MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE MESTRADO EM ENGENHARIA DE DEFESA

DAVI MARINHO DE ARAUJO FALCÃO

AVALIAÇÃO DE DESEMPENHO EM REDES TOLERANTES A ATRASOS PARA O TRÂMITE SEGURO DE MENSAGENS TÁTICAS NA MARINHA DO BRASIL

Rio de Janeiro
2019

INSTITUTO MILITAR DE ENGENHARIA

DAVI MARINHO DE ARAUJO FALCÃO

AVALIAÇÃO DE DESEMPENHO EM REDES TOLERANTES A ATRASOS PARA O TRÂMITE SEGURO DE MENSAGENS TÁTICAS NA MARINHA DO BRASIL

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia de Defesa do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Engenharia de Defesa.

Orientador: Prof. Cel. RONALDO MOREIRA SALLES - Ph.D.
Co-Orientador: Prof. Maj. PAULO HENRIQUE COELHO MARANHÃO - D.Sc.

Rio de Janeiro
2019

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 - Praia Vermelha
Rio de Janeiro - RJ CEP 22290-270

004.69 FALCÃO, DAVI MARINHO DE ARAUJO
S586e Avaliação de desempenho em Redes Tolerantes a Atrasos para o trâmite seguro de mensagens táticas na Marinha do Brasil / DAVI MARINHO DE ARAUJO FALCÃO, orientado por Cel. RONALDO MOREIRA SALLES e Maj. PAULO HENRIQUE COELHO MARANHÃO - Rio de Janeiro: Instituto Militar de Engenharia, 2019.

94p.: il.

Dissertação (mestrado) - Instituto Militar de Engenharia, Rio de Janeiro, 2019.

1. Curso de Engenharia de Defesa. 1. DTN. 2. Redes Tolerantes a Atrasos. 3. cenário marítimo. 4. função discriminante. 5. segurança. I. SALLES, Cel. RONALDO MOREIRA . II. MARANHÃO, Maj. PAULO HENRIQUE COELHO . III. Título. IV. Instituto Militar de Engenharia.

INSTITUTO MILITAR DE ENGENHARIA

DAVI MARINHO DE ARAUJO FALCÃO

AVALIAÇÃO DE DESEMPENHO EM REDES TOLERANTES A ATRASOS PARA O TRÂMITE SEGURO DE MENSAGENS TÁTICAS NA MARINHA DO BRASIL

Dissertação de Mestrado apresentada ao Curso de Mestrado em Engenharia de Defesa do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Engenharia de Defesa.

Orientador: Prof. Cel. RONALDO MOREIRA SALLES - Ph.D.

Co-Orientador: Prof. Maj. PAULO HENRIQUE COELHO MARANHÃO - D.Sc.

Aprovada em 06 de Fevereiro de 2019 pela seguinte Banca Examinadora:

Prof. Cel. RONALDO MOREIRA SALLES - Ph.D. do IME - Presidente

---

Prof. Maj. PAULO HENRIQUE COELHO MARANHÃO - D.Sc. do IME

Prof. TC. JULIO CESAR DUARTE - D.Sc. do IME

Prof^{a}. RAQUEL COELHO GOMES PINTO - D.Sc. do IME

Prof. JOSÉ FERREIRA DE REZENDE - D.Sc. da COPPE/UFRJ

Rio de Janeiro
2019

Aos meus pais Antonio Falcão (*in memorian*) e Miriam Falcão.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me concedido essa oportunidade de fazer um curso de Mestrado pelo Instituto Militar de Engenharia (IME), posso dizer que isso foi a realização de um antigo sonho desde os meus tempos de graduação em Engenharia da Computação pela Universidade de Pernambuco (em 2009).

Agradeço também a Marinha do Brasil por ter me concedido esse tempo de dois anos para o aprimoramento do meu conhecimento profissional, por isso desejo estar apto a contribuir, no meu regresso, com o conteúdo do meu aprendizado para a melhoria dos serviços na Diretoria de Sistemas de Armas da Marinha (DSAM).

Agradeço pelo esforço e o apoio de meus pais Antonio Marinho Falcão Filho (*in memorian*) e Miriam José de Araujo Falcão, especialmente aos incentivos de meu saudoso pai que certamente teria se alegrado muito com esta minha conquista. Agradeço à minha esposa Olga Galdêncio Leocádio Falcão por me apoiar e escutar em todas as vezes que eu precisei desabafar durante o curso.

Agradeço a todos os bons professores que eu tive durante a minha vida acadêmica, em especial ao meu atual orientador o Coronel Ronaldo Moreira Salles. Agradeço ao IME por ter aberto as suas portas para que eu pudesse iniciar e terminar o meu curso com sucesso.

Agradeço a todos os meus amigos que lembraram de mim em suas orações.

Davi Marinho de Araujo Falcão

“Voltei-me, e vi debaixo do sol que não é dos ligeiros a carreira, nem dos fortes a batalha, nem tampouco dos sábios o pão, nem tampouco dos prudentes as riquezas, nem tampouco dos entendidos o favor, mas que o tempo e a oportunidade ocorrem a todos. Eclesiastes 9:11. ”

BÍBLIA SAGRADA.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

AIS	*Automatic Identification System*
DTN	*Delay-Tolerant Networks*
DDoS	*Distributed Denial of Service*
IPqM	Instituto de Pesquisas da Marinha
DOS	*Denial of Service*
DSAM	Diretoria de Sistemas de Armas da Marinha
HF	*High Frequency*
IFF	*Identification Friend or Foe*
MANET	*Mobile Adhoc Network*
NANET	*Nautical Adhoc Network*
STERNA	Sistema Tático de Enlace de Dados em Radiopropagação Naval
TDMA	*Time Division Multiple Access*
UHF	*Ultra High Frequency*
VANET	*Vehicular Ad-hoc Network*
VHF	*Very High Frequency*

RESUMO

As Redes Tolerantes a Atrasos (DTN) são uma evolução das *Mobile Adhoc Network* (MANET) sendo que as DTN atuam em cenários onde os nós estão esparsamente distribuídos, com baixa densidade, cuja conexão seja intermitente e onde uma infraestrutura fim-a-fim não esteja disponível. Por isso, as DTN são recomendáveis para aplicações de alta latência que podem durar de horas até mesmo dias. O cenário marítimo possui características que justificariam o uso de redes DTN, contudo a preocupação com a segurança dos dados também é um aspecto relevante para esse tipo de arquitetura. Por essa razão esse trabalho propõe avaliar Redes Tolerantes a Atrasos no cenário marítimo envolvendo os navios da Marinha do Brasil juntamente com helicópteros para o encaminhamento de mensagens táticas, levando-se em consideração aspectos de segurança nos perímetros onde os contatos acontecem. As simulações compararam o desempenho dos protocolos *Epidemic*, *Spray and Wait* e *Direct Delivery* em 3 diferentes cenários com dimensões distintas. A utilização de Análise Discriminante como técnica de classificação para selecionar os perímetros seguros foi uma sugestão de melhoria do protocolo *Epidemic* para o bloqueio de conexões classificadas como sendo inseguras. A função discriminante detectou e bloqueou todas as conexões classificadas como inseguras, contudo, por esse motivo, houve também uma queda na média de mensagens entregues.

ABSTRACT

Delay-Tolerant Networks (DTN) are an evolution of the Mobile Adhoc Network (MANET) where DTN act in scenarios where nodes are sparsely distributed, with low density, whose connection is intermittent and where an end-to-end infrastructure is not available. Therefore, DTNs are recommended for high latency applications that can last from hours to even days. The maritime scenario has characteristics that would justify the use of DTN networks, however the concern with data security is also a relevant aspect for this type of architecture. For this reason, this work proposes to evaluate Tolerant Networks to Delays in the maritime scenario involving the ships of the Brazilian Navy along with helicopters for the forwarding of tactical messages, taking into account aspects of security in the perimeters where the contacts take place. The simulations compared the performance of the *Epidemic*, *Spray and Wait* and *Direct Delivery* protocols in 3 different scenarios of different sizes. The use of Discriminant Analysis as a classification technique to select the safe perimeters was a suggestion of improvement of the *Epidemic* protocol for blocking connections classified as being insecure. The discriminant function detected and blocked all connections classified as unsafe, however, for this reason, there was also a decrease in the average number of messages delivered.

1 INTRODUÇÃO

O transporte marítimo é responsável por cerca de 90% do comércio internacional, (BRASIL.GOV.BR, 2017). Isso justifica o grande investimento por parte das potências mundiais, direcionado ao meio de transporte marítimo e áreas portuárias, demonstrando que o mar é uma área estratégica que gera riquezas para os países que sabem utilizar corretamente os seus recursos. Por esse motivo o transporte marítimo torna-se prioridade para qualquer país que deseje se desenvolver economicamente.

Juntamente com a crescente demanda do tráfego marítimo, também aumenta a necessidade de se manter os navios comunicáveis para o compartilhamento de informações, tais como: geolocalização dos meios navais, dados meteorológicos de uma determinada região, situação de uma determinada embarcação, pedido de socorro etc.

Contudo o ambiente marítimo não permite a utilização dos recursos de conectividade com a mesma facilidade que se utiliza em terra firme. As redes marítimas são baseadas em rádios convencionais *High Frequency (HF), Very High Frequency (VHF) e Ultra High Frequency (UHF)*, para comunicação nas proximidades da costa, e sistemas de satélites para cobertura de áreas à longas distâncias, porém essas opções são muito lentas e de custo elevado quando comparadas com as soluções de redes que são disponibilizadas em terra firme (ZHOU ET AL., 2013).

Dessa maneira, é uma estratégia de vital importância a escolha de uma arquitetura que venha a atender às necessidades de comunicação em termos de capacidade de participação de nós na rede, velocidade na transmissão e recebimento de mensagens, custos, segurança etc. Principalmente quando os meios em questão são navios pertencentes à Marinha do Brasil, tendo em vista que as informações compartilhadas durante as missões possuem grau de sigilo elevado, trazendo a obrigatoriedade do uso de técnicas que restrinjam o acesso à informação, como por exemplo, soluções baseadas em criptografia. Sabe-se que é possível burlar a segurança e que não existe no mercado soluções infalíveis contra invasão, mas a mentalidade de segurança obriga a adoção de mecanismos que dificultem ao máximo o trabalho do invasor.

1.1 MOTIVAÇÃO

Os navios da marinha brasileira precisam trocar informações táticas entre si durante as suas diversas missões e treinamentos. No entanto, em alto-mar, os navios sofrem com a falta frequente de conectividade, pois naturalmente precisam se afastar do perímetro de suas Estações Rádio-Base.

Deve-se mencionar também que nem sempre a comunicação por enlace de satélite se torna viável tendo em vista o alto custo na locação desse tipo de serviço para trâmite de dados, como também traz uma forte dependência tecnológica em um meio crítico de defesa do país.

Como alternativa de baixo custo para suprir a intermitência nas comunicações, mantendo o desempenho de forma considerada aceitável e ampliando a capacidade de comunicação entre os navios da Marinha do Brasil, esse trabalho irá avaliar a adoção de Redes Tolerantes a Falhas ou Atrasos (DTN) para a comunicação naval pela Marinha do Brasil.

1.1.1 CARACTERIZAÇÃO DO PROBLEMA

A melhoria de desempenho das comunicações terrestres sem fio pode ser facilmente alcançada com a instalação de mais estações base em terra. No entanto o mesmo tipo de solução não pode ser adotada para as comunicações marítimas por conta das restrições naturais do meio marítimo, por isso algumas alternativas para minimizar os problemas já vêm sendo tomadas, como a instalação de modens de longa distância com baixa taxa de transmissão.

A rede tática da Marinha do Brasil, por exemplo, é responsável por concentrar as informações oriundas dos sistemas táticos e enviá-las aos navios. Contudo, os navios sofrem com tempos elevados de intermitência, dificultando a chegada das mensagens a todos os navios, principalmente daqueles que se encontram fora do raio de alcance da rede. Isso faz elevar as taxas de retransmissão de dados na rede como resultado do aumento de erros de entrega.

Estratégias de roteamento que permitam o encaminhamento dessas mensagens entre os navios são utilizadas com a finalidade de se aumentar a probabilidade de entrega com sucesso (KOLIOS AND LAMBRINOS, 2012), (K. YOUNGBUM, 2009). No entanto, as estratégias de roteamento tradicionais baseadas nos protocolos da pilha TCP/IP, exigem que o nó que repassa as mensagens para os nós distantes esteja dentro do raio de alcance da rede sem fio. Ou seja, é preciso que o nó intermediário esteja ainda conectado na rede para poder encaminhar dados para os nós considerados remotos, por estarem longe do

perímetro da rede.

Em relação a segurança, a Marinha do Brasil somente permite o trâmite de mensagens sigilosas de forma criptografada, de forma que se um intruso se apoderar da mensagem, ele não a possua em texto claro. No entanto, isso não impede que técnicas de criptoanálise sejam utilizadas para se tentar deduzir a chave secreta e de alguma forma descriptografar a mensagem, muita das vezes utilizando força bruta (HUANG AND TSO, 2012), (DING ET AL., 2013).

No caso em que um nó malicioso consiga roubar uma chave privada de um outro nó ou até mesmo inferir sobre ela, ele poderá tentar se passar por aquele e assim manter uma comunicação com os demais nós da rede como se fosse um nó legítimo. Mesmo sabendo que as mensagens sigilosas da Marinha do Brasil já tramitam criptografadas, é desejável que essas mensagens sejam somente entregues a nós autorizados, pois sabe-se que o nó atacante tentará inferir o valor da chave usando alguma técnica de criptoanálise.

1.2 JUSTIFICATIVA

A Diretoria de Sistemas de Armas da Marinha (DSAM) juntamente com o Instituto de Pesquisas da Marinha (IPqM) iniciaram a atualização do antigo hardware que era responsável por prover o enlace para o envio e recebimento de mensagens táticas entre os navios da Marinha do Brasil.

O novo enlace de dados foi denominado STERNA (Sistema Tático de Enlace de Dados em Radiopropagação Naval) e está atualmente em fase de desenvolvimento pelo IPqM. Esse hardware interligará todos os sistemas táticos existentes na Marinha.

Algumas das características do STERNA que servirão de informação para o planejamento das simulações:

- Transmissão e recepção de pacotes de dados a longa distância por canal de radiofrequência;
- Modo de operação em *half-duplex* (chaveamento automático em instantes de tempo programável na rede);
- Dados serão transmitidos sempre criptografados e compactados;
- Modos de Operação do Novo Sistema:
  - Operação em Rede TDMA (*Time Division Multiple Access*);

  - Operação Modo Silêncio Rádio: Sistema verifica se o canal está ocupado, caso positivo aguardará antes de transmitir; e
  - Operação em Modo de Teste: O objetivo é verificar integridade da rede;

- Mensagens de controle são enviadas e recebidas pela Estação Controladora da Rede.

Os navios pertencentes a rede trabalham em diferentes Modos de Estação, como mostra a Figura 1.1, que são os seguintes:

- Estação Controladora:
  - Troca de mensagens táticas com as Estações Dependentes;
  - Inicia a rede;
  - Mantém o sincronismo da rede;
  - Inclui ou exclui Estações Dependentes na Rede;
  - Pode delegar a uma Estação Dependente a função de Estação Controladora;
  - Processar as solicitações das Estações Controladoras; e
  - Controle dos *timeslots* concedidos às Estações Dependentes.
- Estação Dependente:
  - Transmitem dados nos *timeslots* definidos pela Estação Controladora; e
  - Em caso de inoperância por um determinado período de tempo, torna-se uma Estação Ouvinte.
- Estação Ouvinte:
  - Se mantém sincronizada recebendo dados da rede, porém não transmitindo;
  - Para transmitir, enviam mensagem à Estação Controladora solicitando *timeslots* e assim passam à Estação Dependente.
- Estação Remota:
  - Não participam da rede por estarem fora do alcance da Estação Controladora;
  - Poderão receber mensagens por uma Estação Dependente em modo *Relay*:

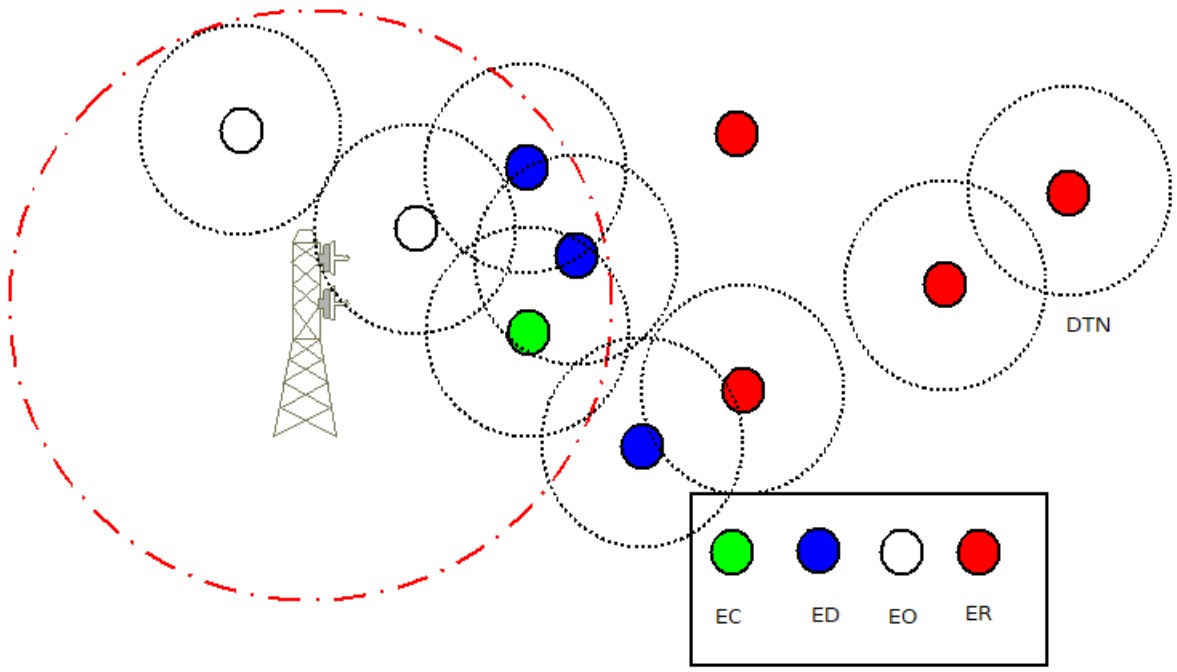


FIG. 1.1: Configuração dos diferentes tipos de Estações da rede do STERNA funcionando em modo híbrido com a arquitetura DTN.

* No modo *Relay* qualquer Estação Dependente poderá retransmitir mensagens para as Estações Remotas encontradas, mas para essa finalidade deverá ser usado um canal de radiofrequência diferente do utilizado na rede principal;

As mensagens táticas, tramitadas entre os *links* táticos, são propositadamente curtas, pois assim geram menos pertubações eletromagnéticas nos perímetros e com isso são mais discretas do que mensagens longas que geram muita pertubação e com isso estão mais sujeitas a detecção e interceptação. A seguir, alguns tipos de mensagens táticas:

- Identificação, posição, rumo e velocidade dos contatos;
- Pontos de referência;
- Mensagens de Comando; e
- Texto livre com até 11 caracteres.

O projeto do STERNA já contempla a retransmissão por *Relay* de uma Estação Dependente (com sinal ativo na rede) para uma Estação Remota (fora do alcance da rede). No entanto a Estação Dependente precisará estar no alcance da rede, dando a ela uma limitação para conseguir chegar suficientemente próximo de uma Estação Remota.

A proposta deste trabalho é formar uma arquitetura híbrida de redes, envolvendo as estações base em terra, como também as embarcações fornecendo uma rede marítima do tipo *mesh* que inclua arquitetura DTN, em conjunto com as demais tecnologias de rede, no intuito de estender a capacidade de conectividade existente. O projeto do STERNA seria uma boa oportunidade para testar DTN nos navios de guerra da Marinha do Brasil.

1.3 OBJETIVOS DA DISSERTAÇÃO

- Demonstrar, através de ambiente de simulação, que protocolos DTN trabalhando, de forma híbrida, com as soluções tradicionais de rede existentes podem potencializar o trâmite de mensagens táticas entre navios na Marinha do Brasil, contribuindo para o aumento da efetividade na entrega de pacotes para os nós afastados da rede.

- Encontrar um método que classifique de forma eficiente as conexões seguras para o bloqueio de conexões consideradas inseguras, dessa forma melhorando a questão da segurança e diminuindo a entrega de mensagens aos navios que estejam localizados em um perímetro considerado inseguro.

- Mostrar que a informação prévia sobre as rotas dos navios em missão no mar poderia indicar padrões de movimentação que serviriam para o aprimoramento da segurança, na detecção de intrusos na rede. Esses resultados contribuiriam na área de segurança das Redes DTN para cenários onde os nós possuem rotas conhecidas.

Como objetivos específicos podem ser listados:

- avaliar o desempenho de roteamento DTN no cenário marítimo da Marinha do Brasil, apresentando ao final como uma solução de baixo custo que se beneficiaria da densidade da rede e da movimentação dos nós, ou seja, utilizando dos recursos que já estariam disponíveis no cenário naval:
  - avaliar o desempenho do protocolo DTN levando-se em consideração as condições de comunicação dos navios no mar; e
  - demonstrar, em ambiente de simulação, que a arquitetura DTN pode contribuir com a entrega de mensagens no cenário marítimo em pontos onde há perda de conexão total da rede. Utilizando a movimentação dos navios como vantagem. Esses resultados viriam através da avaliação dos *logs* gerados durante as simulações, em forma de relatórios, pelo simulador.

- propor uma melhoria, em um dos protocolos DTN, na questão de segurança, classificando as conexões em seguras ou inseguras para a redução do compartilhamento de dados para meios não autorizados e guardando o posicionamento desses encontros no intuito de mapear as regiões de comunicação segura para aprimoramento do módulo de segurança.

1.4 METODOLOGIA

- Serão realizadas uma série de simulações, através de uma ferramenta gratuita de simulação para redes oportunísticas, o The ONE (KERÄNEN ET AL., 2009). Essas simulações ocorrerão em 3 cenários distintos, construídos à partir de rotas reais de navios. Cada simulação irá variar em área, número de mensagens criadas, tamanho das mensagens, número de nós na rede etc;

- Após as simulações, será possível tratar os dados estatísticos que permitirão medir o desempenho dos protocolos em cada cenário marítimo, tais como: quantidade de mensagens entregues em relação ao quantitativo de mensagens criadas, tempo de atraso nas entregas das mensagens, o impacto da inserção de mais navios, o impacto da inserção de veículos de maior velocidade (helicópteros) etc;

- Será utilizada uma ferramenta proprietária, chamada Minitab, para fazer uma análise estatística dos dados a fim de gerar uma função que permita a classificação das conexões em dois grandes grupos: seguras e inseguras, baseando-se em parâmetros existentes nos perímetros das conexões. Esses parâmetros são escolhidos empiricamente, pois a ferramenta permite que sejam realizados ajustes que visem a melhoria dos resultados à medida que parâmetros são adicionados ou removidos da análise;

- Em seguida, novas simulações serão realizadas, porém, dessa vez, com o módulo de segurança ativo no protocolo *Epidemic* a fim de comparar com o desempenho do *Epidemic* padrão e assim inferir sobre as consequências da aplicação do módulo de segurança.

1.5 ORGANIZAÇÃO DA DISSERTAÇÃO

O trabalho atual está dividido da seguinte forma: o Capítulo 2 irá introduzir sobre o tema do funcionamento das redes DTN, suas estratégias de encaminhamento, seus tipos de protocolos, o uso de redes DTN no cenário marítimo e a sua aplicabilidade na Marinha

do Brasil. Também no Capítulo 2 será descrito à respeito dos trabalhos relacionados. No Capítulo 3 será abordado o tema da segurança das redes DTN e uma introdução sobre Análise Discriminante, que é uma técnica multivariada utilizada para classificação de elementos em grupos previamente conhecidos. O Capítulo 4 irá falar especificamente sobre a Simulação, serão apresentadas as ferramentas utilizadas no trabalho, principalmente sobre o The ONE (a principal ferramenta de simulação), finalizando com a apresentação dos cenários utilizados. O capítulo 5 irá descrever os resultados obtidos das várias simulações. Para finalizar o Capítulo 6 irá comentar sobre as conclusões alcançadas pelo trabalho atual, como também sugerir atividades para trabalhos futuros.

2 REDES DTN

2.1 CONCEITO

As Redes Tolerantes a Atrasos (DTN) evoluíram das *Mobile Adhoc Network* (MANET), sendo que as DTN atuam em cenários onde os nós estão esparsamente distribuídos, cuja conexão seja intermitente e onde uma infraestrutura fim-a-fim não esteja disponível (R.S. MANGRULKAR, 2010). Por isso DTN são recomendáveis somente para aplicações de alta latência, que podem durar de horas até mesmo dias.

Outra característica importante sobre as redes DTN, é a possibilidade de encaminhamento de pacotes de forma assíncrona (OTT ET AL., 2006), ou seja, eles não precisam ser recebidos na sequência em que foram enviados, mas as mensagens são montadas no destino de acordo com uma *flag* que indica a ordem que os pacotes serão reorganizados no destinatário.

Uma grande vantagem da DTN sobre as MANETS é que os seus encaminhamentos de pacotes são baseados nas oportunidades de contatos estabelecidos e na probabilidade de transmissão de dados, sem precisar estabelecer uma rota. No entanto, uma MANET precisa passar por duas fases para enviar dados, pois ela primeiro precisa estabelecer uma rota entre a origem e destino para que em sequência, na segunda fase, possa transmitir os dados mantendo a informação da rota até o término da transmissão (R.S. MANGRULKAR, 2010).

Nas redes DTN não existe garantia de estabelecimento de rota antes do encaminhamento, pois os nós estão espaçados, no entanto eles podem trocar dados entre si, quando estabelecem contato por aproximação. Essa abordagem se chama "Armazena e Encaminha", em que o nó DTN mantém aquela informação até conseguir encaminhar para um outro nó intermediário. Esse encontro em que o nó conseguiu verdadeiramente transmitir a informação para o outro é denominado "Contato"ou "Encontro Efetivo"(CARINA T. DE OLIVEIRA, 2007), (SILVA, 2007).

Conexões perenes são beneficiadas pela imobilidade de seus dispositivos conectados a elas, no entanto existem ambientes que são compostos por dispositivos dotados de alta mobilidade e com isso o modelo clássico de rede não fornece suporte para esse tipo de ambiente marcado por constantes conexões / desconexões. Nesse aspecto as Redes Tolerantes a Atrasos (DTN) vieram para contribuir (CARINA T. DE OLIVEIRA, 2007),

(SILVA, 2007), pois as redes DTN se beneficiam da mobilidade dos nós, replicando dados até que eles atinjam o seu destino.

Redes DTN são conhecidas como oportunísticas porque os nós intermediários estão sempre buscando uma oportunidade para encaminhar uma mensagem de uma origem para um destino (FALL, 2003), (R.S. MANGRULKAR, 2010).

Rede DTN é uma arquitetura de redes que propõe melhorar o desempenho de comunicação em ambientes onde não exista uma infraestrutura fim-a-fim, se beneficiando com a mobilidade de seus nós. Pode-se imaginar a sua aplicação em cenários de desastre ou que por alguma limitação, seja ela natural ou não, não seja possível montar uma infraestrutura que possa suprir uma determinada área por completo.

Isso faz com que a arquitetura DTN seja bastante útil em aplicações que tenham essas características como por exemplo em conecções interplanetárias, em uma rede de sensores sem fio, em redes móveis terrestres, em redes Ad-hoc militares (PURI AND SINGH, 2013), (SAMPAIO, 2017) e no cenário de comunicação entre navios no mar (V FRIDERIKOS, 2005).

A aplicação de DTN ao ambiente marítimo, por exemplo, torna-se uma alternativa de baixo custo quando comparado aos elevados preços para a locação de cobertura satelital (CHRYSOSTOMOU, 2013).

Dessa maneira, dispositivos que possuem mobilidade podem levar consigo os dados armazenados em *buffers* e entregá-los a dispositivos intermediários que, consequentemente, se comportarão da mesma forma até que os dados cheguem ao seu destino (FALL, 2003), (V FRIDERIKOS, 2005), (R.S. MANGRULKAR, 2010), (DUTT, 2015), (LUMING WAN AND ZHANG, 2015), (SAMPAIO, 2017).

Na Figura 2.1, os círculos estão simbolizando os raios de alcance do sinal dos nós dotados de mobilidade, em que alguns se beneficiam, recebendo os dados de forma colaborativa através dos nós intermediários. Os dados são transmitidos quando ambos os nós estão dentro do raio de alcance do sinal do outro, é quando ocorrem as conexões representadas, ainda na Figura 2.1, pelos retângulos.

2.2 PROTOCOLOS DE ROTEAMENTO DTN

O roteamento em redes DTN se baseia em duas estratégias, (R.S. MANGRULKAR, 2010) sendo que a primeira delas é a de Inundação ou *Flooding* que se baseia em replicar as mensagens para uma quantidade de nós que sejam suficientes para se atingir o nó de destino.

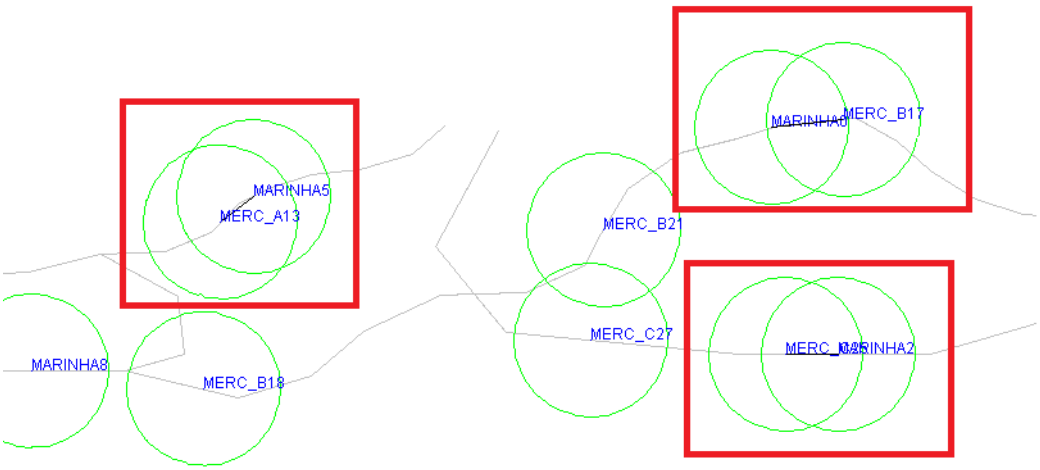


FIG. 2.1: Os nós mais distantemente localizados receberão os dados através de outros nós da rede DTN.

A segunda estratégia é a de Encaminhamento e utiliza o conhecimento prévio sobre a rede para selecionar o melhor caminho para o destinatário, visto que baseia o seu comportamento de forma probabilística.

No entanto existem estratégias que se comportam de forma híbrida alternando o seu comportamento entre as estratégias de Inundação e de Encaminhamento.

2.2.1 ESTRATÉGIA DE INUNDAÇÃO

Nessa estratégia, são criadas cópias múltiplas da mesma mensagem e essas serão enviadas para um conjunto de nós denominados nós *Relay*. Esses nós armazenam essas mensagens até que elas alcancem o nó de destino (FALL AND FARRELL, 2008). Protocolos baseados na estratégia de Inundação não requerem qualquer conhecimento prévio da rede pois não são probabilísticos. A seguir serão descritos o comportamento de alguns deles:

2.2.1.1 SINGLE HOP TRANSITION OU DIRECT DELIVERY

É considerada a estratégia mais simples, em que o nó de origem transmite diretamente ao nó de destino imediatamente quando entram em contato (R.S. MANGRULKAR, 2010), ou seja, não existem retransmissões através de nós intermediários. Nesse tipo de protocolo, cada nó leva somente a sua própria mensagem. A grande vantagem é que não é preciso alocar grandes recursos para esse tipo de protocolo, no entanto, o tempo de atraso é muito superior aos demais e a probabilidade de entrega com esse tipo de configuração, se mostra como a menor.

Esse protocolo somente é recomendável quando existe uma intensa mobilidade de nós na rede, visto que um aumento intenso da mobilidade dos nós acarreta a probabilidade de haver os encontros efetivos. Isso mostra que o protocolo se torna vantajoso quando origem e destino estão a um salto de distância, ou seja, quando eles são vizinhos.

2.2.1.2 TWO-HOP RELAY

Nesse protocolo ocorrem retransmissões envolvendo somente o nó de origem com os nós que ele manteve contato em um primeiro momento. Em seguida, esses nós irão trabalhar de forma a cooperar para que a mensagem chegue ao nó de destino.

Este tipo de protocolo aumenta sensivelmente a probabilidade de entrega em relação ao *Single Hop Transition*, todavia, ainda apresenta as mesmas limitações existentes no protocolo de contato direto, como também aumentam os consumos de largura de banda e de armazenamento (R.S. MANGRULKAR, 2010).

2.2.1.3 ROTEAMENTO EPIDÊMICO

O roteamento epidêmico é considerado o primeiro algoritmo de roteamento DTN. Ele assume que cada nó tenha armazenamento e largura de banda ilimitados e por isso parte do princípio de que todo nó pode armazenar todas as mensagens transmitidas durante a fase de contato. Cada nó mantém uma lista de mensagens em um banco de dados e pode transmitir mensagens inteiras para outros nós durante os posteriores contatos.

Para um cenário onde os nós estão distribuídos de maneira esparsa e que as mensagens trocadas sejam pequenas, ele pode ser considerado um bom protocolo. Contudo, um grande problema do roteamento epidêmico está em que a mensagem continua a se propagar mesmo quando ela já tenha atingido o nó de destino. Outra questão desvantajosa sobre o roteamento epidêmico é que ele é o tipo de protocolo que consome muitos recursos do sistema por causa do seu modo de funcionamento (R.S. MANGRULKAR, 2010).

É assim chamado pelo comportamento semelhante à transmissão de uma doença contagiosa, pois o nó portador da mensagem tenta transmiti-la para todos os nós que ele mantém contato sem critério.

2.2.1.4 SPRAY AND WAIT

É um protocolo que funciona em duas fases, a primeira é chamada a fase de *Spray* em que cada nó irá inundar a rede enviando replicas das mensagens para um número de L nós Relay, sendo esse L um valor que é configurado pelo nó de origem. Se a mensagem

alcançar o nó de destino a transmissão é interrompida, caso contrário ele entra na fase de Wait em que passa a enviar as mensagens somente para os nós que ele realmente mantiver contato. O parâmetro L é calculado levando-se em consideração a densidade, a distribuição e a mobilidade dos nós (R.S. MANGRULKAR, 2010).

2.2.1.5 FIRST CONTACT

É um algoritmo bem simples de se implementar, pois quando uma mensagem é criada o nó de origem detecta quais nós estão em contato com ele naquele instante. Em seguida, o nó de origem seleciona aleatoriamente um desses nós para se encaminhar a mensagem.

Pelo fato da seleção do próximo nó ocorrer de forma aleatória, sem previsão de que esses nós selecionados cheguem a alcançar o nó de destino desejado, pode-se considerar esse protocolo não tão eficiente, apesar de ser de fácil implementação. Nesse contexto, a mensagem poderá nunca chegar ao seu destino e ainda poder ficar oscilando entre um conjunto pequeno de nós concentrados em uma região.

Para se evitar esses *loops*, muitas das vezes é adotado um vetor que guarda a trajetória de onde uma determinada mensagem já passou, de forma a ajudar ao nó atual evitar caminhos já percorridos.

2.2.2 ESTRATÉGIA DE ENCAMINHAMENTO

Nessa estratégia se utiliza o conhecimento prévio, tanto da topologia da rede quanto de qualquer outra informação importante que permita a escolha da melhor rota em direção ao destinatário. Essa melhor rota é a que será selecionada para encaminhar a mensagem, ou seja, as mensagens não serão encaminhadas para os nós de forma aleatória, mas sim baseando-se em informações disponibilizadas previamente e que servem de entrada para protocolos que seguem essa estratégia.

Esse tipo de estratégia não replica as mensagens, mas ao invés disso é designado um caminho, baseado em estimativas, para que a mensagens possa trafegar através dele. Dessa forma economizando os recursos da rede.

Logo abaixo segue a explicação do funcionamento do protocolo *Prophet* que muito bem representa esse tipo de estratégia, pois utiliza de conhecimento prévio para traçar uma rota em direção ao seu destino.

2.2.2.1 PROPHET

Esse protocolo tem como objetivo a redução do desperdício de recursos, como por exemplo, largura de banda e armazenamento. Seu algoritmo parte do princípio que se um determinado nó visitou uma determinada localidade uma quantidade de vezes considerável, então existe uma grande probabilidade de que esse padrão se repita no futuro.

No protocolo de roteamento Prophet, um nó que possua uma maior probabilidade de entrega da mensagem ao destino será reconhecido como o melhor roteador para a entrega da mensagem e por isso esse nó ganha um maior grau de confiabilidade. Essa probabilidade é calculada baseada em um histórico de contatos que são armazenados ao longo do tempo para melhorar as decisões de encaminhamento.

O Prophet se torna indicado em cenários nos quais alguns dos nós se movimentam de acordo com um padrão que não é aleatório. Dispositivos móveis transportados por seres humanos possuem esses padrões de mobilidade, por exemplo.

2.3 PRINCIPAIS PROBLEMAS

Os principais problemas relacionados às Redes Tolerantes a Atrasos estão inseridos nos grandes grupos listados abaixo e dependendo do ambiente de rede e da estratégia de roteamento adotada esses problemas podem se tornar ainda mais acentuados ou atenuados (PURI AND SINGH, 2013) (DUTT, 2015). São eles:

a) Controle de *Buffer*;

b) Controle de Congestionamento;

c) Segurança;

d) Desconexões; e

e) Capacidade Energética (SAMPAIO, 2017).

2.3.1 CONTROLE DE *BUFFER*

Os problemas relacionados ao controle de *Buffer*, baseiam-se no limite da capacidade de armazenamento dos nós, exigindo que medidas sejam tomadas para que essa capacidade não chegue a estourar. Uma boa estratégia é limitar o armazenamento dos dados por um certo período de tempo configurável, de forma que ao atingir o limite de *buffer* os dados considerados expirados possam ser removidos do *buffer* dando espaço para a entrada de novos.

2.3.2 CONTROLE DE CONGESTIONAMENTO

A escolha da estratégia de roteamento irá influenciar diretamente sobre a movimentação dos dados e no consumo da largura de banda da rede.

Essa escolha dependerá do cenário no qual será aplicada a solução DTN, como por exemplo, se o cenário apresentar baixa densidade de nós a estratégia de Inundação se tornaria aconselhável pelo fato de trazer um melhor aproveitamento dos poucos nós disponíveis.

Contudo, a estratégia de Inundação em um cenário de alta densidade poderia causar uma sobrecarga da rede, o que tornaria recomendável o uso de uma estratégia baseada em Encaminhamento, através de algum protocolo de roteamento probabilístico, que selecionaria os nós encaminhadores baseando-se em dados estatísticos de encontros prévios.

Com uma intensa movimentação dos nós transmitindo e recebendo dados entre si, o controle de congestionamento se torna uma preocupação importante nas redes DTN.

2.3.3 SEGURANÇA

A segurança dos dados que trafegam pelas redes DTN é uma questão relevante, tendo em vista que, como em qualquer arquitetura de redes, é preciso estabelecer regras para o acesso aos dados. Por isso é preciso que um nó tenha condições de reconhecer os demais que fazem parte da rede, geralmente por meio de alguma chave para autenticação, e é importante a questão da criptografia dos dados transmitidos entre os nós.

2.3.4 DESCONEXÕES

A grande quantidade de desconexões interfere na efetividade dos contatos dos nós e criando um cenário de muita intermitência. Isso exigirá mais das estratégias dos protocolos DTN a fim de que medidas tomadas e soluções de contorno possam ser aplicadas.

2.3.5 CAPACIDADE ENERGÉTICA

Uma outra limitação, pouco mencionada, mas que influencia na capacidade dos nós continuarem colaborando uns com os outros (na movimentação, no sensoriamento e na transmissão de dados durante os contatos), é a questão da capacidade energética dos nós, tendo em vista que esse ponto afeta em relação a autonomia dos nós. Sem energia suficiente, os nós não terão condições de se manterem ativos e replicando os dados de forma colaborativa na rede.

2.4 DTN NO CENÁRIO MARÍTIMO

Devido às características inerentes do cenário marítimo, as redes DTN dariam aos nós da Rede uma maior flexibilidade, de forma a permitir que esses navios possam, mesmo distantes da rede, continuarem a transmitir as mensagens para as Estações Remotas mais distantes.

O cenário marítimo possui características peculiares que o torna apropriado para o uso de Redes Tolerantes a Atrasos, pelo fato de que as redes DTN são recomendadas somente para cenários calamitosos, marcados por muita intermitência nas conexões da rede, ausência de infraestrutura fim-a-fim e que seja beneficiada pela mobilidade dos nós (neste caso, os navios).

Algumas características importantes que tornam as redes marítimas atrativas para o uso de redes DTN, além da questão da mobilidade dos navios, são as seguintes (CHRYSOSTOMOU, 2013):

- A densidade na distribuição dos navios;
- Capacidade teoricamente ilimitada de *buffer*;
- Não haver problemas com limitação dos recursos de bateria; e
- Pelo fato da mobilidade dos nós não ser muito dinâmica, isso permite que o tempo de contato entre eles possa durar de muitos minutos a até mesmo horas, tornando esse tempo significativo para a transmissão efetiva dos dados (MOHSIN ET AL., 2015).

Com o objetivo de suprir a limitação da cobertura da rede marítima e aumentar a capacidade de transmissões com sucesso entre os nós melhorando as taxas de entrega dos pacotes, torna-se adequado o uso de redes DTN (OTT ET AL., 2006). Essa arquitetura de rede propõe uma melhora no desempenho de comunicação em cenários que não exista uma infraestrutura fim-a-fim.

Em meio a tantos cortes no orçamento das Forças Armadas justificaria aplicar estratégias DTN como forma de utilizar os recursos que já estão disponíveis (como a mobilidade dos nós, por exemplo) e como alternativa ao uso do enlace satelital, que nem sempre é disponibilizado pelo seu alto custo de locação e que gera uma forte dependência tecnológica com empresas oriundas de outros países.

2.5 TRABALHOS RELACIONADOS

Em (LI AND WU, 2007) é proposto o uso de MANET juntamente com um mecanismo que, baseado no histórico de mobilidade dos nós, permita que a rede tome decisões de encaminhamento com maior confiabilidade, tendo em vista que os encaminhamentos duvidosos poderiam gerar erros de entrega de pacotes.

Esse mecanismo baseia-se no fato de que a mobilidade nas MANETs permite que dois nós separados possam se encontrar no futuro para trocar informação e que o histórico desses encontros pode indicar quais dos nós seriam bons encaminhadores com um determinado nível de confiabilidade, para que a mensagem possa chegar ao seu destino final.

Dessa forma a mobilidade seria um fator que reduziria as incertezas, e assim isso refletiria nas decisões sobre rotas a serem tomadas, tendo em vista que as incertezas fazem crescer os custos sobre a transação e diminui a aceitação e cooperação na comunicação, pois só é possível obter colaboração se os nós forem realmente confiáveis.

(MOHSIN AND WOODS, 2014) propõe o uso da *mobile ad-hoc network* (MANET) como alternativa de menor custo para comunicação dos navios através da comunicação via rádios VHF. A rede MANET teria bastante limitações tendo em vista o ambiente marítimo possuir regiões densas como também outras bastante esparsas. O trabalho avaliou quatro protocolos MANET para o cenário marítimo : *Ad hoc On-Demand Distance Vector Protocol* (AODV), *Ad hoc On-Demand Multipath Distance Vector Protocol* (AOMDV), *Dynamic Source RoutingProtocol* (DSR) e *Destination-Sequenced Distance Vector Protocol* (DSDV), sendo que o mais eficiente foi o AOMDV.

Em (MOHSIN ET AL., 2015) também aborda o tema de MANET no cenário marítimo simulando três diferentes tipos de protocolos MANET. Ele também apresenta a aplicação de MANET como alternativa de menor custo para os navios. Chegou-se a conclusão que as rotas que a maioria dos navios desenvolvem no mar tendem a facilitar a entrega de pacotes através de múltiplos saltos.

De acordo com o texto, o desempenho dos protocolos MANET possui uma relação positiva com a densidade e uma relação inversa com a mobilidade e o quão esparso é o cenário. Isso significa que as taxas de entrega aumentam juntamente com a densidade e decrescem quando se aumenta a mobilidade dos nós da rede e quando os cenários se tornam mais esparsos.

(K. YOUNGBUM, 2009) propõe a utilização de uma rede semelhante às VANETS (*Vehicular Ad-hoc Network*) em ambiente marítimo denominada NANET (*Nautical Ad-*

hoc Network). A NANET comporia uma arquitetura híbrida de redes em modo MESH de forma a agregar capacidade de comunicação aos navios.

As simulações observadas ocorreram em três cenários de comunicações marítimas localizadas nos portos, na costa e no oceano. Em cada um deles simulou-se o comportamento da NANET quando esses navios estavam dentro e fora da cobertura das Estações de Acesso ao Rádio.

É importante salientar que o bom desempenho das redes DTN no mar dependerá da densidade dos navios na região, ou seja, que existam navios dentro do alcance máximo dos equipamentos de transmissão dos demais navios. Por exemplo, um modem de banda VHF, em um navio, que possua uma cobertura de raio em torno de 30 km e que tenha uma vizinhança (um ou mais navios) dentro desse alcance máximo poderá se beneficiar mais com as características de mobilidade das redes DTN. Em (CHRYSOSTOMOU, 2013) é defendida uma abordagem híbrida de arquitetura de redes envolvendo DTN e as comunicações marítimas. Realizou simulações em três cenários que variavam em área, comparando com diferentes tipos de protocolos de roteamento: o *Epidemic*, o *Prophet*, o *MaxProp*, *Spray and Wait* e o RAPID.

Chega-se à conclusão que os protocolos de roteamento probabilísticos obtiveram um melhor aproveitamento dos recursos de rede disponibilizados como também apresentou um bom desempenho na entrega de pacotes e que quanto mais informação à respeito da mobilidade futura dos navios mais eficiente o sistema será na detecção de mudanças na topologia da rede.

O trabalho enfatiza também que os benefícios das redes DTN se tornam mais visíveis na rede marítima nos cenários em que os navios estão mais esparsadamente distribuídos.

(KOLIOS AND LAMBRINOS, 2012) também apresenta redes DTN como opção mais econômica para o ambiente marítimo, propondo a utilização do sistema AIS (*Automatic Identification System*) como fonte de informação para os nós da rede a fim de melhorar a predição dos encaminhamentos e assim otimizar as taxas de entrega de mensagens.

O AIS provê várias informações a respeito dos nós, tais como: localização, velocidade, portos de destino e mudanças de curso. Essas informações seriam de grande valia para se saber onde estão os nós de destino das mensagens e quais seriam os nós que teriam maior probabilidade de entregar essas mensagens, ou seja, seriam os nós que estivessem indo na mesma direção dos nós destinatários das mensagens. Contudo, modificações bruscas nas rotas podem tornar o sistema menos previsível e com isso mais passível a falhas e perdas de desempenho.

(GUO ET AL., 2011) enfatizou na melhoria dos algoritmos de roteamento para o

uso em sensores de poluição na água através da categorização dos pacotes de dados, priorizando alguns em detrimento de outros e dando tratamento diferenciado de acordo com o peso que cada pacote recebia.

O objetivo era verificar o impacto dessas mudanças no consumo de bateria, da utilização de *buffer*, na largura de banda etc. Através dessa abordagem foi alcançado um bom resultado à respeito da taxa de entrega de pacotes, atraso e consumo de energia.

(S AND VISWANATHAN, 2012) fala sobre os principais tipos de ataques que são utilizados em redes DTN como : o ataque de DOS (*Denial of Service*) e DDoS (*Distributed Denial of Service*) que são utilizados para perturbar o correto funcionamento de uma arquitetura DTN no encaminhamento de mensagens. Nas redes DTN as mensagens são encaminhadas no momento em que dois nós se encontram e se mantêm no alcance de seus raios de cobertura.

O objetivo era que os nós viessem a colaborar para que as mensagens chegassem nos seus destinatários. Contudo, ataques às redes DTN são realizados através de nós mal intencionados e que trabalham com o intuito de restringir esses encaminhamentos. Esse trabalho defendeu a utilização de métodos para detecção dos nós que apresentaram mal funcionamento a fim de que eles fossem contornados, ou seja, excluídos da rede, permanecendo apenas aqueles nós que verdadeiramente contribuiriam para o encaminhamento das mensagens.

Esses nós mal intencionados, no momento do ataque, se apresentam como bons encaminhadores, mas quando recebem as mensagens, eles as descartam, mesmo não estando com seus *buffers* cheios. Um tipo de ataque de Negação de Serviços (DOS) para redes DTN bastante conhecido é o ataque do buraco negro (*black hole attack*), em que nós mal intencionados atraem para eles o máximo de mensagens da rede possível, para depois descartá-las propositadamente, sem fazer qualquer tipo de tentativa de encaminhamento ou de entrega.

(CHEN AND SHEN, 2016) propõe um mecanismo novo para manter o sigilo da informação de roteamento dos nós. Essa informação de roteamento, chamada no artigo de *routing utility*, é utilizada para se calcular a probabilidade de encaminhamento de mensagens para os destinatários.

As informações de roteamento contém os registros de encontros e a frequência desses encontros. Com elas, é possível estimar quais são os melhores encaminhadores de mensagens na rede DTN para um determinado destinatário. No entanto, em um ataque malicioso é possível gerar dados falsos a fim de que os nós atacantes possam se passar como aqueles que possuem as melhores métricas com a finalidade de concentrar neles

todas as mensagens as quais nunca serão repassadas.

O mecanismo proposto permite que decisões sejam tomadas à partir da divulgação parcial desses dados o restante deles ficariam protegidos por criptografia.

Em (LI ET AL., 2009) é proposto um mecanismo de troca de tíquetes de encontros para trazer maior confiabilidade na escolha dos nós encaminhadores na rede DTN. Os tíquetes serviriam como garantia de que os nós verdadeiramente se encontraram ao longo do tempo evitando que nós maliciosos pudessem criar falsas informações de roteamento a fim de se passarem como bons encaminhadores.

Essa estratégia se tornou eficaz no combate ao ataque do buraco negro, porém ainda era frágil ao ataque de *tailgating*. O ataque de *tailgating* faz com que o nó malicioso provoque falsos encontros com o objetivo de acumular tíquetes, para depois poder parecer ser um bom encaminhador. É um tipo de ataque que requer muita mobilidade e gasto de energia.

Comenta-se que a melhor estratégia para se combater os ataques de buracos negros e de *tailgating* juntos seria o uso de protocolos de roteamento em que utilize propagação aleatória, ou seja, sem utilizar probabilidade.

Percebe-se, de uma forma geral, que a temática central dos trabalhos que abordam as redes DTN no ambiente marítimo é sobre a demonstração da compatibilidade da arquitetura DTN aplicada nesse cenário por meio de simulações envolvendo diferentes tipos de estratégias de DTN e comprovando, através dos resultados, que as redes DTN obtiveram uma perceptível melhora no desempenho de entrega de pacotes beneficiando a comunicação na rede. Dentro desse contexto, os cenários são simulados utilizando os vários tipos de protocolos DTN mostrando-se, ao término, as principais vantagens e desvantagens entre eles. Em relação a segurança existem várias abordagens que, em sua maioria, focam em alguma estratégia atrelada à criptografia e em mecanismos de distribuição de chaves públicas e privadas (LI ET AL., 2009), (CHEN AND SHEN, 2016).

No trabalho atual, em um ambiente de simulação, serão selecionados alguns protocolos DTN para serem comparados, entre eles, quanto ao desempenho na entrega de mensagens, em cenários que possuam características de movimentação no mar. Além disso, será escolhido um, dentre esses protocolos (aquele que mais se adequou ao ambiente marítimo durante as simulações), para receber um módulo de segurança.

O módulo de segurança permitirá que as conexões sejam classificadas, como seguras ou inseguras, a fim de que contribua para redução no compartilhamento de mensagens sigilosas com nós considerados inimigos, ou seja, com aqueles que não forem identificados como pertencentes ao grupo de meios navais da Marinha do Brasil. O módulo pode ser

considerado a maior contribuição deste trabalho na questão de segurança em arquiteturas DTN.

3 RESULTADOS

Este capítulo será responsável por divulgar os resultados das simulações como também tecer comentários sobre os mesmos. Cada simulação realizada envolveu 3 protocolos DTN: *Epidemic/ Direct Delivery / Spray and Wait.*

Cada simulação correspondeu a 12 horas de movimentação em um ambiente marítimo. Inicialmente os Cenários foram simulados todos com a criação de 16 mensagens no total, no entanto simulações adicionais foram realizadas com a criação de 346, 585 e 587 mensagens. Os tamanhos das mensagens nas simulações variaram de 11 a 100 bytes e depois de 11 a 1000 bytes. Também foram realizadas simulações com e sem helicópteros.

3.1 RESULTADOS *DIRECT DELIVERY /EPIDEMIC/ SPRAY AND WAIT.*

3.1.1 CENÁRIO 1

As primeiras simulações nesse cenário compararam o desempenho dos três protocolos *Direct Delivery* , *Epidemic* e *Spray and Wait.* As principais configurações eram: 200 simulações, cada simulação com duração de 12 horas, intervalo de criação de mensagens entre 30 minutos e 1 hora (totalizando 16 mensagens), cada mensagem variava de 11 até 1000 *bytes* e com a participação de 36 nós, sendo que algumas vezes eram substituídos 4 navios por 4 helicópteros. Os resultados podem ser visualizados na Tabela 3.1.1.

Pôde-se observar através dos resultados que o protocolo *Epidemic* demonstrou ser o melhor para a entrega de pacotes no Cenário 1 com 16 mensagens. Essa superioridade foi de 7,80% sobre o *Spray and Wait* e de 32,99% sobre o *Direct Delivery.* Os desempenhos dos protocolos na entrega das mensagens pode ser visualizada nas Figuras 3.1 e 3.2.

Observa-se também que a presença de helicópteros no Cenário 1 contribuiu para uma queda sensível no tempo de atraso da entrega de mensagens em em cerca de 45,27% como pode ser visto na Figura 3.3.

As simulações no Cenário 1 de forma geral mostrou o protocolo *Epidemic* como a opção que obteve o melhor desempenho em termos de entrega de mensagens, cerca de 98,45%. Em seguida veio o protocolo *Spray and Wait* entregando por volta de 90,65 % das mensagens. Em último lugar vem o *Direct Delivery* entregando por volta de 65,46 % das mensagens.

Lembrando que o *Direct Delivery* representa uma configuração mais aproximada de

Protocolo	Epidemic	Direct Delivery	Spray and Wait
N. Nós	36	36	36
Helicóptero	Não	Não	Não
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	15,54	10,13	14,075
Desvio Padrão Entregas	0,861458387	2,412925829	1,45601335
Int. de Conf. Entregas (95%)	0,119389847	0,334408313	0,201789447
Média Atrasos (segundos)	633,554077	4499,69693	2651,976786
Desvio Padrão Atrasos	724,7290005	1481,363213	1091,346891
Int. de Conf. Atrasos (95%)	100,4404693	205,3026942	151,2501829
N. Nós	36	36	36
Helicóptero	Sim	Sim	Sim
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	15,8	10,17	14,58
Desvio Padrão Entregas	0,459407528	2,40207197	1,126920471
Int. de Conf. Entregas (95%)	0,063669465	0,332904073	0,156180339
Média Atrasos (segundos)	338,148658	4340,851267	2396,008554
Desvio Padrão Atrasos	340,5905652	1560,538044	931,8666939
Int. de Conf. Atrasos (95%)	47,20257668	216,2755644	129,1477615
N. Nós	36	36	36
Helicóptero	Não	Não	Não
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	15,525	10,11940299	14,055
Desvio Padrão Entregas	0,867836795	2,411570368	1,487629054
Int. de Conf. Entregas (95%)	0,120273833	0,33422046	0,206171079
Média Atrasos (segundos)	716,466267	4513,030527	2680,495563
Desvio Padrão Atrasos	733,2091293	1489,697799	1099,285796
Int. de Conf. Atrasos (95%)	101,6157336	206,4577877	152,3504389
N. Nós	36	36	36
Helicóptero	Sim	Sim	Sim
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	15,775	10,165	14,585
Desvio Padrão Entregas	0,485337783	2,399282766	1,135438728
Int. de Conf. Entregas (95%)	0,067263149	0,332517516	0,157360888
Média Atrasos (segundos)	415,920536	4349,62299	2400,022832
Desvio Padrão Atrasos	347,5296748	1560,697499	911,5898615
Int. de Conf. Atrasos (95%)	48,16427054	216,2976633	126,3375875

TAB. 3.1: Resultado de simulações do Cenário 1 com a criação de 16 mensagens.

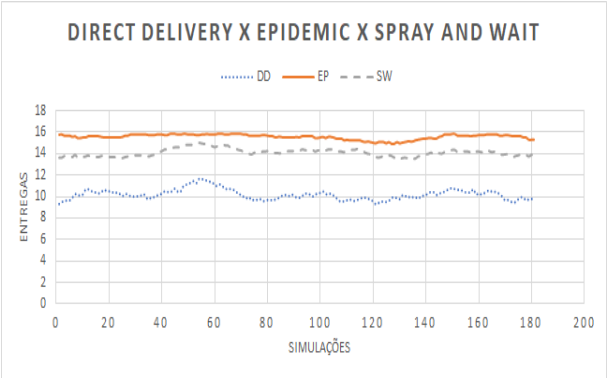


FIG. 3.1: Cenário 1 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas.

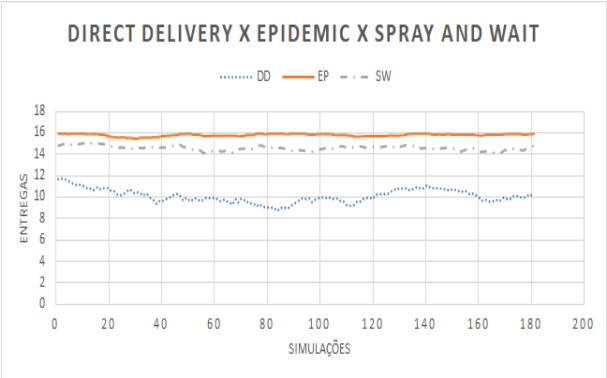


FIG. 3.2: Cenário 1 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas com helicópteros.

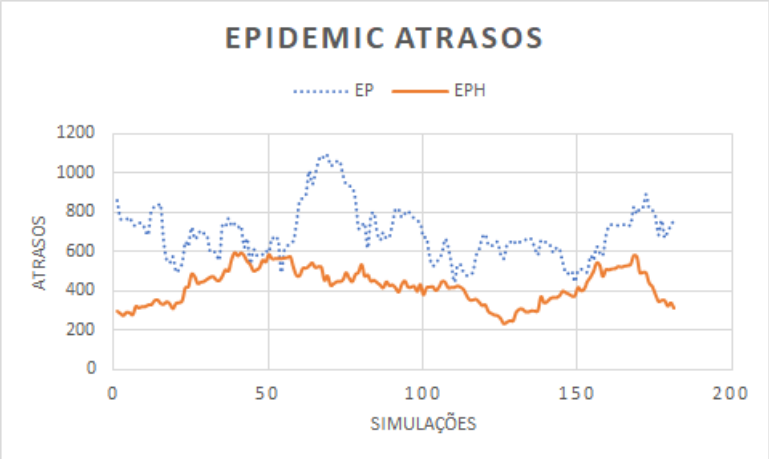


FIG. 3.3: Cenário 1 atrasos do protocolo *Epidemic* com 1000 bytes com e sem helicópteros.

uma rede sem os benefícios das retransmissões de mensagens, semelhante às redes convencionais. Por isso essa configuração foi usada com o intuito de comparar com um cenário sem os benefícios das redes DTN.

Com a inclusão de veículos de maior velocidade representando os helicópteros, no total de 4, pode-se verificar sensível diminuição no tempo de entrega em torno de 45% no protocolo *Epidemic* no Cenário 1, reduzindo os atrasos, como nos mostra a Figura 3.3.

3.1.2 CENÁRIO 2

Nas primeiras simulações do Cenário 2 também comparou-se o desempenho dos três protocolos *Direct Delivery* , *Epidemic* e *Spray and Wait*. As principais configurações também foram: 200 simulações, cada simulação com duração de 12 horas, intervalo de criação de mensagens entre 30 minutos e 1 hora (totalizando 16 mensagens), cada mensagem variava de 11 até 1000 *bytes* e com a participação de 36 nós, sendo que algumas vezes eram

substituídos 4 navios por 4 helicópteros. Os resultados podem ser visualizados na Tabela 3.2.

Protocolo	*Epidemic*	*Direct Delivery*	*Spray and Wait*
N. Nós	36	36	36
Helicóptero	não	não	não
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	8,005	2,425	5,495
Desvio Padrão Entregas	2,99832	1,702607	2,542103
Int. de Conf. Entregas (95%)	0,415538	0,235965	0,352311
Média Atrasos	6195,523	5282,99	6287,029
Desvio Padrão Atrasos	2307,296	3846,225	2853,434
Int. de Conf. Atrasos (95%)	319,769	533,0498	395,4585
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	10,75	2,68	8,16
Desvio Padrão Entregas	2,819084	1,981726	2,883744
Int. de Conf. Entregas (95%)	0,390698	0,274648	0,399659
Média Atrasos	5513,564	5563,865	6285,764
Desvio Padrão Atrasos	1825,773	3672,684	2365,95
Int. de Conf. Atrasos (95%)	253,0346	508,9986	327,898
N. Nós	36	36	36
Helicóptero	não	não	não
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	7,94	2,425	5,48
Desvio Padrão Entregas	2,991848221	1,702607	2,528153
Int. de Conf. Entregas (95%)	0,414641389	0,235965	0,350378
Média Atrasos	6243,399	5289,417	6328,35
Desvio Padrão Atrasos	2314,782	3845,906	2860,967
Int. de Conf. Atrasos (95%)	320,8065	533,0056	396,5026
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	10,72	2,68	8,15
Desvio Padrão Entregas	2,80373	1,981726	2,896454
Int. de Conf. Entregas (95%)	0,38857	0,274648	0,401421
Média Atrasos	5593,831	5599,315	6305,294
Desvio Padrão Atrasos	1834,27	3649,322	2352,569
Int. de Conf. Atrasos (95%)	254,2122	505,7609	326,0435

TAB. 3.2: Resultado de simulações do Cenário 2 com a criação de 16 mensagens.

No segundo Cenário, de forma geral, pôde-se perceber uma queda de desempenho na entrega de mensagens em todos os protocolos quando comparado com o do Cenário 1. Isso se deve ao fato de que a área de simulação sofreu um aumento significativo de 250 km^2 ao mesmo tempo que a quantidade de nós presentes no Cenário 2 permaneceu a mesma do Cenário 1 (36 nós).

Por esse motivo o número de mensagens entregues caíram para todos os protocolos: o *Epidemic* com 61%, *Spray and Wait* com 45% e *Direct Delivery* com 17,55% das 16 mensagens entregues. Contudo o protocolo Epidêmico permaneceu sendo o melhor para o encaminhamento de mensagens no Cenário 2 entregando cerca de 43,43% a mais do que o *Direct Delivery* e 16% a mais que o *Spray and Wait*. Essa ordem pode ser visualizada nos gráficos das Figuras 3.4 e 3.5.

A presença de helicópteros diminuiu cerca de 11,20% o tempo médio de atraso da entrega de mensagens, para o protocolo *Epidemic*, como pode ser visualizado no gráfico da Figura 3.6.

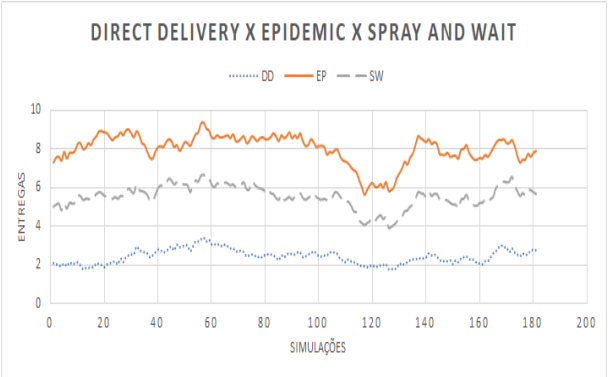


FIG. 3.4: Cenário 2 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas.

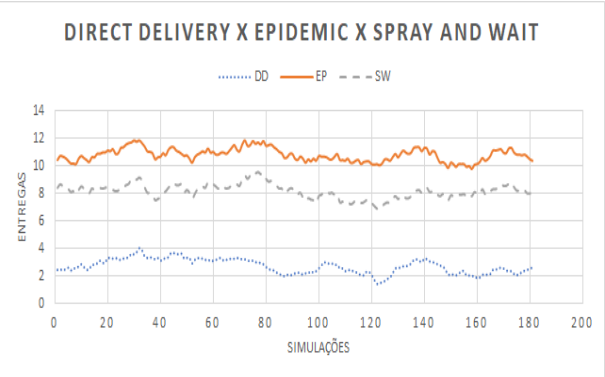


FIG. 3.5: Cenário 2 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas com helicópteros.

Foram realizadas simulações adicionais com 340 e 581 mensagens mantendo-se a mesma quantidade de nós (36 no total), sendo que 4 desses nós desenvolviam velocidades superiores aos demais, (de 100 a 300 km/h) representando os helicópteros. Os dados das novas simulações estão na Tabela 3.3.

De acordo com a Tabela 3.3 nas simulações com o protocolo *Epidemic* 67% das mensagens foram entregues enquanto que o protocolo *Spray and Wait* entregou 53% e o *Direct Delivery* entregou somente 18% das mensagens. Contudo nas simulações com 581 mensagens os protocolos *Epidemic* e *Spray and Wait* empataram com aproximadamente 64% das mensagens entregues enquanto que o protocolo *Direct Delivery* manteve os 18% de mensagens entregues.

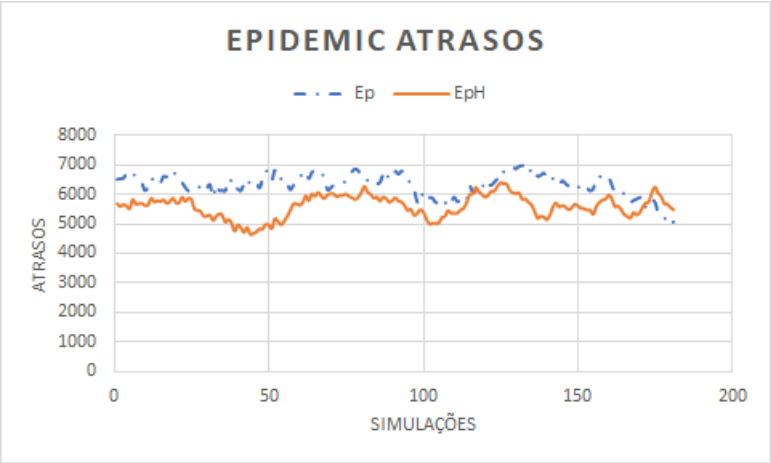


FIG. 3.6: Cenário 2 atrasos do protocolo *Epidemic* com 1000 bytes com e sem helicópteros.

Protocolo	Epidemic	Direct Delivery	Spray and Wait
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	340	340	340
Tamanho (bytes)	1000	1000	1000
Média de Entregas	220,62	57,325	174,355
Desvio Padrão Entregas	42,29373	24,13362	40,39428
Int. de Conf. Entregas (95%)	5,861504	3,344687	5,598258
Média Atrasos	6080,902	5900,831	6391,973
Desvio Padrao Atrasos	1178,592	1123,598	853,8176
Int. de Conf. Atrasos (95%)	163,3415	155,7199	118,3309
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	581	581	581
Tamanho (bytes)	1000	1000	1000
Média de Entregas	360,85	97,88	360,3085
Desvio Padrão Entregas	72,66843	41,28131	72,892
Int. de Conf. Entregas (95%)	10,07115	5,721192	10,10213
Média Atrasos	6429,012	5978,24	6424,89
Desvio Padrao Atrasos	1260,869	985,6946	1259,07
Int. de Conf. Atrasos (95%)	174,7443	136,6078	174,4949

TAB. 3.3: Resultado de simulações do Cenário 2 com a criação de 340 e 581 mensagens, respectivamente.

3.1.3 CENÁRIO 3

Como era de se esperar, aumentando-se o cenário e mantendo-se a mesma quantidade de nós o número de mensagens entregues aos destinatários tende a diminuir. Isso porque são poucos navios para cobrir uma área muito extensa, por isso para melhorar o desempenho, nesse caso, é importante a inclusão de mais nós na rede com a finalidade de se aumentar

a colaboração. Por esse motivo, no Cenário 3, serão feitas algumas simulações com 61 navios, ou seja, 25 nós a mais. Os resultados dessas simulações com 16 mensagens que variavam até 1000 bytes podem ser vistos na Tabela 3.4.

No Cenário 3 o protocolo *Epidemic* entregou cerca de 41,31% das mensagens, o protocolo *Spray and Wait* 34,83% e o *Direct Delivery* cerca de 15,81%. Isso mostrou que mesmo em um cenário bastante esparso e com poucas mensagens, o protocolo *Epidemic* se torna o favorito para o encaminhamento de mensagens, como mostram as Figuras 3.7 e 3.8.

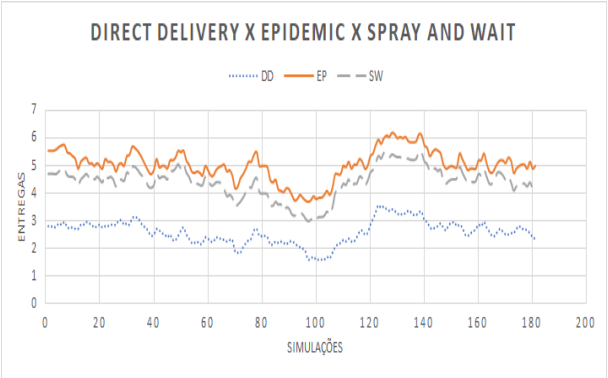


FIG. 3.7: Cenário 3 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas.

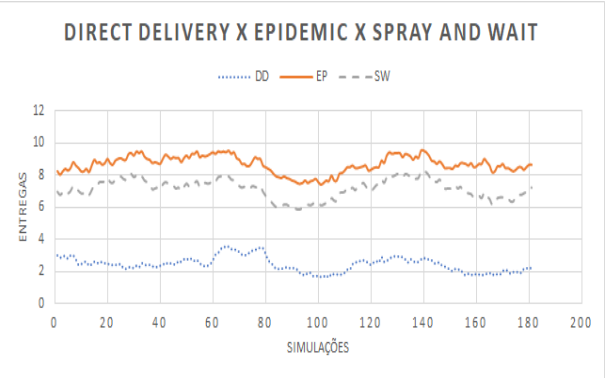


FIG. 3.8: Cenário 3 Direct Delivery x Epidêmic x Spray and Wait com 1000 bytes entregas com helicópteros.

Mesmo com os helicópteros os tempos médios de atrasos no protocolo *Epidemic* subiram em torno de 20 % em relação aos atrasos sem helicópteros, como ilustra a Figura 3.9. Contudo, contribuiu para um aumento na entrega de mensagens de aproximadamente 22%. Isso permite sugerir aumentar a quantidade de nós na rede para suprir as lacunas do Cenário 3.

3.1.3.1 CENÁRIO 3 COM MAIS MENSAGENS E MAIS NAVIOS

À medida que aumenta-se a quantidade de mensagens, sem a adição de novos nós, a tendência é haver perda de desempenho nos protocolos DTN, principalmente nos *Epidemic* e *Spray and Wait*, pois dependem da colaboração dos nós para que as mensagens atinjam os destinatários. Todavia, quando aumenta-se a quantidade de nós no cenário, como mostra a Tabela 3.5, de 36 para 61 nós, pode-se notar uma melhora em torno de 4,21% na entrega das 346 mensagens e de 2,81% na entrega de 585 mensagens, no protocolo *Epidemic*.

Como era esperado, com o aumento do número de nós houve uma melhora no desem-

Protocolo	*Epidemic*	Direct Delivery	Spray and Wait
N. Nós	36	36	36
Helicóptero	não	não	não
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	5,05	2,57	4,415
Desvio Padrão Entregas	2,65381114	1,67004348	2,319412289
Int. de Conf. Entregas (95%)	0,367792701	0,231451965	0,321448236
Média Atrasos	5441,963159	5534,782345	5839,782148
Desvio Padrao Atrasos	3392,778501	4064,948801	3697,086302
Int. de Conf. Atrasos (95%)	470,2064699	563,3628089	512,3806045
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	16	16	16
Tamanho (bytes)	100	100	100
Média de Entregas	8,65	2,455	7,135
Desvio Padrão Entregas	2,623339389	1,820589942	2,399073314
Int. de Conf. Entregas (95%)	0,363569609	0,252316256	0,332488488
Média Atrasos	6730,871305	5245,690009	6739,201352
Desvio Padrao Atrasos	2364,538491	3792,008543	2446,506308
Int. de Conf. Atrasos (95%)	327,7022937	525,5359142	339,0622448
N. Nós	36	36	36
Helicóptero	não	não	não
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	5,05	2,57	4,41
Desvio Padrão Entregas	2,65381114	1,67004348	2,308363644
Int. de Conf. Entregas (95%)	0,367792701	0,231451965	0,319917
Média Atrasos	5494,543077	5542,839125	5875,18148
Desvio Padrao Atrasos	3394,263806	4065,666634	3695,172166
Int. de Conf. Atrasos (95%)	470,412319	563,4622936	512,1153236
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	16	16	16
Tamanho (bytes)	1000	1000	1000
Média de Entregas	8,625	2,455	7,125
Desvio Padrão Entregas	2,611219511	1,820589942	2,389124227
Int. de Conf. Entregas (95%)	0,361889911	0,252316256	0,33110964
Média Atrasos	6776,554359	5253,371795	6742,329184
Desvio Padrao Atrasos	2359,009943	3792,670315	2423,85844
Int. de Conf. Atrasos (95%)	326,9360902	525,6276293	335,9234681

TAB. 3.4: Resultado de simulações do Cenário 3 com a criação de 16 mensagens.

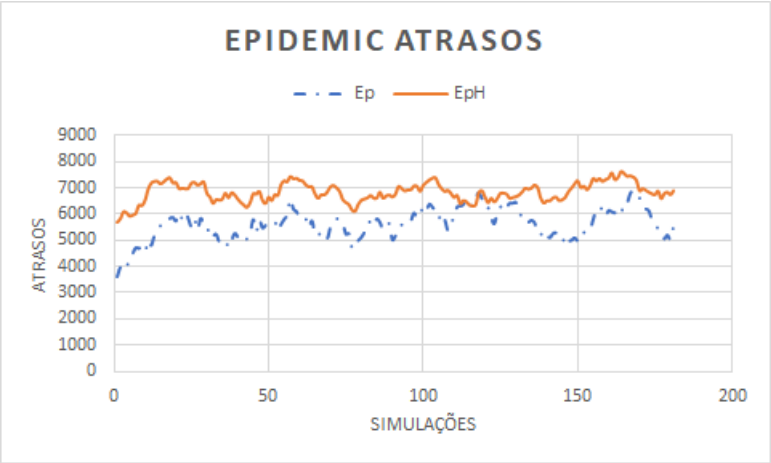


FIG. 3.9: Cenário 3 atrasos do protocolo *Epidemic* com 1000 bytes com e sem helicópteros.

penho dos protocolos *Epidemic* e *Spray and Wait* no Cenário 3, tendo em vista o aumento da densidade dos navios e com isso o crescimento da colaboração entre os nós. Pode-se inferir que melhorando a densidade dos nós na rede DTN, isso influenciará no desempenho no encaminhamento das mensagens pelos protocolos.

3.2 RESULTADOS DE SIMULAÇÕES COM O PROTOCOLO *EPIDEMIC* SEGURO COM FUNÇÃO DISCRIMINANTE

Até o presente momento o desempenho dos protocolos DTN contaram com a colaboração de nós intermediários que não faziam parte da rede da Marinha do Brasil e excluir essas colaborações irá resultar em perda de desempenho, em torno de 50%. Ou seja, cerca de 50% das mensagens entregues com sucesso teve a colaboração de nós que não eram navios da Marinha. Isso implicaria dizer que se simplesmente essas conexões tivessem sido bloqueadas, por volta da metade das mensagens não teriam chegado ao nó de destino. Por esse motivo é preciso pensar na questão da segurança em equilíbrio com o desempenho. Por isso ao tomar a decisão de se bloquear uma conexão considerada insegura essa ação afetará o desempenho da rede DTN.

Por essa razão, foram realizadas novas simulações nas mesmas condições das anteriores, contudo, aplicando-se, dessa vez, funções discriminantes (Omnidirecional e Direcional) para seleção das conexões seguras no protocolo *Epidemic*.

3.2.1 MÓDULO DE SEGURANÇA PARA O PROTOCOLO *EPIDEMIC*

As redes DTN funcionam de forma eficiente em ambiente esparsados, ou seja, em cenários que existam nós que estejam dispersos e não concentrados. Em ambientes com alta

Protocolo	Epidemic	Direct Delivery	Spray and Wait
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	346	346	346
Tamanho (bytes)	1000	1000	1000
Média de Entregas	115,475	55,885	100,815
Desvio Padrão Entregas	24,28018	16,23854	21,67231
Int. de Conf. Entregas (95%)	3,364999	2,250506	3,003574
Média Atrasos	5856,344	5754,148	6002,003
Desvio Padrao Atrasos	1320,625	934,5402	1044,798
Int. de Conf. Atrasos (95%)	183,026	129,5183	144,7989
N. Nós	36	36	36
Helicóptero	sim	sim	sim
N. Mensagens	585	585	585
Tamanho (bytes)	1000	1000	1000
Média de Entregas	192,7	95,285	171,16
Desvio Padrão Entregas	40,26083	27,47175	36,46936
Int. de Conf. Entregas (95%)	5,579764	3,807321	5,054303
Média Atrasos	5967,809	5789,011	6017,444
Desvio Padrao Atrasos	1250,073	866,694	1022,221
Int. de Conf. Atrasos (95%)	173,2481	120,1154	141,67
N. Nós	61	61	61
Helicóptero	sim	sim	sim
N. Mensagens	346	346	346
Tamanho (bytes)	1000	1000	1000
Média de Entregas	130,535	53,565	103,005
Desvio Padrão Entregas	20,83914887	13,03824197	17,5013273
Int. de Conf. Entregas (95%)	2,888105612	1,806974941	2,425515644
Média Atrasos	5228,188159	5483,663908	5790,321355
Desvio Padrao Atrasos	1167,009578	968,635469	926,3002428
Int. de Conf. Atrasos (95%)	161,7363038	134,2435601	128,3763049
N. Nós	61	61	61
Helicóptero	sim	sim	sim
N. Mensagens	585	585	585
Tamanho (bytes)	1000	1000	1000
Média de Entregas	203,26	76,25	160,85
Desvio Padrão Entregas	42,57494	24,96163	35,52998
Int. de Conf. Entregas (95%)	5,900477	3,459442	4,924113
Média Atrasos	5545,287	5188,21	5870,827
Desvio Padrao Atrasos	1351,363	1026,76	1083,837
Int. de Conf. Atrasos (95%)	187,2859	142,2991	150,2094

TAB. 3.5: Resultado de simulações do Cenário 3 com a criação de 346/585 mensagens, com a participação de 36/61 nós e com a inclusão de helicópteros.

densidade de nós as entregas por contatos diretos com os destinatário são beneficiadas em comparação às entregas por encaminhamentos através de nós intermediários. Isso se deve, primeiramente, ao fato de que em cenários mais densos existe uma maior probabilidade de que os nós origem e destino venham a se encontrar e que as mensagens sejam encaminhadas diretamente em modo *relay*.

Nos cenários muito densos as redes DTN não terão o mesmo desempenho que em cenários esparsados, tendo em vista que a rede não se beneficiará de forma colaborativa por meio de mensagens encaminhadas através de nós intermediários que se movimentam no cenário (em cenários muito densos o envio direto entre os *hosts* de origem e destino terá mais vantagens).

Outro problema é que em ambientes de grande concentração, uma DTN irá demandar elevados recursos de roteamento (devido à elevada quantidade de contatos) que envolverá gastos de energia e de armazenamento, principalmente quando o protocolo de roteamento utilizado é não probabilístico, como é o caso do *Epidemic*, protocolo adotado neste trabalho.

Em redes com uma densidade elevada de nós, o protocolo *Epidemic* poderia causar uma sobrecarga na rede gerando uma quantidade excessiva de encaminhamentos, o que provocaria estouros nos limites dos *buffers* dos nós e consequentemente o descarte de mensagens. Contudo nos cenários de baixa densidade o protocolo *Epidemic* se encaixaria como o mais recomendado, pois tentará aproveitar todas as oportunidades para a transmissão de mensagens.

Como visto anteriormente, o ambiente marítimo possui características de baixa densidade de nós e uma grande quantidade de conexões e desconexões ao longo do tempo. Por esse motivo, a arquitetura DTN seria uma solução adicional, de baixo custo, para os cenários que envolveriam os meios navais da Marinha do Brasil, que também dispõe de poucos navios para o patrulhamento de áreas extensas e que sofre constantemente com intermitências da rede. Sendo que a solução normalmente aplicada envolve a alocação de grandes recursos financeiros para requisitar cobertura via enlace de satélites de empresas estrangeiras a fim de poder tramitar mensagens com conteúdo sigiloso.

Dentre os protocolos de roteamento DTN aquele que mais se adequaria aos cenários da Marinha do Brasil e que poderia trazer benefícios ao trâmite de pequenas mensagens do sistema tático é o protocolo *Epidemic*. Por não ser um protocolo determinístico ele fará com que o nó de origem encaminhe mensagens para qualquer nó que também possua o protocolo DTN ativo e que tenha mantido o contato. Ou seja, o protocolo *Epidemic* visa o encaminhamento de mensagens para todos os nós que estão em contato naquele momento,

sem haver qualquer preocupação com as métricas de roteamento dos nós intermediários. Esse tipo de protocolo é recomendável para redes que possuam poucos nós e que queiram aproveitar o máximo de oportunidades de contatos possível. Essas características, desse protocolo, beneficiariam a entrega de mensagens através de encaminhamentos, contudo sem haver preocupação alguma com a questão da segurança.

O comportamento do protocolo *Epidemic* pode ser visualizado no diagrama da Figura 3.10. Pode-se ver no diagrama, que o protocolo *Epidemic* está sempre em busca de novas conexões, no entanto ele prioriza a entrega ao destinatário. Porém, se o nó de origem não estiver em contato direto com algum destinatário, o protocolo irá priorizar os encaminhamentos. Contudo, nessa grande quantidade de encaminhamentos reside o perigo da insegurança.

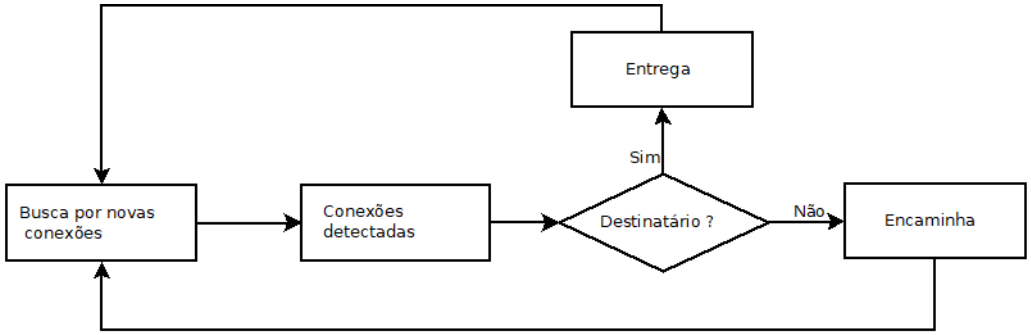


FIG. 3.10: Descrição básica do protocolo *Epidemic*.

Dentre as questões existentes sobre Redes Tolerantes a Atrasos, a Segurança é um dos problemas que precisa ser considerado, visto que da mesma forma que ataques podem ocorrer nas redes convencionais, versões podem vir a ser reproduzidas para redes DTN (FARRELL AND CAHILL, 2006).

Um ataque de Negação de Serviços (DOS) pode ser considerado o mais comum em uma rede DTN e uma estratégia simples para controle desse tipo de ataque é, após a detecção do nó infectado, evitá-lo excluindo-o da rede. Essa detecção só é possível através de análises de comportamento da rede realizadas por nós especificamente selecionados para esse tipo de função.

Dessa forma, um nó detectado com mal funcionamento pode se comportar descartando todas as mensagens que ele deveria encaminhar, contudo esse nó se apresenta na rede como estando em boas condições para realizar os encaminhamentos (Ataque de Buracos Negros) (BURGESS ET AL., 2007).

Existem trabalhos em que o histórico de encaminhamento de pacotes de cada nó

é compartilhado a fim de que o sistema possa detectar os nós que estão funcionando mal e excluí-los da rede (LI AND CAO, 2012), (S AND VISWANATHAN, 2012). O mau comportamento dos nós das redes DTN irá acusar aqueles que são considerados maliciosos e isso só é possível através de monitoramento e do compartilhamento de informações de encaminhamento de pacotes através da rede (KATE ET AL., 2007).

Uma outra característica de um nó com mau funcionamento é quando ele começa a inundar a rede com requisições de forma que gere uma quantidade absurda de pedidos para os nós, deixando-os inoperantes, através de um estouro de *buffer* por exemplo. Esse padrão também pode ser analisado por histórico compartilhado e caso seja detectada alguma anomalia, esses nós seriam excluídos da rede.

A incerteza faz aumentar os custos computacionais e diminui as aceitações de comunicação e de cooperação, por isso a escolha de um modelo de decisão que seja confiável (reduzindo a incerteza) é importante tanto para utilização eficiente dos recursos disponíveis como também no estabelecimento de uma comunicação segura (LI AND WU, 2007).

Como as missões táticas no mar possuem rotas bem definidas e controladas, essas rotas se tornariam carimbos certificadores dos navios da Marinha no mar, e qualquer encontro inesperado poderia ser tratado como uma tentativa de intrusão.

Dessa forma o intruso deverá, além de tentar se passar por um navio aliado, copiar as rotas dos navios para somente assim conseguir se passar como um nó legítimo. Isso exigiria um esforço muito maior para a investida contra a rede DTN que fará com que o intruso gaste mais tempo e energia tentando encontrar essas regiões de maior probabilidade que somente os nós autorizados irão conhecer.

Contudo, para se obter essas regiões seguras de maior probabilidade é necessário encontrar, primeiramente, uma regra que classificaria essas conexões consideradas seguras. Então em posse do histórico de conexões seguras, as demais, que não estivessem nele presentes, seriam bloqueadas. Isso significaria aplicar uma restrição ainda mais forte, o que poderia implicar em perda de desempenho, mas por outro lado seria um ganho em relação à segurança por manter o sigilo de mensagens crítica das missões.

No entanto, na questão da segurança, este trabalho estará focado em encontrar o primeiro quesito para obtenção desses históricos, que é demonstrar um método que funcione para classificar as conexões como sendo seguras ou inseguras. À partir desse mapeamento das conexões seguras é que será possível guardar esses pontos (latitudes e longitudes) a fim de mapear essas regiões para futuras consultas na segunda versão do módulo de segurança.

É importante salientar que o objetivo deste trabalho não está em substituir as téc-

nicas tradicionais de segurança que envolva criptografia, por exemplo. Mas sim, visando em apresentar um modelo baseado em classificação a fim de que possa ser usado conjuntamente com as melhores práticas de segurança, já em vigor.

Da mesma maneira, a arquitetura DTN não viria para substituir as outras arquiteturas, mas sim trabalhar em conjunto com as demais soluções em uma rede híbrida.

3.2.2 SEGURANÇA DAS CONEXÕES

A comunicação via radiotransmissão se dá através de ondas de rádio que se propagam entre as antenas transmissora e receptora, respectivamente. Essas ondas de rádio são na verdade ondas eletromagnéticas. Uma onda eletromagnética possui a capacidade de transportar energia. A onda se propaga através de três fenômenos ondulatórios, são eles: reflexão, refração e difração.

A reflexão ocorre quando a onda atinge uma superfície e volta a se propagar pelo meio de origem mantendo as suas características de velocidade, frequência e comprimento de onda, como mostra a Figura 3.11.

No caso da refração a onda alterna de meio de propagação, por isso a sua velocidade e seu comprimento são alterados, mantendo-se somente a frequência constante, como mostra a Figura 3.12.

A difração é a capacidade da onda de contornar obstáculos. Ocorre, por exemplo, quando uma determinada onda encontra uma barreira que contém uma fenda, então essa onda se propagará através dessa fenda, como mostra a Figura 3.13.

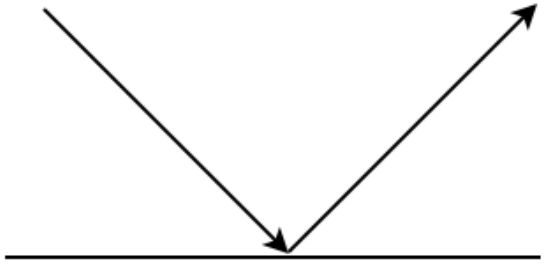


FIG. 3.11: Fenômeno ondulatório da reflexão.

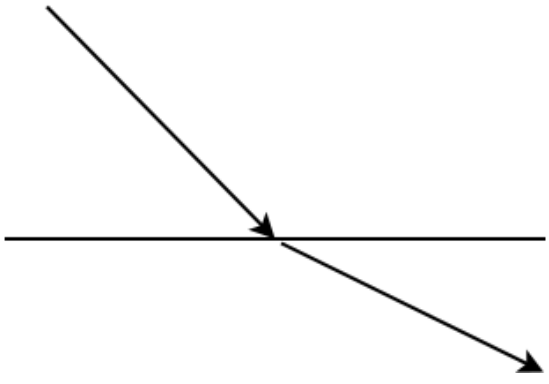


FIG. 3.12: Fenômeno ondulatório da refração.

A antena transmissora converte variações de tensão e corrente em ondas eletromagnéticas enquanto que a receptora realiza o trabalho inverso, transformando a energia

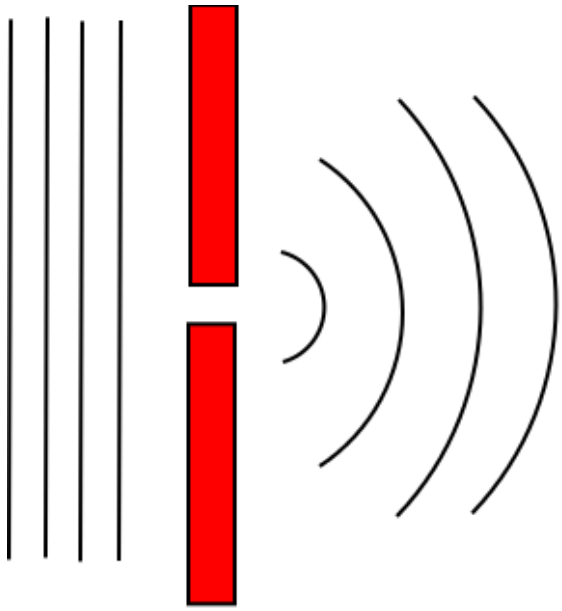


FIG. 3.13: Fenômeno ondulatório da difração.

transportada pelas ondas eletromagnéticas em variações de tensão e corrente elétrica que serão tratados pelo equipamento receptor. As ondas eletromagnéticas são representadas por senoides (uma para o campo elétrico e a outra para o campo magnético).

De forma geral as antenas podem ser classificadas como direcionais e omnidirecionais. Uma antena direcional aumenta o alcance em termos de distância, mas o ângulo de cobertura diminui. Os sinais direcionados são mais fortes pois concentram a potência em uma direção.

As antenas omnidirecionais enviam o sinal para todas as direções. Elas possuem a vantagem de atingir um ângulo de cobertura de 360º. Contudo, mesmo apresentando mais possibilidades de conectividade, irradiando ondas eletromagnéticas para todas as direções, as antenas omnidirecionais acabam fornecendo brechas de segurança.

Antes de se transmitir os dados, o navio de origem identificaria o navio de destino. Pode haver nesse momento uma troca de mensagens cifradas no intuito de se certificar a autenticidade do nó de destino. No entanto, ele detecta também a presença de vários outros navios que apesar de não fazerem parte da sua rede irão receber esses dados captando as ondas eletromagnéticas através de suas antenas. Por esse motivo as mensagens tramitadas devem ser cifradas visando proteger seu conteúdo de forma que somente as pessoas que possuam as chaves possam ter acesso a eles. Contudo, técnicas de criptoanálise podem ser aplicadas nesse contexto com o objetivo de se descobrir o texto em claro.

Possíveis fontes que poderiam fornecer informação sobre a identidade e a distância dos nós no mar seriam as seguintes:

- o sistema AIS (*Automatic Identification System*) que se baseia no compartilhamento de informação entre os navios, dentre elas, de geolocalização;
- a alça optrônica do radar, que é um equipamento usado para detecção de alvos; e
- sistemas *Identification Friend or Foe* (IFF) do radar, que é constituído de um interrogador e um *transponder*. O equipamento interrogador solicita dados de identificação e o *transponder* responde. Os navios da Marinha do Brasil possuem ambos, interrogadores e *transponders*, porém as aeronaves e submarinos somente *transponders*.

O IFF foi um sistema projetado para comando e controle e indica se um dado veículo é aliado, seu porte e distância. É considerado um sistema secundário do radar pois funciona de forma de forma independente do primeiro. O sistema foi desenvolvido na Segunda Guerra Mundial e foi primeiramente empregado nos radares para distinguirem as aeronaves inimigas das aliadas. No primeiro do contato são enviados pulsos de interrogação, que serão decodificados pelo nó de destino. Se o código de interrogação estiver correto, o navio ou aeronave responderá com pulsos de resposta através dos *transponders*. Para essa comunicação são utilizadas faixas de frequências distintas, uma para interrogação e a outra para a resposta.

Com o objetivo de minimizar esses riscos foi proposto neste trabalho a implementação de um módulo de segurança que leva em consideração a configuração do cenário que os nós de origem e de destino estão inseridos, levando-se em consideração parâmetros indicadores de segurança como: a quantidade de navios inimigos presentes, a proximidade do aliado em relação ao inimigo, etc. Esses parâmetros seriam recebidos como entrada e em troca o sistema classificaria a conexão como sendo segura ou insegura.

Esse módulo seria utilizado no protocolo *Epidemic* no intuito de detectar conexões seguras e bloquear as inseguras. Para a classificação dessas conexões foi utilizada uma técnica estatística chamada análise discriminante.

3.2.3 ANÁLISE DISCRIMINANTE

É uma técnica que é aplicada para classificar itens de um espaço amostral que sejam multivariados. Para que a classificação seja possível é necessário o conhecimento prévio à

respeito dos grupos aos quais pertencem os elementos da amostra. Esse conhecimento a priori deverá ser tomado como verdade pelo sistema.

É também necessário fornecer parâmetros que sejam significativos para a correta classificação dos grupos. Por fim, essa técnica cria uma função matemática denominada regra de classificação ou discriminação, a qual será útil para classificar novos itens (desconhecidos) nos grupos já conhecidos.

Para construir uma regra de classificação que seja precisa é necessário conhecer as distribuições de probabilidade das características dos elementos da população.

Quanto mais a regra conseguir minimizar a chance de classificar incorretamente os elementos de uma amostra, maior será a precisão. Para esse objetivo, usa-se o princípio da máxima verossimilhança, o qual se baseia em estimar parâmetros desconhecidos a partir de dados de uma amostra juntamente com uma função de distribuição conhecidos. Através da máxima verossimilhança, os parâmetros desconhecidos podem ser estimados, tentando-se estabelecer uma relação de máxima probabilidade com a função de verossimilhança.

Como no caso de dois fenômenos A e B que possuam distribuição normal ,conhecendo-se a média de cada uma das distribuições μ_A e μ_B e as variâncias, é possível calcular a razão de verossimilhança.

A razão de verossimilhança está descrita na Equação 3.1:

$$\lambda(x) = \frac{f_A(x)}{f_B(x)} \tag{3.1}$$

Sendo que $f_A(x)$ e $f_B(x)$ são as funções de densidade de probabilidade de cada um dos grupos. Neste exemplo pode-se assumir que as funções de densidade de probabilidades são do tipo Normal sendo representadas pela Equação 3.2.

$$\lambda(x) = \frac{\frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu_A)^2/2\sigma^2}}{\frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu_B)^2/2\sigma^2}} \tag{3.2}$$

O $\lambda(x)$ será também chamada de função discriminante e o seu comportamento deverá servir para a classificação entre os dois grupos A e B. Se $\lambda(x) > 1$ então pode-se dizer que o elemento é pertencente ao grupo A pois o seu valor está mais próximo da média μ_A do que μ_B, caso contrário se $\lambda(x) < 1$ então então o elemento será classificado como pertencente ao grupo B pois o valor do elemento está mais próximo da média μ_B do que μ_A.

Contudo, se $\lambda(x) = 1$ haverá a mesma probabilidade desse elemento estar em ambos os grupos A e B, ou seja, enquanto as médias μ_A e μ_B forem distantes, as classificações

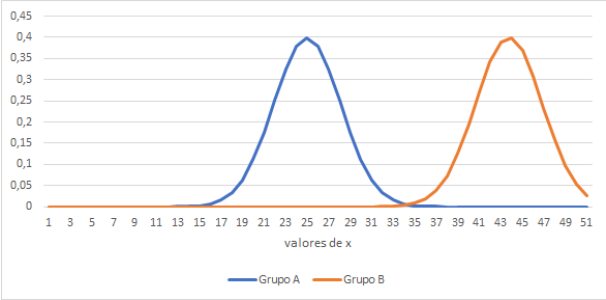


FIG. 3.14: Ausência de intersecção 1.

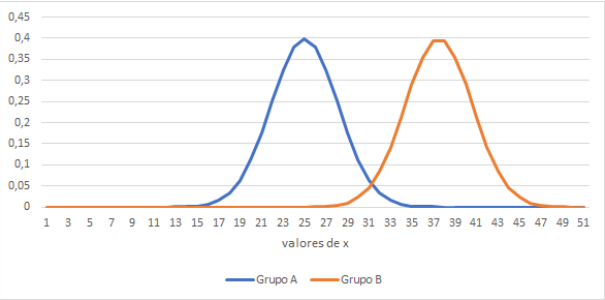


FIG. 3.15: Início de intersecção 2.

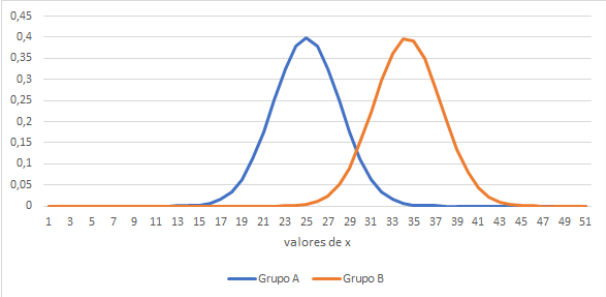


FIG. 3.16: Aumento de intersecção 3.

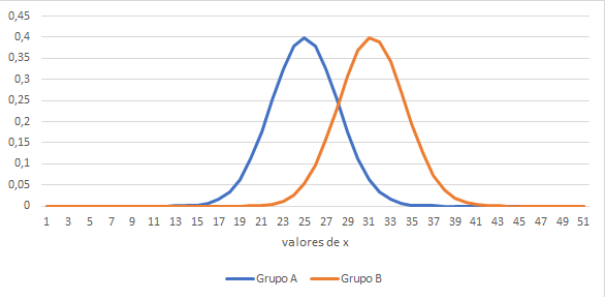


FIG. 3.17: Aumento de intersecção 4.

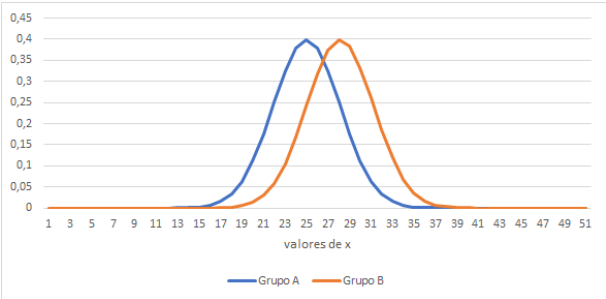


FIG. 3.18: Aumento de intersecção 5.

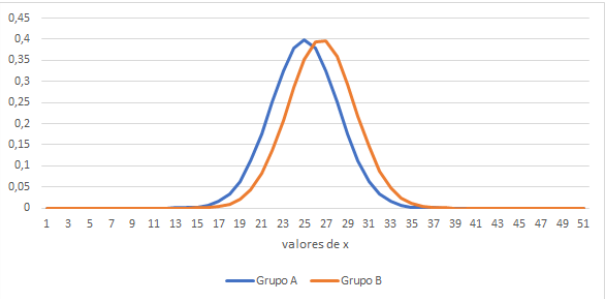


FIG. 3.19: Aumento de intersecção 6.

ocorrerão mais precisamente (ver Figura 3.14), contudo, se as médias dos dois grupos forem muito próximas aparecerá uma região de intersecção que, quanto maior for, dificultará a classificação no grupo correto. Pode-se visualizar o aumento da área de intersecção observando as Figuras 3.15, 3.16, 3.17, 3.18 e 3.19.

as funções discriminantes podem se reescritas como sendo combinações lineares de variáveis independentes usadas para a classificação dos elementos nos grupos conhecidos, esse é o tipo de função chamada de discriminante de Fisher, como mostra a Equação 3.3, onde μ_A e μ_B são as médias das populações e $\sum^{-1}$ é a matriz de covariâncias.

$$fd(x) = (\mu_A - \mu_B)' \sum^{-1} x - \frac{1}{2}(\mu_A - \mu_B)' \sum^{-1} (\mu_A + \mu_B) \tag{3.3}$$

3.2.4 ANÁLISE DISCRIMINANTE DAS CONEXÕES

O objetivo a ser alcançado com análise discriminante nesse trabalho é a classificação das conexões de uma rede DTN como sendo seguras ou inseguras, baseando-se em parâmetros que estão relacionados com os encontros dos nós na rede. Para isto, levou-se em consideração dois tipos de configuração de antenas, sendo elas direcionais ou omnidirecionais.

A direcional possui a vantagem de não espalhar o sinal para todas as direções, sendo assim, ela acaba contribuindo mais com uma possível conexão segura do que uma antena omnidirecional, que irradia seu sinal para todas as direções, como representado na Figura 3.20.

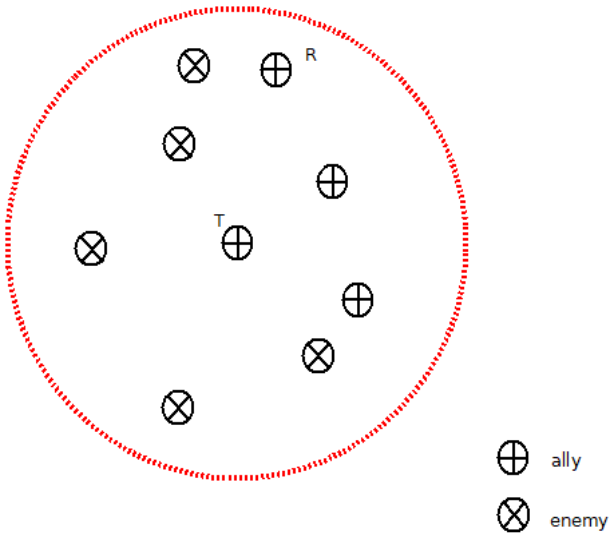


FIG. 3.20: Irradiação omnidirecional. O Transmissor (T) precisa enviar a mensagem para o Receptor (R), porém acaba irradiando para todo o perímetro.

Dessa forma, foram realizadas novas simulações nas quais foram classificadas as cone-

xões quanto à segurança, levando-se em consideração os dois tipos de antenas (direcionais ou omnidirecionais).

Nas simulações, foram levados em consideração a quantidade de aliados e de inimigos presentes no perímetro durante um encontro (considera-se como perímetro, o raio de alcance da antena no momento da conexão, isso variou entre 10 a 13 km), o nó menos distante, a distância entre o nó de origem e o de destino, a distância do inimigo mais próximo, a distância do aliado mais próximo, se o mais próximo é um aliado e se o destinatário da conexão é aliado ou inimigo (possível através do Sistema IFF do radar, por exemplo).

No caso das antenas direcionais levou-se em consideração um ângulo de 90º para as simulações, portanto, à medida que esse ângulo diminui, aumenta-se a diretividade e com isso aumenta-se a segurança, pois a direção de propagação da onda eletromagnética se dará em uma faixa mais estreita e com isso diminui-se a chance de que possa existir um intruso no perímetro que possa captar o sinal transmitido. Dessa forma os parâmetros passados para simulação de segurança em uma antena direcional são a distância do nó de origem ao de destino, se o destinatário é um aliado ou inimigo, a quantidade de inimigos presentes na linha de visada da antena, a quantidade de aliados presentes na linha de visada da antena e se o *host* mais próximo da visada é um aliado ou inimigo.

Diferentemente do modo omnidirecional que irradia o sinal eletromagnético para todas as direções, a função direcional, implementada nesse trabalho, concentrará a irradiação no quadrante no qual se encontra o nó destinatário, excluindo os outros três. Por esse motivo a função da visada direcional passará para a função discriminante direcional somente os dados contidos no quadrante em que o destinatário esteja incluso, totalizando uma cobertura de ângulo de 90 graus.

Esses parâmetros são importantes para se tomar a decisão de se transmitir ou não uma informação no perímetro durante um dado encontro tendo em vista questões que envolvam a presença de navios não autorizados no perímetro e em relação à proximidade com nós inimigos. Por exemplo, se em um dado perímetro inexiste a presença de inimigos, pode-se dizer que a conexão é totalmente segura para se transmitir.

Da mesma forma, se na região de um encontro existem mais aliados do que inimigos e se o nó de destino (aliado) for o nó mais próximo do nó de origem existirá uma possibilidade maior de se considerar essa região como segura.

A Figura 3.22 mostra um transmissor (T) e um receptor (R) em um perímetro com mais aliados (em azul) do que inimigos (em vermelho). Nesse caso, a conexão poderia ser considerada segura. Contudo, se no perímetro de uma conexão estiverem presentes

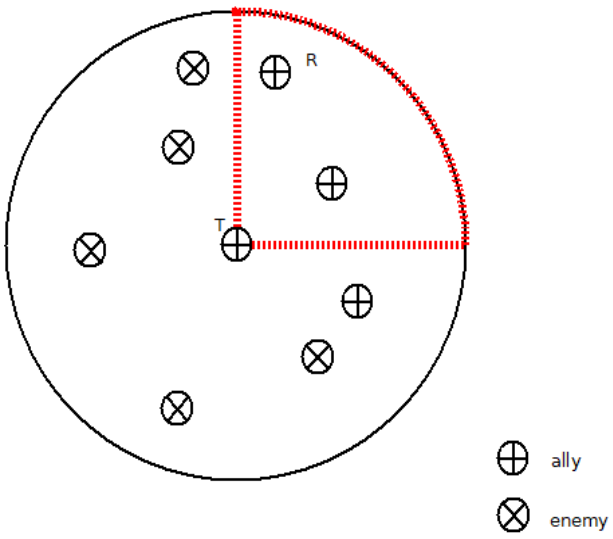


FIG. 3.21: Irradiação direcional. O Transmissor (T) precisa enviar a mensagem para o Receptor (R), para tanto irradia no quadrante cujo o destinatário esteja presente, com um ângulo fixo de 90 graus.

mais inimigos do que aliados, ou se esses inimigos estiverem muito próximos do nó de origem ou do nó de destino, existirá uma grande chance de interceptação de sinal, por isso essa conexão deverá ser considerada insegura. As Figuras 3.23 e 3.24 mostram um transmissor (T) tentando encaminhar mensagens para o receptor (R), ambos são aliados, porém existe um inimigo no perímetro (em vermelho), por isso essa conexão deveria ser classificada como insegura.

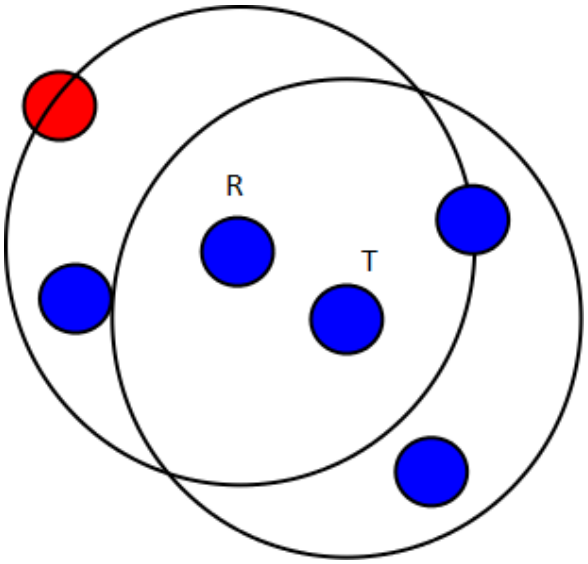


FIG. 3.22: Exemplo de encontro seguro entre transmissor (T) e receptor (R).

Dessa forma, a análise discriminante utiliza os mesmos parâmetros que foram utilizados para classificar a priori os elementos que representam encontros efetivos como seguros

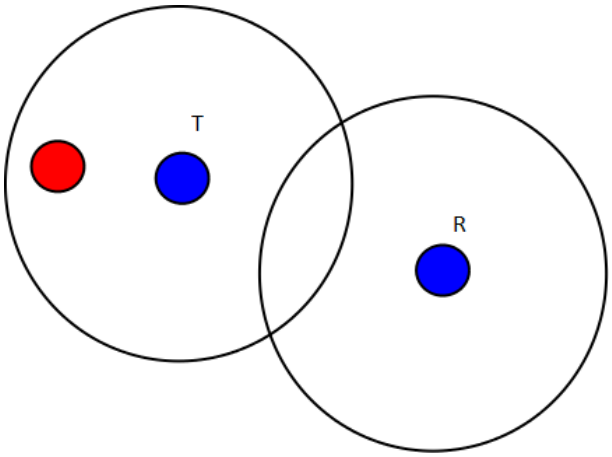


FIG. 3.23: Exemplo 1 de encontro inseguro entre transmissor (T) e receptor (R).

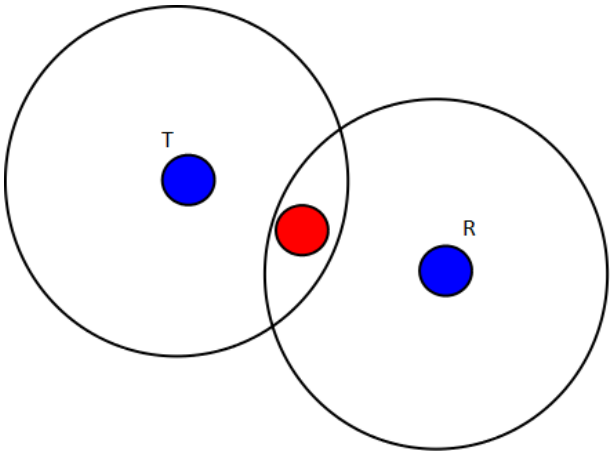


FIG. 3.24: Exemplo 2 de encontro inseguro entre transmissor (T) e receptor (R).

ou inseguros. Para, finalmente, criar uma função discriminante que classifique, com um nível adequado de precisão, os elementos que representam conexões, como sendo seguras ou inseguras.

O software utilizado para se realizar a análise discriminante foi o MINITAB, software da empresa Minitab Inc. Uma empresa privada sediada em *State College*, Pensilvânia, EUA. A seleção dos parâmetros para análise discriminante foi feita de maneira empírica, levando-se em consideração os que fossem mais relevantes na questão da segurança. Nesse processo, parâmetros foram adicionados enquanto que outros foram removidos (por apresentarem pouca relevância durante a análise), a fim de que as funções discriminantes pudessem reproduzir resultados mais próximos dos apresentados a priori. Os dados de classificações a priori foram extraídos de simulações.

3.2.5 PROTOCOLO *EPIDEMIC* COM FUNÇÃO DISCRIMINANTE

Como mencionado anteriormente, o protocolo *Epidemic* foi selecionado, dentre os existentes para redes DTN, tendo em vista a sua capacidade de disseminar dados aproveitando todas as oportunidades de conexão. Com isso a função discriminante poderia ser aplicada na seleção das conexões seguras, fazendo com que o protocolo possa selecionar as conexões baseadas nas condições do perímetro de comunicação. O comportamento do protocolo *Epidemic* em conjunto com a função discriminante pode ser observado no diagrama da Figura 3.25.

Como pode-se ver, comparando com o diagrama mais simplificado na Figura 3.10, o protocolo *Epidemic* passou por melhorias.

Primeiramente, é verificado se existe alguma conexão com o destinatário final das

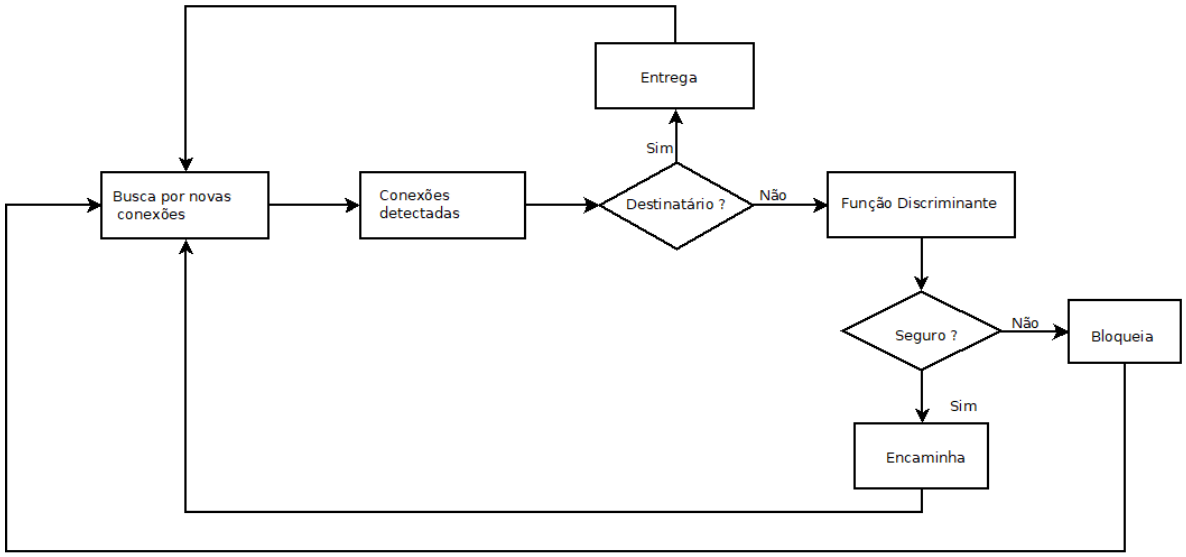


FIG. 3.25: Descrição básica do protocolo *Epidemic* com função discriminante.

mensagens a serem transmitidas, caso exista, essa conexão ganhará prioridade e as mensagens serão entregues ao seu destinatário final. Caso contrário, as mensagens serão encaminhadas, porém, dessa vez, essas conexões serão classificadas. Tenta-se enviar para alguém da lista de conexões, no entanto, a função discriminante (gerada anteriormente durante a análise discriminante) irá detectar se é seguro ou não transmitir os dados através de uma determinada conexão. Sendo considerada segura, os dados serão transmitidos e o nó (o navio) segue em busca de novas oportunidades de conexão ao longo da sua rota, caso contrário a conexão será bloqueada, então novas oportunidades de conexão serão buscadas pelo nó.

Percebe-se que a função discriminante será aplicada somente nos encaminhamentos indiretos das mensagens, portanto, em nada afetará o desempenho das mensagens entregues de forma direta, tendo em vista que, neste trabalho, foi considerado um ponto frágil do protocolo *Epidemic* os seus vários encaminhamentos de mensagens.

O próximo passo será utilizar as informações de localização dos encontros para aplicar uma restrição maior para as conexões, que seriam baseadas no histórico dos encontros considerados seguros. Esse histórico serviria para detectar movimentos anômalos na rede e a função discriminante ajudaria a prover esses pontos.

3.2.6 ANÁLISE DISCRIMINANTE OMNIDIRECIONAL

Foram simuladas 2654 conexões, sendo que delas 2712 foram classificadas como conexões inseguras (Grupo 0) e 798 seguras (Grupo 1) a priori, como pode ser visto na Tabela 3.6.

Grupos		
Grupo	0	1
Contagem	2712	798

TAB. 3.6: Conexões classificadas a priori nos dois grupos.

Esses dados serviram de base para a análise discriminante multivariada das conexões, para se criar uma função discriminante, que é uma expressão matemática, que gera resultados aproximados aos da classificação a priori.

Pode-se verificar de acordo com a Tabela 3.7 que a aproximação da função discriminante gerada com os resultados da classificação a priori obteve uma precisão na classificação a posteriori de quase 100% para ambos os grupos 0 e 1. O mesmo pode ser visto na Tabela 3.8 que mostra a medição da acurácia dos resultados da função discriminante.

		Classe Predita	
	Grupo	0	1
Classe Verdadeira	0	2680	30
	1	32	768
	Total de N	2712	798
	N correto	2680	768
	Proporção (Precisão)	0,988	0,962

TAB. 3.7: Conexões classificadas a posteriori nos dois grupos.

Classificações Corretas		
N	Correto	Proporção (Acurácia)
3510	3448	0,982

TAB. 3.8: Medição da acurácia da função discriminante.

Como mostra a Tabela 3.9 existe uma distância entre os dois grupos. Isso tornou possível uma classificação com maior precisão, tendo em vista que grupos muito próximos geram confusão no momento da classificação, como anteriormente mencionado. Ou seja, quanto mais próximos os grupos maior a probabilidade de erros de classificação.

Por fim, temos uma função discriminante linear para cada um dos grupos fd_0 e fd_1, como mostra a Tabela 3.10.

Distância Quadrática Entre Grupos		
	0	1
0	0	26,834
1	26,834	0

TAB. 3.9: Distância entre os grupos.

Função Discriminante Linear para o Grupo Omnidirecional		
	0	1
constante	-10,8876777247	-25,2637851236
dist_od	0,0006873730	0,0000562900
destinatário	2,2006247937	11,9459910732
ini	2,2603670023	1,7463959821
ali	2,3873702530	2,9789690743
menor_dist	0,0007618536	0,0010964448
mais_prox	2,8212830847	11,5176646994
dist_ini_prox	0,0000026170	0,0000180310
dist_ami_prox	0,0000070485	0,0000108450

TAB. 3.10: Função discriminante para ambos os grupos, para segurança em antenas omnidirecionais.

Através dessas funções é possível realizar classificações a posteriori das novas conexões, por meio dos parâmetros de segurança do perímetro. Os parâmetros das funções discriminantes estão descritos na Tabela 3.11, logo abaixo.

	Descrição dos parâmetros da função discriminante linear para antenas omnidirecionais
constante	Uma constante atribuída pela análise.
dist_od	A distância entre o transmissor e o receptor dos dados.
destinatário	Indica se o destinatário é um aliado ou um inimigo, utilizando para representação os valores um ou zero, respectivamente.
ini	Quantidade de inimigos no perímetro.
ali	Quantidade de aliados no perímetro.
menor_dist	A distância do nó mais próximo ao nó de origem.
mais_prox	Indica quem é o nó mais próximo, se for inimigo é representado por zero, caso contrário será representado por um.
dist_ini_prox	É a distância do inimigo mais próximo ao nó de origem.
dist_ami_prox	É a distância do aliado mais próximo ao nó de origem.

TAB. 3.11: Descrição dos parâmetros das funções discriminantes em antenas omnidirecionais.

Calcula-se cada função discriminante utilizando os valores dos parâmetros que representam a segurança do perímetro, comparado-se os resultados das funções fd_0 e fd_1. Se $fd_0 > fd_1$ significa que a conexão foi classificada como pertencente ao grupo zero (inse-

guro), pois obteve uma pontuação maior para esse grupo. Caso contrário, se $fd_0 < fd_1$ significa que a conexão foi classificada no grupo um e por isso é uma conexão segura.

O modo como são calculadas fd_0 e fd_1, usando os parâmetros do perímetro de segurança, pode ser visto logo abaixo:

$$fd_0(x) = constante_0 + dist\_od_0(x_1) + destinatario_0(x_2) + ini_0(x_3) + ali_0(x_4) + menor\_dist_0(x_5) + mais\_prox_0(x_6) + dist\_ini\_prox_0(x_7) + dist\_ami\_prox_0(x_8)$$

$$fd_1(x) = constante_1 + dist\_od_1(x_1) + destinatario_1(x_2) + ini_1(x_3) + ali_1(x_4) + menor\_dist_1(x_5) + mais\_prox_1(x_6) + dist\_ini\_prox_1(x_7) + dist\_ami\_prox_1(x_8)$$

O vetor x representa os dados de segurança do perímetro, a posteriori, $[x_1, x_2, x_3...x_8]$, que serão utilizados para o cálculo de de fd_0 e fd_1.

3.2.7 ANÁLISE DISCRIMINANTE DIRECIONAL

Seguindo os mesmos passos da análise discriminante realizada para as antenas omnidirecionais foi também realizada uma análise discriminante para a segurança em antenas direcionais. Foram coletados dados de 3510 encontros, sendo que delas 2506 foram classificadas como conexões inseguras (Grupo 0) e 1004 seguras (Grupo 1) a priori, como pode ser visto na Tabela 3.12.

Grupos		
Grupo	0	1
Contagem	2506	1004

TAB. 3.12: Conexões classificadas a priori nos dois grupos.

Pôde-se verificar de acordo com a Tabela 3.13 que a aproximação da função discriminante gerada com os resultados da classificação a priori obteve uma precisão na classificação a posteriori de aproximadamente 100% para ambos os grupos 0 e 1. O mesmo pode ser visto na Tabela 3.14 que mostra a medição da acurácia dos resultados da função discriminante.

Pode-se constatar também, que a aproximação da função discriminante para antenas direcionais se deu de forma bastante precisa, um fator importante para esse resultado se deve ao grande distanciamento entre os grupos 0 e 1 nas simulações direcionais, como pode-se ver na Tabela 3.15. Grupos mais distantes permitem uma classificação mais precisa com menos elementos formando intersecção.

		Classe Predita	
	Grupo	0	1
Classe Verdadeira	0	2506	0
	1	0	1004
	Total de N	2506	1004
	N correto	2506	1004
	Proporção (Precisão)	1	1

TAB. 3.13: Conexões classificadas a posteriori nos dois grupos.

Classificações Corretas		
N	Correto	Proporção (Acurácia)
3510	3510	1

TAB. 3.14: Medição da acurácia da função discriminante.

Distância Quadrática Entre Grupos		
	0	1
0	0	369613
1	369613	0

TAB. 3.15: Distância entre os grupos.

Função Discriminante Linear para o Grupo Direcional		
	0	1
constante	-21,4730403378	-186204,8986442230
dist_od	0,0003314234	-0,2248181938
destinatario	10,9924666567	789,7466812982
qntd_ini_visada	8,3006092303	510,3340114402
qntd_ami_visada	8,1523172741	-154,8431726991
ini_mais_prox_visada	0,0013972843	0,3754072552
ami_mais_prox_visada	0,0000198844	-0,0003384868
host_dest_prox_visada	-1,4013761751	-1706,8102019036

TAB. 3.16: função discriminante para ambos os grupos, para segurança em antenas direcionais.

Através dessas funções é possível realizar classificações a posteriori das novas conexões, por meio dos parâmetros de segurança do perímetro. Os parâmetros das funções discriminantes estão descritos na Tabela 3.17, logo abaixo.

Calcula-se cada função discriminante utilizando os valores dos parâmetros que representam a segurança do perímetro, comparado-se os resultados das funções fd_0 e fd_1. Se $fd_0 > fd_1$ significa que a conexão foi classificada como pertencente ao grupo zero (inseguro), pois obteve uma pontuação maior para esse grupo. Caso contrário, se $fd_0 < fd_1$ significa que a conexão foi classificada no grupo um e por isso é uma conexão segura.

O modo como são calculadas fd_0 e fd_1, usando os parâmetros do perímetro de segu-

	Descrição dos parâmetros da função discriminante linear para antenas direcionais
constante	Uma constante atribuída pela análise.
dist_od	A distância entre o transmissor e o receptor dos dados.
destinatário	Indica se o destinatário é um aliado ou um inimigo, utilizando para representação os valores um ou zero, respectivamente.
qntd_ini_visada	Quantidade de inimigos presentes na visada de 90º.
qntd_ami_visada	Quantidade de aliados presentes na visada de 90º.
ini_mais_prox_visada	A distância do inimigo mais próximo da visada.
ami_mais_prox_visada	A distância do aliado mais próximo da visada.
host_dest_prox_visada	Indica quem é o host de destino mais próximo da visada. Se for um aliado seu valor será um, caso contrário seu valor será zero.

TAB. 3.17: Descrição dos parâmetros das funções discriminantes em antenas omnidirecionais.

rança, pode ser visto logo abaixo:

$fd_0(x) = constante_0 + dist\_od_0(x_1) + destinatario_0(x_2) + qntd\_ini\_visada_0(x_3) + qntd\_ami\_visada_0(x_4) + ini\_mais\_prox\_visada_0(x_5) + ami\_mais\_prox\_visada_0(x_6) + host\_dest\_prox\_visada_0(x_7)$

$fd_1(x) = constante_1 + dist\_od_1(x_1) + destinatario_1(x_2) + qntd\_ini\_visada_1(x_3) + qntd\_ami\_visada_1(x_4) + ini\_mais\_prox\_visada_1(x_5) + ami\_mais\_prox\_visada_1(x_6) + host\_dest\_prox\_visada_1(x_7)$

O vetor x representa os dados de segurança do perímetro, a posteriori, $[x_1, x_2, x_3...x_8]$, que serão utilizados para o cálculo de de fd_0 e fd_1.

3.3 ANÁLISE DOS RESULTADOS DO PROTOCOLO *EPIDEMIC* SEGURO

Neste ponto do trabalho, foram repetidas as simulações com os cenários, no entanto, dessa vez, utilizando as funções discriminantes em um protocolo *Epidemic* modificado. Cada cenário passou por 200 simulações em que se usou sementes diferentes das utilizadas para análise discriminante, no intuito de se testar a eficiência das funções discriminantes. Ou seja, na análise discriminante utilizou sementes de 0 até 199, porém na validação com o *Epidemic* Seguro foram utilizadas sementes de 200 até 399.

3.3.1 CENÁRIO 1

Comparando os resultados, visíveis na Tabela 3.18, o *Epidemic* puro, no Cenário 1, atinge uma média de 57% de encaminhamentos inimigos. Sendo que 37% das mensagens entregues, por ele, foi em consequência de contribuições inimigas. Ou seja, 189 das 511 mensagens entregues receberam ajuda de um nó da rede que não era um aliado. Então, se esses nós inimigos fossem maliciosos e aplicassem o ataque do Buraco Negro, por exemplo, essas 189 mensagens não teriam chegado ao destinatário e prejudicaria o desempenho do protocolo *Epidemic* puro. Isso permite concluir que, no Cenário 1, 61 navios seriam o suficiente para entregar cerca de 87% das mensagens, através de encaminhamentos, pelo protocolo *Epidemic*. Contudo, se 35 desses nós fossem mal intencionados haveria uma redução em torno de 37% do desempenho e cerca 57% das conexões estariam comprometendo a segurança, pois estariam compartilhando dados com navios inimigos.

O protocolo *Epidemic* Bloqueio Total, simplesmente testa se existe algum inimigo no perímetro, caso exista, aquela conexão é bloqueada e nada é transmitido. Comparando com o *Epidemic* puro, pode-se ver uma redução de 8% das entregas, isso se deve ao fato de que a restrição para bloqueio faz com que o protocolo perca muitas oportunidades para encaminhamentos.

No entanto, em relação ao *Epidemic* com função discriminante pôde-se observar um aumento de desempenho de 1%, no *Epidemic* omnidirecional, e de 2% no *Epidemic* Direcional, em relação ao *Epidemic* puro. A diferença de desempenho não foi grande no Cenário 1, em comparação com os demais cenários. No entanto, mais adiante, será visto que essa diferença se tornará maior, à medida que a área dos cenários aumentam.

No protocolo *Epidemic* direcional, no Cenário 1, a função discriminante cometeu erros e com isso permitiu alguns encaminhamentos com inimigos que chegaram em torno de 23% dos encaminhamentos totais, no entanto, das 525 mensagens entregues, em média, houve uma contribuição inimiga de apenas 3%, enquanto que no *Epidemic* puro esse valor foi de 37%.

3.3.2 CENÁRIO 2

Comparando os resultados, visíveis na Tabela 3.19, o *Epidemic* puro, no Cenário 2, atinge uma média de 58% de encaminhamentos inimigos. Sendo que 40% das mensagens entregues, por ele, foi em consequência de contribuições inimigas. Ou seja, 156 das 400 mensagens entregues receberam ajuda de um nó da rede que não era um aliado. Então, se esses nós inimigos fossem maliciosos e aplicassem o ataque do Buraco Negro, por exemplo,

Cenário 1				
Protocolo	Epidemic	Epidemic Bloqueio Total	Epidemic Omnidirecional	Epidemic Direcional
N. Nós	61	61	61	61
Helicóptero	sim	sim	sim	sim
N. Mensagens	587	587	587	587
Tamanho (bytes)	1000	1000	1000	1000
Média de Entregas	511,895	403,8	515,315	525,75
Desvio Padrão Entregas	79,6835	29,73822	29,0168	24,8955
Int. de Conf. Entregas (95%)	11,0434	4,121431	4,02145	3,45028
Média Atrasos	2981,03	4363,974	3535,25	3237,02
Desvio Padrao Atrasos	2962,97	384,3093	794,773	827,459
Int. de Conf. Atrasos (95%)	410,64	53,26157	110,148	114,678
Encaminhamentos inimigos	37%	0%	0%	23%

TAB. 3.18: Comparação de resultado dos protocolos *Epidemic* no Cenário 1.

essas 156 mensagens não teriam chegado ao destinatário e prejudicaria o desempenho do protocolo *Epidemic* puro. Isso permite concluir que, no Cenário 2, 61 navios seriam o suficiente para entregar cerca de 70% das mensagens, através de encaminhamentos, pelo protocolo *Epidemic*. Contudo, se 35 desses nós fossem mal intencionados haveria uma redução em torno de 40% do desempenho e cerca 58% das conexões estariam comprometendo a segurança, pois estariam compartilhando dados com navios inimigos.

O protocolo *Epidemic* Bloqueio Total, simplesmente testa se existe algum inimigo no perímetro, caso exista, aquela conexão é bloqueada e nada é transmitido. Comparando com o *Epidemic* puro, pode-se ver uma redução de 31% das entregas, isso se deve ao fato de que a restrição para bloqueio faz com que o protocolo perca muitas oportunidades para encaminhamentos.

Em relação ao *Epidemic* com função discriminante pode-se observar que a redução de desempenho foi de 13% no *Epidemic* omnidirecional e de apenas 10% no *Epidemic* direcional, em relação ao *Epidemic* puro.

3.3.3 CENÁRIO 3

Comparando os resultados, visíveis na Tabela 3.20, o *Epidemic* puro, no Cenário 3, atinge uma média de 61% de encaminhamentos inimigos. Sendo que 49% das mensagens entregues, por ele, foi em consequência de contribuições inimigas. Ou seja, 108 das 220 mensagens entregues receberam ajuda de um nó da rede que não era um aliado. Então, se esses nós inimigos fossem maliciosos e aplicassem o ataque do Buraco Negro, por exemplo,

Cenário 2				
Protocolo	Epidemic	Epidemic Bloqueio Total	Epidemic Omnidirecional	Epidemic Direcional
N. Nós	61	61	61	61
Helicóptero	sim	sim	sim	sim
N. Mensagens	587	587	587	587
Tamanho (bytes)	1000	1000	1000	1000
Média de Entregas	400,305	223,22	325,545	339,715
Desvio Padrão Entregas	61,0959	39,94521	55,4483	57,4065
Int. de Conf. Entregas (95%)	8,4673	5,536022	7,6846	7,95598
Média Atrasos	5697,84	7860,831	7389,1	7053,1
Desvio Padrao Atrasos	1373,79	584,9476	731,926	814,817
Int. de Conf. Atrasos (95%)	190,394	81,06812	101,438	112,926
Encaminhamentos inimigos	58%	0%	0%	0%

TAB. 3.19: Comparação de resultado dos protocolos *Epidemic* no Cenário 2.

essas 108 mensagens não teriam chegado ao destinatário e prejudicaria o desempenho do protocolo *Epidemic* puro. Isso permite concluir que, no Cenário 3, 61 navios seriam o suficiente para entregar cerca de 37% das mensagens, através de encaminhamentos, pelo protocolo *Epidemic*. Contudo, se 35 desses nós fossem mal intencionados haveria uma redução em torno de 49% do desempenho e cerca 61% das conexões estariam comprometendo a segurança, pois estariam compartilhando dados com navios inimigos.

O protocolo *Epidemic* Bloqueio Total, simplesmente testa se existe algum inimigo no perímetro, caso exista, aquela conexão é bloqueada e nada é transmitido. Comparando com o *Epidemic* puro, pode-se ver uma redução de 16% das entregas, isso se deve ao fato de que a restrição para bloqueio faz com que o protocolo perca muitas oportunidades para encaminhamentos.

Em relação ao *Epidemic* com função discriminante pode-se observar que a redução de desempenho foi de 12% no *Epidemic* omnidirecional e de apenas 10% no *Epidemic* direcional, em relação ao *Epidemic* puro.

A redução de desempenho era esperada, pois as restrições de segurança exigem que muitas conexões sejam bloqueadas. Contudo, o protocolo *Epidemic* com funções discriminantes (omnidirecional e direcional) se comportaram obtendo as menores reduções de desempenho, quando comparados ao *Epidemic* Bloqueio Total. Ou seja, permitiu filtrar as conexões mais arriscadas, porém sem perder tantas oportunidades. O *Epidemic* direcional, por exemplo, pôde concentrar sua restrição em apenas um dos quadrantes, isso permitiu que mais conexões pudessem acontecer do que no *Epidemic* omnidirecional, que

Cenário 3				
Protocolo	Epidemic	Epidemic Bloqueio Total	Epidemic Omnidirecional	Epidemic Direcional
N. Nós	61	61	61	61
Helicóptero	sim	sim	sim	sim
N. Mensagens	587	587	587	587
Tamanho (bytes)	1000	1000	1000	1000
Média de Entregas	220,075	125,32	151,1	159,12
Desvio Padrão Entregas	42,4555	30,56877	38,9046	41,06344644
Int. de Conf. Entregas (95%)	5,88393	4,236538	5,391803	5,690998746
Média Atrasos	5433,81	6560,45	6679,213	6482,001
Desvio Padrao Atrasos	1204,19	853,6813	952,7076	1042,294
Int. de Conf. Atrasos (95%)	166,889	118,312	132,0361	144,4519
Encaminhamentos Inimigos	61%	0%	0%	0%

TAB. 3.20: Comparação de resultado dos protocolos *Epidemic* no Cenário 3.

impõe sua restrição em todas as direções do perímetro.

4 CONCLUSÃO E TRABALHOS FUTUROS

A arquitetura DTN é útil em ambientes onde não existe uma infraestrutura de rede fim-a-fim. A capacidade de alcançar o destinatário de forma colaborativa, se beneficiando da mobilidade dos nós, faz com que a arquitetura DTN seja sugerida para suprir as lacunas deixadas pelas redes convencionais, a fim de que ambas trabalhem em conjunto em uma rede híbrida (arquitetura convencional e DTN).

O cenário marítimo tem características que favorecem o uso de redes DTN, tais como: *buffer* ilimitado, capacidade alta de energia, constante conexões e desconexões, velocidades compatíveis que favorecem contatos prolongados, etc.

O protocolo *Epidemic* foi o eleito para ser utilizado no cenário marítimo, tendo em vista que o seu funcionamento melhor coopera para obter mais oportunidades de contatos, entre os poucos navios da Marinha do Brasil. Porém o *Epidemic* possui a característica de disseminar informação para o máximo de nós possível, sem se preocupar com questões de segurança. Dessa forma, o trabalho atual adicionou um módulo de segurança no protocolo *Epidemic*, que utiliza análise discriminante para classificar as conexões, de encaminhamentos de mensagens, como sendo seguras ou inseguras. Se uma dada conexão for considerada insegura então ela será rejeitada, caso contrário os dados serão transmitidos entre os nós conectados.

O protocolo *Spray and Wait* impõe um tempo de espera, o que faz com que esse protocolo perca, frequentemente, mais oportunidades de conexões, por isso o desempenho do protocolo *Epidemic* seria menos prejudicado com a função discriminante, tendo em vista que o seu funcionamento fará com que ele tenha, naturalmente, mais oportunidades de encontros do que o *Spray and Wait* e o *Direct Delivery*.

A técnica de análise discriminante, neste caso, classificou as conexões em dois grupos: seguras ou inseguras. Esta classificação baseia-se em parâmetros do perímetro, tais como: quantidade de nós inimigos e de aliados presentes no raio de transmissão, a comparação entre as distâncias do destinatário aliado com a do inimigo mais próximo, etc. Esses parâmetros foram escolhidos de forma empírica. Ao final do processo, uma função discriminante é criada para classificar as conexões desconhecidas.

A função discriminante indicará ao protocolo *Epidemic* se é seguro ou não, transmitir dados em uma dada conexão, dependendo apenas da saída da função discriminante. Essa limitação imposta ao protocolo *Epidemic* visa reduzir o compartilhamento de dados

sigilosos com nós não autorizados.

Foi demonstrado que o protocolo *Epidemic* com função discriminante se mostrou mais eficiente do que o *Epidemic* com Bloqueio Total, na entrega de mensagens. Mostrando que a função discriminante alcança um melhor aproveitamento das poucas oportunidades de encontros existentes entre os navios de guerra. Foram verificados alguns erros de classificação, os mais significativos, cerca de 23%, ocorreram no protocolo *Epidemic* com função discriminante direcional, no Cenário 1. Esses erros permitiram que mensagens fossem compartilhadas com nós inimigos no primeiro cenário.

Como a função discriminante é uma aproximação dos dados classificados a priori, ela está sujeita a erros. No entanto, é possível melhorar a função discriminante direcional fornecendo dados mais precisos a priori, ou fazendo ajustes dos parâmetros (adicionando ou excluindo alguns deles), no intuito de gerar funções mais aproximadas e diminuindo os erros. Entretanto, de forma geral, tanto o *Epidemic* Omnidirecional quanto o Direcional contribuíram com mais entregas do que o *Epidemic* Bloqueio total.

A função discriminante pode classificar como insegura até mesmo uma conexão envolvendo dois nós aliados, isso porque a função discriminante leva em consideração outras variáveis que representam informações importantes do perímetro, sobre a segurança. É importante salientar, mais uma vez, que a função discriminante pode gerar saídas que levem a erros de classificação, pois ela é uma aproximação. Dessa maneira, algumas vezes, os dados de entrada sobre uma dada conexão, pode resultar em uma saída que a aproxime mais de um outro grupo que, na verdade, ela não pertença.

Aplicar função discriminante no protocolo Epidêmico é uma forma de aproveitar o poder de disseminação desse protocolo, mas ao mesmo tempo limita a transmissão de dados em áreas consideradas inseguras.

O módulo de segurança acaba estimulando mais conexões entre os aliados, o que por sua vez resultou em mais entregas de mensagens aos nós de destino. Pensando na possibilidade de um nó não aliado tentar aplicar um ataque de Buraco Negro, o módulo de segurança se torna benéfico, pois ajudaria aos nós selecionarem melhor as suas conexões através da função discriminante.

Para que o módulo de segurança venha a funcionar de forma eficiente com o protocolo *Epidemic*, é preciso aumentar a densidade de navios aliados nas regiões em que eles estão numericamente em desvantagem, em relação à quantidade dos nós inimigos (maioria). Duas opções para alcançar esse objetivo seriam:

- aumentar a quantidade dos navios da Marinha do Brasil nas missões com o objetivo

de obter maior probabilidade de colaboração entre os nós aliados. Essa no entanto seria uma opção mais custosa, visto que resultaria na obtenção de novos meios navais ou na circulação mais navios ou helicópteros durante as missões; e

- reconhecer navios passantes (mercantes, pesqueiros etc) como aliados da rede DTN para colaboração com o trâmite de mensagens táticas. Os navios reconhecidos pela rede receberiam essas mensagens, que já estarão protegidas por criptografia (por isso não terão acesso ao conteúdo), podendo colaborar com a rede DTN da Marinha encaminhando essas mensagens. Ao longo da história os navios mercantes já desempenharam um papel fundamental como colaboradores em tempos de guerra. Esse pensamento está alinhado com a Estratégia Nacional de Defesa que prevê o emprego dual dos equipamentos e tecnologias civis, tendo em vista serem úteis ao meio militar em momentos de crise.

Para obter maior eficiência na entrega de mensagens com segurança é preciso investir em colaboração de forma segura, diminuindo a quantidade de bloqueios, através do aumento da quantidade de navios confiáveis na rede. Seria também importante estimular a obtenção de tecnologias de comunicação direcional como padrão nas comunicações dos navios da Marinha do Brasil, tendo em vista serem mais seguras em comparação com a transmissão omnidirecional. Isso seria uma estratégia para que, ao longo do tempo, o histórico de encontros sinalizaria para mais conexões seguras do que inseguras (o contrário do atual cenário), o que contribuiria para que o módulo de segurança pudesse decidir por realizar mais encaminhamentos do que bloqueios, e assim mais mensagens seriam entregues.

Portanto, pode-se concluir que as principais contribuições deste trabalho foram:

- Sinalizar para a necessidade de uma arquitetura de redes, no cenário marítimo da Marinha do Brasil, que inclua DTN como arquitetura complementar, visando que esta seja uma solução de baixo custo e que possa vir a contribuir com a entrega de mensagens em regiões cuja conectividade com a rede convencional não teria alcance;

- Demonstrar, em ambiente de simulação, que o protocolo *Epidemic* foi o que melhor se adaptou ao encaminhamento de mensagens táticas, no cenário marítimo;

- Demonstrar que as funções discriminantes no protocolo *Epidemic* auxiliaram tanto na seleção de conexões seguras, diminuindo a quantidade de compartilhamento de informação com nós não autorizados, como também na melhoria de desempenho na

entrega de mensagens aos destinatários finais, ou seja, superiores aos resultados do protocolo *Epidemic* com função de Bloqueio Total.

4.1 TRABALHOS FUTUROS

Como sugestão para trabalhos futuros, no intuito de prover maior segurança, serão gravados os históricos de conexões seguras, obtidas da função discriminante. A partir desses históricos, o navio poderá consultar se uma dada conexão é previsível, ou não, de ocorrer, pois esses históricos conteriam as geolocalizações (latitudes e longitudes) das conexões seguras indicando os pontos em que haveria a probabilidade de ocorrência desses encontros. Essa estratégia seria válida para proteção contra tentativas de conexão com navios aliados em localizações improváveis, ou seja, útil para se proteger de ataques do tipo *tailgating*, por exemplo.

O comportamento do protocolo *Epidemic* com módulo de segurança e histórico de conexões pode ser visualizado no diagrama da Figura 4.1. De acordo com o diagrama, sendo uma conexão previsível (quando há um histórico à respeito dela), logo após, ela passaria pela classificação da função discriminante, caso contrário, seria totalmente bloqueada, por não haver um histórico sobre a dada conexão. Esse comportamento contribuiria para o bloqueio de meios marítimos que estivessem descrevendo uma movimentação fora do padrão conhecido.

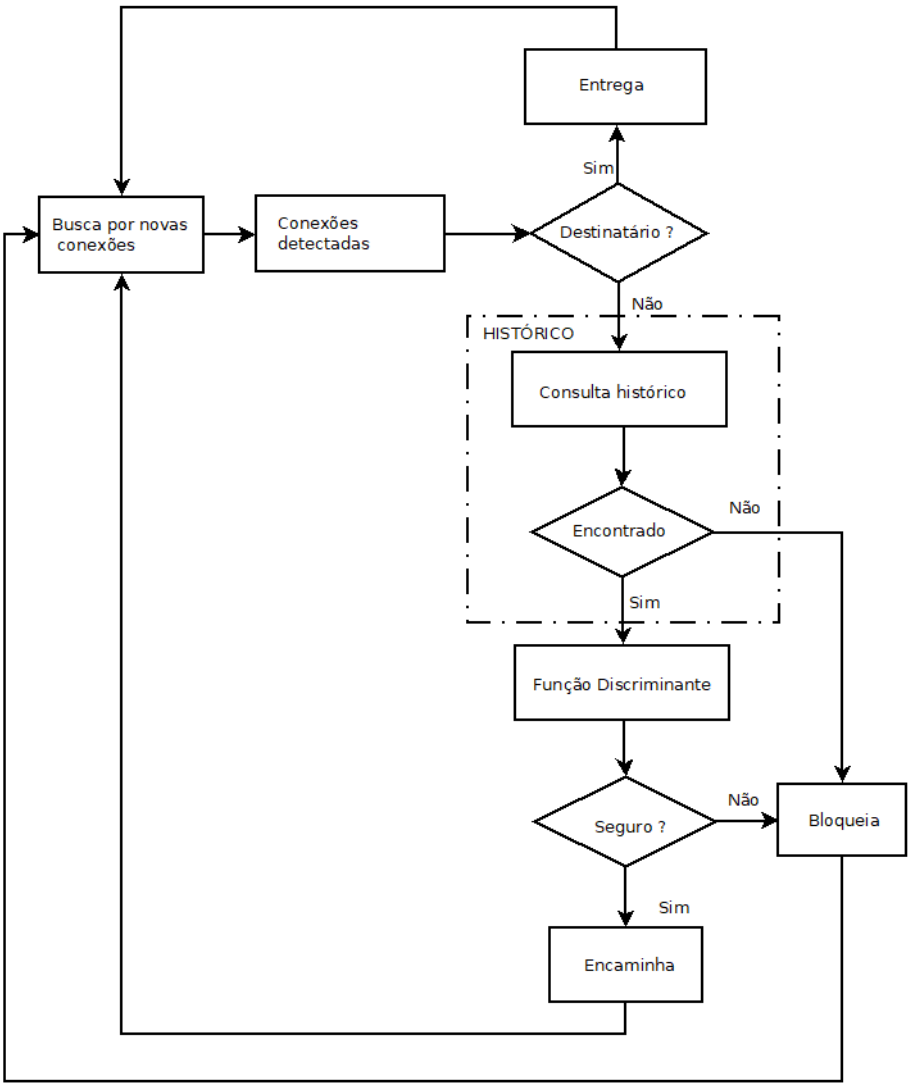


FIG. 4.1: Descrição básica do protocolo *Epidemic* com função discriminante e histórico de conexões.

5 REFERÊNCIAS BIBLIOGRÁFICAS

brasil.gov.br (2017). Essencial para o comércio exterior, transporte marítimo avança no brasil. `http://www.brasil.gov.br/noticias/infraestrutura/2017/11/essencial-para-o-comercio-exterior-transporte-maritimo-avanca-no-brasil`. [Online; accessed 4-December-2018].

Burgess, J., Bissias, G. D., Corner, M. D., and Levine, B. N. (2007). Surviving attacks on disruption-tolerant networks without authentication. In *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '07, pages 61–70, New York, NY, USA. ACM.

Carina T. de Oliveira, Marcelo D. D. Moreira, M. G. R. L. H. M. K. C. e. O. C. M. B. D. (2007). Redes tolerantes a atrasos e desconexões.

Chen, K. and Shen, H. (2016). Distributed privacy-protecting dtn routing: Concealing the information indispensable in routing. In *2016 IEEE 24th International Conference on Network Protocols (ICNP)*, pages 1–2.

Chrysostomou, L. L. C. D. C. (2013). Applying delay tolerant networking routing algorithms in maritime communications in world of wireless mobile and multimedia networks (wowmom).

Ding, Y., Zhou, X., mi Cheng, Z., and lu Zeng, W. (2013). Efficient authentication and key agreement protocol with anonymity for delay tolerant networks. *Wireless Personal Communications*, 70:1473–1485.

Dutt, I. (2015). Issues in delay tolerant networks: A comparative study.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets.

Fall, K. and Farrell, S. (2008). Dtn: an architectural retrospective. *IEEE Journal on Selected Areas in Communications*, 26(5):828–836.

Farrell, S. and Cahill, V. (2006). Security considerations in space and delay tolerant networks. In *2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06)*, pages 8 pp.–38.

Foundation, O. (2018). Openstreetmap. `https://www.openstreetmap.org`. [Online; accessed 8-June-2018].

Guo, Z., Peng, Z., Wang, B., Cui, J., and Wu, J. (2011). Adaptive routing in underwater delay tolerant sensor networks. In *2011 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, pages 1044–1051.

Huang, K. and Tso, R. (2012). A commutative encryption scheme based on elgamal encryption. In *2012 International Conference on Information Security and Intelligent Control*, pages 156–159.

K. YoungBum, K. JongHun. W. YuPeng, C. K. w. J. L. Y. (2009). Application scenarios of nautical ad-hoc network for maritime communications.

Kate, A., Zaverucha, G. M., and Hengartner, U. (2007). Anonymity and security in delay tolerant networks. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, pages 504–513.

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The ONE Simulator for DTN Protocol Evaluation. In *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, New York, NY, USA. ICST.

Kolios, P. and Lambrinos, L. (2012). Optimising file delivery in a maritime environment through inter-vessel connectivity predictions.

Li, F. and Wu, J. (2007). Mobility reduces uncertainty in manets. In *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, pages 1946–1954.

Li, F., Wu, J., and Srinivasan, A. (2009). Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In *IEEE INFOCOM 2009*, pages 2428–2436.

Li, Q. and Cao, G. (2012). Mitigating routing misbehavior in disruption tolerant networks. *IEEE Transactions on Information Forensics and Security*, 7(2):664–675.

Luming Wan, Feiyang Liu, Y. C. and Zhang, H. (2015). Routing protocols for delay tolerant networks: Survey and performance evaluation.

Mohsin, R. and Woods, J. (2014). Performance evaluation of manet routing protocols in a maritime environment. In *2014 6th Computer Science and Electronic Engineering Conference (CEEC)*, pages 1–5.

Mohsin, R. J., Woods, J., and Shawkat, M. Q. (2015). Density and mobility impact on manet routing protocols in a maritime environment. In *2015 Science and Information Conference (SAI)*, pages 1046–1051.

OpenJUMP (2018). Openjump. `http://www.openjump.org/`. [Online; accessed 18-November-2018].

Ott, J., Kutscher, D., and Dwertmann, C. (2006). Integrating dtn and manet routing. In *Proceedings of the 2006 SIGCOMM Workshop on Challenged Networks*, CHANTS '06, pages 221–228, New York, NY, USA. ACM.

Puri, P. and Singh, M. P. (2013). A survey paper on routing in delay-tolerant networks. In *2013 International Conference on Information Systems and Computer Networks*, pages 215–220.

R.S. Mangrulkar, M. A. (2010). Routing protocol for delay tolerant network: a survey and comparison.

S, A. P. and Viswanathan, A. (2012). A survey on detection and mitigation of misbehavior in disruption tolerant networks. *IRACST - International Journal of Computer Networks and Wireless Communications*, 2(6).

SAMPAIO, G. C. (2017). Avaliação de algoritmos dtn para ambiente operacional tático - uma abordagem energética.

Silva, A. T. C. C. (2007). Redes tolerantes a atrasos, protocolos de disseminação e aplicações.

V Friderikos, K. Papadaki. M. Dohler, A. G. H. A. (2005). Linked waters.

Zhou, M., Hoang, V. D., Harada, H., Pathmasuntharam, J. S., Wang, H., Kong, P., Ang, C., Ge, Y., and Wen, S. (2013). Triton: high-speed maritime wireless mesh network. *IEEE Wireless Communications*, 20(5):134–142.

6 APÊNDICES

APÊNDICE 1: FERRAMENTAS DE SIMULAÇÃO

Este capítulo é voltado para a descrição das principais ferramentas que foram adotadas no presente trabalho, para simulação em diferentes cenários (mapas) para medição de desempenho de Redes Tolerantes a Atrasos aplicadas em navios da Marinha do Brasil em missão no mar. Serão apresentadas as características fundamentais que fizeram com que esses programas fossem selecionados para tal finalidade.

6.2 THE ONE

The *Opportunistic Network Environment* (ONE) (KERÄNEN ET AL., 2009), atualmente na versão 1.6.0, é um simulador desenvolvido na linguagem Java, de código aberto e direcionado às pesquisas em Redes Tolerantes a Atrasos (DTN) e Redes Oportunísticas Móveis (OMN). Esse simulador possui uma interface simples que permite a criação de novos cenários de forma rápida, bastando para isso a compreensão dos parâmetros que constam no arquivo de configuração. O *The ONE* também dispõe de uma grande variedade de tipos de relatórios de acordo com a finalidade das simulações. Como por exemplo, se o foco das simulações estiver sobre o controle da capacidade de *buffer* nos nós da rede então um relatório importante a ser configurado seria o do tipo *BufferOccupancyReport*. É importante salientar que, como o código é aberto, tanto o funcionamento das simulações quanto os modelos dos relatórios podem ser facilmente customizados. O *The ONE* funciona tanto em plataformas *Linux* quanto no *Windows* e integrável com a IDE *Eclipse*. O Eclipse se torna uma ferramenta bastante útil para a visualização e edição das classes java do simulador.

6.2.1 MODOS DE SIMULAÇÃO

O *The ONE* possui dois modos de simulação, o modo gráfico e um modo em *batch*. O modo gráfico permite que o usuário visualize toda a movimentação do cenário em uma tela gerada pelo simulador. Essa visualização serve para a homologação do cenário adotado, pois permite que o usuário possa executar os testes necessários antes de dar início a uma sequência de simulações no modo *batch*.

O modo gráfico possui a limitação de somente realizar uma simulação por vez, podendo ser chamado de duas formas distintas por linha de comando no *Windows*:

```
one.bat; ou
one.bat <arquivo_customizado>.
```

A primeira forma, somente *one.bat*, inicializa o *The ONE* com o cenário padrão de simulação contido no arquivo de texto na pasta raíz do simulador com o nome de *default_settings.txt*. A segunda maneira, *one.bat <arquivo_customizado>*, carrega um arquivo de configuração criado pelo próprio usuário com as características de simulação por ele escolhidas.

O modo *batch* permite que um cenário seja executado, de forma sequencial, em uma quantidade de vezes especificada pelo usuário através de linha de comando no formato abaixo especificado, no *Windows*:

```
one.bat -b N <arquivo_customizado>
```

Em que o *-b* representa o modo *batch* e *N* é a quantidade de vezes que o simulador irá executar uma simulação do cenário *<arquivo_customizado>*

6.2.2 O ARQUIVO DE CONFIGURAÇÃO

O arquivo de configuração é um componente de grande importância do *The ONE*. Entender o que cada parâmetro de entrada significa e suas respectivas unidades de medida é de extrema importância para o entendimento do comportamento e dos resultados das simulações, ou seja, um resultado não esperado em uma simulação pode ocorrer pela falta de entendimento em algum parâmetro que possa ter sido omitido ou configurado com um valor incoerente com a realidade. Esses parâmetros irão ditar o comportamento durante as simulações. Pode-se ver, listado logo abaixo, alguns exemplos de parâmetros em um trecho de arquivo de configuração customizado, o nome do cenário *Scenario.name*, o tempo de duração da simulação *Scenario.endTime* (em segundos), o número de grupos presentes no cenário *Scenario.nrofHostGroups*, a periodicidade que as mensagens são criadas *Events1.interval* e quais são os hosts autorizados a serem origem e destino nas mensagens *Events1.hosts*.

```
Scenario.simulateConnections = true
Scenario.updateInterval = 1.0
Scenario.name = Cenario_Navios
Scenario.endTime = 43200
Scenario.nrofHostGroups = 1
MapBasedMovement.nrofMapFiles = 1
MapBasedMovement.mapFile1 = data/rotas/Cenario2/Cenario2_rota1.wkt
```

```
Events.nrof = 1
Events1.class = MessageEventGenerator
Events1.interval = 1800,3600
Events1.size = 11,500
Events1.hosts = 0,9
Events1.time = 0,43200
Report.nrofReports = 3
Report.report1 = MessageStatsReport
Report.report2 = DeliveredMessagesReport
Report.report3 = BufferOccupancyReport
Report.reportDir = reports/MB
MovementModel.worldSize = 1000000, 800000
Group.router = EpidemicRouter
Group.movementModel = MapRouteMovement
Group.routeType = 1
Group.routeFile = data/rotas/Cenario2/Cenario2.osm.wkt
Group.bufferSize = 1G
Group.speed = 0, 5.15
MovementModel.rngSeed = 1
radio.type = InterferenceLimitedInterface
radio.transmitRange = 13000
radio.transmitSpeed = 600
Group1.groupID = TATIC_A
Group1.nrofHosts = 6
Group1.nrofInterfaces = 1
Group1.interface1 = radio
Group1.movementModel = ShortestPathMapBasedMovement
Group1.okMaps = 1
```

Dando continuidade aos parâmetros do arquivo de configuração customizado, o *Report.nrofReports* indica ao simulador a quantidade de relatórios que serão utilizados e *Report.reportDir* o diretório onde os relatórios serão armazenados. Os tipos de relatórios deverão ser especificados, como por exemplo o *MessageStatsReport* que retorna dados estatísticos da simulação de forma sintetizada à respeito de vários aspectos como a probabilidade de entrega, uso do *buffer* do sistema e a quantidade total de mensagens geradas, abortadas, excluídas, encaminhadas, entregues etc.

O parâmetro *MovementModel.worldSize* determina as dimensões (em metros) do ce-

nário que deverão ser compatíveis com as dimensões dos mapas configurados para a simulação do tipo *MapBasedMovement*. O *Group.router* determina qual protocolo de roteamento será adotado na simulação (neste caso foi utilizado o protocolo Epidêmico), o *Group.bufferSize* refere-se ao tamanho do *buffer* padrão, o *Group.routeFile* indica a rota padrão de movimentação dos grupos e o *Group.speed* a velocidade média com qual se movimentam os nós pertencentes aos grupos, em metros por segundo. É também possível configurar um valor mínimo e máximo para as velocidades dos nós dos grupos, isso permitirá uma maior dinâmica entre os nós.

O parâmetro *MovementModel.rngSeed* é muito importante para dar aleatoriedade na movimentação dos nós, cada diferente valor atribuído a esse parâmetro irá gerar um novo padrão na distribuição dos nós, pois esses números servirão de semente para o posicionamento aleatório dos nós no mapa.

É importante mencionar a possibilidade de ser configurada uma lista de valores em cada parâmetro do arquivo de configuração ao invés de um valor único. Por exemplo, em *MovementModel.rngSeed = 1* poderia ser criada uma lista da seguinte forma *MovementModel.rngSeed = [1;2;3;4;5]* em que, no modo *batch*, cada valor é tomado por vez na sequência de simulações, ou seja, na primeira simulação o valor 1 é utilizado como semente em seguida o valor 2 e assim sucessivamente.

Para finalizar, pode-se ver um exemplo de configuração de uma interface de rede denominada *"radio"*. A classe java responsável pelo comportamento da interface será do tipo *InterferenceLimitedInterface*, essa configuração se dá através do parâmetro *radio.type*. Da mesma maneira se configura o raio de cobertura da transmissão (em metros) através do parâmetro *radio.transmitRange* e a velocidade da transmissão dos pacotes de dados (em bytes por segundo) através do parâmetro *radio.transmitSpeed*.

Existem características gerais de configuração de um grupo que podem ser configuradas através do objeto *Group*, no entanto, características diferenciadas de um grupo podem ser configuradas individualmente através do chamado dos parâmetros de um grupo específico como mostrado no *Group1.groupID* (que seta um identificador para os nós pertencentes àquele dado grupo), o *Group1.nrofHosts* (que configura a quantidade de nós que serão atribuídos àquele grupo), o *Group1.nrofInterfaces* (que configura a quantidade de interfaces de rede que cada nó do grupo terá), o *Group1.interface1* (configura na primeira interface do primeiro grupo algum tipo de interface configurada, nesse caso, o tipo *"radio"* foi atribuída), o *Group1.movementModel* (que configura o tipo de movimentação daquele grupo, ou seja, como que os nós do grupo irão se movimentar durante a simulação) e por fim o *Group1.okMaps* que informa ao simulador por quais dos mapas informados, os nós

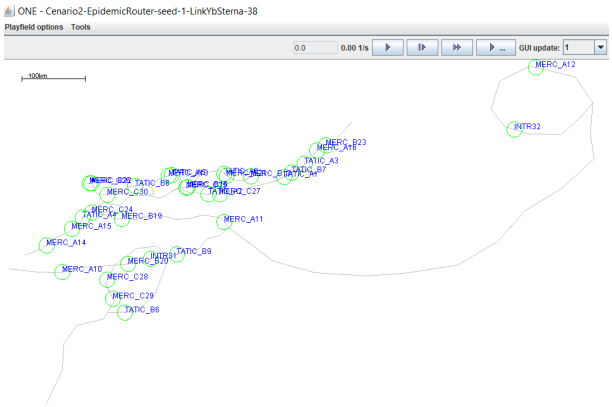


FIG. 6.1: Cenário customizado no modo gráfico do *The ONE*.

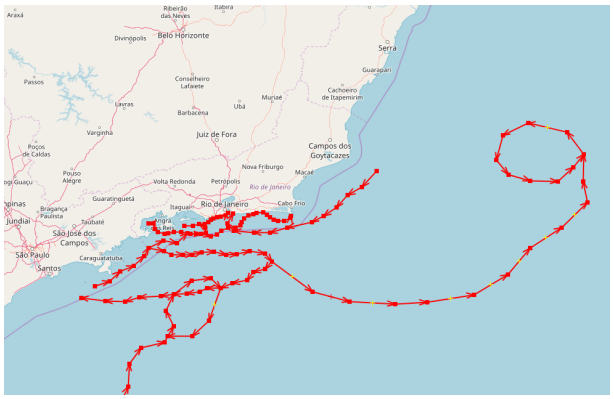


FIG. 6.2: Representação do cenário customizado no mapa.

pertencentes àquele dado grupo, estão autorizados a se movimentar.

Pode-se ver nas Figuras 6.1 e 6.2 respectivamente, um exemplo de cenário customizado no *The ONE* e a sua representação no mapa usando a ferramenta *Java OpenStreetMap Editor* que será abordada na próxima seção.

6.3 OPENSTREETMAP

OpenStreetMap (FOUNDATION, 2018) é uma ferramenta *freeware* amplamente utilizada com o intuito de disponibilizar informação de localização através da edição de mapas por usuários da comunidade. São disponibilizadas as versões *online* e a *offline*.

A versão *online* (como pode ser visto na Figura 6.3) pode ser encontrada no site https://www.openstreetmap.org. No entanto, visando obter maior disponibilidade ao poder salvar os dados *offline*, sem precisar depender de uma conexão estável com a internet, foi escolhida para esse trabalho a ferramenta JOSM *Java OpenStreetMap Editor* que roda no computador do usuário, como mostra a Figura 6.4.

O *Java Open Streetmap Editor* foi importante, nesse trabalho, para a criação e visualização dos cenários de movimentação no mapa. Esses cenários contém as rotas que serão percorridas pelos nós durante as simulações no *The ONE*, mas é importante salientar que os dados gerados pelo editor na extensão padrão .osm representam coordenadas geográficas, ou seja latitudes e longitudes. Por isso antes de passar os dados para o *The ONE* eles precisarão ser convertidos para coordenadas cartesianas X e Y, em metros, na extensão .wkt (*Well Known Text*).

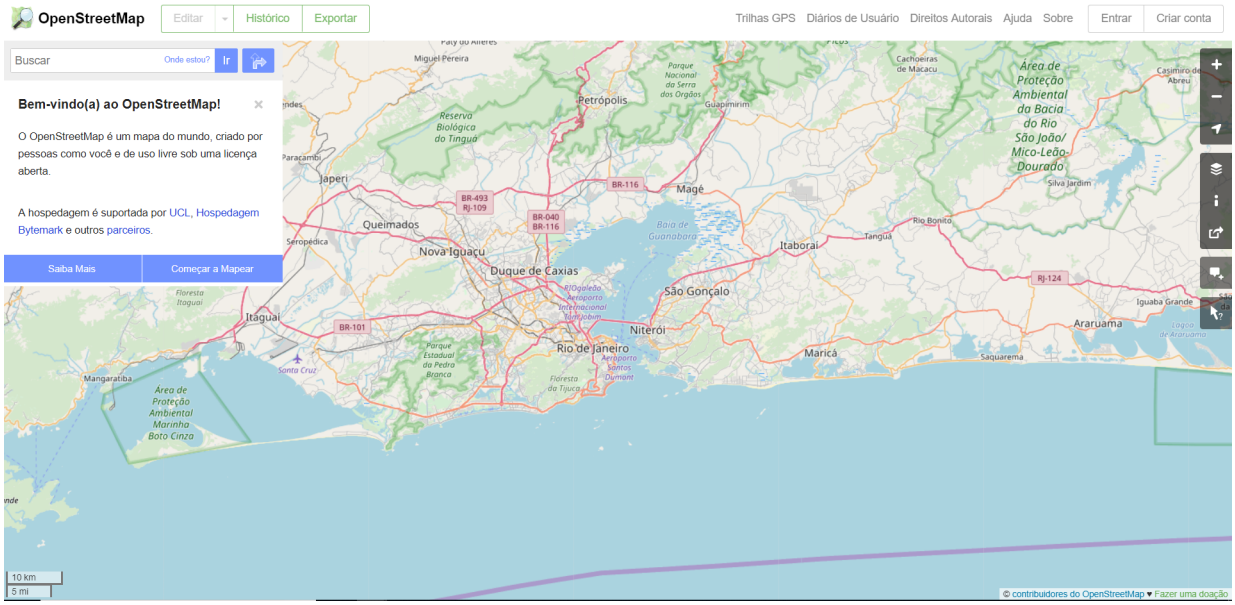


FIG. 6.3: *OpenStreetMap* versão *online*.

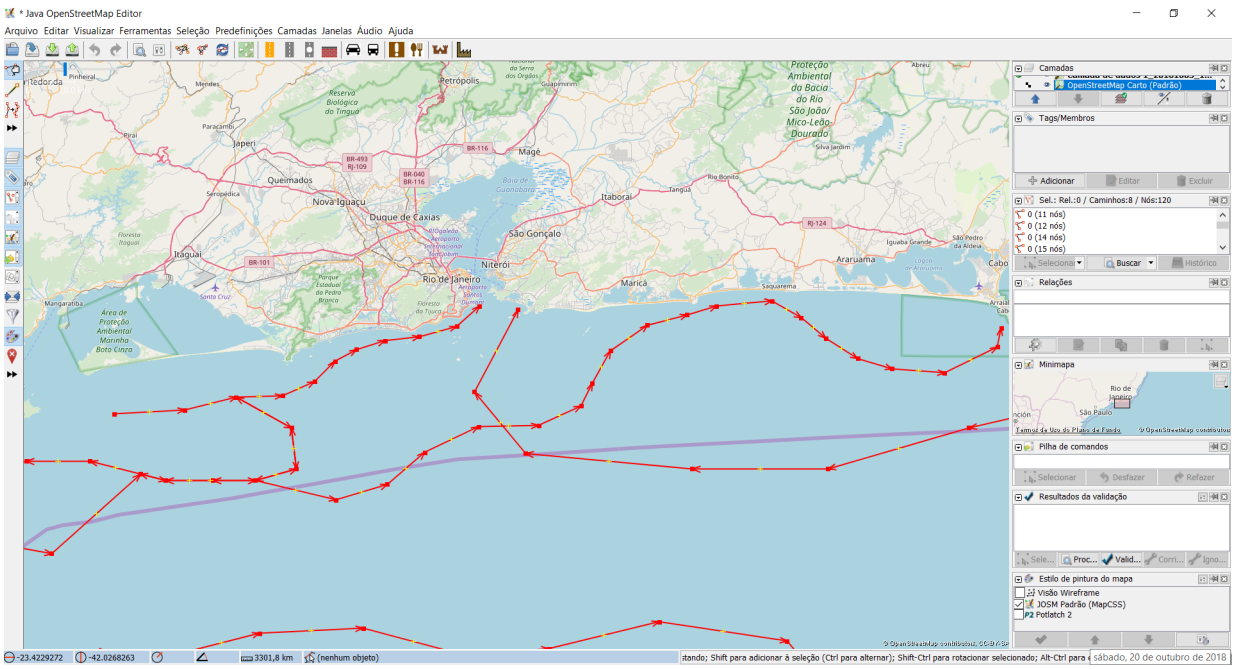


FIG. 6.4: *Java OpenStreetMap Editor* versão *offline* do *OpenStreetMap*.

6.3.1 CONVERTENDO .OSM PARA .WKT

Como mencionado na seção anterior, o formato dos dados gerados pelo *Java Open Street-map Editor* é incompatível com o *The ONE*, por isso é preciso convertê-los para o formato que o simulador reconheça. O *Well Known Text* é o formato reconhecido pelo *The ONE* que é constituído por um arquivo, de extensão .wkt, que contém vetores que formam desenhos geométricos representados através de uma linguagem de marcação, como por

exemplo *POINT(100 200)* que representa um ponto cartesiano localizado na coordenada X na posição 100 e na coordenada Y na posição 200. Dois pontos ligados representam uma reta ou uma linha, como por exemplo *LINESTRING(100 200, 400 500)*, que representa uma linha que parte do ponto p1(100 200) até o ponto p2(400 500). Existem outras linguagens de marcação para o formato .wkt que formam várias outras figuras geométricas mais complexas, no entanto para a simulação das rotas, nesse trabalho, foram utilizadas somente a representação de pontos e de linhas. Pode-se ver respectivamente um cenário no formato .osm e sua representação parcial em .wkt nas Figuras 6.5 6.6.

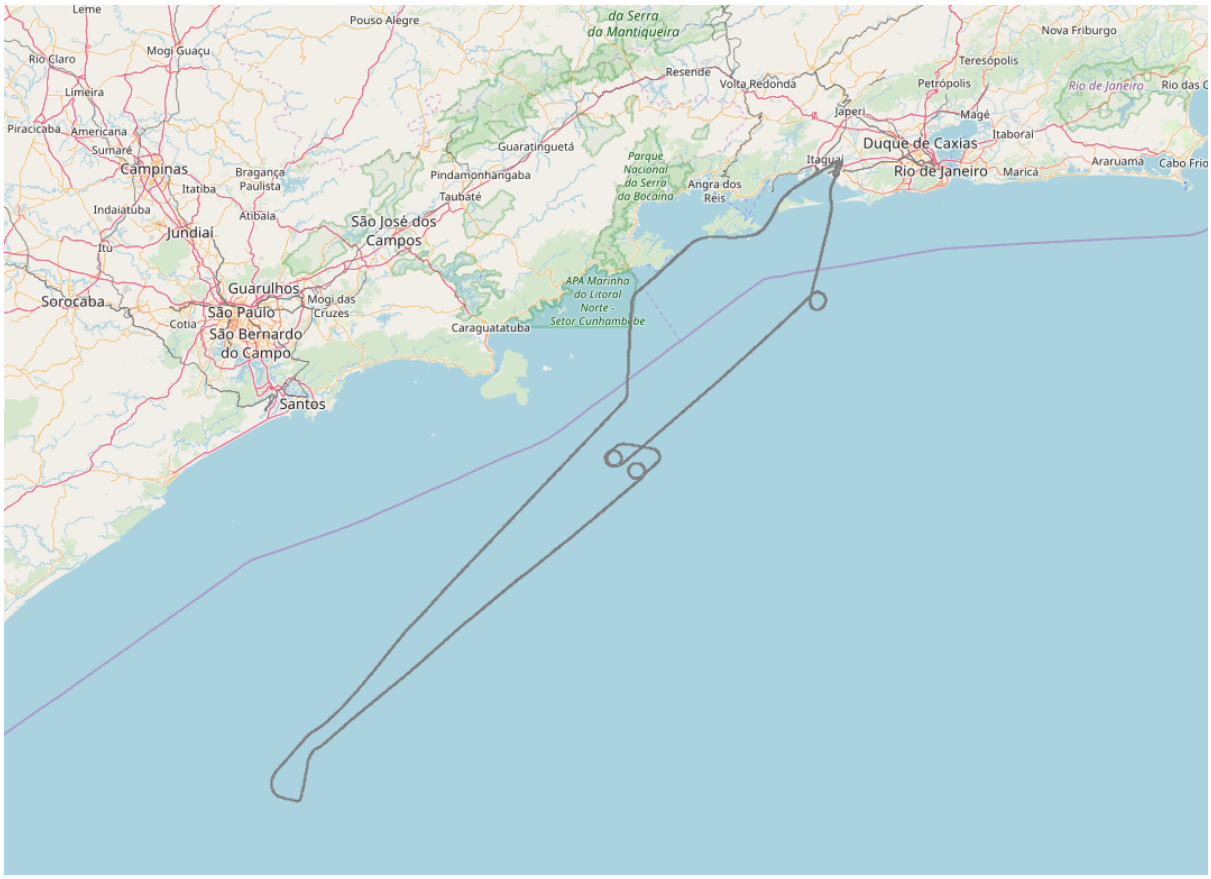


FIG. 6.5: Exemplo de cenário no formato .osm.

Essa conversão é realizada através de um programa de código aberto, escrito em Java, recomendado pela comunidade do *The ONE* que além de mudar o formato de .osm para .wkt também converte os dados de coordenadas geométricas para coordenadas cartesianas (em metros). O nome desse programa é *osm2wkt.jar* e ele é chamado por linha de comando pois não possui uma interface gráfica.

```
LINESTRING (283972.188 310771.022, 283970.316 310769.14,
283961.85 310771.246, 283961.026 310770.808, 283961.192
310768.692, 284024.652 310680.625, 284023.101 310684.847,
284022.834 310687.075, 284021.243 310689.629, 284021.371
310690.961, 284021.497 310692.192, 284021.705 310692.303,
284024.166 310692.63, 284024.58 310692.741, 284025.602
310692.741, 284026.012 310692.63, 284026.411 310692.415,
284027.536 310691.968, 284029.059 310691.297, 284029.553
310690.635, 284030.053 310689.852, 284030.346 310688.967,
284031.666 310688.408, 284031.554 310687.96, 284031.647
310687.41, 284029.484 310686.963, 284029.448 310685.071,
284030.987 310685.183, 284030.865 310684.185, 284029.532
310684.074, 284028.702 310683.291, 284030.232 310682.955,
284031.998 310684.185, 284033.022 310684.297, 284035.68
310684.185, 284037.107 310683.85, 284038.827 310682.629,
284039.226 310681.958, 284041.428 310684.959, 284040.72
310685.183, 284040.104 310685.295, 284038.765 310684.847,
```

FIG. 6.6: Representação do cenário no formato .wkt.

6.4 OPENJUMP

O software *Open Jump* (OPENJUMP, 2018) é utilizado para visualizar os dados convertidos no formato .wkt. É importante para conferir se as estruturas em .osm foram corretamente convertidas antes de passar para o simulador. O *Open Jump* permite inclusive a edição desses dados e a criação de novas estruturas em formato .wkt como pode-se ver na Figura 6.7. Dessa maneira o *Open Jump* serve para realizar ajustes nos dados das rotas e salvá-los novamente em formato .wkt para depois serem utilizados na simulação.

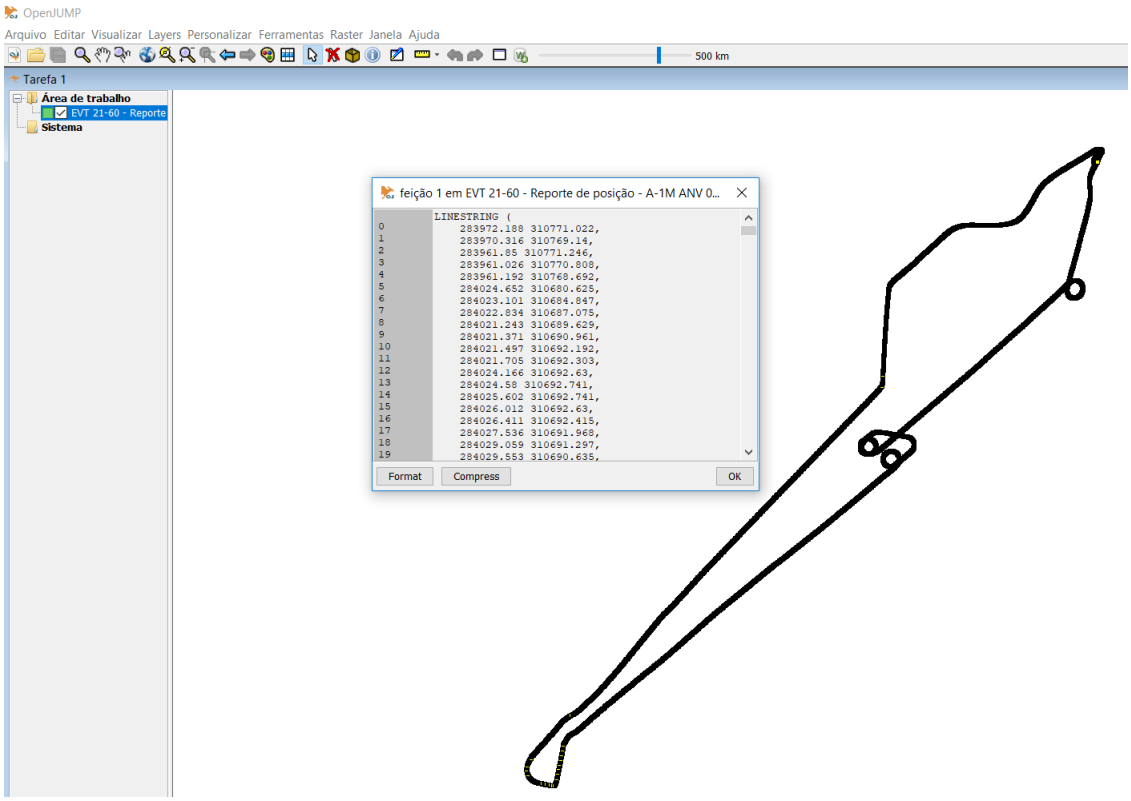


FIG. 6.7: Cenário em .wkt aberto no *Open Jump*.

APÊNDICE 5: APRESENTAÇÃO DOS CENÁRIOS DE SIMULAÇÃO

Serão apresentados os cenários de simulação utilizados. Eles foram criados à partir de rotas reais de navios e helicópteros da Marinha do Brasil e interligados levando-se em consideração a proximidade entre eles, variando de cenários mais simples até os mais complexos que atingem áreas de cobertura maiores.

As simulações, cada uma delas representando um período de tempo de 12 horas, foram realizadas, em um primeiro momento, com 36 navios. Dos 36 nós, 15 deles são identificados como sendo da Marinha do Brasil e 21 são identificados como mercantes, pesqueiros etc (inimigos). Nó inimigo é o termo dado a todo o nó que não pertence à Marinha do Brasil, não necessariamente sendo um nó malicioso com intenção de roubar informação.

Ao longo das simulações foram inseridos 4 helicópteros aliados, ao mesmo tempo que foram removidos 4 navios aliados mantendo-se o quantitativo constante de nós aliados (15 aliados). Esses helicópteros possuíam velocidades variando entre 100 e 300 km/h.

Os helicópteros percorreriam rotas específicas, estrategicamente, que pudessem cobrir uma área onde existissem o maior número de rotas de navios possível. A finalidade se baseia em testar a utilidade dos helicópteros como encaminhadores de mensagens, tendo em vista eles serem mais velozes do que os navios, estarem em contato com os navios de guerra no mar e percorrerem longos percursos, sobrevoando áreas em que passam os navios de guerra.

O objetivo é simular helicópteros que sobrevoam as regiões percorridas pelos navios de forma a aumentar a cobertura de dados. Por possuírem velocidades superiores, os helicópteros poderiam levar mais rapidamente as informações através dos extremos das rotas. Nas simulações, os helicópteros não criam mensagens, somente encaminham.

Mais adiante foram acrescentados navios aliados e inimigos no intuito de melhorar a densidade de nós na rede e com isso melhorar o desempenho da rede DTN. Nesse segundo momento foram incluídos cerca de 61 navios, sendo estes 26 aliados (22 navios e 4 helicópteros) e 35 navios inimigos (mercantes, pesqueiros etc).

Em termos de quantidade de mensagens, partiu-se do princípio que em 12 horas não seriam produzidas uma quantidade muito significativa de mensagens táticas durante as missões no mar, por isso, inicialmente, será simulada em média a criação de 16 mensagens, ou seja, pouco mais do que uma mensagem criada por hora. Isso serviria para testar

missões que produziriam poucas mensagens. Contudo, para melhor testar o desempenho de redes DTN no mar, foram realizadas algumas simulações com a criação de mensagens entre 300 e 600.

O tamanho das mensagens trocadas durante a simulação variaram entre 11 bytes até 1000 bytes, levando-se em consideração que as mensagens do sistema tático são mensagens curtas. Essas mensagens foram transmitidas através de *links* cujas taxas variaram entre 300bps, 600bps, 1200bps e 4800bps (levando-se em consideração as velocidades de transmissão dos *links* táticos da Marinha do Brasil).

Para cada configuração de cenário foram realizadas 200 simulações, nelas foram usadas sementes distintas variando de 0 até 200. Essas diferentes sementes garantem que o sistema crie simulações distintas, por exemplo, os pontos iniciais de cada nó no início de cada simulação, as suas velocidades desenvolvidas em cada uma delas, etc.

Em cada cenário, foram simulados 3 protocolos DTN: o *Direct Delivery*, o *Epidemic* (Epidêmico) e o *Spray and Wait*, os mesmos já definidos conceitualmente no Capítulo 2.

6.6 CENÁRIO 1

O Cenário 1 (ver Figura 6.8) é formado por 8 rotas, sendo que duas delas são exclusivas para tráfego de nós de maior velocidade, que representam helicópteros (rota 3 e rota 5).

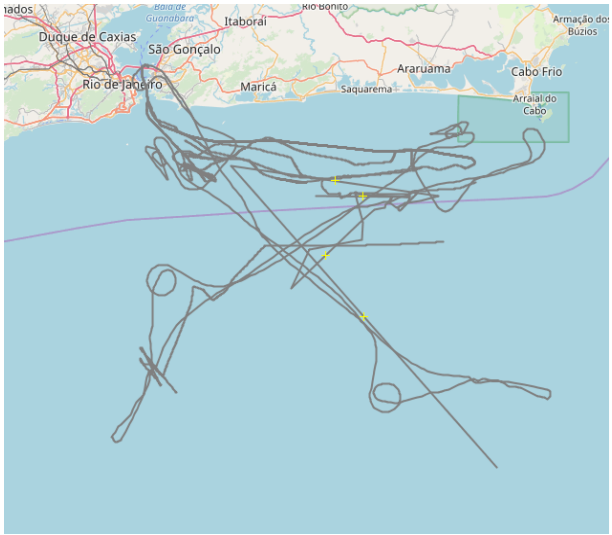


FIG. 6.8: Cenário 1 completo.

O restante das rotas são utilizadas por nós que representam navios percorrendo velocidades que variam em torno de 0 a 18 *knots*, ou seja entre 0 e 9.26 m/s. As rotas de 1 a 8 podem ser visualizadas, na ordem da esquerda para direita e de cima para baixo, nas Tabelas 6.1 e 6.2 .A área total de cobertura do cenário 1 simulado fica em torno dos

$150km^2$. Os navios são distribuídos no cenário, através das rotas, de acordo com o valor da semente que foi atribuída naquele instante e percorrerão as rotas que foram atribuídas ao seu grupo no arquivo de configuração, por exemplo: *Group1.okMaps = 1*.

6.7 CENÁRIO 2

O Cenário 2 (ver Figura 6.9) apesar de conter apenas duas rotas, possui uma área de cobertura superior a do Cenário 1. A área de cobertura do cenário 2 simulado fica em torno dos $400km^2$. Nele não existem rotas exclusivas de helicóptero.

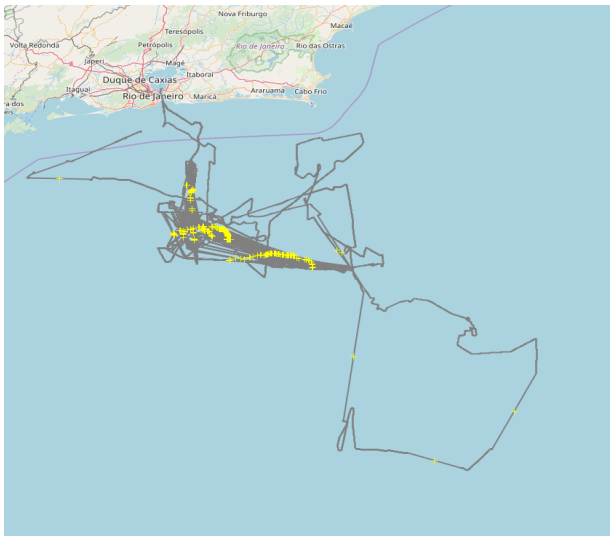


FIG. 6.9: Cenário 2 completo.

O que diferencia esse cenário do anterior, além da área de cobertura maior, é a complexidade da rota 2, que possui vários caminhos próximos uns dos outros e que pode vir a contribuir para futuros encontros entre os nós. Pode-se ver as rotas 1 e 2 do Cenário 2, na ordem da esquerda para a direita, na Tabela 6.3

6.8 CENÁRIO 3

O Cenário 3 (ver Figura 6.10) é formado por 3 rotas, sendo que uma delas é exclusiva para tráfego de nós de maior velocidade que representam helicópteros, como mostra a primeira imagem da Tabela 6.4.

As demais rotas são utilizadas por nós que representam navios percorrendo velocidades que variam em torno de 0 a 18 *knots*, ou seja entre 0 e 9.26 m/s. As rotas de navios do Cenário 3 podem ser vistos na segunda e terceira imagem (de cima para baixo) da Tabela 6.4. A área de cobertura do cenário 3 simulado fica em torno dos $600km^2$.

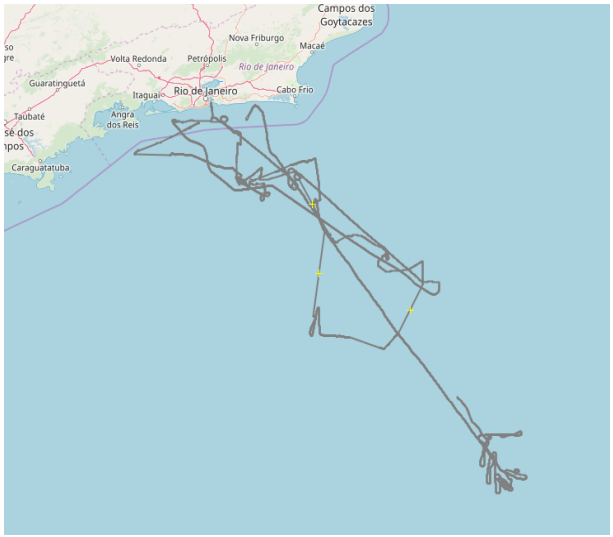
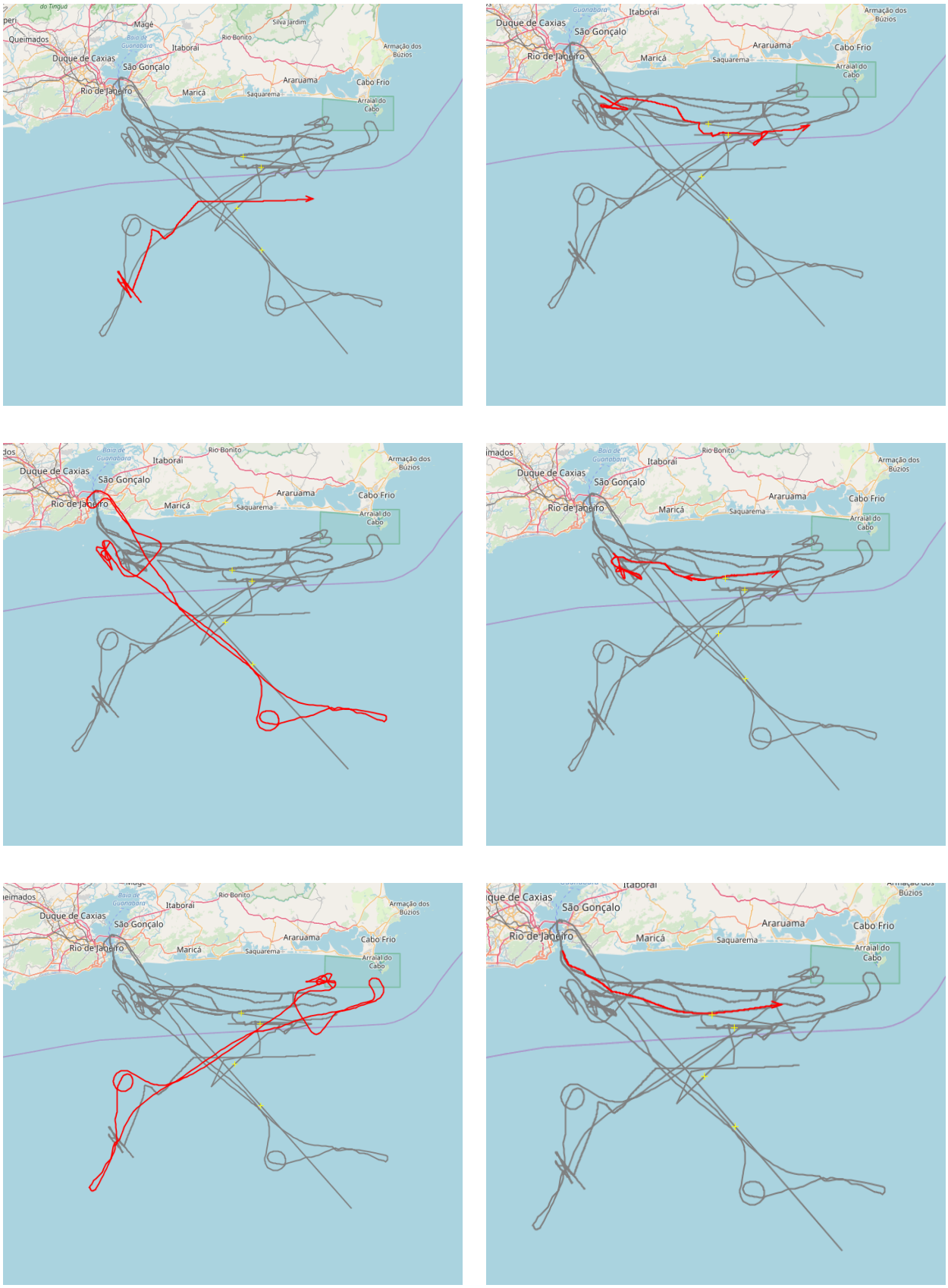
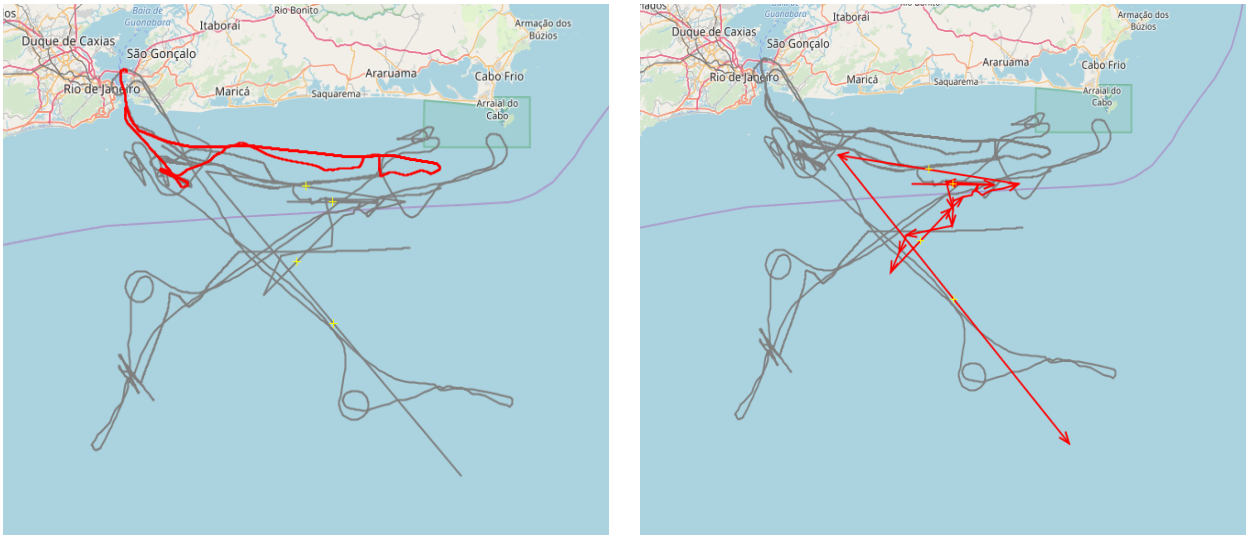


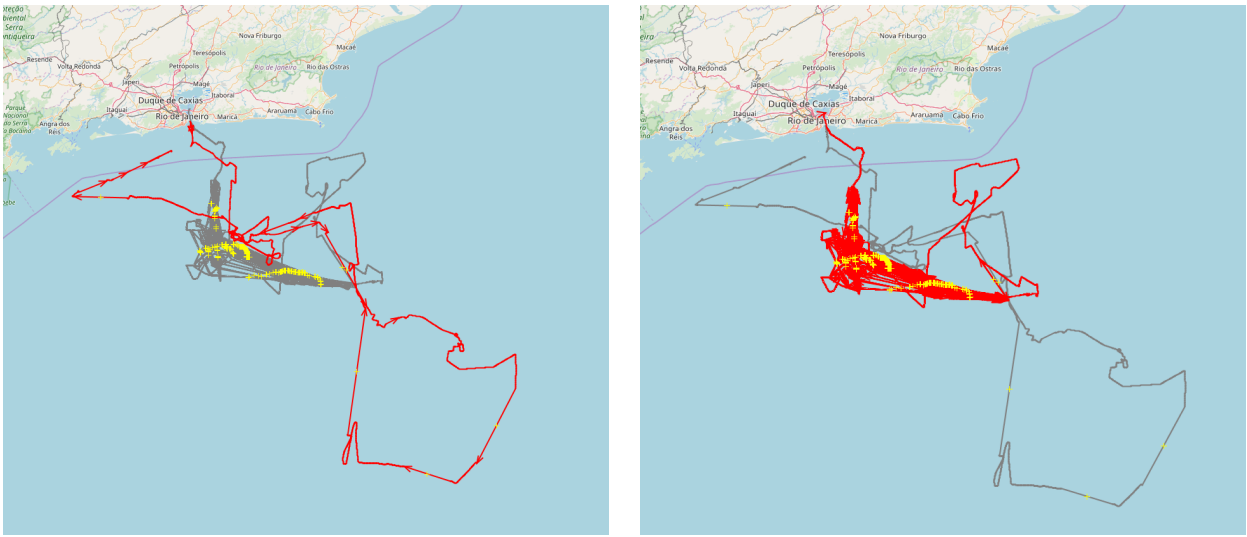
FIG. 6.10: Cenário 3 completo.



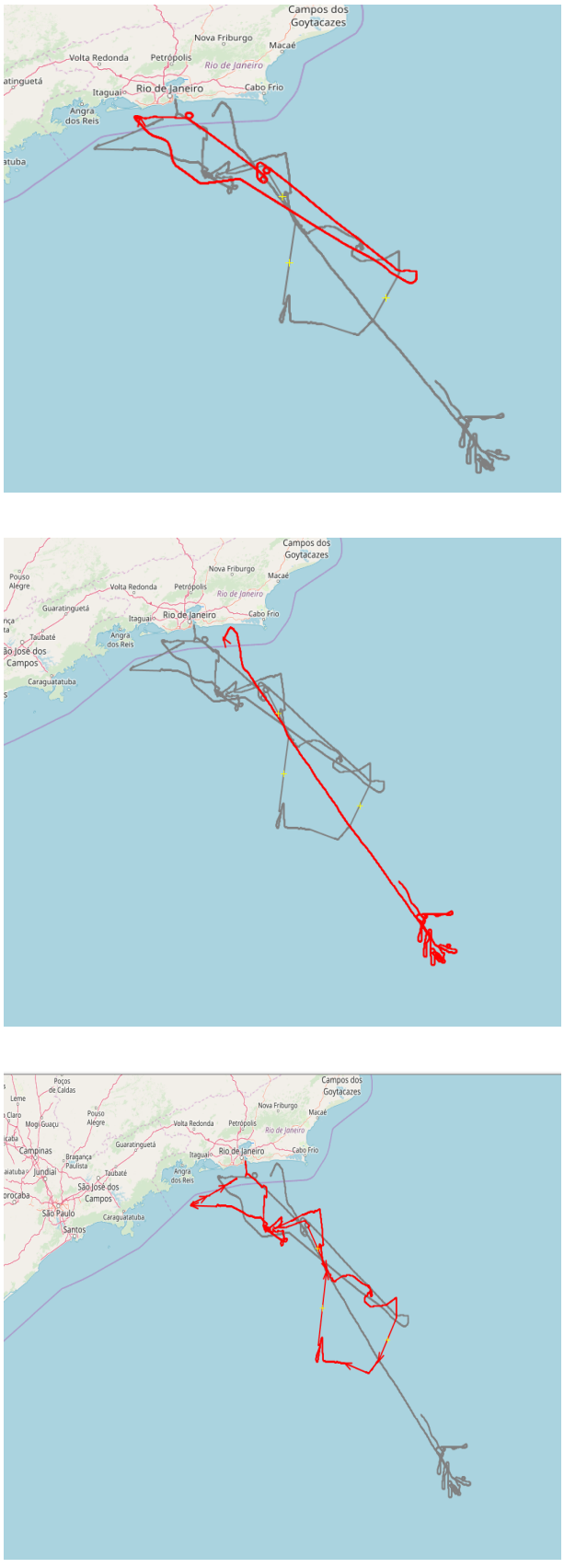
TAB. 6.1: Cenário 1, rotas de 1 a 6, na ordem, da esquerda para direita e de cima para baixo.



TAB. 6.2: Cenário 1, rotas de 7 e 8, na ordem, da esquerda para direita.



TAB. 6.3: Cenário 2, rotas 1 e 2, na ordem, da esquerda para direita.



TAB. 6.4: Cenário 3, rotas 1 até 3, na ordem, de cima para baixo.