Redes de Nova Geração:
Tecnologias Estratégicas de Comunicação

Coordenador: Prof. Otto Carlos Muniz Bandeira Duarte
Grupo de Teleinformática e Automação – GTA
Coordenação dos Programas de Pós-Graduação em Engenharia – COPPE
Universidade Federal do Rio de Janeiro – UFRJ

1 Introdução

A globalização tornou o domínio da tecnologia da informação e das telecomunicações um fator estratégico e fundamental para o desenvolvimento sócio-econômico-cultural de qualquer nação desenvolvida. Cada vez mais se faz necessário o acesso à informação a qualquer instante (*always connected anytime and anywhere*). Hoje, a rede Internet é que procura atender esta necessidade. A Internet atual baseia-se no paradigma de inteligência nas extremidades da rede e no perfil de protocolos TCP/IP. O sucesso extraordinário da Internet fez com que a maioria das aplicações desenvolvidas até hoje se "acomodassem" a este modelo, notadamente pela adaptação das aplicações para funcionarem sobre o protocolo IP (*all over IP*). No entanto, o modelo da Internet vai fazer 40 anos e, portanto, o seu modelo foi proposto para uma realidade bem diferente da que existe hoje. Pode-se afirmar que a Internet evoluiu nestas quatro últimas décadas e também que as mudanças realizadas adaptaram-se muito bem a uma série de desafios que lhe foram impostos. Por outro lado, está cada vez mais claro que o atual modelo não poderá mais se adaptar por muito tempo devido às novas tecnologias e necessidades que estão surgindo. Uma "nova Internet" se faz necessária para um futuro que não deve estar muito distante. Os centros mais desenvolvidos (EUA e Europa) vêm investindo muitos recursos de pesquisa no que se convencionou chamar a "Internet do Futuro" ou a "Nova Geração da Internet".

Os desafios a serem vencidos por esta "nova Internet" são enormes. As redes sem fio assumirão um papel fundamental para garantir mobilidade e ubiqüidade. O número de pontos de acesso sem fio (*hotspots*) deve se multiplicar rapidamente nos centros urbanos. Uma rede única que acomode as diferentes tecnologias sem fio

(wi-fi, wimax, bluetooth, UWB, rede sem fio regional, redes de sensores etc.) é ainda um grande desafio. Muitas tecnologias de redes sem fio devem coexistir e a Intel já promete para os próximos anos um circuito integrado com diferentes tecnologias embutidas. Os problemas de *handoff* horizontal (de uma célula para outra) e vertical (passagem de uma tecnologia para outra) são problemas em aberto.

Além das diferentes tecnologias existem as redes com características específicas. Alguns exemplos de redes de nova geração são as Redes Ad Hoc Móveis [1] (*Mobile Ad Hoc Networks* - MANETs), as Redes Ad Hoc Veiculares (*Vehicular Ad Hoc Networks* - VANETs), as Redes em Malha Sem Fio (*Wireless Mesh Networks* - WMNs) e as Redes Tolerantes a Atrasos e Desconexões [2] (*Delay and Disruption Tolerant Networks* - DTNs). Todas impõem novos problemas a serem vencidos.

A escalabilidade e a complexidade destas novas redes também são novos desafios. Fala-se em centenas de milhares de sensores espalhados pelos centros urbanos e nos nossos lares e novos paradigmas de comunicação começam a ser discutidos tais como M2M (*mobile-to-machine*) e T2T (*thing-to-thing*). A comunicação sem fio traz consigo novos problemas de espectro de freqüência reduzido, taxas de comunicação variáveis, interferências, altas taxas de erros, etc. Também, o crescimento vertiginoso do número de usuários da Internet e a inclusão de dispositivos eletrônicos comunicantes (tais como sensores, etc.) aumentarão enormemente os custos de gerenciamento e operação da rede Internet. Há propostas de mudar radicalmente o atual modelo da Internet que colocam inteligência no interior da rede, ao invés da inteligência apenas nas extremidades, e que usam algoritmos bio-inspirados para tornar as complexas tarefas de gerenciamento e manutenção automáticas. Este novo paradigma de redes convencionou-se chamar de redes autônomas. Um novo esquema de roteamento e um novo protocolo de transporte são também necessários.

Outro desafio importante para a Internet do Futuro é a segurança. O problema da segurança se tornou tão grave que constitui um empecilho à maior utilização da própria rede. Há diferentes pragas virtuais, como a invasão de bancos de dados de empresas, sítios forjados que escondem fraudes e diferentes golpes, e uma quantidade brutal de mensagens de correio eletrônico não solicitadas, os *spams* [3]. A Internet se tornou com o passar dos anos, além de um mecanismo de comunicação e de busca de

informação, um instrumento de negócios. Desta forma, os problemas de segurança que são atualmente enfrentados produzem também extraordinários prejuízos financeiros. Por outro lado, num país como o Brasil e para o Estado do Rio de Janeiro, a Internet é um mecanismo de inclusão social do qual a sociedade não pode abrir mão. A utilização da rede como instrumento de disseminação do conhecimento, mas também para tornar mais eficientes e fazer chegar a toda a população os serviços prestados pelo governo, de forma eletrônica, é fundamental para o desenvolvimento do Estado do Rio e do país. O desenvolvimento e utilização destes serviços passam por garantias de segurança da rede. Com o aumento da escala de uso da Internet e a inserção maciça de redes móveis, todos esses problemas tendem a se tornar ainda mais graves e, assim, o desenvolvimento de medidas de segurança torna-se um ponto chave para a evolução da Internet.

Para atender essas novas demandas, a nova geração de redes deverá dar ênfase à mobilidade, à ubiqüidade, à qualidade de serviço e à segurança. Estes temas foram explicitamente destacados no relatório da Sociedade Brasileira de Computação (SBC) sobre os principais desafios da pesquisa em computação no Brasil até 2016 [4]. O relatório aponta a necessidade de desenvolvimento de novas infra-estruturas de comunicação que levem em conta esses aspectos. O Estado do Rio de Janeiro possui um histórico de pioneirismo no país em tecnologias da informação e comunicação. Portanto, é estratégica a manutenção de sua posição de vanguarda com equipes envolvidas diretamente na concepção e desenvolvimento de soluções que suplantem esses desafios.

O momento atual reflete a forte convergência de mídias (como a Internet, a TV e o telefone celular) cujo gargalo será, sem dúvida, possibilitar o acesso cidadão brasileiro ao conhecimento disponível. Essa garantia de acesso é apontada como um dos principais desafios no relatório da SBC. Essas novas tecnologias podem ser utilizadas como redes de acesso de baixo custo que permitem mobilidade e conectividade até mesmo em locais de difícil acesso. Outra característica importante é a sua flexibilidade. Essas redes atendem tanto usuários que desejam conectividade a todo instante e em qualquer lugar, como comunidades carentes ou localizadas em regiões remotas que necessitam de acesso à Internet e serviços de telefonia.

Nesse projeto serão realizados estudos relevantes para o desenvolvimento de tecnologias de redes de nova geração. O objetivo é a pesquisa e o desenvolvimento de tecnologias estratégicas de comunicação para o Estado do Rio de Janeiro, visto que o acesso à informação e o domínio tecnológico são fatores indispensáveis para o sucesso econômico no mundo globalizado e para a garantia da soberania nacional.

2 Objetivos

Os principais objetivos deste projeto são:

- assegurar a formação e o aperfeiçoamento de estudantes e pesquisadores do Estado do Rio de Janeiro nos temas de pesquisa relacionados neste projeto;
- aplicar, estender, adaptar ou generalizar alguns dos conhecimentos já adquiridos na área de sem fio e segurança;
- propor e avaliar o desempenho de novos modelos, mecanismos, arquiteturas, serviços e protocolos relacionados aos temas deste projeto;
- disponibilizar à comunidade científica, aos construtores de equipamentos de rede e aos desenvolvedores de software, um conjunto de técnicas, módulos e/ou ferramentas de simulação para a avaliação de desempenho de mecanismos de suporte às novas tecnologias emergentes abordadas neste projeto.

Os principais objetivos deste projeto são de médio e longo prazo. A principal meta deste projeto é a construção de um ambiente de pesquisas e a formação de recursos humanos nas áreas de Comunicação Sem Fio e Segurança em Redes de Computadores. Para os próximos 24 meses, os temas abordados são detalhados a seguir.

3 Linhas de Pesquisa

Este projeto irá investigar os mecanismos, protocolos e aplicações que devem servir de base à construção da Internet do Futuro.

A arquitetura da Internet apresenta hoje grandes desafios em termos de como prover garantias de qualidade de serviço e de como prover segurança. Como não há

mecanismos de qualidade de serviço implementados no núcleo da rede, não há como se fornecer garantias, atualmente. Como conseqüência, as comunicações multimídias ainda estão sendo implementadas lentamente. Não é surpresa que "dar suporte ao crescente fluxo de dados multimídia" foi considerado um dos principais desafios da pesquisa em computação no relatório da SBC [4]. A Internet começa a ser usada para telefonia, mas a qualidade nem sempre é satisfatória. Em termos de transmissão de vídeo, os tamanhos de imagem utilizados são reduzidos e a qualidade de imagem é ruim. Pode-se melhorar o serviço para as aplicações multimídias pela instalação de enlaces de comunicação de capacidade cada vez maior. No entanto, o que se tem observado é que a demanda de tráfego é sempre crescente. Desta forma, é necessário também investigar mecanismos de qualidade de serviço que possam ser incorporados à arquitetura da rede.

Neste projeto, serão investigados alguns dos temas fundamentais de segurança na Internet atual e na Internet do Futuro, onde mobilidade e ubiqüidade serão também uma tônica. Assim, serão estudados os mecanismos de segurança para a Internet cabeada, em especial os mecanismos de combate aos *spams* que constituem hoje um problema em aberto. Também serão investigados os mecanismos de segurança necessários às redes sem fio, que são uma tecnologia fundamental para permitir a mobilidade e tornar a Internet ubíqua, mas que apresentam ainda hoje falhas de segurança não resolvidas que precisam ser melhor compreendidas.

Outros grandes desafios que devem ser enfrentados dizem respeito ao desejo por mobilidade e ubiqüidade. Os usuários desejam estar conectados enquanto se movimentam, seja caminhando dentro de um campus universitário, no transporte público, ou dentro de seus carros. Por outro lado, os usuários desejam também estar conectados a todo momento e em qualquer lugar, ou seja, esperam que o acesso à Internet seja ubíquo. A implementação de uma Internet móvel e ubíqua impõe importantes desafios tecnológicos, nos quais as redes sem fio desempenham um papel importante, por permitirem a mobilidade, mas também por permitirem a chegada da Internet a locais de difícil acesso e/ou alto custo de instalação de infra-estrutura de cabos.

A arquitetura da Internet se baseia em um esquema de endereçamento hierárquico.

Esta estrutura de endereçamento é uma das razões do sucesso de um sistema distribuído do porte da Internet. No entanto, a rigidez da estrutura de endereçamento impõe dificuldades à implementação da mobilidade. Uma vez que um endereço IP identifica, em última instância, onde um sistema está conectado à rede, como definir endereços para estações móveis torna-se um problema difícil. Este é um dos principais desafios de projeto da Internet do Futuro.

De outro lado, novas redes móveis sem fio servirão de base para que a Internet do Futuro seja ubíqua. Redes móveis ad hoc permitem aos usuários formar uma rede sob demanda e autoconfigurável. Redes em malha sem fio permitem ao usuário mobilidade e se conectar à Internet mesmo em locais de difícil acesso, sendo uma solução de baixo custo que ajudará, portanto, a democratizar o acesso à rede. Redes ad hoc veiculares, implementadas também com novas tecnologias de comunicação sem fio, permitirão o desenvolvimento de novas aplicações com foco na segurança dos passageiros de veículos automotores, mas também o acesso à Internet pelos seus passageiros. Finalmente, redes tolerantes a atrasos e desconexões serão capazes de levar a Internet às localidades mais distantes do país e, num futuro mais distante, a outros planetas. Estes novos tipos de redes que permitirão tornar a Internet do Futuro ubíqua são temas de pesquisa em efervescência.

Neste projeto, os principais temas de pesquisa necessários à definição da arquitetura da Internet do Futuro foram divididos em quatro linhas de atividades: redes sem fio, redes ad hoc veiculares, redes tolerantes a atrasos e desconexões, e segurança. Nas seções a seguir são descritas as atividades dentro de cada uma destas linhas.

Atividade A1: Redes Sem Fio

O IEEE 802.11, o principal padrão de redes locais sem fio, suporta dois modos de funcionamento das redes sem fio. Um deles é o infra-estruturado, no qual a conexão dos nós da rede é feita via um ponto de acesso. O segundo tipo é o modo ad hoc, no qual as estações podem se comunicar diretamente e de forma distribuída. Caso duas estações estejam fora de alcance, outras estações intermediárias podem encaminhar o tráfego garantindo a comunicação. Assim, as estações trabalham de

forma colaborativa para manter a conectividade da rede.

Roteamento em Redes em Malha Sem Fio

Nas redes ad hoc, a mobilidade dos nós aliada às instabilidades do meio físico podem resultar em baixa conectividade [5]. Desta forma, as redes em malha sem fio utilizam um *backbone* composto por roteadores geralmente fixos. Esses nós estendem a área de cobertura de pontos de acesso e garantem conectividade à rede. Em redes ad hoc móveis, a métrica para a escolha de rotas usualmente utilizada é o número de saltos. Nessas redes, esta métrica é adequada dado o dinamismo dos nós que pode levar a diversas quebras de enlaces. Torna-se então importante obter rapidamente uma rota para o destino, não importando a sua qualidade. Nas redes em malha sem fio, em contrapartida, o número de quebras de enlaces não é tão grande, visto que os roteadores são geralmente fixos. Portanto, os protocolos de roteamento se preocupam mais com as variações da qualidade dos enlaces do que, mais precisamente, com as suas quebras. Além disso, foi observado que minimizando o número de saltos, há uma tendência de escolher rotas formadas por enlaces longos e de pior qualidade [6, 7]. Assim, surgiram as métricas cientes da qualidade [8] que tentam refletir as variações do meio físico nas métricas de roteamento.

Um dos objetivos deste projeto é avaliar o desempenho das principais métricas e protocolos de roteamento para redes em malha sem fio, através da realização de experimentos, a fim de definir quais as métricas e protocolos que mais se adequam a essas redes. Serão realizados experimentos em redes de testes em ambientes fechado e aberto. A fim de comparar as métricas de roteamento, serão avaliados a taxa de perdas, o número de trocas de rotas, a vazão, o tamanho médio das rotas e o tempo de ida e volta (*Round-Trip Time* - RTT).

Capacidade das Redes em Malha Sem Fio

O estudo da capacidade fornecida pelas redes sem fio em malha IEEE 802.11 é um tema de pesquisa bastante importante nos dias atuais. Diversos modelos analíticos foram propostos e estendidos para essa finalidade [9, 10]. No entanto, devido às diversas simplificações adotadas por esses modelos, ainda não é possível capturar com a devida acurácia a capacidade dessas redes. Fenômenos tais como a captura, a interferência co-canal, e os níveis discretos das taxas de transmissão utilizadas, na

maioria das vezes não foram modelados. Nesta atividade, será derivado um modelo analítico para a capacidade das redes sem fio em malha. Durante a concepção do modelo, ele será validado através de simulações no ns-2 [11]. A partir dos resultados extraídos do modelo, ele será utilizado para conceber e avaliar mecanismos para o aumento da capacidade dessas redes.

Modelos de Perda e Seleção Automática de Taxas em Redes IEEE 802.11

A perda de pacotes em redes sem fio é um assunto amplamente tratado desde que surgiram as primeiras tecnologias. Nas redes IEEE 802.11, a perda de pacotes é geralmente representada pelo modelo Gilbert-Elliot [12]. 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 erro e de taxa das redes 802.11. Nesta atividade, é proposto um modelo de Markov Oculto capaz de representar essa importante característica do processo de perda de pacotes. Ainda dentro desse contexto, são avaliadas várias propostas para o controle automático de taxa com o intuito de maximizar o desempenho da rede [13]. Modulação, relação sinal-ruído e probabilidade de perda são conceitos bem estabelecidos, no entanto, a interligação dessas características de forma a escolher a taxa de transmissão ideal tem se mostrado um problema complexo. Há diversos mecanismos propostos, mas poucos foram implementados e avaliados na prática. Mesmo entre os mecanismos que chegaram a ser simulados, ainda há oportunidades para melhorias [14]. Nessa atividade, é planejada a avaliação de alguns mecanismos de controle automático de taxa através de simulação, assim como a implementação e avaliação de um novo mecanismo em ambiente real como parte de um *driver* de uma determinada placa de rede sem fio.

Redes Sem Fio Cognitivas

Um dos principais problemas que afetam as redes sem fio hoje em dia é a escassez de espectro de freqüência, que limitam o seu desempenho e a sua capacidade. Este problema é ainda mais acentuado no caso das redes que utilizam as limitadas faixas de freqüências não-licenciadas, como as redes do padrão IEEE 802.11. Uma das

possíveis soluções para este problema é o emprego de novas tecnologias, como a dos rádios cognitivos, que são capazes de detectar e utilizar oportunidades no espectro de freqüências aumentando o seu desempenho [15, 16]. Assim, tornam-se importantes o estudo e desenvolvimento de novas aplicações que utilizam rádios cognitivos capazes de utilizar o espectro de freqüência de maneira mais eficiente. Nesta atividade serão estudados, propostos e avaliados mecanismos e protocolos necessários à adoção e o correto funcionamento de rádios cognitivos. Para isso, diferentes técnicas de inteligência computacional, tais como algoritmos genéticos, lógica nebulosa e teoria de jogos serão empregadas.

Atividade A2: Redes Ad Hoc Veiculares

Redes ad hoc veiculares, ou VANETs (*Vehicular Ad Hoc NETworks*), são redes de comunicação onde os nós são veículos automotores com interfaces de rede sem fio embarcadas, ou pontos fixos ao longo de estradas ou ruas. Estas redes podem ser consideradas um caso especial das redes ad hoc móveis e vêm recebendo atenção especial [17], pois constituem uma evolução necessária em direção à ubiqüidade.

Diferentes aplicações podem ser vislumbradas para redes ad hoc veiculares. De forma geral, elas podem ser divididas em dois grupos: aplicações de usuário e aplicações de segurança. Para esta atividade, nos concentraremos nas aplicações de usuário, especificamente em sistemas *peer-to-peer* (P2P), com aplicações para sistemas de busca e *download* de arquivos.

Os sistemas *peer-to-peer* (P2P) para VANETs, ou *car-to-car*, apresentam desafios, como a alta mobilidade dos nós, podendo gerar quebras de enlaces e a perda de qualidade das comunicações, pois o tempo de contato entre pares pode não ser suficiente para estabelecer uma conexão e efetuar a transferência desejada. É de grande interesse que um nó saiba selecionar seus parceiros, aumentando as chances de sucesso nas transferências, levando em conta o parceiro com o qual existirá o maior tempo de contato, a melhor relação sinal-ruído, ou outros fatores que favoreçam o *download* do arquivo.

Dada a grande dinamicidade esperada em um cenário como esse, tanto dos participantes quanto dos recursos disponíveis, uma questão importante é a definição de

um protocolo eficiente para a descoberta e seleção dinâmica de recursos. Propõe-se então a concepção de um protocolo capaz de descobrir e selecionar os parceiros mais aptos a oferecer o serviço desejado em um determinado instante em um cenário de VANETs. Esse protocolo deve considerar as diferentes métricas envolvidas e ser robusto a alterações nas condições da rede durante o fornecimento do serviço. Essa robustez deve permitir certa transparência à aplicação demandante em relação aos obstáculos encontrados nas camadas inferiores ao fornecimento adequado do serviço.

Em face ao exposto, o objetivo central desta atividade é desenvolver e aplicar um algoritmo que permita que os nós do sistema P2P decidam quais arquivos desejados devem ser obtidos, quando serão solicitados e de que parceiros da rede, de forma a minimizar o tempo de transferência necessário. Será preciso investigar que informações são necessárias, e como obtê-las, utilizando, por exemplo, otimizações inter-camadas ou até mesmo obtendo informações como o trajeto planejado.

Primeiramente, será realizado um estudo por simulação e em uma segunda etapa, serão realizados testes com um protótipo em escala real no campus Ilha do Fundão da UFRJ utilizando roteadores sem fio, alimentados pela bateria do próprio automóvel. O objetivo dos testes é um estudo de viabilidade da tecnologia 802.11 como suporte de comunicação sem fio em uma VANET, cenário de alta mobilidade, mas de trajetórias particulares.

Atividade A3: Redes Tolerantes a Atrasos e Desconexões

As Redes Tolerantes a Atrasos e Desconexões (*Delay and Disruption Tolerant Networks* - DTNs) têm despertado o interesse de muitos pesquisadores, universidades e empresas da área de redes. As DTNs são caracterizadas por atrasos longos e variáveis, conectividade intermitente e alta taxa de erros. Para contornar os problemas de atrasos e desconexões, as DTNs se servem da técnica de comutação de mensagens além de armazenamento persistente. Na comutação de mensagens nenhum circuito é estabelecido com antecedência entre a origem e o destino, não existindo qualquer fase anterior ao envio de dados. Quando uma mensagem precisa ser enviada, ela é armazenada e encaminhada nó a nó desde a origem até o destino. Por utilizar essa técnica, diz-se que as DTNs são redes do tipo armazena-e-encaminha

(*store-and-forward*), ou seja, primeiro a mensagem é recebida integralmente e armazenada para, em seguida, ser enviada ao próximo nó, que pode ou não ser o destino. O paradigma de DTNs tem sido empregado, com sucesso, para promover a integração social e digital em regiões carentes desprovidas de qualquer infra-estrutura de comunicação. Nestes cenários, são usadas "mulas de dados" (*data Mobile Ubiquitous LAN Extensions* - data MULE), tais como ônibus, para interconectar a região carente a uma rede Internet.

Em síntese, DTN ainda é um tema muito recente que possui diversos aspectos desafiadores. O sucesso de aplicações comerciais nesta área nos próximos anos deve indicar a importância que as DTNs devem assumir no futuro. Neste sentido, dentro desse projeto é proposto o desenvolvimento e a implementação de um protótipo de rede que segue a arquitetura de redes DTN. A implementação corresponde ao desenvolvimento dos principais componentes definidos na arquitetura DTN do grupo de pesquisas em Redes Tolerantes a Atrasos (*Delay Tolerant Networking Research Group* - DTNRG) do *Internet Research Task Force* (IRTF). Através desse protótipo de rede será possível a realização de experimentos, validando diversos protocolos e aplicações em ambientes DTN reais. As aplicações tolerantes a atrasos e desconexões serão testadas com usuários finais munidos de portáteis e/ou assistentes digitais (PDAs) através de interfaces gráficas amigáveis apropriadas para estas aplicações.

Atividade A4: Segurança

Segurança é um dos maiores desafios para as redes de computadores. Na Internet, os prejuízos devido aos ataques de *hackers* atingem desde o usuário doméstico até as grandes empresas, o que justifica os grandes investimentos que vêm sendo feitos nesta área. Na Internet do Futuro, esse problema será ainda maior, devido à utilização de redes sem fio sem infra-estrutura. Outro grande desafio será o combate aos *spams*, ou mensagens eletrônicas não solicitadas. Atualmente esse já é um problema amplamente discutido e combatido, mas com a expansão e diversificação dos serviços oferecidos pela Internet, esse problema tende a se estender ainda mais.

Detecção de Intrusão e Confiança em Redes Ad Hoc

Sistemas de detecção de intrusão (SDI) observam a rede em busca de ações

maliciosas. Em redes ad hoc, os SDI são ainda mais importantes, pois, devido ao roteamento colaborativo, ações maliciosas de uma única estação podem impedir o funcionamento de toda a rede. No entanto, devido a erros de transmissão e colisões, ações comuns na rede podem ser interpretadas como ações maliciosas. Dessa forma, um bom SDI para redes ad hoc deve reduzir a taxa de falsos positivos. Além disso, nas redes sem fio, um nó só pode escutar os pacotes emitidos por nós que estejam dentro do seu alcance. Assim, é preciso que os nós troquem informações sobre ações maliciosas e utilizem um sistema de confiança para julgar essas informações.

O objetivo desta atividade é propor um SDI com baixa taxa de falsos positivos e modelos de confiança para redes ad hoc baseados no aprendizado dos nós. O SDI será inicialmente desenvolvido para a detecção de ações egoístas, ou seja, de nós que, embora façam requisições para transmissão de dados, não encaminham mensagens de dados dos vizinhos para poupar energia. Na área de confiança, um modelo está sendo proposto no qual cada nó da rede é responsável por computar um grau de confiança para seus vizinhos. Para tanto, o modelo proposto define um grau de confiança dependente das experiências acumuladas e da recomendação dos vizinhos.

Controle de Acesso e Sistemas de Distribuição de Chaves

O controle de acesso e a distribuição de chaves em redes infra-estruturadas são feitos de forma centralizada, na qual o administrador cadastra usuários em um sistema de autenticação e as aplicações consultam esse sistema para autorizar ou não o usuário a utilizar algum recurso. Em redes ad hoc, não é possível garantir que um nó responsável pela autenticação estará sempre disponível devido à baixa conectividade. Assim, o controle de acesso deve ser feito de forma distribuída. Além disso, dispositivos móveis possuem baixa capacidade computacional. Sendo assim, esses dispositivos devem utilizar operações criptográficas simples, como criptografia simétrica. Dessa forma, é preciso que exista um sistema de gerenciamento de chave simétrica distribuído sempre disponível.

O objetivo desta parte do projeto é o desenvolvimento de um sistema de controle de acesso, que atualize de forma distribuída a lista de nós autorizados na rede, e o desenvolvimento de um sistema de distribuição de chaves simétricas que, baseado nessa lista de nós autorizados, gerencie o uso de chaves simétricas na rede.

Spams

A adoção de sistemas anti-*spam* é a principal contramedida utilizada no combate aos *spams*. Os falsos positivos de um sistema anti-*spam* têm um impacto muito grande para os usuários, já que uma mensagem legítima pode ser identificada como *spam*, causando grandes transtornos e prejuízos.

O objetivo desta tarefa é desenvolver um sistema anti-*spam* que leve em conta o histórico do comportamento dos usuários na decisão se a mensagem é legítima ou não. Um usuário que já enviou várias mensagens legítimas terá uma probabilidade muito menor de ter suas mensagens classificadas como *spam*. O histórico de comportamento de um usuário é determinado por diversos servidores de correio eletrônico. Na troca de informações entre os servidores é utilizado um sistema de confiança para avaliar a reputação de cada servidor e a confiança nos dados informados.

4 Metodologia

A metodologia empregada é a convencionalmente usada nesta área técnica. Ela consiste dos seguintes passos: estudo bibliográfico e verificação do estado da arte; estabelecimento dos requisitos a serem atendidos e análise qualitativa; elaboração da proposta de tese e disseminação dos resultados.

Verifica-se o estado da arte através de buscas realizadas em revistas especializadas, em anais de congressos e em bases de dados sediadas na Internet. Procura-se identificar as equipes estrangeiras e nacionais que estão trabalhando nas áreas de pesquisa. É estimulada a construção de páginas Web sobre cada tema estudado.

Uma vez delimitada a problemática são estabelecidos os requisitos a serem atendidos. Uma avaliação qualitativa é realizada a fim de se evidenciar as vantagens e desvantagens das arquiteturas (serviços, protocolos, mecanismos, modelos, ferramentas, plataformas etc.) estudadas e procura-se focar nos requisitos a serem atendidos na nova proposta.

O processo de concepção de uma proposta original é complexo e possui diversas peculiaridades. Sempre que possível, procura-se a obtenção de resultados quantitativos através de análises matemáticas, simulações ou implementações. Os resultados

quantitativos da proposta são validados e comparados com as propostas existentes.

Os resultados são submetidos a congressos nacionais e internacionais. As teses, os artigos aceitos em congressos e periódicos e os relatórios técnicos são disponibilizados na Internet através de páginas Web. Os softwares, as ferramentas, as aplicações são também disponibilizadas via Internet.

Os temas focados são tratados segundo abordagens comparáveis ao que há de mais moderno em pesquisa de redes de computadores nos centros mais renomados internacionalmente e perfeitamente adequadas à atualidade do país.

5 Equipe

O projeto será coordenado pelo professor Otto Carlos Muniz Bandeira Duarte da UFRJ. Também fazem parte da equipe os professores José Ferreira de Rezende da UFRJ, que participa do projeto como pesquisador associado, Antônio Tadeu Azevedo Gomes do LNCC, Artur Ziviani do LNCC, Luís Henrique Maciel Kosmalski Costa da UFRJ e Marcelo Gonçalves Rubinstein da UERJ, que participam do projeto como pesquisadores emergentes. Os demais membros da equipe estão listados na tabela a seguir.

O Grupo de Teleinformática e Automação (GTA) iniciou suas atividades em março de 1986. As atividades de pesquisa, desenvolvimento e formação de recursos humanos têm sido orientadas para as áreas de Redes de Computadores, Protocolos de Comunicação e Tecnologias Multimídias. O GTA participa ativamente dos cursos de graduação em Engenharia de Computação e Informação (ECI), Engenharia de Controle e Automação (ECA), Engenharia Eletrônica e de Computação (DEL) da Escola Politécnica (POLI) da UFRJ, e na pós-graduação, no Programa de Engenharia Elétrica (PEE) da Coordenação de Programas de Pós-Graduação em Engenharia (COPPE) da UFRJ. A experiência do GTA no desenvolvimento de protótipos é bastante significativa. Entre estes trabalhos podem ser citados um sistema de comunicação de alto desempenho com as sete camadas OSI, um sistema de comunicação confiável em teleconferência, um protocolo de transporte multidestinatário para ambientes multimídias e uma arquitetura de implementação adaptada

a aplicações multimídias. A formação de recursos humanos de qualidade pode ser comprovada por mais de uma centena de teses de mestrado e doutorado defendidas e mais de 300 publicações. Maiores informações sobre o GTA podem ser obtidas no endereço `http://www.gta.ufrj.br`.

O Programa de Pós-Graduação em Engenharia Eletrônica (PEL) da Universidade do Estado do Rio de Janeiro (UERJ) é parceiro deste projeto através do grupo de pesquisa do professor Marcelo Gonçalves Rubinstein. O Professor Marcelo realizou o mestrado e o doutorado em Engenharia Elétrica no GTA e continua colaborando com o grupo há muitos anos. O professor possui larga experiência em redes sem fio e participou de diversos projetos de pesquisa com o GTA, como o Projeto GIGA Taquara.

O Laboratório Nacional de Computação Científica (LNCC) participa deste projeto através do grupo de pesquisa coordenado por Artur Ziviani, que realizou seu mestrado no GTA e obteve seu doutorado na Université Pierre et Marie Curie (Paris 6) sob a co-orientação de professores do GTA. Há, portanto, um longo histórico de colaboração com o grupo, atestado por diversas publicações em comum ao longo dos últimos anos. Atualmente, o pesquisador coordena projetos de P&D nas áreas de metrologia de redes e medicina assistida por computação.

Doutorandos	**Mestrandos**	**Graduandos**
Alexandre Andrade Pires	André Chaves Mendes	Daniel Vega Simões
Carlos Henrique P. Augusto	Carina Teixeira de Oliveira	Diogo Menezes F. Mattos
Daniel de Oliveira Cunha	Danilo Michalczuk Taveira	Hugo Eiji T. Carvalho
Igor Monteiro Moraes	Fabiana Martins da Silva	Marcelo Duffles D. Moreira
Kleber Vieira Cardoso	Natalia Castro Fernandes	Pedro Miguel Esposito
Marcel William R. da Silva	Natanael Delgado de Freitas	Pedro Silveira Pisa
Miguel Elias M. Campista	Raphael Melo Guedes	Pedro Smith Coutinho
Pedro Braconnot Velloso	Reinaldo Bezerra Braga	Rafael dos Santos Alves
	Savio Rodrigues Cavalcanti	Ulysses Cardoso Vilela

6 Metas, Resultados e Cronograma de Execução

As metas desse projeto são:

- desenvolver uma rede de testes para avaliar o desempenho de protocolos e métricas de roteamento para redes em malha sem fio;
- avaliar e desenvolver mecanismos para o aumento da capacidade das redes em

malha sem fio;

- avaliar mecanismos de controle automático de taxa para redes sem fio IEEE 802.11;
- estudar, avaliar e propor mecanismos e protocolos para a adoção de rádios cognitivos em redes sem fio;
- desenvolver uma rede de testes para avaliar os cenários de mobilidade em uma rede ad hoc veicular;
- estudar e propor algoritmos de seleção de pares para aplicações *peer-to-peer* em redes ad hoc veiculares;
- desenvolver uma rede de testes para avaliar a arquitetura de redes tolerantes a atrasos e desconexões;
- avaliar e propor sistemas de detecção de intrusão, controle de acesso e distribuição de chaves para redes ad hoc;
- avaliar e propor sistemas anti-*spam*.

Ao final de 24 meses espera-se obter 5 protótipos, 5 módulos de software, 5 teses de D.Sc., 10 teses de M.Sc. e 2 Trabalhos de Final de Curso. É possível estimar uma produção científica composta de 41 publicações em periódicos/conferências e 9 relatórios técnicos.

Os protótipos realizados durante o projeto serão:

- uma rede em malha sem fio experimental constituída de roteadores IEEE 802.11 equipados com o *firmware* OpenWRT, executando diversos protocolos de roteamento num ambiente *indoor*;
- uma rede veicular experimental distribuída em automóveis no campus da UFRJ equipados com computadores portáteis com interfaces de rede sem fio IEEE 802.11;
- uma rede DTN experimental, seguindo a arquitetura proposta pelo DTNRG do IRTF, implementando diversos protocolos e aplicações em ambientes reais;

- um sistema anti-*spam* baseado na troca de informações entre servidores de correio eletrônico e na suas respectivas reputações calculadas por um sistema de confiança;

- algoritmos de seleção automática de taxa para o padrão IEEE 802.11 implementados e testados no *driver* MadWifi.

A formação de pessoal qualificado e o desenvolvimento e o conhecimento de novas técnicas, objetos deste projeto, visam suprir uma demanda crescente nos próximos anos por profissionais capazes de instalar e operar redes de comunicação de dados sem fio. Os projetos recentes em curso nos Estados Unidos e Europa na área de Tecnologias da Informação e Comunicação, amplamente divulgados pela imprensa, envolvem investimentos elevados e demonstram a importância do tema abordado nesta pesquisa.

O cronograma de tarefas e resultados é apresentado na tabela abaixo. As tarefas estão divididas por atividades. Os resultados são representados por Tese de Doutorado (D), Tese de Mestrado (M), Projeto de Fim de Curso (F), Relatórios Técnicos (RT), Artigo Submetido a Congresso Nacional (CN), Artigo Submetido a Congresso Internacional (CI), Artigo submetido à Revista (R), Módulo de Software (S) e Protótipo (P).

Atividades, Tarefas e Resultados	**Semestres**			
	1	**2**	**3**	**4**
Atividade 1	X	X	X	
Desenvolvimento da rede de testes	X	X	X	
Avaliação de métricas e protocolos de roteamento		X	X	X
Modelagem da capacidade de redes em malha	X	X		
Módulo de simulação de redes em malha			X	X
Avaliação de modelos de perda para redes sem fio	X			
Modelo analítico para perdas em redes sem fio		X		
Avaliação de mecanismos de seleção de taxa			X	X
Estudo de mecanismos para redes sem fio cognitivas	X	X		
Resultados	1M,5CN	2CI,1R	1F,3RT, 8CN,3CI	5D,4M, 3CI,4R, 2P,1S
Atividade 2	X	X	X	
Estudo de modelos de mobilidade e aplicações P2P	X	X		
Avaliação de algoritmos de seleção de pares	X	X		
Módulo de simulação do algoritmo proposto			X	X
Desenvolvimento do protótipo			X	X
Resultados		2RT	3CN,2RT	1M,1S, 2CI,1R, 1P
Atividade 3	X	X	X	
Estudo das arquiteturas para DTNs	X	X		
Estudo de técnicas de roteamento para DTNs	X	X		
Desenvolvimento do protótipo			X	X
Resultados		1RT	1CN	1M,1P

Atividade 4	X	X	X	
Estudo de SDIs e sistemas de confiança	X	X		
Módulo de simulação do SDI proposto			X	X
Módulo de simulação do sistema de confiança			X	X
Avaliação de mecanismos de controle de acesso	X			
Avaliação de sistemas de distribuição de chaves		X		
Módulo de simulação - CA e dist. de chaves			X	X
Avaliação dos mecanismos anti-*spam*	X	X	X	
Desenvolvimento do protótipo			X	X
Resultados	1RT	1F, 3CN	3M,1CN, 3CI	1R,1P, 3S

7 Orçamento

Este projeto se enquadra na Faixa A definida no Edital para projetos com orçamento máximo de R$ 200.000,00.

Os roteadores, placas de rede e demais equipamentos sem fio IEEE 802.11, computadores portáteis e PDAs serão utilizados na confecção dos protótipos e testes em redes sem fio. O servidor e o dispositivo de armazenamento (*storage*) serão utilizados para a realização de simulações por eventos discretos que requerem um grande número de estados. Portanto, é necessária uma estação de trabalho de alto desempenho (processamento e memória). Além disso, as simulações normalmente requerem um longo tempo de simulação, gerando uma grande quantidade de resultados (*traces*), o que exige grande quantidade de espaço de armazenamento. Os equipamentos de biometria serão utilizados na atividade de segurança para autenticação biométrica. A impressora será utilizada principalmente na criação de documentos e na elaboração de material didático.

A rubrica de serviços de terceiros será usada no pagamento de frete, garantia e instalação dos equipamentos adquiridos no projeto, de serviços de manutenção de equipamentos existentes nos laboratórios envolvidos, e de inscrições em conferências nacionais e internacionais.

A participação em congressos nacionais e internacionais, dentro dos 5% estabelecidos, também está prevista neste projeto.

Item	Qtd.	Unitário (R$)	Total (R$)
Viagens	1	10.000,00	10.000,00
Serviços	1	20.000,00	20.000,00
Equipamentos			
Sem fio			
Roteador Wireless Linksys WRT54GL ou similar	7	436,80	3.057,60
Roteador Wireless Linksys 802.11n WRT300N ou similar	6	692,00	4.152,00
Adaptador PCMCIA 802.11a/b/g 3COM 3CRPAG175B ou similar	5	369,00	1.845,00
Adaptador USB 802.11n Linksys WUSB300N ou similar	7	619,00	4.333,00
Adaptador PCMCIA 802.11n Linksys WPC300N ou similar	10	589,00	5.890,00
Amplificador802.11b/g 1Watt HA2401MG-1000 ou similar	3	569,00	1.707,00
Caixa hermética com antena indoor planar 2,4GHz 15 dBi	8	242,38	1.939,04
Antena Offset 2.4GHz 31,5dBi Wll-150 Zirok ou similar	2	499,74	999,48
Analisador de espectro Wi-fi 2.4GHz Wi-Spy USB ou similar	3	744,00	2.232,00
Notebook			
DELL XPS M1330 (160GB, 2GB RAM, 2.2 GHz) ou similar	7	8.915,11	62.405,77
Biometria			
Leitor de Impressões digitais Microsoft DG2-00004 ou similar	2	149,00	298,00
Scanner de Íris Panasonic DT120 ou similar	1	1.126,00	1.126,00
Servidores			
Storage Fibre Channel DELL AX150 1TB ou similar	1	8.316,00	8.316,00
DELL PE 6850 (5x146GB, 16GB RAM, 4x3.4GHz) ou similar	1	53.018,00	53.018,00
Impressora			
Laserjet P3005DN ou similar	1	3.060,00	3.060,00
PDAs			
HP HW6945 ou similar	6	2.599,00	15.594,00
TOTAL			199.972,89

Referências

[1] N. C. Fernandes, M. D. D. Moreira, P. B. Velloso, L. H. M. K. Costa e O. C. M. B. Duarte, "Ataques e mecanismos de segurança em redes ad hoc", em *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, cap. 2, p. 49–102, agosto de 2006.

[2] C. T. Oliveira, M. D. D. Moreira, M. G. Rubinstein, L. H. M. K. Costa e O. C. M. B. Duarte, "Redes tolerantes a atrasos e desconexões", em *Minicursos do Simpósio Brasileiro de Redes de Computadores - SBRC'2007*, cap. 5, maio de 2007.

[3] D. M. Taveira, I. M. Moraes, M. G. Rubinstein e O. C. M. B. Duarte, "Técnicas de defesa contra *spam*", em *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, cap. 5, p. 202–250, agosto de 2006.

[4] A. C. P. L. F. de Carvalho, A. Brayner, , A. Loureiro, A. L. Furtado, A. von Staa, C. J. P. de Lucena, C. S. de Souza, C. M. B. Medeiros, C. L. Lucchesi, E. S. e Silva, F. R. Wagner, I. Simon, J. Wainer, J. C. Maldonado, J. P. M. de Oliveira, L. Ribeiro, L. Velho, M. A. Gonçalves, M. C. C. Baranauskas, M. Mattoso, N. Ziviani, P. O. A. Navaux, R. da Silva Torres, V. A. F. Almeida,

W. M. Jr. e Y. Kohayakawa, "Grandes desafios da pesquisa em computação no Brasil – 2006 - 2016", relatório técnico, maio de 2006.

[5] M. E. M. Campista, I. M. Moraes, P. M. Esposito, A. A. Jr., D. de Oliveira, L. H. M. K. Costa e O. C. M. B. Duarte, "The ad hoc return channel: a low-cost solution for Brazilian interactive digital TV", *IEEE Communications Magazine*, vol. 45, no. 1, p. 136–143, janeiro de 2007.

[6] D. S. J. D. Couto, D. Aguayo, J. Bicket e R. Morris, "A high-throughput path metric for multi-hop wireless routing", em *ACM International Conference on Mobile Computing and Networking (MobiCom)*, p. 134–146, setembro de 2003.

[7] R. Draves, J. Padhye e B. Zill, "Comparison of routing metrics for static multi-hop wireless networks", em *ACM SIGCOMM*, p. 133–144, agosto de 2004.

[8] C. E. Koksal e H. Balakrishnan, "Quality-aware routing metrics for time-varying wireless mesh networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 11, p. 1984–1994, novembro de 2006.

[9] F. Cali, M. Conti e E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit", *IEEE/ACM Transactions on Networking*, vol. 8, no. 6, p. 785–799, dezembro de 2000.

[10] T.-Y. Lin e J. C. Hou, "Interplay of spatial reuse and sinr-determined data rates in CSMA/CA-based, multi-hop, multi-rate wireless networks", em *IEEE Conference on Computer Communications (INFOCOM)*, p. 803–811, 2007.

[11] K. F. e K. Varadhan, "The ns Manual. UC Berkeley, LBL, USC/ISI e Xerox PARC, Abril de 2007". http: www.isi.edu/nsnam/ns/ns-documentation.html.

[12] J. Aráuz e P. Krishnamurthy, "Markov modeling of 802.11 channels", em *IEEE Vehicular Technology Conference (VTC)*, 2003.

[13] L. Carvalho, J. Angeja e A. Navarro, "A new packet loss model of the IEEE 802.11g wireless network for multimedia communications", *IEEE Transactions on Consumer Electronics*, 2005.

[14] J. C. Bicket, "Bit-rate selection in wireless networks", Tese de Mestrado, Dept. of Electrical Engineering and Computer Science - Massachusetts Institute of Technology, 2005.

[15] S. Haykin, "Cognitive radio: Brain-empowered wireless communications", em *IEEE Journal on Selected Areas in Communications*, fevereiro de 2005.

[16] S. Mangold, Z. Zhong, K. Challapali e C.-T. Chou, "Spectrum agile radio: Radio resource measurements for opportunist ic spectrum usage", em *IEEE GLOBECOM*, novembro de 2004.

[17] CarTALK Project, "Calling all cars, vehicle-to-vehicle communication", 2001. http://www.cartalk2000.net.