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.

Orientadora: Prof[a]. RONALDO MOREIRA SALLES - Ph.D.
Co-Orientador: Prof. 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 RONALDO MOREIRA SALLES e PAULO HENRIQUE COELHO MARANHÃO - Rio de Janeiro: Instituto Militar de Engenharia, 2019.

55p.: il.

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

1. Curso de Sistemas e Computação - teses e dissertações. 1. DTN. 2. Redes Tolerantes a Atrasos. 3. cenário marítimo. 4. baixa densidade. 5. intermitente. 6. segurança. 7. encontros. I. SALLES, RONALDO MOREIRA. II. MARANHÃO, 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 Sistemas e Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Mestre em Ciências em Sistemas e Computação.

Orientadora: Prof[a]. RONALDO MOREIRA SALLES - Ph.D.

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

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

Prof[a]. RONALDO MOREIRA SALLES - Ph.D. do IME - Presidente

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

Prof. JULIO CESAR DUARTE - Ph.D. do IME

Prof. RAQUEL COELHO GOMES PINTO - D.Sc. do IME

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

Rio de Janeiro
2019

Ao Instituto Militar de Engenharia, alicerce da minha formação e aperfeiçoamento.

AGRADECIMENTOS

Meus familiares, cônjuge e mestres.

“Sem publicação, a ciência é morta. ”

GERARD PIEL

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

LA	Los Angeles
NY	New York
PRODASEN	Centro de Informática e Processamento de Dados do Senado Federal
UN	United Nations

LISTA DE ABREVIATURAS E SÍMBOLOS

ABREVIATURAS

Ja	-	jacobiano
JS	-	fluxo secundário (difusivo)
M	-	número de Mach

SÍMBOLOS

Φ	-	termo de dissipação viscosa
Γ	-	coeficiente de difusão efetivo
α	-	fator de sub-relaxação
ϕ	-	variável dependente da equação diferencial geral

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 que uma infraestrutura fim-a-fim não esteja disponível. Por isso DTN é recomendável 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 que envolve os navios da Marinha do Brasil para o encaminhamento de mensagens táticas, levando-se em consideração aspectos de segurança nos perímetros onde os encontros efetivos acontecem.

Palavras-chave: DTN, Redes Tolerantes a Atrasos, cenário marítimo, baixa densidade, intermitente, segurança, encontros.

ABSTRACT

Delay-Tolerant Networks (DTN) are an evolution of the Mobile Adhoc Network (MANET) and DTNs act in scenarios where nodes are sparsely distributed. low-density, whose connection is intermittent and that an end-to-end infrastructure is not available. This is why DTN is 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 Delay-Tolerant Networks in the maritime scenario that involves the ships of the Brazilian Navy for the transmission of tactical messages, taking into consideration the safety aspects in the perimeters where the effective encounters take place.
Keywords: DTN, Delay-Tolerant Networks, maritime scenario, low density, intermittent, security, encounters .

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: sobre a geolocalização dos navios, dados meteorológicos de uma determinada região, da situação de uma determinada embarcação, um 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, como também as redes marítimas que são baseadas em rádios convencionais *High Frequency (HF), Very High Frequency (VHF) e Ultra High Frequency (UHF)* para se comunicarem nas proximidades da costa e sistemas de satélites para cobertura de áreas superiores para viagens à longas distâncias ainda são muito mais lentas e de custo elevado quando comparadas com as redes que são utilizadas em terra firme (ZHOU ET AL., 2013).

Dessa maneira é uma estratégia de vital importância a escolha de uma arquitetura ideal que venha a atender as necessidades de comunicação em termos de capacidade de participação de nós na rede, velocidade, 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 envolvam o controle de acesso à informação como por exemplo soluções baseadas em criptografia. Sabe-se que sempre é possível burlar a segurança e que não existe no mercado solução que garanta 100 % de efetividade 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 recomendar a adição da arquitetura protocolos para Redes Tolerantes a Falhas ou Atrasos (DTN) sobre a pilha de protocolos TCP/IP.

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 adotado 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, para o caso de 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).

E se um nó malicioso conseguir roubar uma chave privada de um outro nó ou até mesmo inferir sobre ela, esse poderá tentar se passar por aquele e assim manter uma comunicação com os demais nós da rede como se fosse um nó legítimo. E 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 OBJETIVOS DA DISSERTAÇÃO

Demonstrar que o uso de um modelo híbrido de redes que inclui o protocolo DTN no trâmite de mensagens táticas entre navios na Marinha do Brasil pode contribuir para o aumento da efetividade na entrega de pacotes para os nós afastados da rede. Também demonstrar que a informação prévia sobre as rotas dos navios em missão no mar poderia indicar padrões de movimentação que sirvam 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, comparando a quantidade de mensagens entregues nos dois modelos (tradicional e DTN); 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.

- propor uma melhoria, em um dos protocolos DTN, na questão de segurança, utilizando informação de histórico de geolocalização dos encontros efetivos dos nós:
  - avaliar o desempenho do novo protocolo DTN seguro em relação ao número de mensagens entregues com sucesso ao destinatário, como também em relação a segurança, com o objetivo de se reduzir a entrega de mensagens em conexões classificadas como inseguras.

1.3 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. Dedicou-se na avaliação de 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, a performance dos protocolos MANET possuem 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 decresce quando se aumenta a mobilidade dos nós da rede e quando os cenários se tornam mais esparsos.

Em (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 maritimas 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 melhor se beneficiar 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 Epidêmico, 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 à 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 das redes 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 é que os nós venham a colaborar para que as mensagens cheguem nos seus destinatários. Contudo, ataques às redes DTN são realizados através de nós mal intencionados que trabalham no intuito de restringir esses encaminhamentos. Esse trabalho defende a utilização de métodos para detecção desses nós que apresentam mal funcionamento a fim de que eles sejam contornados, ou seja, excluídos da rede permanecendo apenas aqueles nós que verdadeiramente contribuirão para o encaminhamento das mensagens.

Esses nós mal intencionados, no momento do ataque, se apresentam como bons encaminhadores, mas no momento em que recebem as mensagens elas são excluídas, 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*).

(CHEN AND SHEN, 2016) propõe um mecanismo novo para manter o sigilo da

informação de roteamento dos nós. Essa informação de roteamento, chamadas no artigo de *routing utility*, são utilizadas 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 por eles.

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 tickets de encontros para trazer maior confiabilidade na escolha dos nós encaminhadores na rede DTN. Os tickets 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 tickets, 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 de *tailgating* juntos seria o uso de protocolos de roteamento em que utilize propagação aleatória, ou seja, sem se utilizar probabilidade.

Percebe-se 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 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).

2 REDES DTN

2.1 DEFINIÇÃO

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 que uma infraestrutura fim-a-fim não esteja disponível (R.S. MANGRULKAR, 2010). Por isso DTN é recomendável 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 ideia de ordem.

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, poder 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 e nesse aspecto as Redes Tolerantes a Atrasos (DTN) vieram para contribuir (CARINA T. DE OLIVEIRA, 2007), (SILVA, 2007), como ilustrado na Figura 2.1.

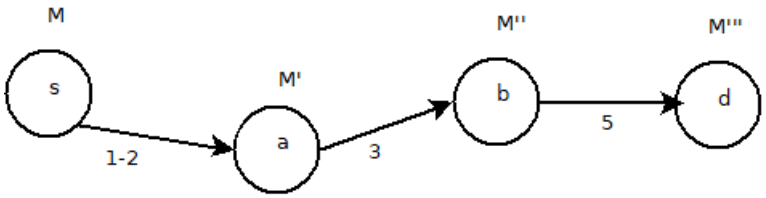

FIG. 2.1: Redes DTN se beneficiam da mobilidade dos nós replicando dados até que eles atinjam o seu destino.

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.

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.

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 ao ambiente de comunicação marítima, por exemplo, se torna uma alternativa de baixo custo em relação aos elevados preços para a locação de cobertura satelital (?).

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, como mostra a Figura 2.2, em que os pontos estão simbolizando nós dotados de mobilidade, em que alguns se beneficiam com a proximidade do sinal da rede provida pela antena, no entanto, outros nós mais afastados receberão dados de forma colaborativa através dos nós intermediários.

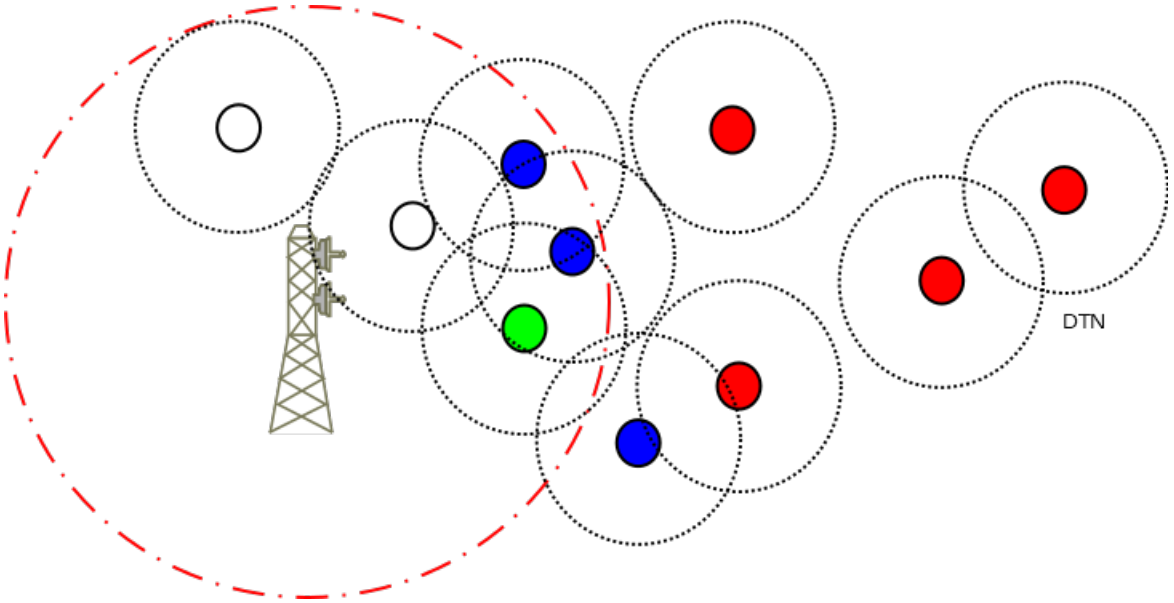

FIG. 2.2: Os nós mais distantemente localizados receberão os dados através de outros nós da rede DTN.

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.

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.

2.3 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. À seguir serão descritos o comportamento de alguns deles:

2.3.1 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, ou seja não existem retransmissões através de nós intermediários.

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 tipo de 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.

2.3.2 TWO-HOP RELAY

Nesse protocolo ocorrem retransmissões entre o nó de origem e os nós que que mantiveram contato, em um primeiro momento, com o nós de origem. Em seguida esses nós irão trabalhar de forma a cooperar para que a mensagem chegue ao nó de destino. Este tipo de protocolo aumenta a probabilidade de entrega, mas também aumentam os consumos de largura de banda e de armazenamento.

2.3.3 ROTEAMENTO EPIDÊMICO

O roteamento epidêmico é considerado o primeiro algoritmo de roteamento DTN. Ele assume que cada nó tenha armazenamento e largura de banda ilimitada e por isso 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 seria 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.

2.3.4 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.

2.3.5 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, é que faz desse protocolo não ser 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 uma determinada mensagem já passou para ajudar ao nó atual evitar caminhos já percorridos.

2.4 ESTRATÉGIA DE ENCAMINHAMENTO

Nessa estratégia se utiliza o conhecimento prévio tanto da topologia da rede quanto 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 baseando-se em informações disponibilizadas previamente e que servem de entrada para protocolos que seguem essa estratégia.

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.

2.4.1 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.

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

2.5 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 **?** Dutt (2015). São eles:

a) Controle de Buffer;

b) Controle de Congestionamento;

c) Segurança;

d) Desconecções; e

e) Capacidade Energética SAMPAIO (2017).

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 DESCONECÇÕES

A grande quantidade de desconecções interferem 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.

2.5.5 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 pois sem energia suficiente os nós não terão condições de se manterem ativos e replicando os dados de forma colaborativa na rede.

2.6 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, continuar 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 há 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 entre muitos minutos e até mesmo horas tornando esse tempo significativo para a transmissão efetiva dos dados (MOHSIN ET AL., 2015).

Logo, com o objetivo de corrigir essa limitação da cobertura da rede marítima para o aumento da capacidade de transmissões com sucesso entre os nós e com isso melhorando o desempenho das taxas de entrega dos pacotes, nesse tipo de cenário, tornando-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.

A proposta deste trabalho é formar uma arquitetura híbrida de rede envolvendo as estações base em terra e também entre as embarcações fornecendo uma rede marítima do tipo *mesh* que inclua redes DTN no intuito de estender a capacidade da rede existente e não para substituir como arquitetura única e absoluta na rede marítima.

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.

2.6.1 NOVA ARQUITETURA DE REDES DA MARINHA DO BRASIL

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 à 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, 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, mas não transmitirão;
  - 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*:
    - No modo *Relay* qualquer Estação Dependente poderá retransmitir mensagens para as Estações Remotas encontradas; e
    - Para isso irá ser usado um canal de radiofrequência diferente do usado na rede principal;

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.

3 MÓDULO DE SEGURANÇA PARA O PROTOCOLO EPIDÊMICO

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 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. 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 Epidêmico, protocolo adotado neste trabalho.

Em redes com uma densidade elevada de nós o protocolo Epidêmico poderia causar uma sobrecarga da 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 Epidêmico se encaixaria como o mais recomendado pois tentará aproveitar todas as oportunidades para a transmissão de mensagens.

O ambiente marítimo possui essas características que envolvem baixa densidade de nós e uma grande quantidade de conexões e desconexões ao longo do tempo. E falando especificamente do cenário da comunicação na Marinha do Brasil que dispõe de poucos navios para percorrer longas distâncias, sofrendo constantemente com intermitências da rede, tendo muitas das vezes que alocar grandes recursos financeiros para requisitar cobertura de rede via enlace de satélites de países estrangeiros a fim de poder tramitar mensagens curtas contendo informação sigilosa de suas diversas operações táticas e que poderiam ao invés disso adotar uma solução de baixo custo que utilizaria os recursos já existentes na rede atual através da arquitetura DTN.

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 Epidêmico. 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 ele tenha mantido o contato.

Ou seja, o protocolo Epidêmico 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.

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 sendo o predileto 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.

Uma outra característica de um nó com mal 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. Esse padrão também pode ser analisado por histórico compartilhado e esses nós também podem ser excluídos da rede.

Ou seja, o 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 (LI AND CAO, 2012), (S AND VISWANATHAN, 2012), (KATE ET AL., 2007).

A incerteza faz aumentar os custos computacionais e diminui as aceitações de comu-

nicação 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, essas rotas se tornariam carimbos certificadores desses navios no mar, e qualquer encontro inesperado poderia ser tratado como uma tentativa de intrusão.

Dessa forma o intruso deverá, além de obter as chaves, descobrir 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.

É importante salientar que o objetivo deste trabalho não pretende substituir o modelo de padrão de chaves criptográficas, mas visando apresentar um modelo baseado em localização a fim de que possa ser usado conjuntamente com o tradicional. Da mesma maneira, a arquitetura DTN não viria para substituir as outras arquiteturas, mas trabalhar em conjunto com as demais em uma rede híbrida.

4 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. Também serão apresentados os cenários que serão utilizados para as simulações.

4.1 FERRAMENTAS DE SIMULAÇÃO

4.1.1 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 estiverem 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.

4.1.1.1 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*:

```
1    one.bat; ou
2    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*:

```
1 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>*

4.1.1.2 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.

Ao ser executado, o *The ONE* possui um arquivo de configuração padrão denominado *default_settings.txt* que contém um modelo de cenário que representa uma movimentação intensa de nós criando mensagens e encaminhando-as. Esse cenário padrão é muito importante para que os novos usuários possam compreender o simulador através dos vários parâmetros de entrada e desse ponto poder fazer os seus próprios cenários com uma quantidade de nós, grupos e rotas bem específicos como pode-se ver na Figura 4.1.

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

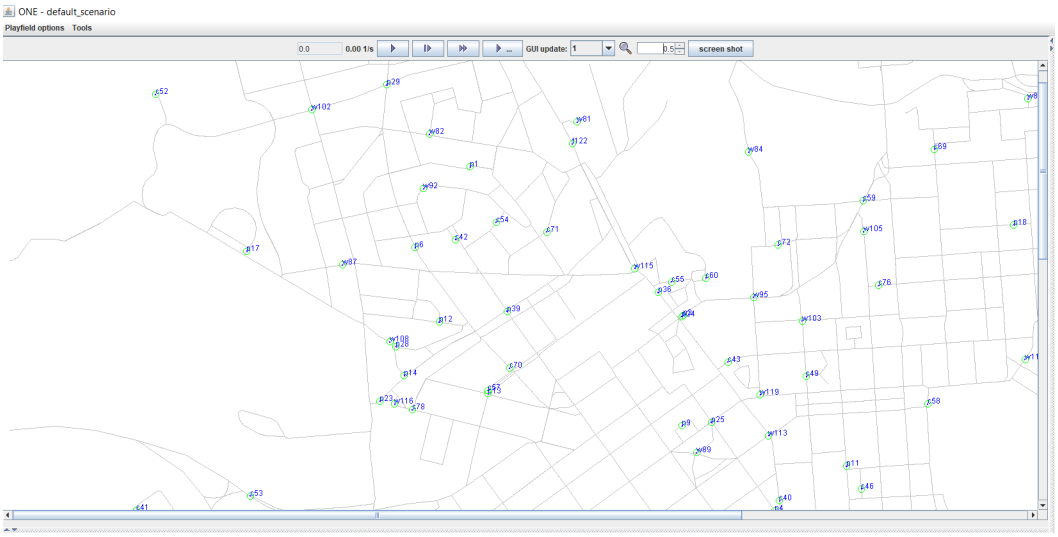

FIG. 4.1: Cenário padrão especificado no arquivo de configuração *default_ settings.txt*, no modo gráfico.

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*.

```
1  Scenario.simulateConnections = true
2  Scenario.updateInterval = 1.0
3  Scenario.name = Cenario_Navios
4  Scenario.endTime = 43200
5  Scenario.nrofHostGroups = 1
6  MapBasedMovement.nrofMapFiles = 1
7  MapBasedMovement.mapFile1 = data/rotas/Cenario2/Cenario2_rota1.wkt
8  Events.nrof = 1
9  Events1.class = MessageEventGenerator
10 Events1.interval = 1800,3600
11 Events1.size = 11,500
12 Events1.hosts = 0,9
13 Events1.time = 0,43200
14 Report.nrofReports = 3
15 Report.report1 = MessageStatsReport
16 Report.report2 = DeliveredMessagesReport
17 Report.report3 = BufferOccupancyReport
18 Report.reportDir = reports/MB
19 MovementModel.worldSize = 1000000, 800000
20 Group.router = EpidemicRouter
21 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 cenário 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).

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 *Move-*

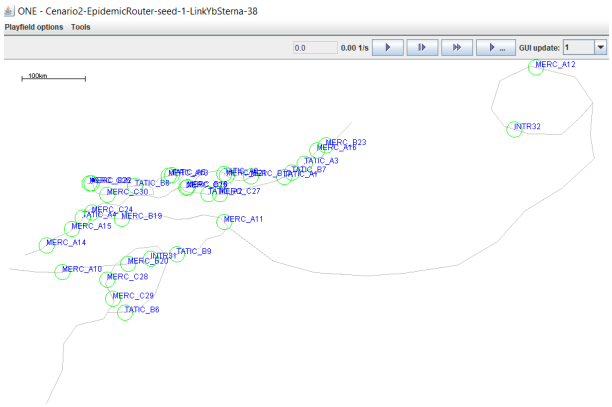

FIG. 4.2: Cenário customizado no modo gráfico do *The ONE*.

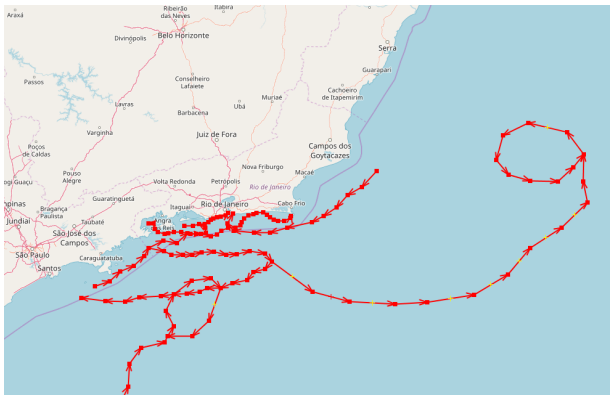

FIG. 4.3: Representação do cenário customizado no mapa.

mentModel.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 pertencentes àquele dado grupo, estão autorizados a se movimentar.

Logo abaixo, pode-se ver nas Figuras 4.2 e 4.3 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.

4.1.2 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 4.4) 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 como preferencial para esse trabalho a ferramenta JOSM *Java OpenStreetMap Editor* que roda no computador do usuário, como mostra a Figura 4.5.

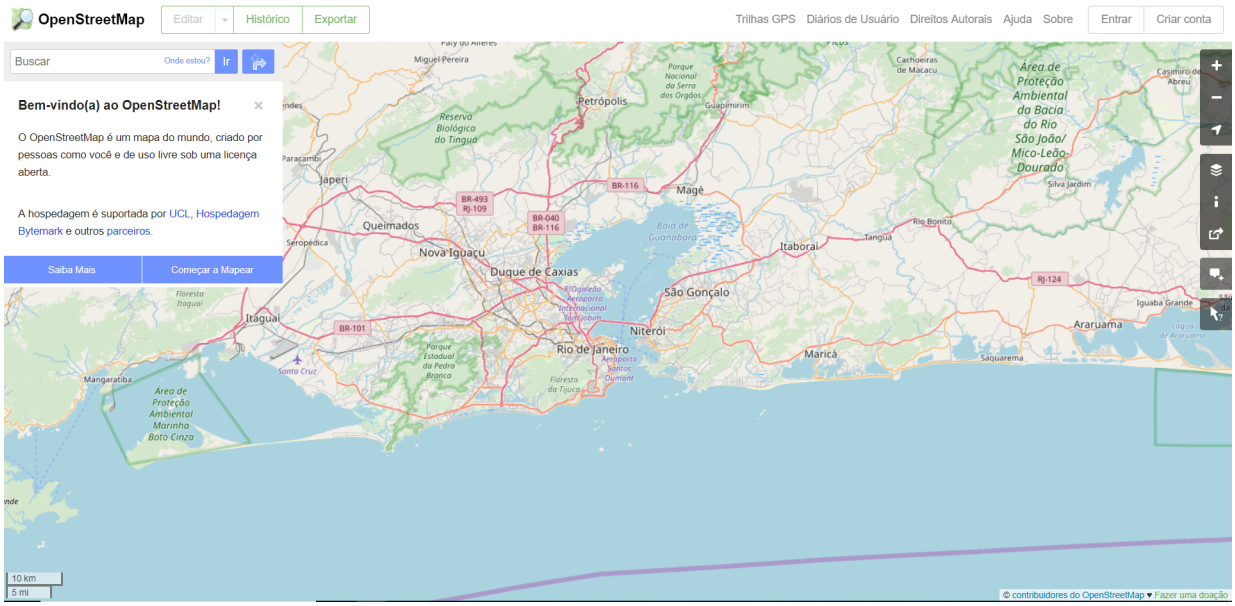

FIG. 4.4: *OpenStreetMap* versão *online*.

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*).

4.1.3 CONVERTENDO .OSM PARA .WKT

Como mencionado na seção anterior, o formato dos dados gerados pelo *Java Open Streetmap Editor* é incompatível com o *The ONE*, por isso é preciso convertê-los para o formato

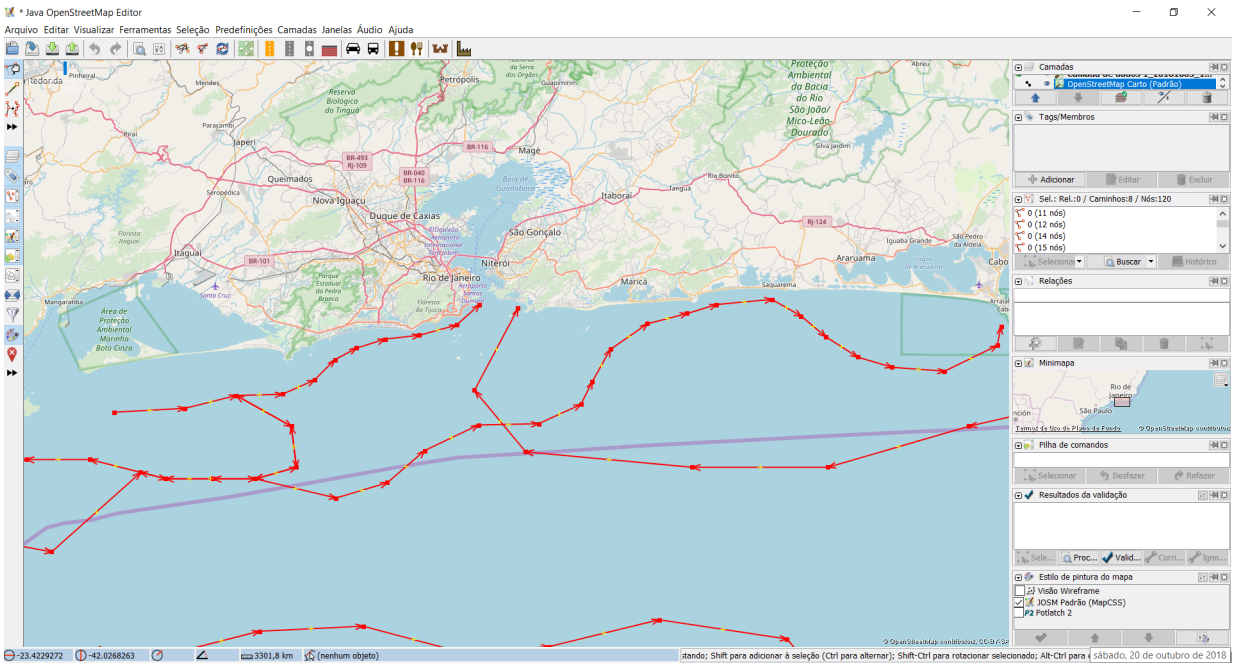

FIG. 4.5: *Java OpenStreetMap Editor* versão *offline* do *OpenStreetMap*.

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 várias 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 4.6 4.7.

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. A forma de chamar o programa *osm2wkt.jar* por linha de comando segue logo abaixo, esse comando irá gerar um arquivo .wkt com o mesmo nome:

```
1 java -jar osm2wkt.jar mapa.osm
```

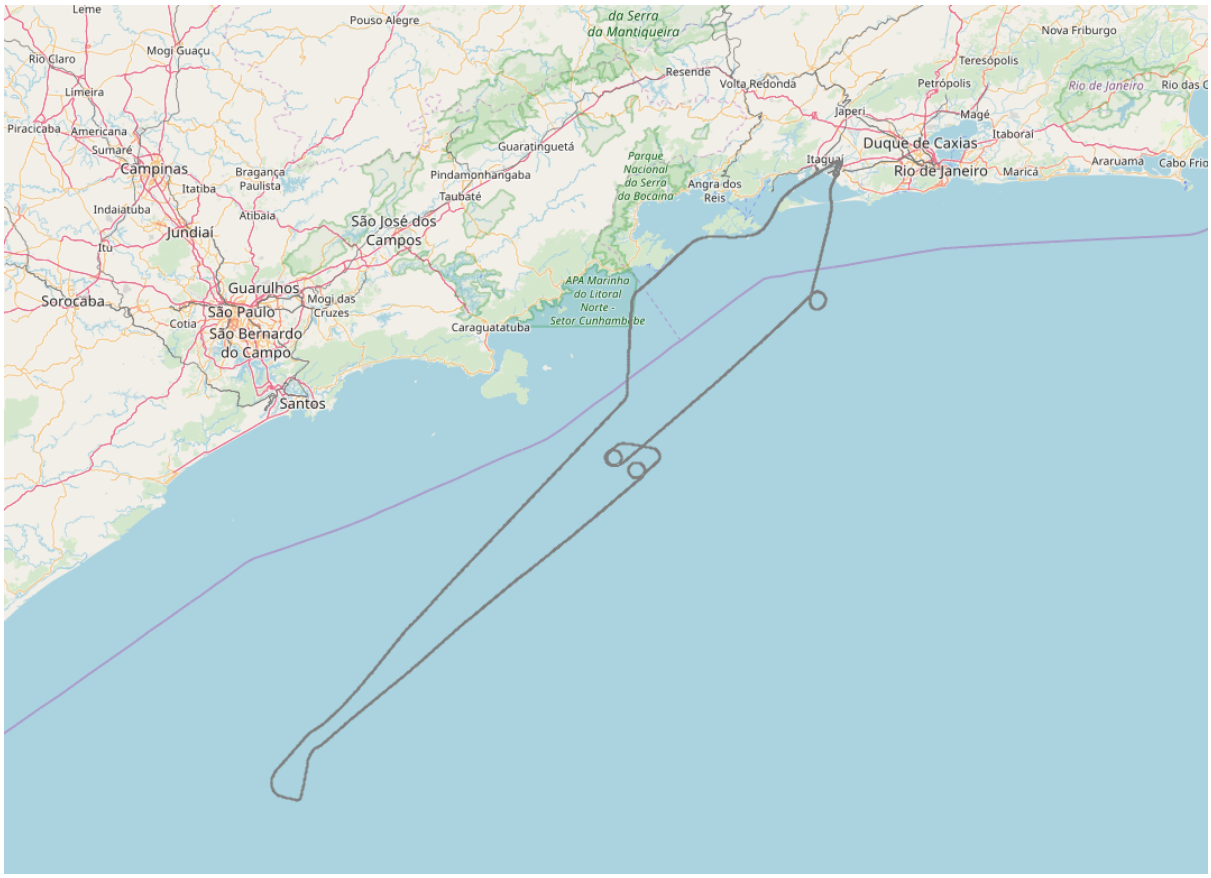

FIG. 4.6: Exemplo de cenário no formato .osm.

```
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. 4.7: Representação do cenário no formato .wkt.

4.1.4 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 4.8. 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.

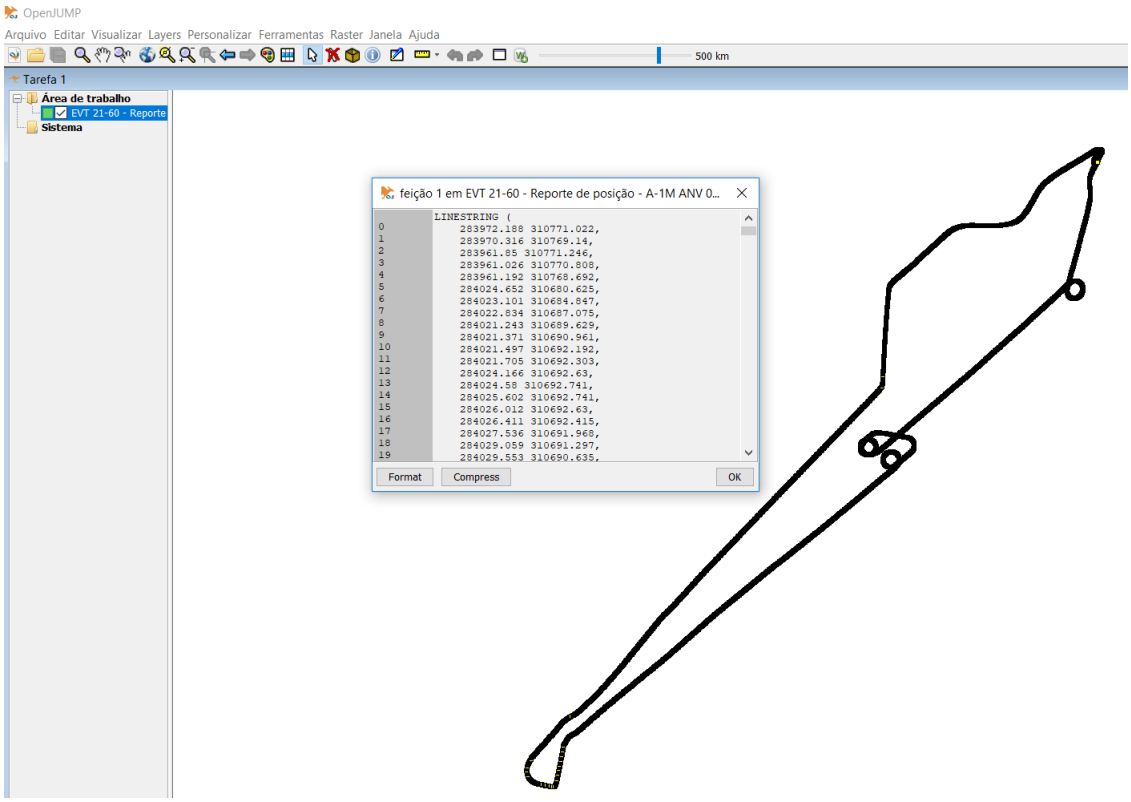

FIG. 4.8: Cenário em .wkt aberto no *Open Jump*.

4.2 CENÁRIOS DE SIMULAÇÃO

4.2.1 APRESENTAÇÃO DOS CENÁRIOS DE SIMULAÇÃO

5 RESULTADOS

5.1 RESULTADOS COM EPIDÊMICO PADRÃO

5.1.1 CENÁRIO 1

5.1.2 CENÁRIO 2

5.1.3 CENÁRIO 3

5.2 RESULTADOS COM EPIDÊMICO SEGURO

5.2.1 CENÁRIO 1

5.2.2 CENÁRIO 2

5.2.3 CENÁRIO 3

6 CONCLUSÃO

Chega-se à conclusão de que uma arquitetura híbrida de redes, no cenário marítimo, que inclua Redes Tolerantes a Atrasos (DTN), é uma solução de baixo custo e que pode vir a contribuir com a entrega de mensagens em regiões onde a conectividade da rede convencional não tenha alcance. Foi visto também que é possível implementar estratégias de segurança nesse cenário.

Para que o método de segurança venha a funcionar de forma eficiente, é preciso aumentar a quantidade de navios aliados nas regiões em que eles estão numericamente em desvantagem em relação à quantidade dos nós inimigos. 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 estão 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, e ainda são vistos como potenciais colaboradores em momentos de crise.

Ou seja, 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.

A estratégia disso seria que ao longo do tempo o histórico de encontros apontaria para mais regiões seguras, o que contribuiria para que o módulo de segurança pudesse decidir por realizar mais encaminhamentos ao invés de bloqueá-los.

REFERÊNCIAS BIBLIOGRÁFICAS

brasil.gov.br (2017). Essencial para o comércio exterior, transporte marítimo avança 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 desconexÃes.

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. [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.

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. [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 â“ International Journal of Computer Networks and Wireless Communications*, 2(6).

SAMPAIO, G. C. (2017). AvaliaÃ§Ã£o de algoritmos dtn para ambiente operacional tÃ¡tico - uma abordagem energÃ‰‰tica.

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.

7 APÊNDICES

APÊNDICE 1: APÊNDICE EXEMPLO

Curabitur tortor. Pellentesque nibh. Aenean quam. In scelerisque sem at dolor. Maecenas mattis. Sed convallis tristique sem. Proin ut ligula vel nunc egestas porttitor. Morbi lectus risus, iaculis vel, suscipit quis, luctus non, massa. Fusce ac turpis quis ligula lacinia aliquet. Mauris ipsum. Nulla metus metus, ullamcorper vel, tincidunt sed, euismod in, nibh. Quisque volutpat condimentum velit.

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nam nec ante. Sed lacinia, urna non tincidunt mattis, tortor neque adipiscing diam, a cursus ipsum ante quis turpis. Nulla facilisi. Ut fringilla. Suspendisse potenti. Nunc feugiat mi a tellus consequat imperdiet. Vestibulum sapien. Proin quam. Etiam ultrices. Suspendisse in justo eu magna luctus suscipit. Sed lectus. Integer euismod lacus luctus magna.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi. Nulla quis sem at nibh elementum imperdiet. Duis sagittis ipsum. Praesent mauris. Fusce nec tellus sed augue semper porta. Mauris massa. Vestibulum lacinia arcu eget nulla. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur sodales ligula in libero. Sed dignissim lacinia nunc.

APÊNDICE 2: APÊNDICE EXEMPLO 02

Curabitur tortor. Pellentesque nibh. Aenean quam. In scelerisque sem at dolor. Maecenas mattis. Sed convallis tristique sem. Proin ut ligula vel nunc egestas porttitor. Morbi lectus risus, iaculis vel, suscipit quis, luctus non, massa. Fusce ac turpis quis ligula lacinia aliquet. Mauris ipsum. Nulla metus metus, ullamcorper vel, tincidunt sed, euismod in, nibh. Quisque volutpat condimentum velit.

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Nam nec ante. Sed lacinia, urna non tincidunt mattis, tortor neque adipiscing diam, a cursus ipsum ante quis turpis. Nulla facilisi. Ut fringilla. Suspendisse potenti. Nunc feugiat mi a tellus consequat imperdiet. Vestibulum sapien. Proin quam. Etiam ultrices. Suspendisse in justo eu magna luctus suscipit. Sed lectus. Integer euismod lacus luctus magna.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi. Nulla quis sem at nibh elementum imperdiet. Duis sagittis ipsum. Praesent mauris. Fusce nec tellus sed augue semper porta. Mauris massa. Vestibulum lacinia arcu eget nulla. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur sodales ligula in libero. Sed dignissim lacinia nunc.

8 ANEXOS

ANEXO 1: ANEXO EXEMPLO

Id magna feugiat. Erat pellentesque sapien in rhoncus dolor augue vel eget. Erat nibh animi ultricies sit rhoncus. Eleifend aliquam luctus sem turpis habitasse. Lectus arcu ut mi nulla luctus facilisis cursus suspendisse class sociis metus vitae leo consequat lorem ullamcorper arcu. Nunc justo aliquam. Quidem volutpat urna. Nonummy nulla blandit donec vitae ultrices. Netus aliquam vivamus. Vehicula libero leo. Vestibulum consectetuer magna. Sapien aliquam arcu netus etiam lectus. Venenatis tristique morbi non nulla tortor commodo gravida ac neque lacinia urna. Elit mauris adipisci. Vitae sed curabitur. Tellus nunc lectus. Nonummy et integer.

Lorem dictumst enim. Dui vestibulum quisque. Dolor posuere risus. Nullam vitae est magnis est tortor metus dolor integer. Massa elit nec euismod et lacus quam ac malesuada est suspendisse ut est pellentesque vivamus lorem amet non vulputate maecenas et id ultrices lacus odio morbi vitae ac aenean in feugiat elit sodales congue proin dui leo bibendum scelerisque faucibus in suscipit. Nulla parturient in. Eget habitasse fringilla. Eget donec excepturi wisi lorem lacinia. Elementum lorem sem. Pede metus sit. Aenean facilisi pellentesque. Purus dictum ante. Neque amet sed.

Sed leo molestie. Elit fusce placerat lectus quis aliquam nulla turpis platea. Integer mus bibendum sed wisi pretium ullamcorper nunc arcu. Ipsum maecenas sed. Et pariatur in. Ut wisi non. Bibendum nec et quisque quam diam sed dolor lorem. Pellentesque fames donec senectus nulla purus dui nibh praesent. Pariatur nulla augue sapien elit imperdiet aliquam ullamcorper orci. Integer nec mauris. Sit magnis vel ut leo a sapien proin at. Etiam sem aliquam bibendum mauris purus ac sagittis ultrices. Mollis eleifend est. Nec vitae posuere at arcu purus. In elementum vehicula.

ANEXO 2: ANEXO EXEMPLO 02

Id magna feugiat. Erat pellentesque sapien in rhoncus dolor augue vel eget. Erat nibh animi ultricies sit rhoncus. Eleifend aliquam luctus sem turpis habitasse. Lectus arcu ut mi nulla luctus facilisis cursus suspendisse class sociis metus vitae leo consequat lorem ullamcorper arcu. Nunc justo aliquam. Quidem volutpat urna. Nonummy nulla blandit donec vitae ultrices. Netus aliquam vivamus. Vehicula libero leo. Vestibulum consectetuer magna. Sapien aliquam arcu netus etiam lectus. Venenatis tristique morbi non nulla tortor commodo gravida ac neque lacinia urna. Elit mauris adipisci. Vitae sed curabitur. Tellus nunc lectus. Nonummy et integer.

Lorem dictumst enim. Dui vestibulum quisque. Dolor posuere risus. Nullam vitae est magnis est tortor metus dolor integer. Massa elit nec euismod et lacus quam ac malesuada est suspendisse ut est pellentesque vivamus lorem amet non vulputate maecenas et id ultrices lacus odio morbi vitae ac aenean in feugiat elit sodales congue proin dui leo bibendum scelerisque faucibus in suscipit. Nulla parturient in. Eget habitasse fringilla. Eget donec excepturi wisi lorem lacinia. Elementum lorem sem. Pede metus sit. Aenean facilisi pellentesque. Purus dictum ante. Neque amet sed.

Sed leo molestie. Elit fusce placerat lectus quis aliquam nulla turpis platea. Integer mus bibendum sed wisi pretium ullamcorper nunc arcu. Ipsum maecenas sed. Et pariatur in. Ut wisi non. Bibendum nec et quisque quam diam sed dolor lorem. Pellentesque fames donec senectus nulla purus dui nibh praesent. Pariatur nulla augue sapien elit imperdiet aliquam ullamcorper orci. Integer nec mauris. Sit magnis vel ut leo a sapien proin at. Etiam sem aliquam bibendum mauris purus ac sagittis ultrices. Mollis eleifend est. Nec vitae posuere at arcu purus. In elementum vehicula.