CNPq - Conselho Nacional de Desenvolvimento Científico

Sistemas de Redes Robustos: Modelos e Ferramentas

Proposta submetida ao CNPq
Edital MCT/CNPq/CT-INFO n^{o} 07/2007

sigla: ReBu

Coordenador:

Virgílio Augusto Fernandes Almeida - virgilio@dcc.ufmg.br
Departamento de Ciência da Computação
Universidade Federal de Minas Gerais

Instituições Participantes:

Departamento de Ciência da Computação - Universidade Federal de Minas Gerais
PEE/COPPE - Universidade Federal do Rio de Janeiro
PESC/COPPE - Universidade Federal do Rio de Janeiro
Instituto de Computação - Universidade Estadual de Campinias
Laboratório Nacional de Computação Científica.
Instituto de Computação - Universidade Federal Fluminense
Depart. de Eletrônica e Telecomunicações - Universidade do Estado do Rio de Janeiro

Sumário

Resumo

Apesar do curto período em operação comercial, é determinante a influência da Internet em diversos setores da sociedade e na forma como esses setores se estruturam e operam. A Internet transformou desde o modo com que nos comunicamos até a Economia e o relacionamento da sociedade com seus governantes. O enorme sucesso da Internet na sociedade deve-se em parte à vasta gama de serviços e aplicações atualmente disponíveis através dela. Além disto, a facilidade com que novos serviços ou aplicações podem ser desenvolvidos e introduzidos propicia sua constante evolução.

Entretanto, o crescimento acelerado e de forma descentralizada da Internet e de suas aplicações traz à tona um questionamento sobre até quando ela será capaz de se adaptar a mudanças inesperadas, ou seja, até quando ela manterá sua robustez. Para qualquer aplicação, a robustez do sistema e da infra-estrutura em que ela reside é fator determinante para a qualidade do serviço provido. Um sistema robusto deve ser escalável, tolerante a falhas (intencionais ou não) e confiável frente aos diferentes padrões de comportamento de seus usuários. Há inúmeros esforços na literatura que visam a proposição de mecanismos eficientes para aumentar um ou outro aspecto da robustez de um dos vários componentes da Internet, seja ele um enlace, um protocolo de roteamento, uma nova arquitetura de aplicação e até mesmo algum mecanismo específico para uma classe de aplicações.

Entretanto, estes esforços têm sido, na grande maioria das vezes, isolados e independentes, resultando em soluções com eficácia restrita. O presente projeto de pesquisa tem por objetivo maior desenvolver um arcabouço unificado de modelos e ferramentas integradas para dotar sistemas de rede e em especial a Internet de robustez frente às variações tecnológicas e aos diferentes padrões de comportamento de seus usuários mais comumente observados, particularmente os considerados maliciosos, oportunistas e, em última instância, anti-sociais. Nosso objetivo, a curto prazo, é avançar o estado da arte neste sentido, tirando proveito da complementariedade de competências dos pesquisadores participantes deste projeto, para abordar problemas específicos, avaliando e integrando técnicas e teorias distintas, tipicamente aplicadas no tratamento de diferentes problemas. Objetiva-se, em última instância, o estabelecimento e a consolidação de uma rede de pesquisa colaborativa e temática envolvendo um grupo de pesquisa multi-institucional para investigação de diversos problemas altamente desafiadores relacionados à robustez de sistemas de redes.

Os resultados científicos esperados devem romper com paradigmas atuais permitindo uma abordagem mais ampla sobre esta questão. Além disto, eles se materializarão na formação de vários alunos de graduação, Mestrado e Doutorado, bem como em um número de publicações em conferências e periódicos de ponta. Portanto, espera-se garantir uma maior difusão dos conhecimentos adquiridos e também a formação de uma nova geração de pesquisadores comprometidos e motivados com a solução dos desafios abordados. Por fim, considerando o papel central que os sistemas de redes, particularmente a Internet, exercem na sociedade moderna, os resultados que se pretende obter terão impacto significativo para o crescimento do País, contribuindo em áreas como inclusão digital, telemedicina, educação a distância, suporte a aplicações de e-ciência, entre outras.

Este projeto vai diretamente ao encontro do desafio no. 5 "**Desenvolvimento tecnológico de qualidade: sistemas disponíveis, corretos, seguros, escaláveis, persistentes e ubíquos**", proposto no documento "**Grandes Desafios para a Computação no Brasil: 2006-2016**".

1 Introdução

Apesar do curto período em operação comercial, a Internet vem tendo uma influência determinante em diversos setores da sociedade. A Internet vem transformando desde a forma com que nos comunicamos até a Economia e o relacionamento da sociedade com seus governantes. É inegável que tais transformações irão moldar as futuras gerações, que terão acesso a um volume de informações e a um número de interlocutores sem precedentes na História. Estimativas indicam que o número de usuários conectados à Internet no mundo já ultrapassou 1 bilhão e meio [59]. No Brasil, este número supera os 40 milhões [3].

O enorme sucesso da Internet na sociedade deve-se em parte à vasta gama de serviços e aplicações que ela atualmente oferece aos usuários. Além disto, mais fundamental ainda é a facilidade com que novos serviços ou aplicações podem ser desenvolvidos e introduzidos na Internet, o que propicia uma constante evolução. Dentre as novidades recentes, podemos citar alguns aplicativos com enorme popularidade atualmente, tais como sistemas de compartilhamento de arquivos (KaZaa [37] e BitTorrent [18]), distribuição de áudio e vídeo (Youtube [78]), telefonia via Internet (Skype [9]), e sistemas baseados em redes de relacionamento e de cooperação (Orkut [62] e MySpace [54]). O número de usuários de tais aplicativos tem crescido de forma marcante e, em muitos pontos da rede, respondem hoje pela maior parte do tráfego observado.

Esta facilidade de introduzir novos aplicativos e serviços é uma consequência natural do modelo original adotado para a arquitetura da infra-estrutura da Internet, que dita que o núcleo da rede deve oferecer apenas um serviço básico de conectividade e que as funcionalidades mais complexas devem ser implementadas nas extremidades da rede. Desta forma, aplicativos e serviços se tornam apenas usuários do serviço básico desta infra-estrutura, que é composta por uma grande variedade de roteadores, enlaces e protocolos. Entretanto, esta infra-estrutura pode limitar fundamentalmente a eficiência dos aplicativos e serviços que podem ser desenvolvidos. Pois para que um aplicativo ou serviço possa ser oferecido de forma eficiente e com qualidade, é necessário que esta infra-estrutura atenda minimanente às suas demandas.

Existe então uma dualidade entre o desenvolvimento de novos aplicativos e serviços e as mudanças na infra-estrutura da Internet. Por um lado, aplicativos precisam lidar com o serviço atualmente oferecido pela infra-estrutura, pressionando-a por mudanças estruturais que atendam às suas necessidades. Por outro lado, a infra-estrutura atual precisa atender satisfatoriamente às demandas, sem incorporar mudanças que possam comprometer sua evolução futura. Além disto, aplicativos cada vez mais precisam considerar o comportamento de seus usuários e como estes utilizam suas várias funcionalidades. Neste contexto, é essencial que tanto os aplicativos e serviços quanto a infra-estrutura da Internet sejam capazes de se adaptar a mudanças inesperadas, ou seja, que sejam *robustos*.

Com base nesta orientação, aplicativos em rede de larga-escala são projetados cada vez mais com uma arquitetura Par-a-Par (P2P) [45], em contrapartida à tradicional arquitetura cliente-servidor. A arquitetura P2P oferece uma maior robustez ao aplicativo, principalmente com relação à capacidade de atender um grande número de usuários, permitindo uma maior escalabilidade. Outra recente preocupação no desenvolvimento de tais aplicativos é torná-los robustos às muitas vulnerabilidades decorrentes do comportamento de seus usuários. Isto é particularmente importante no caso de comportamentos maliciosos, oportunistas e, em última instância, anti-sociais, tais como a disseminação de vírus e *worms* [57, 50], de *spam* [15], e de *conteúdo poluído* [49, 17], além de ataques coordenados (isto é, conluio), visando injetar informações falsas na rede (p. ex: auto-promoção ou difamação de participantes) [24].

Mais ainda que seus aplicativos, a infra-estrutura da Internet precisa ter a capacidade de lidar com o inesperado, tolerando de forma satisfatória as constantes demandas impostas pelos aplicativos. Um exemplo bem sucedido desta caracterísitca é o protocolo

TCP [66], que há decadas atende de forma satisfatória a demanda de uma grande variedade de aplicativos. No entanto, apesar de sua grande efetividade em garantir o bom funcionamento da Internet de hoje, o mecanismo de controle da janela de transmissão adotado pelo TCP não é capaz de lidar com a grande disponibilidade de banda passante nos enlaces ópticos da Internet atual, nem com as características dos enlaces sem fio. Assim sendo, existe uma necessidade de mudar o funcionamento do protocolo de forma a atender às novas demandas, e muitas destas propostas já aparecem na literatura [4]. Entretanto, qualquer mudança que seja efetivamente adotada deve ser capaz de tolerar o futuro incerto que é o surgimento de novos aplicativos. Garantir a robustez da infra-estrutura da Internet é fundamental para permitir sua evolução.

Há inúmeros esforços na literatura que visam a proposição de mecanismos eficientes para aumentar um ou outro aspecto da robustez de um dos vários componentes da Internet, seja ele um enlace ou roteador, um protocolo de roteamento em nível de rede ou aplicação, uma nova arquitetura de aplicação (p.ex: P2P [25]) e até mesmo algum mecanismo específico para uma classe de aplicações (p.ex: mecanismos baseados em moderação, confiança e reputação [21, 20, 73, 40]). Entretanto, estes esforços têm sido, na grande maioria das vezes, isolados e independentes. Isso leva a quatro conseqüências importantes: *i*) muitos dos resultados obtidos, embora positivos, têm sua contribuição restrita por enfatizarem apenas um aspecto ou componente do sistema; *ii*) soluções são propostas partindo de premissas sobre o comportamento dos usuários que não correspondem aos padrões observados na prática, o que pode levar a uma qualidade de serviço bem aquém do esperado e, talvez, inaceitável; *iii*) algumas técnicas genéricas são aplicadas, de forma separada e independente, no tratamento de diferentes problemas em diferentes níveis do sistema, quando uma solução mais abrangente e integrada poderia ser mais adequada; *iv*) a proposta de soluções separadas e independentes pode levar à melhoria de uma certa métrica, mas pode prejudicar outros aspectos do sistema.

Frente a estas observações, torna-se clara a necessidade de um arcabouço *unificado* de mecanismos que contribua para uma maior robustez de sistemas de redes, particularmente da Internet, de forma eficaz e com uma boa relação custo-benefício. Para que essas soluções sejam realmente eficazes, é essencial que as soluções considerem os principais compromissos existentes em todos os componentes que compõem tal sistema, desde a camada de enlace até a camada de aplicação, incluindo o núcleo central (backbone) bem como as várias redes periféricas e de acesso, cabeadas e sem fio, que possibilitam a interconexão das aplicações em uso pelos usuários finais.

Postula-se, portanto, como **grande desafio** deste projeto a avaliação e a integração de diferentes técnicas empregadas para garantir a robustez de sistemas de rede, desenvolvendo um arcabouço unificado que permita uma avaliação mais geral da robustez dos mesmos, bem como a proposição de soluções mais eficazes e com uma visão abrangente para os vários problemas identificados. A escolha de técnicas existentes bem como o projeto de novos mecanismos será embasado em uma caracterização detalhada dos diferentes padrões de comportamento dos sistemas bem como dos usuários que o utilizam, que criará subsídios para o desenvolvimento de modelos que permitam a avaliação dos sistemas em cenários fictícios mas realistas e, consequentemente, a identificação de potenciais vulnerabilidades que devam ser atacadas.

Como todo grande desafio, sua solução não é trivial, e o problema provavelmente permanecerá em aberto por anos. Além disto, existe uma dificuldade real de se sintetizar e unificar diferentes critérios que definem a robustez de um sistema de rede. Nosso objetivo, a curto prazo, é avançar o estado da arte neste sentido, tirando proveito da complementariedade de competências no grupo de pesquisadores participantes deste projeto, para abordar problemas específicos, avaliando e integrando técnicas e teorias distintas, tipicamente aplicadas no tratamento de diferentes problemas. Objetiva-se, em última instância,

a criação de um grupo de pesquisa coeso e unificado, que possa contribuir, de forma conjunta mais efetiva, para a maior robustez de sistemas de rede.

2 O Grande Desafio de Robustez de Sistemas de Redes

A necessidade de transformações fundamentais na infra-estrutura da Internet atual é motivada principalmente por avanços tecnológicos que permitam oferecer uma gama cada vez maior de serviços aos usuários de forma eficiente e com qualidade. É necessário, portanto, que a Internet possa atender a essas demandas evolucionárias. Entre essas necessidades, pode-se citar:

- **Disponibilidade universal de acesso**: com os avanços tecnológicos na área de redes sem fio e a massificação do seu uso, está se tornando cada vez mais fácil conectar-se à Internet de qualquer lugar e a qualquer instante, mesmo quando em movimento (ex. enviar emails pelo PDA de dentro de um táxi). Para lidar com esta necessidade, a rede deve suportar mecanismos mais eficientes para localizar e endereçar dispositivos ligados à rede, cenário muito diferente do que se tinha em mente quando a Internet foi projetada. Por exemplo, uma estrutura de endereçamento rígida e hierárquica provavelmente não é a mais adequada, pois o roteamento deve suportar a mobilidade de forma transparente.

- **Ubiquidade dos dispositivos**: um número cada vez maior de dispositivos de todos os tipos e tamanhos tem sido conectado à Internet. Desde geladeiras e torradeiras até sensores que monitoram ninhos de aves e tremores de terra. A promessa é que sensores de monitoramento se espalhem por centros urbanos, residências, carros, e até mesmo pessoas, todos conectados à Internet oferecendo informações em tempo real. Para lidar com este enorme crescimento do número e da variedade de dispositivos que irão se conectar à Internet, novos paradigmas de comunicação serão necessários, e alguns já começam a ser discutidos, como o T2T (Thing-to-Thing).

- **Segurança e privacidade**: dada sua crescente penetração em nossa sociedade, é cada vez mais importante que a Internet ofereça segurança e privacidade a seus usuários. É cada vez maior a quantidade de informação pessoal e empresarial disponibilizada na Internet, tanto de forma pública quanto privada; proteger esta informação passa a ser fundamental para o funcionamento da Internet. Entretanto, o projeto original da Internet não incluiu aspectos de segurança ou privacidade na infra-estrutura da rede. Assim sendo, a Internet de hoje está vulnerável a ações maliciosas e a comportamentos oportunistas, egoístas e, em última instância, antisociais, por parte de seus usuários. Tornar a Internet resistente a tais padrões de comportamento e anomalias, é certamente uma necessidade dos serviços e aplicações atualmente em desenvolvimento.

Apesar das novas demandas mencionadas, garantir a robustez de sistemas de redes na Internet sempre foi um dos desafios que guiou seu projeto inicial e subsequente desenvolvimento. Entretanto, a robustez dentro deste contexto tradicional, se referia à capacidade do sistema de lidar com falhas em seus componentes ou em padrões de uso pelos usuários. Por exemplo, a Internet deveria continuar funcionando de maneira satisfatória caso um ou alguns de seus componentes (ex. roteadores) parassem de funcionar abruptamente.

Na realidade de hoje, garantir a robustez da Internet passou a ter significado muito mais amplo, capturado pelo próprio significado do conceito de robustez. Robustez, em seu sentido mais genérico, significa "prover algum tipo de funcionalidade na presença de alguma incerteza". Esta generalização permite acomodar diferentes requisitos e aspectos relevantes do sistema em questão, todos necessários para garantir a sua robustez de

forma ampla. Assim, a robustez de um sistema é garantida quando o mesmo é capaz de lidar de forma satisfatória com todos os aspectos que sejam relevantes ao mesmo de forma simultânea e integrada. Propostas de mudanças na infra-estrutura da Internet, por exemplo, devem ser robustas neste sentido mais amplo.

Cabe aqui uma analogia com sistemas bancários que, tradicionalmente, são projetados para serem robustos. Tal robustez se refere à capacidade do sistema de lidar com falhas de componentes de *hardware* e *software*, com horários de pico, onde há uma alta demanda do sistema (p.ex: acesso ao banco de dados), e com erros humanos de digitação, entre outros. Com o avanço tecnológico, tais sistemas precisaram se adaptar para oferecer novos serviços a seus usuários, como por exemplo *online banking*. Ao oferecer tais serviços, questões relacionadas a segurança e ao uso dos sistemas precisaram ser revisitadas, uma vez que o sistema ficaria exposto ao público diretamente. Da mesma forma, o conceito de robustez precisou ser expandido, por exemplo, para incorporar aspectos de segurança em transações bancárias via Internet, bem como aspectos relativos à confiabilidade do sistema bancário frente a possíveis ações maliciosas e/ou oportunistas dos seus usuários (p.ex: substituição de conteúdo disponibilizado originalmente por conteúdo poluído visando diminuir confiabilidade dos usuários no sistema). Vale ressaltar que mudanças fundamentais em um sistema bancário não necessariamente comprometem seu funcionamento ou evolução no futuro, pois trata-se de um sistema único, desenvolvido e administrado por uma única entidade, que pode, em última instância, ser trocado por um outro. Tal possibilidade é totalmente inviável em sistemas abertos, distribuídos, descentralizados e de larga-escala, como a Internet.

Assim como no sistema bancário, diferentes aspectos precisam ser considerados para tornar um sistema de rede robusto. A Figura 1 ilustra alguns destes aspectos que a seguir são apresentados.

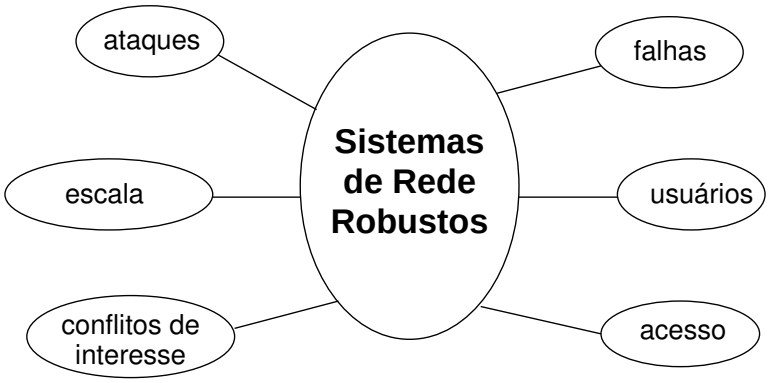

Figura 1: Diferentes aspectos da *robustez* de um sistema de rede.

- **Falhas.** Um sistema robusto a falhas é um sistema que continua operando de forma satisfatória mesmo quando alguns componentes que o compõem falham. A robustez a falhas está diretamente relacionada à confiabilidade do sistema.

- **Ataques.** Um sistema é robusto a ataques quando o mesmo continua operando de forma satisfatória mesmo quando usuários maliciosos tentam propositalmente impedir o seu funcionamento ou comprometer a confiabilidade no mesmo. Como exemplos, podemos citar as epidemias de vírus e *worms*, os ataques de negação de serviço (DoS)[1] a um servidor Web disparado por um *hacker*, bem como ações

[1]De acordo com um recente relatório do CSI/FBI (*Computer Security Institute/Federal Bureau of Investigation*) [19], ataques DoS estão entre os incidentes de segurança que causam as maiores perdas às empresas americanas

maliciosas que visam comprometer a confiabilidade no sistema ou em determinados usuários tais como poluição de conteúdo e ataques de conluio.

- **Escala.** Um sistema é robusto a escala quando o mesmo continua apresentando um desempenho satisfatório quando alguns de seus parâmetros aumenta signitivamente. Por exemplo, isso pode ocorrer quando o número de usuários de um sistema aumenta repentinamente.

- **Usuários.** Um sistema é robusto aos usuários quando o mesmo é capaz de operar de forma satisfatória independente do padrão de comportamento de seus usuários. Neste contexto, estamos assumindo que os usuários não agem de forma maliciosa nem estratégica ou oportunista, mas que simplesmente possuem algum padrão de comportamento. Por exemplo, curtas durações de sessões em uma rede sem fio, concentração das requisições dos usuários em poucos objetos ou funcionalidades providas pelo sistema, etc.

- **Conflitos de interesse.** Um sistema é robusto a conflitos de interesse quando o mesmo é capaz de operar de forma satisfatória mesmo quando há conflitos de interesse entre diferentes entidades presentes no sistema. Neste contexto, diferentes partes do sistema (p.ex: usuários) agem de forma estratégica, cada uma visando apenas o melhor para si própria. Ações oportunistas, tais como *spamming*, visando aproveitar da infra-estrutura para anunciar produtos e serviços, e egoístas (p.ex: *free riding* em sistemas P2P [29]) se encaixam nesta categoria.

- **Acesso.** Um sistema é robusto ao acesso se o mesmo é capaz de operar independente do tipo de acesso ao sistema. Tal forma de robustez está diretamente relacionada com a ubiquidade de acesso, permitindo que usuários acessem o sistema de forma heterogênea.

Os aspectos listados acima podem ser exemplificados por inúmeras questões aparentemente triviais, mas cujas soluções podem ser extremamente complexas de serem derivadas. Considere, por exemplo, a infra-estrutura da Internet de hoje, formada por seus roteadores, canais de comunicação e protocolos. O que fazer para garantir sua robustez? Dada a complexidade desta infra-estrutura, garantir a robustez com relação a um único dos aspectos listados anteriormente passa a não ser trivial. Como outro exemplo, como garantir que uma aplicação da Internet seja robusta a diferentes padrões de comportamento de seus usuários? Para tanto, é preciso garantir que a infra-estrutura em que ela reside também seja robusta aos mesmos padrões.

Neste contexto mais amplo, garantir a robustez de um sistema de rede é um problema que não pode ser resolvido com o atual estado-da-arte. Parte desta dificuldade emerge devido à falta de um arcabouço unificado capaz de representar o problema em um contexto mais amplo, que permita portanto a reutilização de técnicas comuns de forma integrada e otimizada para um objetivo comum, isto é, aumentar a robustez do sistema de redes.

A maioria dos trabalhos que aborda a questão da robustez em sistemas de rede considera aspectos específicos de componentes particulares. Dada sua complexidade, é natural que a questão da robustez seja atacada dividindo o problema em partes menores e resolvendo-as separadamente. O objetivo central da concepção de um sistema de rede é que ele seja robusto com relação a qualquer requisito específico. Por exemplo, como se pode tornar um sistema com servidores Web robusto ao ataque de negação de serviço? Apesar da aparência modesta, tal contribuição é necessária para a melhor compreensão do problema e de possíveis soluções eficazes.

Desta forma, para solucionar os problemas em separado, diferentes técnicas, mecanismos e, de forma mais geral, até mesmo teorias vêm sendo aplicadas visando modelar e

avaliar os aspectos específicos da robustez de um sistema de rede. Por exemplo, a Teoria dos Jogos [63, 55] é utilizada para modelar e avaliar a robustez de sistemas onde há conflito de interesse entre diferentes entidades. Resolver diferentes questões de robustez de diferentes sistemas é um caminho a entender como estes aspectos podem ser unificados, abrindo a perspectiva de novas arcabouços e, a mais longo prazo, a até possíveis teorias que possam capitalizar no atual estado da arte.

É importante ressaltar ainda que um mesmo aspecto específico da robustez pode ser um requisito para diferentes sistemas. Desta forma, é possível que uma solução empregada com sucesso em um sistema possa ser adaptada e utilizada para garantir a robustez de outro sistema. Soluções integradas podem ainda ser projetadas, levando a resultados mais eficazes. Isto ilustra a necessidade de investigar os problemas de forma conjunta, objetivando uma unificação das soluções.

3 Coerência com os Objetivos do Edital

A concepção e o desenvolvimento de um arcabouço unificado de mecanismos para o suporte à robustez em sistemas de redes, como proposto neste projeto, é um problema altamente desafiador. Em particular, este projeto vai diretamente ao encontro do desafio no. 5 "Desenvolvimento tecnológico de qualidade: sistemas disponíveis, corretos, seguros, escaláveis, persistentes e ubíquos", proposto no documento "Grandes Desafios para a Computação no Brasil: 2006–2016", considerando que o conceito de robustez adotado neste projeto abrange todos aspectos elencados na proposição deste grande desafio.

4 Sistemas de Rede e Estado da Arte

A Internet é certamente o maior e mais complexo exemplo de sistema de rede de nosso tempo. Entretanto, no escopo deste projeto, utilizamos o conceito de "sistema de rede" de forma mais abrangente, nos referindo a qualquer sistema formado por componentes ou entidades que estejam separadas (fisica ou logicamente) e que necessitam se comunicar de forma eficiente. Tal sistema pode ser construído em software ou em hardware, e pode ser parte fundamental da Internet ou atuar apenas em suas extremidades, como uma aplicação. Assim sendo, o amplo conceito de robustez introduzido acima pode ser empregado em sistemas de rede quaisquer, e não apenas na Internet. Exemplos de sistema de redes incluem: redes sem fio, redes ópticas, sistemas Peer-to-Peer (P2P) (incluindo tanto a infra-estrutura de rede quanto as aplicações nela residentes), aplicações de redes de relacionamento, incluindo redes de cooperação, de trocas de e-mails (isto é, correio eletrônico) e de mensagens instantâneas, etc.

A seguir, exemplificamos alguns sistemas de rede e aspectos relevantes que precisam ser abordados para garantir a sua robustez. É importante ressaltar que o conceito de robustez irá depender do sistema em questão, entretanto, alguns aspectos serão comuns a diferentes sistemas, ilustrando a possibilidade de adoção de técnicas gerais ou a aplicação conjunta de técnicas complementares que garantam certo aspecto da robustez. A tabela 1 ilustra os diferentes aspectos da robustez destes sistemas, ilustrando a sobreposição dos problemas e a possibilidade de soluções comuns ou integradas.

Redes sem Fio

Garantir a robustez das redes sem fio nos diferentes aspectos enumerados é primordial para a implantação dessas redes e conseqüentemente para a ubiqüidade de acesso. Por utilizarem meio físico compartilhado, as redes sem-fio são extremamente vulneráveis a ataques dos mais variados tipos. Além dos ataques que afetam diretamente os usuários,

Tabela 1: Aspectos da robustez nos diferentes sistemas de redes

	escala	ataques	falhas	padrões de comportamento	acesso	conflitos de interesse
Redes sem Fio	X	X	X	X	X	X
Redes Ópticas	X		X			X
Sistemas P2P	X	X	X	X	X	X
Aplicações de redes	X	X		X	X	X

como a violação da privacidade, outro tipo de ataque diz respeito à falta de cooperação entre os nós no encaminhamento de mensagens, impedindo dessa forma o funcionamento de redes do tipo ad hoc. Assim, para garantir a robustez com relação à segurança das redes sem-fio, em especial as sem infra-estrutura, é necessário o desenvolvimento de técnicas de identificação de usuários, detecção de atividades maliciosas e responsabilização dos usuários.

Dispositivos sem fio contam tipicamente com recursos limitados em termos de energia, operando através de baterias ou outras fontes de energia advindas da natureza. Protocolos e mecanismos devem ser cientes das restrições de cada dispositivo, minimizando as falhas por falta de energia e visando estender o tempo de vida da rede sem fio. Além disso, as redes sem fio são suscetíveis a diversas fontes de interferência: eletromagnética, múltiplos caminhos, co-canal, canal-adjacente, intra-rede, inter-rede, entre outras. Assim, esses mesmos protocolos e mecanismos devem ser projetados de forma distribuída e coordenada para realizar funções como seleção automática de canais de freqüência, controle adaptativo de taxa de transmissão e escalonamento de pacotes de forma a minimizar o efeito dessas várias fontes de interferência.

Vários outros aspectos afetam a robustez das redes sem fio. Por exemplo, a escassez de espectro de freqüência para a operação dessas redes e a mobilidade geram um problema de escala quanto ao número e à densidade de nós. As redes sem fio em malha enfrentam um grande problema de perda de capacidade quando esses fatores aumentam. A necessidade de se otimizar o uso do espectro disponível levou ao surgimento dos rádios cognitivos, cujo objetivo é detectar e utilizar oportunidades no espectro de freqüência, criando um conflito de interesses que pode levar o sistema como um todo a estados indesejáveis. Outra forma de otimizar o uso do espectro disponível é eliminar mensagens de controle desnecessárias e aplicar métricas de roteamento que melhorem o desempenho global da rede.

Um outro aspecto que afeta a robustez das redes sem fio diz respeito à alta dinamicidade de entrada e saída de usuários nessas redes. Esse comportamento leva a uma forte degradação do desempenho. Com relação ao tratamento de falhas, deve-se considerar, em especial nas redes sem fio móveis e esparsas, soluções robustas a atrasos e desconexões. Este tipo de rede permite a troca de informações na rede mesmo quando o ambiente não está sempre conectado, o que pode ser utilizado, por exemplo, para realizar uma inclusão digital de populações carentes localizadas em pontos muito distantes dos grandes centros urbanos.

Outro aspecto da tolerância a falhas é que as redes sem-fio devem ser, ainda, robustas à falta de energia. Dispositivos sem fio tipicamente operam com recursos limitados em termos de energia, operando através de baterias e de energia solar. Protocolos devem ser cientes das restrições de cada dispositivo visando estender o tempo de vida da rede.

Redes Ópticas

A Internet como rede mundial de comunicação conectando usuários em todos os continentes só foi possível devido à existência de enlaces ópticos de alta capacidade. Os avanços de componentes ópticos, nas duas décadas anteriores, e a rápida absorção desta tecnologia

permitiram a efetivação da topologia da Internet em níveis globais [74].

A multiplexação por comprimento de onda permite o uso da vasta quantidade de banda passante existentes nos enlaces ópticos. Assim como em qualquer sistema baseado em multiplexação, a multiplexação por comprimento de ondas requer a correta avaliação do uso dos recursos para atender as demanda das aplicações.

Em redes ópticas transparentes, diversos fenômenos ópticos influenciam a qualidade da transmissão e produzem diferentes taxas de erro, comprometendo a garantia dos requisitos de *Qualidade de Serviço* das aplicações. Estes fenômenos são denominados limitações da camada física e suas causas são diversas, tais como: dispersão modulada de fase, dispersão de fase cruzada, emissão espontânea amplificada e mistura de quatro ondas [77].

A capacidade de fornecer a Qualidade de Serviço desejada para as aplicações depende, em última instância, da capacidade de se prover caminhos com recursos necessários para tal. A alta capacidade disponível torna crítica a adoção de topologias virtuais em rede núcleo que introduzam redundâncias e mecanismos de proteção a falhas, dado que estas acarretam em indisponibilidade de altas quantidades de banda passante. A tolerancia à falhas do núcleo da rede é um aspecto central para a robustez de sistemas de rede. Apesar de existirem inúmeros resultados para o projeto de redes ópticas tolerantes à falhas que consideram as demandas de tráfego como estáticas, o projeto de redes ópticas tolerantes à falhas com demandas dinâmicas requer ainda um grande esforço investigatório. Além disto, as limitações do meio físico, podem tornar um enlace indisponível para a manutenção dos requisitos de Qualidade de Serviço dos fluxos transportados, apesar do enlace permanescer operacionalmente satisfatório para uma série de outras aplicações. Assim, o conceito de falha e seu impacto na robustez do núcleo da rede deve ser estendido para incorporar as limitações físicas do meio [76] [80] [48].

Os algoritmos de roteamento e alocação de onda propõem soluções para a alocação de banda passante mediante requisitos impostos pelos usuários e suas aplicações. A eficácia de soluções integradas da alocação de comprimento de onda e do roteamento influencia de forma decisiva na capacidade da rede de admitir novos usuários e, conseqüentemente, na escalabilidade da rede frente à demanda futura desconhecida. Através destes algoritmos é possível atender a demandas conflitantes por recursos de forma eficiente, maximizando a utilização dos mesmos. Apesar da existência de uma grande quantidade de algoritmos para demandas estáticas, o desenvolvimento destes considerando demanda dinâmica de tráfego, topologias genéricas, tolerancia à falhas e limitações da camada física encontra-se ainda em sua infância; sendo, portanto, fundamental a concepção de algoritmos que incorporem estes diversos aspectos para a robustez do núcleo da rede [69], [16] [11] .

Existe uma grande disparidade entre a demanda de banda de fluxos IPs e a disponibilidade de banda em um comprimento de onda. Assim, diversos fluxos são agregados em um único comprimento de onda. A agregação segue políticas definidas pelos administradores do núcleo da rede. Estas políticas têm, também, um impacto fundamental na capacidade de se admitir novos fluxos (usuários) no núcleo da rede, bem como na capacidade de se prover os requisitos de Qualidade de Serviço destes fluxos, ou seja, na escalabilidade de uma infraestrutura de comunicação. É de suma importância, que técnicas analíticas sejam empregadas na elaboração das mesmas, bem como na resolução dos conflitos de interesse na alocação de recursos para o aumento da robustez do núcleo da rede [60] [16]

Sistemas Par-a-Par

Soluções baseadas em arquiteturas Par-a-Par (ou P2P) vêm se mostrando uma opção interessante à arquitetura cliente-servidor, até então prevalente entre as aplicações na Internet. Embora originalmente as aplicações P2P concentravam em serviços de compartilhamento de arquivos [37, 18], atualmente arquiteturas P2P servem de infra-estrutura para uma gama variada de aplicações incluindo para transmissão de vídeo e áudio em larga escala

[9] e para as máquinas de busca descentralizadas, uma tendência que vem ganhando popularidade na comunidade científica especializada [10, 79, 7, 25].

Ao abolir a figura do servidor central, redes P2P eliminam um ponto único de falha no sistema, o que por si pode ser identificado como um passo significativo em direção a uma maior robustez. Entretanto, essa mesma característica traz consigo um conjunto de desafios que devem ser eficientemente tratados para que redes P2P se firmem como um modelo robusto de serviços em rede.

Ao se basearem na interação direta entre os participantes do sistema, redes P2P devem ser capazes de organizar os nós da rede de forma eficiente e distribuída. Encontrar uma topologia que conecte todos os participantes de forma eficiente e garanta o roteamento entre todos é um desafio que deve ser atacado para garantir a robustez de tais redes em termos de escala, comportamento de usuários e acessos. Por exemplo, há relatos de problemas na rede Skype devido a um número elevado de tentativas de conexão em um curto intervalo de tempo [9, 36].

Por não utilizarem servidores, aplicações P2P devem se organizar em função das máquinas dos usuários do sistema, estando sujeitas aos padrões comportamentais dos mesmos. Portanto, essas máquinas são inerentemente muito menos confiáveis que grandes servidores. Isso as torna mais sujeitas a falhas esporádicas, além de eventos de desconexão iniciados pelos usuários e que são imprevisíveis do ponto de vista dos demais participantes da rede. Esses fatores podem levar a uma alta taxa de entradas e saídas de usuários da rede (padrão também identificado para redes sem fio), fenômeno usualmente denominado *churn* na literatura [70]. Para garantir a robustez de sistemas P2P, torna-se importante então identificar formas de se aumentar a estabilidade do sistema como um todo mesmo na presença destes padrões de comportamento dos usuários, que, por sua vez, podem ser intensificados em determinadas redes de acesso (p.ex: redes sem fio). Estes padrões, por sua vez, precisam ser previamente identificados, caracterizados e modelados [70]. Deve-se também desenvolver mecanismos de tolerância a falhas para lidar com a intermitência e dinamismo das redes P2P. Estes mecanismos devem monitorar os estados dos nós da rede e recuperar a execução das tarefas em conseqüência de alguma falha.

Uma das premissas básicas de operação de redes P2P é que, para o bom funcionamento dos serviços envolvidos, pelo menos uma fração significativa dos participantes deve estar disposta a prover serviços para os demais. Entretanto, usuários podem possuir motivações egoístas para tentar extrair serviços da rede sem oferecer nenhuma parte de seus recursos em troca [28]. Além disto, usuários poderiam explorar o serviço em proveito próprio em ações oportunistas, como por exemplo o *spamming*, já amplamente analisado no sistema de correio eletrônico [30, 32, 31, 71, 51, 44, 33] bem como observado em máquinas de busca centralizadas [61], e que poderia ocorrer em aplicações P2P de compartilhamento e distribuição de conteúdo e nas máquinas de busca descentralizadas também. Mecanismos devem ser implementados para garantir que os conflitos de interesse que emergem destas ações sejam tratados de forma a garantir a robustez do sistema.

Um fator que torna ainda mais premente o desenvolvimento de tais mecanismos é que comportamentos egoístas e oportunistas podem degenerar para situações de ataque explícito ao sistema com objetivos variados. Como exemplo, podemos citar a introdução de um grande volume de cópias poluídas (e portanto inúteis) de arquivos originalmente legítimos e muito populares, visando mascará-los e comprometer a confiabilidade do sistema. Este tipo de ataque, chamado de *poluição de conteúdo*, foi identificado recentemente no sistema KaZaa [49, 17], de grande popularidade. Além disto, diversos nós podem se unir, em um ataque conjunto de conluio ou do tipo Sybil [24] (quando um único usuário atua com múltiplas identidades no sistema), visando extrair o máximo de recursos de um serviço em detrimento dos demais, comprometer a confiabilidade ou até mesmo inviabilizar o serviço, ou ainda por outras intenções ilícitas [24]. Alguns esforços na direção

do desenvolvimento de mecanismos, tipicamente baseados nos conceitos de confiança e reputação foram recentemente propostos para aumentar a robustez de aplicações P2P de compartilhamento de arquivos em alguns destes cenários [21, 20, 73, 40]. Entretanto, estes mecanismos precisam ser estendidos e generalizados para sistemas P2P no sentido mais amplo, incluindo diferentes aplicações bem como a infra-estrutura descentralizada.

Aplicações baseadas em Redes de Relacionamento

Uma das aplicações mais populares na Internet desde os seus primórdios tem sido o correio eletrônico (*e-mail*). Pode-se dizer que essa popularidade se deve, pelo menos em parte, à sua capacidade de facilitar a interação dos usuários através da rede e à praticidade da comunicação assíncrona oferecida. À medida que o número dos usuários da Internet aumenta, outras aplicações também voltadas para a valorização de relacionamentos sociais e formação de comunidades virtuais em torno de temas de interesse comum, como blogs [12, 26], sites de relacionamentos como Orkut [62], Flickr [23] e Youtube [78], também se tornam cada vez mais populares [53]. Essas aplicações exploram as relações entre usuários para melhorar a qualidade de serviços pré-existentes, como no caso de bibliotecas digitais, bem como para prover novos serviços baseados nesses relacionamentos [52]. De forma similar, ferramentas de comunicação instantânea e síncrona também ganham muita popularidade tanto para contatos pessoais quanto profissionais.

No contexto brasileiro, em particular, este tipo de aplicação tem grande popularidade. O Orkut e o Youtube foram recentemente colocados entre os cinco *sites* mais populares no País [1], em função da quantidade de tráfego gerada por eles na Internet brasileira. Podemos citar também o Peabirus [2], um sistema para a criação de comunidades virtuais online com foco em relacionamentos profissionais e que visa fomentar possibilidades de comércio, parcerias de negócios e pesquisa entre empresas, profissionais e pesquisadores. Além destes, também vale à pena citar os serviços de blogs, tails como o UOL blog [12], que atende centenas de milhares de requisições diariamente, e os serviços de notícias com participação da comunidade de usuários, como Digg.com [58] e Slashdot [68], de grande popularidade na rede mundial.

Por se basearem e se espelharem nos conceitos de relações sociais, essas aplicações enfrentam desafios semelhantes aos encontrados em sociedade, que se refletem em demandas por robustez frente a diferentes padrões de comportamento dos usuários, inclusive conflitos de interesse, e diferentes formas de ataques e ações maliciosas.

No caso do correio eletrônico, por exemplo, os spams representam um padrão de comportamento oportunista que ocorre na Internet entre os indivíduos que desejam se aproveitar da infra-estrutura alheia para anunciar produtos e serviços. Estudos recentes reportam que o volume de e-mails considerados spam cresce a uma taxa assustadora, tendo atingido 83% dos e-mails que trafegam pela Internet em 2005 [38]. Vale ressaltar que, como no caso de aplicações P2P, ações de *spamming* podem ocorrer também em outras aplicações baseadas em redes de relacionamento tais como serviços de blogs, Orkut, Youtube. Alguns resultados que evidenciam esta conjectura são apresentados em [26, 34]. Os vários mecanismos de deteção e controle de spam, a vasta maioria voltada para correio eletrônico [8, 14, 35, 44, 51, 71, 32], claramente não têm atingindo resultados satisfatórios. Novos mecanismos anti-spam mais eficazes, explorando características intrínsecas a este tipo de tráfego [33, 31, 30], devem ser projetados visando tornar estes sistemas mais robustos a estas ações bem como ao crescimento do volume total do tráfego na Internet delas resultantes.

As aplicações baseadas em redes de relacionamento, em particular, também estão sujeitas a outros padrões de comportamento oportunistas e maliciosos. Como exemplo, podemos citar a auto-promoção, onde usuários se beneficiam de funcionalidades do sistema (p.ex: recomendações, comentários e mesmo criação de contas falsas) para se promove-

rem ou promoverem o conteúdo disponibilizado. Além disto, como nos sistemas P2P, as aplicações baseadas em redes de relacionamento também estão sujeitas a ataques coordenados de um grupo de usuários, do tipo conluio ou Sybil, visando difamar ou promover um participante ou um conteúdo. Novos mecanismos baseados em recomendações, relacionamentos de confiança e de estabelecimento de reputações precisam ser projetados visando aumentar a robustez de tais sistemas a estes padrões de comportamento. A crescente popularidade destas aplicações cria desafios para garantir sua robustez em termos de escala também. Algumas aplicações de relacionamento incluem milhões de participantes, cada um se relacionando com um número variável de outros usuários [41]. Garantir que os serviços dessas aplicações sejam eficientes e eficazes ao operar com redes tão grandes exige técnicas para extrair dados de caracterização da rede por amostragem [5], por exemplo.

5 Objetivos e Metas

Este projeto envolve desafios importantes e motivadores tanto para a comunidade científica quanto para a sociedade. Portanto, como qualquer projeto com tais características, ele tem objetivos de longa e de curta duração. O objetivo maior, de longa duração, é o desenvolvimento de um arcabouço unificado que integre múltiplas técnicas, mecanismos e teorias visando a consolidação de soluções mais eficazes que contribuam de forma efetiva para aumentar a *robustez* de sistemas de rede. Para se atingir este objetivo, uma série de problemas iniciais são identificados para serem tratados nos dois anos que correspondem ao período de execução deste projeto. Estes problemas foram escolhidos por corresponderem a desafios reais à robustez (ou algum aspecto dela) de sistemas (ou componentes de sistemas) de redes específicos, dentre aqueles apresentados na seção 4. No tratamento destes problemas, pretendemos identificar possibilidades de integração de técnicas em soluções mais robustas, visando progressos efetivos na direção do arcabouço unificado.

As metas deste projeto, que enfatizam os problemas a serem tratados nos próximos dois anos, são:

- Caracterização e modelagem de padrões de comportamento de usuários mais comuns em diferentes sistemas, incluindo padrões maliciosos e oportunistas. Dentre os sistemas escolhidos para análise, citamos o sistema de correio eletrônico, e outros serviços de redes de relacionamento e cooperação (p.ex: Youtube e Flickr), serviços de blog e serviços de notícias.

- Projeto e avaliação de mecanismos de controle e/ou combate a ações maliciosas e oportunistas (p.ex: *spamming*, auto-promoção, poluição de conteúdo) nos diferentes sistemas baseados em redes de relacionamento analisados.

- Projeto e avaliação de mecanismos para garantir a maior robustez de aplicações P2P, particularmente aplicações de distribuição de vídeo e áudio e máquinas de busca descentralizadas, a diferentes padrões de comportamento de usuário, incluindo *free-riding*, ataques de conluio e Sybil, poluição de conteúdo, spamming e também ao alto dinamismo dos pares envolvidos.

- Projeto e avaliação de técnicas para metrologia da Internet em larga escala e de sua aplicação na detecção de anomalias no tráfego de rede.

- Derivação e avaliação de algoritmos de roteamento e alocação de comprimento de onda que incluam redundância de caminho para proteção à falha e limitações da camada física.

- Derivação e avaliação de agregação de tráfego que incluam redundância de camnho para proteção à falha e limitações da camada física.

- Projeto e avaliação de sistemas de confiança e reputação para sistemas de rede cooperativos.
- Projeto e avaliação de mecanismos de segurança e QoS para redes sem fio.
- Formação de alunos de graduação, Mestrado e Doutorado, bem como a publicação de artigos em conferências e periódicos internacionais e nacionais de reconhecida qualidade.

Em suma, objetiva-se o estabelecimento e a consolidação de uma rede de pesquisa colaborativa e temática envolvendo um grupo de pesquisa multi-institucional para investigação de diversos problemas altamente desafiadores relacionados à robustez de sistemas de redes.

6 Metodologia e Estratégia de Ação

O **gerenciamento deste projeto** se dará através de mecanismos para discussão dos problemas em diversos níveis (geral e de cada meta/objetivo específico). Estas discussões serão realizadas através da organização de encontros via vídeo-conferências e *in loco*. Será dada especial atenção à formação de recursos humanos (graduação e pós-graduação), uma vez que o desenvolvimento de novos conhecimentos são solo fértil para o desenvolvimento de dissertações de Mestrado e teses de Doutorado e consequente produção científica de qualidade. Durante os dois anos do projeto, pretende-se organizar dois *workshops* (um no início e outro no final do projeto) para os participantes, visando incentivar a troca de experiências entre eles, o acompanhamento das atividades sendo desenvolvidas e, a divulgação dos resultados obtidos. Além disto, a interação promovida por estes encontros e workshops visa identificar as possibilidades de integração de soluções complementares e fomentar o desenvolvimento de trabalhos conjuntos entre os participantes do projeto.

A **metodologia** básica a ser utilizada na execução do projeto se baseia na premissa de que o desenvolvimento de soluções eficazes para aumentar a robustez de sistemas de rede deve ser respaldado em uma visão abrangente do mesmo, considerando os seus vários componentes, desde as camadas mais inferiores ou periféricas até a camada de aplicação e o núcleo central de conectividade, bem como a forma como os usuários se comportam, na realidade, ao interagir com estes sistemas. Para tanto, a metodologia a ser adotada será moldada em três pilares, a seguir:

- **Caracterização**: identificação e quantificação dos padrões de comportamento do sistema alvo ou dos usuários que o utilizam com relação a alguma propriedade relevante. Em relação aos padrões de comportamento dos usuários, busca-se identificar não somente os padrões mais comuns de uso como também os que representam tentativas de ações egoístas, oportunistas e maliciosas.
- **Modelagem**: modelagem do sistema alvo e dos padrões de comportamento dos seus usuários mais relevantes de forma a capturar os seus aspectos mais essenciais para os problemas relacionados a robustez, permitindo a avaliação do sistema em cenários fictícios mas realistas e a identificação de suas potenciais vulnerabilidades.
- **Algoritmos**: desenvolvimento e posterior avaliação de técnicas, algoritmos e mecanismos que possam oferecer maior robustez ao sistema alvo, tomando como base o conhecimento obtido a partir da caracterização e modelagem tanto do sistema como dos comportamentos de seus usuários.

As próximas seções descrevem, brevemente, as principais etapas e atividades previstas para a execução deste projeto, fazendo referência direta aos objetivos específicos que

pretendemos alcançar ao final dos dois anos de sua execução, conforme apresentado na seção 5. Tendo como base os três pilares acima, as técnicas principais utilizadas incluem as técnicas tradicionais de caracterização estatística [39] bem como aquelas baseadas em teoria de grafos e aplicadas a redes sociais [6, 13, 57, 27, 56, 75, 64, 72], a modelagem estocástica baseada na Teoria das Filas [42, 22] bem como a modelagem via simulação, a teoria de jogos [63, 55] e os algoritmos distribuídos. Um esforço será feito no sentido de identificação de soluções únicas no tratamento de diferentes problemas bem como de soluções integradas para problemas complementares.

6.1 Caracterização e Modelagem de Padrões de Comportamento de Usuários

Nesta etapa, pretendemos identificar e quantificar os padrões de comportamento, particularmente os maliciosos e oportunistas, de usuários de diferentes sistemas bem como identificar os possíveis impactos destes padrões na robustez dos mesmos. Os resultados desta etapa levarão à identificação de vulnerabilidades dos sistemas bem como criarão subsídios para o desenvolvimento de mecanismos mais robustos.

Os sistemas escolhidos para análise incluem o sistema de correio eletrônico, serviços de redes de relacionamento, particularmente o Youtube, o Flickr e o Orkut, os serviços de blogs e o serviço de notícias Slashdot. Para o caso do sistema de correio eletrônico, especificamente, o foco é o *spamming*, já muito estudado mas para o qual ainda não existe uma solução efetiva. Para os demais sistemas, em função da literatura limitada, buscamos realizar um estudo mais amplo dos diversos padrões de comportamento mais comuns e suas implicações para a robustez do sistema.

As atividades previstas nesta etapa são descritas abaixo. Em comum, elas utilizam técnicas tradicionais de caracterização estatística (sumarização de dados, distribuiçõe estatísticas) [39] bem como técnicas de teoria de grafos e técnicas comumentemente aplicadas a estas estruturas, particularmente no contexto de redes sociais [6, 13, 57, 27, 56, 75, 64, 72], além de técnicas de amostragem [5].

Redes de Relacionamento Estabelecidas no Sistema de Correio Eletrônico

Acreditamos que qualquer solução efetiva e eficaz para o controle de spam deve explorar as características inerentes a este tráfego, isto é, características que o distinguem do tráfego de e-mails legítimos, e que são difíceis de serem alteradas pelos *spammers*. Pretendemos estender os trabalhos de caracterização de tráfego de e-mails legítimos e de spams [33, 31, 32, 30] já realizados por alguns membros do grupo de pesquisadores para abordar aspectos dos relacionamentos estabelecidos entre remetentes e destinatários. O envio de um e-mail legítimo é tipicamente respaldado em algum relacionamento social (trabalho, amizade, etc) entre remetente e destinatário, enquanto que spams são normalmente enviados de forma indiscriminada por ferramentas automáticas, com o único objetivo de se atingir o maior número possível de usuários [31, 71]. Logo, dadas as naturezas inerentemente diferentes dos dois tipos de tráfego, pretendemos investigar se os relacionamentos formados entre remetentes e destinatários de e-mails legítimos são estatisticamente diferentes dos relacionamentos estabelecidos para o tráfego spam.

Nesta direção, pretendemos caracterizar e modelar os aspectos associados às redes de relacionamento estabelecidas entre *spammers* e os usuários atingidos por suas mensagens. Pretendemos modelar tais redes como grafos, considerando separadamente o tráfego de spam e o tráfego de e-mails legítimos, além de considerar a ponderação de arestas pelo volume de mensagens trocadas. Pretendemos analisar várias características dos relacio-

namentos, tais como coeficiente de agrupamento, distribuição e correlação dos graus dos vértices e diferentes métricas de reciprocidade. Será também analisada a formação de comunidades entre remetentes e destinatários. Modelos representativos serão propostos para cada aspecto considerado. Estes aspectos serão analisados ao longo de várias janelasde tempo, visando analisar padrões na evolução das redes criadas.

Esperamos obter resultados para as redes de e-mails legítimos que se aproximam daqueles anteriormente caracterizados em diferentes redes sociais, incluindo algumas redes de e-mails [57, 27, 75, 6, 56]. Para as redes estabelecidas entre *spammers* e seus destinatários, esperamos identificar características que sejam qualitativa e quantitativamente diferentes das observadas nas redes de e-mails legítimos, e que sejam mais apropriadas para redes estabelecidas a partir de comportamento malicioso, oportunista ou anti-social.

Padrões de Comportamento em Sistemas de Relacionamento

Pretendemos caracterizar e modelar os padrões de comportamento mais comuns e suas implicações sobre os sistemas de relacionamento escolhidos. Em particular, pretendemos analisar as principais redes que emergem dos relacionamentos e das interações entre os usuários destes sistemas. Por exemplo, o sistema Flickr permite a criação de redes de amigos explicítas bem como de redes implícitas geradas a partir de depoimentos entre usuários. No sistema Youtube, redes são criadas a partir de comentários dos usuários, sejam esses textuais ou mesmo na forma de vídeo-respostas. Por fim, os blogs e sistemas de notícias criam redes estruturais a partir das URLs no texto, mas outras redes também são criadas a partir dos padrões de visitação dos usuários a um sistema de blogs (blogoesfera). Pretendemos também analisar os padrões de evolução destas redes ao longo do tempo. Ao caracterizar os padrões de comportamento dos usuários e de tráfego, pretendemos diagnosticar (identificar e quantificar) padrões de comportamento malicioso e oportunista, tais como *spamming*, auto-promoção, ataques de conluio, etc.

A realização desta etapa depende da disponibilidade de dados reais. Para o caso do sistema de e-mails, nós temos disponíveis dois logs de e-mails categorizados como spams e e-mails legítimos recebidos pelo servidor central da UFMG em dois períodos distintos, cada um contendo mais de 360 mil e-mails. A coleta de novos logs do servidor central da UFMG bem como do servidor do Departamento de Ciência da Computação (DCC) da UFMG já está em andamento. Também estamos em negociação para a obtenção de logs de outras fontes. Também temos disponíveis os logs do tráfego para um grande sistema de blogs. Para o caso dos sistemas sociais, nós já construímos duas ferramentas coletoras de amostras de algumas redes de interações criadas em alguns deles. Pretendemos estender estas ferramentas para capturar outras redes criadas. Em suma, já estão disponíveis logs de várias fontes, cobrindo diferentes períodos, bem como ferramentas de coleta de dados. Estes logs e ferramentas viabilizam a execução desta parte do projeto e nos dão uma vantagem competitiva frente a outros grupos de pesquisa, uma vez que o acesso a uma base de dados heterogênea é bastante difícil, especialmente no exterior, por questões de privacidade. Pretende-se continuar a coletar novos logs durante todo o projeto.

6.2 Novos Mecanismos de Controle a Ações Maliciosas e Oportunistas

Nesta etapa, pretendemos desenvolver novos mecanismos que contribuam para tornar os vários sistemas baseados em redes de relacionamento bem como diferentes aplicações P2P mais robustas aos padrões de comportamento de usuários.

Para o caso do sistema de correio eletrônico, utilizaremos os resultados da etapa 6.1 na construção de mecanismos mais eficazes para deteção e controle de spam. De forma

similar, os resultados obtidos naquela etapa serão utilizados no projeto de mecanismos mais eficazes para identificação de usuários maliciosos e oportunistas nos diferentes sistemas baseados em redes de relacionamento analisados, bem como para o controle ou combate à sua atividade, além de mecanismos de moderação, que permitam aos sistemas identificar interações que podem ser de maior interesse para os demais usuários ou que possam ser prejudiciais, como no caso de *flame wars*. A eficácia dos mecanismos propostos será avaliada via modelagem analítica (p.ex: teoria das filas) e/ou de simulação em diversos cenários realistas, construídos a partir dos resultados obtidos na etapa anterior.

No contexto de aplicações P2P, enfatizaremos as aplicações de distribuição de vídeo e áudio, particularmente ao vivo, bem como das máquinas de busca descentralizadas construídas sobre arquiteturas P2P. Pretendemos desenvolver mecanismos para aumentar a robustez de tais sistemas a *free-riding*, ataques de conluio e Sybil, poluição de conteúdo (ou *spamming*) e também ao comportamento naturalmente dinâmico dos pares. Para as máquinas de busca P2P, mecanismos de replicação de conteúdo serão investigados para aumentar a robustez do sistema às instabilidades criadas a partir da entrada e saída dinâmica dos pares. Técnicas de reorganização da rede com base na observação de padrões de interação, interesses e disponibilidade de recursos também serão avaliadas para os mesmos fins, buscando favorecer uma organização que aumente a robustez da rede nos diversos contextos possíveis. Para a transmissão de vídeo e áudio, mecanismos dinâmicos de reconstrução de rota e de envio de múltiplos fluxos serão investigados para tratar deste problema, considerando também cenários onde a rede é heterogênea, incluindo dispositivos móveis (p.ex: celulares) com recursos limitados. Além disto, os padrões de comportamento malicioso e oportunista conhecidos serão mapeados para ataques específicos na aplicação alvo. Por exemplo, um spammer pode utilizar da máquina de busca descentralizada para retornar o seu conteúdo como altamente relevante para as consultas de usuários, mesmo que não seja este o caso. Mecanismos baseados em reputação (de pares, de conteúdo ou de ambos), incentivo e confiança serão investigados para tratar dos ataques específicos identificados para as aplicações alvo. Os mecanismos propostos serão avaliados via simulação, considerando diferentes arquiteturas P2P (estruturadas, não estruturadas ou híbridas). Além disto, sempre que possível, tentaremos validar os resultados de simulação através de modelagem analítica, particularmente através de modelos epidemiológicos recentemente aplicados a outros padrões de comportamento malicioso, tais como vírus e worms.

6.3 Diagnóstico de Anomalias no Tráfego de Redes

A área de metrologia de redes engloba um conjunto de ferramentas e métodos para inferir e melhor compreender o comportamento, a dinâmica e as propriedades da Internet atual. Nesse contexto de metrologia na Internet, a caracterização eficiente de padrões globais de tráfego de rede é crucial para se identificar uma utilização anômala da rede [65]. Anomalias de tráfego em redes são definidas como alterações significativas e pouco comuns nos padrões esperados em um ou múltiplos pontos da rede, sejam elas intencionais ou não [47]. As causas dessas anomalias de tráfego incluem, por exemplo, ataques distribuídos de negação de serviço em curso [43] e mudanças no encaminhamento IP devido a enganos na configuração de roteadores, falhas de equipamentos ou modificações nas políticas de roteamento BGP [67]. O diagnóstico de anomalias de tráfego, no entanto, apresenta grandes desafios, pois é necessário extrair padrões anômalos de grandes volumes de dados e as causas de anomalias podem ser bastante variadas.

O conceito de diagnóstico de anomalias de tráfego [46] envolve a detecção, a identificação e a quantificação desses fenômenos. A detecção consiste em determinar os pontos no tempo nos quais a rede enfrenta uma anomalia. A identificação envolve a classificação da anomalia a partir de um conjunto de anomalias conhecidas. A quantificação mede a importância da anomalia ao estimar o volume de tráfego anômalo de um determinado tipo

presente na rede. Independentemente das anomalias presentes na rede terem sido causadas intencionalmente ou não, a sua análise é importante, pois essas anomalias de tráfego podem degradar significativamente o serviço de rede, o que torna a sua detecção de grande valia do ponto de vista dos operadores. Portanto, a detecção eficiente e confiável de tais anomalias é essencial para a identificação rápida da ocorrência e para a tomada de ações que as corrijam, se necessário, contributindo para uma maior robustez dos sistemas de redes envolvidos.

O diagnóstico de anomalias contribui diretamente com outros objetivos específicos propostos neste projeto envolvendo a caracterização de padrões de comportamento e a detecção de ações oportunistas e maliciosas em redes sociais e P2P.

6.4 Caracterização, Modelagem e Algoritmos para Robustez em Redes Ópticas

Para se derivar soluções robustas para a agregação de tráfego, roteamento e alocação de comprimento de onda, é necessário que se entenda como é a demanda de tráfego entre os diversos pares origem/destino. Esta demanda é tipicamente traduzida em uma matriz de tráfego, a partir da qual deriva-se a demanda em cada enlace em uma certa topologia de redes. Para se validar os algoritmos propostos utilizando matrizes de tráfego, serão utilizados traços (do ingles *traces*) de tráfego coletado em redes operacionais. Estes traços constituem-se de coleta de informações dos cabeçalhos dos pacotes que passam por um certo ponto da rede. O centro de pesquisa em tráfego de redes NLNAR da CAIDA disponibiliza em seu site (www.nlanr.org) inúmeros traços coletados em diferentes pontos da Internet. Estes serão utilizados para se derivar matrizes de tráfego a serem usadas na validação dos algoritmos propostos. Uma tarefa a ser realizada e a compilação de traces reais, a fim de se construir um benchmark representativo.

Na literatura, existe uma série de relatos de estudos sobre os efeitos das limitações da camada física, como por exemplo o efeito dos fenômenos físicos, mencionados anteriormente na proposta em função da distância a ser percorrida e do conjunto de comprimento de ondas a ser utilizado. Os dados existentes na literatura, que são relatos de experimentos reais observados em *testbeds* operacionais serão utilizados para se definir os efeitos das limitações da camada física na validação dos algoritmos a serem propostos. Uma tarefa a ser realizada é a compilação destes resultados, que estão dispersos na literatura e que são de suma importância para a derivação de algoritmos e políticas que reflitam a realidade e que venham efetivamente contribuir para a robustez de sistemas de rede.

Uma das etapas do estudo é a derivação de algoritmos de roteamento e alocação de ondas, bem como de agregação de tráfego, que considerem proteção contra falhas através da previsão de rotas alternativas utilizadas em caso de ocorrência das mesmas. Os algoritmos para tráfego dinâmico e que consideram limitações do meio físico constituem uma das contribuições originais do projeto. Estes algoritmos utilizam Otimização e Teoria dos Grafos e a derivação destes será uma das etapas a serem realizadas. A validação dos algoritmos propostos será realizada através da comparação com resultados de simulação cujos cenários a serem simulados corresnderão a situações em redes reais, constituindo esta a tarefa final do estudo de robustez em redes ópticas.

6.5 Projeto e Avaliação de Sistemas de Confiança e Reputação para Sistemas de Rede Cooperativos

Uma forma de ataque às redes ad hoc e peer-to-peer diz respeito à falta de cooperatividade entre os nós. O funcionamento dessas redes depende da disponibilidade de cada nó em cooperar com os demais. Quando os nós constituintes da rede estão sob o domínio de uma mesma autoridade, é esperado que cada nó, além de fazer uso dos recursos da rede,

ofereça parte dos seus próprios recursos para o correto funcionamento de uma determinada aplicação. Entretanto, em um cenário mais geral, onde cada nó da rede pertence a uma autoridade diferente, não existem garantias de que todos os nós irão agir de forma cooperativa. Dada essa necessidade de tornar essas redes robustas à ataques por falta de cooperação, surgiram inúmeros estudos de mecanismos descentralizados de incentivos que têm como idéias principais premiar nós que cooperam ou punir nós que não cooperam. Alguns destes mecanismos exploram os conceitos de reputação. A utilização de sistemas baseados em reputação é intensamente estudada e considerada uma solução promissora para esse problema. Neste projeto, os mecanismos que compõem os modelos de reputação serão estudados e avaliados para que em seguida novas soluções sejam propostas para redes cooperativas. Além disso, um sistema de confiança que se baseia nas opiniões própria e apenas dos seus vizinhos será desenvolvido e analisado. A recomendação fornecida para os vizinhos segue uma métrica do grau de confiança baseada na maturidade da relação e nas observações das ações dos nós vizinhos. Ainda, será projetado e avaliado um mecanimo eficiente de detecção e de resposta a nós egoístas em redes ad hoc, reduzindo o número de falso-positivos e possibilitando uma melhora na taxa de entrega de pacotes nas redes ad hoc.

6.6 Projeto e Avaliação de Mecanismos de Segurança e QoS para Redes sem Fio

A falta de robustez das redes sem fio está ligada a diversas vulnerabilidades de segurança e anomalias de desempenho. Nesta etapa, serão projetados e avaliados arquiteturas, protocolos e mecanismos para o aumento dessa robustez.

Com relação a segurança, as redes sem fio necessitam de um controle de acesso com autenticação e autorização dos nós. Em redes com infra-estrutura, o controle de acesso é realizado de forma centralizada por um nó servidor que possui a lista dos nós autorizados e, após a autenticação, permite ou não o acesso à rede. Nas redes sem infra-estrutura, não é possível garantir que todos os nós terão acesso em qualquer momento a um servidor central e, em casos extremos, pode não existir um nó com a função específica de autenticar os demais nós da rede. Assim, a solução para a autenticação e a autorização nas redes sem infra-estrutura deve ser distribuída e robusta a desconexões e conluios. Além disso, essa solução deve ser completa, tratando a distribuição de endereços, a autenticação e a autorização através de um controle distribuído da lista de identidade/autorização dos nós. Após autenticar e autorizar os nós, é preciso ainda distribuir chaves simétricas de forma segura para permitir a assinatura/criptografia de mensagens com baixo consumo energético, pois dispositivos móveis, em geral, possuem restrições de processamento e bateria. Além disso, serão estudadas técnicas que garantam a privacidade, autenticidade, integridade e incontestabilidade nas comunicações sem fio de múltiplos saltos, frente a ataques.

No que diz respeito ao desempenho, as redes sem fio são vulneráveis a problemas de falhas e variações nas condições dos enlaces de comunicação, ao aumento do número de nós e usuários, e à mobilidade. Desta forma, o desempenho das redes sem fio está diretamente relacionada à perda de pacotes nos enlaces de comunicação. Nas redes IEEE 802.11, a perda de pacotes é geralmente representada pelo modelo Gilbert-Elliot. Porém, esse modelo não é apropriado para redes 802.11, sobretudo em ambientes indoor. Os demais modelos propostos ainda prescindem de uma representação adequada do comprimento das rajadas de perda, o qual afeta de forma significativa os mecanismos de controle de taxa das redes 802.11. Portanto, o desenvolvimento de modelos de perda de pacotes que levam em conta essa característica do processo de perda permitirá a concepção de mecanismos de controle automático de taxa robustos a falhas. Neste projeto, será desenvolvido um novo modelo de perdas de pacotes. Em seguida, um novo mecanismo de controle au-

tomático de taxa para redes IEEE 802.11 será proposto e avaliado através de simulações e experimentos. Além do problema de perdas de pacotes, as variações das conddições de propagação dos enlaces exigem dos protocolos responsáveis pelo encaminhamento robustez e auto-organização. Eeste protocolo deve ser robusto e se adaptar sem a intervenção dos usuários. Neste projeto será desenvolvido um novo protocolo de roteamento para redes sem fio com essas características.

Um outro problema enfrentado pelas redes sem fio é a escassez de espectro de freqüência para operação. Esse problema limita o desempenho dessas redes, e consequentemente a capacidade oferecida aos seus usuários, inviabilizando a ubiqüidade dessas redes. Neste contexto, uma nova tecnologia vem sendo desenvolvida nos últimos anos para aliviar esse problema, a qual consiste no emprego de rádios cognitivos, cujo principal objetivo é detectar e utilizar oportunidades no espectro de freqüência. No entanto, existe um problema de conflito de interesses entre os dispositivos que pode levar o sistema como um todo a estados indesejáveis. Neste projeto serão estudados, propostos e avaliados mecanismos e protocolos capazes de tornar uma rede composta por rádios cognitivos robusta a conflitos de interesses no compartilhamento do espectro através do emprego de técnicas de teoria de jogos e algoritmos genéticos.

Por outro lado, a rápida implantação das redes sem fio tem trazido problemas de escala quanto à densidade dos nós. Com a rápida integração de dispositivos sem fio em equipamentos portáteis, residenciais e de escritório, espera-se que a densidade desses nós possa rapidamente ultrapassar aquelas da telefonia celular. No entanto, diferentemente das redes de telefonia celular, as redes sem fio não-licenciadas vêm sendo implantadas de forma totalmente caótica e não planejada. Esse problema de robustez com relação ao número de nós tem recebido uma grande atenção nos últimos anos e será objeto de estudo neste projeto. Esse estudo consistirá na análise da capacidade fornecida pelas redes sem fio em ambientes de alta densidade; a concepção de mecanismos e algoritmos capazes de aumentar a capacidade desse tipo de rede; e a avaliação de desempenho, através de simulações e experimentos, desses mecanismos e algoritmos. Nesse contexto, novos mecanismos que otimizem o desempenho e a capacidade da rede sem fio em malha, através do uso de múltiplas rotas e de múltiplos gateways, serão propostos e avaliados. Além disso, serão estudados mecanismos de suporte à mobilidade e a comunicações em grupo, mecanismos de garantia de QoS para aplicações multimídia e telefonia sobre IP, assim como soluções de gerência de redes sem fio em malha.

A descoberta e a alocação de recursos são também serviços importantes em redes ad hoc, redes de sensores e redes em grade. Esses serviços permitem a interação entre os nós de forma que possam cooperar em atividades e/ou usufruir de recursos. No entanto, estes serviços devem levar em conta os problemas causados pelas falhas e pela entrada ou saídas dos nós da rede. Diversas pesquisas são realizadas em ambientes com grandes desafios em termos de escalabilidade e dinamicidade. Neste projeto serão estudados, propostos e avaliados mecanismos, protocolos e arquiteturas que se adequam a este tipo de ambiente e tornam essas redes robustas a falhas.

As redes tolerantes a atrasos e desconexões (Delay and Disruption Tolerant Networks - DTNs) são aquelas onde não existe a garantia da existência de conectividade fim-a-fim entre os sistemas finais. Desta forma, para se fornecer confiabilidade na entrega de dados nessas redes faz-se necessária a concepção de novos protocolos de comunicação. Neste projeto, protocolos de comunicação de diferentes níveis da pilha de protocolos serão propostos e avaliados quanto à robustez na entrega dos dados.

6.7 Cronograma de Execução

O cronograma de execução das principais atividades descritas nas seções acima, cobrindo um período de 2 anos, é apresentado abaixo. O número em parênteses se refere à seção

Tabela 2: Cronograma de Execução de Atividades

Atividade	**Trimestre**							
	1	2	3	4	5	6	7	8
Caracterização das Redes de E-mails (6.1)	X	X	X					
Evolução Redes de E-mails (6.1)			X	X	X			
Análise das redes sociais em Youtube/Flickr/blogs (6.1)		X	X	X	X	X	X	X
Novas soluções para spam (6.2)					X	X	X	X
Aplicações de áudio/vídeo P2P mais robustas (6.2)	X	X	X	X				
Máquinas de busca P2P mais robustas (6.2)					X	X	X	X
Análise de tráfego Skype (6.3)	X	X	X					
Deteção de tráfego Skype (6.3)				X	X	X		
Deteção de tráfego P2P (6.3)						X	X	X
Levantamento da matriz de tráfego (6.4)	X	X						
Determ. valores de limitações da camada física (6.4)	X	X						
Novas soluções roteamento/alocação de onda (6.4)			X	X	X	X		
Validação de soluções roteamento/alocação de onda (6.4)							X	X
Novas soluções para agregação de tráfego (6.4)			X	X	X	X		
Validação de soluções p/ agregação de tráfego (6.4)							X	X
Mecanismos de reputação para redes cooperativas (6.5)	X	X	X	X				
Deteção de nós egoístas em redes ad hoc (6.5)						X X	X	X
Autenticação/autorização em redes sem fio(6.6)	X	X	X					
Modelos de perdas de pacote em redes sem fio (6.6)	X	X						
Mecanismos de controle de taxa de perdas (6.6)			X	X	X			
Protocolos de roteamento para redes sem fio (6.6)						X	X	X
Mecanismos para robustez a conflitos de interesse (6.6)	X	X	X					
Mecanismos para robustez a escala (6.6)			X	X	X			
Mecanismos para robustez a falhas (6.6)						X	X	X
Novos protocolos de comunicação (6.6)				X	X	X	X	X

em que a atividade é descrita.

7 Equipe, Conhecimento, Experiência e Colaboração Internacional

A equipe deste projeto é constituída por 15 pesquisadores doutores de 5 instituições de ensino e pesquisa.

- Antonio Tadeu Azevedo Gomes (D. Sc. PUC-RJ-2005. Pesq. LNCC)
- Artur Ziviani (Dr. UPMC-2003, Pesq. LNCC, pesq. 2)
- Célio Vinicius Neves de Albuquerque (Ph. D. UCI-2001, Prof. UFF, pesq. 2)
- Daniel Ratton Figueiredo (Ph. D. UMASS-2005, Prof. UFRJ)
- Dorgival Olavo Guedes Neto (Ph. D. UA-1999, Prof. UFMG, pesq.2)
- Edmundo Albuquerque de Souza e Silva (Ph. D. UCLA-1984, Prof. UFRJ, pesq. 1A)

- Edmundo Roberto Mauro Madeira (D. Sc. Unicamp-1991, Prof. Unicamp, pesq.2)
- José Ferreira de Rezende (Dr. UPMC-1997, Prof. UFRJ, pesq. 1D)
- Jussara Marques de Almeida (Ph. D. UW-2003, Prof. UFMG, pesq. 2)
- Luís Henrique Maciel Kosmalski Costa (Dr. UPMC-2001, Prof. UFRJ, pesq. 2)
- Marcelo Gonçalves Rubinstein (D. Sc. COPPE/UFRJ-2001, Prof. UERJ)
- Nelson Luís Saldanha da Fonseca (Ph. D. USC-1994, Prof. Unicamp, pesq. 1C)
- Otto Carlos Muniz Bandeira Duarte (Dr. Ing. ENST-1985, Prof. UFRJ, pesq. 1C)
- Rosa Maria Meri Leão (Dr. UPS-1994, Prof. UFRJ)
- Virgílio Augusto Fernandes Almeida (Ph. D. VU-1987, Prof. UFMG, pesq. 1A)

O projeto procura reunir uma equipe de pesquisadores altamente qualificados, mesclando a experiência de 5 pesquisadores 1 do CNPq com a juventude e o talento de 7 pesquisadores com menos de 7 anos de doutorado. Onze componentes da equipe são pesquisadores do CNPq. A equipe também contempla instituições com grande tradição em pesquisa e grupos de pesquisa emergentes. Portanto, instituições de pesquisa emergentes e jovens pesquisadores fazem parte do projeto de forma a garantir uma maior difusão dos conhecimentos adquiridos e também a formação de uma nova geração de pesquisadores comprometidos e motivados com a solução dos desafios abordados.

Todos os componentes da equipe atuam em formação de recursos humanos de pós-graduação. O número de doutorandos e mestrandos diretamente beneficiados pelo projeto é significativo, somando 15 doutorandos, 21 mestrandos e 16 alunos de iniciação científica.

A equipe deste projeto apresenta uma grande experiência acumulada em diversas áreas do conhecimento específicas e complementares, facilitando sobremaneira a abordagem de diferentes aspectos dos desafios a serem vencidos.

O grupo de pesquisa do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais possui grande experiência em diversos aspectos abordados no projeto, tais como: caracterização e modelagem de comportamento dos usuários; comportamentos maliciosos e oportunistas; problemas de interação que emergem em redes sociais, bem como na modelagem e avaliação de aspectos relacionados à qualidade de serviço provida por sistemas distribuídos em larga escala, como desempenho e disponibilidade.

Dois grupos de pesquisa pertencem à Coordenação dos Programas de Pós-graduação em Engenharia da Universidade Federal do Rio de Janeiro: o grupo de Modelagem/Análise e Desenvolvimento de Sistemas em Computação e Comunicação (LAND) e o Grupo de Teleinformática e Automação (GTA). O LAND possui competência comprovada nas áreas de algoritmos e modelos de análise de desempenho e disponibilidade de sistemas de comunicação; desenvolvimento de ferramentas de desempenho e desenvolvimento de aplicações multimídias. O GTA possui larga experiência em redes sem fio, em protocolos de comunicação e em mobilidade, escalabilidade, qualidade de serviço e segurança em redes de computadores.

O grupo de pesquisa do Instituto de Computação da Universidade Estadual de Campinas possui competência nas áreas de modelagem de tráfego, serviços multimídias e redes ópticas.

O grupo do Programa de Pós-Graduação em Engenharia Eletrônica da Universidade do Estado do Rio de Janeiro (UERJ) possui competência em redes em malha, redes domiciliares e agentes móveis.

O grupo de Mecanismos e Arquitetura para Teleinformática (MARTIN) do Laboratório Nacional de Computação Científica (LNCC) possui experiência em medidas, computação móvel, modelagem em redes de computadores e desenvolvimento de software adaptativo.

A equipe do projeto já possui um bom histórico de trabalhos de pesquisa em conjunto. Muitos dos jovens pesquisadores foram orientados de mestrado ou de doutorado dos pesquisadores mais experientes e, conseqüentemente, com diversas publicações em conjunto. Além disso, os grupos de pesquisa envolvidos já participaram de diversos outros projetos de pesquisa que geraram contribuições de pesquisa conjuntas. Alguns projetos de pesquisa nos quais membros da equipe já participaram conjuntamente são: QUARESMA (CT-Info) , VIMOS (CT-info), TV-DIGITAL (FINEP) e TAQUARA (MCT/FINEP). Neste projeto, devido à característica específica de desafios mais amplos e de mais longo prazo, há uma maior multidisciplinaridade de áreas de conhecimento, mas a experiência passada em trabalhos conjuntos de pesquisa indica que a cooperação entre os grupos das diferentes instituições deve se desenvolver com naturalidade.

Outro aspecto muito importante para a obtenção de resultados significativos neste projeto é a grande interação dos grupos participantes com grupos de pesquisa estrangeiros. Esta interação ocorre de diferentes maneiras como, por exemplo: projetos de cooperação internacional, orientação conjunta de alunos em doutoramento no exterior, ex-orientadores de doutorado, ex-colegas de doutorado etc. Muitos destes pesquisadores estrangeiros participam de projetos nos Estados Unidos e na Europa com objetivos similares ou complementares a este projeto. Espera-se que este projeto possa se beneficiar enormemente da competência técnica e da grande experiência em projetos similares de colaboradores estrangeiros. Entre os pesquisadores que prontificaram a colaborar no projeto podem ser citados:

- Europa
  - Christophe Diot (Thomson Technology Paris Laboratory;
  - Guy Pujolle (Professor UPMC/LIP6);
  - Marcelo Dias de Amorim (Pesquisador CNRS, UPMC/LIP6);
  - Renata Cruz Teixeira (Pesquisadora CNRS, UPMC/LIP6);
  - Serge Fdida (Professor UPMC/LIP6).
- Estados Unidos
- Don Towsley (professor UMASS)

Os pesquisadores deste projeto já atuam em alguns dos desafios identificados. No entanto, esta atuação ocorre ainda de forma fragmentada objetivando soluções incrementais com metas de curto prazo. A reunião dos diversos pesquisadores num único projeto de longo prazo tem por finalidade criar uma competência multidisciplinar que possibilite uma sinergia capaz de abordar os desafios listados e, com isto, obter avanços significativos do estado da arte em longo prazo. Os resultados a serem alcançados devem romper com os paradigmas atuais, permitindo uma abordagem mais ampla sobre a questão da robustez em sistemas de rede.

A seguir, são relacionadas algumas publicações da equipe nas áreas de interesse do projeto que atestam a qualificação e a complementaridade das pesquisas e a adequação da equipe ao projeto. Diversas publicações possuem autores de diferentes grupos de pesquisa participantes deste projeto o que comprova a sinergia já existente entre pesquisadores participantes do projeto.

- Menascé, D., Dowdy, L., Almeida, V., "Performance by Design: Computer Capacity Planning By Example", Prentice Hall Inc., USA, 2004.

- Benevenuto, F., Costa C., Vasconcelos M., Almeida J., Almeida V., Mowbray M., "Impact of Peer Incentives on the Dissemination of Polluted Content", Proc. ACM Symposium on Applied Computing (SAC), Dijon, France, Abril 2006.

- Duarte, F., Mattos, B., Bestavros, A., Almeida V., Almeida J., "Traffic Characteristics and Communication Patterns in Blogosphere", Proc. International Conference on Weblogs and Social Media (ICWSM), Bouder, Colorado, Março, 2007 .

- Gomes, L., Castro, F., Bettencourt, L. Almeida, V., Almeida, J., Almeida, R., "Improving Spam Detection Based on Structural Similarity", Proc. USENIX Steps to Reducing Unwanted Traffic on the Internet (SRUTI2005), Cambridge, MA, Julho 2005

- Velloso, E., Almeida, V., Meira, W., Bestavros, A., Jin, S., "A Hierarchical Characterization of a Live Streaming Media Workload", IEEE/ACM Transactions on Networking, Fevereiro 2006.

- Costa, C., Almeida, J., "Reputation Systems for Fighting Pollution in Peer-to-Peer File Sharing Systems", Proc. Seventh IEEE International Conference on Peer-to-Peer Computing, Galway, Irlanda, Setembro 2007.

- Gomes, L., Almeida, J., Almeida, V., Meira Jr., W, "Workload Models of SPAM and Legitimate E-mails", Performance Evaluation, v. 64, p. 690-714, 2007.

- Costa, C., Almeida, J., Almeida, V., "Fighting Pollution Dissemination in Peer-to-Peer Networks", Proc. ACM Symposium on Applied Computing (SAC), Seul, Coréia do Sul, Março, 2007.

- Neto, H., Almeida, J., Rocha, L., Meira Jr., W., Guerra, P., Almeida, V. "E-commerce: A Characterization of Broadband User Behavior and Their E-Business Activities", ACM SIGMETRICS Performance Evaluation Review, Volume 32 Issue 3, ACM Press, Dezembro 2004.

- Gomes L., Cazita, C., Almeida, J., Almeida, V., Meira Jr., W., " Characterizing a SPAM Traffic", Proc. ACM/SIGCOMM Internet Measurement Conference 2004, Taormina, Itália, Outubro 2004.

- Rocha, B., Almeida, V., Guedes, D. O., "Increasing Quality of Service in Selfish Overlay Networks", IEEE Internet Computing, v. 10, n. 3, p. 24-31, 2006.

- Meira Jr., W., Ferreira, R, Guedes, D. O., "Escalabilidade e Eficiência em Mineração de Dados de Aplicações Internet", Proc. XXXIV Seminário Integrado de Hardware e Software (SEMISH), Rio de Janeiro, 2007.

- Almeida, H., Macambira, T., Guedes, D., Almeida, V., Meira Jr, W., "Um Sistema de Reputação Resistente a Ataques Sybil para Redes Overlay", Proc. III Workshop em Peer-to-Peer (WP2P), Belém 2007. p. 63-74.

- Coutinho, B., Guedes, D. O., Meira Jr., W., Ferreira, R., "Fault-tolerance in Filter Label-stream Applications", Proc. 18th International Symposium on Computer Architecture and High Performance Computing, Gramado 2007.

- Lima, M., Guedes, D. O., "Impacto das Políticas de Replicação na Disponibilidade de Documentos em Redes P2P sob Ataques DoS", Proc. Simpósio Brasileiro de Redes de Computadores, Gramado, 2004.

- Rocha, B., Almeida, V., Guedes, D. O., "Strategies to Improve Reliability in Routing Overlay Networks with Selfish Nodes", Proc. 24o. Simpósio Brasilieiro de Redes de Computadores, Curitiba, 2006.

- Campista, E. M., Passos, D. G., Esposito, P. M., Moraes, I. M., de Albuquerque, C. V. N., Muchaluat-Saade, D., Rubinstein, M. G., Costa, L. H. M. K., Duarte, O. C. M. B., "Routing Metrics and Protocols for Wireless Mesh Networks", IEEE Network Magazine, a ser publicado

- Campista, M. E. M., Moraes, I. M., Esposito, P. M., Amodei Jr., A., Cunha, D. O., Costa, L. H. M. K. e Duarte, O. C. M. B. - "The Ad Hoc Return Channel: a Low-Cost Solution for Brazilian Interactive Digital TV", in IEEE Communications Magazine, ISSN 0163-6804, vol. 45, no. 1, pp. 136-143, janeiro de 2007.

- Rubinstein, M. G., Duarte, O. C. M. B. e Pujolle, G., "Scalability of a Mobile Agents Based Network Management Application", Journal of Communications and Networks, IEEE/Korean Institute of Communications Sciences (KICS), vol. 5, no. 3, pp. 240-248, ISSN 1229-2370, setembro de 2003.

- Costa, L. H. M. K., Fdida, S. e Duarte, O. C. M. B., "Incremental Service Deployment Using the Hop By Hop Multicast Routing Protocol", in IEEE/ACM Transactions on Networking, ISSN 1063-6692, vol. 14, no. 3, pp. 543 - 556, junho de 2006.

- de Albuquerque, C. V. N., Suda, T. e Vickers, B., "Network Border Patrol: Preventing Congestion Collapse and Promoting Fairness in the Internet", IEEE/ACM Transactions on Networking, fevereiro de 2004.

- Hong, D., de Albuquerque, C. V. N., Oliveira, C. e Suda, T., "Evaluating the Impact of Emerging Streaming Media Applications on TCP/IP Performance", IEEE Communications Magazine, abril de 2001.

- Vickers, B., de Albuquerque, C. V. N. e Suda, T., "Source-Adaptive Multi-Layered Multicast Algorithms for Real-Time Video Distribution", IEEE/ACM Transactions on Networking, dezembro de 2000.

- Ziviani, A., Gomes, A. T. A., Monsores, M. L. e Rodrigues, P. S. S., "Network Anomaly Detection using Nonextensive Entropy, IEEE Communications Letters, IEEE Press, ISSN: 1089-7798. Aceito para publicação.

- Gomes, A. T. A., Batista, T. V., Joolia, A. e Coulson G., "Architecting Dynamic Reconfiguration in Dependable Systems". In: Rogério de Lemos; Cristina Gacek; Alexander Romanovsky. Architecting Dependable Systems, Heidelberg: Springer-Verlag, 2007, v., pp.237-261.

- Badue, C. S., Baeza-Yates, R., Ribeiro-Neto, B., Ziviani, A., Ziviani, N., "Analyzing Imbalance among Homogeneous Index Servers in a Web Search System", Information Processing & Management (IPM), Special Issue on Heterogeneous and Distributed Information Retrieval, Elsevier Science, ISSN: 0306-4573, vol. 43, no. 3, pp. 592–608, maio de 2007.

- Gueye, B., Ziviani, A., Crovella, M. e Fdida, S. "Constraint-Based Geolocation of Internet Hosts, IEEE/ACM Transactions on Networking, IEEE/ACM Press, ISSN: 1063-6692, vol. 14, no. 6, pp. 1219–1232, dezembro de 2006.

- Ziviani, A., Fdida, S., de Rezende, J. F. e Duarte, O. C. M. B., "Improving the Accuracy of Measurement Based Geographic Location of Internet Hosts, Computer Networks, Elsevier Science, ISSN: 1389-1286, vol. 47, no. 4, pp. 503–523, março de 2005.

- Augusto, C. H. P. e de Rezende, J. F. - "An Adaptive Approach to Service Discovery in Ad Hoc Networks", in 8th IFIP IEEE International Conference on Mobile and Wireless Communication Networks - MWCN'2006, pp. 61-75, Santiago, Chile, agosto de 2006.

- Cardoso, K. V. e de Rezende, J. F. - "Um Modelo de Markov Oculto para Representação de Perda de Pacotes em Redes 802.11 em Ambientes Indoor", VI Workshop em Desempenho de Sistemas Computacionais e de Comunicação - WPerformance'2007 (XXVII Congresso da Sociedade Brasileira de Computação - CSBC 2007), pp. 653-672, Rio de Janeiro, RJ, junho de 2007.

- Freitag, J., Fonseca, N. L. S., and de Rezende, J. F. - "Tuning of 802.11e Network Parameters", in IEEE Communication Letters, IEEE Press, vol. 10, n. 8, pp. 611-613, ISSN: 1089-7798, agosto de 2006.

- Silva, F. M. e de Rezende, J. F. - "Avaliação de Métodos Matemáticos usados nos Modelos de Reputação de Incentivo à Cooperação", XXV Simpósio Brasileiro de Redes de Computadores - SBRC'2007, pp. 999-1012, Belém, PA, maio de 2007.

- Viana, A. C., Amorim, M. D., Viniotis, Y., Fdida S. e de Rezende, J. F. - "Twins: A Dual Addressing Space Representation for Self-organizing Networks", in IEEE Transactions on Parallel and Distributed Systems", ISSN 1045-9219, vol. 17, n. 12, pp 1468-1481, dezembro de 2006.

- Carvalho, C., Madeira, E. R. M., Verdi, F. L. e Magalhães, M., "Policy-based Fault Management for Integrating IP over Optical Networks", IEEE 5th IP Operations and Management Symposium IPOM´05, 2005, Barcelona. Springer-Verlag, LNCS v. 3751. p. 88-97, 2005

- Carvalho, C., Madeira, E. R. M.. Verdi, F. L. e Magalhães, M., "Gerência de Falhas baseada em Políticas para Redes Ópticas- 24 Simpósio Brasileiro de Redes de Computadores (SBRC 06), Curitiba, 2006.

- da Fonseca, N. L .S., Drummond, A. C. e Gyurek, R., "A Fixed-Parameter Tractable Algorithm for the Wavelength Assignment in WDM Mesh Networks", submetido para IEEE International Conference on Communications 2008.

- Drummond, A. C., da Fonseca, N. L. S. e Devetsikiotis, M. "A Multiobjective Fuzzy Bandwidth Partitioning Model for Self-Sizing Networks", European Journal of Operational Research, aceito para publicação na Special Issue on 'Performance Evaluation of QoS-aware Heterogeneous Systems', 2007.

- Figueiredo, G. B., da Fonseca, N. L. S. e Monteiro, J. A. S., "A Minimum Interference Routing Algorithm with Reduced Computational Complexity", Computer Networks, vol 50, no. 11, p. 1710-1732, 2006.

- Melo, C. A. V. e da Fonseca, N. L. S., "Envelope Process and Computation of the Equivalent Bandwidth of Multifractal Flow", Computer Networks, vol. 48, no. 3, p. 351-375, 2005.

8 Relevância do Trabalho e Impacto dos Resultados

A solução de grandes desafios inspira um pensamento criativo que leva os pesquisadores a buscar soluções que vão além do incremental, mas que, de fato, trazem uma grande contribuição para a sociedade. No entanto, soluções de tal escala requerem longos períodos de pesquisa com equipes de excelência e requerem uma visão mais ampla dos problemas, o que implica em uma necessidade de conhecimento complementar.

Pesquisas de longo prazo sobre o futuro dos sistemas de rede permitem uma revolução tecnológica com potencial para gerar inúmeras novas oportunidades de realizações de alto impacto sócio-econômico. Em especial, para o Brasil, um país em desenvolvimento, se antecipar às novas tendências através da criação de soluções inovadoras pode ser um passo imprescindível para uma melhor inserção dentro da economia mundial.

Nos próximos dez anos, infra-estruturas de serviços de rede abrirão portas para uma variedade de aplicações que custarão pouco para serem construídas e utilizadas. No entanto, o avanço dentro dessas perspectivas está diretamente atrelado ao aprimoramento das técnicas para garantia da robustez desses sistemas de rede. Como exemplos, temos as aplicações comerciais via Internet, que dependem cada vez mais de uma garantia de segurança e privacidade para que os usuários utilizem-nas com mais freqüência. Além disso, mesmo serviços mais básicos, como e-mails ou serviços de voz sobre IP podem ser prejudicados através do envio de spams ou ainda por ataques de negação de serviço que impedem a utilização do serviço durante um longo período. Por outro lado, se as soluções propostas para esses problemas tiverem um custo muito alto, a tecnologia pode ser eliminada do mercado e todos os possíveis benefícios não poderão ser oferecidos à população. Assim, é necessário o desenvolvimento de soluções robustas e baratas. Isso significa que as soluções devem otimizar os recursos disponíveis, tais como o meio físico, bateria, equipamento, entre outros.

Com relação ao impacto social, a Internet, assim como serviços de rede em geral, são parte crucial da infra-estrutura de comunicação, além de serem parte integral dos sistemas de indústria e comércio. Assim, avanços nas tecnologias de rede influenciam e continuarão influenciando diretamente o comportamento da sociedade moderna. Para uma melhor inclusão no contexto internacional, o Brasil precisa acompanhar esse avanço tecnológico, propondo e participando ativamente dessas mudanças. Mais do que isso, o desenvolvimento dos sistemas de rede no Brasil pode permitir uma inclusão digital de grande parte da população carente. Essa inclusão digital, além de permitir que a população carente usufrua das vantagens trazidas pela Internet, tais como e-mails, comércio eletrônico, e-gov, entre outros, também permite o impulsionamento de áreas mais afastadas dos grandes centros. Isso pode ser feio através da educação à distância, da possibilidade de instalação de empresas e centros de pesquisa, e da possibilidade do crescimento das atividades econômicas locais devido ao acesso à rede.

Deve-se então ressaltar o papel preponderante dos sistemas de rede no que se refere à base na sociedade moderna para avanços científicos e sociais de relevância. O grande desafio imposto pelo problema de robustez em sistemas de rede impacta, ao menos indiretamente, outros dos grandes desafios propostos pelo documento "Grandes Desafios da Computação no Brasil: 2006–2016". Em particular, podemos mencionar os desafios de "Gestão da informação em grandes volumes de dados multimídia distribuídos" e "Acesso participativo e universal do cidadão brasileiro ao conhecimento". Sistemas de rede representam a infra-estrutura básica para as soluções de tecnologia de informação e comunicação para esses grandes desafios. Os grandes volumes de informação a serem tratados e geridos são oriundos da inédita disponibilização da informação provida pela Internet e o gerencimento eficiente e distribuído desses grandes volumes de informação certamente se beneficia da presença de um sistema de redes robusto como suporte. De forma similar, a universalização de acesso ao conhecimento do cidadão brasileiro necessariamente passa

por soluções que se utilizem de redes de comunicação robustas para o suporte adequado a aplicações de ensino a distância, inclusão digital e telemedicina.

Assim, o arcabouço unificado de mecanismos para a provisão de sistemas de rede robustos também encontra-se em consonância e se harmoniza com diferentes iniciativas governamentais em projetos de grande vulto para o suporte ao desenvolvimento do país em áreas como inclusão digital, saúde, educação, suporte a aplicações de e-ciência, entre outras. Podemos citar alguns dessses projetos de grande vulto em andamento atualmente que, por serem fortemente dependentes de uma infra-estrutura de comunicação eficiente, inequivocamente se beneficiam da provisão de sistemas de redes mais robustos como os propostos neste projeto para a sua adequada operação e fornecimento de serviços inovadores à sociedade brasileira:

- Sistema Brasileiro de TV Digital – `http://sbtvd.cpqd.com.br/`
- Secretaria de Ensino a Distância do MEC – `http://portal.mec.gov.br/seed/`
- Projeto Rede-Conhecimento do MCT – `http://www.redecomep.rnp.br/projeto/`
- Rede Universitária de Telemedicina (RUTE) – `http://rute.rnp.br/`
- Sistema Nacional de Processamento de Alto Desempenho (SINAPAD) – `http://www.sinapad.lncc.br/`

Portanto, as soluções para os grandes desafios dos sistemas de rede são de grande relevância para o Brasil e para o mundo, impulsionando bilhões de dólares nas mais diversas atividades. Mais do que isso, essas soluções podem permitir uma transformação da sociedade, através do aumento das oportunidades tanto educacionais como comerciais. Assim, o desenvolvimento de um arcabouço unificado de mecanismos embase as soluções para os grandes problemas dos sistemas de rede se torna essencial para todos os países que desejam acompanhar o desenvolvimento econômico mundial dos próximos anos.

9 Cronograma Físico-Financeiro

A Tabela 3 apresenta o orçamento previsto para este projeto no período de 24 meses. O cronograma de desembolso para este orçamento prevê 50% dos valores solicitados para o primeiro ano de atividade e 50% para o segundo ano de atividade do projeto, dentro das rubricas declaradas.

Tabela 3: Orçamento

CUSTEIO

Item	**Valor unitário**	**Quantidade**	**Total**
Material de consumo	—	—	R$ 24.000,00
Diária nacional	R$ 187,83	213	R$ 40.007,79
Diária internacional	R$ 440,00	252	R$ 110.880,00
Passagem nacional	R$ 1.000,00	40	R$ 40.000,00
Passagem internacional	R$ 3.000,00	42	R$ 126.000,00
Serviços de terceiros	—	—	R$ 132.881,03
TOTAL DE CUSTEIO			**R$ 473.768,82**

CAPITAL

Item	**Valor unitário**	**Quantidade**	**Total**
Material Bibliográfico	R$ 200,00	10	R$ 2000,00
–**Equipamento**			
Micro Dual Core com pelo menos 1GB RAM e 160GB Disco	R$ 3.000,00	2	R$ 6.000,00
Micro Dual Core com pelo menos 1.5GB RAM e 200GB Disco	R$ 4.000,00	25	R$ 100.000,00
Micro Dual Core com pelo menos 2GB RAM e 300GB Disco	R$ 5.000,00	2	R$ 10.000,00
Servidor de simulação	R$ 6.000,00	1	R$ 6.000,00
Notebook com pelo menos 1.5GB RAM e 160GB Disco	R$ 6.000,00	6	R$ 36.000,00
Notebook com pelo menos 2GB RAM e 250GB Disco	R$ 8.000,00	3	R$ 24.000,00
Comutador 24 portas GbE + 1 mini-GBIC	R$ 6.000,00	1	R$ 6.000,00
TOTAL DE CAPITAL			**R$ 190.000,0**0

BOLSAS

Tipo	**Meses**	**Quantidade**	**Total**
DTI-2	24	1	R$ 52.484,88
DTI-2	12	1	R$ 26.242,44
DTI-3	24	3	R$ 75.304,08
DTI-3	12	2	R$ 25.101,36
ITI-A	24	8	R$ 57.600,00
TOTAL DE CAPITAL			**R$ 236.732,76**

TOTAL DO PROJETO **R$ 900.501,58**

A justificativa detalhada dos itens solicitados em cada rubrica se segue:

Custeio :

- **Material de Consumo**: compra de material de papelaria e informática necessários ao desenvolvimento do projeto tais como toners, papel, CD, DVD, cartucho de impressora a serem distribuídos entre os pesquisadores das 6 instituições participantes.
- **Passagens e Diárias (nacionais e internacionais)**: participação e apresentação de artigos técnicos com resultados do projeto em conferências e eventos de alto impacto e visibilidade na comunidade científica. São previstas passagens nacionais e internacionais, distribuídas entre os 15 pesquisadores e alguns de seus alunos envolvidos no projeto. Vale ressaltar que uma parte das passagens e diárias nacionais serão utilizadas pelos pesquisadores para visitas técnicas e reuniões internas do projeto, necessárias para a maior integração do grupo e desenvolvimento do projeto.
- **Serviços de Terceiros**: previsão para eventual necessidade de contratação de serviços de terceiros necessários ao desenvolvimento do projeto, bem como a organização de 2 *workshops* para a integração, coordenação e promoção de ações em conjunto entre os 15 pesquisadores das 6 instituições participantes deste projeto, oriundas de 3 estados diferentes.

Capital: os itens solicitados são necessários para atualizar e complementar os recursos de hardware já instalados nos laboratórios das instituições participantes, para melhor desenvolvimento do projeto proposto.

- **Material Bibliográfico**: aquisição de livros nas áreas de interesse do projeto.
- **Microcomputadores**: desenvolvimento e experimentação, em ambientes heterogêneos, das várias soluções e modelos que serão propostos neste projeto.
- **Servidor de Simulação**: realização de experimentos de simulação bem como armazenamento de grandes bases de dados necessários para o desenvolvimento do projeto.
- **Notebooks**: desenvolvimento e experimentação, em ambientes heterogêneos, de soluções para redes sem fio e eventual aprsentação de resultados de pesquisa fora de cada instituição.
- **Comutador**: infra-estrutura de rede necessária.

Bolsas: participação de recursos humanos com diferentes níveis de qualificação na execução das atividades previstas neste projeto.

Referências

[1] Alexa - the web information company. Disponível em http://www.alexa.com. visitado em 02/11/2007.

[2] Peabirus - construa seu caminho. Disponível em http://www.peabirus.com.br. visitado em 02/11/2007.

[3] Pesquisa do ibge. http://www.ibge.gov.br/home/estatistica/populacao/acessoainternet/.

[4] Rfc 2582 - the newreno modification to tcp's fast recovery algorithm, 1999.

[5] Yong-Yeol Ahn, Seungyeop Han, Haewoon Kwak, Sue Moon, and Hawoong Jeong. Analysis of topological characteristics of huge online social networking services. In *Proceedings 16th World Wode Web (WWW) Conference*, Maio 2007.

[6] A. Arenas, L. Danon, A. Diaz-Guilera, P. Gleiser, and R. Guimera. Community analysis in social network. *The European Physical Journal B.*, 38, Março 2004.

[7] Fabiano Atalla, Daniel Miranda, Jussara Almeida, Marcos André Gonçalves, and Virgílio Almeida. Analyzing the impact of churn and malicious behavior on the quality of peer-to-peer web search. In *23rd ACM Symposium on Applied Computing*, March 2008.

[8] H. P. Baker. Authentication approaches. In *Proc. 56th IETF Meeting*, Março 2003.

[9] Salman Baset and Henning Schulzrinne. An analysis of the skype peer-to-peer internet telephony protocol. In *INFOCOM*. IEEE, 2006.

[10] Matthias Bender, Sebastian Michel, Peter Triantafillou, Gerhard Weikum, and Christian Zimmer. P2p content search: Give the web back to the people. In *Fifth International Workshop on Peer-to-Peer Systems*, 2006.

[11] Randeep Bhatia, Murali Kodialam, and T.V. Lakshman. Fast network re-optimization schemes for mpls and optical networks. *Computer Networks*, (50):317–331, 2006.

[12] UOL Blog. http://blog.uol.com.br.

[13] S. Bornholdt and H. G. Schuster. *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley-VCH, 2003.

[14] H. P. Brondmo. Solving spam by establishing a platform for sender accountability. In *Proc. 56th IETF Meeting*, Março 2003.

[15] Vint Cerf. Spam, spim and spit. *Communications of ACM*, 48(2):39–43, 2005.

[16] Bin Chen, Wen-De Zhong, and Sanjay Kumar Bose. Applying saturated cut method for dynamic traffic grooming in ip/mpls over wdm networks. *IEEE COMMUNICATIONS LETTERS*, 10(2):117–119, 2006.

[17] Nicolas Christin, Andreas S. Weigend, and John Chuang. Content availability, pollution and poisoning in file sharing peer-to-peer networks. In *EC '05: Proceedings of the 6th ACM conference on Electronic commerce*, pages 68–77, New York, NY, USA, 2005. ACM.

[18] B. Cohen. Incentives build robustness in bittorrent. In *Proceedings of the Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, USA, 2003.

[19] Computer Emergency Response Team. CSI/FBI - Computer Crime and Security Survey. *Computer Security Institute–FBI*, 2006.

[20] Cristiano Costa and Jussara Almeida. Reputation systems for fighting pollution in peer-to-peer file sharing systems. In *Seventh IEEE International Conference on Peer-to-Peer Computing*, 2007.

[21] Cristiano Costa, Jussara Almeida, and Virgilio Almeida. Fighting pollution dissemination in peer-to-peer networks. In *ACM Symposium on Applied Computing (SAC)*, 2007.

[22] Lawrence Dowdy Daniel Menascé and Virgílio Almeida. *Performance by Design: Computer Capacity Planning by Example*. Prentice Hall Inc., 2004.

[23] Flickr Compartilhamento de Fotos. http://www.flickr.com/.

[24] J. Douceur. The sybil attack. In *International Workshop on Peer-to-Peer Systems (IPTPS), LNCS*, volume 1, 2002.

[25] Christos Doulkeridis, Kjetil Norvag, and Michalis Vazirgiannis. Desent: Decentralized and distributed semantic overlay generation in p2p networks. *Selected Areas in Communications, IEEE Journal on*, January 2007.

[26] Fernando Duarte, Bernardo Mattos, Azer Bestavros, Virgilio Almeida, and Jussara Almeira. Traffic characteristics and communication patterns in blogosphere. In *International Conference on Weblogs and Social Media (ICWSM)*, March 2007.

[27] H. Ebel, L. Mielsch, and S. Bornhold. Scale=free topology of e-mail networks. *Physical Review E.*, 66-035103(R), 2002.

[28] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica. Free-riding and whitewashing in peer-to-peer systems. *Selected Areas in Communications, IEEE Journal on*, 24(5):1010–1019, May 2006.

[29] Michal Feldman, Christos Papadimitriou, John Chuang, and Ion Stoica. Free-riding and Whitewashing in Peer-to-Peer Systems. In *Proc. ACM SIGCOMM (PINS)*, New York, NY, 2004.

[30] L. H. Gomes, R. Almeida, L. M. Bettencourt, V. Almeida, and J. M. Almeida. Comparative graph theoretical characterization of networks of spam and regular email. In *Second Conference on Email and Anti-Spam*, Julho 2005.

[31] L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, and W. Meira. Characterizing a spam traffic. In *Proc. 4th ACM SIGCOMM Internet Measurement Conference*, Outubro 2004.

[32] L. H. Gomes, F. Castro nad R. B. Almeida, L. M. Bettencourt, V. Almeida, and J. M. Almeida. Improving spam detection based on structural similarity. In *Proc. USENIX Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI)*, Julho 2005.

[33] Luiz Gomes, Jussara Almeida, Virgilio Almeida, and Wagner Meira Jr. Workload models of spam and legitimate e-mails. *Performance Evaluation*, 64:690–714, 2007.

[34] Seungyeop Han, Yong-Yeol Ahn, Sue Moon, and Hawoong Jeong. Collaborative blog spam filtering using adaptive percolation search. In *3rd Workshop on Weblogging Ecosystem held in conjunction with WWW 2006*, Maio 2006.

[35] E. Harris. The next step in the spam control war: Greylisting. http://projects.puremagic.com/greylisting.

[36] Todd Hoff. Skype failed the boot scalability test: Is P2P fundamentally flawed? Disponível em http://highscalability.com/skype-failed-boot-scalability-test-p2p-fundamentally-flawed, 2007. visitado em 02/11/2007.

[37] KaZaa Homepage. http://www.kazaa.com.

[38] Message Labs Homepage. http://www.messagelabs.com.uk/.

[39] Raj Jain. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley- Interscience, 1991.

[40] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina. The Eigentrust Algorithm for Reputation Management in P2P Networks. In *Proc. WWW Conf.*, Budapest, Hungary, 2003.

[41] Jon M. Kleinberg. Challenges in mining social network data: processes, privacy, and paradoxes. In *KDD '07: Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 4–5, New York, NY, USA, 2007. ACM.

[42] Leonard Kleinrock. *Queueing Systems*. John Wiley and Sons, 1975.

[43] Ramana Rao Kompella, Sumeet Singh, and George Varghese. On scalable attack detection in the network. 15(1):14–25, February 2007.

[44] B. Krishnamurthy. Shred: Spam harassment reduction via economic desincentives. In *Proc. 56th IETF Meeting*, Março 2003.

[45] James Kurose and Keith Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Pearson Education, 2005.

[46] Anukool Lakhina, Mark Crovella, and Christophe Diot. Diagnosing network-wide traffic anomalies. Portland, OR, USA, August 2004.

[47] Anukool Lakhina, Mark Crovella, and Christophe Diot. Mining anomalies using traffic feature distributions. Philadelphia, PA, USA, August 2005.

[48] YOUNGSEOK LEE and BISWANATH MUKHERJEE. Traffic engineering in next-generation optical networks. *IEEE Communications Surveys & Tutorials*, 6(3):16–33, 2004.

[49] J. Liang, R. Kumar, Y. Xi, and K. Ross. Pollution in p2p file sharing systems. In *Proceedings of IEEE Infocom*, Março 2005.

[50] MessageLabs. Spam and viruses hit all time highs in 2003, publicado no website da message labs, Dezembro 2003. http://www.messagelabs.com.

[51] T. Meyer and B. Whateley. Spambayes: Effective open-source, bayesian based, email classification system. In *Proc. 1st Conference on Email and Anti-Spam (CEAS)*, Julho 2004.

[52] Alan Mislove, Krishna P. Gummadi, and Peter Druschel. Exploiting social networks for internet search. In *Proc. 5th Workshop on Hot Topics in Networks*, Irvine, CA, 2006.

[53] Alan Mislove, Massimiliano Marcon, Krishna P. Gummadi, Peter Druschel, and Bobby Bhattacharjee. Measurement and analysis of online social networks. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, New York, NY, USA, 2007. ACM.

[54] MySpace. www.myspace.com.

[55] J.F. Nash. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences of the United States of America*, 36:48–49, 1950.

[56] M. Newman. Mixing patterns in networks. *Physical Review E.*, 67-026126, 2002.

[57] M. Newman, S. Forrest, and J. Balthrop. E-mail networks and the spread of computer viruses. *Physical Review E*, 66-035101(R):1–4, 2002.

[58] Digg All News and Videos. www.digg.com.

[59] World Internet Usage Statistics News and Population Stats. http://www.internetworldstats.com/stats.htm.

[60] Alicia Nicki, Washington, Chih-Chieh Hsu, Harry Perros, and Michael Devetsikiotis. Approximation techniques for the analysis of large traffic-groomed tandem optical networks. In *Proceedings of the IEEE 38th Annual Simulation Symposium*, pages –, 2005.

[61] A. Ntoulas, M. Najork, M. Manasse, and D. Fetterly. Detecting spam web pages through content analysis. In *15th International Conference on World Wide Web*, 2006.

[62] Orkut. www.orkut.com.

[63] M.J. Osborne and A. Rubinstein. *A Course in Game Theory*. MIT Press, 1994.

[64] R. Pastor-Satorras and A. Vespignani. *Evolution and Structure of the Internet: A Statistical Physics Approach*. Cambridge University Press, 2004.

[65] Animesh Patcha and Jung-Min Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. 51(12):3448–3470, 2007.

[66] J. Postel. Rfc 793 transmission control protocol, 1981.

[67] Matthew Roughan, Tim Griffin, Morley Mao, Albert Greenberg, and Brian Freeman. IP forwarding anomalies and improving their detection using multiple data sources. In *Proc. of the ACM SIGCOMM'2004 Workshop on Network Troubleshooting*, Portland, OR, USA, August 2004.

[68] Stuff that Matters Slashdot: News for Nerds. www.slashdot.org.

[69] Stephen L. Spitler and Daniel C. Lee. Integrating effective-bandwidth-based qos routing and best effort routing. In *Proceedings of IEEE INFOCOM 2003*, pages –, 2003.

[70] Daniel Stutzbach and Reza Rejaie. Understanding churn in peer-to-peer networks. In *IMC '06: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, pages 189–202, New York, NY, USA, 2006. ACM.

[71] R. D. Twining, M. M. Williamson, M. Mowbray, and M. Rahmouni. E-mail prioritization: Reducing delays on legitimate mail caused by junk mail. In *Proc. USENIX Annual Technical Conference*, Junho 2004.

[72] J. Tyler, B. Huberman, and D. Wilkinson. *Email as Spectroscopy: Automated Discovery of Community Structure within Organizations, Communities and Technologies*. B. V. Kluwer, 2003.

[73] Kevin Walsh and Emin Gun Sirer. Fighting peer-to-peer spam and decoys with object reputation. In *In Proceedings of P2PECON Workshop, Philadelphia, Pennsylvania*, August 2005.

[74] Wei Wei. Network design issues for a terabit optical internet. *Communications Engineer*, pages 38–41, April 2003.

[75] B. Wellman, J. Salaff, D. Dimitrova, L. Garton, M. Gulia, and C. Haythomthwaite. Computer networks as social networks: Collaborative work, telework and virtual community. *Annual Review of Sociology*, 22, 1996.

[76] Wang Yao and Byrav Ramamurthy. A link bundled auxiliary graph model for constrained dynamic traffic grooming in wdm mesh networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, 23(8):1542–1555, 2005.

[77] Tong Ye, Qingji Zeng, Wei Wei, Guolong Zhu, Junjie Yang, Yaohui Jin, and Lannes Yannick. Routing algorithms in ip/wdm networks based on hop-constraint lightpath establishment approach. *IEEE COMMUNICATIONS LETTERS*, 9(2):181–183, 2005.

[78] Youtube Broadcasting yourself. www.youtube.com.

[79] D. Zeinalipour-Yatis, V. Kalageraku, and D. Gunopulos. Exploiting locality for scalable information retrieval in peer-to-peer networks. *Information Systems Journal*, 30(4), 2005.

[80] Ákos Szödényi, Szilárd Zsigmond, Balázs Megyer, and Tibor Cinkler. Design of traffic grooming optical virtual private networks obeying physical limitations. In *Proceedings of IEEE*, pages –, 2005.