Contribuições na Área de Sistemas
Distribuídos e Redes de Computadores e suas
Aplicações em Sistemas Embarcados Críticos

Kalinka Regina Lucas Jaquie Castelo Branco

Contribuições na Área de Sistemas Distribuídos e Redes de Computadores e suas Aplicações em Sistemas Embarcados Críticos

Kalinka Regina Lucas Jaquie Castelo Branco

Texto sistematizado do trabalho científico da candidata, apresentado ao Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo, como parte dos requisitos para obtenção do Título de Professor Livre Docente, junto ao Departamento de Sistemas de Computação.

São Carlos/SP

Janeiro/2012

Resumo

Este texto foi elaborado para a participação da autora no Concurso Público de Professor Livre Docente junto ao Departamento de Sistemas de Computação do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (SSC/ICMC/USP). No texto, é apresentada uma sistematização das pesquisas e trabalhos realizados pela autora, delineando seu foco de pesquisa em sistemas computacionais distribuídos e redes de computadores e suas aplicações em sistemas embarcados críticos. Após a conclusão do seu doutorado em 2004 no ICMC, a autora iniciou sua vida acadêmica como docente na Fundação de Ensino Eurípides Soares da Rocha de Marília - UNIVEM, onde deu continuidade nas pesquisas que havia realizado em seu doutorado. Em 2008 foi contratada como docente no ICMC/USP, onde vem trabalhando no uso de redes de computadores e sistemas computacionais distribuídos em sistemas embarcados seguros. São descritas inicialmente as contribuições na área de sistemas computacionais distribuídos e redes de computadores. Em seguida, neste documento são apresentadas as principais linhas de pesquisa exploradas pela autora, destacando-se as contribuições em cada uma delas. São também discutidos os trabalhos em andamento e perspectivas futuras de pesquisa. São descritos os fundamentos e os pressupostos das abordagens que têm sido exploradas pela autora, destacando-se as contribuições e os desenvolvimentos realizados nos últimos sete anos de trabalho acadêmico, período posterior à conclusão do seu doutorado.

Abstract

This document was elaborated to fulfill the requirements of the author's application for the title "Livre Docente" of Associate Professor at the Computer Systems Department of the Institute of Mathematical Sciences and Computing, University of São Paulo (SSC/ICMC/USP). The text systematizes the author's research contribution in the field of distributed computing systems and computer networks and their application in critical embedded systems.

After the completion of her PhD in 2004 at ICMC, she began her academic career as a lecturer in Education Foundation Eurípides Soares da Rocha de Marília, where she continued the research conducted in her doctorate. In 2008, the author has been admitted as Assistant Professor at the University at the ICMC/USP and, since 2008 has been working in the use of computer networks and distributed computing systems in safety-critical embedded systems. Contributions are described initially in the area of distributed computing systems and computer networks. Then, this document presents the main research areas explored by the author, highlighting the contributions of each one. Ongoing works are also described, along with a future work discussion.

The document describes the foundations and assumptions of the approaches that have been explored by the author, highlighting the contributions and developments made in the last seven years of academic work, the period following the completion of her doctorate.

Sumário

1	Introdução	1
1.1	Contextualização	3
1.2	Produção Científica	5
1.3	Orientação a Alunos	8
1.4	Organização do Texto Sistematizado	9
2	Sistemas Computacionais Distribuídos e Redes de Computadores	11
2.1	Considerações Iniciais	11
2.2	Sistemas Computacionais Distribuídos - Programação Paralela/- Distribuída e Escalonamento de Processos	12
2.2.1	Computação Paralela e Escalonamento de Processos	13
2.3	Redes de Computadores - Segurança	17
2.3.1	Ferramentas de Simulação e Virtualização de Redes	18
2.3.2	Ataques, Vulnerabilidades e Contramedidas	21
2.4	Considerações Finais	24
3	Sistemas Embarcados Críticos	26
3.1	Considerações Iniciais	26
3.2	Perspectivas de Pesquisa	27
3.3	Veículos Aéreos Não-Tripulados	33
3.3.1	Modelo de Referência para Veículos Aéreos Não Tripulados	40
3.3.2	MOSA - <i>Mission-Oriented Sensor Array</i>	40
3.4	Metodologias para o desenvolvimento de Sistemas Embarcados Críticos	43

3.5	Considerações Finais	46
4	Conclusões	47
4.1	Discussões e Reflexões	47
4.2	Trabalhos em Andamento e Futuros	48
	Agradecimentos	50

Lista de Figuras

1.1	Construção da carreira acadêmica da autora no tempo.	6
1.2	Publicações da autora após a conclusão do doutorado.	8
3.1	Mapa do esforço em pesquisa.	30
3.2	Mapeamento das publicações.	31
3.3	Mapeamento dos alunos sob orientação.	32
3.4	Mapeamento das colaborações nacionais e internacionais.	33
3.5	Mapeamento dos resumos de iniciação científica publicados.	34
3.6	Mapeamento dos alunos de mestrado da Fase I e de iniciação científica das Fases I e II já concluídos.	35
4.1	Mapeamento das publicações.	49

Capítulo 1

Introdução

Sistemas embarcados são sistemas computacionais que de maneira geral fazem parte de um sistema maior provendo, geralmente, monitoramento e controle em tempo real para todo o sistema.

Sistemas embarcados são considerados críticos em segurança quando eventos de falha podem acarretar perdas de vidas humanas ou perdas de ativos de alto valor. Esses sistemas têm se tornado cada vez mais complexos, tanto em nível de *hardware* como de *software* e têm sido cada vez mais utilizados, graças aos avanços da tecnologia. Esses avanços possibilitam sistemas com maior capacidade de processamento, memória e adaptação a diferentes necessidades, podendo inclusive se comunicar com qualquer outro dispositivo, embarcado ou não.

A comunicação sempre foi uma das maiores necessidades do ser humano. As redes de computadores têm por objetivo compartilhar informações, pois se vive em um mundo informatizado. As redes de computadores vêm para disponibilizar informações que estão distantes trazendo benefícios a todos.

A comunicação entre sistemas embarcados reafirma a importância inegável que têm as redes de computadores nos dias atuais. Seja qual for o tipo de sistema computacional considerado, não é possível o uso racional de redes de computadores sem levar em consideração aspectos importantes como: confiabilidade, disponibilidade, proteção contra ataques e manipulação de informações.

A rede representa, na grande maioria das aplicações, um recurso de comunicação. Diferentes aplicações e sistemas podem se beneficiar com o uso de meios seguros para a troca de informações. Segurança é, portanto, um dos problemas fundamentais no desenvolvimento e uso confiável dessa classe de sistemas. Os trabalhos realizados pela autora têm um dos focos nesta subárea considerada de relevância ímpar, os sistemas embarcados críticos seguros¹.

Boa parte das pesquisas relacionadas com segurança em redes de computadores têm como foco aplicações comerciais. Já o estudo da segurança em sistemas embarcados críticos tem despertado recentemente maior interesse da comunidade científica, tanto pelo número crescente de equipamentos que possuem dispositivos embarcados quanto pelos desafios apresentados nesta classe de aplicações. Solucionar questões sobre confiabilidade, robustez, segurança e disponibilidade dos canais de comunicação é imprescindível para garantir o aspecto crítico desses sistemas. Como exemplo da importância atual desses estudos, destaca-se a criação do Centro de Defesa Cibernética (CDCiber) (**CDCiber, 2012**), mostrando que a segurança de sistemas computacionais, de modo geral, é uma área estratégica e de grande relevância para o país.

No contexto até aqui apresentado, pode-se notar que o desenvolvimento de pesquisas na área de conhecimento de Sistemas Computacionais Distribuídos e Redes de Computadores, e suas aplicações práticas em Sistemas Embarcados Críticos, tem caráter intrinsecamente multidisciplinar. A multidisciplinaridade, que neste texto deve ser entendida como o envolvimento de várias subáreas e disciplinas dentro da grande área de computação (e mesmo fora dela), é imprescindível para o desenvolvimento de sistemas embarcados críticos seguros.

Este texto sistematizado descreve a trajetória e a produção científica da autora após a conclusão do seu doutorado. É feita uma divisão em duas fases de pesquisa: Fase I - fase das pesquisas iniciadas logo após a conclusão do doutorado e que apresentam contribuições focadas na área de sistemas distribuídos e redes de computadores, dando continuidade às pesquisas efetuadas no doutorado e; Fase

---

¹Neste texto o termo sistemas embarcados críticos seguros se refere a incorporação de requisitos de segurança tanto no que se refere a comunicação segura quanto a aspectos físicos dos elementos tratados

II - fase das pesquisas iniciadas com a contratação da autora pela Universidade de São Paulo - USP, onde a concentração das pesquisas, motivada com o surgimento do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos - INCT-SEC, passou a ser no desenvolvimento de sistemas embarcados críticos seguros.

1.1 Contextualização

O primeiro contato da autora deste texto com a área de Sistemas Distribuídos e Redes de Computadores ocorreu em 1997, quando a mesma desenvolveu seu trabalho de mestrado em pesquisas relacionadas com o desenvolvimento de Programas Paralelos no Laboratório de Sistemas Distribuídos e Programação Concorrente (LaSDPC) do ICMC-USP.

Em 1999, a autora iniciou seu doutorado também na área de Sistemas Distribuídos, não só avaliando o desenvolvimento de programas paralelos, mas o impacto que os mesmos poderiam ter quando executados em plataformas distribuídas, focando seu trabalho na obtenção de índices de carga e de desempenho em plataformas distribuídas.

Após o término do seu doutorado em 2004, a autora continuou suas pesquisas na área de escalonamento de processos na Fundação Eurípides Soares da Rocha de Marília - UNIVEM, onde passou a atuar como professora, a partir de 2005, tanto no curso de graduação como no Programa de Pós-Graduação em Ciência da Computação (PPG-CC), sendo que neste último atuou ministrando disciplinas e orientando alunos de mestrado.

Além das pesquisas em escalonamento de processos, outra linha de pesquisa, baseada em redes de computadores foi iniciada, dada a necessidade observada de um melhor conhecimento da infraestrutura de rede do ambiente de computação distribuído. Posteriormente, o foco passou a ser dado na parte de segurança, que se mostrou uma área bastante importante e instigante, proporcionando trabalhos motivadores e desafiadores. Esta passou a ser a principal área de investigação da autora. Alunos de mestrado e de iniciação científica passaram a desenvolver trabalhos também relacionados com esta área.

No final de 2007, a UNIVEM, assim como tantas outras instituições particulares de ensino, parou de investir no programa de pós-graduação. Assim, a partir de 2008 a autora continuou seus trabalhos junto à Universidade de Campinas - UNICAMP, atuando em Limeira no antigo CESET (atual Faculdade Tecnológica). Passou a atuar como docente na graduação e participou ativamente na elaboração de uma proposta do programa de pós-graduação multidisciplinar. Esse programa foi aprovado em agosto de 2008, entretanto a autora não mais se encontrava como docente da UNICAMP nesta data, pois em julho de 2008 passou a atuar no Instituto de Ciências Matemáticas e de Computação, ICMC, da Universidade de São Paulo, USP, no *Campus* de São Carlos.

Com a chegada na USP em julho de 2008, foi integrada ao Laboratório de Sistemas Distribuídos e Programação Concorrente (LaSDPC), onde pode compartilhar experiências e fazer uso das instalações físicas já existentes no mesmo. Participou em setembro de 2008 da elaboração do projeto do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos - INCT-SEC, aprovado em dezembro de 2008. A partir deste fato, novos horizontes de pesquisa surgiram permitindo que essas pudessem estar associadas com aplicações práticas de maior relevância nacional. Particularmente importante tem sido a rede de colaboração disponibilizada pelo INCT-SEC, possibilitando atividades mais consistentes e multidisciplinares das pesquisas empreendidas. Cabe ressaltar que a autora participou de forma bastante atuante na proposição e na criação do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos, o INCT-SEC, que foi um dos 122 institutos aprovados na ocasião. Na constituição da diretoria do INCT-SEC, em fevereiro de 2009, a autora foi indicada e tem atuado como Diretora Administrativa/Operacional do Instituto. A atuação como diretora possibilitou uma vasta gama de aprendizados, incluindo questões administrativas e operacionais de um projeto que envolve aproximadamente 300 pessoas entre pesquisadores e alunos de iniciação científica, mestrado e doutorado. Permitiu também crescimento e amadurecimento pessoais bastantes significativos.

Todo o contexto apresentado possibilitou para a autora uma visão mais ampla e integradora, no sentido de integrar equipes e permitir a geração de projetos e trabalhos multidisciplinares. O sonho pessoal de produzir pesquisa aplicada em

prol da sociedade baseada em grandes equipes de pesquisa inter e multidisciplinar começou a se tornar realidade. Isso levou ao desenvolvimento de projetos em cooperação com diversos pesquisadores de diferentes áreas e instituições, além da parceria com empresas. Produtos, tais como a aeronave não tripulada Tiriba e um piloto automático de aeronaves não tripuladas, passaram a ser realidade e utilizados em diversas aplicações práticas.

Ainda em 2009, mais uma vez associada com a criação do INCT-SEC, surgiu a necessidade de um laboratório que pudesse contemplar a multidisciplinaridade decorrente dos projetos. A autora participou assim da criação do Laboratório de Sistemas Embarcados Críticos - LSEC, do qual é coordenadora desde então. Este laboratório surgiu justamente da necessidade de integrar as diferentes pesquisas que estavam sendo realizadas de modo a compor algo maior e de propósito único. Desde então o LSEC conta com 14 professores pesquisadores (de diferentes áreas da computação e da engenharia), que possuem um objetivo comum, o de prover sistemas embarcados críticos inteligentes e seguros para diversas aplicações. Deste modo, a partir de 2009 a maior parte dos trabalhos da autora está relacionada ao desenvolvimento de sistemas embarcados críticos seguros. Em 2011, com o relativo aumento das atividades iniciadas pelo INCT-SEC em robótica, a autora teve a possibilidade de fazer parte da equipe que propôs o Centro de Robótica de São Carlos - CRob-SC, do qual a autora passou, junto com outros docentes, a integrar o Conselho Diretor.

A Figura 1.1 apresenta a linha de tempo da autora no que tange a sua vida acadêmica. O período a partir de 2005 é o que corresponde a fase após a conclusão do doutorado, a Fase I, compreendida entre os anos 2005 e 2008. A partir de julho de 2008 inicia-se a Fase II, anteriormente mencionada.

1.2 Produção Científica

Em relação à produção científica, após a conclusão do doutorado, a autora publicou 47 artigos em conferências, 12 artigos em periódicos, sendo que desses doze, dois foram aceitos para publicação em 2012. Publicou ainda 8 capítulos de livro, sendo que desses oito, um capítulo foi aceito para publicação em 2012. Participou

Figura 1.1: Construção da carreira acadêmica da autora no tempo.

da editoração de três livros, sendo uma a de um livro internacional, no qual atuou em parceria com os professores Francisco José Mônaco e Júlio Cezar Estrella da USP e Valéria Cardellini e Emiliano Casalicchio da Università di Roma "Tor Vergata". A maior parte da produção da autora concentra-se na área de segurança de sistemas computacionais distribuídos e redes de computadores e suas aplicações em sistemas embarcados. A maior parte dos trabalhos apresentados é publicado em conjunto com alunos orientados pela autora. Os artigos e capítulos foram publicados em veículos qualificados ou cujos organizadores constituem pesquisadores reconhecidos na área. Esses trabalhos são apresentados sucintamente nos próximos capítulos deste texto sistematizado. Além deles, foram publicados artigos em outras áreas, conforme descrito a seguir. Todas as citações de artigos publicados pela autora estão destacadas em negrito para facilitar sua identificação.

Os artigos (**Branco et al., 2006e**), (**Branco et al., 2006f**), (**Branco et al., 2006g**), (**Branco et al., 2006a**), (**Branco et al., 2006b**), (**Branco and Ordonez, 2006**) foram

escritos a partir de resultados do trabalho de doutorado, mas submetidos e publicados após a conclusão do mesmo. Com a entrada na UNIVEM, logo após a defesa do doutorado, a autora trabalhou diretamente com temas focados e relacionados ao seu trabalho de doutorado na área de escalonamento de processos, permitindo a aplicação desses conceitos em diferentes áreas (**Branco and Ordonez, 2007**) e (**Branco et al., 2006c**).

O uso de dispositivos móveis foi considerado e abordado inicialmente no trabalho apresentado em (**Mesquita et al., 2007**) em conjunto com profissionais ligados a empresas, o que permitiu a realização de um trabalho não só conceitual mas que apresentou vários resultados práticos, como a utilização e programação de *smartphones*. O estudo de ontologias ligadas a processos de *handover* ao qual esses dispositivos estão sujeitos encontram-se no trabalho (**Vanni et al., 2010**) desenvolvido em parceria com o professor Edson dos Santos Moreira.

O estudo da heterogeneidade de plataformas distribuídas também foi um dos trabalhos desenvolvidos e cujos resultados são apresentados em (**Souza et al., 2011**). Este trabalho foi realizado em parceria com os professores Paulo Sérgio Lopes de Souza, Marcos José Santana, Regina Helena Carlucci Santana e Sarita Mazzini Bruschi.

Os trabalhos descritos em (**Kawabata et al., 2006a**), (**Kawabata et al., 2006b**) descrevem a avaliação de desempenho do protocolo CMB, um protocolo para simulação distribuída, em cooperação com as professoras Sarita Mazzini Bruschi e Célia Leiko Ogawa Kawabata.

Os artigos (**Chiaramonte et al., 2006**), (**Oliveira et al., 2006a**), (**Oliveira et al., 2006b**), (**Bissoli et al., 2007**) e (**Morony et al., 2006**), são resultados de colaborações nos projetos de implementação de segurança em FPGAs, coordenados pelo professor Edward David Moreno Ordonez.

O estudo de segurança em sistemas embarcados, com ênfase em robôs móveis e veículos terrestre autônomos, tem sido realizado em parceria com os professores Denis Fernando Wolf e Fernando Santos Osório (**Osório et al., 2010a**), (**Osório et al., 2010b**), (**Osório et al., 2009**), (**Saito et al., 2009a**), (**Saito et al., 2009b**).

Na Figura 1.2 é possível observar a evolução das publicações da autora após a conclusão do seu doutorado. É possível notar a concentração das publicações

Figura 1.2: Publicações da autora após a conclusão do doutorado.

na área de escalonamento de processos em 2006 e 2007, anos subsequentes à conclusão do seu doutorado. Em 2009, a autora completava seu primeiro ano como docente da USP e começava a orientar os primeiros alunos de mestrado no programa de pós-graduação, o que ilustra a concentração das pesquisas já focadas em segurança e suas aplicações em sistemas embarcados críticos. Esse panorama leva à melhoria dos resultados em termos de publicações já em 2010. As publicações relacionadas a aplicação de redes de computadores a sistemas embarcados críticos seguros se intensificaram a partir de 2010, representando 77% da produção científica da autora em 2011. Cabe destacar que os outros 33% estão relacionados a segurança em redes de computadores.

A autora também desenvolve trabalhos de extensão e de cunho social. A realização desses trabalhos junto ao projeto EcoEdu Ambiental rendeu a publicação do artigo (**Ribeiro and Branco, 2008**) em parceria com a professora Lubienska Ribeiro, coordenadora do projeto EcoEdu Ambiental.

1.3 Orientação a Alunos

A formação de recursos humanos é tarefa primordial dentro da universidade. Incluem-se aqui alunos de graduação e de pós-graduação, que são de vital importância para o sucesso dos projetos de pesquisa. Desde sua contratação como

docente na UNIVEM, a autora procurou trabalhar com alunos de graduação e pós-graduação, em projetos de iniciação científica, trabalho de final de curso e projetos de mestrado. Isso pode ser observado pelas bolsas de iniciação científica solicitadas e aprovadas.

Atualmente a autora orienta 4 alunos de iniciação científica, sendo 1 bolsista FAPESP. A maior parte deles trabalha em projetos relacionados a segurança de sistemas embarcados críticos. A definição de serviços seguros, de algoritmos criptográficos para sistemas embarcados e boa parte do trabalho técnico do desenvolvimento de *drivers* e interfaces para funcionamento desses sistemas é realizado por eles.

Desde que iniciou a carreira docente, em 2005 na UNIVEM, a autora foi credenciada Programa de Pós-Graduação em Ciência da Computação da Fundação Eurípides Soares da Rocha de Marília. Em 2009, passou a ser credenciada junto ao Programa de Pós-graduação em Ciência da Computação e Matemática Computacional do ICMC-USP. Desde então a autora já concluiu a orientação de 7 alunos de mestrado e orienta atualmente 4 alunos de mestrado e dois alunos de doutorado. Em março de 2012 deve ser concluída mais uma orientação de mestrado.

Todos os alunos formados possuem publicações, no mínimo em veículos nacionais, associadas aos trabalhos realizados. Isso permite formar recursos humanos mais qualificados.

1.4 Organização do Texto Sistematizado

Neste texto sistematizado é apresentada uma descrição das principais contribuições do trabalho realizado pela autora na área de Redes de Computadores e Sistemas Distribuídos e suas aplicações em Sistemas Embarcados Críticos. Os trabalhos desenvolvidos pela autora ou sob sua orientação são apresentados de forma resumida. São apresentados apenas os conceitos principais e os aspectos que distinguem os trabalhos e caracterizam sua contribuição. Os resultados obtidos, as metodologias propostas, e outras informações específicas estão detalhadas nas versões completas dos artigos publicados.

O Capítulo 2 descreve os resultados das pesquisas realizadas na área de Sistemas Computacionais Distribuídos e Redes de Computadores. O Capítulo 3 apresenta os resultados da aplicação das pesquisas realizadas em Redes de Computadores e Sistemas Distribuídos em Sistemas Embarcados Críticos, bem como os trabalhos em andamento. Finalmente, no Capítulo 4, são apresentadas as conclusões e discussões das perspectivas e trabalhos futuros da autora.

Capítulo 2

Sistemas Computacionais Distribuídos e Redes de Computadores

Este capítulo tem como objetivo apresentar os trabalhos desenvolvidos pela autora ou sob sua orientação durante a Fase I de sua carreira. Os trabalhos aqui desenvolvidos focam basicamente estudos relacionados a sistemas computacionais distribuídos e redes de computadores.

2.1 Considerações Iniciais

O surgimento dos sistemas distribuídos deu-se basicamente pela necessidade de compartilhar recursos, normalmente de alto custo e fisicamente separados. Várias mudanças ocorreram nesta área da computação nas últimas décadas, levando a uma alta conectividade dos recursos computacionais. A motivação para interligar os diferentes recursos dos sistemas computacionais não é única, variando desde o simples compartilhamento de discos e impressoras até a disponibilização de uma grande quantidade de processadores, com o consequente aumento na potência computacional disponível, até uma melhor tolerância a falhas do sistema e maior mobilidade dos usuários.

Os sistemas distribuídos permitem a solução de vários problemas de modo mais eficiente, a um custo significativamente mais baixo, motivando diversas pesquisas para explorar estes recursos. Uma delas, a computação paralela, faz uso da grande capacidade de processamento disponível nos sistemas distribuídos. O escalonamento de processos em plataformas distribuídas foi um dos problemas que necessitavam de solução junto com o estudo e o provimento de segurança para as redes de computadores. Neste sentido, os estudos desenvolvidos na Fase I focaram o desenvolvimento de meios de se prover escalonamento de processos em ambientes distribuídos de forma mais eficiente, promovendo melhorias nesse escalonamento. Focaram também no aprendizado e no desenvolvimento de meios de prover maior segurança às redes de computadores.

2.2 Sistemas Computacionais Distribuídos - Programação Paralela/Distribuída e Escalonamento de Processos

Muitas são as definições encontradas para sistemas distribuídos na literatura, como a de Tanenbaum, que define sistemas distribuídos como um conjunto de computadores independentes que aparecem para os usuários do sistema como um único computador (Tanenbaum, 1995); e a de Colours, que define sistemas distribuídos como sistemas onde os componentes de *hardware* e *software* localizados em computadores em uma rede se comunicam e coordenam suas ações por meio de passagem de mensagens (Coulouris et al., 2003).

Ao interpretar essas definições, conclui-se que os sistemas distribuídos permitem agrupar a potência computacional de diversos *hosts* interligados por uma rede de comunicação, para processar colaborativamente determinada tarefa de forma coerente e transparente, ou seja, como se apenas um único computador centralizado estivesse executando a tarefa. Essas definições implicam no *hardware*, formado por máquinas autônomas interligadas, e no *software*, fornecendo a abstração de uma única máquina. Esses sistemas proporcionam algumas vantagens sobre os sistemas convencionais, como menor custo, aumento de veloci-

dade e crescimento incremental, entre outras. Por outro lado, apresentam também muitas desvantagens, dentre as quais se destaca a dificuldade em garantir a segurança.

A computação paralela distribuída surgiu com a disponibilização, a baixo custo, de microcomputadores cada vez mais potentes e de tecnologias de rede de computadores de alto desempenho. Um dos problemas inerentes ao uso da computação paralela distribuída é o fato de cada máquina possuir a sua própria memória local (sistema fracamente acoplado). Com isso, a memória presente no sistema não pode ser acessada diretamente por todo os processadores, o que acarreta um custo mais elevado de comunicação e sincronização dos processos. O mecanismo utilizado para comunicação e sincronização é o de passagem de mensagens.

Sabendo-se que as pesquisas relacionadas a sistemas computacionais distribuídos têm convergido para a busca de um melhor desempenho e, para que esse objetivo seja alcançado, não basta apenas existirem sistemas com grande número de processadores ou de estações de trabalho, fica clara a necessidade de garantir que todos os *hosts* presentes no sistema sejam bem aproveitados (**Branco, 2004**). A aplicação é dividida em processos (tarefas ou *tasks*), e estes, por sua vez, são distribuídos entre os *hosts* que compõem a máquina paralela virtual. Balanceamento de carga é a palavra chave para garantir o bom aproveitamento dos recursos computacionais disponíveis.

2.2.1 Computação Paralela e Escalonamento de Processos

Quando mais de um processo precisa ser executado em um uniprocessador, o sistema operacional precisa decidir qual deles deve ser executado primeiro. Denomina-se escalonamento de processos à escolha de qual processo deve executar naquele determinado instante (Tanenbaum, 2001). Em ambientes paralelos distribuídos, o escalonamento consiste em atribuir processos aos *hosts* e determinar em que ordem esses processos serão executados (El-Rewini et al., 1995). O escalonador é de vital importância para sistemas paralelos distribuídos e é considerado um problema nessa área (Shivaratri et al., 1992). A literatura da área

mostra que os algoritmos de escalonamento se propõem a uma grande variedade de objetivos: compartilhamento de carga, aumento da utilização do processador, redução do tempo de resposta, redução do tempo de execução, balanceamento de carga, entre outros (Shirazi et al., 1995; Mullender, 1993; Feitelson et al., 1996; Feitelson and Rudolph, 1995, 1996, 1998; Xu and Lau, 1997; Cao, 2004; Zhang et al., 2010).

A utilização dos algoritmos de escalonamento, visando ao balanceamento de cargas, pode prover um aumento considerável no desempenho do sistema, uma vez que a otimização e a eficácia do sistema estão diretamente relacionadas com a melhor utilização da capacidade de processamento existente. A escolha correta da política de balanceamento de cargas implica diretamente o desempenho final do sistema e, indiscutivelmente, o balanceamento de cargas é indispensável em um sistema computacional distribuído.

Diversas foram as dificuldades encontradas para o desenvolvimento dos trabalhos relacionados com o escalonamento de processos, dentre elas o grande número de algoritmos, de políticas e de mecanismos de escalonamento (Shirazi et al., 1995; Feitelson et al., 1996; Feitelson and Rudolph, 1995, 1996, 1998; Xu and Lau, 1997; Cao, 2004; Zhang et al., 2010). Com base nas dificuldades observadas e vivenciadas, o trabalho de mestrado do aluno Luiz Carlos Querino Filho (**Querino Filho, 2010**) veio ao encontro da necessidade de se agrupar em um único lugar os diferentes algoritmos e conceitos de escalonamento de processos pulverizados na literatura. A proposta do trabalho foi a geração de um *Framework* para o desenvolvimento de algoritmos de escalonamento de processos. O que se pode observar é que, ao longo dos anos, vários estudos foram conduzidos na busca de novas formas de escalonamento de processos em sistemas paralelos. Nesses trabalhos, algoritmos foram propostos para a melhoria de desempenho na divisão de tarefas entre os vários elementos processadores.

Fazendo uso da taxonomia proposta por (Casavant and Kuhl, 1988), que demonstra relações entre as diversas categorias de algoritmos de escalonamento, e fazendo uso de conceitos de engenharia de *software*, foi possível a definição dos elementos existentes nos algoritmos pertencentes às várias categorias, seus aspectos em comum e as dependências entre eles, dando origem ao FRAPES (FRA-

network of Process hEterogeneous Scheduling) (**Querino Filho et al., 2008**). Por meio de um processo de análise de domínio, foi possível detectar as variações existentes entre os algoritmos de escalonamento e suas principais características, para o detalhamento da estrutura do *Framework*. O FRAPES possibilita a reutilização dos diversos algoritmos de escalonamento existentes por meio de sua categorização dentro da taxonomia de (Casavant and Kuhl, 1988). O processo de análise de domínio realizado possibilitou a caracterização dos algoritmos disponíveis e de suas similaridades gerando um *Framework* robusto (**Querino Filho et al., 2008**).

Um dos elementos que permite a realização de um bom balanceamento de carga, utilizado pelos algoritmos de escalonamento de processos, é o índice de carga que pode estar associado à plataforma ou a cada recurso específico da plataforma. A obtenção desse índice, e mais especificamente do índice de desempenho (**Branco, 2004**), permite que o escalonamento, bem como o balanceamento de carga, possa ser feito de maneira mais eficiente e eficaz.

Com base em (Ferrari and Zhou, 1987), (**Branco et al., 2006d**) e (**Branco and Ordonez, 2006**) observa-se que manter as informações das cargas de trabalho (refletidas nos índices de carga e de desempenho) sempre atualizadas para o escalonador, geralmente, faz com que os *hosts* permaneçam com uma carga coerente mantendo sua potência computacional, sem que o tráfego gerado na rede influencie significativamente no desempenho do sistema como um todo.

Com intuito de validar esses índices de desempenho e de utilizá-los em ambientes reais, dois trabalhos de iniciação científica foram realizados com o objetivo de verificar qual ambiente de passagem de mensagens provia melhores resultados na utilização da computação paralela distribuída em aplicações reais. Os ambientes de passagem de mensagens utilizados foram o JPVM e o MPIJAVA. Foram utilizadas imagens obtidas de tomografias de mamas e foram paralelizados algoritmos de processamento de imagens. Os resultados dos trabalhos de Iniciação Científica dos alunos Priscila Maeda Tiemi Sato e Ricardo José Sabatine foram publicados em (**Saito et al., 2007d**), (**Saito et al., 2007b**), (**Saito et al., 2007c**), (**Sabatine et al., 2007**), (**Saito et al., 2007a**), (**Saito et al., 2007e**), (**Saito et al., 2007d**), (**Saito et al., 2007f**) e (**Saito and Branco, 2009**). Posteriormente, foram feitas a unificação e a comparação dos resultados obtidos por ambos os trabalhos. Os

resultados foram publicados em **(Saito et al., 2008)**. Além dos resultados significativamente melhores quando comparados com os resultados apresentados pela versão sequencial, pôde-se observar que o uso do MPIJava permite um ganho maior de desempenho na execução das aplicações quando comparado ao uso do JPVM.

Ainda que sejam trabalhos relativamente simples, os trabalhos de iniciação científica desenvolvidos serviram de base para identificar a necessidade de se avaliar a troca de informações feita por meio de passagem de mensagens quando comparada a outros meios, por exemplo, via agentes móveis. Nesse sentido, os desafios de se melhorar ainda mais os resultados com o uso da computação paralela distribuída persistiam.

O trabalho da aluna de mestrado Giulianna Marega Marques **(Marque, 2008)** buscou avaliar o impacto da passagem de mensagens quando comparada ao uso de outras formas de comunicação, como por exemplo agentes móveis **(Marques and Branco, 2007)**. O trabalho fez uso de agentes móveis como alternativa para a coleta dos índices de carga e de desempenho em ambientes paralelos distribuídos, objetivando um escalonamento balanceado e confiável, aliado a um bom desempenho (no que se refere ao tempo de execução de aplicações) **(Marques et al., 2007)**. Foi desenvolvido nesse trabalho o PRM (*Performance Resource Monitor*).

O PRM coleta a carga e calcula o índice de carga e de desempenho dos recursos envolvidos e posteriormente interage com o PRS (*Performance Resource Scheduling*), que constitui uma estratégia de escalonamento de processos baseada no uso de agentes móveis. Foi concebido o PAgent (*Performance Agent* - agente móvel responsável pela coleta e disseminação das informações de carga dos recursos). A partir de experimentos realizados foram obtidos resultados que demonstraram a viabilidade no uso de agentes móveis para a troca de informações e coleta dos índices anteriormente citados. Os resultados do uso de agentes móveis no escalonamento de processos foram publicados em **(Marques et al., 2008a)**. Posteriormente, a comparação do uso de agentes móveis e a troca de informações por meio de passagem de mensagens foram publicados em **(Marques et al., 2008b)**.

O trabalho de Marques motivou a investigação do balanceamento de carga em nível de *Kernel*, buscando-se averiguar o impacto que os elementos e técnicas uti-

lizadas em sistemas distribuídos pudessem ter quando utilizados em elementos com menor capacidade de processamento. Com esse objetivo, o trabalho de mestrado do aluno Ivair Lima (Lima, 2008), (Lima et al., 2009a) criou uma extensão de um *Kernel* para prover a distribuição de *bytecodes* em ambientes distribuídos, permitindo um escalonamento de processos com o objetivo de melhorar o balanceamento de cargas. A heterogeneidade da plataforma distribuída, tendo como um dos quesitos dessa heterogeneidade o sistema operacional, permitiu verificar a viabilidade em se prover um escalonamento em nível de *Kernel*, demonstrando a viabilidade do uso dessa estratégia em ambientes com menor capacidade de processamento. Esse trabalho teve como resultado a proposição da AW-*Kernel*, um protótipo para a simulação de facilidades de distribuição de *bytecodes* em nível de *Kernel* (Lima et al., 2009b). A AW-*Kernel* é uma compilação do *Kernel* do sistema operacional *Debian GNU/Linux* instrumentado, que contém uma extensão das chamadas ao sistema que fornecem transparência na transferência de arquivos remotos, por meio do redirecionamento de chamadas locais utilizando *sockets* para o acesso remoto. Foram realizados testes com a AW-*Kernel* tanto em ambientes homogêneos como heterogêneos. Os resultados demonstraram que as transferências feitas com a AW-*Kernel* apresentam tempos estatisticamente melhores que os apresentados por protocolos específicos para transferências de arquivos como o NFS e o FTP, por exemplo.

2.3 Redes de Computadores - Segurança

A comunicação sempre foi uma necessidade da sociedade e uma das maiores necessidades do ser humano, desde o início de sua existência, tendo como um efeito importante o de aproximar comunidades. A troca de informações entre pessoas e computadores geograficamente dispersos motivou o aparecimento das redes de computadores. Uma rede de computadores pode ser definida como um conjunto de computadores autônomos interconectados por meio de um sistema de comunicação (cabo, fibra óptica) permitindo o compartilhamento de recursos computacionais e trocando informações via regras contidas em protocolos (Ta-

nenbaum, 2003). A definição de redes de computadores é usada para sistemas de todos os tamanhos e tipos, desde a Internet até uma rede veicular.

Atualmente, muitas organizações conectadas à Internet tiveram um considerável aumento no orçamento para tratar de forma mais eficaz e eficiente a segurança da sua rede corporativa. Para se proteger de atividades maliciosas, as organizações necessitam monitorar as possíveis falhas de segurança.

2.3.1 Ferramentas de Simulação e Virtualização de Redes

Sabe-se que um dos segmentos de mercado que mais cresceu nos últimos anos é o dos computadores móveis, como os *notebooks* e os *palmtops*. Esse crescimento da computação móvel e a necessidade de transmissão de dados interligando redes, onde não é possível a utilização de meios físicos de transmissão, fomentou o desenvolvimento da tecnologia de redes sem fio, que tem evoluído constantemente. As redes locais sem fio (*Wireless Lan*) já são uma realidade em vários ambientes de redes, principalmente nos que requerem a mobilidade dos usuários. Essas redes sem fio têm proporcionado uma melhora no acesso às informações, em rapidez e mobilidade. Basicamente existem dois tipos de redes móveis sem fio: a infra-estruturada e as redes *ad hoc*. As redes com a topologia *ad hoc* constituem dispositivos capazes de trocar informações diretamente entre si, não precisando de um Ponto de Acesso (PA) ligado em uma rede fixa como na topologia infra-estruturada.

O problema de segurança nas redes *wireless* é agravado pelo fato dos dados trafegarem em ondas de rádio ao invés de cabos, o que facilita o acesso às informações transmitidas. Com o objetivo de solucionar este problema, diversos protocolos de segurança surgiram, sendo um deles o WEP (*Wired Equivalent Privacy*).

O estudo de segurança fazendo uso do protocolo WEP, trabalho de iniciação científica do aluno Adriano dos Santos Lucas (Lucas et al., 2006), veio ao encontro da necessidade de se prover segurança para redes *ad hoc*. O trabalho teve como objetivo, além de permitir um estudo sobre algoritmos criptográficos, estudar redes sem fio por meio da ferramenta de simulação *Network Simulator* -

NS2 (VINT, 2012), e propor modificações no protocolo WEP para torná-lo mais seguro. Esse trabalho teve como subproduto a incorporação do protocolo WEP na ferramenta NS2 para simulação posterior. Esse estudo, apesar de pontual e apresentar pequenas contribuições, permitiu constatar a fragilidade, no aspecto segurança, apresentada, de modo geral, pelos protocolos de rede sem fio.

A fragilidade no aspecto de segurança não está presente somente nas redes sem fio, ela também está presente nas redes cabeadas. Fragilidades e vulnerabilidades inerentes à própria estrutura dos protocolos de redes, que muitas vezes são desenvolvidos sem nenhuma preocupação com segurança, normalmente resultam em incidentes de segurança. O trabalho de iniciação científica realizado pela aluna Mariana Massimino Feres (Feres et al., 2006a), (Feres et al., 2006b) foi proposto para identificar problemas nesses protocolos. Foi estudado o protocolo TCP em duas variações, o TCP Reno e *HighSpeed* TCP (HSTCP).

O controle de congestionamento é uma das tarefas realizadas pelos protocolos da camada de transporte, entre eles o TCP. No caso citado, o controle de congestionamento não é aplicável em redes de alta velocidade, uma vez que este limita a janela de congestionamento em valores abaixo daqueles alcançáveis por esse tipo de interligação (Rezende et al., 2005). Para suprir essa necessidade, vários protocolos de transporte direcionados para redes de alta velocidade estão surgindo, entre eles, o *HighSpeed* TCP (HSTCP), uma versão modificada do TCP proposta por Sally Floyd (Rezende et al., 2005).

O trabalho desenvolvido por Feres permitiu também avaliar, de acordo com os experimentos realizados e os resultados obtidos, que o controle de congestionamento *HighSpeed* apresenta melhor desempenho que o do TCP Reno. Essa diferença é observada principalmente na vazão obtida, com taxas mais elevadas no caso do controle *HighSpeed*. Isso ocorre porque a resposta do *HighSpeed* é mantida igual ao do TCP até uma determinada taxa de perda de segmentos, fazendo com que a janela possua um valor maior que no TCP. Esse estudo permitiu avaliar também a eficiência e a usabilidade da ferramenta *Network Simulator* reforçando a razão do NS ser a ferramenta mais utilizada no meio acadêmico (Coutinho, 2003). Esses trabalhos, apesar de apresentarem resultados pontuais, foram de grande importância para o estabelecimento das bases para diversos trabalhos futuros e

a longo prazo. Um dos trabalhos vislumbrados foi o da utilização da ferramenta NetKit (Rimondini, 2012) para fins educacionais.

O ensino e aprendizagem de redes de computadores não é uma tarefa simples. Assim como diversas outras disciplinas da área de computação, é necessário um conjunto de teoria e prática para reforçar o aprendizado (Rimondini, 2012). Entretanto, diferentemente de uma disciplina de programação onde o aluno pode usar um *software* livre em seu computador pessoal para executar um determinado algoritmo, criar um ambiente de redes exige investimento em equipamentos, o que pode ser oneroso para a instituição de ensino e certamente muito mais difícil para o estudante. Se o ambiente for acadêmico, ele é normalmente compartilhado com outras disciplinas e modificações na configuração promovidas em uma disciplina podem torná-lo indisponível para a realização de outras atividades.

Para a realização de atividades práticas de redes, em um laboratório físico convencional, é necessário um conjunto de computadores adequados ao tamanho da turma. Além disso, estes deverão estar conectados a um conjunto de roteadores de boa qualidade, para que possam ser estudados, por exemplo, os protocolos de roteamento dinâmicos. Além dos roteadores, *switches*, *bridges* e *hubs* devem estar presentes. As senhas de administração destes dispositivos gerenciáveis, bem como dos computadores, devem ser disponibilizadas aos alunos para que estes possam alterar livremente a configuração e fazer os experimentos solicitados.

Foi com intuito de possibilitar que os alunos pudessem ter um melhor aprendizado de redes de computadores e, por conseguinte, de segurança em redes, que foi desenvolvido o trabalho de iniciação científica do aluno Paulo Henrique Gurgel (**Gurgel and Branco, 2010**) que teve como objetivo o desenvolvimento de diversas práticas de laboratório de ensino de redes utilizando a ferramenta NetKit. Foram confeccionados ao todo aproximadamente 20 roteiros de aulas práticas (<http://www.paulogurgel.com.br/netkit.php>) que vão desde atividades mais simples ensinando o uso de *hubs* e *switches* até atividades mais elaboradas que permitem ao aluno aprender de forma prática os conceitos de gerenciamento de redes utilizando o protocolo SNMP (*Simple Network Management Protocol*) e realizar ataques a redes virtuais fazendo uso da ferramenta Trin00 (<http://packetstormsecurity.org>).

Essas práticas de laboratório, associadas aos tutoriais que as acompanham, têm sido de extrema valia para os cursos de redes de computadores e outros cursos relacionados: Engenharia de Segurança, Administração e Gerenciamento de Redes (**Gurgel et al., 2012**). O estudo de protocolos como o IPV6 também tem sido alvo de estudos. A geração de práticas de laboratório por meio da incorporação de *drivers* que permitem a emulação de redes sem fio no NetKit é o foco do projeto de mestrado do aluno Paulo Henrique Gurgel, dando sequência aos estudos iniciados nos trabalhos de iniciação científica e de conclusão de curso desenvolvidos pelo mesmo.

2.3.2 Ataques, Vulnerabilidades e Contramedidas

A internet, proporcionando conectividade em tempo real e abrangência mundial, trouxe um crescimento sem precedentes no volume de informações disponíveis, dificultando seu gerenciamento. Por outro lado, sua grande vulnerabilidade, aliada à existência de novos atores mal intencionados no cenário tanto nacional quanto internacional, fez crescer a preocupação com a proteção da informação que por ela trafega, dando origem à Segurança da Informação.

Com o incremento da internet comercial em meados da década de 1990, a questão da manipulação de informações e da sua segurança ganha maior ênfase, pois a grande rede e seus protocolos, especialmente a família TCP/IP, foram construídos sem muita preocupação com a confidencialidade, a integridade, a disponibilidade e a autenticidade. As vulnerabilidades e as possibilidades de ataques estão sempre presentes. Segurança da informação e comunicação implicam em ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Um ataque é uma tentativa de acesso não autorizado a um sistema ou entidade, ou seja, é o que acontece quando uma ameaça tenta levar vantagem sobre as vulnerabilidades de um determinado sistema. Um ataque (ou intrusão) pode ser formalmente definido, segundo (Heady, 1990) como: "qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibili-

dade dos dados e/ou do sistema". Pode-se ainda definir um ataque, de forma mais abrangente, como qualquer violação à política de segurança de um sistema.

Os ataques podem ser divididos em duas categorias: ataques ativos e ataques passivos (Kurose and Ross., 2009). Ataques ativos correspondem às ameaças que alteram o sistema na tentativa de exploração de alguma vulnerabilidade do mesmo, enquanto que os ataques passivos consistem em ameaças que simplesmente observam as informações que trafegam no sistema. Neste último caso, não são inseridas informações que exploram as vulnerabilidades desse sistema.

Segundo (Kurose and Ross., 2009), os principais tipos de ataques à rede de computadores são: vírus, *worms*, *port scanning* - varredura de portas, DoS (*Denial of Service*) - negação de serviço, DDoS (*Distributed Denial of Service*) - negação de serviço distribuída. Diversas são as ferramentas utilizadas na tentativa de conter os ataques. Entre elas merece destaque os sistemas de detecção de intrusão. Um desses sistemas, foi estudado no trabalho de iniciação científica do aluno Mário Cleber Bidóia, visando utilizar máquinas de estado para conceber cenários de ataques e auxiliar na detecção de ataques (**Bidóia and Branco, 2009**). Entretanto, o uso de máquinas de estado para a confecção de cenários de ataque não é algo de fácil entendimento, tornando a escrita desses cenários um trabalho árduo.

Com objetivo de auxiliar nas tentativas de permitir um melhor tratamento das questões de segurança e de auxiliar no provimento de facilidades na escrita de cenários de ataques (mapeamento de situações de ataques) foi desenvolvido o trabalho de mestrado do aluno Emerson Marconato (**Marconato, 2011**). Foi proposta a utilização de Programação Orientada a Aspectos e UMLintr (Raihan and Zulkernine, 2005; Hussein and Zulkernine, 2006) para a especificação desses cenários de modo a permitir a geração automática de assinaturas, provendo desta forma meios mais fáceis de proteção contra um ataque (**Marconato et al., 2007**).

Com uma análise cuidadosa é possível entender de forma clara a atuação e o comportamento dos diversos elementos envolvidos desde o início até o final de um ataque. Um dos problemas encontrados na área de redes, mais especificamente na área de segurança, é a falta de documentação e do uso de ferramentas que auxiliem tanto na documentação quanto na detecção de problemas e no entendimento desses problemas para que uma solução adequada possa ser

encontrada. Uma boa documentação pode contribuir de forma significativa na análise de medidas de prevenção e dos mecanismos de detecção de um ataque. A utilização da UML permite incorporar grandes benefícios, pois de acordo com Jurjens (2005), a UML é uma linguagem que permite a especificação de padrões de modelagem conhecidos por um grande número de desenvolvedores.

Com o propósito de prover melhores medidas de prevenção a ataques foi desenvolvido o trabalho de mestrado do aluno Paulo Rogério de Mello Cardoso (**Cardoso, 2011**). O objetivo do trabalho envolveu tanto a documentação quanto a especificação de um cenário de ataque de Negação de Serviço Distribuído, almejando facilidades e inovações na detecção deste tipo de ataque. Para isso foi utilizada mais uma vez a UMLintr. Esse trabalho permitiu verificar a necessidade de extensão da UMLintr para permitir a especificação de um ataque mais complexo como é o ataque DDoS. A partir dos resultados obtidos, pode-se concluir que um ambiente de rede que tem o objetivo de minimizar os riscos de um ataque de negação de serviço e, principalmente de um ataque de negação de serviço distribuído, deve estar preparado e ter o conhecimento das formas de atuação destes ataques.

No mundo real, a autenticidade de documentos legais, financeiros e outros é definida por meio da presença de uma assinatura autorizada. Semelhante ao que ocorre com as assinaturas por escrito, a assinatura digital necessariamente deve ser verificável, não falsificável e incontestável (Kurose and Ross., 2009). Isso implica que deve ser possível provar que um documento assinado por uma pessoa foi realmente assinado por ela (verificável) e que apenas aquela pessoa poderia ter assinado o documento (não falsificável), portanto a mesma não pode posteriormente repudiar o documento e negar que o tenha assinado (incontestável).

O fato de se identificar como os ataques acontecem e até mesmo de fazer uso de ferramentas para minimizar a efetividade de um ataque não impedem em 100% das vezes que o mesmo seja bem sucedido. Dessa forma, outros meios e ferramentas são utilizados para prover segurança para informações e sistemas, impondo diferentes barreiras aos atacantes. Dentre essas ferramentas encontram-se a criptografia e as assinaturas digitais.

A assinatura digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos. É um conjunto de operações criptográficas aplicadas a um determinado arquivo, tendo como resultado o que se convencionou chamar de assinatura digital. Essa assinatura permite comprovar: que a mensagem ou arquivo não foi alterado; que foi assinado pela entidade ou pessoa que possui a chave criptográfica utilizada na assinatura.

Ao se considerar os dispositivos móveis, os mesmos não possuem um protocolo eficiente e usual para atribuir confiabilidade às transações, nem mesmo para garantir a integridade e a confiabilidade dos dados, assim como pagamentos *on-line* e transferências de informações sigilosas. Além disso, constituem dispositivos embarcados e por esse motivo apresentam restrições de recursos. Essas restrições e a inerente necessidade de segurança tornam-se um problema. Para solucionar esse problema os alunos Vagner Schoaba (**Schoaba, 2008**) e Felipe Sikansi (**Sikansi and Branco, 2010**), em seus mestrado e iniciação científica respectivamente, propuseram a ADDIMO, um mecanismo de assinatura digital para dispositivos móveis capaz de autenticar e assinar informações trocadas pelos dispositivos (**Schoaba et al., 2010**). Foram utilizados os algoritmos RSA e SHA1 e vários testes foram realizados com o intuito de validar e atestar a eficiência do mecanismo proposto. Um sistema de pagamento seguro foi elaborado e executado fazendo uso de dispositivos móveis como elementos de comunicação e atuantes do processo de registro de compra e pagamento (**Schoaba et al., 2011**), (**Sikansi et al., 2011**).

2.4 Considerações Finais

Sistemas computacionais distribuídos é uma área bastante abrangente que tem tido especial importância, principalmente com o advento da Internet. Nesse sentido, os esforços para melhorar os meios pelos quais as informações são distribuídas se tornam importantes. Os resultados obtidos com a proposição de índices de carga e desempenho e seu uso por meio de agentes móveis, além da possibilidade de se utilizar mecanismos, algoritmos e políticas mais adequadas de escalo-

namento de processos mostraram-se bastante satisfatórios, provendo melhorias nos sistemas.

Obviamente que as redes de computadores, vistas como infraestrutura que compõe a via de comunicação entre os elementos computacionais dispersos, tornam-se elementos passíveis de investigação. De maneira análoga torna-se quase impossível falar sobre redes de computadores sem falar sobre segurança e sem realizar esforços no sentido de prover meios mais seguros para o tráfego das informações.

Segurança é uma área que tem apresentado um interesse crescente de pesquisa, tanto no meio acadêmico quanto no meio comercial, justamente pelo fato de que cada dia mais e mais pessoas tornam-se adeptas do uso da Internet e possuem acesso às mais diversas informações. Nesse sentido, também foram realizadas pesquisas com o intuito de mapear os cenários de ataques, para prevenir e minimizar os riscos associados, bem como para a geração de assinaturas de ataques e para o uso de assinaturas digitais e criptografia, como técnicas para prevenir e dificultar que ataques sejam bem sucedidos. Essa pesquisas apresentaram resultados satisfatórios e bastante significativos.

Todas as pesquisas desenvolvidas durante a Fase I do trabalho da autora tinham como objetivo solucionar problemas pontuais relacionados a domínios específicos. Sistemas embarcados críticos, por outro lado, constituem sistemas multidisciplinares, envolvendo novos desafios e novas áreas de pesquisa. A aplicação das pesquisas apresentadas neste capítulo serviu de motivação para a concepção da pesquisa em sistemas embarcados críticos. No próximo capítulo são mapeadas as pesquisas desenvolvidas em redes de computadores e sistemas distribuídos no cenário dessa classe de sistemas.

Capítulo 3

Sistemas Embarcados Críticos

Este capítulo tem como objetivo apresentar a trajetória atual de pesquisa da autora, considerada a Fase II da sua carreira como pesquisadora, fase esta que se iniciou após sua admissão como docente na USP e focada no desenvolvimento de sistemas embarcados críticos seguros.

3.1 Considerações Iniciais

Como já mencionado, para o desenvolvimento de pesquisa aplicada, como é o caso da que será apresentada neste capítulo, faz-se normalmente necessário um envolvimento multidisciplinar. Este é o caso dos sistemas embarcados críticos e suas aplicações, normalmente representadas por sistemas multidisciplinares complexos.

A desvantagem em se trabalhar com um sistema complexo² é o fato de que a multidisciplinaridade torna a atividade de pesquisa algo mais difícil, contrariamente com o que se tem com uma pesquisa focada em uma área específica. Isso ocorre uma vez que demanda conhecimentos diversos que se encontram espalhados em várias áreas do conhecimento. Para agrupar todo o conhecimento

---

² Um sistema é dito ser um sistema complexo quando suas propriedades não são uma consequência natural de seus elementos constituintes vistos isoladamente.

necessário, um esforço extra de composição de equipe de colaboração torna-se imprescindível. Outro aspecto importante é o da realização física dos sistemas em estudo. Muitas vezes eles não apresentam inovação científica, embora possam representar inovação tecnológica, eles invariavelmente demandam grande quantidade de esforço e recursos para a sua concretização.

Mesmo demandando um esforço extra, a autora acredita que a pesquisa aplicada em sistemas tecnologicamente complexos, por meio da composição e do agrupamento de competências, é um bom caminho para melhorar tecnologicamente o país e produzir uma pesquisa inovadora. Os resultados que serão apresentados nas seções que se seguem parecem vir ao encontro dessa afirmação.

A título de exemplo, cabe apresentar a situação do Brasil em termos tecnológicos. A maior parte da exportação brasileira se dá no setor agrícola, fazendo com que as riquezas e as divisas do país sejam garantidas pela agricultura e não pela produção tecnológica de outros segmentos, diferentemente da China, Rússia e Índia por exemplo. Nesses países, a colaboração e a pesquisa multidisciplinar vêm merecendo destaque, justamente por prover melhorias e inovações tecnológicas. Cabe mencionar que grandes universidades, como é o caso de Harvard e do MIT (*Massachusetts Institute of Technology*), também vêm apostando na multidisciplinaridade como meio de permitir avanços tecnológicos significativos.

O governo brasileiro por meio de políticas mais recentes, apoiado pelo Ministério de Ciência, Tecnologia e Inovação (MCTi), FINEP, Fundações de Apoio a Pesquisa (FAPs) entre outros, tem incentivado o trabalho em rede, visando a colaboração. Cabe destaque para o incentivo à criação dos Institutos Nacionais de Ciência e Tecnologia.

3.2 Perspectivas de Pesquisa

Com a chegada da autora na Universidade de São Paulo, com a acolhida no Laboratório de Sistemas Distribuídos e Programação Concorrente (LaSDPC), e com a criação do INCT-SEC, foi possível vislumbrar uma pesquisa mais unificada e aplicada, dando origem a um trabalho mais focado e multidisciplinar. Nesse sentido, na Figura 3.1 é ilustrado um mapa do esforço em pesquisa, que sintetiza o

projeto acadêmico de pesquisa da autora para os próximos anos. A Figura 3.1 servirá como pano de fundo para ilustrar diferentes *layers* da pesquisa. Essas *layers* permitem definir desde estratégias de incorporação de alunos até visualizar as colaborações de pesquisadores tanto nacionais quanto internacionais.

Ligando e desligando cada uma das *layers* pode-se então obter as visões estratégicas que se deseja. Foram concebidas pelo menos 20 *layers*:

- Alunos de Iniciação Científica
- Alunos de Mestrado
- Alunos de Doutorado
- Alunos de Pós-doutorado
- Colaboradores
- Redes de Computadores e Sistemas Computacionais Distribuídos
- Engenharia de Software
- Hardware
- Sensoriamento Remoto
- Algoritmos Criptográficos
- Algoritmos Paralelos
- Publicações em Journals
- Publicações em Anais de Eventos Nacionais
- Publicações em Anais de Eventos Internacionais
- Artigos em Eventos de Iniciação Científica
- Veículos Aéreos Não Tripulados
- Inteligência Artificial

- Controle
- Banco de Dados
- Materiais

O que se pretende com essa organização da pesquisa é o domínio da tecnologia de sistemas embarcados críticos seguros e inteligentes. Essa é uma visão bastante macroscópica do problema, embora seja possível visualizar que os desafios impostos por esse tipo de pesquisa são inúmeros. Em um primeiro instante, os esforços concentram-se em dois grandes resultados tangíveis: veículos aéreos não tripulados e sistemas embarcados críticos. Os trabalhos desenvolvidos pela autora relacionados a esses resultados tangíveis são descritos nas seções 3.3 e 3.4.

No que tange os sistemas embarcados críticos, a importância tem sido dada na fase de concepção dos mesmos. Os trabalhos têm focado até aqui metodologias para o desenvolvimento dessa classe de sistemas. A possibilidade de contar com a colaboração de vários pesquisadores, nacionais e internacionais, de áreas distintas têm permitido realizar a tarefa de concepção de sistemas desse porte. Neste sentido, a autora tem dedicado esforços em compor uma equipe colaborativa e que tenha um objetivo principal, o desenvolvimento de sistemas embarcados críticos seguros.

O mapa ilustrado na Figura 3.1 é constituído basicamente de 3 níveis denominados: Tecnológico, Implementação e Conceitual. O eixo y do gráfico determina o potencial de inovação das pesquisas realizadas em cada um desses níveis e o eixo x o grau de envolvimento da autora com as áreas de pesquisa consideradas necessárias para o desenvolvimento do cenário global da pesquisa. As cores dos retângulos internos sugerem agrupamento por áreas, constituindo *layers* diferentes para cada área.

O Nível Tecnológico apresenta os temas tecnológicos tratados em trabalhos orientados pela autora ou realizados em colaboração com outros profissionais. Grande parte desses trabalhos é realizado por alunos de iniciação científica. Como é possível observar, a autora trata esses temas de forma mais superficial, sem que ocorra um grau de envolvimento muito elevado, não constituindo o foco

Figura 3.1: Mapa do esforço em pesquisa.

principal de pesquisa da autora e sim áreas que se fazem necessárias para a composição de sistemas mais complexos.

O Nível Implementação apresenta os elementos de pesquisa que envolvem implementação relacionada com disciplinas da ciência de computação. Essa implementação é necessária para que as pesquisas mais conceituais, e foco de trabalho da autora, possam ser desenvolvidas, validadas e testadas. Os trabalhos realizados no Nível Implementação são na maioria dos casos trabalhos de mestrado.

O Nível Conceitual, que na maioria das vezes envolve pesquisas que refletem o estado da arte das áreas consideradas, é destinado na maior parte dos casos para alunos de doutorado e pós-doutorado e requerem um alto grau de envolvimento da autora.

As cores das áreas que compõem o mapa permitem observar os elementos pertencentes a cada subconjunto específico, a título de exemplo, a cor vermelha engloba as atividades relacionadas à área de sistemas computacionais distribuí-

colaboração com outros grupos ou pesquisadores, como pode ser observado no mapa de colaboração. Outros resultados necessários, que caracterizem elementos tecnológicos, poderão ser obtidos a partir de produtos já disponíveis no mercado. O que não se pode desconsiderar é a necessidade da existência desses elementos para compor o quadro de pesquisa pretendido.

Figura 3.3: Mapeamento dos alunos sob orientação.

O mapeamento das colaborações, tanto nacionais (em vermelho) quanto internacionais (em amarelo), é apresentado na Figura 3.4. Alguns dos colaboradores fazem parte do LSEC.

Dada a relevância da formação de recursos humanos, e tendo em vista que muitos dos trabalhos desenvolvidos têm início na atividade de iniciação científica, a Figura 3.5 ilustra os resumos de trabalho publicados em congressos por alunos de iniciação científica. De modo análoga, a Figura 3.6 ilustra os alunos de mestrado da Fase I e os de iniciação científica da Fase I e da Fase II já finalizados.

Figura 3.4: Mapeamento das colaborações nacionais e internacionais.

3.3 Veículos Aéreos Não-Tripulados

Veículo Aéreo Não Tripulado (VANT) constitui um cenário típico de um sistema embarcado crítico complexo. O fato de constituir uma aplicação típica e, de um conhecimento prévio por parte de um dos componentes do grupo no qual a autora está inserida, esse se tornou o sistema embarcado crítico alvo para a aplicação das demais pesquisas realizadas. O desenvolvimento de VANTs convencionais não é propriamente inovador, mas ainda constitui um desafio, principalmente no Brasil. O fator que merece destaque não é o simples desenvolvimento de aeronaves que possam voar e cumprir uma missão, mas sim que essas aeronaves possam ser seguras e apresentar elevados níveis de inteligência embarcada. A proposição e a definição dos fatores que possam vir a prover inteligência e segurança a essas

Figura 3.6: Mapeamento dos alunos de mestrado da Fase I e de iniciação científica das Fases I e II já concluídos.

Algumas aeronaves podem voar de forma autônoma, seguindo uma trajetória de voo pré-programada (baseada em um *grid* ou uma sequência de *waypoints*), conforme demonstrado também no artigo (Trindade Jr et al., 2010), enquanto outras voam recebendo comandos a partir de estações terrestres operadas por pilotos.

O tamanho da aeronave pode variar desde o micro até o grande, e a estação de controle terrestre pode ser implementada em *smartphones*, *tablets*, *notebooks* ou redes de estações de trabalho (estações de controle distribuídas). O avião pode variar não apenas em tamanho, mas também na forma, no tipo de propulsão e no desempenho. A interface homem-máquina pode variar desde um *joystick* até uma interface de usuário tangível (por exemplo, uma mesa tangível com realidade aumentada). O desempenho dos *links* de comunicação e o tipo de carga também são muito importantes para cumprir a missão destinada ao sistema. O capítulo de

livro (Trindade Jr et al., 2012) publicado pela autora em cooperação com outros profissionais destaca as características dessas aeronaves e apresenta uma tabela que visa elucidar a classificação de um VANT. Esse capítulo destaca, também, o VANT Tiriba desenvolvido no escopo do INCT-SEC em parceria com a AGX Tecnologia e que tem servido de base para todos os estudos realizados a partir de 2009 (Branco et al., 2011a).

Todos os artigos relacionados a VANTs encontrados na literatura apresentaram VANTs implementados usando abordagens tradicionais (Roadmap34, 2009), (Valavanis, 2007), (Roadmap32, 2009), (Roadmap30, 2005), (Roadmap27, 2002), (Force, 2009).

Existem *roadmaps* que ilustram os avanços esperados para os VANTs, publicados periodicamente por organizações militares, como a Força Aérea dos Estados Unidos (Roadmap32, 2009). Isso implica que na visão da autora a concepção de VANTs não é o conceito principal, mas sim a concepção de VANTs inteligentes e seguros, tendo em vista que os VANTs, dentro dos próximos 10 anos, devem dominar uma boa parte do espaço aéreo para a realização de diferentes missões, desde agrícolas, passando por inspeções de fronteira chegando até ao transporte automático de cargas. Nesse sentido, acredita-se que em um futuro não muito distante, as únicas aeronaves tripuladas que deverão permanecer atuantes são as que transportam passageiros, a exemplo do que ocorre em outros sistemas de transporte, por exemplo, o metroviário onde o condutor precisa atuar somente em emergências.

Computação orientada a serviços é um paradigma que utiliza serviços como blocos básicos para o desenvolvimento de aplicações. Esse paradigma permite que aplicações sejam construídas em uma rede de cooperação que atravessa as fronteiras das universidades e organizações. Esses blocos devem, entretanto, seguir padrões.

Arquiteturas orientadas a serviços (*Service-Oriented Architecture* - SOA) têm recebido atenção significativa da comunidade de desenvolvimento de *software*, embora haja alguns entendimentos conflitantes sobre os conceitos e o uso de SOA. Vários tipos de arquiteturas orientadas a serviços surgiram e *Web Services* são a implementação mais comum (Erl, 2005). Esta implementação permite a interope-

tabilidade de aplicações com o uso de uma série de padrões baseados em XML (*eXtensible Markup Language*).

A vantagem de usar o paradigma SOA é a interoperabilidade alcançada com a utilização de XML, que permite não apenas comunicação convencional na Web, mas também comunicação entre dispositivos que vão desde um sensor pequeno até equipamentos domésticos sofisticados, comerciais ou industriais. Componentes autodescritivos abertos que permitem integração rápida são característicos nesse tipo de paradigma.

Embora a utilização de SOA no domínio de aplicações voltadas para negócios (Tecnologia de Informação – TI) esteja bem estabelecida, vários aspectos devem ser considerados no domínio dos sistemas embarcados, principalmente a disponibilidade de recursos suficientes (poder de processamento e capacidade de memória). Sistemas embarcados estão ligados ao rápido crescimento da Internet, tecnologias de comunicação, computação pervasiva e aparelhos eletrônicos portáteis. Os tamanhos dos sistemas vão desde pequenos até sistemas grandes, complexos e *multicore*. Em muitos deles há recursos suficientes para que seja possível a utilização de *Web Services*.

Sistemas embarcados críticos possuem alguns requisitos especiais. O desempenho em tempo real é quase obrigatório e deve ser garantido em qualquer circunstância. Alguns mecanismos de SOA, por exemplo, a descoberta de serviços, têm potencial para comportamento não determinístico e não compatível com os requisitos básicos de sistemas embarcados críticos. Por outro lado, sistemas embarcados críticos complexos podem ser quase sempre divididos em seções críticas e não críticas (ou de baixa criticidade). Apesar de possuírem algoritmos mais complexos, as seções críticas são normalmente menores do que as seções não críticas do código.

Muitos sistemas embarcados complexos estão associados a um sistema de informação de alto nível. SOA pode prover a integração entre serviços de sistemas embarcados de baixo nível com serviços de sistemas de informação de alto nível. Essa integração ainda constitui elemento de estudo, apesar de serem muitos os trabalhos relacionados encontrados na literatura (Thramboulidis et al., 2008; Erl, 2005; Karkanakov, 2005; Karkanakov and Spasov, 2005).

Esse uso crescente de VANTS deve fazer com que eles se tornem cada vez mais comum, passando a ser comercializados de forma mais ampla. Nesse cenário, propôs-se o trabalho do aluno de doutorado Douglas Rodrigues que consiste na utilização de arquitetura orientada a serviços em sistemas embarcados críticos. Isso deve facilitar o desenvolvimento de aplicações automatizadas de VANTS, permitindo que esses veículos possam ser inseridos e incorporados mais facilmente no espaço aéreo compartilhado e contribuindo para a sua disseminação. Mais especificamente, esse trabalho tem como foco o desenvolvimento de um *framework*, denominado KBF (*Knowledge Based Framework for Dynamically Changing Applications*), para a utilização de *Web Services* em seções de baixa criticidade de sistemas embarcados críticos complexos, com foco no subsistema de controle de missões de aeronaves não tripuladas. Os resultados preliminares deste trabalho foram publicados em **(Rodrigues et al., 2011d)**.

O KBF deverá permitir a definição de *Web Services* dinamicamente, dependendo da configuração atual do sistema, da disponibilidade de *Web Services* componentes e de uma base de dados com informações de contexto previamente definida. Mais especificamente, o sistema utilizará informações de contexto e de monitoramento para compor ou gerar serviços com diferentes níveis de precisão/-segurança/confiabilidade/desempenho de forma dinâmica e inteligente **(Rodrigues et al., 2011e)**.

As aplicações orientadas a serviços são altamente distribuídas e dinâmicas, e utilizam serviços dos quais só se conhece a interface de utilização, sem informações, normalmente, sobre a sua qualidade. Essas oportunidades de mau funcionamento são inúmeras, podendo acarretar grandes perdas para as empresas, organizações e sistemas que utilizam essa tecnologia. Neste contexto é importante considerar a segurança como um aspecto fundamental na construção de *Web Services*, pois podem existir consequências financeiras ou legais se dados forem interceptados por terceiros ou se dados fraudulentos forem aceitos como válidos.

Buscando solucionar esse problema o trabalho de mestrado do aluno Douglas Rodrigues proveu uma avaliação e comparação de diretrizes e a adequação de técnicas que permitem não somente a criação de *Web Services* seguros, mas também a validação dos serviços utilizados para determinar se a aplicação final pos-

sui as características desejadas no que diz respeito ao desempenho e à segurança. Nesse sentido, foram analisadas as principais especificações de segurança empregadas em *Web Services* no contexto atual, bem como avaliados os algoritmos criptográficos e o comprimento das chaves utilizadas. As especificações e mecanismos como *WS-Security*, *WS-Policy*, *WS-SecureConversation*, entre outros foram tratados e utilizados. A relação segurança/desempenho foi abordada e avaliações relativas às necessidades inerentes tanto da aplicação quanto dos clientes com relação a essas duas características foram definidas. Uma arquitetura de segurança para *Web Services* foi criada e mostrou-se bastante eficiente na proposição de *Web Services* seguros **(Rodrigues et al., 2011c)**, **(Rodrigues et al., 2011b)**, **(Rodrigues et al., 2010)**, **(Rodrigues et al., 2011a)**, **(Rodrigues and Branco, 2010)**, provendo resultados que serão utilizados no seu doutorado.

As contramedidas relacionadas aos principais ataques relacionados a *Web Services* também têm sido alvo de estudo e pesquisa. Nesse sentido, os estudos apresentados em **(Rodrigues et al., 2012)** vão ao encontro de elucidar e apresentar os principais mecanismos e ferramentas utilizados frequentemente na tentativa de minimizar esses ataques. Esse trabalho, além de possibilitar a proposição de contramedidas e ferramentas para minimizar os riscos de ataques serviu também como ponte para estreitar relacionamentos internacionais, a exemplo do professor Marco Vieira da Universidade de Coimbra. Trabalhos de iniciação científica estão sendo desenvolvidos no sentido de desenvolver ferramentas ainda mais robustas para prover segurança a aplicações orientadas a serviço, como é o caso da iniciação científica do aluno Ademir Takeo Akabane.

O estudo de algoritmos criptográficos como o ECC (*Elliptic Curve Cryptography*) tem o intuito de prover segurança aos sistemas embarcados críticos buscando um equilíbrio entre a segurança e o desempenho das aplicações que são executadas. Esse é o trabalho que tem sido desenvolvido pelo aluno de mestrado Daniel Fernando Pigatto em colaboração com a aluna de iniciação científica Natássya Silva. Resultados preliminares que apontam para melhores tempos de resposta obtidos com o uso desse algoritmo em dispositivos em movimento foram publicados em **(Pigatto et al., 2011)** e **(Pigatto et al., 2012)**.

3.3.1 Modelo de Referência para Veículos Aéreos Não Tripulados

Arquitetura é uma estrutura que identifica, define e organiza componentes. O relacionamento e os princípios de projeto dos componentes, funções e interface estabelecidas entre subsistemas também podem ser organizadas e definidas por uma arquitetura.

Um modelo de referência para uma arquitetura é uma arquitetura onde as entidades, relacionamentos e unidades de informação envolvidos nas interações entre e dentro dos subsistemas e componentes são definidos e modelados. Em resumo, é um modelo que incorpora o objetivo básico ou a ideia do sistema e pode ser considerado como uma referência para várias finalidades.

O NIST (*National Institute of Standards and Technologies*) provê um modelo de referência para VANTs (NIST, 2002). Neste padrão específico, o modelo de referência foi proposto para especificar regras militares, usos e comandos de forma compreensível e intuitiva para um comandante humano.

Para que o KBF possa ser desenvolvido, a divisão entre partes críticas e não críticas de um sistema embarcado crítico complexo pode ser feita a partir da definição de um modelo de referência. Essa definição inclui os serviços e protocolos entre as camadas do modelo. A proposta desse modelo de referência para sistemas embarcados críticos e a definição das camadas e dos protocolos constitui o trabalho a ser desenvolvido no doutorado do aluno Emerson Alberto Marconato.

A separação em camadas permite que o sistema seja dividido em subsistemas que podem ter implementações diferentes e ajuda separar em diversos níveis de criticidade as partes que compõem um sistema embarcado crítico complexo.

3.3.2 MOSA - *Mission-Oriented Sensor Array*

Uma das partes do sistema com baixa criticidade em segurança é o controle de missões. O trabalho de mestrado do aluno Rayner de Melo Pires (**Branco et al., 2011b**) tem como objetivo o desenvolvimento de um mecanismo *plug-and-play*

para arranjos inteligentes de sensores. Essa interface é composta basicamente por dois elementos, a SSI (*Smart Sensor Interface*) e o SSP (*Smart Sensor Protocol*).

A SSI é um conceito que facilita a integração da carga paga (*payload*) em um VANT, normalmente representada por sensores, para a realização de missões específicas. Com a SSI, a missão é isolada da aeronave e passa a ser definida por um arranjo de sensores ou MOSA (*Mission Oriented Sensor Array*) **(Rodrigues et al., 2011e), (Pires et al., 2011)**. A aeronave provê a capacidade de deslocamento ao sensor. O sensor é responsável pela missão, direcionando a aeronave para sua realização.

Nem sempre a aeronave pode preencher todos os requisitos necessários para cumprir uma missão específica. Quando conectados, a aeronave e o sensor comunicam-se usando o SSP para trocar informações com o objetivo de decidir sobre os requisitos necessários para a realização da missão. Como resultado, a missão pode ser completamente viável, parcialmente viável ou inviável. Essa etapa é realizada sempre que um novo sensor é conectado. As missões podem ser adaptativas e algumas configurações podem mudar durante a execução de uma missão. A descoberta de serviços proporcionada por SOA pode ser utilizada para permitir que o sensor escolha ou permita a composição do serviço mais adequado para executar a missão proposta.

Diferentes missões, definidas por diferentes subsistemas MOSA e diferentes VANTs, podem ser integrados pelo KBF, que pode fornecer mecanismos para a escolha do melhor serviço que se ajuste ao cenário de utilização do sistema. Este é o mecanismo básico da implementação da SSI e do SSP, fazendo com que a missão possa ser adaptativa.

Quando a unidade MOSA é conectada, a SSI/SSP provê mecanismos para a configuração automática (*plug-and-play*) tanto da unidade quanto da aeronave, determinando-se neste momento a possibilidade de execução da missão, mesmo que de forma parcial. Uma indisponibilidade de um serviço em uso durante a execução de uma missão pode ser contornada pela descoberta de um serviço equivalente. Caso ele exista, a missão poderá ser retomada, com a eventual penalidade de perda de alguma funcionalidade ou precisão.

Fazendo uso da possibilidade da existência de diferentes MOSA, o trabalho da pesquisadora Adimara Culturato (com bolsa de pós-doutorado solicitada junto a FAPESP) (**Culturato et al., 2011**), tem como objetivo o mapeamento de doenças em plantações de eucalipto fazendo uso de imagens coletadas por VANTs. A especificação de um MOSA para detecção dessas doenças permitirá que as informações sejam disponibilizadas mais rapidamente e com menor custo. Além disso, o mapeamento das pragas e doenças permite a aplicação localizada de defensivos, com consequente vantagens econômicas de preservação do meio ambiente. Esse trabalho tem sido desenvolvido em parceria com o professor Onofre trindade Junior da USP, com o professor Edson L. Furtado da UNESP de Botucatu, e com o professor Paulo Estevão Cruvinel da Embrapa Instrumentação. Oportunidades de pesquisa conjunta têm sido vislumbradas e estão em negociação com pesquisadores da *Purdue University* e com a *University of Surrey*.

O trabalho de mestrado da aluna Natássya Silva (**Cruvinel and et. al., 2011**) também vem ao encontro das necessidades na área da agricultura, e portanto também terá colaboração, além do professor Onofre, do professor Paulo Cruvinel. O trabalho da aluna visa o desenvolvimento de um sistema de comunicação seguro para troca de informações entre um VANT e um avião tripulado. O objetivo do avião tripulado é o de fazer a pulverização em áreas de plantio, enquanto que o do VANT é de averiguar a deriva causada por essa pulverização. Estudos serão realizados no intuito de diagnosticar a viabilidade do uso de um VANT do tipo VTOL (*Vertical Take-Off and Landing*) para esse tipo de aplicação.

Como já mencionado, em um futuro próximo, VANTs devem popular boa parte do espaço aéreo para a realização de diversas missões. O estudo da estratégia de utilização do espaço aéreo tem sido liderado pelo professor João Batista Camargo Júnior, da Poli-USP, e realizado em parceria com autora, com o professor Onofre e outros pesquisadores do LSEC. Neste cenário, as aeronaves devem coordenar o uso do espaço aéreo, sem intervenção humana.

A ausência de piloto a bordo da aeronave não tripulada suscita outra questão importante: a substituição das outras funcionalidades desempenhadas pelo piloto humano. A esta substituição propôs-se a denominação *In-flight Awareness* (IFA) (**Rodrigues et al., 2011e**). O piloto humano pode sentir odores alarman-

tes, avaliar a formação de nuvens, ouvir ruídos não habituais, sentir vibrações incomuns, ouvir e transmitir comandos para a torre de controle, bem como ficar ciente das fronteiras políticas e das características do solo sobrevoado. Todo esse conhecimento pode ser utilizado para evitar situações perigosas e selecionar o melhor procedimento em situações de emergência. SOA tem grande potencial para dar suporte à implementação da IFA, devido ao seu comportamento naturalmente dinâmico. As definições e o tratamento adequado da IFA, como uma extensão da filosofia *sense and avoidance*, bem como a definição nesse escopo do *link* de comunicação/transmissão digital seguro e criptografado é o objetivo principal do trabalho de doutorado que será iniciado pelo aluno Daniel Pigatto logo após a conclusão do seu mestrado, estimada para abril de 2012.

3.4 Metodologias para o desenvolvimento de Sistemas Embarcados Críticos

Sistemas embarcados são considerados críticos quando eventos de falha podem acarretar perdas de vidas humanas ou perdas de ativos de alto valor. Em algumas aplicações, como na aviação, sistemas embarcados críticos devem apresentar taxas de falha tão baixas como uma falha grave a cada 10^5 até 10^9 horas de operação.

Sistemas embarcados estão se tornando cada vez mais complexos tanto em hardware quanto em *software*. Sistemas *multicore* e multiprocessadores estão se tornando comuns, aumentando ainda mais a complexidade do *software* (Bergamaschi et al., 2003). Por outro lado, eles estão se tornando mais e mais comuns em ambientes domésticos e profissionais para o controle ou gerenciamento de informação.

A construção de *software* para sistemas embarcados é normalmente mais complexa do que para outros sistemas computacionais. Em tais sistemas, o *software* tem que se comunicar em baixo nível com dispositivos de *hardware*, e deve funcionar por dias e até anos sem parar mesmo em ambientes hostis (alta temperatura, umidade, vibração) (Douglass, 2004). Além disso, há limitações de recursos,

como memória e processamento, sendo necessárias soluções para otimização dos programas, o que não ocorre em outros sistemas computacionais que dispõem de recursos mais abundantes e não têm que atender requisitos de tempo real.

Sistemas embarcados críticos devem seguir normas elaboradas por associações de empresas, órgãos governamentais, como, por exemplo, a RTCA (*Radio Technical Commission for Aeronautics*). Essas normas são importantes para garantir a confiabilidade e adequabilidade desse tipo de sistema, e mais que isso, equipamentos críticos não podem ser comercializados e aplicados sem a sua devida homologação por essas normas. Não basta, simplesmente, projetar e construir um sistema para aplicações críticas que funcione, é preciso que todo o projeto e desenvolvimento sejam baseados em normas e metodologias que tornem esse equipamento seguro e comercializável. Muitas vezes, esse aspecto é mais difícil de ser cumprido do que a técnica envolvida na especificação e implementação do sistema.

O desenvolvimento de sistemas embarcados demanda, dessa forma, uma metodologia de engenharia de *software* diferenciada da adotada para sistemas de informação (Hugues et al., 2008). Nesse sentido, iniciou-se a investigação de metodologias de desenvolvimento que possam atender não somente as necessidades particulares dessa classe de sistemas como também as necessidades específicas das normas e processos de certificação desses sistemas.

A metodologia inicialmente proposta é a chamada SAFE-CRITES (Braga et al., 2011c), (Trindade Jr et al., 2009). A SAFE-CRITES permite o desenvolvimento de aplicações críticas com diferentes níveis de complexidade e desempenho. Como meio de avaliar a metodologia foi desenvolvido um sistema de orientação e controle automático de uma aeronave não tripulada. Fazendo uso da SAFE-CRITES é possível que o *software* de produtos similares possam ser desenvolvidos com pouco esforço, apenas reorganizando e re-mapeando os blocos funcionais já desenvolvidos.

Os resultados preliminares indicam que o uso do SAFE-CRITES fornece maior confiabilidade para o sistema em desenvolvimento e também facilita a geração da documentação necessária para os processos de certificação, por exemplo, aquelas baseadas no padrão da DO178B. Como outro benefício, fornece aos projetistas de

sistemas embarcados críticos uma abordagem de desenvolvimento melhorada, reduzindo significativamente o risco de erros de projeto, bem como uma considerável redução dos tempos totais de concepção e implementação desses sistemas.

A metodologia SAFE-CRITES encoraja a reutilização de componentes pré-certificados, sempre que possível, como forma de aumentar a produtividade e qualidade. Quando a reutilização não for possível, o processo indica os itens que devem ser criados e validados para garantir a qualidade desejada, a fim de tornar possível a certificação a posteriori. Sempre que novos componentes são criados e validados, são documentados e inseridos em um repositório para reutilização futura **(Braga et al., 2011a)**. O projeto e a construção de uma aeronave não tripulada, denominada Tiriba **(Branco et al., 2011a)**, foram desenvolvidos utilizando-se essa metodologia.

No final do projeto da aeronave Tiriba, uma avaliação foi realizada para ver em que medida a reutilização de *software* seria possível para uso no *hardware* de um novo projeto, o SARVant, que possui um *hardware* completamente modificado e desenvolvido para atender a novas exigências. Embora possam ser reutilizados depois de alguns ajustes, os artefatos produzidos no projeto Tiriba não cumprem integralmente os requisitos do maior domínio representado pela família SARVant. Este é o lugar onde linhas de produto de *software* podem ajudar e, nesse sentido, foi proposta a extensão da SAFE-CRITES. A ProLiCES **(Braga et al., 2011b)** constitui, dessa forma, uma extensão do SAFE-CRITES, com base em linha de produtos de *software* para apoiar o desenvolvimento de sistemas embarcados críticos seguros **(Braga et al., 2012)**.

O desenvolvimento dessas metodologias tem sido intensificado e novas ideias têm sido elaboradas e abordadas no sentido de cuidar de forma mais enfática do processo de certificação. Metodologias com vistas a certificação, principalmente voltadas para linha de produtos de *software*, são ainda inexistentes e constituem uma área ampla de estudo e pesquisa. Essa linha de pesquisa tem sido liderada pela professora Rosana Terezinha Vaccari Braga, pesquisadora membro do LSEC e desenvolvida em colaboração com outros pesquisadores como os professores Onofre Trindade Junior e Paulo Cesar Masiero da USP, o pesquisador Martin Bec-

ker do *Fraunhofer Institute for Experimental Software Engineering* da Alemanha e o pesquisador Luciano de Oliveira Neris da empresa AGX Tecnologia.

3.5 Considerações Finais

É inegável a importância apresentada pelos sistemas embarcados críticos atualmente. Quase 90% dos sistemas computacionais existentes são uma forma de sistema embarcado. A criticidade desses sistemas tem sido cada vez mais frequente, uma vez que eles têm desempenhado funções que podem colocar vidas humanas e equipamentos de alto valor econômico em risco.

A segurança desses dispositivos, tanto no sentido de segurança das informações que são transferidas quanto ao acesso aos sistemas físicos e lógicos é um fator que tem merecido atenção não só da comunidade acadêmica, mas também da comunidade empresarial e dos órgãos governamentais.

Um dos sistemas embarcados críticos que tem merecido atenção são os VANTs. O desenvolvimento e a utilização desses veículos requerem o uso de diversos conceitos, levando a necessidade de equipes multidisciplinares de pesquisadores.

Esse capítulo apresentou as pesquisas que foram e estão sendo desenvolvidas pela autora no sentido de conceber VANTs seguros e inteligentes, partindo da sua idealização por meio de modelos (uso de matlab/simulink) e fazendo uso de metodologias apropriadas para o seu desenvolvimento. Mostrou ainda que as pesquisas estão em andamento e devem ser conduzidas por um período que provavelmente ultrapasse a duração da carreira de pesquisa da autora. A complexidade e as possibilidades de atuação nessa área são imensas, permitindo que muitas propostas e idealizações discutidas e pesquisadas hoje venham a ser aplicadas e utilizadas nos próximos 10 anos.

O próximo capítulo apresenta as reflexões e os trabalhos futuros.

Capítulo 4

Conclusões

4.1 Discussões e Reflexões

Esse texto sistematizado descreve o trabalho de pesquisa em sistemas distribuídos e redes de computadores e a produção científica da autora após a conclusão do seu doutorado em 2004.

Em 2008, com sua contratação no Instituto de Ciências Matemáticas e de Computação - ICMC-USP e a aprovação do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos - INCT-SEC, foi criado o Laboratório de Sistemas Embarcados Críticos - LSEC e iniciada uma atuação mais focada na pesquisa em sistemas embarcados críticos seguros. Tanto o INCT-SEC quando o LSEC têm sido de fundamental importância para o desenvolvimento das atividades de pesquisa relacionadas a esse tema, pois permitiram aglutinar pessoas e compor uma equipe multidisciplinar capaz de resolver e solucionar problemas aplicados complexos.

O desenvolvimento de sistemas embarcados críticos, com foco em aviônicos, é fator de grande relevância no cenário nacional, bem como os aspectos de segurança desses sistemas. Diversos resultados relevantes foram obtidos, com avanços significativos em problemas importantes, como é o caso do controle de voo de aeronaves não tripuladas.

A autora tem investido esforços principalmente na área de segurança e no que se refere a comunicação entre dispositivos. Essa comunicação segura e o uso dos diferentes mecanismos e ferramentas que garantam essa segurança tem permitido a obtenção de resultados relevantes. Sendo os sistemas embarcados críticos uma classe importante de sistemas, prover sistemas embarcados críticos seguros é o foco das pesquisas da autora.

Esse foi o panorama no qual a autora investiu seus esforços de pesquisa nos últimos anos, e que possibilitou o aumento da sua participação, inserção e contribuição no meio acadêmico. Essa inserção se deu por meio da participação em eventos científicos, apresentando trabalhos, palestras, tutoriais e seminários, tanto em conferências nacionais e internacionais como: Simpósio Brasileiro de Inteligência Artificial - SBIA, Congresso Latinoamericano de Informática - CLEI, Simpósio Brasileiro de Sistemas Multimídia e Web - WebMedia, *Unmanned Aircraft System Latin Conference* - UAS Latin, entre outros.

É nesse panorama multidisciplinar que todos os alunos, tanto de graduação quanto de pós-graduação sob orientação da autora, estão focados e trabalhando. Os resultados obtidos com essas pesquisas não somente têm sido publicados em eventos científicos, como também tem atraído grande atenção da mídia, por meio de reportagens impressas e na TV. Também têm atraído interesse de empresas e de organizações governamentais, provendo parcerias como: Exército, Polícia Militar Ambiental, AGX Tecnologia, entre outras empresas e instituições. A colaboração de pesquisadores internacionais e nacionais tem possibilitado a integração com diferentes grupos de pesquisa. Essas parcerias devem resultar em novas pesquisas e novos desafios a serem vencidos com potencial para contribuir de forma significativa no aprimoramento do cenário tecnológico nacional.

4.2 Trabalhos em Andamento e Futuros

Nos próximos anos a autora pretende continuar focando suas pesquisas no desenvolvimento de sistemas embarcados críticos seguros. O mapa de esforço em pesquisa apresentado na seção 3.2 é uma ferramenta importante para a manuten-

ção do foco das pesquisas e para que elas possam atingir os objetivos estabelecidos.

As áreas coloridas na Figura 4.1 são as de maior envolvimento e contribuição da autora. É possível observar que são áreas bastante vastas e que vários anos de pesquisa serão necessários para investigar e pesquisar as possibilidades e os desafios apresentados por elas.

Figura 4.1: Mapeamento das publicações.

A autora tem investido em cooperações com outros grupos de pesquisa tanto no Brasil como no exterior. O aluno de doutorado Douglas Rodrigues deve no início de 2013 realizar estágio sanduíche de um ano em universidade estrangeira que tem trabalhos importantes na área. Essa, entre outras ações, deve permitir uma maior integração com pesquisadores estrangeiros.

Agradecimentos

Aos meus alunos e ex-alunos, de graduação e pós-graduação, sem os quais seria impossível a realização de todos os projetos de pesquisa e de vida. Vocês permitiram, e continuarão a permitir que meu sonho de "ensinar" se torne uma realidade a cada dia, pois cada um de vocês tem me ensinado que mais do que ensinar eu tenho a fantástica oportunidade de aprender com cada um de vocês. Meu sincero obrigada.

Aos pesquisadores que tem constituído a "nossa" equipe de trabalho. Aos membros do INCT-SEC com os quais tenho aprendido muito.

Agradeço aos professores e funcionários do ICMC, muitos dos quais tem me apoiado desde que eu ainda era aluna da pós-graduação. Obrigada pela disposição em ajudar sempre.

Em especial, agradeço aos professores do ICMC (em ordem alfabética):

- Denis Fernando Wolf e Fernando Santos Osório sempre companheiros nas discussões e nos desafios. Obrigada por estarem sempre presente, pela amizade sincera e todo trabalho conjunto. Sem vocês certamente tudo teria muito menos graça e todo o trabalho desenvolvido não seria tão divertido.
- José Carlos Maldonado obrigada pela oportunidade em partilhar dos desafios de um projeto como o INCT-SEC. Sempre aprendo muito.
- Marcos José Santana e Regina Carlucci Santana, obrigada pela oportunidade dada desde o meu ingresso no mestrado. Certamente, toda a confiança em mim depositada lá atrás foi o que me possibilitou chegar até aqui hoje.

- Onofre Trindade Júnior, obrigada pela amizade, e por toda a dedicação em me ensinar e me mostrar o caminho das pedras na área de sistemas embarcados, principalmente no tocante a veículos aéreos não tripulados. Obrigada por permitir que eu compartilhe um pouco do seu vasto conhecimento. Obrigada pela amizade sempre sincera, e por conseguir sempre me contagiar com a sua "loucura".
- Rosana Braga, obrigada por compartilhar sua perseverança e seu otimismo sempre.

Agradeço ao suporte financeiro da FAPESP, CAPES e CNPq.

Agradeço a minha super mãe Rosa, por sempre me amar e me apresentar o verdadeiro sentido das palavras coragem e garra.

Finalmente, agradeço ao Luiz Henrique e Pietra, pelo amor, apoio e compreensão de sempre.

Referências Bibliográficas

- Bergamaschi, R., Martin, G., Wolf, W., Ernst, R., Vissers, K., and Kouloheris, J. (2003). The future of system-level design: can we find the right solutions to the right problems at the right time? In *Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis, CO-DES+ISSS '03*, pages 231–231, New York, NY, USA. ACM.
- Bidóia, M. C. and Branco, K. (2009). Definição de assinaturas de ataque em statl. *REGRAD - Revista Eletrônica de Graduação UNIVEM.*, 2(2):25–40.
- Bissoli, M., Branco, K., and Ordonez, E. (2007). Algoritmos de multiplicação de montgomery em hardware e impacto no algoritmo rsa. In *In: Workshop de Sistemas Computacionais de Alto Desempenho - WSCAD, Gramado.*, pages 1–6.
- Braga, R., Branco, K., Trindade Jr, O., and Gimenez, I. (2011a). Evolving tiriba design towards a product line of small electric-powered uavs. In *In: 1a Conferência Brasileira de Sistemas Embarcados Críticos, 2011, São Carlos. Anais do 1º CBSEC. São Paulo - SP*, pages 67–72. EDUSP.
- Braga, R., Branco, K., Trindade Jr, O., Masiero, P., Becker, M., and Neris, L. (2011b). Prolices: An approach to develop product lines for safety-critical embedded systems. In *In: XXXVII Latin-American Informatics Conference (CLEI XXXVII)*, pages 1–16.
- Braga, R., Branco, K., Trindade Jr, O., Masiero, P., Becker, M., and Neris, L. (2012). The prolices approach to develop product lines for safety-critical embedded

- systems and its application to the unmanned aerial vehicles domain. In *Accepted to publication on CLEI electronic journal.*, pages 1–14.
- Braga, R., Branco, K., Trindade Jr, O., and Neris, L. (2011c). Safe-crites: Developing safety-critical embedded systems supported by reuse techniques. In *In: 12th IEEE International Conference on Information Reuse and Integration (IRI 2011).*, pages 206–211.
- Branco, K. and Ordonez, E. (2006). Load indices - past, present and future. In *Anais da International Conference on Hybrid Information Technology, Cheju Island.*, pages 120–129.
- Branco, K. and Ordonez, E. (2007). Load indices on heterogeneous systems past, present and future. *JCIT Journal of Convergence Information Technology.*, 2(2):49–57.
- Branco, K., Pelizzoni, J., Neris, L., Trindade Jr, O., Osório, F., and D.F., W. (2011a). Tiriba a new approach of uav based on model driven development and multiprocessors. In *In: IEEE International Conference on Robotics and Automation - ICRA Communications, 2011, Shanghai.*, pages 6584–6587. IEEE.
- Branco, K., Pires, R., and Trindade Junior, O. (2011b). Desenvolvimento de um mecanismo plug-and-play para arranjos inteligentes de sensores em sistemas aéreos não tripulados. In *Projeto de Mestrado Submetido a FAPESP - Documento Interno.*
- Branco, K., Santana, M., Santana, R., Bruschi, S., and Kawabata, C. (2006a). Usando simulação para avaliar índices de carga em ambientes distribuídos heterogêneos. In *In the Proceedings da XXXII Conferencia Latinoamericana de Informática CLEI 2006. Chile.*, pages 1–10.
- Branco, K., Santana, M., Santana, R., Bruschi, S., and Kawabata, C. (2006b). Vip e pvip - Índices de desempenho para avaliação de sistemas heterogêneos. In *In the Proceedings da XXXII Conferencia Latinoamericana de Informática CLEI 2006. Chile.*, pages 1–10.

- Branco, K., Santana, M., Santana, R., Bruschi, S., Kawabata, C. L., and Ordonez, E. (2006c). Piv e wpiv: Two new performance indices for heterogeneous systems evaluation. *INFOCOMP. Journal of Computer Science.*, 5:64–73.
- Branco, K., Santana, M. J., Santana, R., Cagnin, M. I., Ordones, E. D. M., and Bruschi, S. M. (2006d). Utilização de simulação para avaliação de desempenho de escalonamento de processos. In: Ildeberto Aparecido Rodello, José Remo Ferreira Brega, Kalinka Regina Lucas Jaquie Castelo Branco. (Org.). Escola Regional de Informática São Paulo/Oeste 2006. 1 ed. Marília: UNIVEM, p. 182-214.
- Branco, K., Santana, R., Santana, M., and Bruschi, S. (2006e). A novel simulator for evaluating performance indices on heterogeneous distributed systems environments. In *In the proceedings of the 2006 IEEE International Symposium on Industrial Electronics ISIE'06, Montreal.*, pages 3316–3321.
- Branco, K., Santana, R., Santana, M., and Bruschi, S. (2006f). Piv and wpiv: Performance index for heterogeneous systems evaluation. In *In the proceedings of the 2006 IEEE International Symposium on Industrial Electronics ISIE'06, Montreal.*, pages 323–328.
- Branco, K., Santana, R., Santana, M., Bruschi, S., and Kawabata, C. (2006g). Índices de carga para ambientes paralelos/distribuídos heterogêneos. In *Anais do IV Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPerformance), Campo Grande.*, pages 144–162.
- Branco, K. R. L. J. C. (2004). Índice de carga e desempenho em ambientes paralelos/ distribuídos – modelagem e métricas. Tese de Doutorado do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo.
- Cao, J. (2004). Self-organizing agents for grid load balancing. In *GRID*, pages 388–395.
- Cardoso, P. (2011). Especificação de ataques ddos utilizando uml- uma análise comparativa. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília.*

- Casavant, T. L. and Kuhl, J. G. (1988). A taxonomy of scheduling in general-purpose distributed computing systems. *IEEE Trans. Softw. Eng.*, 14:141–154.
- CDCiber (2012). Brasil se arma contra guerra virtual e cria centro especial de defesa. <http://www.basemilitar.com.br/forum/viewtopic.php?f=5&t=3490&start=60> acessado em janeiro de 2012.
- Chiaromonte, R. B., Ordonez, E., Pereira, F., and Branco, K. (2006). Aspectos de desempenho do sico (sistema de comunicação de dados com suporte dinâmico a segurança). In *In the Proceedings do VII Workshop em Sistemas Computacionais de Alto Desempenho (WSCAD), Ouro Preto.*, pages 1–10.
- Coulouris, G., Dollimore, J., and Kindberg, T. (2003). *Sistemas Distribuídos Conceitos e Projetos*. Prentice Hall., 1 edition.
- Coutinho, M. (2003). Network simulator guia básico para iniciantes. Universidade Federal do Pará - UFPA. Disponível na Internet em : <http://www.cci.unama.br/margalho/networksimulator/pdfs/nsr1.pdf>. Acesso em 15 de janeiro de 2012.
- Cruvinel, P. and et. al. (2011). Desenvolvimento da aplicação aérea de agrotóxicos como estratégia de controle de pragas agrícolas de interesse nacional. In *Projeto Submetido a Embrapa - Documento Interno*.
- Culturato, A. B., Branco, K., Trindade Junior, O., and Furtado, E. (2011). Geração de assinaturas espectrais para detecção de patologias em plantação de eucaliptos - um estudo utilizando vants. In *Projeto de Pós-Doutorado Submetido a FAPESP - Documento Interno*.
- Douglass, B. P. (2004). *Real Time UML: Advances in The UML for Real-Time Systems*. Boston: Addison Wesley, 3 edition.
- El-Rewini, H., Al, H. H., and Lewis, T. (1995). Task scheduling in multiprocessing systems. *j-COMPUTER*, 28(12):27–37.
- Erl, T. (2005). *Service-Oriented Architecture: Concepts, Technology, and Design*. Prentice Hall PTR, Upper Saddle River, NJ, USA.

- Feitelson, D. and Rudolph, L. (1995). Parallel job scheduling: Issues and approaches. In *In: IPPS'95 Workshop on Job Scheduling Strategies for Parallel Processing, Lecture Notes in Computer Science v.949, Santa Barbara, CA, USA*, pages 1–18. IPPS'95.
- Feitelson, D. and Rudolph, L. (1996). Toward convergence in job schedulers for parallel supercomputers. In *In: IPPS'96 Workshop on Job Scheduling Strategies for Parallel Processing, Honolulu, Hawaii, Lecture Notes in Computer Sciences*, page 1162. IPPS'96.
- Feitelson, D. and Rudolph, L. (1998). Metrics and benchmarking for parallel job scheduling. In *In ISSPP'98, Lecture Notes in Computer Science, n. 1459*, pages 1–24. ISSPP'98.
- Feitelson, D., Rudolph, L., Schwiegelshohn, U., Sevcik, K. C., and Wong, P. (1996). Theory and practice in parallel job scheduling. In *In: IPPS'97 Workshop on Job Scheduling Strategies for Parallel Processing, Lecture Notes in Computer Science v.1291, Santa Barbara, Geneva, Switzerland.*, page 1162. IPPS'97.
- Feres, M., Lucas, A., and Branco, K. R. L. J. C. (2006a). Avaliação de desempenho do protocolo tcp com controle e congestionamento highspeed em redes com topologia estrela. In *14º Simpósio Internacional de Iniciação Científica (SIICUSP).*, page 1.
- Feres, M., Lucas, A., and Branco, K. R. L. J. C. (2006b). Avaliação de desempenho do protocolo tcp/ip em redes com topologia estrela utilizando a ferramenta network simulator. In *Anais do XIV Congresso de Iniciação Científica da UFSCar.*, page 37.
- Ferrari, D. and Zhou, S. (1987). An empirical investigation of load indices for load balancing applications. In *In Proceedings of Performance'87, the 12th Int'l Symposium on Computer Performance Modeling, Measurement, and Evaluation.*, pages 512–528. Performance'87.
- Force, A. (2009). United states air force unmanned aircraft systems flight plan 2009-2047. In *Headquarters, United States Air Force Washington DC*.

- GAO (2008). Unmanned aircraft systems - federal actions needed to ensure safety and expand their potential uses within the national airspace system. In GAO-08-511.
- Gurgel, P., Barbosa, E., Branco, K., and Branco, L. (2012). A ferramenta netkit e a virtualização aplicada ao ensino e aprendizagem de redes de computadores. In *Submitted to the Simpósio Brasileiro de Redes de Computadores - SBRC 2012.*, pages 1–10.
- Gurgel, P. H. M. and Branco, K. R. L. J. C. (2010). Ensino de redes ethernet com laboratórios virtuais netkit. In *18º Simpósio Internacional de Iniciação Científica (SIICUSP).*, page 1.
- Heady, R. (1990). The architecture of a network level intrusion detection system. In *Albuquerque*, page 18. University of New Mexico.
- Hugues, J., Paris, G., Perrotin, M., and Tsiodras, T. (2008). Using MDE for the Rapid Prototyping of Space Critical Systems. *19th IEEE/IFIP International Symposium on Rapid System PrototypingI*, pages 10–16.
- Hussein, M. and Zulkernine, M. (2006). Umlintr: A uml profile for specifying intrusions. In *13th Annual IEEE International Conference and Workshop on Engineering of Computer Based Systems (ECBS 2006), 27-30 March 2006, Potsdam, Germany*, pages 279–288. IEEE Computer Society.
- Jurjens, J. (2005). *Secure Systems Development with UML*. Springer Academic Publishers. Alemanha., 1 edition.
- Karkanakov, N. (2005). Experimental analysys of client/server application in embedded systems. In *in Electronics, Sozopol, Bulgária.*, pages 21–23.
- Karkanakov, N. and Spasov, G. (2005). Adaptation of web service architecture in distributed embedded systems. In *in International Conference on Computer Systems and Technologies - CompSysTech' 2005.*, pages 1–6.

- Kawabata, C., Santana, R., Santana, M., Bruschi, S., and Branco, K. (2006a). Avaliação de desempenho em tempo de execução do protocolo de simulação distribuída cmb. In *Anais do IV Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPerformance)*, Campo Grande., pages 1–16.
- Kawabata, C., Santana, R., Santana, M., Bruschi, S., and Branco, K. (2006b). Performance evaluation of a cmb protocol. In *In Proceedings of the Winter Simulation Conference (WSC06)*. Monterey., pages 1012–1019.
- Kurose, J. F. and Ross., K. W. (2009). *Computer Networking: A Top-Down Approach*. Addison Wesley, 5 edition.
- Lima, I. (2008). Aw-kernel: Um protótipo para simulação de facilidades de distribuição de bytécodes em nível de kernel. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília*.
- Lima, I., Marques, G., and Branco, K. (2009a). Aw-kernel: A simulation prototype for distribution of bytécodes in kernel level. In *In Fourth International Conference on Computer Sciences and Convergence Information Technology.*, pages 806–811.
- Lima, I., Marques, G., and Branco, K. (2009b). Aw-kernel: Um protótipo para simulação de facilidades de distribuição de bytecode em nível de kernel. In *In: Octava Conferencia Iberoamericana en Sistemas, Cibernética e Informática: CISCi 2009, 2009, Orlando, Flórida. Anais da Octava Conferencia Iberoamericana en Sistemas, Cibernética e Informática.*, pages 1–6.
- Lucas, A., Feres, M., and Branco, K. R. L. J. C. (2006). Avaliação de desempenho do protocolo wep em redes sem fio ad hoc usando simulador de redes. In *14º Simpósio Internacional de Iniciação Científica (SIICUSP).*, page 1.
- Marconato, E. (2011). Extensão da umlintr para especificação de linguagens de ataque - geração automática de assinaturas de ataque. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília*.
- Marconato, E., Camargo, V., Martimiano, L., and Branco, K. (2007). Uma proposta de extensão da umlintr para especificação de linguagens de ataque . In *In:*

- Escola Regional de Redes de Computadores.1 ed. Santa Maria : UNIPAMPA., pages 76–115. Unipampa.*
- Marque, G. (2008). Avaliação de Índices de carga e de desempenho em ambientes paralelos distribuídos com agentes móveis. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília.*
- Marques, G. and Branco, K. (2007). Coleta de Índice de desempenho em sistemas paralelos distribuídos heterogêneos com agentes móveis - uma proposta. In *Anais do VII SIPM - Simpósio de Informática do Planalto Médio.,* pages 1–12.
- Marques, G., Sabatine, R., and Branco, K. (2008a). Analysis of scheduling techniques in distributed parallel environments using mobile agents. In *In: The Fourth International Conference on Networking and Services - ICNS.,* pages 196–101.
- Marques, G., Sabatine, R., and Branco, K. (2008b). Performance analysis of scheduling techniques in distributed parallel environments. In *In: IEEE International Conference on Industrial Technology, (ICIT 2008) Chengdu.,* pages 1–6.
- Marques, G., Sabatine, R., Nunes, F., and Branco, K. (2007). Processamento de imagens médicas em ambiente paralelo distribuído utilizando agentes móveis. In *In the II Congresso da Academia Trinacional de Ciências, Foz do Iguaçu.,* pages 1–10.
- Mesquita, P., Branco, L., and Branco, K. (2007). Conceitos básicos para desenvolvimento de aplicações de computação móvel. In *In: Escola Regional São Paulo/Oeste.,* pages 49–76. UNIVEM.
- Morony, C. S., Branco, K., and Ordonez, E. (2006). Implementação em fpgas dos algoritmos global - needleman-wunsch e local - smith-waternab de sequenciamento de genes. In *In the Proceedings da XXXII Conferencia Latinoamericana de Informática CLEI 2006. Chile.,* pages 1–10.
- Mullender, S. J. (1993). *Distributed Systems.* Addison-Wesley, 1 edition.
- NIST (2002). National institute of standards and technologies. 4D/RCS: Reference Model Architecture for Unmanned Vehicle Systems Version 2.0.

- Oliveira, A., Ordonez, E., and Branco, K. (2006a). Pers - um processador específico para redes de sensores com primitivas de segurança. In *In the Proceedings do VII Workshop em Sistemas Computacionais de Alto Desempenho (WSCAD), Ouro Preto.*, pages 1–10.
- Oliveira, A., Ordonez, E., Pereira, F., and Branco, K. (2006b). Algoritmo des e aes inseridos em um processador específico para redes de sensores. In *In the Proceedings do 8º Simpósio Segurança em Informática.*, pages 1–10.
- Osório, F., Wolf, D., and Branco, K. (2010a). Mobile robots and autonomous vehicles: Development of intelligent robots and the challenges for artificial intelligence research. In *In: XXXVIth CLEI - Latin American Informatics Conference, 2010, Asuncion, Paraguay. Tutorials: CLEI - Latin American Informatics Conference.*, pages 1–15.
- Osório, F., Wolf, D., Branco, K., and Pessin, G. (2010b). Mobile robots design and implementation: From virtual simulation to real robots. In *In: Virtual Concept, 2010, Bordeaux. Proceedings of IDMMME - Virtual Concept 2010. França : Berlin: Springer Verlag.*, pages 1–6.
- Osório, F., Wolf, D., Pessin, G., Simões, E., and Branco, K. (2009). Simulação virtual de carros em jogos e aplicações de i.a. In *Tutoriais do SBGames. Rio de Janeiro.*, pages 1–30. SBGames.
- Pigatto, D., Silva, N., and Branco, K. (2012). Performance evaluation and comparison of algorithms for elliptic curve cryptography with el-gamal based on miracl and relic libraries. *Accepted for publication Journal of Applied Computing Research (JACR).*, 1(6):1–9.
- Pigatto, D., Silva, N., Sikansi, F., and Branco, K. (2011). Aplicação de criptografia e assinatura digital para prover comunicação segura em veículos terrestres não tripulados. In *II Escola Regional de Alto Desempenho de São Paulo (ERAD-SP 2011).*, pages 1–4.

- Pires, R. M., Rodrigues, D., Branco, K., and Trindade Jr, O. (2011). Mosa - mission oriented sensor array - uma proposta. In *in the Proceedings of the XXXVII Latin-American Informatics Conference (CLEI 2011)*, pages 1–10. CLEI.
- Querino Filho, L. (2010). Proposta de um framework para escalonamento de processos em sistemas computacionais distribuídos. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília*.
- Querino Filho, L., Cagnin, M., and Branco, K. (2008). Proposta de um framework para escalonamento de processos em sistemas computacionais distribuídos. In *In: XI Mostra de Trabalhos de Informática, 2008, Maringá.*, pages 1–12.
- Raihan, M. F. and Zulkernine, M. (2005). Detecting intrusions specified in a software specification language. In *29th Annual International Computer Software and Applications Conference (COMPSAC 2005), 25-28 July 2005, Edinburgh, Scotland, UK - COMPSAC (1)*, pages 143–148. IEEE Computer Society.
- Rezende, J. F., Costa, L. H. M. K., and Rubinstein, M. G. (2005). Avaliação experimental e simulação do protocolo tcp em redes de alta velocidade. In *In: XXI Simpósio Brasileiro de Telecomunicações, 2005, Campinas. Anais do XXI Simpósio Brasileiro de Telecomunicações.*, pages 53–58. SBT'05.
- Ribeiro, L. and Branco, K. (2008). Plantar conhecimento, é fazer talentos aparentemente escondidos florescer. In *XIII Simpósio Luso-Brasileiro de Engenharia Sanitária e Ambiental.*, pages 1–4.
- Rimondini, M. (2012). Emulation of computer networks with netkit. Università degli Studi di Roma Tre. Disponível na Internet em: <http://www.netkit.org/publications/netkit-tr.pdf>. Acesso em 15 janeiro de 2012.
- Roadmap27 (2002). Osd uav roadmap 2002-2027. In *Office of the Secretary of Defense (Acquisition, Technology, and Logistics) Air Warfare*.
- Roadmap30 (2005). Unmanned aircraft systems roadmap 2005-2030. In *Headquarters, United States Air Force Washington DC*.

- Roadmap32 (2009). Unmanned systems roadmap 2007-2032. In *Office of the Secretary of Defense*.
- Roadmap34 (2009). Unmanned systems integrated roadmap fy2009-2034. In *Office of the Secretary of Defense*.
- Rodrigues, D., Estrella, J., Antunes, N., Monaco, F., Branco, K., and Vieira, M. (2012). Engineering secure web services. In *In: Valeria Cardellini; Emiliano Casalicchio; Kalinka Regina Castelo Branco; Júlio Estrella; Francisco Monaco. (Org.). Performance and Dependability in Service Computing: Concepts, Techniques and Research Directions.*, pages 360–380. USA: IGI Global.
- Rodrigues, D., Estrella, J., and Branco, K. (2010). Segurança computacional no desenvolvimento de web services. In *In: Simone das Graças Domingues Prado. (Org.). VII Escola Regional de Informática - São Paulo/Oeste.*, pages 59–82. Bauru.
- Rodrigues, D., Estrella, J., and Branco, K. (2011a). Analysis of security and performance aspects in service-oriented architectures. *International Journal of Security and Its Applications.*, 5:13–30.
- Rodrigues, D., Estrella, J., and Branco, K. (2011b). Desempenho de algoritmos criptográficos em web services utilizando ws-security. In *in the Proceedings of the 17th Brazilian Symposium on Multimedia and the Web (WebMedia)*, pages 182–189. SBC.
- Rodrigues, D., Estrella, J., Pigatto, D., and Branco, K. (2011c). Performance evaluation of security techniques in web services. In *International Conference on Information Integration and Web-based Applications & Services.*, pages 270–277. ACM.
- Rodrigues, D., Estrella, J., Vieira, M., Camargo Jr, J., Branco, K., and Trindade Jr, O. (2011d). Using soa in critical-embedded systems. In *14th IEEE International Conferences on Cyber, Physical and Social Computing (CPSCoM 2011)*, pages 733–738.
- Rodrigues, D., Pires, R., Estrella, J., Vieira, M., Correa, M., Camargo JR, J., Branco, K., and Trindade Jr, O. (2011e). Application of soa in safety-critical embedded

systems. *Communications in Computer and Information Science (Print)*., 206:345–354.

Rodrigues, D. Estrella, J. and Branco, K. (2010). Performance in soa environment. In *In the proceedings of the ICHIT-2010 - International Conference on Convergence and Hybrid Information Technology, Daejeon. (to appear)*, pages 1–8.

Sabatine, R., Saito, P., Nunes, F., and Branco, K. (2007). Utilização da computação paralela distribuída na otimização do processamento de imagens médicas. In *In: Workshop em Sistemas Computacionais de Alto Desempenho - WSCAD CTIC.*, pages 1–6.

Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007a). Abordagem utilizando mpijava para a paralelização de algoritmos de processamento de imagens médicas. In *In: Workshop em Sistemas Computacionais de Alto Desempenho - WSCAD CTIC.*, pages 1–6.

Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007b). Otimização de algoritmos de processamento de imagens médicas utilizando a computação paralela. In *In Anais do VI Simpósio de informática da Região Centro - SIRC.*, pages 1–12.

Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007c). Otimização do processamento de imagens médicas: Uma abordagem utilizando java. In *In Anais do III Workshop de Visão Computacional.*, pages 1–10.

Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007d). Otimização do processamento de imagens médicas utilizando a computação paralela. In *In Anais da 6ª Conferência Iberoamericana en Sistemas, Cibernética e Informática: CИСCI 2007.*, pages 165–170.

Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007e). Processamento de imagens médicas: Otimização no tempo de execução usando computação paralela distribuída. In *Anais do III Simpósio de Instrumentação e Imagens Médicas.*, pages 1–6.

- Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2007f). Uso da computação paralela distribuída para melhoria no tempo de processamento de imagens médicas. In *Anais da XIV Escola Regional de Informática do Paraná - ERI-PR.*, pages 36–47.
- Saito, P., Sabatine, R., Nunes, F., and Branco, K. (2008). Otimização de algoritmos de processamento de imagens médicas utilizando a computação paralela. *Revista Disciplinarum Scientia. Série Ciências Naturais e Tecnológicas*, 7(1):11–23.
- Saito, P., Sabatine, R., Wolf, D., and Branco, K. (2009a). Parallel implementation of mobile robotic self-localization. In *International Conference on Convergence and Hybrid Information Technology ICHIT 2009, 2009, Daejeon, Korea. ACM Proceedings.*, pages 390–396.
- Saito, P., Sabatine, R., Wolf, D., Mendonça, B., and Branco, K. (2009b). A parallel approach for mobile robotic self-localization. In *Fourth International Conference on Computer Sciences and Convergence Information Technology.*, pages 762–767.
- Saito, P. T. and Branco, K. (2009). Modelo de paralelismo para processamento de imagens médicas. *REGRAD - Revista Eletrônica de Graduação UNIVEM.*, 1(1):35–47.
- Schoaba, V. (2008). Addimo assinatura digital para dispositivos móveis. In *Dissertação - Mestrado em Ciências da Computação - Centro Universitário Eurípides de Marília.*
- Schoaba, V., Sikansi, F., Pigatto, D., Branco, L., and Branco, K. (2010). Disimod digital signature for mobile devices. In *In the proceedings of the ICHIT-2010 - International Conference on Convergence and Hybrid Information Technology, Daejeon. (to appear)*, pages 1–8.
- Schoaba, V., Sikansi, F., Pigatto, D., Branco, L., and Branco, K. (2011). Digital signature for mobile devices: a new implementation and evaluation. *IJFGCN- International Journal of Future Generation Communication and Networking.*, 4(2):23–36.

- Shirazi, B., Hurson, A., and Kavi, K. (1995). Introduction to scheduling and load balancing. introdução do primeiro capítulo do livro scheduling and load balancing in parallel and distributed systems. In *IEEE Computer Society, CA, p.2-6, USA*, pages 2–6. Press, Los Alamitos.
- Shivaratri, N. G., Krueger, P., and Singhal, M. (1992). Load distributing for locally distributed systems. In *IEEE Computer*, pages 33–44. IEEE.
- Sikansi, F. E. G. and Branco, K. R. L. J. C. (2010). Sistema de pagamento utilizando um dispositivo móvel através de assinatura digital. In *18º Simpósio Internacional de Iniciação Científica (SIICUSP)*., page 1.
- Sikansi, F. E. G., Pigatto, D. F., and Branco, K. (2011). Assinatura digital para comunicação segura em veículos terrestres não tripulados (vtnt). In *19º Simpósio Internacional de Iniciação Científica (SIICUSP)*., page 1.
- Souza, P., Hitoshi, F., Santana, M., Santana, R., Bruschi, S., and Branco, K. (2011). Applying the heterogeneity level metric in a distributed platform. *INFOCOMP - Journal of Computer Science (UFLA. Impresso)*., 10:17–25.
- Tanenbaum, A. S. (1995). *Distributed Operating Systems*. Prentice-Hall, International Inc., New Jersey, 1 edition.
- Tanenbaum, A. S. (2001). *Modern Operating Systems*. Upper Saddle River, New Jersey: Prentice-Hall, Inc., 2 edition.
- Tanenbaum, A. S. (2003). *Sistemas Operacionais Modernos*. Edition, Bookman., 4 edition.
- Thramboulidis, K. C., Doukas, G. S., and Koumoutsos, G. V. (2008). A soa-based embedded systems development environment for industrial automation. *EU-RASIP J. Emb. Sys.*, 2008.
- Trindade Jr, O., Branco, K., Neris, L., and Chavier, L. (2012). Robôs aéreos. In : *Robótica Móvel - Editora: LTC. Autores-organizadores: Roseli Aparecida Francelin Romero/ICMC-USP, Fernando Santos Osório/ICMC-USP, Denis Fernando Wolf/ICMC-USP, Edson Prestes e Silva Junior/UFRGS.*, pages 461–478. LTC.

- Trindade Jr, O., Neris, L. O., Barbosa, L., and Branco, K. (2010). A layered approach to design autopilots. In *In: IEEE-ICIT 2010 International Conference on Industrial Technology, 2010, Viña del Mar.*, pages 1395–1400. IEEE.
- Trindade Jr, O., Braga, R., Neris, L., and Branco, K. (2009). Uma metodologia para desenvolvimento de sistemas embarcados críticos com vistas a certificação. In *In: IX Simpósio de Automação Inteligente - IX SBAI, 2009, Brasília. Anais do IX Simósio de automação inteligente IX SBAI.*, pages 1–6.
- Valavanis, K. (2007). Advances in unmanned aerial vehicles: State of the art and the road to autonomy. In *International Series on Intelligent Systems, Control, And Automation: Science And Engineering, Volume 33.*
- Vanni, R., Moreira, E., and Branco, K. (2010). Information for handover management in heterogeneous networks: Data representation, languages and integrated platforms. In *In: International Conference on Information Systems and Technology Management, CONTECSI'2010*, pages 3173–3185.
- VINT (2012). Virtual internetwork testbed - disponível na internet em. <http://www.isi.edu/nsnam/vint/> , acesso em 15 janeiro de 2012.
- Xu, C. and Lau, F. (1997). *Load Balancing in Parallel Computers: Theory and Practice.* Kluwer Academic Publishers, Boston, USA, 1 edition.
- Zhang, W., Cao, J., Zhong, Y., Liu, L., and Wu, C. (2010). Fuzzy allocation of fine-grained compute resources for grid data streaming applications. *IJGHPC*, 2(4):1–11.