CENTRO UNIVERSITÁRIO FEEVALE

MARCELO TONIOLLO

SEGURANÇA DE REDES MANET: UMA ANÁLISE SOBRE CRIPTOGRAS WEP, WPA E WPA2

Novo Hamburgo, Novembro de 2008.

MARCELO TONIOLLO

SEGURANÇA DE REDES MANET: UMA ANÁLISE SOBRE CRIPTOGRAS WEP, WPA E WPA2

Centro Universitário Feevale
Instituto de Ciências Exatas e Tecnológicas
Curso de Ciência da Computação
Trabalho de Conclusão de Curso

Professor Orientador: MS. Vandersilvio da Silva

Novo Hamburgo, Novembro de 2008.

RESUMO

Nos dias atuais, a informação tornou-se um bem valioso, havendo assim, uma significativa busca por meios rápidos de troca de dados. As redes wireless, principalmente as *MANET*, ou *Ad-hoc* têm se mostrado muito úteis neste tipo de situação, já que não dependem de nenhuma estrutura física para que exista comunicação entre os dispositivos que estejam trocando informações. Isso permite que a interação entre eles possa ocorrer em qualquer lugar sem dificuldades. Porém este tipo de rede tem mostrado uma deficiência, sua segurança é facilmente burlada por invasores. Por esse motivo o emprego de alguns mecanismos como a criptografia é necessário para manter sua total funcionalidade, porém, mesmo ela pode ser quebrada, conforme comprovado no experimento realizado utilizando três criptografias diferentes para essa configuração de rede.

Palavras-chave: *Wireless, MANET, Ad-Hoc*

ABSTRACT

Currently, there therefore significant searches for one quick data exchange methods. The wireless networks, especially as MANET, or Ad-hoc has been very useful in this kind of situation, which do not depend on any physical structure so that there is communication between devices that to exchanging information. This allows the interaction between them can occur anywhere without difficulties. But this type of network has shown a disability, their safety is easily broken by invaders. Hence the employment of some mechanisms such as encryption is needed to maintain its full functionality, even though it may be broken, as evidenced in the experiment carried out using three different encryption for the network configuration.

Key words: *Wireless, MANET, Ad-Hoc*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

MANETS	*Mobile Ad-hoc Networks*
U.S DARPA	*United States Defense Advanced Research Projects Agency*
PRNET	*Packet Radio Network*
SURAN	*Survivable Adaptive Network*
GLOMO	*Global Mobile Information Systems*
AP	*Acess Point*
DSR	*Dynamic Source Routing Protocol*
DSDV	*Dynamic Destination-Sequenced Distance-Vector Routing*
AODV	*Ad Hoc On-Demand Distance Vector Routing Protocol*
MIT	*Massachusetts Institute of Technology*
RSA	*Rivest, Shamir and Adleman*

SUMÁRIO

INTRODUÇÃO

Na última década, os avanços tecnológicos relacionados às redes de computadores tornaram informações e recursos computacionais acessíveis de praticamente qualquer lugar que disponha de um meio para recebimento e envio destes dados.

Um dos principais fatores que contribuiu para o aumento dessa acessibilidade foi o surgimento das redes *wireless*, uma tecnologia que permite a conexão entre diferentes pontos sem a necessidade do uso de cabos, sejam eles telefônicos, coaxiais ou ópticos, conforme (WIKIPEDIA, 2008). Ao invés disso os equipamentos se utilizam de radiofreqüência (comunicação via ondas de rádio) ou comunicação via infravermelho.

As redes móveis podem, quanto a sua estrutura de acesso, ser classificadas de duas maneiras: Estruturadas e Não-estruturadas.

A arquitetura básica de uma rede *wireless* estruturada é bastante simples, ela consiste na troca de dados entre computadores, através de um *acess point*, que recebe o dado do dispositivo que o está enviando e o repassa para o destinatário.

As redes *MANET*, ou *Ad-hoc*, são redes *wireless* que se diferenciam das estruturas mais conhecidas por não possuírem uma infra-estrutura fixa, ou seja, são redes não estruturadas. Essas redes são compostas de computadores, chamados nodos, que tem a responsabilidade de controlar e distribuir o tráfego de informações, para se comunicarem diretamente entre si.

Um problema corriqueiro desse tipo de rede ocorre principalmente pelo meio de transmissão dos dados, ou seja, radiofreqüência, infravermelho ou qualquer que seja o tipo de tecnologia *wireless* utilizada. Ao contrário das redes convencionais, compostas por um meio físico de conexão, as informações das redes *MANET* ficam livres, podendo ser acessadas de qualquer equipamento que esteja na área de influência da mesma. Sendo assim, estas informações correm o risco de sofrer acessos de indivíduos não autorizados.

A segurança dessas redes é um ponto fundamental para a opção pela utilização desta topologia. Sendo assim, é necessário que seja utilizada uma criptografia que possa proporcionar um bom grau de segurança e privacidade aos usuários.

O primeiro capítulo aborda um apanhado geral sobre a segurança de redes em um modo geral, definindo quem são os intrusos que buscam acessar indevidamente uma rede e quais são seus objetivos ao executarem este ato. São abordados também quais os tipos de ataques possíveis de serem lançados sobre uma rede, além de quais os serviços de segurança são necessários para que a integridade da mesma seja mantida.

O capítulo dois faz um apanhado geral sobre as redes *MANET*, descrevendo sua história, áreas de aplicação, uma breve explicação sobre o funcionamento de seus protocolos de roteamento, suas vulnerabilidades e, por fim, quais as criptografias possíveis de serem aplicadas a essa rede.

O capítulo três fornece informações sobre quais são os objetivos do experimento e quais métodos serão utilizados para e execução do mesmo, apresentando também, as ferramentas disponíveis.

Na seqüência, são apresentados os detalhes sobre o experimento, bem como, os resultados obtidos durante a execução dos experimentos.

1 SEGURANÇA DE REDES

Quando buscamos uma solução para problemas de segurança em uma determinada rede, devemos primeiramente identificar de onde partem as principais ameaças, quais são estas ameaças e, posteriormente, estudar soluções para dificultar ao máximo que o invasor tenha êxito em sua investida.

1.1 Fontes de ameaças à segurança de redes

A popularização dos computadores pessoais durante a década de 90 abriu portas para que não somente indivíduos especializados realizem ataques as redes. Segundo Carvalho (2006), "dá-se o nome de atacante à pessoa que realiza um ataque (tentativa de comprometimento ou invasão) a um sistema computacional, obtendo êxito ou não", definindo também os principais grupos de atacantes, conforme Caletti(2006), da seguinte maneira:

- ***Script Kiddies*:** também chamados de *Newbies*, são conhecidos por terem um baixo grau de conhecimento e utilizarem ferramentas da Internet para invadir sistemas. Eles compõem a maioria dos atacantes existentes atualmente e não possuem um alvo específico;

- ***Hackers*:** possuem um elevado grau de conhecimento. Invadem sistemas sem o intuito de danificá-los, considerando o mesmo, um desafio;

- ***Crackers*:** possuem um elevado grau de conhecimento e o usam para roubar informações e destruir sistemas;

- ***Carders*:** fazem compras pela Internet com cartões de créditos gerados ou roubados;

- ***Cyberpunks*:** possuem um alto grau de conhecimento e se preocupam com a privacidade, publicando falhas de sistemas para que as empresas responsáveis possam corrigi-las;

- ***Insiders*:** são funcionários ou ex-funcionários de uma determinada empresa e tem por objetivo o roubo de informações sigilosas ou o comprometimento dos sistemas da empresa;

- ***Coders*:** são disseminadores de conhecimento. Escrevem programas, livros, artigos e ministram palestras sobre o que já fizeram. Geralmente são hackers famosos que atualmente estão na legalidade;

- ***White Hats*:** através de testes de invasão e análises de segurança, divulgam as vulnerabilidades encontradas para empresas contratantes ou para o público em geral;

- ***Black Hats*:** Invadem sistemas com o intuído de conseguir informações que lhes dê algum retorno financeiro;

- ***Phreackers*:** são responsáveis por fraudes telefônicas. Atualmente o maior alvo deles é a telefonia celular.

1.2 Tipos de ataque às redes

Não importando quem planeja o ataque a uma rede, segundo (Demski, 2000) esse ataque basicamente busca por no mínimo um dos seguintes objetivos:

- **Interceptação:** O atacante busca informações as quais ele não tem permissão de acesso;

- **Interrupção:** O atacante compromete o tráfego de dados pela rede, assumindo o controle do canal de transmissão;

- **Modificação:** Dados são modificados por pessoal não autorizado;

- **Inclusão:** Dados são incluídos em um determinado sistema por um invasor.

1.3 Serviços de segurança

Visando garantir certo grau de segurança nas redes, diversos mecanismos de segurança foram desenvolvidos para manter pessoas não autorizadas distantes de informações confidencias destas redes. Sendo assim, para que essa rede torne-se segura, segundo Kurose (2006), Steffen (2003), Sêmola (2003), e Stalling (1997) alguns critérios devem ser atendidos para que a rede seja considerada segura:

- **Confidencialidade:** a informação deve estar acessível apenas às pessoas autorizadas, ou seja, deve ser protegida quanto ao acesso de pessoal não autorizado;

- **Integridade:** consiste em garantir que os dados não foram alterados por acidente ou por má intenção. A informação deve estar da mesma forma em que foi disponibilizada pelo seu proprietário;

- **Disponibilidade:** define que os dados devem estar disponíveis quando solicitados;

- **Confiabilidade:** garantir que o sistema continuará atuando conforme o determinado;

- **Não repúdio:** garante que quem executou uma determinada transação eletrônica não poderá posteriormente negar sua autoria.

Esses ataques podem ter quatro níveis de complexidade (STEFFEN, 2003):

- **Um para um:** um atacante utiliza uma máquina para atacar outra;
- **Um para vários:** um atacante utiliza uma máquina para atacar várias máquinas;
- **Vários para um:** um ou vários atacantes utilizam o recurso de várias máquinas para atacar uma máquina alvo;
- **Vários para vários:** um ou vários atacantes utilizam os recursos de várias máquinas para atacar várias máquinas alvo.

2 REDES MANET

As redes *MANET*, mais conhecidas como *AD-HOC*, são redes ainda pouco utilizadas comercialmente. Trata-se de uma rede que não possui um nó ou terminal especial para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos (*Acess Point)*. Desta forma, uma Rede de computadores *Ad-hoc* é aquela na qual todos os terminais funcionam como roteadores, encaminhando de forma comunitária as comunicações provenientes de seus terminais vizinhos, conforme demonstrados na Figura 2.1 – Redes Wireless Não Estruturada (*Ad-Hoc)*.

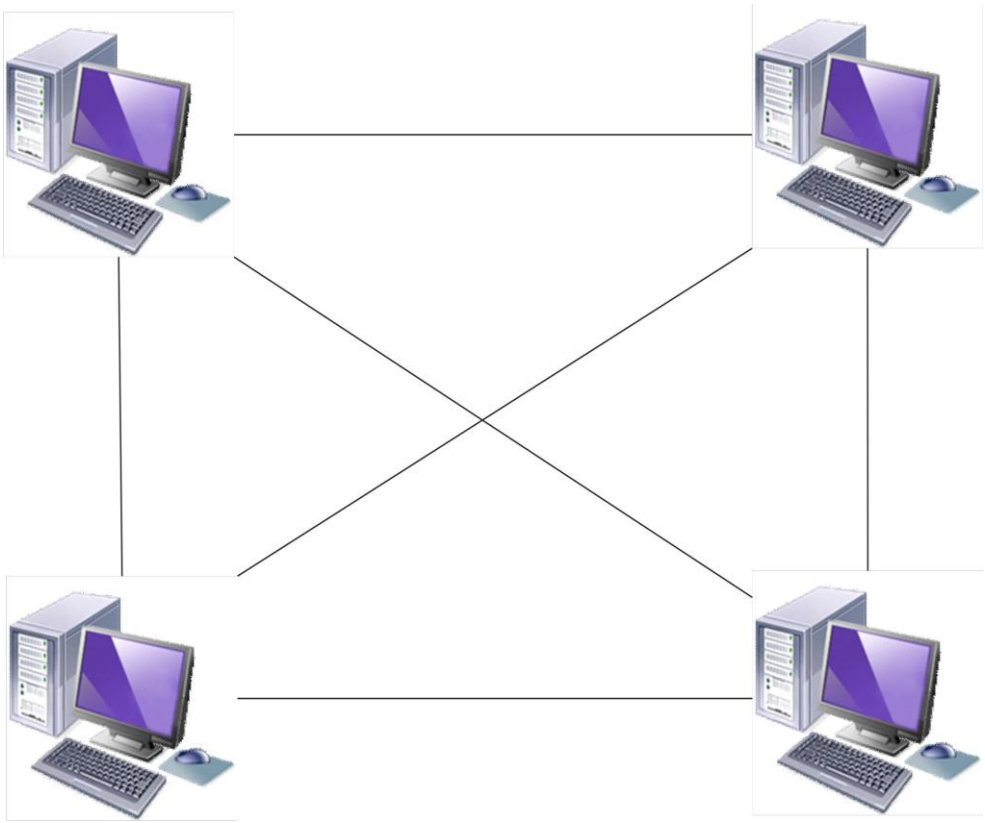

Figura 2.1 - Rede Wireless Não Estruturada (*Ad-Hoc)*

A definição de rede *Ad-hoc* conforme Microsoft(2008*) é:*

> "Uma rede *Ad-hoc* é uma conexão temporária entre computadores e dispositivos usados para uma finalidade específica, como compartilhamento de documentos durante uma reunião ou jogos de computador com vários jogadores. Você também pode compartilhar temporariamente uma conexão de Internet com outras pessoas da sua rede *Ad-hoc*, para que essas pessoas não precisem fazer suas próprias configurações de Internet. As redes *Ad-hoc* são somente sem fio, portanto, você deve ter um adaptador de rede sem fio instalado no computador para configurar ou ingressar em uma rede *Ad-hoc*."

Diferente do modelo não estruturado, as redes wireless estruturadas, tem o tráfego totalmente centralizado em um único ponto de acesso pré instalado, conforme a figura 2.2 – Rede Wireless Estruturada.

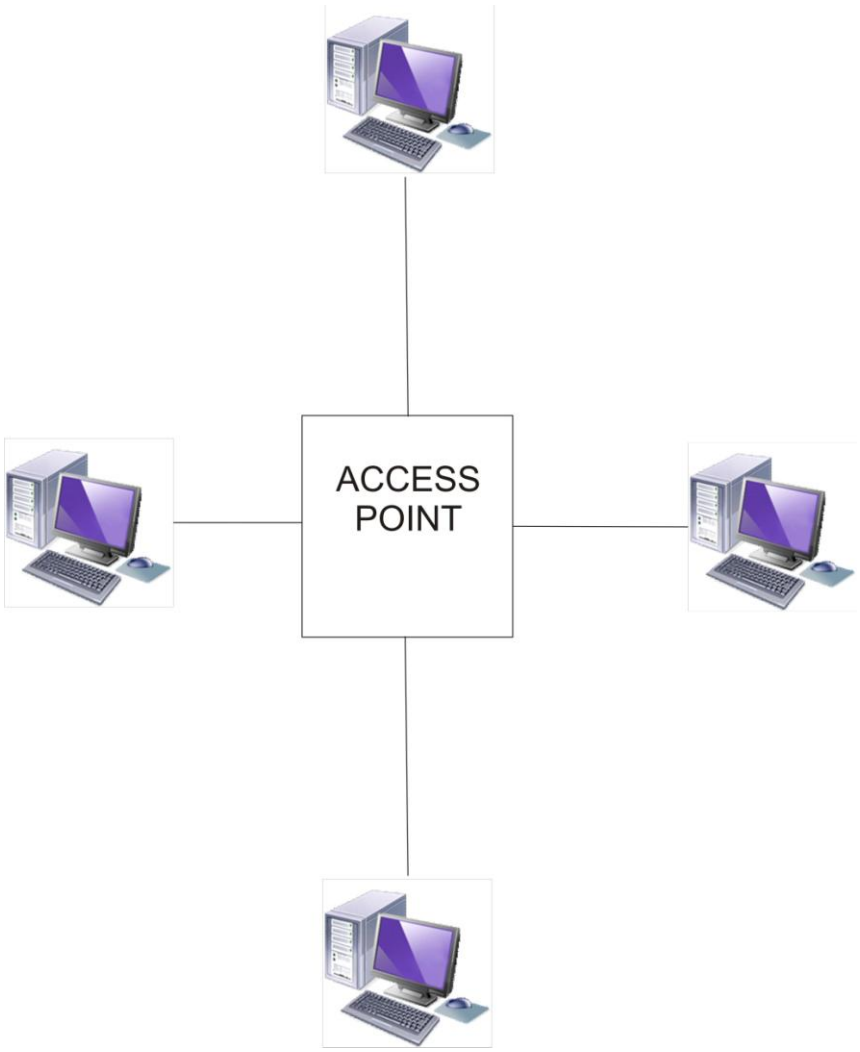

Figura 2.2 - Rede Wireless Estruturada

Comparando com redes baseadas em uma infra-estrutura, as redes *MANETS* apresentarem algumas vantagens. A tabela abaixo demonstra algumas destas delas.

Tabela 2.1 - Vantagens das redes MANET

VANTAGENS	DESCRIÇÃO
Instalação rápida	Redes *ad-hoc* podem ser estabelecidas dinamicamente em locais onde não haja previamente uma infra-estrutura instalada
Tolerância à falhas	A permanente adaptação e reconfiguração das rotas em redes *Ad-hoc* permitem que perdas de conectividade entre os nós possam ser facilmente resolvidas desde que uma nova rota possa ser estabelecida
Conectividade	Dois nós móveis podem se comunicar diretamente desde que cada nó esteja dentro da área de alcance do outro
Mobilidade	A mesma rede pode ser criada em locais diferentes, sem necessidade de mudança em suas configurações

FONTE: Andrade(2008)

Apesar de apresentar essas vantagens, como qualquer outra topologia, também apresenta limitações, como demonstradas na tabela 2.

Tabela 2.2 - Desvantagens das rede MANET

DESVANTAGENS	DESCRIÇÃO
Roteamento	A mobilidade dos nós e uma topologia de rede dinâmica contribuem diretamente para tornar a construção de algoritmos de roteamento um dos principais desafios em redes *ad-hoc*
Banda Passante	Com cabeamento convencional, a banda passante pode chegar a 1Gbps. Nos enlaces via redes wireless temos taxas de até 2Mbps tipicamente
Taxa de Erros	A taxa de erros associada a enlaces sem-fio é mais elevada quando comparada aos enlaces em redes estruturadas

FONTE: Andrade(2008)

2.1 História da Rede *MANET*

O conceito de uma rede *ad-hoc* data do início da década de 70, quando a *U.S DARPA (United States Defense Advanced Research Projects Agency)* iniciou o projeto *PRNET (Packet Radio Network)*, para explorar o uso de redes de pacote de rádio num ambiente tático para comunicação de dados.

Mais tarde, em 1983, a DARPA lançou o programa *SURAN (Survivable Adaptive Network)* para expandir a tecnologia desenvolvida no projeto PRNET para suportar grandes redes, e para desenvolver protocolos de rede adaptativos os quais pudessem adaptar-se às rápidas mudanças de condições em um ambiente tático.

O último da série dos programas iniciados pela DARPA para satisfazer os requisitos de defesa para sistemas de informações robustos e rapidamente expansíveis foi o *GloMo (Global Mobile Information Systems)*, que teve início em 1994. Enquanto as comunicações táticas militares permaneciam a principal aplicação das redes *MANETS*, havia um número

crescente de aplicações não militares, tais como conferência, busca e salvamento (WIKIPEDIA, 2008).

2.2 Áreas de aplicação das redes *MANET*

Tendo em vista essa facilidade para a criação de redes baseadas no modelo *MANET*, estas redes podem ser empregadas em praticamente qualquer área.

As redes de sensores constituem redes *MANET* basicamente utilizadas para mapeamento de ambientes, onde cada nó é responsável pelo mapeamento de uma determinada área. Depois de coletados, os dados são retransmitidos até uma unidade central de processamento onde são realizadas análises a fim de obter resultados mais precisos em busca da melhor solução para cada situação. Algumas aplicações onde este tipo de rede pode ser empregada estão, vigilância, monitoração de ambientes, análises geográficas entre outras.

Como rede pessoal, a concepção deste tipo de rede é simples. O seu principal objetivo é fazer com que diferentes dispositivos como notebooks, celulares, palmtops, e todos os demais que disponham de uma interface para a conexão possam comunicar-se, sem depender de um meio físico para a conexão entre eles.

Como rede de contingência, estas redes podem ser empregadas em áreas onde não há disponibilidade ou viabilidade de instalação de uma rede estruturada, afetada por falha humana, sabotagem ou mesmo vítima de desastres naturais que interrompem a conectividade das redes estruturadas, este tipo de rede pode ser implantada rapidamente. Desta maneira, restabelecendo a conectividade do local até que os reparos na rede principais sejam efetuados com sucesso.

2.3 Roteamento em redes *MANET*

As redes *Ad-hoc* são classificadas como redes de comunicação direta e redes de múltiplos saltos. Nas redes de comunicação direta, cada dispositivo é capaz de comunicar-se somente com dispositivos que estejam ao seu alcance. Em redes *Ad-hoc* de múltiplos saltos, dois dispositivos que são mutuamente inalcançáveis podem se comunicar se houver pelo menos uma cadeia de dispositivos que seja alcançável por ambos.

Em redes sem fio com infra-estrutura, a questão do alcance se resume no dispositivo dentro do raio de atuação do ponto de acesso. Já nas redes *ad-hoc*, os dispositivos podem se

comunicar diretamente desde que haja uma cadeia de comunicação que permita o encaminhamento da informação da origem até o destino (neste caso, atuam como roteadores). Assim, o alcance não fica limitado ao raio de ação de cada dispositivo individualmente, mas à soma dos raios de ação de todos os dispositivos. Por esse motivo, a localização momentânea de um dispositivo com relação aos demais influi diretamente no alcance total da rede.

Por exemplo, em uma rede *Ad-hoc*, uma rota entre dois computadores pode ser formada por vários *hops* (saltos), através de um ou mais dispositivos na rede. Na figura seguinte os círculos demonstram o alcance da comunicação das unidades móveis. Sendo assim, as mensagens de A para D, por exemplo, devem passar por B e C para chegar até D.

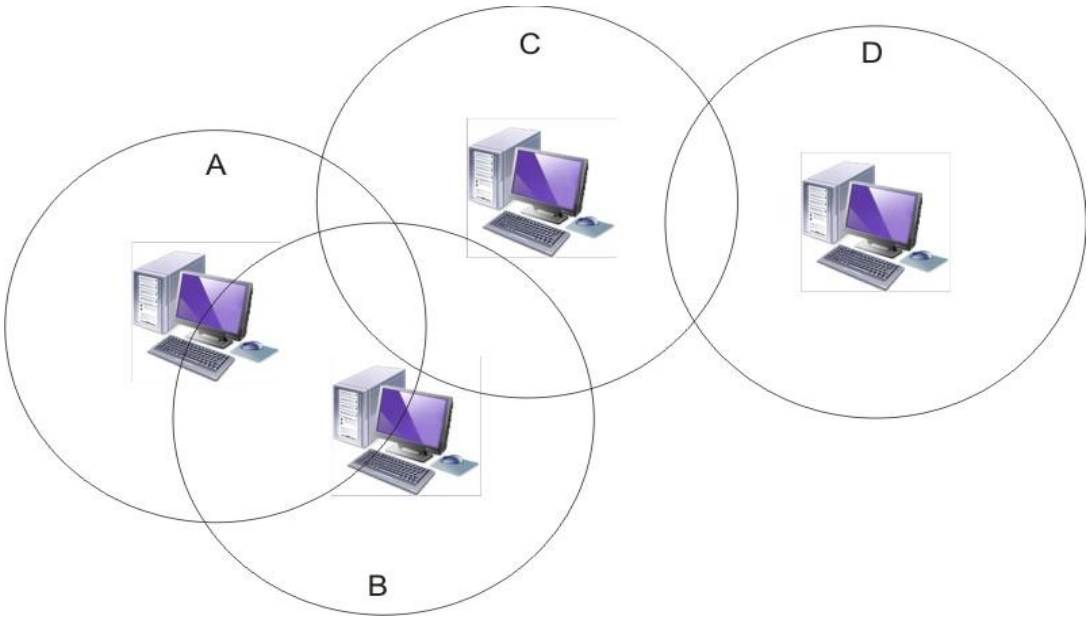

Figura 2.3 - Comunicação em rede Ad-hoc

Alguns dos protocolos mais comumente utilizados para o roteamento dos pacotes nestas redes são o DSR, o DSDV e o AODV.

O DSR é um protocolo específico para o roteamento de pacotes em rede MANET, nele cada nó da rede mantém um cachê com as rotas conhecidas para os demais pontos da rede. Cada pacote lançado na rede contém nele o endereço de toda a rota por onde irá viajar até chegar ao destino final e, caso o destino seja desconhecido, o nodo em questão inunda a rede com "*floods*" de requisição para a identificação das novas rotas na rede.

O DVDS também é um protocolo específico para o roteamento desta topologia de rede, porém ele é muito parecido com protocolos de roteamento de redes convencionais com fio, conforme (BRUEL, 2004). Nele as rotas são mantidas através de tabelas passadas entre os nós da rede periodicamente, criando assim a noção de um número em sequencia, utilizadas para controlar a atualidade das rotas.

O AODV combina as idéias do DSR e do AODV. Assim como o primeiro, as rotas entre dois nós são criadas apenas quando surge a necessidade de comunicação entre eles. E assim como o segundo, as rotas são mantidas em tabelas nos nós, e não enviadas em cada pacote, e é usado um número de seqüência para controle da atualidade das rotas.

Um pequeno comparativo entre os três protocolos pode ser encontrado na Tabela 2.3 – Protocolos de Roteamento MANET.

Tabela 2.3 - Comparativo de Protocolos de roteamento para redes *MANET*

Protocolo de Roteamento	Aquisição de Rota	Inundação para descobrimento da Rota	Atraso para descobrimento de Rota	Falhas em Rotas
DSR	Sob demanda. Adquiri novas rotas somente quando necessário	Sim. Usa o cachê para armazenar informações de rotas e reduzir o overhead	Sim	Um pacote de Route Error é propagado para a fonte apagando o caminho válido
DSDV	Pró-Ativo. Mantém tabela de todas as rotas possíveis	Não	Não	As rotas são atualizadas constantemente através de toda a rede
OADV	Sob demanda. Adquiri novas rotas somente quando necessário	Sim. Usa o cachê para armazenar informações de rotas e reduzir o overhead	Sim	Um pacote de Route Error é enviado em broadcast ou unicast para apagar o caminho inválido

2.4 Vulnerabilidades das redes *MANET*

Desde o início de sua utilização, as redes *MANET* levantam dúvidas de como aplicar técnicas de segurança, já que se tratando de uma rede *Wireless*, as técnicas utilizadas para redes fixas não são eficazes.

O principal problema para a aplicação destas técnicas, é que não há necessidade que o intruso tenha acesso físico a essa rede, tornando inútil o uso de *firewalls* ou dispositivos semelhantes.

Não havendo assim, uma "linha de defesa" para a rede, cada nodo constituinte deve possuir seu próprio mecanismo de defesa contra ataques diretos ou indiretos. Entretanto, mesmo que os nodos estejam protegidos, o meio por onde as informações trafegam continua livre.

Algumas técnicas que são utilizadas nessa topologia de rede são a criptografia e a certificação digital, porém estas técnicas ajudam somente a reduzir as ameaças na rede, e não eliminá-las.

Segundo Diffie e Helman(1976), quando relacionado com segurança de redes, pode-se dizer que os ataques são classificados de duas maneiras:

- **Ataques Ativos:** são ataques que modificam o fluxo da informação, alterando ou impedindo o fluxo de dados na rede.

- **Ataques Passivos:** são ataques que não alteram o fluxo da informação. Basicamente usados para interceptação de pacotes, sem impedir que o destinatário verdadeiro receba a informação.

Dependendo das ações tomadas pelo intruso, é possível utilizar várias subcategorias para classificar seu ataque a rede de dados. Entre elas, pode-se citar, interceptação, análise de tráfego, personificação, modificação, inserção, retransmissão e negação de serviço.

Considerando as diferentes áreas de utilização das redes *Ad-hoc* e, analisando a sua arquitetura, pode-se dizer que estas redes foram desenvolvidas buscando alcançar uma maneira rápida para que dispositivos ligados a ela compartilhem informações sem a necessidade de se conectarem a uma estrutura pré-construída para esta finalidade. Criando

essa facilidade de acesso, muitas brechas de segurança tornaram-se facilmente exploráveis por usuários mal-intencionados (intrusos).

Sendo assim, existem dois níveis distintos de ataques potenciais a este tipo de rede, são eles: ataques aos mecanismos básicos e os ataques aos mecanismos de segurança.

Entre as principais vulnerabilidades das redes Ad-hoc, pode ser citado o meio pela qual ela opera. Ataques passivos de usuários mal-intencionados (intrusos) são relativamente comuns. Estes intrusos podem facilmente interceptar e decodificar pacotes que são transmitidos entre os nodos de uma rede sem que os usuários autorizados percebam a presença do invasor, caracterizando assim, um ataque de interceptação ou Análise de tráfego.

Outra dificuldade encontrada nesta arquitetura de rede é o mecanismo de transmissão de pacotes (roteamento), já que os nodos da rede devem manter um sincronismo para evitar a colisão de pacotes. Os nodos da rede devem manter um sincronismo para que possam se necessário, receber e retransmitir determinado pacote a um nodo não alcançável pelo nodo que enviou o pacote.

Sendo assim, um intruso que ganhe controle de um dos nodos da rede pode paralisar todo seu funcionamento, inundando o canal de transmissão com pacotes e assumindo o controle total do mesmo. Isso impediria que outros nodos distribuíssem dados através da rede, tornando-a assim, totalmente inoperante. Esse tipo de ataque é conhecido como negação de serviço, já que nenhum outro nodo da rede consegue enviar dados para os demais.

Segundo Neto (2004), ataques nos mecanismos de segurança podem ser resumidos nos seguintes:

- Comprometimento de alguma chave de criptografia;
- Substituição por um intruso da chave pública das partes envolvidas;
- Controle por um intruso de uma autoridade certificadora da rede.

Sabendo então que o meio de transmissão provavelmente é o “elo” mais fraco nas redes *MANETS*, os principais ataques a essas redes serão contra ele, porém um único nodo que tenha sua segurança comprometida pode também abrir as portas para um intruso. Portanto, entre as principais ameaças de rede estão:

- ***DOS (Denial of Service):*** são ataques de recusa de serviços, ou seja, o objetivo desses ataques é basicamente interromper ou negar completamente um serviço. Existem diversos tipos de DOS, como consumo de largura de banda, inanição

de recursos, falha de programação e ataques de roteamento. (MCCLURE, 2003);

- ***DDOS (Distributed Denial of Service):*** são ataques DOS distribuídos. O primeiro registro desses ataques foi em fevereiro de 2000, quando os sites Yahoo, eBay, CNN.com e outros saíram do ar. (MCCLURE, 2003);

- ***IP Spoofing:*** essa técnica consiste na falsificação do IP para dificultar a detecção de um atacante ou possibilitar um ataque caso haja algum bloqueio de IP. (SANTOS, 2005);

- ***Sniffers:*** possibilita a análise do tráfego de uma rede e o roubo de informações dentro da mesma. Ele possibilita a captura de pacotes e a verificação do conteúdo transportado. (MELO, 2004);

- ***Port Scanners:*** permitem aos administradores de sistemas ou atacantes obter informações sobre uma determinada rede, tais como, quantos hosts estão ativos e que serviços estão sendo oferecidos, através da análise da portas de serviços TCP e UDP. (CARVALHO, 2006);

- ***Backdoors:*** são as portas dos fundos. É uma técnica que consiste em garantir uma forma de acesso a um determinado sistema. O atacante esconde no sistema um backdoor para depois poder acessar o mesmo sem grandes problemas. (MELO, 2004);

- **Engenharia Social:** essa técnica consiste em enganar um usuário ou administrador para conseguir informações como senhas, dados sobre sistemas, procedimentos e outros;

- **Vírus:** são programas ou fragmentos de códigos que se reproduzem localmente e geralmente possuem uma função específica. Os vírus de computador são as ameaças mais conhecidas por usuários atualmente. (RUSSELL, 2002);

- ***Worm:*** são muito parecidos com um vírus, porém não se reproduzem localmente, ao invés disso se propagam entre sistemas. Além disso, eles têm a capacidade de violar sistemas através da vulnerabilidade de softwares. (RUSSELL, 2002);

- ***Cavalo de Tróia:*** são códigos maliciosos disfarçados como programas. Uma característica deles é que o usuário precisa executá-los. Eles podem criar um backdoor, apagar arquivos, parar serviços e se enviar para outras máquinas. (RUSSELL, 2002).

2.5 Mecanismos de Segurança

Tendo em vista o crescente nível de sofisticação das ferramentas de ataques, cada vez mais se busca mecanismos para impedir que eles sejam bem sucedidos. Isso, entretanto, mostra-se cada vez mais complexo, pois com o passar do tempo e a criação de novas ferramentas de ataque, pessoas com um baixo nível de conhecimento agregaram-se a lista de possíveis invasores, os quais no passado estavam limitados a uma pequena gama de pessoas que detinham um alto conhecimento.

Como citado no capítulo anterior, para a proteção do meio de transmissão, foram criados algoritmos de criptografia conforme (MENEZES, 1997), e entre os mais utilizados podemos citar o WEP, o WPA e o WPA2.

2.5.1 Criptografia

Criptografia é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário, o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Nos dias atuais, onde grande parte dos dados é digital, sendo representado por bits, o processo de encriptação é basicamente feito por algoritmos que fazem o embaralhamento dos bits desses dados a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido.

2.5.2 Chaves Simétricas

É o tipo de chave mais simples e a mesma chave é utilizada tanto pelo emissor quanto por quem recebe a informação. Ou seja, a mesma chave é utilizada para codificação e para a decodificação dos dados.

Vários algoritmos de criptografia foram desenvolvidos a partir de chaves simétricas. Dentre os mais comuns estão o DES, o IDEA e o RC.

DES (Data Encryption Standard), criado pela IBM em 1977, usa chaves de 56 bits, permitindo até 72 quatrilhões de combinações. Apesar disso, foi ‘quebrado’ ou desvendado utilizando-se as chamadas técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet.(PC WORLD,2007)

IDEA (International Data Encryption Algorithm), criado em 1991 por James Massey e Xuejia Lai é um algoritmo que usa chaves de 128 bits e tem estrutura semelhante ao DES. (PC WORLD,2007)

RC (Ron's Code ou Rivest Cipher), criado por Ron Rivest na empresa *RSA Data Security* é muito utilizado em e-mails e usa chaves de 8 a 1024 bits. Há várias versões: RC2, RC4, RC5 e RC6. Cada uma delas difere da outra por trabalhar com chaves de maior complexidade. (PC WORLD,2007)

O uso de chaves simétricas tem desvantagens, e não é indicado para casos que envolvem informações muito valiosas.

2.5.3 Chaves Assimétricas

Conhecida por "chave pública", a chave assimétrica trabalha com duas chaves: uma privada e outra pública.

Alguns algoritmos que usam chaves assimétricas são o RSA (Rivest, Shamir and Adleman), criado em 1977 nos laboratórios do Massachusetts *Institute of Technology (MIT)*, é um dos algoritmos de chave assimétrica mais usados (PC WORLD,2007). Nele, números primos são utilizados da seguinte forma: dois números primos são multiplicados para se obter um terceiro valor. A chave privada são os números multiplicados e a chave pública é o valor obtido.

Outro algoritmo é o ElGamal criado por Taher ElGamal, esse algoritmo usa um problema matemático conhecido por "logaritmo discreto" para se tornar seguro. É freqüente em assinaturas digitais. (PC WORLD,2007)

2.5.4 WEP (Wired Equivalent Privacy)

Foi o primeiro protocolo de segurança adotado. Ele conferia no nível do enlace certa segurança para as redes sem fio. Este protocolo, muito usado ainda hoje, utiliza o algoritmo RC4 para criptografar os pacotes que serão trocados numa rede sem fios a fim de tentar garantir confidencialidade aos dados de cada usuário. Além disso, utiliza-se também a CRC-32 que é uma função que detecta erros ao fazer o "checksum" de uma mensagem enviada. Ela gera um ICV (Integrity Check Value) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho.

No entanto, após vários estudos e testes realizados com este protocolo, encontraram-se algumas vulnerabilidades e falhas que fizeram com que o WEP perdesse quase toda a sua credibilidade.

No WEP, os dois parâmetros que servem de entrada para o algoritmo RC4 são a chave secreta (k) de 40 bits ou 104 bits, além um vetor de inicialização (v) de 24 bits. A partir desses dois parâmetros, o algoritmo gera uma seqüência criptografada RC4 (k, v).

Porém, como no WEP a chave secreta é a mesma utilizada por todos os usuários de uma mesma rede, devemos ter um vetor de inicialização diferente para cada pacote a fim de evitar a repetição de uma mesma seqüência RC4. Essa repetição de seqüência é extremamente indesejável, pois dá margem a ataques bem sucedidos e conseqüente descoberta de pacotes por eventuais intrusos.

Além disso, há também uma forte recomendação para que seja feita a troca das chaves secretas periodicamente, aumentando-se, com isso, a segurança da rede. Essa troca, contudo, quando feita, é realizada manualmente, de maneira pouco prática e por vezes inviável, quando se trata de redes com um número muito alto de usuários.

E ainda uma falha do WEP constatada e provada através de ataques bem sucedidos é a natureza de sua função de detecção de erros. A CRC-32 é uma função linear e que não possui chave. Essas duas características tornam o protocolo suscetível a dois tipos de ataques prejudiciais e indesejáveis. É possível fazer uma modificação de mensagens que eventualmente tenham sido capturadas no meio do caminho sem que isso seja descoberto pelo receptor final, além disso, pelo fato da função não possuir uma chave, é também possível descobrir uma seqüência secreta RC4 e de posse desta ser autenticado na rede e introduzir mensagens clandestinas nesta.

Conforme citado em (RUFINO, 2005):

> "Existem problemas administrativos e técnicos em relação ao protocolo WEP. Em relação ao padrão original, os principais relacionam-se ao fato de usar uma chave única e estática, que deve ser compartilhada entre todos os dispositivos participantes de uma determinada rede. Portanto, caso seja necessária a troca da chave, o processo pode ser trabalhoso e, em alguns casos, inviável. Outro problema vincula-se ao fato de que, na época em que o padrão foi definido (1997), havia restrição dos Estados Unidos referentes à exportação de criptografia com chaves maiores que 40 bits. E, finalmente, foram revelados outros problemas técnicos, que permitem ataques ao próprio algoritmo."

2.5.5 WAP (Wi-Fi Protected Acess)

O sucessor do WEP, o ***WPA (Wi-Fi Protected Access)***, também chamado de WEP2, surgiu de um esforço conjunto de membros da *Wi-Fi Alliance* e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

Com a substituição do WEP pelo WPA, temos como vantagem melhorias a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função de detecção de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação se utiliza do 802.11x e do *EAP(Extensible Authentication Protocol)*, que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

O WPA, que deverá substituir o atual *WEP (Wired Equivalent Privacy)*, conta com tecnologia aprimorada de criptografia e de autenticação de usuário. Cada usuário tem uma senha exclusiva, que deve ser digitada no momento da ativação do WPA. No decorrer da sessão, a chave de criptografia será trocada periodicamente e de forma automática. Assim, torna-se infinitamente mais difícil que um usuário não-autorizado consiga se conectar à WLAN. Porém, conforme citado em (RUFINO, 2006)

> "A despeito do WPA ter características de segurança superiores ao WEP, ainda assim ele apresenta algumas vulnerabilidades já reportadas e que devem ser conhecidas para que seu impacto possa ser minimizado."

A chave de criptografia dinâmica é uma das principais diferenças do WPA em relação ao WEP, que utiliza a mesma chave repetidamente. Esta característica do WPA também é conveniente, porque não exige que se alterem manualmente as chaves de criptografia, ao contrário do WEP.

2.5.3 WPA2 (IEEE 802.11i)

Homologado em junho de 2004, foi desenvolvido com o objetivo de prover mais segurança na comunicação, visto que o protocolo de segurança então utilizado (WEP) apresentava diversas vulnerabilidades. O novo método de criptografia utilizado exige um maior poder computacional do NIC (Network Interface Card) durante o processo de codificação/decodificação, impossibilitando assim, apenas uma atualização de firmware. Parte dos mecanismos apresentados no WPA também é utilizada no WPA2, já que o WPA é baseado em um rascunho do WPA2. Os principais avanços do WPA2 em relação ao WPA são, basicamente, novos algoritmos de criptografia e de integridade.

O WPA2 é tido até o momento como uma solução definitiva de para a segurança, não somente das redes *MANET*, mas de todas as redes sem fio. Porém, essa hegemonia pode ser abalada a partir do momento em que vulnerabilidades em sua segurança sejam descobertas.

3 MÉTRICAS DE SEGURANÇA E FERRAMENTAS DE TESTE

Como já apresentado anteriormente, o principal problema para a utilização das redes *MANET* é a fragilidade em sua segurança. Para avaliar se a utilização desta topologia é viável, uma avaliação da fragilidade das criptografias disponíveis torna-se necessária.

3.1 Proposta

A proposta para essa verificação será a de compor uma rede *MANET,* criptografada com diferentes algoritmos como o WEP, o WPA e o WPA2, e assim efetuar um ataque buscando descobrir a chave da criptografia que está sendo empregada.

3.2 Pontos de Avaliação

A questão de como avaliar a segurança de determinada rede é um questão que tem levantado muitos debates tanto no meio acadêmico, como no meio empresarial, não sendo um atributo quantificável como o desempenho, que pode ser medido, por exemplo, através da taxa de transmissão de *bits* por segundo, se torna difícil atribuir métricas de avaliação para essa questão conforme (Ângelo, 2006).

Por esse motivo, a especificação do que se está medindo deve ser feita cuidadosamente para que contemplem apenas os dados necessários e relevantes para a questão a ser medida.

No presente projeto, buscamos avaliar questões de segurança referentes à eficácia dos métodos de criptografia suportados nas redes *Ad-Hoc*, analisando a princípio três questões básicas, que são:

- Averiguar se é possível acessar indevidamente a rede através da descoberta de sua chave.

- Verificar se a velocidade da rede sofre alguma alteração com o emprego de cada criptografia.
- Tempo necessário para acessarmos indevidamente a rede, através da quebra de seu mecanismo de criptografia.

Dados como estes, permitirão uma análise de qual dos mecanismos utilizados é mais seguro e, conseqüentemente, mais recomendado para ser aplicado a uma rede *Ad-Hoc*, seja ela pessoal ou comercial.

3.3 Método de Aplicação

Os testes serão realizados em três ciclos, compostos de uma seqüência de dez tentativas de invasão para cada uma das criptografias selecionadas.

Após cada ciclo, será elaborada uma estatística sobre os dados colhidos em cada bateria, demonstrando onde, ao final dos ciclos de testes, serão comparados.

3.4 Ferramentas de Teste

Buscando alcançar uma melhor confiabilidade na segurança das redes *wireless* como um todo, uma avaliação de suas fragilidades é necessária, tendo em vista que estas redes são comprovadamente mais suscetíveis a quebras de segurança do que redes que necessitam acesso físico para esse mesmo fim.

Sendo assim, algumas ferramentas desenvolvidas para testar a segurança das redes *wireless* serão empregadas com o intuito de verificar se as criptografias a serem submetidas aos testes suportarão os ataques e manterão a rede livre de intrusos.

As ferramentas escolhidas estão listadas a seguir, juntamente com alguns dados relevantes sobre as mesmas.

3.5 Wellenreiter

O Wellenreiter é uma excelente ferramenta, com interface gráfica, para localizar e monitorar redes wireless. Através do Wellenreiter é possível identificar diversas informações da rede wireless que está sendo monitorada, tais como: Canal de comunicação, o ESSID,

MAC Address, se a rede utiliza ou não algum recurso de criptografia, o fabricante do Access Point, entre outras informações.

A ferramenta também registra todo o tráfego da rede wireless. Sendo assim, você poderá utilizar o Ethereal para abrir o arquivo que foi registrado todo o tráfego, para uma análise mais detalhada das informações. (under-linux, 2008)

3.6 Ethereal

Ethereal é um programa usado por administradores de redes e usuários avançados que desejam monitorar o tráfego de uma rede, analisando e dissecando os pacotes de dados. (Tudo Pcs, 2007)

O Ethereal é um software gratuito e possui versões para Windows, Linux e Unix.

3.6.1 WireShark

Sucessor do Ethereal, o Wireshark é um programa que verifica os pacotes transmitidos pelo dispositivo de comunicação (placa de rede, placa de fax modem, etc.) do computador. O objetivo deste tipo de software, também conhecido como *sniffer*, é detectar problemas de rede, conexões suspeitas, auxiliar no desenvolvimento de aplicativos e qualquer outra atividade relacionada à rede.

O programa analisa o tráfego de pacotes recebidos e organiza-os por protocolo. Todo o tráfego de entrada e saída é analisado e mostrado em uma lista de fácil navegação. Este programa é recomendado para profissionais de informática, especificamente administradores de redes, e para fins educativos. (Ghdpress)

3.7 Kismet

O Kismet é uma ferramenta poderosa, que pode ser usado tanto para checar a segurança de sua própria rede wireless, quanto para checar a presença de outras redes próximas e assim descobrir os canais que estão mais congestionados.

A principal característica do Kismet é que ele é uma ferramenta passiva. Ao ser ativado, ele coloca a placa wireless em modo de monitoramento e passa a escutar todos os

sinais que cheguem até a antena. Mesmo pontos de acesso configurados para não divulgar o ESSID ou com a encriptação ativa são detectados.

Como ele não transmite pacotes, apenas escuta as transmissões, todo o processo é feito sem prejudicar as redes vizinhas e de forma praticamente indetectável. A principal limitação é que, enquanto está em modo de monitoramento, a placa não pode ser usada para outros fins. Para conectar-se a uma rede, você precisa primeiro parar a varredura.

Esta questão da detecção dos pontos de acesso com o ESSID desativado é interessante. Não é possível detectá-los diretamente, pois eles não respondem a pacotes de broadcast, mas o Kismet é capaz de detectá-los quando um cliente qualquer se associa a eles, pois o ESSID da rede é transmitido de forma não encriptada durante o processo de associação do cliente.

A partir daí, o Kismet passa a capturar todos os pacotes transmitidos. Caso a rede esteja encriptada, é possível descobrir a chave de encriptação usando o aircrack (que veremos a seguir), permitindo tanto escutar as conexões, quanto ingressar na rede. (Ghdpress, 2008)

Como o Kismet é uma das ferramentas mais usadas pelos crackers, é sempre interessante usá-lo para verificar a segurança da sua própria rede.

Sendo então um programa apenas de monitoramento, o Kismet torna-se ineficaz no para o tipo de simulação que será implementa neste projeto, porém, ainda assim, uma ferramenta interessante.

3.8 Aircrack

Aircrack-ng é um programa para quebra de chaves WEP e WPA/WPA2-PSK do IEEE 802.11. *Aircrack-ng* pode recuperar a chave WEP, uma vez que um número suficiente de pacotes criptografados seja capturado com o *airodump-ng*. Esta parte do pacote *Aircrack-ng* determina a chave WEP usando dois métodos fundamentais. O primeiro método é via abordagem PTW (Pyshkin, Tews, Weinmann). A principal vantagem da abordagem PTW é que pouquíssimos pacotes de dados são necessários para quebrar a chave WEP.

O segundo método é o método FMS/KoreK. O método FMS/KoreK incorpora vários ataques estatísticos para descobrir a chave WEP e usa estes ataques em combinação com força-bruta.

Adicionalmente, o programa oferece um método de dicionário para determinar a chave WEP. Para quebrar chaves pré-compartilhadas WPA/WPA2, somente o método de dicionário é utilizado.

3.8.1 Como funciona?

O primeiro método é o método PTW (Pyshkin, Tews, Weinmann). Em 2005, Andreas Klein apresentou outra análise da cifra de fluxo RC4. Klein mostrou que há mais relações entre o fluxo de chave RC4 e a chave do que nas relações encontradas por Fluhrer, Mantin, e Shamir, e essas podem ser utilizadas em conjunto para quebrar o WEP. O método PTW faz extensão do ataque do Klein e aperfeiçoa-o para uso contra o WEP. Ele basicamente usa técnicas FMS melhoradas, descritas na seção seguinte. Uma restrição importante em particular é que somente funciona com pacotes ARP Request/Reply e não pode ser empregado contra outro tráfego.

O segundo método é o método FMS/Korek, o qual incorpora múltiplas técnicas. Neste método, múltiplas técnicas são combinadas para quebrar a chave WEP:

- Ataques FMS (Fluhrer, Mantin, Shamir) - técnicas estatísticas
- Ataques Korek - técnicas estatísticas
- Força-Bruta

Quando no uso de técnicas estatísticas para quebrar a chave WEP, cada byte da chave em essencial é manipulado individualmente. Usando técnicas estatísticas, a possibilidade de certo byte na chave ser adivinhado corretamente sobe até 15% quando o Vetor de Inicialização (IV) correto é capturado para um byte de chave particular. Essencialmente, certos IVs “vazam” a chave WEP secreta para bytes de chaves específicos. Esta é a base fundamental das técnicas de estatística.

Por meio do uso de uma série de testes estatísticos chamados de ataques FMS e Korek, votos são acumulados para chaves prováveis para cada byte da chave WEP secreta. Ataques diferentes têm um número diferente de votos associados a eles, já que a probabilidade de cada ataque render a resposta certa varia matematicamente. Quanto mais votos um valor de chave em potencial particular acumular, mais provável será de estar correto. Para cada byte de chave, a tela mostra a provável chave secreta e o número de votos que acumulou até o

momento. A chave secreta com o maior número de votos tem maior probabilidade de estar correta, mas não é garantido. *Aircrack-ng* testará em seqüência a chave para confirmá-la.

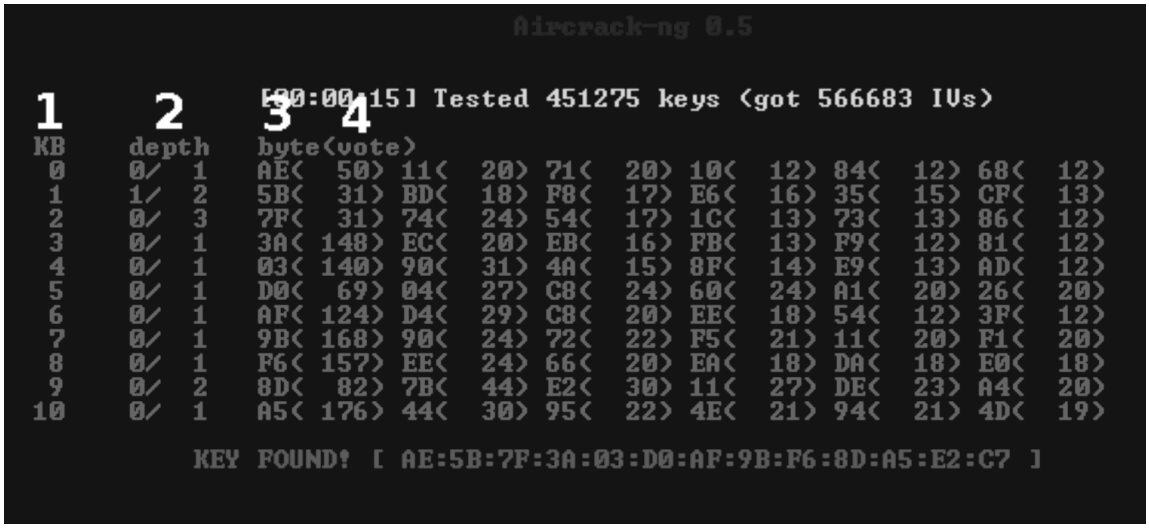

Figura 3.1 - Exemplo do *Aircrack-NG*

No exemplo anterior, pode-se ver que no byte de chave 0(zero), o byte 0xAE coletou alguns votos, 50 nesse caso. Então, matematicamente, é mais provável que a chave comece com AE do que com 11 (que é o segundo na mesma linha), já que a segunda opção recebeu menos da metade da probabilidade. Isso explica por que quanto mais dados são disponíveis, maiores chances o *Aircrack-ng* tem de determinar a chave WEP secreta.

Entretanto, a abordagem estatística pára neste ponto, depois disso, deve-se usar força-bruta para terminar o trabalho. *Aircrack-ng* usa força-bruta nas chaves mais prováveis para, na verdade, determinar a chave WEP secreta.

Ao utilizar o *Aircrack-ng* com um fator de correção 2, ele usará os votos do byte mais provável, e verificar todas as outras possibilidades que são, pelo menos, metade da possibilidade desse byte em uma base de força-bruta. Quanto maior for o fator de correção, mais possibilidades o *Aircrack-ng* tentará numa base de força-bruta. Porém quanto maior for o fator de correção, maior será o número de chaves a serem testadas e, conseqüentemente, o tempo necessário também aumentará. Portanto, com mais dados disponíveis, a necessidade de força-bruta, que requer muito tempo para o processamento, pode ser minimizada.

Para quebrar chaves WEP, um método de dicionário é incluído também. Para WEP, é possível utilizar ou o método estatístico descrito anteriormente ou o método de dicionário,

porém não os dois ao mesmo tempo. Com o método de dicionário, primeiro cria-se um arquivo com chaves ASCII ou chaves hexadecimais. Um único arquivo só pode conter um tipo, e não uma mistura dos dois. Ele é então utilizado como entrada no *Aircrack-ng* e o programa testa cada chave para determinar se está correta ou não.

As técnicas e abordagens acima não funcionam para chaves pré-compartilhadas WPA/WPA2. A única maneira de quebrar essas chaves pré-compatilhadas é por meio de um ataque de dicionário. Essa capacidade está incluída também no *Aircrack-ng*.

Com chaves pré-compartilhadas, os nodos estabelecem material de chaveamento para ser usado no início de suas comunicações. Essa conexão cria uma conexão conhecida como *four-way handshake*, entre os nodos. O *Airodump-ng* pode capturar esse *four-way handshake*, utilizando uma *lista de palavras* (*wordlist*) providenciada, o *Aircrack-ng* duplica o *four-way handshake* para determinar se uma entrada em particular da lista de palavras iguala-se aos resultados do *four-way handshake*. Se igualarem, então a chave pré-compartilhada foi identificada com êxito.

Este processo é computacionalmente complexo, e na prática, chaves muito longas são improváveis de serem descobertas. Outro fator que poderá facilitar a descoberta da chave é uma lista de palavras de boa qualidade. (crackwireless, 2004)

3.8.2 Uso do *Aircrack*

Podem-se especificar múltiplos arquivos de entrada (em formato .cap ou .ivs). Pode-se também executar ambos *airodump-ng* e *Aircrack-ng* ao mesmo tempo, o *Aircrack-ng* fará atualização automática quando novos IVs estiverem disponíveis.

Segue um sumário de todas as opções disponíveis no *Aircrack-ng*:

Tabela 3.1- Parâmetros do *Aircrack-ng*

Opção	Parâmetro	Descrição
-a	Modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-e	Essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-b	Bssid	Selecione a rede alvo baseada no endereço MAC do Access Point.
-p	número de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	Nenhum	Habilita modo quieto (não mostrar status até que a chave seja

		encontrada, ou não).
-c	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres alfa-numérico somente (0×20 - 0x7F).
-t	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-h	Nenhum	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0×30-0×39). Essas chaves são usadas por padrão na maioria dos Fritz!Boxes.
-d	Início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-m	endereço MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique **-m ff:ff:ff:ff:ff:ff** para usar cada um e todos IVs, independente da rede.
-n	número de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-i	Índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.
-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, … -k 17 para desabilitar cada ataque seletivamente.
-x/-x0	Nenhum	[Quebra WEP] Desabilita força-bruta dos últimos bytes de chave.
-x1	Nenhum	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	Nenhum	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	Nenhum	[Quebra WEP] Desabilita multi-processamento da força-bruta (somente SMP).
-y	Nenhum	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	Palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou ”-” sem as aspas para padronizar em (stdin).
-z	Nenhum	Invoca o método PTW de quebrar chaves WEP.

FONTE: Crackwireless(2008)

4 EXPERIMENTO

Visando alcançar uma maior transparência sobre o quão segura e efetiva é a criptografia empregada nas redes *AD-HOC* será realizado um experimento testando a qualidade da segurança oferecida por elas.

Para isso será realizada uma bateria de testes buscando explorar as vulnerabilidades destas criptografias e verificar o quão difícil seria para um usuário não autorizado acessar os dados que trafegam por uma rede deste tipo.

4.1 Descrição do Experimento

Para a realização do experimento será utilizado a ferramenta *Aircrack-ng* devido a ser a única das ferramentas citada a trabalhar tanto com a criptografia WEP, quanto às criptografias WPA/WPA2.

A utilização do *Aircrack-ng* será feita através de uma bateria de testes onde uma rede previamente estruturada utilizando a rede *AD-HOC* em conjunto com as criptografias acima citadas será atacada por um terceiro elemento que busca acessar os dados que trafegam por ela sem autorização.

Essa bateria de testes será repetida por no mínimo três vezes com cada criptografia afim de que os resultados obtidos tornem-se mais verossímeis, evitando assim conclusões incorretas sobre a segurança a ser testada.

4.2 Ambiente de Testes

A realização deste experimento será realizada utilizando uma rede de dois computadores que trafegam informações utilizando as criptografias acima citadas, além de um terceiro equipamento utilizado para efetuar os ataques contra essa rede, conforme demonstrado na imagem a seguir.

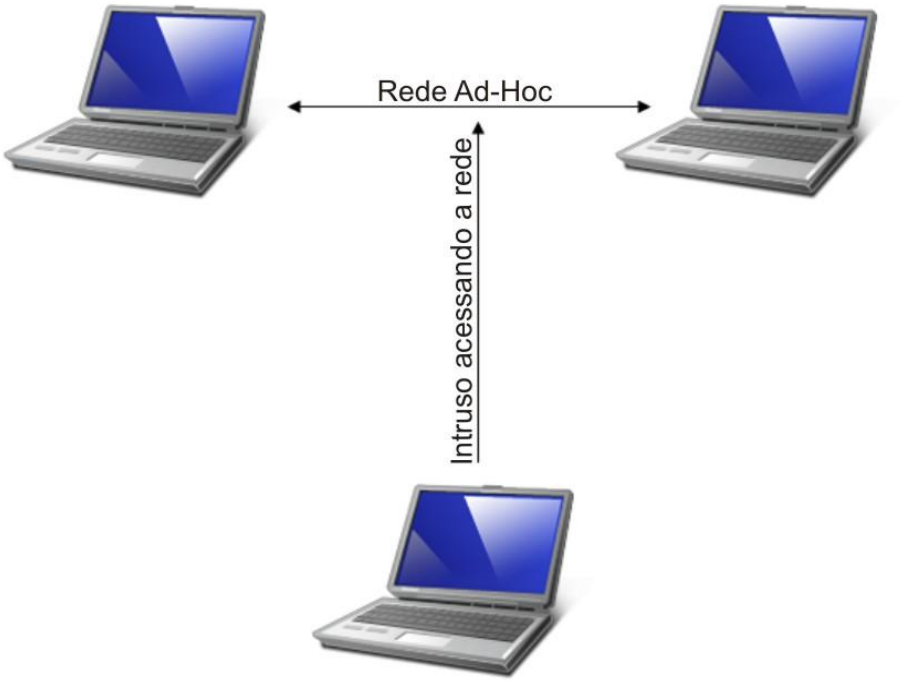

Figura 4.1 - Ambiente de Testes

Para os equipamentos da rede serão utilizados equipamentos com as seguintes configurações:

Tabela 4.1 - Equipamento 1

FABRICANTE	Não Disponível
MODELO	Não Disponível
PROCESSADOR	AMD ATHLON64 X2 4200+
MEMÓRIA	2GB CORSAIR 667mhz
PLACA WIRELESS	Realtek rtl8187
SISTEMA OPERACIONAL	Windows Vista

Tabela 4.2 - Equipamento 2

FABRICANTE	COMPAC
MODELO	PRESÁRIO 3000
PROCESSADOR	AMD Turion64 X2 1.6Ghz
MEMÓRIA	1Gb
PLACA WIRELESS	Realtek rtl8187
SISTEMA OPERACIONAL	Windows XP Home – SP3

Depois de formada a rede, um terceiro equipamento efetuará os ataques a esta rede buscando acessar indevidamente as informações que trafegam por ela. Para este equipamento será utilizada a seguinte configuração:

Tabela 4.3 - Equipamento 3

FABRICANTE	HP DV 2000
MODELO	DV 2000
PROCESSADOR	AMD Turion64 X2 1.6Ghz
MEMÓRIA	1Gb
PLACA WIRELESS	Realtek rtl8187
SISTEMA OPERACIONAL	Linux ArchLinux

4.3 Detalhes do Experimento

O experimento será realizado através de uma bateria de testes como já descrito anteriormente, onde serão capturadas diferentes quantidades de pacotes na rede e através da análise destes, buscar-se-á a chave da criptografia que está sendo usada pela rede no determinado momento.

Através da análise da quantidade de pacotes necessários para que uma determinada chave criptográfica seja encontrada, será possível analisar qual a criptografia oferecerá melhor segurança para os usuários destas redes.

A tabela a seguir representa um exemplo de como os dados serão colhidos durante a execução do experimento.

Tabela 4.4 - Tabela de Testes

Tipo de	Quantidade de Pacotes	Chave	Tempo

Criptografia	Capturados (em milhares)	Encontrada?	Necessário para encontrar a chave
WEP	5		
WEP	10		
WEP	15		
WEP	20		
WEP	25		
WPA	5		
WPA	10		
WPA	15		
WPA	20		
WPA	25		
WPA2	5		
WPA2	10		
WPA2	15		
WPA2	20		
WPA2	25		

O experimento será dividido em diferentes etapas. Na primeira etapa será utilizada a criptografia WEP e serão capturadas amostras para análise do *Aircrack-ng* onde cada uma será composta, conseqüentemente, de cinco, dez, quinze, vinte e vinte cinco mil pacotes sucessivamente, até o momento em que a chave seja descoberta.

Cada uma destas amostras será analisada pelo *Aircrack-ng*, buscando assim a chave da criptografia que está sendo utilizada. Também será avaliado o tempo para fazer a análise destes pacotes, bem como, se a chave foi descoberta ou não.

Esta análise com diferentes quantidades de pacotes provavelmente fornecerá dados mais claros de qual a criptografia mais confiável para ser utilizada, já que teoricamente, uma criptografia que necessite a análise de uma quantidade maior de pacotes tende a ser mais segura do que uma que requeira poucas amostras para que sua chave seja descoberta, visto que a proposta da rede *MANET* é trabalhar como uma rede de curta duração.

Depois de realizados os testes com a criptografia *WEP* acima citados, os mesmos serão realizados novamente com as criptografias *WPA* e *WPA2*.

Ao final dos experimentos espera-se que os dados revelem qual das criptografias está mais vulnerável aos ataques de um invasor e qual a mais protegida, relatando também, a quantidade média de pacotes capturados necessária para burlar a segurança imposta por cada mecanismo, bem como o tempo médio necessário para que a chave de segurança fosse comprometida pelo usuário não autorizado.

5 RESULTADOS

Através dos testes efetuados com as diferentes criptografias, observado que em uma rede *Ad-Hoc*, independentemente da criptografia utilizada, o comportamento é muito semelhante, sendo necessário praticamente o mesmo esforço para quebrar as chaves de todas elas, conforme observado na tabela de resultados a seguir.

Tabela 5.1- Tabela de Resultados

Tipo de Criptografia	Quantidade de Pacotes Capturados (em milhares)	Chave Encontrada?	Tempo Necessário para encontrar a chave
WEP	5	Não	-
WEP	10	Não	-
WEP	15	Sim	4m 31s
WEP	20	Sim	6m 2s
WEP	25	-	-
WPA	5	Não	-
WPA	10	Não	-
WPA	15	Sim	4m 59s
WPA	20	-	-
WPA	25	-	-
WPA2	5	Não	-
WPA2	10	Não	-
WPA2	15	Sim	5m 18s
WPA2	20	-	-
WPA2	25	-	-

A seguir, serão abordados mais detalhadamente os resultados obtidos, explicitando detalhadamente o desempenho de cada uma das técnicas de criptografia empregadas na rede alvo do experimento.

5.1 WEP

Inicialmente foi criada uma rede *Ad-Hoc* utilizando-se a criptografia *WEP* com uma senha alfanumérica. Depois que os dois computadores autorizados se conectaram a rede, iniciou-se a transferência de um arquivo de aproximadamente 600MB para gerar tráfego na rede.

Juntamente a esse procedimento, o computador invasor, utilizando-se do pacote *Aircrack-ng* para capturar os pacotes que estavam sendo transferidos. Automaticamente, a cada 5000 pacotes capturados (5000, 10000, 15000... etc..) o *Aircrack-ng* executa uma nova busca pela chave que esta sendo utilizada para a criptografia naquele momento, mas para que isso ocorra é necessário indicar a rede da qual está ocorrendo à análise.

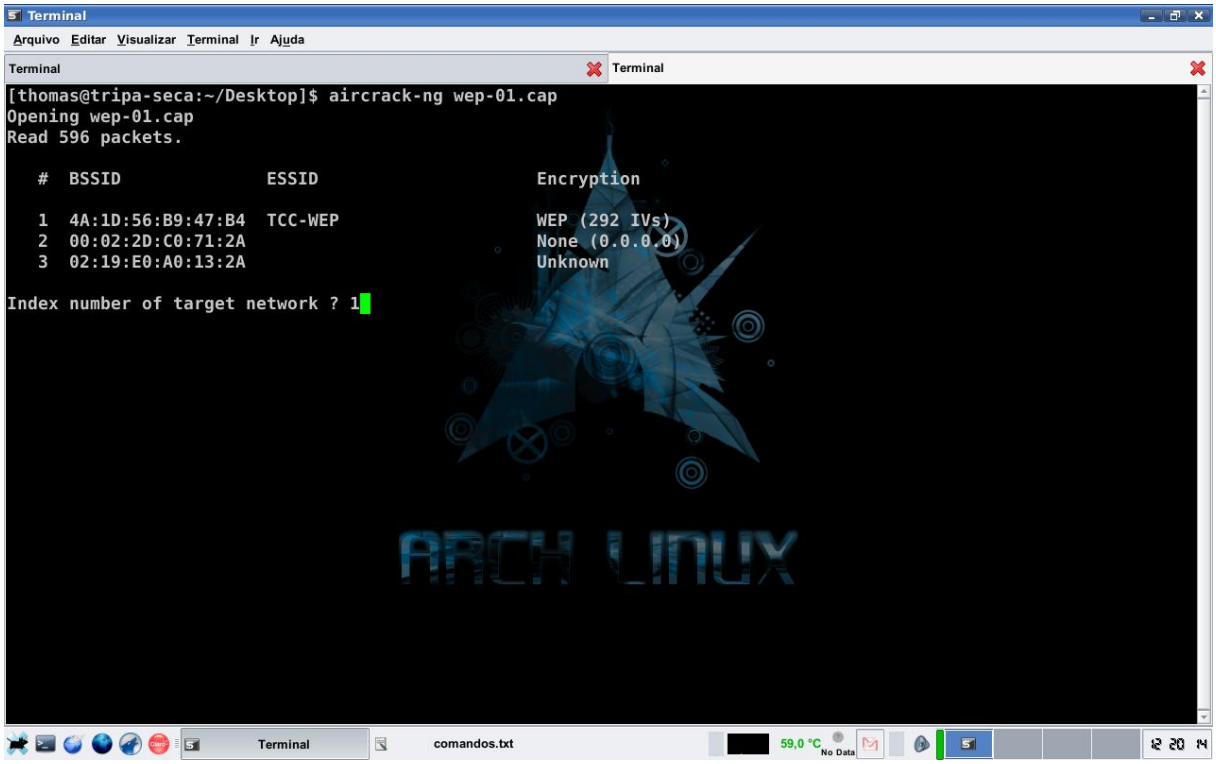

Figura 5.1 - Seleção da rede analisada no *Aircrack-NG*

O *Aircrack-ng*, como visto a seguir, alerta o usuário caso a chave não seja encontrada e comunica com qual quantidade média de pacotes o novo teste será realizado.

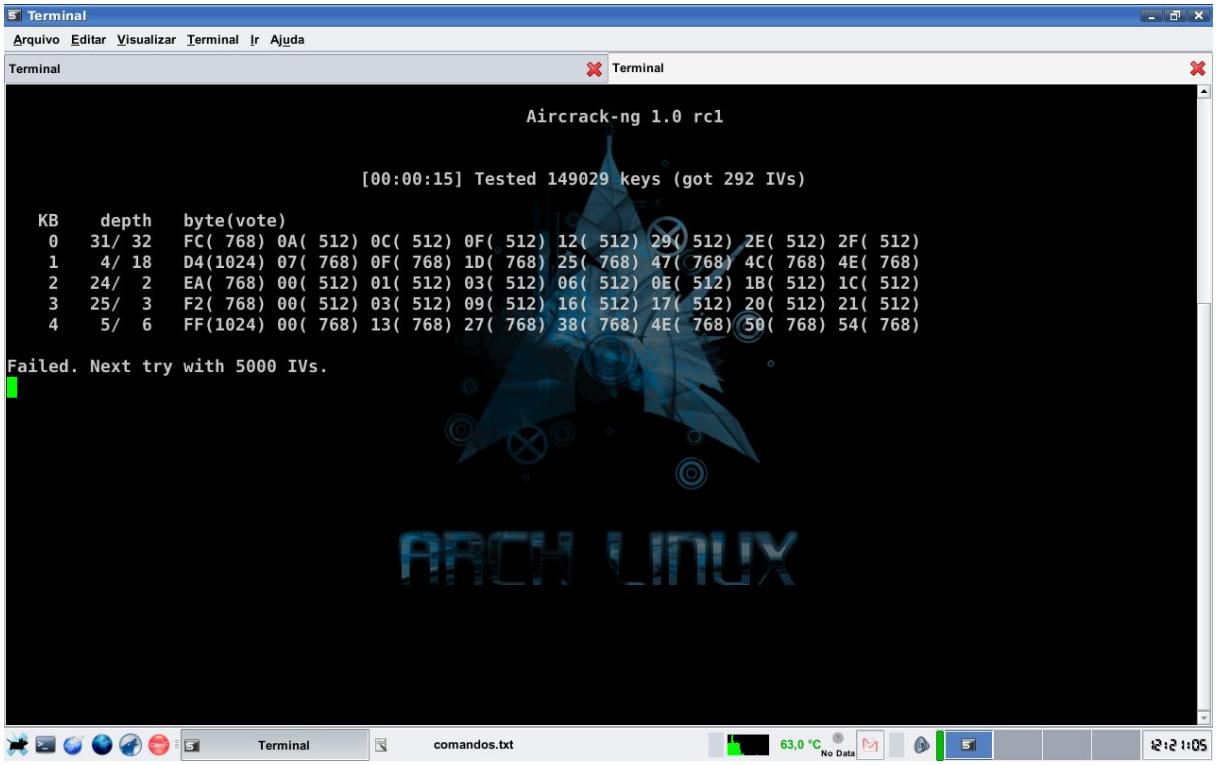

Figura 5.2 - *Aircrack-NG* informando que a chave não foi encontrada

Conforme observado na figura a seguir, foram necessários vinte mil pacotes para que a senha alfanumérica fosse descoberta.

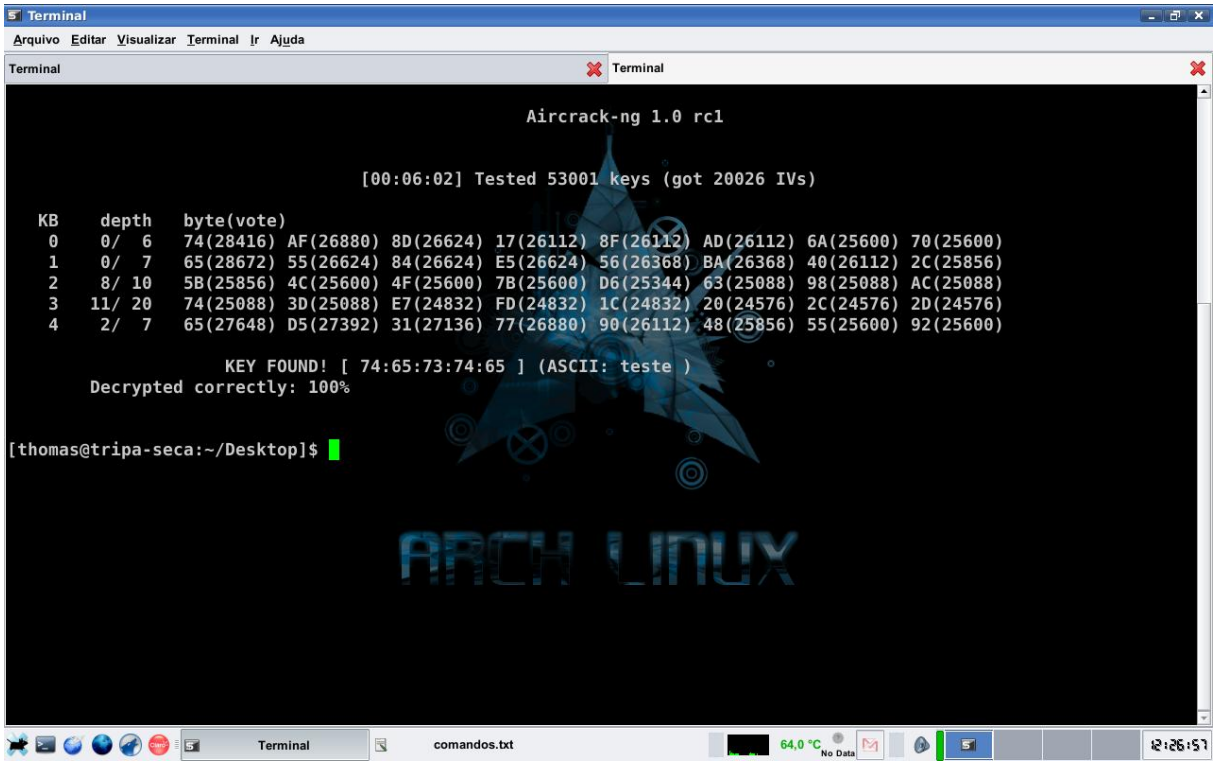

Figura 5.3 - *Aircrack-NG* informando a chave da criptografia alfanumérica da rede WEP

Posteriormente, alterou-se a chave para uma seqüência numérica onde se repetiu o mesmo teste. Neste novo teste com a senha apenas numérica, a qual foi mantida para os demais experimentos, foram necessários quinze mil pacotes, como visto na figura a seguir, para encontrar a chave de criptografia, ou seja, cinco mil pacotes a menos que com a senha alfanumérica.

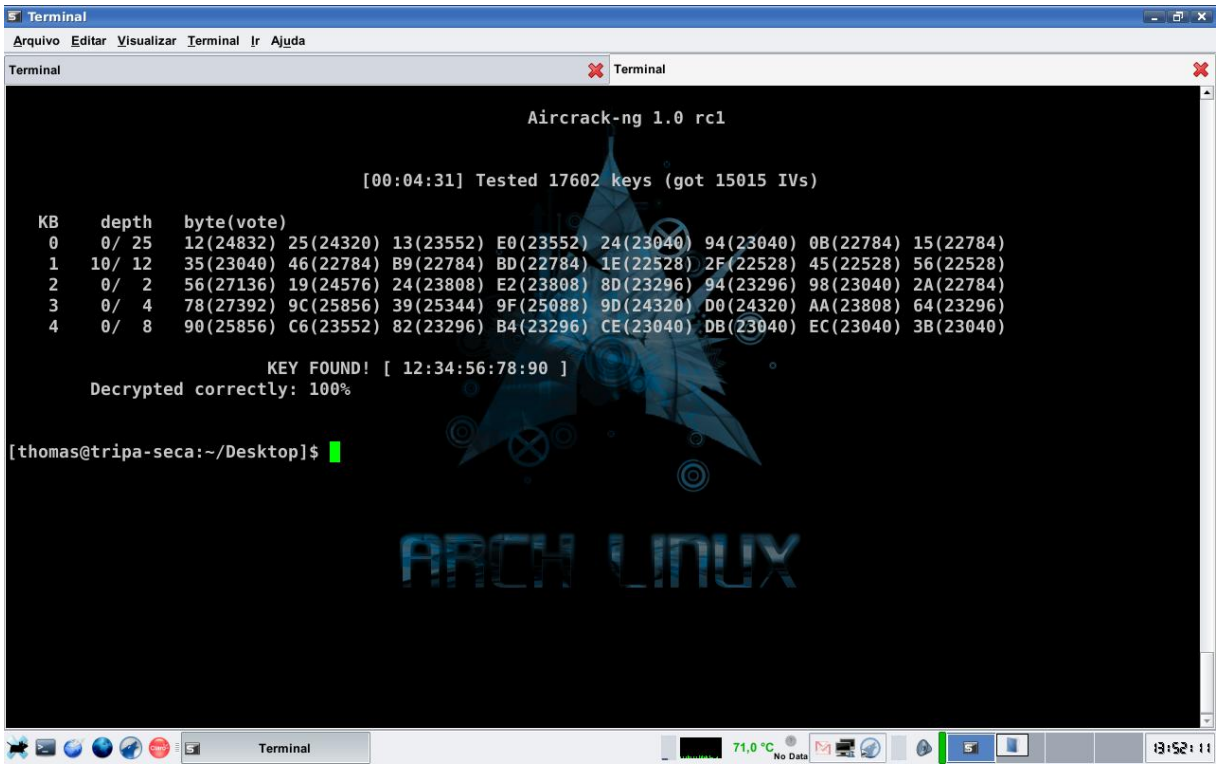

Figura 5.4 –*Aircrack-NG* informando a chave da criptografia WEP numérica

Considerando uma rede onde transitam quantidades significativas de dados entre os participantes, não é necessário muito esforço ou tempo para gerarmos um tráfego de quinze a vinte mil pacotes. Sendo assim, pode-se afirmar que a criptografia WEP não é uma criptografia que apresente bons resultados no quesito segurança.

5.2 WPA

Segundo a bibliografia, a rede com segurança WPA habilitada deveria proporcionar um grau maior de segurança para a rede. Possivelmente isso seja um fato em redes com infra-estrutura, devido a sua característica de conseguir efetuar uma troca de chaves dinamicamente através de um ponto central, porém como em uma rede *Ad-Hoc* esse ponto central é

inexistente e a chave é fixada manualmente, os resultados obtidos pela WPA foram muito similares ao da WEP.

Novamente utilizando uma senha numérica, efetuou-se a transmissão do mesmo arquivo transmitido no teste com a criptografia o WEP e como demonstrado na figura a seguir, foram necessários pouco mais de quinze mil pacotes para encontrar a chave de segurança da criptografia.

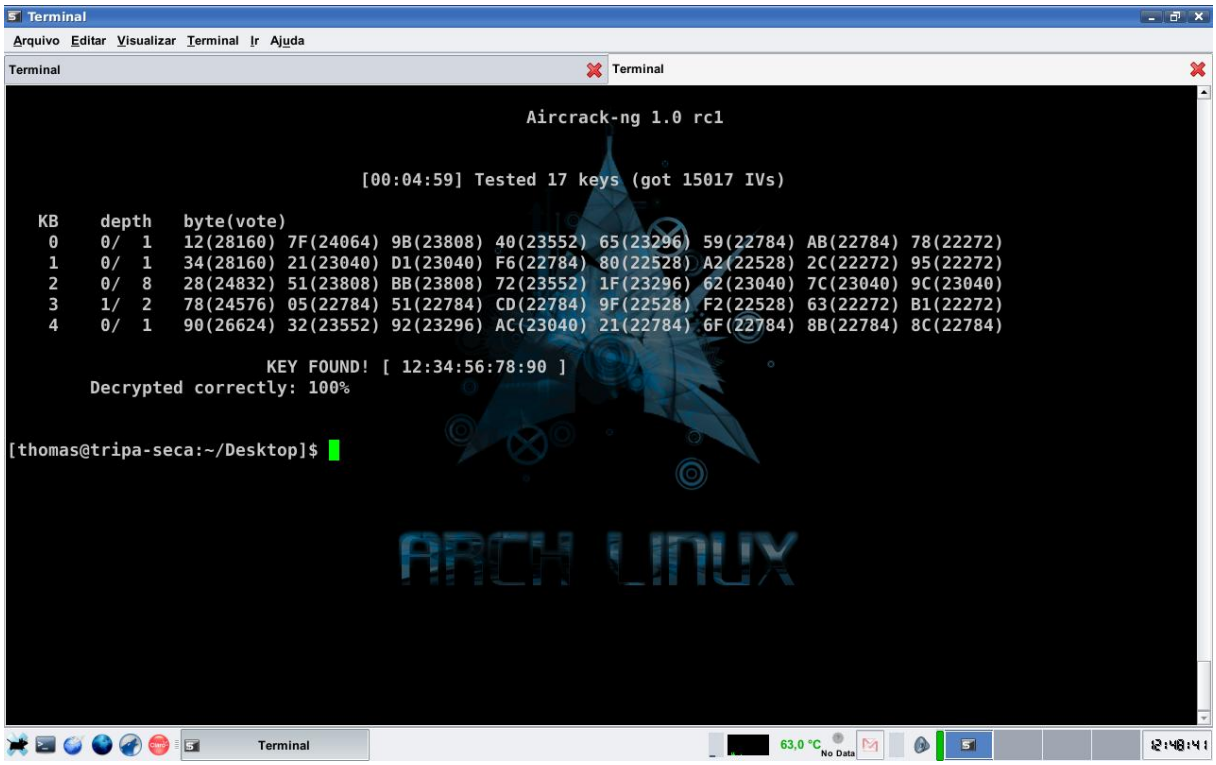

Figura 5.5 - Aircrack-NG informando a chave da criptografia numérica da rede WPA

Sendo assim, a segurança da criptografia WPA nesse tipo de rede, pouco difere da segurança proporcionada pela WEP, tornando assim tão vulnerável quanto sua antecessora. Vale ressaltar que os resultados obtidos são somente para redes *Ad-Hoc*, não podendo afirmar que em uma rede estruturada os resultados sejam os mesmos.

5.3 WPA2

A principal diferença entre o WPA e seu sucessor, o WPA2, é a melhoria no seu mecanismo de distribuição de chaves, dificultando a quebra da chave por força bruta em redes que dispõem deste mecanismo. Porém nas redes *Ad-Hoc*, ela é tão vulnerável quanto à criptografia que a antecede.

Com a chave fixada, o ataque por força bruta é um ponto fraco desta criptografia, já que a sua segurança basicamente está em seu mecanismo de troca de chaves, que por sua vez não pode ser empregado quando utilizamos as redes *Ad-Hoc.*

Sendo assim, a dificuldade para a quebra desta criptografia foi praticamente idêntica ao de sua antecessora, sendo a chave descoberta em pouco mais de cinco minutos.

5.4 Principais Dificuldades

Dentre as principais dificuldades para a execução deste experimento, pode-se citar certamente a diminuta quantidade de material que abordam diretamente a estrutura de rede aqui empregada. Outro grande problema foi a dificuldade encontrada em configurar este ambiente, uma vez que mesmo conectados os dispositivos envolvidos nos testes, em determinados momentos pareciam não localizarem-se na rede, ou simplesmente não conseguirem encontrá-la.

A plataforma do Windows Vista trabalha de forma satisfatória com essa rede, onde a configuração e manutenção da mesma tornam-se simples. Já o Windows XP tem sérios problemas com essas redes, onde, por muitas vezes, ele exibe em suas listas de redes wireless disponíveis redes que já não existem mais ou, muitas vezes, duplicatas da mesma rede, exigindo assim, um bom conhecimento e cuidado redobrado ao lidar com essas redes.

5.5 Considerações Finais

Analisando os resultados obtidos através deste experimento, pode-se afirmar que a segurança das redes *MANET* deixa muito a desejar, e ainda são necessários grandes esforços, e por que não dizer, uma nova tecnologia de segurança que possa focar nesta configuração de rede, já que as técnicas, que por muitas vezes são suficientes em redes estruturadas, em nenhum momento atenderam as necessidade de segurança da rede *Ad-Hoc.*

Já era esperado que a criptografia WEP não oferecesse uma segurança devido ao fato de ser uma criptografia antiga e confirmadamente frágil. Porém, o que foi observado é que nas redes *Ad-Hoc*, nenhuma das criptografias testadas atingiu um nível satisfatório de segurança, e ainda por cima, seu desempenho não foi melhor nem mesmo que a WEP.

Criptografias como a WPA e a WPA2, que baseiam seu princípio de segurança na troca dinâmica de chaves, não podem valer-se disto nas redes *MANET*, já que é necessário que um ponto central coordene essas trocas e, por sua vez repasse a nova chave aos integrantes da rede, o qual nesta rede não existe.

Sendo assim, pode-se afirmar que a segurança dessa rede é ineficaz. Comparado com redes estruturas, tanto wireless quanto cabeadas, a velocidade de transmissão de dados é significativamente menor. Contudo, não se pode afirmar que uma rede *MANET* não tem utilidade, porém seria aconselhável o seu uso somente em ambientes controlados, ou para a transferência de informações que não tenham conteúdo sigiloso.

5.6 Trabalhos Futuros

Visto que durante o desenvolvimento deste projeto as redes *MANET* mostraram-se inseguras de uma maneira preocupante, como sugestão para futuros trabalhos deixa-se temas como o estudo por meios alternativos para manter a segurança. Outro ponto interessante é uma proposta de um mecanismo de roteamento que permita uma troca dinâmica de chaves na rede *MANET*, tornando sua segurança comparável a redes estruturadas.

CONCLUSÃO

Em situações onde não há viabilidade ou necessidade da implantação de uma rede estruturada, seja ela cabeada ou *wireless,* utilizando um *acess point,* as redes *MANETs* são uma solução que podem solucionar problemas de conectividade de uma maneira barata, porém não podemos dizer o mesmo sobre segurança.

Na primeira parte deste trabalho buscou-se fazer um apanhado geral, buscando identificar quem são e quais as expectativas dos intrusos de uma rede, bem como identificar quais os principais ataques que podem ser lançados contra a rede. Logo após, devidamente identificados estes itens, buscou-se quais são os mecanismos de segurança necessários em uma rede para reduzir estes riscos.

Na seqüência, voltou-se para o estudo das redes *MANET,* passando por sua história, áreas de aplicação, mecanismos de roteamento, vulnerabilidades, e seus mecanismos de criptografia, descrevendo as três criptografias mais comuns para essa rede, que por ordem cronológica são WEP, WPA e WPA2, sendo a última criptografia citada uma "versão aperfeiçoada" da WPA.

Muitos autores referenciados fazem menção à dificuldade em manter a rede *MANET* segura, principalmente quando utilizando criptografias mais antigas e sabendo que o meio de transmissão dos pacotes pode ser considerado inseguro por natureza.

Os experimentos realizados revelaram que nenhuma das criptografias utilizadas para a segurança da rede realmente surtiu efeito na rede *MANET,* principalmente devido ao fato de que a chave de criptografia utilizada é fixa, e não dinâmica como em redes com infra-estrutura previamente definida. Não havendo um ponto central (*Access point)*, nenhum dos participantes destas redes toma para si a função de efetuar a troca de chaves dinamicamente, facilitando assim a quebra da mesma utilizando o método da força bruta.

Todos os três métodos mostraram-se facilmente subjugáveis, e não importando a criptografia aplicada, tendo a chave de todas elas sendo descobertas com uma quantia média de quinze mil pacotes capturados.

Por fim, não podemos negar a utilidade desta configuração de rede em locais que necessitem de comunicação e não possuem uma estrutura para isso. Contudo, não podemos afirmar que a segurança utilizada através de criptografias manterá as informações longe dos olhos de possíveis intrusos, sendo sua utilização aconselhada somente em casos onde não haja outro meio de realizar esta comunicação ou caso não exista a preocupação com as informações que estão trafegando pela rede.

REFERÊNCIAS BIBLIOGRÁFICAS

A.J.Menezes, P.C. van Oorschot, S.A.Vanstone, **Handbook of Applied Cryptography,** CRC Press, 1997.

AIRCRACK-NG. ***Aircrack-ng***. Disponível em: <http://www.*Aircrackng*.org/doku.php?id=portugues>, Acesso em: 09 jun. 2008.

ANDRADE, Marcelo B. de. COLLI, Rodrigo. **REDES *AD-HOC***. Disponível em: < http://www.revdigonline.com/artigos_download/art_2.pdf>. Acesso em: 18 jun. 2008.

Ângelo, Fernanda. **Faltam métricas à segurança da informação**. Disponível em:<http://checchia.net/node/130 >. Acesso em: 25 jun. 2008.

BRUEL, Cristiano M.**Redes em Malhas sem Fio**. São Paulo: USP, 2004. Instituto de Matemática e Estatística, Universidade de São Paulo, 2004.

CALETTI, Marcos. **IPS (INTRUSION PREVENTION SYSTEM,UM ESTUDO TEÓRICO E EXPERIMENTAL**. Novo Hamburgo: Feevale, 2006. Monografia (Bacharelado em Ciência da Computação), Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, 2006.

CARVALHO, Luciano Gonçalves. **Segurança de Redes**. Rio de Janeiro: Ciência Moderna, 2006. 90 p.

CRACKWIRELESS, **Como funciona o aircrack-ng e alguns exemplos,** Disponível em: <http://www.crackwireless.890m.com/index.php?option=com_content&task=view&id=7&Itemid=29>, Acesso em 30 out 2008

DEMSKI, Meri Fátima. **Segurança de Informações: Proposta de uma Política**. Novo Hamburgo: Feevale, 2000. Monografia (Bacharelado em Ciência da Computação), Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, 2000. 196 p.

GHDPRESS, **Usando o Wireshark**, Disponível em: <http://www.gdhpress.com.br/redes/leia/index.php?p=cap5-16>, Acesso em 01 nov 2008.

GHDPRESS, Wi-Fi: **Detectando vulnerabilidades com o Kismet,** Disponível em <http://www.gdhpress.com.br/blog/vulnerabilidades-kismet>, Acesso em 26 out 2008.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma Abordagem Top-Down**. 3.ed. Traduzido por Arlete Simalle Marques. São Paulo: Pearson Addison Wesley, 2006. 634 p. Tradução de: Computer Networking a Top-Down Approach Featuring the Internet.

MCCLURE, Stuart et al. **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**. 4.ed. Traduzido por: Daniel Vieira. Rio de Janeiro: Elsevier, 2003. 784 p. Tradução de: Hacking Exposed: Network Security Secrets & Solutions.

MELO, Sandro. Exploração **de Vulnerabilidades em Redes TCP/IP**. Rio de Janeiro: AltaBooks, 2004. 213 p.

MICROSOFT CORPORATION. **Configurar uma rede de computador a computador (ad hoc)**. Disponível em: <http://windowshelp.microsoft.com/Windows/pt-BR/help/293c504fb944-4d5d-835c-f080129bd5dc1046.mspx>. Acesso em: 18 jun. 2008.

NETO, João Carlos, **Segurança em Redes Móveis *Ad-hoc***. São Paulo: USP, 2004. Monografia (Doutorado em Ciência da Computação), Instituto de Matemática e Estatística, Universidade de São Paulo, 2004.

PC WORLD, **Conheça os tipos de criptografia digital mais utilizados**, Disponível em: <http://pcworld.uol.com.br/reportagens/2007/10/05/idgnoticia.2007-10-04.0383475254/>, Acesso em 23 out. 2008.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes sem Fio**. *2*.ed. São Paulo: Novatec, 2005. 224p.

RUSSELL, Ryan et al. **Rede Segura: Network**. 2.ed. Traduzido por Marcos Vieira. Rio de Janeiro: Alta Books, 2002. 652 p. Tradução de: Hack Proofing Your Network.

SANTOS, Bruno Ribeiro. Detecção **de Intrusos Utilizando o SNORT**. Lavras: Universidade Federal de Lavras, 2005. Monografia (Pós-Graduação Latu Sensu em Administração de Rede Linux), Departamento de Computação. 83 p.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Visão Executiva da Segurança da Informação**. Rio de Janeiro: Campus, 2003. 156 p.

STEFFEN JÚNIOR, Julio. **Sistemas de Detecção de Intrusão**. Novo Hamburgo: Feevale, 2003. Monografia (Bacharelado em Ciência da Computação), Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale, 2003. 95 p.

TUDO PCS, **Ethereal: programa para análise de tráfego na rede**, Disponivel em: <http://tudopcsjuauh.blogspot.com/2007/10/ethereal-programa-para-anlise-de-trfego.html>, Acesso em 16 out 2008.

UNDERLINUX, **Teste de Invasão em Redes Wireless** , Disponivel em: <http://under-linux.org/blogs/dennyroger/155-teste-de-invasao-em-redes-wireless.html>, Acesso em 18 out 2008.

W. Diffie, M.E. Helman, **New Directions in Cryptography, IEEE Transactions on Information Theory**, Vol.22, #6,1976,644-654p
W. Stalling, **Cryptography and Network Security: Principles and Practice**, 2°ed, Prentice Hall, 1997

WIKIPEDIA, ***Wireless***, Disponível em <http://pt.wikipedia.org/wiki/*Wireless*>. Acesso em 12 de mar. 2008.

WIKIPEDIA. ***AD-HOC***. Disponível em: <http://pt.wikipedia.org/wiki/Ad_hoc>. Acesso em: 09 jun. 2008.