Universidade do Estado de Santa Catarina (UDESC)
Mestrado em Computação Aplicada
Disciplina de Redes de Computadores (Profª Dra Janine Kniess)

Resumo “BGP resiliente escalável - recuperação rápida de link transitório entre domínios Falhas”

Acadêmico: Sergio Henrique Silva

O trabalho analisado tem como objetivo principal melhorar a confiabilidade de serviços e missão crítica na internet. Falhas na garantia de desempenho são muito comuns na internet, e aplicações de missão crítica como Voice-over-IP ou VOIP, jogos online e outros aplicativos em tempo real dependem da confiabilidade em requisições. O artigo justifica que existem muitas falhas nessas requisições e propõe criar uma solução para melhorá-las, podendo garantir um melhor serviço nessas aplicações.

O trabalho apresenta contribuições relativamente importantes em relação aos trabalhos relacionados da área, pois em abordagens tradicionais as falhas de link de forma reativa. Na literatura encontrada pelo autor, as propostas se concentraram em reduzir tempos de convergência [6] [2] [3] [5], no entanto esses métodos são limitados pela largura de banda e pela complexidade do BGP (Policy-Based Protocol). Como alternativa, à abordagem proativa é apresentada.

Bonaventure et al [5] propõem uma solução usando túneis pré-estabelecidos para redirecionar o tráfego durante as falhas de link. Esta abordagem é apropriada para resolver o problema de falhas transitórias de roteamento ocorrendo no peering eBGP links. Já o R-BGP pré-computa alguns escolhidos estrategicamente em caminhos de que falham e mantém consistência de estado suficiente em todo o domínio para garantir a disponibilidade de caminho contínuo.

O método mais recente, BRAP [4] pode fornecer localmente rotas alternativas na ocorrência de falhas. Métodos proativos garantem que domínios da Internet se recuperem rapidamente de falhas transitórias de link. Porém, a limitação de memória de encaminhamento necessária tem que ser dobrada.

No artigo, os autores propõem uma nova técnica de recuperação rápida, chamado BGP resiliente escalável (SR-BGP), que poderia fornecer restauração rápida na ordem de milissegundos após falhas de link de domínio. O mais importante é que essa solução criada pelos autores, não causa o aumento do tamanho da tabela de roteamento BGP. Os resultados dos experimentos manifestam que o tamanho da tabela de roteamento aumenta 1,2% da corrente, no máximo. Na resiliência a falhas de link de SR-BGP é semelhante a outros abordagens.

De maneira geral, a proposta do autor é um protocolo inter-escalável e resiliente de roteamento de domínio. Desta forma a proposta se desenha como uma técnica de recuperação e resiliência em domínios da internet e endpoints para requsições.

Na elaboração da proposta os autores utilizam de um método onde cada BGP faz o roteamento e mantém as informações de roteamento aprendidas com vizinhos, com isso ele seleciona a melhor rota com base na política local em vez de escolher o mais curto e anuncia a melhor rota para seus próprios vizinhos seguindo a política de exportação.

Na elaboração do trabalho os autores fazem uma revisão sobre os principais conceitos envolvidos na proposta. Faz uma visão geral sobre o redirecionamento com túneis protegidos, bem como faz uma análise da identificação da saída do túnel protegido nas requisições. Os autores ainda trabalham os conceitos relativos à propagação das rotas e túneis, a seleção de rotas de transferência e o encaminhamento de pacotes.

Por fim, os autores fazem uma avaliação como discussão dos resultados da proposta apresentada. Os autores analisam a resiliência de domínios chamados de dual-homed para tratar as falhas e também o tamanho das tabelas de roteamento na solução proposta.

Como conclusões os autores apontam que a chave da abordagem é redirecionar o tráfego para um túnel protegido pré-estabelecido que não é influenciado pela falha do link. Usando um túnel protegido e rota de transferência correspondente, esta abordagem pode maximizar o número de caminhos disponíveis e minimizar o tamanho da tabela de roteamento para que possa fornecer mais resiliência e mais escalabilidade.

Observando de maneira crítica o artigo, observa-se que o artigo é bastante conciso e apresenta a proposta de maneira direta e sem rodeios porém, por mais que ele faça uma comparação com outras propostas a comparação poderia ser mais esmiuçada. Outro ponto importante é que em que pese o problema a ser resolvido seja apresentado claramente, os autores poderiam fazer uma defesa mais clara indicando aplicações mais práticas de onde este problema resolve questões mais objetivas.

Após a publicação deste trabalho, os autores propuseram outros trabalhos na mesma linha. O primeiro deles trata da redução da perda de pacotes burst por meio de encaminhamento sem rota[6], o trabalho é mais focado na redução de perdas e em encaminhamentos de dados que não necessariamente tem uma rota de encaminhamento definida.

Outro trabalho realizado pelos autores tem o objetivo de elaborar uma proposta que possa reduzir a perda de pacotes com redirecionamento baseado em túnel de proteção. Focando na consistência dos dados e no menor número de perda no encaminhamento de dados com a segurança propiciada por um tunelamento. [7]

Ainda relativo às extensões do trabalho realizadas pelos autores, os mesmo se propõe a melhorar a conectividade em redes multi-provedores também com tunelamento. [8]

De maneira geral, a pesquisa e suas extensões tem um problema relevante e uma atualidade significativa, haja vista que, assim como os autores defendem, existe cada vez mais uma demanda por conexões com baixas perdas e baixa tolerância a falhas em aplicações críticas. Esta importância pode ser observada não só no contexto acadêmico mas também em aplicações mercadológicas.

[1] A. Bremler-Barr, Y. Afek, and S. Schwarz. “Improved BGP convergence via ghost flushing”. In Proc. INFOCOM, vol.2 2003, pp.927-937.

[2] D. Pei et al. “Improving BGP convergence through consistency assertions”. In Proc. INFOCOM, vol. 2, 2002, pp.902-911.

[3] D. Pei et al. “BGP-RCN: Improving BGP convergence through root cause notification”. Computer Networks Journal, Vol. 48, Issue 2, 2005, pp. 175-194.

[4] F. Wang, L. Gao. “A backup route aware routing protocol – Fast recovery from transient routing failures”. In Proc. INFOCOM, 2008. [5] O. Bonaventure, C. Filsfils, and P. Francois. “Achieving sub-50ms recovery upon BGP peering link failures”. In Proc. Co-Next, 2005.

[5] J. Lou, J. Xie, R. Hao, X. Li. “An approach to accelerate convergence for path vector protocol”. In Proc. Globecom, vol. 3, 2002, pp. 2390-2394.

[6] Ma, Hailong & Guo, Yunfei & Cheng, Dongnian & Zhang, Jianwei. (2010). Reducing burst packet loss through route-free forwarding. Journal of Electronics (China). 27. 363-370. 10.1007/s11767-010-0324-8.

[7] Ma, Hailong & Guo, Yunfei & Cheng, Dongnian. (2011). Reducing packet loss with protection tunnel based rerouting. Journal of Electronics (China). 28. 10.1007/s11767-011-0714-6.

[8] Ma, Hailong & Guo, Yunfei & Zhang, Jianwei. (2009). Improving the Connectivity of Multi-providers Network with Protected Tunnel. Proceedings of the 2009 Pacific-Asia Conference on Circuits, Communications and System, PACCS 2009. 706-709. 10.1109/PACCS.2009.158.