Fundação Educacional do Município de Assis
Instituto Municípal de Ensino Superior de Assis - IMESA

Paulo Rogério Cerqueira Filho

Tecnologia de Rede Wireless

Assis, SP

2011

Paulo Rogério Cerqueira Filho

TECNOLOGIAS DE REDES WIRELESS

Trabalho de conclusão de curso para obtenção do título de graduação em Tecnologia em Processamento de Dados, apresentado à Fundação Educacional do Município de Assis – FEMA.

Orientador: Prof. Fábio Eder

ASSIS - SP

2011

FICHA CATALOGRAFICA

CERQUEIRA, Paulo Rogério Filho.

Tecnologia em Rede Wireless/ Paulo Rogério Cerqueira Filho
Fundação Educacional do Município de Assis FEMA Assis, 2011.
34p.

Orientador: Prof.ª Fábio Eder.

Trabalho de Conclusão de Curso Instituto Municipal de Ensino – IMESA.

CDD: 001.61
Biblioteca da FEMA

Paulo Rogério Cerqueira

TECNOLOGIAS DE REDES WIRELESS

Trabalho de conclusão de curso para obtenção do título de graduação em Tecnologia e Processamento de Dados, apresentado à Fundação Educacional do Município de Assis – FEMA.

Aprovado em ___/___/____

BANCA EXAMINADORA

_____

Prof.

Fundação Educacional do Município de Assis – FEMA.

_____

Prof.

Fundação Educacional do Município de Assis – FEMA.

_____

Prof.

Fundação Educacional do Município de Assis – FEMA

DEDICATÓRIA

Dedico este trabalho aos meus pais Paulo Rogério Cerqueira e Elvira Berardi Cerqueira por terem me dado meu bem maior: a vida!

Dedico a meus amigos que estiveram sempre comigo me apoiando e me dando muita força: Daniel de Felippo, Wellington, Bruno, Marquinho Ladeira, Felipe Garrido, César Nardi, Karina Ramos, Rosa Zandonadi, Carol Simões, e toda minha turma do TPD, meu esteio na hora das decisões difíceis e à minha irmã Larissa por fazer parte da minha vida.

Ao grande amigo irmão Marcos Paulo pelo incentivo, apoio, força, equilíbrio e muita garra nos momentos de dificuldade.

AGRADECIMENTOS

Agradeço em primeiro lugar à DEUS por ser a base das minhas conquistas;
Aos meus pais Paulo e Elvira, por acreditarem e terem interesse em minhas escolhas, apoiando-me para que eu possa seguir firme na minha batalha;
Aos amigos de classe, ao professor Orientador Fábio Eder pela dedicação em suas orientações prestadas na elaboração deste trabalho, me incentivando e colaborando no desenvolvimento de minhas ideias.

RESUMO

Por ser um assunto fascinante e presente no cotidiano atual, o tema Wireless, rede sem fio, é o objeto deste estudo, principalmente quando se trata da segurança dos dados que são transportados por esse tipo de rede, que se mostra um tanto frágil. Porém novas tecnologias estão surgindo como as criptografias que dão mais tranquilidade ao usuário. Com a popularização do Wireless, redes sem fio, aumentaram as perspectivas de seu uso no sistema Empresarial e cada vez mais as empresas têm se esforçado para obter vantagens competitivas e ficar à frente da concorrência, principalmente quanto ao quesito segurança. A expansão das redes sem fio é uma realidade presente em vários segmentos da sociedade como: saúde, educação, segurança pública, transportes, meio ambiente, e também nos ambientes industriais, comerciais e residenciais e ainda para fins militares. A evolução tecnológica dos dispositivos de segurança, como os protocolos e chaves, com destaque para a criptografia, é uma prerrogativa que revolucionará a coleta e processamento de informações, e pretende solucionar sua vulnerabilidade frente aos ataques de invasores inescrupulosos. Os protocolos mais utilizados, hoje, para as redes sem fio são WEP, WAP, WAP2. Este trabalho será fundamentado teoricamente em artigos pesquisados, em sites da internet, livros, revistas e dissertações que abordam direta ou indiretamente o assunto.

Palavras-chave: Wireless, redes sem fio, segurança, internet, protocolos.

ABSTRACT

Because it is a fascinating subject and present in the daily life of our present time, the theme Wireless, wireless network, is the object of this study, especially when it comes to the safety of data that is transported by this type of network, which shows somewhat fragile. But new technologies are emerging as the encryptions that give more tranquility to the user. With the popularization of Wireless, wireless networks, increased the prospects of its use in the enterprise system and increasingly companies are struggling to gain competitive advantage and stay ahead of the competition, mainly regarding the security aspect. The expansion of wireless networks is a present reality in various segments of society such as: health, education, public safety, transportation, environment, and also in industrial, commercial and residential environments and even for military purposes. The technological evolution of security devices, such as protocols and keys, with emphasis on encryption, is a prerogative that revolutionize the collecting and processing information, and want to solve their vulnerability against unscrupulous invaders attacks. Most protocols used today, for wireless networks are WEP, WAP, WAP2. This work will be based theoretically in articles searched, on internet sites, books, journals and dissertations dealing directly or indirectly the subject.

Word-keys: Wireless, nets without wire, security, Internet, protocols.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

AES - Advanced Encription Standard
AP - Access Pointer
ARP - Address Resolution Protocol
ARPANET - Advanced Research Projects Agency Network
DARPA - Defense Advanced Research Projects Agency
EAP - Extensible Authentication Protocol
IAS - Servidor de Autenticação Interna
IEEE - Internet Engineering Task Force
IMP – Processador de Interface das Mensagens
KSA – Key Scheduling Algorithm
LAN - Local Área Network
MIT - Massachussets Institute of Thechnology
NPL – Nuclear PhysicsnLaboratory
RADIUS- Remote Authentication Dial-In User Servic
RC - Ron's Code ou Rivest Cipher
TKIP - Temporal Key Integrity Protocol
UCLA – Uniservidad of California at Los Angeles
WAN - Wide Área Network
WPA - Wi-Fi Protected Access
WEP - Wired Equivalent Privacy Wep

SUMÁRIO

1. TECNOLOGIAS DE REDES WIRELESS

1. INTRODUÇÃO

A tecnologia da informação teve um crescimento espantoso nas últimas décadas e a internet é uma ferramenta que se popularizou rapidamente atingindo o fenômeno da globalização, uma vez que consegue mobilizar a humanidade em tempo real, conforme o desenrolar dos acontecimentos, mostra disso, as catástrofes no Japão e as mobilizações revolucionárias no Oriente Médio.

Não podemos falar em internet sem relacionar conectividade com tecnologias de redes que evoluem a cada dia e uma das que estão surgindo com bastante força no mercado são as redes Wireless, ou seja, redes sem fio.

A popularização das redes sem fio vem sendo cada vez mais uma opção de conectividade para empresas, hotéis, hospitais, aeroportos, inclusive usuários domésticos, pois oferece várias vantagens em relação às redes convencionais, como maior mobilidade, flexibilidade, rapidez e facilidade de instalação. (RUFINO, 2005).

As redes locais sem fio constituem-se como uma alternativa às redes convencionais com fio, fornecendo as mesmas funcionalidades, mas de forma flexível, de fácil configuração e com boa conectividade em áreas prediais ou de campus. Dependendo da tecnologia utilizada, rádio frequência ou infravermelho, e do receptor, as redes Wireless podem atingir distâncias de até 18 metros. (SILVA, 1998).

1.1 – Motivação

Cada vez mais as organizações têm se esforçado para obter vantagens competitivas e ficar à frente da concorrência. Utilizando-se das ferramentas e técnicas apresentadas na tecnologia da informatização, criando ambientes e procedimentos buscam uma maior eficiência, onde seus efeitos reflitam positivamente para alcançar os objetivos da empresa.

Todas essas evoluções, aliadas ao processo de globalização, trouxeram novos desafios e a possibilidade de participar de um estudo para o desenvolvimento de um projeto que venha a atender essas necessidades do mercado é sempre um desafio para todo profissional se sentir motivado a aprofundar-se numa pesquisa sobre a segurança das novas tecnologias de redes Wireless.

Por se tratar de um assunto atual que está inserido no cotidiano das pessoas, é um tema que fascina pela sua grandeza e utilidade, principalmente aos jovens profissionais que estão iniciando sua carreira.

Por isso este trabalho objetiva possibilitar estudos no desenvolvimento de novas tecnologias para redes Wireless, mais especificamente no padrão IEEE 80211 e suas extensões, analisando seus mecanismos de segurança e conceitos essenciais para uma implantação segura.

1.2 – Perspectiva de Contribuição

O ponto ainda vulnerável no desenvolvimento das tecnologias de rede é o capital humano, que apesar do conceito, relativamente novo no Brasil, foi menos desenvolvido, que as tecnologias. Ainda hoje são mais utilizadas as experiências práticas que o conhecimento cientifico, o que não é suficiente para atender o mercado competitivo e exigente que busca sempre a excelência e a eficácia no atendimento.

Divulgar este trabalho por meio de artigos que possam ser colocados na mídia é uma forma de contribuir para diminuir a carência de literatura para tais abordagens e apresentar subsídios para estudiosos da área e quaisquer outros interessados no assunto.

1.3– Metodologia de pesquisa

Este estudo terá como método a pesquisa exploratória, utilizando-se de pesquisas bibliográficas em livros, artigos, teses, dissertações, internet, anotações em aula, etc.

No desenvolvimento dos comentários serão abordados alguns pressupostos:

- Realizar comentários por Seção, com indicação dos dispositivos correspondentes;
- Apresentar alguns conceitos e orientações, quando julgados necessários.

Num primeiro momento será feita uma abordagem da evolução da informática para depois serem comentados os conceitos e modelos de referência OSI, modelos de referência TCP/IP, as redes sem fio, suas características, padrões e modos de transmissão. Será estudado ainda o protocolo *Wired Equivalent Protocol* – WEP e principalmente sobre as tecnologias de segurança das redes Wireless, que é o tema desse estudo.

2 – BREVE ABORDAGEM HISTÓRICA DA INTERNET

A internet, ou rede mundial de computadores surgiu em plena Guerra Fria. Criada com objetivos militares seria uma das formas das forças armadas norte-americanas de manter as comunicações em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações.

Com base em informações colhidas no site http://www.aisa.com.br/futuro.html falando a respeito da origem da internet, sabemos que **o**s primeiros registros de interações sociais que poderiam ser realizadas através de redes foi uma série de memorandos escritos por J.C.R. Licklider**,** do MIT – *Massachussets Institute of Technology*, em agosto de 1962, discutindo o conceito da "Rede Galáxica". Ele previa vários computadores interconectados globalmente, pelo meio dos quais todos poderiam acessar dados e programas de qualquer local rapidamente. Em essência, o conceito foi muito parecido com a Internet de hoje. Licklider foi o primeiro gerente do programa de pesquisa de computador do DARPA, começando em outubro de 1962. Enquanto trabalhando neste projeto, ele convenceu seus sucessores Ivan Sutherland, Bob Taylor e Lawrence G. Roberts da importância do conceito de redes computadorizadas.

Em 1965, Roberts e Thomas Merrill conectaram um computador TX-2 em Massachussets com um Q-32 na Califórnia com uma linha discada de baixa velocidade, criando assim o primeiro computador de rede do mundo. O resultado deste experimento foi a comprovação de que computadores poderiam trabalhar bem juntos, rodando programas e recuperando dados quando necessário em máquinas remotas, mas que o circuito do sistema telefônico era totalmente inadequado para o intento. Foi confirmada assim a convicção de Kleinrock sobre a necessidade de trocas de pacotes.

No final de 1966, Roberts começou a trabalhar no DARPA para desenvolver o conceito das redes computadorizadas e elaborou o seu plano para a ARPANET, publicado em 1967.

Na conferência onde ele apresentou este trabalho, houve também uma apresentação sobre o conceito de redes de pacotes desenvolvidas pelos ingleses:

Donald Davies e Roger Scantlebury, da NPL- Nuclear *Physics Laboratory*. Os trabalhos desenvolvidos no MIT (1961-67), RAND (1962-65) e NPL (1964-67) estavam se desenrolando em paralelo sem que nenhum dos pesquisadores soubessem dos outros trabalhos. A palavra "pacote" foi adotada do trabalho desenvolvido no NPL e a velocidade de linha proposta para ser usada no projeto da ARPANET foi *up graded* de 2,4 Kb para 50 Kb.

Em agosto de 1968, depois de Roberts e o grupo do DARPA terem refinado a estrutura e especificações para a ARPANET, uma seleção foi feita para o desenvolvimento de um dos componentes chaves do projeto: o processador de interface das mensagens (IMP). Um grupo dirigido por Frank Heart (Bolt Beranek) e Newman (BBN) foi selecionado.

Devido à teoria de trocas de pacotes de Kleinrock e seu foco em análise, desenho e mensuração, seu Centro de Mensuração de Rede da UCLA foi escolhido para ser o primeiro nó (ponta) da ARPANET. Isso aconteceu em setembro de 1969, quando BBN instalou o primeiro IMP na UCLA e o primeiro servidor de computador foi conectado.

O projeto chamado Aumento do Intelecto Humano, de Doug Engelbart, que incluía NLS (um precursor dos sistemas de hipertexto), no SRI - *Stanford Research Institute*, foi o segundo nó ou ponta. SRI passou a manter as tabelas de "*Host Name*" para o mapeamento dos endereços e diretório do RFC. Um mês depois, quando SRI foi conectado à ARPANET, a primeira mensagem entre servidores foi enviada do laboratório de Kleinrock para o SRI.

Dois outros "nodes" foram acrescentados então: a UC Santa Barbara e a Universidade de Utah. Este dois nós incorporavam projetos de aplicações visuais, com Glen Culler e Burton Fried na UCSB investigando métodos de uso de funções matemáticas para restaurar visualizações na rede e Robert Taylor e Ivan Sutherland em Utah investigando métodos de representação em terceira dimensão na rede.

Assim, no final de 1969, quatro servidores estavam conectados na ARPANET e, mesmo naquela época, os trabalhos se concentravam tanto na rede em si como no estudo das possíveis aplicações da rede. Esta tradição continua até hoje.

Mas foi somente no ano de 1990 que a Internet começou a alcançar a população em geral. Neste ano, o engenheiro inglês Tim Bernes-Lee desenvolveu a *World Wide Web*, possibilitando a utilização de uma interface gráfica e a criação de sites mais dinâmicos e visualmente interessantes. A partir deste momento, a Internet

cresceu em ritmo acelerado. Muitos dizem que foi a maior criação tecnológica, depois da televisão na década de 1950.

A década de 1990 tornou-se a era de expansão da Internet. Para facilitar a navegação pela Internet, surgiram vários navegadores (*browsers*) como, por exemplo, o *Internet Explorer* da Microsoft e o *Netscape Navigator*. O surgimento acelerado de provedores de acesso e portais de serviços online contribuiu para este crescimento.

A internet passou a ser utilizada por vários segmentos sociais. Os estudantes passaram a buscar informações para pesquisas escolares, enquanto jovens a utilizavam apenas por diversão em sites de games.

As salas de chat tornaram-se pontos de encontro para um bate-papo virtual a qualquer momento. Desempregados iniciaram a busca de empregos através de sites de agências de empregos ou enviando currículos por e-mail.

As empresas descobriram na Internet um excelente caminho para melhorar seus lucros e as vendas *online* dispararam, transformando a Internet em verdadeiros *shoppings centers* virtuais.

Nos dias atuais, é impossível pensar o mundo sem a Internet. Ela tomou parte dos lares de pessoas do mundo todo. Estar conectado a rede mundial passou a ser uma necessidade de extrema importância. A Internet também está presente nas escolas, faculdades, empresas e diversos locais, possibilitando acesso às informações e notícias do mundo em apenas um click.

3 - REDES SEM FIO - WIRELESS

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. Sendo assim, o *Wireless* combina a mobilidade do usuário com a conectividade e a velocidades elevadas de até 155 Mbps, em alguns casos.

Segundo de Engst& Fleischman (2005):

> As redes wireless seguem as mesmas características de todos os dispositivos sem fio. Um transceptor envia sinais através de ondas de radiação eletromagnética, que se propagam a partir de uma antena que recebe estes sinais propagados nas frequências corretas.

Este tipo de rede pode ser aplicado no monitoramento, rastreamento, coordenação e processamento em diferentes contextos. Por exemplo, podem-se interconectar sensores para fazer o monitoramento e controle das condições ambientais numa floresta, oceano ou um planeta. A interconexão de sensores através de redes sem fio, com a finalidade de executar uma tarefa de sensoriamento maior, irá revolucionar a coleta e processamento de informações.

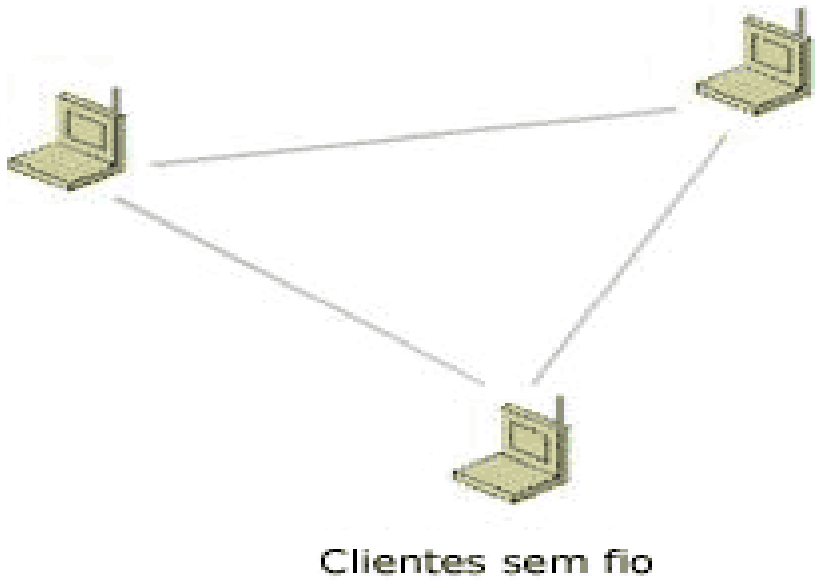
As redes locais sem fio já são uma realidade em vários ambientes de redes, principalmente nos que requerem mobilidade dos usuários. As aplicações são as mais diversas e abrangem desde aplicações médicas, por exemplo, visita a vários pacientes com sistema portátil de monitoramento, até ambientes de escritório ou de fábrica.

Figura 1 – Rede sem fio

Apesar das limitações de cobertura geográfica, utilizando-se a arquitetura de sistemas de distribuição, pode-se aumentar a abrangência da rede sem fio, fazendo uso de vários sistemas de distribuição interconectados via rede com fio, num esquema de *roaming* entre micro células, semelhante a um sistema de telefonia celular convencional.

Para que qualquer tecnologia seja aceita é necessária a criação de um padrão na indústria para que seja garantida a compatibilidade e confiabilidade entre equipamentos de vários fabricantes. Atualmente a organização responsável pelo desenvolvimento destes padrões é o IEEE –*Institute of Eletricaland Electronics Engineers*. (BASTOS, 2003)

As redes sem fio,



denominadas 801.11, necessitam de determinados componentes para sua adequada operação, e a utilização de ondas de rádio para a transmissão entre as estações, é uma delas e os diversos tipos de equipamentos como: placas de Interconexão de Componentes Periféricos (PCI), internas, placas de Barramento Serial Universal (USB), externas, e adaptadores de placas *ethernet*, permitem o acesso a estas redes. Dos principais padrões de redes sem fio, se destacam a Interoperabilidade Mundial para Acesso por Microondas (*Wi Max)*, *Bluetooth*, *Wi-Fi* e Infravermelhos *Infra Red*. Tanto o *Wi Max* como o *Bluetooth* são utilizados para comunicação entre pequenos dispositivos de uso pessoal. (TORRES 2001)

O padrão IEEE 802.11 foi o primeiro padrão definido para as redes sem fio. Essas redes até então trabalhavam na freqüência de 2.4 GHz, suportando velocidades de até 2 Mbps Ao longo do tempo foram criados vários grupos dentro do IEEE 802.11, conhecidos como grupos tarefa (*Task Groups*) que definiram novas características operacionais e técnicas para as redes sem fio. (ROSNAM; LEARY, 2003).

Para mover *frames* de estação para estação, o padrão utiliza meio sem fio. Inicialmente, uma camada física de radio frequência e uma de infravermelho foram padronizadas, no entanto, as de radio frequência provaram ser mais popular. (GAST, 2002).

Estações são dispositivos computacionais com interfaces de rede sem fio. Normalmente estações são *notebooks* ou computadores de mão como os *hand helds*; porém não é necessário que as estações sejam computadores portáteis. A utilização de redes sem fio não se dá apenas pela mobilidade, mas também pelo fato e não precisar da instalação de cabos e pela sua flexibilidade, facilitando quaisquer mudanças que possam ser feitas na estrutura de uma organização. Qualquer dispositivo que contenha uma IEEE 802.11 conforme MAC e camada física. (STALLINGS, 2001).

3.1 - Segurança em redes sem fio

As perspectivas futuras fazem da internet um meio atraente para as empresas com a popularização das tecnologias, como a *Wireless*, mergulhando num nível cada vez mais elevado de interatividade e movimento na Web, encontrando formas

criativas de aproveitar esse nicho para maximizar seus lucros, antevendo aí uma estratégia de *marketing*.

Com a expansão da conectividade em banda larga, diversas aplicações têm sido desenvolvidas e um estudo sobre a viabilidade da aplicação das tecnologias das redes sem fio na área de saúde, educação, para o ensino à distância, das teleconferências, no monitoramento de segurança, mecanismos de controle, seja nos ambientes industriais, residenciais, no tráfego, nas florestas e mares, ou para fins militares, seria interessante e útil.

Entretanto, a existência de certa fragilidade que todo novo conceito pode apresentar no aspecto de sua evolução, o problema com a segurança de dados que o sistema transporta se evidencia numa constante preocupação dos usuários.

A primeira rede sem fio foi criada em 1970, com o objetivo de conectar quatro ilhas na qual situavam os *campi* da universidade do Havaí. Mais tarde, na década de 80, as redes sem fio são inseridas na computação pessoal. (LACERDA, 2007)

No início as redes sem fio utilizavam transceptores infravermelhos e não ondas de rádio, o que fazia com que os serviços fossem de baixa qualidade e confiabilidade, devido a constantes quedas e um alto grau de interferências. As redes sem fio com tecnologia de ondas de rádio tiveram destaque no início da década de 90, quando os processadores evoluíram o suficiente para gerenciar os dados enviados e recebidos nesta tecnologia (ENGST & FLEISCHMAN (2005).

Para superar os problemas de segurança, as organizações devem determinar processos específicos e bem definidos para o uso de dispositivos sem fio, desde as funções na qual ele será usado, o que será armazenado nesses dispositivos e qual a segurança aplicada a eles para evitar que os dados sejam comprometidos em uma situação de exceção. Desta forma, políticas e padrões são fundamentais, pois uma rede sem fio deve operar sobre o preceito de que existem nodos maliciosos dispostos a obter e manipular dados indevidos. (SOUZA, SILVA, GUIMARÃES (2009), apud TORRES 2001; LACERDA (2007)

Muitas vezes o mais importante para uma empresa que utiliza redes sem fio não são as informações que trafegam em suas redes, mas a capacidade de mantê-las seguras, por isso muito se investe, principalmente com os protocolos, chaves e regras, para tentar amenizar essa insegurança. A proteção dos dados trafegados na rede pode ser realizada com base em diversas estratégias, destacando-se a

criptografia, que permite que os dados trafeguem fora de uma ordem lógica e compreensível.

As redes sem fio oferecem várias formas de proteção, exigindo domínio técnico para sua instalação e configuração, com o objetivo de minimizar os riscos de invasões. Como exemplo, o posicionamento físico dos equipamentos na rede determina um melhor desempenho do sistema, diminuindo a probabilidade de acessos não autorizados e demais tipos de ataque. Durante sua configuração e disposição dos equipamentos, devem ser observados os padrões em uso e a potência dos equipamentos.

Existem alguns protocolos, citados em artigo apresentado por Souza, Silva e Guimarães, para aprimorar a segurança das redes sem fio que serão vistos a seguir:

O algoritmo de criptografia Privacidade Equivalente (WEP21) é parte do padrão IEEE 802.11 - ratificado em Setembro de 1999 e se utilizava para proteger redes sem fios do tipo, *Wi-Fi*. Este algoritmo opera na camada de enlace e utiliza o método criptográfico Roteamento Coloniale4 (RC4) da Empresa RSA Data Security, Inc.

Trata-se de um Algoritmo para Criptografia de Chave Pública que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secrets hared key*) de 40 ou 104 bits. O IV é concatenado à *secrets haredkeyes* forma uma chave de 64 ou 128 bits, que é utilizado para criptografar as informações.

O WEP também utiliza o Ciclo de Checagem de Redundância (CRC-32) para calcular a Soma de Verificação (*checksum*) da mensagem que é inclusa no pacote, o que garante a integridade dos dados. Então, o receptor recalcula o *checksum* para garantir que a mensagem não foi alterada. Provê recursos de criptografia de 128 bits integrados com os equipamentos da rede 802.11.

As chaves criptográficas são simétricas, porém não são gerenciáveis e podem ser descobertas por usuários mal-intencionados. Como prevenção a esta situação, existe um mecanismo que permite que estas chaves sejam atualizadas em intervalos regulares, dificultando seu processo de quebra.

A principal desvantagem do WEP é possibilitar que um atacante que deseja ter acesso à rede possa, por meio de escuta, obter a chave, tornando possível a descriptação dos dados da rede. Outra desvantagem observada é que a chave deve ser conhecida por todos que acessam a rede, o que pode facilitar a distribuição não

autorizada da chave. (SOUZA, SILVA, GUIMARÃES, 2009, apud MACIEL, 2003; ARTHAS, 2004)

Apesar da suas vulnerabilidades, o WEP é uma camada adicional na segurança da rede sem fio. Para corrigir as falhas no WEP, foi criado outro protocolo de criptografia mais robusto, o WPA. (SOUZA, SILVA, GUIMARÃES, 2009, apud MACIEL, 2003; ARTHAS, 2004)

O *Wi-Fi* de Acesso Protegido (WPA) é um subconjunto do padrão de segurança 802.11 baseado no 802.11. A Wi-Fi Alliance, em parceria com o IEEE, criou o protocolo WPA para fornecer um tratamento mais seguro e ao mesmo tempo compatível com o hardware utilizado pelo WEP. Desta forma, a atualização do *firmware* dos dispositivos *Wi-Fi* que utilizam o WEP pode ser migrada para WPA sem mudanças em sua arquitetura.

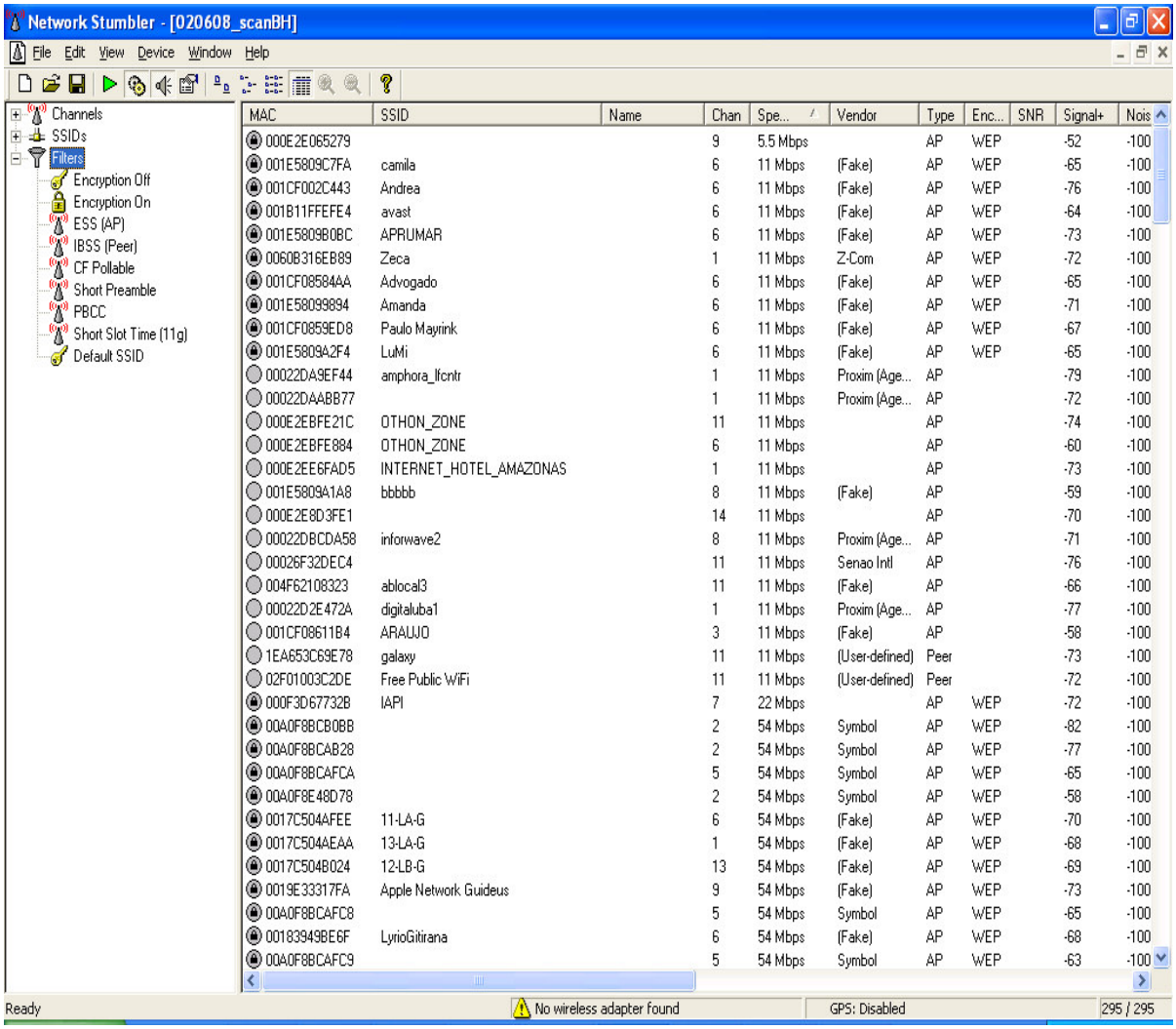
O WPA possui formas de autenticação, privacidade e controle de integridade das informações mais sofisticada que o WEP. Porém, no WPA, ao contrário do WEP, inexiste suporte para conexões *Ad-Hoc*. (SOUZA, SILVA, GUIMARÃES, 2009, *apud* MACIEL, 2003; ARTHAS, 2004)

O WPA é implementado para atender a substituição do WEP, cifrando as informações e garantindo a privacidade do tráfego, e autenticar o usuário via padrões 802.1x e Protocolo de Autenticação Extensiva (EAP). Para cifrar os dados, o WPA utiliza duas técnicas. A primeira é direcionada para pequenas redes através de uma chave previamente compartilhada (*pré-sharedkey* ou WPA-PSK), que é responsável por reconhecer o dispositivo pelo concentrador. A outra técnica utiliza um Servidor de Autenticação Remota (RADIUS). (SOUZA, SILVA, GUIMARÃES, 2009, *apud* MICROSOFT).

O sistema de compartilhamento da chave é semelhante ao WEP, cuja troca das chaves é feita manualmente, o que caracteriza sua melhor indicação para redes de pequeno porte, onde os dispositivos estão acessíveis na maior parte do tempo. (SOUZA, SILVA, GUIMARÃES, 2009, *apud* MICROSOFT) Esta chave, em conjunto o endereço do Controle de Acesso de Mídia (MAC) do transmissor, forma outra chave chamada Chave de Endereço Temporária Transmissão (TTAK), conhecida como “Chave da 1ª fase.” (SOUZA, SILVA, GUIMAREÃES apud LACERDA, 2007).

Tela principal do *NetStumbler* em modo de Varredura:

Figura 2 -Tela NetStumbler em modo Varredura:



é gerada de acordo com o endereço MAC das estações. Inclusive, pode ser programado para alterar o IV a cada pacote trafegado na rede, por sessão ou período, o que torna a captura mais difícil da transmissão. (SOUZA, SILVA, GUIMAREÃES *apud* LACERDA, 2007; MICROSOFT).

Para melhor identificar o método de criptografia utilizado pelas redes sem fio, torna-se necessária a apresentação do modo de funcionamento do algoritmo criptográfico RC4, criado em 1987. (SCHNEIER, 1996).

O algoritmo RC4 funciona como um algoritmo de fluxo, ou seja, é utilizado para enviar um conjunto de bits cifrados em um fluxo contínuo. Neste tipo de algoritmo, não se pode esperar o acúmulo de certo número de bits para transmitir. É classificado como sendo de chave simétrica, ou seja, a chave de cifragem é a mesma de decifragem.

O RC4 cria bytes pseudoaleatórios a partir de uma semente de tamanho variável. Estes bytes formam a chave de criptografia que será utilizada para encriptar uma mensagem, através de operações XOR *bit* a *bit*. Ao receber esta mensagem cifrada, o destinatário deve executar o algoritmo da mesma maneira (realizando XOR bit a bit com a mesma chave), recuperando a mensagem. A criação da chave RC4 funciona da seguinte maneira:

- o RC4 recebe uma semente K de n *bits* (entre 1 e 2048). A partir desta semente, cria um vetor *S* de 256 bytes. Este vetor tem suas posições permutadas, de acordo o valor da semente;
- com o vetor formado, o algoritmo utiliza seus dados para criar uma sequência de números pseudoaleatórios para criptografar a mensagem. Conforme a mensagem vai sendo enviada, o vetor *S* tem seu conteúdo alterado.

A figura 3 apresenta o código KSA - Key *Scheduling Algorithm*, utilizado para permutar o vetor S, e o código PRNG para gerar os números pseudoaleatórios. Sendo: *K*: segredo compartilhado; *N*: número de posições do vetor *S*, *l*: tamanho da chave *K* (em bytes).

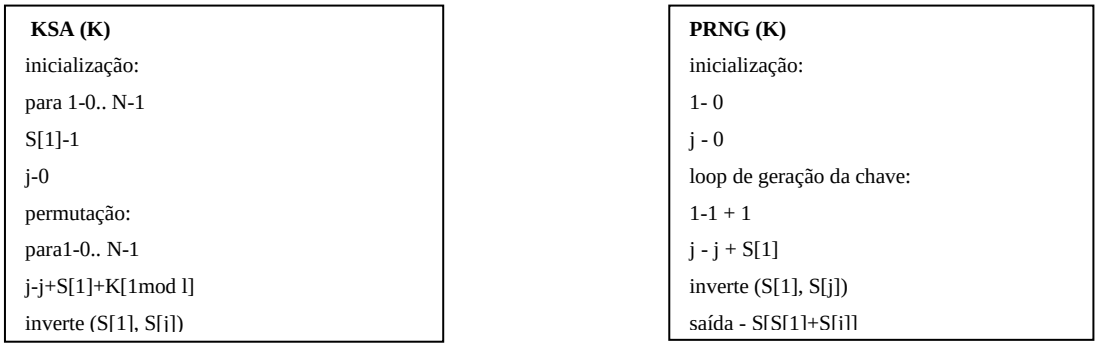
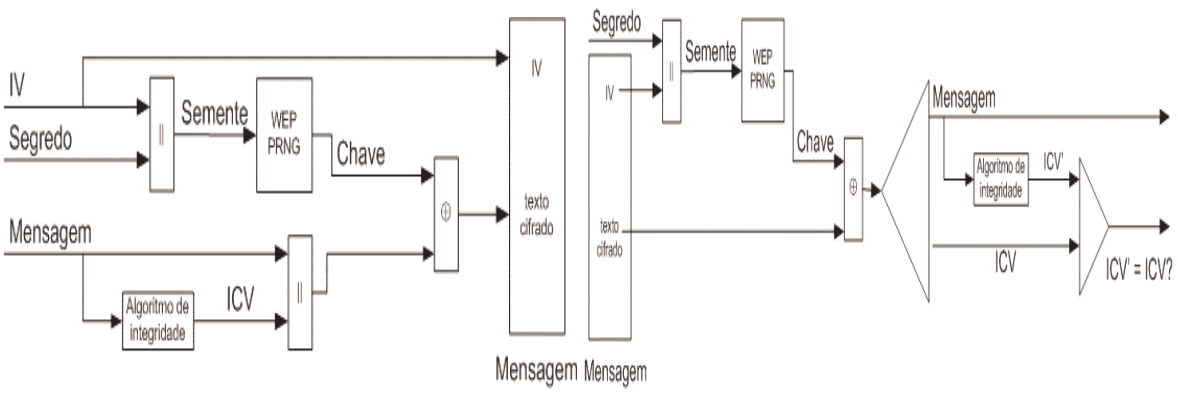


Figura 3 – algoritmos KSA e PRNG

O protocolo WEP funciona utilizando o gerador de números PRNG, do RC4. A semente para geração da chave é uma combinação do segredo compartilhado com um vetor aleatório de 24 *bits* chamado IV (*Initialization Vector*). Para cada quadro, o protocolo WEP deve selecionar um IV diferente, permitindo que a chave secreta permaneça a mesma, enquanto a semente é alterada, mantendo o sincronismo.

Como o destinatário da mensagem deve criar a chave de decifragem a partir da mesma semente, o remetente envia o IV escolhido sem criptografia com o quadro. Desta forma, o destinatário pode unir o segredo compartilhado com o IV escolhido e utilizar estas informações como semente no PRNG.

Para verificar que os dados não foram alterados durante a comunicação, é utilizado um algoritmo redundante do tipo CRC-32 (*Cyclic Redundancy Check*) denominado ICV – *Integrity Check Value*. O esquema do Funcionamento do WEP é apresentado na figura 4, sendo (a) esquema de cifragem e (b) decifragem.



(a) Cifragem (b) Decifragem

Figura 4 – protocolo WEP cifragem e decifragem

Para que o WEP possa prover segurança, uma chave nunca deve ser reutilizada, isto é muito importante, pois no momento em que o número de possíveis IVs for esgotado, o segredo deverá ser modificado. O motivo deste fato vem da possibilidade de um atacante obter uma chave (não a semente, mas a chave utilizada nas operações XOR) e com ela obter os dados cifrados com a mesma chave em outro momento.

O EAP é um modelo para autenticação também definido no WPA, que utiliza o padrão 802.1x e possibilita inúmeras formas de autenticação, inclusive certificação digital. Este padrão pode trabalhar em conjunto com outras tecnologias, como o servidor de autenticação RADIUS. (SOUZA, SILVA, GUIMAREÃES *apud* MICROSOFT).

O 802.1x utiliza o protocolo EAP para gerenciar a forma como a autenticação mútua será feita na rede. Ele possibilita a escolha de um método específico de autenticação a ser utilizado como senhas, certificado digital ou *tokens* de

autenticação. O autenticador não precisa entender o método de autenticação, ele simplesmente transmite os pacotes EAP do usuário a ser autenticado para o servidor de autenticação e vice-versa. Os Pontos de Acesso 802.1X sem fio podem ser configurados como clientes RADIUS para que possam ser enviadas solicitações de contas e acesso para os servidores RADIUS que executam o Servidor de Autenticação Interna (IAS).

O IAS controla a autenticação dos usuários e dispositivos à rede por meio de diretivas de acesso remoto centralizado. São vários os tipos de EAP que suportam os diversos métodos de autenticação:

• EAP-LEAP(Cisco de pouco peso - EAP): Elaborado pela CISCO Systems– Fabricante de dispositivos de rede, usa o conhecido método de usuário e senha para enviar a identidade do usuário à ser autenticado no servidor;

• EAP-TLS(Camada de Segurança de Transporte): Utiliza o certificado X.509 que é o padrão que especifica os certificados digitais para autenticação. Foi especificado no padrão de especificação para *Internet* RFC;

• PEAP(EAP Protegido): Mais popularizado pela Microsoft nos sistemas operacionais Windows XP e Server 2003, oferece autenticação baseada em senha e exige que o servidor de autenticação possua um certificado digital, porém não exige certificados nos clientes.

Entre o WPA e o WPA2, a principal diferença está no método criptográfico. O WPA

utiliza o TKIP com RC4, enquanto o WPA2 utiliza Norma de Encriptação Avançada (AES) em conjunto com o TKIP e chave de 256 bits, que é um método de criptografia mais seguro.

O AES permite chaves de 128, 192 e 256 bits, tendo então uma ferramenta criptográfica muito mais poderosa. Já no WPA2, a chave de 256 bits é padrão. Com o AES no mercado, houve uma necessidade de computadores com hardware mais evoluído, capazes de realizar o processamento criptográfico. Os dispositivos WPA2 são integrados por um coprocessador para realizar os cálculos da criptografia AES. . (SOUZA, SILVA, GUIMARÃES, 2009, *apud* MICROSOFT.

4 – PESQUISA

Foi feita uma pesquisa através da imagem tirada no centro de Assis-SP, no edifício Capitão Assis, na Avenida Rui Barbosa, para mensurar o grau de segurança das redes de internet, nessa região.

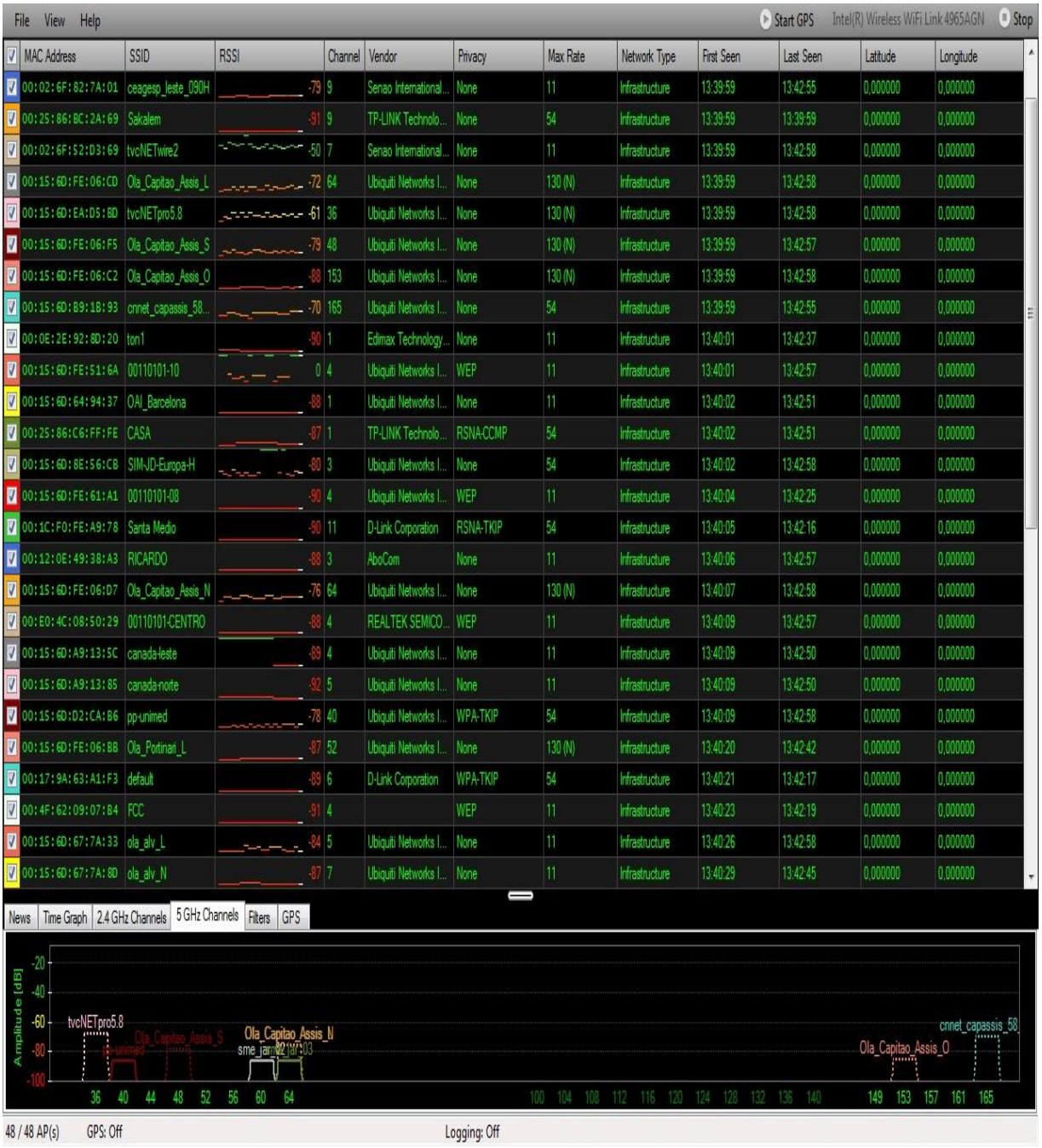


Figura 5 – Imagem da região central da Avenida Rui Barbosa, em Assis – SP.

Decodificando algumas informações para melhor compreensão da leitura da imagem a figura 5:

MAC ADDRESS = O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet. (Exemplo= 00:00:5E:00:01:03)

SSID: Nome da rede, cada pessoa coloca um nome para o reconhecimento.

RSSI: potência em porcentagem como forma de medir a potencia do sinal.

CHANNEL: cada aparelho, ao fazer a configuração tem as opções de 1 a 12. É necessário fazer essa varredura para que não fiquem vários equipamentos no mesmo canal, e com isso causando lentidão na rede da internet de ambas as partes.
VENDOR: Nome do roteador ou equipamento transmissor.
PRIVACY: tipo de segurança utilizada, que pode ser: NONE, WAP e WPA2
NONE: é quando esta aberta a rede sem criptografia.
MAX RATE:= potência do roteador por megas.

As redes criptografadas, na maioria dos casos utilizam o método WEP, cuja segurança é falha e facilmente quebrável com um programa especialista.

A segurança é um ponto fraco das redes sem fio, pois o sinal propaga-se pelo ar, por isso devemos utilizar medidas de proteção, para deixarmos de estar vulnerável para invasões.

Os principais tipos de segurança são: WEP, WPA e WPA2.

O protocolo tipo WEP é a opção de segurança recomendada caso não haja suporte para WPA.

O tipo de segurança WAP inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

O protocolo de segurança WPA2 utiliza Norma de Encriptação Avançada (AES) em conjunto com o TKIP e chave de 256 bits, que é um método de criptografia mais seguro, (numérico, símbolos e caracteres).

4.1 – Resultados Obtidos

Ao realizar a varredura na Avenida Rui Barbosa, no centro da cidade de Assis-SP, foram encontrados vários tipos de redes sem fio com as mais diversas formas de segurança ou até mesmo com a falta dela. Dentre as redes encontradas, podem-se citar como exemplo, redes abertas, fechadas e fechadas com criptografia.

Das vinte e seis redes encontradas no trajeto, quatro eram criptografadas, dezoito são redes abertas sem qualquer tipo de segurança, duas utilizam o padrão WAP2, o que se tem de melhor no mercado em questão de segurança e uma utiliza o padrão RSNA-TKIP. As velocidades variam entre 5.5 Mbps e 54 Mbps, ficando a grande maioria com a maior taxa de transmissão.

Pode-se analisar, pelos dados obtidos, que a população dessa região da Avenida Rui Barbosa, em Assis-SP, utiliza das seguintes redes: uma baixa porcentagem é criptografada e 100% dessa criptografia é o protocolo WEP, cuja velocidade de transmissão da maioria dessas redes mapeadas é de 54 Mbps.

Das redes encontradas, observamos um grande número que não possuíam nível de segurança adequado que pode provocar acessos maliciosos até mesmo por parte de usuários mal intencionados que sejam inexperientes. À medida que a popularização de redes sem fio aumenta e cada vez mais usuários inexperientes as configuram em casa ou no trabalho, observa-se uma falta de segurança preocupante.

Os assistentes de configuração têm se tornado a fonte usada pelos usuários para garantir a segurança dos dados. Entretanto, estes assistentes se valem, em sua maioria, da criptografia WEP, segundo os achados deste estudo. Ora, conforme vimos pela literatura, esta forma de segurança é a mais precária, tornando a rede vulnerável a ataques. Fica claro que os usuários de redes sem fio da região pesquisada não valorizam uma segurança maior em suas redes, provavelmente por falta de embasamento.

Mesmo com níveis de segurança implementados nas redes sem fio, elas sempre apresentarão riscos e vulnerabilidades. Em qualquer caso, o cliente e o concentrador são sempre alvo de ataques e possíveis falhas, devendo receber atenção especial e constante.

O avanço da tecnologia e a disseminação das redes sem fio, não resolveram alguns problemas, tais como o armazenamento da senha, tanto para o cliente quanto para servidor. Até mesmo os certificados digitais estão vulneráveis a ataques. Ainda como uma solução para essa insegurança, tem-se os cartões e *tokens* processados, com objetivo de diminuir as possibilidades de fraude e cópia de informações confidenciais.

5. CONSIDERAÇÕES FINAIS

Pode-se, após análise dos dados pesquisados, perceber que, apesar da evolução na tecnologia das redes sem fio, o quesito segurança ainda se encontra um pouco vulnerável quando se trata de transporte de dados na rede, onde eles podem ser alvo de ataques de alguns malfeitores. Mas não podemos negar também que estudos existem para encontrar uma maneira de sanar este problema e a

criptografia é um deles, que vem encontrando credibilidade por parte dos estudiosos no assunto e também pelos usuários.

Tecnicamente, as redes sem fio apresentam uma série de vulnerabilidades que tem origem na concepção do padrão. A melhor forma de garantir um acréscimo de segurança neste tipo de ambiente é através de políticas e procedimentos de segurança específicos para esta nova tecnologia. Uma política específica para redes sem fio envolve, no mínimo, a configuração cuidadosa dos equipamentos utilizados ou a limitação dos equipamentos que podem acessar a rede, dificultando a operação de atacantes. Manter registros das atividades na rede e sistemas de identificação de intrusão e em redes onde as informações internas da instituição são confidenciais, os pontos de acesso de dispositivos sem fio deve ser considerado como pontos de acesso público.

Infelizmente estes procedimentos acarretam queda de desempenho da rede, e maior consumo de energia dos dispositivos sem fio, alimentados por baterias. Este fato é uma barreira na utilização destas medidas de segurança e também interfere na análise de possíveis padrões de segurança que possam vir a ser adotados. Mesmo em casos onde os custos da utilização de mecanismos de segurança extras são válidos, sabe-se que são possíveis ataques bem sucedidos em redes sem fios.

Um dos fatores que causam preocupação é o desconhecimento dos usuários a respeito da segurança que sua rede lhe oferece. À medida que a popularização das redes sem fio aumenta, cada vez mais usuários inexperientes configuram-nas em casa ou no trabalho, nisso observa-se uma falta de segurança.

Como se percebe, já existe dispositivo no mercado que pode ser utilizado para sanar essa falha, no entanto, fica claro que os usuários de redes sem fio, da região pesquisada, não valorizam uma segurança maior em suas redes, provavelmente por falta de embasamento, por isso se tornam alvo fácil de pessoas inescrupulosas que interceptam as informações que trafegam na rede.

6 – REFERÊNCIAS

Bibliográficas:

ENGST, Adam; FLEISHMAN, Glenn. Kit do Iniciante em Redes Sem Fio: O guia prático sobre redes Wi-Fi para Windows e Macintosh.2ª ed. São Paulo. Pearson Makron Books, 2005.

GAST. M. S. 802.11 Wireless Networks: The Definitive Guide. 1. Ed. [S.1.]: O' Reilly, 2002. 464 p.

LACERDA, Pablo de Souza. Análise de Segurança em Redes Wireless 802.11x.Universidade Federal de Juiz de Fora, 2007, 49.

ROSNAM, P.; LEARY, J. **Wireless LAN Fundamentals**. 1. ed.: Cisco Press, 2003.

RUFINO, Nelson Murilo de O. **Segurança em redes sem fio.** 2. ed. São Paulo: Novatec,
2005.

SCHNEIER, Bruce. **Applied Cryptography. Second Edition: protocols, algorithms, and source code in C**. John Wiley & Sons Inc. 1996.

TALLINGS, William. Wireless Communications and Networking, Library of Congress Cataloging-in-Publication, 2001.

TORRES, Gabriel; Redes de Computadores. Curso Completo; Editora Axcel Books do Brasil, 2001; Pags. 258 a 271.

Eletrônicas:

ARTHAS, Kael. Tutorial Wireless. 2004. Disponível em: http://www.babooforum.com.br /idealbb/view. asp?topicID=269602.

BARRY, M. Leiner. **A brief history of the internet.** Disponível em: http://www.aisa.com.br/historia.html#intro

BASTOS, A. Arquitetura IEEE 802.2003. Disponível em: http://www.dei.isep.pt/i802.html

MICROSOFT. Configurando Redes Sem Fio IEEE 802.11 Com Windows XP Para Residências e Pequenas Empresas. 2005. Disponível em http://www.microsoft.com/brasil/security/gui/dance/prodtech/winxp/wifisoho.mspx

_____. Decisão sobre uma Estratégia de Rede sem Fio Protegida. 2004. Disponível em: http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx

_____. Usando o 802.1X e a Criptografia Para Proteger WLANs.Disponível em: http://www.microsoft.com/brasil/security/gui dance/topics/wireless/secmod172.mspx

_____. Visão Geral da Atualização de Segurança WPA Sem Fio no Windows XP. 2005. Disponível em: http://support.microsoft.com/kb/815485/pt-br

SILVA, A. J. S. **As tecnologias de redes wireless.** Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa 15 de maio de 1998 | volume 2, número5. Disponível em: http://www.rnp.br/newsgen/9805/wireless.html