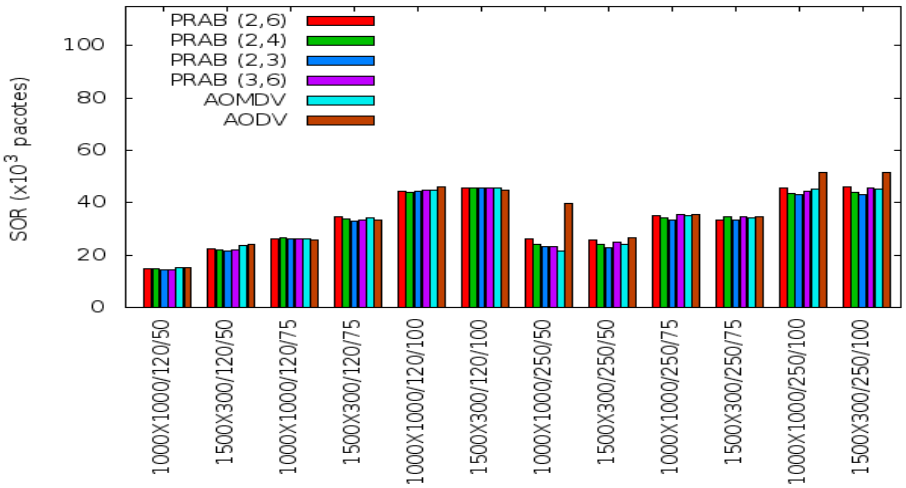


(b) Cenário2 - Velocidade 8

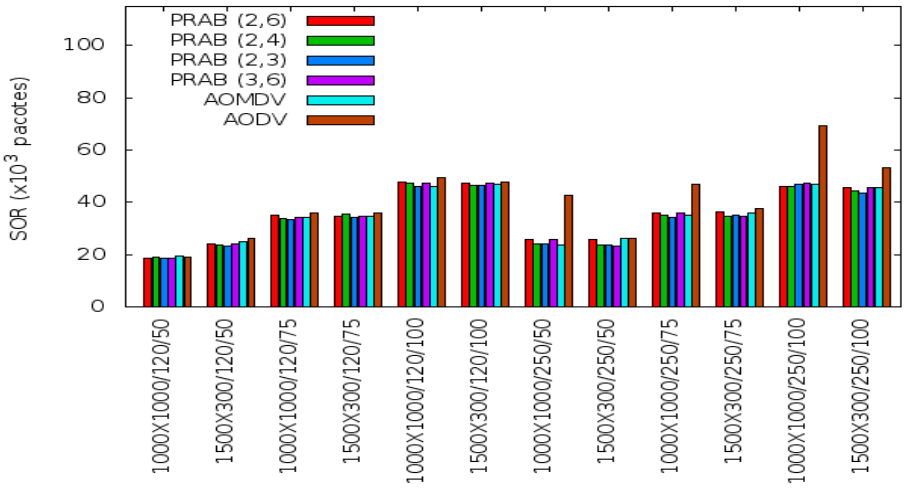


(c) Cenário2 - Velocidade 16

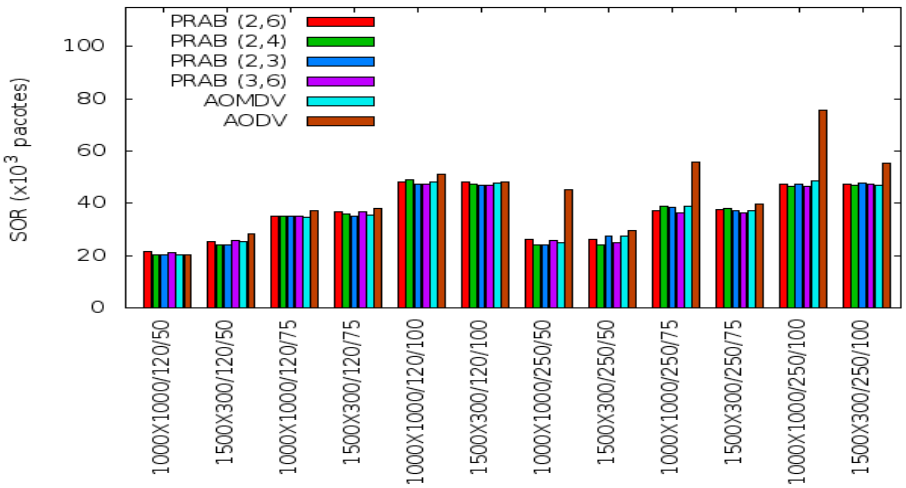
Figura 6.33: Sobrecarga versus densidade da rede - 20% de nós *blackhole* na rede.



(a) Cenário2 - Velocidade 1



(b) Cenário2 - Velocidade 8

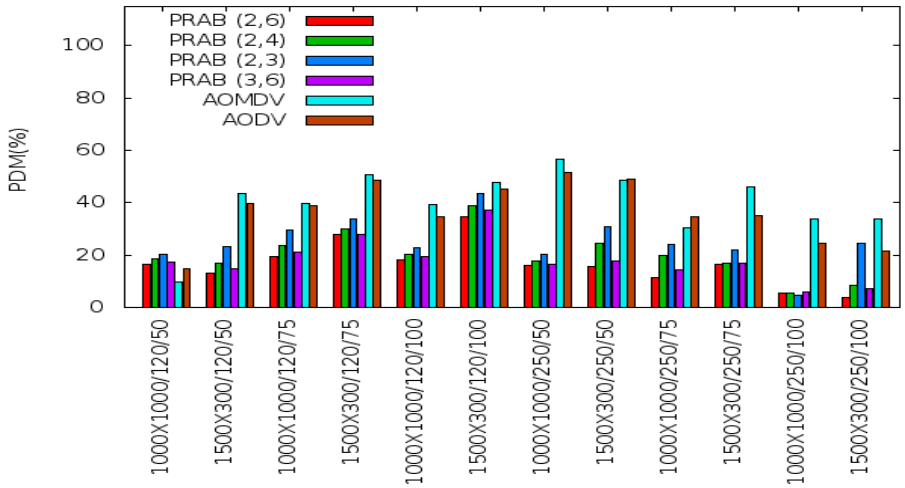


(c) Cenário2 - Velocidade 16

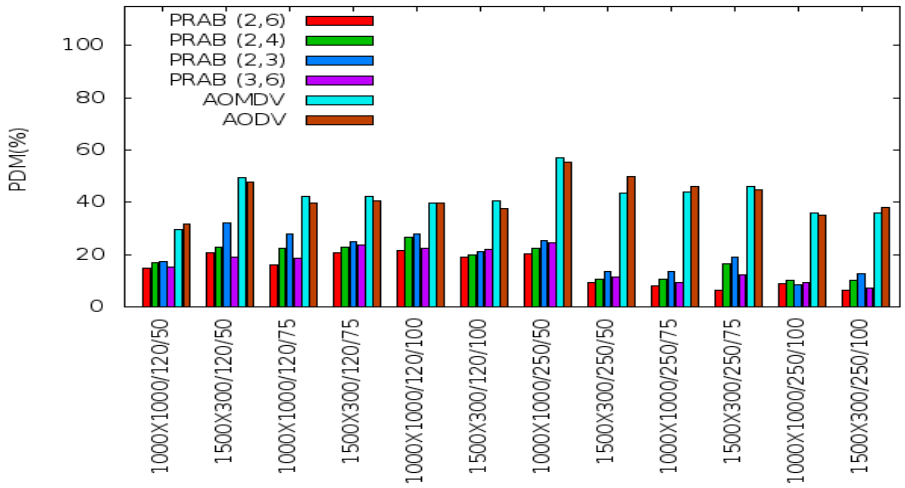
Figura 6.34: Sobrecarga versus densidade da rede - 40% de nós *blackhole* na rede.

As figuras 6.35 e 6.36 mostram os resultados obtidos para a porcentagem de pacotes de dados descartados por nós maliciosos com a variação da densidade na rede, em redes com 20% e 40% de nós atacantes, respectivamente. Em redes com raio de 120m o número de pacotes descartados por nós maliciosos é baixo, pois a maioria dos pacotes são descartados pela falta de conectividade. Assim, nota-se nas figuras 6.35 e 6.36, que em redes com raio de 120m, o número de pacotes descartados pela ação de nós *blackhole* se mantêm constante ou aumenta levemente com o crescimento da densidade da rede. Esta situação é constatada porque neste tipo de rede o aumento do número de nós torna a rede mais conexa, aumentando o número de rotas válidas e o número de pacotes transmitidos pela rede, consequentemente aumentando também o número de pacotes descartados por nós maliciosos.

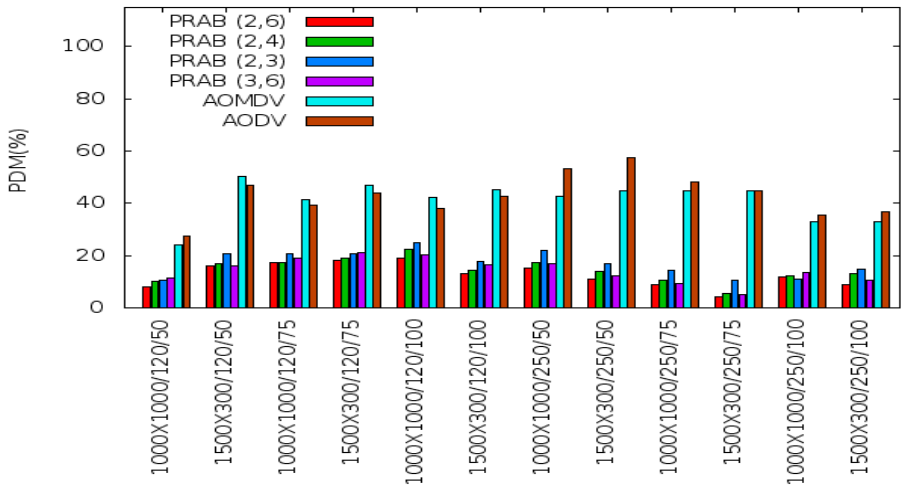
Redes com raio de 250m são conexas para 50, 75 ou 100 nós. Assim, o número de rotas válidas e o de pacotes transmitidos na rede são altos e, a maioria dos descartes são causados pelos nós *blackhole*. Em redes conexas, o aumento do número de nós faz com que os protocolos, principalmente o PRAB, consigam entregar mais pacotes de dados, logo o número de pacotes descartados por nós *blackhole* tende a diminuir.



(a) Cenário2 - Velocidade 1

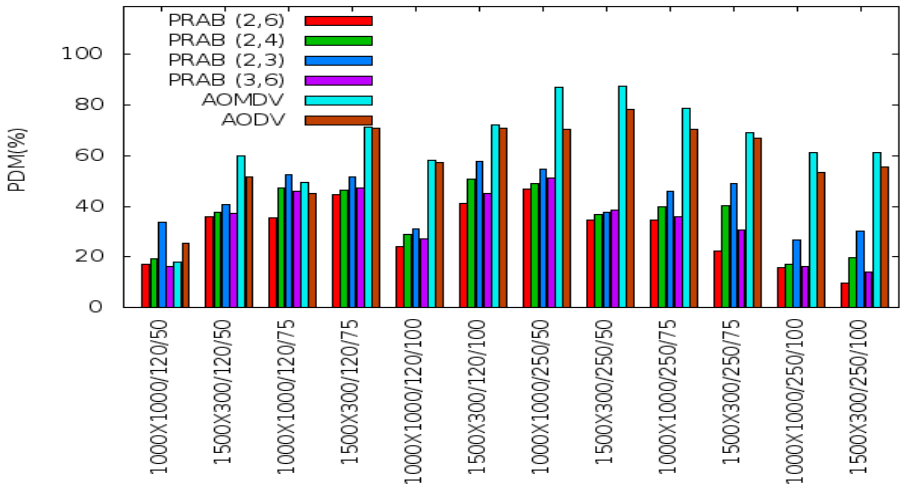


(b) Cenário2 - Velocidade 8

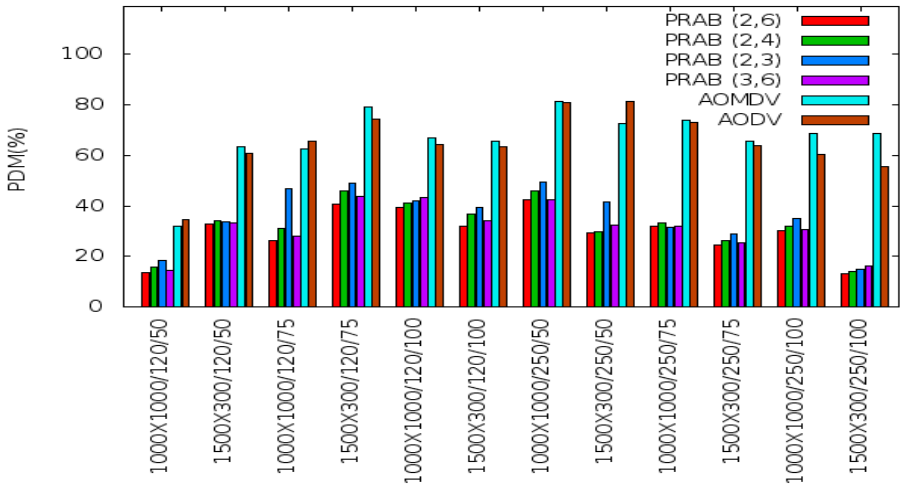


(c) Cenário2 - Velocidade 16

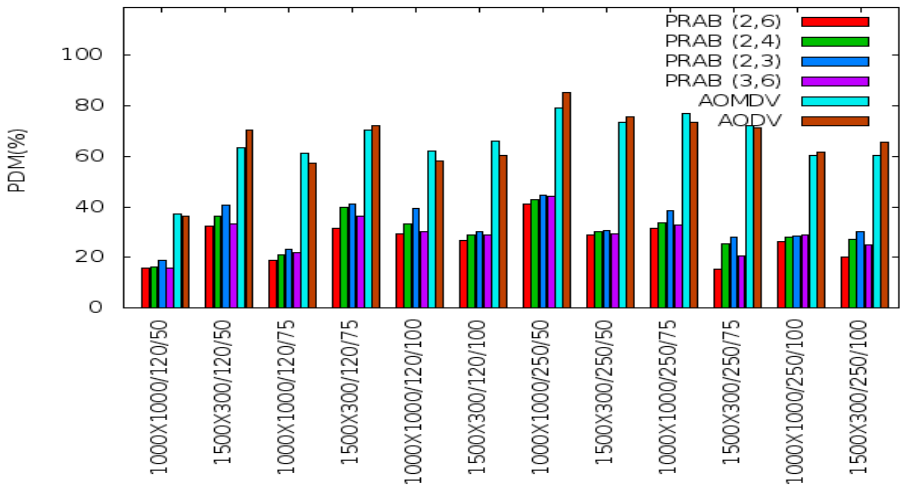
Figura 6.35: Quantidade de pacotes de dados descartados por nós *blackhole* versus densidade da rede - 20% de nós *blackhole* na rede.



(a) Cenário2 - Velocidade 1



(b) Cenário2 - Velocidade 8

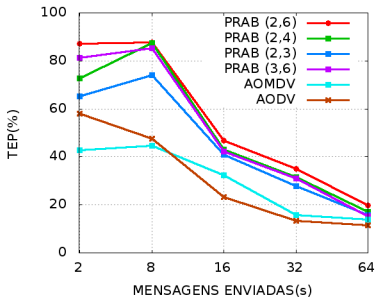


(c) Cenário2 - Velocidade 16

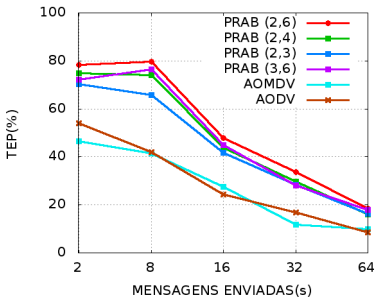
Figura 6.36: Quantidade de pacotes de dados descartados por nós *blackhole* versus densidade da rede - 40% de nós *blackhole* na rede.

6.3.3 Variando o tráfego de mensagens na rede - cenário 3

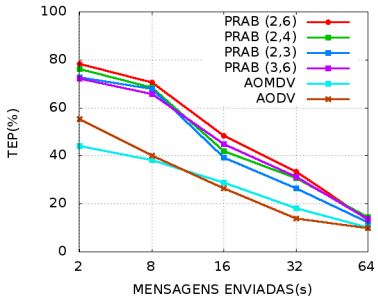
As figuras 6.37 e 6.38 mostram os resultados obtidos para a taxa de entrega dos dados com a variação do tráfego de mensagens na rede, em redes com 20% e 40% de nós atacantes, respectivamente.



(a) Cenário3 - Velocidade 1

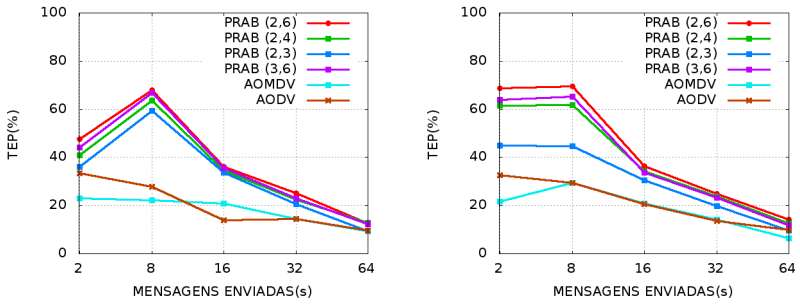


(b) Cenário3 - Velocidade 8

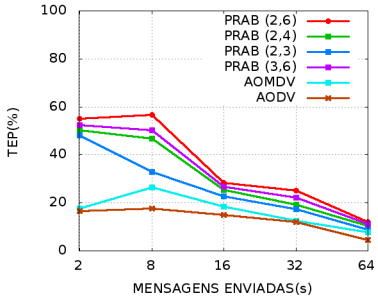


(c) Cenário3 - Velocidade 16

Figura 6.37: Taxa de entrega dos dados versus trafego da rede - 20% de nós *blackhole* na rede.



(a) Cenário3 - Velocidade 1 (b) Cenário3 - Velocidade 8

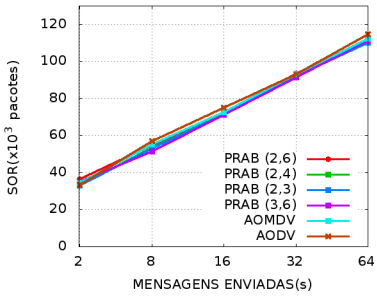


(c) Cenário3 - Velocidade 16

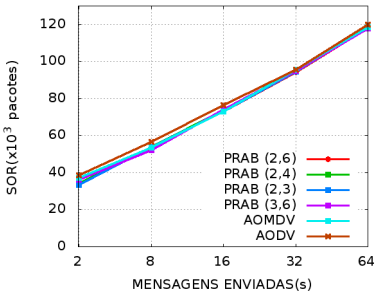
Figura 6.38: Taxa de entrega dos dados versus trafego da rede - 40% de nós *blackhole* na rede.

É possível observar nas figuras 6.37 e 6.38, que a taxa de entrega de todos os protocolos diminui com o aumento do número de mensagens enviadas na rede, para todos os casos. Contudo, o PRAB obteve melhores resultados independentemente do percentual de mensagens enviadas na rede. O PRAB com parâmetro $L = (2, 6)$ se destacou em relação aos outros parâmetros quanto à taxa de entrega. Com o aumento do número de mensagens enviadas, a taxa de entrega diminui, pois os descartes por congestionamento e *buffer overflow* aumentam acentuadamente.

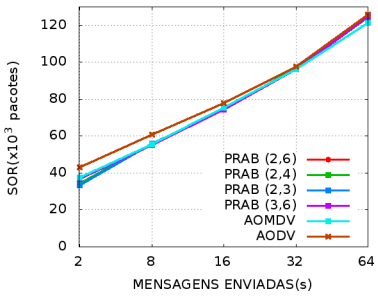
As figuras 6.39 e 6.40 mostram os resultados obtidos para a sobrecarga de roteamento com a variação do tráfego de mensagens na rede, em redes com 20% e 40% de nós atacantes, respectivamente.



(a) Cenário3 - Velocidade 1

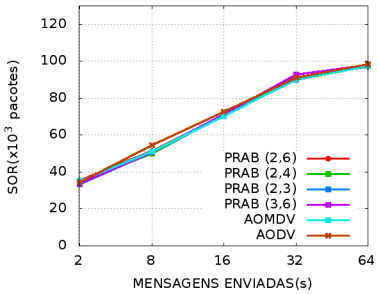


(b) Cenário3 - Velocidade 8

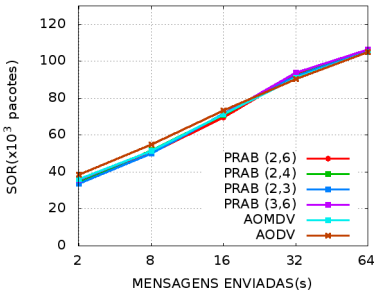


(c) Cenário3 - Velocidade 16

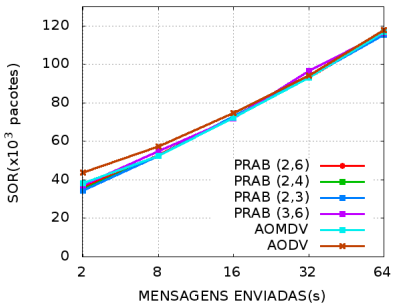
Figura 6.39: Sobrecarga versus trafego da rede - 20% de nós *blackhole* na rede.



(a) Cenário3 - Velocidade 1



(b) Cenário3 - Velocidade 8

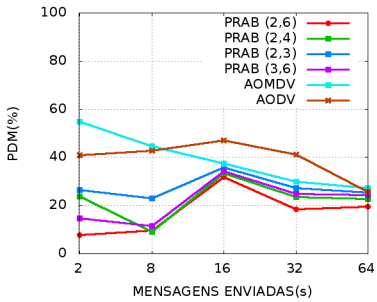


(c) Cenário3 - Velocidade 16

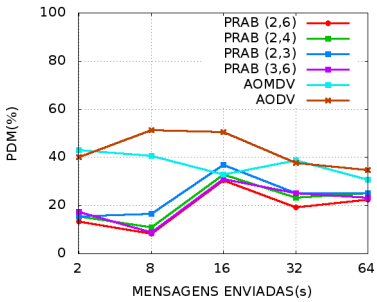
Figura 6.40: Sobrecarga versus trafego da rede - 40% de nós *blackhole* na rede.

Verifica-se nas figuras 6.39 e 6.40, que o aumento do número de mensagens enviadas implica no aumento da sobrecarga de roteamento para ambas as porcentagens de descarte. O PRAB e o AOMDV mantém resultados semelhantes, enquanto o AODV obteve os maiores valores de sobrecarga na maioria dos casos. O aumento da sobrecarga ocorre porque o número excessivo de mensagens faz com que estas fiquem mais tempo armazenadas nos *buffers* dos nós, aumentando assim a possibilidade de rotas com falhas para a entrega das referidas mensagens.

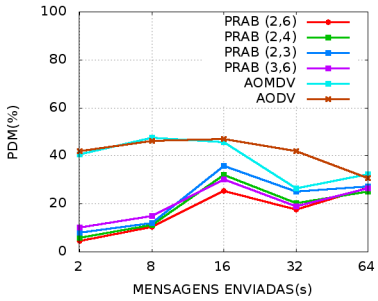
As figuras 6.41 e 6.42 mostram os resultados obtidos para a porcentagem de pacotes descartados por nós maliciosos com a variação do tráfego de mensagens na rede, em redes com 20% e 40% de nós atacantes, respectivamente.



(a) Cenário3 - Velocidade 1

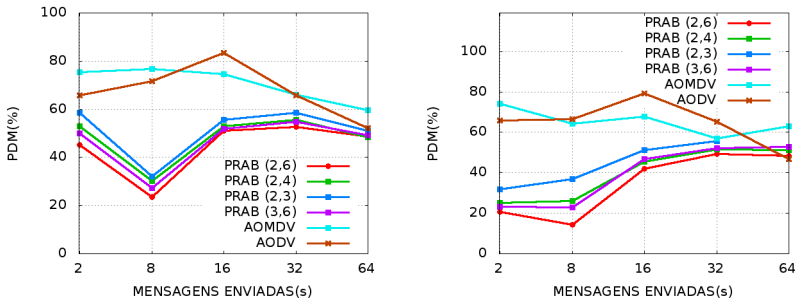


(b) Cenário3 - Velocidade 8

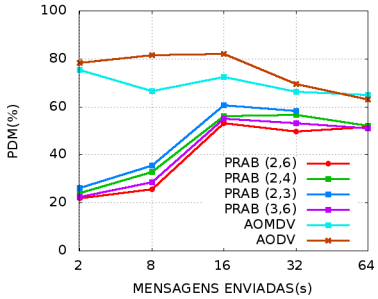


(c) Cenário3 - Velocidade 16

Figura 6.41: Quantidade de pacotes descartados versus trafego da rede - 20% de nós *blackhole* na rede.



(a) Cenário3 - Velocidade 1 (b) Cenário3 - Velocidade 8



(c) Cenário3 - Velocidade 16

Figura 6.42: Quantidade de pacotes descartados versus trafego da rede - 40% de nós *blackhole* na rede.

Com o aumento do número de mensagens enviadas na rede ocorre a redução da taxa de entrega dos dados. Porém, nota-se nas figuras 6.41 e 6.42, que não é possível observar o aumento do número de pacotes descartados por nós maliciosos na mesma proporção. Tal situação é observada porque o aumento do número de mensagens transmitidas implica em descartes por outras naturezas, como congestionamento e *buffer overflow*. Com 20% de descarte por nós atacantes e 64 mensagens enviadas por segundo, o AODV entrega 11% dos pacotes de dados, o AOMDV 13% e o PRAB com parâmetro $L = (2, 6)$ 19%. Entretanto, os descartes por nós *blackhole* são somente 25% para o AODV, 27% para o AOMDV e 19% para o PRAB com parâmetro $L = (2, 6)$. Mesmo com estas implicações, os protocolos AOMDV e AODV originais têm mais pacotes descartados por nós maliciosos em relação ao PRAB em todos os parâmetros. Com o aumento do número de mensagens enviadas, os protocolos AOMDV e AODV diminuem o número de descartes por nós maliciosos, justamente por terem descartes por congestionamento e *buffer overflow* em maiores taxas. Por sua vez, o protocolo PRAB mantém os descartes por nós maliciosos constantes ou

obtém um leve aumento. Tal fato pode ser observado devido a divisão dos pacotes em partes menores e, o uso das múltiplas rotas contribuirem para a diminuição dos descartes por congestionamento e *buffer overflow*.

6.4 Síntese dos resultados e análises

Os resultados apresentados analisam o comportamento do protocolo de roteamento proposto em redes com alto percentual de nós *blackhole*. Inicialmente, investiga-se o impacto da variação do percentual de nós atacantes na rede. Observa-se que o protocolo PRAB é superior em relação à taxa de entrega em todos os percentuais de atacantes analisados, apresentando ganhos superiores a 50% em alguns casos. Destaca-se a capacidade do PRAB em manter a taxa de entrega superior a 50%, mesmo em redes com 60% de nós atacantes. Outra característica que merece destaque é fato do PRAB manter-se superior quanto à taxa de entrega, mesmo quando a rede possui alto tráfego de mensagens, como 32 ou 64 mensagens enviadas por segundo.

Os ganhos do PRAB em relação ao número de pacotes descartados por nós maliciosos são superiores em até 45% para o cenário 1(a), e em até 52% no cenário 1(b). Contudo, é importante ressaltar que em todos os percentuais de atacantes analisados, o PRAB reduz o número de pacotes descartados pela ação de nós *blackhole*. Com o aumento do número de mensagens enviadas na rede, os protocolos AOMDV e AODV diminuem o número de descartes por nós maliciosos, justamente por terem descartes por congestionamento e *buffer overffow* em maiores taxas. Por sua vez, o protocolo PRAB mantém os descartes por nós maliciosos constantes ou obtém um leve aumento. Tal fato pode ser observado devido à divisão dos pacotes em partes menores, e o uso das múltiplas rotas contribuírem para a diminuição dos descartes por congestionamento e *buffer overffow*.

Analisou-se também a sobrecarga de roteamento. O PRAB manteve a sobrecarga semelhante a do protocolo AOMDV para todos os percentuais de atacantes analisados. Tal fato ocorre porque os processos de descoberta de rotas para ambos os protocolos são iguais. O protocolo AODV é o que apresenta os maiores valores para sobrecarga de roteamento, pois para qualquer falha de rota, o AODV precisa iniciar uma nova operação

de descoberta de rotas, o que implica em um envio maior de pacotes de roteamento para toda rede.

Quanto a vazão dos pacotes de dados, o aumento do percentual de atacantes diminui a vazão de todos os protocolos analisados. Entretanto, o PRAB obtém melhores resultados em relação ao AODV e ao AOMDV, independentemente do percentual de nós atacantes na rede. O PRAB entrega mais pacotes de dados em comparação aos outros protocolos analisados, consequentemente possui uma quantidade de dados transferidos maior. No cenário 1(b), o PRAB transfere até cinco vezes mais dados do que os protocolos AOMDV e AODV. No cenário 1(a), o PRAB transfere até sete vezes mais dados do que os outros protocolos.

Examinou-se ainda o atraso fim-a-fim das transmissões dos pacotes de dados entregues corretamente. O AODV obtém valores mais elevados em relação ao AOMDV e PRAB. Isto ocorre porque a disponibilidade das rotas alternativas presente no AOMDV e PRAB, em caso de falhas de rotas, elimina a latência da descoberta de rotas. O atraso fim-a-fim do protocolo PRAB é maior em relação ao do protocolo AOMDV. Isto se deve ao fato de que para o PRAB, a latência é a diferença entre o tempo em que a primeira parte saiu da origem e a última parte necessária para reconstruir a informação chegou ao destino. Uma análise precipitada pode levar à conclusão de que o PRAB, por possuir uma latência mais alta, reduz o desempenho da rede em relação ao AOMDV. Porém, o PRAB entrega mais pacotes de dados aos nós destinos que o AOMDV, o que mantém por mais tempo o tráfego de dados na rede.

CAPÍTULO 7

CONCLUSÃO

Redes ad hoc são redes que não necessitam de infra-estrutura pré-existente. Suas unidades são na maioria pequenas, portáteis, alimentadas por baterias e se comunicam umas com as outras através de sinais de rádio.

Nestas redes, os nós são móveis, a topologia é dinâmica e todos os nós devem funcionar como roteadores de mensagens. Neste contexto, o roteamento torna-se uma questão complexa, pois deve suportar a topologia dinâmica e falta de operações centralizadas, ao tempo em que visa garantir a entrega das mensagens com pequena sobrecarga e atraso.

A segurança dos nós é outro ponto complexo que merece a atenção. Devido à ausência de infra-estrutura e o roteamento colaborativo, um nó *blackhole* pode rotear para si mesmo todos os pacotes de dados destinados a outro nó e, então descartá-los. Ou ainda, um nó *blackhole*, pode não interferir no processo de estabelecimento das rotas e somente descartar pacotes que passam por ele. O objetivo destas ações de ataque é provocar um colapso no funcionamento e no desempenho da rede.

Esta dissertação apresenta o PRAB, um novo protocolo cujo objetivo é reduzir o impacto do descarte de pacotes em rede ad hoc causados por ataques do tipo *blackhole*. Para isso, combina um esquema de partilha de informações baseado no teorema chinês do resto e roteamento multi-caminhos.

No PRAB, cada pacote transmitido pode ser dividido em partes menores e, cada uma destas partes pode ser enviadas da origem para o destino por um caminho diferente. No destino, não são necessárias todas as partes que foram transmitidas para reconstruir a informação original, ou seja, algumas destas partes podem ser descartas por nós *blackhole* e mesmo assim a informação original pode ser reconstruída.

Desta forma, o novo protocolo proposto busca evitar que nós *blackhole* possam prejudicar o fluxo de dados entre dois nós, sem qualquer conhecimento prévio sobre o compor-

tamento do nó atacante.

As avaliações do PRAB são realizadas através de simulações em três cenários, representando redes com diferentes tamanhos, números de nós e percentuais de nós *blackhole*. No primeiro cenário, considera-se um ambiente de rede hostil, com alto percentual de nós atacantes, variando-se o tamanho da área da rede, o número de nós, a velocidade em que os nós se movimentam e a quantidade de nós atacantes. No segundo cenário, considera-se o aumento da densidade da rede, variando-se o número de nós, a velocidade, o raio de alcance, a área da rede e o percentual de atacantes. No terceiro cenário, examina-se o aumento do tráfego de mensagens na rede, variando-se o número de mensagens enviadas por segundo, o percentual de atacantes e a velocidade dos nós.

Nas avaliações realizadas, pode-se observar que a taxa de entrega do protocolo PRAB é superior a dos protocolos AODV e AOMDV para todos os percentuais de atacantes analisados. Em redes com área de 1500mX300m e 50 nós, o PRAB com parâmetro $L = (2, 6)$ obteve ganhos superiores a 46% e 50% em relação ao AODV e AOMDV, respectivamente.

Quanto à vazão dos pacotes de dados, o aumento do percentual de atacantes diminui a vazão de todos os protocolos analisados. Entretanto, o PRAB obteve melhores resultados em relação ao AODV e AOMDV, independentemente do percentual de nós atacantes na rede. Em redes com 1000mX1000m, o PRAB transfere até cinco vezes mais dados do que os protocolos AOMDV e AODV. Já em redes com área de 1500mX300m, o PRAB transfere até sete vezes mais dados do que os outros protocolos.

Os ganhos do PRAB em relação ao número de pacotes descartados por nós maliciosos foram superiores em até 45% para redes com área de 1000mX1000m e até 52% para redes com área de 1500mX300m. Ressalta-se ainda, que em todos os percentuais de atacantes analisados, o PRAB reduz o número de pacotes descartados pela ação de nós *blackhole*. Com isso, pode-se verificar que o protocolo PRAB é mais tolerante a ação de nós *blackhole* em relação aos seus concorrentes, o AODV e o AOMDV.

A sobrecarga de roteamento do protocolo PRAB é semelhante a do protocolo AOMDV em todos os percentuais de atacantes analisados. Já o protocolo AODV, é o que apresenta

os maiores valores para sobrecarga de roteamento, pois para qualquer falha de rota, ele precisa iniciar uma operação de descoberta de rotas, o que implica em um envio maior de pacotes de roteamento para toda rede.

Para o atraso fim-a-fim na entrega dos pacotes de dados, AODV obteve valores mais elevados em relação ao AOMDV e PRAB. Tal fato decorre da disponibilidade das rotas alternativas presente no AOMDV e PRAB, em caso de falhas de rotas, eliminar a latência da descoberta de rotas. O atraso fim-a-fim do protocolo PRAB é maior em relação ao do protocolo AOMDV. Isto se deve ao fato de que para o PRAB, a latência é a diferença entre o tempo em que a primeira parte saiu da origem e a última parte necessária para reconstruir a informação chegou ao destino.

Os resultados alcançados mostram que o sistema de roteamento proposto fornece equilíbrio entre segurança e desempenho no roteamento diante de ataques de nós *blackhole*. O sistema teve melhoria na taxa de entrega e vazão dos pacotes de dados, bem como na redução do impacto da ação de nós maliciosos, independente do percentual de nós atacantes na rede.

BIBLIOGRAFIA

[1] X. Bangnan and H. sven. The Role of Ad hoc Networking in Future Wireless Communications. In *International Conference on Communication Technology Proceedings, 2003. ICCT*, pages 1353–1358. 2003.

[2] V.N Talooki and K. Ziarati. Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks. In *APCC'06. Asia Pacific Conference*, pages 1–5. 2006.

[3] E.M Royer and T. Chai-Keong. A review of current routing protocols for ad hoc mobile wireless networks. In *Personal Communications, IEEE*, pages 46–55. 1999.

[4] S. Djahel, F. N. abdesselam, and Z. Zhang. Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE communications surveys and tutorials*, pages 1–14, 2010.

[5] C. Murthy and B. Mano. Ad hoc wireless networks: architetures and protocols, 2004. Prentice Hall Professional Technical Reference.

[6] A. Hasswa, M. Zulkernine, and H. Hassanein. Routeguard: an intrusion detection and response system for mobile ad hoc networks. In *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob' 2005), IEEE International Conference*, pages 336–343.

[7] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks*, 11(1):21–38, 2005.

[8] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, 2003.

[9] A. Patwardhan, J. Parker, M. Iorga A. Joshi, and T. Karygiannis. Secure routing and intrusion detection in ad hoc networks. In *Third IEEE International Conference on Pervasive Computing and Communications*, pages 8–12, 2005.

[10] Y. Huang, W. Fan, W. Lee, and P. Yu. Cross Feature Analysis for Detecting Ad-Hoc Routing Anomalies. In *Proceedings of the 23rd International Conference on Distributed Computing Systems*, pages 478–487. 2003.

[11] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu. An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network. In *24th IEEE International Conference on Advanced Information Networking and Applications*, pages 775–780. 2010.

[12] X.P. Gao and W. Chen. A novel gray hole attack detection scheme for mobile ad-hoc network. *IFIP International Conference on Network and Parallel Computing Workshops*, pages 209–214, 2007.

[13] D.M. Shila and T. Anjali. Defending selective forwarding attacks in wmns. *IEEE International Conference on Electro/Information Technology*, pages 96–101, 2008.

[14] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto. Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method. *International Journal of Network Security*, 5(3):338–346, Novembro 2007.

[15] CE. Perkins and P. Bhagwat. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. In *ACM SIGCOMM 94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244. 1994.

[16] C. Perkins and E. M. Royer. Ad-hoc on-demand distance vector (AODV) routing. In *IEEE WMCSA. Workshop on Mobile Computing Systems and Applications*, pages 90–100. 1999.

[17] M. Marina and S. Das. On-demand multipath distance vector routing for ad hoc networks. *Network Protocols, 2001*, pages 14–23, 2001.

[18] M. K. Marina and S. R. Das. On-demand multipath distance vector routing for ad hoc networks. *Wireless Communication Mobile Computing*, 6:969–988, 2006.

[19] S. J. Lee and M. Gerla. Aodv-br: Backup routing in ad hoc networks. *IEEE WCNC. Wireless Communications and Networking Conference*, pages 1311–1316, 2000.

[20] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, 353:153–179, 1996.

[21] V. D. Park and M. S. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. *IEEE INFOCOM. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, pages 1405–1413, 1997.

[22] E. Gafni and D. Bertsekas. Distributed algorithms for generating loop-free routes in networks with frequently changing topology. *IEEE Transactions on Communications*, 29(1):11–18, 1981.

[23] L. Wang, L. Zhang, Y. Shu, and M. Dong. Multipath source routing in wireless ad hoc networks. *Electrical and Computer Engineering*, 1:379–483, 2000.

[24] S. J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. *IEEE International Conference on Communications. ICC 2001*, 10:3201–3205, 2001.

[25] A. Valera, W. Seah, and S. Rao. Cooperative packet caching and shortest multipath routing in mobile ad hoc networks. *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, pages 260–269, 2003.

[26] R. Leung, J. Liu, E. Poon, A. Chan, and B. Li. Mp-dsr: A qos-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. *Proceedings of the 26th IEEE Annual Conference on Local Computer Networks (LCN 2001)*, pages 132–141, Novembro 2001.

[27] M. Medadian, A. Mebadi, and E. Shahri. Combat with blackhole attack in aodv routing protocol. *Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications*, pages 15–17, 2009.

[28] Y. F. Alem and Z. C. Xuan. Preventing blackhole attack in mobile ad hoc networks using anomaly detection. *IEEE 9th Malaysia International Conference on Communications*, pages 672–677, 2010.

[29] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255–256, 2000.

[30] A. Patcha and A. Mishra. Collaborative security architecture for blackhole attack prevention in mobile ad hoc networks. *Radio and Wireless Conference*, pages 75–78, 2003.

[31] MY. SU, KL. Chiang, and WC Liao. Mitigation of blackhole nodes in mobile ad hoc networks. *International Symposium of Parallel and Distributed Processing with Applications (ISPA)*, page 162, Setembro 2010.

[32] L. Tamilselvan and V. Sankaranarayanan. Prevention of blackhole attack in manet. *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, page 21, 2007.

[33] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, 6 ed, 2008.

[34] E.D. Karnin, J.W. Greene, and M.E. Hellman. *Concrete Mathematics.* Addison Wesley Publishing Company, 6 ed, 1990.

[35] S.C. Coutinho. *Números Inteiros e Criptografia RSA.* Computação e Matemática. IMPA, 2 ed, 2003.

[36] H. Krawczyk. Secret sharing made short. *13th annual international cryptology conference on Advances in cryptology*, 1994.

[37] A. Parakh and S. Kak. Space efficient secret sharing for implicit data security. *Journal Information Sciences: an International Journal*, Janeiro 2011.

[38] L. F. L. Nascimento J. A. Junior and L. C. P. Albini. Using the redundant residue number system to increase routing dependability on mobile ad hoc networks. *Cyber Journals: Multidisciplinary Journals in Science and Technology - Journal of Selected Areas in Telecommunications (JSAT)*, pages 67–73, 2011.

[39] Mattbe S. Gast. *802.11 Wireless Networks*. OReilly media, 2005.

[40] Douglas E. Comer. *Interligação em redes com TCP/IP*. Editora Campus, 1998.

[41] The network simulator. `http://www.isi.edu/nsnam`. Acesso em: Janeiro, 2011.

[42] M.S. Gast. 802.11 Wireless Networks. O'Really, 2002.

[43] Ieee. draft supplement to part 11: Wireless medium access control and physical layer specifications: Medium access control enhancements for quality of service, 2002.