UNIVERSIDADE DO EXTREMO SUL CATARINENSE - UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

ANGÉLICA DA CUNHA

ASPECTOS DE SEGURANÇA EM REDE SEM FIO AD HOC

CRICIÚMA

2012

ANGÉLICA DA CUNHA

ASPECTOS DE SEGURANÇA EM REDE SEM FIO AD HOC

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Msc. Paulo João Martins

CRICIÚMA

2012

ANGÉLICA DA CUNHA

ASPECTOS DE SEGURANÇA EM REDE SEM FIO AD HOC

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Redes de Computadores.

Criciúma, 28 de novembro de 2012.

BANCA EXAMINADORA

Prof. MSc. Paulo João Martins - UNESC
Orientador

Prof. MSc. Rogério Antônio Casagrande - UNESC

Prof. Esp. Sérgio Coral - UNESC

Dedico aos meus pais Sônia e José Carlos e ainda aos meus queridos amigos que me incentivaram a concluir mais esse passo na minha vida.

AGRADECIMENTOS

Agradeço a primeiramente a Deus por todas as bênçãos e oportunidades que me concedeu.

A minha mãe Sônia e ao meu pai José por sempre me apoiarem e incentivarem em todos os momentos.

A todos os professores do curso que me proporcionaram o conhecimento necessário para que eu pudesse

concluir essa etapa, em especial ao meu orientador Paulo pela paciência e dedicação.

Agradeço também a todos os amigos e colegas pela amizade e companheirismo.

Muito Obrigado a Todos Vocês.

“A melhor maneira de ficar em segurança é nunca se sentir seguro.”

Benjamin Franklin

RESUMO

Em meio aos avanços tecnológicos, cada vez há uma maior necessidade em se fazer uso de ferramentas que ajudem a manter as informações protegidas, ainda mais no que diz respeitos a redes ad hoc que ainda são pouco exploradas. Este trabalho consiste em um estudo sobre este modelo de rede dando enfoque nos mecanismos de segurança para poder aumentar a sua confiabilidade. São apontadas algumas vulnerabilidades e técnicas de segurança como protocolos seguros, criptografia, certificados digitais e outros para tentar impedir que tais ataques obtenham sucesso na descoberta de informações ou ocasionem problemas no desempenho das funcionalidades da rede. Ao final deste trabalho foi realizado teste de ataque e uma solução para o mesmo com objetivo de mostrar uma proposta de melhoria contra tal vulnerabilidade.

Palavras-chave: Rede Sem Fio, Ad Hoc, Segurança, Ataques, Vulnerabilidade.

ABSTRACT

Amid the technological advances, there is an ever greater need to make use of tools that help you keep your information protected, even when it about respects the ad hoc networks that are still unexplored. This work is a study on this network model focusing on security mechanisms in order to increase its reliability. Was pointed out some vulnerabilities and security techniques like secure protocols, encryption, digital certificates, and others to try to prevent such attacks of have succeed in discovering information or problems caused in the performance of network functionalities. At the end of this work was realized test out attacks and a solution for the same, with goal a proposal to show improvement against this vulnerability.

Keywords: Wireless, Ad Hoc, Security, Attacks, Vulnerability.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AC	Autoridade Certificadora
AODV	Ad Hoc On-Demand Distance Vector Routing
CSMA	Carrier-Sense Multiple Access
CTS	Clear To Send
DARPA	Defense Advanced Research Projects Agency
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
DSS	Digital Signature Standard
DSSS	Direct Sequence Spread Spectrum
ERR	Route Error
FHSS	Frequency Hopping Spread Spectrum
ICP	Infraestrutura de Chaves Públicas
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MRP	MultiPoint Relay
OLSR	Optimized Link State Routing
PKI	Public Key Infraestructure
PSK	Pre-Shared Key
RDP	Route Discovery Packet
REP	Reply Packet

REQ	Route Reply
RREQ	Route Request
RTS	Request To Send
SEAD	Secure Efficient Distance Vector Routing for Ad Hoc
SHA	Secure Hash Algorithm
SPAAR	Secure Position Aided Ad Hoc Routing
TCP	Transmission Control Protocol
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TIC	Tecnologia da Informação e Comunicação
TTL	Time-to-Live
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

SUMÁRIO

1 INTRODUÇÃO

As redes ad hoc surgiram no começo da década de 70, quando uma instituição de pesquisa dos Estados Unidos, passou a estudar como estabelecer uma comunicação via rádio em um ambiente tático militar. Havia naquela época grande necessidade de mobilidade dos dispositivos, o que seria de grande utilidade para que eles pudessem se comunicar por meio da rede e tivessem a facilidade na conexão de novos dispositivos.

Uma das vantagens deste modelo de rede é pelo fato de serem redes sem fio, que dispensam o uso de um ponto de acesso comum entre os computadores conectados a ela, de modo que os dispositivos da rede ao qual estão conectados funcionem como se fossem um roteador, compartilhando informações de dispositivos vizinhos. De acordo com Buiati (2004) o uso destas redes em operações de resgate, salvamentos e catástrofes naturais em conjunto com comunicação com satélite pode ser extremamente útil.

As redes ad hoc devido a sua capacidade de mobilidade, flexibilidade e rapidez em montá-la, são utilizadas para fins militares, salas de aula, para uso empresarial, pois podem ser facilmente utilizada em uma empresa para comunicação de setores. Em geral podem ser utilizadas em ambientes que necessitem de uma conexão entre si, inclusive não restringem o uso apenas de computadores, pode-se também conectar uma impressora ou celular a rede, por exemplo, desde que possuem suporte para isto. Conforme Buiati (2004) Também podem ser aplicáveis em ambientes de negócios, conferências, feiras onde participantes desejam disseminar ou compartilhar informações rapidamente por meio de seus laptops e PDAs.

A grande parte de pesquisas destas redes esta voltada para ao desenvolvimento de mecanismos básicos de operação. Mas ainda deve ser feito muito no que diz respeito sobre os requisitos de segurança, principalmente levando em consideração os cenários de operações hostis, como por exemplo, em aplicações militares e comerciais. No caso, supõe-se que a complexidade e os aspectos que envolvem os mecanismos de segurança variam com o tipo da aplicação ao qual será destinada. Conforme Soares (1995) segurança envolve procedimentos para minimizar a vulnerabilidade de bens e recursos, onde

vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém.

Muitas ameaças em relação a ataques a redes sem fio ad hoc estão em alguns serviços do tipo Channel Jamming, Denial of service, Device Theft, Eavesdropping, Masquerade, Message Forgery, Message Replay, The Docomo E-mail Vírus, entre outros, pois possuem uma arquitetura sem fio e sem infraestrutura dificultando assim que tais ataques serem detectados. Por exemplo, ataques do tipo Denial Of Service (ataques de negação de serviço) que ao conseguir invadir um sistema fazem com que o infectado e os nós utilizadores da rede tenham sua mídia de comunicação obstruída de modo que não se comuniquem de forma adequada, ou até mesmo faça com que o infectado tenha seus recursos gastos, como memória e processamento, ou ainda forçar ele a reiniciar e assim não possa fornecer mais seu serviço.

Com base nisto, o objetivo deste trabalho foi de identificar alguns pontos de vulnerabilidade em redes sem fio ad hoc e assim propor um modelo de segurança para tal que será definido ao longo do projeto.

1.1 OBJETIVO GERAL

Descrever algumas vulnerabilidades em redes sem fio ad hoc e fazer uso de técnicas de segurança para aumentar a confiabilidade neste modelo de rede no ambiente Windows Seven.

1.2 OBJETIVOS ESPECÍFICOS

1) Compreender e utilizar os conceitos de redes sem fio ad hoc.
2) Descrever algumas vulnerabilidades que ocorrem em redes sem fio ad hoc no que tange a segurança.
3) Estudar e aplicar técnicas de segurança em redes ad hoc.
4) Descrever um modelo de segurança em redes ad hoc visando impedir ataques das vulnerabilidades que serão abordadas no projeto.

1.3. JUSTIFICATIVA

Nos dias atuais em que o mundo é dominado por redes de computadores, faz-se de grande importância que as informações de um sistema sejam protegidas e gerenciadas. A grande maioria das empresas, instituições, organizações ou usuários residenciais, optam por armazenar informações em um sistema de segurança (AAD; HUBAUX; KNIGHTLY, 2004).

Neste caso a importância de fazer uso de mecanismos de segurança é vital, já que com a crescente tecnologia voltada à informação também é crescente o número de técnicas de intrusão a informação por indivíduos não autorizados.

Inicialmente, para fornecer segurança a redes sem fio ad hoc devem ser levados em conta os atributos básicos de segurança: autenticidade, confidencialidade, disponibilidade, integridade e não repúdio. Estas medidas visam evitar o vazamento de informações, fraudes, erros, uso indevido, sabotagens e roubo de informações (BUIATI, 2004), a segurança em redes sem fio se faz cada vez mais necessária já que o seu ponto fraco é a forma de transmissão de informações que é realizada pelo ar que podem ser capturadas a distâncias utilizando-se de uma antena amplificada.

Como as redes ad hoc têm ausência de infraestrutura todos os nós da rede funcionam como um roteador e assim pode ser realizado o encaminhamento das mensagens entre si, ou seja, todos os nós possuem o protocolo de roteamento. Todos os nós da rede estão sob o controle dos próprios usuários da rede e não como em redes comuns que possuem um administrador, por este motivo elas ficam ainda mais vulneráveis a ataques.

Os ataques a redes ad hoc móveis podem ser divididos em passivos ou ativos (MURTHY; MANO, 2004), os ataques passivos apenas realizam a espionagem dos dados da rede sem afetá-la de modo operacional, já os ataques ativos são caracterizados pela manipulação de dados da rede pelo atacante. Pesquisas apontam que os ataques ativos são os mais realizados e podem afetar as várias camadas do modelo OSI.

Devido à necessidade de segurança nas redes ad hoc, por meio deste trabalho visou-se a criação um modelo para a prevenção de algumas técnicas de ataques, foram realizados testes e a documentação dos mesmos, de forma que

outros possam utilizá-los, validando também o fato do conhecimento que foi adquirido com o estudo do tema proposto ao longo deste projeto.

1.4 ESTRUTURA DO TRABALHO

Com a finalidade de facilitar o entendimento dos assuntos aqui abordados, este trabalho foi dividido em 5 capítulos. O primeiro procurou esclarecer sobre o que será tratado no restante deste trabalho destacando a justificativa e os objetivos traçados.

No segundo capítulo é apresentada uma visão geral sobre a importância da segurança da informação, o funcionamento das redes sem fio ad hoc juntamente com a arquitetura que este tipo de rede pode assumir. Ainda neste capítulo, são abordadas as vantagens e desvantagens das redes ad hoc e alguns conceitos relacionados à segurança.

No terceiro capítulo são analisados os trabalhos correlatos que fazem referencia a segurança em redes sem fio ad hoc.

No quarto capítulo são abordadas as vulnerabilidades e métodos de ataque em redes sem fio ad hoc, destacando as técnicas de ataque existentes. Neste capitulo são apresentados o funcionamento de algumas das principais técnicas de ataque.

No quinto capítulo são apresentadas algumas características referentes à segurança das redes sem fio ad hoc. Neste capítulo destacam-se aspectos relacionados às questões de segurança dos mecanismos básicos de proteção. Criptografia, proteção de enlace e física, protocolos, certificados digitais também são abordados entre outros.

2 REDES SEM FIO AD HOC

A agência norte-americana Defense Advanced Research Projects Agency (DARPA) foi a responsável pelo surgimento das redes sem fio ad hoc, anos depois a mesma criou um programa chamado SURAN com a finalidade de expandir e proporcionar suporte a redes de maior porte, por meio do desenvolvimento de protocolos de rede que fossem mais flexiveis em termos de adaptação referente as variações das condições do ambiente, como por exemplo em um ambiente militar.

A DARPA, em 1994, criou o seu último programa chamado de GLOMO, onde este era um sistema robusto de informações com rapidez de expansão. Algum tempo depois com os avanços das tecnologias em redes sem fio ad hoc em ambientes militares, começaram a surgir outras aplicações voltadas para as áreas de busca e salvamento.

2.1 CONCEITO

As redes sem fio ad hoc ou também chamadas de Móbile Ad Hoc Network (MANET) é um tipo de rede ao qual não possuem um ponto de acesso entre os computadores conectados à mesma, sendo que estes funcionam como um roteador, formando uma rede em que a comunicação circula comunitariamente entre os terminais vizinhos. Segundo Kotviski (2011), no caso das redes convencionais os computadores necessitam de um ponto e acesso para fazerem a comunicação entre si, onde todas as informações irão passar por ele.

Esta é uma das vantagens das redes sem fio ad hoc, sua flexibilidade de transporte, montagem de rede e a não necessidade de um ponto de acesso, fazendo com que a informação trafegue diretamente entre os dispositivos conectados a rede, não somente computadores, mas também podem ser incluídas impressoras, celulares, entre outros, porém será apenas utilizado neste projeto o estudos de redes sem fio ad hoc somente entre computadores. Esta característica pode e deve ser aproveitada para aumentar tanto o desempenho da rede usando seus múltiplos caminhos quanto a sua segurança (BERNARDO; DUARTE, 2004).

A topologia de uma rede sem fio ad hoc pode mudar com muita frequência já que os nós que fazem parte desta rede podem ser movidos de forma

arbitrária. Levando em consideração a energia das baterias e a passagem de banda, torna-se um desafio o roteamento destas redes, onde se faz também necessária à reconfiguração constante destas redes devido à variação de conectividade entre os nós móveis.

2.2 FUNDAMENTO

Existe um enorme interesse em redes ad hoc, devido às suas inúmeras vantagens para determinado tipos de aplicações. Como possuem uma infraestrutura fixa, elas podem ser montadas de modo rápido e fácil. Devido a este fato, estas redes são adequadas a situações em que não existe ou em lugares em que não pode ser utilizada uma infraestrutura de comunicação por motivos de segurança, custo, entre outros.

Além disso, como as redes ad hoc em sua organização e controle não dependem de alguns terminais, sua performance não será afetada se por exemplo houver uma falha em algum terminal da rede ou até se algum nó deixar de fazer parte da rede. Podem ser adicionados com muita facilidade novos terminais a rede sem que ocorra danos ou prejuízos para a comunicação de informações.

Pode-se citar algumas aplicações comuns de neste tipo de rede como por exemplo PDAs, laptops e outros dispositivos portáteis. Com o passar do tempo, houve redução quanto ao tamanho dos equipamentos eletrônicos, ou seja, isto ocasionou o desenvolvimento de diversos tipos de dispositivos portáteis para a computação. Parte destes dispositivos possuem acesso a algum tipo de conexão em rede, como por exemplo rede local e acesso à Internet. Esta tecnologia atual necesssita que os dispositivos portáteis, para se conectar, estejam dentro de uma zona de alcance, desta forma reduzindo de forma drástica a abrangência e também a mobilidade do sistema.

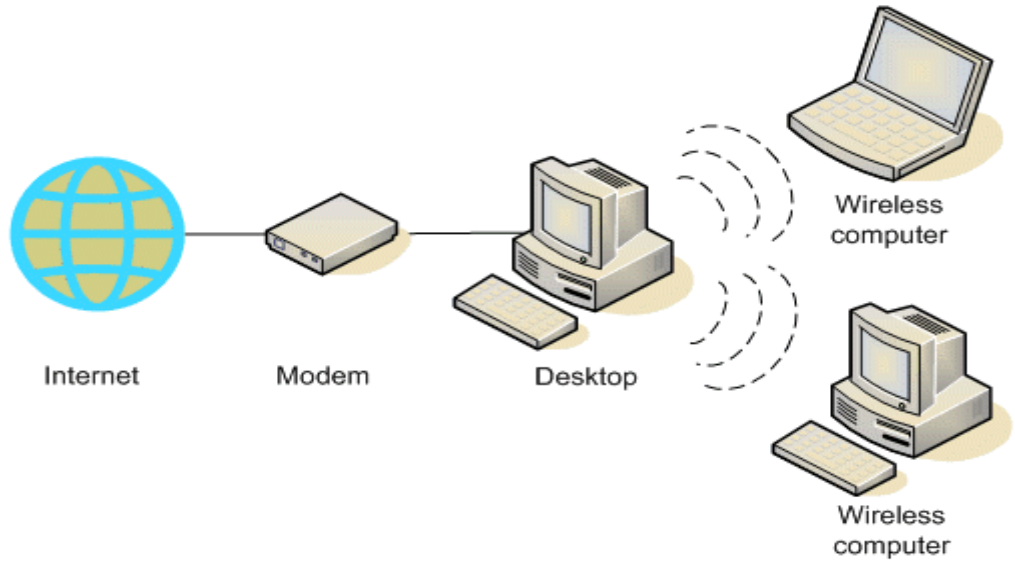
A utilização de uma rede ad hoc está associada a cenários onde exista uma necessidade de se instalar rapidamente uma rede (PINHEIRO, 2005). Normalmente, são cenários onde não há uma infraestrutura de rede previamente instalada. Algumas das aplicações são citadas a seguir: coordenação de equipes de resgate em situações de desastre como terremotos, furacões e inundações, troca de informações táticas em campos de batalha, compartilhamento de informações em reuniões e aulas.

2.3 ARQUITETURA DE REDE SEM FIO AD HOC

É formada por terminais de comunicação flexíveis, com hardware de custo inferior a redes cabeadas. Esses equipamentos fazem comunicação multissaltos por meio de interfaces Wi-Fi, possuindo ainda interface local Ethernet 10/100 Mbit/s, a qual pode viabilizar o tráfego de serviços de dados ou de Voip (MURTHY ; MANO, 2004). Implementam as funcionalidades de controle de acesso e roteamento necessárias para estabelecer as conexões, podendo operar como terminal de acesso residencial, repetidor ou gateway para redes externas.

O terminal ad hoc suporta transmissões em faixa de frequência de 230 MHz, conferindo flexibilidade e alcance de operação ao sistema.

Figura 1 – Arquitetura Rede Ad Hoc



Fonte: José (2012).

Diferente das redes convencionais não existe pontos de acesso, assim, na há estações de suporte a mobilidade, ou seja, não tem estrutura de conexão, e os nós são dependentes de outros nós para manter a rede conectada. Dessa forma as redes ad hoc são utilizadas principalmente em situações onde não é possível, ou não se faz necessário instalar uma rede fixa. A conectividade entre os nós móveis muda de forma constante, requerendo uma permanente adaptação e reconfiguração de suas rotas. Assim, limitações de banda passante e de energia das baterias dos nós torna o roteamento, principalmente o multiponto, em redes ad hoc um desafio.

2.4 VANTAGENS E DESVANTAGENS DA UTILIZAÇÃO DE REDES SEM FIO AD HOC

Várias vantagens e desvantagens podem ser citadas ao se comparar redes ad hoc com redes convencionais. De acordo com Pinheiro (2005), algumas das vantagens são:

a) **Instalação rápida:** as redes ad hoc podem ser montadas dinamicamente em locais onde não tem uma infraestrutura instalada previamente;
b) **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 quando se estabelece uma nova rota;
c) **Conectividade:** os nós móveis podem se comunicar diretamente entre si desde que cada nó esteja dentro da área de alcance do outro;
d) **Mobilidade:** principal vantagem em relação às redes fixas.

De mesmo modo pode-se citar algumas desvantagens abaixo:

a) **Roteamento:** A mobilidade dos nós e sua estrutura dinâmica contribuem fazendo com que a construção de algoritmos de roteamento seja um dos principais desafios em redes ad hoc;
b) **Localização:** a localização de um nó em uma rede ad hoc é muito importante, pois além do endereço da máquina não ter relação com o posicionamento atual do nó, não há também informações geográficas que possam auxiliar na determinação da posição deste nó;
c) **Taxa de erros:** associada com os enlaces sem-fio passa a ser mais elevada que em comparação com os enlaces em redes estruturadas;
d) **Banda passante:** Com o cabeamento convencional, ela pode chegar a 1Gbps. Em enlaces via redes wireless temos taxas de até 2Mbps tipicamente.

2.5 PROTOCOLO DE ROTEAMENTO

Não há um consenso sobre o tipo de protocolo de roteamento de redes ad hoc que seja condizente a todos os cenários ao qual são posicionadas. Cada protocolo em si possui vantagens e desvantagens indo de acordo com situações específicas.

Conforme Pinheiro (2005), o algoritmo de roteamento deve evitar a formação de loops, mesmo que seja por curtos intervalos. Soluções do tipo ad hoc como Time-To-Live (TTL) devem ser evitadas, pois abordagens mais estruturadas podem levar a um melhor desempenho.

Quando um nó precisa estabelecer uma comunicação, então se faz necessário a criação de rotas, onde, deste modo, alguns recursos como banda passante e energia são utilizados de uma forma com maior eficiência. A única desvantagem seria o tempo gasto em se realizar a descoberta de uma rota.

A operação proativa é recomendada em alguns cenários onde não há uma aceitação da utilização destes protocolos devido a sua latência, deste modo esta operação funciona armazenando previamente as rotas em tabelas de roteamento.

Segundo Pinheiro (2005), é desejável a existência de técnicas de segurança para evitar espionagem e modificação de dados transmitidos. Sem alguma forma de segurança proporcionada pela camada de rede ou de enlace, os algoritmos de roteamento são vulneráveis a vários tipos de ataques. Estes devem estar aptos à adaptação para os períodos de inatividade dos nós sem maiores consequências, independentes se tais períodos forem ou não comunicados previamente, os métodos de segurança e ataques em redes ad hoc serão apresentados nos próximos capítulos.

Os protocolos devem saber lidar com limitações típicas destas redes como, por exemplo: o consumo de energia ocasionado pelos nós móveis, limite de banda passante e as altas taxas de erro.

No entanto, com a mobilidade da rede, ocorrem constantes quebras de enlaces e frequentes mudanças de topologia, que podem aumentar muito o custo de se manter sempre atualizadas as informações topológicas da rede. Principalmente quando a carga da rede e baixa, fazendo com que muitas das rotas que são mantidas atualizadas não cheguem nem a ser utilizadas, causando um desperdício

de banda e processamento. Com isso, passou-se a utilizar os protocolos reativos, ou também chamados de sob demanda. Nesse tipo de protocolo, sempre que há a necessidade de uma rota para algum destino, o protocolo começa um processo de descoberta de rota para esse destino.

Esse processo e baseado em uma espécie de inundação da rede com o pedido de rota ate que o destino seja alcançado. O destino envia então para a fonte um reconhecimento de que foi alcançado, com a devida rota utilizada. Nessa abordagem, a principal vantagem e o fato de se ter um menor overhead na rede, já que esse tipo de rede apresenta rotas muito dinâmicas. Muitas das mensagens de roteamento de um protocolo proativo acabariam se tornando desnecessárias, já que enlaces poderiam se romper antes das rotas que passassem por ele chegasse a ser utilizadas, tornando mais eficiente à descoberta de rotas sob demanda. Contudo, esse mecanismo acarreta em um aumento do tempo de latência do estabelecimento das conexões, o que se mostra ser uma troca vantajosa na maioria dos casos.

Em meio aos vários protocolos de roteamento existentes, neste trabalho serão abordados apenas quatro dos protocolos mais utilizados em redes ad hoc, os protocolos são os seguintes: AODV e DSR, ambos reativos; OLSR e DSDV, ambos pró-ativos.

2.5.1 Classificação

Os protocolos de roteamento podem ser classificados de duas formas, como reativos e pró-ativos (YI et al, 2001).

Os protocolos reativos o descobrimento de rotas funcionam sob demanda, ou seja, somente quando um nó quiser realizar uma comunicação com algum membro da rede. Depois do estabelecimento da rota, ela passa a ser mantida por um mecanismo de manutenção de rotas ate que a mesma passe a não ter mais acesso ou ser inapta.

O uso de protocolo reativo diminui o fluxo de mensagens redundantes na comunicação para descobrimento de rotas na rede, assim, possibilitando maior economia de banda e de energia, mas por outro lado, mostra um maior atraso no envio dos pacotes.

Os protocolos de roteamento pró-ativos tem a finalidade de manter a consistência das informações sobre as topologias que estão armazenadas nas

tabelas de roteamento. Tais protocolos necessitam que cada nó possua no mínimo uma tabela para poder armazenar as informações de roteamento, onde as atualizações de informações são realizadas no momento em que um nó percebe que a topologia de rede foi alterada. Ou seja, neste protocolo é realizada uma avaliação continua das rotas, possibilitando que quando uma rota for requisitada ela poderá ser usada imediatamente.

Tabela 1 – Comparativo entre protocolos dos tipos Pró-Ativos e Reativos.

Características	Pró-Ativos	Reativos
Organização da Rede	Plano/Hierárquico	Plano
Topologia	Periódica	Sob Demanda
Disponibilidade de Rotas	Sempre Disponível	Quando Necessária
Tempo de Conexão	Baixo	Alto
Mobilidade	Atualizações Periódicas	Manutenção de Rotas
Overhead	Alto	Baixo

Fonte: Souza (2008).

2.5.1.1 Protocolo Optimized Link State Routing (OLSR)

Esse protocolo é pró-ativo, ou seja, troca informações periodicamente com os nós sobre a rede, com a finalidade de atualizar constantemente as tabelas de roteamento. O OLSR é um dos principais protocolos em uma rede ad hoc (QUAYYUM et al, 2001), que tem como objetivo diminuir a quantidade de nós da rede que encaminha estados de enlace, de modo que elimine mensagens redundantes.

A técnica utilizada neste protocolo é chamada de *MultiPoint Relay* (MRP), para demonstrar melhor seu funcionamento tenhamos como exemplo uma rede Ad Hoc sem o protocolo OLSR, quando um nó receber um pacote de informação, ele irá retransmitir esses dados aos nós vizinhos da rede. Então acontece o que é denominado como inundação, ou flooding, pois desse modo todos os nós passarão a receber o pacote, porem ele será enviado varias vezes de diversos vizinhos, gerando assim o que é caracterizado como overhead, ou seja, a sobrecarga de mensagens redundantes na rede.

Utilizando o OLSR o numero de nós da rede que reenvia os pacotes passa a ser limitado, ou seja, entre os nós haverá os nós chamados de MPR onde a escolha de cada um é realizada em consenso em todos os vizinhos próximos. Assim quando houver necessidade de atualizar uma informação, os nós MPR retransmitem os pacotes aos seus nós vizinhos, cada nó MPR que recebe a informação vai retransmitindo aos próximos nós ate que todos recebam a mensagem porem cada nó só receberá uma vez.

2.5.1.2 Protocolo Ad Hoc On-Demand Distance Vector (AODV)

Este protocolo tem a finalidade de se adaptar a cenários de alta mobilidade, desse modo possibilita evitar desperdícios de banda e reduz o processamento nos nós. Utiliza tabelas tradicionais de roteamento, assim é armazenado somente o salto seguinte para o nó de destino. É um protocolo reativo que em meio à necessidade de envio de pacotes a um nó de destino do qual não esta na tabela de roteamento, se inicia o processo de descoberta de rotas (Perkins et al, 2003).

Conhecida como um sub-protocolo do AODV, a manutenção de rotas neste protocolo se faz muito importante. Tem como finalidade fazer a validação das rotas contidas no cachê. A movimentação dos nós pode gerar um corte de uma ligação ao qual estava em uma tabela de roteamento dos nós já que os nós são móveis, então através da manutenção de rotas são enviados de modo periódico pacotes de *hellos* entre todos os nós da rede para analisar se existe alguma ruptura nas rotas. Se ocasionar de algum nó não receber o pacote, então se detecta um erro na transmissão, onde é enviado no mesmo momento um pacote indicando o erro ao nó de origem e aos nós que se faz necessário indicar tal erro. Dessa forma, quando um nó recebe o pacote de erro, passa a ter seu cachê atualizado, e assim, removendo da sua lista de rotas, todas as ligações quebradas anteriormente que foram armazenadas.

2.5.1.3 Protocolo Dynamic Source Routing (DRS)

Esse protocolo possui o melhor desempenho em cenários onde se possui baixa velocidade de mobilidade de nós (JOHNSON et al, 2001). No DSR os nós

armazenam um cachê do roteamento com as rotas conhecidas por cada nó. É um protocolo reativo do qual os nós se moverem a uma velocidade muito alta, as rotas armazenadas no cachê se tornam invalidas rapidamente, devido ao fato de não possuir uma verificação periódica das informações sobre a topologia da rede. O roteamento no DSR é por fone, desse modo o nó de origem tem conhecimento de todos os caminhos até o seu nó de destino. É divido em dois sub-protocolos que são: Descoberta e Manutenção de Rotas.

Em meio às semelhanças que esse protocolo possui em relação ao AODV, podem-se apontar algumas diferenças como o fato de que cada nó no protocolo DSR possuir em sua tabela de roteamento de todos os *hops*, de origem até o destino, desse modo, em seu cachê ele tem armazenado todo o caminho ou caminhos com todos os nós em que o pacote terá que percorrer. Já o protocolo AODV armazena apenas o próximo nó em seu cachê, ou seja, somente o *hop* em que o pacote deverá ser enviado, possuirá só uma entrada para cada destino. Segundo Perkins et al (2001) o protocolo AODV apresenta um desempenho melhor em redes com grande quantidade e mobilidade de nós, enquanto o protocolo DSR é melhor em redes com baixa mobilidade e números de nós.

2.5.1.4 Protocolo Destination-Sequenced Distance-Vector (DSDV)

É um protocolo pró-ativo com base no Distance-Vector e a implementação de números sequenciais (MURTHY; MANO, 2004), onde tem a possibilidade de identificar se uma entrada na tabela de roteamento for modificada e também quem foi o individuo que a ocasionou.

As tabelas de roteamento do DSDV possuem os campos de destino (onde é indicado todos os nós da rede e os caminhos possíveis para realizar o envio de dados), próximo (o nó próximo que deve ser enviado a mensagem para que alcance o seu nó destinatário), métrica (cálculo de saltos até alcançar o nó desejado), sequência (tem objetivo de sincronizar as informações que foram recebidas e para não ocasionar loops infinitos), tempo de registro (marcação do tempo) e estabilidade de dados (informa a estabilidade da rota).

A atualização deste protocolo é realizada quando uma informação for recebida por um nó, onde é analisado o número da tabela com o número de sequência da mensagem que foi recebida. Quando a informação recebida é mais

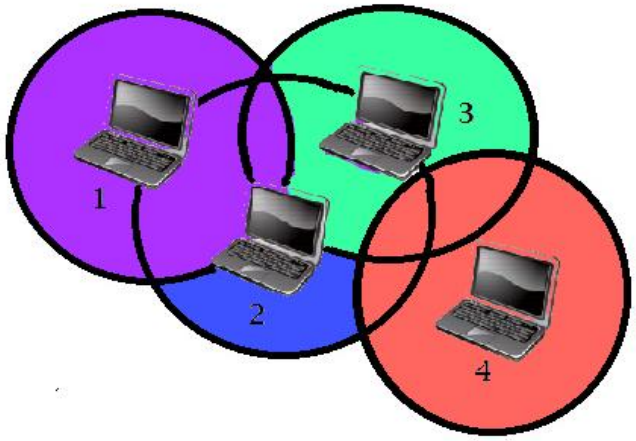
recente que a armazenada na tabela, a mesma é atualizada. Se caso for igual a existente em sua tabela somente será atualizada se a métrica da tabela for diferente.

2.6 COMUNICABILIDADE DE REDE AD HOC

As redes sem fio ad hoc são redes de comunicação direta, ou seja, cada dispositivo tem a capacidade de se comunicar apenas com os dispositivos que estão ao seu alcance. As redes ad hoc também são redes de múltiplos saltos, onde, por exemplo, dois dispositivos que estão em posições fora de alcance um ao outro, podem comunicar-se caso haja algum dispositivo que seja alcançável mutuamente pelos dois. 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 (PINHEIRO, 2005).

O alcance, portanto não fica limitado de acordo com cada dispositivo de modo individual, mas sim o alcance se dá pela soma dos raios de ação de todos os dispositivos que estão conectados a rede. Pode-se observar na Figura 2 um exemplo de rede ad hoc onde o alcance de comunicação de cada dispositivo é representado por um circulo, desse modo, para enviar uma mensagem de 1 para 4 tem que passar por 2 e 3, exemplificando assim que uma rota que conecta dois computadores pode conter vários saltos, podendo ser por um ou mais dispositivos da rede.

Figura 2 – Comunicação entre dispositivos em uma rede Ad Hoc



Fonte: Do autor.

2.7 IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Nos dias atuais a informação é essencial para os usuários seja de modo pessoal como de modo empresarial. Através da globalização a informação passa a ser vital para as organizações se estas quiserem prosperar no mercado. A informação é considerada um patrimônio importantíssimo para a boa condução de negócios, onde a mesma deve ser protegida e gerenciada de forma correta.

Conforme Soares (1995, p.448) faz abordagem:

> Segurança são procedimentos para minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos, onde vulnerabilidade é qualquer fraqueza que pode ser explorada para violar um sistema ou as informações que ele contém.

Ultimamente com a evolução rápida das Tecnologias da Informação e Comunicação (TICs), de acordo com Ghalin (2004) fez com que as organizações tivessem uma maior eficiência e agilidade referentes às tomadas de decisões, onde se fez necessário que as mesmas em sua maioria se pusessem a usar sistemas de informação. Devido a este fato pode-se observar a importância de se utilizar mecanismos de segurança e também de mecanismos de armazenamento das informações.

Anteriormente a área de TIC era muito defasada e simplória, já que a mesma era realizada guardando dados em papéis, por exemplo, apenas em arquivos os quais eram armazenados fisicamente sendo trancados em algum lugar específico, assim com a chegada das novas tecnologias esta atividade ficou mais complexa e assim dispondo de mecanismos mais seguros em alguns fatores.

3 VULNERABILIDADES E MÉTODOS DE ATAQUES EM REDES SEM FIO AD HOC

As vulnerabilidades podem ser divididas em vulnerabilidades dos mecanismos básicos e vulnerabilidade dos mecanismos de segurança. A primeira faz referência aos esquemas de criptografias, ou seja, aos mecanismos básicos de operação da rede, onde o mais crítico dele é o roteamento, e assim passam a fazer troca de dados criptografados. Já a vulnerabilidade dos mecanismos de segurança é mais complexa e agrega um determinado número diversificado de soluções, mas tornou-se consenso que o ponto crítico é o gerenciamento das chaves do sistema de segurança (HU et al, 2003). As redes ad hoc, devido à possibilidade de emprego em ambientes hostis, devem agregar mecanismos de forma a contornar o estado vulnerável em que se pode encontrar a rede quando da captura de um dos seus dispositivos.

A vulnerabilidade do sistema se dá quando os seus mecanismos básicos, por meio de alguma ação maliciosa, se tornam possíveis modificações, inserções ou replicações de dados de forma errônea nas operações da rede, ou mesmo faz possível um comportamento malicioso deixando assim que aconteçam interrupções nas operações do sistema. Os ataques podem vir de varias direções e visar qualquer nó da rede, bastando que o nó atacado esteja no alcance de transmissão do nó atacante (FERNANDES et al, 2006). Os mecanismos de segurança tem seu sistema vulnerável na criação e distribuição de chaves criptográficas onde permite que as mesmas passem a ser utilizadas para fins maliciosos por usuários não autorizados do qual o objetivo seria acessar os serviços e recursos da rede como um usuário autenticado.

Os ataques de negação de serviço constitui um grande perigo num sistema DOS, e em redes ad hoc, podem se capaz de ter sua origem numa falha de operação por meios não intencionais ou em por meio de agentes maliciosos através de algum nó da rede. As consequências para o funcionamento da rede irão depender da aplicação e do conhecimento de que os atacantes possuem. A identidade falsa é um ataque que pode ocasionar muitos prejuízos aos usuários da rede, devido ao fato de um nó se disfarçar de outro para realizar ações maliciosas a fim de se infiltrar e obter informações sigilosas da rede.

A possibilidade de descoberta de uma informação por indivíduos não autorizados deve ser combatida principalmente em de aplicações que necessitam de

um grau de segurança maior devido ao sigilo que dependem suas informações. Estas informações críticas devem ser protegidas contra ataques de exposição a fim de manter em sigilo detalhes como localização dos nós, chaves, senhas e identidade de operadores e proprietários dos dispositivos.

3.1 TÉCNICAS EXITENTES UTILIZADAS EM ATAQUES

A seguir são abordadas algumas técnicas de ataques utilizadas atualmente em redes ad hoc.

3.1.1 Ataques Passivos e Ataques Ativos

Na rede ad hoc os ataques podem ser divididos em passivos ou ativos (MURTHY; MANO, 2004). e também internos e externos, onde estes ataques têm como objetivos principais a descoberta de informações restritas a usuários na autorizados e também impedir que sejam realizados as operações da rede.

O ataque passivo assim como o interno são os ataques que mais afetam a rede, pois os mesmos agem de forma que compromete que o nó realize outros ataques aos demais nós. Enquanto aos ataques passivos e externos pode-se dizer que é o menos comprometedor, visando que nem por causa deste motivo ele deve ser desconsiderado em um sistema de segurança, ele é caracterizado pela captura de informações na rede.

Os ataques passivos não afetam a operação dos sistemas que compõem a rede, ou seja, a espionagem que apenas captura os dados da rede sem alterá-los. Enquanto os ataques ativos caracterizam-se pela alteração de informações do sistema, assim, estes ataques modificam, criam, excluem ou inutilizam a transmissão e uso de dados pelos usuários da rede, e também é importante ressaltar que estes ataques são os que mais são utilizados pelos invasores e podem atuar em diversas camadas do modelo OSI.

Nos ataques passivos, o atacante não interfere no funcionamento da rede, mas pode escutá-la e analisar o seu tráfego. O atacante tem acesso à informação, porém não a altera ou destrói. Os ataques passivos são de difícil detecção por não influírem no comportamento da rede.

3.1.2 Camada Física

Os ataques mais difíceis de serem tratados estão na camada física devido ao fato de exercerem utilização incorreta e sem autorização da rede sem fio por algum dispositivo móvel externo ao usuário que compõem a mesma. Mas os ataques nesta camada são os mais fáceis em comparação com redes cabeadas já que não se faz necessário à conexão física e sim apenas a conexão sem fio para poder se comunicar com os nós. Pode-se citar ainda que os ataques desta camada física são característicos do meio físico ao qual é utilizado, e não específico das redes ad hoc (HU et al, 2003).

3.1.3 Camada de Enlace

A camada enlace tem como objetivo realizar a transmissão de forma segura de dados ponto a ponto. É na camada de enlace que são definidos os links de dados, e é onde encontramos protocolos e tecnologias (CORRÊA, 2009). Deste modo, esta camada, os ataques visam à retransmissão de quadros, a prioridade de mensagens e os códigos corretores de erro, características específicas do IEEE 802.11, a tecnologia mais usada nas redes ad hoc. A solução para esses ataques consiste de uma implementação mais robusta do protocolo de enlace, prevendo o comportamento malicioso.

3.1.4 Camada de Rede

Na camada rede acontece a maior parte dos ataques, devido tanto às características críticas da rede, quanto às vulnerabilidades dos protocolos de roteamento (LAMPORT et al, 1982). Muitos dos ataques a essa camada possuem soluções eficientes, com métodos preventivos capazes de reduzir bastante à interferência do atacante na rede.

3.1.5 Ataques Multicamadas

Existem alguns ataques que não estão ligados a uma camada específica do modelo OSI, mas que podem afetar diversas camadas (HU et al , 2003).

3.2 FUNCIONAMENTO DAS TÉCNICAS DE ATAQUES

A seguir serão abordadas as formas como agem algumas técnicas de ataques utilizadas em redes sem fio ad hoc.

3.2.1 Espionagem

Esta técnica de ataque é caracterizada por ser do tipo passiva, pois ela somente escuta trafego sem modificar os dados da rede. Por meio de algum ponto vulnerável do sistema o atacante passa a roubar informações. Quando o atacante utiliza o tráfego observado para aprender a localização dos recursos críticos da rede, o ataque é chamado de Revelação de Informações Críticas (Homing/ Information Disclosure) (WOOD; STANKOVIC, 2002). Uma vez que esses pontos são encontrados, essas informações são passadas para outros nós maliciosos que poderão realizar ataques ativos. Neste caso, os protocolos de roteamento fazem uso de encaminhamento geográfico ficam extremamente, os atacantes ativos passam a ter a posição exata deste nos o que torna muito fácil localizar e atacar o nó.

Em casos de espionagem a proteção contra é de responsabilidade das camadas superiores, ao qual tem a finalidade de cuidar da privacidade das informações. Como a espionagem de informações de roteamento pode levar à exposição da topologia da rede para o atacante, o sigilo através da criptografia passa a ser uma necessidade do roteamento (KARLOF; WAGNER, 2003).

3.2.2 Interferência

O ataque de inferência é bem conhecido onde consiste em gerar de forma continua interferências na frequência de comunicação da rede. Se for uma rede com apenas um canal de comunicação este ataque será muito eficiente e realizado de forma bem simples. Um adversário pode impedir totalmente o funcionamento de uma rede com N nós utilizando k nós maliciosos distribuídos randomicamente (WOOD; STANKOVIC, 2002).

A interferência contínua é fácil de ser detectada, já que é necessário que o nó que foi atacado ou um nó próximo da área afetada possa observar que há um nível constante de energia e que isso que esta ocasionando a falha na comunicação

da rede e não a falta de resposta. Assim com a percepção interferência o nó que a detectar e que não esteja comprometido nela pode alertar aos demais nos da rede que evitem transportar informações pelas rotas afetadas. Mesmo que o resultado do ponto de vista da aplicação seja o mesmo em relação à perda de pacotes ou pela interferência, esta é mais grave por impedir que o nó envie ou receba pacotes, ou mesmo que se faça uma notificação para algum nó de monitoramento.

3.2.3 Interferência Esporádica

Este modo de interferência pode ser muito pior que a interferência contínua (WOOD; STANKOVIC, 2002). Consiste em criar varias interferências de curto período, o que ocasiona que a rede tenha sua comunicação defasada, ou seja, estas interferências são o suficiente para impedir a comunicação. Seus ataques são de grande eficiência já que são responsáveis por poderem causar um alto prejuízo em relação ao consumo da bateria do nó que esta sob ataque, de modo que o mesmo faz varias retransmissões, mas ao mesmo tempo em que o nó atacado esta com grande consumo de bateria o nó atacante tem apenas um custo mínimo, assim este realiza somente pequenas transmissões em alguns períodos de tempo. A interferência esporádica é um ataque difícil de ser detectado, a melhor maneira evitar que este ataque tenha grandes efeitos se dá pelo método de espalhamento de espectro.

3.2.4 Método de Espalhamento de Espectro

Algumas tecnologias de transmissão sem fio impõem um nível de dificuldade a mais a ataques da camada física (STALLINGS, 2004), um exemplo são as técnicas de modulação com base em FHSS. Algumas dessas técnicas como o *Direct Sequence Spread Spectrum* (DSSS) e FHSS possuem o objetivo de proporcionar uma maior resistência em relação às interferências de fontes de faixas que possam ter uma frequência abaixo do normal. Tem como base a utilização de uma largura de banda maior para realizar a transmissão de informações de acordo com uma velocidade especificada. O FHSS a técnica de espalhamento de espectro é realizada através de saltos contínuos na frequência de uma portadora para outra (GARCIA, 2002), tendo como objetivo assim minimizar as possíveis interferências.

Quando um atacante quer atacar a rede ele necessita saber a sequencia da portadora esta sendo utilizada, caso contrário ele não será capaz de gerar interferências inviabilizando transmissão de informações. Com o DSSS é capaz de aumentar a capacidade de dados em um sinal, desse modo ele mapeia cada bit de dados em uma cadeia de bits que serão transmitidos, denominada seqüência de chips. Este método faz com que seja espalhado um bit de informação por tempo, aumentando assim a eficiência contra interferências na comunicação. Uma seqüência de chips é transmitida a cada valor binário transmitido.

Pode-se dizer que estas técnicas de modulação por espalhamento de espectro não dispõem nenhuma proteção de criptografia, apenas faze uso de certo grau de segurança inerente. Sua segurança é gerada a partir do armazenamento oculto dos códigos de chips e de seqüência de portadoras, pois se estes códigos não forem protegidos o nível de segurança quanto a sua descoberta será mínimo, já que eles são de acesso fácil. Desse modo, ataques como de negação de serviço são extremamente simples de serem aplicados, pois não possuem quase nenhuma proteção, mas esta ainda é a melhor maneira de combatê-los.

3.2.5 Exaustão de Bateria por Colisão

Este ataque é caracterizado pelo consumo de bateria do nó atacado em que o nó atacante faz com que este fique retransmitindo informações de forma continua, por meio de algum recurso malicioso implantado na camada de enlace do nó afetado. As retransmissões funcionam da seguinte maneira: por exemplo quando se ouve o inicio da transmissão é gerada uma colisão tardia no fim do quadro. No caso desta colisão intencional ocorrer com um pacote isso poderia acarretar em um aumento exponencial do *back-off* em alguns protocolos *Medium Access Control* (MAC) (WOOD; STANKOVIC, 2002). Dessa forma a utilização continua dessa técnica ocasiona ao nó atacada a exausta da sai bateria já que a transmissão de dados é uma tarefa que exige um certo consumo e que deve ser realizada apenas quando se faz preciso.

Outra forma deste ataque que pode ser utilizado em ataques é denominada de ataque da interrogação, onde o nó que realiza o ataque é chamado de nó suicida devido ao fato deste mesmo explorar algumas características de protocolos da subcamada MAC, *Request To Send* (RTS), *Clear To Send* (CTS),

alem de mensagens de dados. O ataque do nó atacante faz com que seja forcado um grande numero de respostas ao CTS do nó atacado, assim fazendo com que haja muitos pedidos de alocação do canal com vários RTS iguais, dessa forma ambos entram em conflito.

Como a camada de enlace possui um determinado nível de confiança entre os nós que compõem a rede, o tratamento este ataque de exausta de bateria se torna difícil de ser tratado. Soluções para essa variação do ataque são obtidas na reformulação dos protocolos, tornando-os mais robustos a comportamentos inadequados (WOOD; STANKOVIC, 2002). Sendo que um nó atacante terá um gasto pequeno de energia utilizando da negação continua de acesso ao canal, tornando impedido o funcionamento da rede.

3.2.6 Ataque Bizantino

Caracteriza-se pelo ataque de um nó malicioso ou mais nós com objetivo de ocasionar vários problemas entre eles estão relacionados problemas em *loops* de roteamento, envio de pacotes de roteamento inexistente ou falso, escolha das piores rotas, assim esta técnica aproveita-se de problemas que a rede possa ter quanto a tolerância a falhas. Além disso, os nós também podem executar um encaminhamento seletivo (MURTHY; MANO, 2004). Apesar de o nó estar mostrando algumas anomalias, para os outros nós ele estará funcionando de forma normal o que torna difícil deste modo detectar este ataque.

O nome ataque bizantino tem uma origem curiosa, a idéia é baseada no problema dos generais bizantinos, distribuídos em campo com suas tropas para organizar o ataque à cidade inimiga (LAMPORT et al, 1982). Eles fazem a comunicação entre si através de mensagens, mas pode ser que haja um ou mais generais traidores entre eles o que se faz necessário um algoritmo que garanta que os generais leais possam chegar a um acordo, sem serem confundidos pelos traidores.

O objetivo é que todos os generais leais entrem em consenso com um plano de ação e os generais traidores não os influenciem a optar por um plano ruim. Dessa forma é necessário que a mesma informação seja recebida por todos os generais leais e se um general leal esta mandando uma informação esta mesma deve ser passada a todos os outros generais leais. Podemos simplificar o problema

seguindo pelo ponto que um general envia sua ordem a dois tenentes, a solução é trivial porque não se tem como alterar o que foi dito já que a comunicação é de forma direta, então o pode-se ser concluído que o problema se inicia a partir de três generais.

Com base nos armazenamento das rotas de todos os nós da rede pelos protocolos de roteamento pró-ativos da rede ad hoc, já que o nó tem em sua tabela de roteamento armazenada todas as mensagens de rota que recebe dos seus nós vizinho, o ataque tem com estratégia disponibilizar várias rotas para nós inexistentes, assim aumenta progressivamente o tamanho da tabela de roteamento, até que a mesma não consiga mais armazenar dados e o nó não possa mais armazenar as rotas reais. Enquanto os protocolos reativos que armazenam muitas rotas para um mesmo destino, passam a ficar vulneráveis a esse tipo de ataque devido ao nó atacante poder enviar rotas por meio dos nós inexistentes.

Em redes ad hoc este ataque causa sérios danos já que os nós da rede têm recursos mais escassos, ou seja, estes gastos de energia com a recepção de mensagens excessiva e o estouro do buffer são extremamente fatais. Uma forma de prevenção para este ataque é tornar limitado o número máximo de rotas na tabela de roteamento e bloquear a aceitação de entradas apenas para nós autenticados na rede.

3.2.7 Replicação de Pacotes

Este método de ataque tem como objetivo fazer a ocupação do meio de transmissão e assim levar os nós da rede à exaustão. O ataque consiste em enviar réplicas de pacotes de roteamento antigas (WOOD; STANKOVIC, 2002).

Não existe muitas soluções para este ataque já que se supõe que o nó envia mensagens de roteamento antigas por meio da observação do número de sequência, que se pode propor seria tirar este nó das rotas, mas mesmo assim não poderia impedir o mesmo de continuar as suas replicações de roteamento, idêntico ao que acontece na camada física no ataque da interferência.

3.2.8 Envenenamento de Cache

Similar ao ataque de estouro da tabela de roteamento, O ataque de envenenamento de cachê consiste em fazer anúncios falsos de rotas para os outros nós da rede. Esse ataque se aproveita em especial de protocolos sob demanda, como o AODV (PERKINS et al., 2003), mantendo rotas para nós que foram armazenadas recentemente. Estes protocolos, diferentemente dos pró-ativos, permitem que nó atacante anuncie uma rota falsa antes de outro nó autenticado da rede, pois este protocolo anuncia para onde deve ser mandado o pacote sempre não se tem uma rota.

Com base nos protocolos pró-ativos esse ataque é possível, mas seria necessário mandar anúncios de rota falsos para todos os destinos em todas as rodadas de atualização. Uma solução para evitar este ataque seria utilizar sistemas baseados em monitoramento e punição.

3.2.9 Inundação de Sync

Este ataque tem como objetivo gerar vários pedidos de conexão ao nó atacado, com base na comunicação por meio do TCP ao qual é necessário certo tempo para realizar a conexão e processo pelo qual a conexão ocupa um espaço de memória no nó até que o mesmo seja concluído. Estes pedidos de conexão nunca serão completados irão provocar a alocação de muitos recursos ate que aconteça o estouro da memória.

Uma solução seria limitar o número de conexões para impedir a exaustão de recursos, mas devido ao grande numero de pedidos falsos de conexão não seria possível impedir que os outros nós da rede percam suas conexões (MURTHY; MANO, 2004). Também pode ser utilizada a implantação de certos desafios na rede para ocasionar diminuição da velocidade em que o nó atacante gere os pedidos de conexão falsos.

3.2.10 Dessincronização

Este ataque consiste em um terceiro nó influenciar em uma conexão de outros dois nós legítimos. O nó atacante manda mensagens falsas com pedido de

retransmissões, observando o número de sequencial utilizado na comunicação. O atacante então monitora se os outros nós estão trocando informações para analisar se o ataque foi ou não descoberto. Uma maneira de proteger contra a dessincronização seria o uso de criptografias para troca de mensagens e também autenticação de usuários.

3.2.11 Ataque de Pressa (Rushing Attack)

Através deste ataque pode-se formar um buraco negro, ao qual se aplica aos protocolos de roteamento sob demanda que guardam apenas uma rota para cada destino em sua tabela. Ao receber uma mensagem de solicitação de rota, o atacante o envia rapidamente a todos os nós da rede, assim faz com que todas as respostas venham a passar por ele. Desse modo, o nó atacante passa a ser o primeiro a responder e todas as respostas que viriam dos outros nós da rede são descartadas, ou seja, assim a rede passa a se tornar vulnerável pelo fato e todas as rotas sempre passarem pelo nó malicioso.

Como na visão do protocolo de roteamento esta tudo ocorrendo de forma normal na rede, caracteriza-se assim um ataque difícil de detectar. A solução seria tentar identificar algumas formas de poder enviar mensagens modo mais rápido, um exemplo seria o protocolo de enlace. De fato, existem vários métodos para acelerar o envio da mensagem, e que não exigem muitos recursos do nó malicioso (HU et al., 2003).

Os protocolos MAC possuem um atraso maior entre a recepção e a transmissão dos pacotes. Pode-se citar os protocolos MAC que tem divisão de tempo para acesso ao meio, assim o nó precisa esperar chegar a sua vez de fazer transmissões, ou também os protocolos de acesso ao meio que tem *Carrier-Sense Multiple Access* (CSMA), desse modo evitam colisões, pois possuem um *backoff*. Um nó malicioso ainda pode burlar um espaço de tempo do roteamento entre o recebimento de um RREQ ate o momento da sua transmissão, o qual também seria utilizado para evitar colisões. Portanto se um nó atacante quiser enviar de forma rápida um pacote basta ignorar os tempos de espera.

Outra maneira de executar esse ataque seria, por exemplo, provocar a criação de filas nas interfaces dos nós da rede, de forma a que o nó atacante repasse o pacote enquanto os demais nós estão processando os pacotes que estão

na fila. Esse tipo de atitude do nó malicioso é mais fácil em sistemas que utilizam autenticação da mensagem, pois ele poderia gerar várias mensagens com defeito, levando os vizinhos a perder tempo verificando as mensagens. Uma das soluções para este ataque seria o uso de múltiplas rotas disjuntas ou trançadas, assim passariam a garantir que mesmo em meio a atração do tráfego de rotas para o nó malicioso, todas as demais continuariam seguras.

3.2.12 Direcionamento Falso

Este ataque realiza a fabricação de mensagens com o objetivo de gerar negação de serviço para um determinado nó. São enviadas várias mensagens direcionando o tráfego para uma região pré-determinada ao qual se deseja atacar. Na versão da Internet do ataque de direcionamento falso, também denominada de ataque *Smurf*, o nó malicioso cria pacotes *echo*, ao qual o nó da vitima fica como se fosse o emissor que passara então a receber diversas *echo-backs*.

Esse ataque pode ser realizado por mecanismos além do uso de *echos*. O caso do protocolo DSR é um exemplo, onde o atacante pode responder às requisições de rotas com caminhos falsos que incluem o nó que se deseja atacar (JOHNSON; MALTZ, 1996).

3.2.13 Ganância

O ataque de ganância tem como objetivo obter sempre o maior tempo para transmissão, assim recebendo o nome de ganância. Este ataque não prejudica de modo explicito o funcionamento da rede. Como um nó que esteja apresentando problemas de bateria teria este mesmo comportamento do nó malicioso se caracteriza difícil de detectar este ataque. O modo mais eficiente de evitar este ataque seria através da utilização de redundâncias, o que garantiria uma segunda rota para garantir a entrega de pacotes, mesmo que, ainda assim, alguns pacotes seriam perdidos devido à demora no envio.

3.2.14 Encaminhamento Seletivo

A confiança nos nós vizinhos de faz uma das características principais das redes ad hoc para a transmissão de informações. Mas um nó malicioso pode enviar somente alguns pacotes, neste caso o objetivo não é prejudicar uma área especifica ou todos os nós da rede. O nó malicioso tem a opção de enviar, ou não, uma mensagem ou todas as mensagens para um determinado nó, e também pode enviar todas as mensagens de roteamento para impedir a transmissão de informações.

Uma forma de encaminhamento seletivo especial é o conhecido como egoísmo, em que o objetivo é fazer com que o nó não encaminhe nenhuma mensagem aos demais nós, e assim passe apenas as suas mensagens. Pode-se ressaltar que o egoísmo nem sempre é considerado um ataque, devido ao fato de este comportamento poder ser uma opção de algum nó da rede, em meio a uma escolha não cooperativa do próprio nó. A detectação deste ataque é difícil, similar à ganância, já que os nós que apresentam pouca energia e perdas de pacotes se mostram com características idênticas.

3.2.15 Buraco Negro

O objetivo deste ataque é atrair todos os pacotes e então destruí-los, o buraco negro é caracterizado com um caso extremo de encaminhamento seletivo. Dependendo da posição do nó atacante, este ataque pode ser fatal na rede, ocasionando a parada do seu funcionamento. Mas comparado com o encaminhamento seletivo a sua detecção é muito simples, pois rapidamente parte da rede não estará mais funcionando.

Outro fator que o buraco negro ocasiona é o alto consumo dos recursos dos nós a sua volta devido à atração de um grande numero de trafego para si, tanto em termos do meio, pois fica extremamente sobrecarregado, quanto em termos de recursos destes nós.

Se ocorrer a exaustão dos nós poderia ocasionar o particionamento da rede. Do mesmo modo que o encaminhamento seletivo, ao iniciar o ataque o nó atacante se torna atrativo aos demais nós na escolha de rotas.

Nos casos de ataque de buraco negro a solução mais fácil seria utilização de múltiplas rotas, assim como fazer uso de métodos como investigação e autorização que põem ajudar na prevenção e detecção.

3.2.16 Túnel de Minhoca

Neste ataque dois atacantes criam um túnel de comunicação por um enlace de baixa latência, onde trocam dados da rede, passam então a replicá-la do outro lado do túnel, desse modo tornam atrativo o enlace formado por ambos. Então, os nós atacantes têm a possibilidade de convencer os nós da rede de que podem se comunicar com certo destino de uma forma mais simples por somente um salto, assim poupam os nós de realizarem diversos saltos entre o nó e o seu destino, saltos que de fato existem. Assim os nós maliciosos impedem que os outros nós da rede percebam que esta havendo um ataque à rede mostrando o túnel como um canal seguro e com baixa latência.

Uma forma simples de obter esse resultado é utilizar uma conexão por fio entre os dois nós, fazendo uma transmissão mais rápida que o encaminhamento por múltiplos saltos (HU et al, 2003). Outra possibilidade seria a utilização de um enlace direcional sem fio de longa distância, para conseguir maior velocidade que comunicações que normalmente utilizariam mais que um salto (HU et al, 2003). Também existe uma técnica que se mostra eficiente no caso deste ataque, que é o envio e *bits* direto sem a espera de pacotes antes de iniciar a transmissão.

É importante ressaltar que, quando o atacante construir o túnel de forma honesta e confiável, nenhum prejuízo direto é causado à rede, ou seja, passa a ser um serviço empregado em aprimorar a eficiência da conexão. Mas se o ataque fizer com que os nós atacantes fiquem em uma posição privilegiada, possibilita que os mesmo passem a ocasionar diversos prejuízos à rede.

Como um nó não precisa ser autenticado para enviar um pacote e dados, este ataque pode facilmente ser realizado mesmo em meio a implementações de autenticidade e confiabilidade na rede. É importante destacar que, para as camadas superiores, ele é invisível, e igualmente para a camada de roteamento, a princípio é complicado perceber a sua presença.

3.2.17 Exaustão de Bateria

O ataque como já explicita o nome, tem como objetivo consumir a bateria do nó atacado, até que o mesmo seja inativado. Desse modo, ele pode ser aplicado a várias camadas. Se o ataque fosse realizado por meio de interferências, seria tratado como um problema da camada física. Já se a interferência for gerada com o objetivo de gerar retransmissões, seria tratado como um problema da camada de enlace. O ataque também pode dificultar a sua detecção por meio de retransmissão de mensagens reais da rede.

Tantas versões para o mesmo ataque se justificam pela importância da vida útil da bateria para dispositivos móveis, e, pela mesma razão, várias metodologias para poupar bateria já foram desenvolvidas (WOOD; STANKOVIC, 2002). Por este motivo os aplicativos de segurança que necessitam do modo promíscuo são bastante criticados, já que a tarefa de ouvir a rede de forma continua consome muita energia do nó, assim o mais indicado é colocá-lo dormindo sempre que houver possibilidade. Outros nomes dados a esse ataque são *Sleep Deprivation Attack* e *Spam Attacks* (MURTHY; MANO, 2004).

3.2.18 Negação de Serviço

O ataque de negação de serviço pode ser definido como qualquer ação que reduza ou elimine a capacidade da rede de realizar uma de suas funções esperadas (WOOD; STANKOVIC, 2002). Este ataque é causado por qualquer ação que e alguma maneira prejudique a rede, como por exemplo falhas de hardware, defeitos de programas, exaustão de recursos com ou sem intenção, condições ambientais não favoráveis ou qualquer interação dos mesmos.

Assim, os ataques ativos poderiam gerar uma negação de serviço na rede, dando a esse ataque uma classificação de multicamadas. Existe também a negação de serviços distribuída que é uma forma de ataque de negação de serviço mais perigosa, onde muitos atacantes estão distribuídos pela rede com o propósito de fazer um conluio impedindo que usuários legítimos possam tem acesso aos serviços. Ressaltando que este ataque tem um efeito muito mais rápido sobre a rede, podendo ocasionar o impedimento total do seu funcionamento sem dificuldades.

3.2.19 Sybil

Baseado no fato de ser quase impossível os nós que não se conhecem apresentem identidades convincentes. Assim, o ataque sybil acontece quando um único hardware assume múltiplas identidades em uma rede (NEWSOME et al, 2004). Uma entidade pode dispor de diversas identidades, se não houver um ponto central que faca o controle dessa associação de identidade para cada entidade. O sybil ocorre quando uma entidade não autorizada, por exemplo, consegue gerar certificados para os nós da rede (JOHN, 2002).

Em vista de que muitos sistemas utilizam de sistemas de réplicas de dados armazenados, para obter maior garantia contra violação de integridade, e sistemas de fragmentação de tarefas, para maior segurança contra violação de privacidade, este ataque de sybil passa a ser muito perigoso. Em ambas situações, a redundância, passa a ser um ponto crucial. Desse modo quando o nó malicioso assume suas múltiplas identidades, assim o sistema pode escolher este nó para armazenar as réplicas ou fragmentos, ou seja, dessa forma destruiria toda a segurança do sistema já que o nó malicioso ficaria com todas as informações.

O ataque de sybil não necessariamente é utilizado para atacar somente armazenamentos distribuídos, outra forma de ataque é o roteamento de múltiplos percursos. Os protocolos que fazem uso desta técnica visam escolher caminhos disjuntos ou trançados para minimizar possíveis atacantes na rota. O sybil pode ser realizado de modo que ponha uma identidade falsa em cada uma das rotas, assim todos os caminhos passarão pelo nó atacante.

Com base no campo de roteamento, outro problema comum, ao qual não tem relação com redundância, é o ataque ao roteamento geográfico. Nesta situação, o nó atacante indica sempre uma de suas identidades sybil como o nó mais próximo ao destino, fazendo com que todos os pacotes de roteamento passem pela mesma.

Outra forma de um ataque sybil é através da utilização dos nós sybils para falsificar resultados de votações na rede. O nó atacante cria inúmeras identidades para votarem em seu favor, sempre que houver algum mecanismo cooperativista para a tomada de decisões.

Outro método de ataque é a alocação injusta de recursos, que pode acontecer em redes que fazem divisão temporal para acesso ao meio. Neste caso, o

nó malicioso utiliza todas as suas identidades falsas para obter um maior tempo de acesso. Por fim, outra utilização para os nós sybils acontece em redes que utilizam mecanismos de confiabilidade. Em tais redes, a índole do nó é dada pela observação de suas ações. Um nó só é considerado malicioso se cometer diversas ações consideradas ruins ou se cometer uma grande ação ruim.

Assim, duas estratégias podem ser utilizadas. A primeira seria o espalhamento da culpa, na qual o nó sybil utiliza cada uma de suas identidades para fazer pequenas ações ruins, de forma que nenhuma delas possa ser considerada maliciosa. A outra estratégia seria utilizar uma identidade para realizar uma ou mais ações ruins até que ela fosse expulsa, classificada como maliciosa. Quando isso acontecesse o nó geraria uma nova identidade e a usaria para continuar atacando.

3.2.20 Identidade Falsa (*Impersonating*) e Ataque de Replicação

Ambos os ataques são similares ao sybil. Os ataques de identidade falsa e replicação fazem com que os nós maliciosos tenham controle de uma ou mais identidades da rede, mas nestes, porém, as entidades não são falsas, todas as identidades são reais e cada uma delas estará ligada a um ou mais hardwares distintos. A Replicação tem o objetivo de inserir diversos nós maliciosos, sem a menor dificuldade de se pegar inúmeras identidades. Desta forma, os nós maliciosos replicam alguma identidade roubada e utilizam as réplicas simultaneamente dentro da rede (CHAN et al, 2003).

É importante ressaltar que, em geral, estes ataques acontecem após uma violação ou uma quebra de algoritmo criptográfico, assim o atacante passa a ter o segredo da rede, pode participar de todas as atividades como um nó legítimo. Após se tornar um atacante interno, o nó malicioso passa a executar a maioria dos ataques já descritos, com muita facilidade através de suas réplicas.

A detecção de um ataque de replicação é muito fácil, em vista de sua gravidade, pois ele identifica uma mesma identidade em vários pontos da rede. No caso da identidade falsa, se o nó legítimo tiver sido destruído, a detecção é muito mais complicada, pois a identidade é única na rede.

Outra variação da Identidade Falsa é o Ataque do Homem no Meio (*Man-inthe-Middle*) (MURTHY; MANO, 2004), ou seja, o nó atacante intercepta uma comunicação, enganando os nós que deveriam comunicar-se. Essa técnica só pode

ocorrer em redes que não possuem um terceiro ponto para autenticar a comunicação entre os dois primeiros.

3.2.21 Violação

O ataque de violação consiste na violação física dos nós visando obter informações confidenciais, através da inserção de códigos maliciosos ou troca de partes do hardware, alem de também fazer com que o nó fique comprometido. É um dos ataques mais perigosos para redes onde os nós ficam desprotegidos.

De fato, não é simples garantir a segurança de todos os nós quando se refere à de redes de larga escala. Em geral, existem diversas falhas de comunicação, que fazem com que seja inviável identificar uma falha de um nó a qual foi forçado a desligar ou destruído. Uma solução para este ataque seria a resistência a violação.

Uma maneira de aumentar a resistência à violação com base em software é a utilização de associações de segurança temporárias. Um exemplo seria colocar uma senha ou impressão digital em que o sistema operacional somente deixe enviar requisições de rota após informar estes dados para se autenticar na rede. Em caso de perda ou roubo do equipamento, o usuário que não possuir autorização não poderá gerar pedidos de rota. Quando esta tentativa for feita, o sistema operacional do nó pode tomar alguma atitude adicional, como destruir qualquer chave armazenada no sistema, aumento sua resistência à violação (YI et al, 2001). Porém este método é considerado por muitos usuários como inconveniente. A utilização de hardware resistente à violação possui, naturalmente, um problema de custo-benefício. Quanto mais seguro o hardware, mais caro (ANDERSON; KUHN, 1996). Além disso, como na segurança do software, não existe sistema de hardware inviolável.

4 TRABALHOS CORRELATOS

Atualmente existem vários projetos e implementações referentes a segurança em rede sem fio ad hoc, dentre esses projetos pode-se destacar os seguintes:

4.1 PROTEGENDO REDES AD HOC COM CERTIFICADOS DIGITAIS E LIMITE CRIPTOGRÁFICO

Este projeto foi realizado em 2007, na cidade Niterói no Rio de Janeiro, foi feito pelo acadêmico Wagner Gaspar Brazil da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Mestre em Processamento Paralelo e Distribuído.

Propõe uma arquitetura de ICP de alta disponibilidade e robusta de forma a minimizar os ataques do tipo buraco negro e falsificação de identidade contra redes ad hoc. A arquitetura se propõe a trocar um número de mensagens de controle reduzido aumentando assim a sua escalabilidade e desempenho.

Os resultados obtidos mostram uma redução de até 92% no número de mensagens no protocolo de renovação de certificados comparados com alguns métodos existentes.

4.2 SEGURANÇA EM REDES MÓVEIS AD HOC

Este projeto foi desenvolvido em 2006, na cidade de São Paulo, foi feito pelo acadêmico João Carlos Neto do curso de Ciência da Computação da Universidade de São Paulo (USP).

O trabalho apresenta as características das redes ad hoc abordando os alguns mecanismos de segurança neste tipo de rede e formas de ataque.

Os resultados ao final do trabalho mostram o potencial das redes sem fio ad hoc e que, contudo, se faz necessário estabelecer um ponto de equilíbrio entre a flexibilidade e as oportunidades inerentes com as vulnerabilidades apresentadas.

4.3 SEGURANÇA EM REDES AD HOC

Este artigo foi desenvolvido em 2003, na cidade do Rio de Janeiro, foi feito pelo acadêmico Luciano Renovato de Albuquerque do Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia da Universidade Federal do Rio de Janeiro (COPPE).

Esse trabalho realiza uma pesquisa aprofundada em temas que envolvem redes sem fio do tipo Ad Hoc, principalmente relacionado à segurança.

Conclui-se que para avaliar o desempenho de um determinado protocolo em uma rede Ad Hoc um fator muito importante é a mobilidade. A mobilidade e a quantidade de nós presentes na rede são fatores que influenciam a quantidade de rotas que poderão estar disponíveis em um determinado momento. A princípio um dos principais problemas para implementar uma rede utilizando um protocolo seguro como o ARAN seria a inclusão de um ponto central, o servidor de certificados.

4.4 SISTEMAS DETECTORES DE INTRUSÃO EM REDES AD HOC

Este artigo foi desenvolvido em 2003, na cidade do Rio de Janeiro, foi feito pelos acadêmicos Antonio Alexandre Castro Soares e Otto Carlos Muniz Bandeira Duarte da Universidade Federal do Rio de Janeiro (UFRJ).

Apresenta as características, arquiteturas e modelos de detecção atualmente utilizados nos sistemas detectores de intrusão em redes ad hoc.

Conclui-se que a ação coordenada de reação a intrusão, diversos aspectos ainda estão em aberto, assim novos estudos na área apontam para estratégias chamadas de aviso antecipado de intrusão, que basicamente procuram alertar e articular uma ação global antes que uma intrusão possa ser detectada no nó de um serviço.

5 SEGURANÇA EM REDE SEM FIO AD HOC

Alguns dos atributos de segurança que uma rede de comunicação deve possuir são: disponibilidade, confiabilidade, integridade, autenticidade e não repúdio. A disponibilidade implica em uma rede ter sobrevivência mesmo em meio a um ataque de negação de serviço ou então alguma operação lançada sobre as camadas do sistema. Já a confidencialidade garante que certa informação não venha a ser descoberta por indivíduos não autorizados.

A integridade tem o objetivo de assegurar que uma mensagem seja corrompida quando ela passa por uma transferência na rede, ou seja, garante que não haja atividades maliciosas por meio de algum nó (STALLING, 1976), mas isso não inclui falha na interface de radio. A autenticação deve capacitar os nos de confirmar a identidade de seus pares de comunicação, evitando tentativas de mascaramento e personificação por nos mal intencionados. O não repúdio confere ao sistema a capacidade de sempre identificar a origem de uma mensagem, o que e muito útil quando da necessidade de detectar nos comprometidos.

O sistema de segurança tem como objetivo garantir que a funcionalidade da rede e suas características não sejam afetadas em função de situações que possam acontecer e ocasionar restrições as suas características, sua dinâmica de comportamento da rede e também comprometer o seu desempenho. Pode-se assim afirmar que criar e implementar arquiteturas para estas redes ad hoc suprindo estas necessidades de segurança é uma tarefa muito custosa.

5.1 ARQUITETURAS PARA SEGURANÇA EM REDES SEM FIO AD HOC

Uma das proteções básicas dos mecanismos de operação é a troca de mensagens dos usuários da rede. Desse modo é adotado esquemas de criptografia onde são adaptados a este tipo de ambiente. Assim pode-se observar um ponto que tem muita vulnerabilidade em relação ao sistema de segurança que é o gerenciamento de chaves criptografadas.

Para uma maior segurança e eficácia no sistema de segurança seriam usadas chaves assimétricas, o que será abordado ao longo do trabalho, para fazer a autenticação e estabelecer de forma segura a comunicação entre os nós da rede. Devem-se considerar algumas características para este esquema como, por

exemplo: as propriedades de autoridade da rede, o acesso que um nó tem na rede, a relação em que os nós tem entre si é em comparação dos nós com a rede ao todo e também a confiabilidade distribuída na rede. Um dos problemas que estão presentes quanto à inicialização do sistema seriam a redundância quanto à topologia e a confiabilidade da rede.

Com relação a estes problemas são impostos esquemas de criptografia com infraestrutura de chaves públicas, como por exemplo, assinaturas digitais, assim cada nó teriam duas chaves, uma pública e uma privada, e também uma entidade confiável entre cada no da rede e as suas respectivas chaves públicas. Desse modo a chave pública dos nós fica disponível na rede e cada nó possui para si, confidenciando, sua chave privada. Pode ser feito pedido de chaves públicas na rede pelos nós para renovações das mesmas para o certificado distribuído.

5.1.1 Proteção Física

Faz-se uma das medidas de segurança dos dispositivos móveis. Não deve ser considerada uma medida simples devido ao fato de haver alguns cenários onde ocorre a possibilidade de furto do dispositivo. Uma tecnologia que pode ser uma solução nestes casos é o Smart Cards (HUBAUX et al, 2001), já que utiliza o dispositivo móvel apenas como interface carregando os dados vitais em si. A implementação de um hardware tamper resistent não é uma solução definitiva ainda devido à limitação dos smart cards e a possibilidade da obtenção de suas informações, por meios óbvios e outros bem menos convencionais (ex.: hardware específico). Para obter uma maior segurança quanto o meio físico do equipamento podem ser utilizados programas de rastreamento, como por exemplo ztrace e computrace, que possibilitam que a maquina quando se comunique com a internet automaticamente envie a localização do equipamento para uma central, podendo assim ser encontrado. E também pode ser feito um seguro da maquina, similar aos seguros para carros.

5.1.2 Proteção do Enlace

Devido ao fato de toda a comunicação ser realizada pelo ar, deve ser implantada uma estratégia para que a transação de dados evite que técnicas

maliciosas sejam realizadas facilmente por algum hardware ou outro aparelho. Uma solução possível e o espalhamento do espectro por salto em frequências, *Frequency Hopping Spread Spectrum* (FHSS). Segundo Garcia (2002) a técnica de FHSS codifica dados e modula os sinais de modos diferentes para equilibrar velocidade, distância e capacidade de transmissão, ou seja, a frequência será divida em sub-canais e realizara vários saltos de uma frequência para outra aleatoriamente varias vezes por segundo transmitindo os dados por tais sub-canais.

5.1.3 Wired Equivalent Privacy (WEP)

É uma chave que compartilha uma senha utilizada para criptografar e descriptografar o tráfego de dados sem fios, onde somente podem ser lidas pelos outros dispositivos que possuam a mesma chave.

A chave WEP é armazenada em cada computador da rede, de modo que os dados possam ser criptografados e descriptografados à medida que são transmitidos por ondas de rádio na rede sem fios.

A criptografia pode ser realizada de dois modos: 64 bits que compreendem 5 caracteres alfabéticos ou 10 números hexadecimais, ou 128 bits que compreendem 13 caracteres alfabéticos ou de 26 números hexadecimais.

Mas no algoritmo deste protocolo foram encontradas algumas vulnerabilidades desse modo passando a não ser muito confiável em questão de segurança. A mais significativa está relacionada a determinados valores que permitem a quebra da chave secreta, mesmo assim este protocolo ainda é utilizado, oferecendo apenas um nível básico de proteção (GRÜNEWALD, 2005).

5.1.4 Wi-Fi Protected Access (WPA)

Esse método disponibiliza um nível maior de proteção de dados e no controle ao acesso da rede local sem fios. O WPA utiliza uma chave mestra compartilhada, assim tendo uma criptografia mais robusta. Essa chave pode ser uma chave dinâmica atribuída por um servidor de autenticação para oferecer controle de acesso e gestão centralizados (MORENO, 2005).

Num ambiente doméstico ou de empresas pequenas, o WPA é executado de um modo doméstico especial chamado *Pre-Shared Key* (Chave pré-

compartilhada) (PSK) que utiliza chaves ou senhas inseridas manualmente pelo utilizador para fornecer a segurança.

Embora tanto as chaves WEP de 64, quanto às de 128 *bits* sejam vulneráveis, é sempre recomendável usar chaves de 128 bits, que são um pouco mais difíceis de quebrar.

5.1.5 Wi-Fi Protected Access 2 (WPA2)

É baseado no padrão IEEE 802.11i e utiliza como mecanismo de criptografia chamado protocolo *Advanced Encryption Standard* (AES). Suporta as características adicionais de segurança do padrão 802.11i que não estão incluídas nos produtos que suportam WPA. Assim como o WPA, o WPA2 provê autenticação e criptografia, propondo a garantia de confidencialidade, autenticidade e integridade em redes sem-fio. A principal vantagem do WPA2 é a compatibilidade com o WPA, que permite a utilização, além do AES, do TKIP e EAP (SOUZA, 2005).

5.1.6 Criptografia

A criptografia pode ser entendida com um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível e vice-versa (SIMON, 1999). Sendo assim a criptografia é uma técnica onde a informação é transformada passando da sua forma original para uma forma ilegível, desse modo apenas o destinatário vai conhecê-la, dificultando que a mesma seja lida por um individuo não autorizado.

No campo computacional, a criptografia surgiu devido a necessidade de transmitir informações sensíveis por meios de comunicação não confiáveis (MAIA, 2005). A criptografia tem como objetivo garantir que haja segurança no sigilo de informações que são trafegadas em um ambiente computacional. Ela passa a ser usada para criptografar os dados antes que os mesmos sejam enviados aos destinatários, assim, se houver a interceptação destes dados, dificilmente eles serão compreendidos.

A criptografia computacional é usada para garantir:

1. Sigilo: somente os usuários autorizados têm acesso às informações.

2. Integridade da informação: garante ao usuário que a informação está correta, que a mesma não foi alterada acidentalmente ou intencionalmente.
3. Autenticação do usuário: é o processo que permite ao sistema verificar a identidade do usuário ou dispositivo com quem está se comunicando (MAIA, 2005).

Figura 3 – Criptografia de chaves

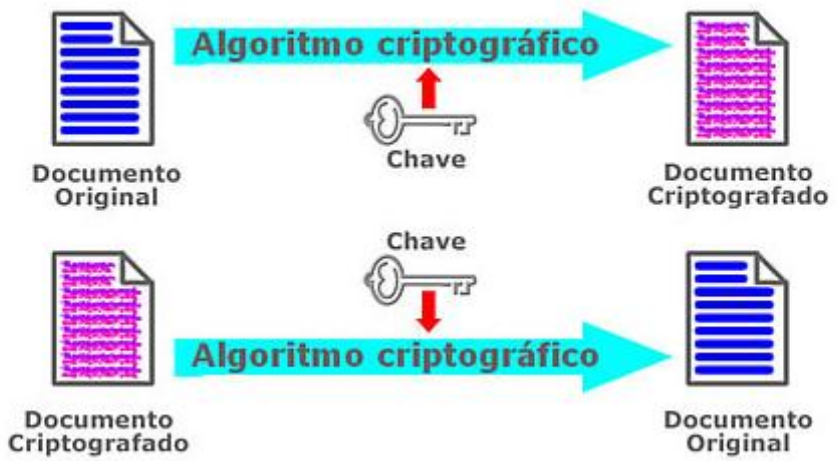
Fonte: Piropo (2007).

A criptografia é uma ferramenta fundamental para prover segurança, pois por meio dela, é possível atender a todos os requisitos clássicos (NATALIA; et al, 2006). A maioria dos ataques a redes poderia ser solucionada pela utilização de um mecanismo criptográfico seguro. Ela se divide em dois segmentos: simétrica e assimétrica.

5.1.6.1 Criptografia Simétrica

A criptografia simétrica é caracterizada pela existência de uma chave privada, da qual é compartilhada entre todos os nós que necessitam fazer uma conexão. Esta chave será utilizada para enviar um texto criptografado ao invés de um texto normal em aberto. As principais operações realizadas pelos algoritmos simétricos são o ou-exclusivo, a troca de colunas, a troca de linhas, a permutação, a rotação e a expansão, que são operações de baixo custo computacional. As combinações dessas operações devem ser capazes de tornar difícil a descoberta da mensagem para quem não possui a chave privada.

Figura 4 – Criptografia Simétrica



Fonte: Piropo (2007).

Com base nisto, a eficiência desses algoritmos é calculada por meio do seu custo computacional e pela sua capacidade de modificar a saída através de uma pequena mudança na entrada. Chave simétrica possui a vantagem de não exigir muito poder de computação. Isso ocorre porque os algoritmos simétricos trabalham com deslocamentos e permutas sobre blocos de dados que serão cifrados usando chaves de 56 a 256 bits (EHRSAM et al, 1975) . Por esse motivo, os algoritmos assimétricos também são conhecidos como algoritmos de blocos.

5.1.6.2 Criptografia Assimétrica

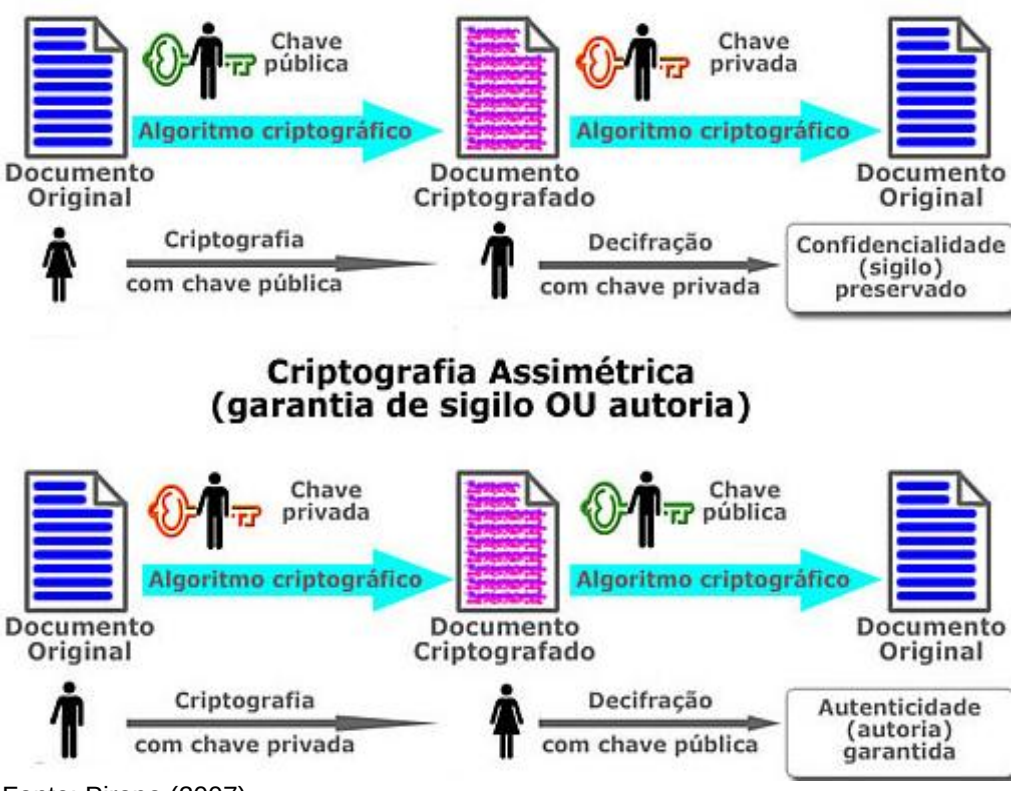
Este modelo criptográfico possui duas chaves: chave pública e chave privada. A chave pública é distribuída entre os membros da rede, e a privada é mantida em segredo pelo nó. A criptografia assimétrica possui um maior custo computacional em relação a simétrica, devido ao fato de utilizar operações como a exponenciação. O principal objetivo é fazer com que, por meio de uma das chaves, não seja possível encontrar a outra. As duas chaves podem ser usadas de modo que:

- O individuo que possui a chave pública de outro usuário pode enviar mensagens cifradas para o proprietário da chave privada que pertence a respectiva chave pública. A mensagem será decifrada pela chave privada. Essa chave privada não pode ser reconstruída por meio da

chave pública e a chave publica também não pode ser reconstruída através da chave privada.

- O proprietário da chave privada pode cifrar uma mensagem com esta chave e o individuo que receber a mensagem poderá ter a certeza da autenticidade do emissor já que somente irá poder ler a mensagem utilizando a própria chave pública.

Figura 5 – Criptografia Assimétrica



Fonte: Piropo (2007).

A chave privada não deve ser compartilhada e o risco dela ser descoberta é menor que em comparação com a criptografia simétrica. O usuário somente necessita guardar a chave privada em segurança e possuir as chaves públicas dos usuários com os quais trocará informações. As chaves públicas devem ser protegidas contra a ameaça de troca com um atacante da rede que desse modo poderia se passar pelo proprietário da chave. Assim, os algoritmos assimétricos resolvem o problema de distribuição de chave que os algoritmos simétricos têm, mas por outro lado possuem o problema de proteger as chaves públicas.

Técnicas de distribuição de chaves de forma segura e a assinatura de mensagens podem ser feitas através da criptografia assimétrica.

É comum fazer uso, em redes cabeadas, de características dos dois tipos de criptografia para garantir segurança na comunicação, denominado de criptografia híbrida. Neste método, é trocado um segredo entre os nós da rede através de chaves públicas, do qual este segredo servirá como uma chave privada para criptografar a comunicação posterior usando criptografia simétrica, ou seja, de menor custo computacional. Primeiro ambos os nós trocam suas chaves públicas, a seguir, o nó X gera uma chave privada, depois a criptografa com chave pública de Y e a envia. O nó Y decifra a mensagem com sua chave privada e gera uma mensagem contendo a chave privada, criptografada com a chave pública de X, para confirmar que obteve sucesso em revelar o segredo. É importante ressaltar que este método não é suficiente para garantir a autenticação e confiabilidade das mensagens, já que um nó malicioso poderia realizar o Ataque do Homem do Meio, do qual forjaria a comunicação para os dois nós.

Tabela 2 – Criptografia Simétrica e Assimétrica

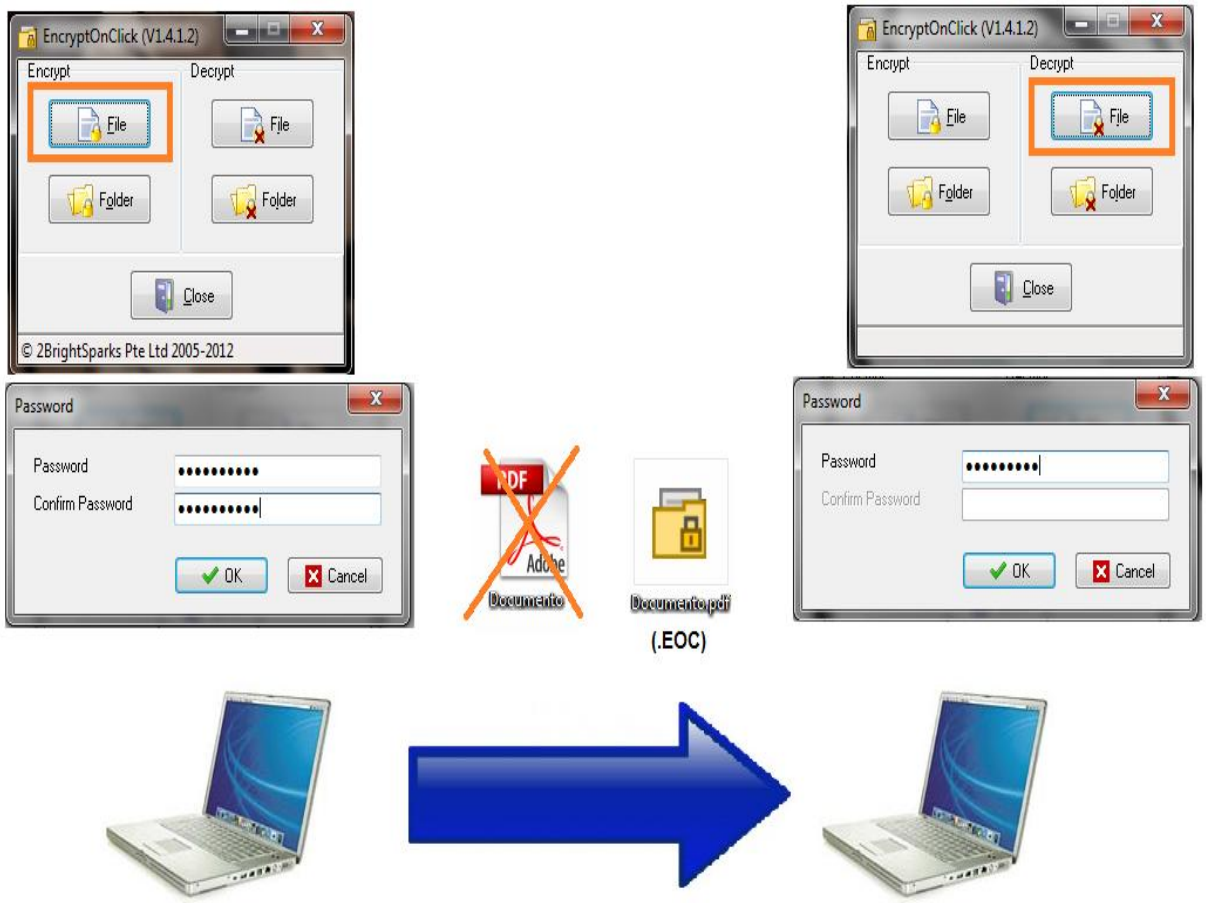
Simetrica	Assimetrica
Rapida	Lenta
Gerência e distribuição das chaves é complexa	Gerência e distribuição das chaves é complexa
Não oferece assinatura digital	Oferece assinatura digital

Fonte: Do Autor.

Foi realizado um teste com o software EncryptOnClick para verificar como passa a ser a transmissão e mensagens na rede com criptografia. O EncryptOnClick um programa gratuito que possui encriptação de 256 bits. Primeiramente precisa-se ter o programa instalado nos computadores em que se deseja fazer troca de mensagens, pois sem ele o Windows não reconhece o arquivo. Ele funciona da seguinte forma: possui quatro botões, os dois primeiros é para criptografar o documento e os outros dois são para descriptar o documento. Pode-se escolher colocar senhas em um arquivo, na opção file, ou em uma pasta, na opção folder.

Quando um arquivo ele é criptografado ele passa a ficar com seu nome original seguido de ponto(.) e mais a extensão em que era antes de ser criptografado (txt, pdf, doc, etc.), e muda a sua extensão para .EOC, que é a extensão do programa. As imagens do programa podem ser observadas na Figura 6.

Figura 6 – Criptografia de arquivo com EncryptOnClick



Fonte: Do Autor.

5.1.7 Assinatura Digital

É a versão digital da assinatura de mão que é autenticada em cartório. A autenticação ou assinatura digital garante o não repudio para envio e recebimento de mensagens ou arquivos. Ela é gerada utilizando chave privada de um usuário, do qual somente ele vai conhecer e ter acesso. A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia assimétrica que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados (PINHEIRO, 2008). Assim quando um usuário assinar uma mensagem, não terá como negar que o fez porque somente ele possuirá sua chave privada, sendo que é muito importante que esta chave seja guardada em segurança e sua chave pública correspondente esteja em uma entidade confiável.

Segundo Pinheiro (2008), uma assinatura digital não é reutilizável, ou seja, não pode ser transferida para outro documento. Ela pode ser implementada em três modos: Função *Hash* por através de padrões MD5 e *Secure Hash Algorithm* (SHA)*, Digital Signature Standard*(DSS) e utilizando o conceito de chaves públicas (PINHEIRO, 2008).

Uma técnica muito utilizada que une criptografia simétrica e assimétrica é o envelopamento digital, onde são realizadas as seguintes etapas:

- Um emissor vai cifrar uma mensagem com a uma chave simétrica q ele irá gerar e enviar juntamente com a mensagem;
- O emissor cifra um hash da mensagem cifrada com sua chave privada;
- É cifrada, pelo emissor, a chave simétrica com a chave pública, onde ambas são enviadas para o receptor.
- A mensagem é recebida pelo receptor, que a decifra a chave simétrica com a sua chave privada e o hash com a chave publica de quem a enviou, obtendo dessa forma, a chave simétrica e a garantia de que o emissor foi quem enviou a mensagem;
- É calculado o hash, pelo receptor, verificando a integridade da mensagem;
- Com isso, o hash anexado na mensagem ser igual o hash gerado, a mensagem é decifrada com a chave simétrica. Essa técnica garante a troca de chaves simétricas, a autenticação, integridade, confidencialidade e não repudio da mensagem envolvida na comunicação (CALLAS et al, 1998).

A assinatura digital deve possuir algumas propriedades como:

- Verificação do autor, data e hora da assinatura;
- Autenticação do conteúdo original;
- Deve ser capaz de poder ser verificada por terceiros.

Pode ser divida também em dois tipos: direta e arbitrária. A assinatura digital direta que engloba apenas os indivíduos comunicantes, origem e destino. A

assinatura arbitrária possui um arbitro entre a origem e o destino que verifica a mensagem antes de ser enviada para o destino.

5.1.8 Certificado Digital

Auxiliam na autenticação de usuários em redes de comunicações, são equivalentes a cédulas de identificação como RG, CPF e passaporte, é um arquivo binário, que pode ser armazenado em um dispositivo de segurança como *smart cards* e *tokens*. Os certificados digitais são assinados por uma Autoridade Certificadora (AC) que lhe provê a garantia de autenticidade.

Os certificados digitais garantem a identificação de uma instituição, pessoa física ou um endereço da internet, ele é um arquivo em media com 1Kb onde possui uma chave criptográfica e dados do proprietário. O programa Infraestrutura de Chaves Públicas (ICP) siglas derivadas da Public Key Infrastructure (PKI) em inglês, o ICP–Brasil é uma série de medidas legais, técnicas e normas que possibilitaram o surgimento de versões virtuais de CPFs e CNPJs., ele grava os dados: nome, CPF, RG, etc, Algumas certificadoras mais conhecidas são a Verisign, a Thawte e a brasileira Certisign.

Os certificados digitais possuem chaves eletrônicas vinculadas para poder utilizar de criptografia e assinar informações digitais. Assim, possibilita fazer verificação para descobrir se o usuário tem ou não autorização de utilizar determinada chave, prevenindo o uso de chaves falsas na identificação de pessoas. Através da criptografia dos certificados digitais impedem que a assinatura eletrônica seja falsificada, alterada e ate mesmo copiada, tornando-o inviolável. Eles possuem três princípios de segurança na comunicação: autenticação, privacidade e inviolabilidade. O certificado digital possui as informações da chave pública junto com o nome do proprietário, numero de série, nome da AC emissora e a assinatura da certificadora juntamente com a sua chave privada.

5.1.8.1 Certificados Digitais em Aplicativos

Pode-se utilizar de certificados digitais em alguns aplicativos como o Windows Live Mail, Google Chrome, Firefox e Internet Explorer.

Para gerenciar certificados no Windows Live Mail se deve acessar *ferramentas*, em *opções de proteção*, em seguida na guia *segurança*, após em *identidades digitais*. Realizados os passos, acrescentam-se certificados em *importar/exportar*, em *avançado* para marcar as finalidades do certificado, então escolha o botão *Importar* e/ou *Exportar*.

No Google Chrome primeiro em acessa-se *ferramentas*, representado pela Chave Inglesa no canto superior direito. Em seguida *configurações avançadas* e em *HTTPS/SSL,* logo *gerenciar certificados*.

No Firefox acessa-se em *ferramentas* e em *opções*, na guia *avançado*, logo no sub-menu *criptografia*, marque as caixas *SSL 3.0* e *TLS 1.0*. Em seguida *certificados*. se não houver nenhum disponível, selecione *importar* e procure aonde estão seus certificados gerados (Disco C) para importá-los. Existem também outras opções de gerenciamento de certificados, como backup, adicionar certificados em pessoas, servidores, autoridades, entre outros.

Para o Internet Explorer através de *ferramentas*, *opções da internet*, logo em *conteúdo* e clique no botão *certificados* e importe/exporte os certificados. Em *editores*, mesmas opções de *importar/exportar* certificados. Executando essas ações automaticamente serão sincronizadas entre si.

5.1.9 Senhas Seguras

O uso de senhas fracas, ou seja, senhas que sejam fáceis de imaginar e descobrir são um dos maiores problemas na utilização deste tipo de autenticação representando cerca de 80% dos problemas de segurança (SÊMOLA, 2006). As senhas fortes possibilitam que a segurança em uma rede possa ser mais robusta.

Muitos casos de intrusão ocorrem pelo uso de senhas mal elaboradas, e não por uma falha do sistema. Para criar uma senha segura deve-se levar em consideração alguns fatores como quantidade de caracteres (deve conter no mínimo 8) e não elaborar senhas com dados pessoais ou de familiares (nomes, datas, entre outros). O ideal é utilizar senhas aleatórias, que incluam letras minúsculas, maiúsculas, números e símbolos (CARMONA, 2005).

De acordo com (ALBERTO, 2006) senhas seguras são obtidas através de:

- Não utilizar dados pessoais como seu nome ou de parentes, datas de nascimento de integrantes da família, mesmo que haja combinações entre as informações ou pequenas alterações na escrita;
- Dados que possam ser desvendados facilmente incluindo endereços, placa do carro, números de documentos também são alvos fáceis;
- Nunca anote senhas em papéis, agendas ou algum lugar que outras pessoas possam ter acesso, o melhor lugar para armazenar senhas sem nenhum risco é na sua memória;
- Senhas criadas a partir de palavras existentes em dicionários, tanto nacionais quanto estrangeiros podem ser desvendadas com ataques de dicionário;
- Não utilizar senhas com apenas um tipo de caractere, chaves fortes devem conter letras maiúsculas e minúsculas, caracteres especiais e números;
- Uma senha deve combinar no mínimo 8 caracteres;
- Nunca utilizar sequências de dígitos do teclado, como, “qwe123” ou “qwerty”, nem seqüência de números “123456”;
- Não utilize a mesma senha em lugares diferentes, pois se a senha for desvendada apenas um local será atacado;
- A troca das senhas deve acontecer regularmente, no período de aproximadamente 3 meses;
- Muito cuidado ao digitar uma senha em público, já que muitos invasores usam esse método para coletar senhas.

Alguns métodos podem ser utilizados para criação de senhas mais fortes, como por exemplos existem sites na internet que elaboram ou analisam a senha para saber se a mesma é segura ou não. Para criar senhas pode-se citar os sites Password.Es http://password.es/ (site em espanhol) e o Strong Password Generator http://strongpasswordgenerator.com/ (site em inglês) ambos são gratuitos.

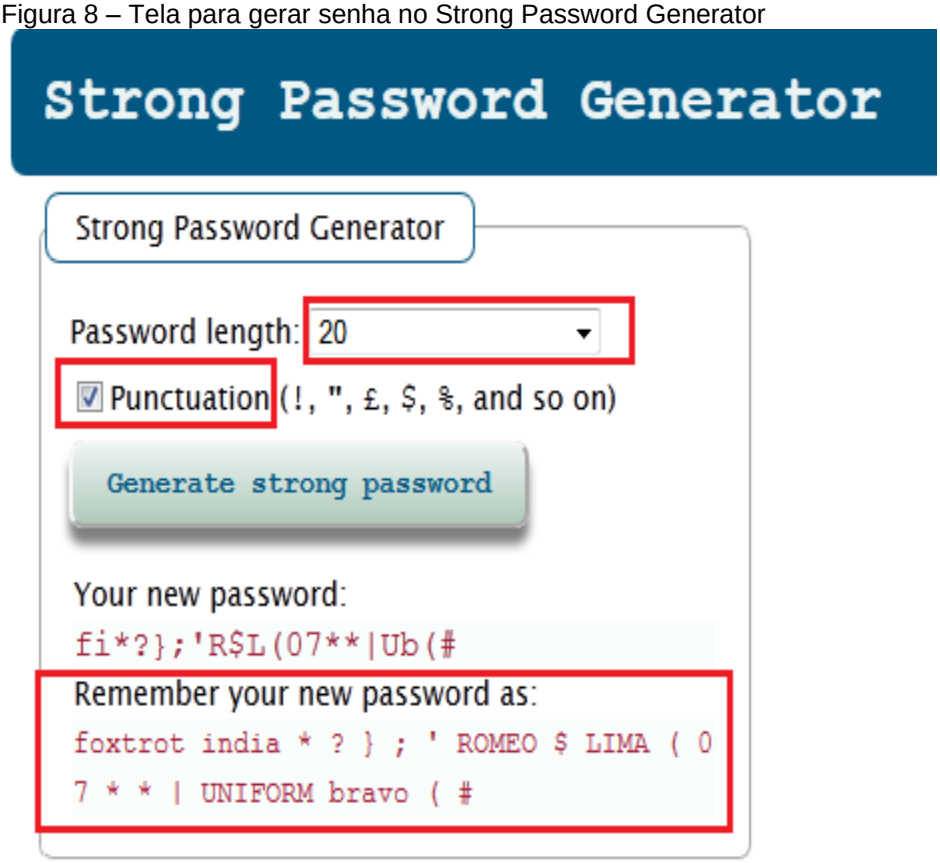
No Password.Es possui as opções de número de caracteres da senha, possuir letras minúsculas e maiúsculas, números e símbolos, analisando o nível da senha após a mesma ser gerada, como mostra a Figura 7 :

Figura 7 – Tela para criar senhas com Password.Es

Fonte: Password.Es, (2012).

O Strong Password Generator é similar ao Password.Es porém ao gerar a senha automaticamente é gerada uma frase para auxiliar a recordar a mesma, mas a opção de escolha de caracteres é limita em apenas incluir ou não símbolos e no tamanho de dígitos, pois as letras maiúsculas, minúsculas e números já estão incluídos no gerador de senhas. Podemos observar a tela do Strong Password Generator na Figura 8:

Figura 8 – Tela para gerar senha no Strong Password Generator



Fonte: Strong Password Generator, (2012).

Um site para verificação de senhas é o Password Meter, que pode ser acessado por http://www.passwordmeter.com/ (site em inglês) que analisa a senha digitada com os requisitos de segurança em relação ao tamanho, uso de letras maiúsculas/minúsculas, números, símbolos, repetição de caracteres e sequência de números do teclado.

O Password Meter é gratuito e de fácil uso, somente necessita digitar a senha que o programa a analisa instantaneamente mostrando os resultados da análise apontando para falhas quanto à elaboração desta senha. Não cria senhas infalíveis, pois não existe uma senha que seja completamente segura, mas proporciona senhas mais fortes contribuindo para ter maior segurança contra indivíduos maliciosos.

Realizado uma análise com a senha *computacao2012,* o resultado não foi de uma senha forte possuindo apenas 58% de segurança e os motivos foram apontados pelo programa como:

- Ausência de letras maiúsculas;
- Ausência de símbolos;

- Atendia apenas 2/4 dos requisitos básicos de segurança que o programa indica como necessários para uma senha segura. O programa pede para possuir no mínimo 3/4 dos requisitos que são: letras maiúsculas, letras minúsculas, números e símbolos. A senha possui apenas letras minúsculas e números.
- Caracteres repetidos (c, o, a, 2);
- Letras minúsculas consecutivas (computação);
- Números consecutivos (2012);
- Números em ordem sequencial (12).

A tela de análise pelo Password Meter está representada na Figura 10.

Figura 9 – Tela de primeira análise de senha Password Meter.

Test Your Password		Minimum Requirements
Password:	computacao2012	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	58%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	14	+ 56
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	10	+ 8
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	8	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	9	- 18
Consecutive Numbers	Flat	-(n*2)	3	- 6
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Fonte: Password Meter, (2012).

Outra pesquisa foi realizada com uma senha atendendo a todos os requisitos especificados como faltantes na análise anterior, utilizando tamanho de dígitos superior 8, letras maiúsculas, letras minúsculas, símbolos, números, sem repetição e sequência de caracteres, onde o resultado obtido foi de uma senha segura. O resultado pode ser observado na Figura 10.

Figura 10- Tela de segunda análise de senha no Password Meter.

Test Your Password		Minimum Requirements
Password:	@nG&^L1cA	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✱	Number of Characters	Flat	+(n*4)	9	+ 36
✱	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 12
✱	Lowercase Letters	Cond/Incr	+((len-n)*2)	2	+ 14
✓	Numbers	Cond	+(n*4)	1	+ 4
✱	Symbols	Flat	+(n*6)	3	+ 18
✱	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
✱	Requirements	Flat	+(n*2)	5	+ 10
Deductions					
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Fonte: Password Meter, (2012).

Para criar senhas seguras também podem ser realizadas com base em métodos existentes como a criação de senhas por formas geométricas do teclado. Segundo Oliveira (2004), trata-se de olhar para o teclado, imaginar uma figura geométrica e 'ligar os pontos', apertando os botões correspondentes à figura (que pode ser um quadrado, uma seta, um 'L' enorme, um triângulo, um zigue-zague, ou qualquer outra coisa).

Mas é muito importante cuidar para que nenhuma pessoa saiba que sua senha é com base nesta técnica, pois ela pode descobrir facilmente através de

varias tentativas, por isso é fundamental o cuidado na hora da digitação se não possui alguém prestando atenção ao que é digitado no teclado.

Outro método seria as senhas pronunciáveis, ou seja, palavras escritas com a junção de uma ou mais vogais com consoantes, ou com a troca de algumas vogais e consoantes por números e símbolos como, por exemplo, *caianocla* ou *qu3r0mu1tof3r1@$.* Pode-se criar varias palavras de acordo com a criatividade utilizada. É imprescindível que, para retardar ao máximo os ataques por 'força bruta', ela seja grande (OLIVEIRA, 2004), assim, que sejam criadas palavras que não existem para que não possam ser descobertas com um ataque de dicionário.

Muitos usuários utilizam a técnica de criar senhas por meio de frases ou textos, para poderem se lembrar de forma rápida e fácil, seja uma música, poesia, passagem bíblica entre outros. Um exemplo de criação por meio de uma música *Olha que coisa mais linda, Mais cheia de graça, É ela menina, Que vem e que passa*, onde neste caso seria a senha *oqcmlmcdgeemqveqp* ou para ser ainda mais forte em relação à quebra podia acrescentar as vírgulas *oqcml,mcdg,eem,qveqp.* Alem da facilidade em recordar a senha, outra vantagem deste método seria a possibilidade de criar senhas extensas sem ter problemas de esquecê-la.

Uma técnica similar a de frases seria a de palavras em conjunto, que é a elaboração se senhas a partir da junção de palavras, como por exemplo, *abacate+gato+boneca* obtendo assim *abagabon.*

Outras opções de senhas também seriam a criação através de caracteres utilizando *alt*+tecla como, por exemplo, *alt*+r = ® ou *alt*+c = ©, vantagem de criar senhas com caracteres alt é que muitos softwares utilizados em quebra de senhas não faz uso desses caracteres somente letras números e símbolos do teclado. E ainda outra opção é criar senhas por chave significativas, ou seja, podem ser datas, nomes, lugares, enfim, dados que apenas o usuário saiba, como placa do primeiro carro, nome do primeiro livro, música que gostava na infância e outros, podem unir nomes com palavras e/ou números contendo um número razoável de dígitos como, por exemplo, *1994omagicodeozlivro1*.

5.1.10 Protocolos Seguros

O roteamento seguro em redes ad hoc possui algumas dificuldades, devido sua topologia dinâmica, à necessidade de funcionar de forma eficaz com

recursos limitados, a largura da banda de rede, a capacidade de processamento da CPU, memória e bateria dos computadores integrantes da rede. Os protocolos de roteamento sem segurança são aperfeiçoados para propagar novas informações rapidamente, exigindo interações do protocolo de roteamento mais rápidas e frequentes do que as exigidas em uma rede tradicional (YIH-CHUN et al, 2002).

Uma rede ad hoc tem muita vulnerabilidade a certos tipos de ataques maliciosos devido a sua topologia dinâmica e a falta de infraestrutura. Essas redes não possuem garantia de que o caminho escolhido para realizar a comunicação com determinado nó, está seguro contra ataques mal intencionados. Muitos protocolos são propostos focados na idéia de encontrar o menor caminho entre dois nós o mais rápido possível, entretanto existem aplicações que requerem mais do que a certeza da determinação da menor rota (YI et al, 2001). Com base nisto, são propostos protocolos de roteamento seguro.

Pode-se realizar um roteamento seguro dos nós de uma rede de duas maneiras: através de protocolos de roteamento orientados a topologia e protocolos de roteamento orientados a posicionamento.

5.1.10.1 Protocolos de Roteamento com Base em Topologia

Neste tópico será abordado o funcionamento de alguns protocolos de roteamento em redes ad hoc orientados a topologia, apresentando suas vantagens e desvantagens.

5.1.10.1.1 Aran

O ARAN é um protocolo reativo originado a partir do AODV que implementa criptografia assimétrica por meio de certificados digitais (PERKINS; ROYER, 1999). Cada nó da rede preliminarmente efetua uma autenticação salto a salto das mensagens de roteamento, através de uma banda não utilizada pela rede, para garantir maior integridade e autenticidade na troca de mensagens entre os nós e também prevenir ataques de fabricação de roteamento. Porém tem como desvantagem a necessidade de uma AC, servidor central, para realizar a certificação. Como possui certificação digital, cada pacote que é encaminhado por nó tem que ser assinado pelo mesmo, ocasionando assim um procedimento que

consome maior tempo e recurso computacional e, além disso, provoca um aumento progressivo no tamanho do pacote a cada salto. Este protocolo tenta resolver algumas falhas de segurança apresentadas pelos protocolos AODV e DSR (SANZGIRI et al, 2002).

Quando um nó for construir a rota, ele envia um *Route Discovery Packet* (RDP), pacote de descoberta com o certificado digital do nó para realizar a descoberta do caminho. O pacote de descoberta contém uma identificação RDP, o endereço do nó que deseja acessar (destino), certificado do nó remetente e uma chave de sessão que tem a finalidade de prevenir contra ataques do tipo *replay*. O destino quando receber o RDP envia um *Reply Packet* (REP), pacote resposta, para o nó de origem. O pacote REP possui a identificação, endereço do nó de origem, certificado digital do nó de destino e a chave de sessão do nó de origem. O REP chegando ao nó de destino, o nó valida o caminho percorrido através da avaliação da assinatura e da chave de sessão enviada pelo mesmo. Se uma rota for desativada o nó recebera uma mensagem de erro para o nó de origem e os demais da rota para q haja a atualização das tabelas de roteamento.

Segundo Sanzgiri et al (2005) aponta para um desempenho do ARAN tão efetivo quanto o AODV na descoberta e manutenção de rotas, mas possui um aumento no *overhead* de pacotes e na latência da descoberta de rota.

5.1.10.1.2 Ariadne

É um protocolo de roteamento baseado no protocolo DSR. O Ariadne baseia-se em mecanismos de autenticação como o *Timed Eficient Stream Loss-Tolerant Authentication* (TESLA) (JOHNSON et al, 2001). Este protocolo usa de criptografia simétrica, na construção e manutenção de rotas, provendo de uma maior integridade e autenticação no envio de mensagens. Segundo Johnson et al (2001), ele pode ser implementado como: distribuição de par de chaves entre todos os nós, cadeias *hash* para autenticação dos nós e assinaturas digitais.

Possui alguns pré-requisitos para a sua utilização, um deles é a necessidade de realizar uma sincronização de tempo entre os nós da rede, para estipular o tempo de transmissão ponto-a-ponto de um nó para os demais da rede. Outro pré-requisito é que se estabeleçam chaves secretas para a comunicação dos nós e uma forma de realizar a distribuição do TESLA, chave pública, para cada nó.

O TESLA tem sua autenticação com referentes a adição de MACs nas mensagens dos nós para autenticar o *broadcast.* O cálculo dos MACs é realizado com base em chaves assimétricas já que necessita verificar a autenticidade das mensagens dos nós da rede ponto-a-ponto. Para ser mais eficiente o TESLA alcança a assimetria necessária nas chaves através da geração de cadeias *hash* (RIVEST et al, 1978), com necessidade de sincronismo entre os relógios dos dispositivos, devido ao fato de se estabelecer um cronograma que será distribuído a todos os nós da rede para a publicação de chaves.

O modelo de cadeias hash se destaca pela simplicidade em utilizar uma variação de infraestrutura de chaves públicas do protocolo TESLA para autenticar os nós (HU et al, 2003). Desse modo, a chave pública vai ser responsável por sincronizar os relógios para revelar as chaves, assim, se um nó receber uma chave em um período de tempo inferior ao previsto, supõe se que a este chave foi divulgada e a rede pode estar sendo atacada por um ataque de fabricação de roteamento.

O Ariadne com cadeias *hash* funciona da seguinte maneira: se um nó não encontrar um determinado caminho é enviado uma *Route Request* (RREQ), ou seja, uma mensagem de solicitação de rota para o destino desejado. Por cada nó que esta REQ percorrer vai sendo autenticado este mesmo nó na tabela de roteamento e na lista de caminho percorrido. O nó de destino armazena a *Route Reply* (REQ), mensagem de resposta, até que todos os nós intermediários revelem suas chaves e o nó possa validar que nenhuma chave foi publicada anteriormente, adicionando na mensagem o código MAC. Se um nó não obtém sucesso na entrega de pacotes após determinadas tentativas de retransmissões, é transmitida ao nó de origem, uma mensagem de erro *Route Error* (ERR) autenticada (HU et al, 2003).

Este protocolo previne contra ataques de fabricação de roteamento e *sinkhole* e em relação ao desempenho ocorre um grande envio de mensagens de sinalização e atrasos na verificação de chaves, ocasionando um aumento de processamento além de retardo na descoberta de rotas ponto-a-ponto resultando em uma diminuição na taxa de entrega de pacotes.

5.1.10.1.3 Secure Efficient Distance Vector Routing for Ad Hoc (SEAD)

É um protocolo pró-ativo que, de acordo com Hu et al (2003), apresenta um mecanismo de roteamento seguro inspirado no DSDV, baseado em cadeias hash ao invés de criptografia assimétrica e na abordagem por vetores de distância. O SEAD é indicado para ambientes onde há restrições de recursos. O seu objetivo é dar proteção a rede contra ataques múltiplos que realizam informações de roteamento falsas, ou seja, o SEAD autentica as mensagens de atualizações roteamento do DSDV. Os nós da rede ao transmitirem sua mensagem de atualização, selecionam um elemento da cadeia *hash* gerada e autentica a métrica e o número sequencial de cada entrada na sua tabela de rotas (GUERRERO; ASOKAN, 2002).

É priorizado pelo nó rotas com métricas de valores menores para impedir que algum nó mal intencionado forge métricas de valores maiores ou iguais a eu foi autenticada, ou seja, os próximos nós terão sempre uma métrica maior que a recebida. Em caso de um nó receber uma mensagem de atualização, ele somente irá validá-la após realizar uma verificação da métrica e do número sequencial do valor hash e caso exista algo incorreto a mensagem será descartada.

O SEAD gera mais overhead de pacotes, porém ainda possui taxas de entrega de pacotes muito melhores que o DSDV. Uma vantagem é que permite a criação de tabelas de roteamento em menor tempo contribuindo para mais desempenho em ambientes com muita mobilidade.

5.1.10.2 Protocolos Orientados em Posicionamento

Neste tópico será abordado o funcionamento de alguns protocolos de roteamento em redes ad hoc orientados ao posicionamento geográfico, apresentando suas vantagens e desvantagens.

5.1.10.2.1 Ad Hoc On-Demand Position-Based Private Routing Protocol (AO2P)

O anonimato do usuário é um fator importante de segurança para proteger a privacidade pessoal em redes móveis ad hoc. O protocolo AO2P visa proporcionar privacidade com base em uma comunicação anônima entre os nós da

rede. Este protocolo utiliza um esquema de competição de acesso, ou seja, não faz troca de mensagens para determinar a posição dos saltos pra criar a rota, mas os receptores deste protocolo se dividem de acordo com o grau de proximidade em relação a distância do nó de destino. A construção de rotas se da através da proximidade entre o receptor e o destino formando a rota com o menor número de saltos.

A privacidade da posição do nó destino é garantida através de um método que gerencia as posições e torna anônima sua identidade e sua posição. Porém o AO2P é vulnerável a alguns ataques de colaboração, como por exemplo, ataques de *blackhole* e *wormhole*. Uma vez que qualquer nó é comprometido, passa a ser incluído em uma rota, pode conduzir ataques diferentes, que são muito difíceis de identificar devido aos identificadores pseudo no AO2P.

5.1.10.2.2 Secure Position Aided Ad Hoc Routing (SPAAR)

Protocolo que visa proteger a rede em ambientes hostis de nós mal intencionados, desse modo, não é publicada, a nenhum nó da rede, a sua topologia, seja ele autenticado ou não. O SPAAR funciona, primeiramente, com a criptografia de chaves pública e privada entre os nós e a AC, e outro mecanismo que realizará a criptografia assimétrica da comunicação entre um nó e sua vizinhança. As rotas são criadas através do envio de mensagens de *hello* criptografadas aos nós próximos, onde estes decriptografam a mensagem e incluem o nó a sua lista de vizinhos reenviando a mensagem à origem. A manutenção da tabela de vizinhos é feita através do envio de mensagens de atualização de rota pelos nós, utilizando a chave do grupo de vizinhos para protegê-la (CARTER; YASINSAC, 2003), onde estas mensagens são transportadas com as mensagens de RREQ e RREP e ainda mensagens de localização.

Para prevenir ataques de replay, este protocolo não replica mensagens dos nós após validá-las, todas as mensagens enviadas são criptografadas com o número do transmissor visando evitar isso.

A descoberta de rotas é realizada através do envio de uma RREQ criptografada aos nós próximos, onde o que estiver mais perto do destino desejado ira armazenar o endereço d transmissor em sua tabela de rotas e irá enviar uma mensagem ao nó seguinte e assim consecutivamente ate alcançar o destino.

Quando chegar ao destino, este enviara uma resposta RREP criptografada pelo mesmo caminho por cada nó e quando esta mensagem chegar à origem será atualizado a sua rota com a posição do destino.

Caso alguma rota for inativada é enviada uma mensagem ERR ao nó que tentou acessá-la, sendo também atualizada nas tabelas de roteamento por cada nó que a mensagem percorrer. O protocolo SPAAR tende a reduzir o *overhead* de roteamento porem gera maior *overhead* no processamento por consequência de sua proteção.

5.2 ANÁLISE DE SEGURANÇA EM REDE AD HOC

Neste projeto foram realizados testes através dos softwares CommView e AirCrack para tentar invadir uma rede ad hoc.

5.2.1Descrição do Cenário

A rede sem fio ad hoc da qual trata esse trabalho foi implementada através de três notebooks que formam a rede, configurados para trabalharem em modo ad hoc, e um notebook externo atacante. Na Tabela 3 mostra os detalhes da configuração dos notebooks.

Tabela 3 – Configuração notebooks utilizados nos testes.

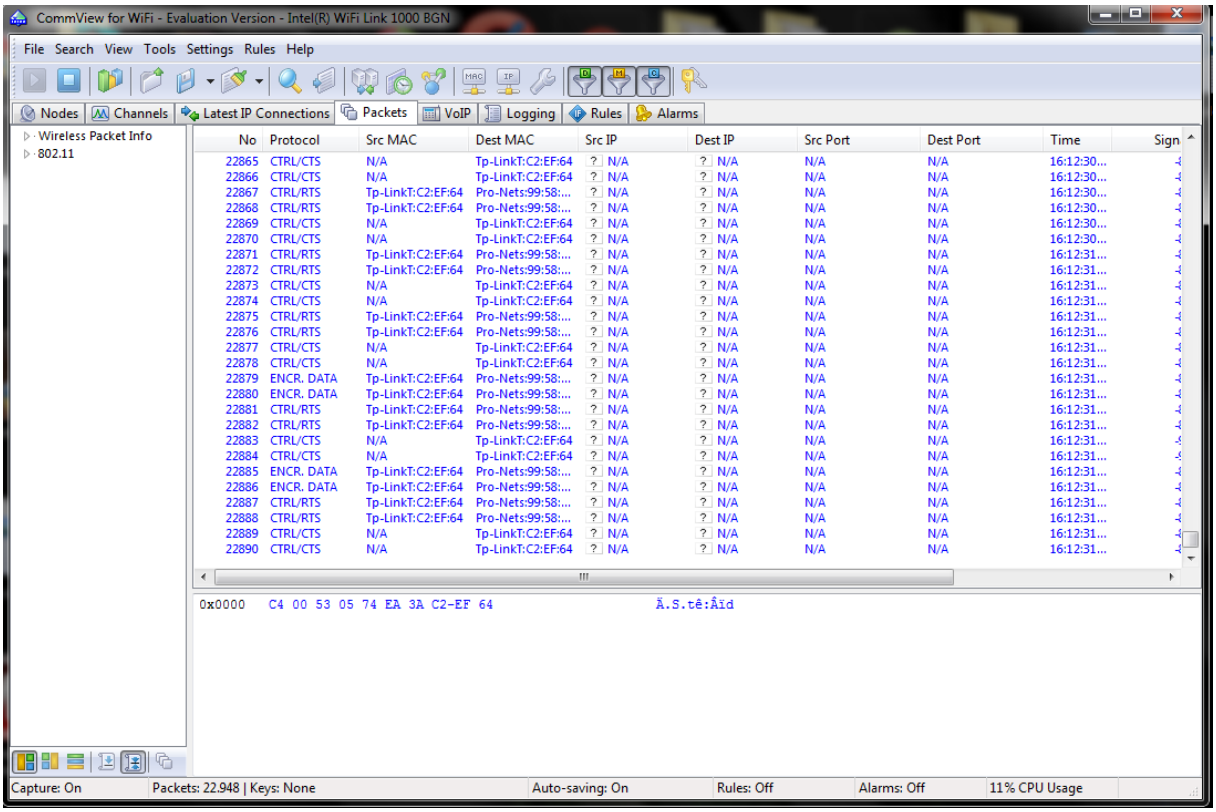
Notebooks usados nos testes.	
Sistema Operacional :	Windows 7
Processador:	Intel Core i5 2.53
Placa de Rede Wireless:	Intel(R) WiFi Link 1000 BGN
Bateria:	Nihon Hewlett Packard Li-Ion 10.8v (3 hrs uso)

5.2.2 Teste com CommView

Primeiramente foi utilizado o CommView (Figura 11), software que monitora e analisa o tráfego de rede, para visualizar as redes próximas. O CommView é usado tanto por profissionais ou administradores de rede, como pode

ser utilizado até por um simples usuário que queira monitorar uma rede. Possui uma interface amigável ele combina desempenho e flexibilidade, com a facilidade de uso.

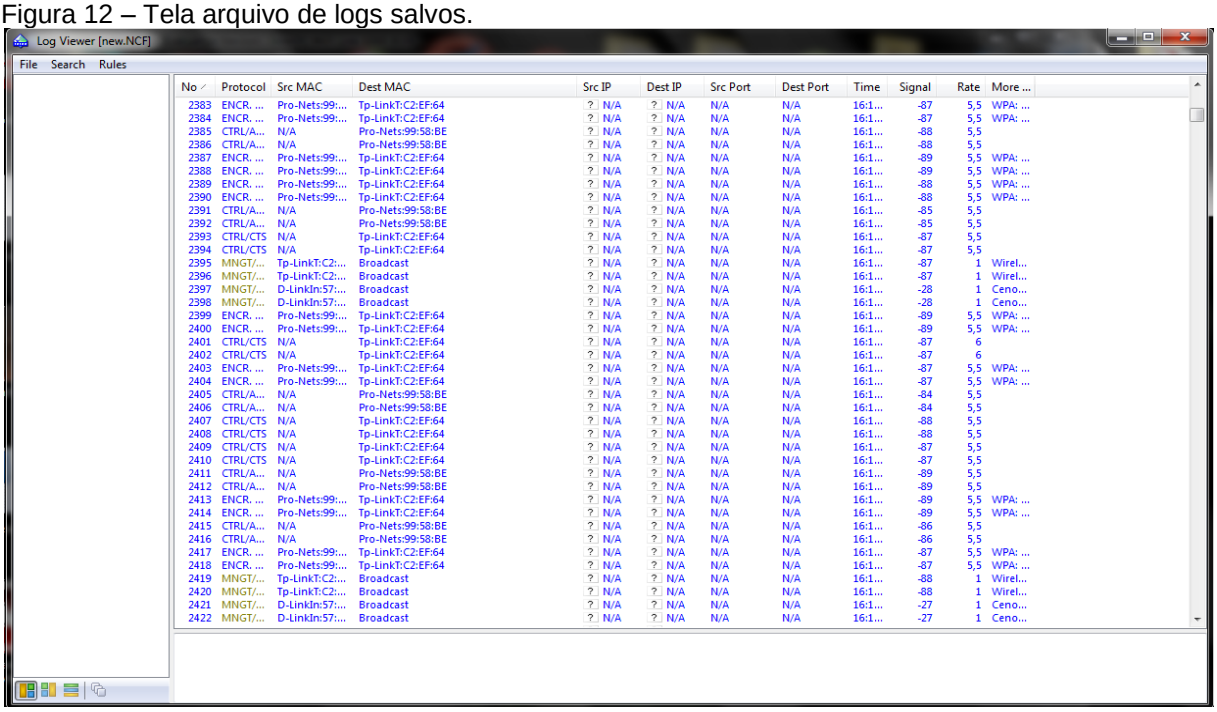
Figura 11 – Tela do CommView



Através do CommView foram capturados pacotes de rede, cerca de 80 mil pacotes em cada teste de captura, para poder tentar descobrir a senha da rede wireless a ser atacada. Ressaltando que a rede ad hoc que foi criada, através dos três notebooks, estava frequentemente realizando comunicação entre si, porque para se descobrir é fundamental que haja a tráfego na rede.

Após coletar os pacotes foi gerado um arquivo com todos os *logs* dentro que será utilizado posteriormente pelo AirCrack como mostra a Figura 12 :

Figura 12 – Tela arquivo de logs salvos.



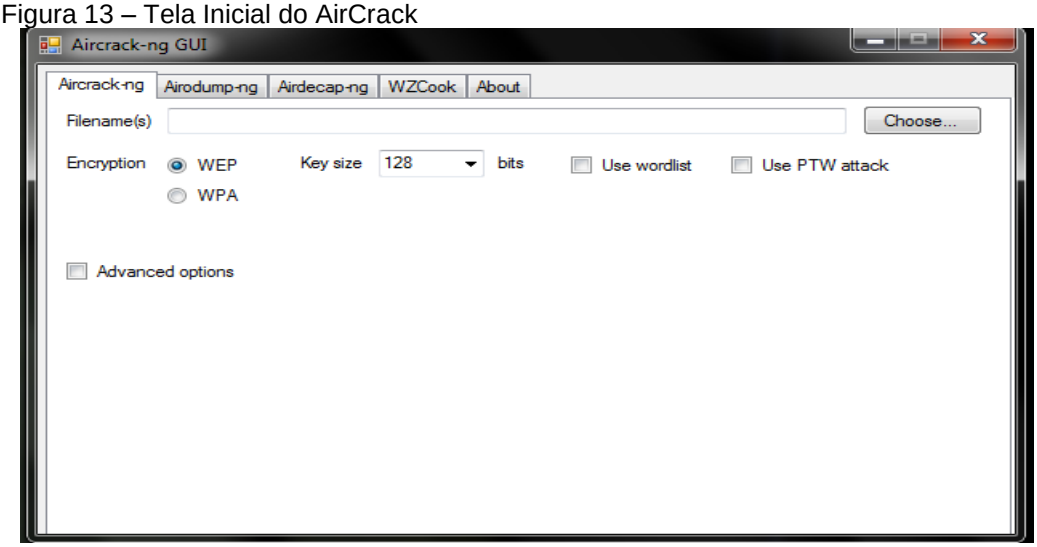
O passo seguinte é utilizar este arquivo de logs no AirCrack para poder tentar descobrir a senha da rede que será atacada.

5.2.3 Testes com AirCrack

É um *sniffer* de pacote, funciona com qualquer placa wireless cujo *driver* suporta modo de monitoramento bruto e pode capturar e analisar o tráfego.

Na Figura 13 pode-se observar a tela inicial do AirCrack onde será carregado o arquivo dos *logs* salvos pelo Commview.

Figura 13 – Tela Inicial do AirCrack



Após carregar o arquivos de *logs* no AirCrack irá abrir uma tela com os endereços das redes e com os pacotes carregados de cada uma delas como mostra a Figura 14. Primeiramente a rede ad hoc foi configurada com criptografia WEP tendo sua senha formada apenas por números *0123456789*. O AirCrack conseguiu descobri-la após a captura de vários pacotes como mostra na Figura 15.

Figura 14 – Tela AirCrack

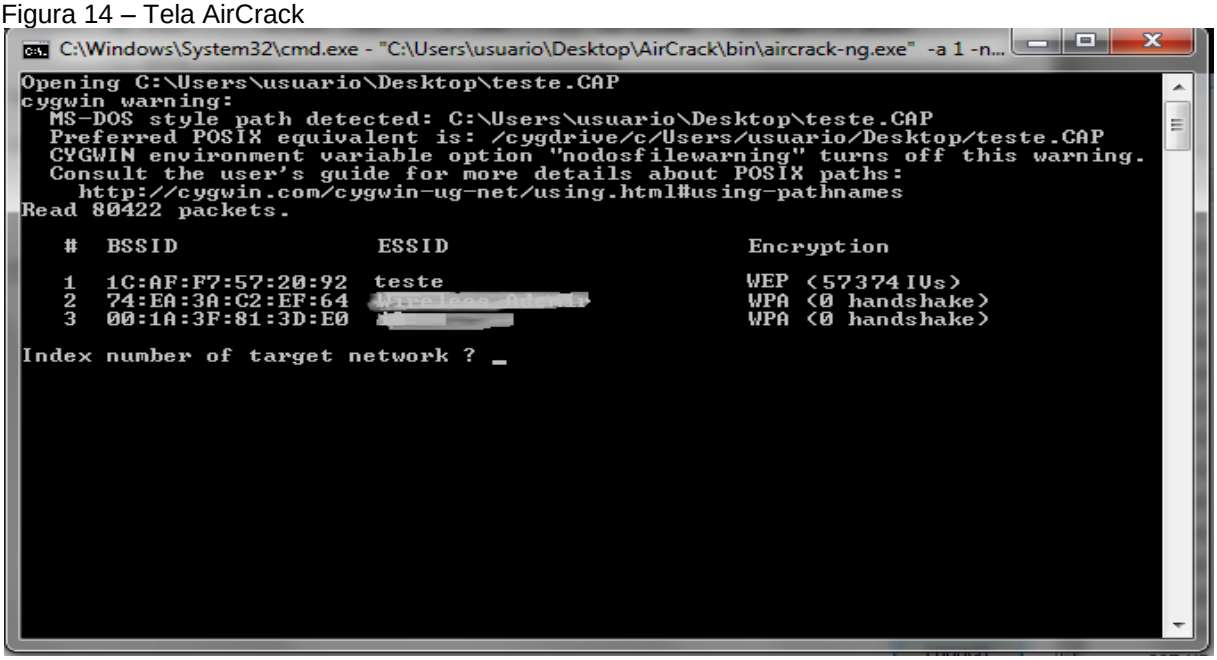
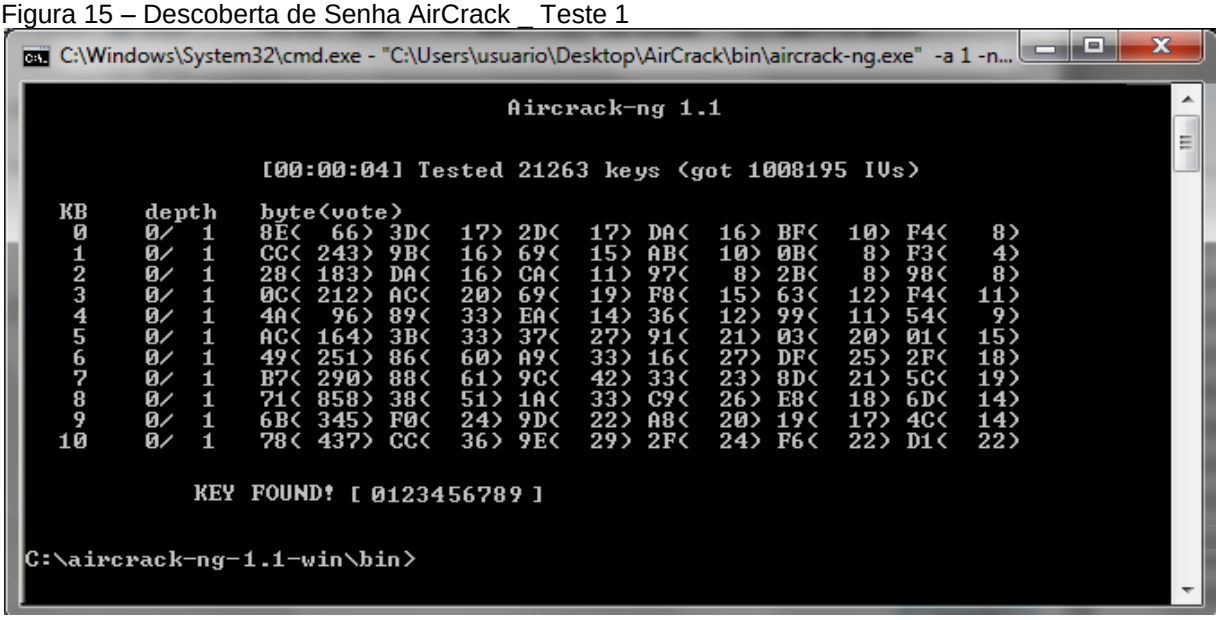
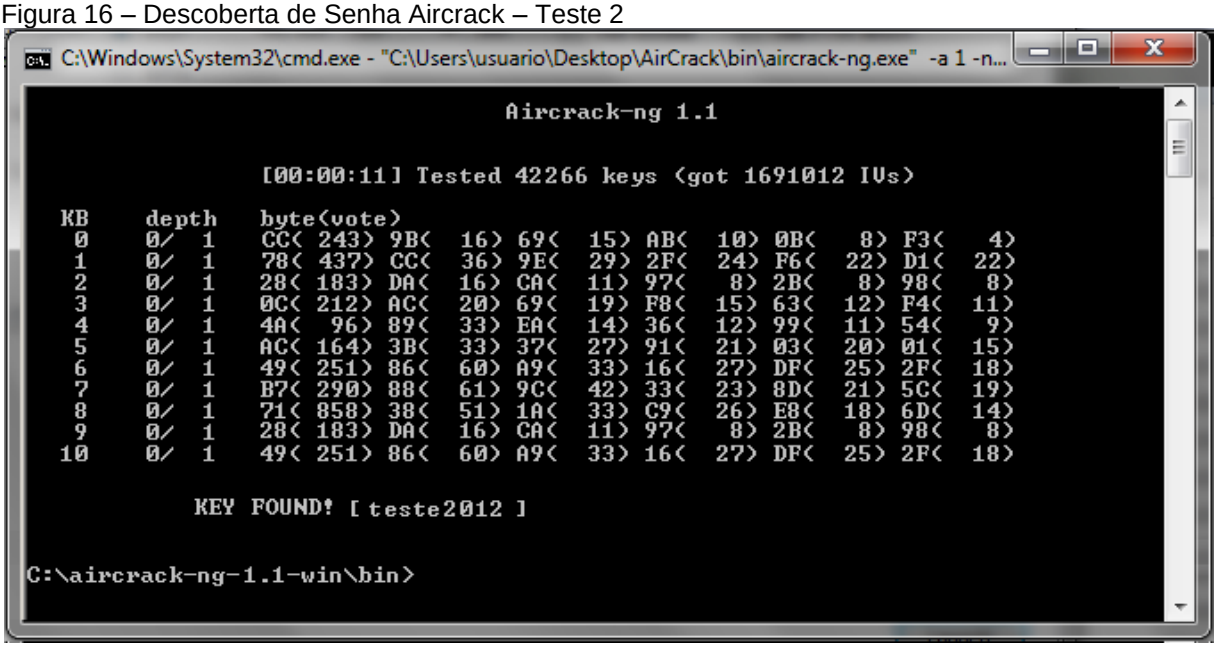


Figura 15 – Descoberta de Senha AirCrack _ Teste 1



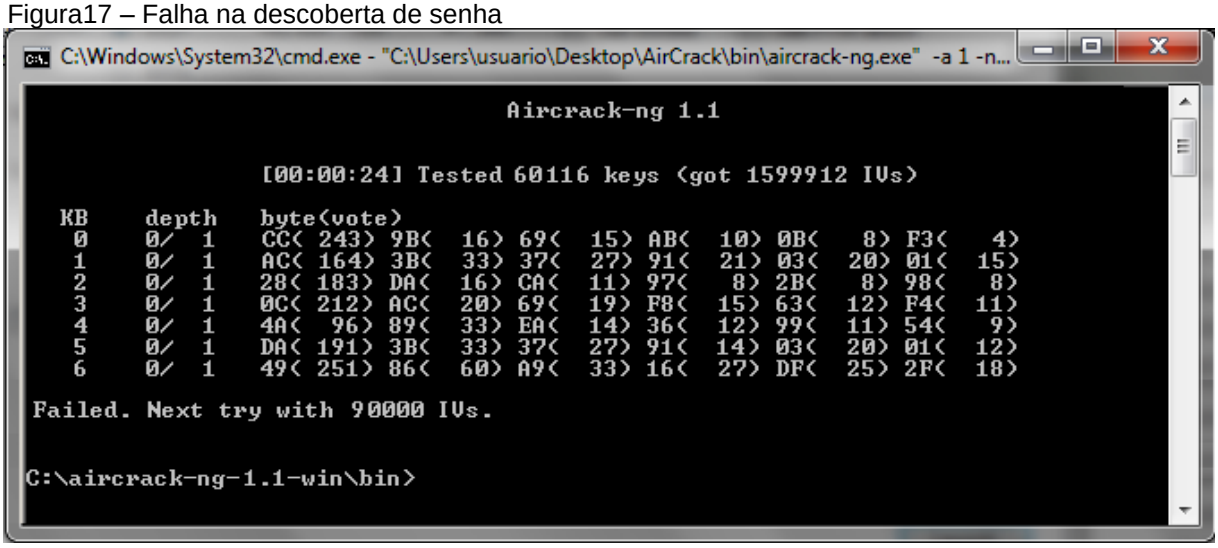
Os testes com quebra de senhas WEP foram realizados ainda mais dois onde criou-se a senha seguinte com letras e números (teste2012). Esta senha também foi descoberta pelo Aircrack, como mostra a Figura 16.

Figura 16 – Descoberta de Senha Aircrack – Teste 2



Porém no seguinte teste realizado com uma senha com letra.números e símbolos (t&st32o!%) e outra senha com vários dígitos (coapl67j92w), onde o Aircrack não conseguiu obter êxito na descoberta como pode-se observar na Figura 17.

Figura17 – Falha na descoberta de senha



Posteriormente foram realizados testes com chaves WPA onde foram verificados os mesmos resultados dos realizados com chaves WEP sendo testadas as mesmas senhas que neste modelo. O AirCrack conseguiu quebrar senhas curtas contendo somente números ou somente letras ou ainda com letras e números, mas quando se cria uma senha mais elaborada com números e letras com vários caracteres ou ainda utilizando de símbolos e caracteres especiais o AirCrack não conseguiu descobrir a senha da rede. E também foram realizados testes com WPA2 mas para este modelo de chave não foi obtido êxito com nenhuma senha testada. Os resultados dos testes de senhas podem ser observados na Tabela 4.

Tabela 4 – Resultados dos testes de senhas.

Senhas	WEP	WPA	WPA2
123456789	Sim	Sim	Não
teste2012	Sim	Sim	Não
t&st32o!%	Não	Não	Não
coapl67j92w	Não	Não	Não

Ao final dos testes pôde-se concluir que para maior segurança contra quebra de chaves WEP, WPA e WPA2 seria a utilização de chaves WEP e WPA com mínimo de 8 dígitos e senha composta por números, letras e símbolos. Porém ainda o método, mas seguro seria o WPA2 que nos testes realizados não foi possível em nenhum momento a descoberta de senha. Vale ressaltar também que o

sucesso da quebra de senha varia muito dependendo do tempo de captura de pacotes e do tráfego que esta ocorrendo na rede, e da *wordlist* que o programa utilizar para fazer os testes de força bruta.

6 CONCLUSÃO

Este trabalho abordou alguns problemas de segurança em redes sem fio ad hoc causado por várias técnicas de ataque. Foram propostos alguns métodos de prevenção de ataques a este modelo de rede como criptografia, certificados digitais, protocolos seguros entre outros.

Buscou-se fazer uma análise para identificar quais são as expectativas dos intrusos de uma rede, bem como identificar quais os principais ataques que podem ser usados em uma rede, e em seguida verificar os mecanismos de segurança necessários em uma rede, para reduzir estes riscos.

Foram realizados testes com as criptografias WEP, WPA e WPA2 a fim de testar a segurança em um cenário de rede. Pode-se observar que o uso de senhas seguras é de vital importância, sendo um dos mecanismos de segurança essenciais para obter-se uma proteção inicial e cabível a rede. O uso de senhas fracas, como foi testado, possibilita ao atacante conseguir a chave da rede de maneira muito fácil, apenas escutando o tráfego entre os dispositivos e fazendo uso de uma ferramenta de ataque de dicionário essa senha é descoberta facilmente. O uso de chaves WEP e WPA mostrou-se vulnerável a descoberta de chave quando se faz uso de senhas fracas, o ataque de dicionário obteve sucesso em todas as chaves fracas testadas. Esses dois modelos de protocolos somente podem garantir um nível maior de segurança quando são adotadas senhas seguras dificultando a descoberta pelo agente malicioso. Já o uso de chaves WPA2 foi o protocolo mais seguro entre os três, pois tanto o uso de senhas fracas como de senhas seguras possibilitou ao atacante identificar a chave da rede.

Dos resultados obtidos com os testes pode-se afirmar que o protocolo mais indicado para o usuário que desejar ter um nível maior de segurança deve ser o protocolo WPA2, ou se forem usados os outros protocolos que sejam elaboradas ou que utilizem softwares para a criação de senhas seguras, evitando assim possíveis intrusos à rede. Também vale ressaltar que para uma segurança maior em uma rede ad hoc se faz muito importante o uso de protocolos seguros, para possibilitar um roteamento seguro dos nós e também o uso de softwares como o EncryptOnClick, citado neste trabalho, para que a troca de mensagens entre a rede obtenha maior segurança, e que mesmo em casos de ataques, ocasionará que o atacante tenha maior dificuldade em descriptar a mensagem ou até mesmo nunca

consiga fazê-lo. Portanto os dados críticos e informações sigilosas devem ser transmitidos utilizando métodos mais confiáveis, uma vez que não se consegue confiar na confidencialidade de qualquer informação que trafega na rede.

Espera-se que o levantamento bibliográfico e os testes realizados neste trabalho possam ser ampliados e utilizados no quesito de segurança. Que esta contribuição efetue mais um passo para assegurar maior confiabilidade em rede sem fio ad hoc.

A partir desta pesquisa pode-se dar continuidade por meio de algumas sugestões de trabalhos futuros:

a) Realizar mais testes utilizando outros métodos de ataques em redes sem fio ad hoc;
b) Implementar protocolos seguros para verificar a segurança dos mesmos em meio a um ataque neste modelo de rede;
c) Realizar testes com outros softwares de criptografia para troca de mensagens;
d) Utilizar de outros programas de ataque de dicionário para verificar a segurança dos protocolos WEP, WPA e WPA2;
e) Realizar testes de ataque de falsificação de identidade em uma rede com certificado digital e assinatura digital para verificar a autenticidade dos usuários.

REFERÊNCIAS

AAD, I.; HUBAUX, J.P.; KNIGHTLY, E. **Denial of Service Resilience in Ad Hoc Networks**, Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, USA. 2004.

ANDERSON, R.; KUHN, M. **Tamper resistance - a cautionary note**. Second USENIX Workshop en Electronic Commerce. 1996.

BERNARDO, A.M. Villela; DUARTE, Otto Carlos **. Maximum throughput analysis in ad hoc networks.** Springer Berlin / Heidelberg. Proceedings of Third International IFIP-TC6 Networking Conference, volume 304, Athens, Greece. 2004.

BUIATI, Fábio Mesquita. **Protocolo seguro para auto configuração de endereços de redes móveis ad hoc**. Dissertação (Mestrado) – Universidade de Brasília. Brasília. 2004.

BUTTYAN, L.; HUBAUX, J. P. **Enforcing service availability in mobile ad-hoc wans**. Em IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC*)*, Boston, USA. 2000.

CALLAS, J.; DONNERHACKE, L.; FINNEY, H.; THAYER, R. **Openpgp message format**. USA. 1998.

CARMONA, Tadeu. **Segredos da Espionagem Digital**. São Paulo. SP. 2005.

CARTER, Stephen; YASINSAC, Alec. **Secure Position Aided Ad hoc Routing**. Computer Science Department - Florida State University . Florida, USA. 2003.

CHAN, H.; PERRIG, A.; SONG, D. **Random key predistribution schemes for sensor networks**. IEEE Symposium on Security and Privacy, 2003.

CORRÊA, Gabriel de Figueiredo. **Tipos de Ataques por Camadas**. Disponível em http://gabritech.blogspot.com.br/2009/10/tipos-de-ataques-por-camada-camada-de.html. Acessado em setembro de 2011.

DUARTE , L**. Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x**. Monografia. Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, SP. 2003.

EHRSAM, William Friedrich; MEYER, Carl H. W.;POWERS, Robert Lowell; SMITH, John Lynn; TUCHMAN, Walter Leonard. Product block cipher system for data security. U.S. Patent 3.962.539. 1975.

FERNANDES, N. C. et al**. Ataques e mecanismos de segurança em redes ad hoc**. In: Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais – SBSEG, Santos, SP. 2006.

GAHLIN, C. **Secure ad hoc networking**. Master's thesis, University of Umea. Work in progress. 2004.

GUERRERO, M.; ASOKAN, N. **Securing ad hoc routing protocols**. ACM Workshop on Wireless Security (WiSe) in conjunction with MobiCom. 2002

HU, Y. C.; PERRIG, A.; JOHNSON, D. B. **Rushing attacks and defense in wireless ad hoc network routing protocols**. Second ACM Workshop on Wireless Security (WiSe 03). 2003.

JOHN, R. Douceur. **The sybil attack**. In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS 02), Cambridge, MA, USA. 2002.

JOHNSON, D. B.; MALTZ, D. A. **Dynamic source routing in ad hoc wireless networks, mobile computing**. Em Kluwer Academic Publishers, volume 353. Mobile Computing (ed. T. Imielinski and H. Korth). 1996.

JOHNSON, D. B.; MALTZ, D. A.; BROCH, J. **DSR: the dynamic source routing protocol for multihop wireless ad hoc networks**. Addison Wesley Professional. New York, USA. 2001.

KARLOF, C.; WAGNER, D. **Secure routing in wireless sensor networks: attacks and countermeasures**. IEEE International Workshop on Sensor Network Protocols and Applications. 2003.

KOTVISKI, Adriel**, O que são redes ad hoc?**. Disponível em www.tecmundo.com.br/2792-O-que-sao-redes-ad-hoc-.htm. Acessado em outubro de 2011.

LAMPORT, L.; SHOSTAK, R.; PEASE, M. **The byzantine generals problem**. ACM Transactions on Programming Languages and Systems (TOPLAS), volume 4, 1982.

MAIA, Roberto. **Segurança em Redes Wireless-802.11i**. Disponível em: http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html. Acessado em outubro de 2012.

MORENO,Edward David; PEREIRA, Fábio Dacêncio; CHIARAMONTE, Rodolfo Barros. **Criptografia em Software e Hardware**. São Paulo, SP. 2005.

MURTHY, C.; MANO, B. **Ad Hoc wireless networks: architectures and protocols**. Prentice Halll Professional Technical Reference. 2004.

NEWSOME, J.; SHI, E.; SONG, D.; PERRIG, A. **The Sybil attack in sensor networks: Analysis & defenses**. 3rd IEEE/ACM Information Processing in Sensor Networks 2004 - IPSN 04. 2004.

PERKINS, C. E.; ROYER, E. M. **Ad hoc on-demand distance vector routing**. IEEE WORKSHOP ON MOBILE COMPUTING SYSTEMS AND APPLICATIONS 2, New Orleans. USA. 1999.

PERKINS, C. E.; ROYER, E. M.; DAS, S. R.; MARINA, M. K. **Performance comparison of two on-demand routing protocols for ad hoc networks**. IEEE Personal Communications, 2001.

PERKINS, C. E.; ROYER, E. M.; DAS, R. S. **Ad Hoc On-Demand Distance Vector Routing**. Request for Comments: 3561. 2003.

PINHEIRO, José Mauricio Santos. **Redes Móveis Ad Hoc**. Rio de Janeiro, RJ. 2005.

PINHEIRO, José Mauricio Santos. **Assinatura e Certificado Digital**. Curso Tecnólogo de Redes de Computadores. Volta Redonda, RJ. 2008.

PIROPO, Benito. **Atributos Digitais I: Confidencialidade e Autenticidade**. Belo Horizonte, MG. 2007.

QUAYYUM, A.; VIENNOT, L.; LAOUITI, A. **Multipoint relaying: An efficient technique for flooding in mobile wireless networks**. 35th Annual Hawaii International Conference on System Sciences, 2001.

RIVEST, R. L.; SHAMIR, A.; E ADLEMAN, L. M. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM 21, 1978.

SANZGIRI, K.; DAHILL, B.; LEVINE, B. N.; SHIELDS, C.; BELDING-ROYER, E. M. **A secure routing protocol for ad hoc networks**. In IEEE International Conference on Network Protocols – ICNP. 2002.

SÊMOLA, Marcos. **Saiba criar senhas seguras**. Disponível em http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2006-08-18.5368218714/ Acesso em agosto de 2012.

SIMON, S., **The Code Book**, Anchor Books, EUA, 1999.

SOARES, L.F.G; LEMOS, G; COLCHIER, S. **Redes de computadores: das LANs, MANs, WANs às Redes ATM**. Rio de Janeiro: Campus. 1995.

STALLING, W. **Cryptography and Network Security: Principles and Practice**, 2nd ed., Infrmation Theory, vol. 22, 1976.

STALLINGS, W. **Business Data Communications**. Prentice-Hall, 5th edição. 2004.

YI, Seung; NALDURG, Prasad; KRAVETS, Robin. **A Security-Aware Routing Protocol for Wireless Ad Hoc Networks**. Em ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001). University of Illinois at Urbana-Champaign, Long Beach, CA. 2001.

YIH-CHUN, Hu; JOHNSON, David B.; PERRIG, Adrian, **SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks**, in the 4th IEEE Workshop on Mobile Computing Systems and Applications, 2002.

WILLIAN F.; EHRSAM, C. H. W. **Product block cipher system for data security**.USA. 1975.

WOOD, A.; STANKOVIC, J. **Denial of service in sensor networks**. Computer, 2002.

APÊNDICE(S)

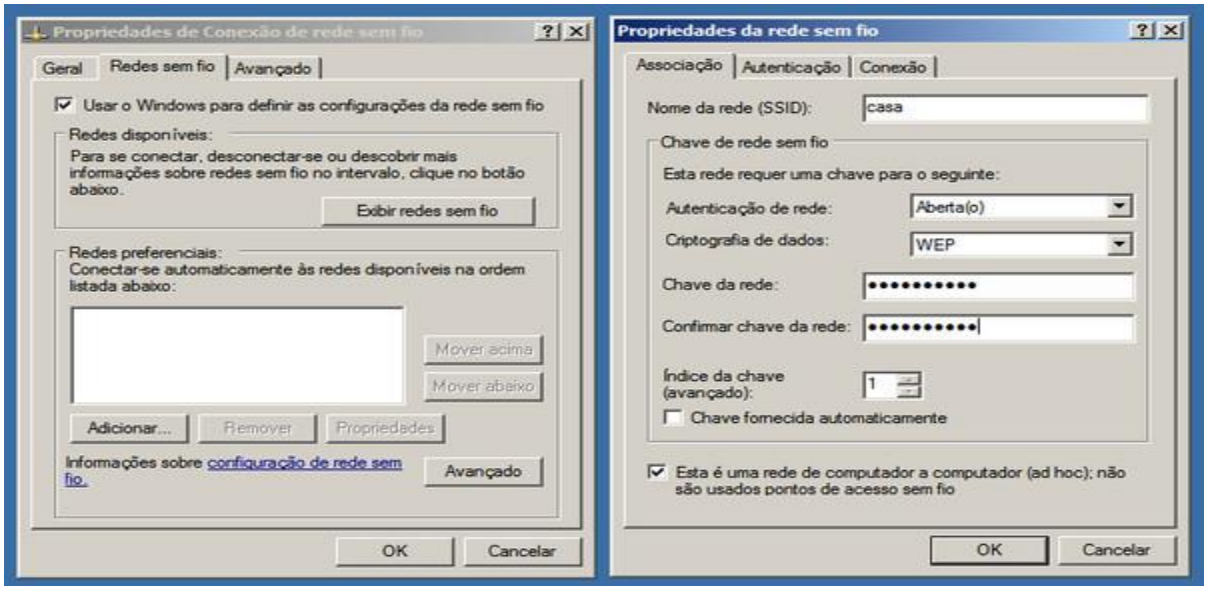
APÊNDICE A – Montagem Rede Ad Hoc

Assim como é possível ligar dois micros diretamente usando duas placas Ethernet e um cabo cross-over, sem usar hub, também é possível criar uma rede wireless entre dois computadores sem usar um ponto de acesso. Necessita apenas configurar ambas as placas para operar em modo Ad Hoc. A velocidade de transmissão é a mesma, mas o alcance do sinal é bem menor, já que os transmissores e as antenas das interfaces não possuem a mesma potência do ponto de acesso. Pelo mesmo motivo, a velocidade também tende a cair muito mais rapidamente conforme aumenta a distância.

Um uso comum para o modo Ad Hoc é quando você tem em mãos dois notebooks com placas wireless. Um deles pode ser ligado ao modem ADSL (com fio) para acessar a internet e compartilhar a conexão com o segundo usando a placa wireless, que fica livre dos fios.

Depois de configurada, a placa wireless é vista pelo sistema como um dispositivo de rede normal. Pode-se compartilhar a conexão da mesma forma que em um micro com duas placas de rede.

Para criar uma rede Ad Hoc no Windows 7, acesse o *Painel de Controle* > *Conexões de rede*. Dentro das propriedades da conexão de redes sem fio, acesse a aba *Redes sem fio* e clique no *Adicionar*. Na tela seguinte, defina o SSID da rede Ad Hoc, marque a opção *Esta é uma rede de computador (ad hoc); não são usados pontos de acesso sem fio*, como mostra as imagens abaixo:

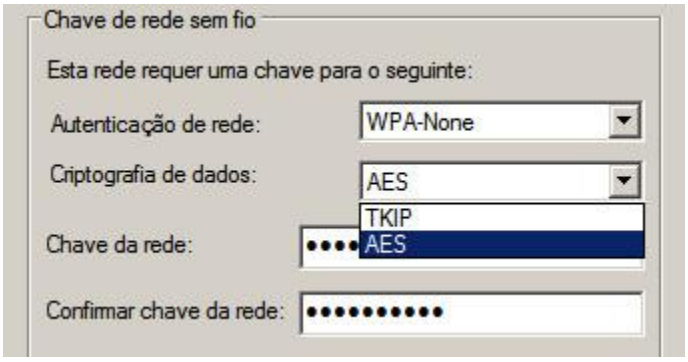


Assim como ao configurar um ponto de acesso, pode-se ativar o uso de criptografia. O modo mais compatível é escolher a opção *Aberta* na opção *Autenticação de rede* e usar a opção *WEP* na opção *Criptografia de dados*, definindo uma chave de acesso, desmarque a opção Chave fornecida automaticamente.

Embora tanto as chaves *WEP* de 64, quanto às de 128 bits sejam vulneráveis, é sempre recomendável usar chaves de 128 bits, que são um pouco mais difíceis de quebrar. A chave pode conter 13 caracteres ASCII (letras, números e caracteres especiais) ou 26 caracteres em hexa (números e as letras de A a F). Também tem a opção de definir uma chave de 64 bits, use 5 caracteres (em ASCII) ou 10 caracteres (em hexa).

Esta configuração permitirá que a rede seja acessada por praticamente qualquer dispositivo, incluindo micros com placas antigas, 802.11b, palmtops, consoles e smartphones com redes Wi-Fi. O WEP é fácil de quebrar, mas os risco é minimizado devido ao alcance reduzido da rede Ad Hoc. Se a segurança não for uma prioridade, esta é a configuração recomendável.

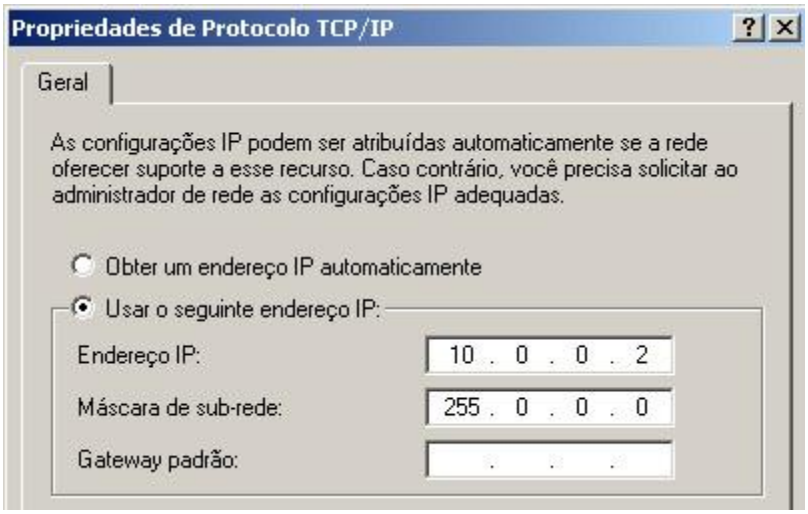
Existe também a opção de usar o *WPA-None*, uma versão simplificada do WPA, destinada ao uso em conexões Ad Hoc, onde pode escolher entre usar o TKIP ou o AES como sistema de criptografia. A maior deficiência do WPA-None em relação ao WPA ou WPA2 usado em redes wireless em modo infraestrutura (com ponto de acesso) é que no WPA-None as chaves são estáticas e por isso são muito mais fáceis de serem quebradas. Na prática, o WPA-None com TKIP equivale ao WEP em termos de segurança (a única vantagem é que pode-se definir uma chave mais longa), enquanto o AES é apenas um pouco mais seguro, como pode ser observado na imagem abaixo:



Depois de criar a conexão Ad Hoc em um dos computadores, ela passa a aparecer para os demais na lista de redes disponíveis, permitindo que eles se conectem diretamente, após fornecerem a chave de encriptação, como na figura a seguir:

Em uma rede Ad Hoc todos os micros estão no mesmo nível hierárquico, sem uma autoridade central. Todas as estações configuradas para usarem o mesmo SSID e as mesmas configurações de encriptação, estabelecem contato e criam uma rede ponto a ponto.

Inicialmente, os computadores terão acesso apenas um ao outro, sem acesso à web e sem DHCP. Depois de conectá-los à rede ad-hoc, você ainda precisará definir endereços manualmente, dentro de uma das faixas reservadas a redes locais, como a 10.x.x.x e a 192.168.x.x, como observamos na figura abaixo:



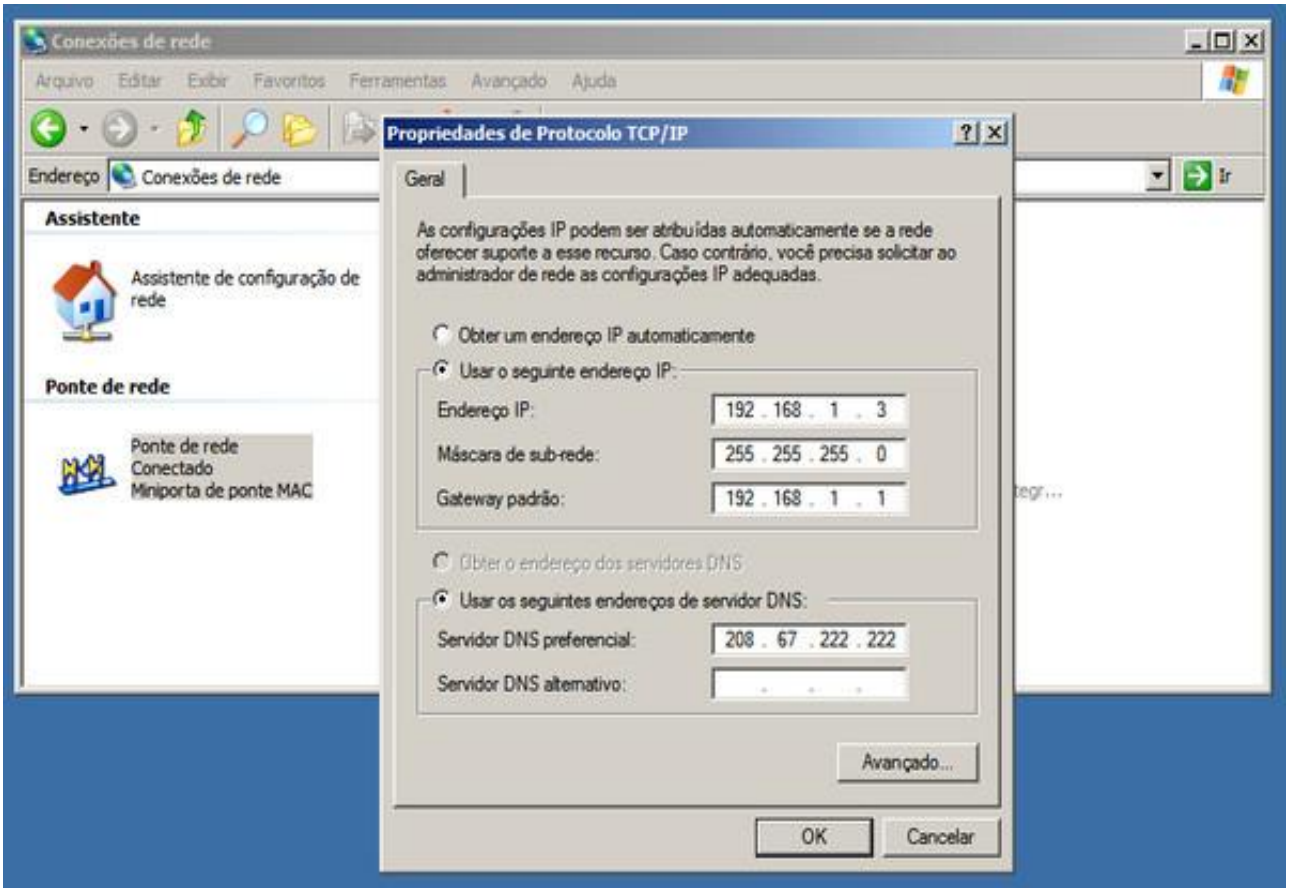
Para compartilhar o acesso à web ou à rede local com os computadores da rede Ad Hoc, é necessário que um dos computadores esteja conectado simultaneamente às duas redes e possa assim atuar como gateway, como no caso de um notebook com a rede wireless e uma placa cabeada.

A primeira opção é ativar o ICS, clicando sobre o ícone da conexão local. Isso vai atribuir o endereço "192.168.0.1" à placa wireless e permitir que os micros da rede Ad Hoc acessem a web recebam endereços IP automaticamente. Eles poderão inclusive acessar outros micros da rede local através do gateway, mas não poderão ser acessados por outros computadores fora da rede Ad Hoc.

A segunda opção é criar uma conexão de ponte, combinando a interface da rede local e a interface wireless. Com isso, os micros da rede Ad Hoc passarão a fazer formalmente parte da rede local, recebendo endereços IP do servidor DHCP, tendo acesso a todos os recursos da rede e podendo compartilhar arquivos e pastas com os demais computadores.

Para isso, seleciona-se as duas interfaces no *Painel de Controle* > *Conexões de rede* e ative a opção *Conexões de ponte*, conforme a figura abaixo:

Acesse em seguida as propriedades da *Ponte de rede* e defina um endereço IP e a máscara dentro da faixa usada na rede local. Será através desse endereço que o computador poderá ser acessado tanto pelos micros da rede local, quanto pelos da rede Ad Hoc, abaixo esta a imagem desse processo:



Assim os micros da rede Ad Hoc passam a ser configurados da mesma forma que os demais micros da rede, seja via DHCP, ou seja, usando IPs dentro da faixa usada na rede. A principal observação é que eles dependem do micro usado como gateway para ter acesso à rede. Se ele for desligado, ou ficar fora de alcance, o acesso é perdido.

Tutorial extraído de http://www.hardware.com.br/tutoriais/configurando-ad-hoc/pagina2.html.

APÊNDICE B - ARTIGO

Aspectos de Segurança em Rede Sem Fio Ad Hoc

Angélica da Cunha[1], Paulo João Martins[2]

[1]Acadêmica do Curso de Ciência da Computação – Unidade Acadêmica de Ciências, Engenharias e Tecnologias – Universidade do Extremos Sul Catarinense (UNESC) – Criciúma – SC

[2]Professor do Curso de Ciência da Computação – Unidade Acadêmica de Ciências, Engenharias e Tecnologias – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma – SC

angelica_cdc22@hotmail.com, pjm@unesc.net

Abstract. *Amid the technological advances, there is an ever greater need to make use of tools that help you keep your information protected, even when it about respects the ad hoc networks that are still unexplored. This work is a study on this network model focusing on security mechanisms in order to increase its reliability. Was pointed out some vulnerabilities and security techniques like secure protocols, encryption, digital certificates, and others to try to prevent such attacks of have succeed in discovering information or problems caused in the performance of network functionalities. At the end of this work was realized test out attacks and a solution for the same, with goal a proposal to show improvement against this vulnerability.*

Keywords: *Wireless, Ad Hoc, Security, Attacks, Vulnerability.*

Resumo. *Em meio aos avanços tecnológicos, cada vez há uma maior necessidade em se fazer uso de ferramentas que ajudem a manter as informações protegidas, ainda mais no que diz respeitos a redes ah hoc que ainda são pouco exploradas. Este trabalho consiste em um estudo sobre este modelo de rede dando enfoque nos mecanismos de segurança para poder aumentar a sua confiabilidade. São apontadas algumas vulnerabilidades e técnicas de segurança como protocolos seguros, criptografia, certificados digitais e outros para tentar impedir que tais ataques obtenham sucesso na descoberta de informações ou ocasionem problemas no desempenho das funcionalidades da rede. Ao final deste trabalho foi realizado teste de ataque e uma solução para o mesmo com objetivo de mostrar uma proposta de melhoria contra tal vulnerabilidade.*

Palavras-chave: *Rede Sem Fio, Ad Hoc, Segurança, Ataques, vulnerabilidade.*

1. Introdução

As redes ad hoc surgiram no começo da década de 70, quando uma instituição de pesquisa dos Estados Unidos, passou a estudar como estabelecer uma comunicação via rádio em um ambiente tático militar. Uma das vantagens deste modelo de rede é pelo fato de serem redes sem fio, que dispensam o uso de um ponto de acesso comum entre os computadores conectados a ela, de modo que os dispositivos da rede ao qual estão

conectados funcionem como se fossem um roteador, compartilhando informações de dispositivos vizinhos. De acordo com Buiati (2004) o uso destas redes em operações de resgate, salvamentos e catástrofes naturais em conjunto com comunicação com satélite pode ser extremamente útil. Em geral podem ser utilizadas em ambientes que necessitem de uma conexão entre si, inclusive não restringem o uso apenas de computadores, pode-se também conectar uma impressora ou celular a rede, por exemplo, desde que possuem suporte para isto.

Nos dias atuais, faz-se de grande importância que as informações de um sistema sejam protegidas e gerenciadas. A grande maioria das empresas, instituições, organizações ou usuários residenciais, optam por armazenar informações em um sistema de segurança [Aad; Hubaux; Knightly, 2004]. Neste caso a importância de fazer uso de mecanismos de segurança é vital, já que com a crescente tecnologia voltada à informação também é crescente o número de técnicas de intrusão a informação por indivíduos não autorizados.

Inicialmente, para fornecer segurança a redes sem fio ad hoc devem ser levados em conta os atributos básicos de segurança: autenticidade, confidencialidade, disponibilidade, integridade e não repúdio. Estas medidas visam evitar o vazamento de informações, fraudes, erros, uso indevido, sabotagens e roubo de informações [Buiati, 2004], a segurança em redes sem fio se faz cada vez mais necessária já que o seu ponto fraco é a forma de transmissão de informações que é realizada pelo ar que podem ser capturadas a distâncias utilizando-se de uma antena amplificada.

Os ataques existentes em redes ad hoc móveis podem ser realizados de duas maneiras: os ataques passivos que realizam a espionagem dos dados da rede sem afetá-la de modo operacional, e os ataques ativos que são caracterizados pela manipulação de dados da rede pelo atacante.

Com base nisto, o objetivo deste trabalho se faz em descrever algumas vulnerabilidades em redes sem fio ad hoc e fazer uso de técnicas de segurança para aumentar a confiabilidade neste modelo de rede.

2. Vulnerabilidades e Métodos de Ataques em Redes Sem Fio Ad Hoc

As vulnerabilidades podem ser divididas em vulnerabilidades dos mecanismos básicos e vulnerabilidade dos mecanismos de segurança. A primeira faz referência aos mecanismos básicos de operação da rede, onde o mais crítico dele é o roteamento, e assim passam a fazer troca de dados criptografados. Já a vulnerabilidade dos mecanismos de segurança tornou-se consenso que o ponto crítico é o gerenciamento das chaves do sistema de segurança [Hu et al, 2003]. As redes ad hoc, devido à possibilidade de emprego em ambientes hostis, devem agregar mecanismos de forma a contornar o estado vulnerável em que se pode encontrar a rede quando da captura de um dos seus dispositivos.

A possibilidade de descoberta de uma informação por indivíduos não autorizados deve ser combatida principalmente em de aplicações que necessitam de um grau de segurança maior devido ao sigilo que dependem suas informações. Estas informações críticas devem ser protegidas contra ataques de exposição a fim de manter em sigilo detalhes como localização dos nós, chaves, senhas e identidade de operadores e proprietários dos dispositivos.

2.1 Ataques Passivos e Ataques Ativos

Na rede ad hoc os ataques podem ser divididos em passivos ou ativos [Murthy; Mano, 2004], e também internos e externos, onde estes ataques têm como objetivos principais a descoberta de informações restritas a usuários na autorizados e também impedir que sejam realizados as operações da rede.

O ataque passivo, assim como o interno, são os ataques que mais afetam a rede, pois os eles agem de forma que comprometem que o nó realize outros ataques aos demais nós. Enquanto aos ataques passivos e externos pode-se dizer que é o menos comprometedor, visando que nem por causa deste motivo ele deve ser desconsiderado em um sistema de segurança, ele é caracterizado pela captura de informações na rede.

Nos ataques passivos, o atacante não interfere no funcionamento da rede, mas pode escutá-la e analisar o seu tráfego. O atacante tem acesso à informação, porém não a altera ou destrói. Os ataques passivos são de difícil detecção por não influírem no comportamento da rede.

3. Segurança em Rede Sem Fio Ad Hoc

O sistema de segurança tem como objetivo garantir que a funcionalidade da rede e suas características não sejam afetadas em função de situações que possam acontecer e ocasionar restrições as suas características, sua dinâmica de comportamento da rede e também comprometer o seu desempenho. Pode-se assim afirmar que criar e implementar arquiteturas para estas redes ad hoc suprindo estas necessidades de segurança é uma tarefa muito custosa.

Uma das proteções básicas dos mecanismos de operação é a troca de mensagens dos usuários da rede. Desse modo é adotado esquemas de criptografia onde são adaptados a este tipo de ambiente. Assim pode-se observar um ponto que tem muita vulnerabilidade em relação ao sistema de segurança que é o gerenciamento de chaves criptografadas.

3.1 Criptografia

A criptografia pode ser entendida com um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algoritmo, convertendo um texto original em um texto ilegível e vice-versa [Simon, 1999]. A criptografia tem como objetivo garantir que haja segurança no sigilo de informações que são trafegadas em um ambiente computacional. Ela passa a ser usada para criptografar os dados antes que os mesmos sejam enviados aos destinatários, assim, se houver a interceptação destes dados, dificilmente eles serão compreendidos.

Ela se divide em dois segmentos: simétrica e assimétrica. A criptografia simétrica é caracterizada pela existência de uma chave privada, da qual é compartilhada entre todos os nós que necessitam fazer uma conexão (Figura 1). Chave simétrica possui a vantagem de não exigir muito poder de computação. Isso ocorre porque os algoritmos simétricos trabalham com deslocamentos e permutas sobre blocos de dados que serão cifrados usando chaves de 56 a 256 bits [Ehrsam et al, 1975] . Por esse motivo, os algoritmos assimétricos também são conhecidos como algoritmos de blocos.

A criptografia assimétrica possui duas chaves: chave pública e chave privada. A chave pública é distribuída entre os membros da rede, e a privada é mantida em segredo

pelo nó. Ela possui um maior custo computacional em relação à simétrica, devido ao fato de utilizar operações como a exponenciação. O principal objetivo é fazer com que, por meio de uma das chaves, não seja possível encontrar a outra.

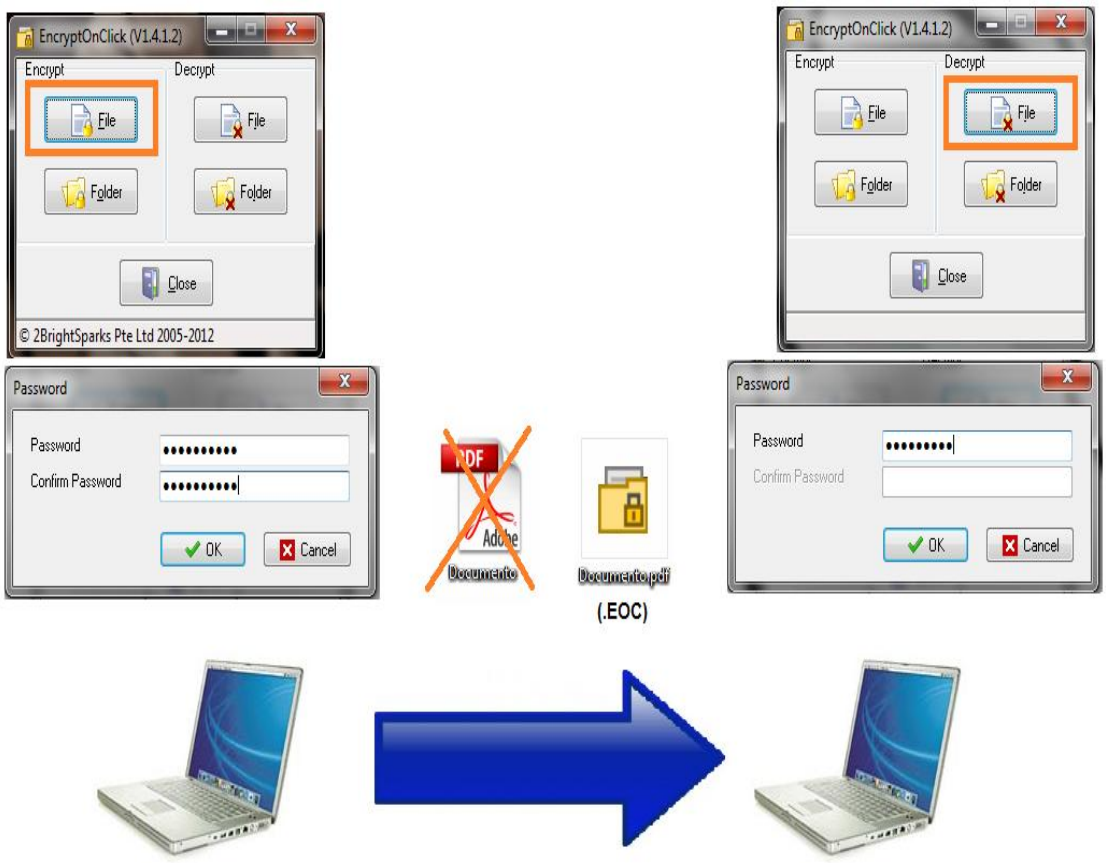


Figura 1. Criptografia de Arquivo com EncriptOnClick

3.2 Assinatura Digital

É a versão digital da assinatura de mão que é autenticada em cartório. A autenticação ou assinatura digital garante o não repudio para envio e recebimento de mensagens ou arquivos. Ela é gerada utilizando chave privada de um usuário, do qual somente ele vai conhecer e ter acesso.

A assinatura digital é um conjunto de procedimentos matemáticos realizados com a utilização de técnicas de criptografia assimétrica que permite, de forma única e exclusiva, a comprovação da autoria de um determinado conjunto de dados [Pinheiro, 2008]. Assim quando um usuário assinar uma mensagem, não terá como negar que o fez porque somente ele possuirá sua chave privada, sendo que é muito importante que esta chave seja guardada em segurança e sua chave pública correspondente esteja em uma entidade confiável.

3.2 Certificado Digital

Auxiliam na autenticação de usuários em redes de comunicações, são equivalentes a cédulas de identificação como RG, CPF e passaporte, é um arquivo binário, que pode ser armazenado em um dispositivo de segurança como *smart cards* e *tokens*. Os

certificados digitais são assinados por uma Autoridade Certificadora (AC) que lhe provê a garantia de autenticidade.

Os certificados digitais garantem a identificação de uma instituição, pessoa física ou um endereço da internet, ele é um arquivo em media com 1Kb onde possui uma chave criptográfica e dados do proprietário. Algumas certificadoras mais conhecidas são a Verisign, a Thawte e a brasileira Certisign.

Os certificados digitais possuem chaves eletrônicas vinculadas para poder utilizar de criptografia e assinar informações digitais. Assim, possibilita fazer verificação para descobrir se o usuário tem ou não autorização de utilizar determinada chave, prevenindo o uso de chaves falsas na identificação de pessoas.

3.3 Senhas Seguras

O uso de senhas fracas, ou seja, senhas que sejam fáceis de imaginar e descobrir são um dos maiores problemas na utilização deste tipo de autenticação representando cerca de 80% dos problemas de segurança [Sêmola, 2006]. As senhas fortes possibilitam que a segurança em uma rede possa ser mais robusta.

Para criar uma senha segura deve-se levar em consideração alguns fatores como quantidade de caracteres (deve conter no mínimo 8) e não elaborar senhas com dados pessoais ou de familiares (nomes, datas, entre outros). O ideal é utilizar senhas aleatórias, que incluam letras minúsculas, maiúsculas, números e símbolos [Carmona, 2005].

Alguns métodos podem ser utilizados para criação de senhas mais fortes, como por exemplos existem sites na internet que elaboram ou analisam a senha para saber se a mesma é segura ou não. Para criar senhas pode-se citar os sites Password.Es http://password.es/ (site em espanhol) e o Strong Password Generator http://strongpasswordgenerator.com/ (site em inglês) ambos são gratuitos. Um site para verificação de senhas é o Password Meter, que pode ser acessado por http://www.passwordmeter.com/ (site em inglês) que analisa a senha digitada com os requisitos de segurança em relação ao tamanho, uso de letras maiúsculas/minúsculas, números, símbolos, repetição de caracteres e sequência de números do teclado.

3.4 Protocolos Seguros

O roteamento seguro em redes ad hoc possui algumas dificuldades, devido sua topologia dinâmica, à necessidade de funcionar de forma eficaz com recursos limitados, a largura da banda de rede, a capacidade de processamento da CPU, memória e bateria dos computadores integrantes da rede. Os protocolos de roteamento sem segurança são aperfeiçoados para propagar novas informações rapidamente, exigindo interações do protocolo de roteamento mais rápidas e frequentes do que as exigidas em uma rede tradicional [Yih-Chun et al, 2002].

Essas redes não possuem garantia de que o caminho escolhido para realizar a comunicação com determinado nó, está seguro contra ataques mal intencionados. Muitos protocolos são propostos focados na idéia de encontrar o menor caminho entre dois nós o mais rápido possível, entretanto existem aplicações que requerem mais do que a certeza da determinação da menor rota [Yi et al, 2001]. Com base nisto, são

propostos protocolos de roteamento seguro. Dentre os protocolos seguros existente estão os seguintes: ARAN, ARIADNE, SEAD, AO2P e SPAAR .

4. Análise de Segurança em Rede Ad Hoc

Para verificar a segurança neste modelo de rede foram realizados testes através dos softwares CommView e AirCrack para tentar realizar a invasão.

4.1 Ambiente de Testes

Foi implementada uma rede ad hoc para poderem ser realizados os testes de ataques (Tabela 1), através de três notebooks para formar a rede, configurados para trabalharem em modo ad hoc, e um notebook externo atacante.

Tabela 1. Configuração dos notebooks utilizados nos teste.

Notebooks usados nos testes.	
Sistema Operacional :	Windows 7
Processador:	Intel Core i5 2.53
Placa de Rede Wireless:	Intel(R) WiFi Link 1000 BGN
Bateria:	Nihon Hewlett Packard Li-Ion 10.8v (3 hrs uso)

4.2 Testes Realizados

Primeiramente foi utilizado o CommView (Figura 2), software que monitora e analisa o tráfego de rede, para visualizar as redes próximas. O CommView é usado tanto por profissionais ou administradores de rede, como pode ser utilizado até por um simples usuário que queira monitorar uma rede. Possui uma interface amigável ele combina desempenho e flexibilidade, com a facilidade de uso.

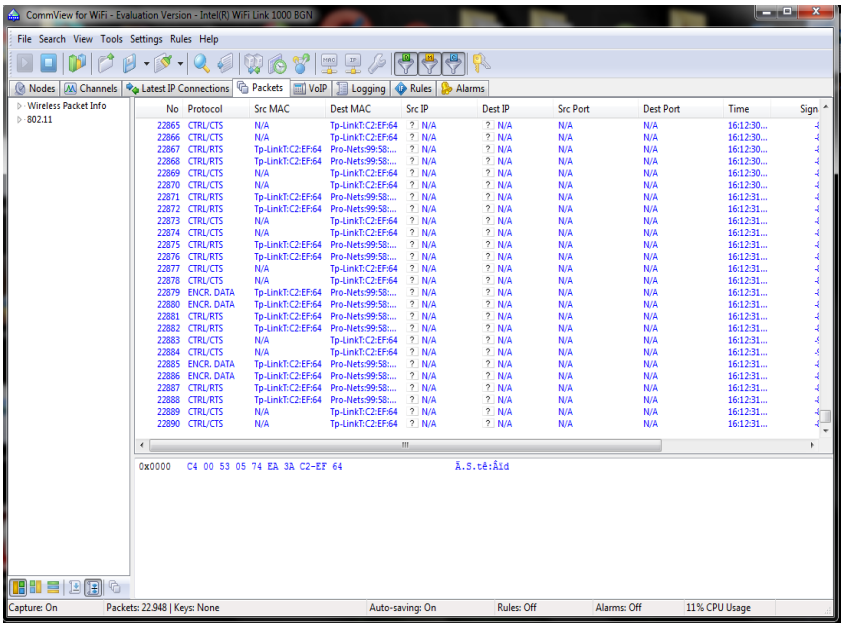


Figura 2. Tela do CommView.

Através do CommView foram capturados pacotes de rede, cerca de 80 mil pacotes em cada teste de captura, para poder tentar descobrir a senha da rede wireless a ser atacada. Ressaltando que a rede ad hoc que foi criada, através dos três notebooks, estava frequentemente realizando comunicação entre si, porque para se descobrir é fundamental que haja a tráfego na rede. Após coletar os pacotes foi gerado um arquivo com todos os *logs* dentro que será utilizado em seguida pelo AirCrack para tentar descobrir a senha da rede que será atacada.

O AirCrack é um *sniffer* de pacote, funciona com qualquer placa wireless cujo *driver* suporta modo de monitoramento bruto e pode capturar e analisar o tráfego. Após carregar o arquivos de *logs* no AirCrack (Figura 3) irá abrir uma tela com os endereços das redes e com os pacotes carregados de cada uma delas. Primeiramente a rede ad hoc foi configurada com criptografia WEP, a seguir com a criptografia WPA e depois com WPA2, onde foram realizados vários testes com quatro tipos diferentes de senhas, para testar qual modelo se senha se mostra mas segura nestes modelos de criptografia .

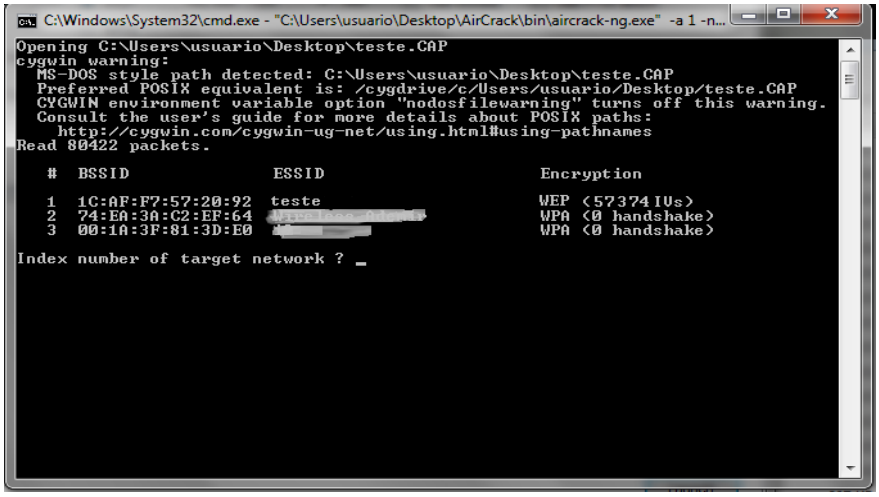


Figura 3. Tela do AirCrack.

5. Resultados

Dos resultados obtidos neste trabalho ao final dos testes (Tabela 2) foi verificado que para maior segurança contra quebra de chaves WEP, WPA e WPA2 seria a utilização de chaves WEP e WPA com mínimo de 8 dígitos e senha composta por números, letras e símbolos. Os primeiros testes com senhas fáceis (senha 123456789 e teste2012) foram facilmente descobertas pelo AirCrack. Já as duas outras senhas não foi obtido êxito na obtenção da senha, pois são senhas com números, símbolos e caracteres mistos.

Tabela 2. Resultados dos Testes de Senhas.

Senhas	WEP	WPA	WPA2
123456789	Sim	Sim	Não
teste2012	Sim	Sim	Não
t&st32o!%	Não	Não	Não
coapl67j92w	Não	Não	Não

Porém ainda o método, mas seguro seria o WPA2 que nos testes realizados não foi possível em nenhum momento à descoberta de senha. Pode-se observar que o uso de senhas seguras é de vital importância, sendo um dos mecanismos de segurança essenciais para obter-se uma proteção inicial e cabível a rede. O uso de senhas fracas, como foi testado, possibilita ao atacante conseguir a chave da rede de maneira muito fácil, apenas escutando o tráfego entre os dispositivos e fazendo uso de uma ferramenta de ataque de dicionário essa senha é descoberta facilmente. Vale ressaltar também que o sucesso da quebra de senha varia muito dependendo do tempo de captura de pacotes e do tráfego que esta ocorrendo na rede, e da *wordlist* que o programa utilizar para fazer os testes de força bruta.

6. Conclusão

Este trabalho abordou alguns problemas de segurança em redes sem fio ad hoc causado por várias técnicas de ataque. Foram propostos alguns métodos de prevenção de ataques a este modelo de rede como criptografia, certificados digitais, protocolos seguros entre outros.

Buscou-se fazer uma análise para identificar quais são as expectativas dos intrusos de uma rede, bem como identificar quais os principais ataques que podem ser usados em uma rede, e em seguida verificar os mecanismos de segurança necessários em uma rede, para reduzir estes riscos.

Foi verificado que o protocolo mais indicado para o usuário que desejar ter um nível maior de segurança deve ser o protocolo WPA2, ou se forem usados os outros protocolos que sejam elaboradas ou que utilizem softwares para a criação de senhas seguras, evitando assim possíveis intrusos à rede. Também vale ressaltar que para uma segurança maior em uma rede ad hoc se faz muito importante o uso de protocolos seguros, para possibilitar um roteamento seguro dos nós e também o uso de softwares como o EncryptOnClick, citado neste trabalho, para que a troca de mensagens entre a rede obtenha maior segurança, e que mesmo em casos de ataques, ocasionará que o atacante tenha maior dificuldade em descriptar a mensagem ou até mesmo nunca consiga fazê-lo. Portanto os dados críticos e informações sigilosas devem ser transmitidos utilizando métodos mais confiáveis, uma vez que não se consegue confiar na confidencialidade de qualquer informação que trafega na rede.

Espera-se que o levantamento bibliográfico e os testes realizados neste trabalho possam ser ampliados e utilizados no quesito de segurança. Que esta contribuição efetue mais um passo para assegurar maior confiabilidade em rede sem fio ad hoc.

Referências

Aad, I.; Hubaux, J.P.; Knightly, E. (2004). Denial of Service Resilience in Ad Hoc Networks, Proceedings of the 10th annual international conference on Mobile computing and networking, Philadelphia, USA.

Buiati, Fábio Mesquita. (2004). Protocolo seguro para auto-configuração de endereços de redes móveis ad hoc. Dissertação (Mestrado) – Universidade de Brasília. Brasília.

Carmona, Tadeu. (2005). Segredos da Espionagem Digital. São Paulo. SP.

Ehrsam, William Friedrich; Meyer, Carl H. W.; Powers, Robert Lowell; Smith, John Lynn; Tuchman, Walter Leonard. (1975). Product block cipher system for data security. U.S. Patent 3.962.539.

Hu, Y. C.; Perrig, A.; Johnson, D. B. (2003). Rushing attacks and defense in wireless ad hoc network routing protocols. Second ACM Workshop on Wireless Security (WiSe 03).

Murthy, C.; Mano, B. (2004). Ad Hoc wireless networks: architectures and protocols. Prentice Halll Professional Technical Reference.

Pinheiro, José Mauricio Santos. (2008). Assinatura e Certificado Digital. Curso Tecnólogo de Redes de Computadores. Volta Redonda, RJ.

Sêmola, Marcos. (2012). Saiba criar senhas seguras. Disponível em http://idgnow.uol.com.br/seguranca/firewall/idgcoluna.2006-08-18.5368218714/ Acesso em agosto de 2012.

Simon, S. (1999). The Code Book. Anchor Books. EUA.

Yi, Seung; Naldurg, Prasad; Kravets, Robin. (2001). A Security-Aware Routing Protocol for Wireless Ad Hoc Networks. Em ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001). University of Illinois atUrbana-Champaign, Long Beach, CA.

Yih-Chun, Hu; Johnson, David B.; Perrig, Adrian. (2002). SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, in the 4th IEEE Workshop on Mobile Computing Systems and Applications.