AS NOVAS TECNOLOGIAS WIRELESS

José Ibanes Chaves Junior

Discente da Faculdade de Informática de Presidente Prudente (FIPP) da Universidade do Oeste Paulista (Unoeste) E-mail: kqjames@hotmail.com.

Palavras-chave: Redes sem fio; Wireless; Wi-fi; Bluetooth; Infravermelho; WiMax.

Keywords: Wireless; Wi-fi; Bluetooth; infrared; WiMax.

RESUMO:

As novas tecnologias *Wireless* vieram acompanhadas de uma série de termos para designá-las. Esses termos acabam deixando o usuário confuso e, às vezes, perdido. Mas confusão entre tecnologias, termos, padrões e variações pode ser facilmente desfeita com um breve estudo das mesmas.

ABSTRACT

New Wireless Technologies came followed with a number of terms to designate them. These terms let the user confused, and sometimes, bewildered. Although confusion among technologies, terms, standards and variations can be easily undone with a brief study of them.

INTRODUÇÃO

As novas tecnologias *Wireless* estão cada vez mais presentes no dia-a-dia do homem pós-moderno. Seja utilizando o controle-remoto, o aparelho de som, o telefone celular ou qualquer outro aparelho que trabalhe com conexões *sem fio.* Mas o que significa rede *Wireless?*

A palavra Wireless é composta por duas outras palavras: *Wire* e *Less*, A primeira (*Wire*) significa fio ou cabo, e a segunda (*Less)* significa *sem*. Assim, temos o significado

de WIRELESS: sem fios ou sem cabos, caracterizando, então, qualquer meio de comunicação sem fios ou cabos.

Dentro desse modelo de comunicação, existem várias tecnologias como *Wi-fi*, *infravermelho*, *bluetooth* e *Wi-Max*, as quais serão apresentadas a seguir, uma vez que o objetivo deste trabalho é apresentar as principais características delas e proporcionar aos usuários não-especialistas um conhecimento básico para que entendam o que é a rede *Wireless.*

Características das redes sem fio

Wi-Fi

Wi-Fi é uma marca licenciada originalmente pela Wi-Fi Alliance para descrever a tecnologia de redes sem fio embarcadas (WLAN - Wireless Local Área Network) baseadas no padrão IEEE 802.11. A sigla Wi-Fi significa "Wireless Fidelity" ou fidelidade sem fio. Refere-se a um conjunto de equipamentos que permitem estabelecer uma rede local sem fios (WIKIPEDIA,2007a);

Uma rede sem fio usa ondas de rádio da mesma forma que os telefones celulares e outros equipamentos. Explicando melhor, o sinal de uma rede sem fio fica disponível no "ar", e qualquer equipamento que possua a tecnologia Wi-Fi pode se conectar à rede.

Segundo Loes (2006), o sinal de Internet ou de uma Intranet sai do cabo e ganha o ar, em forma de ondas de rádio, e passa a ser captado por qualquer equipamento habilitado com essas tecnologias wireless. Em redes Wi-Fi do tipo 802.11g (que é um dos padrões desta tecnologia), a velocidade pode chegar a 54 Mbps, enquanto as 802.11b se limitam a 11 Mbps. Com isso, os usuários ganham liberdade para acessar documentos importantes, informações de estoque, e-mails ou um simples perfil no Orkut em qualquer lugar coberto pela rede.

Loes diz também que uma rede Wi-Fi consiste basicamente em uma conexão de internet a cabo ligado a um access point que emite um sinal sem fio de Internet e que se comunica com um laptop, um desktop ou um PDA compatível com esta tecnologia.

Dados encontrados na enciclopédia Wikipédia, os principais padrões da família IEEE 802.11 são:

IEEE 802.11a: Padrão Wi-Fi para freqüência 5 GHz com capacidade teórica de 54 Mbps.

IEEE 802.11b: Padrão Wi-Fi para freqüência 2,4 GHz com capacidade teórica de 11 Mbps. Este padrão utiliza DSSS (Direct Sequency Spread Spectrum – Seqüência Direta de Espalhamento de Espectro) para diminuição de interferência.

IEEE 802.11g: Padrão Wi-Fi para freqüência 2,4 GHz com capacidade teórica de 54 Mbps.

Wi-Fi Protected Access (WPA e WPA2): padrão de segurança instituído para substituir padrão WEP (Wired Equivalent Privacy) que possuí falhas graves de segurança, possibilitando que um hacker pudesse quebrar a chave de criptografia após monitorar poucos minutos de comunicação.

A maneira mais comum de utilizar o *Wi-fi* é disponibilizando o acesso a Internet por meio de um roteador *Wireless* ligado a um PC com conexão a Internet. Desta maneira, a conexão é compartilhada para todos os aparelhos conectados à rede sem fio. É assim que funciona os "hotspots" disponíveis em aeroportos, hotéis e cybers café. Observe a figura a seguir:

Fonte: Brain e Wilson (2006).

Infravermelho

O infravermelho foi descoberto em 1800 por William Herschel, um astrônomo inglês de origem alemã. Hershell colocou um termômetro de mercúrio no espectro obtido por um prisma de cristal com o a finalidade de medir o calor emitido por cada cor. Descobriu que o calor era mais forte ao lado do vermelho do espectro, observando que ali não havia luz. Esta foi a primeira experiência que demonstrou que o calor pode ser captado em forma de imagem, como acontece com a luz visível (WIKIPEDIA, 2007b).

De acordo com Pedralho, Gomes e Nolêto (2005), a forma mais popular de conectividade sem fio ainda é o infravermelho (IrDA – Infrared Data Association), utilizado em milhões de dispositivos no mundo inteiro. Sua taxa de transmissão é relativamente alta (4 Mbps) e consome pouca energia.

Entretanto, há a necessidade do dispositivo ter obrigatoriamente seu sensor no campo de visão linear do outro e seu alcance é de apenas 1m. Além disto, o infravermelho só permite conexão entre dois dispositivos simultâneos, limitando bastante seu potencial.

Devido a essas limitações, esta tecnologia já possui um sucessor que é o Bluetooth. O Bluetooth pode ser uma escolha bem mais adequada quando utilizados para a transmissão de dados pequenos e em pequenas redes tipo piconets, iremos estudar melhor esta tecnologia no próximo assunto.

Bluetooth

O nome Bluetooth é uma homenagem ao rei da Dinamarca e Noruega Harald Blåtand - em inglês Harold Bluetooth (traduzido como dente azul, embora em dinamarquês signifique *de tez escura*). Blåtand é conhecido por unificar as tribos norueguesas, suecas e dinamarquesas. Da mesma forma, o protocolo procura unir diferentes tecnologias, como telefones móveis e computadores. O logotipo do Bluetooth é a união de duas runas nórdicas para as letras H e B, suas iniciais (WIKIPEDIA,2007c).

Para Pedralho, Gomes e Notêlo (2005), Bluetooth é uma tecnologia sem fio para transmissão de dados e voz entre dispositivos. Foi projetado visando prover uma interface universal para equipamentos, além da remoção dos cabos e diminuição do custo de conexões, tudo isso através da utilização de sinais de radiofreqüência gratuitos para estabelecer a comunicação entre os dispositivos. A grande vantagem desta tecnologia é o fato de ser sem fio, de baixo custo e automático.

Segundo Layton e Franklin (2006), A rede bluetooth transmite dados via ondas de rádio de baixa potência. Ela se comunica em uma freqüência de **2,45 gigahertz** (para ser exato, entre 2,402 GHz e 2,480 GHz). Essa banda de freqüência, chamada de ISM, foi reservada por acordo internacional para o uso de dispositivos industriais, científicos e médicos.

As bandas ISM (Instrumentation, Scientific & Medical), compreendem três segmentos do espectro (902 a 928 MHz, 2.400 a 2.483,5 MHz e 5.725 a 5.850 MHz) reservados para uso sem a necessidade de licença.

Fonte: Layton e Franklin (2006).

Para que os dispositivos terceiros que utilizam também a banda ISM não interfiram em uma conexão, o protocolo Bluetooth divide a banda passante em 79 canais e altera a freqüência aproximadamente 1600 vezes por segundo, tornando improvável mas não impossível uma interferência.

Os dispositivos são classificados de acordo com a potência e alcance, em três níveis:

Classe 1 (100 mW, com alcance de até 100 m).

Classe 2 (2,5 mW e alcance até 10 m).

Classe 3 (1 mW e alcance de 1 m, uma variante muito rara).

Cada dispositivo é dotado de um número único de 48 bits que serve de identificação. Em relação à sua velocidade pode chegar a 721 Kbps e possui três canais de voz.(WIKIPEDIA,2007c).

Wi-Max

Os principais problemas da Internet hoje em dia é que o acesso a banda larga não chega em qualquer lugar e o problema do Wi-Fi é que o alcance da conexão é considerado relativamente pequeno. Com o objetivo de resolver estes problemas, surgiu esta nova tecnologia chamada WiMax.

Segundo a enciclopédia Wikipédia, o padrão IEEE 802.16, completo em outubro de 2001 e publicado em 8 de abril de 2002, especifica uma interface sem fio para redes metropolitanas (WMAN). Foi atribuído a este padrão, o nome **WiMAX** (Worldwide Interoperability for Microwave Access/Interoperabilidade Mundial para Acesso de Micro-

ondas). O termo WiMAX foi cunhado por um grupo de indústrias conhecido como WiMax Forum cujo objetivo é promover a compatibilidade e inter-operabilidade entre equipamentos baseados no padrão **IEEE 802.16**. Este padrão é similar ao padrão Wi-Fi (IEEE 802.11), que já é bastante difundido, porém agrega conhecimentos e recursos mais recentes, visando uma melhor performance de comunicação. O padrão WiMAX tem como objetivo estabelecer a parte final da infra-estrutura de conexão de banda larga (last mile) oferecendo conectividade para uso doméstico, empresarial e em hotspots.

As principais características desta tecnologia são:

Velocidade do serviço de banda larga.

Cobertura ampla como o serviço para celulares.

Rede Wireless ao invés de cabos, tornando possível levar a Internet banda larga a lugares que os cabos não chegam.

De acordo com Grabianowski e Brain (2006), na prática, o WiMAX funcionaria como o WiFi, mas com velocidades mais altas, em distâncias maiores e para um número bem maior de usuários. O WiMAX poderia acabar com as áreas que hoje não têm acesso à Internet de banda larga porque as empresas de telefonia e TV a cabo ainda não levaram os fios necessários até estes remotos locais. Um sistema WiMAX consiste em duas partes:

Uma **torre WiMAX**, parecida em seu conceito com a torre de telefonia celular - uma única torre WiMAX pode fornecer cobertura para uma área muito grande - aproximadamente 8.000 km2.

Um **receptor WiMAX** - o receptor e a antena poderiam ser uma pequena caixa ou um cartão PCMCIA, ou poderiam ser integrados ao laptop como o WiFi o é hoje.

Fonte: Grabianowski e Brain (2004).

O WiMAX tem potencial para fazer pelo acesso à Internet de banda larga o que os telefones celulares fizeram pelo acesso telefônico. Da mesma maneira que muitas pessoas desistiram de seus telefones fixos em favor dos celulares, o WiMAX poderia substituir os serviços de cabo e DSL, fornecendo acesso universal à Internet praticamente em qualquer lugar para onde você for. Grabianowski e Brain (2004).

Os autores afirmam, também, que a conexão WiFi mais rápida consegue transmitir ate 54 megabits por segundo sob boas condições. O WiMAX deve ser capaz de transmitir até **70 megabits por segundo.** Mesmo que estes 70 megabits sejam divididos entre dezenas de empresas ou centenas de residências, ainda assim cada usuário terá taxas de transferência no mínimo equivalentes às da Internet a cabo. A grande diferença não é a velocidade, mas sim à **distância**. Neste quesito o WiMAX deixa o WiFi quilômetros atrás. O alcance do WiFi é de cerca de 30 metros, já o WiMAX poderá cobrir uma área de **50 quilômetros** com acesso sem fio. O alcance maior é devido às freqüências usadas e à

capacidade do transmissor. É claro que, a esta distância, terrenos, clima e grandes construções vão acabar reduzindo o alcance máximo em alguns casos, mas o potencial existe para cobrir grandes áreas.

O objetivo do WiMAX é abranger com altas taxas de transferência as áreas de difícil acesso, impossíveis ou complicadas de serem cobertas por cabos. Tudo isso, claro, por um custo relativamente pequeno.

CONSIDERAÇÕES FINAIS

As novas tecnologias *Wireless* surgiram para tomar espaço no mercado de telecomunicações, tendo em vista o baixo custo da instalação, a sua manutenção e o fácil acesso em locais que os cabos não podem chegar ou, mesmo quando chegam, poluem o ambiente de trabalho. Sua instalação é simples, rápida, sem nenhuma preocupação com a infra-estrutura e os indesejáveis cabos.

Vale ressaltar que apesar da rede sem fio ser uma alternativa muito interessante para quem procura portabilidade, cujos locais de acesso são variáveis como escritórios, empresas, universidades, aeroportos, etc., não se deve esquecer a questão da segurança da informação trafegada, uma questão bastante questionada por usuários. Afinal, essas informações trafegam no ar e, às vezes, podem sofrer ataques de pessoas de índoles duvidosas.

Esse problema da segurança tem sido resolvido com as técnicas de criptografias, embora não sejam ainda tão seguras quanto as tradicionais redes cabeadas. E, por essa razão, para montar uma rede, onde a segurança é o fator mais importante, é aconselhável levar em conta o custo/benefício.

Finalmente, com a esperança de auxiliar o usuário não-especialista a compreender as tecnologias *Wireless*, tão presentes em nosso dia-a-dia, para que possa optar entre elas, escolher a que melhor satisfaz sua necessidade.

REFERÊNCIAS BIBLIOGRÁFICAS

BRAIN, Marshall e WILSON, Tracy V. Traduzido por HowStuffWorks Brasil. **"Como funciona a rede WiFi".** 2006. Disponível em: <http://informatica.hsw.uol.com.br/rede-wifi.htm>. Acesso: 24 nov. 2007.

GRABIANOWSKI, Edward e BRAIN, Marshall - **"Como funciona o WiMax"**. 2004. Disponível em http://informatica.hsw.uol.com.br/wimax1.htm, Acesso: 24 nov. 2007.
INFRARED DATA ASSOCIATION (IrDA). **IrSimple, IrDA Classic.** 2006. Disponível em <http://www.irda.org/>. Acesso 10 nov. 2007.
Layton, Julia; Franklin, Curt – **"Como funciona o Bluetooth".** 2006. Disponível em:

http://eletronicos.hsw.uol.com.br/bluetooth1.htm. acesso: 24 nov. 2007.

Loes, João. **"Wi-Fi, infravermelho, bluetooth. Tire suas dúvidas!".** Disponível em : <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=265>. Acesso: 24 nov. 2007.
PEDRALHO, André; GOMES, Antônio e NOTÊLO, Tomaz. "Bluetooth: da teoria à prática – O mundo sem cabos". **WebMobile**, Rio de Janeiro, v.3 n.1, p.16-18, Jun/Jul, 2005.
TANEMBAUM, A.S. **"Computer Networks".** 4 Ed. New Jersey, Estados Unidos, Prentice Hall, 2003.
WIKIPÉDIA, **"Wi-Fi".** 2007. Disponível em: <http://pt.wikipedia.org/wiki/Wi-fi#Tabela_de_freq.C3.BC.C3.AAncias_e_pot.C3.AAncia>. Acesso em: 5 nov. 2007a.
WIKIPÉDIA, **"Radiação infravermelha".** 2007. Disponível em: <http://pt.wikipedia.org/wiki/Infrared_Data_Association>. Acesso: 05 nov 2007b.
WIKIPÉDIA, "**Bluetooth"**. 2007. Disponível em <http://pt.wikipedia.org/wiki/Bluetooth>. acesso:05 nov. 2007c.
WIKIPÉDIA, **"WiMax"**. 2007. Disponível em <http://pt.wikipedia.org/wiki/Wimax>. Acesso: 05 nov. 2007d.

INCUBADORA DE EMPRESA: INSTRUMENTO PARA A COMPETITIVIDADE DAS ORGANIZAÇÕES

Everton Clayton Bentlin[1]; Haroldo Cesar Alessi[2]

[1]Discente da Faculdade de Informática de Presidente Prudente (FIPP) da Universidade do Oeste Paulista (UNOESTE). email: everton@unoeste.edu.br
[2]Docente da Faculdade de Informática de Presidente Prudente (FIPP) da Universidade do Oeste Paulista (UNOESTE). email: haroldo@unoeste.br

Palavras-chave: Tecnologia; Competitividade; Incubadoras de Empresas; Empresas de Base Tecnológica.

Resumo

O desenvolvimento tecnológico constitui uma realidade cada vez mais almejada pelas organizações. Nesse contexto, destaca-se a atuação das incubadoras de empresas, como mecanismos de apoio à criação de um ambiente econômico propício à inovação. A prática da incubação, assim, é uma realidade cada vez mais presente no cenário contemporâneo, constituindo instrumentos essenciais para o sucesso e solidificação de empresas iniciantes no mercado, com destaque as Empresas de Base Tecnológica (EBTs) que, atuando em mercados tecnologicamente avançados, buscam na incubação uma forma de ingressarem com sucesso no mercado em que atuam.

1 Introdução

O desenvolvimento tecnológico constitui uma realidade cada vez mais almejada pelas organizações que, diante de um cenário de grande dinamicidade e incerteza, buscam agir de forma competitiva e se consolidar no mercado.

A inserção de novas tecnologias no cenário mundial constitui um processo que desperta o interesse de diversos empreendedores. No entanto, um dos pontos principais e que preocupam, principalmente, as pequenas empresas iniciantes no mercado, é a fase de criação do negócio. A imaturidade e a falta de orientação dos empreendedores no processo de abertura e acompanhamento da empresa, durante seu processo inicial, torna comum o fechamento do negócio poucos anos depois de sua abertura.

Neste contexto, verifica-se um crescimento significativo no número de empreendedores que buscam as incubadoras de empresas como forma de concretizar o seu

negócio. Os recursos tecnológicos e organizacionais disponibilizados por essas estruturas auxiliam as empresas iniciantes com o intuito de facilitar e monitorar o processo de inserção dessas empresas no mercado.

2 Objetivo

O objetivo do presente artigo é relatar a importância das incubadoras de empresas no processo de inovação tecnológica e demonstrar que o processo de incubação constitui uma boa forma para que jovens empresas ingressem e sobrevivam de forma satisfatória no mercado e alcancem vantagem competitiva agregando valor ao seu produto.

3 Justificativa

Esse estudo justifica-se pela necessidade de um entendimento mútuo, bem como da adoção de acordos e medidas estratégicas pelas entidades envolvidas – incubadoras e empresas incubadas – que contribuem para superar possíveis problemas, como mortalidade, dificuldades de acesso ao mercado, preconceito do mercado com relação as jovens empresas, etc. promovendo uma solidificação eficaz de empresas incubadas no atual ambiente econômico.

4 Material e Métodos

Foram adotadas para o presente estudo, pesquisas bibliográficas, que segundo Marconi e Lakatos (2006), são um apanhado geral sobre os principais trabalhos já realizados, por serem capazes de fornecer dados atuais relevantes relacionados com o tema.

5 Revisão Bibliográfica

5.1 Tecnologia

Conforme afirma Hatch (1997), a tecnologia pode ser descrita em termos de três elementos principais: (1) físico e artefatos, (2) atividades e processos, e (3) conhecimento necessário para realizar o desenvolvimento e aplicação dos elementos físicos e das atividades. Assim, Scott (2003) a define como sendo uma combinação física e intelectual de todo trabalho desempenhado por uma organização, incluindo não apenas o *hardware*

utilizado para o desempenho das atividades, mas também habilidades e conhecimentos necessários para tal.

5.2 Incubadoras de Empresas

Segundo Hackett e Dilts (2004a apud ANDINO e FRACASSO, 2005), incubadoras constituem espaços compartilhados que fornecem para as empresas iniciantes recursos tecnológicos e organizacionais, sistemas de criação de valor agregado, bem como monitoramento e ajuda empresarial. Para Andino e Fracasso (2005) as incubadoras visam, assim, reduzir a probabilidade de fracasso e acelerar o processo de consolidação de novas empresas.

5.2.1 Processo de Incubação

O processo de incubação de uma empresa deve seguir etapas e oferecer para as empresas incubadas toda infra-estrutura física e intelectual necessária para seu desenvolvimento, em vista que a negligência de algumas dessas etapas durante o processo de incubação pode levar a empresa ao fracasso. Diante do exposto, cabe destacar as Empresas de Base Tecnológica (EBTs) como potenciais candidatas a processos de incubação. Muitas empresas desse tipo vêem na incubação uma estratégia eficaz para ganharem vantagem competitiva e se manterem no mercado.

5.2.2 Empresas de Base Tecnológica

A importância da tecnologia no desenvolvimento do atual cenário econômico mundial destaca as Empresas de Base Tecnológica (EBTs) como importantes nesse contexto. A literatura sobre o tema apresenta diversos conceitos relativos a essas empresas, com destaque para a definição de Lemos e Maculan (1998) que conceituam EBTs como organizações que atuam em setores tecnologicamente avançados, incorporando em seu processo produtivo elevado grau de conhecimento técnico-científico, com grande domínio de tecnologias de produção complexas.

Nesse sentido, a incubação constitui uma boa opção para que as EBTs ingressem no mercado, alcancem vantagem competitiva agregando valor ao seu produto e sobrevivam no mercado. No entanto, o processo de incubação dessas empresas ainda é passível de

problemas e dificuldades que podem prejudicar e, até mesmo, inibir a sua introdução no mercado.

6 Conclusão

A dinamicidade da atual economia torna as novas tecnologias instrumentos importantes para a manutenção das empresas no mercado. Dessa forma, as incubadoras surgem como meios facilitadores do processo de inovação, fornecendo apoio na criação e desenvolvimento de novas empresas, por meio do fornecimento de formação técnica e gerencial aos seus empreendedores.

Com o auxílio das incubadoras, os empreendedores têm a sua disposição um ambiente propício para o desenvolvimento de seu projeto, recebendo constante acompanhamento, orientação e avaliação de seu negócio. Dessa forma, empresas que passam pelo processo de incubação adquirem uma maior capacitação, estando mais preparadas para enfrentar as dificuldades e se consolidar no mercado.

No entanto, o processo de incubação em alguns setores de atividade ainda é passível de preconceitos e necessidades que dificultam, por vezes, um aproveitamento ainda maior desse tipo de atividade.

Referências Bibliográficas

ANDINO, B. F. A.; FRACASSO, A. M. Efetividade do Processo de Incubação de Empresas. In: ENANPAD, 2005. **Anais...**

HATCH, M. J. **Organization theory:** modern, symbolic, and postmodern perspectives. New York: Oxford University Press, 1997.

LEMOS, M. V.; MACULAN, A. D. O Papel das incubadoras no apoio às empresas de base tecnológica. In: SIMPÓSIO DE GESTÃO DA INOVAÇÃO TECNOLÓGICA, 20., 1998. **Anais...**

MARCONI, M. A.; LAKATO, E. M. **Fundamentos da Metodologia Cientifica**. 6.ed São Paulo: Atlas, 2006.

SCOTT, W. R. **Organizations: rational, natural, and open systems**. 5. ed. New Jersey: Prentice Hall, 2003.

DESENVOLVIMENTO DE UMA FERRAMENTA PARA CONTROLE DE RESIDÊNCIAS UTILIZANDO DISPOSITIVOS MÓVEIS

Everton Clayton Bentlin[1]; Kleber Manrique Trevizani[2]

[1]Discente da Faculdade de Informática de Presidente Prudente (FIPP) da Universidade do Oeste Paulista (UNOESTE). email: everton@unoeste.edu.br
[2]Docente da Faculdade de Informática de Presidente Prudente (FIPP) da Universidade do Oeste Paulista (UNOESTE). email: kleber@unoeste.br

Palavras-chave: Dispositivos Móveis, Computação Ubíqua, Redes sem Fio

1 Formulação do Problema

A computação móvel tem transformado a computação numa atividade que pode ser carregada para qualquer lugar. Os principais motivos dessa transformação são a miniaturização dos dispositivos eletrônicos e o aumento da oferta de conectividade. (Weiser, 1991) previu que os computadores proverão informações e serviços quando e onde forem necessários. A visão dele descreve uma proliferação de dispositivos de diferentes tamanhos, desde dispositivos portáteis até grandes dispositivos compartilhados. Tal proliferação de dispositivos realmente aconteceu com os dispositivos usados normalmente, como por exemplo, os PDAs, laptops e *whiteboards* de grande escala. Ele vislumbrou a uma década que, no futuro, computadores habitariam os mais triviais objetos como etiquetas de roupas, xícaras de café, interruptores de luz, canetas, etc, de forma invisível para o usuário.

Um dos dispositivos mais presentes nos estilo de vida atual são os aparelhos de telefonia celular. Milhares de operadoras/empresas em todo mundo desenvolvem novas aplicações e conteúdos para usuários de celular, incorporando funcionalidades diversas como câmeras fotográfica, câmeras de vídeo, apresentadores multimídia, jogos, recepção de TV, acesso a Internet, entre outras.

Os avanços na tecnologia permitem que os dispositivos móveis se comuniquem com computadores ou outros aparelhos eletrônicos possibilitando a utilização desses dispositivos para automação de tarefas simples e cotidianas como acender luzes, abrir portões, ligar ar-condicionados, etc.

2 Objetivos do Projeto

O objetivo deste projeto é desenvolver um sistema que possa comandar funções de dispositivos eletrônicos de um local (residência, escritório ou empresa, por exemplo) a partir de qualquer lugar do mundo, utilizando um aparelho de telefonia celular, desde que o mesmo esteja conectado à Internet, através de uma rede Wi-Fi ou através do sinal disponibilizado pela operadora.

O local a ser conectado deve possuir um computador executando um serviço de rede, especialmente projetado para controlar os dispositivos do local. Tal serviço receberá as requisições da aplicação instalada no celular, executará a ação no dispositivo e devolverá o resultado da requisição (positivo ou negativo) para a aplicação do celular. O serviço de rede localizado no computador será projetado e construído de modo a facilitar a adição de novos dispositivos de hardware. Nesse sentido, para cada dispositivo novo a ser suportado, deverá ser desenvolvido um driver que permita o controle de suas funcionalidades.

A partir do aparelho celular, o usuário poderá ligar, desligar, configurar dispositivos e programar horários para os dispositivos ligarem ou desligarem, de acordo com sua necessidade. O sistema, localizado no computador do local controlado, enviará uma confirmação para o celular depois que a ações forem aceitas ou executadas.

3 Justificativas do Projeto

O projeto justifica-se pela idéia de utilizar os recursos que a computação móvel oferece para aqueles que querem estar a frente em questão de conforto e comodidade.

4 Metodologia e Plano de Trabalho

O projeto será iniciado por uma revisão bibliográfica para estudar como os aparelhos celulares acessam a Internet. No próximo passo serão desenvolvidos programas simples que utilizam a Internet através do aparelho celular visando o estudo prático dessa tecnologia. Em seguida, será feita a análise de requisitos e o projeto do sistema, detalhando e documentando quais as características desejáveis do projeto. A seguir será realizada a sua implementação, seguida de testes de funcionalidade, onde os resultados obtidos e os detalhes de implementação serão registrados em uma monografia.

Vale ressaltar que a comunicação do software, localizado no computador do local a ser controlado, com os dispositivos do local não será realizada neste projeto. No entanto, o software oferecerá uma API para O desenvolvimento de *drivers* que controlarão tais dispositivos. Para testar a aplicação, será utilizada uma maquete de uma residência de modo a ilustrar o funcionamento do projeto.

5 Equipamento e Material

O projeto será desenvolvido na Faculdade de Informática de Presidente Prudente (FIPP) que disponibiliza a infra-estrutura necessária para o desenvolvimento do projeto proposto. Serão utilizados livros disponíveis na biblioteca e materiais disponíveis na Internet além de um aparelho celular com acesso a Internet via Wi-Fi. Também será utilizada uma maquete de residência, já existente na universidade.

Referências Bibliográficas

WEISER, Marc. “The Computer for the 21st Century”, Scientific American, vol.265, no.3, 1991.
TANENBAUM, Andrew. Redes de computadores - 4. ed., Prentice Hall, 2002.
STALLINGS, W. Redes e Sistemas de Comunicação de Dados: Teoria e aplicações corporativas. São Paulo: Campus, 2005, 5ª edição.
MUCHOW, John W. “Core J2ME : tecnologia e MIDP”., Pearson Makron Books, 2007.
KUROSE, James F. Redes de computadores e a Internet : uma abordagem top-down, Pearson Addison Wesley. 3. ed. 2007.
http://twiki.dcc.ufba.br/pub/MAT570/LivroseArtigos/045_AraujoRB.pdf, acessado em 19 de Fevereiro de 2008.

UM ESTUDO DO FUNCIONAMENTO DA CRIPTOGRAFIA SIMÉTRICA E ASSIMÉTRICA COMO FERRAMENTA DE SEGURANÇA COMPUTACIONAL EM REDES LOCAIS E NA WEB

Cleverson Moreira de Souza[1]
Camila Pires Cremasco[2]

[1]Acadêmico de Tecnologia em Processamento de Dados – FAI; Rua Nove de Julho, 730. Centro. Adamantina-SP. 17800-000; mscleverson@gmail.com
[2]Professora Doutora – FAI; Rua Nove de Julho, 730. Centro. Adamantina-SP. 17800-000; cpcremasco@hotmail.com

Palavras-chave: Criptografia. Segurança. Informações

INTRODUÇÃO

Os computadores armazenam arquivos em meios de armazenamento diferentes, tais como fitas magnéticas, discos rígidos, discos flexíveis e discos óticos que podem ser programas-fonte, programas-objeto, programas executáveis, dados numéricos, texto, registros de folha de pagamento, imagens gráficas, gravações de áudio, banco de dados, entre outros e podem ser acessados diretamente ou seqüencialmente, dentro de um sistema de computação ou uma rede de computadores.

Estes arquivos são acessados por vários usuários, que tem a necessidade de compartilhar informações. O envio e o recebimento de informações sigilosas é uma necessidade antiga, que existe há centenas de anos. Com o surgimento da Internet e sua facilidade de entregar informações de maneira precisa e extremamente rápida, surge a necessidade de usar ferramentas de segurança baseada na criptografia (kriptós = escondido oculto; grápho = grafia) para permitir que apenas o emissor e o receptor tenham acesso livre à informação trabalhada.

A criptografia é a arte de escrever em códigos ou em cifras, pode se considerar uma ciência tão antiga quanto à própria escrita, uma vez que já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalha. O mais interessante é que a tecnologia de criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do

computador, a área realmente floresceu incorporando complexos algoritmos matemáticos (TERADA, 2000).

Hoje esta ferramenta é fundamental em qualquer cooperação, para assegurar a confiabilidade dos dados emitidos e recebidos através das redes.

METODOLOGIA

Nos dias de hoje, as técnicas de criptografia mais conhecidas envolvem o conceito de chaves, as chamadas "chaves criptográficas". Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação.

Um modelo de criptografia que surgiu na década de 70 e se tornou padrão no mundo todo foi o DES (Data Encrytion Standard). Implementado em 1977, o DES é usado principalmente em navegadores Internet ou smart cards, podendo assim ser implementado tanto em Hardware quanto em Software. O DES é um algoritmo simétrico, porque o emissor e o receptor utilizam a mesma chave para decifrar as mensagens. Este algoritmo utiliza uma string alfanumérica como chave para codificar e decodificar a mensagem, sendo um cifrário composto, porque utiliza mais de um cifrário para criptografar a mensagem, aumentando a segurança (TERADA, 2000b).

Além dos algoritmos simétricos, existem algoritmos assimétricos, que são conhecidos como algoritmos de “chave pública” que utiliza duas chaves, sendo uma para cifrar (chave pública) e outra para decifrar (chave privada) a mensagem garantindo assim maior segurança. As chaves públicas dos usuários são divulgadas e as chaves privadas são mantidas em segredo pelos usuários, porque uma mensagem enviada cifrada com a chave pública só pode ser decifrada com a chave privada do usuário receptor (TERADA, 2000c).

O algoritmo mais popular é o RSA, sendo ideal utilizá-lo com chaves privadas de mais de 90 bits. Os algoritmos ou cifrários assimétricos utilizam como chaves públicas um número extenso, que pode ser fatorado em seus números primos. As chaves privadas são os números primos que multiplicados entre si produzem o número composto que é a chave pública (BUCHMANN, 2002).

A criptografia é uma poderosa ferramenta de segurança que esta em evolução junto com a tecnologia. No entanto, é necessário modelar novas ferramentas e aplicá-las na segurança de dados sigilosos. Esta pesquisa consiste no estudo dos principais modelos de criptografia para aproveitar melhor sua aplicação e desenvolver novas ferramentas de segurança computacional.

MATERIAIS E MÉTODOS

Foi feito um estudo dos principais algoritmos de criptografia e observou-se que em relação aos algoritmos de chave simétrica (One-Time Pad), o problema reside em como obter e manter um canal seguro para a troca de chaves, pois sempre pode haver alguém espionando o canal e assim, passivamente, obter uma cópia da chave transmitida, e não há como detectar a presença do espião, já os algoritmos de chave assimétricos (RSA) têm sua segurança baseada numa pretensa intratabilidade computacional pelo fato de que os algoritmos de fatoração para os computadores atuais são de ordem exponencial, o que praticamente invalida a quebra do protocolo, porém, a fatorização de números pode ser feita em tempo polinomial num computador quântico, o que coloca em xeque a segurança desses sistemas criptográficos.

Conforme testes realizados, conclui-se que em qualquer dos métodos é impossível saber classicamente se há alguém monitorando o canal de comunicação. Uma saída para esses problemas é encontrada na Criptografia Quântica cuja segurança é baseada nas leis da Física Quântica e promete que se alguém interceptar a troca de chaves será possível detectar sua presença e se as chaves são usadas no método One-Time Pad, então segurança completa é obtida.

DISCUSSÃO

Em alguns testes, foi observado que as chaves simétricas têm uma melhor performance do que a criptografia assimétrica. Ela também é mais difícil de ser quebrada, se usarmos chaves grandes, do mesmo, jeito podemos destacar algumas desvantagens. Elas requerem um sistema seguro para envio das chaves e cada par de usuários precisa de um único par de chaves. É um tipo de cifragem que provê confidencialidade, mas não garante autenticidade e não repúdio.

Existe uma maior escalabilidade no método assimétrico sem contar que esse método provê autenticação e não repúdio. Em contrapartida, embora seja um método muito mais seguro, as chaves assimétricas são mais lentas principalmente por possuírem tarefas matemáticas muito mais intensas.

Apesar do sistema ser mais lento, seria melhor utilizar chaves assimétricas em redes de longa distância ou na Internet, devido à autenticação e não repúdio, já em redes locais e seria mais aconselhado usar chaves simétricas por causa da confidencialidade.

CONCLUSÃO

Nos últimos dez anos houve um avanço extraordinário na disseminação e popularização da Internet e o advento das chamadas “lojas virtuais” para comércio eletrônico e das “home-bankings” que possibilitem translações bancárias através de uma senha (ou chave) de conhecimento apenas da pessoa autorizada. Há também diversos serviços de notícias e informações econômicas, sociais artísticas, médicas, técnico-científicas, etc. Tais serviços oferecem conforto, economia e rapidez em tarefas outrora cansativas, custosas e demoradas. Sistemas de comunicação como a Internet são controlados por computadores em rede pelo qual a informação trafega desde a origem onde ela está armazenada ou foi criada até o destino onde o solicitante da informação se encontra. Muitas vezes há mais de um computador que repassa a mesma informação entre origem e destino, principalmente quando estão geograficamente distantes, surgindo à necessidade de se usar criptografia. Criptografia só pode ser considerada como tal se quatro princípios básicos forem seguidos e oferecidos: confidencialidade, autenticação, integridade da informação e não repudiabilidade (o remetente não pode negar o envio da informação). É por isso que a criptografia é um recurso tão importante na transmissão de informações pela Internet e, mesmo assim, não é capaz de garantir 100% de segurança, pois sempre existe alguém que consegue criar um jeito de quebrar uma codificação. Por isso é que técnicas existentes são aperfeiçoadas e outras são criadas, como a "Criptografia Quântica". Na criptografia há ainda outros conceitos envolvidos, como a Função Hashing (usada em assinaturas digitais), e aplicações, como a Certificação Digital.

REFERÊNCIAS BIBLIOGRÁFICAS

JOHANNES A. BUCHMANN. **Introdução à Criptografia**. São Paulo: Editora Berkeley, 2002.

NIVIO ZIVIANI. **Projeto de Algoritmos**. Belo Horizonte: Thomson, 2003.

ROUTO TERADA. **Segurança de Dados "Criptografia em Redes de Computador"**. São Paulo: Editora Edgard Blugher Ltda, 2000.

THOMAS H. CORMEN, CHARLES E. LEISERSON, RONALD L. RIVEST e CLIFFORD STEIN. **Algoritmos "Teoria e Prática"**. Rio de Janeiro: Editora Campus, 2001.