Research, Society and Development, v. 9, n. 8, e473985535, 2020
(CC BY 4.0) | ISSN 2525-3409 | DOI: http://dx.doi.org/10.33448/rsd-v9i8.5535

Uma Abordagem para Mitigar Ataque Blackhole em Redes Tolerantes a Atrasos e Desconexões utilizando Múltiplos Caminhos

An Approach to Mitigate Blackhole Attack on Delay Tolerant Networks using Multiple Paths

Un enfoque para mitigar el ataque de agujeros negros en redes tolerantes para retrasos y desconexiones utilizando múltiples rutas

Recebido: 11/06/2020 | Revisado: 01/07/2020 | Aceito: 01/07/2020 | Publicado: 18/07/2020

Rodrigo Perlin
ORCID: https://orcid.org/0000-0003-1906-9158
Universidade Federal de Santa Maria, Brasil
E-mail: rodrigo_perlin@hotmail.com
Ricardo Tombesi Macedo
ORCID: https://orcid.org/0000-0001-7469-8446
Universidade Federal de Santa Maria, Brasil
E-mail: rmacedo1987@gmail.com
Sidnei Renato Silveira
ORCID: https://orcid.org/0000-0002-4506-8522
Universidade Federal de Santa Maria, Brasil
E-mail: sidneirenato.silveira@gmail.com
Antonio Rodrigo Delepiane de Vit
ORCID: https://orcid.org/0000-0002-9452-0108
Universidade Federal de Santa Maria, Brasil
E-mail: rodrigodevit@inf.ufsm.br
Roberto Franciscatto
ORCID: https://orcid.org/0000-0002-3644-520X
Universidade Federal de Santa Maria, Brasil
E-mail: roberto.franciscatto@gmail.com

Resumo

As redes tolerantes a atrasos e desconexões (Delay Tolerant Networks – DTNs) são redes que não precisam de infraestrutura e utilizam da locomoção dos seus nós para se comunicar.

Todavia, ataques do tipo Buracos Negros (do inglês, Blackhole) consistem em uma ameaça para o funcionamento destas redes ao descartar pacotes de usuários legítimos. Na literatura há esforços para solucionar o ataque blackhole em DTNs. No entanto, as formas implementadas consomem uma grande quantidade de recursos da rede, pois funcionam por meio da geração de cópias da mensagem. Neste contexto, este trabalho apresenta uma abordagem de mitigação que se utiliza da Mojette e múltiplos caminhos para fragmentar, enviar e recuperar o dado e sem o alto desgaste da rede. A abordagem foi desenvolvida utilizando a IDE (Integrated Development Environment) Eclipse em conjunto com o simulador de ambiente de rede oportunista The ONE (The Opportunistic Network Environment Simulator). Nesse ambiente foram desenvolvidos dois cenários com diferentes situações, a fim de realizar três simulações, visando a avaliar a abordagem que tem como objetivos transmitir e recuperar o pacote ainda que existam descartes. Os resultados obtidos por meio das simulações revelam que a abordagem apresenta uma taxa de remontagem de no mínimo 75%, ainda que a taxa de pacotes perdidos seja de 62,50%.

Palavras-chave: Redes tolerantes a atrasos e desconexões; Ataque blackhole; Mitigação.

Abstract

Delay and Tolerant Networks (DTNs) are networks that do not need infrastructure and use their nodes to communicate. However Blackhole attacks (Blackhole) constitute a threat to the functioning of these networks by dropping packets from legitimate users. There are attempts in the literature to solve the blackhole attack on DTNs. However, the implemented forms consume a large amount of network resources because they work by generating copies of the message. This paper presents a Mitigation approach that uses Mojette and multiple paths to fragment, send and retrieve data without high network wear. The approach was developed using the Eclipse IDE in conjunction with The Opportunistic Network Environment Simulator. In this environment two scenarios with different situations were developed in order to perform three simulations, aiming to evaluate the approach that aims to transmit and retrieve the package even if there are discards. Simulation results show that the approach has a re-assembly rate of at least 75%, even though the lost packet rate is 62.50%.

Keywords: Delay and tolerant networks; Blackhole attack; Mitigation.

Resumen

Las redes tolerantes al retraso (DTN) son redes que no necesitan infraestructura y utilizan la locomoción de sus nodos para comunicarse. Sin embargo, los ataques de BlackHole

representan una amenaza para el funcionamiento de estas redes al descartar paquetes de usuarios legítimos. En la literatura hay esfuerzos para resolver el ataque del agujero negro en las ETD. Sin embargo, los formularios implementados consumen una gran cantidad de recursos de red, ya que funcionan generando copias del mensaje. En este contexto, este trabajo presenta un enfoque de mitigación que utiliza Mojette y múltiples formas de fragmentar, enviar y recuperar los datos y sin el alto desgaste de la red. El enfoque se desarrolló utilizando el Eclipse IDE (Entorno de desarrollo integrado) junto con el simulador de entorno de red oportunista The ONE (El simulador de entorno de red oportunista). En este entorno, se desarrollaron dos escenarios con diferentes situaciones, con el fin de realizar tres simulaciones, con el objetivo de evaluar el enfoque que tiene como objetivo transmitir y recuperar el paquete, incluso si hay descartes. Los resultados obtenidos a través de las simulaciones revelan que el enfoque presenta una tasa de reensamblaje de al menos 75%, aunque la tasa de paquetes perdidos es 62.50%.

Palabras clave: Redes tolerantes para retrasos y desconexiones; Ataque de agujero negro; Mitigación.

1. Introdução

As redes tolerantes a atrasos e desconexões (Delay Tolerant Networks – DTNs) são um exemplo de rede do tipo armazena-e-encaminha (store-and-forward), ou seja, antes da mensagem ser enviada, a rede a armazena para, somente depois enviá-la ao próximo nó, não havendo necessidade destes nós estarem sempre conectados (Nunes e Dotti, 2009). Nesse contexto, torna-se vantajoso utilizar essa tecnologia em cenários marítimos ou de grande extensão, pelo fato das DTNs não precisarem de infraestrutura e explorarem a conectividade intermitente entre nós móveis para transferir dados. Em outras palavras, os nós trocam dados quando se movem para o intervalo de transmissão (Navaz et al. 2015). Oliveira et al (2007) destacam outras aplicações para as DTNs, tais como: comunicações sem fio, comunicações entre dispositivos móveis, comunicações entre dispositivos com restrições de energia, comunicações rurais e comunicações interplanetárias, entre outras. Além disso, as redes tolerantes a atrasos e desconexões são economicamente mais baratas em comparação aos *links* de satélite utilizados nas comunicações da marinha (Hao-Min et al. 2010). Entretanto, existe o *blackhole*, uma forma de ataque que afeta um ou vários nós de uma DTN (Alves Júnior & Albini, 2012). Analisando um cenário marítimo, as complicações são mais graves visto que, além da alta complexidade na comunicação, o *blackhole* (buraco negro) funciona por meio de

protocolos de roteamento na camada de rede, e sua principal caraterística inclui o descarte dos pacotes recebidos pois, após ser selecionado para o recebimento dos pacotes por ter indicado possuir uma rota mais curta ao destino, os descarta sem enviá-los (Soundaravalli, 2017). Além disso, visando aumentar suas chances de ser selecionado para recebimento de dados, utiliza-se de uma probabilidade falsa de recebimento e entrega forjada pelo próprio nó mal-intencionado (Ren et al. 2010).

Na literatura, há diferentes soluções para o ataque *blackhole* em DTNs. As abordagens para solucionar esse ataque são classificadas em: (i) identificação, (ii) mitigação e (iii) prevenção. Conforme Navaz et al (2015), a existência de um protocolo para mitigação é crucial e altamente desejável em uma DTN, pois há cenários em que a prevenção de *blackhole* será impossível. Dentro da mitigação, as principais abordagens estudadas neste trabalho compreendem diferentes propostas. Hinai et al (2012) propõem o SnW, um protocolo de roteamento para mitigar ataques *blackhole* em DTNs. Suas escolhas são feitas com base em níveis, por meio de duas fases, utilizando o conceito de enviar cópias da mensagem para vários nós até que a mesma chegue ao destino ou por transmissão direta. Alves Júnior & Albini (2012) apresentaram um protocolo de roteamento que usa múltiplos caminhos e combina um esquema de partilha de informações, baseado no teorema chinês dos restos, aspirando melhorar a mitigação em redes *ad hoc*. Guedon & Normand (2005) usaram a *Mojette*, uma aplicação de geometria discreta, baseada em projeções e cálculos de matemática simples. Seu funcionamento se caracteriza por armazenar e fragmentar a informação para depois enviá-la, tendo como diferencial o ganho em desempenho e uma melhor recuperação da informação.

Neste contexto, este trabalho apresenta uma abordagem para mitigação de ataques de buracos negros em DTNs. A abordagem oferece uma proposta de mitigação com uma menor sobrecarga da rede e uma melhor margem de recuperação da informação. Para isso, o funcionamento da abordagem foi dividido em três etapas distintas: (i) a fragmentação da informação utilizando a transformada *Mojette*, (ii) o envio das partes usando rotas distintas e roteamento de múltiplos caminhos, (iii) a remontagem da informação original utilizando a transformada *Mojette* inversa e (iv) a utilização de um simulador para coletar resultados. Para o desenvolvimento e testes utilizamos a IDE (*Integrated Development Environment*) *Eclipse* em conjunto com o simulador de ambiente de rede oportunista, The ONE, do inglês *The Opportunistic Network Environment Simulator*, como sistema para simular a rede de nós. Uma avaliação de desempenho com três simulações foi executada com o objetivo de medir a taxa de remontagem e o número de pacotes perdidos. Elas foram implementadas por meio de

dois diferentes cenários, os quais foram criados na IDE *Eclipse* com o The ONE. No primeiro cenário criamos uma simulação de um navio em movimento em alto mar. O segundo cenário se caracteriza pelo fato do navio não se mover. Os resultados obtidos revelam que a abordagem apresenta uma taxa de recuperação satisfatória, pois houve taxa de remontagem de 75%, ainda que a taxa de pacotes perdidos seja de 62,5%.

Neste contexto, este trabalho está organizado da seguinte maneira: a seção 2 apresenta o referencial teórico. A seção 3 descreve os trabalhos relacionados. A seção 4 detalha a abordagem definida. A seção 5 apresenta as simulações desenvolvidas. Encerrando o artigo são apresentadas as considerações finais e as referências empregadas.

2. Fundamentação Teórica

Esta seção apresenta um breve referencial teórico sobre as áreas envolvidas no desenvolvimento deste trabalho. A subseção 2.1 apresenta fundamentos de redes de computadores. A subseção 2.2 introduz os principais conceitos sobre a rede tolerante a atraso e desconexão (DTN). A seção 2.3 explica como um ataque *blackhole* funciona em uma rede DTN.

2.1. Fundamentos de Redes de Computadores

As redes de computadores foram criadas e, até hoje, são usadas para comunicação e troca de informações. Porém, conforme a evolução tecnológica foi ocorrendo, as redes foram ganhando complexidade. Pensando em uma forma de minimizar isso foi criado o contexto de camadas de rede, que usa a divisão em camadas para tornar mais fácil a identificação de erros e falhas. Nesse contexto, cada camada possui funções independentes e diferentes das demais (Tanenbaum, 2003). Os pacotes são uma sequência de dados ou estrutura unitária de transmissão de dados enviada por uma rede de computadores. Por exemplo, quando um computador (*host*) tem uma mensagem para ser enviada para outro computador, primeiro o computador divide a mensagem em pacotes, ou seja, partes menores, sendo que cada um conterá o seu número na sequência. Esses pacotes são, então, injetados na rede e posteriormente depositados no *host* receptor, onde são novamente montados para formar a mensagem original (Tanenbaum, 2003). Esse processo de enviar ou receber pacotes acontece por meio de rotas.

Em DTNs, os protocolos de roteamento aspiram criar uma rota que aproveite ao

máximo os possíveis contatos que ocorram entre os nós, visando a melhor maneira de entregar o pacote ao destino (Vieira et al, 2013). Todavia, o termo roteamento, designa duas atividades distintas e independentes. A primeira é classificada como o estabelecimento do melhor caminho do ponto de origem ao destino (rota). Esse processo de estabelecimento do melhor caminho pode ser executado de dois modos: dinâmico ou estático (Mendes, 2007). A segunda atividade se nomeia como o processo de despachar cada pacote ao seu destino final ou ao próximo roteador. No roteamento dinâmico, os roteadores podem descobrir as informações, de forma automática, e compartilhá-las com outros roteadores via protocolos de roteamento dinâmicos.

Os protocolos são regras sobre o modo de como se dará a comunicação entre as partes envolvidas. Protocolos de roteamento dinâmico têm a vantagem de permitirem determinar o melhor caminho para um destino se o atual torna-se inacessível devido à queda de um *link* ou se uma região fica inacessível em virtude do congestionamento. Já o roteamento estático das informações necessárias para o roteador encaminhar os pacotes é colocado manualmente por uma pessoa e, assim, não contando com a função automática de determinar o melhor caminho para um destino caso o atual ser inacessível (Ross, 2013). Um nó, por sua vez, pode ser definido como um ponto de conexão, um ponto de redistribuição ou um terminal de comunicação de uma rota. Sua definição depende da rede e da camada de protocolo usado. Um nó de rede ativo é capaz de enviar, receber ou transmitir informações por meio de um canal de comunicação.

2.2. Rede Tolerante a Atraso e Desconexão

Uma rede tolerante a atraso e desconexão tem, como características principais, os atrasos e suas desconexões. Os atrasos, em comparação com outras redes, são mais frequentes, pois o roteamento acontece de forma assimétrica. Embora muitas vezes, esses atrasos aconteçam pela desconexão de um nó e pode se pensar em uma perda do pacote, todavia, ocorre o armazenamento dos pacotes nos nós intermediários. Esse processo torna possível a desconexão sem perda do dado (Cao &Sun, 2013). As desconexões podem ocorrer pela alta mobilidade que provoca constantes mudanças na topologia da rede, por péssimas condições de comunicação ou por economia de recursos. Esses fatores colaboram para existir uma conectividade intermitente da rede durante horas ou dias (Oliveira et al, 2008). Então, em se tratando das DTNs se considera o contato uma parte fundamental, visto que por ele acontece a troca de dados entre os nós. Todavia, sempre existe a possibilidade de atraso e

desconexão para qualquer tipo de contato. Dependendo do tipo de contato, as falhas podem acontecer mais frequentemente. A arquitetura DTN classifica os contatos em: persistente, sob demanda, programado, oportunista e previsível (Cerf & Burleigh, 2002).

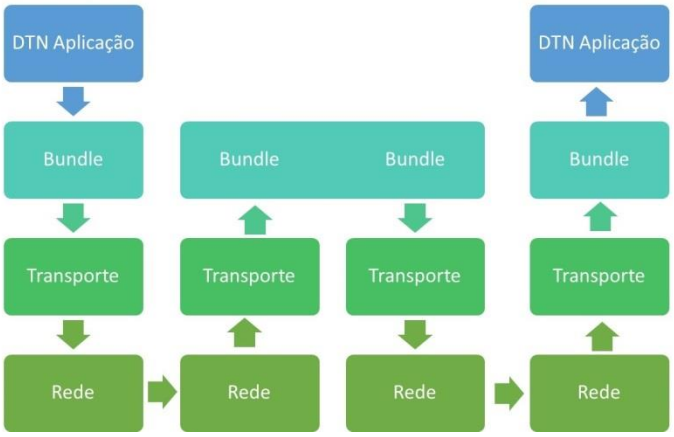
Há diversos protocolos de transmissão desenvolvidos aspirando superar problemas inerentes às redes intermitentes. Esses protocolos podem ser classificados basicamente em dois grupos: probabilísticos e não probabilísticos. Os protocolos probabilísticos são baseados em dados estatísticos calculados pelos encontros entre nós, quantidade de retransmissões de uma mensagem, tempo de existência dos pacotes na rede e da quantidade de confirmações de recebimento emitidas por um destinatário. Já os protocolos não probabilísticos têm como característica a pulverização de cópias desses, pressupondo que quanto mais cópias forem espalhadas na rede, maior será a probabilidade de entrega. Segundo Mangrulkar & Atique (2010) o roteamento em DTN se caracteriza por dispor de duas estratégias principais: inundação e encaminhamento. A estratégia de inundação tem como caraterística a replicação das mensagens para aumentar chances de chegar ao destino. A estratégia de encaminhamento se baseia em utilizar o conhecimento da rede para selecionar a melhor rota ao destino. Na estratégia de inundação há criação de múltiplas cópias da mesma mensagem estas cópias são entregues ao conjunto de nós de retransmissão. Os nós de retransmissão fazem o papel de armazenar as mensagens até o momento que elas entrem em contato com o nó de destino (Fall, 2010). Essa replicação de mensagens tem a finalidade de aumentar a probabilidade de entrega da mensagem ao destino. Um exemplo desse conceito aparece em algumas abordagens de mitigação de ataques *blackhole*, pois uma das técnicas empregadas é a de enviar cópias da mensagem por diversas rotas.

Na estratégia de encaminhamento existe o uso da topologia de rede e do conhecimento local ou global para encontrar a melhor rota até o destino (Mangrulkar & Atique, 2010). A abordagem parte do princípio de enviar por um único caminho escolhido, por meio da avaliação de parâmetros da rede. Um exemplo dessa abordagem é a estratégia de roteamento de gradiente, considerada adequada para a rede de sensores porque segue um gradiente de melhora dos valores da função, ao passo que vai em direção ao destino (Khadar & Razafindralambo, 2007).

A DTN pode usar vários protocolos para entregar seus pacotes, porém o uso do protocolo de pacotes (*bundle protocol*) é de extrema importância, pois serve para organizar o envio agrupado de pacotes e não mais como pacotes individuais. Esse processo de organização permite atribuir, a cada *bundle*, graus diferentes de atraso e importância. Sua localização está entre a camada de aplicação e a camada de transporte, conforme mostra a

Figura 1 (Vieira et al, 2013).

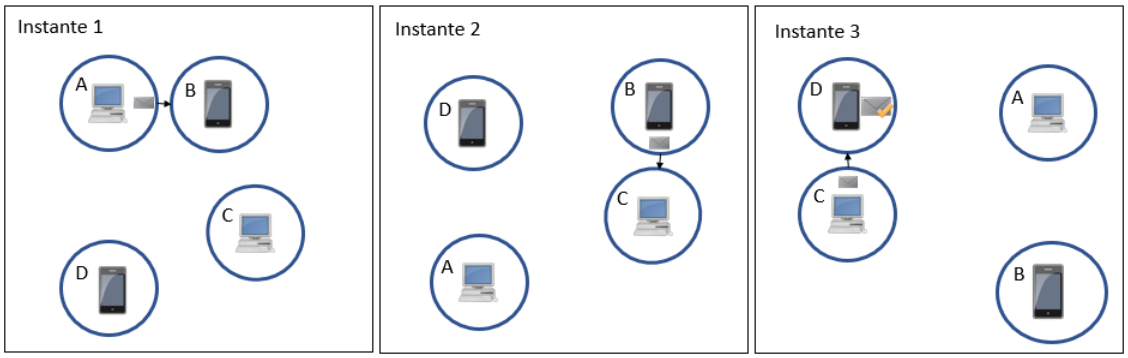
Figura 1. Ilustração do processo de comunicação.



Fonte: Os autores (2020).

Uma curiosidade sobre essas redes é que elas também são chamadas de redes de oportunidades, porque o nó intermediário sempre procura a oportunidade de retransmitir a mensagem da origem para o destino (Mangrulkar & Atique, 2010). Em DTNs, quando o nó destino está desconectado, o nó intermediário armazena as suas mensagens e as repassa por meio de conexões estabelecidas posteriormente quando ele estiver ativo na zona de transmissão (Campos et al, 2009). Esse conceito pode ser visto na Figura 2.

Figura 2. Exemplo de uma Rede Tolerante a Atraso e Desconexão.

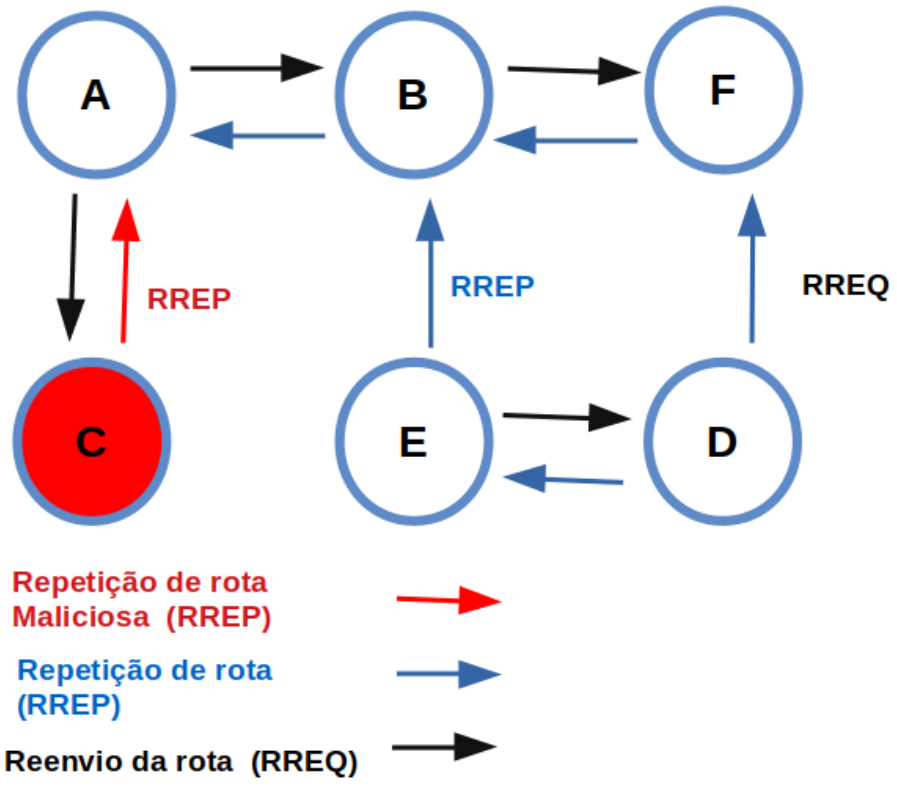


Fonte: Os autores (2020).

2.3. Ataque *Blackhole*

De acordo com Al-Shurmanet et al (2004), o buraco negro, ou *blackhole*, é um ataque que atinge um nó ou vários nós em redes tolerantes a atrasos e desconexões. Seu funcionamento acontece por meio de um nó mal-intencionado que usa o protocolo de roteamento para apresentar-se como o caminho mais curto para o nó de destino. Para fazer isso, quando ele se encontra com um nó confiável, apresenta um histórico falso de encontro com outros nós confiáveis. Depois de forjar a informação e atrair os pacotes para o nó mal-intencionado, diferentemente dos nós comuns, ele descarta as mensagens (Soundaravalli, 2017). Conforme Baburaj & Alagarsamy (2015) o buraco negro é o ataque onde o nó de origem recebe informações de roteamento falsas, porque o nó malicioso forja informações de encontros com outros nós (como mostra a Figura 3). Entretanto, esse processo de eliminar pacotes recebidos e forjar encontros faz ocorrer um padrão anormal de frequência de encontros e do número de mensagens enviadas, em comparação com encontros de nós confiáveis (Pham & Yeo, 2015), o que permite que essa técnica seja utilizada para detectar o ataque.

Figura 3. Exemplo de Funcionamento do Ataque Blackhole em DTNs.



Fonte: Os autores (2020).

Na Figura 3 está representado o ataque de buraco negro em DTNs, onde o nó A é o nó de origem e o nó D refere-se ao nó de destino. Nesse contexto, o nó C se caracteriza pelo nó malicioso (buraco negro), o qual responde ao RREQ (*route request*) enviado pela origem (A) comum. A resposta falsa relata que dispõe da rota mais curta para o nó de destino (D). Além disso, forja ser um nó confiável. Essa prática é feita simulando encontros com outros nós. Assim, a origem (nó A) escolhe de forma errada e envia os pacotes de dados para um nó malicioso. O nó malicioso pode descartar ou consumir o pacote, mas percebe-se que ele não repassa ao nó E os pacotes (Gupta & Sharma, 2016).

3. Revisão Bibliográfica

Na literatura, há diferentes soluções para o ataque *blackhole* em DTNs. As abordagens para solucionar esse tipo de ataque são classificadas em: (i) identificação, (ii) mitigação, (iii) prevenção. Todavia, conforme Navaz et al (2015), existir um protocolo para mitigação é altamente desejável em uma DTN, pois existem cenários em que a prevenção de blackhole será impossível. Dentro da mitigação Hinai et al (2012) propõem um protocolo de geração e envio de cópias da mensagem por múltiplos caminhos ou comunicação direta para aumentar a probabilidade de entrega. Alves Júnior & Albini (2012) também utilizaram múltiplos caminhos, embora tentaram corrigir o problema de desgaste da rede utilizando um teorema chinês, o qual provou ser ineficiente. Já a *Mojette*, do trabalho de Guedon & Normand (2005), trata de uma aplicação geométrica de menor custo processual. O menor desgaste ocorre por utilizar somente contas de adição e subtração. O TB-SnW foi apresentado como um protocolo de roteamento para mitigar ataques *blackhole* em DTNs por Hinai et al (2012). O seu funcionamento, embora seja parecido com um protocolo baseado em inundações, impõe um limite ao número total de cópias e transmissões por mensagem. O SnW trabalha relacionando duas fases e utilizando dois modos de execução. Na fase de Spray, para cada mensagem originada em um nó de origem, um número fixo de cópias de mensagens é inicialmente distribuído pela origem e possivelmente recebido por outros nós. Na segunda fase, definida de *Wait*, se os destinos não forem encontrados na fase de *Spray*, cada nó encaminhará a mensagem apenas para seu destino, ou seja, transmissão direta. O modo de funcionamento normal funciona quando um nó encaminha uma única cópia da mensagem para qualquer outro nó que encontrar. Já no modo binário, o nó transmissor transfere metade das cópias que está mantendo para os nós conectados. Assim que o nó tiver distribuído quase todas as suas mensagens, mantendo somente uma cópia da mensagem, ele mudará para a fase de *Wait*, em

que vai manter essa cópia até que esteja em contato direto com o destino final. Apesar de que o protocolo de roteamento pode aumentar o potencial de entrega das mensagens utilizando esta abordagem, existe uma sobrecarga da rede resultante do processo de gerar cópias da mensagem, assim não importando se a rede está livre de *blackhole* ou se sofre desse tipo de ataque.

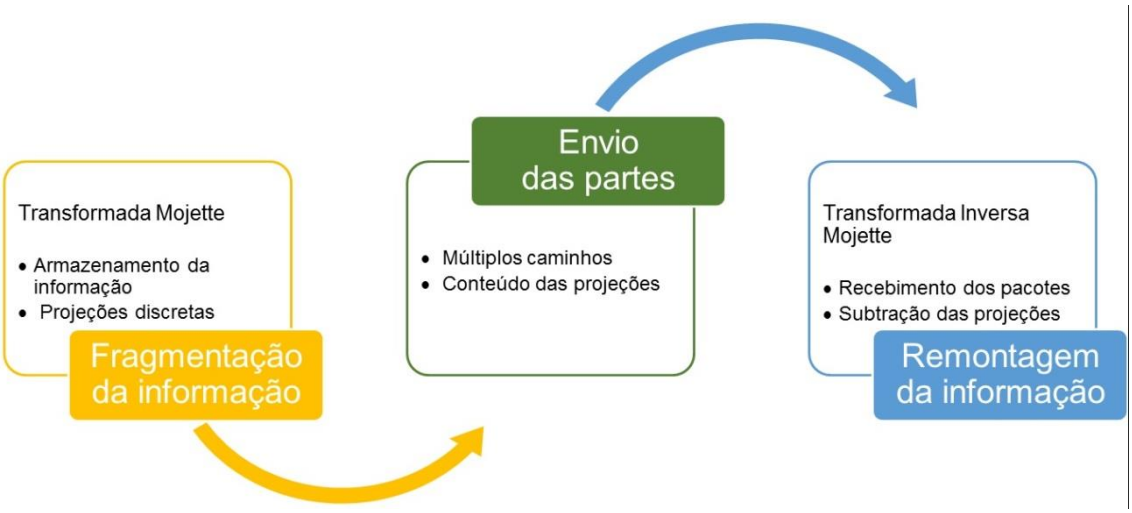
Em Alves Júnior & Albini (2012), foi proposto um protocolo de roteamento de múltiplos caminhos, que combina um esquema de partilha de informações, baseado no teorema chinês dos restos. O funcionamento do protocolo acontece em etapas distintas: a divisão da informação original com base no teorema chinês, a transmissão das partes usando rotas disjuntas, por meio do roteamento de múltiplos caminhos e a remontagem da informação original no destino. O teorema chinês, simplificadamente, funciona dividindo a mensagem em N partes de mesmo tamanho, as quais são enviadas por C caminhos diferentes e disjuntos. O tamanho de cada parte deve ser D/K, em que D se caracteriza pelo tamanho da informação original e K se define pelo número de partes necessárias para reconstruir a informação original. O protocolo desenvolvido foi comparado com os outros protocolos de roteamento usados em redes *Ad-hoc*. O resultado, em um cenário onde mais de 60% dos nós da rede são atacantes, apresentou uma taxa de entrega maior que 50% e houve uma redução superior a 50% no número de pacotes descartados. Embora os resultados sejam animadores, os autores destacam o problema de sobrecarga extra, ocasionada pela divisão da informação. Guedon & Normand (2005) apresentam o uso da *Mojette* para demonstrar como a geometria discreta pode ser uma ferramenta para otimizar rede e armazenamento. *Mojette* é uma aplicação de geometria discreta que funciona por contas de adições e subtrações, acarretando um menor custo de processamento no cenário computacional. Além disso, por sua redundância na transformação, os dados enviados podem ser fragmentados sem perda. O estudo explica o uso de geometria discreta para armazenar um suporte geométrico discreto e depois o projeta em direções discretas para, no futuro, recuperá-lo por meio do processo inverso, mesmo se alguma parte da informação for perdida. A recuperação dos dados acontece pela *inverse mojette transform*, que reconstrói, ainda que com uma pequena fração do dado. A *mojette transform* oferece uma aplicação para recuperar dados, além de segurança pois, caso um servidor for atacado ou destruído por *hackers*, seu conteúdo pode ser restaurado por qualquer conjunto de outros servidores ou, caso seu conteúdo for roubado, não poderá ser utilizado sozinho pelo usuário. Ainda que, o trabalho apresenta uma forma de fragmentar e transmitir os dados sem sobrecarga, essa aplicação não foi utilizada no contexto de redes, o que traria grande desempenho.

Neste trabalho propomos usar a transformada *Mojette* para fragmentar os dados, e os enviar por múltiplos caminhos e serem remontados pela *Mojette* transformada inversa. O processo de envio se assemelha ao proposto no trabalho de Alves Júnior & Albini (2012), onde são enviados os pacotes por múltiplas rotas disjuntas por meio de roteamento de múltiplos caminhos. Porém, no trabalho de Alves Júnior & Albini (2012), a fragmentação e a restauração do dado são realizadas por meio de um teorema chinês. Neste protocolo usaremos a *Mojette* (Guedon & Normand, 2005). Esta abordagem reduz significativamente a sobrecarga de rede, pois realiza sua fragmentação e restauração por uma aplicação que usa somente cálculos de adição e de subtração. Além disso, possibilita a restauração ainda que haja perda de uma parte da mensagem. Isto permite o desenvolvimento de aplicações em alto nível para o roteamento e segurança em redes tolerantes a atrasos e desconexões.

4. Abordagem de Mitigação Aplicada

A abordagem de mitigação aplicada neste trabalho está organizada em três etapas distintas: (i) a etapa de fragmentação da informação divide o dado em partes menores, utilizando a transformada *Mojette*; (ii) a etapa de envio das partes utiliza de múltiplos caminhos para diminuir a chance de perda total da informação e (iii) a etapa de remontagem da informação agrupa os pacotes recebidos pelos múltiplos caminhos utilizando a transformada *Mojette* inversa. A Figura 4 ilustra as etapas da abordagem.

Figura 4. Etapas da abordagem.



Fonte: Os autores (2020).

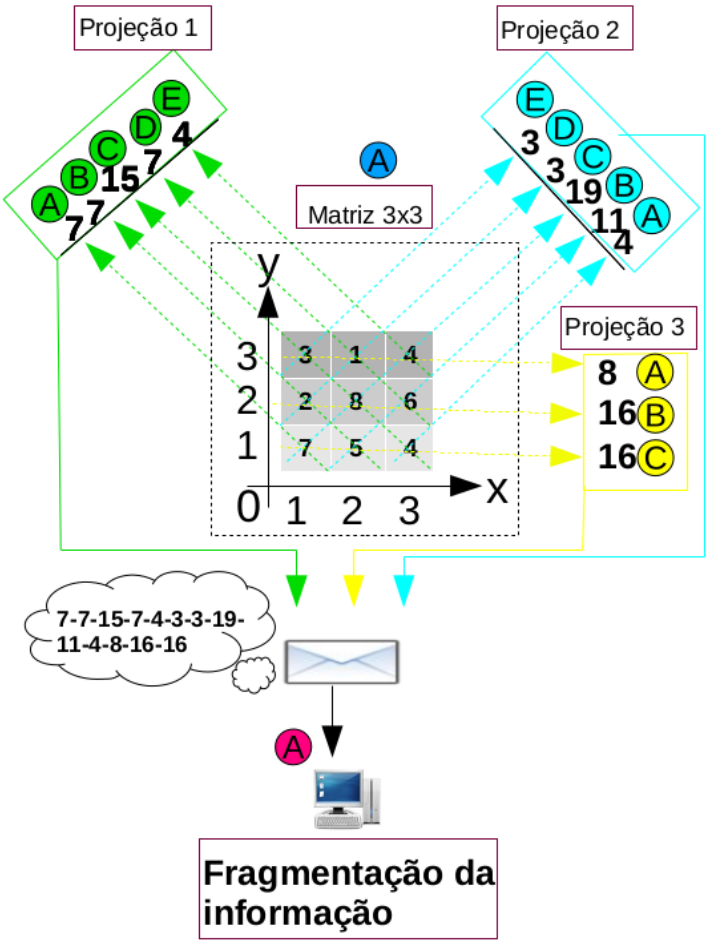
4.1. Fragmentação da Informação

A fragmentação funciona como parte essencial desta abordagem, pois para ser efetivo o envio por múltiplos caminhos, necessita-se enviar pacotes com conteúdo diferente pelas rotas. Todavia, se for realizada uma fragmentação utilizando lógica, existe a possibilidade de aumentar a margem de recuperação da informação. Nesse contexto, utilizamos a transformada Mojette para fragmentar usando o mínimo de processamento e empregando lógica como nos trabalhos de Serfozo et al. (2007) e Guedon & Normand (2005), mas em contextos diferentes.

Como exemplo, apresentamos uma aplicação que possui o seu funcionamento inicial por um suporte geométrico (conforme mostra a Figura 5), uma Matriz 3x3 (A), utilizada para armazenar a informação e gerar projeções. As projeções são resultados da adição das unidades atingidas pelo raio reto na matriz, projetadas em direções discretas.

Por exemplo, na Figura 5 na matriz 3 x 3 (A), na posição y = 3 x = 3 o valor equivalente da projeção 1 parte (E) equivale a 4 por ser a única unidade atingida. Já na posição y = 2 x = 1 e y = 2 x = 2 os valores são, respectivamente, 2 e 5. Assim, o valor equivalente da projeção 1 parte (B) equivale a 7, pois houve a soma das duas unidades e, dessa forma, acontece subsequente com as outras partes das projeções. A direção da projeção é fixo anti-horário, como em trigonometria quando vai de 0 a 180 para evitar valores negativos.

Figura 5. Fragmentação em Ação.



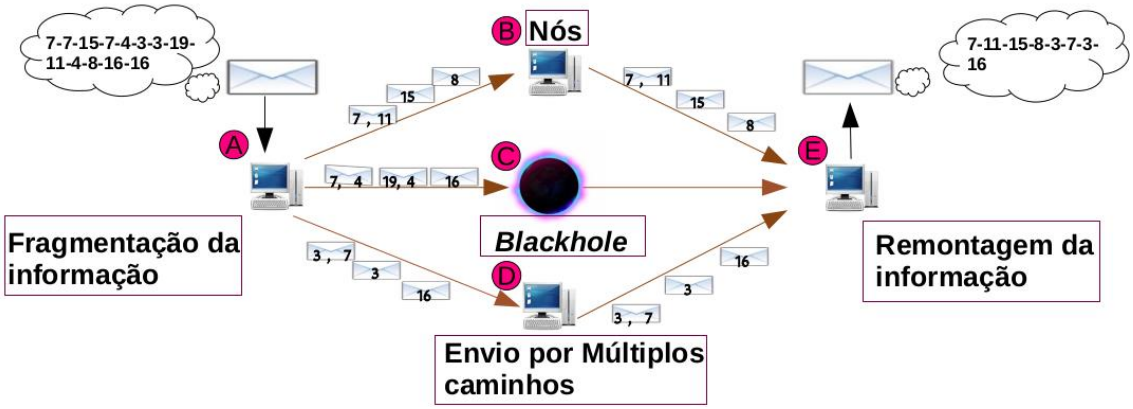
Fonte: Os autores (2020).

4.2. Envio por múltiplos caminhos

Atualmente, a técnica de múltiplos caminhos está sendo utilizada em diversas áreas de redes. O motivo dessa aceitação está relacionado aos benefícios ocasionados pela mesma. Alguns destes benefícios podem ser interessantes para a mitigação, tais como o balanceamento de carga, a tolerância a falhas, a agregação de banda e a redução do atraso (Tsai & Moors, 2006). Além disso, conforme Lou et al (2003), utilizar múltiplos caminhos fortalece a segurança da rede, que tem grande importância para a mitigação. Nesse contexto, a Figura 6 apresenta o conceito de múltiplos caminhos para contornar a perda total da informação enviada. O nó emissor (A) encaminha mensagens contendo partes das projeções, usando mais de uma rota para chegar ao nó de destino (E). Percebe-se que se utilizam os nós B, C, D como nós intermediários. Esse exemplo, além da demonstração do uso de múltiplos caminhos, também apresenta o funcionamento do ataque *blackhole* (nó C).

Conforme o exemplo da Figura 6, os pacotes das rotas B e D chegaram até seu destino, porém os pacotes enviados pela rota C foram descartados.

Figura 6. Envio por múltiplos caminhos.



Fonte: Os autores (2020)

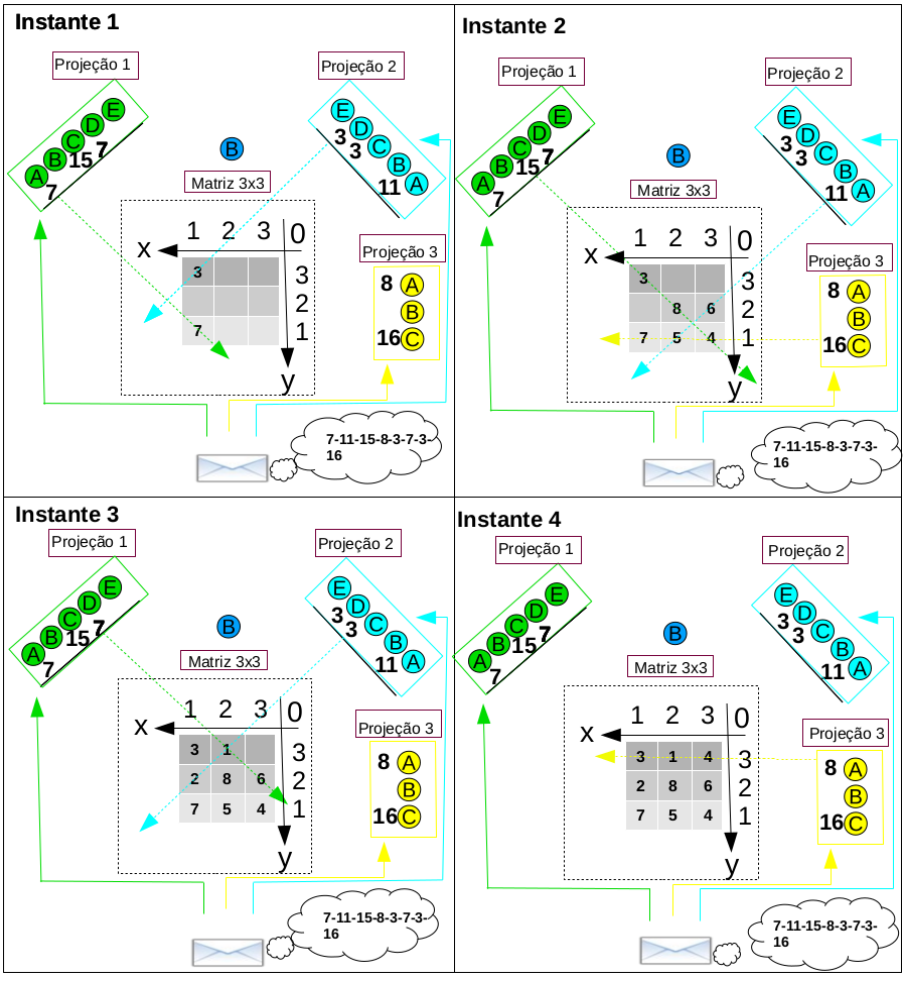
4.3. Remontagem da Informação

A remontagem acontece como parte final da abordagem proposta. O preenchimento das unidades da matriz acontece por subtração das partes das projeções recebidas. As partes das projeções recebidas servem como ponteiros lógicos para o preenchimento do restante do suporte geométrico, conforme mostra a Figura 7. Esse trabalho é realizado pela inversa transformada *Mojette*, que remonta a matriz utilizando um conceito lógico empregado na fragmentação. Entretanto, agora o processo é inverso. Essa proposta de remontagem foi utilizada, também, por Serfozo et al (2007) e Guedon & Normand (2005), para proporcionar um maior grau de recuperação da informação. No exemplo utilizado (Figura 7), representamos um caso com uma matriz 3x3, porém a lógica se mantém, caso ela seja de maior ou menor complexidade, pois o processo de recuperação funciona por meio de lógica matemática. Neste exemplo recebemos os valores (7, 15, 7) da projeção 1, (3, 3, 11) da projeção 2 e (8, 16) da projeção 3. Dessa forma, a remontagem começa ajustando as partes das projeções em seus devidos lugares e preenchendo as unidades possíveis da matriz, conforme a Figura 7, instante 1. Depois disso, usaremos a parte (C) da projeção 1 equivalente a 15. Porém, existe uma unidade já preenchida (y = 3 x = 1) dessa projeção. Então usaremos o resultado de 15 - 3 = 12. Analisando a projeção 1, parte (C), os resultados possíveis para atingir valor 12 são: 12 +0, 11 + 1, 10 + 1, 9 + 3, 8 + 4, 7 + 5 e 6 + 6 ou a ordem inversa desses. Para a projeção 2, parte (B), os resultados possíveis para atingir o valor 11 são: 6 + 5,

7 + 4, 8 + 3, 9 + 2, 10+ 1 e 11 + 0 ou a ordem inversas desses. Na projeção 3, parte (C), os resultados possíveis para atingir o valor 16 são vários, mas existe uma unidade preenchida com valor 7 (y = 1x = 1). Sendo assim, assumimos que as outras duas unidades tem que resultar em 9. Portanto os resultados possíveis são: 9 + 0, 8 + 1, 7 + 2 , 6 + 3 e 5 + 4. Entretanto, os números utilizados nessas somas também fazem parte das outras duas projeções citadas anteriormente, já que y = 1 x = 3 faz parte da projeção 1 e y = 1 x = 2 faz parte de projeção 2. Assim sendo, o único resultado aceito na projeção 3 parte (C) é 5 + 4, pois o 4 foi usado, também, para preencher a projeção 1 parte (C) e o 5 para completar a projeção 2 parte (B), Figura 7, instante 2.

Após essa análise, o restante da matriz é preenchido com um processo simples de subtração dos valores das projeções pelos números já preenchidos, como mostra a Figura 7, instantes 3 e 4. Todavia, a recuperação da matriz (B) foi completa, ainda que houve o descarte de algumas partes das projeções pelo *blackhole*.

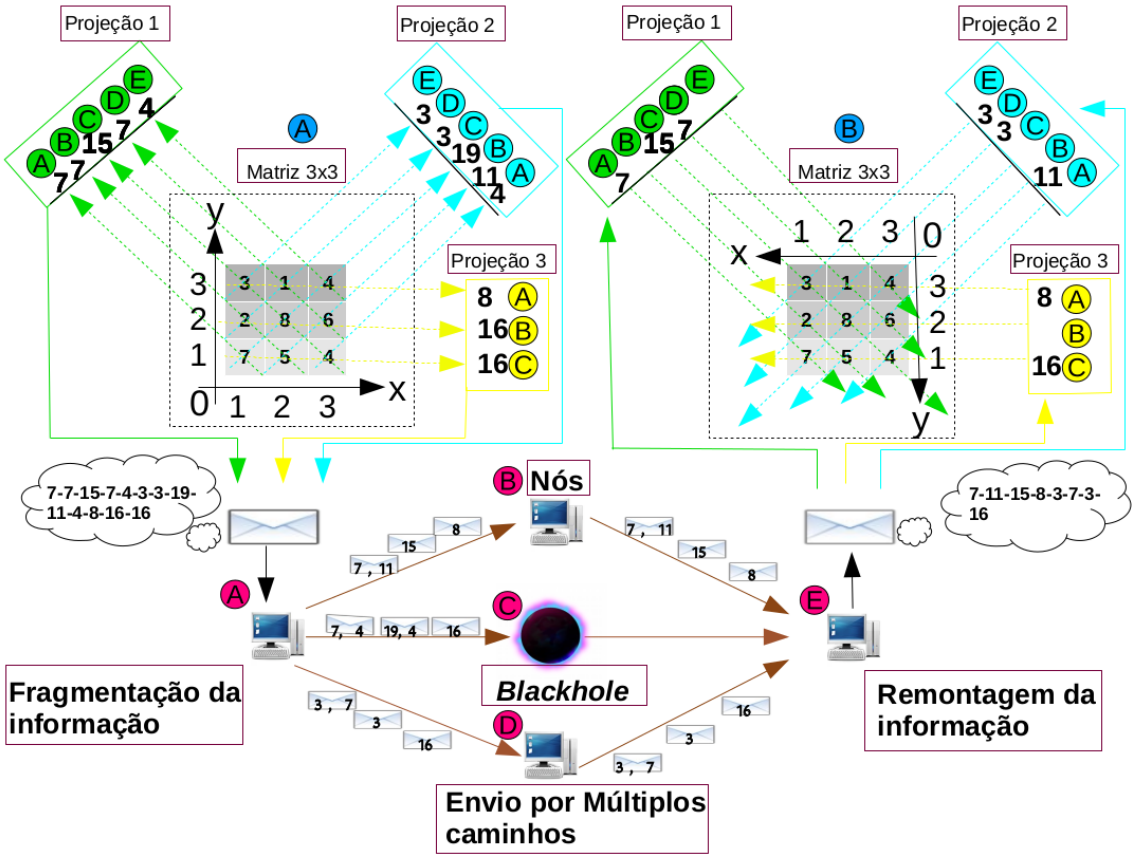
Figura 7. Matriz 3x3 (B), instantes de remontagem.



Fonte: Os autores (2020)

A Figura 8 demonstra, graficamente, a abordagem completa em ação.

Figura 8. Abordagem Completa em Ação.



Fonte: Os autores (2020)

Os resultados da primeira simulação apresentaram uma taxa de remontagem de 75% e 62,5% de pacotes perdidos. No segundo cenário se desenvolveu a segunda simulação, analisando os pacotes entregues ao destino para, assim, chegar à taxa de remontagem. Como no primeiro cenário, um total de oito pacotes foi enviado ao destino, mas desses três foram perdidos (C2,C3, C8) e cinco (C4, C5, C6, C7, C9) foram recebidos pelo nó de destino. Com esses pacotes entregues houve a restauração de 100% do dado, pela *Mojette* Inversa. A taxa representa a recuperação total, visto que se perderam 37,50% dos pacotes devido ao ataque.

Ainda no segundo cenário aconteceu a terceira simulação onde se perdeu metade dos pacotes, visando testar o limite máximo de perda, com uma taxa de recuperação integral. Um total de oito pacotes foi enviado ao destino, todavia desses quatro foram perdidos (C2, C3, C8, C9) e quatro (C4, C5, C6, C7) foram recebidos pelo nó de destino. Com esses pacotes entregues houve a restauração de 100% do dado, pela *Mojette* Inversa. Essa taxa representa uma porcentagem recuperação ótima, pois cerca de 50% dos pacotes foram descartados pelo

ataque.

5. Considerações Finais

Neste trabalho apresentamos uma abordagem para mitigar o ataque *blackhole* em DTNs utilizando múltiplos caminhos. A abordagem proposta não se utiliza de múltiplas cópias para recuperar o dado, diferentemente dos trabalhos estudados. Também, diante de alguma perda de pacotes pelo ataque *blackhole*, a abordagem proposta consegue recuperar a maioria ou total dos pacotes. Uma avaliação de desempenho foi conduzida, onde utilizamos dois cenários, criados na IDE *Eclipse*, em conjunto com o simulador de ambiente de rede oportunista The ONE. As métricas utilizadas nos cenários para avaliação foram a taxa de recuperação e a taxa de pacotes perdidos. Os resultados mostram que a abordagem consegue ter uma taxa de remontagem de 100%, ainda que exista a perda da metade dos pacotes, como apresentado na terceira simulação. Como trabalhos futuros serão realizadas avaliações de desempenho, considerando outros tipos de ataques.

Referências

Al-Shurman, M., Yoo, S. M., & Park, S. (2004). Black hole attack in mobile ad hoc networks. In: *Proceedings of the 42Nd Annual Southeast Regional Conference*, ACM-SE 42, 96–97, New York, NY, USA. ACM. Disponível em: https://doi.org/10.1145/986537.986560. Acesso em agosto, 2019.

Alves Júnior, J., & Albini, L. C. P. (2012). Um protocolo de roteamento resistente a ataques blackhole sem detecção de nós maliciosos. In *Simpósio Brasileiro de Telecomunicações*. Disponível em: http://sbrt.org.br/sbrt2012/publicacoes/97960_1.pdf. Acesso em agosto, 2019.

Baburaj, C., & Alagarsamy, K. (2015). *An efficient secure routing mechanism for preventing wormhole and black hole attacks in a trusted DTN environment*. 9, 140–147. Disponível em: https://www.researchgate.net/publication/284601517_An_efficient_secure_routing_mechanism_for_preventing_wormhole_and_black_hole_attacks_in_a_trusted_DTN_environment. Acesso em setembro, 2019.

Cao, Y., & Sun, Z. (2013). Routing in delay/disruption tolerant networks: a taxonomy, survey and challenges. *IEEE Communications Surveys Tutorials*, 15(2),654–677. Disponível em: https://ieeexplore.ieee.org/document/6196145. Acesso em agosto, 2019.

Campos, C. A. V., Fernandes, R. M. S., & Moraes, L. F. M. (2009). Uma avaliação das redes tolerantes a atrasos e desconexões através de traces reais de mobilidade humana. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Disponível em: http://ce-resd.facom.ufms.br/sbrc/2009/055.pdf. Acesso em outubro, 2019.

Cerf, V., & Burleigh, S. H. (2002). *Delay-tolerant network architecture*: The evolving interplanetary internet. Disponível em: https://tools.ietf.org/html/draft-irtf-ipnrg-arch-01. Acesso em agosto, 2019.

Fall, K. (2010). A delay-tolerant network architecture for challenged internets. In *Proceeding of annual conference of the special Internet Group on Data Communication* ACM Siggomm '03, pages 27–34. Disponível em: https://dl.acm.org/doi/10.1145/863955.863960. Acesso em agosto, 2019.

Guedon, J., & Normand, N. (2005). *The Mojette transform*: The first ten years. In Andres, E.; Damiand, G.; Lienhardt, P. Discrete Geometry for Computer Imagery, volume 3429 of Lecture Notes in Computer Science, 79–91. Disponível em: https://link.springer.com/chapter/10.1007/978-3-540-31965-8_8. Acesso em maio, 2019.

Gupta, D. D., & Sharma, R. (2016). Blackhole detection and prevention strategies in DTN. *International Journal of Engineering and Computer Science*, 5(8). Disponível em: http://www.ijecs.in/index.php/ijecs/article/view/2091. Acesso em maio, 2019.

Hao-Min, L., Ge Y., Pang, A., & Pathmasuntharam, J. S. (2010). *Performance study on delay tolerant networks in maritime communication environments.* In Oceans'10 IEEE Sydney, 1–6. Disponível em: https://ieeexplore.ieee.org/document/5603627. Acesso em agosto, 2019.

Hinai, A. A., Zhang, H., Chen, Y. (2012). Mitigating blackhole attacks in delay tolerant networks. In 2012 13th *International Conference on Parallel and Distributed Computing,*

Applications and Technologies, pages 329–334. Disponível em: https://ieeexplore.ieee.org/document/6589301. Acesso em junho, 2019.

Khadar, F., & Razafindralambo, T. (2007). Performance evolution of gradient routing strategy for wireless sensor network. In *Proceeding of annual conference of the special Internet Group on Data Communication* (ACM Siggomm '03, 5550, 535–547. Disponível em: https://www.researchgate.net/publication/43107635_Performance_Evaluation_of_Gradient_Routing_Strategies_for_Wireless_Sensor_Networks. Acesso em outubro, 2019.

Lou, W., Liu, W., Zhang, Y., & Fang, Y. (2003). Spread: improving network security by multi-path routing. *In IEEE Military Communications Conference*, 2003. MILCOM 2003, 2, 808–813. Disponível em: https://link.springer.com/article/10.1007/s11276-007-0039-4. Acesso em setembro, 2019.

Mangrulkar, R. S., & Atique, M. (2010). Routing protocol for delay tolerant network: A survey and comparison. In 2010 *International Conference on Communication Control and Computing Technologies*, pages 210–215. Disponível em: https://ieeexplore.ieee.org/document/5670553. Acesso em setembro, 2019.

Mendes, D. R. (2007). *Redes de Computadores*: Teoria e prática. Rio de Janeiro: Novatec.

Navaz, A. S. S., Rex, J., & Mary, P. (2015). An efficient intrusion detection scheme for mitigating nodes using data aggregation in delay tolerant network. *International Journal of Scientific and Engineering Research* 6(9),421-428. Disponível em: https://www.researchgate.net/publication/282331850_An_Efficient_Intrusion_Detection_Scheme_for_Mitigating_Nodes_Using_Data_Aggregation_in_Delay_Tolerant_Network. Acesso em outubro, 2019.

Nunes, C. M., & Dotti, F. L. (2009). Uma nova estratégia de roteamento para redes tolerantes a atrasos. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Disponível em: https://pdfs.semanticscholar.org/02bb/c6c16b37b7bb30446cec80ffd6a8d63908ef.pdf. Acesso em agosto, 2019.

Oliveira, C. T., Taveira, D. M., Braga, R. B., & Duarte, O. C. M. B. (2008). Uma proposta de roteamento probabilístico para redes tolerantes a atrasos e desconexões. In *26 Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Disponível em: http://ce-resd.facom.ufms.br/sbrc/2008/052.pdf. Acesso em outubro, 2019.

Oliveira, C. T., Moreira, M. D. D., Rubinstein, M. G., Costa; L; H. M. K., & Duarte, O. C. M. B. (2007) Redes Tolerantes a Atrasos e Desconexões. Capítulo 5, Minicurso. *25.o Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*. Disponível em: https://www.gta.ufrj.br/ftp/gta/TechReports/OlDu07.pdf. Acesso em junho, 2020.

Pham, D., & Yeo, C. K. (2015). Detecting colluding blackhole and greyhole attack in delay tolerant networks. *IEEE Transactions on Mobile Computing* 15(5):1-1. Disponível em: https://www.researchgate.net/publication/282544907_Detecting_Colluding_Blackhole_and_Greyhole_Attack_in_Delay_Tolerant_Networks. Acesso em outubro, 2019.

Ren, Y., Chuah, M. C., Yang, J., & Chen, Y. (2010). Detecting blackhole attacks in disruption-tolerant networks through packet exchange recording. In 2010 *IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks* (WoWMoM), 1–6. Disponível em: https://ieeexplore.ieee.org/document/5534944. Acesso em outubro, 2019.

Ross, J. (2013). *Redes de computadores*. Rio de Janeiro: Antenna Edicões Técnicas.

Serfozo, P., Vasarhelyi, J., & Turán, J. (2007). *Application of mojette transform in internet distributed databases*. 65 – 70. Disponível em: https://www.researchgate.net/publication/4266052_Application_of_Mojette_Transform_in_Internet_Distributed_Databases. Acesso em outubro, 2019.

Soundaravalli, D. (2017). Identify intrigue blackhole and greyhole attacks in prorogation sophisticated networks. In 2017 *International Conference on Technical Advancements in Computers and Communications* (ICTACC), 160–162. Disponível em: https://ieeexplore.ieee.org/document/8067599. Acesso em maio, 2019.

Tanenbaum, A. S. (2003). *Redes de computadores*. Rio de Janeiro: Campus.

Tsai, J., & Moors, T. (2006). *A review of multipath routing protocols: From wireless adhoc to mesh networks*. Disponível em: http://www2.ee.unsw.edu.au/~timm/pubs/06acorn/published.pdf. Acesso em maio, 2019.

Vieira, A., Filho, C. J., & Patel, A. (2013). Vdtn-tod: Routing protocol vanet/dtn ba-sed on trend of delivery. *Advanced International Conference on Telecommunications*, AICT, 2013, 135–141. Disponível em: https://www.researchgate.net/publication/288727744_VDTN-ToD_Routing_protocol_VANETDTN_based_on_trend_of_delivery. Acesso em agosto, 2019.

Porcentagem de contribuição de cada autor no manuscrito

Rodrigo Perlin – 50%

Ricardo Tombesi Macedo – 20%

Sidnei Renato Silveira – 10%

Antonio Rodrigo Delepiane de Vit – 10%

Roberto Franciscatto – 10%