

# Tolerância à falha dos agentes de mobilidade do protocolo Mobile IP

Luciano Da Silva Santos e Marco Antonio Grivet Mattoso Maia

**Resumo**—O crescimento da Internet e os avanços da tecnologia de comunicações sem fio tornaram possível a oferta de novos serviços de telecomunicações que são cada vez mais atrativos para segmentos crescentes da população. Entretanto, a mobilidade do usuário é um dos fatores mais desafiadores para o desenvolvimento de mecanismos de acesso a estes serviços. Com o objetivo de resolver os problemas decorrentes desta mobilidade, o grupo Internet Engineering Task Force (IETF) vem desenvolvendo pesquisas sobre novos protocolos para este novo cenário. Embora tais estudos venham recebendo inúmeras contribuições da comunidade científica, é verdade também que existem estudos numa menor proporção relacionados à ocorrência de falhas em sistemas que comportem mobilidade. O objetivo deste artigo é apresentar uma nova proposta de um mecanismo de tolerância a falhas dos agentes de mobilidade que possa positivamente contribuir com as pesquisas nesta área.

**Palavras-Chave**—Rede Local Sem Fio; IP Móvel; Qualidade de Serviço; Agente Doméstico; Agente Estrangeiro; Gerência de Redes.

**Abstract**—The growth of the Internet and the advances of the wireless communication technology are the major facts that are allowing the offer of new non-conventional telecommunication services, very attractive to a growing segment of the population. However, one of the main challenging factors for their development is the mobility of the mobile stations. In order to solve the problems related to the introduction of mobility in this new access form, the Internet Engineering Task Force (IETF) has developed research that investigates new protocols for this new scenery. Although this research are receiving countless contributions from the scientific community, it is also true that fault tolerance aspects are not receiving proportional attention. The purpose of this paper is to positively contribute to this discussion by presenting a new proposal of fault's tolerance of the Mobility Agents.

**Keywords**—Wireless Local Area Network; Mobile IP; Quality of Service; Home Agent; Foreign Agent; Network Management.

## I. INTRODUÇÃO

Devido ao crescimento da Internet e o rápido progresso da tecnologia de comunicação sem fio, tem se observado uma demanda cada vez maior por sistemas que permitam o acesso à Internet. Tais sistemas têm como principal característica a mobilidade do usuário, que é um dos principais fatores desafiadores para o desenvolvimento desta nova forma de acesso. Os usuários móveis (entenda-se celulares, laptops e etc...) acarretam constantes mudanças no comportamento dos Agentes Estrangeiros (Foreign Agents-FA's) durante a execução do serviço de dados, uma vez que tal mobilidade provoca o trânsito do usuário por diversas áreas de cobertura (células)

Luciano Da Silva Santos e Marco Antonio Grivet Mattoso Maia, são respectivamente mestre e professor do Centro de Estudos de Telecomunicações, Pontifícia Universidade Católica, Rio de Janeiro, Brasil. E-mails: mgrivet, luciano@cetuc.puc-rio.br

servidas por diferentes equipamentos e operadoras. Agentes Estrangeiros são roteadores das redes estrangeiras que suportam as conexões das estações móveis com a rede, garantindo o fornecimento do serviço solicitado pelo usuário. Portanto, para evitar a interrupção da sessão durante as mudanças de agentes e integrar as redes sem fio às já existentes que operam com o protocolo IP (Internet Protocol) amplamente empregado, a Internet Engineering Task Force (IETF) definiu o Mobile IP como o protocolo padrão.

O objetivo desse artigo não é analisar o desempenho deste protocolo no que concerne à mobilidade dos usuários durante o processo de Handoff, uma vez que esta análise tem sido extensamente realizada em diversos artigos da literatura. Entretanto é aqui apresentada uma proposta de tolerância à falhas dos Agentes Estrangeiros e dos Agentes de Origem (Home Agents-HA's). Esses agentes são dinamicamente alocados como membros de redundância de outros agentes, de modo a: i) promover uma distribuição mais adequada da carga de tráfego dos agentes defeituosos entre os membros de redundância e ii) prover alocação das estações móveis afetadas pela falha do seu Agente de Origem em outros agentes do mesmo tipo, observando o nível de prioridade que o serviço usufruído por esses usuários exige. Os Agentes de Origem são roteadores da rede de origem das estações móveis que além de desempenhar a mesma função de um Agente Estrangeiro também são responsáveis por gerenciar todas as atividades dessas estações móveis, independente de sua localização.

A motivação encontrada para este tema provém do fato de que a grande parte das pesquisas hoje realizadas e os Request For Comments (RFC's) propostos preocupam-se mais com a questão do desempenho destes protocolos nos processos de handoff, de segurança (autenticação e autorização da conta do usuário) e do registro local dos usuários do que com questões igualmente importantes como possíveis falhas dos Agentes de Mobilidade (HA e FA). Além disso, as poucas propostas existentes nessa linha de pesquisa propõem a utilização de redundância de hardware para suprir as falhas dos agentes defeituosos. Existem ainda propostas nas quais a determinação dos membros de redundância é feita dinamicamente, aproveitando-se de outros Agentes de Mobilidade ativos (livres de falha) em outros domínios da rede.

Este artigo encontra-se organizado da forma: na seção 2 são apresentados aspectos relativos ao protocolo MobileIP, relevantes para a compreensão da proposta apresentada. Na seção 3 são discutidos alguns trabalhos relacionados a esse tema. A seção 4 apresenta uma nova proposta de tolerância à falhas dos Agentes de Mobilidade. Na seção 5 são descritos o cenário de simulação e os resultados alcançados. Finalmente a seção 6 apresenta a conclusões desta pesquisa.

## II. FUNCIONAMENTO DO MOBILE IP

Qualquer que seja a área de cobertura em que uma estação móvel se encontra, esta recebe uma mensagem de anúncio (Agent Advertisement) do Agente de Mobilidade local. Se esta estação móvel estiver localizada em sua rede de origem, ela opera de forma similar a um host fixo. Caso esteja em uma rede estrangeira, um novo endereço IP (denominado de *care-of address*) é associado ao seu endereço de origem. Para melhor entender o funcionamento do MobileIP [1],[2], assume-se que a estação móvel encontra-se em uma rede estrangeira.

A estação móvel, após receber e processar a mensagem de anúncio transmitida pelo Agente Estrangeiro, envia uma mensagem de solicitação de registro (Registration Request) para este agente que a processa e a retransmite para o Agente de Origem dessa estação móvel. Este agente por sua vez processa essa solicitação e envia uma resposta de registro (Registration Reply) para aquele Agente Estrangeiro concedendo ou não o registro da estação móvel. Em caso afirmativo, ele atualiza a sua lista de associações dos endereços IP das estações móveis (chamada de *Mobility Binding*) de seu domínio com os endereços IP dos Agentes Estrangeiros que suportam as conexões destas estações nos domínios estrangeiros. Em seguida, o Agente Estrangeiro adiciona o endereço IP desta estação móvel a sua lista de visitantes e envia essa resposta de registro para essa estação móvel.

Ao fim desta atividade, a estação móvel está habilitada a se comunicar com qualquer outra estação, fixa ou móvel. Todos os pacotes a ela destinados são enviados para a sua rede de origem e em seguida o seu Agente de Origem, por meio de consulta a sua lista (mobility binding), encontra o endereço IP do Agente Estrangeiro que está suportando a conexão com aquela estação, a ele enviando todos os pacotes. Ao recebê-los, o Agente Estrangeiro, após consulta a sua lista de visitantes, retransmite-os para aquela estação móvel.

## III. TRABALHOS RELACIONADOS

As propostas de tolerância à falha dos Agentes de Mobilidade que empregam redundância de hardware [3],[4] apresentam um desempenho melhor quando comparadas com aquelas em que membros de redundância são dinamicamente alocados no caso de falhas. Isto é verdadeiro quando a carga de tráfego gerenciada por esse hardware redundante não ultrapassa a sua capacidade. Entretanto, quando tais cargas são elevadas, esta situação se inverte. Isso é explicado pelo fato de que na proposta de alocação dinâmica, as cargas de tráfegos dos agentes defeituosos são distribuídas para os demais agentes enquanto que nas propostas de redundância de hardware, essas cargas estão restritas ao hardware redundante.

O ponto negativo da proposta de alocação dinâmica [5] reside no fato destas propostas não considerarem os impactos na qualidade de serviço (QoS) e no retardo sofrido pelos pacotes de dados, vital para aplicações como serviços de Vídeo Conferência, jogos interativos e o serviço VoIP (Voice over IP).

## IV. NOVA PROPOSTA DE TOLERÂNCIA À FALHA

### A. Agentes de Mobilidade

A nova proposta de tolerância à falhas dos Agentes de Mobilidade (HA e FA) que é aqui apresentada, leva em

consideração a existência de uma gerência de rede e a não utilização de redundância de hardware. Assim os membros de redundância dos agentes defeituosos serão outros agentes do mesmo tipo (FA ou HA) que são dinamicamente alocados e responsáveis pela gerência da carga de tráfego dos agentes defeituosos. As grandezas usadas nesta alocação são i) a carga de tráfego disponível de cada agente ativo no momento da falha e ii) os retardos sofridos pelos pacotes IP decorrentes desta realocação. Com objetivo de evitar uma degradação excessiva no desempenho desses agentes, adota-se um esquema de diferentes níveis de prioridades para os serviços.

Nesta nova proposta de tolerância à falhas, a introdução do mecanismo de gerenciamento de fila do tipo *Random Early Detection* (RED) [10] é analisada, de modo a evitar que os buffers desses agentes operem com sobrecargas freqüentes.

As principais contribuições dessa nova proposta são: i) o emprego de um parâmetro adicional, a saber, o retardo introduzido aos pacotes de dados, para a determinação dos membros de redundância de modo a conseguir uma distribuição mais equânime da carga de tráfego dos agentes defeituosos; ii) prover alocação das estações móveis afetadas pela falha do seu Agente de Origem em outros HA's ativos, observando o nível de prioridade que o serviço usufruído por esses usuários exige e iii) utilização de mecanismos de gerenciamento de fila (por exemplo, RED) para avaliar o desempenho dos Agentes Estrangeiros.

A arquitetura de rede ilustrada na figura 1 é aqui usada como exemplo para facilitar o entendimento dos procedimentos executados na proposta aqui discutida. A gerência de rede pode ser subdividida em:

- *Gerência de Configuração* (GC): responsável pela gerência e configuração dos equipamentos de redes (HA, FA, roteadores do Core Network, Estação Base Controladora (Base Station Controllers) e Estação Base Transceptora (Base Transceiver Station)) bem como a rede de interconexão.
- *Gerência de Desempenho* (GD): gerencia o desempenho dos equipamentos de redes citados acima, observando as cargas de tráfegos desses equipamentos e os retardos sofridos pelos pacotes de dados.
- *Gerência de Falha* (GF): responsável por detectar e informar à gerência de configuração a ocorrência de falhas nos equipamentos de redes.
- *Gerência de Segurança* (GS): responsável por monitorar o correto acesso aos equipamentos de redes.

### B. Agentes Estrangeiros

Após a falha e detecção de um ou mais Agentes Estrangeiros (FA's), a GD envia as informações de monitoramento para a GC, que incluem: i) informações de carga de tráfego de cada FA livre de falha, ii) a carga de tráfego de todos os enlaces entre BSC's e BTS's, iii) os retardos de propagação sofridos pelos pacotes de dados ao percorrerem os enlaces ativos entre as BTS's e FA's ativos e iv) o retardo de propagação sofridos pelos pacotes de dados entre um FA ativo e possíveis destinos na rede fixa. Esse conjunto de informações é utilizado pela

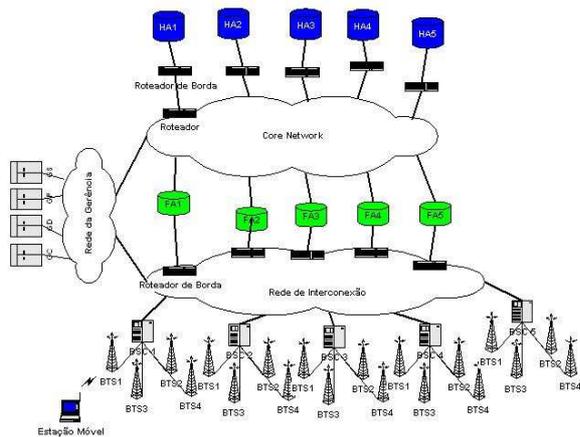


Fig. 1. Arquitetura de rede.

GC para alocar dinamicamente os demais agentes ativos como membros de redundância dos agentes defeituosos.

A seguir, essa gerência envia mensagem para todas as BSC's com intuito de ativar as suas novas configurações e conseqüentemente o funcionamento dos backups selecionados. Os enlaces que conectam cada BSC afetada pela falha do seu FA aos membros de redundância dos agentes defeituosos são ativados de tal forma que cada BTS controlada por esta BSC seja conectada a um FA ativo por intermédio da mesma BSC. Após esta ação, a GC envia mensagem para todos agentes membros de backup, exigindo que este inicie o processo de registro através do envio de mensagens de anúncio para as áreas de coberturas das BTS's que foram afetadas pela falha do seu FA. Desta forma, executa-se um procedimento de "handoff virtual", pois embora as estações móveis permaneçam na mesma área de cobertura elas são registradas em seus respectivos Agentes de Origem como estando em outro domínio. Portanto, as cargas de tráfego dos agentes defeituosos serão divididas em porções menores e distribuídas, não necessariamente de forma uniforme, para todos os membros de backup.

De modo a evitar a sobrecarga dos buffers dos Agentes Estrangeiros ativos, é proposto o emprego do algoritmo de enfileiramento Random Early Detection (RED) [10] nos buffers desses agentes.

1) *Alocação dos FA's como Membro de Backup:* Após envio pelo GD do conjunto de informações citadas acima para a GC, esta gerência processa esse conjunto de informações por meio de um software especial de modo a definir os membros de backup dos FAs defeituosos. Este software executa os seguintes procedimentos:

- *Primeiro procedimento:* Para cada FA ativo é calculada a largura de banda disponível no link que conecta este agente a seu roteador de borda (Edge). Em seguida, as informações de retardo médio total para cada BTS tendo um dos FAs ativos como possível membro de backup são organizadas por ordem crescente. Caso duas ou mais BTSs possuam o mesmo valor de retardo, é dada prioridade àquela BTS que possui uma maior carga de tráfego dentre as que produzem os mesmos valores de

retardos.

- *Segundo procedimento:* Os FAs ativos são organizados por ordem decrescente quanto a sua capacidade de tráfego disponível.
- *Terceiro procedimento:* Para o FA que apresentou a maior carga de tráfego disponível, o software da GC tenta alocar todas as BTS's atingidas pelas falhas dos seus FA's nesta primeira opção. Portanto neste procedimento, os retardos introduzidos aos pacotes que partem ou se destinam a estas BTSs utilizando esta primeira opção como possível membro de backup, são comparados com um valor do retardo limiar, proposta entre 150 a 400ms, por ser essa faixa aceitável para serviços da classe conversacional onde as exigências de retardos são mais rigorosas. Caso o valor do retardo para uma determinada BTS em análise seja menor ou igual ao valor do retardo limiar, essa BTS é analisada quanto a introdução de sua carga de tráfego nesta opção de membro de backup. Caso essa carga de tráfego possa ser agregada neste FA em análise, essa BTS terá um caminho lógico configurado para esse FA. Caso não seja possível configurar essa BTS nesta primeira opção de membro de backup, tenta-se a segunda opção e assim por diante. Caso nenhuma das opções existentes de FA's possa ser usada, o quarto procedimento deve ser executado.
- *Quarto procedimento:* O retardo limiar desse software é automaticamente reconfigurado para receber o valor do menor retardo que um dos Agentes Estrangeiros ativos pode causar aos pacotes de dados caso este seja escolhido como membro de backup. Após a execução desta reconfiguração o terceiro procedimento é re-executado com este novo valor de limiar.

### C. Agentes de Origem

O procedimento adotado após a detecção de falha de um ou mais HA's é totalmente idêntico ao associado à falhas em um FA, distinguindo-se apenas nos critérios adotados para alocação dos HA's ativos como membros de redundância. Este tópico é detalhado na subseção seguinte.

1) *Alocação dos HA's como Membro de Backup:* Após receber as informações adequadas, a GC cria a lista de membros de backup dos HA's defeituosos por meio da seqüência dos seguintes procedimentos:

- *Primeiro procedimento:* Para cada HA ativo, sua carga de tráfego disponível é calculada e armazenada numa lista.
- *Segundo procedimento:* Para cada BTS associada a uma estação móvel afetada pela falha de seu HA, os retardos introduzidos aos pacotes de dados tendo cada HA ativo como possível membro de backup são determinados.
- *Terceiro procedimento:* Para cada BTS do procedimento anterior, as opções de HA's ativos são organizadas por ordem crescente quanto aos retardos introduzidos aos pacotes de dados. Em caso de empate, é dada prioridade ao HA que possui a maior banda disponível.
- *Quarto procedimento:* Todas as BTS's que possuem o mesmo HA como primeira opção de membro de backup

são inseridas numa nova lista que é ordenada quanto aos retardos médios introduzidos aos pacotes de dados.

- *Quinto procedimento:* Para cada uma destas listas, duas outras são criadas : 1) uma para as estações móveis atingidas pela falha do seu Agente de Origem e que utilizam os serviços de dados de taxa fixa como os de Vídeo Conferência e VoIP e 2) outra para os usuários também atingidos pela falha do mesmo HA e que utilizam serviços TCP, cuja vazão é difícil de estimar.

O passo seguinte é a alocação das estações móveis atingidas pela falha de seus Agentes de Origem na primeira opção disponível de membro de backup. Esse processo é executado para cada uma das listas acima criadas e é feito de forma a atender primeiramente as estações móveis com serviços de taxa fixa. Para o caso TCP, a carga de tráfego remanescente de cada HA é dividida entre as estações móveis da segunda lista. Caso o resultado dessa divisão seja superior a um limiar pré-definido de banda, estas estações móveis são alocadas nos seus respectivos Agentes de Origem de primeira opção de membro de backup. Caso contrário, o número de estações móveis da segunda sub-lista é decrementado e o processo de divisão é repetido. Cada estação móvel descartada neste processo compõe uma nova lista a ser possivelmente alocada na segunda opção disponível por meio de um procedimento idêntico. Esta atividade é repetida até que todas as estações móveis sejam alocadas a algum membro de backup.

## V. SIMULAÇÃO

Para a análise de desempenho, os resultados obtidos (proposta 1) são comparados com os aqueles obtidos quando se considera apenas o parâmetro carga de tráfego disponível nos Agentes de Mobilidade livres de falhas para a determinação dos membros de backup (proposta 2), que é a sugerida na literatura corrente.

### A. Ambiente de Simulação

A ferramenta de simulação aqui empregada foi o Network Simulator (NS-2) [6]. A arquitetura de rede utilizada é a ilustrada na figura 1, que consiste de 5 Agentes de Origem, 5 Agentes Estrangeiros, 10 roteadores de borda, sendo que cada um destes está conectado a um Agente de Mobilidade. Nela, o Core Network é constituído de 10 roteadores. Cada rede estrangeira também possui uma BSC que coordena as atividades de 4 Estações Base Transceptoras, perfazendo um total de 5 BSC's e 20 BTS's. Há uma rede de interconexão entre os roteadores de borda da rede estrangeira e as BSC's e nela, cada roteador de borda é conectado a BSC por meio de um enlace de 150 Kb/s de banda. Conectado aos roteadores do Core Network, há seis nós que simulam diferentes estações da rede fixa que utilizam os serviços VoIP e de Vídeo Conferência para comunicação com as estações móveis. Outro serviço também simulado foi o FTP, para o qual foram criados 4 servidores FTP. A tabela 1 ilustra os valores dos parâmetros utilizados para a simulação desses serviços, cujos valores de foram baseados nas referências [7],[8].

O ambiente de simulação conta com 320 estações móveis, sendo que cada Agente de Origem inicialmente gerencia 64

TABELA I

VALORES DOS PARÂMETROS UTILIZADOS NA SIMULAÇÃO DOS SERVIÇOS DE DADOS

Tipo de Serviço	Tamanho do Pacote (bytes)	Taxa de Transmissão (kbps)	Tempo Ativo (seg)	Tempo Ocioso (seg)
VoIP	210	12	1.4	1.7
FTP	1000	128	-	-
Video Conf.	1000	-	10	10

estações móveis. Destas, 35,63%, 35,31% e 29,06% utilizam respectivamente os serviços VoIP, Vídeo Conferência e FTP. As estações móveis deslocam-se com destinos e velocidades aleatórias.

O modelo de rádio propagação escolhido foi o de Sombreamento (*Shadowing Model*) cujos parâmetros utilizados são os referentes ao ambiente outdoor em área urbana, ou seja, desvio padrão de 8,0 dB e expoente de perda de propagação de 3.5. Para a reprodução de um ambiente outdoor que emprega o padrão IEEE 802.11, foram utilizadas as características do equipamento Air Plus DWL-900AP+ [9] que funciona como um ponto de acesso (AP).

### B. Resultados

1) *Tolerância à Falhas nos FA's:* Foram simulados no cenário descrito três falhas nos roteadores da rede estrangeira (FA).

A primeira falha ocorreu no Agente Estrangeiro 2 (FA02) aos 113 segundos da simulação. Pela nova proposta, os Agentes Estrangeiros 1 e 3 foram eleitos como membros de backup do agente defeituoso, enquanto que a proposta 2 apontou apenas o Agente Estrangeiro 1 .

Foi analisado o enlace entre o Agente Estrangeiro 1 e seu roteador de borda, sendo nele monitoradas as taxas de pacotes perdidos de todos os serviços. Não foram registradas perdas de pacote na simulação da proposta 1 e do cenário sem falhas. Já na proposta 2, foram registradas perdas de pacotes para os serviços FTP e de Vídeo Conferência, que podem ser explicadas pela sobrecarga em seu buffer a partir do instante da falha, pois este agente tornou-se membro de backup de todas as BTS's afetadas. Este fato indica que a introdução de mais um parâmetro no processo de decisão permite uma melhor distribuição da carga de tráfego dos agentes defeituosos. As perdas para o caso FTP podem ser vistas na figura 2 .

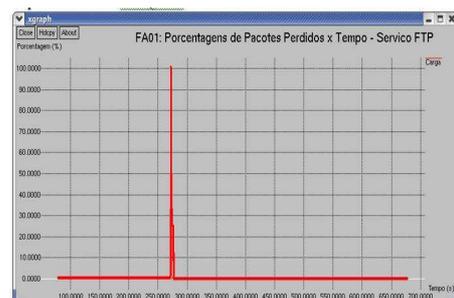


Fig. 2. Link FA01 Edge01: Taxa de perdas dos pacotes do serviço FTP.

Em seguida analisou-se o efeito que o mecanismo RED introduz na proposta 1 ao ser utilizado como gerenciador de buffer em todos os Agentes Estrangeiros. Embora não tenham sido registradas quaisquer tipo de perdas de pacotes no enlace em análise, observou-se que os picos de retardo passaram a ter um valor maior mas uma incidência menor quando comparados com os do mecanismo First In First Out (FIFO). A figura 3 ilustra o comportamento destes retardos e refletem o nível de sobrecarga do buffers desses dispositivos de rede. Verifica-se ainda que o monitoramento do tamanho da fila, realizado pelo mecanismo RED, permitiu acomodar as pequenas rajadas de pacotes de dados que ocorreram entre 100 e 200 segundos, sem produzir sobrecargas no buffer do FA01.

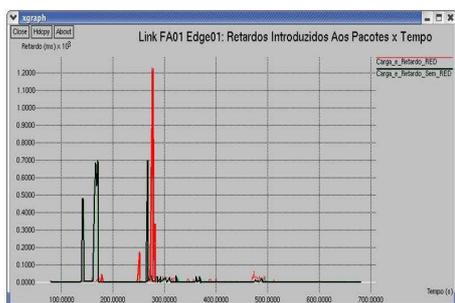


Fig. 3. Link FA01 Edge01: Efeito do mecanismo RED no enlace em análise.

Esta análise foi repetida para o enlace que conecta o Agente Estrangeiro 3 ao seu roteador de borda. Para o serviço de vídeo conferência foram registradas perdas de pacotes de dados de respectivamente 3,25% e 6,25% nas propostas 1 e 2. Este fato indica que mesmo antes desse agente tornar-se membro de backup de qualquer agente defeituoso, seu buffer operava em regime de sobrecarga. Para o serviço FTP foram registradas perdas nas proposta 1 e 2, enquanto que para o serviço VoIP, a perda foi registrada apenas na proposta 1.

As razões para estas perdas podem ser encontradas na análise da figura 4 que descreve o comportamento dos retardos medidos até o roteador de borda da rede estrangeira 3 (Edge03), pois estes refletem o nível da carga de tráfego que este agente passa a experimentar ao tornar-se membro de backup do FA02 defeituoso.

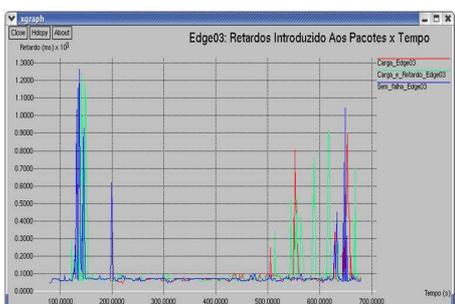


Fig. 4. Retardos médios medidos até o roteador de borda 3.

A perda registrada na proposta 2 de 6,25% no serviço de vídeo conferência pode ser explicada pois o FA02 falhou 14 segundos antes de sua ocorrência e o processo de sinalização

produziu retardos de enfileiramento nos roteadores do Core Network, fazendo com que esta perda não fosse registrada naquele instante. Provavelmente essa perda deve ter ocorrido em algum roteador do Core Network próximo ao Agente Estrangeiro analisado.

A pequena perda de 3,25% no serviço de Vídeo Conferência na proposta 1 ocorreu no instante 202 segundos. Ela pode ser explicada pelo efeito que o processo de sinalização teve sobre o *Time To Live* desses pacotes. Como pode ser visto na figura 4, não foi registrado nenhum pico de retardo significativo próximo ao instante mencionado, podendo-se estender esta explicação para as perdas no serviço VoIP registradas nos instantes de 202 e 203 e de 486 a 489 segundos da simulação da nova proposta.

Outra observação importante a ser comentada nos serviços de Vídeo Conferência e FTP da simulação da proposta 2 é o registro de perdas de pacotes no intervalo entre 527 e 531 segundos. Nesse intervalo não se registrou nenhuma perda de pacotes, revelando que a carga adicional de tráfego na proposta 2 foi direcionada para o Agente Estrangeiro FA01, afetando o desempenho do FA03 que não é membro de backup do agente defeituoso FA02.

Analisando o intervalo de 500 a 600 segundos da simulação, é possível notar na figura 4 que na proposta 1, os picos de retardos passam a ocorrer mais frequentemente do que na proposta 2. Isto se deve ao fato de que, além do efeito que a carga de tráfego adicional direcionada ao FA01 produziu sobre o FA03, há o efeito da carga de tráfego adicional que o FA03 recebeu ao tornar-se também membros de backup do FA02. Esses picos de retardos observados na nova proposta são frutos da sobrecarga que o FA03 registra neste intervalo de tempo e explicam as perdas que nela ocorrem.

Quanto a introdução do mecanismo RED no buffers dos FA's, observou-se no enlace em análise que as taxas de pacotes perdidos para os serviços de Vídeo Conferência e FTP ocorreram de forma mais intensa e duradoura. Para explicar essas perdas, a probabilidade de descarte de pacotes (figura 5) foi monitorada no buffer desse dispositivo. Tais perdas estão relacionadas com o princípio básico de funcionamento deste dispositivo, que não espera até que o buffer fique cheio para iniciar o seu mecanismo de descarte.

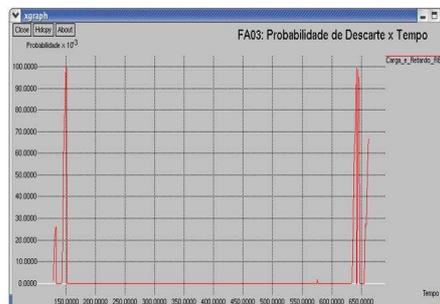


Fig. 5. Probabilidade de descarte de pacotes monitorada no buffer do FA03.

Na ocorrência da segunda falha, a GC selecionou em ambas as propostas o FA05 como membro de backup do FA04 defeituoso. Quanto à utilização do mecanismo RED, foi possível notar um aumento de 20,41% no número de pacotes que

chegam a esse membro de backup (FA05). Esse mecanismo produziu um efeito positivo sobre a taxa de transmissão média da rede, pois evitou a ocorrência de oscilações.

Na ocorrência da terceira falha, nota-se uma confirmação das observações feitas quando da primeira falha. A proposta 1 permitiu uma melhor distribuição da carga de tráfego dos agentes defeituosos, enquanto que na proposta 2, as perdas registradas ocorreram com mais frequência e intensidade. Quanto a introdução do mecanismo RED na proposta 1, foi possível observar que em grandes rajadas de pacotes de dados, as perdas de pacotes ocorreram de forma mais intensa e com frequência maior nos buffers dos Agentes Estrangeiros determinados como membros de backup.

2) *Tolerância à Falha nos HAS*: Foram simuladas três falhas nos roteadores da rede de origem (HA) e os resultados são mostrados a seguir. Para cada BTS que possui sob sua área de cobertura pelo menos uma estação móvel afetada pela falha de seu HA, foi monitorado o comportamento do retardo produzido nos pacotes.

A primeira falha ocorreu no instante 277 segundos no Agente de Origem 2 (HA02). O emprego da proposta 1 determinou que as estações móveis atingidas por esta falha e que estavam sob a área de cobertura da BTS5, fossem alocadas ao Agente de Origem 4. Já na proposta 2, estas mesmas estações móveis foram alocadas no Agente de Origem 5. Na figura 6 é possível verificar que a nova proposta apresentou melhores resultados. Nela, o Agente de Origem 4, além de ser a primeira opção de membro de backup quanto ao menor retardo introduzido aos pacotes, é também a segunda opção de membro de backup quanto à carga de tráfego disponível. Esse fato vem confirmar que a melhor forma de se determinar os membros de backup dos agentes defeituosos é analisando simultaneamente os dois parâmetros: retardo introduzido aos pacotes de dados e a carga de tráfego disponível nesses agentes ativos livres de falha.

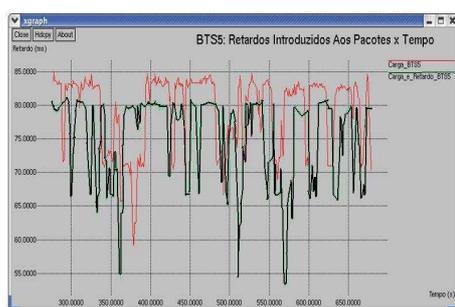


Fig. 6. Primeira falha: Retardos médios medidos até BTS5.

A segunda falha ocorreu no instante 344 segundos no Agente de Origem 4 (HA04). Na nova proposta, as estações móveis da área de cobertura da BTS9 foram alocadas ao HA05, enquanto que na proposta 2, estas estações foram alocadas ao HA03. A terceira e última falha ocorreu no instante 419 segundos, no Agente de Origem 3 (HA03). Na proposta 1, as estações móveis da área de cobertura da BTS13 foram alocadas ao HA05, enquanto que na proposta 2, estas estações foram alocadas ao HA01. Em todos os casos, nos instantes imediatamente após a ocorrência da falha, a nova

proposta apresentou um desempenho melhor ou semelhante ao da proposta 2.

## VI. CONCLUSÕES

A nova proposta de tolerância à falhas dos agentes apresentada neste artigo consegue promover uma distribuição mais equânime da carga de tráfego dos FA's defeituosos entre os membros de backup. Essa melhor distribuição produz uma menor sobrecarga nos buffers destes agentes quando comparada com a de referência, permitindo um melhor comportamento quanto ao retardo e perdas de pacotes. Esse fato é de extrema importância para os cenários que vêm sendo desenhados para as futuras gerações dos sistemas celulares, onde as exigências de QoS tornar-se-ão cada vez mais severas.

Quanto à introdução do mecanismo RED, foi possível verificar que as pequenas rajadas de pacotes são acomodadas sem produzir sobrecargas frequentes. Entretanto, na condição de grandes rajadas, observou-se um aumento na duração e intensidade das perdas de pacotes, pois esse mecanismo não espera que o buffer se lote para iniciar a sua ação.

Quanto à tolerância à falha dos Agentes de Origem, observou-se nos instantes seguintes à ocorrência da falha, a nova proposta apresentou um desempenho melhor ou semelhante àquele da proposta de referência.

É possível também notar que a nova proposta é mais flexível quando comparada com a de referência, pois nesta as melhores opções de membro de backup são aquelas que apresentam apenas os menores retardos introduzidos aos pacotes. Sendo assim, a nova proposta consegue distribuir melhor a carga de tráfego das estações móveis atingidas pela falha do seu Agente de Origem e impor um menor retardo aos pacotes de dados.

## AGRADECIMENTOS

Pesquisa apoiada pelo CETUC/PUC-RIO. Luciano da Silva Santos fez mestrado na PUC/Rio financiado pela CAPES e atualmente é engenheiro da operadora Oi. Marco Grivet reconhece o suporte da bolsa de produtividade do CNPq.

## REFERÊNCIAS

- [1] Perkins, C.E.(Ed.), *IPMobility Support for Ipv4*, Internet RFC 3220, Category: Standards Track, January 2002.
- [2] Kwon, T. T.; Gerla, M., *Mobility Management For VoIP Service: Mobile IP vs. SIP*, IEEE Wireless Communications, pp. 66-75, October 2002.
- [3] Ghosh, R.; Varghese, G., *Fault-Tolerant Mobile IP*, Technical Report WUCS-98-11, Washington University, April 1998.
- [4] Hong, C. S et al., *An Efficient Fault Tolerance Protocol with Backup Foreign Agents in a Hierarchical Local Registration Mobile IP*, ETRI Journal, Vol 24, no 1, February 2002.
- [5] Lin, J.W.; Arul, J., *An Efficient Fault Tolerant Approach for Mobile IP in Wireless Systems*, IEEE Transactions On Mobile Computing, Vol 2, no 3, July-September 2003.
- [6] Fall, K.(Ed.); Varadhan, K. (Ed.), *The ns Manual*, Disponível em: <http://www.isi.edu/nsnam/ns/ns-documentation.html>.
- [7] 3GPP Technical Standards TS 22.105. Service and Service Capabilities *Service and Service Capabilities*, 2001.
- [8] Vassiliou, J. A. et al., *A Simulation Environment for Enhanced UMTS Performance Evaluation*, Framework of IST-2001-34900 SEACORN project.
- [9] Wireless Equipment (IEEE 802.11), *D-Link Air Plus DWL-900AP+*, disponível em [http://www.link.ca/datasheets/DWL-900AP+\\_ds.pdf](http://www.link.ca/datasheets/DWL-900AP+_ds.pdf).
- [10] Peterson L.L.; Davie S.B., *Computer Networks: A systems Approach*, 4.th Ed., Morgan Kaufmann Publishers, 2007.
- [11] Luciano da Silva Santos, *Tolerância a Falhas dos Agentes de Mobilidade do Protocolo Mobile IP*, Dissertação de Mestrado, PUC-Rio, Agosto de 2005.