Um mecanismo distribuído de incentivo baseado em crédito para redes oportunistas

Daniel de M. C. Christiani[1], **Antônio Augusto de A. Rocha**[2], **Carlos A. V. Campos** [1]

[1]Programa de Pósgraduação em Informática (PPGI)
Universidade Federal do Estado do Rio de Janeiro (UNIRIO)
Rio de Janeiro – RJ – Brasil

[2]Instituto de Computação
Universidade Federal Fluminense (UFF)
2420-240 Niterói – RJ – Brasil

Abstract. *Incentive mechanisms are increasingly needed in opportunistic networks that contain nodes with selfish behavior. For this, there are mechanisms based on credit but, that need a virtual bank (central entity) to promote the incentive. However, the existence of this central entity in an opportunistic network may not be possible. Therefore, a credit incentive mechanism is proposed in this paper. The main contribution is that the mechanism does not use a virtual bank for the distribution of credits (reward for forwarding messages), but rather a decentralized approach. In addition, it was proposed a mathematical modeling to represent the collection and distribution of credits in order to avoid Edge Insertion attacks, in certain cases. Finally, the proposed mechanism was evaluated through simulation using real mobility traces and different routing protocols, and compared its performance with the RELICS incentive mechanism. Based on the results obtained we can say that the proposed mechanism is promising in the sense of diminishing the occurrence of selfish nodes.*

Resumo. *Mecanismos de incentivo são cada vez mais necessários em redes oportunistas que contém nós com o comportamento egoísta. Para isso, existem mecanismos baseados em crédito mas, que necessitam de uma banco virtual (entidade central) para promover o incentivo. Entretanto, a existência desta entidade central em uma rede oportunista pode não ser possível. Sendo assim, neste artigo é proposto um mecanismo de incentivo baseado em créditos. A principal contribuição é o fato do mecanismo não utilizar um banco virtual para a distribuição dos créditos (recompensa pelo encaminhamento das mensagens), mas sim uma abordagem descentralizada. Além disso, foi proposta uma modelagem matemática para representar a cobrança e distribuição de créditos buscando evitar ataques do tipo Edge Insertion, em determinados casos. Por fim, o mecanismo proposto foi avaliado, via simulação, utilizando traces reais de mobilidade e diferentes protocolos de roteamento, e comparado seu desempenho com o mecanismo de incentivo RELICS. Com base nos resultados obtidos podemos dizer que o mecanismo proposto é promissor no sentido de diminuir a ocorrência de nós egoístas* [1].

[1]O primeiro autor deste trabalho foi bolsista da CAPES ao longo do seu curso de mestrado.

1. Introdução

Para cenários de redes de computadores sem fio que apresentem longos atrasos e frequentes desconexões, a arquitetura TCP/IP pode não funcionar adequadamente. Por isso, novas arquiteturas e protocolos de redes são necessários. Uma destas novas abordagens são as redes oportunistas e um dos seus principais desafios é o roteamento das mensagens, uma vez que nestes cenários é necessário determinar rotas sem o estabelecimento de um caminho fim-a-fim entre a origem e o destino [Seregina et al. 2017].

O problema de desconexões frequentes pode ocorrer em redes oportunistas devido a diferentes fatores, como por exemplo, a mobilidade ocasionada pelas constantes mudanças na topologia da rede, pela necessidade de economia de recursos, restrição de disponibilidade de serviços ou outra característica particular da rede em questão [Junior and Campos 2015].

Para realizar a transferência de uma informação, esta mensagem deve ser armazenada e encaminhada nó a nó desde a origem até o destino, ou seja, é utilizada uma técnica, conhecida nestes cenários como armazena-carrega-e-encaminha (*store-carry-and-forward*). Na qual primeiro a mensagem é recebida integralmente e armazenada para que seja possível seu envio ao próximo nó, que pode ou não ser o destino [Zhu et al. 2013].

Para compensar o gasto de recursos dos dispositivos utilizados nessas redes, são utilizados mecanismos de incentivo [Shevade et al. 2008, Wang et al. 2014, Seregina et al. 2017, Ning et al. 2017], como por exemplo, o pagamento aos nós envolvidos na transmissão da informação como forma de incentivo. Para isso, foi criada uma unidade centralizadora com o objetivo de gerenciar as chamadas moedas virtuais. Porém, essa unidade não condiz com uma das principais características das redes oportunistas. Uma vez que essas redes sofrem com as frequentes desconexões, a dependência de uma entidade externa se torna um fator negativo.

A motivação deste artigo vem da necessidade de um mecanismo de incentivo que dispense a necessidade de uma unidade centralizadora externa a uma rede oportunista para utilização de moedas virtuais sem perda de confiabilidade, sendo resistente a possíveis ataques de nós maliciosos.

Embora a existência desta entidade centralizadora pareça a solução para os problemas referentes à segurança do mecanismo de moedas virtuais ela torna a rede oportunista, uma rede distribuída, dependente dela, ou seja, caso aconteça algo a esta entidade toda a transmissão de mensagens entre os nós da rede é afetada.

Por outro lado a utilização de moedas virtuais é um eficiente mecanismo de incentivo, sendo necessário um estudo da viabilidade de fazê-lo, sem que aconteça perda da consistência da informação referente a estas moedas, por meio de ataques de nós maliciosos na rede em que a mensagem está sendo transmitida.

O presente artigo aborda os diferentes tipos de mecanismos de incentivo para redes sem fio e a mitigação dos efeitos do egoísmo, além do problema do gasto duplo (*double spending*). Como objetivo principal, é proposto um novo mecanismo de incentivo baseado em créditos no qual não seja necessária a existência de uma entidade centralizadora. Além disso, o mecanismo proposto foi implementado em um simulador de redes tole-

rantes a atraso e é realizada uma comparação entre como é feito um encaminhamento de mensagens através de protocolos de roteamento, pelos quais, nós egoístas se recusam a encaminhar mensagens, e como os mecanismos de incentivo atuam para melhorar esta entrega, para que seja possível demonstrar o funcionamento e o desempenho do mecanismo proposto. Nesta comparação foram abordadas as métricas referentes não só em relação à fração de entrega, mas também em relação ao atraso médio e a sobrecarga de mensagens(*overhead*) durante o encaminhamento dessas mensagens.

Este artigo se divide em 5 seções, sendo a primeira a Introdução. Na Seção 2 será apresentado o conceito de egoísmo em redes oportunistas e também alguns exemplos de mecanismos de incentivo presentes na literatura. Na Seção 3 é proposto um mecanismo de incentivo distribuído baseado em créditos, com o seu sistema de pagamento e uma formalização matemática. Na Seção 4 serão apresentados os resultados obtidos. As conclusões e propostas para trabalhos futuros se encontram na Seção 5.

2. Egoísmo e mecanismos de incentivo

As redes DTNs são muitas vezes compostas por dispositivos utilizados por pessoas racionais e que nem sempre escolhem colaborar de forma altruística. Assim, como os dispositivos utilizados são portáteis e costumam acompanhar a mobilidade humana, foram desenvolvidos protocolos de roteamento que se aproveitam de características baseadas em um contexto social [Junior and Campos 2015], como amizade, comunidade e principalmente o egoísmo [Zhu et al. 2013]. O egoísmo em redes oportunistas pode ser definido como a recusa de um nó em gastar os seus recursos, como bateria e largura de banda, ao invés de trabalhar cooperativamente com outros nós em uma rede. Em [Chen and Chen 2007] são estabelecidos pelo menos 3 conceitos muito utilizados pela literatura sobre o comportamento dos nós, sendo eles:

1. Nós Colaborativos: são os nós que compartilham os recursos durante o encaminhamento da mensagem passando as informações verdadeiras.
2. Nós Egoístas: são os nós que não compartilham recursos durante o encaminhamento de mensagens.
3. Nós Maliciosos: são nós que corrompem o sistema com informações inválidas durante um ataque a rede.

Para mitigar os efeitos do egoísmo, foram propostos diversos mecanismos de incentivo pela literatura. Estes mecanismos buscavam alcançar este objetivo de duas formas: a primeira forma seria identificar os nós que se comportarem de forma egoísta e ou removê-los da rede, ou negá-los o serviço de encaminhamento de mensagens. A segunda forma seria incentivar a colaboração dos nós, impedindo que seja possível que qualquer nó se beneficie com um comportamento egoísta. Como é uma tarefa muito difícil e custosa identificar nós egoístas em uma rede oportunista, a segunda abordagem tem sido a mais utilizada pela literatura.

Os mecanismos de incentivo foram criados para compensar o gasto de recursos dos nós e para incentivar a colaboração em redes oportunistas podem ser divididos em três categorias: (i) - os mecanismos de incentivo baseados em *tit-for-tat*, (ii) - baseados em reputação e (iii) - os mecanismos de incentivo baseados em créditos ou moedas virtuais.

Os mecanismos baseados em *tit-for-tat* são modelados em uma relação entre cada par de nós, ou seja, um nó irá transmitir os pacotes de outro nó na mesma medida que

tem seus pacotes transmitidos. O problema desta abordagem ocorre quando dois nós acabam de se encontrar. Como ambos não possuem conhecimento prévio um sobre o outro, e nenhum pacote foi transmitido entre os mesmos, não é possível estabelecer se o outro nó irá cooperar, e caso ambos os nós decidam esperar que seus pacotes sejam transmitidos primeiro antes de cooperarem, nenhum pacote será transmitido na rede. [Shevade et al. 2008] apresenta dois conceitos relacionados aos nós envolvidos na transmissão de mensagens, o conceito de generosidade, que consiste no fato de um nó encaminhar um determinado número de pacotes antes de retaliar um possível nó egoísta e o conceito da contrição, mecanismo para evitar que dois nós parem de transmitir pacotes um do outro devido a uma retaliação mútua. Assim, um nó é capaz de perceber que a redução do encaminhamento de suas mensagens foi causada por uma ação egoísta passada, e por isso não retalia de volta.

Os mecanismos de incentivo baseados em reputação utilizam uma métrica para estimar o grau de colaboração de um determinado nó na rede, ou seja, quanto mais colaborativo o nó, maior a sua reputação [Zhu et al. 2013]. Nessa proposta cada nó mantém o controle dos pacotes que o mesmo tenha enviado a um vizinho particular. Porém, esta técnica acaba por enfrentar o problema da grande separação espacial entre o encaminhamento de mensagens sucessivas em redes oportunistas, uma vez que é significativamente difícil verificar se um determinado pacote foi ainda transmitido ou não [Uddin et al. 2010].

Segundo [Zhu et al. 2013] os esquemas baseados em crédito visam introduzir uma forma para regular as relações de pacotes de encaminhamento entre os nós diferentes, os quais recebem esta moeda virtual por meio dos envios de pacotes feitos para os outros nós. Para cada pedido de encaminhamento, o banco virtual cobra ao remetente uma quantidade extra desta moeda virtual, e os nós intermediários resgatam suas recompensas em algo que funciona como um banco após a entrega destes pacotes ser bem-sucedida. Esta técnica muitas vezes é utilizada para incentivar os nós egoístas. No entanto, estes mecanismos de incentivo necessitam de um banco virtual para realizar as operações de cobrança e recompensa entre os nós.

O presente artigo busca propor uma solução para este problema através de um mecanismo de incentivo baseado em créditos que possa ser realizado de forma descentralizada pelos nós de uma rede oportunista.

3. O mecanismo proposto

O trabalho aqui apresentado propõe uma abordagem semelhante à utilizada nas redes de BitCoins[2], para solucionar o problema apresentado na seção anterior e também para descrever como estas moedas serão geradas e mantidas pelo sistema. Ou seja, esta proposta visa criar um mecanismo de incentivo baseado em créditos, apresentando como diferencial a não utilização de um banco virtual. Essas moedas virtuais, geradas a partir da retransmissão de mensagens na rede, serão utilizadas para recompensar os nós que trabalharem de forma cooperativa.

O mecanismo proposto, a partir daqui, chamaremos de DiCent (*DIstributive inCENTive*). Nas seguintes subseções apresentaremos o sistema de pagamento para os

[2]O BitCoin é uma moeda virtual que foi proposta por um hacker, ou um grupo de hackers sob o pseudônimo de Hatoshi Sakamoto. Por funcionar de maneira descentralizada, algumas de suas características serão utilizadas nesta proposta.

créditos, a descrição do funcionamento do DiCent e uma formulação matemática para demonstrar a validade do mecanismo proposto.

3.1. Sistema de pagamento

Para tratar o pagamento de créditos como incentivo aos nós retransmissores, o mecanismo proposto utilizou as equações apresentadas por [Chen and Chan 2010] no desenvolvimento do MobiCent para garantir a cooperação dos nós, e evitar ataques de *edge insertion* pelos nós retransmissores. Os detalhes matemáticos de como serão realizadas o pagamento e a cobrança de créditos estão descritas na subseção da formalização matemática do mecanismo proposto.

Os créditos serão distribuídos conforme o algoritmo MDR apresentado em MobiCent [Chen and Chan 2010]. O mecanismo proposto não realiza uma distribuição de moedas prévia. Conforme exista uma lista de mensagens para ser enviada, o mecanismo verifica se o nó que receberá a mensagem não gastará nenhum crédito (ou seja, início da rede) e assim, enquanto não for atingido um valor máximo fixado em 4100 moedas, os nós destinatários continuarão gerando créditos. Quando o número de moedas criadas atingirem o valor máximo, o incentivo a colaboração será realizado através da troca de moedas entre os nós da rede, sendo que a mensagem apenas será enviada caso o nó destino tenha créditos suficientes para recompensar os nós retransmissores.

Para receber o seu pagamento, um nó deverá analisar todas as transações que estão em seu registro. Se o nó estiver na lista de nós retransmissores, o mesmo irá somar o número de créditos oferecidos como recompensa. Se o nó for o nó destino, deverá diminuir uma quantidade de créditos igual ao pago, ou seja, enquanto houver nós retransmissores, todas as transações terão seus créditos atualizados. Este procedimento também ocorrerá com os outros nós que participarem da transação, para que o nó que está atualizando os créditos saiba quantos créditos cada nó possui, ou seja, independente de ser o nó emissor, o nó destino, ou mesmo um nó retransmissor, deverá ocorrer atualização no registro do mesmo com estas informações, e caso seja um novo nó na retransmissão, o mesmo deverá ser incluído na lista de nós.

3.2. O funcionamento do mecanismo DiCent

O funcionamento do mecanismo proposto começa após receber do protocolo de roteamento a lista de mensagens a serem enviadas reorganizada conforme a política predeterminada pelo protocolo de roteamento utilizado. Para poder funcionar corretamente, o mecanismo proposto necessita que o protocolo de roteamento forneça as informações sobre o número de saltos percorrido pela mensagem até a entrega e a lista de nós retransmissores. Essas informações são necessárias para a distribuição da recompensa e a cobrança do nó destino, assim como é realizado nos mecanismos de incentivo MuRIS e MobiCent.

O mecanismo proposto realiza uma comparação do *registro* dos nós envolvidos na transmissão da mensagem. Estes *registros* (implementados como uma lista de transações) contêm a gravação do histórico de transações para que os nós possam ter controle de todos os créditos existentes na rede, de forma distribuída e autônoma, a qual é semelhante às tabelas de rank utilizadas por [Uddin et al. 2010], no RELICS. Essa comparação inicial é realizada para que, ao trocar as informações sobre os registros, os nós tenham o conhecimento do número de créditos que um nó vizinho tem antes de enviar uma mensagem. Isto

tem por objetivo impedir que um nó receba uma mensagem mesmo sem ter créditos para pagar pelo recebimento.

Para isso, foi implementada a classe *transações* contendo as informações acerca de quais nós participaram do encaminhamento da mensagem, o momento da entrega da mensagem e também da quantidade de créditos que foram pagos e recebidos como recompensa pela entrega da mensagem. Para saber quantos créditos um nó possui, deve-se olhar em todas as transações, em quais delas o nó participou como retransmissor e em quais o mesmo foi o destino da mensagem. Ao somar os créditos ganhos, e subtrair os créditos perdidos, é possível determinar quantas moedas o nó possui, e assim tomar a decisão de encaminhar ou não a mensagem.

O mecanismo proposto realiza as seguintes verificações antes de entregar a mensagem ao nó destinatário: (i) - a possibilidade de serem criados novos créditos, (ii) - a existência de créditos para pagar pela transmissão da mensagem e (iii) - o número de saltos já percorridos pela mensagem.

Por sua vez, o nó destinatário envia uma lista com as informações referentes às mensagens já entregues, antes da entrega da mensagem, para que possa calcular a quantidade de créditos a ser paga aos nós que participaram da operação. Antes de enviar uma mensagem ao nó destinatário, caso todas as verificações sejam bem sucedidas, o mecanismo solicita ao protocolo de roteamento que a mensagem seja entregue, e essa operação é incluída no *registro*.

A mensagem deverá conter informações necessárias para inserir a *transação* no *registro*, como informação do nó emissor, a lista de nós retransmissores e o momento em que a mensagem foi entregue, para que o mecanismo possa funcionar de forma distribuída. Caso a mensagem seja enviada com sucesso, os dois nós deverão inserir esta operação em seus *registros*. Se a conexão entre os nós cair antes do fim da transmissão de uma mensagem, a operação não será incluída no *registro*. Se a transmissão for efetuada com sucesso, ambos os nós poderão adicionar a operação mesmo que a conexão caia logo em seguida, já que as suas cópias da mensagem possuem todas as informações necessárias para isto.

O mecanismo proposto possui algumas restrições: controle da quantidade de saltos que uma mensagem poderá tentar durante a transmissão da mensagem em 6 saltos, limite de criação de 64 créditos por hora créditos. O objetivo destas restrições é prevenir que um nó ataque a rede gerando uma quantidade muito grande de créditos, e impedindo que os outros nós recebam as suas mensagens.

Um grande problema do mecanismo proposto está no fato de que para impedir que os nós destino sejam beneficiados com um ataque de *Edge Insertion* seria necessário cobrar dos nós destino uma quantidade de moedas virtuais superior do que a quantidade de moedas que será distribuída como incentivo para os nós retransmissores. Isto causaria uma redução da quantidade de créditos existentes na rede. Esta perda de créditos obrigaria o mecanismo de incentivo a estar sempre criando novas moedas para suprir as que foram perdidas.

3.3. Modelagem e formalização matemática

Para demonstrar a validade do mecanismo DiCent, assim como provar que o mecanismo proposto incentiva a colaboração dos nós, e não permite que os nós retransmissores se beneficiem com um ataque do tipo *Edge Insertion*, foi feita uma formalização matemática nesta seção.

O mecanismo proposto utilizará uma fórmula baseada nos lemas e teoremas desenvolvidos por [Chen and Chan 2010] e [Wang et al. 2014].

Para validar matematicamente o mecanismo proposto, neste trabalho, utilizaremos as seguintes definições:

N = Número máximo de nós que podem participar da entrega da mensagem, onde: $\forall N \in \mathbb{N}$ e $N > 1$.

n = Número de nós que efetivamente participaram da entrega da mensagem, onde $\forall n \in \mathbb{N}$ e $N \geq n \geq 1$

$R_{(n)}$: Recompensa que cada nó receberá se n nós participarem da retransmissão.

$C_{(n)}$: Quantidade de créditos cedidos pelo nó destino aos nós retransmissores, se n nós participarem da retransmissão.

Para cada nó que participar da entrega da mensagem a recompensa é igual a:

$$\mathbb{R}_{(n)} = 2^{N-n} \tag{1}$$

Cobrança do nó destino: O nó destinatário deverá pagar uma quantidade de créditos exatamente igual à soma dos valores recebidos como recompensa oferecida a todos os nós retransmissores.

$$\mathbb{C} = \sum_{i=0}^{n} \mathbb{R}_i \tag{2}$$

Exemplo: Partindo do pressuposto que o total de nós N = 10 e o total dos nós participantes são $n = 4$, a quantidade de créditos recebidos como recompensa por cada nó retransmissor é $210 - 4 = 26 = 64$ créditos.

3.4. Teoremas

Teorema 1: *Para impedir que os créditos sejam criados de forma descontrolada, causando uma perda do valor dos créditos, ou que os créditos sejam perdidos durante o pagamento do incentivo, o valor cobrado ao nó destino será sempre igual ao valor oferecido como recompensa a todos os nós que efetivamente participaram da retransmissão da mensagem.*

Prova: Base da Indução: Como base para a indução matemática, utilizaremos um valor de $n = 1$. Substituindo este valor na equação anterior temos como base para a indução $2^{N-1} = 1 \times 2^{N-1}$. Como esta equação é verdadeira para qualquer valor de N, a Base da Indução está validada.

Hipótese Indutiva:

$$\sum_{k=1}^{K} 2^{N-k} = k \times 2^{N-k} \tag{3}$$

Prova de $k+1$: Ao substituir o k na Hipótese Indutiva por $k+1$, temos que:

$$\sum_{k=1}^{k+1} 2^{N-(k+1)} = (k+1)2^{N-(k+1)} \tag{4}$$

Resolvendo o somatório, temos $(k+1) \times 2^{N-(k+1)}$. Assim, igualamos a primeira parte com a segunda parte da igualdade, e temos que $(k+1) \times 2^{N-(k+1)} = (k+1)2^{N-(k+1)}$. Como esta equação é verdadeira para qualquer valor de k, o Teorema 1 está provado como gostaríamos de demonstrar.

Teorema 2: *Os nós retransmissores não devem ter incentivo ao utilizar um ataque de Edge Insertion.*

Lema 1: Para que um nó retransmissor não seja incentivado a utilizar um ataque de Edge Insertion, $R_{(n)} \geq R_{(n+1)}$.

Prova do Lema 1: Como visto nas definições, a recompensa recebida por cada nó retransmissor é de $R_{(n)}$. Ao utilizar um ataque de Edge Insertion, o nó atacante irá inserir um nó sybil na lista de nós retransmissores para ganhar uma quantidade de créditos como recompensa igual a soma obtida pelo nó atacante e o nó sybil. Com a inserção do nó sybil, o número de nós retransmissores aumentou para $(n+1)$. Com isso, a recompensa obtida por cada nó mudou para $R_{(n+1)}$. Para que o nó atacante não se beneficie, a quantidade de créditos recebida pelo nó atacante mais a quantidade de créditos recebida pelo nó sybil deve ser igual ou menor do que a quantidade que o nó receberia se não utilizasse o ataque, ou seja:

$$\mathbb{R}_{(n)} \geq \mathbb{R}_{(n+1)} \tag{5}$$

Prova: Prova por indução: Para a base da prova por indução matemática será utilizado $n = 1$. Substituindo os valores nas equações anteriores temos: $2^{N-1} \leq 2 \times 2^{N-(1+1)}$. Diminuindo em 1 o expoente da primeira parte da inequação, colocando o número 2 em evidência, temos $2 \times 2^{N-2} \leq 2 \times 2^{N-2}$, o que valida a base da indução.

Para a hipótese indutiva será utilizada a inequação $2^{(N-k)} \leq 2 \times 2^{N-(k+1)}$.

Para a prova de $K+1$, na inequação e $2^{N-(k+1)} \leq 2 \times 2^{N-(k+2)}$ basta novamente modificar a primeira parte da inequação para $2 \times 2^{N-(k+2)} \leq 2 \times 2^{N-(k+2)}$ provando o teorema como queríamos demostrar.

Teorema 3: *O nó destino não deve ter incentivo ao utilizar um ataque de Edge Insertion.*

Prova: Como o mecanismo proposto não é capaz de impedir que o nó destino se beneficie com um ataque de Edge Insertion, será fornecido um contra exemplo para demonstrar isto.

Contra exemplo: Supondo que $n = 2$ e $N = 5$. A recompensa recebida por cada nó que participar da retransmissão será de $2^{5-2} = 8$. A cobrança do nó destino será de 16 créditos. Ao realizar o ataque, a recompensa cedida a cada nó será de $2^{5-3} = 4$, e a cobrança será de 12 créditos. Como a cobrança do nó destino ao realizar o ataque é menor do que a cobrança ao não realizar o ataque, o mecanismo é capaz de impedir que o nó destino se beneficie com um ataque de Edge Insertion, como queríamos demonstrar.

Teorema 4: *Nenhum nó deve ser incentivado a realizar ciclos no encaminhamento da mensagem.*

Prova: Para demonstrar que nenhum nó poderia se beneficiar com este tipo de ataque, deve-se considerar que cada nó receberá 2^{N-n} como recompensa. Caso a mensagem seja repassada duas vezes por todos os nós do ciclo, ao invés de apenas uma vez, o número de nós retransmissores será aumentado em k. Com isto, cada nó retransmissor receberia $2^{N-(n+k)}$ de recompensa, e os nós do ciclo receberiam $2 \times 2^{N-(n+k)}$, que é igual à $2^{N-(n+k-1)}$.

Ciclo de um nó $(k = 1)$:

Se $k = 1$, a recompensa recebida será de 2^{N-n} que é a mesma recompensa que o nó receberia sem o ciclo.

Ciclo de mais de um nó $(k > 1)$:

Se $k > 1$, a recompensa recebida pelo no será de $2^{N-(n+k-1)}$. Como $2^{N-n} \geq k \times 2^{N-(n+k+1)}$, o nó não poderá se beneficiar com a criação de ciclos. Como não é possível que um nó receba mais créditos com a criação de um ciclo, nenhum nó irá ser adicionado mais de uma vez na lista de nós retransmissores, como queríamos demonstrar.

3.5. Algoritmo de incentivo dos nós

Quando um nó da rede proposta entrar em contato com um nó vizinho, cada um deles irá trocar informações sobre as operações já realizadas na rede e atualizar o seu registro de operações.

1. Ao estabelecer uma conexão com um nó vizinho, cada nó da rede irá requisitar as mensagens a serem enviadas pelo protocolo de roteamento.
2. Estas mensagens serão então ordenadas de acordo com parâmetros definidos pelo protocolo de roteamento, e com a recompensa esperada com a entrega da mensagem.
3. As mensagens serão então transmitidas criptografadas.
4. Quando uma mensagem chegar ao nó de destino, este irá enviar moedas para todos os nós que participaram da retransmissão. O nó de origem e os outros nós que participaram da retransmissão irão enviar as chaves necessárias para descriptografar a mensagem.

4. Avaliação de desempenho

Esta seção apresenta uma avaliação, via simulação, do mecanismo DiCent para avaliar a sua efetividade e compará-lo com outros mecanismos de incentivo da literatura. Nesta avaliação será usado o simulador de redes oportunistas ONE [Keränen et al. 2009], no qual foi implementado o mecanismo DiCent. Assim, a avaliação fará uso do protocolo

de roteamento Prophet, de traces realísticos de contato de usuários sem fio e comparará o desempenho do DiCent com o mecanismo RELICS que foi usada a implementação disponibilizada pelos seus autores do RELICS.

Os traces de contato foram extraídos do projeto CRAWDAD para simular a movimentação e contato de usuários em uma conferência. Assim, o dataset INFOCOM 05 [Scott et al 2006], extraído durante a IEEE INFOCOM'2005, cuja coleta de dados representou o movimento de 41 nós no período entre os dias 7 e 10 de Março de 2005. A respeito da carga de mensagens na rede, foram criadas 1000 mensagens ao longo da simulação, cada uma com 2,5 KB de tamanho. O buffer dos nós que compõem a rede foi definido como 100MB, para evitar que houvesse descarte de mensagens por sobrecarga do mesmo. O tempo de vida (TTL) avaliado para cada mensagem foi de 15h, 24h, 36h, 48h e o tempo total de simulação foi de 275.000 segundos (quase 77 horas).

4.1. Métricas de desempenho

As métricas escolhidas para comparação entre os mecanismos de incentivo foram a fração de entrega, o atraso médio e o overhead. Estas métricas são normalmente usadas na avaliação de redes tolerantes a atraso ou oportunistas [da Nóbrega Gomes et al. 2017].

Fração de entrega da mensagem: razão entre as mensagens que foram entregues aos nós destinos e as mensagens que foram efetivamente criadas pelos nós emissores. Portanto, as cópias das mensagens que foram criadas durante o processo de encaminhamento pelos nós retransmissores não são contadas por esta métrica.

Overhead (sobrecarga) médio de mensagens: mede quantas mensagens foram criadas pelos nós retransmissores para que as mensagens sejam entregues. Essa métrica é calculada ao diminuir a quantidade de mensagens retransmitidas (messages relayed) pelo número de mensagens entregues, e então dividir o resultado pelo número de mensagens entregues.

Atraso médio na entrega da mensagem: média entre o intervalo de tempo entre o momento em que uma mensagem é criada até o momento em que a mesma é entregue. Assim, primeiro é calculado o atraso de cada pacote, subtraindo o tempo em que a mesma foi entregue do momento em que a mesma foi criada. Este valor de atraso é somado para cada mensagem entregue, e depois, a soma dos atrasos individuais é dividida pelo número de mensagens entregues.

4.2. Resultados obtidos

O intuito da avaliação foi comparar o comportamento dos mecanismos de incentivo em relação ao cenário no qual é considerado o comportamento de nós egoístas. Para representar a ação de nós egoístas durante as simulações, foram utilizados nós frugais (Frugal nodes), assim como nos trabalhos [Shevade et al. 2008, Uddin et al. 2010]. Estes nós apresentam uma quantidade extrema de egoísmo, e apenas retransmitem suas próprias mensagens, se recusando a enviar mensagens que tenham sido criadas por outros nós. Em [Shevade et al. 2008], é dito que, caso todos os nós sejam frugais, o comportamento da rede se degenera, e a entrega de mensagens ocorre apenas de forma direta, ou seja, as mensagens apenas seriam entregues caso o destino entre em contato com o emissor.

Como este cenário seria compatível com o uso do protocolo de roteamento por entrega direta, e não representaria um cenário em que apenas alguns nós apresentariam um

comportamento egoísta, para ilustrar o efeito do egoísmo nos protocolos de roteamento foi utilizado o mesmo padrão de egoísmo apresentado por [Uddin et al. 2010]. No presente trabalho, os nós múltiplos de 5, começando pelo nó 0, foram escolhidos para serem nós frugais. Este número de nós frugais foi escolhido pois, caso o número de nós egoístas fosse muito reduzido, os efeitos dos nós egoístas na rede não seriam tão evidentes. Da mesma forma, caso o número de nós egoístas fosse muito grande, a rede se comportaria de forma idêntica ao uso do protocolo de roteamento por entrega direta, não permitindo observar a diferença entre os efeitos do egoísmo nos diferentes protocolos de roteamento.

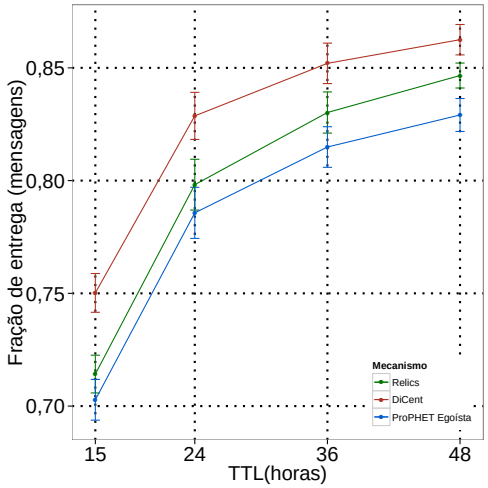

Figura 1. Média da fração de entrega utilizando o protocolo de roteamento ProPHET junto com os mecanismos de incentivo DiCent e RELICS

Como é possível observar na Figura 1, o mecanismo DiCent apresentou uma maior fração de entrega em relação à apresentada pelo mecanismo RELICS e pelo protocolo de roteamento ProPHET na presença de nós egoístas. Também é possível observar que, embora a média da fração de entrega apresentada pelo ProPHET na presença de nós egoístas tenha coincidido com a fração de entrega de mensagens do mecanismo RELICS, dentro da margem de erro utilizada, o mecanismo RELICS apresentou uma tendência a apresentar uma fração de entrega maior do que a apresentada pelo ProPHET com nós egoístas, o que se confirmou nas simulações realizadas com um TTL de 48 horas. Isto indica que, com esta quantidade de nós frugais, o incentivo realizado pelo mecanismo RELICS, dada a margem de erro e no trace de mobilidade utilizado para estas simulações, apenas pode ser considerado benéfico para a fração de entrega ao se utilizar um valor de TTL próximo ou maior do que 48 horas.

Já o mecanismo DiCent, apresentou uma maior fração de entrega do que o mecanismo RELICS em todos os cenários ilustrados pelo gráfico, mesmo considerando o intervalo de confiança de 95%. Isto mostra que as limitações causadas pelo rank do RELICS impediram que mais mensagens fossem entregues do que a distribuição de créditos do DiCent. Outra observação a ser feita é que, em todos os cenários ilustrados pela Figura 1, houve um grande aumento da fração de entrega entre as simulações realizadas com um TTL de 15 horas e de 24 horas. Isso indica que, ao aumentar o TTL dentro deste intervalo de tempo, houve muitas novas oportunidades de contato para a entrega da mensagem, o que provocou o aumento observado. Embora ainda tenha havido um aumento

da fração de entrega até as simulações utilizando um TTL de 48 horas, a diferença entre as frações de entrega apresentadas entre as simulações com um TTL de 48 e 36 horas foram inferiores às observadas com um TTL entre 15 e 24 horas. Isso indica que, no trace de mobilidade utilizado, não houve um aumento expressivo das oportunidades de transmissão de mensagens ao se utilizar um TTL acima de 24 horas. Como os nós no mecanismo RELICS começam com um valor de rank que permitiria apenas o envio de duas mensagens, e o DiCent permite que os nós enviem um número maior de mensagens ao criar créditos, o mecanismo proposto mostrou-se capaz de permitir uma maior fração de entrega de mensagens do que a utilização do rank de nós usando o RELICS.

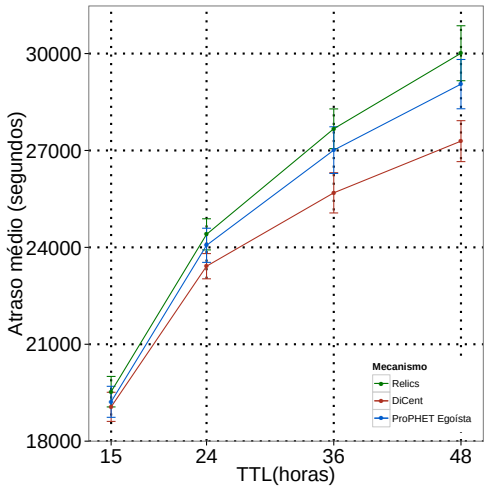

Figura 2. Atraso médio na entrega de mensagens utilizando o protocolo ProPHET junto com os mecanismos de incentivo DiCent e RELICS.

A segunda métrica analisada foi o atraso médio. Como pode ser observado na Figura 2, o atraso médio apresentado pelo protocolo de roteamento ProPHET com nós egoístas e o apresentado pelos mecanismos de incentivo DiCent e RELICS apresentaram resultados dentro do intervalo de confiança ao se utilizar um TTL de 15 e 24 horas. No entanto, o gráfico ilustra uma tendência de que, ao aumentar o TTL, o mecanismo de incentivo RELICS apresentaria um valor de atraso médio superior ao do protocolo de roteamento ProPHET com nós frugais, e o mecanismo proposto apresentaria um valor de atraso médio inferior ao RELICS e ao ProPHET, tendência esta que foi confirmada nas simulações com um TTL de 48 horas. Como no mecanismo RELICS as mensagens são enviadas de acordo com uma prioridade estabelecida pelo rank do nó emissor, ao contrário do mecanismo proposto, que prioriza mensagens com um menor número de saltos, o mecanismo DiCent, neste cenário entregou primeiro mensagens que possuíam um atraso médio inferior às que foram entregues pelo mecanismo RELICS, já que é possível que algumas mensagens que foram priorizadas pelo mecanismo RELICS, por terem um nó emissor com rank elevado, possuíam um número de saltos mais alto do que as mensagens entregues pelo mecanismo proposto, e também um maior valor de atraso. Conforme foi aumentando o tempo de vida dos pacotes, novas oportunidades de entrega foram surgindo, independente do mecanismo. No entanto, devido à característica do mecanismo RELICS de priorizar as entregas onde há um ganho de reputação maior, ao invés do DiCent que sempre prioriza os caminhos mais curtos, a diferença entre o atraso dos dois mecanismos

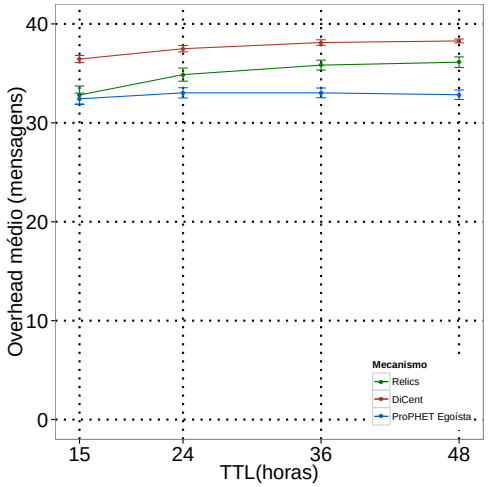

Figura 3. Overhead médio na entrega de mensagens utilizando o protocolo de roteamento ProPHET junto com os mecanismos de incentivo DiCent e RELICS.

tende a aumentar junto com o tempo de vida dos pacotes.

Como pode ser observado na Figura 3, o comportamento egoísta dos nós frugais utilizando o protocolo ProPHET impediu que o valor de overhead médio ultrapassasse uma média de 33 mensagens, já que os nós egoístas descartaram todas as mensagens que chegaram até eles. Embora o overhead encontrado nas simulações realizadas com o mecanismo de incentivo RELICS e um TTL de 15 horas tenham sido bem próximas às encontradas com as simulações do ProPHET com nós egoístas, o overhead médio encontrado ao se utilizar o mecanismo de incentivo RELICS apresentou um valor crescente quando o TTL foi aumentado.

O mecanismo DiCent também apresentou a mesma tendência de aumento, mas apresentou valores de overhead superiores aos encontrados pelo mecanismo RELICS. Isto mostra que, ao custo de criar uma quantidade maior de mensagens, o mecanismo proposto conseguiu uma fração de entrega maior, e também entregar estas mensagens com um atraso menor. Este número maior de mensagens criadas pelo mecanismo DiCent está ligado ao limite máximo de saltos, ou seja, quanto maior a quantidade máxima de saltos que uma mensagem possa realizar, maior será o overhead. O limite máximo para a quantidade de mensagens criadas, caso haja créditos suficientes, seria o mesmo gerado pelo protocolo de roteamento epidêmico. Além disso, o fato de que o RELICS criou uma quantidade menor de mensagens, mesmo que ambos os mecanismos tenham utilizado o ProPHET como protocolo de roteamento, pode ser explicado pelo fato de que as mensagens com um nó de origem com um rank igual ou inferior a 1 não foram retransmitidas pelos nós que utilizaram o mecanismo RELICS.

5. Conclusão e trabalhos futuros

Neste artigo foi proposto um mecanismo de incentivo que é capaz de utilizar uma abordagem de incentivo por créditos de maneira distribuída, sem a necessidade de um banco virtual para gerenciar as transações realizadas entre os nós. No lugar deste banco virtual foi proposto um registro contendo todas as transações realizadas entre os nós, onde é possível descobrir quantas moedas cada nó possui antes de enviar uma mensagem.

Através do modelo matemático apresentado na Seção 3 para o pagamento de créditos foi possível demonstrar que ao utilizar o mecanismo proposto nenhum nó retransmissor poderia se beneficiar ao utilizar um ataque de *Edge Insertion*. No entanto, evitar que o nó destino se beneficie por este ataque sem que haja uma perda de créditos ainda é um desafio.

Como um trabalho futuro, pretendemos analisar a criação e perda de moedas em uma rede em que os nós possam entrar e sair a qualquer momento. Este cenário também seria um grande desafio quanto à segurança e autenticação dos nós, já que isso também teria de ser feito pelos nós da rede, de forma descentralizada. Também pretendemos realizar simulações envolvendo outros traces de mobilidade e protocolos de roteamento, para avaliar os efeitos no mecanismo DiCent.

Referências

Chen, B. B. and Chan, M. C. (2010). Mobicent: a credit-based incentive system for disruption tolerant network. In *IEEE INFOCOM'2010*, pages 1–9.

Chen, H. and Chen, G. (2007). A resource-based reputation rating mechanism for peer-to-peer networks. In *Sixth GCC'2007*, pages 535–541.

da Nóbrega Gomes, E., Campos, C. A. V., de Lucena, S. C., and Viana, A. C. (2017). A message removal mechanism for delay tolerant networks. In *Advances in Ubiquitous Networking 2*, pages 43–55. Springer.

Junior, N. M. and Campos, C. A. V. (2015). Socleer: A social-based energy-efficient forwarding protocol for opportunistic networks. In *2015 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 757–762.

Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The one simulator for dtn protocol evaluation. In *Proceedings of the 2nd SIMUTOOLS*, page 55.

Ning, T., Liu, Y., Yang, Z., and Wu, H. (2017). Incentive mechanisms for data dissemination in autonomous mobile social networks. *IEEE Transactions on Mobile Computing*, PP(99):1–1.

Seregina, T., Brun, O., El-Azouzi, R., and Prabhu, B. J. (2017). On the design of a reward-based incentive mechanism for delay tolerant networks. *IEEE Transactions on Mobile Computing*, 16(2):453–465.

Shevade, U., Song, H. H., Qiu, L., and Zhang, Y. (2008). Incentive-aware routing in dtns. In *IEEE ICNP'2008*, pages 238–247.

Uddin, M. Y. S., Godfrey, B., and Abdelzaher, T. (2010). Relics: In-network realization of incentives to combat selfishness in dtns. In *18th IEEE ICNP'2010*, pages 203–212.

Wang, Y., Chuah, M.-C., and Chen, Y. (2014). Incentive based data sharing in delay tolerant mobile networks. *IEEE Transactions on Wireless Communications*, 13(1):370–381.

Zhu, Y., Xu, B., Shi, X., and Wang, Y. (2013). A survey of social-based routing in delay tolerant networks: positive and negative social effects. *Communications Surveys & Tutorials, IEEE*, 15(1):387–401.