Avaliação Experimental da Eficácia de um *Watchdog* em Redes Oportunistas Móveis

Diogo Soares[1], Bruno Matthaus[1], Edjair S. Mota[1], Celso B. Carvalho[2]

[1]Instituto de Computação – Universidade Federal do Amazonas (UFAM)
Av. General Rodrigo Octávio Jordão Ramos – 3000 – Manaus – AM – Brasil

[2]Programa de pós-graduação em engenharia elétrica (PPGEE)
Universidade Federal do Amazonas (UFAM)

{diogo.soares, bmmso, edjair}@icomp.ufam.edu.br, ccarvalho_@ufam.edu.br

Abstract. *Detection of selfish behavior is crucial to the proper functioning of opportunistic mobile network (OMN) operations. Previous work focused on developing reputation systems or trust models. However, these approaches assume the existence of an efficient model of selfish nodes, such as watchdogs. Most studies, however, do not present an analysis of the efficiency of watchdog implementation at an experimental level. This article discusses the design, implementation, and validation of a watchdog, in order to verify the effectiveness of the detection process and to understand the effects of this mechanism for increasing density of messages in the network. The experimental results, obtained using the environment The ONE, showed that the implementation of watchdog discussed here is very promising.*

Resumo. *A detecção de comportamento egoísta é crucial para o funcionamento adequado das operações em redes oportunistas móveis. Trabalhos anteriores têm concentrado esforços em desenvolver sistemas de reputação ou modelos de confiança. Contudo, essas abordagens assumem a existência de um modelo eficiente de detecção de nós egoístas, tal como os watchdogs. A maioria dos estudos, no entanto, não apresenta uma análise da eficiência da implementação do watchdog em um nível experimental. Este artigo discute o projeto, a implementação e a validação de um watchdog, com o objetivo de verificar a eficácia no processo de detecção e compreensão dos efeitos desse mecanismo para valores crescentes da densidade de mensagens na rede. Resultados experimentais, utilizando-se o ambiente The ONE, mostram que a implementação do watchdog aqui discutida é bastante promissora.*

1. Introdução

O tradicional mecanismo TCP/IP assume a existência de um caminho fim-a-fim estabelecido entre um nó origem e um nó destino durante uma comunicação. Além disso, com o objetivo de garantir a entrega de pacotes, o TCP implementa mecanismos como o reconhecimento de pacotes utilizando ACK, utilização de temporizadores de retransmissão e a utilização de *buffers* para permitir a entrega ordenada de pacotes. Entretanto, alguns cenários de redes sem fio podem não assumir tais premissas devido às condições de mobilidade, limitações do meio de comunicação sem fio e limitações de recursos dos nós, ocasionando frequentes desconexões das comunicações da rede. Neste contexto, surgiram as

Redes Oportunistas Móveis (*Opportunistic Mobile Networks* - OMN) [Misra et al. 2016], que operam com o conceito de Redes Tolerantes a Atrasos e Desconexões (DTN - *Delay Tolerant Networks*) [Fall 2003]. Em redes OMN, cada nó possui um *buffer*, podendo armazenar de modo persistente uma mensagem e repassá-la para outros nós, até que a mensagem seja entregue ao destinatário, através do que é chamado de contato oportunista.

A fim de possibilitar a comunicação em redes DTN, Fall et al [Fall 2003] propôs a camada de agregação que, posicionada entre as camadas de aplicação e transporte, permite implementar o paradigma *store, carry and forward*. Assim, estas redes funcionam sem uma hierarquia, e cada nó opera de modo independente. Nesta forma de operação, é essencial que os nós da rede atuem como colaboradores na comunicação, isto é, cada nó precisa carregar uma réplica da mensagem original de forma a aumentar a probabilidade de entrega de uma réplica da mensagem ao nó destinatário. No entanto, tal proposta pode esgotar rapidamente recursos dos nós da rede, como espaço de *buffer* e energia, estimulando assim, um comportamento egoísta dos nós. Esta atitude egoísta dos nós afeta o desempenho e o funcionamento esperado dos principais algoritmos para redes OMN.

Modelos para detecção e mitigação do comportamento egoísta têm sido estudados na literatura principalmente aliados a mecanismos de reputação ou incentivo. Basicamente, tais mecanismos supõem a existência de um mecanismo de detecção, comumente chamado de *watchdog*, utilizado para realizar algum processamento ou tomada de decisão como eliminar o nó da comunicação na rede ou incentivar este nó a participar da comunicação. Embora haja uma gama de estudos que foquem no estudo de mecanismos de reputação ou incentivo [Miao et al. 2012], até onde sabemos, não há estudos que verifiquem o impacto que os *watchdogs* causam no desempenho destes mecanismos. Enquanto alguns trabalhos usam *watchdogs* probabilísticos [Li et al. 2017, Hernandez-Orallo et al. 2012], isto é, com uma probabilidade de eficácia de detecção durante os contatos, outros trabalhos [Dias et al. 2015, Michiardi and Molva 2002] não apresentam de modo claro o projeto de implementação de seus *watchdogs*, seus problemas de projeto e, por conseguinte, o impacto que causariam em redes OMN.

No presente artigo, propomos a implementação de um *watchdog* usando o simulador *Opportunistic Network Environment* (The ONE) [Keränen et al. 2009] e uma avaliação de desempenho em redes OMNs, utilizando traces de mobilidade extraídos de experimentos reais. Para tanto, consideramos que durante um contato, um nó da rede pode rejeitar ou receber uma mensagem devido a outros motivos além do egoísmo tais como falta de espaço de armazenamento em *buffer*, interrupção do contato durante a transferência de mensagens, baixa energia no dispositivo, entre outros. Destacamos que, com o objetivo de compreender os impactos causados por um *watchdog* em uma OMN, este trabalho não utiliza qualquer conjunto de modelos de incentivo ou reputação apresentados na literatura.

Assim, as principais contribuições deste trabalho são:

- Entender as principais dificuldades no projeto, modelagem e implementação de um *watchdog* numa rede OMN. Percebemos que alguns aspectos como o não estabelecimento de respostas de reconhecimento entre os segmentos, típicos da arquitetura TCP/IP, a segurança da informação e a falta de uma organização centralizada da rede representam dificuldades para a implantação de um *watchdog*. O

trabalho proposto visa servir como referência para preencher essa lacuna observada na literatura;
- Estudar o impacto dos tipos de rejeição de mensagens em redes OMNs, uma vez que a rejeição de mensagens entre os nós pode ocorrer por motivos como queda de conexão, *buffer* cheio, egoísmo, entre outros.

O restante deste trabalho está organizado da seguinte forma: na Seção 2 são apresentados os principais trabalhos relacionados ao tema abordado neste trabalho, enquanto que na Seção 3 abordamos os principais desafios de implementação e implantação de um *watchdog*. A Seção 4 apresenta a metodologia de avaliação utilizada, enquanto que a Seção 5 apresenta os resultados obtidos neste trabalho. Finalmente, na Seção 6 apresentam-se as conclusões e trabalhos futuros.

2. Trabalhos Relacionados

O estudo do comportamento egoísta têm sido estudado anteriormente. Uma abordagem amplamente utilizada tem sido métodos de reputação. Nesta abordagem, os nós são ranqueados conforme observações de monitoramento. Assim, no caso deste tipo de abordagem, há a necessidade de um mecanismo que possa detectar comportamentos egoístas na rede, considerando as principais características de uma OMN.

Alguns mecanismos de detecção foram estudados em redes *Ad Hoc* móveis (MANETs) para monitorar o comportamento de repasses na rede. Entre eles, destacamos o trabalho proposto por Liu et al., o esquema 2ACK [Liu et al. 2007]. Neste mecanismo, quando um nó repassa uma mensagem ele retorna um pacote de ACK com 2 saltos de limite na sua configuração, que faz o caminho reverso ao que uma mensagem estava sendo repassada. O objetivo é realizar uma espécie de TCP heurístico, no qual a ausência de uma resposta após um tempo pode indicar que o nó agiu de modo egoísta. Contudo, esta abordagem pode induzir a uma taxa considerável de congestionamento na rede além da dificuldade de escolha de limiares de tempo de observação. O alto tempo entre contatos (tempo até um nó encontrar outro nó novamente) e aspectos sociais também podem afetar o *feedback* eficiente.

Devido a fatores específicos de redes OMNs, como falta de infraestrutura de comunicação e alta latência, várias abordagens propostas na literatura utilizam o mecanismo *watchdog* [Marti et al. 2000, Li and Das 2010, Hernández-Orallo et al. 2015, Buchegger and Le Boudec 2002, Michiardi and Molva 2002]. O *watchdog* é um mecanismo proposto em [Marti et al. 2000] no qual um *watchdog* é um componente presente em um conjunto de nós que continuamente monitora a rede em busca de detectar nós egoístas, nós maliciosos (nós que injetam informações falsas na rede), *gray holes* (tipo de ação maliciosa no qual os nós, silenciosamente, descartam alguns pacotes de seus *buffers* mesmo quando os recursos não estão expirando), entre outros. Seu funcionamento no monitoramento promíscuo da comunicação entre outros nós objetiva captar o modo como pacotes são repassados. Além disso, cada nó monitora seus próprios repasses e em cada novo encontro compartilham os dados monitorados. Sua implementação consiste na gerência de uma tabela de repasses, no qual a cada pacote ouvido na rede ele é comparado com a versão existente na tabela de repasses e então é eliminado. Se uma entrada na tabela de repasses ultrapassar um limiar de tempo, então é incrementado uma *flag* de falha de repasse para o nó que estava responsável por aquele repasse. Como redes OMN podem

ter um longo atraso nos encontros entre os nós, encontrar um limiar vantajoso para cada tipo de mobilidade pode ser uma tarefa árdua. Os autores também definem outras fraquezas dos *watchdogs* tais como colisões, falsas detecções e raio de transmissão limitado. Novamente, a literatura carece de trabalhos que analisam profundamente a eficiência do *watchdog* sem o uso de outros mecanismos como reputação e incentivo.

Em trabalhos posteriores, Orallo et al. realizaram estudos analíticos com *watchdogs* com o intuito de identificar o funcionamento destes com a premissa de erros na fase de detecção [Hernández-Orallo et al. 2015, Hernández-Orallo et al. 2014, Hernandez-Orallo et al. 2012]. O *watchdog* é um mecanismo analítico onde a cada contato pode ou não ocorrer uma detecção, que é modelada por uma probabilidade de detecção. Posteriormente, foram adicionadas as probabilidades de detecção correta, isto é, quando um nó é identificado como egoísta e é egoísta ou identificado como egoísta e não é egoísta. Quando a probabilidade de detecção é muito baixa, o impacto no tempo de detecção é alto devido a baixa quantidade de vezes que os *watchdogs* são efetivamente acionados. Contudo, tal estimativa não tem sido estudada previamente em redes OMN.

Em outro trabalho posterior, Soares et al. investigou o uso de *watchdogs* analíticos aliados a um modelo de reputação [Soares et al. 2014]. Neste, a probabilidade de detecção correta é avaliada utilizando técnicas de aprendizagem de máquina e demonstraram que mesmo quando o erro do *watchdog* era em torno de 25%, poderia ser bem utilizado com o modelo de reputação apresentado. Novamente, a acurácia do *watchdog* é apenas avaliada de modo analítico.

Em [Li and Das 2010], Li e Das propuseram um *watchdog* agregado a outro mecanismo que envia mensagens de controle para a rede. Após cada repasse de um nó que possui uma cópia de mensagem, uma nova mensagem de *feedback* é gerada e enviada para o nó que originou a mensagem para sinalizar que este realizou o repasse, assim ampliando o mecanismo de operação do *watchdog*. Embora o aumento no número de mensagens ocorra, os autores argumentam que a simplicidade do projeto de *watchdog* não degrada o desempenho geral da rede.

Levando em consideração as pesquisas existentes e suas lacunas, este trabalho propõe o projeto de um *watchdog* específico para redes OMN e uma avaliação mais completa do seu comportamento como estimativa de erros e o impacto numa rede OMN real. Para isso definimos cenários de comunicação nos quais pôde-se variar a densidade de mensagens geradas na rede a partir das características de interação social destes cenários.

3. Detecção de Egoísmo Usando *Watchdog*

O objetivo de um *watchdog* é poder acompanhar transações de repasse de mensagens realizadas na rede. Para isso, Marti et al. definem um *buffer* com pacotes enviados e a cada novo pacote ouvido na rede, o pacote ouvido é comparado com o conteúdo do *buffer*. Se a comparação resulta em um acerto, o pacote enviado é removido do *buffer*, caso contrário, ao estourar um limiar de tempo, sinaliza-se o nó responsável pelo repasse daquele pacote como egoísta [Marti et al. 2000].

Durante o projeto de construção do *watchdog* em redes OMN, algumas questões foram levantadas. Entre estas destacamos:

- Como criar um mecanismo que seja livre de inserções, por parte dos nós, de si-

tuações que não tenham ocorrido. Se um nó não repassa uma mensagem, ele não pode inserir no *watchdog* uma entrada de repasse para esta mensagem;
- Como considerar rejeições de repasse por motivo não egoísta na construção do *watchdog*. Por exemplo, um nó A passa uma mensagem para o nó B, contudo B rejeita carregar a mensagem consigo por estar com o *buffer* cheio. A ausência de garantia de transmissão, como ocorre no TCP tradicional, deixa o nó A sem o conhecimento do sucesso na transmissão;
- Como fazer o *watchdog* refletir a realidade das operações de rede ocorridas em cada nó. Assim, acreditamos que o mecanismo do *watchdog* deve funcionar na camada de transporte, integrada aos protocolos de roteamento e gerência.

No mecanismo proposto, cada nó da rede possui um *buffer* de repasses, que chamaremos de *watchdog* daqui em diante. O nosso *watchdog* foi modelado como sendo uma tabela contendo informações de cada repasse realizado em uma tupla `<timestamp, messageId, from, to>`. Desta forma, cada tupla do *watchdog* passa a funcionar como um tipo *hash*, no qual cada membro da tupla funciona como uma chave de busca composta. Assim, um nó pode acompanhar de modo simples o andamento de repasses na rede.

A cada repasse realizado, uma entrada é adicionada na tupla tanto no nó realizando o repasse como no nó que está recebendo a mensagem para repasse. Neste ponto, assumimos que as operações que ocorrem no *watchdog* refletem o real comportamento das operações do nó, isto é, se um nó recebendo o repasse aceita carregar a mensagem consigo, este adiciona uma entrada no *watchdog*. Caso haja uma rejeição (egoísmo, *buffer* cheio, pouca energia, queda da conexão, estratégias de gerenciamento de *buffer* ou roteamento), este não adiciona uma entrada no *watchdog*. No entanto, vale ressaltar que no projeto das redes OMN, o envio de mensagens é feito sem a total confirmação de recebimento, clássico na arquitetura TCP/IP, assim, o nó que está encaminhando a mensagem adiciona a entrada no *watchdog*, atribuindo um voto de confiança que a mensagem foi repassada com sucesso.

Além disso, adicionamos a característica colaborativa ao *watchdog*, conforme já comprovada sua eficácia em trabalhos anteriores. Para isto, a cada encontro, nós não egoístas compartilham o resultado de seus *watchdogs* e realizam um *merge* entre eles, adquirindo assim as informações que o outro *watchdog* havia obtido. Ressaltamos aqui que um dos objetivos deste trabalho neste primeiro momento não é abordar alguns aspectos de segurança envolvidos no processo de compartilhamento como modelos criptográficos ou nós maliciosos que criam informações em seus *watchdogs* e compartilham com a rede.

Na Figura 1, é demonstrado um exemplo de como ocorre o funcionamento do *watchdog*. No tempo 1, o nó A cria uma mensagem M1, encontra o nó B e envia M1. Nó B não recebe a M1 (egoísmo ou erros na transmissão), desse modo o *watchdog* em A adiciona entrada de envio e *watchdog* de B, responsável pelo monitoramento de ações de comunicação, não adiciona entrada. No tempo 2, nó A encontra nó C, encaminha uma cópia de M1 e, compartilham as suas entradas do *watchdog*, difundindo as informações sobre repasses. Quando C encontra B, C verifica que os repasses não foram executados por B e sinaliza que B falhou no repasse. Dado que B pode não aceitar custodiar a mensagem por várias razões, este trabalho realiza um estudo mais amplo sobre sinalizações corretas do *watchdog* de modo a verificar a eficácia do *watchdog*.

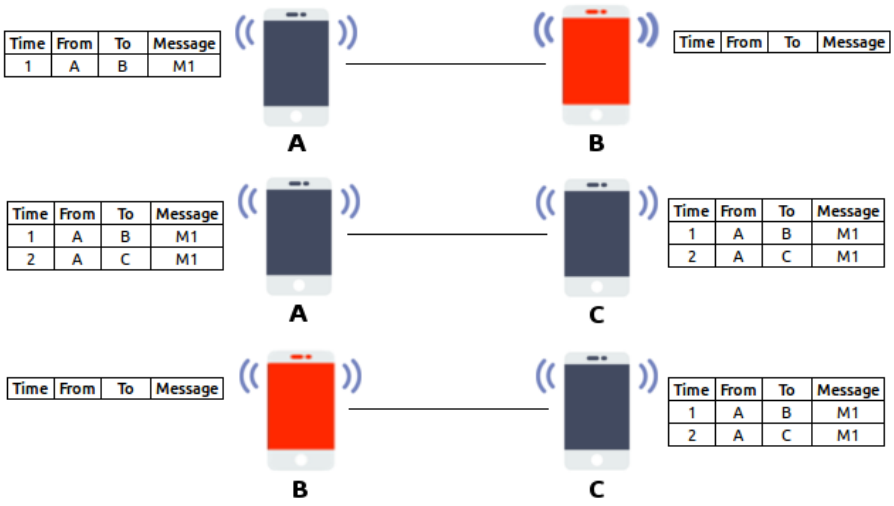

Figura 1. Exemplo de funcionamento do *watchdog* considerando o aspecto colaborativo

Neste trabalho é assumido que cada nó possui um espaço de armazenamento separado do *buffer* de dados, suficientemente grande para armazenar o *watchdog*. Embora não sejam estudados a fundo, alguns mecanismos conhecidos de gerenciamento de *buffer* podem ser aplicados aqui de modo a criar um tamanho fixo para o *watchdog*. Assim sendo, algumas heurísticas podem ser aplicadas como o FIFO (*First In First Out*) ou outras características sociais para eliminar informações sobre nós que têm probabilidade de encontro é mais baixa [Souza et al. 2014]. Desse modo, escolhemos projetar o *watchdog* sem controle de congestionamento e com controle de congestionamento de 6 horas, isto é, entradas superiores a 6 horas no *watchdog* são removidas.

4. Avaliação de Desempenho

Nesta seção serão apresentados os resultados obtidos para o *watchdog* implementado, que foi experimentalmente avaliado usando o simulador The ONE (*Opportunistic Network Environment*) [Keränen et al. 2009], que implementa a arquitetura DTN, de modo que fosse possível combinar esse modelo de comunicação em uma OMN com a estratégia proposta.

4.1. Cenário Utilizado

Os cenários utilizados foram *traces* de contatos extraídos de experimentos reais de mobilidade e contatos. Diferentemente de outros trabalhos na literatura que utilizaram modelos de mobilidade aleatórios, este trabalho visa verificar o comportamento dos *watchdogs* sob condições mais realistas de redes OMN como perfis sociais de mobilidade e contato entre os nós.

Os cenários utilizados foram os experimentos Sassy [Bigwood et al. 2011] e Haggle-Infocom05 [Chaintreau et al. 2007], cuja as características são detalhadas na Tabela 1. A motivação que nos levou a escolha destes cenários foi que ambos representam modelos distintos de interação social como pode ser observado através de dados sobre

Tabela 1. Dados estatísticos dos *traces* utilizados

	Sassy	**Infocom5**
Número de nós	25	41
Duração (dias)	79	3
Tipo de dispositivo	T-Motes	iMote
Número de contatos	7565	22459
Contatos por minuto	1,651	4,902
Tempo médio de contato (s)	9,476	231,755
Média da maior componente detectada	1,087	5,051
Grau médio dos nós	0,008	0,477

Tabela 2. Parâmetros de simulação

	Sassy	**Infocom5**
Tempo de execução (horas)	72	48
TTL (minutos)	300	
Tamanho de *buffer*	$5M$	
Roteamento	Epidêmico	
Mensagens geradas/hora	2/hora	
Tamanho das mensagens	$(250k, 500k)$	
Velocidade de transmissão	$250kBps$	

densidade de contatos e tempo de duração entre contatos. Como o desempenho de algoritmos para redes OMNs pode variar dependendo dos padrões de conectividade e mobilidade, é de suma importância a análise das variações que possam ocorrer no desempenho do *watchdog* nestes ambientes. No caso do experimento Sassy, o grafo de conectividade é mais esparso, dificultando a comunicação fim-a-fim entre nós socialmente mais distante.

Para simulação dos nós egoístas, utilizamos a abordagem de egoísmo individual. O egoísmo individual se refere ao fato de que um nó egoísta age deste modo com quaisquer outro nó em contato. Assim, escolhemos porcentagens de nós da rede como sendo egoístas no início na rede. Assim, variamos a porcentagem de nós egoístas entre 10% a 50%, com saltos de 10%. Além disso, escolhemos manter os nós como egoísta do início ao final da simulação, assim como nós não egoístas permanecem assim até o fim de cada simulação. Cada simulação foi executada 20 vezes com 90% de intervalo de confiança. Parâmetros extras de simulação são apresentados na Tabela 2.

4.2. Métricas Analisadas

Neste trabalho analisamos os impactos e eficiência dos *watchdogs* no âmbito de redes OMN. Para isto analisamos a avaliação de desempenho em duas etapas, primeiramente a eficiência dos *watchdogs* é avaliada quantitativamente a partir dos resultados da simulação, enquanto uma análise subjetiva dos impactos é descrita na seção de Resultados.

Para realizar a análise de eficiência, verificamos a quantidade de acertos e erros do *watchdog*. Cada detecção do *watchdog* pode ser avaliada como um Verdadeiro Positivo (VP), isto é, uma detecção de nó como egoísta quando este nó é egoísta e Falso Positivo (FP), quando um nó é detectado pelo *watchdog* como egoísta, quando este não é egoísta.

Assim, avaliamos a taxa de VP e FP detectados pelos *watchdogs* da rede em cada cenário.

Além disso, analisamos os tipos de rejeições de repasse na rede, conforme variamos o nível de egoísmo. Um dos principais motivos de falhas de *watchdog* conforme trabalhos anteriores são erros causados na comunicação. Desse modo, utilizamos os tipos de rejeição existentes no simulador The ONE e adicionamos a rejeição por egoísmo.

5. Resultados

Nesta seção são apresentados os resultados obtidos ao executar o projeto de experimentos definidos na seção anterior.

5.1. Análise de Rejeições de Repasse por Egoísmo

A taxa de rejeições pode ser definida pelo total de rejeições de repasse por egoísmo em relação ao somatório de todas as rejeições que ocorreram. A hipótese da análise dessa métrica visa entender se a taxa de rejeições pode influenciar a acurácia dos *watchdogs*. Dados que trabalhos anteriores assumem que uma das desvantagens do *watchdog* estão relacionadas a problemas na comunicação de rede, então é de suma importância entender como esse comportamento ocorre.

A Figura 2 apresenta a porcentagem média de rejeições para os traces Sassy e Infocom5. Como pode ser observado nos resultados, a hipótese de que quanto maior o nível de egoísmo entre os nós da rede, maior a taxa de rejeição por egoísmo entre os repasses, sendo quase 70% dos tipos de rejeição para 20% de nós egoístas no *trace* Sassy e chegando a 70% dos tipos de rejeição para 40% de nós egoístas no *trace* Infocom5. A justificativa é que o *trace* Infocom possui uma quantidade de contatos por minuto 3 vezes maior que no Sassy. Assim, a taxa de ocupação de *buffer* ocorre mais rápido no Infocom5, levando a mais rejeições por falta de espaço de armazenamento. Além disso a quantidade de múltiplas conexões no Infocom5 é maior e utilizamos o limite de transmissões simultâneas de pacotes igual a 1, levando também a rejeições por canal ocupado.

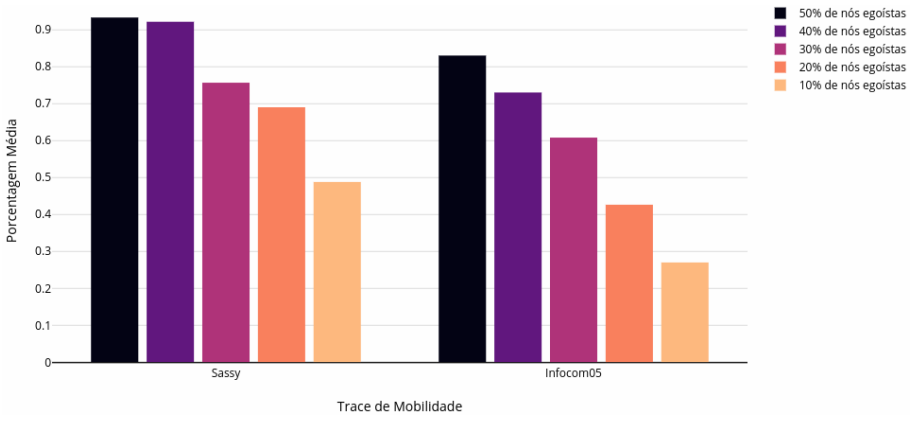

Figura 2. Porcentagem média de rejeição de repasse pelos nós da rede por motivação egoísta

Adicionalmente, verificamos a correlação de pearson[1] entre o nível de nós egoístas e a porcentagem de rejeições por motivo egoísta. Nossos resultados mostram uma

[1]https://pt.wikipedia.org/wiki/Coeficiente_de_correlação_de_Pearson

correlação de $\simeq 0,62$ para o cenário Sassy e $\simeq 0,87$ para o cenário Infocom5. Isso é explicado pela intensidade de pacotes na rede, conforme há diminuição de egoísmo, maior o número de pacotes na rede, aumentando assim a taxa de ocupação de *buffer* e utilização de recursos.

5.2. Acurácia do *Watchdog*

A análise da acurácia foi feita utilizando o aspecto de monitoramento e compartilhamento do *watchdog*. Assim, analisamos também a taxa de conhecimento da rede dos nós egoístas, isto é, a quantidade de nós detectados egoístas corretamente em todos os nós da rede pelo somatório do caso perfeito, no qual todos os nós conhecem os nós egoístas da rede.

A Figura 3 demonstra os resultados obtidos para o *trace* Sassy. Com relação a acurácia, a hipótese levantada era que a taxa de acertos seria maior conforme o nível de conhecimento da rede aumentasse. Aqui, ressaltamos que esse conhecimento da rede é apenas o conhecimento de nós egoístas que realmente são egoístas. No Sassy, tivemos uma variação de taxa de verdadeiros positivos com 75% de acerto mesmo que metade da rede seja egoísta, o que demonstra um bom resultado para o *watchdog* mesmo para um *trace* no qual a comunicação entre os nós é mais esparsa. A explicação da variação podemos atribuir para a escolha dos nós egoístas. Percebemos que quando nós egoístas eram menos populares ou tinha menos contatos, havia uma dificuldade maior de detectá-los corretamente. Esse fato corrobora para uma outra hipótese levantada neste trabalho: o funcionamento dos *watchdogs* tem total influência dos padrões de mobilidade. Acreditamos que esse fato também influenciou na taxa de rejeições por egoísmo nesse *trace*, dado que neste *trace*, a anulação de um nó popular gera muito mais impacto que no Infocom5.

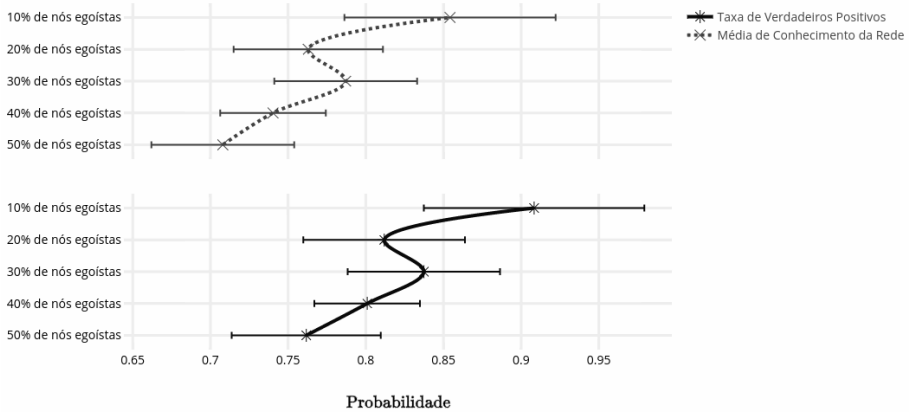

Figura 3. Taxa de verdadeiros positivos e média de conhecimento da rede no Sassy

A Figura 4 demonstra o resultado para o Infocom5. A diferença é notável na acurácia, sendo que mesmo quando a taxa de egoísmo é muito baixa (10% dos nós), a taxa de detecções corretas se mantém acima dos 97% considerando a variação entre os resultados. A explicação dessa diferença para o Sassy se dá no fato de que a comunicação no Infocom5 é mais densa, assim a quantidade de mensagens trocadas é maior, logo a quantidade de contatos suficientes para detectar nós egoístas através do *watchdog* é alcançada de modo muito veloz neste trace. Embora isso fosse um resultado esperado, vale ressaltar que até esse ponto não utilizamos o controle de congestionamento no *watchdog*, assim,

embora a acurácia tenha sido alta, o *overhead* de mensagens foi muito alto, como vai ser demonstrado mais adiante.

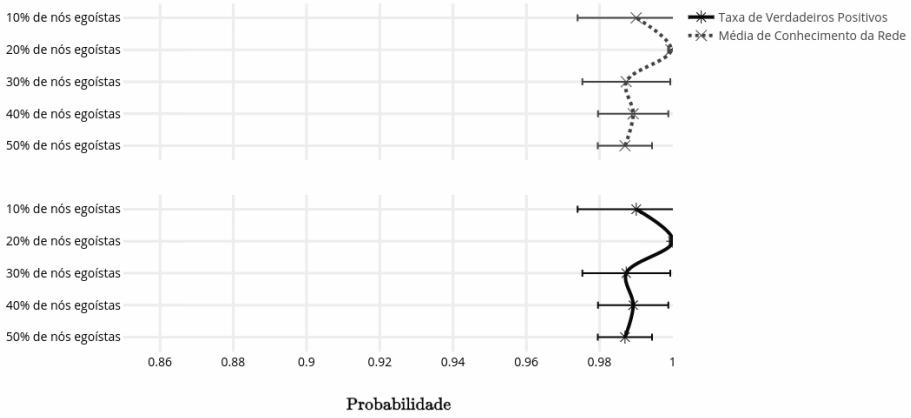

Figura 4. Taxa de verdadeiros positivos e média de conhecimento da rede no Infocom5

Analisamos também a taxa de falsos positivos gerados em nosso experimento. Observa-se por meio dos gráficos na Figura 5, que o *watchdog* gera uma taxa de falsos positivos muito alta. Enquanto que no cenário Infocom5, a densidade mais alta de repasses na rede gera uma quantidade de rejeições maior por falta de espaço de *buffer* e por transmissões simultâneas, então a taxa de falsos positivos é tão alta quanto a taxa de verdadeiros positivos no Infocom5. A razão para isso é o efeito *gossip*, no qual um nó adquire uma informação incorreta e compartilha exaustivamente, sendo auxiliado pela grande quantidade de contatos entre os nós da rede.

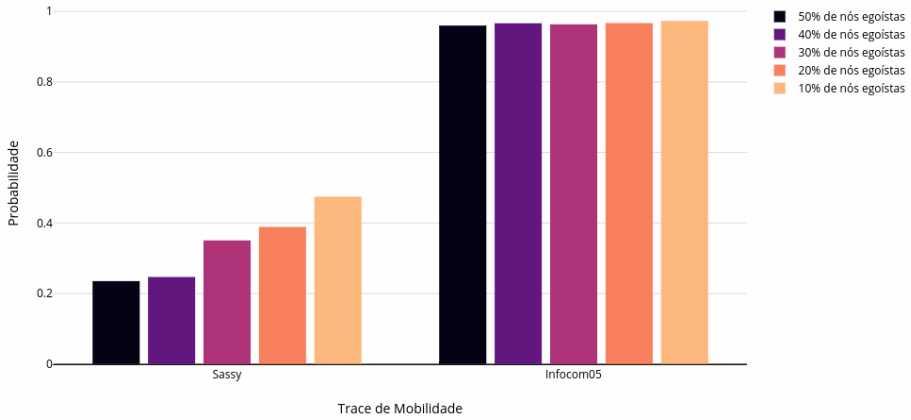

Figura 5. Taxa de falsos positivos sinalizados no Infocom5

Com o intuito de diminuir a taxa de falsos positivos, criamos um mecanismo que chamamos de controle de *feedback* positivo. Esse mecanismo é semelhante ao controle de garantia de entrega de pacotes no TCP/IP e também se assemelha ao protocolo de detecção 2ACK. Contudo, em nossa versão, *feedback* positivo é enviado apenas para o nó no salto anterior quando uma mensagem é armazenada no seu *buffer*. O resultado é apresentado na Figura 6 e demonstra uma diminuição de 45% da taxa de falsos positivos no cenário Infocom e diminuição de até 68% quando 10% dos nós da rede são egoístas.

No cenário Sassy a diminuição foi de aproximadamente 100% para 50% dos nós da rede sendo egoístas e até 75% menor quando 10% dos nós da rede são egoístas. Ou seja, a utilização de um mecanismo para evitar o aumento na taxa de falsos positivos no *watchdog* é essencial, pois assumimos aqui que é muito mais problemático a detecção de um nó egoísta quando este não é egoísta (falso positivo) do que não detectar um nó egoísta, pois assim, um nó que participa da rede pode ser radicalmente prejudicado.

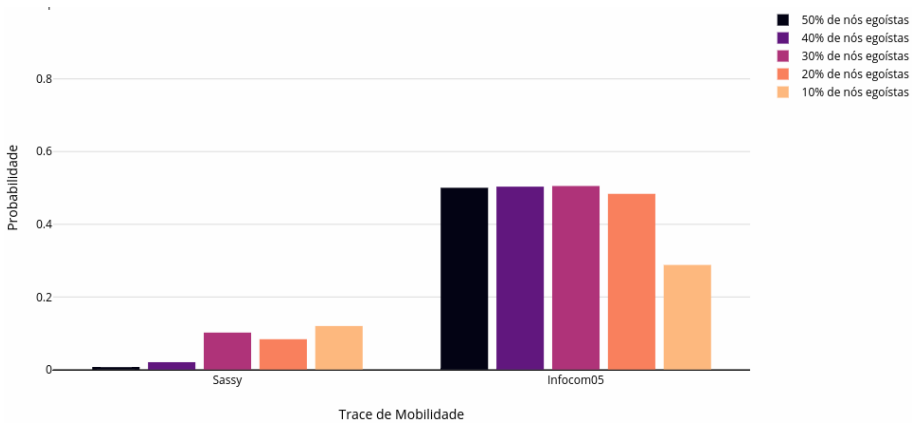

Figura 6. Taxa de falsos positivos sinalizados no Infocom5 com controle de *feedback* positivo

Embora a taxa de falsos positivos tenha caído, não assumimos qualquer erro na transmissão desse *feedback*. Porém, dado que essa mensagem de controle não é propagada, a mesma também não deve gerar alta taxa de falhas devido a erros no canal de rede. Além disso, não há geração de congestionamento extra na rede.

5.3. Controle de Congestionamento do *Watchdog*

Um dos principais problemas já relatados em trabalhos anteriores sobre *watchdogs* é a geração de congestionamento extra na rede, isto é, mensagens trocadas entre *watchdogs*. Devido ao tempo de simulação baixo escolhemos realizar um controle de congestionamento equivalente a $1/4$ do período de um dia, isto é, 6 horas.

A Figura 7 demonstra os resultados para o cenário Infocom5. Como podemos ver, há uma melhoria significativa de $\simeq 65\%$ quando aplicado o controle de congestionamento de 6 horas. Enquanto que no cenário Sassy, a melhoria foi de $\simeq 35\%$, conforme demonstrado na Figura 8.

Inicialmente, nossa hipótese era de que o controle de congestionamento afetaria significantemente o desempenho do *watchdog*, conforme demonstrado anteriormente. No entanto, nossos experimentos mostram que a acurácia média (VP e FP) permanecem praticamente inalteradas, com diferenças entre elas de menos de 5%. Por esse motivo, não vamos prolongar o estudo da acurácia, quando aplicado o controle de congestionamento.

Como pode ser observado, o *watchdog* possui dificuldades já relatadas e comprovadas com este trabalho. Contudo, o controle de congestionamento pode ser facilmente aplicado sem a perda do desempenho. Adicionalmente, este estudo demonstra uma simples otimização para a diminuição da taxa de FP com o controle de *feedback* positivo.

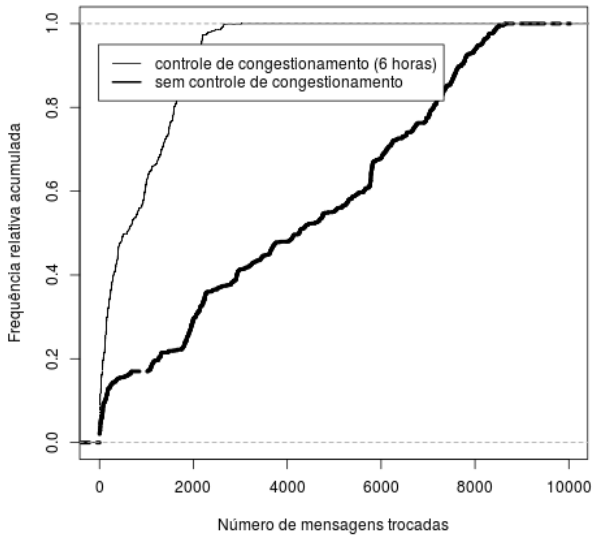

Figura 7. Congestionamento de mensagens no cenário Infocom5

6. Conclusões

Muitos trabalhos na literatura no âmbito de detecção de nós egoístas ou nós maliciosos em redes OMN utilizam técnicas para detectar estes a partir do monitoramento de repasses na rede. Uma das abordagens mais comuns é o *watchdog*, implementado previamente para redes *ad hoc* móveis. Contudo, é notável a falta de trabalhos que verificaram o real impacto deste mecanismo em uma OMN, com padrões de mobilidade e interação social variáveis.

Este trabalho propõe o projeto de implementação de um *watchdog* para OMN. Destacamos alguns questionamentos sobre a implementação e realizamos testes em ambientes OMN utilizando *traces* de mobilidade e utilizando o simulador The ONE.

O projeto de implementação demonstrou que há uma dificuldade de projeto não destacado em trabalhos prévios. Além disso, a avaliação demonstra que a taxa de verdadeiros positivos se mantém acima dos 70% mesmo com uma intensidade menor de contatos. Entretanto, verificamos que a taxa de falsos positivos pode ser muito alta em cenários de intensa comunicação e troca de mensagens entre *watchdogs*. Assim, desenvolvemos um esquema simples de *feedback* positivo. Tal mecanismo mostrou melhorias significativas na diminuição da taxa de falsos positivos, principalmente nos cenários onde a intensidade da comunicação era maior como no Infocom5.

Além disso, fizemos uma breve análise sobre o controle de congestionamento do *watchdog* e demonstramos que a taxa de VP e FP pode ser mantida estável mesmo considerando um tempo mais curto de informação dentro do *watchdog*.

Para trabalhos futuros, planejamos avaliar o mecanismo proposto utilizando algumas abordagens de modelos de reputação propostos na literatura. Além disso, planejamos avaliar o comportamento dinâmico entre os nós, isto é, nós que mudam de comportamento conforme a utilização de seus recursos torna-se escassa. Por fim, pretendemos avaliar a

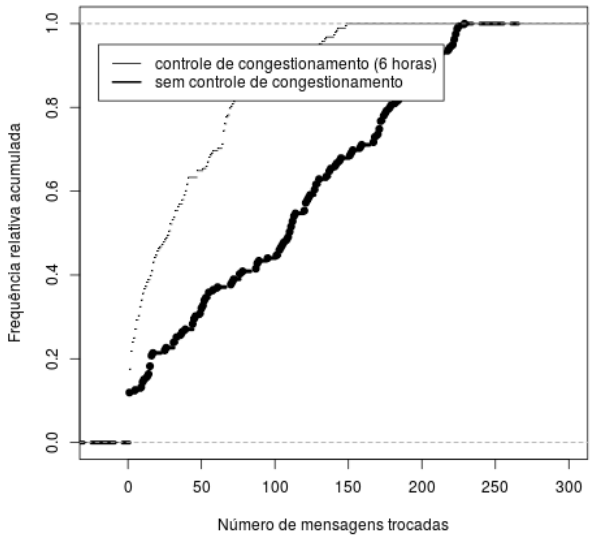

Figura 8. Congestionamento de mensagens no cenário Sassy

variação de outros parâmetros da rede como roteamento e gerenciamento de *buffer* baseado em aspectos sociais e a geração de mensagens na rede.

Referências

[Bigwood et al. 2011] Bigwood, G., Henderson, T., Rehunathan, D., Bateman, M., and Bhatti, S. (2011). CRAWDAD dataset st_andrews/sassy (v. 2011-06-03). Downloaded from `https://crawdad.org/st_andrews/sassy/20110603`.

[Buchegger and Le Boudec 2002] Buchegger, S. and Le Boudec, J.-Y. (2002). Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '02, pages 226–236, New York, NY, USA. ACM.

[Chaintreau et al. 2007] Chaintreau, A., Hui, P., Crowcroft, J., Diot, C., Gass, R., and Scott, J. (2007). Impact of human mobility on opportunistic forwarding algorithms. *IEEE Transactions on Mobile Computing*, 6(6):606–620.

[Dias et al. 2015] Dias, J. A. F. F., Rodrigues, J. J. P. C., Xia, F., and Mavromoustakis, C. X. (2015). A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. *IEEE Transactions on Industrial Electronics*, 62(12):7929–7937.

[Fall 2003] Fall, K. (2003). A delay-tolerant network architecture for challenged internets. In *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '03, pages 27–34, New York, NY, USA. ACM.

[Hernández-Orallo et al. 2014] Hernández-Orallo, E., Olmos, M. D. S., Cano, J.-C., Calafate, C. T., and Manzoni, P. (2014). A fast model for evaluating the detection of selfish nodes using a collaborative approach in manets. *Wireless Personal Communications*, 74(3):1099–1116.

[Hernandez-Orallo et al. 2012] Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., and Manzoni, P. (2012). Improving selfish node detection in manets using a collaborative watchdog. *IEEE Communications Letters*, 16(5):642–645.

[Hernández-Orallo et al. 2015] Hernández-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., and Manzoni, P. (2015). Cocowa: A collaborative contact-based watchdog for detecting selfish nodes. *IEEE Transactions on Mobile Computing*, 14(6):1162–1175.

[Keränen et al. 2009] Keränen, A., Ott, J., and Kärkkäinen, T. (2009). The one simulator for dtn protocol evaluation. In *In Proceedings of the 2nd International Conference on Simulation Tools and Techniques (SIMUtools*.

[Li and Das 2010] Li, N. and Das, S. K. (2010). Radon: Reputation-assisted data forwarding in opportunistic networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*, MobiOpp '10, pages 8–14, New York, NY, USA. ACM.

[Li et al. 2017] Li, W., Galluccio, L., Bassi, F., and Kieffer, M. (2017). Distributed faulty node detection in delay tolerant networks: Design and analysis. *IEEE Transactions on Mobile Computing*, PP(99):1–1.

[Liu et al. 2007] Liu, K., Deng, J., Varshney, P. K., and Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in manets. *IEEE Transactions on Mobile Computing*, 6(5):536–550.

[Marti et al. 2000] Marti, S., Giuli, T. J., Lai, K., and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, pages 255–265, New York, NY, USA. ACM.

[Miao et al. 2012] Miao, J., Hasan, O., Mokhtar, S. B., Brunie, L., and Yim, K. (2012). An analysis of strategies for preventing selfish behavior in mobile delay tolerant networks. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 208–215.

[Michiardi and Molva 2002] Michiardi, P. and Molva, R. (2002). *Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks*, pages 107–121. Springer US, Boston, MA.

[Misra et al. 2016] Misra, S., Saha, B. K., and Pal, S. (2016). *Opportunistic Mobile Networks: Advances and Applications*. Springer Publishing Company, Incorporated, 1st edition.

[Soares et al. 2014] Soares, D., Mota, E., Souza, C., Manzoni, P., Cano, J. C., and Calafate, C. (2014). A statistical learning reputation system for opportunistic networks. In *2014 IFIP Wireless Days (WD)*, pages 1–6.

[Souza et al. 2014] Souza, C., Mota, E., Galvao, L., Manzoni, P., and Cano, J. C. (2014). Drop less known strategy for buffer management in dtn nodes. In *Proceedings of the Latin America Networking Conference on LANC 2014*, LANC '14, pages 6:1–6:7, New York, NY, USA. ACM.