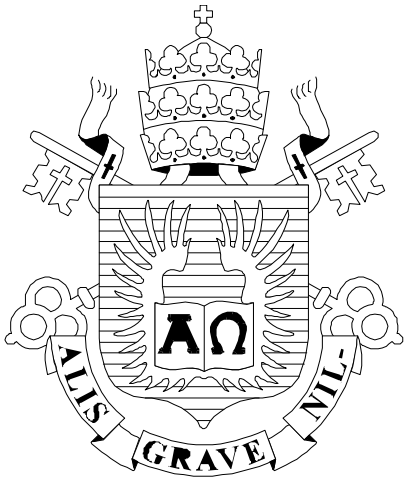

PUC

ISSN 0103-9741

Monografias em Ciência da Computação
n° 04/10

Gerenciamento Autonômico de Redes: Participação do LES no Projeto *Horizon*

Carlos José Pereira de Lucena Firmo Freire
Viviane Torres da Silva
Baldoino Fonseca dos Santos Neto
Manoel Teixeira de Abreu Netto
Elder José Reioli Cirilo Ingrid Oliveira de Nunes
Dárlinton Barbosa Feres Carvalho

Departamento de Informática

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO
RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22453-900
RIO DE JANEIRO - BRASIL

Monografias em Ciência da Computação, No. 04/10 ISSN: 0103-9741
Editor: Prof. Carlos José Pereira de Lucena 04, 2010

Gerenciamento Autonômico de Redes: Participação do LES no Projeto *Horizon*

Carlos José Pereira de Lucena, Firmo Freire, Viviane Torres da Silva[1]

Baldoino Fonseca dos Santos Neto, Manoel Teixeira de Abreu Netto,

Elder José Reioli Cirilo, Ingrid Oliveira de Nunes, Dárlinton Barbosa Feres Carvalho

[1]Departamento de Ciência da Computação – Universidade Federal Fluminense (UFF)
bneto@inf.puc-rio.br, mnetto@inf.puc-rio.br, viviane.silva@ic.uff.br,

ecirilo@inf.puc-rio.br, lucena@inf.puc-rio.br, firmo@inf.puc-rio.br,

ionunes@inf.puc-rio.br, darlinton@gmail.com

Abstract. The Laboratory of Software Engineering (LES) intends to use the research developed in the context of multi-agent systems to enable the Horizon project to incorporate intelligence and autonomy into network management systems. It will be performed through the development of an infrastructure based on self-organizing agents regulated by norms and situated into the different network devices which will be endowed with rationality, reactivity, pro-activity and sociability.

Keywords: Autonomic Management, Multi-agent Systems.

Resumo. O Laboratório de Engenharia de Software (LES) visa utilizar os trabalhos desenvolvidos no contexto de sistemas multiagentes para dar suporte ao projeto *Horizon* na incorporação de inteligência e autonomia nos sistemas de gerenciamento de redes. Isto será realizado por uma infra-estrutura baseada em agentes auto-organizáveis regulados por normas, situados nos diferentes dispositivos que compõe a rede, e dotados de racionalidade, reatividade, pró-atividade e sociabilidade.

Palavras-chave: Gerenciamento Autonômico de Redes, Sistemas Multiagentes.

Responsável por publicações:

Rosane Teles Lins Castilho
Assessoria de Biblioteca, Documentação e Informação
PUC-Rio Departamento de Informática
Rua Marquês de São Vicente, 225 - Gávea
22453-900 Rio de Janeiro RJ Brasil
Tel. +55 21 3114-1516 Fax: +55 21 3114-1530
E-mail: bib-di@inf.puc-rio.br
Web site: http://bib-di.inf.puc-rio.br/techreports/

1 Introdução

Desde sua origem, a Internet tem crescido e o seu uso está cada vez mais diversificado. Estima-se que, em dezembro de 2008, a Internet já havia passado a marca de um bilhão e meio de usuários. No entanto, apesar de essa expansão do uso da rede indicar aprovação e aceitação por parte dos usuários, algumas limitações começam a surgir para atender novos requisitos como segurança, confiabilidade, disponibilidade e qualidade de serviço.

Isto porque os requisitos levantados para a Internet na década de 70 correspondiam a uma rede entre universidades onde os usuários eram confiáveis e tinham conhecimentos técnicos sobre a rede. Hoje, a realidade é diferente, pois pessoas com todo tipo de formação e distribuídas por todo o globo têm acesso à rede, criando um ambiente totalmente distinto e cheio de conflitos [Clarck, Wroclawski, Sollins and Braden, 2005] .

Além disto, a Internet foi projetada dando ênfase à descentralização, generalidade e heterogeneidade na camada de rede. Sua estrutura é baseada nos princípios de um núcleo de rede simples e transparente com a inteligência nos sistemas finais que são ricos em funcionalidades. Hoje, no entanto, esses princípios levam a usuários frustrados quando algo não funciona, pois os nós do núcleo não são capazes de solucionar problemas automaticamente. Isto implica em uma alta sobrecarga para depuração de erros e configuração manual.

Diante do cenário apresentado, existe um consenso de que a Internet precisará ser reformulada, criando a "Internet do Futuro". Essa nova Internet deve manter os princípios que levaram ao sucesso atual, tais como a facilidade para implantação de novas aplicações e a adaptabilidade de seus protocolos, mas as entidades que a compõem devem ser capazes de realizar autonomamente tarefas, tais como auto-configuração (realiza reconfiguração automaticamente em função de mudanças), auto-cura (reages a disfunções e mau funcionamento em tempo de execução), auto-otimização (otimiza recursos automaticamente), auto-proteção (protege-se contra ataques inesperados) e, por fim, auto-organização.

Neste contexto, a equipe do Laboratório de Engenharia de Sofware da PUC-Rio (LES) tem utilizado o paradigma de sistemas multiagentes que visa a construção de sistemas compostos por entidades, chamadas agentes, com capacidade de autonomia, pró-atividade, reatividade e sociabilidade, objetivando incorporar no projeto *Horizon* a inteligência e autonomia necessária para efetivação das tarefas supracitadas.

2 Fundamentação

2.1 Sistemas MultiAgentes (SMA)

SMA são sistemas compostos por entidade inteligentes, chamadas agentes. Segundo [Wooldridge, 2002] um agente é um sistema computacional que está situado em algum ambiente e que é capaz de ações autônomas neste ambiente como forma de alcançar os seus objetivos definidos em sua modelagem.

Por definição, um conjunto de propriedades pode ser atribuído aos agentes de software:

- Autonomia: capacidade de decidir suas ações sem intervenção externa, por exemplo, por um usuário.
- Reatividade: os agentes são capazes de perceber o ambiente em que estão inseridos e reagir em tempo hábil e de forma adequada para satisfazerem os objetivos que foram modelados.
- Pró-Atividade: os agentes são capazes de exibir comportamentos baseados em metas, tomando iniciativas para a realização dos seus objetivos.
- Sociabilidade: os agentes são capazes de interagir com outros agentes do sistema e através desse relacionamento buscar maneiras de atingir seus objetivos propostos.

2.2 Auto-organização

Auto-organização é definida em [Serugend, Gleizes and Karageorgos, 2005] como o mecanismo ou processo que permite a um sistema lidar com o dinamismo, crescimento da distribuição, complexidade e mudanças dinâmicas nos requisitos, em tempo de execução, sem um comando externo explícito.

2.3 Normas

Sistemas multi-agentes abertos são sociedades em que entidades autônomas, heterogêneos e independentemente projetadas podem trabalhar para semelhantes ou diferentes fins. A fim de lidar com a heterogeneidade, autonomia e diversidade de interesses entre os diferentes membros, tais sistemas estabelecem um conjunto de normas que são utilizadas como um mecanismo de controle para garantir uma ordem desejável em que os agentes possam trabalhar em conjunto [Lopez, 2003].

Tais normas regulam o comportamento dos agentes definindo obrigações (indica que os agentes são obrigados a realizar algo), a permissão (indica que os agentes estão autorizados a agir de uma maneira particular) e proibições (indica que os agentes são proibidos de agir de uma determinada maneira). Além disso, as normas podem dar estímulo para a sua realização através da definição de recompensas e pode desencorajar a sua violação, declarando punições.

2.4 Confiança

Confiança é a segurança, certeza daquele que tem fé na probidade (honradez, integridade de caráter, honestidade) de alguém [Guedes, Silva and Lucena,2006] .

2.5 Reputação

Reputação pode ser entendida como a avaliação social (opinião) que uma entidade possui sobre uma outra entidade, grupo de entidades ou organização [Guedes, Silva and Lucena,2006] .

3 Problemas e Soluções

3.1 Segurança

Usuários, provedores de serviço, indústria e desenvolvedores de aplicações têm manifestado cada vez mais preocupação com aspectos de segurança. Não há mais como ignorar as graves ameaças de segurança que hoje se proliferam pela Internet, como a disseminação de vírus e cavalos de Tróia, a negação de serviço [Laufer and et. Al., 2005] e o envio de *spams* [Taveira, Moraes, Rubinstein and Duarte, 2006]. As perspectivas para o futuro da guerra dos sistemas de defesa contra os atacantes são desanimadoras. As formas de ataque estão se tornando cada vez mais sofisticadas e se adaptam às evoluções dos sistemas de defesa, levando a crer que tal guerra não terminará tão cedo. Não obstante, a arquitetura da Internet atual não prevê nenhum mecanismo que limite o comportamento das estações-finais maliciosas e proteja as estações corretas. Quando os primeiros ataques surgiram na Internet, os defensores do paradigma fim-a-fim diziam que os problemas de segurança deveriam ser tratados pelas estações-finais. No entanto, o enorme crescimento dos ataques distribuídos de negação de serviço (*Distributed Denial-of-Service - DDoS - attacks*) indicou que pelo menos alguns mecanismos de segurança devem ser providos pelo núcleo da rede. Além disso, a atual arquitetura não prevê nenhum tipo de proteção contra ataques aos próprios elementos de rede.

Uma das principais causas que motiva todos os problemas de segurança atuais é a ausência da segurança no projeto da arquitetura da rede. Uma vez que a rede, inicialmente, era utilizada apenas por usuários confiáveis e que possuíam conhecimento técnico, não existia necessidade de criar mecanismos para proteger a infra-estrutura ou os usuários da rede. Com a comercialização da Internet, milhares de usuários começaram a participar da rede, trazendo inúmeras ameaças. Não apenas os usuários maliciosos causam problemas, mas também os usuários que não possuem conhecimento técnico suficiente para manter sua máquina atualizada e livre de ameaças. Nesses casos, é possível transformar a máquina de um usuário não-malicioso em um robô (*bot*) para realizar ataques distribuídos de negação de serviço ou ainda torná-la um disseminador de vírus e outras pragas virtuais. Assim, a arquitetura que antes provia um serviço confiável e seguro, hoje se mostra frágil e incapaz de prover robustez aos requisitos básicos.

Diante deste cenário nota-se que as principais falhas de segurança da Internet, encontra-se na ausência de mecanismos capazes de identificar e responsabilizar as diferentes entidades presentes na rede em resposta as suas ações [Andersen and et. Al, 2008].

Neste contexto, uma solução promissora é a utilização de normas para regular as ações de tais entidades através de obrigações, permissões e proibições, e realizar punições ou premiações em resposta ao cumprimento ou não de tais normas, por exemplo a reputação ou confiança de uma determinada entidade poderia ser incrementada ou decrementada de acordo com as suas atitudes.

3.2 Confiabilidade da Rede e Disponibilidade dos Serviços

Os provedores de serviço (*Internet Service Providers - ISPs*) têm como desafio a oferta de um serviço de rede confiável, robusto e sempre disponível. Entretanto, a atual infra-estrutura de rede não possui a confiabilidade da rede telefônica, que oferece disponibilidade da ordem de três noves, ou 99,9%, e que tem como meta chegar a mais de cinco noves através de redundâncias e equipamentos de alta confiabilidade.

Um serviço que é afetado de forma especial por essa falta de confiança é a telefonia IP. Com o advento da tecnologia de voz sobre IP (*Voice over IP* - VoIP), muitos acreditaram que esse serviço substituiria a telefonia convencional. Entretanto, alguns serviços de emergência como polícia, bombeiro e hospitais não podem ser baseados em um sistema com baixa confiabilidade. Além disso, muitas empresas preferem arcar com os custos da telefonia tradicional para possuir um serviço confiável. Outra questão importante é que muitos problemas na Internet atual são detectados devido à notificação da falha aos administradores por usuários.

Uma vez que o perfil majoritário dos usuários da Internet é de pessoas que não têm conhecimento técnico, a ausência de mecanismos capazes de realizar automaticamente diagnósticos e correção de erros na rede causa grande insatisfação. Isso demonstra a necessidade de soluções capazes de realizar tarefas, tais como auto-cura e auto-configuração.

3.3 Sistemas de Controle

A Internet carece de sistemas de controle eficientes. Esse problema fica mais evidente nas redes de nova geração, formadas por dispositivos como sensores, celulares e PDAs, nos quais a energia deve ser poupada. *Nesses casos, mecanismos de controle distribuídos devem ser projetados de forma a economizar a bateria dos dispositivos. Assim, a criação de sistemas capazes de realizar auto-otimização sem sobrecarregar os dispositivos conectados é uma solução promissora.*

3.4 Qualidade de Serviços

A demanda cada vez maior pela transmissão de voz, vídeo e aplicações de entretenimento, como jogos online, deixa evidente a necessidade da implantação de mecanismos que melhorem a qualidade de serviço, a exemplo diminuição do tempo que um pacote leva do remetente ao remetente. Entretanto, a Internet faz seu melhor esforço para transportar cada pacote o mais rapidamente possível, mas não faz nenhuma promessa sequer sobre o atraso fim-a-fim para um pacote individual.

Neste contexto, a arquitetura Diffserv [IETF, 2010] cujo objetivo é introduzir classes de tráfego, designar cada pacote a uma das classes, atribuir diferentes níveis de serviços nas filas de roteadores aos pacotes conforme suas classes e cobrar dos usuários segundo a classe a que eles pertencem, parece ser uma iniciativa promissora. *Entretanto, considerando que atualmente milhares de usuários participam da Internet, trazendo inúmeras ameaças, a fim de alcançarmos uma Internet confiável, disponível e segura não basta utilizarmos uma política de preços para definir novas classes, mas também é necessário premiarmos aqueles que contribuem para a estabilidade da rede e punir, caso contrario. Ou seja, usuários devem ser alocados em classes não levando em consideração somente o seu poder aquisitivo, mas também atributos que o caracterizam, tais como reputação, confiança, etc.*

4 Trabalhos Desenvolvidos no LES

Como resultado das dissertações, teses e pós-doutorados elaboradas nos últimos anos pelo grupo do LES, importantes contribuições têm sido feitas no âmbito dos diferentes conceitos abordados na seção anterior, tais como normas, reputação, confiança, auto-cura, auto-configuração e auto-organização. Segue abaixo uma breve descrição de alguns destes trabalhos:

1. **Normas**: Uma linguagem para representação de normas onde é possível especificar a entidade responsável por cumprir uma determinada norma, e as punições e recompensas provenientes do cumprimento ou não de tal normas. Tal linguagem pode ser vista em [Silva, 2008] .
2. **Reputação e Confiança**: DRPMAS [Costa, Lucena, Cowan and Alencar, 2008], um *framework* de recomendação que oferece suporte a diferentes métodos e modelos de reputação e confiança.
3. **Auto-***(Auto-cura, Auto-configuração, Auto-Proteção, Auto-Otimização e Auto-Organização)
    a. JAAF [Neto, Costa, Netto, Silva and Lucena, 2009], um *framework* que possibilita a implementação de mecanismos capazes de coletar informações sobre a execução de um determinado recurso, analisar tais informações a fim de descobrir soluções para eventuais problemas, decidir qual a melhor solução e, por fim, efetivar a solução selecionada. Desta forma, possibilitando a realização de auto-cura, auto-configuração, auto-proteção e auto-otimização.
    b. Um método de engenharia baseado em simulação para apoiar o projeto, desenvolvimento, simulação, validação e refinamento de sistemas multi-agentes auto-organizáveis e uma arquitetura baseada em simulação. Tais trabalhos podem ser vistos em [Gatti, 2009].
    c. GenArch [Cirilo, Nunes, Kulesza and Lucena], uma ferramenta de derivação de linhas de produto de software está sendo estendido a-fim de possibilitar sobre possíveis adaptações em uma linguagem de alto nível que expressa as variabilidades do sistema e automaticamente derivar ações de adaptação a partir de modelos arquiteturais.

5 Visão Geral da Proposta

Diante do apresentado, o LES visa utilizar os trabalhos desenvolvidos pela sua equipe a fim de possibilitar a construção de sistemas multiagentes capazes de realizar auto-organização guiada por normas, tais agentes presentes no sistema estão distribuídos entre os diferentes dispositivos presentes na rede e são dotados de autonomia, racionalidade, reatividade, pró-atividade e sociabilidade, como apresentado na. Com isso, possibilitando a incorporação de inteligência e autonomia ao projeto *Horizon*.

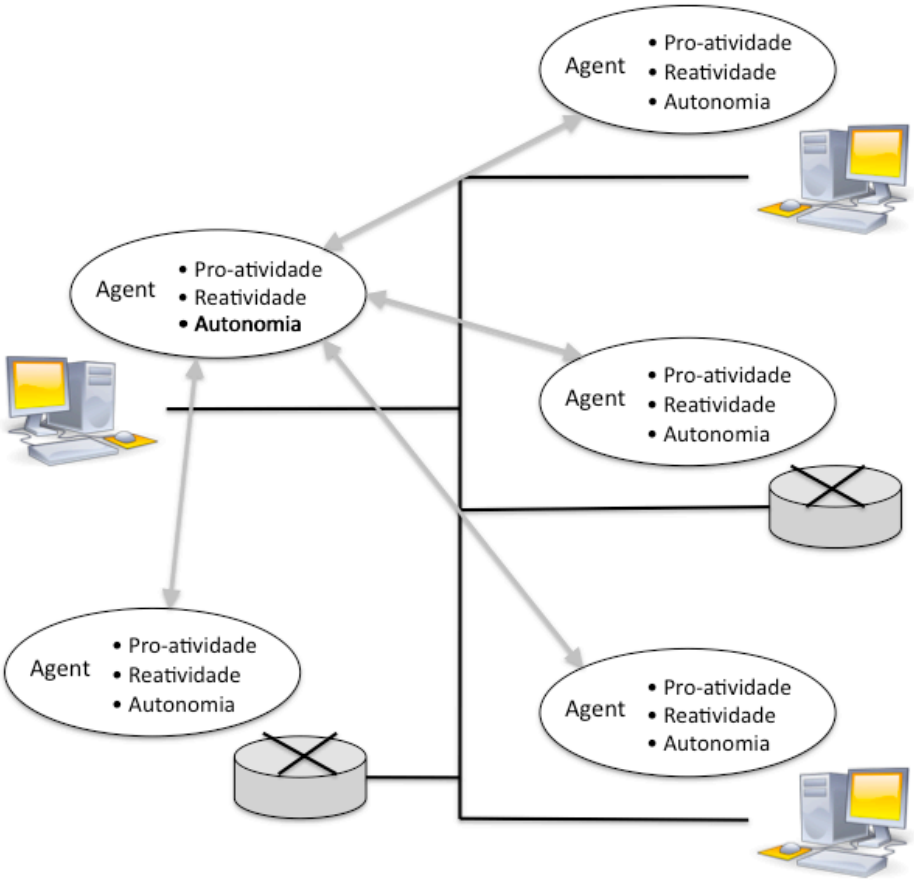

Figure 1: Visão Geral da Internet do Futuro

Referências Bibliográficas

[Clarck, Wroclawski, Sollins and Braden, 2005] Clark, D. D., Wroclawski, J., Sollins, K. R. e Braden, R. (2005). Tussle in Cyberspace: Defining Tomorrow's Internet. *IEEE/ACM Transactions on Networking*, 13(3):462–475.

[Wooldridge, 2002] M. Wooldridge. An introduction to multiagent systems. Wiley,

2002.

[Serugend, Gleizes and Karageorgos, 2005] Serugendo, G. Di M., Gleizes, M.-P. and Karageorgos, A. "Self-Organisation in MAS", Knowledge Engineering Review 20(2):165-189, Cambridge University Press, 2005.

[Lopez, 2003]F. Lopez-Lopez. Social Power and Norms: Impact on agent behavior. PhD thesis, University of Southampton, 2003.

[Guedes, Silva and Lucena,2006] GUEDES, José de Souza Pinto ; SILVA, Viviane Torres da ; LUCENA, C. J. P. . A Reputation Model Based on Testimonies. In: Workshop on Agent-Oriented Information System (AOIS) at the 18th Conference on Advanced Information Systems Engineering (CAiSE), 2006, Gran Ducado de Luxemburgo. Proceedings, 2006. p. 37-47.

[Laufer and et. Al., 2005] Laufer, R. P., Moraes, I. M., Velloso, P. B., Bicudo, M. D. D., Campista, M. E. M., de O. Cunha, D., Costa, L. H. M. K. e Duarte, O. C. M. B. (2005). Negação de Serviço: Ataques e Contramedidas. Em *Minicursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2005*, páginas 1–63.

[Taveira, Moraes, Rubinstein and Duarte, 2006] Taveira, D. M., Moraes, I. M., Rubinstein, M. G. e Duarte, O. C. M. B. (2006). Técnicas de Defesa Contra Spam. Em *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, páginas 202–250.

[Andersen and et. Al, 2008] Andersen, D. G., Balakrishnan, H., Feamster, N., Koponen, T., Moon, D. e Shenker, S. (2008). Accountable Internet protocol (AIP). Em *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*, páginas 339–350. ACM.

[IETF, 2010] http://www.ietf.org/rfc/rfc2475.txt

[Silva, 2008] V. Silva. From the specification to the implementation

of norms: an automatic approach to generate rules from norms to govern the behavior of agents. Autonomous Agents and Multi-Agent Systems, pages 113–155, 2008.

[Costa, Lucena, Cowan and Alencar, 2008] COSTA, A.; LUCENA, C. J. P.; SILVA, V. T.; COWAN, D. ; ALENCAR, P.. **A hybrid diagnostic-recommendation system for agent execu-tion in multi-agent systems**. In: ICSOFT 2008 – 3RD INTERNATIONAL CON-

FERENCE ON SOFTWARE AND DATA TECHNOLOGIES, PORTO, PORTUGAL, 2008.

[Neto, Costa, Netto, Silva and Lucena, 2009] NETO, B.; COSTA, A.; NETTO, M.; SILVA, V. ; LUCENA, C.. **Jaaf: A framework to implement self-adaptive agents**. In: PROCEEDINGS OF THE 21ST INTERNATIONAL CONFERENCE ON SOFTWARE ENGI- NEERING AND KNOWLEDGE ENGINEERING (SEKE'2009), 2009.

[Gatti, 2009] Gatti, M. A. C. (2009) Engineering of Self-Organizing Emergent Multi-Agent Systems: A Design Method and Architecture. PhD Thesis. PUC-Rio.

[Cirilo, Nunes, Kulesza and Lucena] CIRILO, E.J.R., NUNES, I., KULESZA, U., LUCENA, C.J.P. (2009), Automating the Product Derivation Process of Multi-Agent Systems Product Lines, XXIII Simpósio Brasileiro de Engenharia de Software (SBES 2009), Fortaleza, Brasil, pp. 12-21.