Concepção, Desenvolvimento e Análise de um Sistema de Gerência de Segurança para Redes de Telecomunicações

RESUMO: Gerência de Segurança contra fraudes e intrusões será um dos principais tópicos de investigação nas próximas gerações de sistemas distribuídos. Um sistema seguro (*secure*) provê proteção contra erros de usuários não confiáveis, enquanto um sistema correto (*safe*) provê proteção contra erros de usuários confiáveis. Este trabalho propõe uma metodologia para o desenvolvimento de gerência segura e correta, em sistemas distribuídos em geral, e em sistemas de comunicação sem fio em particular. Inicialmente, apresenta-se a especificação e validação formal do sistema distribuído de segurança para provar sua correção. Então, descreve-se como técnicas neurais podem ser empregadas na gerência de segurança de redes de telecomunicações sem fio, contra fraudadores que utilizam telefones clonados ou habilitados impropriamente. Os resultados indicam que com a taxa de erro de 2,5% obtida na classificação dos usuários de telecomunicações é possível reduzir significativamente as perdas das companhias telefônicas em vários milhões de dólares. Em acréscimo, apresenta-se como a arquitetura CORBA pode ser usada para suportar e elevar a segurança do sistema. Na implementação realizada, o sistema garante controle de acesso, autenticação, confidencialidade, integridade, disponibilidade e não-repúdio – e tem também a capacidade de informar as companhias telefônicas e as vítimas tão logo o sistema detecta uma fraude. Essa automática e imediata notificação, ao contrário da espera até a emissão da conta telefônica mensal, ajuda a reduzir os prejuízos das companhias e usuários. Finalmente, como uma derivação desta pesquisa, foi desenvolvida uma aplicação para disponibilizar com segurança, via Web, a conta telefônica constantemente atualizada, e dessa forma os próprios usuários tornam-se aptos para detectar e minimizar fraudes. A parceria com uma empresa de telecomunicações[1], que disponibilizou sua base de dados, foi fundamental na obtenção dos resultados por esta investigação científica.

ABSTRACT: *Safety and security management against frauds and intrusions will be one of the major issues in the next distributed systems generations. A secure system provides protection against errors of untrusted users, while a safe system provides protection against errors of trusted users. This thesis proposes a methodology for the development of a secure and safe management in distributed systems in general, and wireless communication systems in particular. Initially, a formal specification and validation of the distributed security system is presented in order to prove it correctness. Then, it is described on how neural techniques can be employed in the security management of wireless networks against intruders that use mobile phones cloned and subscribed improperly. The results indicate that the 2.5 error rate obtained in the classification of telecommunication users, it is possible to reduce significantly the telecom carrier' losses to several millions dollars. Furthermore, it is showed how CORBA architecture can be used to support and enhance the security of the system. In the implementation, the system guarantees access control, authentication, confidentiality, integrity, availability and non-repudiation – and has also the capability to inform the telecom carrier and the victims as soon as the system detects a fraud. This automatic and immediate notification, instead of waiting until the end of monthly bill cycle, will help to reduce loses to the carrier and users. Finally, as an outgrowth of this research a secure application has been developed for On-Line Phone Bill via the Web-server, and in this manner, the users also became able to detect and minimize frauds. The partnership with a telecommunication company[1], that provided its data base, it was decisive to get the results by this academic investigation.*

1 Introdução

"Safety and Security are two reliable properties of a system. A 'safe' system provides protection against errors of trusted users, while a 'secure' system protects against errors introduced by untrusted users." (Alexander, 1998)

Esta pesquisa científica é motivada pelas necessidades decorrentes do rápido crescimento das redes sem fio (*wireless*)[2] e da telefonia móvel (*mobile*)[3]. A telefonia móvel irá provocar importantes mudanças no cotidiano das pessoas; no entanto, tais mudanças somente serão viáveis quando os usuários estiverem confiantes sobre a segurança das redes sem fio. A demanda crescente por serviços seguros e de alto desempenho disponíveis via aparelhos celulares com acesso global, tais como pesquisas na Internet, comércio eletrônico e vídeo-conferência, constitui a principal tendência da próxima geração de redes móveis.

Vive-se em um mundo onde não existem fronteiras. Gerência (Aidarous, 1998; Sloman, 1994) de segurança (Dowd, 1998; Stallings, 1995; Rozemblit, 1999; Pfleeger, 1997) contra intrusões (Denning, 1987; Stillerman, 1999) e fraudes (Notare, 1999) em telefonia móvel (Gibson, 1996; Riezenman, 2000) representa uma das principais questões pertinentes à próxima geração de redes sem fio[4] (Prasad, 1999; Calhoun, 1999; Chaudhury, 1999; Lu, 1999). Assim, em vez de ignorar as preocupações dos usuários quanto à segurança, as empresas de telecomunicações devem identificar esses problemas e tratá-los de em uma maneira direta e objetiva (Shaw, 1999). Em acréscimo, com o objetivo de convencer os usuários a utilizar essa nova tecnologia, as empresas de telecomunicações devem esclarecer como conseguiram equacionar a segurança dos seus sistemas móveis.

As indústrias e empresas provedoras de serviços que conseguirem visualizar essa mudança e concentrar seus esforços sobre a segurança das redes sem fio e Internet serão bastante beneficiadas – e podem ser as únicas a sobreviver. Atualmente, as

[1] Telefônica Celular/RS.

[2] O IEEE 802.11 (Nee, 1999) é o padrão para redes locais sem fio (*Wireless Local Area Networks – WLANs*). O objetivo desse padrão é oferecer um modelo de operação a fim de resolver as questões de incompatibilidade entre fabricantes de equipamentos WLAN.

[3] Em julho de 1999 foi atingido o número de 10.000.000 de aparelhos vendidos no Brasil, sendo que a média de venda nos últimos 6 meses foi de um celular a cada 6 segundos no Brasil. Em 1990 eram apenas 40.000 aparelhos – 1 para cada 2.000 pessoas. Hoje existem 7 aparelhos para cada 100 brasileiros e nos Estados Unidos são 23 aparelhos para cada grupo de 100 habitantes (revista *Veja*, 14/07/99, p. 42-43). Segundo o jornal *Diário Catarinense* (03/01/2000, p. 3), a telefonia celular vai crescer 80% no Brasil no ano 2000. Serão 27 milhões de celulares, o que pelas previsões oficiais só seria atingido em 2003.

[4] Telefones celulares analógicos constituem a primeira geração; digitais, a segunda. A terceira é marcada pela convergência com a Internet, incluindo alta velocidade de acesso sem fio, de 384Kbps a 54Mbps. Atualmente os celulares digitais transmitem dados a velocidades em torno de 14,4Kbps (FREITAS, L. E-tudo: the Web connection. *Varig Inflight Magazine*, n.133, p.54-122, nov. 1999.).

empresas de telecomunicações estão tendo grande prejuízo[5] em virtude da carência de soluções eficientes na gerência de segurança contra fraudes na telefonia móvel. Considerando a previsão para o ano de 2003 de um aumento de 70% sobre as atuais perdas[6] causadas por fraudes em telefones móveis, esta pesquisa demonstra uma metodologia para a gerência segura, correta e interoperável como solução eficiente para esse problema.

1.1 Fraudes de Clonagem e de Habilitação em Telefonia Móvel

Antes de os telefones móveis tornarem-se largamente utilizados, a maior ameaça para a segurança de uma rede, na maioria das organizações, eram as linhas discadas. Embora essas linhas ainda demandem atenção, o risco que oferecem são menores quando comparadas com as conexões sem fio. Para romper a segurança de um sistema sem fio, é necessário apenas utilizar um equipamento de rádio portátil, também conhecido como *scanner*. Com esse equipamento é possível registrar as freqüências de telefones celulares que estão operando em áreas próximas (em torno de 100 metros) e programar outros telefones para realizar chamadas nas freqüências capturadas, de modo que as chamadas sejam debitadas nas contas telefônicas dos proprietários que tiveram as freqüências captadas.

No entanto, à medida que essas fraudes técnicas (leia-se clonagem) tornam-se mais difíceis devido às novas tecnologias dos aparelhos digitais, os esforços voltam-se para fraudar o processo de habilitação de telefones celulares, que é independente de tecnologia, seja analógica, seja digital. Esse tipo de fraude, que ocorre no momento da habilitação, é favorecida pelas facilidades que as operadoras oferecem para os usuários assinarem seus serviços telefônicos – de modo que as habilitações são realizadas em nome de terceiros, que não irão pagar pelas chamadas, alegando desconhecê-las[7]. Na **fraude de habilitação**, também conhecida como fraude de inadimplência ou ainda de subscrição (*subscription*), o criminoso geralmente utiliza o nome de outra pessoa para assinar o serviço de telefonia celular. Esse serviço é utilizado até ser desativado por falta de pagamento (geralmente 30 dias após o início da habilitação do serviço)[8]. Dessa forma, um fraudador pode utilizar um celular diferente a cada mês, cada um em nome de um assinante diferente. Mas provavelmente todos esses aparelhos terão um padrão de chamadas em comum. É importante salientar que não existe *hardware* capaz de impedir ou minimizar tal fraude. A **fraude de clonagem** envolve a cobrança de chamadas de clones na conta de um assinante legítimo através do uso indevido dos códigos referentes ao Número Serial Eletrônico (*Electronic Serial Number – ESM*) e ao Número de Identificação do Celular (*Mobile Identification Number – MIN*) capturados do aparelho original quando deste é feita uma chamada. Cada telefone celular é único, e portanto possui códigos ESN e MIN distintos. O código ESN é definido pelo fabricante e o MIN é programado pelo provedor do serviço telefônico. Para ser inicializada uma chamada, o telefone transmite ambos os códigos – ESN e MIN – quando a tecla "enviar" (*send*) é pressionada. A clonagem ocorre pela captura, nas ondas aéreas, dos códigos MIN e ESN de um aparelho de um assinante legal, seguida pela transferência desses códigos para outro telefone celular (i.e., o clone). O celular falso provoca a rede a considerar que este é o telefone do assinante em vez de uma unidade clonada. Com isso, a cobrança das chamadas feitas através telefone clonado irão ser adicionadas na fatura telefônica do assinante legal. O exemplo típico é o do impostor que atua com um *scanner* em um *shopping center* capturando as informações dos telefones celulares em utilização. O impostor pode então transferir as informações capturadas para vários telefones, produzindo assim diversos clones[9]. Embora a clonagem dos novos telefones D-AMPS (*digital*), GSM (*Global Systems for Mobile Communications*), IS-95 ou IS-136 (*Interim Standard*) seja muito mais complexa devido aos razoáveis mecanismos de autenticação, ainda é muito fácil clonar um telefone AMPD (*Advanced Mobile Phone System*), como apresentado na Figura 1.1. Os tradicionais telefones celulares analógicos (i.e., sistemas AMPS) são muito vulneráveis a fraudes. Na verdade, com o número serial de 32 bits e o número telefônico de 34 bits, a conversa realizada na área de uma célula pode ser facilmente rastreada por um receptor. Soluções associadas à segurança serão incluídas na próxima geração de redes sem fio, proporcionadas pelo *hardware* digital. Porém, mais do que dificultar a clonagem através de novos equipamentos digitais, vários outros métodos de prevenção devem ser instaurados, já que fraudes tais como o uso de nome de terceiros na habilitação não podem ser impedidas ou minimizadas via *hardware*. Nesse contexto, novas ferramentas para a detecção de fraudes, tais como redes neurais, são armas que devem ser usadas em uma guerra já deflagrada.

Este trabalho, a partir de uma metodologia no escopo da gerência de segurança de redes sem fio, investiga o uso da tecnologia de redes neurais como uma das ferramentas para combater este desafiante problema de fraudes na telefonia móvel.

---

[5] Segundo o IDC (www2.uol.com.br/info/infonews/091999/) mais de meio milhão de dólares diários; segundo a indústria de celular Bell Atlantic (www.ba.com/nr/96/feb/2-29cellfraud.html), uma perda de um milhão e meio de dólares diários apenas nos EUA. No Brasil, os crimes de clonagem e subscrição já atingiram 2% do faturamento anual das empresas (revista *Veja*, 08/10/97, p. 86).

[6] O que irá representar 57 milhões de dólares apenas nos Estados Unidos, segundo o IDC (<www2.uol.com.br/info/infonews/091999/>).

[7] Em acréscimo a esses dois tipos de fraudes (isto é, clonagem e habilitação), ainda é possível comentar sobre um terceiro tipo denominado *tumbling fraud*. Nesse caso, um celular "criminoso" reprograma aleatoriamente seu número telefônico ou Número Serial Eletrônico (ESN) após cada chamada, tirando proveito do processo de validação de chamadas que ocorre quando um usuário realiza sua primeira chamada fora da área para a qual o telefone foi habilitado.

[9] Podem existir alguns indícios que um assinante de telefone celular pode identificar para detectar o uso fraudulento do seu celular em antecipação a uma empresa de telefonia: ligações freqüentes de números telefônicos errados para o telefone do proprietário original; quedas de conexão; dificuldade em efetuar chamadas; existência de chamadas que constantemente recebem sinal de ocupado e números errados (seria importante questionar aqueles que lhe telefonam freqüentemente para saber se existe alguma dificuldade em efetuar uma ligação para o seu número telefônico); e a existência de chamadas indevidas que possam aparecer na sua conta telefônica. Certamente esses itens fornecidos pela AT&T não garantem a segurança da rede, e em acréscimo, é importante enfatizar que a responsabilidade da segurança da rede não é do usuário (que está pagando pelo serviço), mas da empresa telefônica que deve fornecer um serviço seguro.

1.2 Trabalhos Relacionados

Existem estratégias distintas através das quais é tratado o problema das fraudes nas telecomunicações móveis: (*i*) criptografia; (*ii*) bloqueio; (*iii*) verificação de usuário; e (*iv*) análise de tráfego (Stewart, 1999). Nesta seção, são discutidos prós e contras de cada um destes esquemas de prevenção e detecção de fraudes.

(i) Criptografia: Uma das formas para prevenir fraudes, a criptografia, apresenta dois benefícios principais: dificultar que criminosos detectem os pares de código ESN/MIN e prevenir o sistema contra a escuta clandestina. A criptografia consiste em transformar uma mensagem legível (*plaintext*) em uma mensagem codificada e não legível (*ciphertext*) para só então transmiti-la. Além de uma chave (*shared key)*, a criptografia utiliza um algoritmo para codificar (*encryption algorithm*) e um algoritmo para decodificar (*decryption algorithm*) a mensagem (Stallings, 1995). Embora é simples incluir criptografia nos celulares digitais, nos analógicos são extremamente caros e difíceis de criptografar. Por isso, a criptografia ainda não pode ser considerada uma solução eficaz. Em acréscimo, telefones digitais (GSM) já foram clonados através da quebra da criptografia (em abril de 1998, Universidade da Califórnia)[10]. Outro obstáculo para a adoção de criptografia consiste na oposição do Escritório Norte-Americano de Investigação Federal (*Federal Bureau of Investigation – FBI*) e da Agência Norte-Americana de Segurança (*National Security Agency – NSA*). Estas agências temem que, se for permitido o uso de criptografia, criminosos poderão codificar as ligações telefônicas dos mesmos. Tal medida impossibilitaria que o FBI e a NSA realizassem escutas em chamadas telefônicas suspeitas. Embora essa estratégia seja uma boa contribuição para sistemas mais seguros, ela não é aplicável em aparelhos analógicos e nem em fraudes de habilitação.

(ii) Bloqueio: Com o objetivo de proteção, algumas operadoras bloqueiam usuários de risco a realizarem alguns tipos de chamadas. A venda de telefones celulares também pode ser restrita, isto é, somente os clientes que comprovarem renda poderão adquirir um aparelho. Entretanto, se a companhia dificultar a assinatura ou chamadas de clientes potenciais, esta não estará somente perdendo clientes mas também a concorrência e possivelmente seu lugar no mercado. O bloqueio de chamadas internacionais é uma estratégia em que a companhia perde muitas possíveis chamadas, e conseqüentemente lucros. A *TIM TELESC* é um exemplo de companhia que utiliza a estratégia de bloqueio das chamadas internacionais de todos os seus clientes[11]. O bloqueio (leia-se não-disponibilidade de serviço) não chega a ser uma solução para a gerência de segurança, mas uma alternativa para sistemas sem segurança.

(iii) Verificação de Usuário: Várias empresas já desenvolveram mecanismos para a verificação de usuário. A *Nynex Mobile* e a *Cellular One* foram as empresas que iniciaram a investigação sobre o uso de Números de Identificação Pessoal (*Personal Identification Numbers – PIN*). De acordo com a *Nynex*[12], o dispositivo de senha é a ferramenta mais eficiente disponível no momento. De janeiro a setembro de 1995, o uso de senhas reduziu a fraude em mais de 80% nos mercados analisados. Além de este valor de 80% não corresponder a um eficiente resultado, este trabalho considera que o usuário não pode ser imbuído de mais senhas. Pelo contrário, o usuário merece um serviço seguro em retorno ao que está sendo pago.

(iv) Análise de Tráfego: Análise de trafego começa a ser utilizada para detectar padrões de chamadas suspeitas, tais como o aumento repentino da duração das chamadas e o aumento de chamadas internacionais, e também para determinar se é fisicamente possível um assinante efetuar uma chamada no local corrente em relação ao local e horário da última chamada. No entanto, na maioria das companhias, tais como a *Tele Centro Sul*, apenas faturas de valores elevados são investigadas, sem considerar, por exemplo, que um usuário já possui um padrão de chamadas internacionais para determinado número em determinado horário, tendo apenas aumentado a duração das mesmas. Este procedimento é muito pouco eficiente na detecção de fraudes. Em acréscimo, em muitos casos, as chamadas só são analisadas após a emissão da fatura mensal, quando as perdas já serão muito grandes. Outro aspecto muito negativo nesse contexto é o grande número de funcionários necessários para analisar as contas telefônicas de valores elevados e contatar os usuários. Como relatado por um representante da *Bell Atlantic*, em 90% dos casos a operadora local irá notificar o cliente antes do bloqueio do seu número[11]. Esta pesquisa acredita que o número de 90% não representa o melhor resultado e que o atraso em informar os clientes pode provocar profundas perdas para os clientes e para as companhias. Dessa maneira, tal porcentagem necessita ser aumentada, principalmente a partir da utilização de um método automático e imediato de avisar os clientes (sem a necessidade do grande número de funcionários), para somente após bloquear o serviço.

1.3 Proposta e Principais Contribuições

Com a crescente popularidade das redes móveis e com as rápidas mudanças na indústria de telecomunicações sem fio, a preocupação com a segurança dos usuários de equipamentos celulares deveria ser muito maior. Este trabalho propõe uma gerência de segurança em sistemas distribuídos em geral (Simon, 1996) e em sistemas de comunicação sem fio em particular (Lu, 1999; Riezenman, 2000). A gerência de segurança proposta é validada em um sistema de detecção do uso inadequado de operações de telefones celulares através de análise de tráfego, em que os usuários são classificados em grupos de acordo com seus padrões de utilização do aparelho[13] (Notare, 1998).

A classificação dos usuários em grupos realizada através do emprego de redes neurais ajuda o sistema a identificar quando chamadas não correspondem aos padrões do usuário deste telefone, constituindo um possível clone; bem como identificar o padrão de um usuário como muito similar a um padrão de um antigo inadimplente, constituindo um usuário que habilita um

---

[10] VEJA. Segredo Fácil: Hackers provam que celulares digitais podem ser clonados. p. 81, 22 abr. 1998.

[11] Todos os assinantes desta companhia necessitam solicitar o desbloqueio para utilizar o serviço. Em acréscimo, não são avisados da não-disponiblidade deste serviço pelo qual pagam.

[12] <http://www.craftsreport.com/april96/cellularfraud.html>.

[13] As informações sobre os usuários utilizadas para a classificação dos mesmos continuam sigilosas para o usuário e para a companhia. O que difere neste trabalho é o conhecimento prévio destas informações, ou seja, não apenas no término do ciclo mensal quando da impressão da conta telefônica.

celular com a prévia intenção de não pagar pelos serviços, satisfazendo-se em usá-lo apenas até ser desabilitado por falta de pagamento – geralmente o aparelho é comprado em nome de terceiros. Assim, quando uma ligação telefônica realizada por um telefone legal ou clonado é concluída, o sistema verifica se as características da chamada está dentro dos padrões do usuário (características estas armazenadas previamente em um arquivo de padrões), e também se a chamada é fisicamente possível[14]. Uma mensagem automática (economizando gastos da companhia com pessoal) é enviada ao cliente assim que uma possível fraude de clonagem seja detectada. No caso da fraude de habilitação, o sistema identifica um padrão similar a um antigo inadimplente e então investiga para certificar-se da identidade de quem está utilizando o aparelho, ou seja, se é quem realmente diz ser. Essa imediata notificação e investigação, ao contrário da espera até a emissão da fatura no final do mês, ajuda na redução dos prejuízos da companhia, bem como na eliminação dos danos que podem ser repassados para os clientes como, associá-los a criminosos. Além do gerenciamento contra as fraudes de clonagem e de habilitação a partir das companhias, este trabalho também oferece uma aplicação disponível via Web, onde os usuários de telecomunicações podem observar suas contas telefônicas constantemente atualizadas, o que permite que o próprio usuário detecte e minimize fraudes associadas à clonagem. O sistema engloba os serviços de controle de aceso, autenticação, confidencialidade, integridade, disponibilidade e não-repúdio de comunicação. Esses serviços de segurança são implementados em Java com suporte CORBA, e incluem mecanismos tais como assinatura e certificado digital, que são muito importantes mas ainda negligenciados por empresas como bancos e companhias de cartão de crédito[15]. E como importante característica o sistema é validado formalmente a partir das especificações de serviço e de protocolo, de acordo com o padrão ISO 8807.

Neste escopo, a solução proposta para a gerência de segurança de sistemas distribuídos engloba principalmente três tecnologias: (1) redes neurais, para o reconhecimento de padrões de uso da telefonia móvel; (2) CORBA, para a distribuição segura de agentes e gerente; e (3) LOTOS, para a especificação e validação formal, com o objetivo de provar a correção do sistema. Mais especificamente, este trabalho visa:

(1) propor uma metodologia para a gerência de segurança, segura e correta, de sistemas distribuídos, aplicá-la em um sistema de segurança para telecomunicações móveis (leia-se pesquisa aplicada e transferência de tecnologia) e sugerir pesquisas onde esta metodologia possa ser aplicada;
(2) oferecer um paradigma para a especificação e verificação formal, de acordo com o padrão ISO 8807, a fim de validar sistemas de segurança distribuídos e garantir matematicamente sua correção, com o objetivo de atingir o nível máximo de segurança caracterizado pelo Departamento de Defesa dos Estados Unidos;
(3) descrever a implementação de como o CORBA e seu módulo de segurança pode ser usado para suportar, manter e proteger sistemas de segurança distribuídos, neste caso um sistema para telefonia móvel, onde a comunicação entre agentes e gerente é realizada de maneira segura. Para garantir a segurança e a privacidade do usuário, foi mostrado como o módulo de segurança oferecido por Java/Web pode contribuir no sistema distribuído, em que a comunicação entre usuários e servidor incorpora os principais mecanismos de segurança;
(4) propor e conceber um serviço de alarme imediato e automático, para contatar, informar e confirmar a existência de uma clone diretamente com o usuário (vítima da fraude). Este serviço é similar aos atuais serviços de "despertador automático", em que as mensagens são recebidas e enviadas sem a necessidade da presença de um funcionário, e dessa forma viabilizar o sistema também economicamente;
(5) investigar e desenvolver os sistemas SSCC e SIPI contra fraudes na comunicação móvel (i.e., clonagem e habilitação), que através do emprego de redes neurais monitora e identifica fraudadores. A escolha correta das características e do algoritmo de classificação é decisiva na eficiência da detecção das fraudes, contribuindo para a redução dos prejuízos das companhias telefônicas e dos usuários; e
(6) conceber e desenvolver o sistema SETWeb, que permite aos usuários (previamente cadastrados) observarem suas contas telefônicas, constantemente atualizadas, via Web. O SETWeb garante a segurança do cliente, quando este acessa sua conta telefônica, através de mecanismos implementados sobre as tecnologias Java e CORBA. A principal característica do SETWeb é possibilitar que os próprios usuários detectem, rapidamente, a existência de ligações telefônicas ilícitas na sua conta telefônica, i.e., detectem ligações realizadas por clones de seu aparelho celular (principalmente via Web, mas também via telefone, similarmente ao sistema "hora certa").

Embora recentemente exista um grande interesse no desenvolvimento de telefones celulares dotados de novas tecnologias em *hardware*[16], que tornam muito mais difíceis a clonagem, muito pouco trabalho está sendo eficaz em termos de *software*. Em acréscimo, fraudes de habilitação não podem ser evitadas por *hardware*. A metodologia proposta neste trabalho é uma solução para ambas – fraudes de clonagem e fraudes de habilitação. Veja a seguir uma visão geral do sistema de gerência de segurança SSTCC[17] – Sistema de Segurança para Telecomunicações Contra Clonagem e Inadimplência (que engloba os sistemas SSCC – Sistema de Segurança Contra Clonagem de Celulares, SIPI – Sistema de Identificação de Prováveis Inadimplentes e SETWeb – Sistema de Extrato Telefônico via Web). Em resumo, o módulo Adaptador lê as ligações *on-line* (do arquivo *Call Detailed Register*); o módulo Agente monitora e detecta possíveis fraudes

[14] Por exemplo, duas ligações de um mesmo usuário realizadas em um intervalo de 5 minutos e que partiram de localidades distantes 500 Km revelam a existência de um clone, pois uma destas ligações é fisicamente impossível de ter sido realizada pelo mesmo aparelho.
[15] Importantes bancos e companhias de cartões de crédito disponibilizam serviços via Web sobre protocolos para segurança, tais como SSL (*Secure Socket Layer*) e SET (*Secure Electronic Transaction*); porém não exigem a certificação digital – a garantia para o usuário de que está acessando o *site* correto.
[16] Como, por exemplo, a tecnologia *Boot Block Flash* utilizada pela *Intel Corporation*, que codifica o ESN.
[17] SSTCC® - Este programa (*software*), bem como sua marca, encontra-se protegido contra utilização não autorizada, total ou parcial, conforme a Lei 9.609 de 19/02/1998, regulamentada pelo Decreto 2.556 de 20/04/1998, c/c Lei 9.610 de 19/02/1998, estando devidamente registrado no INPI sob o nº 99001177, ficando os infratores sujeitos às sanções cíveis e penais previstas nos respectivos diplomas legais.

(utilizando técnicas neurais); e o módulo Gerente recebe notificações do módulo Agente e envia alarmes automáticos e imediatos aos usuários (por telefone e por correio) no caso da fraude de clonagem e investiga prováveis futuros inadimplentes no caso da fraude de habilitação. Em acréscimo, a possibilidade de observar a conta telefônica através da Web (conta telefônica constantemente atualizada) permite que o próprio usuário identifique clones de seu aparelho. A demonstração da metodologia proposta detalhando o desenvolvimento de cada componente do sistema distribuído de segurança é o objeto deste trabalho.

1.4 Organização deste Trabalho

Este trabalho está organizado como segue. A Seção 2 descreve o uso do padrão ISO 8807, com a finalidade de especificar e validar formalmente o sistema. A Seção 3 demonstra como as técnicas de redes neurais podem ser utilizadas para classificação de informações de acordo com padrões específicos dos usuários de telecomunicações. A Seção 4 apresenta a implementação do sistema distribuído de segurança e mostra como os componentes de segurança CORBA e Java podem suportar, manter e enriquecer a segurança do sistema. A Seção 5 discute os resultados obtidos, conclusões e futuros trabalhos.

2 Especificação e Validação Formal (ISO 8807)

"To our knowledge, the formality of trusted systems systems designed to substitute formal proof of security in place of experimental satisfaction has to date found little place on the Web. We know of no Web use of formal evaluation criteria such as those in the US Defense Department's Orange Book." (Rubin, 1998)

Esta Seção 2 oferece um paradigma para a especificação e validação formal de sistemas distribuídos. A Técnica de Descrição Formal (TDF) utilizada é o padrão ISO 8807 – LOTOS: *Language of Temporal Ordering Specification* (Brinksma, 1988). O principal objetivo do emprego desta técnica de alto rigor matemático é prover a prova formal de correção do sistema. O Sistema de Segurança para Telecomunicações Contra Clonagem e Inadimplência (SSTCC), já apresentado informalmente na Seção 1.3, é agora especificado formalmente, com a utilização de uma abordagem de refinamentos sucessivos (Vissers, 1988), a qual permite que o sistema seja validado ao longo do seu desenvolvimento – e não somente após a obtenção da especificação final. A validação do sistema emprega a ferramenta Eucalyptus ToolSet 2.3 (Garavel, 1997) em ambiente Sun Solaris 2.6.

2.1 A Técnica de Descrição Formal LOTOS

Para especificar rigorosamente sistemas distribuídos é conveniente utilizar técnicas de descrição formal a fim de prover maior confiabilidade a tais sistemas, geralmente complexos. As linguagens de especificação formal são baseadas em teorias matemáticas e estão associadas a métodos de especificação precisos e não ambíguos. Técnicas de Descrição Formal (TDFs) servem para definir os aspectos de comportamento e também os aspectos de dados de sistemas (Pires, 1994; Queiroz, 1994).

LOTOS (Brinksma, 1988) e ESTELLE (*Extended Finite-State Machine Language*) são TDFs normalizadas pela ISO (*International Organization for Standardization*), enquanto SDL (*Specification and Description Language*) é uma TDF normalizada pelo ITU-TS (*International Telecommunications Union – Telecommunication Standardization Sector*). A metodologia proposta neste trabalho optou por LOTOS, pois, principalmente: (1) enquanto SDL e ESTELLE são baseadas em linguagens de programação (Chill e Pascal, respectivamente), LOTOS é independente de linguagem de programação; (2) existem ótimas ferramentas para a validação de especificações LOTOS, tais como o CADP (*Caesar/Aldebaran Development Package*); (3) LOTOS é um padrão internacional (ISO 8807); e (4) o nível de abstração é uma das mais importantes características para o desenvolvimento de sistemas. LOTOS apresenta, além do elevado nível de abstração, outras características inerentes às TDF como o poder de expressão e a estruturação de especificações (Queiroz, 1994). LOTOS é uma TDF que reúne duas álgebras: a primeira álgebra é utilizada para a descrição de aspectos de comportamento e corresponde a uma extensão de Cálculo de Sistemas Comunicantes (*Calculus of Communicating Systems – CCS*) (Milner, 1980); a segunda álgebra é utilizada para a descrição dos aspectos de dados e corresponde à linguagem *ACT ONE* (Ehrig, 1985). Em LOTOS Básico (isto é, a parte de *LOTOS* que representa apenas os aspectos de comportamento dos sistemas) uma especificação é constituída por uma hierarquia de definições de processos.

2.2 Especificação de Serviço do SSTCC

Inicialmente, no nível mais alto de abstração, o sistema SSTCC[18] pode ser visto como uma caixa preta, dotada de quatro portas de comunicação (porta `mail_alarm`, porta `phone_alarm`, porta `online_bill` e porta `check_owner`), para a troca de mensagens com os usuários de uma dada companhia telefônica. Veja a Figura 2.1.

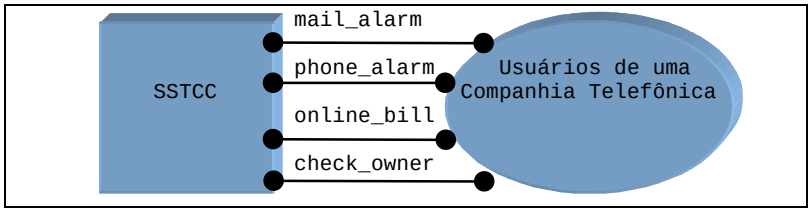


FIGURA 2.1 – REPRESENTAÇÃO GRÁFICA DO SSTCC.

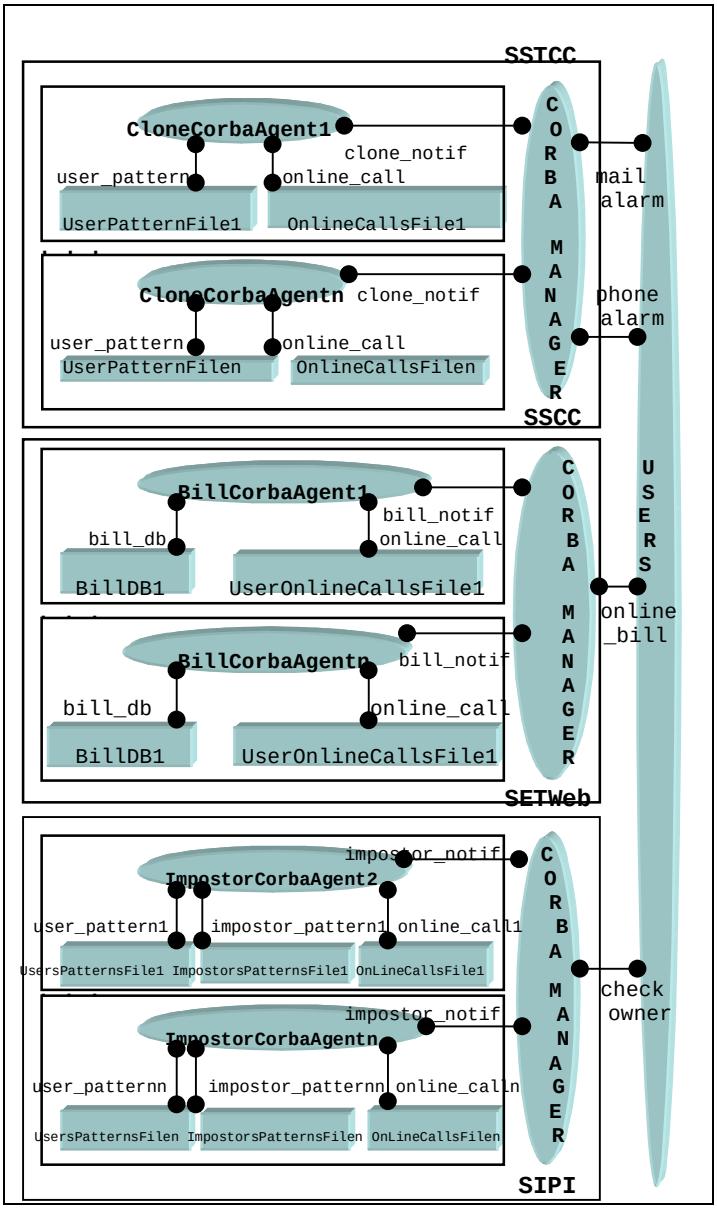
[18] Sistema de Segurança Contra Clonagem e Inadimplência.

A porta `mail_alarm` é utilizada para que o SSTCC envie alarmes de suspeita de existência de clones, diretamente ao usuário, pelo correio comum. Já a porta `phone_alarm` permite que o SSTCC empregue o telefone celular para esta finalidade. O envio de alarmes através do celular tem, como maior vantagem, o tempo; enquanto que o envio de denúncias pelo correio tem, como maior vantagem, a segurança. A porta `online_bill` é utilizada para que a companhia telefônica possa disponibilizar aos seus usuários a conta mensal atualizada on-line. Finalmente, a porta `check_owner` é utilizada pela companhia telefônica para investigar suspeitas de prováveis inadimplentes. O sistema SSTCC fica permanentemente ativo, o que caracteriza um comportamento infinito desse sistema. Esse comportamento sugere uma especificação LOTOS com funcionalidade `noexit`. Veja a Figura 2.2.

```
Specification SstccService[mail_alarm,phone_alarm,online_bill,check_owner]:noexit
behaviour SstccService[mail_alarm,phone_alarm,online_bill,check_owner]  where
process SstccService[mail_alarm,phone_alarm,online_bill,check_owner]:noexit:=
(i;mail_alarm; (phone_alarm;SstccService[mail_alarm,phone_alarm,online_bill,check_owner]
     [] SstccService[mail_alarm,phone_alarm,online_bill,check_owner]))
[](online_bill;SstccService[mail_alarm,phone_alarm,online_bill,check_owner])
[](check_owner;SstccService[mail_alarm,phone_alarm,online_bill,check_owner])
endproc
endspec
```

FIGURA 2.2 – ESPECIFICAÇÃO LOTOS DO SSTCC.

FIGURA 2.3 – ARQUITETURA GERAL DO SSTCC.



O comportamento do sistema SSTCC é definido pelo processo `SstccService`, o qual pode executar uma ação na porta `mail_alarm`, para o envio de uma denúncia pelo correio comum (considera-se que essa ação é sempre possível). Em seguida, tem-se uma escolha indeterminística com duas opções. A primeira opção indica o envio de uma denúncia pelo telefone celular, através de uma ação na porta `phone_alarm` (admite-se que essa ação nem sempre é possível), e, em seguida, o processo `SstccService` é chamado, recursivamente, para poder transmitir outra opção. Esta outra opção, por sua vez, trata a situação na qual não foi possível enviar a denúncia pelo telefone celular (por motivo de defeito do aparelho, por estar fora de área, por estar desligado ou por ser chamado em horário inadequado, por exemplo). Dessa forma, após algum tempo de espera, ocorre uma ação interna `i` (não-observável) e o processo `SstccService` é chamado recursivamente. A especificação mais abstrata do sistema SSTCC corresponde a uma formalização dos requisitos dos usuários (serviço) desse sistema. Ela serve de base para os refinamentos posteriores da concepção do SSTCC, ao longo do projeto. E é utilizada na prova de correção da especificação final do sistema (as duas especificações devem ser equivalentes quanto à observação – *observational equivalence)*.

2.3 Especificações de Protocolo do SSTCC

O sistema SSTCC, já representado no nível mais alto de abstração na Seção 2.3, pode agora, pela especificação `SstccProtocol`, ser detalhado de modo a considerar seus três subsistemas ou componentes: (1) SSCC – Sistema de Segurança Contra Clonagem de Celular, representado pelo processo `SsccClone`; (2) SETWeb – Sistema de Extrato Telefônico via Web, representado pelo processo `SetwebBill`; e (3) SIPI – Sistema de Identificação de Prováveis Inadimplentes, representado pelo processo

`SipiImpostor`. A arquitetura geral do sistema SSTCC, incluindo os três principais processos refinados que o compõem pode ser observada na Figura 2.3. Ao longo desses refinamentos apresentados, o sistema pode ser constantemente validado através do emprego de ferramentas apropriadas (Garavel, 1997) – não sendo necessário, portanto, obter a especificação final para dar início aos procedimentos de validação. Na seção 2.4, a seguir, são apresentados os procedimentos de validação.

2.4 Validação Formal de Sistemas

"À partir d'une représentation d'un système sous forme d'automate, il est possible d'observer et de vérifier certaines propriétés de ce système, telles que la présence de situations de blocage" (Arnold, 1989). Uma das grandes vantagens do uso de TDFs é a possibilidade de demonstrar a correção de uma especificação. O termo "validação" pode ser usado para descrever as atividades de demonstração de correção, ou apenas aumento de confiabilidade, de uma especificação ou implementação. Enquanto teste e simulação são úteis para encontrar erros, verificação fornece a prova formal de correção do sistema.

2.5 Experimentos na Validação Formal do Sistema SSTCC

EUCALYPTUS reúne um conjunto de ferramentas em uma interface gráfica. A principal ferramenta utilizada por este trabalho é a CADP (*Caesar/Aldebaran Development Package*), que possui dois principais componentes: (i) CAESAR; e (ii) ALDEBARAN. (i) CAESAR: CAESAR é um compilador que traduz uma especificação LOTOS em um programa C (para ser executado ou simulado) ou em um LTS (para ser verificado utilizando ferramentas de bissimulação e/ou de lógica temporal). Por exemplo, é possível comparar o LTS de um protocolo com o LTS do serviço implementado pelo protocolo. Ambos LTSs são gerados utilizando CAESAR e comparados utilizando ALDEBARAN. (ii) ALDEBARAN: ALDEBARAN é uma ferramenta para verificação de sistemas de comunicação, representados por Sistemas de Transições Rotuladas (LTS), i.e., as transições de estados são rotuladas por nomes de ações. Isso permite a redução de LTSs sob várias relações de equivalência (tais como bissimulação forte, equivalência quanto à observação, bissimulação de retardo e equivalência segura). Os algoritmos de verificação utilizados pelo ALDEBARAN são baseados em estudos, principalmente de Paige-Tarjan and Fernandez-Mounier (Garavel, 1997).

Para a obtenção da prova formal de correção do sistema, inicialmente gera-se o LTS (*Labelled Transition System*) correspondente à especificação de protocolo do arquivo `sttcProtocol.lotos`. A Figura 2.35 mostra que o LTS gerado, correspondente à especificação LOTOS `SstccProtocol` LOTOS, possui 194.401 estados e 1.645.926 transições. Similarmente, gera-se o LTS associado à especificação `SstccService.lotos`. A Figura 2.43 mostra que o LTS associado à especificação de serviço contém somente 3 estados e 6 transições.

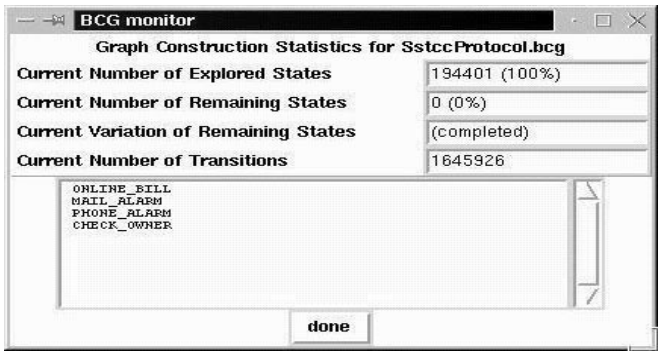


FIGURA 2.35 - LTS - SSTCCPROTOCOL.

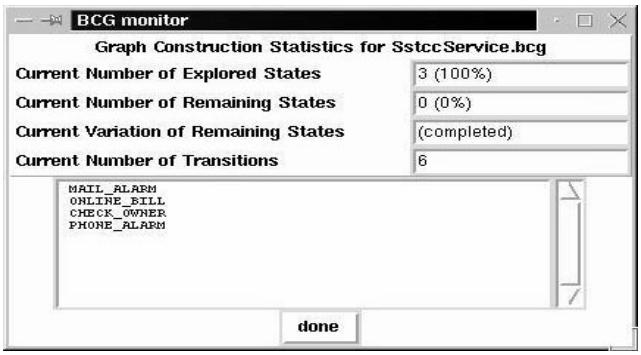


FIGURA 2.43 – LTS - SSTCCSERVICE.

Então é possível comparar o LTS que representa o protocolo com o LTS que representa o serviço esperado. O resultado obtido, TRUE, significa que o protocolo executa o serviço esperado. Note que o processo de validação é considerado composto por simulações, testes e verificações. Enquanto as simulações e os testes são utilizados apenas para encontrar erros, a verificação proporciona a obtenção da prova formal (matemática) de correção do sistema. Essa prova visa satisfazer os requisitos do nível máximo de segurança de acordo com o Departamento de Defesa do EUA. Veja a Tabela 2.1.

TABELA 2.1 – NÍVEIS DE SEGURANÇA – DEPARTAMENTO DE DEFESA DOS EUA.

Nível de segurança	Principal característica introduzida
Division D	*Minimal protection* – proteção mínima.
Division C	*Discretionary protection* – proteção discreta.
Division B	*Mandatory protection* – proteção obrigatória.
Division A	*Verified protection* – proteção verificada.
Class A1	*Verified design* – projeto verificado. Análise formal e prova matemática de que o sistema de computação casa com a política de segurança do sistema e suas especificações de projeto. Distribuição confiável que garante a segurança do sistema.

Dessa maneira, a metodologia de análise formal e a prova matemática apresentada nesta Seção 2 visam garantir o projeto verificado, em conformidade com o mais alto nível de segurança (*ClassA1*) apresentado na Tabela 2.1.

2.6 Resultados

O uso da Técnica de Descrição Formal LOTOS (ISO 8807) mostrou-se de grande eficiência e eficácia no desenvolvimento do sistema, garantindo a segurança de um padrão que possui rigor matemático para a especificação e ainda grande poder de análise e projeto de sistemas distribuídos complexos. Através de ferramentas como a Eucalyptus[19], as especificações puderam ser validadas ao longo dos seus refinamentos, i.e., desde a especificação mais abstrata até a mais refinada do sistema. Das formas de validação, i.e., simulações, testes e verificações, atenção especial foi dada às verificações, pois, enquanto simulações e testes têm (apenas) a finalidade de encontrar erros, as verificações vão além, provendo prova formal de correção do sistema. O procedimento utilizado para obter a prova de correção entre os refinamentos da especificação foi a geração de sistemas de transições rotuladas (LTS), tanto da (1) especificação mais abstrata `SstccService`, associada ao serviço requerido, quanto da (2) especificação mais refinada `SstccProtocol`, associada ao protocolo obtido. A prova formal de correção obtida, de acordo com o padrão ISO 8807, visa garantir o nível máximo (*ClassA1*) da Tabela de Segurança do Departamento de Defesa dos EUA descrita no *Orange Book* (Simon, 1996).

Como trabalhos futuros, pretende-se continuar os refinamentos da especificação de protocolo do sistema de modo a agregar os tipos abstratos de dados. Dessa maneira, o código C gerado automaticamente a partir das especificações LOTOS poderá contribuir ainda mais substancialmente em rapidez e segurança nas atividades de implementação.

3 Detecção de Intrusão com Redes Neurais Artificiais

"The classificator efficience is directly proportionally to the object characteristics choosed. A good classification performance requires the selection of effective characteristics and also a classificator that make a well use of these characteristics – considering limited treinee data and computational resources. Training the network successfully involves many choices and training experiments. From these experiments, the developer learns which configurations train the network most successfully for the application in hand. The developer is thus an architect for a neural network." (Dayhoff, 1990)

Esta Seção 3 apresenta a gerência de segurança para detecção de intrusão (Denning, 1987; Lunt, 1988; Lunt, 1989) e fraudes (Stewart, 1999) em redes de telecomunicações móveis (Gibson, 1996) com a utilização de redes neurais artificiais (Barreto, 1997) para o reconhecimento de padrões (Duda, 1973; Lippmann, 1989; Hush, 1993) dos usuários. Dois classificadores de padrões (algoritmos) são investigados: Kohonen, não-supervisionado (Kohonen, 1982) e Funções de Base Radial, supervisionado (Todesco, 1995). O principal objetivo do emprego da técnica de reconhecimento de padrões neste trabalho é detectar fraudes em telecomunicações móveis (clonagem e inadimplência) já no seu início (i.e., nas primeiras chamadas ilegais e não apenas quando a fatura mensal for emitida), e dessa forma minimizar os prejuízos. Esta Seção 3 apresenta como o Sistema de Segurança para Telecomunicações Contra Clonagem e Inadimplência (SSTCC) reconhece os padrões de cada usuário de telecomunicações e, também, como detecta rapidamente as chamadas fora dos padrões de cada usuário. A implementação dos algoritmos de redes neurais artificiais (Kohonen e RBF) é realizada através do emprego das ferramentas MatLab 5.2.1 (MatLab, 1992) e ToolBox (Demuth, 1998) em ambiente Windows, com equipamento PentiumII.

3.1 Modelo Neural

Devido a sua aplicabilidade, tem havido grande interesse dos pesquisadores em relação às Redes Neurais (*Artificial Neural Networks – ANN*). Este campo tem tido grande crescimento nas indústrias de computação e sistemas de telecomunicações de grande porte. Redes neurais são redes essencialmente interconectadas paralelamente e uma de suas mais relevantes propriedades é a possibilidade de aprendizagem. Redes Neurais estimam uma função sem requerer uma descrição matemática da funcionalidade da saída da rede em relação à entrada: elas aprendem por exemplos. Pelo aprendizado, uma rede neural pode descobrir padrões e a relação entre eles, e organizá-los para realizar associações. Como conseqüência, elas são amplamente utilizadas para resolver problemas de classificação. Redes neurais (Dayhoff, 1990), quando vistas como uma rede adaptativa, podem ser analisadas como uma máquina de memória distribuída que é naturalmente capaz de armazenar conhecimento experimental e colocá-lo em disponibilidade para uso. Redes neurais são similares a mente em dois aspectos: (i) o conhecimento é adquirido pela rede através de processos de aprendizagem; e (ii) os pesos das conexões entre os neurônios, conhecidos como sinapses, são armazenados como conhecimento. O procedimento utilizado para representar o processo de aprendizagem, comumente chamado de algoritmo de aprendizagem, tem a função de modificar os pesos das conexões das redes visando alcançar um objetivo projetado.

3.2 Uso de Classificador Não-Supervisionado – Kohonen

Diversos modelos de rede neural têm sido propostos com a finalidade de classificar dados de acordo com alguma relação de similaridade. Nesta Seção 3.2 emprega-se o modelo Kohonen (Kohonen, 1982; Schneider, 1999; Meyer, 1994; Ritter, 1990; Ingber, 1993) para a detecção de fraudes em telefonia móvel a partir da classificação dos usuários em grupos, de acordo com a similaridade de uso do aparelho. O modelo Kohonen provê um modelo de rede neural de organização adaptativa de mapas topológicos de características que provêem componentes importantes para sistemas de reconhecimento de padrões complexos.

3.2.1 Experimentos

O objetivo destes experimentos é mostrar de que forma as redes neurais podem ser aplicadas como ferramenta de identificação de fraudadores que utilizam telefones celulares impropriamente. E além disso, investigar particularmente o

[19] A equipe VASY (Validação de Sistemas) do INRIA-França, que desenvolveu a ferramenta CADP, participa ativamente na atualização do padrão ISO 8807. Inclusive, o editor deste padrão, Ed Brinksma, foi membro da banca de defesa de PhD de uma pesquisadora da equipe.

impacto do modelo Kohonen na performance do sistema neural de detecção de fraudes em operações de telefonia móvel. Classificar os usuários de telecomunicações em grupos tem por objetivo possibilitar que o sistema SSTCC identifique ligações telefônicas que não correspondam aos padrões de utilização de um usuário que pertença a determinado grupo. Estes experimentos visam a concepção e o desenvolvimento do modelo de redes neurais requerido, a fim de prover a melhor performance (eficiência) para aplicações específicas – neste caso, fraudes em telefonia móvel – e sugerir alguma recomendação para a futura geração de sistemas sem fio (*wireless*). Uma boa performance na classificação requer uma boa seleção de características efetivas e um classificador que faça uso dessas características de modo eficiente, considerando os dados de treinamento limitados e os recursos computacionais disponíveis. Foram selecionadas as seguintes características: (i) `caller_number` (somente para teste, não para treinamento); (ii) `called_number` (para identificar o tipo da chamada, i.e., local, internacional, etc); (iii) `time` (para classificar de acordo com as diferentes tarifas/horários durante o dia); (iv) `duration` (para identificar longas chamadas fora do padrão do usuário); e (v) `date` (para identificar os diferentes padrões durante os dias de semana e finais de semana). A fase de teste permitiu trabalhar com a sensibilidade de classificação. Pequenas alterações inseridas no conjunto de dados devem gerar – e geraram – a mesma saída (agrupamento), a fim de evitar que falsos alarmes sejam enviados. De maneira similar, grandes alterações devem resultar – e resulataram – em um diferente agrupamento para o usuário, a fim de garantir que o usuário seja avisado sobre a existência de uma fraude.

3.3 Uso de Classificador Supervisionado – RBF

Nesta Seção 3.3 é proposto o emprego do algoritmo supervisionado Função de Base Radial (*Radial Basis Function* – RBF) para o reconhecimento dos padrões dos usuários de telecomunicações (Lee, 1993). RBF é um excelente classificador e também um aproximador universal de funções (Todesco, 1995). A arquitetura da RBF consiste em uma camada de entrada, uma camada escondida e uma camada de saída. Os nós da camada de saída formam uma combinação linear e usam o classificador de tipo Kernel. A função RBF em sua camada escondida produz uma resposta para os estímulos de entrada (padrões). Quando a entrada está dentro de uma pequena região localizada no espaço de entrada, a função RBF produz uma resposta significativamente diferente de zero.

3.3.1 Experimentos Iniciais

O algoritmo para a classificação dos usuários de telecomunicações segundo seus padrões de utilização do telefone, que compreende *K-Means*, *P-NearestNeighbour* e *Gauss* (para a obtenção dos centros, variância e saída da camada escondida, respectivamente), foi implementado com os *softwares* MatLab (MatLab, 1992) e ToolBox (Demuth, 1998). Nesta Seção 3.3.1, os experimentos de classificação com o método supervisionado RBF foram realizados com o uso dos conhecidos dados de *Copenhagen*, utilizados por vários pesquisadores (Todesco, 1995) em vez de dados reais (i.e., ligações telefônicas reais, que serão utilizadas na próxima Seção 3.3.2). Esse procedimento permitiu comprovar a eficiência do algoritmo (RBF), uma vez que tais dados já foram anteriormente classificados utilizando-se outros algoritmos – e dessa forma as taxas de erro de cada algoritmo puderam ser comparadas. Tais dados foram classificados em sete tipos: 1) usuários que fazem apenas ligações locais curtas; 2) usuários que fazem muitas ligações locais; 3) usuários que fazem poucas ligações de longa distância; 4) usuários que fazem muitas ligações de longa distância; 5) usuários que fazem poucas ligações curtas internacionais; 6) usuários que fazem muitas ligações internacionais curtas; e 7) usuários que fazem muitas ligações internacionais longas. Salienta-se que a classe 2 inclui a classe 1, a classe 3 inclui a classe 2, e assim por diante. Os dados foram armazenados em quatro arquivos (A1.dat, A2.dat, B1.dat, e B2.dat), onde A1 e B1 incluem 4.061 amostras e A2 e B2 4.050 amostras. A1 é utilizado para a geração dos centros, A2 para treinar a rede, B1 para testar a rede e B2 para a gerar a taxa de erro. Cada amostra de A1 e A2 contém três características: 1) o número do telefone chamado; 2) o dia/hora da ligação; e 3) a duração da ligação. Cada amostra de A2 e B2 contém duas informações: 1) o número do telefone que fez a ligação; e 2) o padrão a que essa ligação pertence. Cada amostra nos arquivos A1 e B1 corresponde a um padrão nos arquivos A2 e B2, respectivamente. É dessa maneira que a rede aprende de forma supervisionada. Os dois conjuntos de dados (1 e 2) foram cruzados como dados de treinamento e de testes a fim de gerar a taxa de erro de classificação final. Durante os experimentos, variou-se a quantidade de neurônios da camada escondida entre 50 e 150. Um resultado muito bom, de 4,2027%, foi obtido utilizando-se 110 neurônios na camada escondida. Este resultado de 4,2025% é considerado bom, i.e., eficiente, pois, utilizando-se estes mesmos dados com outros algoritmos, a taxa de erro foi maior. Pode-se citar *Back Propagation* (PPA), *Multi-Layer Perceptrons* (MLP) e *Parametrical*, que apresentaram taxas de erro de 5,4%, 5,8%, e 6,5%, respectivamente. O resultado obtido com o classificador *Radial Basis Function* para a detecção de fraudes na telefonia móvel, considerando a taxa de erro de 4,2%, pode reduzir significativamente as perdas em milhões de dólares, conforme pode ser observado na Figura 3.1.

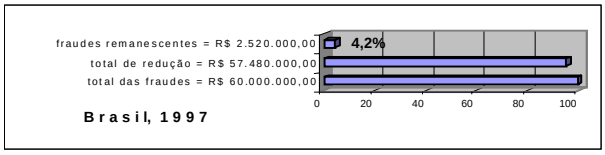


FIGURA 3.1A – REDUÇÃO DAS PERDAS (BRASIL).

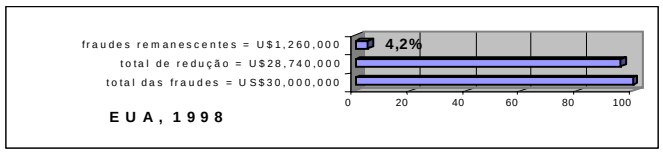


FIGURA 3.1B – REDUÇÃO DAS PERDAS (EUA).

Dessa forma, considerando as perdas no Brasil[20], em 1997, estas poderiam ser reduzidas de R$ 60.000.000,00 para R$ 2.520.000,00; e considerando as perdas nos Estados Unidos, em 1998, estas poderiam ser reduzidas de US$ 33.400.000 para US$ 1.402.800. Segundo dados do IDC[21], de setembro de 1999, atualmente as companhias perdem meio milhão de dólares por dia com esses tipos de fraudes.

[20] GONÇALVES, D.N. Olho na conta: cresce o número de vítimas de telefones celulares clonados. *Veja*, São Paulo. p. 86, 8 out.1997.

3.3.2 Experimentos Avançados

Após obter um resultado encorajador do uso da RBF com os dados de *Copenhagen* (Seção 3.3.1) – o que permitiu a comparação com outros algoritmos, nesta Seção 3.3.2 o mesmo algoritmo é utilizado agora com dados reais, ou seja, ligações de uma companhia telefônica brasileira[22]. Os usuários foram agrupados em uma ordem hierárquica crescente (do menos provável ao mais provável padrão de fraude) de acordo com o tipo de ligações que efetuam[23]: 1) local; 2) interurbana, dia/horário com desconto, curta; 3) interurbana, dia/horário sem desconto, curta; 4) interurbana, dia/horário com ou sem desconto, longa; 5) especial, dia/horário com ou sem desconto, curta; 6) especial, dia/horário com ou sem desconto, longa; 7) internacional, dia/horário com desconto, curta; 8) internacional, dia/horário sem desconto, curta; 9) internacional, dia/horário com desconto, longa; e 10) internacional, dia/horário sem desconto, longa. No menor nível (1) estão os usuários que fazem apenas ligações locais (em qualquer horário e de qualquer duração). No maior nível (10) estão os usuários que fazem inclusive ligações internacionais, em horários sem desconto e de longa duração. A taxa de erro obtida com a utilização de dados reais foi ainda melhor que quando utilizados os dados de *Copenhagen*. A taxa de erro obtida foi de 2,5%, com 80 neurônios na camada escondida. Esta taxa de erro de 2,5% foi o melhor resultado de classificação obtido por esta investigação científica.

3.4 Resultados

Se, por um lado, existe uma grande quantidade de pesquisas associadas ao *hardware* das redes de telecomunicações sem fio, ou seja, ao aparelho celular digital, tornando-o muito mais seguro contra as fraudes de clonagem, por outro lado, existem realmente poucas investigações associadas a soluções eficazes contra fraudes via *software*. Importante salientar que as fraudes associadas à habilitação (*subscription)* são independentes do *hardware* utilizado e que apenas soluções via *software* são possíveis. Esta Seção 3 apresentou uma solução via *software* para a detecção de intrusão em redes móveis. A solução consiste em um sistema que emprega redes neurais contra as fraudes de clonagem e de habilitação. Apresentou-se também a performance do sistema, que incluiu dados reais de uma companhia telefônica. Os resultados mostraram a eficácia do sistema SSTCC em identificar fraudes e, desta forma, reduzir os prejuízos das companhias telefônicas e os danos que poderiam causar aos seus clientes. Considerando a taxa de erro obtida na classificação (de 2,5% utilizando 80 neurônios na camada escondida), os atuais prejuízos de US$ 500.000 diários podem ser reduzidos para US$ 12.500 diários. O sistema de detecção e eliminação do clone tem como importante característica o monitoramento e aviso automático ao usuário. Dessa maneira, a companhia não necessita de muitos funcionários dedicados a essa atividade. O aviso ao usuário é realizado através de uma mensagem gravada do tipo "despertador automático", além do aviso que segue por correio. Os resultados indicam que o sistema reduz significativamente os prejuízos das companhias telefônicas, bem como as perdas/riscos que os (inocentes) clientes podem ter. Dessa forma, as companhias podem reduzir o preço dos seus serviços (ligações) e, por conseguinte, beneficiar os seus usuários.

Como trabalhos futuros, planeja-se investigar a performance do sistema quando as quatro características consideradas forem subdivididas; por exemplo, as ligações internacionais divididas em países e as interurbanas em estados. Essa divisão é muito importante para a detecção de inadimplentes, pois nesta fraude não se compara o atual padrão com o padrão armazenado do mesmo usuário, mas sim a similaridade do atual padrão com o dos inadimplentes anteriores – e nesse caso dez agrupamentos não são suficientes. Também pretende-se investigar a determinação do padrão do usuário on-line (a cada dez ligações do mesmo) não mais como o padrão vencedor (que mais vezes ocorre), mas sim analisando quantos padrões são diferentes do atual padrão do usuário. O objetivo desta investigação tem sua justificativa, pois, mesmo considerando que ligações fraudulentas ocorrem com maior freqüência do que as ligações do próprio usuário (o que justifica optar apenas pelo vencedor), poderia também ocorrer o seguinte: o "vencedor" ser apenas duas ligações iguais e idênticas ao padrão do usuário no meio de oito diferentes, e dessa forma uma fraude poderia não ser identificada. Mas no caso de optar pela "maioria diferente" das dez em vez do "vencedor", o sistema conseguiria considerar uma maioria (por exemplo oito) de ligações distintas e diferentes do padrão atual do usuário. Em acréscimo, planeja-se investigar os resultados de classificação utilizando outras técnicas, tais como Raciocínio Baseado em Casos (Ramos, 1999; Cruz, 1998) e ferramentas estatísticas como SPSS. Finalmente, considera-se a possibilidade de estender esse sistema para outras áreas, como a clonagem de cartões de crédito e o marketing direcionado pela determinação de padrões de consumo.

4 Implementação da Gerência de Segurança Distribuída

"The choice of CORBA and Java combined with the open Interface Definition Language Interface leads to a highly open, extensible, and distributed solution. By having a protocol-defined interface, CORBA forces the separation of an object interface and implementation from its use." (Haggerty, 1998)
"CORBA offers a useful methodology and middleware for building interoperable databases." (Dogac, 1998)

Esta Seção 4 apresenta a implementação da gerência de segurança em sistemas distribuídos através do suporte da arquitetura CORBA (OMG, 1998; Haggerty, 1998). O principal objetivo do emprego desta técnica (arquitetura de distribuição) no escopo deste trabalho é prover o máximo de segurança na comunicação entre agentes e gerente e na comunicação entre usuários e servidor Web. Para isso, diversos mecanismos são implementados em Java (Oppliger, 1999; McGraw, 1997; Naughton, 1986) a fim de garantir que a comunicação não seja interrompida, interceptada, modificada ou fabricada ilicitamente. Criptografia é um dos principais mecanismos utilizados, que juntamente com os mecanismos de

---

[21] <www2.uol.com.br/info/infonews/091999/>, <www2.uol.com.br/info/infonews/091999/>, <www.uol.com.br/idgnow/entre/entre22.htm>.
[22] Nesses experimentos são consideradas todas as ligações efetivadas pelos usuários da Telefônica Celular no Rio Grande do Sul, nos dias 01/08/99 (domingo) e 02/08/99 (segunda-feira), totalizando 4.255.973 ligações.
[23] Investigações poderão ser realizadas a fim de verificar o comportamento (performance) de um maior refinamento de grupos, isto é, classificar as ligações internacionais por continentes e as interurbanas por regiões.

assinatura e certificado digital tornam o controle de acesso e a comunicação muito mais seguros. O Sistema SSTCC é implementado em Java sobre a arquitetura CORBA, de modo a se beneficiar dos recursos de segurança oferecidos por ambas as técnicas através de uma política de segurança adequada que fornece os serviços de controle de acesso, autenticação, confidencialidade, integridade, disponibilidade e não-repúdio. A implementação do sistema é realizada através do emprego das ferramentas *Java Developer Kit JDK 1.2.1, Symantec Visual Café 3.0* e *Visibroker 3.4 for Java*.

4.1 Gerência de Segurança e Redes de Telecomunicações

Sistemas Distribuídos necessitam ser protegidos de acesso não autorizado, destruição ou modificação maliciosa e perdas acidentais de integridade de dados (Stallings, 1995). Um sistema que provê verificação, i.e., **prova matemática** é referido como um Sistema Confiável (*Trusted System*). Em um esforço para satisfazer suas próprias necessidades, e também como um serviço para a população, o Departamento de Defesa dos Estados Unidos, em 1981, estabeleceu o Centro de Computação Segura (*Computer Security Center*), dentro da Agência Nacional de Segurança (*National Security Agency* – NSA), com o objetivo de encorajar a ampla disponibilidade de Sistemas Confiáveis para Computadores (*Trusted Computer Systems*). O Centro classifica os produtos de acordo com o alcance das características de segurança que eles oferecem. Em essência, o Centro visa avaliar produtos disponíveis comercialmente em relação aos requerimentos de segurança acima apresentados (Simon, 1996). Um eficaz plano de gerência de segurança deve englobar os elementos necessários para prover os seguintes **serviços** (Dowd, 1998): 1) controle de acesso (usuários autorizados); 2) confidencialidade (informações permanecem privadas); 3) autenticação (originador da mensagem é quem diz ser); 4) não-repúdio (originador da mensagem não pode negar que a enviou); e 5) integridade (mensagem não foi modificada em trânsito). Porém, não necessariamente uma política de segurança deve prover o nível máximo de segurança; mas, sim, deve-se procurar o nível adequado de segurança para as necessidades de cada usuário e/ou aplicação de modo a também oferecer a performance e os custos mais adequados.

4.2 Implementação dos Sistemas SSCC e SIPI

Considerando que as ligações telefônicas (armazenadas em CDRs - *Call Detailed Register)* ficam distribuídas na rede telefônica e que existe um processo Agente junto a cada CDR, os processos Agentes também se encontram distribuídos. Para realizar a comunicação entre os agentes distribuídos e o Gerente (que é um módulo centralizado) emprega-se CORBA como tecnologia de objetos distribuídos (Pavlou, 1997; Dogac, 1998). O módulo Adaptador é responsável por esperar o recebimento de novas ligações que chegam a todo instante em uma central telefônica gravados nos CDRs. O módulo Agente é responsável, juntamente com a rede neural, pela detecção da possível fraude de clonagem propriamente dita. É ele quem envia para a rede neural o conjunto contendo o número especificado de chamadas lidas pelo Adaptador e é ele também quem recebe o resultado do processamento da rede neural. De posse do resultado emitido pela rede neural, verifica se o padrão calculado está de acordo com o padrão previamente definido para o usuário. Se o padrão estiver de acordo, ele entra em estado de dormência até que o Adaptador o invoque novamente. Caso contrário, envia um alerta para o Gerente (Hermida, 1999; Milioli, 1999).

A função do módulo Gerente é receber notificações dos diversos módulos Agentes e avisar o proprietário da linha sobre uma possível fraude nesta. O cliente é avisado de duas formas: 1) através de uma mensagem automática e imediata via o prórpio telefone; e 2) através de uma mensagem impressa enviada pelo correio para o endereço que consta no cadastro. Em ambos os casos o aviso tem como objetivo confirmar ou não a realização das chamadas pelo usuário. Cabe então à empresa tomar as devidas providências caso haja a confirmação da fraude por parte do cliente. Em acréscimo, o gerente disponibiliza informações de similaridade de padrões das atuais chamadas com inadimplentes anteriores. Em acréscimo, como é possível observar na Figura 4.1, os alarmes automáticos podem ser configurados[24] (Spíndola, 1999).

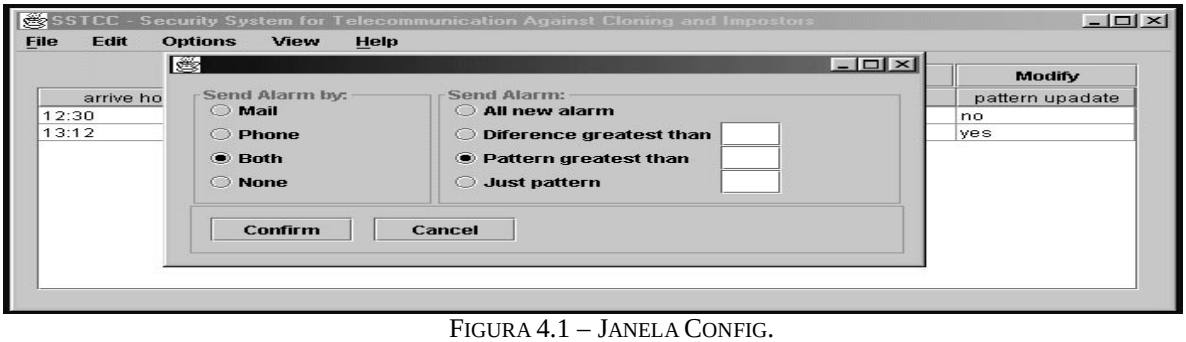


FIGURA 4.1 – JANELA CONFIG.

Ou seja, as notificações vindas do módulo Agente podem só ser enviadas automaticamente aos usuários quando a diferença de padrões (atual e novo) for maior que x; quando o padrão for maior que x; ou então somente quando o padrão for igual a x.

Além da segurança prevista na comunicação com suporte CORBA (OMG, 1998) da implementação da segurança oferecida pelas ferramentas disponíveis no JDK, o SSTCC provê ainda um esquema específico de autenticação e autorização via ORB (Désiré, 1999). Esse mecanismo de autenticação baseia-se em um pseudo-objeto do CORBA e os interceptores do

[24] Os alarmes poderão ser também enviados via fax e e-mail.

Visibroker. Esse mecanismo consiste em que o cliente (Agente), após fornecer sua identificação (*ID*/*login*) de usuário e sua senha para entrar em uma sessão de aplicação, obtenha um identificador de sessão, ou *ticket*. Esse *ticket* contém a identificação e a senha do usuário em uma forma criptografada, que juntamente com a requisição do cliente é enviado pelo ORB a cada vez que o cliente, faz uma invocação em um objeto. Quando a requisição chega ao servidor (Gerente), ela é interceptada por um interceptor e o *ticket* é checado para averiguar se o cliente tem a permissão. Em acréscimo, é de importância decisiva[25] garantir que as notificações enviadas pelos agentes cheguem ao gerente. Para garantir a disponibilidade (i.e., a não-interrupcão) das notificações, o sistema utiliza o mecanismo de *time-stamp*. Esse mecanismo consiste em um "selo de tempo" enviado de tempos em tempos pelos Agentes ao Gerente, devendo este último retornar uma confirmação (*ack*) aos Agentes correspondentes informando que receberam as notificações.

4.3 Implementação do Sistema SETWeb

O Sistema SETWeb permite que os usuários das empresas de telecomunicações verifiquem seus extratos telefônicos atualizados *on-line* durante todos os dias do mês. Isso possibilita a imediata detecção – pelos próprios usuários – de ligações indevidas que possam ocorrer por causa de fraudes de clonagem de celulares. O sistema SETWEb é composto por módulos Adaptadores distribuídos por todos os Servidores Regionais. Tais adaptadores são responsáveis por ler cada chamada registrada e disponibilizá-las em bancos de dados para que o Módulo Montador de Conta as requisite. Após uma prévia validação da identificação do usuário através da *applet*, este mostra a página gerada pelo Módulo Montador (Souza, 1999). Para a implementação dos mecanismos de segurança do Sistema SETWeb, investigou-se: 1) a segurança oferecida pelos navegadores (*browsers);* 2) os serviços de segurança da arquitetura CORBA e da linguagem Java; e 3) as facilidades para a autenticação dos clientes autorizados são disponibilizadas através de protocolos tais como SSL (*Secure Sockets Layer*), SSH (*Secure Shell*), HTTPS (*Hypertext Transfer Protocol* sobre *SSL* – um exemplo de uma extensão ao protocolo HTTP para o estabelecimento de transações WWW seguras) e o protocolo SET (*Secure Eletronic Transaction*). A gerência de permissões é feita pela ferramenta `policytool`, ou através da configuração manual do arquivo `java.policy` localizado no diretório `\jdk1.2\jre\lib\security`. No SETWeb, a mesma foi utilizada com o intuito de permitir que as informações do usuário fossem armazenadas em um BD localizado no *host* servidor, assim como permitir que o usuário, consultasse informações de sua chave privada. Para a implementação dos serviços de segurança foram utilizadas classes da linguagem Java pertencentes à API `java.security`, tais como: 1) `java.security.KeyPairGenerator`: responsável por contactar um Provedor de Serviços de Criptografia (CSP) para que o mesmo dispare o processo de criação de chaves; 2) `java.security.PrivateKey`: responsável pela criação de chaves privadas; 3) `java.security.PublicKey`: responsável pela criação de chaves públicas; 4) `java.security.Signature`: responsável por contactar um Provedor de Serviços de Criptografia (CSP) para que o mesmo dispare o processo de criação de assinaturas digitais; 5) `java.security.KeyFactory`: utilizada para instanciar uma chave pública produzida com o algoritmo DAS (Digital Signature Algorithm); e 6) `java.security.spec.X509EncodedKeySpec`: utilizada para instanciar chaves a partir de um arquivo externo, caso o usuário já possua sua chave privada. É verificada sua conformidade com o padrão X.509. Em resumo, a implementação dos mecanismos de criptografia, assinatura e certificado digital, apresentados acima, garante os serviços de controle de acesso, confidencialidade, autenticidade, integridade e não-repúdio. Investigações também foram realizadas considerando as Funções de Relatório de Alarmes de Segurança (SARF), baseadas nas recomendações estabelecidas pelo *International Telecommunication Union* (ITU). A implementação, também com suporte CORBA, tem o objetivo de proporcionar que o gerenciamento de segurança do SETWeb possa ser realizado remotamente, pela própria Web, e dessa forma o gerente responsável pela segurança do SETWeb ganha maior flexibilidade para as tarefas de gerenciamento (Borges, 1999).

4.4 Resultados

O crescimento da Internet e suas oportunidades de negócios[26] é algo que não pode ser mais ignorado. Somente nos EUA o faturamento em 1999 das atividades vinculadas à Internet foi de US$ 507 bilhões. Isso significa que as transações na rede já representam o primeiro setor da economia – o setor aéreo vem em segundo lugar com US$ 335 bilhões e a telefonia em terceiro com US$ 300 bilhões[27]. Considerando esse exemplo, pode-se facilmente imaginar a crescente necessidade de prover soluções de segurança eficientes e adequadas para tais sistemas.

Nesta Seção 4, apresentaram-se investigações de segurança na Web em três escopos distintos, i.e., (1) protocolos – associados à soluções para a camada de transporte; (2) ambiente – associado à segurança provida pelos navegadores; e (3) linguagens e arquiteturas – associadas aos recursos disponíveis por Java e CORBA. Dessa forma, a metodologia proposta neste trabalho como paradigma para o desenvolvimento de sistemas de gerência de segurança engloba diferentes serviços: (1) a autenticidade do usuário e do provedor de serviços é verificada; (2) a confidencialidade e integridade de senhas e informações é garantida, i.e., os dados trafegam de maneira confiável; (3) a disponibilidade dos serviços e informações é

[25] Neste caso, mais importante que confiabilidade, por exemplo.

[26] Os negócios eletrônicos entre empresas irão dobrar a cada 12 meses nos próximos 5 anos. O valor negociado entre companhias, que foi de US$ 43 bilhões em 1998, deve atingir US$ 1,3 trilhão em 2003. Uma justificativa para esse crescimento é o valor da transação. Pode-se citar como exemplo que a compensação de um cheque em uma agência custa em torno de US$ 1,08; por telefone cai para a metade desse valor; por computador em sistemas do tipo *home banking* custa US$ 0,26; enquanto que pela Internet o custo fica em apenas US$ 0,13 [Freitas]. Segundo o jornal Doário Catarinense de 09/04/2000, página 19, a previsão é que os negócios com comércio eletrônico devam atingir US$ 8,3 bilhões em 2003 apenas na América Latina (em 1999 foram movimentados US$ 194 milhões). Nos EUA, o maior mercado de comércio eletrônico, a previsão é de que ultrapasse os US$ 184 bilhões em 2004 (em 1999 foram US$ 20 bilhões).

[27] DIÁRIO CATARINENSE. Crescimento da Internet nos Estados Unidos. out.1999.

garantida; (4) o não-repúdio é impedido, ou seja, o usuário e o provedor de serviços não podem desmentir o fato de participarem do processo de consulta, se tiverem participado; e (5) o controle de acesso é implementado, inclusive de forma a facilitar mecanismos futuros de auditoria.

A implementação de segurança foi distinta em relação aos módulos do sistema. No caso da implementação dos Sistemas SSCC e SIPI, por exemplo, mecanismos para a prevenção de interrupção na comunicação entre agentes e gerente (envio de notificações) são de maior importância do que mecanismos de confidencialidade. Já no caso da implementação do Sistema SETWeb, a importância maior está nos mecanismos de autenticação e confidencialidade no acesso às contas telefônicas pelos usuários do que na interrupção deste serviço. Em acréscimo, a política de segurança adotada prevê um nível de segurança maior para os usuários quando acessam suas contas telefônicas do que quando os mesmos acessam informações gerais, tais como valores de tarifas no servidor Web da companhia telefônica. Também, observou-se uma melhor performance na implementação desses mecanismos de segurança quando implementados em uma máquina diferente daquela onde está o servidor Web. As soluções de segurança implementadas para autenticação e autorização utilizam o CORBA para o envio de identificação e senha dos usuários, de forma criptografada. Em acréscimo, especificamente para o sistema SETWEb, como solução para o controle de acesso dos usuários que não possuem JVM com as classes CORBA (ainda a maioria), utiliza-se essencialmente a segurança provida pelo JDK 1.2 através das ferramentas `policytool` e `keytool`. A segurança implementada no sistema SETWeb oferece assinatura e certificado digital. Enquanto a maioria dos sites de comércio eletrônico (inclusive bancos) atualmente disponíveis requer mecanismos para assinatura digital (a fim de que os sites comprovem que o usuário é quem diz ser), pouquíssimos sites requerem mecanismos para certificado digital (a fim de que os usuários tenham a certeza de que estão acessando o site que pensam ser). Para exemplificar o perigo que pode ser a falta de um mecanismo de certificação digital, considere que um usuário digite como endereço do seu banco <http://www.bancodobrasil.com.br> (endereço errado) em vez de <http://www.bancobrasil.com.br> (endereço correto). Imagine, também, que um fraudador fez uma réplica (aliás, muito fácil de ser feita) das informações da página verdadeira na página falsa. O usuário, inocentemente, coloca sua identificação e senha na tela inicial. Grande e desagradável surpresa será descobrir posteriormente que uma *applet* acaba de transferir todo o saldo da sua conta para uma outra. E a preocupação relacionada à segurança na Web (WWW) é cada vez maior, pois a cada dia agregam-se mais usuários e mais tecnologias. Pode-se citar como uma nova tecnologia o MMM[28] (Modo de Mídia Móvel), em que a Internet é acessada pelo próprio aparelho de telefone celular. Essa tecnologia está sendo lançada pela empresa Nokia[29], da Finlândia, país onde sete em cada dez habitantes têm telefone celular. Nokia, Motorola, Samsung e IBM criaram o Protocolo para Aplicações Sem Fio (*Wireless Application Protocol – WAP*), um padrão para a comunicação entre portáteis digitais. É a terceira geração[30], em que os telefones multimídia integram Internet, TV e pager. Em acréscimo, Ericsson, IBM, Nokia, Intel e Toshiba criaram em 1998 um sistema de radiotransmissão[31] que possibilita que o celular abra o portão de casa, receba mensagens da secretária eletrônica e acenda as luzes. Definitivamente, a terceira geração só terá sucesso se provida de forte segurança.

Como trabalhos futuros, pretende-se atualizar o sistema de acordo com a nova numeração de DDD (com número da operadora e complementar o SETWeb com a telefonia móvel que agregou o algarismo 9 em todos os números). Em acréscimo, implementar o mecanismo de mensagens automáticas (para enviar os alarmes ao usuários via telefone), o que só será possível quando o sistema for implantado em uma companhia telefônica. Atualmente ela é realizada com uma simulação através dos recursos multimídia dos computadores. Finalmente, em conformidade com o padrão WAP da terceira geração de telefonia móvel, disponibilizar a conta telefônica *on-line* no próprio aparelho – incluindo opção de pagamento.

5 Conclusão e Futuros Trabalhos

"Network security: it's time to take it seriously." (Dowd, 1998)

Futuros avanços na gerência de segurança de redes são necessários para que as promessas das telecomunicações móveis sejam cumpridas. Telefones móveis irão alterar para sempre muitos aspectos de nossas vidas, mas não enquanto os usuários potenciais não se convencerem da segurança das redes sem fio. Fraudes de telefones celulares têm recebido grande atenção recentemente devido aos prejuízos que as companhias telefônicas têm acumulado ultimamente.

Embora avanços têm sido feitos em *hardware*, em que a clonagem de celulares que utilizam tecnologias tais como GSM é muito mais difícil dos que utilizam AMPS (apesar de a tecnologia digital GSM também já ter sido clonada), poucos resultados eficazes têm sido obtidos em *software*. Além disso, os *softwares* atuais (i) não são rápidos e eficientes na detecção de alteração dos padrões dos usuários e não dispõem de mecanismos automáticos para avisar os clientes sobre impostores que estejam fraudando seus telefones móveis, necessitando, dessa forma, de uma grande quantidade de funcionários para realizar a tarefa de avisar os clientes; (ii) não oferecem detecção de fraudes de habilitação (*subscription*), pois não reconhecem o padrão de utilização do telefone em relação a inadimplentes existentes; e (iii) utilizam apenas "satisfação experimental" (*experimental satisfaction*) para garantir a correção do sistema de segurança. Em acréscimo, alguns sistemas oferecem a visualização da conta telefônica via Web, porém apenas no final de cada mês, quando as ligações ilícitas que podem ser verificadas já terão produzido um grande prejuízo.

[28] MMM é um trocadilho com WWW de ponta-cabeça.
[29] Nokia é o nome de um rio no interior da Finlândia.
[30] A primeira foi a geração dos analógicos; e a segunda, a dos digitais.
[31] Realizado por um chip chamado *Bluetooth* que envia ondas eletromagnéticas por uma saída de infravermelho. A propósito, o nome é uma homenagem a um chefe viking que unificou tribos inimigas na Dinamarca no Século IX.

5.1 Sumário das Contribuições

Considerando as cinco áreas de gerência de redes, i.e., configuração, falhas, performance, contabilização e segurança, esta última não tem recebido a atenção devida. Com o aumento da popularidade da telefonia móvel (*mobile communication*) e das transações comerciais eletrônicas (*e-commerce*), é chegada a hora de reconhecer as necessidades de segurança dos usuários potenciais e de tratá-las de maneira honesta. Os resultados apresentados neste trabalho validam a eficiência da metodologia proposta para o gerenciamento seguro e correto de sistemas distribuídos em geral e de redes de comunicação sem fio (*wireless communication*) em particular. As contribuições deste trabalho associadas à gerência de segurança em sistemas distribuídos, às redes de comunicação sem fio e às fraudes de clonagem e de habilitação na telefonia móvel estão sumarizadas a seguir.

(1) uma metodologia que reúne três tecnologias (LOTOS, Redes Neurais e CORBA) para a gerência de segurança segura, correta e interoperável de sistemas distribuídos, com validação demonstrada através do desenvolvimento de um sistema de segurança para telecomunicações móveis;

(2) um modelo para a obtenção da prova formal de correção de sistemas distribuídos, com o objetivo de atingir o nível de segurança *ClassA1* do *Orange Book* (ao contrário dos atuais métodos não formais de verificação de correção de sistemas);

(3) uma implementação CORBA/Java para suportar a segurança e a privacidade na comunicação entre agentes e gerente de sistemas distribuídos e Internet (considerando os serviços de segurança de controle de acesso, autenticação, confidencialidade, integridade, disponibilidade e não-repúdio);

(4) um serviço de aviso automático e imediato para obter a confirmação das fraudes suspeitas. A vantagem de o aviso ser automático é a economia da empresa com pessoal; e a vantagem de ser imediato é a economia, com a significativa redução nos valores das fraudes;

(5) um sistema eficaz contra fraudes de clonagem e habilitação na comunicação móvel que detecta intrusões através do emprego de redes neurais. Os resultados obtidos mostram que, usando 80 neurônios na camada intermediária da rede, foi obtida uma taxa de erro de classificação muito boa (2,5%), e dessa forma o sistema pode contribuir significativamente para a redução das perdas das companhias telefônicas em vários milhões de dólares; e

(6) um sistema provido de assinatura e certificação digital, em que os usuários ao longo do mês podem acessar suas contas telefônicas via Web, o que permite que monitorem e detectem por si próprios a existência de clones de seu aparelho.

Os resultados obtidos por esta investigação científica indicam que o sistema de gerência de segurança (concebido de acordo com a metodologia de desenvolvimento de sistemas distribuídos proposta e com a cooperação entre universidade e empresa) provê um serviço inovador que auxilia fortemente os usuários de telecomunicações móveis contra os danos que podem sofrer, quer seja danos econômicos (terem que pagar por chamadas que não fizeram), quer seja danos morais (serem envolvidos com pessoas e/ou negócios de que não tenham conhecimento). Em acréscimo, os resultados demonstram que o sistema de segurança SSTCC reduz significativamente os prejuízos das companhias telefônicas, que por sua vez podem oferecer serviços mais baratos para toda a população.

Em acréscimo às contribuições técnico-científicas apresentadas anteriormente na Seção 5.1, nos três anos de doutoramento (março97-março00) foram obtidas 3 publicações em livro/periódico/edição, 8 publicações IEEE, 16 internacionais, 5 SBT/SBC, 58 nacionais, 4 relatórios de pesquisa CNPq, 3 prêmios e 52 citações.

5.2 Futuros Trabalhos

Esta pesquisa técnico-científica oferece várias sugestões para futuras investigações, como pode ser observado a seguir:

(1) empregar a metodologia proposta em outras aplicações distribuídas, tais como a clonagem de cartões de crédito e a divulgação direcionada de produtos e serviços (*marketing* direcionado). Tais aplicações, assim como as fraudes na telefonia, também são distribuídas, necessitam de forte segurança e são baseadas em reconhecimento de padrões dos usuários. Em acréscimo, estender a implementação de notificação de fraude aos usuários para além dos atuais avisos por celular e por correio, de forma a possibilitar também os avisos por fax e correio eletrônico (*e-mail*), como forma de agregar ainda mais segurança ao sistema;

(2) incorporar os tipos abstratos de dados nas especificações LOTOS, de modo que o código C gerado automaticamente a partir dessas especificações LOTOS possa contribuir ainda mais com segurança e rapidez de implementação;

(3) investigar e desenvolver novos algoritmos de classificação, além de subdividir as características consideradas (i.e., dividir "ligações internacionais" e "ligações interurbanas" por regiões) visando reduzir ainda mais a taxa de erro obtida nesta pesquisa. Investigações também podem considerar Raciocínio Baseado em Casos (*Case Base Reasonic*) e métodos estatísticos nas tarefas de classificação;

(4) alterar a interface entre o Agente Java/CORBA e a Rede Neural/MatLab, atualmente via arquivo ASCII. Ou seja, obter melhor performance do sistema ao utilizar o MCC (*MatLab Compiler Command*) para traduzir o programa MatLab para C/Java e então inseri-lo no código do Agente;

(5) atualizar o sistema de acordo com as modificações realizadas recentemente no sistema de telecomunicações brasileiro, i.e., as alterações no DDD (Discagem Direta à Distância) com opção de escolha da operadora, e também o acréscimo de um dígito na numeração dos celulares; e

(6) implantar o sistema em companhias telefônicas, inicialmente na companhia telefônica brasileira que colabora com este trabalho, de modo a possibilitar a implementação efetiva do aviso automático aos usuários (somente possível neste ambiente), e em acréscimo possibilitar a análise da performance do sistema em ambiente real.

Considera-se que estas linhas de investigações sugeridas são importantes contribuições no escopo desta pesquisa científica.

Referências Bibliográficas

"Que a busca pelo novo continue movendo o mundo." Albert Einstein

AIDAROUS, S., PLEVYAK, T. *Telecommunications network management*: technologies and implementations. Piscataway, NJ, USA : IEEE Press, 1998. 352 p.

ALEXANDER, D. S., ARBAUGH, W.A., KEROMYTIS, A.D., SMITH, J.M. Safety and security of programmable networks infrastructures, *IEEE Communications Magazine*, New York, v.36, n.10, p.84-92, out.1998.

ARNOLD, A. Systèmes de transitions finis et sémantique des processus communicants. In: TECHNIQUE et science informatiques. Université Bordeaux, 1989, p.193-216.

BARRADAS, O. Você e as telecomunicações. *Telebrasil* – Associação Brasileira de Telecomunicações. Rio de Janeiro, RJ: Editora Interciência, 1995. 277p.

BARRETO, J.M. *Inteligência artificial no limiar do século XXI*. Florianópolis: Duplic, 1997.

BORGES, P. R. *Gerenciamento de um serviço de extrato telefônico na internet por funções de relatório de alarmes de segurança*. Florianópolis, 1999. Projeto de Conclusão de Curso (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Universidade Federal de Santa Catarina.

BRINKSMA, E. *ISO 8807*: LOTOS (Language of Temporal Ordering Specifications), 1988.

CALHOUN, G. *Third generation wireless communications*: post shannon architectures. Norwood, MA, USA : Artech House Publishers, 1999. 300p. ISBN 1-58053- 043-5.

CHAUDHURY, P., MOHR, W., ONOE, S. The 3GPP proposal for IMT-2000. *IEEE Communications Magazine*, New York, v.37, n.12, p.72-81, dez.1999.

CHEN, G., RIXON, J., KONG, Q. Integration CORBA and Java for ATM connection management. In: IEEE DSOM'97 - INTERNATIONAL WORKSHOP FOR DISTRIBUTED SYSTEMS OPERATIONS AND MANAGEMENT. *Proceedings*... Sydney, Australia, 1997. p.104-117.

CRUZ, F.A.S., NOTARE, M.S.M.A., WESTPHALL, C.B, MARTINS, A., WEBER-LEE, R., BARCIA, R.M. Using case-based reasoning in an intelligent management system. In: EIS'98. *Proceedings*... Tenerife, Spain, 11-13 fev.1998. p.1093-1099.

DAYHOFF, J. *Neural network architectures*: an introduction, Ed. Van Nostrand Reinhold, 1990.

DEMUTH, H., BEALE, M. Neural network Tollbox: for use with MatLab. *User Guide*, Version3, 1998. p.1-7, 7, 33.

DENNING, D. An intrusion-detection model. *IEEE Transactions on Software Engineering*, New York, v.13, n.2, p.222-232, 1987.

DÉSIRÈ, N. *Um modelo de gerência de segurança baseado em objetos distribuídos*. Florianópolis, 1999. Trabalho Individual (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

DOGAC, A., DENGI, C., ÖSZU, M.T. Distributed object computing platforms. *Communications of the ACM*, New York, v.41, n.9, p.95-103, set.1998.

DOWD, P., MCHENRY, J.T. Network security: it's time to take it seriously. *IEEE Computer Magazine*, New York, v.31, n.9, p.24-28, set.1998.

DUDA, R. O., HART, P.E. *Pattern classification and scene analysis*. New York, NY : John Wiley & Sons, Inc., 1973.

EHRIG, H., MAHR, B. *Fundamentals of algebraic specifications*. Ed. Springer-Verlag, 1985.

GARAVEL, H. *CADP*: Eucalyptus manual. Grenoble, France: INRIA/VASY, 1997. <http://www.inrialpes.fr/vasy/cadp/>.

GIBSON, J.D. *The mobile communications handbook*. Piscataway, NJ, USA : IEEE Press, 1996. 726p. ISBN 0-8493- 8573-3.

HAGGERTY, P., SEETHARAMAN, K. The benefits of CORBA-based network management. *Communications of the ACM*, New York, v.41, n.10, p.73-79, out.1998.

HAUW, L.H., CANELA, Z., VOYER, F. A CORBA-based TMN prototype with Web access. In: IEEE DSOM'97 - INTERNATIONAL WORKSHOP FOR DISTRIBUTED SYSTEMS OPERATIONS AND MANAGEMENT. *Proceedings*... Sydney, Australia, 1997. p.81-93.

HERMIDA, A., VALE, W. *Implementação Java dos módulos agentes e adaptador do SSTCC - Sistema de Segurança para Telecomunicações Contra Clonagem e Inadimplência*. Florianópolis, 1999. Projeto de Conclusão de Curso (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

HUSH, D.R., HORNE, B.G. Progress in supervised neural networks: what's new since Lippmann. *IEEE Signal Processing Magazine*, p.8-39, jan.1993.

INGBER, L. Simulated annealing: practive versus theory. *Mathematical Computing Modellilng*, v.18, n.11, p.29-57, 1993.

KOHONEN, T. Self-organized formation of topologically correct feature maps. In: BIOLOGICAL Cybernetics, 1982, p.59-69.

LEE, S., RHEE, M. A. Gaussian potential function network with hierarquically self-organzing learning. *Pattern Recognition Letters*, v.14, n.3, p.221- 227, 1993.

LIPPMANN, R.P. Pattern classification using neural networks. *IEEE Communications Magazine*, New York, p. 47-64, nov.1989.

LU, W., BI, Q. Wireless mobile ATM technologies for third-generation wireless communications. *IEEE communications Magazine*, New York, v.37, n.11, p.36-82, nov.1999.

LUNT, T. Automated audit trail analysis and intrusion detection: asurvey. In: INTERNATIONAL COMPUTER SECURITY CONFERENCE. *Proceedings*..., 1988. p. 65-73.

LUNT, T. et. al. Knowledge-based intrusion detection. In: ARTIFICIAL INTELLIGENCY SYSTEMS IN GOVERNEMENT CONFERENCE. *Proceedings*..., mar. 1989.

MATLAB USER'S GUIDE - For Microsoft Windows: High-Performance Numeric Computation and Visualization Software. Englewood Cliffs, NJ : The Math Works Inc., Prentice Hall, , 1992.

MATOS, A.V. *Gerência de segurança em aplicações de bancos de dados na Web*. Florianópolis, 1999. Dissertação (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

McGRAW, G., FELTEN, E. *Java security*. New York : John Wiley & Sons, 1997. 192p. ISBN 0-471-17842-X.

MEYER, J.W. Self-Organizing Processes. In: CONPAR'94 - VAPP VI. *Lecture Notes in Computer Science 824*. Berlin : Spring-Verlag , 1994, p.842-853.

MEYER, B. Every little bit counts: toward more reliable software. *IEEE Computer Magazine*. New York, v.32, n.11, p.131-135, nov. 1999.

MILIOLI, C.F., CASTELLO, W. *Sistema de segurança contra telefones celulares clonados*. Florianópolis, 1999. Projeto de Conclusão de Curso (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

MILNER, R. *A calculus of communicating systems*. Berlin : Springer-Verlag, 1980.

NAUGHTON, P. *The Java handbook*: the authoritative guide to the Java Revolution. Berkeley, USA : McGraw-Hill, 1986. 424p. ISBN 0-07-882199-1.

NEE, R. van, AWATER, G., MORIKURA, M, TAKANASHI, H., WEBSTER, M., HALFORD, K. New high-rate wireless LAN standards. *IEEE. Communications Magazine*, New York, v.37, n.12, p.82-88. dez. 1999.

NOTARE, M.S.M.A., CRUZ, F. A. S., SOBRAL, J.B.M., ALVES, J.B.M., RISO, B. G., WESTPHALL, C. B. Distributed Management in the Security Area for Cloned Mobile Phones, In: IEEE DSOM'98. *Proceedings*... Newark, Delaware, USA, 1998. p.14-24.

OMG. *Security service specification in CORBA services*: common objects services specification. 1998.

OPPLIGER, R. *Security technologies for the World Wide Web*. Norwood, MA, USA : Artech House Publisher, 1999. ISBN 1-58053-045-1.

ORFALI, R., HARKEY, D. *Client/server programming with Java and CORBA*. New York : John Wiley & Sons, 1997.

PAVLOU, G. From protocol-based to distributed object-based management architectures. In: IEEE DSOM'97 - INTERNATIONAL WORKSHOP FOR DISTRIBUTED SYSTEMS OPERATIONS AND MANAGEMENT. *Proceedings*... Sydney, Australia, 1997. p. 25-40.

PFLEEGER, C., COOPER, D. Security and privacy: promising advances. *IEEE Software*, New York, p.110-111, sep./out. 1997.

PIRES, L.F. *Architectural notes*: a framework for distributed systems development. Enschede, The Netherlands : CIP – Gegevens Koninklijke Biliotheek, 1994.

PRASAD, R. *Third generation mobile communications systems*. Norwood, MA, USA : Artech House Publishers, 1999. ISBN 1-58053-082-6.

QUEIROZ, J.A.M., CUNHA, P.R.F. *Sistemas distribuídos*: de especificações LOTOS a implementações. Recife : UFPE-DI, jul. 1994.

RAMOS, A.M., ALVES, J.B.M. Experiential knowledge. In: IEEE LANOMS'99. *Proceedings*... Rio de Janeiro, RJ, p. 236-244. ISBN: 85-900382-3-8.

RIEZENMAN, M.J. Technology 2000 analysis & forecast: communications. *IEEE Spectrum Magazine*, New York, v.37, n.1, p.33-39, jan. 2000.

ROZEMBLIT, M. *Security for telecommunications network management*. Piscataway, NJ : IEEE Press.1999. ISBN 0-7803-3490-6.

RUBIN, A. D., GEER, D. E., A Survey of Web Security. *IEEE Computer*, New York, v.l.31, n.9, p.34-41, sept. 1998.

SCHNEIDER, Maria Laura. *Detecção de Intrusão em Redes Móveis através de Redes Neurais*. Florianópolis, 1999 Trabalho Individual (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

SHAW, J. *Strategic Management in Telecommunications*. Norwood, MA, USA : Artech House Publishers, 1999. ISBN 1-58053-018-4.

SIMON, E. *Distributed Informations Systems*: From client/server to distributed multimedia. Maidenhead, Berkshire, England : McGraw-Hill, 1996. 414p.

SLOMAN, M.; TWIDLE, K. *Domains:* a framework for struturing management policy. Wokingham, UK : Addison-Wesley, 1994.

SOUZA, F., LEITE, K. *Sistema de extrato telefônico via Web em Java com suporte CORBA*. Florianópolis, 1999. Projeto de Conclusão de Curso (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

SPÍNDOLA, Fernando. *Implementação Java do módulo gerente do SSTCC - Sistema de Segurança para Telecomunicações Contra Clonagem e Inadimplência*. Florianópolis, 1999. Projeto de Conclusão de Curso (Curso de Graduação em Ciência da Computação) - Departamento de Informática e de Estatística, Centro Tecnológico, Universidade Federal de Santa Catarina.

STALLINGS, W. *Network and internetwork security*: principles and practice. Englewood Cliffs, NJ, USA : Prentice-Hall/IEEE Press, 1995. 462p. ISBN 0-02-415483-0.

STEWART, K. A., EE 4984 *Telecommunication Networks Project 1*: Cellular Telephone Fraud, <http://fiddle.ee.vt.edu/courses/ee4984/proj_95/stewart.html>.

STILLERMAN, M., MARCEAU, C. Intrusion Detection for Distributed Applications, *Communications of the ACM*, New York, v.42, n. 7, p.62-69, july 1999.

TODESCO, J. *Pattern Recognition using Artificial Neuronal Networks with a Radial Basis Function*: *an application for a human chromosome classification*. Florianópolis, 1995. Tese (Curso de Engenharia de Produção e Sistemas) – Departamento de Engenharia de Produção, Centro Tecnológico, Universidade Federal de Santa Catarina.

VISSERS, C.A., SCOLLO, G., SINDEREN, M.V. *Architecture and specification style in formal descriptions of distributed systems*. University of Twente, The Netherlands, 1988.